A step beyond Freiman's theorem for set addition modulo a prime

Pablo Candela[1] Oriol Serra[2] Christoph Spiegel[3]

November 8, 2019

Abstract

Freiman's 2.4-Theorem states that any set $A \subset \mathbb{Z}_p$ satisfying $|2A| \leq 2.4|A| - 3$ and $|A| < p/35$ can be covered by an arithmetic progression of length at most $|2A| - |A| + 1$. A more general result of Green and Ruzsa implies that this covering property holds for any set satisfying $|2A| \leq 3|A| - 4$ as long as the rather strong density requirement $|A| < p/10^{215}$ is satisfied. We present a version of this statement that allows for sets satisfying $|2A| \leq 2.48|A| - 7$ with the more modest density requirement of $|A| < p/10^{10}$.

1 Introduction

Given a set $A \subset G$ in some additive group G, we define its *sumset* as

$$A + A = \{a + a' : a, a' \in A\} \subset G. \tag{1}$$

We will often denote this sumset by $2A$, which should not be confused with the dilate $2 \cdot A = \{2a : a \in A\}$. When dealing with inverse questions in additive combinatorics, one is typically interested in understanding the structure of a set A for which only some additive property is known, e.g. that the so-called *doubling* $|2A|/|A|$ is small. One of the most important results in this area is Freiman's Theorem, which states that any finite set of integers can be efficiently covered by a generalized arithmetic progression, where the size and the dimension of the progression depend only on the doubling. The bounds for this result were later improved and the ambient group generalized to many different contexts, see for example [3, 9, 17, 18, 19].

[1]Universidad Autónoma de Madrid, and ICMAT, Ciudad Universitaria de Cantoblanco, Madrid 28049, Spain, pablo.candela@uam.es. Supported by the Spanish Ministerio de Economía y Competitividad project MTM2017-83496-P.

[2]Universitat Politécnica de Catalunya, Department of Mathematics, 08034 Barcelona, Spain, oriol.serra@upc.edu. Supported by the Spanish Ministerio de Economía y Competitividad projects MTM2014-54745-P and MDM-2014-0445.

[3]Universitat Politécnica de Catalunya and Barcelona Graduate School of Mathematics, Department of Mathematics, Edificio Omega, 08034 Barcelona, Spain, christoph.spiegel@upc.edu. Supported by the Spanish Ministerio de Economía y Competitividad FPI grant under the project MTM2014-54745-P, the project MTM2017-82166-P and the María de Maetzu research grant MDM-2014-0445.

In the more specific case of finite sets of integers $A \subset \mathbb{Z}$ with *very* small sumsets, that is $|2A| \leq 3|A| - 4$, Freiman showed that in fact A can be covered by a normal (i.e. 1-dimensional) arithmetic progression of length at most $|2A| - |A| + 1$. This result is easily seen to be tight. An equivalent statement for subsets $\mathcal{A}$ of the cyclic group $\mathbb{Z}_p$, where p is a prime, is widely believed to hold as well, assuming certain modest restrictions regarding the cardinality of $\mathcal{A}$ with respect to p. However, such a statement has turned out to be more difficult to prove.

It was Freiman himself who first showed that the same covering property holds for any set $\mathcal{A} \subset \mathbb{Z}_p$ satisfying $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| < p/35$, see [5]. Rødseth [16] later showed that the density requirement can be weakened to $p/10.7$. A more general result of Green and Ruzsa [8] immediately gives the same conclusion for all sets satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as long as they also satisfy the rather strong density requirement $|\mathcal{A}| < p/10^{215}$. The second author and Zémor obtained a result with the same covering conclusion and no restrictions regarding the size of $|\mathcal{A}|$ itself, but assuming that $|2\mathcal{A}| \leq (2 + \varepsilon)|\mathcal{A}|$ with $\varepsilon < 10^{-4}$, see [20]. Recently, the latter bound was relaxed to $\varepsilon < 0.1368$, under the mild additional assumption $|2\mathcal{A}| \leq 3p/4$, see [2].

We present a version of this statement that improves upon the constant 2.4 present in the results of Freiman and Rødseth, without requiring quite as strong a density condition as in the result of Green and Ruzsa.

Theorem 1.1. *Let p be a prime and let $\mathcal{A} \subset \mathbb{Z}_p$ satisfy $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| < p/10^{10}$. Then there is an arithmetic progression $P \subset \mathbb{Z}_p$ such that $\mathcal{A} \subset P$ and $|P| \leq |2\mathcal{A}| - |\mathcal{A}| + 1$.*

Similar to both the result of Freiman and that of Green and Ruzsa, the proof of this statement uses a Fourier-analytic rectification argument that allows one to transplant a significant part of the set into the integers, where the corresponding covering result can be applied. Unlike the result of Freiman however, we will allow the doubling of that part to go past the $3|A| - 4$ barrier in the integers. To do so, we will use a result of Freiman and Deshoulliers to prove a covering result for sets of integers with doubling slightly above that barrier. This also implies that, unlike in the original approach, we have to take the additive dimension of our sets into consideration.

We believe that the ideas in this paper are capable of yielding significantly better constants than the ones obtained here. The biggest obstacle in improving either the density requirement or the constant 2.48 will be the relatively poor covering given by Proposition 2.3. A conjecture of Freiman (see for example [7]) claims that in fact one should be able to replace the constant 10^9 with 4 in that proposition, resulting in a significant improvement of the density requirement of our main statement. So far only very little has been proven in that direction. Freiman himself solved the case $3|A| - 3$, and Jin [12] obtained a result in the case $(3 + \varepsilon)|A|$ for some undetermined $\varepsilon > 0$.

Outline. In *Section 2* we will introduce some tools required in order to prove Theorem 1.1. We will first state and prove a covering result for sets of integers having doubling slightly above the $3|A| - 4$ threshold. We will then give an overview of some well-established rectification principles. Using these tools we will then prove Theorem 1.1 in *Section 3*. We make some concluding remarks in *Section 4*.

2 Preliminaries

Let us formally define some common notions and concepts. We say that a set $A \subset \mathbb{Z}$ is in *normal form* if $A \subset \mathbb{N}_0$, $0 \in A$ and $\gcd(A) = 1$. Note that one can easily put any finite set $A \subset \mathbb{Z}$ into normal form without affecting its cardinality or additive properties, by setting $A' = (A - \min(A))/\gcd(A - \min(A))$. If a set A is covered by an arithmetic progression of length k then it follows that the normal form A' of that set satisfies $\max(A') \leq k - 1$.

Let A and B be two subsets of some (not necessarily identical) abelian groups. A bijection $f : A \to B$ is said to be a *Freiman isomorphism of order* k, or F_k*-isomorphism* for short, if for any elements $a_1, \ldots, a_k, a'_1, \ldots, a'_k \in A$ we have

$$a_1 + \cdots + a_k = a'_1 + \cdots + a'_k \quad \Leftrightarrow \quad f(a_1) + \cdots + f(a_k) = f(a'_1) + \cdots + f(a'_k). \tag{2}$$

One can think of this as a generalization of a group isomorphism for which only operations of depth at most k are required to be preserved. A subset A of an arbitrary abelian group is said to be *rectifiable of order* k if it is F_k-isomorphic to a set of integers. Note that we will generally only be interested in the case $k = 2$, where we will just use the term *rectifiable*. Lastly, the *additive dimension* $\dim(A)$ of a set $A \subset \mathbb{Z}^r$ is defined to be the largest $s \in \mathbb{N}$ for which A is F_2-isomorphic to some subset of $\mathbb{Z}^s$ that is not contained in a hyperplane.

In what follows we will usually use the notation $\mathcal{A}$ to refer to sets in some cyclic group $\mathbb{Z}_m$ and the usual notation A to refer to sets in the integers. Often $\mathcal{A}$ will refer to the canonical projection from $\mathbb{Z}$ to some $\mathbb{Z}_m$ of some $A \subset \mathbb{Z}$.

2.1 Covering Statements

Deshouillers and Freiman stated the following result regarding covering properties of subsets of $\mathbb{Z}_m$ with very small sumset. Note that – unlike the main statement this paper is interested in – this result concerns arbitrary $\mathbb{Z}_m$, that is, the integer m does not have to be prime. This explains the weaker bounds and more complex statement.

Theorem 2.1 (Deshouillers and Freiman [4])**.** *For any set $\mathcal{A} \subset \mathbb{Z}_m$ satisfying $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$ and $|\mathcal{A}| \leq n/10^9$ there exists a proper subgroup $H < \mathbb{Z}_m$ such that the following holds:*

1. *If $\mathcal{A}$ is included in one coset of H then $|\mathcal{A}| > |H|/10^9$.*
2. *If $\mathcal{A}$ meets exactly 2 or at least 4 cosets of H then it is included in an ℓ-term arithmetic progression of cosets of H where*

$$(\ell - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|. \tag{3}$$

3. *If $\mathcal{A}$ meets exactly three cosets of H then it is included in an ℓ-term arithmetic progression of cosets of H where*

$$(\min(\ell, 4) - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|. \tag{4}$$

Furthermore, if $\ell \geq 2$ then there exists a coset of H containing at least $2/3\,|H|$ elements from $\mathcal{A}$.

Note that if m is prime, then the subgroup H in the statement has to be the trivial group $\{0\}$ and $\mathcal{A}$ clearly meets exactly $|\mathcal{A}|$ cosets of it, so we are in case 2 of the statement as long as $|\mathcal{A}| \geq 4$. The conclusion in this case is the same as that of Theorem 1.1.

We will also need the following straightforward observation in order to distinguish between integer sets of different additive dimension.

Lemma 2.2. *Let $A \subset \mathbb{Z}$ be given in normal form with $|A| \geq 3$ and $m > 1$ such that $m \mid \max(A)$. If the canonical projection of A into $\mathbb{Z}_m$ is rectifiable, then* $\dim(A) \geq 2$.

Proof. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ denote the canonical projection. Note that $\{(a, \varphi(a)) : a \in A\} \subset \mathbb{Z} \times \mathbb{Z}_m$ is F_2-isomorphic to A, since for any $a_1, a_2, a_3, a_4 \in A$ we have $a_1 + a_2 = a_3 + a_4$ if and only if $(a_1, \varphi(a_1)) + (a_2, \varphi(a_2)) = (a_3, \varphi(a_3)) + (a_4, \varphi(a_4))$. As $\mathcal{A} = \varphi(A)$ is rectifiable, there exists some F_2-isomorphism f mapping $\mathcal{A}$ into the integers. By the same argument as before, it follows that $\{(a, \varphi(a)) : a \in A\}$ and hence also A is F_2-isomorphic to $\{(a, f(\varphi(a))) : a \in A\} \subset \mathbb{Z}^2$. We may without loss of generality assume that $f(0) = 0$ and note that since A is in normal form and $|A| \geq 3$, there must exist some $a' \in A$ such that $\varphi(a') \neq 0$ and hence also $f(\varphi(a')) \neq 0$. Using the requirement that $m \mid \max(A)$, we observe that the three points $(0, f(\varphi(0))) = (0, 0)$, $(\max(A), f(\varphi(\max(A))) = (\max(A), 0)$ and $(a', f(\varphi(a'))) \neq (a', 0)$ do not lie in a hyperplane of $\mathbb{Z}^2$ and therefore $\dim(A) \geq 2$ as desired. □

We can now state and prove the main new ingredient needed for the proof of Theorem 1.1. It should be noted that the proof has some slight similarities with the proof of Freiman's $3|A|-4$ Theorem in the integers by modular reduction (see [15]), but there is a new component in the argument here, consisting of taking into account the Freiman dimension of the set.

Proposition 2.3. *Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9\,|A|$.*

Proof. Let $A \subset \mathbb{Z}$ satisfy $|2A| \leq 3.04|A| - 3$ as well as $\max(A) \geq 10^9|A|$, and assume without loss of generality that A is in normal form. We will show that we must have $\dim(A) \geq 2$, which contradicts the assumption that A is 1-dimensional. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_{\max(A)}$ denote the canonical projection and observe that $\mathcal{A} = \varphi(A)$ satisfies $|\mathcal{A}| = |A| - 1 < \max(A)/10^9$. Let B denote the set of elements $x \in 2A$ such that $x + \max(A)$ is also in $2A$. Since 0 and $\max(A)$ are both in A we have $B \supset A$, whence $|2A| = |2\mathcal{A}| + |B| \geq |2\mathcal{A}| + |A|$, and so

$$|2\mathcal{A}| \leq |2A| - |A| \leq 2.04|A| - 3 \leq 2.04|\mathcal{A}|.$$

We can therefore apply Theorem 2.1, obtaining that $\mathcal{A}$ is covered by some small arithmetic progression of cosets of some proper subgroup $H < \mathbb{Z}_{\max(A)}$. Let us go through the cases given by this theorem. In the following $\mathbb{1}_C$ will denote the indicator function of some given set C.

1. As A is in normal form, $\mathcal{A}$ cannot be contained in a single coset of H.

2. If $\mathcal{A}$ meets exactly 2 or at least 4 cosets of H then it is included in an ℓ-AP of cosets of H, where by (3) we have $\ell \leq 1.04|\mathcal{A}|/|H| + 1 \leq (1.04 + 3/2)|\mathcal{A}|/|H|$, the last equality

following from the last sentence in Theorem 2.1. Using that $|\mathcal{A}| < 10^{-9}\max(A)$ we deduce that

$$\ell \leq 3|\mathcal{A}|/|H| < \tfrac{1}{2}\left|\mathbb{Z}_{\max(A)/|H|}\right|. \tag{5}$$

Letting $m = \max(A)/|H|$ we now observe that, since A is in normal form, its canonical projection into $\mathbb{Z}_m$ cannot be contained in a proper subgroup of $\mathbb{Z}_m$. It follows that the common difference of the ℓ-term arithmetic progression covering this projection of A does not divide m, whence we can dilate by the inverse mod m of this common difference, and it follows that the projection of A is F_2-isomorphic to some subset of an interval of size $m/2$ in $\mathbb{Z}_m$. This projection is therefore rectifiable, so by Lemma 2.2 we have $\dim(A) \geq 2$.

3. If $\mathcal{A}$ meets exactly 3 cosets of H, then we argue in a way similar to case 2, considering the projection of A to $\mathbb{Z}_m$ where $m = \max(A)/|H|$. Here, however, we distinguish two cases, according to whether the 3 cosets are in arithmetic progression or not.

   Assume that these cosets are in arithmetic progression with difference d. If we can rectify the 3-term progression formed by the cosets' representatives, then we can rectify the projection of A into $\mathbb{Z}_m$. By applying Lemma 2.2 as in case 2 we again obtain the contradiction $\dim(A) \geq 2$. If we cannot rectify the 3-term progression, then we must have either $m < 6$, $d = m/3$ or $d = m/4$. We certainly have $m \geq 6$ since by (4) we have $|H| \leq (|2\mathcal{A}| - |\mathcal{A}|)/2 \leq 0.52|\mathcal{A}|$, and as noted above we also have $\max(A) \geq 10^9|\mathcal{A}|$, so $m \geq 10^9$. Furthermore, if $d = m/3$ or $d = m/4$ then m is multiple of d and clearly A cannot have been in normal form.

   If the cosets do not form an arithmetic progression, then we have $\mathcal{A} \subseteq H \cup (H+c_1) \cup (H+c_2)$ for some $c_1, c_2 \in \mathbb{Z}_{\max(A)}$ satisfying $c_2 \not\equiv 2c_1$, $c_1 \not\equiv 2c_2$ and $c_1 + c_2 \not\equiv 0$ in $\mathbb{Z}_{\max(A)}/H$. Moreover, we may assume that either $2c_1 \not\equiv 0$ or $2c_2 \not\equiv 0$ in $\mathbb{Z}_{\max(A)}/H$ as otherwise $\mathcal{A}$ would only meet 2 cosets of H. We therefore assume without loss of generality that $2c_2 \not\equiv 0$ in $\mathbb{Z}_{\max(A)}/H$. If furthermore $2c_2 \not\equiv 2c_1$ in $\mathbb{Z}_{\max(A)}/H$, then $\{\mathbb{1}_{H+c_2}(\varphi(a)) : a \in A\}$ is F_2-homomorphic to A and therefore $\dim(A) \geq 2$ as A is F_2-isomorphic to

$$\left\{(\mathbb{1}_{H+c_2}(\varphi(a)), a) : a \in A\right\} \subset \mathbb{Z}^2 \tag{6}$$

   which is not contained in some hyperplane of $\mathbb{Z}^2$ as $\varphi(0) = \varphi(\max(A)) \in H$ but $\varphi(a') \in H + c_2$ for some $a' \in A$. If however $2c_1 \equiv 2c_2 \not\equiv 0$ in $\mathbb{Z}_{\max(A)}/H$, then likewise we can argue that $\dim(A) \geq 2$ as A now is F_2-isomorphic to

$$\left\{(\mathbb{1}_{H}(\varphi(a)), a) : a \in A\right\} \subset \mathbb{Z}^2 \tag{7}$$

   which for the same reason is also not contained in any hyperplane of $\mathbb{Z}^2$.

It follows that $\dim(A) \geq 2$, which contradicts the assumption that A is 1-dimensional. □

We will also need the following two results due to Freiman that will enable us to deal with sets past the $3|A| - 4$ threshold that are not 1-dimensional.

Theorem 2.4 (Freiman)**.** *Every finite set $A \subset \mathbb{Z}$ of additive dimension d satisfies*

$$|2A| \geq (d+1)|A| - \binom{d+1}{2}. \tag{8}$$

For a proof see [6, Lemma 1.14].

Theorem 2.5 (Freiman)**.** *Let $A \subset \mathbb{Z}^2$ be a 2-dimensional set that cannot be embedded in any straight line and that satisfies $|2A| < {}^{10}/_3\,|A| - 5$ and $|A| \geq 11$. Then A is contained in a set which is isomorphic to*

$$\{(0,0),(0,1),(0,2),\ldots,(0,k_1-1),(1,0),(1,1),\ldots,(1,k_2-1)\} \tag{9}$$

where $k_1, k_2 \geq 1$ and $k_1 + k_2 \leq |2A| - 2|A| + 3$.

The above result is [6, Theorem 1.17]. We shall use the following consequence.

Corollary 2.6. *Any 2-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq {}^{10}/_3\,|A| - 5$ is contained in the union of two arithmetic progressions P_1 and P_2 with the same common difference such that $|P_1 \cup P_2| \leq |2A| - 2|A| + 3$. Furthermore, the sumsets $2P_1$, $P_1 + P_2$ and $2P_2$ are disjoint.*

A proof of this can be immediately derived from the following statement.

Lemma 2.7. *Given $d \geq 1$ and a finite set $A \subset \mathbb{Z}^d$ of dimension d not contained in a hyperplane, we can extend any Freiman-isomorphism φ mapping A to some $A' \subset \mathbb{Z}$ to an affine linear map.*

Proof. Assume to the contrary that φ is not affine linear. As $\dim(A) = d$, there exist d elements $a_1, \ldots, a_d \in A$ spanning $\mathbb{Z}^d$. Let φ_e denote the affine linear map $\mathbb{Z}^d \to \mathbb{Z}$ determined by $a_1, \ldots, a_d \in \mathbb{Z}^d$ as well as 0, that is $\varphi_e(a_i) = \varphi(a_i)$ for $i = 1, \ldots, d$ and $\varphi_e(0) = \varphi(0)$. As φ is not affine linear, we must have $\varphi_e(x) \neq \varphi(x)$ for some $x \in A \setminus \{a_1, \ldots, a_d, 0\}$. It follows that $A'' = \{(a, \varphi_e(a) - \varphi(a)) : a \in A\} \subset \mathbb{Z}^{d+1}$ cannot be contained in a hyperplane, that is $\dim(A'') \geq d + 1$. However, one can easily verify that A'' is Freiman-isomorphic to A', giving us a contradiction. □

Proof of Corollary 2.6. Let $A' \subset \mathbb{Z}^2$ denote a set that is F_2-isomorphic to A and not contained in a line. By Theorem 2.5 we can assume that A' is contained in two lines of combined size less than $|2A| - 2|A| + 3$. By Lemma 2.7 the F_2-isomorphism φ mapping A' to A can be extended to an affine linear map, implying the desired statement. □

2.2 The Fourier-analytic Rectification

It is obvious that at least half of any set $\mathcal{A} \subset \mathbb{Z}_p$ can be rectified. It is reasonable to expect that if $\mathcal{A}$ is 'concentrated' in some sense, then one should be able to rectify significantly more than just half of the set. Freiman stated such a result using the language of large Fourier coefficients. In the following $\widehat{\mathbb{1}}_{\mathcal{A}}(x) = \sum_{a \in \mathcal{A}} e^{2\pi i a x/p}$ will denote the Fourier transform of the indicator function of some set $\mathcal{A} \subset \mathbb{Z}_p$.

Theorem 2.8 (Freiman [6]). *For any $\mathcal{A} \subset \mathbb{Z}_p$ and $d \in \mathbb{Z}_p^\star$ there exists $u \in \mathbb{Z}_p$ such that*

$$\big|[u, u + p/2) \cap d \cdot \mathcal{A}\big| \geq \frac{|\mathcal{A}| + |\widehat{\mathbb{1}}_{\mathcal{A}}(d)|}{2}. \tag{10}$$

It should be noted that an improved version of this result can be obtained using a result of Lev [14]. However, we will stick to using Theorem 2.8 when proving our main statement, as the improvement that would follow from using Lev's result is negligible in our case. Lastly, it was also Freiman who noted that a small sumset implies the existence of a large Fourier coefficient and hence a certain 'concentration' of the set. We state this observation in the following form. The proof follows by a standard application of the Cauchy-Schwarz inequality.

Lemma 2.9 (Freiman [6]). *For any $\mathcal{A} \subset \mathbb{Z}_p$ there exists $d \in \mathbb{Z}_p^\star$ such that*

$$\big|\widehat{\mathbb{1}}_{\mathcal{A}}(d)\big| \geq \left(\frac{p/|2\mathcal{A}| - 1}{p/|\mathcal{A}| - 1}\right)^{1/2} |\mathcal{A}|. \tag{11}$$

Proof. We start by observing that

$$\sum_{a=0}^{p-1} \widehat{\mathbb{1}}_{\mathcal{A}}(a)^2 \overline{\widehat{\mathbb{1}}_{2\mathcal{A}}(a)} = \sum_{a=0}^{p-1} \sum_{x_1, x_2 \in \mathcal{A}} \sum_{x_3 \in 2\mathcal{A}} e^{2\pi i a(x_1 + x_2 - x_3)/p} = |\mathcal{A}|^2 p.$$

Now if $|\widehat{\mathbb{1}}_{\mathcal{A}}(a)| \leq \theta\,|\mathcal{A}|$ for all $a \neq 0 \mod p$ and

$$\theta < \left(\frac{p/|2\mathcal{A}| - 1}{p/|\mathcal{A}| - 1}\right)^{1/2}$$

then using Cauchy-Schwarz one would get the contradiction

$$\begin{aligned}
\sum_{a=0}^{p-1} \widehat{\mathbb{1}}_{\mathcal{A}}(a)^2 \overline{\widehat{\mathbb{1}}_{2\mathcal{A}}(a)} &= |\mathcal{A}|^2\,|2\mathcal{A}| + \sum_{a=1}^{p-1} \widehat{\mathbb{1}}_{\mathcal{A}}(a)^2 \overline{\widehat{\mathbb{1}}_{2\mathcal{A}}(a)} \\
&\leq |\mathcal{A}|^2\,|2\mathcal{A}| + \theta|\mathcal{A}| \left(\sum_{a=1}^{p-1} |\widehat{\mathbb{1}}_{\mathcal{A}}(a)|^2\right)^{1/2} \left(\sum_{a=1}^{p-1} |\widehat{\mathbb{1}}_{2\mathcal{A}}(a)|^2\right)^{1/2} \\
&= |\mathcal{A}|^2\,|2\mathcal{A}| + \theta|\mathcal{A}| \left(|\mathcal{A}|p - |\mathcal{A}|^2\right)^{1/2} \left(|2\mathcal{A}|p - |2\mathcal{A}|^2\right)^{1/2} < |\mathcal{A}|^2 p.
\end{aligned}$$

The desired statement follows. □

3 Proof of Theorem 1.1

Note that throughout the proof we will simplify notation by just writing $p/2$ and $p/3$ rather than the correct rounded version. In all cases there will be an appropriate amount of slack that justifies this simplification.

Let $d \in \mathbb{Z}_p^\star$ and $u \in \mathbb{Z}_p$ be such that $\mathcal{A}_1 = [u, u + p/2) \cap d \cdot \mathcal{A}$ satisfies

$$|\mathcal{A}_1| = \max_{u', d'} |[u', u' + p/2) \cap d' \cdot \mathcal{A}|. \tag{12}$$

We assume without loss of generality that $d = 1$ and $u = 0$. By Theorem 2.8 and Lemma 2.9 we have that

$$|\mathcal{A}_1| \geq \left(1 + \left(\frac{p/|2\mathcal{A}| - 1}{p/|\mathcal{A}| - 1}\right)^{1/2}\right) \frac{|\mathcal{A}|}{2} > 0.8175\,|\mathcal{A}|. \tag{13}$$

We note that $\mathcal{A}_1$ satisfies $|2\mathcal{A}_1| \leq 3.04|\mathcal{A}_1| - 7$ as otherwise we would get the contradiction

$$2.48\,|\mathcal{A}| - 7 \geq |2\mathcal{A}| \geq |2\mathcal{A}_1| > 3.04|\mathcal{A}_1| - 7 > 2.484\,|\mathcal{A}| - 7. \tag{14}$$

As $\mathcal{A}_1$ is contained in an interval of size less than $p/2$, it is rectifiable and hence there exists some F_2-isomorphic set $A_1 \subset \mathbb{Z}$. We note that due to Theorem 2.4 we have $\dim(A_1) \in \{1, 2\}$. Let us distinguish between these two cases.

Case 1. If $\dim(A_1) = 1$, then by Proposition 2.3 it is contained in an arithmetic progression of size less than $10^9|\mathcal{A}_1|$. If the common difference r of this progression is not 1, we may dilate by $r^{-1} \mod p$ and translate once more, so that we may assume that $\mathcal{A}_1 \subset [0, 10^9|\mathcal{A}_1|]$. Since $|\mathcal{A}_1|$ is by assumption the most elements any $p/2$-segment can contain of any dilate of $\mathcal{A}$, it follows that $\mathcal{A} \subset [0, 10^9|\mathcal{A}_1|] \cup [p/2, p/2 + 10^9|\mathcal{A}_1|]$. Therefore $\big(2 \cdot \mathcal{A}\big) \subset [0, 2 \cdot 10^9\,|\mathcal{A}_1|] \subset [0, p/2)$. Hence all of $\mathcal{A}$ can be rectified, so the $3|A| - 4$ statement in the integers gives the desired covering.

Case 2. If $\dim(A_1) = 2$ then we apply Corollary 2.6, obtaining progressions P_1, P_2 with union covering A_1, with same common difference r. We claim that we can assume without loss of generality that $\mathcal{A}_1 \subset [0, 3|\mathcal{A}|) \cup [c, c + 3|\mathcal{A}|) \subset [0, p/2)$ with $0, c + 3|\mathcal{A}| - 1 \in \mathcal{A}$ for some $c \in \mathbb{Z}_p$ and $|\mathcal{A}_1 \cap [0, 3|\mathcal{A}|)| \geq |\mathcal{A}_1|/2$. Indeed, if $r \neq 1$, then we can dilate by $r^{-1} \mod p$ so as to ensure that $r^{-1} \cdot \mathcal{A}_1 \subseteq [0, 3|\mathcal{A}|) \cup [c, c+3|\mathcal{A}|)$ with $0, c+3|\mathcal{A}|-1 \in r^{-1} \cdot \mathcal{A}$. If $c+3|\mathcal{A}| < p/2$, then the first two requirements are met and we can ensure that $|r^{-1} \cdot \mathcal{A}_1 \cap [0, 3|\mathcal{A}|)| \geq |\mathcal{A}_1|/2$ by multiplying the set with -1 and translating if necessary. If $p/2 - 3|\mathcal{A}| \leq c \leq p/2 + 3|\mathcal{A}|$, then $2 \cdot r^{-1} \cdot \mathcal{A}_1$ must lie in $[-6|\mathcal{A}|, 6|\mathcal{A}|]$ and arguing as in case 1 we conclude that $2 \cdot r^{-1} \cdot \mathcal{A} \subset \{0, p/2\} + [-6|\mathcal{A}|, 6|\mathcal{A}|]$, so $4 \cdot r^{-1} \cdot \mathcal{A} \subset [-12|\mathcal{A}|, 12|\mathcal{A}|]$ and again we can rectify all of $\mathcal{A}$ and complete the argument this way. Lastly, if $p/2 + 3|\mathcal{A}| < c$ then we simply translate the set by $-c$ to meet the first two requirements and again multiply by -1 if necessary. This proves our claim.

Now, let $\mathcal{S}' = [0, 3|\mathcal{A}|)$, $\mathcal{S}'' = [c, c + 3|\mathcal{A}|)$, $\mathcal{A}_1' = \mathcal{A}_1 \cap \mathcal{S}'$ and $\mathcal{A}_1'' = \mathcal{A}_1 \cap \mathcal{S}''$. By the claim above we have $|\mathcal{A}_1'| \geq |\mathcal{A}_1|/2$ and $\mathcal{S}' \cup \mathcal{S}'' \subset [0, p/2)$. We now show that

$$\mathcal{R} := \mathcal{A} \setminus \mathcal{A}_1 = \mathcal{A} \setminus (\mathcal{S}' \cup \mathcal{S}'') \subset [2c - 3|\mathcal{A}|, 2c + 6|\mathcal{A}|) = 2\mathcal{S}'' + [-3|\mathcal{A}|, 0]. \tag{15}$$

We start by observing that by assumption $\mathcal{A}_1 = \mathcal{A} \cap (\mathcal{S}' \cup \mathcal{S}'')$ was the most of $\mathcal{A}$ we could rectify. It follows that $[0, p/2) \setminus (\mathcal{S}' \cup \mathcal{S}'')$ does not contain any elements of $\mathcal{A}$. Next, let us assume that there exists $a \in \mathcal{A}$ satisfying $a \in [-3|\mathcal{A}|, 0)$. Since $\mathcal{A}_1 \cup \{a\}$ cannot be rectified, we must have $c + 3|\mathcal{A}| > p/2 - 3|\mathcal{A}|$. This implies that $[c, c + 3|\mathcal{A}|) \subset [p/2 - 6|\mathcal{A}|, p/2)$, whence

$$2 \cdot (\mathcal{A}_1 \cup \{a\}) \subset [-12|\mathcal{A}|, 6|\mathcal{A}|) \subset [0, p/2) - 12|\mathcal{A}|,$$

which contradicts our maximality assumption about $\mathcal{A}_1$. It follows that $\mathcal{A} \cap [-3|\mathcal{A}|, 0) = \emptyset$. Arguing similarly, we see that $\mathcal{A} \cap [c + 3|\mathcal{A}|, c + 6|\mathcal{A}|) = \emptyset$: certainly $\mathcal{A} \cap [c + 3|\mathcal{A}|, p/2) = \emptyset$, and

if there is $a \in \mathcal{A} \cap [p/2, c+6|\mathcal{A}|) \subset [p/2, p/2+3|\mathcal{A}|)$ then $[c, c+3|\mathcal{A}|) \subset [p/2-6|\mathcal{A}|, p/2)$, and so $2 \cdot (\mathcal{A}_1 \cup \{a\}) \subset [-12|\mathcal{A}|, 12|\mathcal{A}|)$, again contradicting our maximality assumption.

Next, we note that

$$2\mathcal{A}_1 \subset [0, 6|\mathcal{A}|) \cup [c, c+6|\mathcal{A}|) \cup [2c, 2c+6|\mathcal{A}|).$$

It follows that if there exists $a \in \mathcal{A}$ satisfying

$$a \in [p/2, 0) \setminus \big([-3|\mathcal{A}|, 6|\mathcal{A}|) \cup [c-3|\mathcal{A}|, c+6|\mathcal{A}|) \cup [2c-3|\mathcal{A}|, 2c+6|\mathcal{A}|)\big),$$

then $a + \mathcal{A}_1'$ does not intersect $2\mathcal{A}_1$ and we get the contradiction

$$\begin{aligned} |2\mathcal{A}| \geq |2\mathcal{A}_1| + |a + \mathcal{A}_1'| &\geq (2|\mathcal{A}_1'| - 1) + (2|\mathcal{A}_1''| - 1) + (|\mathcal{A}_1'| + |\mathcal{A}_1''| - 1) + |\mathcal{A}_1'| \\ &\geq 3.5|\mathcal{A}_1| - 3 > 2.48|\mathcal{A}| - 7. \end{aligned}$$

Note that we have used that $2\mathcal{A}_1' \cap (A_1' + A_1'') = \emptyset$ as well as $2\mathcal{A}_1'' \cap (A_1' + A_1'') = \emptyset$ as given by Corollary 2.6. Using the previous observations, it follows that equation (15) is established and we have $\mathcal{A} = \mathcal{A}_1' \cup \mathcal{A}_1'' \cup \mathcal{R}$ where $\mathcal{R} = \mathcal{A} \cap [2c-3|\mathcal{A}|, 2c+6|\mathcal{A}|)$. Note that we may assume that $|\mathcal{R}| \geq 0.17|\mathcal{A}|$ as otherwise $|\mathcal{A}_1| \geq 0.83|\mathcal{A}|$ and in equation (14) we would in fact get $|2\mathcal{A}_1| \leq 3|\mathcal{A}| - 4$, which due to Theorem 2.4 would contradict our assumption that $\mathcal{A}_1$ is 2-dimensional.

We note that $2\mathcal{A} \supseteq 2\mathcal{A}_1 \cup (\mathcal{A}_1'' + \mathcal{R})$ and that trivially $|\mathcal{A}_1'' + \mathcal{R}| \geq |\mathcal{R}|$. It follows that $\mathcal{A}_1'' + \mathcal{R}$ must intersect $2\mathcal{A}_1$ since otherwise we would get the contradiction

$$|2\mathcal{A}| \geq |2\mathcal{A}_1| + |\mathcal{R}| \geq 3.17|\mathcal{A}_1| - 2 > 2.48|\mathcal{A}| - 7.$$

It follows that one of the following must hold:

(i) If $(\mathcal{A}_1'' + \mathcal{R}) \cap 2\mathcal{A}_1'' \neq \emptyset$, then we must have

$$3c + 9|\mathcal{A}| - p \geq 2c \quad \text{and} \quad 3c - 3|\mathcal{A}| - p \leq 2c + 6|\mathcal{A}|,$$

and therefore $c \in [p - 9|\mathcal{A}|, p + 9|\mathcal{A}|]$. However, we know that $c \leq p/2$ and that the cardinality of $\mathcal{A}$ is sufficiently small with respect to p, so we get a contradiction. it follows that

(ii) If $(\mathcal{A}_1'' + \mathcal{R}) \cap (\mathcal{A}_1' + \mathcal{A}_1'') \neq \emptyset$, then we must have

$$3c + 9|\mathcal{A}| - p \geq c \quad \text{and} \quad 3c - 3|\mathcal{A}| - p \leq c + 6|\mathcal{A}|,$$

and therefore $c \in [p/2 - 9/2\,|\mathcal{A}|, p/2 + 9/2\,|\mathcal{A}|]$. Consequently, in this case $\mathcal{A}_1'$ and $\mathcal{R}$ are focused around 0 and $\mathcal{A}_1''$ is focused around $p/2$. It follows that a dilation by a factor of 2 focuses all parts of $\mathcal{A}$ around 0, that is

$$2 \cdot \mathcal{A} \subset [-12|\mathcal{A}|, 15|\mathcal{A}|) \subset -12|\mathcal{A}| + [0, p/2).$$

This means that all of $\mathcal{A}$ can be rectified and we can just apply the $3|\mathcal{A}| - 4$ statement in the integers to get the desired covering property.

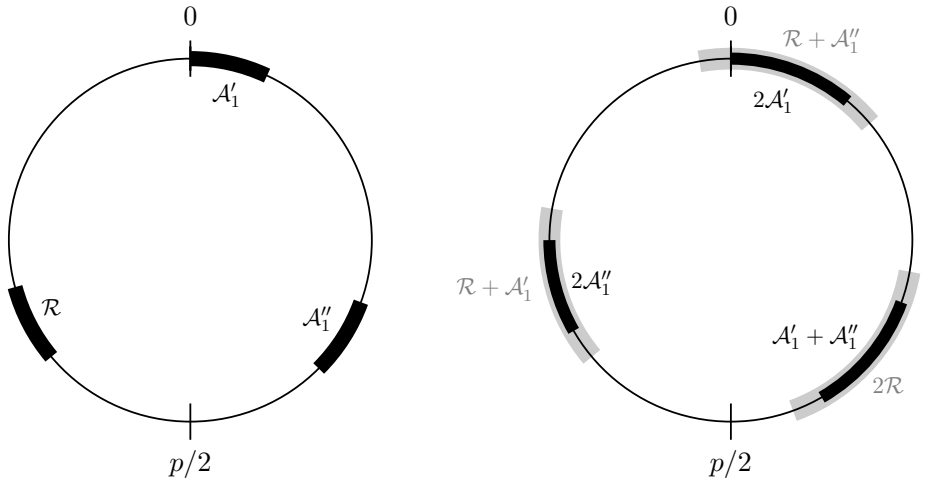

Figure 1: Distribution of $\mathcal{A}$ and $2\mathcal{A}$ in $\mathbb{Z}_p$ in case (iii).

(iii) If $(\mathcal{A}_1''+\mathcal{R})\cap 2\mathcal{A}_1' \neq \emptyset$, then we must have

$$3c+9|\mathcal{A}|-p\geq 0 \quad \text{and} \quad 3c-3|\mathcal{A}|-p\leq 6|\mathcal{A}|,$$

and therefore $c\in[p/3-3|\mathcal{A}|, p/3+3|\mathcal{A}|]$. Consequently, in this case $\mathcal{A}_1', \mathcal{A}_1''$ and $\mathcal{R}$ (or rather the intervals containing them) are roughly "equally distributed" in $\mathbb{Z}_p$, that is they are respectively focused around $0, p/3$ and $2p/3$ as illustrated in Figure 1. It follows that a dilation by a factor of 3 focuses all parts of $\mathcal{A}$ around 0, that is

$$3\cdot\mathcal{A}\subset[-27|\mathcal{A}|, 54|\mathcal{A}|)\subset -27|\mathcal{A}|+[0,p/2).$$

This again means that all of $\mathcal{A}$ can be rectified and we can just apply the $3|\mathcal{A}|-4$ statement in the integers to get the desired covering property.

It follows that we have proven the statement of Theorem 1.1. □

4 Concluding remarks

It is probably unreasonable to expect that this rectification methodology (of rectifying a large part of the set and arguing from there) will lead to a proof of the full conjecture with tight constants. In fact, the more natural direction seems to be to apply covering results in the cyclic group in order to prove covering statements in the integers. Both Lev and Smeliansky's proof of Freiman's $3|A|-4$ statement in the integers as well as the proof of Proposition 2.3 fall into that category.

Even if all other ingredients existed in their ideal form, the rectification argument through a large Fourier coefficient appears to imply an inherent loss in the density. This is a problem concerning not only Freiman's original approach and the result presented here, but also the broader result of Green and Ruzsa.

Two almost identical conjectures, differing only by a constant of 1, have been made as to what the true form of a statement like Theorem 1.1 should look like, see [11, 10, 1] as well as [20]. It is clear that any such statement should include the following result of Vosper.

Theorem 4.1 (Vosper [21]). *Let $\mathcal{A} \subseteq \mathbb{Z}_p$ satisfy $|\mathcal{A}| \geq 2$ and $|2\mathcal{A}| \leq p-2$. Then $|2\mathcal{A}| = 2|\mathcal{A}|-1$ if and only if $\mathcal{A}$ is an arithmetic progression.*

The conjecture stated in [20] has the advantage of being such a generalization, but unfortunately it does not hold in its stated form. On the other hand, we believe the conjecture stated in [11, 10, 1] to be true, but it does not include the result of Vosper. We therefore propose the following combined version of the conjecture, which implies Vosper's theorem when $|\mathcal{A}| \geq 4$.

Conjecture 4.2. *Let a set $\mathcal{A} \subset \mathbb{Z}_p$ be given. If either*

(i) $0 \leq |2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) \leq \min(|\mathcal{A}| - 4, p - |2\mathcal{A}| - 2)$ *or*

(ii) $0 \leq |2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) = |\mathcal{A}| - 3 \leq p - |2\mathcal{A}| - 3$

then $\mathcal{A}$ can be covered by an arithmetic progression of length at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Let us provide two examples which show that this statement, if true, is tight. The first example proves the need for the requirement $|2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) \leq p - |2\mathcal{A}| - 2$ in case (i) and the second example proves that the case $|2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) = |\mathcal{A}| - 3$ needs to be handled separately.

Example 4.3 (Serra and Zémor [20]). *Given $k \geq 2$ and $0 \leq x \leq k-3$ let $p = 2k + 2x - 1$ be prime and $\mathcal{A} = \{0\} \cup \{x+2, x+3, ..., (p+1)/2\} \subset \mathbb{Z}_p$ so that $|\mathcal{A}| = k$. We have*

$$2\mathcal{A} = \{x+2, \ldots, p-1, 0, 1\} = \mathbb{Z}_p \setminus \{2, \ldots, x+1\}$$

so that $|2\mathcal{A}| = 2|\mathcal{A}| - 1 + x = p - x$. Clearly $\mathcal{A}$ cannot be covered by an arithmetic progression of length at most $|\mathcal{A}| + x = |2\mathcal{A}| - |\mathcal{A}| + 1$.

To see that this example not only implies the requirement $|2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) \leq p - |2\mathcal{A}| - 1$ but also $|2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) \leq p - |2\mathcal{A}| - 2$, note that $|2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) = p - |2\mathcal{A}| - 1$ would imply that the prime p is even.

Example 4.4. *Take a prime $p = 4t - 1$ where $t \geq 2$. Let $\mathcal{A} = \{0, \ldots, t\} \setminus \{t-1\} \cup \{2t\}$, that is $|\mathcal{A}| = t + 1$. We have*

$$2\mathcal{A} = \{0, \ldots, 2t-2\} \cup \{2t, \ldots, 3t-2\} \cup \{3t\} = \mathbb{Z}_p \setminus \{2t-1, 3t-1, 3t+1, \ldots, 4t-2\}$$

so that $|2\mathcal{A}| = 3t - 1 = 3|\mathcal{A}| - 4 = 2|\mathcal{A}| - 1 + x = p - t = p - (x+2)$ where $x = |\mathcal{A}| - 3$. Clearly $\mathcal{A}$ cannot be covered by an arithmetic progression of length at most $|\mathcal{A}| + x = |2\mathcal{A}| - |\mathcal{A}| + 1$.

Besides satisfying these two examples as well as implying the full strength of Vosper's Theorem in the case $|2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) = 0$, Conjecture 4.2 would also imply the following part of a conjecture of Freiman [7] in the integers, giving perhaps some additional intuition as to its slightly unusual shape.

Corollary 4.5. *Assume that Conjecture 4.2 holds and let $A \subset \mathbb{Z}$ be a 1-dimensional set in normal form for which $\max(A)$ is prime. If $|2A| = 3|A| - 4 + b \leq 4|A| - 8$, then A can be covered by an arithmetic progression of length at most $2(|A| + b - 2) + 1$. If $|2A| = 4|A| - 7$, then A can be covered by an arithmetic progression of length at most $4|A| - 8$.*

Proof. Let $\mathcal{A}$ denote the canonical embedding of A into $\mathbb{Z}_{\max(A)}$. We start with the case $|2A| \leq 4|A| - 8$ and note as in the proof of Proposition 2.3 that

$$|2\mathcal{A}| \leq |2A| - |A| \leq 2|\mathcal{A}| - 1 + (b-1) \leq 3|\mathcal{A}| - 5.$$

Setting $x = |2\mathcal{A}| - (2|\mathcal{A}| - 1) \leq b - 1 \leq |\mathcal{A}| - 4$ it would follow from case (i) of Conjecture 4.2 that either $|2\mathcal{A}| > \max(A) - (x+2)$ and therefore we get the desired covering property for A, or that $\mathcal{A}$ can be contained in an arithmetic progression of length at most $|\mathcal{A}| + x \leq (\max(A) + 1)/2$, implying that $\mathcal{A}$ is rectifiable and therefore by Lemma 2.2 contradicting the requirement that A is 1-dimensional.

Now if $|2A| = 4|A| - 7$ then $x = |2\mathcal{A}| - (2|\mathcal{A}| - 1) \leq |\mathcal{A}| - 3$ and we again either get the desired covering property from Conjecture 4.2, or we get a contradiction to the requirement that A is 1-dimensional. □

Note that this proof is essentially the same as that of Proposition 2.3. The requirement that $\max(A)$ is prime does not appear in Freiman's original conjecture and is artificial, but the corollary gives an indication of the relationship between Conjecture 4.2 and the mentioned conjecture by Freiman. In fact, the bounds given in the statement would imply that $\max(A)$ is even in the extremal case. To prove such a statement without that condition one would require an analogue of Conjecture 4.2 in general $\mathbb{Z}_m$, that is a strengthening of the results of Kemperman [13] or Deshouillers and Freiman [4]. To our knowledge, such a conjecture has not been explicitly formulated and might in fact be very intricate to state.

Acknowledgements. We are very grateful to the anonymous referee for useful remarks that helped to improve this paper.

References

[1] P. Candela and A. De Roton. On sets with small sumset in the circle. *The Quarterly Journal of Mathematics*, 70(1):49–69, 2018.

[2] P. Candela, D. González-Sánchez, and D. J. Grynkiewicz. On sets with small sumset and m-sumfree sets in $\mathbb{Z}/p\mathbb{Z}$. *arXiv preprint arXiv:1909.07967*, 2019.

[3] M.-C. Chang et al. A polynomial bound in Freiman's theorem. *Duke mathematical journal*, 113(3):399–419, 2002.

[4] J.-M. Deshouillers and G. A. Freiman. A step beyond Kneser's theorem for abelian finite groups. *Proceedings of the London Mathematical Society*, 86(1):1–28, 2003.

[5] G. Freiman. Inverse problems in additive number theory. Addition of sets of residues modulo a prime. In *Dokl. Akad. Nauk SSSR*, volume 141, pages 571–573, 1961.

[6] G. Freiman. Foundations of a structural theory of set addition. Translated from the Russian. Translations of mathematical monographs. *American Mathematical Society, Providence, RI*, 1973.

[7] G. A. Freiman and O. Serra. On doubling and volume: chains. *Acta Arithmetica*, 186:37–59, 2018.

[8] B. Green and I. Z. Ruzsa. Sets with small sumset and rectification. *Bulletin of the London Mathematical Society*, 38(1):43–52, 2006.

[9] B. Green and I. Z. Ruzsa. Freiman's theorem in an arbitrary abelian group. *Journal of the London Mathematical Society*, 75(1):163–175, 2007.

[10] D. J. Grynkiewicz. *Structural additive theory*, volume 30. Springer Science & Business Media, 2013.

[11] Y. O. Hamidoune, O. Serra, and G. Zémor. On the critical pair theory in $\mathbb{Z}/p\mathbb{Z}$. *arXiv preprint math/0507561*, 2005.

[12] R. Jin. Freiman's inverse problem with small doubling property. *Advances in Mathematics*, 216(2):711–752, 2007.

[13] J. H. B. Kemperman. On small sumsets in an abelian group. *Acta Mathematica*, 103(1-2):63–88, 1960.

[14] V. F. Lev. Distribution of points on arcs. *Integers*, 5(2):A11, 2005.

[15] V. F. Lev and P. Y. Smeliansky. On addition of two distinct sets of integers. *Acta Arithmetica*, 70(1):85–91, 1995.

[16] Ø. J. Rødseth. On Freiman's 2.4-theorem. *Skr. K. Nor. Vidensk. Selsk*, (4):11–18, 2006.

[17] I. Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Mathematica Hungarica*, 65(4):379–388, 1994.

[18] T. Sanders. Appendix to Roth's theorem on progressions revisited by J. Bourgain. *Journal d'Analyse Mathématique*, 104(1):193–206, 2008.

[19] T. Schoen. Near optimal bounds in Freiman's theorem. *Duke Mathematical Journal*, 158(1):1–12, 2011.

[20] O. Serra and G. Zémor. Large sets with small doubling modulo p are well covered by an arithmetic progression. In *Annales de l'institut Fourier*, volume 59, pages 2043–2060, 2009.

[21] A. G. Vosper. The critical pairs of subsets of a group of prime order. *Journal of the London Mathematical Society*, 1(2):200–205, 1956.