ACTA ARITHMETICA
171.3 (2015)

A structure theorem for sets of small popular doubling

by

Przemysław Mazur (Oxford)

1. Introduction. Let us start by recalling Freiman's $3k-3$ Theorem. It states that every finite subset $A \subset \mathbb{Z}$ satisfying $|A+A| < 3|A|-3$ is contained in an arithmetic progression of length $|A+A|-|A|+1$. Comparing this with the lower bound $|A+A| \geq 2|A|-1$ valid for all nonempty finite subsets of $\mathbb{Z}$, we can see that this result concerns sets for a quite large range of values of $|A+A|$. Our goal is to give a similar result for a set with a few *popular* sums. Note that it cannot be done directly; the reason is that the set $S_k(A) = \{x \in \mathbb{Z} : |A \cap (x-A)| \geq k\}$ of k-popular sums is empty if $k \geq 3$ and A is a highly independent set. Instead, we need to consider a different quantity, namely the *average* size of S_k for $1 \leq k \leq t$, which also appeared quite natural to Pollard [Pol74] back in 1974.

At this point it is convenient to use the notion of convolution. From now on, we will consider any abelian group G to be equipped with the counting measure, which leads to the definition

$$f * g(x) = \sum_{y \in G} f(y)g(x-y)$$

for any functions $f, g : G \to \mathbb{C}$ for which the above expression makes sense (i.e. is absolutely convergent; we will use it mostly for f, g being indicator functions of finite sets). Having this notation, we can restate Pollard's Theorem as

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \min(1_A * 1_B(x), t) \geq \min(|A| \cdot |B|, t \cdot \min(p, |A|+|B|-t))$$

for any prime p and sets $A, B \subset \mathbb{Z}/p\mathbb{Z}$. It is not hard to prove the corresponding statement for subsets of the integers (and even easier to deduce it from Pollard's Theorem); in particular, for a single set $A \subset \mathbb{Z}$ and an integer $0 \leq t \leq |A|$ we have $\sum_{x \in \mathbb{Z}} \min(1_A * 1_A(x), t) \geq t(2|A|-t)$. One

2010 *Mathematics Subject Classification*: Primary 11P70.
Key words and phrases: small popular doubling, structure theorem, coset, progression, regularity lemma.

DOI: 10.4064/aa171-3-2

can also prove (or deduce from Vosper's Theorem [Vos56], a corresponding statement for $\mathbb{Z}/p\mathbb{Z}$) that the only sets for which we have equality in the above inequality are arithmetic progressions.

Our goal is to extend this structure theorem to be able to recognize sets $A \subset \mathbb{Z}$ satisfying $\sum_{x\in\mathbb{Z}} \min(1_A * 1_A(x), t) \le (2+\delta)t|A|$ for suitable ranges of parameters t and δ as those that can be almost entirely covered by an arithmetic progression. Specifically, for $t/|A| \searrow 0$ we can pick δ as big as $1/4 - O(t/|A|)$. Note that we cannot expect all of A to be covered by an arithmetic progression: a simple counterexample is an arithmetic progression with one extra point as far away as we like. The reader can check that for that set and t, $|A|/t$ sufficiently large, the parameter δ can be as close to 0 as we like, yet our set cannot be covered with an arithmetic progression of bounded length.

In the next sections we use this result to slightly modify the regularity lemma proven by Green and Morris [GM15], which allows us to improve the estimates on the probability that a sumset of a random subset A of natural numbers misses at least k elements. More precisely, we will show not only that the sequence $p_k = 2^{k/2} \cdot \mathbb{P}(|\mathbb{N} \setminus (A+A)| \ge k)$ is bounded, but also that it is increasing (and therefore convergent) along indices of the same parity (i.e. odd or even).

Before proceeding, let us state precisely the results to be proven.

Theorem 1.1. *Let $S \subset \mathbb{Z}$ be a set of size $N > 0$ and let t be a positive integer. Suppose that*

$$\sum_{x\in\mathbb{Z}} \min(1_S * 1_S(x), t) \le (2+\delta)Nt$$

for some $\delta > 0$. Then there is an arithmetic progression P of length at most $(1+2\delta)N + 6t$ containing all but at most $5t/2$ points of S, provided that $\delta + 5t/N \le 1/4$.

Theorem 1.2. *Let $A \subset \mathbb{N}$ be a set chosen randomly by picking each element of $\mathbb{N}$ independently with probability $1/2$. Define*

$$p_k = 2^{k/2}\mathbb{P}(|\mathbb{N} \setminus (A+A)| \ge k).$$

Then the subsequences $\{p_{2k}\}$ and $\{p_{2k+1}\}$ are both increasing and bounded and therefore convergent. In particular $\mathbb{P}(|\mathbb{N} \setminus (A+A)| \ge k) = \Theta(2^{-k/2})$ and the implied constants can only oscillate between c and $c\sqrt{2}$ for some $c > 0$ as $k \to \infty$.

2. Wrapping argument. In this section we start proving Theorem 1.1 with similar methods that Lev and Smeliansky [LS95] used to prove (a generalisation of) Freiman's $3k-3$ Theorem. More precisely, their first step was to wrap the set S modulo $q := \max S - \min S$ and consider a subset of a finite group instead. Note that since the sets $S+\min S$ and $S+\max S$ share only one element, this wrapping procedure results in a huge decrement in the doubling constant. In our situation, taking just two endpoints would be too careless to achieve good results; luckily we can still find two points near the ends such that wrapping modulo their difference gives us what we need.

PROPOSITION 2.1. *Let $S \subset \mathbb{Z}$ be a finite set and suppose that $N := |S| > 0$. Let t be a positive integer satisfying $2t < N$ and suppose that*

$$\sum_{x\in\mathbb{Z}} \min(1_S * 1_S(x), t) \le (2+\delta)Nt$$

for some $\delta \ge 0$. Then there exist a positive integer n and an integer x such that the set $S' = (S \cap [x, x+n)) \pmod{n}$ (the image of $S \cap [x+n)$ under the projection modulo n) satisfies the following conditions:

- $|S'| \ge N - 2t$,
- $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} \min(1'_S * 1'_S(x), t) \le (1 + 2\delta + 6t/N)Nt.$

In the final statement the parameter δ comes with coefficient 2, which leads to some limitations in the statement of Theorem 1.1, such as $\delta < 1/4$. We believe that this argument can be modified to give the coefficient 1, which would extend the range of δ up to $1/2$ and consequently allow us to prove the corresponding statement in a finite group of prime order using similar methods (for that we need to let $\delta > 6 - 4\sqrt{2} > 1/3$).

Proof of Proposition 2.1. Divide S into three subsets A, B, C with $|A| = |C| = t$, $|B| = N - 2t$, $\max A < \min B$, $\max B < \min C$ (intuitively they are the left, middle and right part respectively). Let f, g, h be the corresponding indicator functions (i.e. $f = 1_A$, $g = 1_B$, $h = 1_C$). Substituting them into the convolution we get

$$1_S * 1_S = (f+g+h) * (f+g+h) \ge 2(f*g + g*h),$$

where the inequality comes from discarding some of the positive summands. Note that since $\max(A+B) < \max(B+C)$, the functions $f*g$ and $g*h$ are supported on disjoint sets and therefore the above implies

$$\sum_{x\in\mathbb{Z}} \min(2f*g(x), t) + \sum_{x\in\mathbb{Z}} \min(2g*h(x), t) \le \sum_{x\in\mathbb{Z}} \min(1_S * 1_S(x), t) \le (2+\delta)Nt.$$

Now we use the easy inequality $s^2 \ge t(2s - \min(2s, t))$, valid for all real s. Specifically, we substitute $s = f*g(x)$ and $s = g*h(x)$ for all $x \in \mathbb{Z}$ and add them up to get

$$\sum_{x\in\mathbb{Z}} (f*g)^2(x) + \sum_{x\in\mathbb{Z}} (g*h)^2(x) \ge t(4t(N-2t) - (2+\delta)Nt) = (2-\delta)Nt^2 - 8t^3.$$

Here we have also used the previous estimate and the formula $\sum_{x\in\mathbb{Z}} f*g(x) = \sum_{x\in\mathbb{Z}} g*h(x) = t(N-2t)$. Note that since each $x\in\mathbb{Z}$ can be written in exactly $f*g(x)$ ways as a sum $x=a+b$ for $a\in A$ and $b\in B$ (and similarly for $g*h$), the above expression is in fact equal to

$$\sum_{x\in\mathbb{Z}}(f*g)^2(x)+\sum_{x\in\mathbb{Z}}(g*h)^2(x)=\sum_{a\in A}\sum_{b\in B} f*g(a+b)+\sum_{c\in C}\sum_{b\in B} g*h(b+c).$$

By choosing $a\in A$ and $c\in C$ for which the inner sums are above average, we can see that

$$\sum_{b\in B} f*g(a+b)+\sum_{b\in B} g*h(b+c)\geq(2-\delta)Nt-8t^2$$

for some a and c (as $|A|=|C|=t$). Since $f*g$ and $g*h$ are bounded by both 1_S*1_S and t, we have actually proved that

$$\sum_{x\in(a+B)\cup(c+B)}\min(1_S*1_S(x),t)\geq(2-\delta)Nt-8t^2.$$

This is just enough to define the wrapping procedure. Indeed, projection modulo $c-a$ merges the sets $a+B$ and $c+B$ into a single copy of B, on which the sum of the values of the above function cannot exceed $t|B|=t(N-2t)$. After a short calculation $(2+\delta)Nt-((2-\delta)Nt-8t^2)+t(N-2t)=(1+2\delta)Nt+6t^2$ we see that the set S' for $x=a$ and $n=c-a$ satisfies

$$\sum_{x\in\mathbb{Z}}\min(1_{S'}*1_{S'}(x),t)\leq(1+2\delta)Nt+6t^2. \blacksquare$$

Now our goal is to show that S' is close to a coset of a subgroup of $\mathbb{Z}/n\mathbb{Z}$ which would correspond to a progression in $\mathbb{Z}$. We will deal with that problem in the next section.

3. Popular doubling less than 3/2.

3. Popular doubling less than $3/2$. The next step of the proof by Lev and Smeliansky was to use Kneser's Theorem stating that for any finite subsets A,B of an abelian group G the subgroup of all elements h satisfying $A+B+h=A+B$ has cardinality at least $|A|+|B|-|A+B|$ (cf. [Kne53]). The proof of that theorem requires checking a lot of scenarios and it is not clear how one could modify it to work for popular sums. On the contrary, the proof of a weaker statement that if $|A|=|B|=N$ and $|A+B|<\frac{3}{2}N$ then $A+B$ is a coset of a subgroup is much easier and, as it turns out, generalisable to our setting. Specifically, in this section we will proceed towards the following statement.

Proposition 3.1. *Let G be an abelian group and let $A,B\subset G$ be sets of size $N>0$. Let $t,\eta>0$ be real numbers satisfying $\eta+t/N\leq 1/2$. Moreover,* *suppose that*

$$\sum_{x\in G}\min(1_A*1_B(x),t)\le(1+\eta)Nt.$$

Then there exists a subgroup $H\le G$ and cosets C_A and C_B of H such that:

- $|H|\le(1+\eta)N$,
- $|A\setminus C_A|+|B\setminus C_B|\le t$.

Note that in this section we do not require t to be an integer anymore. Let us also remark that we only need the above statement for $A=B$, but the proof of the general case is not much harder so we decided to include it here. For convenience of the reader we split it into several lemmas. First of all we want to find the subgroup H. Although the statement of the following lemma appears to be new, the methods going into its proof were used in [Fou77].

Lemma 3.2. *Let G be an abelian group and let $A,B\subset G$ be sets of size $N>0$. Let $t,\eta>0$ be real numbers satisfying $\eta+t/N\le1/2$. Moreover, suppose that*

$$\sum_{x\in G}\min(1_A*1_B(x),t)\le(1+\eta)Nt.$$

Then there exists a subgroup $H\le G$ such that:

- $1_A*1_{-A}(x)\ge(1-\eta)N$ *and* $1_B*1_{-B}(x)\ge(1-\eta)N$ *for all* $x\in H$,
- $1_A*1_{-A}(x)<2t$ *and* $1_B*1_{-B}(x)<2t$ *for all* $x\in G\setminus H$.

Before we proceed, let us observe that the triangle inequality for the symmetric difference of sets $|V\triangle W|\le|U\triangle V|+|U\triangle W|$ can be rearranged as

$$|U\cap V|+|U\cap W|\le|U|+|V\cap W|.$$

We will frequently use a variant of this inequality, namely

$$|U\cap(V-v)|+|U\cap(W-w)|\le|U|+|V\cap(W-w+v)|$$

for various choices of v,w. We will refer to all such statements as the triangle inequality.

Proof. Set $D=\{x\in G:1_A*1_B(x)\ge t\}$. Note that D contains most of the sums $a+b$: more precisely,

$$\begin{aligned}&\#\{(a,b)\in A\times B:a+b\in D\}\\&\quad=\sum_{x\in D}1_A*1_B(x)=\sum_{x\in D}t+\sum_{x\in G}\max(1_A*1_B(x)-t,0)\\&\quad=t|D|+\sum_{x\in G}1_A*1_B(x)-\sum_{x\in G}\min(1_A*1_B(x),t)\ge t|D|+N^2-(1+\eta)Nt.\end{aligned}$$

Now let $H = \{x \in G : 1_A * 1_{-A}(x) \geq 2t\}$. We will show that for any $h \in H$ we have $1_B * 1_{-B}(x) \geq (1-\eta)N$. Let us start by noticing that for any $a \in A \cap (A+h)$ we have

$$|B \cap (B+h)| \geq |(B+a) \cap D| + |(B+a+h) \cap D| - |D|$$

by the triangle inequality. Now let $f : G \to [0,1]$ be an auxiliary function supported on $A \cap (A+h)$ and satisfying the condition $\sum_{x\in G} f(x) = 2t$ (there exists one by choice of h). Multiplying the above inequality by $f(a)$ and adding them up over A we get

$$2t|B \cap (B+h)| \geq \sum_{a\in A} (f(a) + f(a-h))|(B+a) \cap D| - 2t|D|.$$

Now we combine the inequalities

$$\sum_{a\in A} 2|(B+a) \cap D| \geq 2t|D| + 2N^2 - 2(1+\eta)Nt,$$

$$\sum_{a\in A} (2 - f(a) - f(a-h))|(B+a) \cap D| \leq |B| \sum_{a\in A} (2 - f(a) - f(a-h)) = N(2N - 4t)$$

to get

$$|B \cap (B+h)| \geq \frac{2t|D| + 2N^2 - 2(1+\eta)Nt - (2N^2 - 4Nt) - 2t|D|}{2t} = (1-\eta)N.$$

In a similar way we can prove that $1_B * 1_{-B}(x) \geq 2t$ implies $1_A * 1_{-A} \geq (1-\eta)N$. Since $(1-\eta)N \geq 2t$, we have just constructed the set H satisfying all the postulated inequalities. It remains to show that H is a subgroup. This follows from the triangle inequality: if $h_1, h_2 \in H$, then

$$|A \cap (A + h_1 - h_2)| \geq |A \cap (A+h_1)| + |A \cap (A+h_2)| - |A| \geq 2(1-\eta)N - N = (1-2\eta)N \geq 2t,$$

and consequently $h_1 - h_2 \in H$. ∎

Let us now turn for a moment to some estimates of expressions of the form $\sum_{x\in G} \min(F(x), t)$.

LEMMA 3.3. *Let G be an abelian group and let $F : G \to [0, M]$ satisfy $\sum_{x\in G} F(x) < \infty$. Then for any $t \in [0, M]$ we have*

$$\sum_{x\in G} \min(F(x), t) \geq \frac{t}{M} \sum_{x\in G} F(x).$$

Proof. Notice that $\frac{t}{M}F(x) \leq \min(t, F(x))$ for each individual x. ∎

Corollary 3.4. *Let G be an abelian group and let $F : G \to [0, \infty)$ satisfy $\sum_{x\in G} F(x) < \infty$. Then for any $t' > t > 0$ we have*

$$\sum_{x\in G} \min(F(x), t) \geq \frac{t}{t'} \sum_{x\in G} \min(F(x), t').$$

Proof. Just use the above lemma for $\min(F(x), t')$. ■

Corollary 3.5. *Let G be an abelian group and let $A, B \subset G$ be sets of size $N > 0$. Let $t, \eta > 0$ be real numbers satisfying $\eta + t/N \leq 1/2$. Moreover, suppose that*

$$\sum_{x\in G} \min(1_A * 1_B(x), t) \leq (1 + \eta)Nt.$$

Then for any $t' > t$ we have

$$\sum_{x\in G} \min(1_A * 1_B(x), t') \leq (1 + \eta)Nt'.$$

Let us go back to our main considerations. We have already constructed a set D containing most of the sums $a + b$ and the subgroup H satisfying certain inequalities. Now it is time to construct a *coset* C of H containing most of the sums $a + b$. We will do it in two steps: first we show that C contains just enough sums to perform calculations quite accurately, which in turn will give us the cosets C_A and C_B with the desired properties.

Lemma 3.6. *Let G be an abelian group and let $A, B \subset G$ be sets of size $N > 0$. Let $t, \eta > 0$ be real numbers satisfying $\eta + t/N \leq 1/2$. Moreover, suppose that*

$$\sum_{x\in G} \min(1_A * 1_B(x), t) \leq (1 + \eta)Nt.$$

Then there exists a coset C of a subgroup H satisfying $|C| \leq (1 + \eta)N$ and

$$\#\{(a, b) \in A \times B : a + b \in C\} > (1 + \eta)N^2/2.$$

Proof. Let H be the subgroup constructed in Lemma 3.2. We want to translate H to make it contain most of the sums $a+b$, so a reasonable choice is to take $x_0 \in G$ for which $1_A * 1_B(x_0)$ is maximal and set $C = H + x_0$. Let $k = N - 1_A * 1_B(x_0)$. Note that by the previous considerations for any $t' < N/(1 + \eta)$ we have

$$\sum_{x\in G} \min(1_A * 1_B(x), t') < N^2 = \sum_{x\in G} 1_A * 1_B(x),$$

which implies $1_A * 1_B(x_0) \geq N/(1 + \eta)$ or in other words $k \leq \eta N/(1 + \eta)$. Moreover, by the triangle inequality, $|1_A * 1_B(x + x_0) - 1_A * 1_{-A}(x)| \leq k$; in particular C contains the set $C' = \{x \in G : 1_A*1_B(x) \geq 2t+k\}$. Therefore we are interested in the size of the set $\#\{(a,b)\in A\times B : a+b\in C'\}$. By the same calculations as for the set D in the proof of Lemma 3.2 we know that

$$\#\{(a,b)\in A\times B : a+b\in C'\} \ge N^2-(1+\eta)N(2t+k)+(2t+k)|C'|.$$

Here we have also used the previous corollary with $t'=2t+k$. Let us bound the size of C' from below. We know that

$$\begin{aligned} N^2 &= \sum_{x\in G} 1_A * 1_B(x) \\ &= \sum_{x\in G} \min(1_A*1_B(x), 2t+k) + \sum_{x\in C'} (1_A*1_B(x)-(2t+k)) \\ &\le (1+\eta)N(2t+k)+|C'|(N-2t-2k), \end{aligned}$$

which rearranges to $|C'| \ge \frac{N(N-(1+\eta)(2t+k))}{N-2t-2k}$. Substituting this into the previous bound we get

$$\#\{(a,b)\in A\times B : a+b\in C'\} \ge N^2 - \frac{N(2t+k)(\eta N-(1+\eta)k)}{N-2t-2k}.$$

It is easy to check that the right hand side is a decreasing function in t, so we can substitute $t=(1/2-\eta)N$ to get

$$\#\{(a,b)\in A\times B : a+b\in C'\} \ge N^2 - \frac{N((1-2\eta)N+k)(\eta N-(1+\eta)k)}{2(\eta N-k)}.$$

Now it is also easy to see that this being greater than $\frac{1+\eta}{2}N^2$ is equivalent to $(\eta N-k)^2+(1-2\eta)\eta Nk+\eta k^2>0$, which is true because we have assumed $\eta>0$.

Now we only need to bound the size of C; by the triangle inequality it is contained in $C''=\{x\in G : 1_A*1_B(x)\ge(1-\eta)N-k\}$, so using the corollary with $t'=(1-\eta)N-k>t$ we get

$$\begin{aligned} t'|C| \le t'|C''| &= \sum_{x\in C''} \min(1_A*1_B(x), t') \\ &\le \sum_{x\in G} \min(1_A*1_B(x), t') \le (1+\eta)Nt'. \end{aligned}$$

Thus we have proved both the desired inequalities. ■

Proof of Proposition 3.1. Let H and C be as above. By an averaging argument, there exist $a\in A$ and $b\in B$ with $|(A+b)\cap C|>\frac{1+\eta}{2}N$ and $|(B+a)\cap C|>(1+\eta)/2$. Define $C_A=C-b$ and $C_B=C-b$. Now let us estimate the sum of $\min(1_A*1_B(x),t)$ separately on and outside C_A+C_B. To do so, let $f,g,h : G\to[0,1]$ be auxiliary functions supported on C_B,

$G\setminus C_B$ and $G\setminus C_A$ respectively, satisfying $f,g\le 1_B$, $h\le 1_A$ and

$$\begin{aligned}&\sum_{x\in G} f(x)=t,\\ &\sum_{x\in G} g(x)=\min(|B\setminus C_B|,t),\\ &\sum_{x\in G} h(x)=\min\Big(|A\setminus C_A|,t-\sum_{x\in G} g(x)\Big).\end{aligned}$$

Now we have the following estimates:

$$\begin{aligned}\sum_{x\in C_A+C_B}\min(1_A*1_B(x),t)&\ge\sum_{x\in C_A+C_B}1_{A\cap C_A}*f(x)>\frac{(1+\eta)Nt}{2},\\ \sum_{x\notin C_A+C_B}\min(1_A*1_B(x),t)&\ge\sum_{x\notin C_A+C_B}(1_{A\cap C_A}*g(x)+1_{B\cap C_B}*h(x))\\ &>\frac{(1+\eta)N}{2}\sum_{x\in G}(g(x)+h(x)).\end{aligned}$$

Comparing these with the initial estimate

$$\sum_{x\in G}\min(1_A*1_B(x),t)\le(1+\eta)Nt$$

we see that $\sum_{x\in G}(g(x)+h(x))<t$, which is only possible if $\sum_{x\in G}g(x)=|B\setminus C_B|$ and $\sum_{x\in G}h(x)=|A\setminus C_A|$. Therefore $|A\setminus C_A|+|B\setminus C_B|<t$.

To finish the proof, notice that $|H|=|C|\le(1+\eta)N$. ■

Before proceeding, let us remark that in fact the larger the subgroup H, the fewer points of A and B are allowed to lie outside C_A and C_B respectively. One can try to calculate even more precisely, using the fact that now actually $1_A*1_B(x)\ge t$ for all $x\in C=C_A+C_B$. However, we do not need it, so we leave the result as it is.

4. Completing the proof of Theorem 1.1. Suppose we have the set S for which $\sum_{x\in\mathbb{Z}}\min(1_S*1_S(x),t)\le(2+\delta)Nt$. We use Lemma 2.1 to obtain a set $S'\subset\mathbb{Z}/n\mathbb{Z}$ of size at least $N-2t$ satisfying $\sum_{x\in\mathbb{Z}}\min(1_{S'}*1_{S'}(x),t)\le(1+2\delta)Nt+6t^2$. We see that the assumptions of Proposition 3.1 are satisfied with $A=B=S'$ as long as

$$\frac{1}{2}\ge\frac{(1+2\delta)N+6t-|S'|}{|S'|}+\frac{t}{|S'|}=\frac{(1+2\delta)N+7t-|S'|}{|S'|},$$

in other words $3|S'|\ge(2+4\delta)N+14t$, which is certainly true if $\delta+5t/N\le 1/4$. Proposition 3.1 then tells us that S' is essentially contained in a coset of a subgroup of size at most $(1+2\delta)N+6t$, with the exception of at most $t/2$ points. Unwrapping the situation back again, we see that S has all but at most $5t/2$ elements contained in an arithmetic progression of length at most $(1+2\delta)N+6t$. ∎

5. Regularity and counting sets with small sumset. This section is devoted to a lemma of Green and Morris on counting subsets of a cyclic group of prime order satisfying certain bounds on the size of the subset. Unfortunately we cannot just quote their result, as we need a slight modification of it. Therefore we need to move back to the statement of the regularity lemma, or more precisely to [GM15, Theorem 2.1], stated below.

Lemma 5.1 (Green–Morris, regularity lemma). *For every $\varepsilon > 0$, there exists $\delta = \delta(\varepsilon) > 0$ such that the following is true. Let $p > p_0(\varepsilon)$ be a sufficiently large prime and let $A \subset \mathbb{Z}/p\mathbb{Z}$ be a set. There is a dilate $A^* = \lambda A$ and a prime q with $1/\varepsilon^{10} \le q \le p^{1-\delta}$ such that the following holds. If $A_i^* = A^* \cap I_i(q)$ for each $i \in \mathbb{Z}/q\mathbb{Z}$ then, for at least $(1-\varepsilon)q^2$ pairs $(i,j) \in (\mathbb{Z}/q\mathbb{Z})^2$,*

$$\min(|A_i^*|, |A_j^*|) \le \varepsilon p/q \quad \textit{or} \quad |A_i^* + A_j^*| \ge (2-\varepsilon)p/q.$$

Here we adopted the notation $I_i(q) = \{x \in \mathbb{Z}/p\mathbb{Z} : x/p \in [i/q, (i+1)/q)\}$. Note that $[i/q,(i+1)/q)+[j/q,(j+1)/q) \subset [(i+j)/q,(i+j+2)/q)$ as subsets of $\mathbb{R}/\mathbb{Z}$; intersecting those sets with $\mathbb{Z}/q\mathbb{Z}$ embedded in $\mathbb{R}/\mathbb{Z}$ in a natural way, we get the inclusion $I_i + I_j \subset I_{i+j} \cup I_{i+j+1}$.

It is now time to prove some bounds on the number of sets having fixed size and whose sumset also has fixed size. We cannot improve the bound given by Green and Morris; instead we will introduce a better bound for the number of *exceptional* sets and at the same time use our result to prove that every nonexceptional set has a certain structure. Specifically, we will proceed towards the proof of the following statement.

Proposition 5.2. *Let $\delta > 0$ and let $N > N_0(\delta)$ be a large natural number. For every $k, m \in \mathbb{N}$ satisfying $\delta N \le k \le N$ and $2k-1 \le m \le 2N-1$ the following is true. The family of all subsets $X \subset \{1,\dots,N\}$ with $|X| = k$ and $|X+X| = m$ can be divided into two classes; one of them, the class of exceptional subsets, has cardinality at most $2^{(m/2)H((2k-1)/m)-\delta N}$, and each nonexceptional set (member of the other class) is almost contained in an arithmetic progression P of length at most $(1+1200\delta)m/2$, so that*

$$|(X+X) \setminus (P+P)| \le 24\delta N.$$

For the definition of the function H see the Appendix.

Before we proceed, let us make a few remarks. Firstly, our result is only valid in subsets of integers and not in cyclic groups of prime order; the reason is that Theorem 1.1 is of the same kind. Secondly, even in that case it does not improve the estimate of Green and Morris on the number of *all* subsets with $|X| = k$ and $|X + X| = m$; however, the additional structure allows us to prove Theorem 1.2.

Since we are following Green and Morris's argument, we will also need Pollard's Theorem. It has already appeared in the introduction, but let us state it once again in a somewhat more precise form.

THEOREM 5.3 (Pollard). *Let p be a prime number and let $A, B \subset \mathbb{Z}/p\mathbb{Z}$ be two sets. Let t be an integer satisfying*

$$\max(0, |A| + |B| - p) \leq t \leq \min(|A|, |B|).$$

Then

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \min(1_A * 1_B(x), t) \geq t(|A| + |B| - t).$$

Also, since Theorem 1.1 refers to subsets of integers, we have to make it more compatible with the regularity lemma, which refers to subsets of a finite group. To link those two statements, we prove the following lemma.

LEMMA 5.4. *Let p be a prime and let $P, Q \subset \mathbb{Z}/p\mathbb{Z}$ be arithmetic progressions satisfying $|P| \leq p/4$ and $|P \cap Q| \geq |Q|/2 + 1$. Then the set $P \cap Q$ is an arithmetic progression with the same common difference as Q.*

Proof. By dilating if necessary, we can assume that P is an interval (i.e. the common difference of P is 1). Since $|P \cap Q| \geq |Q|/2 + 1$, there are two consecutive elements of Q that belong to P. That means that the common difference of Q, say d, is less than the size of P. Suppose for a contradiction that $P \cap Q$ is not a progression of common difference d. In other words, if we look at the elements of Q in order, we see at least two separate groups of elements of $P \cap Q$ with at least one element of $Q \setminus P$ in between. Since the common difference of Q is d, each group of elements of $P \cap Q$ has cardinality at most $\lceil |P|/d \rceil$ and each group of elements of $Q \setminus P$ (maybe except those containing the endpoints) has cardinality at least $\lfloor (p - |P|)/d \rfloor$. Also, if we dentote $l = \lceil |P|/d \rceil$, then

$$\left\lfloor \frac{p - |P|}{d} \right\rfloor > \frac{p - |P|}{d} - 1 \geq \frac{3|P|}{d} - 1 > 3\left\lceil \frac{|P|}{d} \right\rceil - 4 = 3l - 4,$$

so in fact $\lfloor (p - |P|)/d \rfloor \geq 3l - 3$. From $d < |P|$ we know that $l \geq 2$. Now denoting by $k \geq 2$ the number of groups of elements of $P \cap Q$, we see that the number of groups of $Q \setminus P$ not containing the endpoints is $k - 1$. By assumption $Q \setminus P$ has at least two elements less than $P \cap Q$, which leads to

$$kl \geq |P \cap Q| \geq |Q \setminus P| + 2 \geq (k - 1)(3l - 3) + 2.$$

Rearranging gives $(2k - 3)(2l - 3) \leq -1$, which is impossible since both of the factors are positive. ■

Proof of Proposition 5.2. Suppose that $\delta > 0$ is a sufficiently small constant. Let $N > N_0(\delta)$ be a large natural number and let $p \in [8N, 16N]$ be a prime. We consider each subset of $[N]$ to be a subset of $\mathbb{Z}/p\mathbb{Z}$ via the natural embedding $[N] \hookrightarrow \mathbb{Z}/p\mathbb{Z}$. Then for a subset $A \subset [N]$ with $|A| \geq \delta N$ we can use the regularity lemma with $\varepsilon = 2^{-7}\delta^4$ to obtain a dilate $A^* = \lambda A$, a prime number q and a corresponding partition $A_i^* = A^* \cap I_i$. We can assume that N_0 is so large that $q \leq \delta^2 p$. We know that for at least $(1-\varepsilon)q^2$ pairs $(i,j) \in (\mathbb{Z}/q\mathbb{Z})^2$, either

$$\min(|A_i^*|, |A_j^*|) \leq \varepsilon L \quad \text{or} \quad |A_i^* + A_j^*| \geq (2-\varepsilon)L,$$

where $L = p/q$. Now let $S = \{i \in \mathbb{Z}/q\mathbb{Z} : |A_i^*| > \varepsilon L\}$. We will call the set A *exceptional* if $|S| \leq (1/2 - 2\delta)mq/p$, and *nonexceptional* otherwise. Now we need to check that those two classes actually have the postulated properties.

The number of exceptional subsets can be estimated as follows. First we choose a prime $q \leq \delta^2 p$, then we choose a set $S \subset \mathbb{Z}/q\mathbb{Z}$ of size at most $(1/2 - 2\delta)mq/p$; there are at most 2^q ways of doing that. Having chosen S, we specify A^* by choosing $A^* \cap S'$ and $A^* \setminus S'$, where $S' = \bigcup_{i \in S} I_i$. We take into account that $|A^* \setminus S'| \leq \varepsilon p$ to deduce that the number of choices of A^* is bounded by

$$\sum_{q \leq \delta^2 p} \left(2^q \sum_{j \leq \varepsilon p} \binom{p}{j} \binom{\lfloor (1/2-\delta)(1+q/p)m \rfloor}{k-j} \right).$$

The bound $|S'| \leq (1/2 - 2\delta)(1 + q/p)m$ comes from the fact that S' is a union of at most $(1/2-\delta)mq/p$ sets of size at most $p/q+1$ each. Since A is a dilate of A^*, the bound for the number of exceptional subsets is p times the above quantity. Using the estimates from the Appendix, we get the claimed bound.

Now let us turn to nonexceptional sets. Suppose that for a set A the regularity lemma gave us a set S with $|S| > (1/2 - 2\delta)mq/p$. We would like to show that S is Freiman 2-isomorphic to a set of integers and satisfies the assumption of Theorem 1.1. To prove the former, note that by definition of ε-regularity there has to be at least one pair i, j with $|A_i^* + A_j^*| \geq (2-\varepsilon)p/q$. The set $A_i^* + A_j^*$ is contained both in $I_{i+j} \cup I_{i+j+1}$ and in $A^* + A^* \subset \{2\lambda, 3\lambda, \ldots, 2N\lambda\}$. These are progressions satisfying the assumptions of Lemma 5.4; in that case we can argue that the intersection $(I_{i+j} \cup I_{i+j+1}) \cap \{2\lambda, 3\lambda, \ldots, 2N\lambda\}$ is an interval of length at least $(2-\varepsilon)p/q$. Now let λ' be an integer less than $p/2$ in absolute value and satisfying $\lambda\lambda' \equiv 1 \pmod{p}$. It is easy to see that

$$|\lambda'| \leq \frac{2N-2}{(2-\varepsilon)p/q - 1} \leq \frac{q}{7}$$

since we have a progression of length $(2-\varepsilon)p/q$ and common difference λ' contained in the interval $[2, N]$. Note also that if $i \in S$, then the interval I_i

intersects $\{\lambda, 2\lambda, \dots, N\lambda\}$. Therefore $\lambda' I_i$ intersects $\{1, \dots, N\}$, but $\lambda' I_i$ is itself contained in an interval of length $|\lambda'|p/q \le p/7$. This interval has to be contained in $[-p/7, N+p/7] \subset [-p/7, 2p/7]$ by the intersection property. Therefore $|\lambda'|i \in [-q/7, 2q/7]$ as an element of $\mathbb{Z}/q\mathbb{Z}$, and so all of S has to be contained in an arithmetic progression of length less than $q/2$, as required.

We also need to get the bound for $\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t)$ to be able to use Theorem 1.1. To do so, set $t = \lfloor 2^{-3}\delta^2 q\rfloor$ and let T be the set of all $y \in \mathbb{Z}/q\mathbb{Z}$ for which there exist $i, j \in S$ with $|A_i^* + A_j^*| \ge (2-\varepsilon)p/q$. The sumset $A_i^* + A_j^*$ is contained in $I_{i+j} + I_{i+j+1}$, which allows us to write

$$\begin{aligned}\frac{(2-\varepsilon)p|T|}{q} &\le \sum_{y\in T} |(A+A)\cap(I_y \cup I_{y+1})| \\ &= \sum_{y\in T+\{0,1\}} |(A+A)\cap I_y| + \sum_{y\in T\cap(T+1)} |(A+A)\cap I_y| \\ &\le |A+A| + \sum_{y\in T\cap(T+1)} |I_y| \le m + |T\cap(T+1)|\left(\frac{p}{q}+1\right).\end{aligned}$$

Multiplying by q/p we get $(2-\varepsilon)|T| \le |T\cap(T+1)|(1+q/p) + mq/p$, which leads to

$$\begin{aligned}|T+\{0,1\}| = 2|T| - |T\cap(T+1)| &\le \frac{q(m+|T\cap(T+1)|)}{p} + \varepsilon|T| \\ &\le \frac{q}{p}(m+q+\varepsilon p) \le \frac{q(m+\delta^2 p)}{p} \le \frac{(1+\delta)mq}{p}.\end{aligned}$$

This will be more useful later, but at the moment the most important thing for us is that $|T| \le (1+\delta)mq/p$. On the other hand, every $y \in (\mathbb{Z}/q\mathbb{Z})\setminus T$ corresponds to $1_S * 1_S(y)$ "bad" pairs (i,j) for which $\min(|A_i^*|, |A_j^*|) > \varepsilon p/q$, yet $|A_i^* + A_j^*| < (2-\varepsilon)p/q$. The number of these does not exceed εq^2, and therefore

$$\begin{aligned}\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t) &= \sum_{y\in T} \min(1_S * 1_S(y), t) + \sum_{y\notin T} \min(1_S * 1_S(y), t) \\ &\le t|T| + \varepsilon q^2 \le \frac{mqt}{p}\left(1+\delta+\frac{\varepsilon pq}{mt}\right).\end{aligned}$$

Combining the inequalities $t \ge 2^{-4}\delta^2 q$, $m \ge 2^{-3}\delta p$ and $\varepsilon = 2^{-7}\delta^4$, we can bound the above by $(1+2\delta)mqt/p$. Recalling that $|S| \ge (1/2 - 2\delta)mq/p$, we see that we can use Theorem 1.1 if δ is sufficiently small. Indeed, we can rewrite the bounds as

$$\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t) \le \left(2 + \frac{12\delta}{1-4\delta}\right)t|S|.$$

Since $1/(1-4\delta) \leq 25/24$, we can argue that all of S, except perhaps $5t/2$ elements, is contained in a progression $Q \subset \mathbb{Z}/q\mathbb{Z}$ of length at most $|S|(1+25\delta)+6t$.

Now we use the assumption on $|T+\{0,1\}|$ to say something about the common difference of Q. By Pollard's Theorem applied to $S \cap Q$ we know that

$$\sum_{y\in Q+Q} \min(1_S * 1_S(y), t) \geq t(2|S\cap Q|-t) \geq t(2|S|-6t).$$

Subtracting off those elements of $Q+Q$ that are not in T, we get

$$\sum_{y\in (Q+Q)\cap T} \min(1_S * 1_S(y), t) \geq t(2|S|-6t) - \varepsilon q^2.$$

This means that $|(Q+Q)\cap T| \geq 2|S| - 6t - \varepsilon q^2/t$, or in other words

$$|(Q+Q)\setminus T| \leq 2(25\delta|S|+6t) + 6t + \varepsilon q^2/t = 50\delta|S| + 18t + \varepsilon q^2/t.$$

By the estimate we already know, $\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \min(1_S * 1_S(y), t) \leq (1+\delta)mqt/p$, and by Pollard's Theorem we see that

$$2|S| - t \leq (1+\delta)\frac{mq}{p} \leq \frac{60mq}{50p},$$

so $2|S| \leq 61mq/(50p)$. Also, $18t \leq 18\delta mq/p$ and $\varepsilon q^2/t \leq \delta mq/p$, which altogether gives $|(Q+Q)\setminus T| \leq 100\delta mq/p$.

Now we will examine how the set $Q+Q$ behaves under addition of $\{0,1\}$. The elements of $Q+Q$ inside T form a subset of $T+\{0,1\}$ of size at most $(1+\delta)mq/p$. The part outside T will get at most doubled, so it will have size at most $200\delta mq/p$. Therefore $|Q+Q+\{0,1\}| \leq (1+201\delta)mq/p$. But $Q+Q$ is a progression of length at least

$$2|S\cap Q| - 1 \geq 2|S| - 5t - 1 \geq \frac{mq}{p}(1-4\delta-6\delta) = \frac{(1-10\delta)mq}{p},$$

and therefore adding $\{0,1\}$ to it produces at most $211\delta mq/p$ new elements. By dilating, we can assume that Q is an interval and the set we are adding is $\{0,d\}$ for some d. But then we see that $d \leq 211\delta mq/p$.

Now consider the dilation by d inside $\mathbb{Z}/p\mathbb{Z}$; then the intervals I_y for $y \in Q$ become progressions of common difference d, and Q corresponds to an "interval" of such progressions. Their union is almost an interval itself—the only problem being near endpoints, where the progressions do not necessarily start at the points we like. We can compensate this by adding at most p/q points for each "residue class modulo d" to get a genuine interval. The quotation marks mean that we are working modulo p, so technically we cannot consider residue classes modulo other numbers, but we have proved that we use only half of the space, so we can pretend we work in the integers.

In the end we get an interval P of length at most $(|Q|+2d)(p/q+1)$ containing almost all of A; estimating that gives

$$(|Q|+2d)\left(\frac{p}{q}+1\right) \le \frac{mq}{p}\left(\frac{1+201\delta}{2}+422\delta\right)(1+\delta^2)\frac{p}{q} \le \frac{(1+1200\delta)m}{2}.$$

Now note that the elements of $A+A$ outside $P+P$ are at worst the ones in I_y with $y \notin Q+Q$. Each $y \in T$ corresponds to at least $(1-\varepsilon)p/q-1$ elements of $A+A$, so since

$$|(Q+Q)\cap T| \ge 2|S| - 6t - \frac{\varepsilon q^2}{t} \ge \frac{mq}{p}(1-4\delta-6\delta-\delta) = \frac{1-11\delta}{mq}p,$$

we see that the intersection $(A+A)\cap(P+P)$ has at least

$$\frac{1-11\delta}{mq}p\left((1-\varepsilon)\frac{p}{q}-1\right) \ge (1-12\delta)m$$

elements. This means that $|(A+A)\setminus(P+P)| \le 12\delta m \le 24\delta N$, as claimed. ∎

6. Proof of Theorem 1.2. In this section we use the previous results to get Theorem 1.2; first let us note that it can be easily reduced to the following statement.

PROPOSITION 6.1. *There exist absolute constants C_0, ε_0, k_0 such that the following is true. Suppose that $A \subset \mathbb{N}$ is a set chosen randomly by picking each element of $\mathbb{N}$ independently with probability $1/2$. Then for every $k > k_0$,*

$$\mathbb{P}(|\mathbb{N}\setminus(A+A)| \ge k \text{ and } 1 \in A) \le C_0(2+\varepsilon_0)^{-k/2}.$$

Comparing this with what we are trying to prove in the end, we see that this statement says that for a set A satisfying $|\mathbb{N}\setminus(A+A)| \ge k$ it is exponentially (in k) unlikely to contain 1.

Proof of Theorem 1.2 assuming Proposition 6.1. Let $A \subset \mathbb{N}$ be a random subset. Note that the conditional distribution of A on the event $1 \notin A$ is exactly the same as the initial distribution of $A+1$. This, and the fact that $\mathbb{P}(1 \in A) = 1/2$, allows us to write (for each $k \ge 2$)

$$\begin{aligned} p_k - p_{k-2} &= 2^{k/2}\cdot\mathbb{P}(|\mathbb{N}\setminus(A+A)| \ge k) - 2^{(k-2)/2}\cdot\mathbb{P}(|\mathbb{N}\setminus(A+A)| \ge k-2) \\ &= 2^{k/2}\big(\mathbb{P}(|\mathbb{N}\setminus(A+A)| \ge k) - \tfrac{1}{2}\mathbb{P}\big(|\mathbb{N}\setminus((A+1)+(A+1))| \ge k\big)\big) \\ &= 2^{k/2}\big(\mathbb{P}(|\mathbb{N}\setminus(A+A)| \ge k) - \mathbb{P}(|\mathbb{N}\setminus(A+A) \ge k \text{ and } 1 \notin A)\big) \\ &= 2^{k/2}\cdot\mathbb{P}(|\mathbb{N}\setminus(A+A)| \ge k \text{ and } 1 \in A). \end{aligned}$$

The above quantity is obviously nonnegative, which makes both sequences $\{p_{2k}\}$ and $\{p_{2k+1}\}$ increasing. Proposition 6.1 allows us to assert they are bounded. Indeed, if $k > k_0$, then

$$\begin{aligned}p_k - p_{k-2} &= 2^{k/2}\mathbb{P}(|\mathbb{N}\setminus(A+A)| \geq k \text{ and } 1 \in A)\\ &\leq 2^{k/2}C_0(2+\varepsilon_0)^{-k/2} = C_0\left(\frac{2}{2+\varepsilon_0}\right)^{k/2}.\end{aligned}$$

Let $\lambda = 2/(2+\varepsilon_0) < 1$. Summing the above inequalities we see that for any $k > k_0$ we get

$$p_k - p_{k_0} \leq \sum_{s=k_0/2}^{\infty} C_0\lambda^s = \frac{C_0\lambda^{k_0/2}}{1-\lambda} < \infty.$$

Actually the above is true only for k of the same parity as k_0; for the remaining values we simply replace all instances of k_0 with k_0+1. ∎

Proof of Proposition 6.1. Let δ be a small quantity and $k > N_0(\delta)$ be from the statement of Proposition 5.2. Set $X = A \cap [10k]$. First, following Green and Morris, let us estimate the probability that A misses one of the elements greater than $10k$. For each such element m we have at least $\lfloor m/2 \rfloor$ pairs of (not necessarily distinct) natural numbers u, v with $u + v = m$; the probability that $u, v \in A$ is at least $1/4$. Therefore the probability that $m \notin A+A$ is bounded by $(3/4)^{(m-1)/2}$ and the total contribution for numbers greater than $10k$ is at most

$$\sum_{m=10k+1}^{\infty}\left(\frac{3}{4}\right)^{(m-1)/2} < 2^{-k}.$$

We will then consider the sum on the left hand side a quantity less than $C_0(2+\varepsilon_0)^{-k/2}$; our goal is to divide the set of admissible events into classes with probability of each being bounded by this expression.

From this point on we can assume that A contains all the numbers greater than $10k$, and consequently $\mathbb{N}\setminus(A+A) = [10k]\setminus(X+X)$. Let us estimate the probability that $|X| \leq 10\delta k$; since X is uniformly distributed among all subsets of $[10k]$, we can estimate it by $2^{10k(H(\delta)-1)}$. If δ is small enough, this implies the claimed bound.

Now assume that $|X| > 10\delta k$ and estimate the probability that X is exceptional (according to the statement of Proposition 5.2) and obeys the inequality $|[10k]\setminus(X+X)| \geq k$. This probability is bounded by

$$2^{-10k}\sum_{k'>10\delta k}\ \sum_{m=2k'-1}^{19k} 2^{\frac{m}{2}H(\frac{2k'-1}{m})-10\delta k}.$$

The estimate $m \leq 19k$ comes from the fact that $X + X$ misses at least k points from $[10k] \subset [20k]$. Bounding each term crudely, i.e. using $H(x) \leq 1$, $m \leq 19k$, we get the bound of $200k^2 2^{-k/2-10\delta k}$, again as good as we need. Now let us consider non-exceptional subsets X. Using the Green–Morris

Theorem on counting *all* subsets [GM15, Proposition 3.1], we know that the number of non-exceptional subsets with $|X+X| = m$ is bounded by

$$\sum_{k'=0}^{m/2} 2^{10\delta k}\binom{m/2}{k'}.$$

If we restrict the range of m to $m \le (19-30\delta)k$, the above expression divided by 2^{10k} is still bounded as we need. Therefore we can assume that in fact $|X+X| \ge (19-30\delta)k$.

Our bound shows that the corresponding progression P has size at least $(1-10\delta)m/2 \ge (19/2 - 10^3\delta)k$. Therefore it has common difference 1. Suppose now that $X+X$ contains at least $2\cdot 10^4\delta k$ elements less than $k/2$. We know that $(X+X)\setminus(P+P) \le 12\delta m \le 240\delta k$, which means that the least element of P is at most $(1-19000\delta)k/2$. On the other hand, since

$$|P| \le \frac{1-1200\delta}{2}m \le \left(\frac{19}{2} - 12000\delta\right)k,$$

there are at least $7000\delta k$ elements of $(10k, 20k]$ not in $P+P$, which belong to $A+A$ anyway. But out of them only $240\delta k$ can belong to $X+X$, so that leaves over $6000\delta k$ elements of $(A+A)\setminus(X+X)$ in $[20k]$. Adding to that $m \ge (19-30\delta)k$ elements of $X+X$ we see that $A+A$ in fact misses less than k elements, so this case cannot hold.

Suppose now that A (equivalently X) contains less than $2\cdot 10^4\delta k$ elements less than $k/2$. So far we have not used the fact that $1 \in A$. We are going to do this now. Let

$$B = X \cap (0, (k+1)/2], \qquad C = X \cap ((k+1)/2, k], \qquad D = X \cap (k, \infty).$$

Clearly $A+A \supset (1+C)\cup(C+C)\cup(D+D)$ and those subsets are disjoint. So certainly $|\mathbb{N}\setminus(A+A)| \ge k$ if

$$|\mathbb{N}\setminus(D+D-2k)| \ge k - (2k - |C| - |C+C|) = |C| + |C+C| - k.$$

By Green–Morris's estimate [GM15, Theorem 1.3] we can assume that the probability of the latter is bounded by $C_\varepsilon(2-\varepsilon)^{-(|C|+|C+C|-k)}$ for any $\varepsilon > 0$ and a suitable constant $C_\varepsilon > 0$. Note that the probability cannot exceed 1, so the trivial bound is actually better if $|C| + |C+C| < k$. On putting everything together, the total probability that $|\mathbb{N}\setminus(A+A)| \ge k$ is bounded by

$$2^{-k/2}\sum_B 2^{-k/2}\sum_C C_\varepsilon \min(1, (2-\varepsilon)^{-(|C|+|C+C|-k)/2}).$$

Now by Green–Morris's bound on the number of sets with small sumset [GM15, Proposition 3.1] we can divide the inner sum into classes depending on the size of $|C|$ and $|C+C|$. This way we get a bound of

$$C_\varepsilon \cdot 2^{-k} \sum_B \sum_{l,m\le k} 2^{\delta k} \binom{m/2}{l} \min(1, (2-\varepsilon)^{-(l+m-k)/2}).$$

Now we have the upper bound on the size of B, which turns the outer sum into the additional coefficient $2^{kH(4\cdot 10^4\delta)/2}$. The only way the above expression could fail to be bounded as we need is if we could find among the expressions $\binom{m/2}{l} \cdot \min(1, (2-\varepsilon)^{-(l+m-k)/2})$ one that is greater than $(2-\eta)^{k/2}$ for some small value of η. This first requires m to be close to k as the binomial coefficient $\binom{m/2}{l} \le 2^{m/2}$ has to be at least $(2-\eta)^{k/2}$. Also, we need to have $(2-\varepsilon)^{-(l+m-k)/2} \ge (1-\eta/2)^{k/2}$, which requires $l+m$ to be not much larger than k. Those two in turn imply that l is small compared to k, in which case $\binom{m/2}{k}$ does not exceed $(2-\eta)^{k/2}$. This indicates that our initial assumption was false and our bound in fact is always satisfied. ■

Appendix. Estimates of binomial coefficients. In the Appendix we are going to prove some useful inequalities concerning binomial coefficients. Before we do that, let us define the binary entropy function $H : [0,1] \to \mathbb{R}$ as

$$H(t) = t \log_2 \frac{1}{t} + (1-t) \log_2 \frac{1}{1-t}.$$

Note that it does not quite make sense if $t = 0$ or $t = 1$, so we extend H continuously by setting $H(0) = H(1) = 0$. One can easily prove that $0 \le H(t) \le 1$ for all $t \in [0,1]$ with the only extremal values being $H(0) = H(1) = 0$ and $H(1/2) = 1$. Also, H is continuous, increasing on $[0,1/2]$, decreasing on $[1/2,1]$, and obeys the equality $H(t) = H(1-t)$. By calulating the second derivative, one can see that H is concave, which together with previous observations leads to the triangle inequality $H(|x+y|) \le H(|x|) + H(|y|)$ valid for all x, y for which all the expressions make sense.

LEMMA A.1. *Let $n, k \ge 0$ be integers and let $\delta \in [0,1/2]$. Then*

$$\frac{2^{nH(k/n)}}{n+1} \le \binom{n}{k} \le 2^{nH(k/n)}, \qquad \sum_{j=0}^{\lfloor \delta n \rfloor} \binom{n}{j} \le 2^{nH(\delta)}.$$

Proof. Let us begin with the last inequality. Take a set of size n and choose a subset of it at random by picking each element independently with probability δ. Then for any $j \le \delta n$ the probability that a given j-element subset is chosen is $\delta^j(1-\delta)^{n-j}$. Since $\delta \le 1-\delta$, we can bound it from below by

$$\delta^j (1-\delta)^{n-j} \ge \delta^{\delta n} (1-\delta)^{(1-\delta)n} = 2^{-nH(\delta)}.$$

But the total probability cannot exceed 1, so the number of all those sets, equal to $\sum_{j=0}^{\lfloor \delta n \rfloor} \binom{n}{j}$, has to be at most $2^{nH(\delta)}$.

Turning to the first two inequalities, assume without loss of generality that $k \leq n/2$; we can do that as we can always replace k with $n-k$, given that $\binom{n}{k} = \binom{n}{n-k}$ and

$$H\left(\frac{k}{n}\right) = H\left(1 - \frac{k}{n}\right) = H\left(\frac{n-k}{n}\right).$$

In this case let $\delta = k/n \leq 1/2$ and consider again the same random experiment. Writing the total probability as a sum of probabilities of choosing a particular set, we get

$$\sum_{j=0}^{n} \binom{n}{j} \delta^j (1-\delta)^{n-j} = 1.$$

Note that the expression $\binom{n}{k} 2^{-nH(k/n)}$ is one of the summands in the above sum, and by comparing two consecutive ones we can check that it is actually the largest out of $n+1$ summands. Therefore $1/(n+1) \leq \binom{n}{k} 2^{-nH(k/n)} \leq 1$, as needed. ■

References

[Fou77] J. F. F. Fournier, *Sharpness in Young's inequality for convolution*, Pacific J. Math. 72 (1977), 383–397.

[GM15] B. J. Green and R. Morris, *Counting sets with small sumset and applications*, Combinatorica (2015) (online).

[Kne53] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*, Math. Z. 58 (1953), 459–484.

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

[Pol74] J. M. Pollard, *A generalisation of the theorem of Cauchy and Davenport*, J. London Math. Soc. 8 (1974), 460–462.

[Vos56] G. Vosper, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. 31 (1956), 200–205.

Przemysław Mazur
Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road, Oxford OX2 6GG, United Kingdom
E-mail: przemyslaw.mazur@maths.ox.ac.uk

Received on 27.2..2015
and in revised form on 27.7.2015 (8095)