ARTICLE IN PRESS

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Small doubling in cyclic groups

Vsevolod F. Lev

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel

ARTICLE INFO

Article history:
Received 11 November 2020
Received in revised form 26 June 2022
Accepted 29 June 2022
Available online xxxx
Communicated by L. Smajlovic

MSC:
primary 11P70
secondary 11B75

Keywords:
Small doubling
Doubling constant
Coset progressions

ABSTRACT

We give a comprehensive description of the sets A in finite cyclic groups such that $|2A| < \frac{9}{4}|A|$; namely, we show that any set with this property is densely contained in a (one-dimensional) coset progression. This improves earlier results of Deshouillers-Freiman and Balasubramanian-Pandey.

Contents

E-mail address: seva@math.haifa.ac.il.

https://doi.org/10.1016/j.jnt.2022.06.001

1. Introduction

One of the central problems of additive combinatorics is to understand the structure of small-doubling sets, or *approximate subgroups*, which are sets A of group elements such that the sumset $2A := \{a + b\colon a, b \in A\}$ has size comparable with the size of A.

We use the additive notation throughout since we will be concerned with abelian groups only, and particularly with the finite cyclic groups, which we denote $\mathbb{Z}_n$; here n is the order of the group. Our goal is to prove the following result.

Theorem 1.1. *Let n be a positive integer. If a set $A \subseteq \mathbb{Z}_n$ satisfies $|2A| < \frac{9}{4}|A|$, then one of the following holds:*

(i) *There is a subgroup $H \leq \mathbb{Z}_n$ such that A is contained in an H-coset and $|A| > C^{-1}|H|$, where $C = 2 \cdot 10^5$.*
(ii) *There is a proper subgroup $H < \mathbb{Z}_n$ and an arithmetic progression P of size $|P| > 1$ such that $|P + H| = |P||H|$, $A \subseteq P + H$, and*

$$(|P| - 1)|H| \leq |2A| - |A|.$$

(iii) *There is a proper subgroup $H < \mathbb{Z}_n$ such that A meets exactly three H-cosets, the cosets are not in an arithmetic progression, and*

$$3|H| \leq |2A| - |A|.$$

We notice that the coefficient $\frac{9}{4}$ in Theorem 1.1 is in fact a threshold in the sense that the assumption $|2A| < \frac{9}{4}|A|$ cannot be relaxed even to $|2A| \leq \frac{9}{4}|A|$: for instance, if n is large enough, and $A = \{-1, 0, 1\} \cup \{a\}$ with $a \notin \{-3, \dots, 3\}$ and $2a \notin \{-2, \dots, 2\}$, then $|2A| = \frac{9}{4}|A|$ while A does not have the structure described in Theorem 1.1.

Theorem 1.1 improves the following result by Deshouillers and Freiman.

Theorem 1.2 *([DF03, Theorem 1]). Let n be a positive integer. If a set $A \subseteq \mathbb{Z}_n$ satisfies $|2A| < 2.04|A|$, then one of the following holds:*

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

(i) *There is a subgroup $H \le \mathbb{Z}_n$ such that A is contained in an H-coset and $|A| > 10^{-9}|H|$.*

(ii) *There is a proper subgroup $H < \mathbb{Z}_n$ and an arithmetic progression P of size $|P| > 1$ such that $A \subseteq P + H$ and*

$$(|P| - 1)|H| \le |2A| - |A|.$$

(iii) *There is a proper subgroup $H < \mathbb{Z}_n$ such that A meets exactly three H-cosets, the cosets are not in an arithmetic progression, and*

$$3|H| \le |2A| - |A|.$$

Moreover, in (ii) *and* (iii) *there is an H-coset containing at least $\frac{2}{3}|H|$ elements of A.*

We notice that in the cases (ii) and (iii) of both Theorem 1.1 and Theorem 1.2, we have $|H| \le |2A| - |A| < |2A|$, which establishes properness of H as an immediate consequence of the other assertions.

Similarly, if the equality $|P + H| = |P||H|$ of Theorem 1.1 (ii) fails to hold, then $P + H$ is a coset of a subgroup of size at most $(|P| - 1)|H| \le |2A| - |A| < \frac{5}{4}|A| < C|A|$. Therefore, $|P + H| = |P||H|$ can be enforced by simply reclassifying the set A from type (ii) to type (i) whenever possible.

In the same vein, the existence of an H-coset containing at least $\frac{2}{3}|H|$ (and indeed, a somewhat larger proportion) of the elements of A is not difficult to derive assuming the other assertions, both for Theorem 1.1 and Theorem 1.2, provided $|P| > 2$. This is immediate in the case (iii) of either of the two theorems; for the case (ii), we delegate the exact statement and the proof to Proposition A.1 in the Appendix.

A version of Theorem 1.2 was proved by Balasubramanian and Pandey [BP18, Theorem 2] who have, essentially, improved the coefficient from 2.04 to 2.1 under some extra assumptions.

Two other classical results which Theorems 1.1 and 1.2 are worth comparing with are Kneser's theorem and Freiman's $(3n - 3)$-theorem; see Sections 4 and 6 for the formulations and references. Kneser's result deals with small-doubling sets in arbitrary abelian groups, but requires the doubling coefficient $|2A|/|A|$ to be smaller than 2. The $(3n - 3)$-theorem, on the other hand, allows the doubling coefficient to be as large as $3 - o(1)$, but assumes the underlying group to be torsion-free; specifically, it says that if A is a finite subset of a torsion-free abelian group such that $|2A| \le 3|A| - 4$, then A is contained in an arithmetic progression P with $|P| - 1 \le |2A| - |A|$. Both Kneser's and Freiman's theorem are employed in our argument.

The proof of Theorem 1.1 is inductive, and for the induction to go through, we actually prove the following version of the theorem.

Theorem 1.3. *Let n be a positive integer. If a set $A \subseteq \mathbb{Z}_n$ is not contained in a coset of a proper subgroup and satisfies $|2A| < \min\{\frac{9}{4}|A|, n\}$, then one of the following holds:*

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

(i) $|2A| - |A| > C_0^{-1} n$ *where* $C_0 = 1.5 \cdot 10^5$.

(ii) *There is a proper subgroup* $H < \mathbb{Z}_n$ *and an arithmetic progression* P *of size* $|P| > 1$ *such that* $|P + H| = |P||H|$, $A \subseteq P + H$, *and*

$$(|P| - 1)|H| \le |2A| - |A|.$$

(iii) *There is a proper subgroup* $H < \mathbb{Z}_n$ *such that* A *meets exactly three* H*-cosets, the cosets are not in an arithmetic progression, and*

$$3|H| \le |2A| - |A|.$$

Deduction of Theorem 1.1 from Theorem 1.3. Suppose that $A \subseteq \mathbb{Z}_n$ satisfies $|2A| < \frac{9}{4}|A|$ and, without loss of generality, assume also that $0 \in A$ and $|A| \ge 2$. Let $L \le \mathbb{Z}_n$ be the subgroup generated by A.

If $2A = L$, then $|A| > \frac{4}{9}|2A| = \frac{4}{9}|L|$; thus, A has the structure of Theorem 1.1 (i). Assuming now that $2A \ne L$, we apply Theorem 1.3 to the set A with L (instead of $\mathbb{Z}_n$) as the underlying group, and consider two possible cases.

If $A \subset L$ satisfies the inequality of Theorem 1.3 (i), then $C_0^{-1}|L| \le |2A| - |A| < \frac{5}{4}|A|$, so that $|A| > \frac{4}{5C_0}|L| > \frac{1}{C}|L|$; this is case (i) of Theorem 1.1.

On the other hand, it is clear that Theorem 1.3 (ii) implies Theorem 1.1 (ii), and similarly Theorem 1.3 (iii) implies Theorem 1.1 (iii). □

We thus focus on the proof of Theorem 1.3; once it is completed, Theorem 1.1 will follow. We will also ignore the equality $|P + H| = |P||H|$ of Theorem 1.3 (ii): if it is violated, then $P + H$ is a coset of a subgroup of size at most $(|P| - 1)|H| \le |2A| - |A| < |2A| < n$, so that A is contained in a coset of a proper subgroup, contrary to the assumptions of the theorem.

As explained above, the coefficient 9/4 of Theorem 1.1 cannot be replaced with a larger one. However, it is plausible to expect that the following can be true.

Conjecture 1.4. *For any* $\varepsilon > 0$ *there exist positive constants* $C_1(\varepsilon)$ *and* $C_2(\varepsilon)$ *such that if* n *is a positive integer, and* $A \subseteq \mathbb{Z}_n$ *satisfies* $|A| < (C_1(\varepsilon))^{-1} n$ *and* $|2A| < (3 - \varepsilon)|A|$, *then there are a subset* $P \subseteq \mathbb{Z}_n$ *with* $|2P|/|P| \le |2A|/|A|$ *and a proper subgroup* $H < \mathbb{Z}_n$ *such that* $A \subseteq P + H$, $(|2P| - |P|)|H| \le |2A| - |A|$, *and either* $|P| \le C_2(\varepsilon)$, *or* P *is an arithmetic progression.*

We remark that the inequality $|2P|/|P| \le |2A|/|A|$ follows in fact from the other assertions:

$$|A| \left(\frac{|2P|}{|P|} - 1 \right) \le |P||H| \left(\frac{|2P|}{|P|} - 1 \right) = (|2P| - |P|)|H| \le |2A| - |A| = |A| \left(\frac{|2A|}{|A|} - 1 \right).$$

Theorem 1.1 and Conjecture 1.4 show that any set with the small doubling coefficient is, essentially, obtained by "lifting" a small-doubling set which is either nicely struc-

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

tured (an arithmetic progression), or otherwise belongs to a finite collection of sporadic examples.

Our argument follows the general line of reasoning introduced by Freiman in [F61] and then pursued by other authors; namely, we use character sums to conclude that small doubling leads to a biased distribution, and then use the bias as a starting point for the combinatorial part of the proof. The improvements come from a refinement in the character sums component, in the spirit of [LS20]; from replacing the main auxiliary result used in Deshouillers-Freiman [DF03, Theorem 2] with its stronger version [L22, Theorem 2], see Section 3; and, finally, from using an intricate combinatorial analysis.

The rest of the paper is structured as follows. In the next section we introduce the notation that will be used throughout and considered standard. In Section 3 we prove Theorem 1.3 in the special case where the image of the small-doubling set under a suitable homomorphism is *rectifiable*; although this case is of principal importance, the proof is, essentially, just a reduction to [L22, Theorem 2]. In Section 4 we present Kneser's theorem and a relaxed version of Kemperman's theorem. In Section 5 we establish a number of properties of the sets with a "very small" doubling coefficients, including the asymmetric case. Some other general results on set addition in abelian groups, mostly of combinatorial nature, are gathered in Section 6. Section 7 establishes a number of results about the minimal counterexample set (which, as we eventually show, does not exist). Two more results of this sort, Lemmas 8.1, and 9.1, show that the minimum counterexample set, if it exists, meets at least four cosets of any subgroup, with the obvious exceptions; these two lemmas are singled out into dedicated Sections 8 and 9. Their proofs are quite technical and some readers may prefer to skip the details and proceed to Section 10 where the character sum component of the argument is presented. The proof is completed in the concluding Section 11.

2. Notation

Let G be an abelian group.

2.1. Groups

By $A+B$ we denote the Minkowski sum of the sets $A, B \subseteq G$; that is, $A+B = \{a+b\colon a \in A,\ b \in B\}$. We write $2A := A+A$.

For a subgroup $H \le G$, the canonical homomorphism $G \to G/H$ is denoted φ_H; thus, for instance, if $\mathbb{Z}$ is the group of integers, then $\mathbb{Z}_n = \varphi_{n\mathbb{Z}}(\mathbb{Z})$. For $g_1, g_2 \in G$, we may occasionally write $g_1 \equiv g_2 \pmod{H}$ as an alternative to $g_1 - g_2 \in H$, $g_1 + H = g_2 + H$, or $\varphi_H(g_1) = \varphi_H(g_2)$.

The *period* (or *stabilizer*) of a subset $S \subseteq G$ is the subgroup $\pi(S) := \{g \in G\colon S+g = S\} \le G$, and S is *periodic* or *aperiodic* according to whether $\pi(S) \ne \{0\}$ or $\pi(S) = \{0\}$.

The *index* of a subgroup $H \le G$, denoted $[G:H]$, is the size of the quotient group G/H; thus, if G is finite, then $[G:H] = |G|/|H|$.

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

We say that a coset $g + H$ is *determined* by a subset $A \subseteq G$ if the intersection $A \cap (g + H)$ is nonempty. In this case we also say that A *meets*, or *intersects*, $g + H$.

The coset $g + H$ is *proper* if the subgroup H is proper.

An *involution* of G is an element $g \in G$ of order 2. Importantly, a cyclic group has at most one involution.

A finite subset A of an abelian group will be called a *very-small-doubling set* (VSDS for short) if $|2A| < \frac{3}{2}|A|$; equivalently, if A is contained in a finite coset with density exceeding 2/3, see Section 5.

2.2. Progressions

For an integer $N \geq 1$, the N-term arithmetic progression in G with difference $d \in G$ and initial term $g \in G$ is the set $P = \{g, g+d, \dots, g+(N-1)d\}$; thus, for instance, singletons and cosets of finite nonzero subgroups are considered arithmetic progressions, while the empty set is not. A progression is *primitive* if its difference generates G. Singletons are not considered primitive.

For real $u \leq v$, by $[u, v]$ we denote both the set of all integers z satisfying $u \leq z \leq v$, and the image of this set under the canonical homomorphism $\varphi_{n\mathbb{Z}}$ from the group of integers to the cyclic group under consideration.

2.3. Local isomorphism and rectification

We say that a subset $S \subseteq G$ is *rectifiable* if it is *locally isomorphic* (or *Freiman-isomorphic*) to a set of integers; that is, if there is a mapping $\lambda\colon S \to \mathbb{Z}$ such that for any $s_1, \dots, s_4 \in S$, we have $s_1 + s_2 = s_3 + s_4$ if and only if $\lambda(s_1) + \lambda(s_2) = \lambda(s_3) + \lambda(s_4)$. Taking $s_1 = s_3$, we see that λ is bijective; hence, $|\lambda(S)| = |S|$. It is equally easy to see that $|2\lambda(S)| = |2S|$.

If $d \in G$ is an element of order $N \geq 2$, then any arithmetic progression with difference d, and with at most $(N + 1)/2$ terms, is rectifiable. Indeed, this is the only kind of rectifiable sets that actually appear below.

2.4. Regularity

For an integer $k \geq 2$, we say that a set $A \subseteq \mathbb{Z}_n$ is *k-regular* if it has the structure of Theorem 1.3 (ii) with a k-element progression P, and that A is *singular* if it has the structure of Theorem 1.3 (iii). Thus, Theorem 1.3 essentially says that any small-doubling set $A \subseteq \mathbb{Z}_n$ which is not densely contained in a coset is either regular or singular.

3. Theorem 1.3 for rectifiable sets

One of the key ingredients of our argument is the following refinement of [DF03, Theorem 2].

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

Theorem 3.1 *([L22, Theorem 2]). Suppose that F is a finite group, and that A is a finite subset of the group $G := \mathbb{Z} \times F$. Let s be the number of elements of the image of A under the projection $G \to \mathbb{Z}$ along F. If $|2A| < 3(1 - 1/s)|A|$, then there exist an arithmetic progression $P \subseteq G$ of size $|P| \geq 3$ and a subgroup $H \leq \{0\} \times F$ such that $|P + H| = |P||H|$, $A \subseteq P + H$, and $(|P| - 1)|H| \leq |2A| - |A|$.*

The equality $|P + H| = |P||H|$ (which is somewhat implicit in [L22]) is, in fact, an easy consequence of the other assertions, as it follows by considering the difference of P. The difference cannot be contained in the subgroup $\{0\} \times F$, since in this case P, and therefore also $P + H$ and $A \subseteq P + H$, would be contained in a coset of $\{0\} \times F$, leading to $s = 1$ and thus contradicting the assumption $|2A| < 3\big(1 - \frac{1}{s}\big)|A|$. Thus, the difference is of infinite order, and therefore the difference of any two distinct elements of P is of infinite order, too, and does not belong to the finite subgroup H.

The following result establishes Theorem 1.3 in the special case where the image of A under a suitable homomorphism is sufficiently large and rectifiable.

Proposition 3.2. *Suppose that n is a positive integer, $L \leq \mathbb{Z}_n$ is a subgroup, and $A \subseteq \mathbb{Z}_n$ is a subset with $\varphi_L(A)$ rectifiable. If $|2A| < 3(1 - 1/s)|A|$, where $s = |\varphi_L(A)|$, then there exist an arithmetic progression $P \subseteq \mathbb{Z}_n$ of size $|P| > 1$ and a proper subgroup $H < \mathbb{Z}_n$ such that $A \subseteq P + H$, $|P + H| = |P||H|$, and $(|P| - 1)|H| \leq |2A| - |A|$.*

We close this section with the deduction of Proposition 3.2 from Theorem 3.1.

Proof of Proposition 3.2. Since $\varphi_L(A)$ is rectifiable, there is a local isomorphism, say λ, from $\varphi_L(A)$ to $\mathbb{Z}$, and then the mapping $\psi\colon A \to \mathbb{Z} \times \mathbb{Z}_n$ defined by

$$\psi(a) := (\lambda \circ \varphi_L(a), a), \ a \in A$$

is a local isomorphism between A and its image in $\mathbb{Z} \times \mathbb{Z}_n$. Consequently, the set $\psi(A) \subseteq \mathbb{Z} \times \mathbb{Z}_n$ satisfies $|\psi(A)| = |A|$ and $|2\psi(A)| = |2A|$. As a result,

$$\frac{|2\psi(A)|}{|\psi(A)|} = \frac{|2A|}{|A|} < 3\Big(1 - \frac{1}{s}\Big).$$

On the other hand, the size of the projection of the set $\psi(A) \subseteq \mathbb{Z} \times \mathbb{Z}_n$ onto the first component of the direct product is $|\lambda \circ \varphi_L(A)| = |\varphi_L(A)| = s$. Thus, we can apply Theorem 3.1 to the set $\psi(A)$ to find an arithmetic progression $Q \subseteq \mathbb{Z} \times \mathbb{Z}_n$ of size $|Q| \geq 3$ and a subgroup $K \leq \{0\} \times \mathbb{Z}_n$ such that

$$\psi(A) \subseteq Q + K \tag{3.1}$$

and

$$(|Q| - 1)|K| \leq |2\psi(A)| - |\psi(A)| = |2A| - |A|; \tag{3.2}$$

moreover, the elements of Q reside in pairwise distinct K-cosets, and K is proper in $\{0\} \times \mathbb{Z}_n$ since otherwise we would have $|K| = n$ and then

$$2n \le (|Q| - 1)|K| \le |2A| - |A| < 2|A| \le 2n.$$

Denoting by ω the projection of $\mathbb{Z} \times \mathbb{Z}_n$ onto the second coordinate, we let $H := \omega(K) \le \mathbb{Z}_n$ and $P := \omega(Q) \subseteq \mathbb{Z}_n$. From (3.1) and (3.2), and in view of $|P| \le |Q|$ and $|H| = |K|$, we readily conclude that $A \subseteq P + H$ and $(|P| - 1)|H| \le |2A| - |A|$. It remains to show that the elements of P lie in pairwise distinct H-cosets, and that $|P| > 1$.

To address the former point, we write $Q = \{g, g+d, \dots, g+(N-1)d\}$ where $N := |Q| \ge 3$. For $0 \le i < j \le N-1$, the elements $\omega(g+id), \omega(g+jd) \in P$ are in the same H-coset if and only if $(i-j)\omega(d) \in H$; that is, if and only if $i \equiv j \pmod{\operatorname{ord}(\omega(d))}$, where $\operatorname{ord}(\omega(d))$ is the order of $\omega(d)$ in $\mathbb{Z}_n/H$. Moreover, in this case $\omega(g + id) + H = \omega(g + jd) + H$. Thus, if $\operatorname{ord}(\omega(d)) \ge N$, then all elements of P reside in distinct H-cosets, while if $\operatorname{ord}(\omega(d)) < N$, then the sum $P + H$ will not be affected if we replace P with its sub-progression $\omega(\{g + id \colon 0 \le i < \operatorname{ord}(\omega(d))\})$.

Finally, we show that $|P| > 1$. To this end we notice that if $|P| = 1$, then A is contained in an H-coset; as a result,

$$(|Q| - 1)|K| \ge 2|K| = 2|H| \ge 2|A| > |2A| - |A|$$

contradicting (3.2). □

We remark that the quantity $|\varphi_L(A)|$ is the number of L-cosets determined by A. The situation where this quantity is too small for Theorem 3.1 to be applicable is much more difficult to deal with.

4. Kneser's and Kemperman's theorems

Recall that the *period* of a subset A of an abelian group G is the subgroup $\pi(A) := \{g \in G \colon A + g = A\} \le G$, and that A is *periodic* if $\pi(A)$ is nonzero.

The following fundamental result due to Kneser is heavily used in our argument.

Theorem 4.1 *(Kneser [K53,K55]; see also [M65]). Let A and B be finite, non-empty subsets of an abelian group G such that*

$$|A + B| \le |A| + |B| - 1.$$

Then, writing $H := \pi(A + B)$, we have

$$|A + B| = |A + H| + |B + H| - |H|.$$

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

Since, in the above notation, $|A+H| \geq |A|$ and $|B+H| \geq |B|$, Theorem 4.1 shows that $|A+B| \geq |A|+|B|-|\pi(A+B)|$ holds for any finite, nonempty subsets A and B of an abelian group.

Corollary 4.2. *Let A and B be finite, non-empty subsets of an abelian group G. If*

$$|A+B| < |A|+|B|-1,$$

then $A+B$ is periodic.

Theorem 4.1 along with the corollary just stated will be referred to as *Kneser's theorem.*

Kemperman's structure theorem [K60] deals with the equality case of Kneser's theorem. Following Kemperman, we say that a pair (A,B) of finite subsets of an abelian group G is *elementary* if at least one of the following conditions holds:

(i) $\min\{|A|,|B|\} = 1$;
(ii) A and B are arithmetic progressions sharing a common difference $d \in G$, the order of which in G is at least $|A|+|B|-1$;
(iii) $A = g_1 + (H_1 \cup \{0\})$ and $B = g_2 - (H_2 \cup \{0\})$, where $g_1, g_2 \in G$ and H_1, H_2 are non-empty subsets of a subgroup $H \leq G$ such that $H = H_1 \cup H_2 \cup \{0\}$ is a partition of H. Moreover, g_1+g_2 is the only element of $A+B$ with a unique representation as $a+b$ with $a \in A$ and $b \in B$;
(iv) $A = g_1 + H_1$ and $B = g_2 - H_2$, where $g_1, g_2 \in G$ and H_1, H_2 are non-empty, aperiodic subsets of a subgroup $H \leq G$ such that $H = H_1 \cup H_2$ is a partition of H. Moreover, every element of $A+B$ has at least two representations as $a+b$ with $a \in A$ and $b \in B$.

The following theorem proved in [L06] is a simplified and relaxed version of the main result of [K60].

Theorem 4.3 *([L06, Theorem 1]). Let A and B be finite, non-empty subsets of a nontrivial abelian group G, satisfying $|A+B| \leq |A|+|B|-1$. Suppose that either $A+B \neq G$, or there is a group element with a unique representation as $a+b$ with $a \in A$ and $b \in B$. Then there exists a finite, proper subgroup $H < G$ such that*

(i) *$|C+H|-|C| \leq |H|-1$ with C substituted by any of the sets A, B, and $A+B$;*
(ii) *$(\varphi_H(A), \varphi_H(B))$ is an elementary pair in the quotient group $G/H = \varphi_H(G)$.*

5. The very-small-doubling property

We say that a finite set A in an abelian group is a very-small-doubling set (abbreviated below as VSDS) if $|2A| < \frac{3}{2}|A|$. Thus, for instance, any coset, and in particular

any singleton, is a VSDS, while a two-element set is a VSDS if and only if it is a coset.

The following two lemmas are easy corollaries from Kneser's theorem. Their (much subtler) noncommutative versions are due to Freiman [F73] and Olson [O84, Theorem 1], respectively.

Lemma 5.1. *A finite set A in an abelian group is a VSDS if and only if there is a subgroup H such that A is contained in an H-coset and $|A| > \frac{2}{3}|H|$. Moreover, in this case $A - A = H$, and $2A$ is an H-coset.*

Lemma 5.2. *If A and B are finite subsets of an abelian group, then either $|A + B| \geq |A| + \frac{1}{2}|B|$, or B is contained in a coset of the period $H := \pi(A + B)$.*

Corollary 5.3. *Suppose that A and B are finite subsets of an abelian group such that $|A + B| < |A| + \frac{1}{2}|B|$. Let $H := \pi(A + B)$. If $|A| \leq |B|$, then $|B| > \frac{2}{3}|H|$, as a result of which $B - B = H$, $2B$ is an H-coset, and B is a VSDS.*

Proof. By Lemma 5.2, B is contained in an H-coset. On the other hand,

$$|H| \leq |A + B| < |A| + \frac{1}{2}|B| \leq \frac{3}{2}|B|$$

and the rest follows from Lemma 5.1. □

Lemma 5.4. *Suppose that A and B are finite, nonempty subsets of an abelian group, and let $H := \pi(A + B)$. If $|A + B| < 2\min\{|B|, \frac{3}{4}|A|\}$, then $|A| > \frac{2}{3}|H|$ and $|B| > \frac{1}{2}|H|$; moreover, each of the sets A and B is contained in an H-coset and, indeed, $A + B$ is an H-coset.*

Although Lemma 5.4 is essentially contained, for instance, in [BP18, Propositions 2 and 3] and [DF03, Proposition 2.1], we present a complete proof.

Proof. Since $2\min\{|B|, \frac{3}{4}|A|\} \leq |B| + \frac{3}{4}|A| < |A| + |B|$, by Kneser's theorem,

$$|A + H| + |B + H| - |H| = |A + B| < 2|B| \tag{5.1}$$

and also

$$|A + H| + |B + H| - |H| = |A + B| < \frac{3}{2}|A|. \tag{5.2}$$

This readily gives $|B| > \frac{1}{2}|H|$ and $|A| > \frac{2}{3}|H|$.

Let $\alpha := |A + H|/|H|$ and $\beta := |B + H|/|H|$. From (5.1) we get $\alpha + \beta - 1 < 2\beta$; hence $\alpha < \beta + 1$ and therefore $\alpha \leq \beta$. Similarly, (5.2) gives $\alpha + \beta - 1 < \frac{3}{2}\alpha$, leading to $\beta \leq (\alpha + 1)/2$. Consequently, $\alpha \leq \beta \leq (\alpha + 1)/2$, whence $\alpha = \beta = 1$. This means

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

that each of A and B is contained in an H-coset, and then $A+B$ is an H-coset by the definition of H. $\square$

Corollary 5.5. *Suppose that A and B are finite, nonempty subsets of an abelian group. If A is not a VSDS, then $|A+B| \geq 2\min\{|B|, \frac{3}{4}|A|\}$.*

6. More lemmas

In this section we present a number of auxiliary results used in the proof of Theorem 1.3. Some of the results are classical or well-known, some are original.

Lemma 6.1. *Suppose that K is a subgroup, and that A and B are finite subsets of an abelian group such that A is contained in a single K-coset and $|A| \geq \frac{1}{2}|K|$.*

(i) *If $|B| > |K| - |A|$, then $|A+B| \geq |K|$.*
(ii) *If $|B| > 2(|K|-|A|)$, then either B is also contained in a single K-coset, or $|A+B| \geq |A|+|K|$.*

Proof. Write $B = B_1 \cup \cdots \cup B_k$ where $|B_1| \geq \cdots \geq |B_k| > 0$, the union is disjoint, and each B_i is contained in a single K-coset, with the cosets pairwise distinct.

(i) If $k=1$, then $|A+B| = |K|$ by the pigeonhole principle; if $k \geq 2$, then $|A+B| \geq k|A| \geq 2|A| \geq |K|$.

(ii) If $k=2$, then $|B_1| \geq \frac{1}{2}|B| > |K| - |A|$ whence $|A+B| = |A+B_1| + |A+B_2| \geq |K| + |A|$; if $k \geq 3$, then $|A+B| \geq 3|A| \geq |K| + |A|$. $\square$

Freiman's classical result known as "the $(3n-3)$-theorem" can be stated as follows.

Theorem 6.2 *(Freiman [F61]). Suppose that A is a finite, nonempty set of integers, and $l \geq 1$ is an integer. If A is not contained in an l-term arithmetic progression, then $|2A| \geq \min\{l, 2|A|-3\} + |A|$.*

For a modern exposition of Theorem 6.2 and related results see, for instance, [G13, Chapter 7], [N96, Theorem 1.13], or [TV06, Theorem 5.11].

We need yet another well-known result of Freiman.

Lemma 6.3 *(Freiman [F62b]). Suppose that Z is a finite subset of the unit circle in the complex plane. If*

$$\Big|\sum_{z\in Z} z\Big| = \eta|Z|, \quad \eta \in [0,1],$$

then there is an open arc of the circle of the angle measure π containing at least $\frac{1}{2}(1+\eta)|Z|$ elements of Z.

The following basic lemma shows that rectifiable sets cannot have a strong correlation with finite cosets.

Lemma 6.4. *If A is a rectifiable subset of an abelian group G, then for any finite subgroup $K \le G$ and any element $g \in G$ we have $|A \cap (g+K)| \le \frac{1}{2}(|K|+1)$.*

Proof. Let $A_0 := (A-g) \cap K$. If $|A_0| > \frac{1}{2}(|K|+1)$ then, by the pigeonhole principle, $2A_0 = K$ and moreover, any element of K has at least two representations as a sum of two elements of A_0. At the same time, for any finite integer set B with $|B| \ge 2$, there are at least two elements of $2B$ possessing a unique representation as a sum of two elements of B. Thus, A_0 is not rectifiable; hence, neither is A. □

Lemma 6.5. *Suppose that A and B are finite subsets of an abelian group G such that $|A+B| \le |A|+|B|-1$, $|A|+|B| \le |G|-1$, and $\min\{|A|,|B|\} \ge 2$. If B is rectifiable, not an arithmetic progression, and not contained in a proper coset, then there is a nonzero, finite, proper subgroup $H < G$ such that B meets exactly two H-cosets, and has exactly $\frac{|H|+1}{2}$ elements in each of them.*

Proof. In view of $|A+B| \le |A|+|B|-1 < |A|+|B| < |G|$, we can apply Theorem 4.3 to find a finite, proper subgroup $H < G$ such that $|B+H| \le |B|+|H|-1$ and $(\varphi_H(A), \varphi_H(B))$ is an elementary pair in the quotient group G/H. Denoting by k the number of H-cosets determined by B, we have $|B+H| = k|H|$ and then, by Lemma 6.4,

$$k|H| = |B+H| \le |B|+|H|-1 \le \frac{|H|+1}{2}\,k + |H| - 1,$$

which simplifies to

$$(k-2)(|H|-1) \le 0.$$

Thus, either $k \le 2$, or $H = \{0\}$. In the latter case (A,B) is an elementary pair in G; however, this option is ruled out by the assumptions of the lemma. We cannot have $k=1$ either as B is not contained in a proper coset. Thus, $k=2$, and then B meets two H-cosets and has exactly $\frac{|H|+1}{2}$ elements in each of them. □

Lemma 6.6. *Suppose that $\mathcal{A} = \{\alpha_1, \alpha_2, \alpha_3\}$ is a subset of an abelian group such that all sums $\alpha_i + \alpha_j$ with $1 \le i \le j \le 3$ are pairwise distinct (as a result of which $\alpha_1, \alpha_2, \alpha_3$ are pairwise distinct). If there are indices $i, j, k, l \in \{1,2,3\}$ and a group element $\beta \notin \mathcal{A}$ such that $\beta = \alpha_i + \alpha_j - \alpha_1 = \alpha_k + \alpha_l - \alpha_2$, then either $\mathcal{A}$ is contained in a four-term arithmetic progression, or $\{\alpha_1, \alpha_2, \beta\}$ is a coset of a 3-element subgroup.*

Proof. From $\alpha_i + \alpha_j - \alpha_1 \notin \mathcal{A}$ we get $i, j \in \{2,3\}$, and from $\alpha_k + \alpha_l - \alpha_2 \notin \mathcal{A}$ we get $k, l \in \{1,3\}$. If $\{i,j\}$ shares a common element with $\{k,l\}$, then assuming for definiteness that this element is $i = k$ we get $\alpha_j - \alpha_1 = \alpha_l - \alpha_2$ and consequently $\alpha_j + \alpha_2 = \alpha_l + \alpha_1$,

which is impossible in view of $j \neq 1$. Thus, $\{i, j\}$ is disjoint from $\{k, l\}$, and without loss of generality, we can assume that $k = l \notin \{i, j\}$.

If $i \neq j$, then $\{i, j\} = \{2, 3\}$, $k = l = 1$, and $\beta = \alpha_2 + \alpha_3 - \alpha_1 = 2\alpha_1 - \alpha_2$, implying $\alpha_3 + 2\alpha_2 = 3\alpha_1$. Thus, $\alpha_3 = \alpha_1 + 2(\alpha_1 - \alpha_2)$ and $\alpha_2 = \alpha_1 - (\alpha_1 - \alpha_2)$, showing that $\mathcal{A}$ is contained in a 4-term progression.

Finally, if $i = j$, then either $i = 3$ and $k = l = 1$, or $i = 2$ and $k = l = 3$, or $i = 2$ and $k = l = 1$. In the first case we have $2\alpha_3 - \alpha_1 = 2\alpha_1 - \alpha_2$ leading to $\alpha_2 + 2\alpha_3 = 3\alpha_1$, in the second case we similarly have $\alpha_1 + 2\alpha_3 = 3\alpha_2$; up to a renumbering, these cases were considered above. In the third case where $i = 2$ and $k = l = 1$, we get $3\alpha_1 = 3\alpha_2$ and $\beta = 2\alpha_2 - \alpha_1$; that is, $\delta := \alpha_2 - \alpha_1$ has order 3, and we have $\alpha_2 = \alpha_1 + \delta$ and $\beta = \alpha_1 + 2\delta$. $\square$

7. Partial results and the minimal counterexample

In this section, assuming that Theorem 1.3 is wrong, we study the properties of the minimal counterexample set.

Lemma 7.1. *Suppose that Theorem 1.3 is wrong. If $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible, then $|2A + L| - |2A| > |A + L| - |A|$ holds for any nonzero subgroup $L < \mathbb{Z}_n$ satisfying $2A + L \neq \mathbb{Z}_n$.*

Proof. Suppose that $A \subseteq \mathbb{Z}_n$ is not contained in a proper coset and satisfies $|2A| < \min\{\frac{9}{4}|A|, n\}$ (as a result of which $n \geq 3$), but none of the conclusions of the theorem hold true.

Suppose also, for a contradiction, that $L \leq \mathbb{Z}_n$ is a nonzero subgroup with $|2A + L| - |2A| \leq |A + L| - |A|$ and $2A + L \neq \mathbb{Z}_n$. Notice that the last condition implies that L is proper.

Write $\mathcal{A} := \varphi_L(A)$. If we had $|\mathcal{A}| = 1$, then A would be contained in a single L-coset; thus, $|\mathcal{A}| \geq 2$. On the other hand, $2A + L \neq \mathbb{Z}_n$ shows that $2\mathcal{A} \neq \mathbb{Z}_n/L$. We also have

$$|2A + L| \leq |A + L| + |2A| - |A| < |A + L| + \frac{5}{4}|A| \leq \frac{9}{4}|A + L|,$$

whence

$$|2\mathcal{A}| = \frac{|2A + L|}{|L|} < \frac{9}{4}\frac{|A + L|}{|L|} = \frac{9}{4}|\mathcal{A}|.$$

The minimality of n shows now that the set $\mathcal{A} \subseteq \mathbb{Z}_n/L$ is not a counterexample to Theorem 1.3. This means that there is a proper subgroup $\mathcal{H} < \mathbb{Z}_n/L$ such that one of the following holds:

(i) $|2\mathcal{A}| - |\mathcal{A}| > C_0^{-1}|\mathbb{Z}_n/L|$.

(ii) There is an arithmetic progression $\mathcal{P} \subseteq \mathbb{Z}_n/L$ of size $|\mathcal{P}| > 1$ with $\mathcal{A} \subseteq \mathcal{P} + \mathcal{H}$ and

$$(|\mathcal{P}| - 1)|\mathcal{H}| \leq |2\mathcal{A}| - |\mathcal{A}|.$$

(iii) $\mathcal{A}$ meets exactly three $\mathcal{H}$-cosets which are not in an arithmetic progression, and

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

Let $H := \varphi_L^{-1}(\mathcal{H}) \leq \mathbb{Z}_n$; notice that $\mathcal{H} \neq \mathbb{Z}_n/L$ implies $H \neq \mathbb{Z}_n$.

In the case (i), we have

$$|2A| - |A| \geq |2A + L| - |A + L| = (|2\mathcal{A}| - |\mathcal{A}|)|L| > C_0^{-1}n.$$

In the case (ii), we define $\widetilde{c}, \widetilde{d} \in \mathbb{Z}_n/L$ to be the initial term and the difference of $\mathcal{P}$. Choosing $c, d \in \mathbb{Z}_n$ with $\varphi_L(c) = \widetilde{c}$ and $\varphi_L(d) = \widetilde{d}$, and letting $P := \{c, c + d, \ldots, c + (|\mathcal{P}| - 1)d\}$, we get a progression $P \subseteq \mathbb{Z}_n$ with $|P| = |\mathcal{P}| > 1$ and $\varphi_L^{-1}(\mathcal{P}) = P + L$. From $\mathcal{A} \subseteq \mathcal{P} + \mathcal{H}$ we derive then that $A \subseteq P + H$, and from $(|\mathcal{P}| - 1)|\mathcal{H}| \leq |2\mathcal{A}| - |\mathcal{A}|$ we obtain

$$(|P| - 1)|H| = (|\mathcal{P}| - 1)|\mathcal{H}||L| \leq (|2\mathcal{A}| - |\mathcal{A}|)|L| = |2A + L| - |A + L| \leq |2A| - |A|.$$

Finally, in the case (iii) it is immediately seen that A is contained in a union of three H-cosets which are not in an arithmetic progression. Also,

$$3|H| = 3|\mathcal{H}||L| \leq (|2\mathcal{A}| - |\mathcal{A}|)|L| = |2A + L| - |A + L| \leq |2A| - |A|.$$

In any case, A has the structure described in the theorem; hence, is not a counterexample. □

Lemma 7.2. *Suppose that Theorem 1.3 is wrong. If $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible, then $2A$ is aperiodic.*

Proof. Let $L := \pi(2A)$. Observing that $2A + L = 2A \neq \mathbb{Z}_n$, we apply Lemma 7.1. The inequality of the lemma is clearly violated, showing that L is the zero subgroup. □

Lemma 7.3. *Suppose that Theorem 1.3 is wrong. If $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible, then $|A + L| \geq |A| + |L|$ holds for any nonzero, proper subgroup $L < \mathbb{Z}_n$.*

Proof. Since $A \subseteq \mathbb{Z}_n$ satisfies the assumptions of Theorem 1.3, it is not contained in a proper coset, and $2 \leq |2A| < \min\{\frac{9}{4}|A|, n\}$. Suppose for a contradiction that, in addition, we also have

$$|A + L| < |A| + |L| \tag{7.1}$$

with $L < \mathbb{Z}_n$ nonzero and proper. Since $|2A| < n$ implies $|A| \le \frac{1}{2}n$ by the pigeonhole principle, and since the properness of L implies $|L| \le \frac{1}{2}n$, as a consequence of (7.1) we have $|A+L| < n$. Thus, there is an L-coset disjoint from A, and since A is not contained in a proper coset, we conclude that, indeed, $|L| \le \frac{1}{3}n$. Reusing (7.1), we now get

$$|A+L| < \frac{5}{6}n. \tag{7.2}$$

Consider the coset decomposition

$$A = (a_0 + L_0) \cup (a_1 + L_1) \cup \cdots \cup (a_k + L_k),$$

where $L_0, L_1, \ldots, L_k \subseteq L$ are nonempty, $a_0, a_1, \ldots, a_k \in A$, and $a_i \not\equiv a_j \pmod{L}$ for all $i, j \in [0, k]$, $i \ne j$. Renumbering, we further assume that $0 < |L_0| \le |L_1| \le \cdots \le |L_k|$. From

$$(|L| - |L_0|) + (|L| - |L_1|) + \cdots + (|L| - |L_k|) = |A+L| - |A| < |L|$$

we derive that $|L_i| + |L_j| > |L|$, and therefore $(a_i + L_i) + (a_j + L_j) = a_i + a_j + L$ for all $i, j \in [0, k]$, with the only possible exception of $i = j = 0$. As a result,

$$|2A+L| - |2A| = |L| - |2L_0| \le |L| - |L_0| \le |A+L| - |A|, \tag{7.3}$$

and applying Lemma 7.1, we conclude that $2A + L = \mathbb{Z}_n$. Substituting this equality back to (7.3) and using (7.2), we obtain

$$|2A| - |A| \ge n - |A+L| > \frac{1}{6}n.$$

Therefore A satisfies the condition of Theorem 1.3 (i), a contradiction. □

Lemma 7.4. *Suppose that Theorem 1.3 is wrong. If $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible, then for any subset $B \subseteq \mathbb{Z}_n$ with $|A| \ge |B| \ge 2$ we have $|A+B| \ge |A| + |B|$.*

Proof. Suppose that $|A| \ge |B| \ge 2$ and $|A+B| < |A| + |B|$. Observing that these assumptions along with $|A| \le \frac{1}{2}n$ (following from $2A \ne \mathbb{Z}_n$) give $|A+B| < n$, we apply Theorem 4.3 to conclude that there is a finite, proper subgroup $L < \mathbb{Z}_n$ such that $|A+L| \le |A| + |L| - 1$ and $(\varphi_L(A), \varphi_L(B))$ is an elementary pair in the quotient group $\mathbb{Z}_n/L$. By Lemma 7.3, we have $L = \{0\}$; thus, (A, B) is an elementary pair in the original group $\mathbb{Z}_n$. Inspecting the list of elementary pairs from Section 4, we see that (A, B) is neither type (i) nor type (ii). (If A were an arithmetic progression, it would be regular.) Thus, (A, B) is elementary of type (iii) or (iv). In each of these cases, there is a subgroup $H \le \mathbb{Z}_n$ such that each of A and B is contained in an H-coset, and $|A| + |B| \ge |H|$. Since A is not contained in a proper coset, we actually have $H = \mathbb{Z}_n$,

and then $2|A| \geq |A| + |B| \geq n$ whence $|A| \geq \frac{1}{2}\,n$. Combined with the observation at the beginning of the proof, this gives $|A| = \frac{1}{2}\,n$.

On the other hand, since $2A$ is aperiodic (Lemma 7.2), by Kneser's theorem we have $|2A| \geq 2|A|-1$. Therefore $|2A|-|A| \geq |A|-1 = \frac{1}{2}\,n-1 \geq C_0^{-1}n$, the last estimate following from $n = 2|A| \geq 4$. This shows that A satisfies the inequality of Theorem 1.3 (i). □

Lemma 7.5. *Suppose that Theorem 1.3 is wrong. If $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible, then for any pair of nonempty subsets $A', A'' \subseteq A$ with $A' \cup A'' = A$, we have $|A' + A''| \geq |A'| + |A''| - 1$.*

Proof. Assuming $|A'+A''| < |A'|+|A''|-1$, let $L := \pi(A'+A'')$. Notice that L is nonzero by Kneser's theorem, and that L is proper as otherwise we would have $2A \supseteq A'+A'' = \mathbb{Z}_n$ contradicting the assumptions of Theorem 1.3.

Let $g_1, \ldots, g_k$ be representatives of the L-cosets determined by A. We have

$$\begin{aligned}
|A+L| - |A| &= \sum_{i=1}^{k} (|L| - |(g_i+L) \cap A|) \\
&\leq \sum_{\substack{1\leq i\leq k \\ (g_i+L)\cap A' \neq \varnothing}} (|L| - |(g_i+L) \cap A|) + \sum_{\substack{1\leq i\leq k \\ (g_i+L)\cap A'' \neq \varnothing}} (|L| - |(g_i+L) \cap A|) \\
&\leq \sum_{\substack{1\leq i\leq k \\ (g_i+L)\cap A' \neq \varnothing}} (|L| - |(g_i+L) \cap A'|) + \sum_{\substack{1\leq i\leq k \\ (g_i+L)\cap A'' \neq \varnothing}} (|L| - |(g_i+L) \cap A''|) \\
&= (|A'+L| - |A'|) + (|A''+L| - |A''|).
\end{aligned}$$

By Kneser's theorem and the assumption $|A'+A''| < |A'|+|A''|-1$, the right-hand side is

$$|A'+A''| + |L| - |A'| - |A''| < |L|.$$

Thus, $|A+L| - |A| < |L|$, contradicting Lemma 7.3. □

Lemma 7.6. *Suppose that Theorem 1.3 is wrong. If $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible, then $4 \leq |A| \leq C_0^{-1}n$ and $8 \leq |2A| \leq 2C_0^{-1}n$.*

Proof. Applying Lemma 7.4 with $B = A$ we get $|2A| \geq 2|A|$, resulting in

$$2 \leq |A| \leq |2A| - |A| \leq C_0^{-1}n$$

and, consequently, in

$$|2A| \leq |A| + C_0^{-1}n \leq 2C_0^{-1}n.$$

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

It remains to show that $|A| \geq 4$ and, therefore, $|2A| \geq 8$.

We thus have to treat the cases where $|A| = 2$ and $|A| = 3$. If $|A| = 2$, then $|2A| \leq 3$, contradicting Lemma 7.4 (applied with $B = A$). If $|A| = 3$, then $|2A| \geq 6$ by Lemma 7.4 and therefore A is not an arithmetic progression. Moreover, taking $H = \{0\}$ we have $3|H| \leq |2A| - |A|$; thus, A is singular, a contradiction. □

A well-known inequality (sometimes called *the first Ruzsa triangle inequality*, see [N96, Lemma 7.4] or [TV06, Lemma 2.6]) asserts that if A is a finite subset of an abelian group, then $|A - A||A| \leq |2A|^2$. We need the following slight refinement of this inequality.

Lemma 7.7. *If A is a finite subset of an abelian group, then*

$$|A - A||A| \leq |2A|^2 - |2A| + |A|.$$

Proof. For a group element d, let $r(d)$ denote the number of representations $d = s_1 - s_2$ with $s_1, s_2 \in 2A$. The key observation is that every representation $d = a_1 - a_2$ with $a_1, a_2 \in A$ gives rise to $|A|$ representations $d = (a_1 + a) - (a_2 + a)$ with $a \in A$ and, thus, with $a_1 + a, a_2 + a \in 2A$. Consequently, if $d \in A - A$, then $r(d) \geq |A|$; from this inequality, and considering the contributions of the summands corresponding to $d = 0$,

$$\begin{aligned} |2A|^2 &= \sum_{d \in 2A - 2A} r(d) = \sum_{\substack{d \in 2A - 2A \\ d \neq 0}} r(d) + |2A| \\ &\geq \sum_{\substack{d \in A - A \\ d \neq 0}} |A| + |2A| = (|A - A| - 1)|A| + |2A|. \quad \square \end{aligned}$$

The last lemma of this section is a technical but important fragment of the proof of Lemma 10.1 in Section 10. We present it separately to avoid overloading the argument in Section 10 with technical details.

Lemma 7.8. *Suppose that Theorem 1.3 is wrong, and that $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible. Denote by N the number of elements $d \in A - A$ possessing a unique representation as $d = a' - a''$ with $a', a'' \in A$. Then, letting $\tau := |2A|/|A|$, we have*

$$\frac{1}{\tau} + \frac{1}{\tau^2} + \frac{\tau - 2}{\tau |A|} - \frac{N}{\tau |A|^3} > \frac{52}{81}. \tag{7.4}$$

We remark that the constant $\frac{52}{81}$ is the value of the sum $1/\tau + 1/\tau^2$ at $\tau = 9/4$; therefore, the assertion would follow immediately if we could show that $N < (\tau - 2)|A|^2$. Unfortunately, this inequality does not hold in general.

Proof of Lemma 7.8. Consider the graph Γ with A as a vertex set, where the vertices $a, b \in A$ are adjacent if and only if $a - b$ has a unique representation as a difference of two

elements of A. Notice that the edges of Γ are in a one-to-two correspondence with the uniquely representable elements; therefore N is even and the number of edges is $N/2$. By $r(d)$ we denote the number of representations of an element $d \in A - A$ as $d = a' - a''$ with $a', a'' \in A$.

Let $\mathcal{P}$ be the set of all directed paths in Γ of length 2; that is, the set of all ordered triples $(a, b, c) \in A \times A \times A$ with b adjacent to both a and c and $a \neq c$. We have

$$|2A| \geq |(A + a) \cup (A + b) \cup (A + c)| \geq 3|A| - 2 - r(a - c),$$

whence $r(a - c) \geq (3 - \tau)|A| - 2$; in other words, denoting by M the set of all nonzero elements with at least $m := (3 - \tau)|A| - 2$ representations in $A - A$, we have $a - c \in M$. Notice that $|A| \geq 4$ by Lemma 7.6; along with the assumption $|2A| < \frac{9}{4}|A|$ this gives $m = 3|A| - |2A| - 2 > \frac{3}{4}|A| - 2 \geq 1$ as a result of which $m \geq 2$.

With every path $(a, b, c) \in \mathcal{P}$ we associate the set of all ordered pairs $(x, y) \in A \times A$ with $x - y = a - c$; thus, there are at least m pairs associated with every path. This totals to at least Km pairs, where K is the number of paths. Notice that pairs corresponding to different paths can coincide, but for every fixed element $d \in M$, there are at most $|A|$ pairs (x, y) with $x - y = d$. Therefore, $|M| \geq Km/|A|$. Since, by the well-known "cherry-counting argument",

$$K = 2\sum_{a \in A} \binom{\deg(a)}{2} = \sum_{a \in A} \deg(a)(\deg(a) - 1)$$
$$\geq \frac{1}{|A|}\left(\sum_{a \in A} \deg(a)\right)^2 - \sum_{a \in A} \deg(a) = \frac{N^2}{|A|} - N,$$

we have

$$|M| \geq \left(\frac{N^2}{|A|^2} - \frac{N}{|A|}\right) m.$$

In view of $m \geq 2$, we thus have at least $\left(\frac{N^2}{|A|^2} - \frac{N}{|A|}\right) m + 1$ nonuniquely representable elements (including 0), along with N uniquely representable elements. This leads to $|A - A| \geq \left(\frac{N^2}{|A|^2} - \frac{N}{|A|}\right) m + 1 + N$ and then, by Lemma 7.7

$$|2A|^2 - |2A| + |A| \geq |A - A||A| \geq \left(\frac{N^2}{|A|} - N\right)((3 - \tau)|A| - 2) + N|A| + |A|,$$
$$\tau^2 |A|^2 - \tau|A| - \left(3 - \tau - \frac{2}{|A|}\right) N^2 - ((\tau - 2)|A| + 2)N \geq 0. \tag{7.5}$$

By Lemma 7.4 and the assumptions, we have $2 \leq \tau < \frac{9}{4}$. In this range the left-hand side is an increasing function of τ for any fixed $|A|$ and N, and a decreasing function of N for any fixed $|A|$ and τ. Moreover, substituting $\tau = \frac{9}{4}$ and $N = 3|A|$ into the left-hand

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

side of (7.5) we get the value $\frac{39}{16}|A|(4-|A|) \le 0$. It follows that $N < 3|A|$. This means that it suffices to prove (7.4) with N replaced by $3|A|$.

Accordingly, we let

$$f(a,t) := \frac{1}{t} + \frac{1}{t^2} + \frac{t-2}{ta} - \frac{3a}{ta^3},$$

aiming to show that $f(|A|,\tau) > \frac{52}{81}$ whenever $2 \le \tau < \frac{9}{4}$ and $|A| \ge 4$. Indeed, observing that $f(a,t)$ is a decreasing function of t in the range $2 \le t < \frac{9}{4}$, $a \ge 4$, we obtain

$$f(|A|,\tau) > f\Big(|A|, \frac{9}{4}\Big) = \frac{52}{81} + \frac{1}{9|A|} - \frac{4}{3|A|^2} \ge \frac{52}{81}, \quad |A| \ge 12.$$

To treat the remaining cases where $4 \le |A| \le 11$, we use the fact that the actual value of the doubling coefficient $\tau = |2A|/|A|$ can be noticeably smaller than $9/4$. Specifically, a brute force computation shows that for all pairs (a,s) of integers satisfying $4 \le a \le 11$ and $a \le s < \frac{9}{4}a$ we have $f(a,t) > \frac{52}{81}$, where $t := s/a$, the only exception being the pair $(a,s) = (5,11)$. In this last case we essentially repeat the argument above with $|A| = 5$, $|2A| = 11$, and $\tau = 11/5$ taking special care to avoid loss of accuracy. Namely, substituting $|A| = 5$ and $\tau = 11/5$ into the left-hand side of (7.4), we see that it suffices to show that $N \le 10$. Since N is even, assume for a contradiction that $N \ge 12$; consequently,

$$m = 3|A| - |2A| - 2 = 2$$

and

$$K \ge \frac{N^2}{|A|} - N \ge \frac{144}{5} - 12 = \frac{84}{5}$$

whence, in fact, $K \ge 17$. Furthermore, since A is aperiodic by Lemma 7.2, for any nonzero element $d \in A - A$ we have $r(d) \le |A| - 1 = 4$; hence,

$$|M| \ge \frac{Km}{|A|-1} = \frac{1}{2}K \ge \frac{17}{2};$$

thus, $|M| \ge 9$. Finally, $|A - A| \ge |M| + 1 + N \ge 22$, which is impossible in view of $|A - A| \le |A|(|A|-1) + 1 = 21$. $\square$

8. The case where A meets at most two cosets

The goal of this section is to prove the following result.

Lemma 8.1. *Suppose that Theorem 1.3 is wrong, and that $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible. Then A meets at least three cosets of any subgroup $F < \mathbb{Z}_n$ of index $|\mathbb{Z}_n/F| \ge 3$.*

Proof. Suppose for a contradiction that A meets at most two F-cosets. Since A is not contained in a proper coset, this means that, in fact, A meets *exactly* two F-cosets; say, $A = A_1 \cup A_2$ with $A_i \subseteq g_i + F$ $(i \in \{1, 2\})$ and $g_1 \not\equiv g_2 \pmod F$. Notice that $\varphi_F(g_2 - g_1)$ generates $\mathbb{Z}_n/F$ as otherwise A would be contained in a proper coset; consequently, $2A$ meets exactly three F-cosets and

$$|2A| = |2A_1| + |A_1 + A_2| + |2A_2| = |A + A_2| + |2A_1| = |A + A_1| + |2A_2|;$$

moreover, $2A_1$, $A_1 + A_2$, and $2A_2$ reside in pairwise distinct F-cosets.

Without loss of generality, we assume $|A_1| \geq |A_2|$.

Claim 8.1. *A_1 is a VSDS.*

Proof. Suppose first that $|A_2| \geq 2$. In this case $|A + A_2| \geq |A| + |A_2|$ by Lemma 7.4, and we conclude that

$$|2A_1| = |2A| - |A + A_2| \leq |2A| - |A| - |A_2| = |2A| - 2|A| + |A_1|.$$

Consequently,

$$|2A_1| < \frac{1}{4}|A| + |A_1| \leq \frac{3}{2}|A_1|.$$

Now suppose that $|A_2| = 1$ and, for a contradiction, that $|2A_1| \geq \frac{3}{2}|A_1|$. We have in this case $|A_1| \geq 3$ by Lemma 7.6, and also

$$\frac{9}{4}|A| > |2A| = |A + A_2| + |2A_1| = |A| + |2A_1| \tag{8.1}$$

implying

$$\frac{3}{2}|A_1| \leq |2A_1| < \frac{5}{4}|A| = \frac{5}{4}|A_1| + \frac{5}{4}. \tag{8.2}$$

As a result, $|A_1| \leq 4$. In fact, we cannot have $|A_1| = 3$ as $|2A_1| \geq \frac{3}{2}|A_1|$ would then imply $|2A_1| \geq 5$, whence $\frac{5}{4}|A| > |2A_1| \geq 5$ leading to $|A| \geq 5 > |A_1| + |A_2|$.

Thus, $|A_1| = 4$ and then $|2A_1| = 6 = 2|A_1| - 2$ by (8.2). Let $H := \pi(2A_1)$, and $k := |A_1 + H|/|H|$. By Kneser's theorem, H is nonzero and $6 = |2A_1| = (2k - 1)|H|$. It follows that either $k = 1$ and $|H| = 6$, or $k = 2$ and $|H| = 2$. In the former case A is contained in a union of two H-cosets and, by (8.1),

$$|2A| - |A| = |2A_1| = 6 = |H|;$$

therefore, A is 2-regular. In the latter case A_1 is a union of two H-cosets; therefore A is contained in a union of three H-cosets and, by (8.1),

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

$$|2A| - |A| = |2A_1| = 6 = 3|H|,$$

showing that A is either 3-regular, or singular. $\square$

We therefore have $|2A_1| < \frac{3}{2}|A_1|$; consequently, by Lemma 5.1, the set A_1 is contained in a coset of a subgroup $L < \mathbb{Z}_n$ with $|A_1| > \frac{2}{3}|L|$ and $L = A_1 - A_1$. Since A_1 is contained in an F-coset, we have $L \le F$; consequently, $A_1 + L$ is disjoint from $A_2 + L$ and moreover, the L-cosets determined by $2A_1$, $A_1 + A_2$, and $2A_2$ are distinct from each other.

Write $A_2 = B_1 \cup \cdots \cup B_k$ where the sets B_i are nonempty, each of them is contained in an L-coset, and the k cosets are pairwise distinct. Since $|A_1 + A_2| = |A_1 + B_1| + \cdots + |A_1 + B_k| \ge k|A_1|$, we have

$$\frac{9}{4}\,|A| > |2A| = |2A_1| + |A_1 + A_2| + |2A_2| \ge (k+1)|A_1| + |A_2| \ge \Big(\frac{1}{2}k + 1\Big)|A|,$$

whence $k \le 2$.

If $k = 1$ then $A = A_1 \cup B_1$. By Lemma 7.5,

$$|2A| = |2A_1| + |A_1 + B_1| + |2B_1| \ge |L| + (|A| - 1) + |B_1|,$$

implying $|2A| - |A| \ge |L|$; therefore A is 2-regular.

Thus, $k = 2$. Without loss of generality, we assume that $|B_1| \ge |B_2|$.

As remarked above, the L-cosets determined by the sets $2A_1$, $A_1 + A_2 = (A_1 + B_1) \cup (A_1 + B_2)$, and $2A_2 = 2B_1 \cup (B_1 + B_2) \cup 2B_2$ are pairwise distinct. It is also immediately seen that the coset of $A_1 + B_1$ is distinct from that of $A_1 + B_2$, and that the coset of $B_1 + B_2$ is distinct from both the coset of $2B_1$ and that of $2B_2$. Consequently, in the decomposition

$$2A = 2A_1 \cup (A_1 + B_1) \cup (A_1 + B_2) \cup 2B_1 \cup (B_1 + B_2) \cup 2B_2 \tag{8.3}$$

all six sets in the right-hand side reside in pairwise distinct L-cosets, with the possible exception of the sets $2B_1$ and $2B_2$.

If at least one of A_1 and B_1 is not a coset of a subgroup of $\mathbb{Z}_n$, then $|2A_1| + |2B_1| \ge |A_1| + |B_1| + 1$; therefore, in view of the disjointness and by Lemma 7.5,

$$\begin{aligned}
|2A| &\ge |2A_1| + |2B_1| + |A_1 + B_1| + |B_2 + (A_1 \cup B_1)| \\
&\ge (|A_1| + |B_1| + 1) + |A_1| + (|A| - 1) \\
&\ge \frac{3}{2}\,|A_1| + \frac{1}{2}\,(|A_1| + |B_1| + |B_2|) + |A| \\
&= \frac{3}{2}\,|A_1| + \frac{3}{2}\,|A| \\
&\ge \frac{9}{4}|A|,
\end{aligned} \tag{8.4}$$

a contradiction.

Thus, both A_1 and B_1 are cosets. Moreover, recalling that A_1 is contained in an L-coset and $|A_1| \geq \frac{2}{3}|L|$, we conclude that A_1 is an L-coset. Let $K \leq L$ be the subgroup such that B_1 is a K-coset.

If $K \neq \{0\}$, then we notice that the first five sets in the right-hand side of (8.3) are K-periodic, and since $2A$ is aperiodic by Lemma 7.2, the set $2B_2$ is not contained in the union of these five sets. Therefore, as a slight modification of (8.4),

$$\begin{aligned}
|2A| &\geq |2A_1| + |2B_1| + |A_1 + B_1| + |B_2 + (A_1 \cup B_1)| + 1 \\
&\geq (|A_1| + |B_1|) + |A_1| + (|A| - 1) + 1 \\
&\geq \frac{3}{2}\,|A_1| + \frac{1}{2}\,(|A_1| + |B_1| + |B_2|) + |A| \\
&\geq \frac{9}{4}|A|,
\end{aligned}$$

a contradiction.

We conclude that A_1 is an L-coset and $|B_1| = 1$, as a result of which also $|B_2| = 1$.

If $2B_1 \neq 2B_2$ then $|2(B_1 \cup B_2)| = 3$ and in view of Lemma 7.6 we get

$$\begin{aligned}
|2A| &= |2A_1| + |A_1 + (B_1 \cup B_2)| + |2(B_1 \cup B_2)| \\
&= 3|L| + 3 \\
&= 3|A| - 3 \\
&\geq \frac{9}{4}|A|,
\end{aligned}$$

a contradiction.

Therefore $2B_1 = 2B_2$ and $|2A| = 3|L| + 2 = |A| + 2|L|$.

Write $B_1 = \{b_1\}$ and $B_2 = \{b_2\}$. Since B_1 and B_2 are in distinct L-cosets, we have $b_2 - b_1 \notin L$. However, $2B_1 = 2B_2$ shows that $b_2 - b_1$ is the unique involution of $\mathbb{Z}_n$. Therefore, L does not contain the involution, and we conclude that $|L| > 2$.

If $|L| = 3$ then A is a union of an L-coset and a coset of the two-element subgroup. As a result, A is contained in a union of two cosets of the six-element subgroup H lying above L, while $|2A| - |A| = 2|L| = |H|$; thus, A is 2-regular.

Finally, if $|L| \geq 4$, then $|2A| = 3|L| + 2 \geq \frac{9}{4}(|L| + 2) = \frac{9}{4}\,|A|$, a contradiction. □

9. The case where A meets exactly three cosets

In this section we prove the following result.

Lemma 9.1. *Suppose that Theorem 1.3 is wrong, and that $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible. If $L < \mathbb{Z}_n$ is a proper subgroup such that $\varphi_L(A)$ is rectifiable, then $|\varphi_L(A)| \geq 4$; that is, A meets at least four L-cosets.*

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

As mentioned in the Introduction, the proof is rather technical and some readers may prefer to skip it and proceed to the next section.

Proof. Aiming at a contradiction, we assume that $|\varphi_L(A)| \le 3$ and then, indeed, $|\varphi_L(A)| = 3$ by Lemma 8.1. Let $A = A_1 \cup A_2 \cup A_3$ be the L-coset decomposition of A. Since the set $\varphi_L(A) = \{\varphi_L(A_1), \varphi_L(A_2), \varphi_L(A_3)\}$ is rectifiable, it is either an arithmetic progression, or a *Sidon set* meaning that the sums $\varphi_L(A_i) + \varphi_L(A_j)$ with $1 \le i \le j \le 3$ are pairwise distinct. Accordingly, the sets

$$A_1 + A_2,\ A_2 + A_3,\ A_3 + A_1,\ 2A_1,\ 2A_2,\ 2A_3$$

sets determine six pairwise distinct L-cosets except that, after a suitable renumbering, the cosets determined by $2A_2$ and $A_1 + A_3$ may coincide.

Suppose first that all the six sets listed are pairwise disjoint. By Lemma 7.4, for each $i \in [1, 3]$ we have

$$|A| + |A_i| \le |A + A_i| = |A_1 + A_i| + |A_2 + A_i| + |A_3 + A_i|$$

except if $|A_i| = 1$ in which case the left-hand side must be replaced with $|A| + |A_i| - 1$. Since $|A| \ge 4$ in view of Lemma 7.6, there is at least one index i with $|A_i| > 1$. Therefore, taking the sum over all $i \in [1, 3]$ we obtain

$$4|A| - 2 \le 2|2A| - (|2A_1| + |2A_2| + |2A_3|) \le 2|2A| - |A|.$$

Thus $|2A| \ge \frac{5}{2}|A| - 1$ and, consequently, $\frac{9}{4}|A| > \frac{5}{2}|A| - 1$; as a result, $|A| < 4$, contradicting Lemma 7.6.

We therefore assume for the rest of the proof that $A_1 + A_3$ is *not* disjoint from $2A_2$; hence, $2A$ meets exactly five L-cosets. Notice that in this case, for any subgroup H such that each of A_1, A_2, and A_3 is contained in an H-coset, the three cosets are in an arithmetic progression.

We have

$$|2A| = |A_1 + A_2| + |A_2 + A_3| + |2A_1| + |2A_3| + |(A_1 + A_3) \cup (2A_2)|;$$

our goal is to show that either

$$|2A| \ge \frac{9}{4}|A|,$$

or there is a subgroup H such that each of A_1, A_2, A_3 is contained in an H-coset, and

$$|2A| \ge |A| + 2|H|$$

(in which case A is 3-regular). Once any of these estimates gets established, we have reached a contradiction and the proof is over. We thus assume that the estimates in question do not hold. We also make the following assumptions:

(i) $|A| \geq 4$ (by Lemma 7.6);
(ii) $|A + A_i| \geq |A| + |A_i| - 1$ for any $i \in \{1, 2, 3\}$; moreover, if $|A_i| > 1$, then the term -1 in the right-hand side can be dropped (by Lemma 7.4);
(iii) $|A_i + A_j| + |A_j + A_k| \geq |A| - 1$ for any permutation (i, j, k) of the index set $\{1, 2, 3\}$ (by Lemma 7.5 and in view of $(A_i + A_j) \cup (A_j + A_k) = A_j + (A_i \cup A_k)$).

These assumptions will be used throughout the proof without any further explanations or references.

Claim 9.1. *We have*

$$|2A_1| + |2A_2| + |2A_3| < \frac{5}{4}|A| + 1.$$

Consequently, at least one of A_1, A_2, and A_3 is a VSDS.

Proof. The first assertion follows from

$$\frac{9}{4}|A| > |2A| \geq (|A_1 + A_2| + |A_2 + A_3|) + (|2A_1| + |2A_2| + |2A_3|)$$
$$\geq |A| - 1 + (|2A_1| + |2A_2| + |2A_3|),$$

the second is an immediate corollary of the definition of a VSDS and Lemma 7.6. □

Claim 9.2. *Among the sets A_1, A_2, and A_3, at most one is a singleton; thus, $|A| \geq 5$.*

Proof. Suppose first that $|A_1| = |A_2| = 1$. Then $|A| = |A_3| + 2$ and if A_3 is not a coset, then

$$|2A| \geq |A_1 + A_3| + |A_2 + A_3| + |2A_3| + |2A_1| + |A_1 + A_2|$$
$$= 2|A_3| + |2A_3| + 2 \geq 3|A_3| + 3 = 3|A| - 3 \geq \frac{9}{4}|A|,$$

as wanted. If, on the other hand, A_3 is a coset, then arguing the same way we get $|2A| \geq 3|A| - 4$; that is, $|2A| - |A| \geq 2|A| - 4 = 2|A_3|$ showing that A is 3-regular.

Similarly, if $|A_1| = |A_3| = 1$, then $|A| = |A_2| + 2$ and either

$$|2A| \geq |A_1 + A_2| + |2A_2| + |A_2 + A_3| + |2A_1| + |2A_3|$$
$$= 2|A_2| + |2A_2| + 2 \geq 3|A_2| + 3 = 3|A| - 3 \geq \frac{9}{4}|A|,$$

or A_2 is a coset, $|2A| \geq 3|A|-4$, and then A is 3-regular in view of $|2A|-|A| \geq 2|A|-4 = 2|A_2|$. $\square$

Claim 9.3. *If A_2 is not a VSDS, then both A_1 and A_3 are VSDS.*

Proof. Recalling Claim 9.1, suppose for a contradiction that, say, A_3 is the only VSDS among A_1, A_2, A_3; thus, $|2A_1| \geq \frac{3}{2}|A_1|$ and $|2A_2| \geq \frac{3}{2}|A_2|$; furthermore, there is a subgroup H such that A_3 is contained in an H-coset and $|A_3| > \frac{2}{3}|H|$. As a result,

$$\begin{aligned}|2A| &\geq (|A_1+A_2|+|A_2+A_3|)+|2A_1|+|2A_2|+|2A_3| \\ &\geq |A|-1+\frac{3}{2}|A_1|+\frac{3}{2}|A_2|+|H| \\ &= \frac{5}{2}|A|-\frac{3}{2}|A_3|+|H|-1 \\ &\geq \frac{5}{2}|A|-\frac{1}{2}|H|-1. \end{aligned} \tag{9.1}$$

On the other hand, if A_2 is not contained in an H-coset, then $|A_2+A_3| \geq 2|A_3|$ resulting in

$$\begin{aligned}|2A| &\geq |A_1+A_2|+|A_2+A_3|+|2A_1|+|2A_2|+|2A_3| \\ &\geq \frac{1}{2}(|A_1|+|A_2|)+2|A_3|+\frac{3}{2}|A_1|+\frac{3}{2}|A_2|+|H| \\ &= 2|A|+|H|. \end{aligned} \tag{9.2}$$

From (9.1) and (9.2) we get

$$\begin{aligned}\left\lceil \frac{9}{4}|A| \right\rceil - 1 &\geq |2A| \\ &\geq \frac{2}{3}\left(\frac{5}{2}|A|-\frac{1}{2}|H|-1\right)+\frac{1}{3}(2|A|+|H|) \\ &= \frac{7}{3}|A|-\frac{2}{3}. \end{aligned}$$

However, the resulting inequality

$$\left\lceil \frac{9}{4}|A| \right\rceil - 1 \geq \frac{7}{3}|A|-\frac{2}{3}$$

is possible only for $|A| = 5$. Recalling that A_3 is a VSDS while A_1 and A_2 are not, we conclude that in this case $|A_1| = |A_2| = 2$ and $|A_3| = 1$. This further results in $|2A_1| = |2A_2| = 3$ and $|A_1+A_2| \geq 3$ (for the last estimate notice that $|A_1+A_2| = 2$ would mean that A_1 is contained in a coset of the period of A_2 and vice versa, and

then both A_1 and A_2 would be cosets of the two-element subgroup, and hence VSDS). Consequently,

$$|2A| \geq |A_1 + A_2| + |A_2 + A_3| + |2A_1| + |2A_2| + |2A_3| \geq 3 + 2 + 3 + 3 + 1 = 12 > \frac{9}{4}\,|A|,$$

a contradiction showing that A_2 is contained in an H-coset.

We now show that A_1 is contained in an H-coset, too. Assuming it is not, we have

$$|A_1 + A_2| \geq \max\{|A_1|, 2|A_2|\} \geq \frac{3}{8}\,|A_1| + \frac{5}{4}\,|A_2|$$

and, similarly,

$$|A_3 + A_1| \geq \max\{|A_1|, 2|A_3|\} \geq \frac{3}{8}\,|A_1| + \frac{5}{4}\,|A_3|.$$

Furthermore, $|2A_1| \geq \frac{3}{2}\,|A_1|$ (as we assume that A_1 is not a VSDS), and trivially, $|2A_3| \geq |A_3|$ and $|A_2 + A_3| \geq |A_2|$. Therefore,

$$\begin{aligned}\frac{9}{4}\,|A| &> |A_1 + A_2| + |A_3 + A_1| + |A_2 + A_3| + |2A_1| + |2A_3| \\ &\geq \left(\frac{3}{4}\,|A_1| + \frac{5}{4}\,|A_2| + \frac{5}{4}\,|A_3|\right) + |A_2| + \frac{3}{2}\,|A_1| + |A_3| \\ &= \frac{9}{4}\,(|A_1| + |A_2| + |A_3|),\end{aligned}$$

a contradiction.

We have thus shown that each of A_1, A_2, and A_3 is contained in an H-coset. Furthermore, $|A_2| \leq \frac{2}{3}|H| < |A_3|$; hence, by Lemma 5.2, either $|A_2 + A_3| \geq |A_2| + \frac{1}{2}|A_3|$, or A_3 is contained in a coset of the period $\pi(A_2 + A_3)$. In the latter case we have $H = A_3 - A_3 \subseteq \pi(A_2 + A_3)$; since, on the other hand, $A_2 + A_3$ is contained in an H-coset, we actually have $|A_2 + A_3| = |H|$. Therefore,

$$\begin{aligned}|2A| &\geq (|A_1 + A_2| + |A_3 + A_1|) + |A_2 + A_3| + |2A_1| + |2A_3| \\ &\geq (|A| - 1) + 2|H| + |2A_1| \\ &\geq |A| + 2|H|\end{aligned}$$

so that A is 3-regular.

Assuming thus that $|A_2 + A_3| \geq |A_2| + \frac{1}{2}|A_3|$, in view of

$$|2A_3| = |H| \geq \max\left\{|A_3|, \frac{3}{2}\,|A_2|\right\} \geq \frac{3}{4}\,|A_3| + \frac{3}{8}\,|A_2| \tag{9.3}$$

we get

$$\begin{aligned}|2A| &\geq (|A_1+A_2|+|A_3+A_1|)+|A_2+A_3|+|2A_1|+|2A_3| \\ &\geq |A|-1+\Big(|A_2|+\frac{1}{2}|A_3|\Big)+\frac{3}{2}|A_1|+\Big(\frac{3}{4}|A_3|+\frac{3}{8}|A_2|\Big) \\ &= \frac{9}{4}|A|-1+\frac{1}{4}|A_1|+\frac{1}{8}|A_2|.\end{aligned}$$

Since neither of A_1 and A_2 are VSDS, we have $|A_1|, |A_2| \geq 2$. Therefore

$$\frac{1}{4}|A_1|+\frac{1}{8}|A_2| > \frac{3}{4}$$

leading to a contradiction, with the only exception of the case where $|A_1| = |A_2| = 2$ and, moreover, (9.3) holds with equalities. In this exceptional case we have $|H| = \frac{3}{2}|A_2| = 3$, so that A_1 and A_2 are two-element subsets of the three-element subgroup H. Hence, by the pigeonhole principle, all sums $A_i + A_j$ with $i, j \in [1, 3]$ are H-cosets; therefore $2A$ is periodic, contradicting Lemma 7.2. □

We now consider two cases, according to whether A_2 is or is not a VSDS.

Case 1: A_2 is a VSDS.

Suppose that A_2 is a VSDS, and let $H := A_2 - A_2$.

Claim 9.4. *We have* $|A_1 + H| + |A_3 + H| \geq 3|H|$.

Proof. Suppose for a contradiction that each of A_1 and A_3 is contained in a single H-coset. Since $|2A_2| = |H|$, using the trivial estimates $|2A_i| \geq |A_i|$ and $|A_2 + A_i| \geq |A_2|$, where $i \in \{1, 3\}$, we get

$$\frac{9}{4}|A| > |2A| = |2A_1|+|2A_3|+|A_1+A_2|+|A_2+A_3|+|2A_2| \geq |A|+|A_2|+|H| \quad (9.4)$$

and we conclude that

$$\frac{5}{4}|A| > |A_2|+|H|. \quad (9.5)$$

If $|A_1| + |A_2| \leq |H|$ and $|A_3| + |A_2| \leq |H|$, then taking the sum we get

$$2|H| \geq |A|+|A_2|. \quad (9.6)$$

Combining (9.5) and (9.6),

$$|A_2| < \frac{5}{4}|A|-|H| \leq \frac{3}{2}|H|-\frac{5}{4}|A_2|$$

whence $|A_2| < \frac{2}{3}|H|$, a contradiction showing that either $|A_1| + |A_2| > |H|$, or $|A_3| + |A_2| > |H|$ holds true. Assuming the latter for definiteness, by the pigeonhole principle

we have $|A_2 + A_3| = |H|$, and then from (9.4) we obtain $|2A| \geq |A| + 2|H|$; hence, A is 3-regular. $\square$

Claim 9.5. *We have* $|A_2| < \frac{1}{4}|A|$.

Proof. Assuming that, say, A_1 meets at least two H-cosets (cf. Claim 9.4), we have $|A_1 + A_2| \geq 2|A_2|$ and then

$$\frac{9}{4}|A| > |2A| \geq |A_3 + A| + |2A_1| + |A_1 + A_2|$$
$$\geq (|A| + |A_3| - 1) + |A_1| + 2|A_2| = 2|A| + |A_2| - 1.$$

To complete the proof, we show that the term -1 in the right-hand side can be dropped. It is easy to see that otherwise the following conditions are meat simultaneously: $|A_3| = 1$, there is a subgroup K such that A_1 is a K-coset, $|A_1 + A_2| = 2|A_2|$, and $2A_2 \subseteq A_1 + A_3$. The first and the last conditions show that A_1 contains an H-coset; hence, $K \geq H$. Therefore $A_1 + A_2$ is a K-coset, and the condition $|A_1 + A_2| = 2|A_2|$ shows that $|K| = 2|H|$ and that A_2 is an H-coset. It follows that $|A| = |K| + |H| + 1$, $|A_2| = |H|$, and

$$|2A| = |A_3 + A| + |A_2 + A_1| + |2A_1| = |A| + 2|K|;$$

therefore A is 3-regular. $\square$

To complete the treatment of the present case where A_2 is a VSDS, we prove the following claim which is in clear contradiction with the previous one.

Claim 9.6. *We have* $|A_2| \geq \frac{1}{4}|A|$.

Proof. Let $\delta := |2A_2 \setminus (A_1 + A_3)|$ and

$$\delta_i := \begin{cases} |2A_i| - |A_i| & \text{if } |A_i| > 1 \\ -1 & \text{if } |A_i| = 1 \end{cases}, \qquad i \in \{1, 3\}.$$

The quantity δ_i shows whether A_i is a singleton ($\delta_i = -1$), a coset of a nonzero subgroup ($\delta_i = 0$), or neither ($\delta_i > 0$).

By Lemma 7.4, we have $|A + A_i| + |2A_i| \geq |A| + 2|A_i| + \delta_i$, $i \in \{1, 3\}$. Consequently, taking the sum of

$$|2A| \geq |A_1 + A| + |A_3 + A| - |A_1 + A_3| + \delta$$

and

$$|2A| \geq |A_2 + (A_1 \cup A_3)| + |A_3 + A_1| + |2A_1| + |2A_3| + \delta$$

we get

$$\begin{aligned}\frac{9}{2}|A| - \frac{1}{2} &\geq 2|2A| \\ &\geq (|A_1 + A| + |2A_1|) + (|A_3 + A| + |2A_3|) + |A_2 + (A_1 \cup A_3)| + 2\delta \\ &\geq 2|A| + 2|A_1| + 2|A_3| + (|A| - 1) + \delta_1 + \delta_3 + 2\delta \\ &= 5|A| - 2|A_2| + \delta_1 + \delta_3 + 2\delta - 1\end{aligned}$$

whence

$$|A_2| \geq \frac{1}{4}|A| + \frac{1}{2}(\delta_1 + \delta_3) + \delta - \frac{1}{4}.$$

Since $\delta_1+\delta_3 \geq -1$ by Claim 9.2, we assume for the rest of the proof that $\delta_1+\delta_3 \in \{-1, 0\}$, that $\delta = 0$ (that is, $2A_2 \subseteq A_1 + A_3$), and (switching A_1 and A_3, if needed) that $\delta_1 \leq \delta_3$; that is, either $\delta_1 = -1$ and $\delta_3 \in \{0, 1\}$, or $\delta_1 = \delta_3 = 0$. Moreover, by Claim 9.4, in each of these cases we can assume that A_3 meets at least two H-cosets. (If A_3 meets just one H-coset, then A_1 meets at least two; hence $\delta_1 \geq 0$, leading to $\delta_1 = \delta_3 = 0$, and we switch A_1 and A_3 without violating any of the assumptions.)

Suppose first that $\delta_1 = -1$ and $\delta_3 = 0$; thus, $|A_1| = 1$ and A_3 is a coset of a nonzero subgroup, say K. Since $2A_2 \subseteq A_1 + A_3$, and since $2A_2$ is an H-coset, while $A_1 + A_3$ is a K-coset, we have $H \leq K$. A simple counting shows now that $|A| = |A_2| + |K| + 1$ while $|2A| = 3|K| + |A_2| + 1$; therefore, $|2A| - |A| = 2|K|$ and A is 3-regular.

Next, we consider the case where $\delta_1 = -1$ and $\delta_3 = 1$; that is, A_1 is a singleton, and A_3 is not a coset. By Claim 9.2, we have $|H| \geq |A_2| \geq 2$. Furthermore, in view of $2A_2 \subseteq A_1 + A_3$, the set A_3 contains an H-coset; moreover, the containment is proper since A_3 meets at least two H-cosets. As a result,

$$|A_2 + A_3| \geq \max\{|A_2| + 1, |A_3|\} \geq \frac{1}{2}(|A_2| + 1 + |A_3|) = \frac{1}{2}|A|$$

and, consequently,

$$\frac{9}{4}|A| > |2A| = |A_1 + A| + |A_2 + A_3| + |2A_3| \geq |A| + \frac{1}{2}|A| + (|A_3| + 1) = \frac{5}{2}|A| - |A_2|$$

which gives the desired estimate $|A_2| \geq \frac{1}{4}|A|$.

Finally, we consider the case where $\delta_1 = \delta_3 = 0$; that is, A_1 is a coset of a nonzero subgroup H_1, and A_3 is a coset of a nonzero subgroup H_3. Since $2A$ is aperiodic, and $2A_2 \subseteq A_1 + A_3$, we have $H_1 \cap H_3 = \{0\}$. Furthermore, $|A| = |H_1| + |A_2| + |H_3|$ and

$$\begin{aligned}|2A| &= |2A_1| + |2A_3| + |A_1 + A_3| + |A_1 + A_2| + |A_2 + A_3| \\ &\geq |H_1| + |H_3| + |H_1||H_3| + |H_1| + |H_3| \\ &= (|H_1| - 2)(|H_3| - 2) + 4|H_1| + 4|H_3| - 4\end{aligned}$$

$$\geq 4|A| - 4|A_2| - 4.$$

If we had $|A_2| \leq \frac{1}{4}|A| - \frac{1}{4}$, this would further lead to

$$\frac{9}{4}|A| > |2A| \geq 3|A| - 3$$

contradicting Claim 9.2. □

Case 2: A_2 is not a VSDS.

Suppose that A_2 is not a VSDS. By Claim 9.3, in this case both A_1 and A_3 are VSDS. Assuming for definiteness that $|A_3| \geq |A_1|$, consider the subgroup $H := A_3 - A_3$.

Claim 9.7. *A_2 is contained in a single H-coset.*

Proof. Assuming the opposite, we have $|A_2 + A_3| \geq 2|A_3|$ and, by Corollary 5.5,

$$|A_1 + A_2| \geq \max\left\{|A_1|, |A_2|, \min\{2|A_1|, \frac{3}{2}|A_2|\}\right\}.$$

Consequently,

$$\begin{aligned}\frac{9}{4}|A| &> |2A| \\ &\geq |2A_1| + |2A_3| + |A_1 + A_2| + |A_2 + A_3| + |2A_2| \\ &\geq |A_1| + |A_3| + \max\{|A_1|, |A_2|, \min\{2|A_1|, \frac{3}{2}|A_2|\}\} + 2|A_3| + \frac{3}{2}|A_2|\end{aligned}$$

leading to

$$\max\{|A_1|, |A_2|, \min\{2|A_1|, \frac{3}{2}|A_2|\}\} < \frac{5}{4}|A_1| + \frac{3}{4}|A_2| - \frac{3}{4}|A_3| \leq \frac{1}{2}|A_1| + \frac{3}{4}|A_2|.$$

However, the resulting estimate is easily shown to be wrong by analyzing the four cases where $|A_1| \leq \frac{1}{2}|A_2|$, $\frac{1}{2}|A_2| \leq |A_1| \leq \frac{3}{4}|A_2|$, $\frac{3}{4}|A_2| \leq |A_1| \leq \frac{3}{2}|A_2|$, and $|A_1| \geq \frac{3}{2}|A_2|$. (Less rigorous, but more convincing is to let $t := |A_1|/|A_2|$, rewrite the inequality in question as $\max\{1, t, \min\{2t, \frac{3}{2}\}\} < \frac{1}{2}t + \frac{3}{4}$, and plot both sides as functions of t). □

Next, we show that the set A_1 is contained in a single H-coset, too.

Claim 9.8. *A_1 is contained in a single H-coset.*

Proof. Assuming the opposite, the sum $A_1 + A_3$ meets at least two H-cosets, and has at least $|A_3|$ elements in every H-coset that it meets. Consequently, $|(2A_2) \cup (A_1 + A_3)| \geq |2A_2| + |A_3| \geq \frac{3}{2}|A_2| + |A_3|$. Therefore

$$\begin{aligned}\frac{9}{4}|A| &> |2A| \\ &\geq (|A_1+A_2|+|A_2+A_3|)+|2A_1|+|2A_3|+|(2A_2)\cup(A_1+A_3)| \\ &\geq (|A|-1)+|A_1|+|A_3|+\left(\frac{3}{2}|A_2|+|A_3|\right) \\ &\geq \frac{5}{2}|A|-1\end{aligned}$$

contradicting Lemma 7.6. □

We have thus shown that each of A_1, A_2, and A_3 is contained in an H-coset. We also recall that, by our present assumptions, A_1 and A_3 are VSDS, while A_2 is not, and that $A_3 - A_3 = H$ and $|A_1| \leq |A_3|$; as a result, $|A_2| \leq \frac{2}{3}|H| < |A_3|$.

Case 2.1: $\max\{|A_1|, |A_2|\} \geq \frac{1}{2}|A_3|$. If $|A_2| \geq \frac{1}{2}|A_3|$, then in view of $|A_3| > \frac{2}{3}|H|$ we have $|A_2| + |A_3| > |H|$. Therefore $A_2 + A_3$ is an H-coset and

$$\begin{aligned}|2A| &\geq |A_1+A_2|+|A_2+A_3|+|A_3+A_1|+|2A_1|+|2A_3| \\ &\geq |A_2|+|H|+|A_3|+|A_1|+|H| \\ &= |A|+2|H|\end{aligned}$$

so that A is 3-regular.

Similarly, if $|A_1| \geq \frac{1}{2}|A_3|$, then $|A_1| + |A_3| > |H|$. Therefore $A_1 + A_3$ is an H-coset and then

$$\begin{aligned}|2A| &\geq (|A_1+A_2|+|A_2+A_3|)+|A_3+A_1|+|2A_1|+|2A_3| \\ &\geq (|A|-1)+|H|+1+|H| \\ &= |A|+2|H|\end{aligned}$$

shows that A is 3-regular.

Case 2.2: $\max\{|A_1|, |A_2|\} < \frac{1}{2}|A_3|$. We have

$$\begin{aligned}\frac{9}{4}|A|-\frac{1}{4} &\geq |2A| \\ &\geq (|A_1+A_2|+|A_2+A_3|)+|A_1+A_3|+|2A_1|+|2A_3| \\ &\geq (|A|-1)+|A_3|+|A_1|+|A_3| \\ &\geq |A_1|+\frac{5}{4}|A_3|+\frac{3}{4}\left(\frac{1}{3}|A_1|+\frac{5}{3}|A_2|+1\right)+|A|-1 \\ &= \frac{9}{4}|A|-\frac{1}{4}.\end{aligned}$$

This shows that $|2A_1| = |A_1|$ and $|2A_3| = |A_3|$; that is, both A_1 and A_3 are cosets. Since $A_3 - A_3 = H$ and A_1 is contained in an H-coset, we conclude that A_3 is an H-coset and that there is a subgroup $K \le H$ such that A_1 is a K-coset. In this case $|A| = |K| + |A_2| + |H|$ and from

$$|2A_1| = |K|,\ |A + A_3| = 3|H|,\ |A_2 + A_1| \ge |A_2|,$$

we get $|2A| \ge 3|H| + |K| + |A_2|$; hence, $|2A| - |A| \ge 2|H|$ and A is 3-regular. □

10. Character sums and partial rectification

This section combines a character-sum argument and combinatorial reasoning. Its central component is a lemma which, loosely speaking, shows that over 90% of a counterexample set must be well-structured. The lemma is a version of [DF03, Proposition 4.2] incorporating a critically important trick from [LS20]. Historically, quoting from [DF03], "the underlying idea comes from [F61] (...) where the case of prime modulus n was dealt with".

Recall that an arithmetic progression in a cyclic group is *primitive* if its difference generates the group.

Lemma 10.1. *Suppose that Theorem 1.3 is wrong. If $A \subseteq \mathbb{Z}_n$ is a counterexample with n smallest possible, then there exist a subgroup $H < \mathbb{Z}_n$ of index $m := n/|H| \ge 37$, and a primitive arithmetic progression $P \subseteq \mathbb{Z}_n$ with $|P| \le (m+1)/2$, such that $|(P+H) \cap A| > 0.9|A|$.*

Proof. We assume that $|2A| < \min\{\frac{9}{4}|A|, n\}$ (since A satisfies the assumptions of Theorem 1.3), that $|2A| - |A| \le C_0^{-1} n$ (since A fails to satisfy the conclusion of the theorem), and that $|A + B| \ge |A| + |B|$ holds for any subset $B \subseteq \mathbb{Z}_n$ with $2 \le |B| \le |A|$ (in view of Lemma 7.4); in particular, $\tau := |2A|/|A| \ge 2$. Also, $|2A| \ge 2|A| \ge 8$ and $n \ge C_0|A| \ge 4C_0$ by Lemma 7.6.

For a finite subset B and an element x of an abelian group, we let $B^{(x)} := B \cap (B+x)$; therefore, $|B^{(x)}|$ is the number of representations of x as a difference of two elements of B, and in particular $|B^{(x)}| = 0$ if $x \notin B - B$. We have

$$\sum_{x \in B-B} |B^{(x)}| = |B|^2$$

and

$$B^{(x)} + B \subseteq (2B)^{(x)}; \tag{10.1}$$

the latter relation, sometimes called the *Katz-Koester observation*, can be proved as follows:

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

$$B^{(x)} + B = (B \cap (B + x)) + B \subseteq (2B) \cap ((2B) + x) = (2B)^{(x)}.$$

We also have

$$\sum_{x \in B-B} |B^{(x)}|^2 = \mathsf{E}(B),$$

where $\mathsf{E}(B)$ (standardly called the *energy* of B) is the number of quadruples $(b_1, \dots, b_4) \in B^4$ with $b_1 + b_2 = b_3 + b_4$. We recall the basic estimate

$$\mathsf{E}(B) \geq \frac{|B|^4}{|2B|} \tag{10.2}$$

following easily from the Cauchy-Schwartz inequality.

Let $S := 2A$ and $\tau := |S|/|A|$. Denoting by $\widehat{A}$ the counting-measure Fourier transform of the indicator function of the set A, and similarly for the set S, we have

$$\frac{1}{n} \sum_{\chi \in \widehat{\mathbb{Z}_n}} |\widehat{A}(\chi)|^2 |\widehat{S}(\chi)|^2 = \sum_{x \in A-A} |A^{(x)}||S^{(x)}| \geq \sum_{x \in A-A} |A^{(x)}||A + A^{(x)}|; \tag{10.3}$$

here the equality follows, for instance, by a direct computation, both sums involved counting the number of solutions to $a_1 - a_2 = s_1 - s_2$ with $a_1, a_2 \in A$ and $s_1, s_2 \in S$, and the inequality follows from (10.1). Let D be the set of all those $x \in \mathbb{Z}_n$ with $|A^{(x)}| = 1$, and let $N := |D|$. By Lemma 7.4 we have $|A + A^{(x)}| \geq |A| + |A^{(x)}|$ unless $x \in D$. Consequently, denoting the sum in the left-hand side of (10.3) by σ,

$$\begin{aligned}
\sigma &\geq \sum_{x \in A-A} |A^{(x)}||A + A^{(x)}| \\
&\geq \sum_{\substack{x \in A-A \\ x \neq 0}} |A^{(x)}|(|A| + |A^{(x)}|) - \sum_{x \in D} |A^{(x)}|^2 + |A||S| \\
&= \sum_{x \in A-A} |A^{(x)}|(|A| + |A^{(x)}|) - N + |A||S| - 2|A|^2 \\
&= |A|^3 + \mathsf{E}(A) + (\tau - 2)|A|^2 - N
\end{aligned}$$

where the terms $|A||S|$ and $-2|A|^2$ arise from the summand corresponding to $x = 0$. In view of (10.2) and Lemma 7.8, we conclude that

$$\sigma \geq |A|^3 + \frac{|A|^3}{\tau} + (\tau - 2)|A|^2 - N > \frac{52}{81}\tau|A|^3. \tag{10.4}$$

We split the sum in the left-hand side into two parts,

$$\sigma_0 = \frac{1}{n} \sum_{\substack{\chi \in \widehat{\mathbb{Z}_n} \\ |\ker \chi| \geq n/36}} |\widehat{A}(\chi)|^2 |\widehat{S}(\chi)|^2$$

and

$$\sigma_1 = \frac{1}{n} \sum_{\substack{\chi \in \widehat{\mathbb{Z}_n} \\ |\ker \chi| < n/36}} |\widehat{A}(\chi)|^2 |\widehat{S}(\chi)|^2$$

(the bound $n/36$ is needed for the combinatorial part of the argument, presented in the next section, to go through). Let φ denote Euler's totient function. For any divisor $d \mid n$, there are exactly $\varphi(d)$ characters $\chi \in \widehat{\mathbb{Z}_n}$ with $|\ker \chi| = n/d$. Therefore

$$\sigma_0 \le \frac{1}{n} |A|^2 \sum_{\substack{\chi \in \widehat{\mathbb{Z}_n} \\ |\ker \chi| \ge n/36}} |\widehat{S}(\chi)|^2 \le \frac{1}{n} \Phi |A|^2 |S|^2 = \frac{1}{n} \Phi \tau^2 |A|^4, \tag{10.5}$$

where

$$\Phi = \sum_{\substack{1 \le d \le 36 \\ d \mid n}} \varphi(d) \le \sum_{d=1}^{36} \varphi(d) = 396.$$

Recalling that $(\tau - 1)|A| = |2A| - |A| \le C_0^{-1} n$, we therefore have

$$\sigma_0 \le \frac{396 \tau^2}{(\tau - 1) C_0} |A|^3. \tag{10.6}$$

Turning to the sum σ_1, we let

$$\eta := \max_{\substack{\chi \in \widehat{\mathbb{Z}_n} \\ |\ker \chi| < n/36}} |\widehat{A}(\chi)| / |A|$$

(thus, $\eta < 1$) and use the first inequality in (10.5) and Parseval's identity to get

$$\begin{aligned} \sigma_1 &\le \frac{1}{n} \eta^2 |A|^2 \sum_{\substack{\chi \in \widehat{\mathbb{Z}_n} \\ |\ker \chi| < n/36}} |\widehat{S}(\chi)|^2 \\ &= \frac{1}{n} \eta^2 |A|^2 \left(\sum_{\chi \in \widehat{\mathbb{Z}_n}} |\widehat{S}(\chi)|^2 - \sum_{\substack{\chi \in \widehat{\mathbb{Z}_n} \\ |\ker \chi| \ge n/36}} |\widehat{S}(\chi)|^2 \right) \\ &\le \eta^2 (|A|^2 |S| - \sigma_0). \end{aligned}$$

Therefore, by (10.6),

$$\begin{aligned}\sigma_0+\sigma_1 &\le \eta^2|A|^2|S|+(1-\eta^2)\sigma_0\\ &\le \left(\eta^2+(1-\eta^2)\cdot\frac{396\tau}{(\tau-1)C_0}\right)\tau|A|^3.\end{aligned}$$

Combining this estimate with (10.4) we obtain

$$\eta^2+(1-\eta^2)\cdot\frac{396\tau}{(\tau-1)C_0}>\frac{52}{81},$$

and since

$$\frac{396\tau}{(\tau-1)C_0}<\frac{2\cdot 396}{1.5\cdot 10^5}<0.0053$$

we conclude that

$$\eta^2+0.0053(1-\eta^2)>\frac{52}{81};$$

as a result, $\eta>0.8$.

Thus, there exists a character $\chi\in\widehat{\mathbb{Z}_n}$ such that $|\ker\chi|<n/36$ and

$$|\widehat{A}(\chi)|>0.8|A|.$$

Letting $H:=\ker\chi$ and $m:=n/|H|$ (so that $m\ge 37$, $H=m\mathbb{Z}_n$, and $\mathbb{Z}_n/H\cong\mathbb{Z}_m$), there is a zero-kernel character $\zeta\in\widehat{\mathbb{Z}_n/H}$ such that $\chi=\zeta\circ\varphi_H$, where $\varphi_H\colon\mathbb{Z}_n\to\mathbb{Z}_n/H$ is the canonical homomorphism. In terms of this character ζ, the last estimate can be rewritten as

$$\Big|\sum_{a\in A}\zeta(\varphi_H(a))\Big|>0.8|A|.$$

The summands in the left-hand side are complex roots of unity of degree m, and by Lemma 6.3, there exists a subset $A'\subseteq A$ of size $|A'|>\frac{1}{2}(1+0.8)|A|=0.9|A|$, and an open arc $\mathcal{C}$ of the unit circle, of angle measure π, such that $\zeta(\varphi_H(a))\in\mathcal{C}$ for all $a\in A'$. The arc $\mathcal{C}$ contains at most $\lfloor(m+1)/2\rfloor$ roots of unity of degree m, which are in a geometric progression. As a result, the set $\varphi_H(A')$ is contained in a primitive arithmetic progression $Q\subseteq\mathbb{Z}_n/H$ of size $|Q|\le(m+1)/2$; hence,

$$A'\subseteq\varphi_H^{-1}(Q). \tag{10.7}$$

Fix $c,d\in\mathbb{Z}_n$ such that $c+H$ and $d+H$ are the initial term and the difference of the progression Q, respectively, and d generates $\mathbb{Z}_n$; the latter condition is possible to satisfy since $d+H$ generates $\mathbb{Z}_n/H$. Letting $P:=\{c,c+d,\dots,c+(|Q|-1)d\}\subseteq\mathbb{Z}_n$, we have $\varphi_H(P)=Q$, whence $\varphi_H^{-1}(Q)=P+H$. This completes the proof in view of (10.7). □

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

11. Proof of Theorem 1.3

Suppose that the theorem is wrong. Let n be the smallest positive integer for which the assertion fails, and let $A \subseteq \mathbb{Z}_n$ be a counterexample set satisfying the assumptions, but not the conclusion of the theorem. As a result, A is not contained in a proper coset, $4 \le |A| \le C_0^{-1}n$ and $8 \le |2A| \le 2C_0^{-1}n$ by Lemma 7.6, and $2A$ is aperiodic by Lemma 7.2.

Applying Lemma 10.1, we find a subgroup $L < \mathbb{Z}_n$ of index $m := n/|L| \ge 37$, and a primitive arithmetic progression $Q_0 \subseteq \mathbb{Z}_n$ with $|Q_0| \le (m+1)/2$ such that the set $A' := (Q_0 + L) \cap A$ has size $|A'| > 0.9|A|$. The condition $|Q_0| \le (m+1)/2$ along with the primitivity of Q_0 ensures that $\varphi_L(Q_0)$ is rectifiable. Thus, $\varphi_L(A')$ is contained in a rectifiable subset of $\mathbb{Z}_n/L$; hence, is itself rectifiable. Let $A'' := A \setminus A'$. We observe that the L-cosets determined by A' are distinct from those determined by A'': $(A' + L) \cap (A'' + L) = \varnothing$. Also,

$$|2A'| \le |2A| < \frac{9}{4}\,|A| < \frac{5}{2}\,|A'|. \tag{11.1}$$

It suffices to prove that $\varphi_L(A)$ is rectifiable, as in this case $|\varphi_L(A)| \ge 4$ by Lemma 9.1, and applying Proposition 3.2 we conclude that A is *not* a counterexample.

Claim 11.1. *The set A'' is nonempty.*

Proof. If $A'' = \varnothing$, then $A = A'$; as a result, $\varphi_L(A) = \varphi_L(A')$ is rectifiable. □

In view of $|A''| < 0.1|A|$, as an immediate corollary of Claim 11.1 we have

$$|A''| < \frac{1}{9}\,|A'| \quad \text{and} \quad |A| \ge 11. \tag{11.2}$$

Claim 11.2. *The set A' is not contained in a proper coset.*

Proof. Suppose that A' is contained in a proper coset, and let $g + F$, with $g \in \mathbb{Z}_n$ and $F < \mathbb{Z}_n$, be the smallest coset containing A'. If $a_1, \dots, a_k$ list representatives of the F-cosets intersecting A'', other than the coset $g + F$ (which can possibly contain elements of A'') then $2A', a_1 + A', \dots, a_k + A'$ reside in pairwise distinct F-cosets and, therefore, are disjoint. As a result

$$(k+1)|A'| \le |2A'| + |a_1 + A'| + \cdots + |a_k + A'| \le |2A| < \frac{9}{4}\,|A| < \frac{5}{2}|A'|,$$

showing that $k \le 1$. Indeed, $k = 1$ as if we had $k = 0$, then A were contained in $g + F$, which is a proper coset.

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

Reversing the last computation,

$$\frac{5}{2}\,|A'| > \frac{9}{4}|A| > |2A| \geq |2A'| + |a_1 + A'|$$

whence $|2A'| < \frac{3}{2}|A'|$. Therefore A' is a VSDS; moreover, by Lemma 5.1 and the minimality of F, we have $A'-A' = F$, $|2A'| = |F|$, and $|A'| > \frac{2}{3}|F|$. Now from $|F| < \frac{3}{2}\,|A'| < \frac{3}{2}|A|$ and Lemma 7.6 we see that $|F| < \frac{1}{3}\,n$. On the other hand, $A \subseteq (g+F) \cup (a_1+F)$, contradicting Lemma 8.1. □

Recall that we have defined $m := n/|L|$.

Claim 11.3. *For any subgroup $K \leq L$, the set $\varphi_K(A')$ is not contained in an arithmetic progression with $\lceil \frac{m}{6} \rceil$ or fewer terms.*

Proof. If, for some $a, d \in \mathbb{Z}_n$ and $k \geq 1$ we have

$$\varphi_K(A') \subseteq \{\varphi_K(a) + i\varphi_K(d) \colon i \in [0, k-1]\},$$

then

$$\varphi_L(A') \subseteq \{\varphi_L(a) + i\varphi_L(d) \colon i \in [0, k-1]\}.$$

Therefore, it suffices to prove the assertion in the special case where $K = L$.

By Lemma 5.1 and Claim 11.2, the set A' is not a VSDS; hence

$$|2A'| \geq \frac{3}{2}|A'|. \tag{11.3}$$

If A contained an element $a \notin 2A' - A'$, then $a + A'$ would be disjoint from $2A'$, and from (11.3) we would get

$$|2A| \geq |a + A'| + |2A'| \geq \frac{5}{2}\,|A'| > \frac{9}{4}\,|A|,$$

contradicting the assumptions. Thus,

$$A \subseteq 2A' - A'. \tag{11.4}$$

Suppose now that $\varphi_L(A')$ is contained in an arithmetic progression with $k \leq \lceil \frac{m}{6} \rceil$ terms. Then, by (11.4), the set $\varphi_L(A)$ is contained in a progression with $3k - 2 \leq \frac{m+1}{2}$ terms. Since A is not contained in a proper coset, the difference of this progression generates $\mathbb{Z}_n/L$. It follows that $\varphi_L(A)$ is rectifiable. □

By Lemma 9.1, if $\varphi_L(A)$ is rectifiable, then $|\varphi_L(A)| \geq 4$. We now show that the conclusion $|\varphi_L(A)| \geq 4$ holds true regardless of the rectifiability of $\varphi_L(A)$.

Claim 11.4. *The set A determines at least four distinct L-cosets; that is, $|\varphi_L(A)| \geq 4$.*

Proof. With Lemma 8.1 in mind, suppose for a contradiction that A determines exactly three L-cosets. By Claims 11.1 and 11.2, the set A' meets exactly two of these three cosets. Hence, $|\varphi_L(A')| = 2$; therefore, $\varphi_L(A')$ is a (two-term) progression, contradicting Claim 11.3. □

Write $s := |\varphi_L(A')|$, and let $A' = A_1 \cup \cdots \cup A_s$ where each of the sets $A_1, \ldots, A_s$ is contained in an L-coset, the cosets are pairwise disjoint, and $|A_1| \geq \cdots \geq |A_s| > 0$. By Claims 11.2 and 11.3, we have $s \geq 3$, and we proceed to consider separately the cases where $s = 3$, $s = 4$, $s = 5$, and $s \geq 6$. (The "typical" scenario is addressed in the last case, which also is much less technical to treat; for this reason, the reader may consider skipping directly to this case.)

Case 1: $s = 3$.

By Claim 11.3, and in view of $|\varphi_L(A')| = 3 \leq \lceil \frac{m}{6} \rceil$, the set $\varphi_L(A')$ is not an arithmetic progression; hence, in the representation

$$2A' = 2A_1 \cup 2A_2 \cup 2A_3 \cup (A_1 + A_2) \cup (A_2 + A_3) \cup (A_3 + A_1)$$

the union is disjoint and indeed, all sets in the right-hand side reside in distinct L-cosets. (We cannot have $\varphi_L(2A_i) = \varphi_L(2A_j)$ with $i \neq j$ since this would imply $2\varphi_L(A_i) = 2\varphi_L(A_j)$, contradicting rectifiability of $\varphi_L(A')$.) Thus, recalling (11.1),

$$\begin{aligned}\frac{5}{2}(|A_1| + |A_2| + |A_3|) &= \frac{5}{2}|A'| > |2A'| \\ &= |2A_1| + |2A_2| + |2A_3| + |A_1 + A_2| + |A_2 + A_3| + |A_3 + A_1|. \qquad (11.5)\end{aligned}$$

Claim 11.5. *The set A_1 is a VSDS; moreover, letting $K := A_1 - A_1$, we have $K \leq L$.*

Proof. Assume for a contradiction that A_1 is not a VSDS, and suppose first that A_2 is not a VSDS either. Then $|2A_1| \geq \frac{3}{2}|A_1|$, $|2A_2| \geq \frac{3}{2}|A_2|$, and $|A_1 + A_2| \geq |A_2| + \frac{1}{2}|A_1|$ by Corollary 5.3. Combining these estimates with (11.5) and the basic bound $|A_i + A_j| \geq |A_i|$ $(1 \leq i \leq j \leq 3)$, we conclude that

$$\begin{aligned}\frac{5}{2}(|A_1| + |A_2| + |A_3|) &> \frac{3}{2}|A_1| + \frac{3}{2}|A_2| + |A_3| + |A_2| + \frac{1}{2}|A_1| + |A_2| + |A_1| \\ &= 3|A_1| + \frac{7}{2}|A_2| + |A_3|\end{aligned}$$

leading to $3|A_3| > |A_1| + 2|A_2|$, a contradiction.

Thus, A_2 is a VSDS. Let $K' := A_2 - A_2$, and let k denote the number of the K'-cosets determined by A_1; since $|A_1| \geq |A_2| > \frac{2}{3}|K'|$ and A_1 is not contained in a K'-coset

with density exceeding 2/3, we have $k \geq 2$. Also, $|2A_1| \geq \frac{3}{2}|A_1|$ and $|A_1 + A_2| \geq k|A_2|$. Thus, (11.5) gives

$$\frac{5}{2}(|A_1| + |A_2| + |A_3|) > \frac{3}{2}|A_1| + |A_2| + |A_3| + k|A_2| + |A_2| + |A_1|$$

whence

$$3|A_3| > (2k-1)|A_2| \geq 3|A_2|,$$

a contradiction showing that A_1 is a VSDS. Finally, we notice that $K = A_1 - A_1$ implies $K \leq L$ (as A_1 is contained in an L-coset). □

Let K denote the subgroup of Claim 11.5; thus, A_1 is contained in a K-coset and $|A_1| > \frac{2}{3}|K|$.

Claim 11.6. *Each of the sets A_1, A_2, A_3 is contained in a K-coset.*

Proof. If neither A_2 nor A_3 is contained in an K-coset, then $|A_2 + A_1| \geq 2|A_1|$ and $|A_3 + A_1| \geq 2|A_1|$ whence, by (11.5)

$$\frac{5}{2}(|A_1| + |A_2| + |A_3|) > |A_1| + |A_2| + |A_3| + 2|A_1| + |A_2| + 2|A_1|$$

resulting in

$$5|A_1| < |A_2| + 3|A_3|,$$

which contradicts the assumption $|A_1| \geq |A_2| \geq |A_3|$.

If A_2 is not contained in an K-coset, while A_3 is, then $|A_1+A_2| \geq 2|A_1|$ and $|A_2+A_3| \geq 2|A_3|$, and then

$$\frac{5}{2}(|A_1| + |A_2| + |A_3|) > |A_1| + |A_2| + |A_3| + 2|A_1| + 2|A_3| + |A_1|,$$
$$3|A_1| + |A_3| < 3|A_2|,$$

a contradiction to $|A_1| \geq |A_2|$.

Finally, if A_2 is contained in an K-coset, while A_3 is not, then $|A_1 + A_3| \geq 2|A_1|$ and $|A_2 + A_3| \geq 2|A_2|$; as a result,

$$\frac{5}{2}(|A_1| + |A_2| + |A_3|) > |A_1| + |A_2| + |A_3| + |A_1| + 2|A_2| + 2|A_1|,$$
$$3|A_1| + |A_2| < 3|A_3|,$$

a contradiction to $|A_1| \geq |A_3|$.

The assertion follows. □

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

Let $A'' = B_1 \cup \cdots \cup B_t$ be the K-coset decomposition of A''; that is, each of $B_1, \ldots, B_t$ is contained in a K-coset, and the cosets are pairwise disjoint. Write $\mathcal{A}' := \varphi_K(A')$, $\mathcal{A}'' := \varphi_K(A'')$, and $\mathcal{A} := \varphi_K(A)$; thus, $|\mathcal{A}'| = 3$, $|\mathcal{A}''| = t$, and $|\mathcal{A}| = 3 + t$.

We have

$$\frac{9}{4}\,|A| > |2A| \geq |A + A_1| \geq (3+t)|A_1| \geq \frac{3+t}{3}|A'| > \frac{3+t}{3} \cdot 0.9|A|$$

whence $t \leq 4$. We now improve this estimate as follows.

Claim 11.7. *We have $t \leq 2$.*

Proof. Let $\mathcal{H} := \pi(\mathcal{A} + \mathcal{A}')$. If $|\mathcal{A} + \mathcal{A}'| < |\mathcal{A}| + \frac{1}{2}|\mathcal{A}'|$, then by Lemma 5.2, the set $\mathcal{A}'$ is contained in an $\mathcal{H}$-coset. Consequently, A' is contained in a coset of the subgroup $\varphi_K^{-1}(\mathcal{H})$. Hence, by Claim 11.2, we have $\varphi_K^{-1}(\mathcal{H}) = \mathbb{Z}_n$; that is, $\mathcal{H} = \mathbb{Z}_n/K$, meaning that $\mathcal{A} + \mathcal{A}' = \mathbb{Z}_n/K$. Therefore, $|\mathcal{A} + \mathcal{A}'| = n/|K| \geq n/|L| \geq 37 > (3+t) + \frac{3}{2} = |\mathcal{A}| + \frac{1}{2}|\mathcal{A}'|$, a contradiction.

We therefore conclude that $|\mathcal{A} + \mathcal{A}'| \geq |\mathcal{A}| + \frac{1}{2}\,|\mathcal{A}'|$ and then indeed, rounding to an integer, $|\mathcal{A} + \mathcal{A}'| \geq 5 + t$. It follows that the set $A + A'$ consists of the $|\mathcal{A}| = 3 + t$ subsets $2A_1, A_1 + A_2, A_1 + A_3, A_1 + B_1, \ldots, A_1 + B_t$, and at least two more subsets of size at least $|A_3|$ each, all these subsets being pairwise disjoint. As a result,

$$|A + A'| \geq (t+3)|A_1| + 2|A_3|. \tag{11.6}$$

On the other hand,

$$|A + A'| \leq |2A| < \frac{9}{4}\,|A| < \frac{5}{2}\,|A'| = \frac{5}{2}\,(|A_1| + |A_2| + |A_3|).$$

Comparing this estimate with (11.6), we get

$$(t+3)|A_1| + 2|A_3| < \frac{5}{2}\,(|A_1| + |A_2| + |A_3|),$$
$$(2t+1)|A_1| < 5|A_2| + |A_3|,$$

whence $t \in \{1, 2\}$, as claimed. $\square$

If $|(\mathcal{A}' + \mathcal{A}'') \setminus 2\mathcal{A}'| \geq 2$, then $|(A' + A'') \setminus (2A')| \geq 2|A_3|$, leading to

$$\frac{5}{2}\,(|A_1| + |A_2| + |A_3|) = \frac{5}{2}\,|A'| > \frac{9}{4}\,|A| > |2A| \geq |2A'| + 2|A_3|. \tag{11.7}$$

On the other hand, from (11.5) and the trivial estimate $|A_i + A_j| \geq |A_i|$ $(1 \leq i \leq j \leq 3)$,

$$|2A'| \geq 3|A_1| + 2|A_2| + |A_3|.$$

From this estimate and (11.7) we get

$$\frac{5}{2}\left(|A_1|+|A_2|+|A_3|\right) > 3|A_1|+2|A_2|+3|A_3|,$$
$$|A_1|+|A_3| < |A_2|$$

which is obviously wrong.

Thus, $|(\mathcal{A}'+\mathcal{A}'')\setminus 2\mathcal{A}'| \le 1$. Consequently, for any $\beta \in \mathcal{A}''$ there are (at least) two elements $\alpha \in \mathcal{A}'$ with $\beta+\alpha \in 2\mathcal{A}'$. Applying Lemma 6.6 and taking into account that $\mathcal{A}'$ is not contained in a four-term progression by Claim 11.3, we conclude that if $\alpha_1, \alpha_2 \in \mathcal{A}'$ are elements with $\beta+\alpha_1, \beta+\alpha_2 \in 2\mathcal{A}'$, then $\{\alpha_1, \alpha_2, \beta\}$ is a coset of the three-element subgroup of $\mathbb{Z}_n/K$. If $t=1$, then this shows that A is contained in a union of two cosets of a subgroup of size at most $3|K|$, contradicting Lemma 8.1. If $t=2$, then writing $\mathcal{A}''=\{\beta_1,\beta_2\}$, and applying Lemma 6.6, there are elements $\alpha, \alpha_1, \alpha_2 \in \mathcal{A}'$ with $\alpha \ne \alpha_1$, $\alpha \ne \alpha_2$ such that both $\{\alpha, \alpha_1, \beta_1\}$ and $\{\alpha, \alpha_2, \beta_2\}$ are cosets of the three-element subgroup of $\mathbb{Z}_n/K$. Sharing the same common element α, these cosets must be identical, which is impossible since, for instance, $\beta_1 \notin \{\alpha, \alpha_2, \beta_2\}$.

Case 2: $s=4$**.**

By Claim 11.3, the set $\varphi_L(A')$ is not contained in an arithmetic progression with five or fewer terms; as a result, by Theorem 6.2 (as applied to the set of integers locally isomorphic to $\varphi_L(A')$, with $l=5$), we have

$$|2\varphi_L(A')| \ge 9; \tag{11.8}$$

that is, $2A'$ meets at least nine L-cosets. Of these cosets, four are the cosets determined by the sums $A_1+A_1, \dots, A_1+A_4$, and at least five more are determined by some other sums of the form A_i+A_j, with $2 \le i \le j \le 4$. Using the trivial estimate $|A_i+A_j| \ge |A_i|$ for these sums, and observing that in the resulting estimate the summand $|A_4|$ can appear at most once, and $|A_3|$ at most twice, we get

$$\frac{5}{2}|A'| > |2A'| \ge |A_1+A_1|+\dots+|A_1+A_4|+2|A_2|+2|A_3|+|A_4|. \tag{11.9}$$

Claim 11.8. *A_1 is a VSDS.*

Proof. Assuming for the contradiction that A_1 is not a VSDS, by Corollary 5.3 we have $|A_1+A_2| \ge |A_2|+\frac{1}{2}|A_1|$. Substituting to (11.9), we obtain

$$\begin{aligned}\frac{5}{2}|A'| &> \frac{3}{2}|A_1| + \left(|A_2|+\frac{1}{2}|A_1|\right) + 2|A_1|+2|A_2|+2|A_3|+|A_4| \\ &= 4|A_1|+3|A_2|+2|A_3|+|A_4|.\end{aligned}$$

This simplifies to the obviously wrong inequality

$$3|A_1| + |A_2| < |A_3| + 3|A_4|,$$

a contradiction proving the claim. □

Let $K := A_1 - A_1$; thus, K is a subgroup of L, and A_1 is contained in a K-coset with $|A_1| > \frac{2}{3}|K|$; also, $|2A_1| = |K|$. Notice that K is nonzero (else $|A_1| = 1$ and then $|A'| = 4$ contradicting (11.2)).

From (11.9), and in view of $|2A_1| = |K|$, we have

$$\frac{5}{2}|A'| > |K| + 3|A_1| + 2|A_2| + 2|A_3| + |A_4|,$$
$$|A_2| + |A_3| + 3|A_4| > |A_1| + 2|K|,$$

resulting in $|A_1| + 3|A_4| > 2|K|$. Hence,

$$|A_1| + |A_4| = \frac{1}{2}(|A_1| + 3|A_4|) + \frac{1}{2}(|A_1| - |A_4|) > |K|,$$

and then indeed $|A_1| + |A_i| > |K|$ for all $i \in [1, 4]$, leading, by Lemma 6.1, to

$$|A_1 + A_i| \geq |K|. \tag{11.10}$$

Substituting this estimate back to (11.9), we now get

$$\frac{5}{2}|A'| > 4|K| + 2|A_2| + 2|A_3| + |A_4|,$$
$$5|A_1| + |A_2| + |A_3| + 3|A_4| > 8|K|, \tag{11.11}$$

which leads to

$$7|A_1| + 3|A_4| > 8|K|,$$
$$|A_1| + \frac{1}{2}|A_i| \geq |A_1| + \frac{1}{2}|A_4| > |K|, \tag{11.12}$$

for all $i \in \{2, 3, 4\}$.

Claim 11.9. *Each of the sets A_1, A_2, A_3, A_4 is contained in a single K-coset.*

Proof. If, for some $i \in \{2, 3, 4\}$, the set A_i determines two or more K-cosets, then in view of (11.12), by Lemma 6.1 (ii) we have $|A_1 + A_i| \geq |A_1| + |K|$. Using (11.9) and (11.10), we then get

$$\frac{5}{2}|A'| > 4|K| + |A_1| + 2|A_2| + 2|A_3| + |A_4|,$$
$$3|A_1| + |A_2| + |A_3| + 3|A_4| > 8|K|,$$

which is wrong since $|A_1| \le |K|$. $\square$

Notice that from (11.11)

$$8|K| < 5|A_1| + |A_2| + |A_3| + 3|A_4| \le 6|K| + 2(|A_3| + |A_4|).$$

It follows that $|A_i| + |A_j| > |K|$, and therefore $A_i + A_j$ is a K-coset for all $i, j \in [1, 4]$ with the possible exception of $i = j = 4$. Consequently, from (11.8) we obtain

$$\frac{5}{2}\,|A'| > |2A'| \ge 8|K| + |A_4|. \tag{11.13}$$

Let $\mathcal{A}' := \varphi_K(A')$, $\mathcal{A}'' := \varphi_K(A'')$, and $\mathcal{A} := \varphi_K(A)$. Thus $|\mathcal{A}'| = 4$, and from (11.8) we have

$$|2\mathcal{A}'| = |2\varphi_K(A')| = |\varphi_K(2A')| \ge |\varphi_L(2A')| = |2\varphi_L(A')| = 9.$$

Indeed, if we had $|2\mathcal{A}'| \ge 10$, then instead of (11.13) we would be able to get the estimate

$$\frac{5}{2}\,|A'| > |2A'| \ge 9|K| + |A_4|,$$

which is wrong in view of $|A'| \le 3|K| + |A_4|$. Thus $|2\mathcal{A}'| = 9$. Observing that $\mathcal{A}'$ determines $\binom{4}{2} + 4 = 10$ sums $\alpha_1 + \alpha_2$ with $\alpha_1, \alpha_2 \in \mathcal{A}'$, we conclude that exactly two of these sums coincide, while the rest are distinct from each other and from the two coinciding sums.

Write $t := |\mathcal{A}''|$ and $A'' = B_1 \cup \dots \cup B_t$ where each of $B_1, \dots, B_t$ is contained in a K-coset, and the cosets are pairwise distinct; notice that $|\mathcal{A}| = 4 + t$.

If $\mathcal{A}' + \mathcal{A}'' \not\subseteq 2\mathcal{A}'$, then there are $i \in [1, 4]$ and $j \in [1, t]$ such that the sum $A_i + B_j$ is disjoint from $2A'$; consequently, from (11.13)

$$\frac{5}{2}\,|A'| > \frac{9}{4}\,|A| > |2A| \ge |2A'| + |A_i + B_j| \ge (8|K| + |A_4|) + |A_4|,$$
$$5|A'| > 16|K| + 4|A_4|,$$
$$5|A_1| + 5|A_2| + 5|A_3| + |A_4| > 16|K| \ge 16|A_1|,$$

a contradiction.

Therefore, $\mathcal{A}' + \mathcal{A}'' \subseteq 2\mathcal{A}'$ implying

$$2\mathcal{A} = 2\mathcal{A}' \cup 2\mathcal{A}''. \tag{11.14}$$

In addition, from $\mathcal{A}' + \mathcal{A}'' \subseteq 2\mathcal{A}'$ we derive that $\mathcal{A} + \mathcal{A}' \subseteq 2\mathcal{A}'$, and since the inverse inclusion holds trivially, we have, indeed, $\mathcal{A} + \mathcal{A}' = 2\mathcal{A}'$. Thus,

$$|\mathcal{A}'| = 4,\ |\mathcal{A}''| = t,\ |\mathcal{A}| = 4 + t,\ |\mathcal{A} + \mathcal{A}'| = |2\mathcal{A}'| = 9. \tag{11.15}$$

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

From $A_1+A_1,\dots,A_1+A_4,A_1+B_1,\dots,A_1+B_t\subseteq 2A$ we get

$$\frac{9}{4}\,|A|>|2A|\ge (t+4)|A_1|\ge \frac{t+4}{4}\,|A'|>0.9\,\frac{t+4}{4}\,|A|$$

which yields $t\le 5$. We can improve this bound as follows.

Claim 11.10. *We have $t\le 3$.*

Proof. Let $\mathcal{H}:=\pi(\mathcal{A}+\mathcal{A}')$. If $|\mathcal{A}+\mathcal{A}'|<|\mathcal{A}|+\frac{1}{2}|\mathcal{A}'|$, then by Lemma 5.2, the set $\mathcal{A}'$ is contained in an $\mathcal{H}$-coset. Consequently, A' is contained in a coset of the subgroup $\varphi_K^{-1}(\mathcal{H})$. Hence, by Claim 11.2, we have $\varphi_K^{-1}(\mathcal{H})=\mathbb{Z}_n$; that is, $\mathcal{H}=\mathbb{Z}_n/K$, meaning that $\mathcal{A}+\mathcal{A}'=\mathbb{Z}_n/K$. Therefore, $|\mathcal{A}+\mathcal{A}'|=n/|K|\ge n/|L|\ge 37>6+t=|\mathcal{A}|+\frac{1}{2}|\mathcal{A}'|$, a contradiction.

Thus, $|\mathcal{A}+\mathcal{A}'|\ge|\mathcal{A}|+\frac{1}{2}|\mathcal{A}'|=t+6$ showing that the set $A+A'$ consists of the $|\mathcal{A}|=4+t$ subsets $2A_1,A_1+A_2,A_1+A_3,A_1+A_4,A_1+B_1,\dots,A_1+B_t$, and at least two more subsets of size at least $|A_4|$ each (with all these subsets pairwise disjoint). As a result,

$$|A+A'|\ge (t+4)|A_1|+2|A_4|.$$

On the other hand,

$$|A+A'|\le|2A|<\frac{9}{4}\,|A|<\frac{5}{2}\,|A'|=\frac{5}{2}\,(|A_1|+|A_2|+|A_3|+|A_4|).$$

Comparing the last two estimates, we get

$$(2t+3)|A_1|<5|A_2|+5|A_3|+|A_4|$$

whence $t\le 3$. $\square$

Case 2.1: $t=1$. In this case we have $A=A'\cup A''$ where $A'=A_1\cup A_2\cup A_3\cup A_4$ with $A_1,\dots,A_4$ residing in pairwise distinct K-cosets, and where A'' resides in yet another K-coset. Moreover, in view of (11.15), and recalling that A_i+A_j is a K-coset for all $i,j\in[1,4]$ with the possible exception of $i=j=4$, the set $2A'$ is a disjoint union of eight K-cosets, and one more set which is either a K-coset, or the set $2A_4$ (contained in a K-coset). Also, from (11.14), there are at most two K-cosets intersecting $2A$, but not entirely contained in $2A$: namely, the cosets determined by $2A_4$ and by $2A''$. It follows that $|2A+K|-|2A|\le(|K|-|2A_4|)+(|K|-|2A''|)$. Also, $|A+K|-|A|=5|K|-|A|$. On the other hand, we observe that K is nonzero (as otherwise we would have $|A|=|\mathcal{A}|=5$ contradicting (11.2)), and that $2A+K\ne\mathbb{Z}_n$ (otherwise $\frac{n}{|K|}=|2\mathcal{A}|\le|2\mathcal{A}'|+1=10$ while, on the other hand, $\frac{n}{|K|}\ge\frac{n}{|L|}\ge 37$). Consequently, we can apply Lemma 7.1 to get

$$(|K| - |2A_4|) + (|K| - |2A''|) > 5|K| - |A|,$$
$$|A| > 3|K| + |2A_4| + |2A''|$$

which is wrong in view of

$$|A| = |A_1| + |A_2| + |A_3| + |A_4| + |A''| \le 3|K| + |A_4| + |A''|.$$

Case 2.2: $t \in \{2, 3\}$. In this case $|\mathcal{A}'| = 4$, $|\mathcal{A}''| = t$, $|\mathcal{A}| = 4 + t$, and $|\mathcal{A} + \mathcal{A}'| = |2\mathcal{A}'| = 9 = |\mathcal{A}| + |\mathcal{A}'| - (t - 1)$. Furthermore, $|\mathcal{A}| + |\mathcal{A}'| = t + 8 \le 11 < |\mathbb{Z}_n/L| \le |\mathbb{Z}_n/K|$, $|\mathcal{A}| \ge |\mathcal{A}'| \ge 2$, and $\mathcal{A}'$ is rectifiable (as a result of the rectifiability of $\varphi_L(A')$), not an arithmetic progression (by Claim 11.3), and not contained in a proper coset (as a consequence of Claim 11.2). Thus, the assumptions of Lemma 6.5 are satisfied. Applying the lemma, we conclude that there is a nonzero, proper subgroup $\mathcal{H} < \mathbb{Z}_n/K$ such that $\mathcal{A}'$ meets two $\mathcal{H}$-cosets and has exactly $(|\mathcal{H}| + 1)/2$ elements in each of them. Since $|\mathcal{A}'| = 4$, we have $|\mathcal{H}| = 3$; thus, we can write $\mathcal{A}' = \{\alpha_1, \alpha_1 + \delta, \alpha_2, \alpha_2 + \delta\}$ where δ is an element of the group $\mathbb{Z}_n/K$ of order 3 (so that $\mathcal{H} = \{0, \delta, 2\delta\}$), and $\alpha_1, \alpha_2 \in \mathbb{Z}_n/K$ belong to distinct $\mathcal{H}$-cosets.

As a result of (11.14), we have $\mathcal{A}'' \subseteq (2\mathcal{A}' - \alpha_1) \cap (2\mathcal{A}' - \alpha_2)$, where the two sets in the right-hand side are

$$2\mathcal{A}' - \alpha_1 = \{\alpha_1, \alpha_2, 2\alpha_2 - \alpha_1\} + \mathcal{H}$$

and

$$2\mathcal{A}' - \alpha_2 = \{\alpha_1, \alpha_2, 2\alpha_1 - \alpha_2\} + \mathcal{H}.$$

The elements $2\alpha_1 - \alpha_2$ and $2\alpha_2 - \alpha_1$ lie in distinct $\mathcal{H}$-cosets, since otherwise we would have $3(\alpha_1 - \alpha_2) \in \mathcal{H}$ and then $\mathcal{A}'$ would be contained in a coset of a nine-element subgroup, contradicting Claim 11.2 in view of $|\mathbb{Z}_n/K| \ge n/|L| > 9$. Therefore, $\mathcal{A}'' \subseteq \{\alpha_1, \alpha_2\} + \mathcal{H}$, and it follows that $\mathcal{A} \subseteq (\alpha_1 + \mathcal{H}) \cup (\alpha_2 + \mathcal{H})$. Consequently, A is contained in the union of two cosets of the subgroup $\varphi_K^{-1}(\mathcal{H})$. Since this subgroup has size at most $|K||\mathcal{H}| = 3|K| \le 3|L| < n/2$, we can invoke Lemma 8.1 to complete the proof.

Case 3: $s = 5$**.**

By Claim 11.3, the set $\varphi_L(A')$ is not contained in an arithmetic progression with seven or fewer terms; as a result, by Theorem 6.2 (as applied to the set of integers locally isomorphic to $\varphi_L(A')$, with $l = 7$), we have

$$|2\varphi_L(A')| \ge 12; \tag{11.16}$$

that is, $2A'$ meets at least twelve L-cosets. Of these cosets, five are the cosets determined by the sums $A_1 + A_1, \ldots, A_1 + A_5$, and at least seven more are determined by some other sums of the form $A_i + A_j$, with $2 \le i \le j \le 5$. Using the trivial estimate $|A_i + A_j| \ge |A_i|$

for these sums, and observing that in the resulting inequality the summand $|A_5|$ can appear at most once, $|A_4|$ at most twice, and $|A_3|$ at most three times, we get

$$\begin{aligned}\frac{5}{2}\,|A'| > |2A'| &\geq |A_1+A_1|+\cdots+|A_1+A_5|+|A_2|+3|A_3|+2|A_4|+|A_5| \\ &\geq 5|A_1|+|A_2|+3|A_3|+2|A_4|+|A_5| \\ &= 2|A'|+3|A_1|-|A_2|+|A_3|-|A_5|.\end{aligned} \tag{11.17}$$

It follows that

$$5|A_1|+|A_3| < 3|A_2|+|A_4|+3|A_5|. \tag{11.18}$$

Claim 11.11. *A_1 is a VSDS.*

Proof. If $|2A_1| \geq \frac{3}{2}\,|A_1|$, then the summand $5|A_1|$ in (11.17) can be replaced with $\frac{11}{2}\,|A_1|$, and then (11.18) can be improved to $6|A_1|+|A_3| < 3|A_2|+|A_4|+3|A_5|$. However, this implies $6|A_1| < 3|A_2|+3|A_5|$ which is obviously wrong. □

With Claim 11.11 in mind, let $K := A_1 - A_1$; thus, $K \leq L$ is a subgroup, A_1 is contained in a K-coset, $|A_1| > \frac{2}{3}|K|$, and $|2A_1| = |K|$. Notice that K is nonzero (else $|A_1| = 1$ and then $|A'| = 5$ contradicting (11.2)).

From (11.18) we get

$$5|A_1| < 3|A_2|+3|A_5| \leq 3|A_1|+3|A_5|$$

whence $|A_i| \geq |A_5| > \frac{2}{3}\,|A_1|$ for each $i \in [1,5]$. Therefore $|A_1|+|A_i| \geq \frac{5}{3}\,|A_1| > |K|$, and then $|A_1+A_i| \geq |K|$ by Lemma 6.1. Consequently, we can improve (11.18) to write

$$\begin{aligned}\frac{5}{2}\,|A'| > |2A'| &\geq 5|K|+|A_2|+3|A_3|+2|A_4|+|A_5| \\ &= 2|A'|+5|K|-2|A_1|-|A_2|+|A_3|-|A_5|.\end{aligned}$$

It follows that

$$\begin{aligned}|A'| &> 10|K|-4|A_1|-2|A_2|+2|A_3|-2|A_5|, \\ 5|A_1|+3|A_2|+|A_4|+3|A_5| &> 10|K|+|A_3|, \\ 10|K| < 5|A_1|+3|A_2|+3|A_5| &\leq 8|K|+3|A_5|,\end{aligned}$$

implying

$$|A_2| \geq \cdots \geq |A_5| > \frac{2}{3}|K|. \tag{11.19}$$

Therefore

$$|A_i| + 2|A_1| > 2|K|. \tag{11.20}$$

Claim 11.12. *Each of the sets $A_1, \dots, A_5$ is contained in a single K-coset.*

Proof. By Lemma 6.1, from (11.20) it follows that if, for some index $i \in [2,5]$, the set A_i meets two or more K-cosets, then $|A_1 + A_i| \ge |K| + |A_1|$. Hence, in this case

$$\frac{5}{2}|A'| > (5|K| + |A_1|) + |A_2| + 3|A_3| + 2|A_4| + |A_5|$$
$$= 5|K| + 2|A'| - |A_1| - |A_2| + |A_3| - |A_5|,$$

leading to

$$3|A_1| + 3|A_2| + |A_4| + 3|A_5| > 10|K| + |A_3|$$

which is wrong as the sum in the left-hand side is at most $9|K| + |A_4|$. □

As it follows from Claim 11.12 and (11.19), we have $|A_i + A_j| = |K|$ for all $i, j \in [1,5]$. Hence, $2A'$ is K-periodic and

$$|2A'| \ge 12|K|$$

(cf. (11.16)); indeed, equality holds as $|A'| \le 5|K|$ implies $|2A'| < \frac{5}{2}|A'| < 13|K|$.

Let $\mathcal{A}' := \varphi_K(A')$, $\mathcal{A}'' := \varphi_K(A'')$, and $\mathcal{A} := \varphi_K(A)$; thus $|\mathcal{A}'| = 5$ and $|2\mathcal{A}'| = 12$. Also, write $t := |\mathcal{A}''|$ and $A'' = B_1 \cup \dots \cup B_t$ where each of $B_1, \dots, B_t$ is contained in a K-coset and the cosets are pairwise distinct; notice that $|\mathcal{A}| = 5 + t$.

If $\mathcal{A}' + \mathcal{A}'' \not\subseteq 2\mathcal{A}'$, then there are $i \in [1,5]$ and $j \in [1,t]$ such that the sum $A_i + B_j$ is disjoint from $2A'$; consequently,

$$\frac{5}{2}|A'| > |2A| \ge |2A'| + |A_i + B_j| \ge 12|K| + |A_5|,$$
$$5|A'| > 24|K| + 2|A_5|,$$
$$5|A_1| + 5|A_2| + 5|A_3| + 5|A_4| + 3|A_5| > 24|K|$$

which is wrong.

Therefore, $\mathcal{A}' + \mathcal{A}'' \subseteq 2\mathcal{A}'$; as a result, $\mathcal{A} + \mathcal{A}' \subseteq 2\mathcal{A}'$, and since the inverse inclusion is trivial, we have, indeed, $\mathcal{A} + \mathcal{A}' = 2\mathcal{A}'$.

The relation $\mathcal{A}' + \mathcal{A}'' \subseteq 2\mathcal{A}'$ also shows that $2\mathcal{A} = (2\mathcal{A}') \cup (2\mathcal{A}'')$. Since $2A$ is aperiodic by Lemma 7.2, while $2A'$ is K-periodic as a consequence of (11.19), we conclude that there exist $i, j \in [1,t]$ such that $B_i + B_j$ is disjoint from $2A'$.

From $A_1 + A_1, \dots, A_1 + A_5, A_1 + B_1, \dots, A_1 + B_t \subseteq 2A$ we get

$$\frac{9}{4}|A| > |2A| \ge (t+5)|A_1| \ge \frac{t+5}{5}|A'| > 0.9\,\frac{t+5}{5}|A|$$

which yields $t \le 7$. We now prove a sharper estimate.

Claim 11.13. *We have $t \le 4$.*

Proof. Arguing as in the proof of Claim 11.10, from Lemma 5.2 we obtain

$$|\mathcal{A}+\mathcal{A}'| \ge |\mathcal{A}| + \frac{1}{2}|\mathcal{A}'| = (5+t) + \frac{5}{2}.$$

Thus, the set $A + A'$ consists of the $|\mathcal{A}| = 5 + t$ subsets $2A_1, A_1 + A_2, A_1 + A_3, A_1 + A_4, A_1 + A_5, A_1 + B_1, \dots, A_1 + B_t$, and at least $\lceil \frac{5}{2} \rceil = 3$ more subsets of size at least $|A_5|$ each (with all these subsets pairwise disjoint). As a result,

$$|A + A'| \ge (t + 5)|A_1| + 3|A_5|.$$

On the other hand,

$$|A+A'| \le |2A| < \frac{9}{4}|A| < \frac{5}{2}|A'| = \frac{5}{2}(|A_1| + |A_2| + |A_3| + |A_4| + |A_5|).$$

Comparing the last two estimates, we get

$$(2t + 5)|A_1| + |A_5| < 5|A_2| + 5|A_3| + 5|A_4|$$

whence $t \le 4$. $\square$

Case 3.1: $t = 1$. As explained above, in this case $2B_1$ is disjoint from $2A'$. As a result, $|2A| \ge |2A'| + |2B_1| \ge 12|K| + |A''|$ and then

$$\frac{9}{4}(|A'| + |A''|) = \frac{9}{4}|A| > |2A| \ge 12|K| + |A''|, \tag{11.21}$$
$$9|A'| + 5|A''| > 48|K|,$$
$$48|K| < \frac{86}{9}|A'| \le \frac{430}{9}|K|$$

(the inequalities in the last line following from (11.2) and Claim 11.12), which is wrong.

Case 3.2: $t = 2$. Write $\beta_i := \varphi_K(B_i)$, $i \in \{1, 2\}$; thus, $\mathcal{A}'' = \{\beta_1, \beta_2\}$. Since $2\mathcal{A}'' \not\subseteq 2\mathcal{A}'$, there is a pair of indices $1 \le i \le j \le 2$ such that $\beta_i + \beta_j \notin 2\mathcal{A}'$. Suppose first that (i, j) is a unique pair with this property. In this situation we have $|2A + K| - |2A| = |K| - |B_i + B_j|$ and $|A + K| - |A| = 7|K| - |A|$. On the other hand, K is nonzero (as otherwise we would have $|A| = |\mathcal{A}| = 7$), and $2A + K \ne \mathbb{Z}_n$ (otherwise $\frac{n}{|K|} = |2\mathcal{A}| \le |2\mathcal{A}'| + \binom{t}{2} + t = 15$ while, on the other hand, $\frac{n}{|K|} \ge \frac{n}{|L|} \ge 37$). Consequently, $|K| - |B_i + B_j| > 7|K| - |A|$ by Lemma 7.1, which yields

$$|A| > 6|K| + |B_i + B_j|.$$

From this estimate and

$$|A| = |A'| + |A''| \le 5|K| + |B_1| + |B_2|$$

we get $|B_1|+|B_2| > |B_i+B_j|+|K|$, which is impossible in view of $\max\{|B_1|, |B_2|\} \le |K|$ and $\min\{|B_1|, |B_2|\} \le |B_i + B_j|$.

We therefore conclude that there are at least two pairs (i, j) with $1 \le i \le j \le 2$ and $\beta_i + \beta_j \notin \mathcal{A}'$. If, moreover, one can find two such pairs so that the sums $\beta_i + \beta_j$ are distinct from each other, then the two corresponding sumsets $B_i + B_j$ jointly contain at least $|B_1| + |B_2| = |A''|$ elements (which may not be obvious, but is not difficult to see either). Consequently,

$$|2A| \ge |2A'| + |A''| \ge 12|K| + |A''|$$

leading to a contradiction as in the case $t = 1$, cf. (11.21).

We are left with the case where there are at least two pairs of indices $1 \le i \le j \le 2$ with $\beta_i + \beta_j \notin 2\mathcal{A}'$, but the sums $\beta_i + \beta_j$ are equal to each other for all such pairs (i, j). Since $\beta_1 + \beta_2$ is distinct from each of $2\beta_1$ and $2\beta_2$, we actually have $2\beta_1 = 2\beta_2$; that is, the two pairs are $(1, 1)$ and $(2, 2)$, while $\beta_1 + \beta_2 \in 2\mathcal{A}'$. Acting as above, we get in this case $|2A + K| - |2A| = |K| - |2B_1 \cup 2B_2|$ and $|A + K| - |A| = 7|K| - |A|$, whence $|K| - |2B_1 \cup 2B_2| > 7|K| - |A|$ by Lemma 7.1. Therefore $|A| > 6|K| + |2B_1 \cup 2B_2|$ which, along with $|A| = |A'| + |A''| \le 5|K| + |B_1| + |B_2|$, gives $|B_1| + |B_2| > |2B_1 \cup 2B_2| + |K|$. This, however, is impossible in view of $\max\{|B_1|, |B_2|\} \le \min\{|K|, |2B_1 \cup 2B_2|\}$.

Case 3.3: $t \in \{3, 4\}$. In this case $|\mathcal{A}'| = 5$, $|\mathcal{A}''| = t$, $|\mathcal{A}| = 5 + t$, and $|\mathcal{A} + \mathcal{A}'| = |2\mathcal{A}'| = 12 = |\mathcal{A}| + |\mathcal{A}'| - (t - 2)$. Furthermore, $|\mathcal{A}| + |\mathcal{A}'| = 10 + t \le 14 < 36 < n/|L| \le |\mathbb{Z}_n/K|$, $|\mathcal{A}| \ge |\mathcal{A}'| \ge 2$, and $\mathcal{A}'$ is rectifiable (as a result of the rectifiability of $\varphi_L(A')$), not an arithmetic progression (by Claim 11.3) and not contained in a proper coset (as a consequence of Claim 11.2). Thus, the assumptions of Lemma 6.5 are satisfied. Applying the lemma, we conclude that $|\mathcal{A}'|$ is even, a contradiction.

Case 4: $s \ge 6$**.** In this case $\tau' := |2A'|/|A'| < \frac{5}{2} = 3(1 - 1/s)$. In view of this estimate, and since $\varphi_L(A')$ is a rectifiable subset of $\mathbb{Z}_n/L$, we can apply Proposition 3.2 to the set A' to find a proper subgroup $H' < \mathbb{Z}_n$ and a progression $P' \subseteq \mathbb{Z}_n$ of size $|P'| > 1$ such that $A' \subseteq P' + H'$, $|P' + H'| = |P'||H'|$, and $(|P'| - 1)|H'| \le |2A'| - |A'|$.

By Claim 11.2 and Lemma 5.1, and since $2A' \subseteq 2A \ne \mathbb{Z}_n$, we have

$$|2A'| \ge \frac{3}{2}|A'|. \tag{11.22}$$

If A contained an element $a \notin (2P' - P') + H'$, then $a + A' \subseteq a + P' + H'$ would be disjoint from $2A' \subseteq 2P' + H'$, and in view of (11.22) we would get

$$|2A| \ge |a + A'| + |2A'| \ge \frac{5}{2}\,|A'| > \frac{9}{4}\,|A|,$$

contradicting the small-doubling assumption. Thus,

$$A \subseteq 2P' - P' + H'. \tag{11.23}$$

Let d denote the difference of P'. Since A is contained in a coset of the subgroup generated by d and H', this subgroup is not proper; that is, the order of $\varphi_{H'}(d)$ in the quotient group $\mathbb{Z}_n/H'$ is $m' := n/|H'|$.

On the other hand, from Lemma 7.6,

$$\begin{aligned}|2P' - P'| &\le 3|P'| - 2 = 3(|P'| - 1) + 1 \\ &\le \frac{3}{|H'|}\,(|2A'| - |A'|) + 1 < \frac{3}{|H'|}\,|2A| + 1 \\ &\le \frac{3}{|H'|} \cdot 2C_0^{-1}n + 1 = 6C_0^{-1}m' + 1 < \frac{m'}{2} + 1.\end{aligned}$$

Thus, $\varphi_{H'}(2P'-P')$ is an arithmetic progression with the difference generating $\mathbb{Z}_n/H'$, and of size not exceeding $(|\mathbb{Z}_n/H'|+1)/2$; hence, a rectifiable set. In view of (11.23), the set $\varphi_{H'}(A)$ is rectifiable, too. Also, since A meets at least four H'-cosets by Lemma 9.1,

$$|2A| < \frac{9}{4}\,|A| \le 3\Big(1 - \frac{1}{|\varphi_{H'}(A)|}\Big)|A|.$$

Consequently, we can apply Proposition 3.2 to find a proper subgroup $H < \mathbb{Z}_n$ and a progression $P \subseteq \mathbb{Z}_n$ of size $|P| > 1$ such that $A \subseteq P + H$, $|P + H| = |P||H|$, and $(|P| - 1)|H| \le |2A| - |A|$. Thus A is regular, contrary to the choice of A as a counterexample set.

This completes the proof in the case $s \ge 6$.

Acknowledgment

I am grateful to David Grynkiewicz for his interest and useful conversations, and to the referee for a very careful reading of the manuscript and a number of truly valuable remarks and suggestions.

Appendix A. Rich cosets in small-doubling sets

We show here that if a set A satisfies the assumptions and conclusion (ii) of Theorem 1.1 (hence, also of Theorem 1.2), then there exists an H-coset such that a large proportion of its elements lies in A, except if the whole set A is contained in a coset, or in a union of two cosets of a small subgroup; see the discussion following the statement of Theorem 1.2 in the Introduction.

Proposition A.1. *Let n be a positive integer. Suppose that $A \subseteq \mathbb{Z}_n$ is a set satisfying $\tau := |2A|/|A| \le 2.257$, and that $H < \mathbb{Z}_n$ is a subgroup, and $P \subseteq \mathbb{Z}_n$ is an arithmetic progression of size $|P| \ge 3$ such that $A \subseteq P+H$ and $(|P|-1)|H| \le |2A|-|A|$. If A is not contained in a coset of a subgroup of size at most $3|A|$, or in a union of two cosets of a subgroup of size at most $\frac{5}{9}|A|$, then there exists an H-coset containing at least $\frac{4}{3\tau-1}|H|$ elements of A.*

Proof. We assume that $\tau > 1$ as otherwise A is a coset.

Suppose for a contradiction that in every H-coset contained in $P+H$ there are less than $\frac{4}{3\tau-1}|H|$ elements of A. Define m_1, m_2, and M to be the smallest, second smallest, and largest among the $|P|$ values $\{|(z+H)\cap A| \colon z \in P\}$, respectively; thus $m_1 \le m_2 \le M < \frac{4}{3\tau-1}|H|$ and $|A| \le |P|M < \frac{4}{3\tau-1}|P||H|$.

If the number of H-cosets meeting A is less than $|P|$, then averaging we obtain

$$M \ge \frac{|A|}{|P|-1} = \frac{|2A|-|A|}{(\tau-1)(|P|-1)} \ge \frac{|H|}{\tau-1} \ge \frac{4}{3\tau-1}|H|.$$

Therefore, A meets all H-cosets contained in $P+H$. Hence, $2A$ meets all H-cosets contained in $2P+H$; we assume that all these cosets are pairwise distinct as otherwise $2P+H$ is a coset of a subgroup of size at most $2(|P|-1)|H| \le 2(|2A|-|A|) = 2(\tau-1)|A| \le 3|A|$, with A contained in a (possibly, different) coset of this subgroup.

We define the *deficiency* of a set $S \subseteq \mathbb{Z}_n$ by $\mathsf{D}(S) := |(S+H)\setminus S|$. Clearly, we have $\mathsf{D}(A) = |P||H|-|A|$ and $\mathsf{D}(2A) = (2|P|-1)|H|-|2A|$; as a result, the inequality $(|P|-1)|H| \le |2A|-|A|$ can be equivalently rewritten as

$$\mathsf{D}(2A) \le \mathsf{D}(A). \tag{A.1}$$

On the other hand,

$$\tau = \frac{|2A|}{|A|} = \frac{(2|P|-1)|H|-\mathsf{D}(2A)}{|P||H|-\mathsf{D}(A)}$$

whence

$$\tau\mathsf{D}(A) = ((\tau-2)|P|+1)|H| + \mathsf{D}(2A). \tag{A.2}$$

From (A.2) and (A.1),

$$(\tau-1)\mathsf{D}(A) \le ((\tau-2)|P|+1)|H|. \tag{A.3}$$

If we had $\tau < \frac{5}{3}$ then, as an easy corollary from Kneser's theorem, A would be contained in a union of two cosets of a subgroup of size at most $\frac{5}{9}|A|$, or in a single coset of a subgroup of size at most $\frac{5}{3}|A|$; thus, $\tau \ge \frac{5}{3}$.

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

The trivial estimate $\mathsf{D}(A) > \left(1 - \frac{4}{3\tau-1}\right)|P||H| = \frac{3\tau-5}{3\tau-1}|P||H|$ along with (A.2), and with the inequality $|P| \geq 3$, yield

$$\begin{aligned}\mathsf{D}(2A) &> \tau\frac{3\tau-5}{3\tau-1}|P||H| - ((\tau-2)|P|+1)|H| \\ &\geq 3\tau\frac{3\tau-5}{3\tau-1}|H| - (3\tau-5)|H| \\ &= \frac{3\tau-5}{3\tau-1}|H| \\ &\geq 0.\end{aligned}$$

Therefore $2A + H \neq 2A$, and it follows that there is an H-coset in $2P + H$ which is not entirely contained in $2A$. Suppose that there is *exactly* one H-coset with this property, and write it as $z_1 + z_2 + H$ where $z_1, z_2 \in P$. Let $I := |(z_1 + H) \cap A|$. We have then $\mathsf{D}(2A) \leq |H| - I$ and $\mathsf{D}(A) \geq |H| - I + \left(1 - \frac{4}{3\tau-1}\right)(|P|-1)|H|$. Substituting into (A.2) we obtain

$$\tau|H| - \tau I + \tau\Big(1 - \frac{4}{3\tau-1}\Big)(|P|-1)|H| \leq ((\tau-2)|P|+1)|H| + (|H|-I),$$

which simplifies to

$$\Big(2 - \frac{4\tau}{3\tau-1}\Big)(|P|-1)|H| \leq (\tau-1)I.$$

Consequently,

$$\begin{aligned}\frac{4(\tau-1)}{3\tau-1}|H| > (\tau-1)I &\geq \Big(2 - \frac{4\tau}{3\tau-1}\Big)(|P|-1)|H| \\ &\geq 2\Big(2 - \frac{4\tau}{3\tau-1}\Big)|H| = \frac{4(\tau-1)}{3\tau-1}|H|\end{aligned}$$

which is obviously wrong. Thus, there are at least two H-cosets contained in $2P + H$, but not entirely contained in $2A$. Therefore,

$$m_1 + m_2 \leq |H| \tag{A.4}$$

by the pigeonhole principle.

We have

$$\begin{aligned}\mathsf{D}(A) &\geq (|H| - m_1) + (|H| - m_2) + (|H| - M)(|P| - 2) \\ &= |P|(|H| - M) + (2M - m_1 - m_2).\end{aligned}$$

Substituting into (A.3) we get

$$(\tau-1)|P|(|H|-M)+(\tau-1)(2M-m_1-m_2)\le((\tau-2)|P|+1)|H|,$$
$$(|H|-(\tau-1)M)|P|\le|H|-(\tau-1)(2M-m_1-m_2). \tag{A.5}$$

Assuming $|P|\ge 4$, in view of

$$|H|-(\tau-1)M>\Big(1-\frac{4(\tau-1)}{3\tau-1}\Big)|H|=\frac{3-\tau}{3\tau-1}\,|H|>0$$

we derive that $2M+m_1+m_2\ge\frac{3}{\tau-1}\,|H|$ and then

$$m_1+m_2>\left(\frac{3}{\tau-1}-2\cdot\frac{4}{3\tau-1}\right)|H|=\frac{\tau+5}{(\tau-1)(3\tau-1)}\,|H|>|H|$$

(where the last inequality follows from the assumption $\tau\le 2.257$), contradicting (A.4).

Thus, $|P|=3$ and from (A.5)

$$M+m_1+m_2\ge\frac{2}{\tau-1}\,|H|. \tag{A.6}$$

Let $A=A_1\cup A_2\cup A_3$ where each set A_i resides in an H-coset, and the sets are numbered so that $|A_1|=m_1$, $|A_2|=m_2$, and $|A_3|=M$. The set $2A$ meets five H-cosets, of which three are determined by the sums $A_1+A_3,\ A_2+A_3$, and $2A_3$, and two more are determined by two of the three sums $2A_1,\ A_1+A_2,\ 2A_2$. From the trivial bound $|A_i+A_j|\ge\max\{|A_i|,|A_j|\}$ $(i,j\in\{1,2,3\})$, any two out of the last three cosets jointly contain at least $|A_1|+|A_2|=m_1+m_2$ elements of A; therefore

$$|2A|\ge|A_1+A_3|+|A_2+A_3|+|2A_3|+m_1+m_2; \tag{A.7}$$

similarly,

$$|2A|\ge|2A_2|+|A_2+A_3|+|2A_3|+m_1+m_2. \tag{A.8}$$

(We notice that $2A_2+H\ne 2A_3+H$ since the H-cosets in $2P+H$ are pairwise distinct.)

If $M+m_1>|H|$, then also $M+m_2>|H|$ and $2M>|H|$ whence $|A_1+A_3|=|A_2+A_3|=|2A_3|=|H|$; consequently, by (A.7),

$$\tau\,|A|=|2A|\ge 3|H|+m_1+m_2=3|H|+|A|-M>\frac{9\tau-7}{3\tau-1}\,|H|+|A|. \tag{A.9}$$

If, on the other hand, $M+m_1\le|H|$, then $m_2\ge\frac{3-\tau}{\tau-1}\,|H|>\frac12\,|H|$ by (A.6); as a result, $|2A_2|=|A_2+A_3|=|2A_3|=|H|$. Substituting into (A.8), we see that (A.9) holds true in this case, too.

Finally, as a consequence of (A.9), we have $|A|\ge\frac{9\tau-7}{(3\tau-1)(\tau-1)}\,|H|$, and then

$$m_1+m_2=|A|-M>\left(\frac{9\tau-7}{(3\tau-1)(\tau-1)}-\frac{4}{3\tau-1}\right)|H|=\frac{5\tau-3}{(3\tau-1)(\tau-1)}\,|H|>|H|$$

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001

contradicting (A.4). □

References

[BP18] R. Balasubramanian, P.P. Pandey, On a theorem of Deshouillers and Freiman, Eur. J. Comb. 70 (2018) 284–296.

[DF03] J.-M. Deshouillers, G.A. Freiman, A step beyond Kneser's theorem for abelian finite groups, Proc. Lond. Math. Soc. (3) 86 (1) (2003) 1–28.

[F61] G.A. Freiman, Inverse problems in additive number theory. Addition of sets of residues modulo a prime, Dokl. Akad. Nauk SSSR 141 (3) (1961) 571–573 (in Russian).

[F62b] G.A. Freiman, Inverse problems of additive number theory, VII. On addition of finite sets, IV, Izv. Vysš. Učebn. Zaved., Mat. 31 (6) (1962) 131–144.

[F73] G.A. Freiman, Groups and the inverse problems of additive number theory, in: Number-Theoretic Studies in the Markov Spectrum and in the Structural Theory of Set Addition, Kalinin. Gos. Univ., Moscow, 1973, pp. 175–183.

[G13] D.J. Grynkiewicz, Structural Additive Theory, Developments in Mathematics, vol. 30, Springer, Cham, 2013.

[K60] J.H.B. Kemperman, On small sumsets in an abelian group, Acta Math. 103 (1960) 63–88.

[K53] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, Math. Z. 58 (1953) 459–484.

[K55] M. Kneser, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, Math. Z. 61 (1955) 429–434.

[L06] V.F. Lev, Critical pairs in abelian groups and Kemperman's theorem, Int. J. Number Theory 2 (3) (2006) 379–396.

[L22] V.F. Lev, Small doubling in groups with moderate torsion, SIAM J. Discrete Math. 36 (1) (2022) 315–335.

[LS20] V.F. Lev, I.D. Shkerdov, Small doubling in prime-order groups: from 2.4 to 2.6, J. Number Theory 217 (2020) 278–291.

[M65] H.B. Mann, Addition Theorems: The Addition Theorems of Group Theory and Number Theory, Interscience Publishers, a Division of John Wiley and Sons, New York, 1965.

[N96] M. Nathanson, Additive Number Theory. Inverse Problems and the Geometry of Sumsets, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996.

[O84] J.E. Olson, On the sum of two sets in a group, J. Number Theory 18 (1984) 110–120.

[TV06] T. Tao, V. Vu, Additive Combinatorics, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006.

Please cite this article in press as: V.F. Lev, Small doubling in cyclic groups, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.06.001