Annals of Mathematics **180** (2014), 621–652
http://dx.doi.org/10.4007/annals.2014.180.2.5

Sets of integers with no large sum-free subset

By Sean Eberhard, Ben Green, and Freddie Manners

Abstract

Answering a question of P. Erdős from 1965, we show that for every $\varepsilon > 0$ there is a set A of n integers with the following property: every set $A' \subset A$ with at least $\left(\frac{1}{3} + \varepsilon\right) n$ elements contains three distinct elements x, y, z with $x + y = z$.

Contents

1. Introduction

An old argument of Erdős [Erd65] shows that every set A of n nonzero integers contains a subset $A' \subset A$ of size $|A'| \geqslant \frac{1}{3}n$ which is *sum-free*, meaning $x + y = z$ has no solutions with $x, y, z \in A'$. The argument is simple: for $\theta \in \mathbb{R}/\mathbb{Z}$, the set A_θ of $x \in A$ such that $\frac{1}{3} < \{\theta x\} < \frac{2}{3}$ is clearly sum-free, and if θ is chosen uniformly at random, then the expected size of A_θ is $\frac{1}{3}n$, so $|A_\theta| \geqslant \frac{1}{3}n$ for some θ.

Let $f(n)$ be the largest k such that every set of n nonzero integers contains a sum-free subset of size k. Erdős's lower bound $f(n) \geqslant \frac{1}{3}n$ has not been much improved. As pointed out by Alon and Kleitman [AK90], Erdős's argument can be modified to show $f(n) \geqslant \frac{1}{3}(n+1)$: if $\theta \approx 0$, then A_θ is empty, so for some θ, we must actually have $|A_\theta| > \frac{1}{3}n$, so $|A_\theta| \geqslant \frac{1}{3}(n+1)$. The best

The second author is supported by ERC Starting Grant 274938, Approximate Algebraic Structures and Applications.

known lower bound is due to Bourgain [Bou97], who showed $f(n) \geqslant \frac{1}{3}(n+2)$ for $n \geqslant 3$ using an elaborate Fourier-analytic technique. In particular, it is unknown whether $f(n) \geqslant \frac{1}{3}n + \omega(n)$ for some $\omega(n) \to \infty$, though this seems likely.

In the opposite direction, considering the largest element of a subset $A \subset \{1, \dots, n\}$ gives an obvious upper bound of $f(n) \leqslant \frac{1}{2}(n+1)$. Improvements to this upper bound have all implicitly used the following device. Suppose that A is a set of size m with no sum-free subset of size larger than $f(m)$ and that B is a set of size n with no sum-free subset of size larger than $f(n)$. Then if $M \in \mathbb{N}$ is sufficiently large, $A \cup MB$ is a set of size $m+n$ with no sum-free subset of size larger than $f(m)+f(n)$, so $f(m+n) \leqslant f(m)+f(n)$. This condition is well known to imply that $f(n)/n$ converges to $\inf f(n)/n$, so to show $f(n) \leqslant cn + o(n)$ it suffices to find a single set A with no sum-free subset of size larger than $c|A|$. Let $\sigma = \lim f(n)/n = \inf f(n)/n$.

In [Erd65] Erdős mentioned that Hinton proved $\sigma \leqslant \frac{7}{15} \approx 0.467$. He also pointed out, attributing the construction to Klarner, that the set $A = \{2,3,4,5,6,8,10\}$ shows $\sigma \leqslant \frac{3}{7} \approx 0.429$. Using a set of size 29 Alon and Kleitman [AK90] showed $\sigma \leqslant \frac{12}{29} \approx 0.414$. In her thesis, Malouf [Mal94] (as well as Furedi, according to Guy [Guy04]) used $A = \{1,2,3,4,5,6,8,9,10,18\}$ to show $\sigma \leqslant \frac{2}{5} = 0.4$. Lewko [Lew10] used a set of size 28 to show $\frac{11}{28} \approx 0.393$. Incidentally, in a 1992 letter [Erd92] to Klarner, Erdős claims this same bound of $\frac{11}{28}$, but he includes no proof.

Recently, Alon [Alo13] showed that for each n, there exists m such that $f(m)/m < f(n)/n$. Thus there is no n such that $f(n)/n = \sigma$. Applying this to Lewko's bound, Alon showed, for instance, that $\sigma \leqslant \frac{11}{28} - \varepsilon$ for some $\varepsilon \approx 10^{-50000}$.

The question of whether $\sigma = \frac{1}{3}$ has been mentioned several times [AS08], [CL07], [Erd65], [Erd73], [Guy04], [Kol96]. Our purpose in this paper is to answer this question affirmatively.

THEOREM 1.1. *There is a set of n positive integers with no sum-free subset of size greater than $\frac{1}{3}n + o(n)$.*

By the above argument it suffices to find, for each $\varepsilon > 0$, a single set A with no sum-free subset of size larger than $\left(\frac{1}{3}+\varepsilon\right)|A|$. In fact we find a set A such that every subset A' of size larger than $\left(\frac{1}{3}+\varepsilon\right)|A|$ contains a solution to $x+y=z$ with $x \neq y$. This answers a further question asked in [Erd65].

One of the ingredients of our argument is a rough structure theorem for sets A satisfying conditions of the form $|A-A| < 4|A|$, which may be of independent interest. Specifically, if A is a set of integers with $|A-A| \leqslant (4-\varepsilon)|A|$, then A has density at least $\frac{1}{2} + c\varepsilon$ on some arithmetic progression of length $\gg_\varepsilon |A|$.

2. **Overview of the proof**

The proof of Theorem 1.1 breaks down naturally into several parts. We outline these informally here and give an indication of how they combine.

Note that there are certain local obstructions to a set A having the desired property, that is to say having no sum-free subset A' with $|A'| \geqslant (\frac{1}{3}+\varepsilon)|A|$. For instance, not more than $\left(\frac{1}{3}+\varepsilon\right)|A|$ of the elements of A can be odd, as these form a sum-free set in A. We think of this as an obstruction coming from $\mathbb{Z}/2\mathbb{Z}$. Not more than $\left(\frac{1}{3}+\varepsilon\right)|A|$ of the elements of A can be congruent to 2 or 3 (mod 5), an obstruction coming from $\mathbb{Z}/5\mathbb{Z}$. Similarly, not more than $\left(\frac{1}{3}+\varepsilon\right)|A|$ elements can be contained in an interval $[x, 2x)$, an obstruction coming from $\mathbb{R}$.

In fact we shall see in Section 3 that, in some sense, these restrictions coming from $\mathbb{Z}/Q\mathbb{Z}$ for various Q and from $\mathbb{R}$ are the *only* obstructions to A having the desired property.

To deal with these restrictions modulo Q and in $\mathbb{R}$ we consider a *weight function* $w : \mathbb{Z}/Q\mathbb{Z} \times [0,1] \to (0,\infty)$. Roughly speaking, we will define a set $A \subset \{1,\dots,N\}$ in such a way that a proportion $w(x,y)$ of the elements of A lie near the value yN and are congruent to x (mod Q). The "local" version of our problem is then roughly the following.

Problem 2.1 (Local problem). Find w such that if $A \subset \mathbb{Z}/Q\mathbb{Z} \times [0,1]$ is open and if $\int_A w(x,y)d\mu \geqslant \frac{1}{3}+\varepsilon$, then A contains a summing triple $x, y, x+y$. Here, μ denotes the uniform probability measure on $\mathbb{Z}/Q\mathbb{Z} \times [0,1]$.

In Section 3, we show that if w satisfies a slightly stronger version of Problem 2.1 (specifically Proposition 3.1), then a set A may be constructed from w as suggested above and Theorem 1.1 holds for this A. The actual construction of A, which involves a random selection argument, occurs at (3.3). A crucial tool in showing that A has the required property (and elsewhere in the paper) is the *arithmetic regularity lemma* due to the second-named author and Tao [GT10]. The statement of this is recalled in Lemma A.2.

The remainder of the paper is concerned with constructing the weight function w, that is to say with solving the local problem. This construction is rather involved. At its heart is an iterative argument (Lemma 5.2) allowing us to take a near-solution w such that if $\int_A w(x,y)d\mu \geqslant \alpha$, then A contains many summing triples, and improve it to a nearer-solution w', with corresponding parameter $\alpha' < \alpha$. The sequence $\alpha, \alpha', \alpha'', \dots$ obtained in this way converges rapidly to $\frac{1}{3}+\varepsilon$.

The main driver for this iterative argument is a structural result concerning sum-free (or almost sum-free) subsets of $\mathbb{Z}/Q\mathbb{Z} \times [0,1]$ with (uniform) measure just a little more than $\frac{1}{3}$. The crucial result here is Corollary 5.1,

which states that such sets "avoid zero," i.e., have very little mass on $H \times I$, where $H \leqslant \mathbb{Z}/Q\mathbb{Z}$ is a subgroup of small index and $I \subset [0,1]$ is a (not too small) open interval containing 0. Thus if w is chosen to have a lot of its mass concentrated on $H \times I$, then $\int_A w(x,y)d\mu$ is small whenever $\mu(A)$ is a bit more than $\frac{1}{3}$. The iteration then works in some sense by applying the same arguments to $A \cap (H \times I)$. In particular, the weight w we construct blows up near zero.

The basis of Corollary 5.1 is the simple observation that a sum-free subset A of $\mathbb{Z}/Q\mathbb{Z} \times [0,1]$ of measure more than $\frac{1}{3}$ must satisfy $\mu(A-A) < 4\mu(A)$. In Section 4 we prove a weak structure theorem for such sets, Corollary 4.2. This in turn is deduced from Theorem 4.1, which concerns sets of *integers* $A \subset \{1,\dots,N\}$ satisfying the same condition, that $|A-A| \leqslant 4|A| - \varepsilon N$. The conclusion is that they have density at least $\frac{1}{2} + c\varepsilon$ on a progression of length $\gg_\varepsilon N$, a result which may be of independent interest. (This theme is elaborated upon briefly in Section 6, which is independent of the rest of the paper.) The proof of Theorem 4.1 uses the arithmetic regularity lemma again, as well as an application of the Brunn-Minkowski inequality for open subsets of $\mathbb{R}^2$.

On account of our double application of the arithmetic regularity lemma, the $o(n)$ term in Theorem 1.1 is more or less ineffective. The authors believe that the main obstacle to a more effective $o(n)$ here is the use of the arithmetic regularity lemma in Section 4, which for all we know could be replaced by more elementary arguments.

Notation. We will introduce various pieces of notation as we go along. Throughout the paper we will also use the following at least somewhat standard notation.

The expression $O_{A_1,\dots,A_k}(1)$ denotes a constant which may depend on $A_1,\dots,A_k$, and $O_{A_1,\dots,A_k}(Y) = O_{A_1,\dots,A_k}(1)Y$. If we write $X \ll_{A_1,\dots A_k} Y$, then we mean that $X \leqslant O_{A_1,\dots,A_k}(Y)$. The expression $o_{A_1,A_2,\dots,A_k;N\to\infty}(1)$ denotes an expression which tends to zero as $N \to \infty$, the rate at which this happens being possibly dependent on the parameters $A_1,\dots,A_k$. On account of its relative ugliness we will use this notation sparingly.

If $f : \{1,\dots,N\} \to \mathbb{C}$ is a function, then we write

$$\|f\|_{\ell^p(N)} = \left(\frac{1}{N}\sum_{n\leqslant N}|f(n)|^p\right)^{1/p}.$$

We will use this only when $p = 1$ or 2. The normalisation, which is perhaps nonstandard, ensures that $\|f\|_{\ell^1(N)} \leqslant \|f\|_{\ell^2(N)} \leqslant \|f\|_\infty$.

3. The main argument

In this section we prove Theorem 1.1 assuming the existence of a weight function $w : \mathbb{Z}/Q\mathbb{Z} \times [0,1] \to (0,\infty)$, the role of which was briefly outlined

in the preceding section. Proposition 3.1 below, whose proof will occupy Sections 4 and 5, specifies the properties we shall require of w. Before stating this proposition we introduce some pieces of nomenclature.

We will view both $\mathbb{Z}/q\mathbb{Z} \times [0,1]$ and $\mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d$, for various integers q and d, as metric spaces. On each of these spaces X we place an "obvious" metric, namely a suitable product metric of the discrete metric on $\mathbb{Z}/q\mathbb{Z}$ and the Euclidean metrics on $[0,1]$ and on $(\mathbb{R}/\mathbb{Z})^d$. This allows us to talk about Lipschitz functions on X: if $F : X \to \mathbb{C}$, then we define $\|F\|_{\mathrm{Lip}}$ to be the infimum of all constants K such that $|F(x) - F(x')| \leqslant K\, d(x, x')$ for all $x, x' \in X$.

We will also put natural measures on these spaces X, which we will always denote by μ. (More precise notation such as $\mu_{\mathbb{Z}/q\mathbb{Z}\times[0,1]}$ would be rather ugly and unnecessary.) The measure μ will always be the product of the uniform probability measures on each factor, namely the uniform measure on $\mathbb{Z}/q\mathbb{Z}$ (which assigns mass $1/q$ to each point), and normalised Lebesgue measure on $[0,1]$ and the torus $(\mathbb{R}/\mathbb{Z})^d$.

Finally, if X is one of the sets above and if $\Psi : X \to \mathbb{C}$ is a function, then we define

$$T(\Psi) = \int \Psi(x)\Psi(x')\Psi(x+x')d\mu(x)d\mu(x'). \tag{3.1}$$

We also write $T(A) = T(1_A)$ if $A \subset X$. We use the same notation when $X = \{1, \dots, N\}$ with the uniform probability measure, so if $f : \{1, \dots, N\} \to \mathbb{C}$ is a function, we write

$$T(f) = \frac{1}{N^2} \sum_{n,n' \leqslant N} f(n)f(n')f(n+n'). \tag{3.2}$$

By a *weight function* we simply mean a function $w : \mathbb{Z}/Q\mathbb{Z} \times [0,1] \to (0,\infty)$ such that $\int w\, d\mu = 1$. If $\mathbb{T} = (\mathbb{R}/\mathbb{Z})^d$ and $Q \mid q$, then by $w \times 1_{\mathbb{T}} : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T} \to (0,\infty)$ we mean the function given by $(w \times 1_{\mathbb{T}})(x,y,z) = w(x \pmod Q, y)$.

Proposition 3.1. *Let $\varepsilon > 0$. Then there is an integer Q and a Lipschitz weight function $w : \mathbb{Z}/Q\mathbb{Z} \times [0,1] \to (0,\infty)$ with the following property. If $\mathbb{T} = (\mathbb{R}/\mathbb{Z})^d$ and $Q \mid q$, then for any continuous function $\Psi : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T} \to [0,1]$ such that $\int \Psi \cdot (w \times 1_{\mathbb{T}}) d\mu \geqslant \frac{1}{3} + \varepsilon$, we have $T(\Psi) \gg_\varepsilon 1$.*

Note that because Q and w depend only on ε, there are constants $c_1(\varepsilon)$ and $c_1'(\varepsilon)$ such that $0 < c_1(\varepsilon) \leqslant w(x) \leqslant c_1'(\varepsilon)$ for every $x \in \mathbb{Z}/Q\mathbb{Z} \times [0,1]$, and there is a constant $L(\varepsilon)$ such that $\|w\|_{\mathrm{Lip}} \leqslant L(\varepsilon)$. Choose $c_2(\varepsilon)$ to be the implied constant in Proposition 3.1 so that the conclusion of the proposition is that $T(\Psi) \geqslant c_2(\varepsilon)$.

The next lemma is quite standard. In it we encounter the notion of the Gowers U^2-norm $\|f\|_{U^2(N)}$, whose definition and relevant basic properties are recalled in Appendix A.

LEMMA 3.2. *Suppose that $p : \{1, \dots, N\} \to [0, 1]$ is a function. Then there is a set $A \subset \{1, \dots, N\}$ such that $\|1_A - p\|_{U^2(N)} \ll N^{-1/4}$.*

Proof. Choose A at random by including n in A with probability $p(n)$, these choices being independent for different n. We claim that A has the required property on average. Write $X_n = 1_A(n) - p(n)$. Then the random variables X_n are independent, bounded by 1, and of mean zero. We have

$$\|1_A - p\|^4_{U^2(N)} \ll \frac{1}{N^3} \sum_{n_1+n_2=n_3+n_4} X_{n_1} X_{n_2} X_{n_3} X_{n_4}.$$

The expected value of any term on the right-hand side with n_1, n_2, n_3, n_4 distinct is 0. This accounts for all except $O(N^2)$ terms, and so $\mathbb{E}\|1_A - p\|^4_{U^2(N)} \ll 1/N$. The result follows immediately. □

Fix $\varepsilon > 0$, and let Q and w be as in Proposition 3.1. By Lemma 3.2 there is a set A such that

$$1_A(n) = \frac{1}{\|w\|_\infty} w(n \,(\mathrm{mod}\, Q), n/N) + g_{\mathrm{unf}}(n), \tag{3.3}$$

where $\|g_{\mathrm{unf}}\|_{U^2(N)} = o(1)$. Since $\int w = 1$ and w has Lipschitz constant $O_\varepsilon(1)$, it follows from Lemmas A.6 and A.8 that

$$\frac{|A|}{N} = \frac{1}{\|w\|_\infty} + o_{\varepsilon; N\to\infty}(1). \tag{3.4}$$

We shall show that this set A satisfies Theorem 1.1.

THEOREM 3.3. *Let $N > N_0(\varepsilon)$ be sufficiently large, let A be the set just constructed, and suppose $A' \subset A$ has no solutions to $x + y = z$. Then $|A'| \leqslant (\frac{1}{3} + 2\varepsilon)|A|$.*

Proof. Let $A' \subset A$ be a subset of A such that $|A'| \geqslant (\frac{1}{3} + 2\varepsilon)|A|$. We apply the *arithmetic regularity lemma* [GT10] to $1_{A'}$. The statement of this lemma is recalled in Lemma A.2. Let

$$\delta = \min\left(\frac{c_2(\varepsilon)c_1(\varepsilon)^3}{20c_1'(\varepsilon)^3}, \frac{\varepsilon}{4c_1'(\varepsilon)}, \frac{1}{100}\right), \tag{3.5}$$

and let $\mathcal{F} : \mathbb{N} \to \mathbb{R}_+$ be a growth function, depending on ε, to be specified later. Applying the regularity lemma with parameter $\frac{1}{8}\delta^4$ and growth function $\mathcal{F}$, we obtain an integer $M \ll_{\varepsilon,\mathcal{F}} 1$ and a decomposition

$$1_{A'} = f_{\mathrm{tor}} + f_{\mathrm{sml}} + f_{\mathrm{unf}}, \tag{3.6}$$

where $\|f_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant \delta^4/16$, $\|f_{\mathrm{unf}}\|_{U^2(N)} \leqslant 1/\mathcal{F}(M)$ and

$$f_{\mathrm{tor}}(n) = F(n \,(\mathrm{mod}\ q), n/N, \theta n) \tag{3.7}$$

for some M-Lipschitz $F : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to [0,1]$ and some $(\mathcal{F}(M), N)$-irrational $\theta \in (\mathbb{R}/\mathbb{Z})^d$, where $q, d \leqslant M$. For the rest of this section, write $\mathbb{T} = (\mathbb{R}/\mathbb{Z})^d$.

We may regard the $\bmod q$ dependence of f_{tor} as $\bmod qQ$ dependence instead without affecting the Lipschitz constant of F. Relabelling, we may assume that $Q \mid q$ and $q \ll_\varepsilon M$.

The property that A' is a subset of A manifests as an approximate upper bound for F in terms of the weight w. As the next lemma shows, by absorbing the error into f_{sml} we can assume that $F \leqslant \|w\|_\infty^{-1}(w \times 1_{\mathbb{T}})$ pointwise.

Lemma 3.4. *Suppose $\mathcal{F}$ grows sufficiently rapidly depending on ε and $N \geqslant N_0(\varepsilon, \mathcal{F})$ is sufficiently large. Then we can modify the decomposition* (3.6) *to $1_{A'} = f'_{\mathrm{tor}} + f'_{\mathrm{sml}} + f_{\mathrm{unf}}$, where $\|f'_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant \delta^2$ and $f'_{\mathrm{tor}} = F'(n \,(\mathrm{mod}\ q), n/N, \theta n)$ for some $O_\varepsilon(M)$-Lipschitz function $F' : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to [0,1]$ such that $F' \leqslant \|w\|_\infty^{-1}(w \times 1_{\mathbb{T}})$ pointwise.*

Proof. Let $F' = \min\left(F, \|w\|_\infty^{-1}(w \times 1_{\mathbb{T}})\right)$, $f'_{\mathrm{tor}}(n) = F'(n \,(\mathrm{mod}\ q), n/N, \theta n)$, and $h = f_{\mathrm{tor}} - f'_{\mathrm{tor}}$. It suffices to prove $\|h\|_{\ell^2(N)} \leqslant \frac{1}{2}\delta^2$.

Now substituting in the definition of h, we have

$$\begin{aligned}\|h\|_{\ell^2(N)}^2 &= \mathbb{E}_{n \leqslant N} h(n)^2 \\ &= \mathbb{E}_{n \leqslant N} h(n) \left(f_{\mathrm{tor}}(n) - \|w\|_\infty^{-1}(w \times 1_{\mathbb{T}})(n \,(\mathrm{mod}\ Q), n/N, \theta n)\right).\end{aligned}$$

Recalling that $1_{A'} = f_{\mathrm{tor}} + f_{\mathrm{sml}} + f_{\mathrm{unf}}$ and that

$$1_A(n) = \|w\|_\infty^{-1}(w \times 1_{\mathbb{T}})(n \,(\mathrm{mod}\ Q), n/N, \theta n) + g_{\mathrm{unf}}(n),$$

we may rewrite this as

$$\|h\|_{\ell^2(N)}^2 = \mathbb{E}_{n \leqslant N} h(n)\big(- (1_A(n) - 1_{A'}(n)) - f_{\mathrm{sml}}(n) + (-f_{\mathrm{unf}}(n) + g_{\mathrm{unf}}(n))\big).$$

To estimate this, we split into three terms as suggested by the bracketing. The first term is $\leqslant 0$ since $h \geqslant 0$ and $1_{A'} \leqslant 1_A$ pointwise. The second term may be estimated by the Cauchy-Schwarz inequality, remembering that $h \leqslant 1$ pointwise:

$$\mathbb{E}_{n \leqslant N} h(n) f_{\mathrm{sml}}(n) \leqslant \|f_{\mathrm{sml}}\|_{\ell^2(N)} \|h\|_{\ell^2(N)} \leqslant \|f_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant \tfrac{1}{8}\delta^4.$$

Finally, by Lemma A.9, the third term is extremely tiny if $\mathcal{F}$ grows quickly enough. Putting all this together gives $\|h\|_{\ell^2(N)}^2 \leqslant \frac{1}{4}\delta^4$, and the lemma follows. □

Relabelling f'_{tor} as f_{tor}, f'_{sml} as f_{sml} and F' as F, we may thus assume that (3.6) and (3.7) hold with $\|f_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant \delta^2$, $\|f_{\mathrm{unf}}\|_{U^2(N)} \leqslant 1/\mathcal{F}(M)$ and

some $O_\varepsilon(M)$-Lipschitz function $F : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to [0,1]$ such that $F \leqslant \|w\|_\infty^{-1}(w \times 1_{\mathbb{T}})$ pointwise, so in other words

$$F = \|w\|_\infty^{-1}\Psi \cdot (w \times 1_{\mathbb{T}})$$

for some continuous $\Psi : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T} \to [0,1]$. By combining this decomposition with Proposition 3.1 and the counting lemmata in the appendix we can finish the proof of Theorem 3.3.

Using (3.6), Cauchy-Schwarz and Lemma A.8, we have

$$\begin{aligned}\frac{|A'|}{N} &= \mathbb{E}_{n\leqslant N}F(n \,(\mathrm{mod}\ q), n/N, \theta n) + \mathbb{E}_{n\leqslant N}f_{\mathrm{sml}}(n) + \mathbb{E}_{n\leqslant N}f_{\mathrm{unf}}(n)\\ &\leqslant \mathbb{E}_{n\leqslant N}F(n \,(\mathrm{mod}\ q), n/N, \theta n) + 2\delta.\end{aligned}$$

Thus by the Lipschitz property of F, the irrationality of θ and Lemma A.4 we have

$$\frac{|A'|}{N} \leqslant \int F\,d\mu + 3\delta = \frac{1}{\|w\|_\infty}\int \Psi \cdot (w \times 1_{\mathbb{T}})\,d\mu + 3\delta.$$

If $N > N_0(\varepsilon)$ is large enough, then (3.4) implies that

$$\frac{|A|}{N} \geqslant \frac{1}{\|w\|_\infty} - \delta.$$

Assuming that $|A'| \geqslant (\frac{1}{3} + 2\varepsilon)|A|$, and recalling that δ was chosen so that $\delta \leqslant \varepsilon/4c_1'(\varepsilon)$, it follows from these two observations that

$$\int \Psi \cdot (w \times 1_{\mathbb{T}})\,d\mu \geqslant \tfrac{1}{3} + \varepsilon.$$

Proposition 3.1 now implies $T(\Psi) \geqslant c_2(\varepsilon)$, so by the pointwise bounds $c_1(\varepsilon) \leqslant w \leqslant c_1'(\varepsilon)$, we have

$$T(F) = T\left(\|w\|_\infty^{-1}\Psi \cdot (w \times 1_{\mathbb{T}})\right) \geqslant \frac{c_2(\varepsilon)c_1(\varepsilon)^3}{c_1'(\varepsilon)^3}.$$

Write $c_3(\varepsilon)$ for this latter quantity. By Lemma A.5 it follows that (if $\mathcal{F}$ grows sufficiently rapidly and N is big enough)

$$T(f_{\mathrm{tor}}) \geqslant T(F) - \tfrac{1}{2}c_3(\varepsilon) \geqslant \tfrac{1}{2}c_3(\varepsilon).$$

Finally, from Lemma A.10 together with the bounds

$$\|f_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant \delta^2, \quad \|f_{\mathrm{unf}}\|_{U^2(N)} \leqslant 1/\mathcal{F}(M)$$

and the choice of δ, we conclude that

$$T(A') = T(f_{\mathrm{tor}} + f_{\mathrm{sml}} + f_{\mathrm{unf}}) \geqslant \tfrac{1}{4}c_3(\varepsilon).$$

In particular, A' has $\gg_\varepsilon N^2$ solutions to $x + y = z$ with $x \neq y$. This concludes the proof of Theorem 3.3 and hence of Theorem 1.1 (modulo the results of the next two sections and the appendix). □

4. **Sets of doubling less than 4**

In this section we study sets A satisfying $|A-A| \leqslant (4-\varepsilon)|A|$ or various related but slightly weaker conditions. Our particular aim is to prove Corollary 4.2 below, which will be crucial in the construction of the weight function w in Proposition 3.1. However, some special cases and corollaries of our main result may be of independent interest, and we highlight these in Section 6.

We remind the reader of our convention, mentioned at the beginning of Section 3, that the "natural" uniform measure on a space X, whether it be $\mathbb{Z}/q\mathbb{Z} \times [0,1]$, $\mathbb{T}$, $\{1,\dots,N\}$, etc., is denoted μ. When we want to refer to the size (i.e., counting measure) of a set A, particularly a subset $A \subset \{1,\dots,N\}$, we will use the notation $|A|$.

If X is a space endowed with a measure μ (one of the above) then, as usual, we define the *convolution* of two sufficiently nice functions $f_1, f_2 : X \to \mathbb{C}$ by $f_1 * f_2(x) = \int f_1(y) f_2(x-y) d\mu(y)$. In the case $X = \{1,\dots,N\}$ we allow f_1, f_2 and $f_1 * f_2$ to be defined on $\mathbb{Z}\backslash\{1,\dots,N\}$ as well, but we continue to use the measure μ which gives each point a mass $1/N$. If A is a set and t is a real number then, we define $\mathrm{D}_t(A) = \{x : 1_A * 1_{-A}(x) \geqslant t\}$, the set of "$t$-popular differences" of A. Note that $\mathrm{D}_t(A) \subset A - A$ if $t > 0$.

The main result of this section is the following.

THEOREM 4.1. *For every $\varepsilon > 0$, there is some $\delta \gg_\varepsilon 1$ such that the following holds. If $A \subset \{1,\dots,N\}$ is a set with $|\mathrm{D}_\delta(A)| \leqslant 4|A| - \varepsilon N$, then there is an arithmetic progression $P \subset \{1,\dots,N\}$ of length $|P| \gg_\varepsilon N$ such that $|A \cap P| \geqslant (\frac{1}{2} + \frac{1}{5}\varepsilon)|P|$.*

The reader may find it helpful to think of the hypothesis $|\mathrm{D}_\delta(A)| \leqslant 4|A| - \varepsilon N$ as a slight weakening of $|A-A| \leqslant 4|A| - \varepsilon N$. To motivate this theorem, we first derive the corollary which will enable us in Section 5 to construct a weight function satisfying Proposition 3.1.

COROLLARY 4.2. *Let $\varepsilon > 0$ and $q \in \mathbb{N}$. Then there is $\delta \gg_\varepsilon 1$ such that if $A \subset \mathbb{Z}/q\mathbb{Z} \times [0,1]$ is an open set with $\mu(\mathrm{D}_\delta(A)) \leqslant 4\mu(A) - \varepsilon$, then there is a subgroup $H \leqslant \mathbb{Z}/q\mathbb{Z}$ of index $[\mathbb{Z}/q\mathbb{Z} : H] \ll_\varepsilon 1$, an element $x \in \mathbb{Z}/q\mathbb{Z}$, and a subinterval I of $[0,1]$ of length $\mu(I) \gg_\varepsilon 1$ such that A has density at least $\frac{1}{2} + \frac{1}{7}\varepsilon$ on $(x+H) \times I$.*

Proof. Let $A \subset \mathbb{Z}/q\mathbb{Z} \times [0,1]$ be an open set such that $\mu(\mathrm{D}_\delta(A)) \leqslant 4\mu(A) - \varepsilon$. Then for some positive integer K depending on ε and A, there is a subset $A' \subset A$, a union of sets of the form $\{a\} \times \left(\frac{i-1}{K}, \frac{i}{K}\right)$, such that $\mu(A') \geqslant \mu(A) - \frac{1}{32}\varepsilon$. (Note that none of our final quantities can or will depend on K.) Then since $A' \subset A$,

$$\mu(\mathrm{D}_\delta(A')) \leqslant \mu(\mathrm{D}_\delta(A)) \leqslant 4\mu(A) - \varepsilon \leqslant 4\mu(A') - \tfrac{7}{8}\varepsilon.$$

With an abuse of notation rename A' simply A.

For N a large multiple of q, consider the map $\pi : \{1, \dots, N\} \to \mathbb{Z}/q\mathbb{Z} \times [0,1]$ defined by $\pi(n) = (n \pmod q, n/N)$. It is clear (see Lemma A.6) that for large N, the image of $\{1, \dots, N\}$ under π is highly equidistributed in $\mathbb{Z}/q\mathbb{Z} \times [0,1]$. In particular, we have

$$\mathbb{E}_{n \leqslant N} \psi(\pi(n)) = \int_{\mathbb{Z}/q\mathbb{Z} \times [0,1]} \psi(x) d\mu(x) + o_{K;N\to\infty}(1) \tag{4.1}$$

whenever ψ is "nice"; in particular, whenever ψ has one of the following three forms:

(i) the characteristic function of a union of sets $\{a\} \times \left(\frac{i-1}{K}, \frac{i}{K}\right)$,
(ii) the characteristic function of the intersection of a set of type (i) with a translate of another set of type (i),
(iii) a continuous function with Lipschitz constant K.

(Note that, conditional on one of these hypotheses, the quantity $o_{K;N\to\infty}(1)$ is asserted to be independent of ψ.)

In particular, if $B = \pi^{-1}(A)$, by case (i) of (4.1) we have[1]

$$\mu(B) = \mathbb{E}_{n \leqslant N} 1_A(\pi(n)) = \mu(A) + o_{K;N\to\infty}(1). \tag{4.2}$$

Furthermore, we claim that

$$\mu(\mathrm{D}_{2\delta}(B)) \leqslant \mu(\mathrm{D}_{\delta}(A)) + o_{K,\delta;N\to\infty}(1). \tag{4.3}$$

This is a little trickier to justify. First note that by case (ii) of (4.1),

$$\begin{aligned} 1_B * 1_{-B}(n) &= \mathbb{E}_{m \leqslant N} 1_A(\pi(m))\, 1_A(\pi(m) - \pi(n)) \\ &= \int_{\mathbb{Z}/q\mathbb{Z} \times [0,1]} 1_A(x)\, 1_A(x - \pi(n)) d\mu(x) + o_{K;N\to\infty}(1) \\ &= 1_A * 1_{-A}(\pi(n)) + o_{K;N\to\infty}(1). \end{aligned}$$

In particular, if $N > N_0(K, \delta)$ is large enough, then if $n \in \mathrm{D}_{2\delta}(B)$, then $\pi(n) \in \mathrm{D}_{3\delta/2}(A)$, that is to say if $1_B * 1_{-B}(n) \geqslant 2\delta$, then $1_A * 1_{-A}(\pi(n)) \geqslant 3\delta/2$. Now let $\chi : [0,1] \to [0,1]$ be a function such that $\chi(x) = 1$ for $x \geqslant 3\delta/2$, $\chi(x) = 0$ for $x \leqslant \delta$, and χ has Lipschitz constant $O(1/\delta)$. What we have shown implies that if $N > N_0(K, \delta)$, then

$$\mathbb{E}_{n \leqslant N} \chi \circ (1_A * 1_{-A})(\pi(n)) \geqslant \mu(\mathrm{D}_{2\delta}(B)).$$

Now $1_A * 1_{-A}$ has Lipschitz constant at most K, so $\chi \circ (1_A * 1_{-A})$ has Lipschitz constant at most $O(K/\delta)$. Thus by case (iii) of (4.1),

$$\begin{aligned} \mathbb{E}_{n \leqslant N} \chi \circ (1_A * 1_{-A})(\pi(n)) &= \int_{\mathbb{Z}/q\mathbb{Z} \times [0,1]} \chi \circ (1_A * 1_A)(x) d\mu(x) + o_{K,\delta;N\to\infty}(1) \\ &\leqslant \mu(\mathrm{D}_{\delta}(A)) + o_{K,\delta;N\to\infty}(1). \end{aligned}$$

This completes the justification of the claim (4.3).

[1]Note that this would not be true if A were an arbitrary open set, for example if A were a set of small measure containing $\mathbb{Z}/q\mathbb{Z} \times (\mathbb{Q} \cap [0,1])$.

Comparing (4.2) and (4.3) and recalling the hypothesis that $\mu(\mathrm{D}_\delta(A)) \leqslant 4\mu(A) - \frac{7}{8}\varepsilon$, we see that if $N > N_0(K, \varepsilon, \delta)$ is large enough, then $|\mathrm{D}_{2\delta}(B)| \leqslant 4|B| - \frac{5}{6}\varepsilon N$. Choose $\delta \gg_\varepsilon 1$ small enough that Theorem 4.1 holds with 2δ in place of δ and $\frac{5}{6}\varepsilon$ in place of ε. Then there is a progression $P \subset \{1, \dots, N\}$ of length $L = |P| \gg_\varepsilon N$, say $P = \{x_0 + \lambda d : \lambda = 0, 1, \dots, L-1\}$, such that $|B \cap P| \geqslant (\frac{1}{2} + \frac{1}{6}\varepsilon)|P|$.

It is readily seen that the image $\pi(P)$ is highly equidistributed (as $N \to \infty$) on $\pi(x_0) + H \times I$, where $H \leqslant \mathbb{Z}/q\mathbb{Z}$ is the subgroup of index $\gcd(q, d) \leqslant d \ll_\varepsilon 1$, and $I = \left[0, \frac{dL}{N}\right]$ has length $\frac{dL}{N} \gg_{\varepsilon,\alpha} 1$, so by a variant of (4.1), case (i), we have

$$\frac{|B \cap P|}{|P|} = \frac{\mu(A \cap (\pi(x_0) + H \times I))}{\mu(\pi(x_0) + H \times I)} + o_{\varepsilon,K;N\to\infty}(1).$$

Therefore, if N is large enough depending on ε and K,

$$\mu(A \cap (\pi(x_0) + H \times I)) \geqslant (\tfrac{1}{2} + \tfrac{1}{7}\varepsilon)\mu(\pi(x_0) + H \times I). \qquad \square$$

We devote the rest of this section to the proof of Theorem 4.1. The argument uses several nontrivial ingredients: the arithmetic regularity lemma (Lemma A.2) again, a "stability" version of Kemperman's theorem due to Tao [Taoa], [Taob, §3.2] and the Brunn-Minkowski theorem. We begin with the regularity lemma. Let the hypotheses be as in Theorem 4.1; thus $A \subseteq \{1, \dots, N\}$ is a set with $|\mathrm{D}_\delta(A)| \leqslant 4|A| - \varepsilon N$. Let $\mathcal{F} : \mathbb{N} \to \mathbb{R}_+$ be a growth function depending on ε to be chosen later. Let $\tilde{\varepsilon} = \min\left(\varepsilon, \frac{1}{1000}\right)$. Then there is some $M \ll_{\varepsilon,\mathcal{F}} 1$ such that

$$1_A = f_{\mathrm{tor}} + f_{\mathrm{sml}} + f_{\mathrm{unf}},$$

where $\|f_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant \tilde{\varepsilon}^{10}$, $\|f_{\mathrm{unf}}\|_{U^2(N)} \leqslant 1/\mathcal{F}(M)$ and

$$f_{\mathrm{tor}} = F(n \,(\mathrm{mod}\ q), n/N, \theta n)$$

for some $F : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to [0,1]$ such that $q, d, \|F\|_{\mathrm{Lip}} \leqslant M$ and for some $(\mathcal{F}(M), N)$-irrational $\theta \in (\mathbb{R}/\mathbb{Z})^d$. As usual we abbreviate $(\mathbb{R}/\mathbb{Z})^d$ to $\mathbb{T}$.

Let $\tilde{M} = \lceil \tilde{\varepsilon}^{-10} M \rceil$, and for $a \in \mathbb{Z}/q\mathbb{Z}$ and $i \in \{1, \dots, \tilde{M}\}$, consider the progressions

$$I_{a,i} = \left\{ n \in \left(\frac{(i-1)N}{\tilde{M}}, \frac{iN}{\tilde{M}} \right] : n \equiv a \ (\mathrm{mod}\ q) \right\}.$$

Define $F_{a,i} : \mathbb{T} \to [0,1]$ by $F_{a,i}(x) = F(a, i/\tilde{M}, x)$. Then since F is M-Lipschitz, $F_{a,i}$ is M-Lipschitz and f_{tor} differs by at most $\tilde{\varepsilon}^{10}$ from a function f_{struct} which we define by

$$f_{\mathrm{struct}}(n) = \sum_{a \,(\mathrm{mod}\, q)} \sum_{i=1}^{\tilde{M}} 1_{I_{a,i}}(n) F_{a,i}(\theta n).$$

Absorbing the error of $\tilde{\varepsilon}^{10}$ into f_{sml}, we have a decomposition

$$1_A = f_{\mathrm{struct}} + f'_{\mathrm{sml}} + f_{\mathrm{unf}},$$

where $\|f'_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant 2\tilde{\varepsilon}^{10}$ and $\|f_{\mathrm{unf}}\|_{U^2(N)} \leqslant 1/\mathcal{F}(M)$. Now given an arbitrary growth function $\tilde{\mathcal{F}}$ depending on ε, we may choose $\mathcal{F}$ to grow sufficiently rapidly depending on ε so that $\mathcal{F}(M) \geqslant \tilde{\mathcal{F}}(\tilde{M})$, whence $\|f_{\mathrm{unf}}\|_{U^2(N)} \leqslant 1/\tilde{\mathcal{F}}(\tilde{M})$ and θ is $(\tilde{\mathcal{F}}(\tilde{M}), N)$-irrational. Clearly we may now rename $\tilde{M}$ as M, f'_{sml} as f_{sml} and $\tilde{\mathcal{F}}$ as $\mathcal{F}$, so that

$$1_A = f_{\mathrm{struct}} + f_{\mathrm{sml}} + f_{\mathrm{unf}}, \tag{4.4}$$

where $\|f_{\mathrm{sml}}\|_{\ell^2(N)} \leqslant 2\tilde{\varepsilon}^{10}$, $\|f_{\mathrm{unf}}\|_{U^2(N)} \leqslant 1/\mathcal{F}(M)$,

$$f_{\mathrm{struct}}(n) = \sum_{a (\mathrm{mod}\, q)} \sum_{i=1}^{M} 1_{I_{a,i}}(n) F_{a,i}(\theta n),$$

and

$$I_{a,i} = \left\{ n \in \left(\frac{(i-1)N}{M}, \frac{iN}{M} \right] : n \equiv a \,(\mathrm{mod}\ q) \right\}.$$

Write $\alpha(a,i)$ for the density of A on $I_{a,i}$. We will show that $\alpha(a,i) \geqslant \frac{1}{2} + \frac{1}{5}\varepsilon$ for some (a,i). Note that while $|I_{a,i}|$ need not be exactly N/qM, at worst it differs from N/qM by 2. We will deal with this small discrepancy taking $N \geqslant N_0(\varepsilon)$ sufficiently large depending on ε. This is acceptable: if $N < N_0(\varepsilon)$, then Theorem 4.1 is trivially satisfied by taking P to be a suitable singleton.[2]

We proceed by examining how the behaviour of 1_A is modelled by the more "structured" functions $F_{a,i}(\theta n)$, which in view of the decomposition (4.4) involves estimating the effect of f_{sml} and f_{unf}. The term f_{sml} is the more troublesome of the two. The following simple lemma is useful here.

LEMMA 4.3. *For all $(a,i) \in \mathbb{Z}/q\mathbb{Z} \times \{1,\dots,M\}$ outside an exceptional subset E of size at most $\tilde{\varepsilon}^4 qM$, we have $\mathbb{E}_{n \in I_{a,i}} |f_{\mathrm{sml}}(n)| \leqslant \tilde{\varepsilon}^5$.*

Proof. If this were not the case, we would have

$$\mathbb{E}_{n \leqslant N} |f_{\mathrm{sml}}(n)| > \frac{1}{N} \left(\frac{N}{qM} - 2 \right) qM\tilde{\varepsilon}^9 \geqslant 2\tilde{\varepsilon}^{10},$$

whence by Cauchy-Schwarz $\|f_{\mathrm{sml}}\|_{\ell^2(N)} > 2\tilde{\varepsilon}^{10}$, a contradiction. □

LEMMA 4.4. *Let E be as in the preceding lemma. For all $(a,i) \in \mathbb{Z}/q\mathbb{Z} \times \{1,\dots,M\}$ outside E, we have $\int_{\mathbb{T}} F_{a,i} \geqslant \alpha(a,i) - \tilde{\varepsilon}^4$.*

Proof. By Lemma A.8 the average of f_{unf} over any progression $I_{a,i}$ is less than $\frac{1}{3}\tilde{\varepsilon}^4$ provided that $\mathcal{F}$ grows sufficiently rapidly, and by Lemma 4.3 for all

[2]Alternatively, one could arrange that N is always multiple of qM, in which case $|I_{a,i}|$ is exactly N/qM.

$(a,i) \notin E$, the average of f_{sml} on $I_{a,i}$ is also at most $\frac{1}{3}\tilde{\varepsilon}^4$. Thus if $(a,i) \notin E$, we have

$$\alpha(a,i) = \mathbb{E}_{n\in I_{a,i}} 1_A(n) \leqslant \mathbb{E}_{n\in I_{a,i}} F_{a,i}(\theta n) + \tfrac{2}{3}\tilde{\varepsilon}^4 \leqslant \int_{\mathbb{T}} F_{a,i} + \tilde{\varepsilon}^4.$$

Assuming that $\mathcal{F}$ grows sufficiently rapidly, the last step follows from the $(\mathcal{F}(M), N)$-irrationality of θ and Lemma A.3. □

We need a slightly technical lemma concerning level sets of Lipschitz functions.

LEMMA 4.5. *Let $\eta > 0$. If $\mathcal{F}$ grows sufficiently quickly depending on η, then the following is true. If $F : \mathbb{T} \to [0,1]$ is M-Lipschitz, θ is $(\mathcal{F}(M), N)$-irrational and $I \subset \{1,\dots,N\}$ is any progression of length at least N/M^2, then the proportion of $n \in I$ such that $F(n\theta) > \eta$ is at least $\mu(\{x \in \mathbb{T} : F(x) > 2\eta\}) - \eta$.*

Proof. We want to compute $\mathbb{E}_{n\in I}\chi \circ F(n\theta)$, where χ is the cutoff $1_{x\geqslant\eta}$. Replace χ by a function $\tilde{\chi}$ with $\|\tilde{\chi}\|_{\mathrm{Lip}} \ll 1/\eta$ such that $\tilde{\chi}(x) = 0$ for $x < \eta$ and $\tilde{\chi}(x) = 1$ for $x \geqslant 2\eta$. Then $\mathbb{E}_{n\in I}\chi \circ F(n\theta) \geqslant \mathbb{E}_{n\in I}\tilde{\chi} \circ F(n\theta)$. However the function $\tilde{\chi}\circ F$ is Lipschitz with $\|\tilde{\chi}\circ F\|_{\mathrm{Lip}} \ll M/\eta$ and so, if $\mathcal{F}$ grows sufficiently rapidly, since θ is so irrational, Lemma A.3 implies that $\mathbb{E}_{n\in I}\tilde{\chi} \circ F(n\theta) \geqslant \int_{\mathbb{T}} \tilde{\chi} \circ F - \eta$. On the other hand, the integral here is at least the measure of $\{x : F(x) \geqslant 2\eta\}$. □

The following lemma has more meat to it and is a crucial ingredient of our argument. It encodes the fact that if B_1, B_2 are open subsets of a torus, then the measure $\mu(B_1 + B_2)$ is at least $\min(\mu(B_1) + \mu(B_2), 1)$, a 1953 result due to Macbeath [Mac53]. More accurately, we require a "robust" version of this result which was obtained in [GR05, Prop. 6.1], and recently given the following elegant formulation by Tao [Taob]: if $S_1, S_2 \subset \mathbb{T}$ are open and $0 \leqslant t \leqslant \min(\mu(S_1), \mu(S_2))$, then

$$\int_{\mathbb{T}} \min(1_{S_1} * 1_{S_2}, t)\, d\mu \geqslant t \min(\mu(S_1) + \mu(S_2) - t, 1). \tag{4.5}$$

LEMMA 4.6. *Let $0 < \eta < 1$, and suppose that $F_1, F_2 : \mathbb{T} \to [0,1]$ are M-Lipschitz functions such that $\int F_1, \int F_2 \geqslant 2\eta^{1/6}$. Then the measure of the set of x for which $F_1 * F_2(x) \geqslant \eta$ is at least $\min\left(\int F_1 + \int F_2, 1\right) - 4\eta^{1/6}$.*

Proof. Let $S_i = \{x : F_i(x) > \eta^{1/3}\}$ for $i = 1, 2$. Clearly $\mu(S_i) \geqslant \int F_i - \eta^{1/3}$ so, in particular, $\mu(S_1), \mu(S_2) \geqslant \eta^{1/6}$. By (4.5) we therefore have

$$\int_{\mathbb{T}} \frac{\min(1_{S_1} * 1_{S_2}(x), \eta^{1/6})}{\eta^{1/6}} dx \geqslant \min(\mu(S_1) + \mu(S_2) - \eta^{1/6}, 1).$$

Writing X for the set of $x \in \mathbb{T}$ such that $1_{S_1} * 1_{S_2}(x) \geqslant \eta^{1/3}$, the left-hand side here is bounded by $\mu(X) + \eta^{1/6}$, so $\mu(X) \geqslant \min(\int F_1 + \int F_2, 1) - 4\eta^{1/6}$. On the other hand, for $x \in X$, we certainly have $F_1 * F_2(x) \geqslant \eta^{2/3} 1_{S_1} * 1_{S_2}(x) \geqslant \eta$. □

LEMMA 4.7. *If $(a,i),(a',i') \notin E$ and $\alpha(a,i),\ \alpha(a',i') \geqslant 2\tilde{\varepsilon}^2$, then*

$$|\operatorname{D}_{\tilde{\varepsilon}^{20}/10M^2}(A) \cap I_{a-a',i-i'}| \geqslant \frac{N}{qM}\min(\alpha(a,i)+\alpha(a',i'),1) - \frac{10\tilde{\varepsilon}^2 N}{qM},$$

and the same bound holds for $|\operatorname{D}_{\tilde{\varepsilon}^{20}/10M^2}(A) \cap I_{a-a',i-i'+1}|$.

If f is a function on an abelian group, we write f° for the function $f^\circ(x) = f(-x)$.

Proof. Dealing with $I_{a-a',i-i'}$ and $I_{a-a',i-i'+1}$ are similar, so we focus on the former. By Lemma 4.4 then, it suffices to prove

$$|\operatorname{D}_{\tilde{\varepsilon}^{20}/10M^2}(A) \cap I_{a-a',i-i'}| \geqslant \frac{N}{qM}\min\Big(\int F_{a,i} + \int F_{a',i'}, 1\Big) - \frac{8\tilde{\varepsilon}^2 N}{qM}$$

for (a,i) and (a',i') outside E and such that $\int F_{a,i}, \int F_{a',i'} \geqslant \tilde{\varepsilon}^2$.

For all except maybe $2\tilde{\varepsilon}^2 N/qM$ values of $d \in I_{a-a',i-i'}$ (those near the left ends),

$$|I_{a,i} \cap (d + I_{a',i'})| \geqslant \frac{\tilde{\varepsilon}^2 N}{qM}, \tag{4.6}$$

and for any such d we have, if $\mathcal{F}$ is sufficiently rapidly growing,

$$\begin{aligned} f_{\mathrm{struct}}|_{I_{a,i}} * f^\circ_{\mathrm{struct}}|_{I_{a',i'}}(d) &= \sum_{n \in I_{a,i} \cap (d+I_{a',i'})} F_{a,i}(\theta n)\, F_{a',i'}(\theta(d+n)) \\ &\geqslant |I_{a,i} \cap (d+I_{a',i'})| \left(F_{a,i} * F^\circ_{a',i'}(\theta d) - \tfrac{1}{4}\tilde{\varepsilon}^{12}\right). \end{aligned} \tag{4.7}$$

Here we used the $(\mathcal{F}(M),N)$-irrationality of θ, Lemma A.3 and the fact that the product of two M-Lipschitz functions, each of which is bounded pointwise by 1, is $2M$-Lipschitz. By Lemma A.11, $F_{a,i} * F^\circ_{a',i'}$ is also M-Lipschitz, so again by the $(\mathcal{F}(M),N)$-irrationality of θ and by Lemma 4.5, the proportion of $d \in I_{a-a',i-i'}$ such that $F_{a,i} * F^\circ_{a',i'}(\theta d) \geqslant \frac{1}{2}\tilde{\varepsilon}^{12}$ is at least $\mu(Y) - \tilde{\varepsilon}^{12}$, where

$$Y = \{y : F_{a,i} * F^\circ_{a',i'}(y) \geqslant \tilde{\varepsilon}^{12}\}.$$

But by Lemma 4.6 with $\eta = \tilde{\varepsilon}^{12}$, $\mu(Y) \geqslant \min\big(\int F_{a,i} + \int F_{a',i'}, 1\big) - 4\tilde{\varepsilon}^2$. Putting this all together,

$$f_{\mathrm{struct}}|_{I_{a,i}} * f^\circ_{\mathrm{struct}}|_{I_{a',i'}}(d) \geqslant \frac{\tilde{\varepsilon}^{14} N}{4qM}$$

for a set of $d \in I_{a-a',i-i'}$ of size at least

$$\frac{N}{qM}\min\Big(\int F_{a,i} + \int F_{a',i'},\ 1\Big) - \frac{7\tilde{\varepsilon}^2 N}{qM}.$$

Now by Lemma 4.3 and Young's inequality (Lemma A.12) we can absorb the contribution of f_{sml} and conclude that

$$(f_{\mathrm{struct}} + f_{\mathrm{sml}})|_{I_{a,i}} * (f_{\mathrm{struct}} + f_{\mathrm{sml}})^\circ_{I_{a',i'}}(d) \geqslant \frac{\tilde{\varepsilon}^{14} N}{5qM}$$

for these same values of d. Finally we add in the contribution of f_{unf}. Recalling from (4.4) that $1_A = f_{\mathrm{struct}} + f_{\mathrm{sml}} + f_{\mathrm{unf}}$, Lemma A.13 implies that

$$1_A|_{I_{a,i}} * 1_{-A}|_{I_{a',i'}}(d) \geqslant \frac{\tilde{\varepsilon}^{14}N}{8qM}$$

for all d in a subset $I_{a-a',i-i'}$ of size at least

$$\frac{N}{qM}\min\Big(\int F_{a,i} + \int F_{a',i'},\, 1\Big) - \frac{8\tilde{\varepsilon}^2 N}{qM}.$$

All these d lie in $\mathrm{D}_{\tilde{\varepsilon}^{14}/8qM}(A)$, which is of course contained in $\mathrm{D}_{\tilde{\varepsilon}^{20}/10M^2}(A)$. □

To use the bound supplied by the preceding lemma we apply the Brunn-Minkowski theorem, which states that if $X, Y \subset \mathbb{R}^d$ are open, then $\mu(X+Y)^{1/d} \geqslant \mu(X)^{1/d} + \mu(Y)^{1/d}$. We require the case $d = 2$. For a wider discussion and proof, see [Gar02].

Lemma 4.8. *Given a function $\alpha : \mathbb{Z}/q\mathbb{Z} \times \{1, \dots, M\} \to [0,1]$ and $(x,y) \in \mathbb{Z}/q\mathbb{Z} \times \{-M, \dots, M\}$, define $\tilde{\alpha}(x,y) = \max(\alpha(a,i) + \alpha(a',i'))$, where the maximum is taken over all $(a,i), (a',i') \in \mathbb{Z}/q\mathbb{Z} \times \{1, \dots, M\}$ such that $\alpha(a,i)$, $\alpha(a',i') > 0$, $a - a' = x$ and either $i - i' = y$ or $i - i' + 1 = y$. Then*

$$\sum_{x,y} \tilde{\alpha}(x,y) \geqslant 4 \sum_{a,i} \alpha(a,i).$$

Proof. Consider the open sets $X, X' \subset \mathbb{Z}/q\mathbb{Z} \times \mathbb{R}^2$ defined by

$$X = \bigcup_{(a,i) \in \mathbb{Z}/q\mathbb{Z} \times \{1,\dots,M\}} \{a\} \times (i-1, i) \times (0, \alpha(a,i)),$$

$$X' = \bigcup_{(a',i') \in \mathbb{Z}/q\mathbb{Z} \times \{1,\dots,M\}} \{a'\} \times (i'-1, i') \times (-\alpha(a',i'), 0).$$

Note that

$$\begin{aligned} X - X' &= \bigcup_{(a,i),(a',i')} \{a - a'\} \times (i - i' - 1, i - i' + 1) \times (0, \alpha(a,i) + \alpha(a',i')) \\ &= \bigcup_{(x,y) \in \mathbb{Z}/q\mathbb{Z} \times \{1,\dots,M\}} \{x\} \times (y-1, y) \times (0, \tilde{\alpha}(x,y)), \end{aligned}$$

where in the last equality we have ignored a set of measure zero. Thus, if ν is the product of counting measure on $\mathbb{Z}/q\mathbb{Z}$ and Lebesgue measure λ on $\mathbb{R}^2$, we have $\nu(X) = \nu(X') = \sum_{a,i} \alpha(a,i)$ and $\nu(X - X') = \sum_{x,y} \tilde{\alpha}(x,y)$. It therefore suffices to show that

$$\nu(X - X') \geqslant 4\nu(X).$$

The case $q = 1$ of this is immediate from the Brunn-Minkowski inequality. A simple argument allows us to extend this to general q. Indeed, let X_a, X'_a be the fibres of X, X' respectively above $a \in \mathbb{Z}/q\mathbb{Z}$. Then X_a, X'_a are open subsets

of $\mathbb{R}^2$. Pick a such that $\lambda(X_a) = \lambda(X'_a) = \sum_i \alpha(a,i)$ is largest. If $X_a \neq \emptyset$, then the Brunn-Minkowski inequality implies that

$$\lambda(X_a - X'_{a_*}) \geqslant \left(\lambda(X_a)^{1/2} + \lambda(X_{a_*})^{1/2}\right)^2 \geqslant 4\lambda(X_a).$$

However, the sets $X_a - X'_{a_*}$ are disjoint as a ranges over $\mathbb{Z}/q\mathbb{Z}$, since each lies in a different fibre over $\mathbb{Z}/q\mathbb{Z}$. Therefore

$$\nu(X - X') \geqslant \sum_{a : X_a \neq \emptyset} \lambda(X_a - X'_{a_*}) \geqslant \sum_{a : X_a \neq \emptyset} 4\lambda(X_a) = 4\lambda(X). \qquad \square$$

In fact we need the following more robust variant of the above, easily deduced from it.

LEMMA 4.9. *Let $\eta > 0$. Given a function $\alpha : \mathbb{Z}/q\mathbb{Z} \times \{1, \dots, M\} \to [0,1]$ and $(x,y) \in \mathbb{Z}/q\mathbb{Z} \times \{-M, \dots, M\}$, define $\tilde{\alpha}(x,y) = \max(\alpha(a,i) + \alpha(a',i'))$, where the maximum is taken over all $(a,i), (a',i') \in \mathbb{Z}/q\mathbb{Z} \times \{1, \dots, M\}$ such that $\alpha(a,i),\ \alpha(a',i') > \eta$, $a - a' = x$ and either $i - i' = y$ or $i - i' + 1 = y$. Then*

$$\sum_{x,y} \tilde{\alpha}(x,y) \geqslant 4 \sum_{a,i} \alpha(a,i) - 4\eta q M.$$

Proof. Let

$$\alpha^\dagger(a,i) = \begin{cases} \alpha(a,i) & \text{if } \alpha(a,i) > \eta, \\ 0 & \text{otherwise.} \end{cases}$$

Then if we define, as in Lemma 4.8, $\tilde{\alpha}^\dagger(x,y) = \max(\alpha^\dagger(a,i) + \alpha^\dagger(a',i'))$, where the maximum is taken over all $(a,i), (a',i')$ such that $\alpha^\dagger(a,i), \alpha^\dagger(a',i') > 0$, $a - a' = x$ and either $i - i' = y$ or $i - i' + 1 = y$, then $\tilde{\alpha}^\dagger = \tilde{\alpha}$ as defined above. It follows then from Lemma 4.8 that

$$\sum_{x,y} \tilde{\alpha}(x,y) = \sum_{x,y} \tilde{\alpha}^\dagger(x,y) \geqslant 4 \sum_{a,i} \alpha^\dagger(a,i) \geqslant 4 \sum_{a,i} \alpha(a,i) - 4\eta q M. \qquad \square$$

Now we are ready to put everything together and complete the proof of Theorem 4.1. Let $\delta = \tilde{\varepsilon}^{20}/10M^2$. Then certainly $\delta \gg_\varepsilon 1$. Recall that $\alpha(a,i)$ is the density of A on $I_{a,i}$. Define

$$\alpha'(a,i) = \begin{cases} \alpha(a,i) & \text{if } (a,i) \notin E, \\ 0 & \text{if } (a,i) \in E. \end{cases}$$

Then Lemma 4.7 may be rephrased as follows: if $\alpha'(a,i), \alpha'(a',i') \geqslant 2\tilde{\varepsilon}^2$, then

$$|\,\mathrm{D}_\delta(A) \cap I_{a-a',i-i'}| \geqslant \frac{N}{qM} \min(\alpha'(a,i) + \alpha'(a',i'), 1) - \frac{10\tilde{\varepsilon}^2 N}{qM},$$

with the same bound for $|\,\mathrm{D}_\delta(A) \cap I_{a-a',i-i'+1}|$. It follows that

$$|\,\mathrm{D}_\delta(A)| \geqslant \frac{N}{qM} \sum_{x,y} \min(\tilde{\alpha}'(x,y), 1) - 10\tilde{\varepsilon}^2 N,$$

where $\tilde{\alpha}'$ is as defined from α' as in Lemma 4.9 with $\eta = 2\tilde{\varepsilon}^2$. Recalling that $\tilde{\varepsilon} = \min(\varepsilon, \frac{1}{1000})$, this implies

$$|\,\mathrm{D}_\delta(A)| \geqslant \frac{N}{qM}\sum_{x,y}\min(\tilde{\alpha}'(x,y), 1+\tfrac{2}{5}\varepsilon) - \tfrac{9}{10}\varepsilon N.$$

Supposing that $\tilde{\alpha}'(x,y) < 1+\frac{2}{5}\varepsilon$ for all (x,y), Lemma 4.9 implies

$$|\,\mathrm{D}_\delta(A)| > \frac{4N}{qM}\sum_{a,i}\alpha'(a,i) - \tfrac{99}{100}\varepsilon N > \frac{4N}{qM}\sum_{a,i}\alpha(a,i) - \tfrac{999}{1000}\varepsilon N > 4|A| - \varepsilon N.$$

Thus if $|\,\mathrm{D}_\delta(A)| \leqslant 4|A| - \varepsilon N$, there must be some (x,y) such that $\tilde{\alpha}'(x,y) \geqslant 1+\frac{2}{5}\varepsilon$, whence for some (a,i) we must have $\alpha(a,i) \geqslant \frac{1}{2}+\frac{1}{5}\varepsilon$. This completes the proof of Theorem 4.1.

5. **Construction of the weight function**

In this section we prove Proposition 3.1 by constructing an appropriate weight function w. The reader may wish to take this opportunity to recall the statement of that result. A key ingredient in the proof is the following corollary of the results of the Section 4. It states that an "almost sum-free" open subset of $\mathbb{Z}/q\mathbb{Z}\times[0,1]$ with density larger than $\frac{1}{3}$ must "avoid the origin." Recall that μ is the natural probability measure on $\mathbb{Z}/q\mathbb{Z}\times[0,1]$, namely the product of the uniform measure on $\mathbb{Z}/q\mathbb{Z}$ and the Lebesgue measure.

Corollary 5.1. *Let $\varepsilon,\eta>0$ and $q\in\mathbb{N}$. Suppose that $A\subset\mathbb{Z}/q\mathbb{Z}\times[0,1]$ is an open set with $\mu(A)\geqslant\frac{1}{3}+\varepsilon$ and $T(A)\leqslant\eta$. Then $\mu(A\cap(H\times I))\ll_\varepsilon\eta$ for some subgroup $H\leqslant\mathbb{Z}/q\mathbb{Z}$ of index $\ll_\varepsilon 1$ and some interval I around 0 of length $\gg_\varepsilon 1$.*

Proof. We may assume that $\eta\leqslant\eta_0(\varepsilon)$ for some $\eta_0(\varepsilon)$ to be specified later. If not, the corollary is trivial by taking $H=\mathbb{Z}/q\mathbb{Z}$ and $I=[0,1]$. Let $\delta\gg_\varepsilon 1$ be as in Corollary 4.2. Recall that $\mathrm{D}_\delta(A)=\{x: 1_A*1_{-A}(x)\geqslant\delta\}$, and first suppose that $\mu(\mathrm{D}_\delta(A))>4\mu(A)-\varepsilon$. Write $\mathrm{D}_\delta(A)_+=\mathrm{D}_\delta(A)\cap(\mathbb{Z}/q\mathbb{Z}\times[0,1])$. Since $\mathrm{D}_\delta(A)$ is symmetric about 0, we have $\mu(\mathrm{D}_\delta(A)_+)>2\mu(A)-\frac{1}{2}\varepsilon$. It follows that $\mu(A)+\mu(\mathrm{D}_\delta(A)_+)>3\mu(A)-\frac{1}{2}\varepsilon>1+2\varepsilon$, and so by the pigeonhole principle, $\mu(A\cap\mathrm{D}_\delta(A)_+)>2\varepsilon$. This implies that $T(A)\geqslant 2\varepsilon\delta\gg_\varepsilon 1$. If $\eta_0(\varepsilon)$ is small enough, then this is more than η, and the corollary is established in this case.

The other possibility is that $\mu(\mathrm{D}_\delta(A))\leqslant 4\mu(A)-\varepsilon$. In this case, by Theorem 4.2 there is a subgroup $H\leqslant\mathbb{Z}/q\mathbb{Z}$ of index $m\ll_\varepsilon 1$ and an interval $I\subset[0,1]$ of length $\ell\gg_\varepsilon 1$ such that A has density at least $\frac{1}{2}+\frac{1}{7}\varepsilon$ on $(x+H)\times I$ for some $x\in\mathbb{Z}/q\mathbb{Z}$. Let $\varepsilon'=\frac{1}{7}\varepsilon\ell$, and suppose that $(h,t)\in H\times[0,\varepsilon']$. Then both $A\cap((x+H)\times I)$ and $\big(A\cap((x+H)\times I)\big)+(h,t)$ lie in $(x+H)\times I'$, where $I'=I+[0,\varepsilon']$. Noting that $\mu(H\times I)=\ell/m$ and $\mu(H\times I')=(\ell+\varepsilon')/m$, we have

$$\mu(A\cap(A+(h,t)))\geqslant 2\left(\tfrac{1}{2}+\tfrac{1}{7}\varepsilon\right)\mu(H\times I)-\mu(H\times I')\geqslant\frac{\varepsilon'}{m}.$$

It follows that $T(A) \geqslant \mu(A \cap (H \times [0,\varepsilon']))\frac{\varepsilon'}{m}$. Since $T(A) \leqslant \eta$, this implies that $\mu(A \cap (H \times [0,\varepsilon'])) \leqslant \eta m/\varepsilon' \ll_\varepsilon \eta$, and we have proved the corollary in this case too. □

Using the above corollary, we can construct a weight function on $\mathbb{Z}/Q\mathbb{Z} \times [0,1]$ for some $Q \ll_\varepsilon 1$, packing most of its weight near 0 in a certain sense, and prove that it satisfies Proposition 3.1. Our iterative strategy[3] is embodied in the following lemma.

LEMMA 5.2. *Let $\varepsilon > 0$, and suppose that $\alpha \geqslant \frac{1}{3} + \frac{1}{8}\varepsilon$. Suppose we are given a Lipschitz weight function $w : \mathbb{Z}/Q\mathbb{Z} \times [0,1] \to (0,\infty)$ and $\eta > 0$ such that if $Q \mid q$ and $A \subset \mathbb{Z}/q\mathbb{Z} \times [0,1]$ is an open set such that $T(A) \leqslant \eta$, then*

$$\int_A w \, d\mu \leqslant \alpha.$$

Then for some Q', there is a Lipschitz weight function $w' : \mathbb{Z}/Q'\mathbb{Z} \times [0,1] \to (0,\infty)$ and $\eta' > 0$ such that if $Q' \mid q'$ and $A \subset \mathbb{Z}/q'\mathbb{Z} \times [0,1]$ is an open set such that $T(A) \leqslant \eta'$, then

$$\int_A w' \, d\mu \leqslant \alpha',$$

where $\alpha' = \frac{3}{4}\alpha + \frac{1}{4}\left(\frac{1}{3} + \frac{1}{8}\varepsilon\right)$.

The constants $\frac{1}{4}$ and $\frac{3}{4}$ here are not important; they can be replaced by any δ and $1-\delta$ such that $0 < \delta < \frac{1}{3}$.

Proof. Apply Corollary 5.1 with $\frac{1}{8}\varepsilon$ replacing ε. Thus if $A \subset \mathbb{Z}/q\mathbb{Z} \times [0,1]$ is open, $\mu(A) \geqslant \frac{1}{3} + \frac{1}{8}\varepsilon$ and $T(A) \leqslant \eta'$, then $\mu(A \cap (H \times [0,\varepsilon'])) \ll_\varepsilon \eta'$, where $H \leqslant \mathbb{Z}/q\mathbb{Z}$ is a subgroup of index at most C_ε and $\varepsilon' \gg_\varepsilon 1$. Let $M = C_\varepsilon!$. Then the index $[\mathbb{Z}/q\mathbb{Z} : H]$ necessarily divides M, so for every $x \in \mathbb{Z}/q\mathbb{Z}$, we have $Mx \in H$.

For $t \in \left[\frac{1}{2}, 1\right]$ and $q \in \mathbb{N}$, define $\pi_t : \mathbb{Z}/q\mathbb{Z} \times [0,1] \to \mathbb{Z}/Mq\mathbb{Z} \times [0,1]$ by $\pi_t(x,y) = (Mx, t\varepsilon' y)$. Then, by the above, if $A \subset \mathbb{Z}/Mq\mathbb{Z} \times [0,1]$ is open, $\mu(A) \geqslant \frac{1}{3} + \frac{1}{8}\varepsilon$ and $T(A) \leqslant \eta'$, then $\mu(A \cap \operatorname{im}\pi_t) \ll_\varepsilon \eta'$.

Let $Q' = MQ$, and define w'_t on $\mathbb{Z}/Q'\mathbb{Z} \times [0,1]$ by

$$w'_t(x) = \tfrac{3}{4} 1_{\operatorname{im}\pi_t}(x) \frac{w(\pi_t^{-1}(x))}{\mu(\operatorname{im}\pi_t)} + \tfrac{1}{4}. \tag{5.1}$$

This definition can be made to look a little more natural as follows. Define measures ν on $\mathbb{Z}/Q\mathbb{Z} \times [0,1]$ and ν'_t on $\mathbb{Z}/Q'\mathbb{Z} \times [0,1]$ by $\nu(A) = \int 1_A w \, d\mu$ and $\nu'_t(A) = \int 1_A w'_t \, d\mu$. Then the relationship between ν and ν'_t is $\nu'_t = \frac{3}{4}(\pi_t)_*\nu + \frac{1}{4}\mu$, where the push-forward measure is defined as usual by $\pi_*\nu(A) = \nu(\pi^{-1}(A))$.

[3]This strategy was suggested to us by the proof of the contraction mapping theorem.

Now suppose $Q' \mid q'$, say $q' = Mq$ where $Q \mid q$, and $A \subset \mathbb{Z}/q'\mathbb{Z} \times [0,1]$ is open and $T(A) \leqslant \eta'$. If $\mu(A) \geqslant \frac{1}{3} + \frac{1}{8}\varepsilon$ then, as noted above, $\mu(A \cap \operatorname{im} \pi_t) \ll_\varepsilon \eta'$. Therefore

$$(\pi_t)_*\nu(A) = \nu(\pi_t^{-1}(A)) \leqslant \|w\|_\infty \mu(\pi_t^{-1}(A)) = \|w\|_\infty \frac{\mu(A \cap \operatorname{im} \pi_t)}{\mu(\operatorname{im} \pi_t)} \ll_\varepsilon \eta' \|w\|_\infty,$$

so $\nu_t'(A) \leqslant O_\varepsilon(\eta'\|w\|_\infty) + \frac{1}{4}$, and this can be made to be less than $\frac{1}{3}$ by taking η' sufficiently small depending on ε and $\|w\|_\infty$.

Suppose instead $\mu(A) \leqslant \frac{1}{3} + \frac{1}{8}\varepsilon$. If $\eta' \leqslant \mu(\operatorname{im} \pi_{1/2})^3 \eta$, then we have $T(\pi_t^{-1}(A)) \leqslant \eta$ for all $t \in [\frac{1}{2}, 1]$, so in this case we have

$$\nu_t'(A) = \tfrac{3}{4}\nu(\pi_t^{-1}(A)) + \tfrac{1}{4}\mu(A) \leqslant \tfrac{3}{4}\alpha + \tfrac{1}{4}\left(\tfrac{1}{3} + \tfrac{1}{8}\varepsilon\right) = \alpha'.$$

To complete the proof, we must show that w' can be chosen to be Lipschitz. In fact w_t' generally has a jump discontinuity[4] at every point of the form $(Mk, t\varepsilon')$, but we can remedy this by defining

$$w' = 2\int_{\frac{1}{2}}^{1} w_t' \, dt. \tag{5.2}$$

Then if $Q' \mid q'$, $A \subset \mathbb{Z}/q'\mathbb{Z} \times [0,1]$ is open and $T(A) \leqslant \eta'$, then

$$\int_A w' \, d\mu = 2\int_{\frac{1}{2}}^{1} \nu_t'(A) \, dt \leqslant 2\int_{\frac{1}{2}}^{1} \alpha' \, dt = \alpha',$$

while from (5.1) and (5.2) it is fairly clear that w' is Lipschitz. □

By applying Lemma 5.2 iteratively we get a weak version of Proposition 3.1.

PROPOSITION 5.3. *Let $\varepsilon > 0$. Then there is an integer Q and a Lipschitz weight function $w : \mathbb{Z}/Q\mathbb{Z} \times [0,1] \to (0,\infty)$ with the following property. If $Q \mid q$, then for any open set $A \subset \mathbb{Z}/q\mathbb{Z} \times [0,1]$ such that $\int 1_A w \, d\mu \geqslant \frac{1}{3} + \varepsilon$, we have $T(A) \gg_\varepsilon 1$.*

Proof. Apply Lemma 5.2 iteratively starting with $Q = 1$, $w \equiv 1$, $\alpha = 1$, and $\eta = 1$. After $n = 100\log(1/\varepsilon)$ steps we obtain an integer Q and a weight w on $\mathbb{Z}/Q\mathbb{Z} \times [0,1]$ satisfying the hypotheses of that lemma with some $\eta > 0$ and

$$\alpha = \left(\tfrac{3}{4}\right)^n + \tfrac{1}{4}\left(1 + \tfrac{3}{4} + \left(\tfrac{3}{4}\right)^2 + \cdots + \left(\tfrac{3}{4}\right)^{n-1}\right)\left(\tfrac{1}{3} + \tfrac{1}{8}\varepsilon\right) < \tfrac{1}{3} + \tfrac{1}{4}\varepsilon. \qquad \square$$

[4]This would not, in actual fact, be a fatal hole in our argument; in Section 3 we could instead have dealt with the larger class of piecewise Lipschitz functions. This is a little complicated, however, and the Lipschitz hypothesis is convenient.

To obtain Proposition 3.1 from Proposition 5.3, we must replace 1_A by an arbitrary continuous function Ψ, and we must introduce the additional factor of $\mathbb{T} = (\mathbb{R}/\mathbb{Z})^d$. Both of these improvements turn out to be relatively straightforward.

Proof of Proposition 3.1. We will show that w, the weight function on $\mathbb{Z}/Q\mathbb{Z} \times [0,1]$ constructed in Proposition 5.3, has property required by Proposition 3.1. We do this in stages, beginning with the following.

Claim I. Consider the "discrete torus" $\mathbb{T}_{\mathrm{disc}} = \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_d\mathbb{Z}$, where $q_1, \dots, q_d > q$ are distinct primes. Suppose $A \subset \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T}_{\mathrm{disc}}$ is open and $\int 1_A(w \times 1_{\mathbb{T}_{\mathrm{disc}}})d\mu \geqslant \frac{1}{3} + \frac{1}{4}\varepsilon$. Then $T(A) \gg_\varepsilon 1$. (Here, $\mathbb{Z}/Q\mathbb{Z} \times [0,1] \times \mathbb{T}_{\mathrm{disc}}$ is endowed with the uniform probability measure μ.)

Proof of Claim I. Let $q' = qq_1 \dots q_d$, and consider the μ-preserving isomorphism

$$\mathbb{Z}/q'\mathbb{Z} \times [0,1] \xrightarrow{\psi} \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T}_{\mathrm{disc}}$$

given by

$$\psi(x,y) = (x \,(\mathrm{mod}\, q), y, x \,(\mathrm{mod}\, q_1), \dots, x \,(\mathrm{mod}\, q_d)).$$

If $A \subset \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T}_{\mathrm{disc}}$ is open and $\int 1_A(w \times 1_{\mathbb{T}_{\mathrm{disc}}})\, d\mu \geqslant \frac{1}{3} + \frac{1}{4}\varepsilon$, then $\int 1_{\psi^{-1}(A)} w \, d\mu \geqslant \frac{1}{3} + \frac{1}{4}\varepsilon$, so Proposition 5.3 implies $T(A) = T(\psi^{-1}(A)) \gg_\varepsilon 1$.

Claim II. The same claim holds if $\mathbb{T}_{\mathrm{disc}}$ is replaced by the genuine torus $\mathbb{T} = (\mathbb{R}/\mathbb{Z})^d$ and $\frac{1}{4}\varepsilon$ is replaced with $\frac{1}{2}\varepsilon$. That is, if $A \subset \mathbb{Z}/Q\mathbb{Z} \times [0,1] \times \mathbb{T}$ is open and $\int 1_A(w \times 1_{\mathbb{T}}) \geqslant \frac{1}{3} + \frac{1}{2}\varepsilon$, then $T(A) \gg_\varepsilon 1$.

Proof of Claim II. This is a standard discretisation argument. We may find some $\kappa > 0$ and a subset $A' \subset A$ such that A' is a disjoint union of sets of the form $\{x\} \times I \times J$, where $I \subset [0,1]$ is an open interval of length κ and $J \subset \mathbb{T}$ is an open cube of side-length κ, and $\int 1_{A'}(w \times 1_{\mathbb{T}}) \geqslant \frac{1}{3} + \frac{1}{3}\varepsilon$. Regard $\mathbb{T}_{\mathrm{disc}}$ as a subgroup of $\mathbb{T}$ by mapping $(x_1, \dots, x_d) \in \mathbb{T}_{\mathrm{disc}}$ to $\left(\frac{x_1}{q_1}, \dots, \frac{x_d}{q_d}\right) \in \mathbb{T}$. Set

$$A'_{\mathrm{disc}} = A' \cap (\mathbb{Z}/Q\mathbb{Z} \times [0,1] \times \mathbb{T}_{\mathrm{disc}}).$$

Then as $q_1, \dots, q_d \to \infty$, both $\int 1_{A'_{\mathrm{disc}}}(w \times 1_{\mathbb{T}_{\mathrm{disc}}})\, d\mu \to \int 1_{A'}(w \times 1_{\mathbb{T}})\, d\mu$ and $T(A'_{\mathrm{disc}}) \to T(A')$, so by the previous claim $T(A) \geqslant T(A') \gg_\varepsilon 1$.

Finally, we are ready to verify Proposition 3.1 itself, which differs from Claim II only in the presence of a general continuous function $\Psi : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T} \to [0,1]$ in place of the characteristic function 1_A. Suppose that Ψ is given and $\int \Psi \cdot (w \times 1_{\mathbb{T}})\, d\mu > \frac{1}{3} + \varepsilon$. Consider the open set $A = \left\{x : \Psi(x) > \frac{1}{2}\varepsilon\right\} \subset \mathbb{Z}/q\mathbb{Z} \times [0,1] \times \mathbb{T}$. Since

$$\tfrac{1}{3} + \varepsilon \leqslant \int \Psi \cdot (w \times 1_{\mathbb{T}}) = \int_A \Psi \cdot (w \times 1_{\mathbb{T}}) + \int_{A^c} \Psi \cdot (w \times 1_{\mathbb{T}}) \leqslant \int 1_A (w \times 1_{\mathbb{T}}) + \tfrac{1}{2}\varepsilon,$$

we have $\int 1_A(w \times 1_{\mathbb{T}}) \geqslant \frac{1}{3} + \frac{1}{2}\varepsilon$. By Claim II we therefore have $T(A) \gg_\varepsilon 1$, and thus $T(\Psi) \geqslant \left(\frac{1}{2}\varepsilon\right)^3 T(A) \gg_\varepsilon 1$. This (at last!) completes the proof of Proposition 3.1 and hence of Theorem 1.1. □

6. **More on sets of doubling less than** 4

The purpose of this section is to expand just a little more on the results of Section 4, which may be of independent interest. The first theorem below is a direct consequence of Theorem 4.1; the second is the corresponding consequence of Corollary 4.2 in the case $Q = 1$.

THEOREM 6.1. *If $A \subset \{1, \dots, N\}$ is a set such that $|A - A| \leqslant 4|A| - \varepsilon N$, then there is an arithmetic progression $P \subset \{1, \dots, N\}$ of length $\gg_\varepsilon N$ on which A has density at least $\frac{1}{2} + \frac{1}{5}\varepsilon$.*

THEOREM 6.2. *If $A \subset [0, 1]$ is an open set such that $|A - A| \leqslant 4|A| - \varepsilon$, then there is an interval $I \subset [0, 1]$ of length $\gg_\varepsilon 1$ on which A has density at least $\frac{1}{2} + \frac{1}{7}\varepsilon$.*

Remarks.

(i) Neither the constant $\frac{1}{5}$ in Theorem 6.1 (or Theorem 4.1) nor the constant $\frac{1}{7}$ in Theorem 6.2 is optimal. Indeed, if one allows the implied constants to depend on η, then our proof can be modified to get $\frac{1}{4} - \eta$ for both these constants.

(ii) A similar conclusion to Theorem 6.2 could be obtained if one instead had *two* sets A and B satisfying $|A - B| < |A| + |B| + 2|A|^{1/2}|B|^{1/2} - \varepsilon$. The conclusion would then be that there are intervals I_A and I_B such that the densities of A, B on I_A, I_B respectively sum to at least $1 + \frac{1}{3}\varepsilon$ (or up to $1 + (\frac{1}{2} - \eta)\varepsilon$, constants depending on η). There would be a similar generalisation of Theorem 6.1. We leave the proof of these results as an exercise to the interested reader. One annoying additional complication would be the need to have an arithmetic regularity lemma valid for two sets simultaneously. While such a statement can be easily established by modifying the arguments of [GT10], no such result currently appears in the literature.

(iii) We are not aware of any reason that the length of I or P could not be bounded below by some quite reasonable function of ε, but our argument does not give one. Much better quantitative results are available under the assumption that $|A - A| < 3|A|$; see [Ruz91].

Consider the discrete case $A \subset \{1, \dots, N\}$. Note that the hypothesis $|A - A| \leqslant 4|A| - \varepsilon N$ implies $|A| \geqslant \frac{1}{4}\varepsilon N$. Thus one can consider Theorem 6.1 to contain a "hidden hypothesis" to the effect that A is somewhat dense in $\{1, \dots, N\}$. If instead one assumed only that $|A - A| \leqslant (4 - \varepsilon)|A|$, then our

argument would give bounds depending on $\alpha = |A|/N$ as well as ε. Using a "Freiman modelling" argument of a type pioneered by Ruzsa, however, we can overcome this. We first isolate a lemma due to Lev [Lev97] (though earlier results of Sárközy [Sár89] would also suffice).

LEMMA 6.3. *Let P be a finite arithmetic progression of length greater than* 12, *and let $X \subset P$ be a set with $|X| > \frac{1}{2}|P|$. Then $5X - 4X$ contains P.*

Proof. The statement of the lemma being affine-invariant, we may suppose without loss of generality that $X = \{1, \dots, N\}$. Since $|X| > N/2$, the highest common factor of the elements of X is 1. By [Lev97, Lemma 1] with $k = 2$ (and a short computation), $4X$ contains an interval of length at least $4(\frac{N}{2} - 3) > N$. It follows that $4X - 4X$ contains $\{-N, \dots, N\}$, and the result follows immediately. □

In the proof of the next lemma we will use the notion of a *Freiman homomorphism*. See [TV10, Def. 5.21] for details.

THEOREM 6.4. *Let $\varepsilon > 0$. Suppose that A is a finite set of integers such that $|A - A| \leqslant (4 - \varepsilon)|A|$. Then there is an arithmetic progression $P \subset \mathbb{Z}$ of length $\gg_\varepsilon |A|$ on which the density of A is at least $\frac{1}{2} + c\varepsilon$.*

Proof. By [GR06, Th. 1.4], every set $A \subset \mathbb{Z}$ with $|A - A| \leqslant 4|A|$ is Freiman 18-isomorphic to a subset of $\{1, \dots, N\}$ for some $N \ll |A|$. Let $\pi : A \to A' \subset \{1, \dots, N\}$ be this Freiman isomorphism. Then clearly $|A'|/N \gg 1$, so $|A' - A'| \leqslant 4|A'| - \varepsilon' N$ with $\varepsilon' \gg \varepsilon$. By Theorem 6.1 to A', there is a progression $P' \subset \{1, \dots, N\}$ of length $|P'| \gg_\varepsilon N$ on which the density of A' is at least $\frac{1}{2} + \frac{1}{5}\varepsilon'$. Finally, by the preceding lemma, $P' \subset 5A' - 4A'$, so it follows from basic facts about Freiman homomorphisms (see [TV10, §5.2] for example) that $\pi^{-1} : A' \to A$ induces a Freiman 2-homomorphism $\tilde{\pi}^{-1} : P' \to \mathbb{Z}$ coinciding with π^{-1} on $A' \cap P'$. The image $P = \tilde{\pi}^{-1}(P')$ is then a progression of length $\gg_\varepsilon |A|$ on which A has density at least $\frac{1}{2} + c\varepsilon$. □

Remarks.

(i) The value for c given by this argument is something like 2^{-1000}.
(ii) Under stronger conditions such as $|A + A| < 3|A|$ or $|A - A| < 3|A|$, more precise information can be obtained; see [Fre73, Th. 1.9] or [LS95].
(iii) Statements of the same form as Theorem 6.4, but with $\frac{1}{2} + c\varepsilon$ replaced by some small quantity $f(\varepsilon) > 0$, follow from versions of Freiman's theorem [Fre73, Th. 2.8], [Bil99, Th. 1.2]. These statements come with more effective lower bounds on the length of P.

Appendix A. Regularity and counting lemmata

In this appendix we collect some tools used in the main part of the paper. All of these are more or less standard, or at least have easily quotable references.

The arithmetic regularity lemma. We begin with the arithmetic regularity lemma, the main result of [GT10], used twice in the paper. As reassurance to the reader who views that paper with trepidation, we remark that the majority of it is given to applications, and only Sections 1 and 2 are relevant to us. Furthermore, that paper establishes a regularity lemma for the Gowers U^{s+1}-norm for general s, whereas we only need the case $s = 1$. This means that the notion of a *nilsequence*, beyond the abelian case, is not relevant here. A complete, self-contained proof of the arithmetic regularity lemma in the form we need it here can be written up in less than ten pages. The first-named author has provided such a write-up online [Ebe].

We begin by defining a quantitative notion of irrationality for vectors $\theta \in \mathbb{R}^d$.

Definition A.1. Suppose that $\theta \in \mathbb{R}^d$. Let $N \geqslant 1$ be an integer, and let $A > 0$ be some real parameter. We say that θ is (A, N)-irrational if whenever $q_1, \dots, q_d$ are integers, not all zero, with $\sum_i |q_i| \leqslant A$ we have $\|q_1\theta_1 + \cdots + q_d\theta_d\|_{\mathbb{R}/\mathbb{Z}} \geqslant A/N$.

Lemma A.2. *Suppose we are given a parameter $\delta > 0$ and a growth function $\mathcal{F} : \mathbb{N} \to \mathbb{R}_+$. Then there exists $M_{\max} \ll_{\delta,\mathcal{F}} 1$ such that for any function $f : \{1, \dots, N\} \to [0, 1]$, there is an $M \leqslant M_{\max}$ and a decomposition $f = f_{\text{tor}} + f_{\text{sml}} + f_{\text{unf}}$ into functions taking values in $[-1, 1]$, where $\|f_{\text{sml}}\|_{\ell_2(N)} \leqslant \delta$, $\|f_{\text{unf}}\|_{U^2(N)} \leqslant 1/\mathcal{F}(M)$ and $f_{\text{tor}}(n) = F(n(\text{mod}\, q), n/N, \theta n)$ for some $q, d \leqslant M$ and some function $F : \mathbb{Z}/q\mathbb{Z} \times [0, 1] \times (\mathbb{R}/\mathbb{Z})^d \to [0, 1]$ with Lipschitz constant at most M. Furthermore, the element $\theta \in (\mathbb{R}/\mathbb{Z})^d$ may be taken to be $(\mathcal{F}(M), N)$-irrational.*

Here $\|g\|_{U^2(N)}$ is the Gowers $U^2(N)$-norm, whose definition will be recalled below. We do not offer a proof of this lemma, but merely a guide to extracting this result from [GT10]. The function f_{tor} written here is the same thing as, in the language of that paper, a "$(\mathcal{F}(M), N)$-irrational virtual nilsequence of degree $\leqslant 1$, complexity $\leqslant M$ and scale N." Once we have justified this assertion, Lemma A.2 is essentially the same as [GT10, Th. 1.2], the proof of which occupies Section 2 of that paper. The definition of an irrational virtual nilsequence of degree $\leqslant s$ is rather long and complicated for general s, but for $s = 1$, a great deal simplifies: a *filtered nilmanifold* of degree 1 and complexity $\leqslant M$ (cf. [GT10, Def. 1.4]) is just the torus $(\mathbb{R}/\mathbb{Z})^d$ for $d \leqslant M$, a *polynomial orbit* of degree 1(cf. [GT10, Def. 1.7]) is just a sequence of the form $n \mapsto \theta n$ for some $\theta \in (\mathbb{R}/\mathbb{Z})^d$, and a *virtual nilsequence* of degree 1 and complexity $\leqslant M$ at scale N (cf. [GT10, Def. 1.9]) is just a function $F(n \,(\text{mod}\, q), n/N, \theta n)$ with $\theta \in (\mathbb{R}/\mathbb{Z})^d$, $d, q, \|F\|_{\text{Lip}} \leqslant M$. Finally, an (A, N)-irrational sequence (cf. [GT10, Def. A.6]), in the case that the sequence has the form $n \mapsto \theta n$ where $\theta \in (\mathbb{R}/\mathbb{Z})^d$, coincides with the notion of irrationality defined above.

Equidistribution and counting. If $\theta \in (\mathbb{R}/\mathbb{Z})^d$ is highly irrational in the sense of Definition A.1, then the sequence θn is highly equidistributed on $(\mathbb{R}/\mathbb{Z})^d$ as n ranges over fairly long progressions. Moreover, the triple

$$(n \,(\mathrm{mod}\ q), n/N, n\theta)$$

is highly equidistributed in $\mathbb{Z}/q\mathbb{Z} \times [0,1] \times n\theta$ as n varies over $\{1,\dots,N\}$. We prove various statements of this type required in the main body of the paper. The first is quite classical.

LEMMA A.3. *Suppose that $\theta \in (\mathbb{R}/\mathbb{Z})^d$ is (A,N)-irrational, and let $F : (\mathbb{R}/\mathbb{Z})^d \to \mathbb{C}$ be a function with Lipschitz constant at most M. Suppose that $P \subset \{1,\dots,N\}$ is an arithmetic progression of length at least ηN. Then, provided that $A > A_0(M,d,\eta,\delta)$ is large enough,*

$$\left|\mathbb{E}_{n\in P} F(\theta n) - \int F\, d\mu\right| \leqslant \delta.$$

Proof. The key here (as usual in equidistribution theory) is to take a Fourier expansion of F and truncate it. In particular, we may find $M_0 = O_{M,d,\delta}(1)$ and coefficients c_m with $c_0 = \int F$ and $c_m = O_{M,d}(1)$ for $m \neq 0$ such that

$$\left|F(x) - \sum_{|m|\leqslant M_0} c_m e(m\cdot x)\right| \leqslant \delta/2$$

uniformly in x. For a proof see, for example, [GT08, Lemma A.9]. It follows, of course, that

$$\left|\mathbb{E}_{n\in P} F(\theta n) - \int F\, d\mu\right| \leqslant \sum_{|m|\leqslant M_0, m\neq 0} |c_m||\mathbb{E}_{n\in P} e(m\cdot\theta n)| + \frac{\delta}{2}.$$

Thus we need only show that

$$\mathbb{E}_{n\in P} e(m\cdot\theta n) = o_{m,\eta;A\to\infty}(1)$$

and then take A sufficiently large. If the common difference of the arithmetic progression P is h, then by summing the geometric progression we have the bound

$$\mathbb{E}_{n\in P} e(m\cdot\theta n) \ll \frac{1}{\eta N \|(m\cdot\theta)h\|_{\mathbb{R}/\mathbb{Z}}}.$$

If $A > |h|(|m_1|+\cdots+|m_d|)$ (where $m = (m_1,\dots,m_d)$) then, by the definition of (A,N)-irrationality, $\|(m\cdot\theta)h\|_{\mathbb{R}/\mathbb{Z}} \geqslant A/N$. The result follows immediately. □

Our second result is a little more involved but is proved in essentially the same way as the last lemma. It states that if θ is highly irrational and N is sufficiently large, then $(n \,(\mathrm{mod}\ q), n/N, \theta n)$ is highly equidistributed in $\mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d$.

LEMMA A.4. *Suppose that $\theta \in (\mathbb{R}/\mathbb{Z})^d$ is (A,N)-irrational. Let $q \in \mathbb{N}$, and let $F : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to \mathbb{C}$ be a function with Lipschitz constant at most M. Let $\delta > 0$ be arbitrary. Then, provided that $A > A_0(M,q,d,\delta)$ and $N > N_0(M,q,d,\delta)$ are large enough,*

$$\left|\mathbb{E}_{n \leqslant N} F(n(\mathrm{mod}\, q), n/N, \theta n) - \int F \, d\mu\right| \leqslant \delta.$$

Proof sketch. Again the idea is to take a truncated Fourier expansion of F, but because $F|_{\mathbb{Z}/q\mathbb{Z}\times\{0\}\times(\mathbb{R}/\mathbb{Z})^d}$ and $F|_{\mathbb{Z}/q\mathbb{Z}\times\{1\}\times(\mathbb{R}/\mathbb{Z})^d}$ need not agree, the expansion looks a little more complicated. The key point is that F can be extended to an M-Lipschitz function $\mathbb{Z}/q\mathbb{Z} \times [-1,1] \times (\mathbb{R}/\mathbb{Z})^d \to \mathbb{C}$ such that $F(x,y,z) = F(x,-y,z)$, so F may be approximated by a sum of the functions $\phi_{a,m,\mathbf{m}}$ given by

$$\phi_{a,m,\mathbf{m}}(x,y,z) = e\left(\frac{a}{q}x + \frac{m}{2}y + \mathbf{m}\cdot z\right) + e\left(\frac{a}{q}x - \frac{m}{2}y + \mathbf{m}\cdot z\right), \tag{A.1}$$

where $a \in \mathbb{Z}/q\mathbb{Z}, m \in \mathbb{Z}$ and $\mathbf{m} \in \mathbb{Z}^d$. Then just as in the proof of the previous lemma we need only check that

$$\mathbb{E}_{n \leqslant N} \phi_{a,m,\mathbf{m}}(n \,(\mathrm{mod}\ q), n/N, \theta n) = o_{a,m,\mathbf{m},q;A,N\to\infty}(1) \tag{A.2}$$

provided that $a, m, \mathbf{m}$ are not all zero. Substituting in, the left-hand side is

$$\mathbb{E}_{n \leqslant N}\left(e\left(\left(\frac{a}{q} + \frac{m}{2N} + \mathbf{m}\cdot\theta\right)n\right) + e\left(\left(\frac{a}{q} - \frac{m}{2N} + \mathbf{m}\cdot\theta\right)n\right)\right). \tag{A.3}$$

Summing the geometric progressions, we see that this is bounded by ε unless

$$\left\|\frac{a}{q} + \frac{m}{2N} + \mathbf{m}\cdot\theta\right\|_{\mathbb{R}/\mathbb{Z}} \ll \frac{1}{N\varepsilon}. \tag{A.4}$$

Supposing first that $\mathbf{m} \neq 0$, inequality (A.4) implies

$$\left\|\frac{mq}{2N} + q\mathbf{m}\cdot\theta\right\|_{\mathbb{R}/\mathbb{Z}} \ll \frac{q}{N\varepsilon},$$

and hence

$$\|\mathbf{m}'\cdot\theta\|_{\mathbb{R}/\mathbb{Z}} \ll \frac{q}{N\varepsilon} + \frac{mq}{2N},$$

where $\mathbf{m}' = q\mathbf{m}$. If A is sufficiently large in terms of ε, q, m and $\mathbf{m}$, this is contrary to the (A,N)-irrationality of θ.

Now suppose that $\mathbf{m} = 0$. Then if N is large enough depending on m and q, (A.4) implies that $a = 0$. Thus $a = \mathbf{m} = 0$, and hence $m \neq 0$. Then the expression (A.3) is $\mathbb{E}_{n\leqslant N}\,(e(mn/2N) + e(-mn/2N)) = 0$, so (A.2) certainly follows in this case as well. □

The next result is a kind of "counting lemma." It eventually allows one to relate summing triples $(x,y,x+y)$ in $A \subset \{1,\dots,N\}$ with summing triples

in $(\mathbb{R}/\mathbb{Z})^d$ weighted by f_{tor}. Recall the operator T, defined at the beginning of Section 3: if $f : \{1, \dots, N\} \to \mathbb{C}$, then

$$T(f) = \frac{1}{N^2} \sum_{n,n'} f(n) f(n') f(n+n'),$$

and if $F : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to \mathbb{C}$, then

$$T(F) = \int F(x) F(x') F(x+x')\, d\mu(x)\, d\mu(x').$$

LEMMA A.5. *Suppose that $\theta \in (\mathbb{R}/\mathbb{Z})^d$ is (A,N)-irrational. Let $q \in \mathbb{N}$, and let $F : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to \mathbb{C}$ be a function with Lipschitz constant at most M. Let $f(n) = F(n(\mathrm{mod}\, q), n/N, \theta n)$. If $A > A_0(q, M, \varepsilon)$ and $N > N_0(q, M, \varepsilon)$ are large enough, then*

$$|T(f) - T(F)| = |T_{\{1,\dots,N\}}(f) - T_{\mathbb{Z}/q\mathbb{Z}\times[0,1]\times(\mathbb{R}/\mathbb{Z})^d}(F)| \leqslant \varepsilon.$$

Proof sketch. Write $\pi(n) = (n \,(\mathrm{mod}\ q), n/N, \theta n)$. We showed in Lemma A.4 that, if θ is highly irrational, $\pi(n)$ is highly equidistributed in $X = \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d$ as n ranges in $\{1, \dots, N\}$. It follows that as n, n' range over $\{1, \dots, N\}$, the pair $(\pi(n), \pi(n'))$ is highly equidistributed in $X \times X$ and, in particular,

$$\mathbb{E}_{n,n' \in \{1,\dots,N\}} F_*(\pi(n), \pi(n')) \approx \int F_*(x, x') d\mu(x) d\mu(x')$$

for any Lipschitz function $F_* : X \times X \to \mathbb{C}$. Applying this with $F_*(x, x') = F(x)F(x')F(x+x')$ gives the stated result. □

Finally, we require the following simple result which does not mention θ at all.

LEMMA A.6. *Let $q \in \mathbb{N}$. Suppose that $w : \mathbb{Z}/q\mathbb{Z} \times [0,1] \to \mathbb{C}$ has Lipschitz constant at most M. Then*

$$\mathbb{E}_{n \leqslant N} w(n(\mathrm{mod}\, q), n/N) = \int w\, d\mu + o_{q,M;N\to\infty}(1).$$

Proof sketch. Split into progressions $P_a = \{n \leqslant N : n \equiv a \,(\mathrm{mod}\ q)\}$. Then one need only show that

$$\mathbb{E}_{n \in P_a} w(a, n/N) = \int_0^1 w(a, y) dy + o_{M;N\to\infty}(1),$$

which is fairly obvious from the definition of the Riemann integral. □

Properties of the Gowers U^2-norm. The statement of the arithmetic regularity lemma involved the Gowers $U^2(N)$-norm of a function. Here we recall some basic properties of this norm, whose proofs may be found in several places. We begin by recalling the definition. For a fuller discussion, see [GT10].

Definition A.7. Let $f : \{1, \dots, N\} \to \mathbb{C}$ be a function. Then we define $\|f\|_{U^2(N)} = \|f\|_{U^2(G)}/\|1_{\{1,\dots,N\}}\|_{U^2(G)}$, where $G = \mathbb{Z}/N'\mathbb{Z}$ for some arbitrary $N' > 4N$ and

$$\|f\|_{U^2(G)}^4 = \mathbb{E}_{x,h_1,h_2 \in G} f(x)\overline{f(x+h_1)f(x+h_2)}f(x+h_1+h_2).$$

In this definition, f is regarded (by abuse of notation) as a function on G by defining $f(x) = 0$ if $x \in G \setminus \{1, \dots, N\}$, where $\{1, \dots, N\}$ is regarded as embedded in G in the natural manner. It is not hard to see that this definition does not depend on the exact choice of N'. Introducing the group G is a technical device which is useful in several parts of the theory.

We begin with a standard lemma.

LEMMA A.8. *Suppose that $f : \{1, \dots, N\} \to \mathbb{C}$ is a function. Then $|\mathbb{E}_{n \leqslant N} f(n)| \ll \|f\|_{U^2(N)}$. More generally, suppose that $P \subset \{1, \dots, N\}$ is a progression of length at least ηN. Then $|\mathbb{E}_{n \in P} f(n)| \ll \eta^{-1}\|f\|_{U^2(N)}$.*

Proof. We establish the second statement, the first being a special case of it. Fix a prime $N' \in [4N, 8N]$, and write $G = \mathbb{Z}/N'\mathbb{Z}$ as in the definition of the Gowers $U^2(N)$-norm. Note that the $U^2(N)$-norm and the $U^2(G)$-norm are comparable up to an absolute constant. We use the inequality

$$\begin{aligned}|\mathbb{E}_{x \in G} f(x)g(x)| &= \left|\sum_r \hat{f}(r)\hat{g}(r)\right| \\ &\leqslant \left(\sum_r |\hat{f}(r)|^4\right)^{1/4}\left(\sum_r |\hat{g}(r)|^{4/3}\right)^{3/4} \\ &= \|f\|_{U^2(G)}\left(\sum_r |\hat{g}(r)|^{4/3}\right)^{3/4}.\end{aligned}$$

Here the Fourier transform $\hat{f}(r) = \mathbb{E}_{x \in G} f(x)e(-rx/N')$ is the discrete Fourier transform on G, and we have used Hölder's inequality and the well-known fact (see, for example, [TV10, Chapter 11]) that $\|f\|_{U^2(G)} = \|\hat{f}\|_{\ell^4}$. Taking $g = 1_P$, the characteristic function of the progression P, it suffices to show that $\sum_r |\hat{g}(r)|^{4/3} = O(1)$. Dilating, we may assume that the common difference of P is 1. But then we have, upon summing the geometric progression, the bound $|\hat{g}(r)| \ll \min(1, |r|^{-1})$, from which the result follows immediately. □

The next lemma is a more complicated result along similar lines.

LEMMA A.9. *Suppose that $d, q, M \in \mathbb{N}$ and that $\delta > 0$. There for some $\delta_* = \delta_*(d, q, M, \delta) > 0$ and all sufficiently large $N \geqslant N_0(d, q, M, \delta)$, the following is true. Let $f(n) = F(n \pmod q, n/N, \theta n)$, where $F : \mathbb{Z}/q\mathbb{Z} \times [0,1] \times (\mathbb{R}/\mathbb{Z})^d \to [0,1]$ is M-Lipschitz and $\theta \in (\mathbb{R}/\mathbb{Z})^d$, and suppose $g : \{1, \dots, N\} \to [-1,1]$ satisfies $\|g\|_{U^2(N)} \leqslant \delta_*$. Then $|\mathbb{E}_{n \in N} f(n)g(n)| \leqslant \delta$.*

In other words, the "structured objects" and the "pseudorandom objects" of the regularity lemma do not correlate.

Proof sketch. As in the proof of Lemma A.4, the idea is to decompose F as a Fourier expansion of length $O_{\delta,d,q,M}(1)$, plus a uniformly small error:

$$F = \sum_{a,m,\mathbf{m}} c_{a,m,\mathbf{m}}\phi_{a,m,\mathbf{m}} + F_{\mathrm{sml}},$$

where $\phi_{a,m,\mathbf{m}}$ is given by (A.1), $|c_{a,m,\mathbf{m}}| \leqslant 1$ and $\|F_{\mathrm{sml}}\|_{\ell^\infty} \leqslant \frac{1}{2}\delta$. Note

$$\phi_{a,m,\mathbf{m}}(n \,(\mathrm{mod}\ q), n/N, \theta n) = e(\beta_+ n) + e(\beta_- n), \tag{A.5}$$

where $\beta_\pm = \frac{r}{q} \pm \frac{m}{2N} + \mathbf{m}\cdot\theta$ (though this exact form is unimportant). However, writing $e(\beta n) = e(\beta(n+h_1+h_2))e(-\beta h_1)e(-\beta h_2)$ and averaging over h_1, h_2, it follows by the Gowers-Cauchy-Schwarz inequality [TV10, Chap. 11] that $|\mathbb{E}_{n\leqslant N} e(\beta n)g(n)| \ll \|g\|_{U^2(N)}$ uniformly in $\beta \in \mathbb{R}$, so

$$|\mathbb{E}_{n\leqslant N}\phi_{a,m,\mathbf{m}}(n \,(\mathrm{mod}\ q), n/N, \theta n)g(n)| \ll \delta_*$$

uniformly in $a, m, \mathbf{m}$. It follows that

$$\begin{aligned}|\mathbb{E}_{n\leqslant N} f(n)g(n)| &= |\mathbb{E}_{n\in N} F(n \ (\mathrm{mod}\ q), n/N, \theta n)g(n)| \\ &\leqslant \sum_{a,m,\mathbf{m}} |\mathbb{E}_{n\leqslant N}\phi_{a,m,\mathbf{m}}(n \,(\mathrm{mod}\ q), n/N, \theta n)g(n)| + \tfrac{1}{2}\delta \\ &\leqslant O_{\delta,d,q,M}(\delta_*) + \delta/2,\end{aligned}$$

so for δ_* sufficiently small depending on δ, d, q and M, $|\mathbb{E}_{n\leqslant N} f(n)g(n)| \leqslant \delta$. □

Miscellany. We turn now to some rather miscellaneous lemmas. Recall that if $f : \{1, \dots, N\} \to \mathbb{C}$ is a function, then $T(f) = \mathbb{E}_{n,n'\leqslant N} f(n)f(n')f(n+n')$.

Lemma A.10. *Suppose that $f, \tilde{f} : \{1, \dots, N\} \to [-1, 1]$ are functions. Then $|T(f) - T(\tilde{f})| \leqslant 7\|f - \tilde{f}\|_{\ell^1(N)}$ and $|T(f) - T(\tilde{f})| \ll \|f - \tilde{f}\|_{U^2(N)}$.*

Recalling that $\|\cdot\|_{\ell^1(N)} \leqslant \|\cdot\|_{\ell^2(N)} \leqslant \|\cdot\|_\infty$, we also have $|T(f) - T(\tilde{f})| \leqslant 7\|f - \tilde{f}\|_{\ell^2(N)}$ and $|T(f) - T(\tilde{f})| \leqslant 7\|f - \tilde{f}\|_\infty$.

Proof. Write $g = f - \tilde{f}$. Writing $f = \tilde{f} + g$, $T(f)$ may be expanded as a sum of eight terms, one of which is $T(\tilde{f})$, the other seven of which are trilinear terms of the form $\mathbb{E}_{n,n'} f_1(n)f_2(n')f_3(n+n')$ with at least one of the f_i being equal to g. Using the hypothesis that all the f_i's are bounded by 1, the estimate

$$|\mathbb{E}_{n,n'} f_1(n)f_2(n')f_3(n+n')| \leqslant \|f_i\|_{\ell^1(N)}$$

is an easy consequence of the triangle inequality.

The case of the Gowers $U^2(N)$-norm is dealt with in a similar way, using instead the bound

$$|\mathbb{E}_{n,n'} f_1(n)f_2(n')f_3(n+n')| \ll \|f_i\|_{U^2(N)}.$$

This is an instance of a *generalised von Neumann theorem*, for which there are many references, including [TV10, Lemma 11.4]. □

LEMMA A.11. *Let X be a compact metric abelian group endowed with a translation-invariant metric d and a translation-invariant probability measure μ. Suppose that $f : X \to \mathbb{C}$ is a function with $\|f\|_{\mathrm{Lip}} \leqslant K$, thus $|f(x)-f'(x)| \leqslant Kd(x,x')$. Let $g : X \to \mathbb{C}$ be any continuous function with $\|g\|_\infty \leqslant 1$. Then the convolution $f * g(x) = \int f(y)g(x-y)d\mu(y)$ also has Lipschitz constant at most K.*

Proof. We have

$$\begin{aligned} f*g(x) - f*g(x') &= \int (f(x-y)-f(x'-y))g(y)d\mu(y) \\ &\leqslant \int |f(x-y)-f(x'-y)|d\mu(y) \\ &\leqslant K \sup_y d(x-y,x'-y) = Kd(x,x'). \end{aligned}$$ □

The next lemma is an instance of Young's inequality, but we include the (short) proof for ease of reference.

LEMMA A.12. *Let $P, P' \subset \{1,\dots,N\}$ be arithmetic progressions with the same length. Let $f : P \to \mathbb{C}$ and $g : P' \to \mathbb{C}$ be two functions. Suppose that both are bounded pointwise by 1 and that either $\mathbb{E}_{n\in P}|f(n)| \leqslant \eta$ or $\mathbb{E}_{n\in P'}|g(n)| \leqslant \eta$. Write $f*g(n) = \frac{1}{N}\sum_m f(m)g(n-m)$. Then $\|f*g\|_\infty \leqslant \eta|P|/N$.*

Proof. Suppose that $\mathbb{E}_{n\in P}|f(n)| \leqslant \eta$. Then we have

$$|f*g(n)| = \frac{1}{N}\left|\sum_m f(m)g(n-m)\right| \leqslant \frac{1}{N}\sum_m |f(m)| \leqslant \eta|P|/N.$$

The case $\mathbb{E}_{n\in P}|g(n)| \leqslant \eta$ is similar. □

LEMMA A.13. *Let $f, \tilde{f}, g : \{1,\dots,N\} \to [-1,1]$ be functions such that $\|\tilde{f}-f\|_{U^2(N)} \leqslant \delta$. Then $|\tilde{f}*g(d) - f*g(d)| \leqslant 4\delta^{1/2}$ for all except at most $40\delta N$ values of d.*

Proof. The functions f and g may be regarded as functions on $G = \mathbb{Z}/N'\mathbb{Z}$, where $N' = 4N$, in a natural way. Let $h = \tilde{f} - f$. Then

$$\begin{aligned} \mathbb{E}_{x\in G}|\mathbb{E}_{y\in G}h(y)g(x-y)|^2 &= \sum_r |\hat{h}(r)|^2|\hat{g}(r)|^2 \\ &\leqslant \left(\sum_r |\hat{h}(r)|^4\right)^{1/2}\left(\sum_r |\hat{g}(r)|^4\right)^{1/2} \\ &= \|h\|_{U^2(G)}^2\|g\|_{U^2(G)}^2 \leqslant \|h\|_{U^2(G)}^2 \leqslant 10\delta^2. \end{aligned}$$

Once again we have used basic facts about the $U^2(G)$-norm and the discrete Fourier transform as may be found in [TV10, §4.2]. Replacing the expectations over G by sums, we obtain

$$\sum_x |h * g(x)|^2 \leqslant 640\delta^2 N.$$

Thus there cannot be more than $40\delta N$ values of x for which $|h * g(x)| \geqslant 4\delta^{1/2}$. □

References

[Alo13] N. Alon, Paul Erdős and probabilistic reasoning, in *Erdős Centennial*, *Bolyai Soc. Math. Stud.* **25**, Springer-Verlag, New York, 2013, pp. 11–33. http://dx.doi.org/10.1007/978-3-642-39286-3_1.

[AK90] N. Alon and D. J. Kleitman, Sum-free subsets, in *A Tribute to Paul Erdős*, Cambridge Univ. Press, Cambridge, 1990, pp. 13–26. MR 1117002. Zbl 0718.11006. http://dx.doi.org/10.1017/CBO9780511983917.003.

[AS08] N. Alon and J. H. Spencer, *The Probabilistic Method*, third ed., *Wiley-Intersci. Ser. Discrete Math. Optim.*, John Wiley & Sons, Hoboken, NJ, 2008, with an appendix on the life and work of Paul Erdős. MR 2437651. Zbl 1148.05001. http://dx.doi.org/10.1002/9780470277331.

[Bil99] Y. Bilu, Structure of sets with small sumset, in *Structure Theory of Set Addition*, *Astérisque* **258**, Soc. Math. France, Paris, 1999, pp. xi, 77–108. MR 1701189. Zbl 0946.11004.

[Bou97] J. Bourgain, Estimates related to sumfree subsets of sets of integers, *Israel J. Math.* **97** (1997), 71–92. MR 1441239. Zbl 01011389. http://dx.doi.org/10.1007/BF02774027.

[CL07] E. S. Croot, III and V. F. Lev, Open problems in additive combinatorics, in *Additive Combinatorics*, *CRM Proc. Lecture Notes* **43**, Amer. Math. Soc., Providence, RI, 2007, pp. 207–233. MR 2359473. Zbl 1183.11005.

[Ebe] S. Eberhard, The abelian arithmetic regularity lemma, unpublished. Available at https://www.dpmms.cam.ac.uk/~se288/abelianregularity.pdf.

[Erd65] P. Erdős, Extremal problems in number theory, in *Proc. Sympos. Pure Math., Vol. VIII*, Amer. Math. Soc., Providence, R.I., 1965, pp. 181–189. MR 0174539. Zbl 0144.28103.

[Erd73] P. Erdős, Problems and results on combinatorial number theory, in *A Survey of Combinatorial Theory* (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, Colo., 1971), North-Holland, Amsterdam, 1973, pp. 117–138. MR 0360509. Zbl 0263.10001.

[Erd92] P. Erdős, Letter to Klarner, 1992. Available at http://www.plambeck.org/oldhtml/mathematics/klarner/ep/index.htm.

[Fre73] G. A. Freĭman, *Foundations of a Structural Theory of Set Addition*, Amer. Math. Soc., Providence, R. I., 1973, translated from the Russian, *Trans. Math. Monogr.* **37**. MR 0360496. Zbl 0271.10044.

[Gar02] R. J. Gardner, The Brunn-Minkowski inequality, *Bull. Amer. Math. Soc.* **39** (2002), 355–405. MR 1898210. Zbl 1019.26008. http://dx.doi.org/10.1090/S0273-0979-02-00941-2.

[GR05] B. Green and I. Z. Ruzsa, Sum-free sets in abelian groups, *Israel J. Math.* **147** (2005), 157–188. MR 2166359. Zbl 1158.11311. http://dx.doi.org/10.1007/BF02785363.

[GR06] B. Green and I. Z. Ruzsa, Sets with small sumset and rectification, *Bull. London Math. Soc.* **38** (2006), 43–52. MR 2201602. Zbl 1155.11307. http://dx.doi.org/10.1112/S0024609305018102.

[GT08] B. Green and T. Tao, Quadratic uniformity of the Möbius function, *Ann. Inst. Fourier* (*Grenoble*) **58** (2008), 1863–1935. MR 2473624. Zbl 1160.11017. http://dx.doi.org/10.5802/aif.2401.

[GT10] B. Green and T. Tao, An arithmetic regularity lemma, an associated counting lemma, and applications, in *An Irregular Mind*, *Bolyai Soc. Math. Stud.* **21**, János Bolyai Math. Soc., Budapest, 2010, pp. 261–334. MR 2815606. Zbl 1222.11015. http://dx.doi.org/10.1007/978-3-642-14444-8_7.

[Guy04] R. K. Guy, *Unsolved Problems in Number Theory*, third ed., *Problem Books in Math.*, Springer-Verlag, New York, 2004. MR 2076335. Zbl 1058.11001. http://dx.doi.org/10.1007/978-0-387-26677-0.

[Kol96] M. N. Kolountzakis, Some applications of probability to additive number theory and harmonic analysis, in *Number Theory* (New York, 1991–1995), Springer-Verlag, New York, 1996, pp. 229–251. MR 1420213. Zbl 0861.11015.

[Lev97] V. F. Lev, Optimal representations by sumsets and subset sums, *J. Number Theory* **62** (1997), 127–143. MR 1430006. Zbl 0868.11017. http://dx.doi.org/10.1006/jnth.1997.2012.

[LS95] V. F. Lev and P. Y. Smeliansky, On addition of two distinct sets of integers, *Acta Arith.* **70** (1995), 85–91. MR 1318763. Zbl 0817.11005.

[Lew10] M. Lewko, An improved upper bound for the sum-free subset constant, *J. Integer Seq.* **13** (2010), Article 10.8.3, 15. MR 2718234. Zbl 1216.11029. Available at https://cs.uwaterloo.ca/journals/JIS/VOL13/Lewko/lewko3.pdf.

[Mac53] A. M. Macbeath, On measure of sum sets. II. The sum-theorem for the torus, *Proc. Cambridge Philos. Soc.* **49** (1953), 40–43. MR 0056670. Zbl 03083529. http://dx.doi.org/10.1017/S0305004100028012.

[Mal94] J. L. Malouf, *Combinatorial Approaches to Integer Sequences*, ProQuest LLC, Ann Arbor, MI, 1994, Ph.D. thesis, University of Illinois at Urbana-Champaign. MR 2691850. Available at http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:9512476.

[Ruz91] I. Z. Ruzsa, Diameter of sets and measure of sumsets, *Monatsh. Math.* **112** (1991), 323–328. MR 1141099. Zbl 0737.28006. http://dx.doi.org/10.1007/BF01351772.

[Sár89] A. Sárközy, Finite addition theorems. I, *J. Number Theory* **32** (1989), 114–130. MR 1002119. Zbl 0674.10042. http://dx.doi.org/10.1016/0022-314X(89)90102-9.

[Taoa] T. Tao, A variant of Kemperman's theorem, blog post. Available at http://terrytao.wordpress.com/2011/12/26/a-variant-of-kempermans-theorem/.

[Taob] T. Tao, *Spending Symmetry*, in preparation. Available at http://terrytao.wordpress.com/books/spending-symmetry/.

[TV10] T. Tao and V. H. Vu, *Additive Combinatorics*, *Cambridge Stud. Adv. Math.* **105**, Cambridge Univ. Press, Cambridge, 2010, paperback edition of [MR 2289012]. MR 2573797. Zbl 1179.11002. http://dx.doi.org/10.1017/CBO9780511755149.

(Received: January 22, 2013)
(Revised: September 5, 2013)

Mathematical Institute, University of Oxford, Oxford, United Kingdom
E-mail: eberhard@maths.ox.ac.uk

Mathematical Institute, University of Oxford, Oxford, United Kingdom
E-mail: ben.green@maths.ox.ac.uk

Mathematical Institute, University of Oxford, Oxford, United Kingdom
E-mail: manners@maths.ox.ac.uk