SMALL DOUBLING IN GROUPS WITH MODERATE TORSION

VSEVOLOD F. LEV

Abstract. We determine the structure of a finite subset A of an abelian group given that $|2A| < 3(1-\varepsilon)|A|,\ \varepsilon > 0$; namely, we show that A is contained either in a one-dimensional coset progression of size comparable with $|A|$, or in a union of fewer than ε^{-1} cosets of a finite subgroup.

The bounds $3(1-\varepsilon)|A|$ and ε^{-1} are best possible in the sense that none of them can be relaxed without tightening another one, and the estimate obtained for the size of the coset progression containing A is sharp.

In the case where the underlying group is infinite cyclic, our result reduces to the well-known Freiman's $(3n-3)$-theorem; the former thus can be considered as an extension of the latter onto arbitrary abelian groups, provided that there is "not too much torsion involved".

1. Introduction and summary of results

For subsets A and B of an additively written abelian group, by $A+B$ we denote the set of all group elements representable as $a+b$ with $a \in A$ and $b \in B$. We abbreviate $A+A$ as $2A$ and define the *doubling coefficient* of a finite, nonempty set A to be the quotient $|2A|/|A|$.

It is a basic, well-known fact that if A is a finite set of integers, then $|2A| \ge 2|A|-1$; more generally, if A and B are finite nonempty subsets of a torsion-free abelian group, then $|A+B| \ge |A|+|B|-1$. An extension of this fact onto general abelian groups with torsion is a deep result due to Kneser (see Section 3).

In another direction, Freiman [F62] has established the structure of integer sets A satisfying $|2A| \le 3|A|-3$; that is, roughly speaking, sets with the doubling coefficient smaller than 3. This result, commonly referred to as *Freiman's* $(3n-3)$*-theorem*, along with its generalizations onto distinct set summands, can be found in any standard additive combinatorics monograph; see, for instance, [G13, Theorem 7.1], [N96, Theorem 1.13], or [TV06, Theorem 5.11].

It is a difficult open problem to combine the results of Kneser and Freiman establishing the structure of sets with the doubling coefficient less than 3 in abelian groups with torsion. This paper is intended as a step towards the solution of this problem.

Our main result shows that a small-doubling set is either contained in the union of a small number of cosets of a finite subgroup, or otherwise is densely contained in a one-dimensional coset progression.

Theorem 1. *Let A be a finite subset of an abelian group G such that A cannot be covered with fewer than n cosets of a finite subgroup of G, for some real $n > 0$. If $|2A| < 3\big(1 - \frac{1}{n}\big)|A|$, then there exist an arithmetic progression $P \subseteq G$ of size $|P| \geq 3$ and a finite subgroup $K \leq G$ such that $|P+K| = |P||K|$, $A \subseteq P+K$, and $(|P|-1)|K| \leq |2A| - |A|$.*

Remark 1. The equality $|P+K| = |P||K|$ in the statements of Theorem 1 and Theorem 2 below is an easy corollary of the other assertions: if it fails, then there are two elements of P that fall into the same K-coset; hence, $P+K$ is a coset of a finite subgroup; therefore $n \leq 1$, which is inconsistent with the assumption $|2A| < 3(1-1/n)|A|$. For this reason, we can simply ignore the equality in question in the proofs of these theorems.

Remark 2. Letting $\tau = |2A|/|A|$, the conclusion $(|P|-1)|K| \leq |2A|-|A|$ can be rewritten as $|P+K| \leq (\tau-1)|A| + |K|$; the meaning of this estimate is that A is dense in $P+K$.

We derive Theorem 1 from the following, essentially equivalent, result.

Theorem 2. *Suppose that an abelian group G has the direct sum decomposition $G = \mathbb{Z} \oplus H$ with $H < G$ finite. Let $A \subseteq G$ be a finite set, and let n be number of elements of the image of A under the projection $G \to \mathbb{Z}$ along H. If $|2A| < 3\big(1 - \frac{1}{n}\big)|A|$, then there exist an arithmetic progression $P \subseteq G$ and a subgroup $K \leq H$ such that $|P+K| = |P||K|$, $A \subseteq P+K$, and $(|P|-1)|K| \leq |2A| - |A|$. Moreover, letting $\tau := |2A|/|A|$, we have $3 \leq |P| \leq (\tau-1)n+1$.*

The equality $G = \mathbb{Z} \oplus H$ means that G is the direct sum of its infinite cyclic subgroup and the subgroup H. To simplify the notation, we identify the former with the group of integers.

The following example shows that Theorems 1 and 2 are sharp in the sense that the assumption $|2A| < 3(1-\frac{1}{n})|A|$ cannot be relaxed, and the conclusion $(|P|-1)|K| \leq |2A| - |A|$ cannot be strengthened.

Example 1. Let $P := [0, l]$ and $A := \big([0, n-2] \cup \{l\}\big) + K$, where l and n are integers with $l \geq n-1 \geq 2$, and $K \leq H$; thus, $|A| = n|K|$. If $l > 2n-3$, then $|2A| = (3n-3)|K| = 3\big(1-n^{-1}\big)|A|$, while A fails to have the structure described in Theorems 1 and 2 as $|2A| - |A| = (2n-3)|K| < (|P|-1)|K|$. Thus, to conclude that a set $A \subseteq \mathbb{Z} \oplus H$ with $|2A| < 3(1-\varepsilon)|A|$ is densely contained in a coset progression, one needs to assume that A cannot be covered with fewer than ε^{-1} cosets of a finite subgroup (or make some other assumptions).

On the other hand, if $l \leq 2n-3$, then $|2A| = (l+n)|K|$; therefore, $|2A| - |A| = (|P|-1)|K|$, showing that the corresponding estimates of Theorems 1 and 2 are best possible.

Remark 3. The inequality $|P| \geq 3$ of Theorem 2 follows in fact automatically from the other assertions of the theorem. Specifically, one cannot have $|P| = 1$ because this would lead to $n = 1$, and consequently to $|2A| < 0$. One cannot have $|P| = 2$ either because this would result in $n = 2$ and $|2A| < \frac{3}{2}|A|$. The latter, in its turn, is known to imply (see, for instance, Lemma 1 below) that A is contained in a coset of a finite subgroup of G; hence, in an H-coset. This, however, contradicts the equality $n = 2$. The same applies to Theorem 1.

Similarly, the upper-bound estimate $|P| \le (\tau - 1)n + 1$ in Theorem 2 follows from

$$(\tau - 1)|A| = |2A| - |A| \ge (|P| - 1)|K| \ge (|P| - 1)\frac{|A|}{n},$$

and we thus can safely forget this estimate for the rest of the paper.

Remark 4. In the particular case where H is trivial, and A is a subset of the infinite cyclic group, Theorem 2 is equivalent to the $(3n-3)$-*theorem*, see [F62] or [N96, Theorem 1.13]. Theorem 2 thus can be considered as an extension of the $(3n-3)$-theorem onto the groups with torsion.

Remark 5. As a corollary of Theorem 2, for any finite set $A \subseteq \mathbb{Z} \oplus H$, denoting by n the size of the projection of A onto $\mathbb{Z}$ along H, we have $|2A| \ge (2 - \frac{1}{n})|A|$. This follows by observing that, assuming the opposite,

$$\left(1 - \frac{1}{n}\right)|A| > |2A| - |A| \ge (|P| - 1)|K| \ge (n - 1)|K| \ge \left(1 - \frac{1}{n}\right)|A|.$$

We remark that, while the resulting estimate $|2A| \ge (2 - \frac{1}{n})|A|$ may not be completely trivial, it is not particularly deep either, and can be proved independently of Theorem 2, with a simple combinatorial reasoning in the spirit of the proof of Lemma 6 in Section 4.

It might be possible to use our method to treat sumsets of the form $A+B$ with $A \ne B$, and in particular to prove analogues of Theorems 1 and 2 for the difference sets $A - A$. We will not pursue this direction further in the present paper.

Theorem 2 can be compared against the following result of Balasubramanian and Pandey, which is an elaboration on an earlier result of Deshouillers and Freiman [DF86, Theorem 2].

Theorem 3 (Balasubramanian-Pandey [BP18, Theorem 5])**.** *Let $d \ge 2$ be an integer and suppose that $A \subseteq \mathbb{Z} \oplus (\mathbb{Z}/d\mathbb{Z})$ is a finite set with $|2A| < 2.5|A|$. For $z \in \mathbb{Z}$, let $A_z := A \cap (z + \mathbb{Z}/d\mathbb{Z})$, and let $B := \{z \in \mathbb{Z} \colon A_z \ne \varnothing\}$. If $|B| \ge 6$ and $\gcd(B - B) = 1$, then there exists a subgroup $K \le \mathbb{Z}/d\mathbb{Z}$ and elements $x, y \in \mathbb{Z}/d\mathbb{Z}$ such that, letting $l := \max B - \min B$, we have*

i) *$A \subseteq \{(b, bx + y) \colon b \in B\} + K$;*
ii) *there exists $b \in B$ with $|A_b| \ge \frac{2}{3}|K|$;*
iii) *$l|K| \le |2A| - |A|$.*

Balasubramanian and Pandey also include the estimate $l < \frac{3}{2}|B|$ into the statement, but in fact this estimate follows easily from i) and iii):

$$l|K| < 2.5|A| - |A| = \frac{3}{2}\,|A| \le \frac{3}{2}\,|B||K|.$$

In the same vein, i) and iii) imply an estimate which is only slightly weaker than ii): namely, by iii) we have $l|K| \le (\tau-1)|A|$; therefore, by averaging, there exists an element $b \in B$ with

$$|A_b| \ge \frac{|A|}{|B|} \ge \frac{(\tau-1)|A|}{(\tau-1)(l+1)} \ge \frac{l}{l+1}\frac{|K|}{\tau-1} > \frac{2}{3}\Big(1 - \frac{1}{l+1}\Big)\,|K|,$$

where $\tau = |2A|/|A|$. To match the Balasubramanian-Pandey estimate $\max_{b\in B}|A_b| \ge \frac{2}{3}|K|$, we prove in Section 2 the following theorem showing (subject to Theorem 2) that if n is sufficiently large, then there exists a K-coset containing at least $\frac{|K|}{\tau-1}$ elements of A.

Theorem 4. *Suppose that G, H, A, n, P, and K are as in Theorem 2, and let $\tau := |2A|/|A|$. If $n \ge \frac{4\tau-6}{(\tau-2)(3-\tau)}$, then there exists a K-coset containing at least $\frac{|K|}{\tau-1}$ elements of A.*

Compared to Theorem 3, our Theorem 2 allows the doubling coefficient to be as large as $3 - o(1)$ (instead of 2.5), which is best possible, as shown above. Besides, Theorem 2 applies to the groups $\mathbb{Z} \oplus H$ with H not necessarily cyclic, and makes no assumptions about the projection of A onto the torsion-free component.

The layout of the remaining part of the paper is as follows. In Section 2 we deduce Theorems 1 and 4 from Theorem 2, allowing us to concentrate on the proof of the latter theorem for the rest of the paper. In Section 3 we collect some general results needed for the proof. In Section 4 we prove some basic estimates related to the particular settings of Theorem 2 (in contrast with Section 3 where the results are of general nature). Section 5 contains two lemmas which, essentially, establishe the special cases of Theorem 2 where the set A can be partitioned into two or three "additively independent" subsets. Finally, we prove Theorem 2 in Section 6.

2. Deduction of Theorems 1 and 4 from Theorem 2

Proof of Theorem 1. Let A be a finite subset of an abelian group G such that A cannot be covered with fewer than n cosets of a finite subgroup of G, while

$$|2A| < 3\Big(1 - \frac{1}{n}\Big)|A|, \tag{1}$$

with a real $n > 0$. We want to prove, assuming Theorem 2, that there exist an arithmetic progression $P \subseteq G$ and a finite subgroup $K \le G$ such that $A \subseteq P + K$ and $(|P|-1)|K| \le |2A| - |A|$. As explained in Section 1 (Remarks 1 and 3), the progression will satisfy $|P| \ge 3$ and $|P + K| = |P||K|$.

Without loss of generality, we assume that G is generated by A. By the fundamental theorem of finitely generated abelian groups, there is then an integer $r \geq 0$ and a finite subgroup $H \leq G$ such that $G \cong \mathbb{Z}^r \oplus H$. Indeed, we have $r \geq 1$ as otherwise G would be finite; hence, A would be contained in just one single finite coset (the group G itself), forcing $n \leq 1$ and thus contradicting the small-doubling assumption (1).

Let $G' := \mathbb{Z} \oplus H$. To avoid confusion, throughout the proof we use the direct product notation for the elements of the groups G and G'.

Fix an integer $M > 0$ divisible by all positive integers up to $|2A|$, and consider the mapping $\psi\colon G \to G'$ defined by

$$\psi(x_1, \dots, x_r, h) := (x_1 + Mx_2 + \dots + M^{r-1}x_r, h); \quad x_1, \dots, x_r \in \mathbb{Z},\ h \in H.$$

If M is large enough (as we assume below), then distinct elements of A have distinct images under ψ, and similarly for $2A$; consequently, writing $A' := \psi(A)$, we have $|A'| = |A|$ and $|2A'| = |2A|$, whence

$$|2A'| < 3\Big(1 - \frac{1}{n}\Big)|A'|$$

(we implicitly use here the equality $2\psi(A) = \psi(2A)$).

Denote by m the number of elements of the projection of A onto the first (torsion-free) component of G. If M is sufficiently large, then m is also the number of elements of the projection of A' onto the first component of G'. Since A is not contained in a union of fewer than n cosets, we have $m \geq n$, resulting in

$$|2A'| < 3\Big(1 - \frac{1}{m}\Big)|A'|.$$

Applying Theorem 2, we conclude that there exist a finite arithmetic progression $P' \subseteq G'$ and a subgroup $K \leq H$ such that $A' \subseteq P' + K$ and

$$(|P'| - 1)|K| \leq |2A'| - |A'| = |2A| - |A|. \tag{2}$$

We assume that P' is the shortest progression possible with $A' \subseteq P' + K$.

Write $N := |P'| - 1$, and let $c \in G'$ and $(d, h) \in G'$ denote the initial term and the difference of the progression P', respectively; thus,

$$P' = c + \{j(d, h)\colon j \in [0, N]\}; \quad d \in \mathbb{Z},\ h \in H.$$

Notice that $d \neq 0$, as otherwise we would have $A' \subseteq P' + K \subseteq c + H$, as a result of which A', and therefore also A, would be contained in a single H-coset.

Since P' is the shortest possible progression with $A' \subseteq P' + K$, there are elements $(a_1, \dots, a_r, f), (b_1, \dots, b_r, g) \in A$ such that $\psi(a_1, \dots, a_r, f) = c$ and $\psi(b_1, \dots, b_r, g) = c + N(d, h)$; consequently,

$$(b_1 - a_1) + M(b_2 - a_2) + \dots + M^{r-1}(b_r - a_r) = Nd.$$

Since $N = |P'| - 1 \leq |2A| - |A| < |2A|$, and recalling that M was chosen to be divisible by all poitive integers up to $|2A|$, we have $N \mid M$, and therefore $b_1 - a_1$ is a multiple of

N. Thus

$$d = (b_1 - a_1)N^{-1} + MN^{-1}(b_2 - a_2) + \dots + M^{r-1}N^{-1}(b_r - a_r), \tag{3}$$

where all summands in the right-hand side are integers.

We know that for any element $(\alpha_1, \dots, \alpha_r, \eta) \in A$, there exist $j \in [0, N]$ and $k \in K$ such that

$$\begin{aligned}(\alpha_1 + \dots + M^{r-1}\alpha_r, \eta) &= c + j(d, h) + (0, k) \\ &= (a_1 + \dots + M^{r-1}a_r, f) + j(d, h) + (0, k).\end{aligned}$$

Recalling (3), we obtain

$$(\alpha_1 - a_1) + \dots + M^{r-1}(\alpha_r - a_r) = jd = j(b_1 - a_1)N^{-1} + \dots + jM^{r-1}(b_r - a_r)N^{-1};$$

that is,

$$(\alpha_1 - a_1)N + \dots + M^{r-1}(\alpha_r - a_r)N = j(b_1 - a_1) + \dots + jM^{r-1}(b_r - a_r) \tag{4}$$

with $j \in [0, N]$ depending on the element $(\alpha_1, \dots, \alpha_r, \eta) \in A$. (Notice that N depends on M, but is bounded: $N \le N|K| \le |2A| - |A|$ by (2).) Choosing M sufficiently large, from (4) we get

$$(\alpha_i - a_i)N = j\,(b_i - a_i),\ 1 \le i \le r, \tag{5}$$

showing that $(b_i - a_i)j$ is divisible by N. Using again the fact that P' is the shortest possible progression with $A' \subseteq P' + K$, we conclude that the possible values of j that can emerge from different elements $(\alpha_1, \dots, \alpha_r, \eta) \in A$ are coprime. Hence, there is a linear combination of these values, with integer coefficients, which is equal to 1. Consequently, from (5), all numbers $(b_i - a_i)N^{-1}$, $1 \le i \le r$, are integers, and then, by (5) again,

$$(\alpha_1, \dots, \alpha_r, \eta) = (a_1, \dots, a_r, f) + j((b_1 - a_1)N^{-1}, \dots, (b_r - a_r)N^{-1}, h) + (0, \dots, 0, k).$$

This shows that $A \subseteq P + K$, where $P \subseteq G$ is the $(N+1)$-term arithmetic progression with the initial term $(a_1, \dots, a_r, f)$ and the difference $((b_1 - a_1)N^{-1}, \dots, (b_r - a_r)N^{-1}, h)$. Finally, by (2),

$$|2A| - |A| = |2A'| - |A'| \ge (|P'| - 1)|K| = (|P| - 1)|K|.$$

$\square$

Proof of Theorem 4. Let B denote the projection of A onto $\mathbb{Z}$ along H; thus, $|P| \ge |B| = n$, with equality if and only if B is an arithmetic progression. If B is *not* an arithmetic progression then, indeed, $|P| \ge n+1$ and, by averaging, there is a K-coset containing at least

$$\frac{|A|}{n} \ge \frac{|A|}{|P| - 1} \ge \frac{|K|}{\tau - 1}$$

elements of A (the last inequality following from the estimate $|2A|-|A|\ge(|P|-1)|K|$ of Theorem 2). Suppose thus that B is a progression and, consequently, $|P|=n$ and $|2A|-|A|\ge(n-1)|K|$, whence

$$|A|\ge\frac{n-1}{\tau-1}\,|K|.$$

Let

$$M:=\max\{|A\cap(g+K)|\colon g\in P\},\ \mu:=|M|/|K|,$$
$$P_0:=\big\{g\in P\colon |A\cap(g+K)|\le\frac12\,|K|\big\},\ P_1:=P\setminus P_0,\ \text{and } m:=|P_0|.$$

Notice that $M>\frac12\,|K|$ as otherwise we would have

$$\frac12\,|K|\ge M\ge\frac{|A|}{n}\ge\Big(1-\frac1n\Big)\frac{|K|}{\tau-1},$$

which is easily seen to contradict $\tau<3(1-\frac1n)$. Therefore P_1 is nonempty, and $m<n$.

We want to show that $\mu\ge\frac{1}{\tau-1}$. Suppose for a contradiction that this is wrong. Since $P+K$ is a union of n pairwise disjoint K-cosets, of which m contain at most $\frac12|K|$ elements of A, and the remaining $n-m$ contain at most M elements each, we have

$$\frac{n-1}{\tau-1}\,|K|\le|A|\le m\cdot\frac12|K|+(n-m)\cdot M, \tag{6}$$

leading to

$$\frac{n-1}{\tau-1}\le\frac12\,m+(n-m)\mu<\frac12\,m+\frac{n-m}{\tau-1},$$

where the last inequality follows from the assumption $\mu<1/(\tau-1)$. This simplifies to the estimate

$$m<\frac{2}{3-\tau} \tag{7}$$

which we will need shortly.

The set $2P_1+K$ is a union of $|2P_1|\ge2|P_1|-1=2(n-m)-1$ distinct K-cosets contained in $2A$ by the pigeonhole principle. The set $P+P_1+K$ is a union of $|P+P_1|\ge|P|+|P_1|-1=2n-m-1$ distinct K-cosets, each of them containing at least $\frac12\,|K|$ elements of $2A$. We thus can find $2n-2m-1$ cosets represented by the elements of $2P_1$, and then m more cosets represented by the elements of $P+P_1$. Altogether, we get $2n-m-1$ cosets containing at least

$$(2n-2m-1)|K|+\frac12\,|K|m=\Big(2n-\frac32\,m-1\Big)|K|$$

elements of $2A$. It follows that

$$2n-\frac32\,m-1\le\frac{|2A|}{|K|}=\tau\frac{|A|}{|K|}\le\Big(\frac12m+(n-m)\mu\Big)\tau<\Big(\frac12m+\frac{n-m}{\tau-1}\Big)\tau,$$

cf. (6). Rearranging the terms gives

$$\Big(1-\frac{1}{\tau-1}\Big)n<\Big(\frac32+\frac\tau2-\frac{\tau}{\tau-1}\Big)m+1;$$

that is, using (7),

$$\frac{\tau-2}{\tau-1}n < \frac{\tau^2-3}{2(\tau-1)}m+1 < \frac{\tau^2-3}{(\tau-1)(3-\tau)}+1$$

leading to

$$n < \frac{\tau^2-3}{(\tau-2)(3-\tau)} + \frac{\tau-1}{\tau-2} = \frac{4\tau-6}{(\tau-2)(3-\tau)},$$

and the assertion follows. □

The rest of the paper is devoted to the proof of Theorem 2.

3. General results

In this section we collect some general results valid in any abelian group, regardless of the particular settings of Theorem 2.

For a subset S of an abelian group, let $\pi(S)$ denote the *period (stabilizer)* of S; that is, $\pi(S)$ is the subgroup consisting of all those group elements g with $S+g=S$. The set S is called *aperiodic* or *periodic* according to whether $\pi(S)$ is or is not the zero subgroup.

We start with a basic theorem due to Kneser which is heavily used in our argument; see, for instance, [G13, Theorem 6.1], [N96, Theorem 4.1], or [TV06, Theorem 5.5].

Theorem 5 (Kneser, [Kn53, Kn55])**.** *If B and C are finite, non-empty subsets of an abelian group with*

$$|B+C| \le |B|+|C|-1,$$

then letting $L:=\pi(B+C)$ we have

$$|B+C| = |B+L|+|C+L|-|L|.$$

Theorem 5 will be referred to as *Kneser's theorem.*

Since, in the notation of Kneser's theorem, we have $|B+L|\ge|B|$ and $|C+L|\ge|C|$, the theorem shows that $|B+C|\ge|B|+|C|-|L|$, leading to

Corollary 1. *If B and C are finite, non-empty subsets of an abelian group, such that $|B+C|<|B|+|C|-1$, then $B+C$ is periodic.*

The following lemma is well known, but tracing back its origin is hardly possible. (The subtler noncommutative version of the lemma, to our knowledge, has first appeared in [F73], and then in [O75].)

Lemma 1. *Let B be a finite subset of an abelian group. If $|2B|<\frac{3}{2}|B|$, then there is a subgroup L such that $B-B=L$, and $2B$ is an L-coset (as a result of which B is contained in a unique L-coset).*

We give a somewhat nonstandard, self-contained proof of the lemma.

Proof of Lemma 1. For a group element g, denote by $r(g)$ the number of representations of g as a difference of two elements of B. If $g \in B - B$, then choosing arbitrarily $b, c \in B$ with $g = b - c$ we get

$$r(g) = |(b + B) \cap (c + B)| \geq 2|B| - |2B| > \frac{1}{2}\,|B|.$$

By the pigeonhole principle, for any $g_1, g_2 \in B - B$ there are representations $g_1 = b_1 - c_1,\ g_2 = b_2 - c_2$ with $c_1 = c_2$; consequently, $g_1 - g_2 = b_1 - b_2 \in B - B$, showing that $L := B - B$ is a subgroup. Clearly, B is contained in a unique L-coset.

As we have shown, for every element $g \in L = B - B$ we have $r(g) > \frac{1}{2}\,|B|$. As a result,

$$|B|(|B| - 1) = \sum_{g \in L \setminus \{0\}} r(g) > \frac{1}{2}\,|B| \cdot (|L| - 1),$$

implying $|B| > \frac{1}{2}\,|L|$. Recalling that B is contained in a unique L-coset, and using the pigeonhole principle again, we conclude that $2B$ is an L-coset. □

Lemma 2. *Suppose that B is a subset of an abelian group with $0 \in B$. If $N \geq 2$ is an integer such that $|B| = N + 1$ and $|2B| = 2N + 1$ (thus $|2B \setminus B| = N$), then one of the following holds:*

i) *there exist $b_1, \dots, c_N \in B$ such that $2B \setminus B = \{b_1 + c_1, \dots, b_N + c_N\}$, and every element of B appears among $b_1, \dots, c_N$ not more than N times;*
ii) *there is a subgroup L with $|L| = N$ and a group element g with $2g \notin L$ such that $B = L \cup \{g\}$. (In this case there exist $b_1, \dots, c_N \in B$ such that $2B \setminus B = \{b_1 + c_1, \dots, b_N + c_N\}$, and every element of B appears among $b_1, \dots, c_N$ exactly once, except that 0 does not appear at all, and g appears $N + 1$ times.)*
iii) *$N = 2$ and there is a subgroup L with $|L| = 2$ and a group element g with $2g \notin L$ such that $B = (g + L) \cup \{0\}$.*
iv) *$N = 2$ and $B = \{0, g, 2g\}$ where g is a group element of order at least 5.*

Proof. Leaving the case $N = 2$ to the reader (hint: write $B = \{0, b, g\}$ and consider two cases: $b + g = 0$ and $b + g \neq 0$), we confine ourselves to the general case where $N \geq 3$.

To begin with, we choose $b_1, \dots, c_N \in B$ arbitrarily to have $2B \setminus B = \{b_1 + c_1, \dots, b_N + c_N\}$. Since all sums $b_i + c_i$ are distinct, for any $g \in B$ there is at most one index $i \in [1, N]$ with $b_i = c_i = g$. Consequently, if there is an element $g \in B$ which appears at least $N + 1$ times among $b_1, \dots, c_N$ (as we now assume), then in fact it appears $N + 1$ times exactly: namely, $b_i = c_i = g$ for some $i \in [1, N]$ and, besides, for each $j \neq i$, exactly one of b_j and c_j is equal to g. Redenoting, we assume that $b_1 = c_1 = \dots = c_N = g$.

Notice that $2g = b_1 + c_1 \in 2B \setminus B$ along with $0 \in B$ show that $g \neq 0$. Write $B_0 := B \setminus \{0\}$ and $B_g := B \setminus \{g\}$. Since the sums $b_i + c_i = b_i + g$ are pairwise distinct, so are the elements $b_1, \dots, b_N \in B$. Moreover, $b_1, \dots, b_N$ are nonzero in view of $b_i + g = b_i + c_i \notin B$ and $g \in B$, and since $|B_0| = N$, it follows that $\{b_1, \dots, b_N\} = B_0$; consequently, $2B \setminus B = g + B_0$.

If there exist some $b, c \in B_g$ with $b+c \notin B$, then choosing $i \in [1, N]$ with $b_i + g = b + c$ and replacing b_i with b and c_i with c in the $2N$-tuple $(b_1, \dots, c_N)$, we get another $2N$-tuple $(b'_1, \dots, c'_N)$ such that the sums $b'_i + c'_i$ list all elements of $2B \setminus B$. If $i \in [2, N]$, then g appears exactly N times among $b'_1, \dots, c'_N$, so that no other element of B can appear $N+1$ or more times. Similarly, if $i = 1$, then in view of $c'_2 = \dots = c'_N = g$, and since all sums $b'_2 + c'_2, \dots, b'_N + c'_N$ are pairwise distinct, every element $b \in B_g$ appears at most $3 < N+1$ times among $b'_1, \dots, c'_N$. Thus, the assertion holds true in this case.

Suppose therefore that $b, c \in B_g$ with $b + c \notin B$ do not exist; that is, $2B_g \subseteq B$. This gives $|2B_g| \le |B_g| + 1$; hence, by Lemma 1 and in view of $0 \in B_g$, the set $L := B_g - B_g = 2B_g$ is a subgroup. Furthermore, since $B_g \subseteq 2B_g = L$ and $|B_g| \ge |2B_g| - 1 = |L| - 1$, we have either $B_g = L$, or $B_g = L \setminus \{l\}$ with some $l \in L$, $l \ne 0$. In the former case $B = L \cup \{g\}$ and $2B = L \cup (g+L) \cup \{2g\}$, with $2g \notin L$ in view of $|2B| = 2N+1 = 2|B|-1 = 2|L|+1$. The latter case where $B_g = L \setminus \{l\}$ is in fact impossible as in this case we would have $l \ne g$ (otherwise $B = L$ and then $|2B| = |B|$) and consequently $l \in 2B_g \setminus B$, contradicting the present assumption $2B_g \subseteq B$. □

Lemma 3. *Suppose that Δ is a subgroup, and that B and C are subsets of an abelian group. Let φ_Δ denote the canonical homomorphism onto the quotient group. If $C + \Delta = C$, then $\varphi_\Delta(B \cap C) = \varphi_\Delta(B) \cap \varphi_\Delta(C)$; consequently, $\varphi_\Delta(B \cap C) = \varphi_\Delta(C)$ is equivalent to $\varphi_\Delta(C) \subseteq \varphi_\Delta(B)$.*

We omit the proof which is an easy exercise in basic algebra.

Lemma 4. *If G is an abelian group with the direct sum decomposition $G = \mathbb{Z} \oplus H$, then every subgroup $F < G$ is of the form $F = \langle g \rangle + K$, where $K = F \cap H$ and $g \in G$.*

Proof. The assertion is immediate if $F \le H$; assume therefore that $F \not\le H$. In this case the projection of F onto $\mathbb{Z}$ along H is a non-zero subgroup of $\mathbb{Z}$; let d be its generator. For $k \in \mathbb{Z}$, the "slice" $F(k) := F \cap (k + H)$ is non-empty if and only if $d \mid k$. Furthermore, for any k_1, k_2 divisible by d, and any fixed $d \in F(k_2 - k_1)$, we have $F(k_1) + d \subseteq F(k_2)$. This shows that all slices $F(k)$ with k divisible by d are actually translates of each other; hence, each of them is a coset of the subgroup $F(0) = K$.

Fix arbitrarily $g \in F(d)$. For any integer k divisible by d, we have $(k/d)g \in F \cap (k + H) = F(k)$. It follows that $F(k) = (k/d)g + K$ for any integer k with $d \mid k$. As a result, $F = \langle g \rangle + K$. □

We need the following lemma in the spirit of [BP18]. The idea behind the lemma can in fact be traced back to [L98], at least in the case where $|B| = |C|$.

Lemma 5. *Suppose that B and C are finite, nonempty integer sets, and write $m := |B|$ and $B = \{b_1, \dots, b_m\}$, where the elements of B are numbered in an arbitrary order. Then there exist $c_2, \dots, c_m \in C$ such that the sums $b_2 + c_2, \dots, b_m + c_m$ are distinct from each other and from the elements of the set $b_1 + C$.*

Proof. The proof follows the line of reasoning of [BP18].

Let $n := |C|$ and consider the family of $m+n-1$ sets

$$\begin{aligned} &b_1+C,\dots,b_1+C \quad (n \text{ sets})\\ &b_2+C,\dots,b_m+C \quad (m-1 \text{ sets}). \end{aligned}$$

We use the Hall marriage theorem to show that this set family has a system of distinct representatives; clearly, this will imply the result.

Suppose thus that for some $1 \le k \le m+n-1$ we are given a subsystem $\mathcal{S}$ of k sets from among those listed above, and show, to verify the hypothesis of Hall's theorem, that $|\cup_{S\in\mathcal{S}} S| \ge k$. Let $B' \subseteq B$ consist of all those elements $b \in B$ such that at least one of the sets in $\mathcal{S}$ has the form $b+C$. Then $\cup_{S\in\mathcal{S}} S = B'+C$ and we thus want to show that $|B'+C| \ge k$. Since $|B'+C| \ge |B'|+|C|-1$, it suffices to show that $|B'|+n-1 \ge k$. Indeed, this inequality is trivial for $k \le n$, while for $k \ge n$ it becomes evident upon writing $k = n+r$ $(r \ge 0)$ and observing any $n+r$ sets under consideration determine at least $r+1 = k-n+1$ elements b_i. ☐

Corollary 2. *Suppose that the abelian group G has the direct sum decomposition $G = \mathbb{Z} \oplus H$ with $H < G$ finite. Let B, C be finite, nonempty subsets of G. If m and n denote the sizes of the images of B and C, respectively, under the projection $G \to \mathbb{Z}$ along H, then*

$$|B+C| \ge \left(1+\frac{n-1}{m}\right)|B|.$$

Proof. Denote by ψ the projection in question, and write $\psi(B) := \{b_1,\dots,b_m\}$, where b_1 is chosen so that $|\psi^{-1}(b_1)\cap B| \ge |B|/m$; otherwise, the elements of $\psi(B)$ are numbered arbitrarily. Let $B_i := \psi^{-1}(b_i)\cap B$ $(1 \le i \le m)$. By Lemma 5 applied to the sets $\psi(B)$ and $\psi(C)$, there are (not necessarily distinct) elements $c_2,\dots,c_m \in \psi(C)$ such that all sums $b_2+c_2,\dots,b_m+c_m$ are distinct from each other and from the elements of the set $b_1+\psi(C)$. Consequently, the sumsets $B_2+(\psi^{-1}(c_2)\cap C),\dots,B_m+(\psi^{-1}(c_m)\cap C)$ are disjoint from each other and from each of the n sumsets $B_1+(\psi^{-1}(c)\cap C),\ c \in \psi(C)$. As a result,

$$\begin{aligned} |B+C| &\ge \sum_{i=2}^{m} |B_i+(\psi^{-1}(c_i)\cap C)| + \sum_{c\in\psi(C)} |B_1+(\psi^{-1}(c)\cap C)|\\ &\ge |B_2|+\dots+|B_m|+n|B_1| = |B|+(n-1)|B_1| \ge |B|+\frac{n-1}{m}|B|. \end{aligned}$$

☐

4. Basic Estimates

We collect in this section some basic estimates used in the proof of Theorem 2.

Suppose that A is a finite subset of the group $G = \mathbb{Z}\oplus H$, where $H < G$ is finite abelian. For each $z \in \mathbb{Z}$, let $A_z := A\cap(z+H)$, and write $B := \{z \in \mathbb{Z}\colon A_z \ne \varnothing\}$; that is, B is the image of A under the projection of G onto $\mathbb{Z}$ along H. Suppose, furthermore, that $\min B = 0$, $\max B = l > 0$, $0 \in A_0$, and $\delta \in A_l$. Finally, write $n := |B|$, $\sigma := |A_0| + |A_l|$, and $A^* := A_0 \cap (A_l - \delta)$; thus, for instance,

$$\sigma \ge 2|A^*|. \tag{8}$$

Lemma 6. *We have* $|2A| + |A^*| \ge \sigma n$.

Proof. Considering the projections of the "slices" A_z onto $\mathbb{Z}$, we get

$$\begin{aligned} |2A| &\ge \sum_{\substack{z\in B\\ z<l}} |A_0 + A_z| + |A_0 + A_l| + \sum_{\substack{z\in B\\ z>0}} |A_z + A_l| \\ &\ge (n-1)|A_0| + |A_0 + A_l| + (n-1)|A_l|. \end{aligned}$$

To estimate the sum $A_0 + A_l$ we notice that both $A_0 + \delta$ and A_l are subsets of $A_0 + A_l$, whence

$$|A_0 + A_l| \ge |(A_0 + \delta) \cup A_l| = (|A_0| + |A_l|) - |A^*|.$$

Combining these estimates yields the sought inequality. □

Corollary 3. *Let* $\tau := |2A|/|A|$. *If* $\tau < 3(1 - \frac{1}{n})$, *then*

$$(3-\tau)(\tau|A| + |A^*|) > 3\sigma, \tag{9}$$

$$3|A| - |2A| > \sigma, \tag{10}$$

and

$$|2A| < 3|A| - 2|A^*|. \tag{11}$$

Proof. To prove (9), we multiply the inequality of the lemma by the inequality $3 - \tau > \frac{3}{n}$ following from $\tau < 3(1 - \frac{1}{n})$, and then substitute $|2A| = \tau|A|$.

For (10), we use (9) and (8) to get

$$\begin{aligned} 3|A| - |2A| = (3-\tau)|A| &> \frac{1}{\tau}\left(3\sigma - (3-\tau)|A^*|\right) = \frac{3}{\tau}\sigma - \left(\frac{3}{\tau} - 1\right)|A^*| \\ &\ge \frac{3}{\tau}\sigma - \left(\frac{3}{\tau} - 1\right)\cdot\frac{\sigma}{2} = \frac{1}{2}\left(\frac{3}{\tau} + 1\right)\sigma > \sigma. \end{aligned}$$

Finally, (11) follows from (10) and (8):

$$|2A| < 3|A| - \sigma \le 3|A| - 2|A^*|.$$

□

5. Two special cases

In this section we prove two lemmas which, essentially, establish the special cases of Theorem 2 where the set A splits into two or three "additively independent" parts.

Lemma 7. *Suppose that the abelian group G has the direct sum decomposition $G = \mathbb{Z} \oplus H$ with $H < G$ finite. Let $A_1, A_2 \subset G$ be finite, nonempty subsets of G, and for $i \in \{1, 2\}$ let $n_i := |\psi(A_i)|$, where $\psi\colon G \to \mathbb{Z}$ is the projection along H. Then*

$$|2A_1| + |A_1 + A_2| + |2A_2| \geq 3\Big(1 - \frac{1}{n_1 + n_2}\Big)(|A_1| + |A_2|).$$

Example 2. If, for $i \in \{1, 2\}$, we let $A_i = P_i + K$, where P_i are arithmetic progressions with the same difference not contained in H, and where $K \leq H$, then $n_i = |P_i|$ and

$$|2A_1| + |A_1 + A_2| + |2A_2| = 3(|P_1| + |P_2| - 1)|K| = 3\Big(1 - \frac{1}{n_1 + n_2}\Big)(|A_1| + |A_2|).$$

This shows that the estimate of the lemma is best possible.

Proof of Lemma 7. Recall that for a subset S of an abelian group, by $\pi(S)$ we denote the period of S; see Section 3.

For $i \in \{1, 2\}$, we have $\pi(2A_i) \leq H$ (as $2A_i$ are finite), and $|\psi(2A_i)| \geq 2n_i - 1$, whence

$$|2A_i| \geq (2n_i - 1)\,|\pi(2A_i)|.$$

On the other hand, by Kneser's theorem,

$$|2A_i| \geq 2|A_i| - |\pi(2A_i)|.$$

Multiplying the latter inequality by $2n_i - 1$ and adding the former to the result (to cancel out the term $|\pi(2A_i)|$) we get

$$|2A_i| \geq \Big(2 - \frac{1}{n_i}\Big)|A_i|, \quad i \in \{1, 2\}. \tag{12}$$

Similarly, letting $n := n_1 + n_2$ and observing that

$$|\psi(A_1 + A_2)| = |\psi(A_1) + \psi(A_2)| \geq n_1 + n_2 - 1 = n - 1,$$

we get $|A_1 + A_2| \geq (n - 1)|\pi(A_1 + A_2)|$ and $|A_1 + A_2| \geq |A_1| + |A_2| - |\pi(A_1 + A_2)|$, implying

$$|A_1 + A_2| \geq \Big(1 - \frac{1}{n}\Big)(|A_1| + |A_2|). \tag{13}$$

On the other hand, by Corollary 2

$$|A_1 + A_2| \geq \frac{n-1}{n_1}\,|A_1| \tag{14}$$

and

$$|A_1 + A_2| \geq \frac{n-1}{n_2}\,|A_2|. \tag{15}$$

Taking the sum of (13), (14), and (15) with the weights $\frac{n-3}{n-1}$, $\frac{1}{n-1}$, and $\frac{1}{n-1}$, respectively, we get

$$|A_1+A_2| \ge \left(1-\frac{3}{n}\right)(|A_1|+|A_2|)+\frac{|A_1|}{n_1}+\frac{|A_2|}{n_2},$$

and taking the sum of this resulting inequality with the inequalities (12) yields the desired estimate. □

Lemma 8. *Suppose that the abelian group G has the direct sum decomposition $G = \mathbb{Z}\oplus H$ with $H<G$ finite. Let $A_1, A_2, A_3 \subset G$ be finite, nonempty subsets of G, and for $i\in\{1,2,3\}$ let $n_i := |\psi(A_i)|$, where $\psi\colon G\to\mathbb{Z}$ is the projection along H. If $n_2\ge 2$, then*

$$\begin{aligned}|2A_1|+|2A_2|+|2A_3|+|A_1+A_2|+|A_2+A_3|& \\ \ge 3\Big(1-\frac{1}{n_1+n_2+n_3}\Big)&(|A_1|+|A_2|+|A_3|).\end{aligned}$$

The obvious modification of Example 2 shows that, in the absence of additional information, the estimate of the lemma is best possible.

Proof of Lemma 8. We argue in terms of the quantities $c_i := |A_i|/n_i$, $i\in\{1,2,3\}$. Reusing (14) and (15), and writing $n := n_1+n_2+n_3$, it suffices to prove that

$$\begin{aligned}&(2n_1-1)c_1+(2n_2-1)c_2+(2n_3-1)c_3\\ &\qquad +(n_1+n_2-1)\max\{c_1,c_2\}+(n_2+n_3-1)\max\{c_2,c_3\}\\ &\qquad\qquad \ge 3\Big(1-\frac{1}{n}\Big)(n_1c_1+n_2c_2+n_3c_3);\end{aligned}$$

equivalently,

$$\begin{aligned}&(n_1+n_2-1)\max\{c_1,c_2\}+(n_2+n_3-1)\max\{c_2,c_3\}\\ &\qquad \ge c_1+c_2+c_3+\Big(1-\frac{3}{n}\Big)(n_1c_1+n_2c_2+n_3c_3). \qquad (16)\end{aligned}$$

Let

$$\lambda_i := \frac{n+(n-3)n_i}{(n_i+n_2-1)n}, \quad i\in\{1,3\}.$$

It is easily verified that $\lambda_i\in[0,1]$, whence $\max\{c_i,c_2\}\ge\lambda_ic_i+(1-\lambda_i)c_2$. Therefore,

$$\begin{aligned}(n_1+n_2-1)&\max\{c_1,c_2\}+(n_2+n_3-1)\max\{c_2,c_3\}\\ &\ge \frac{1}{n}(n+(n-3)n_1)c_1+\frac{1}{n}(n+(n-3)n_3)c_3+tc_2\\ &=(c_1+c_3)+\Big(1-\frac{3}{n}\Big)(n_1c_1+n_3c_3)+tc_2, \qquad (17)\end{aligned}$$

where

$$\begin{aligned} t &= (n_1+n_2-1)+(n_2+n_3-1)-\frac{1}{n}\big((n+(n-3)n_1)+(n+(n-3)n_3)\big) \\ &= (n+n_2-2)-\frac{1}{n}\left(n^2-n-(n-3)n_2)\right) \\ &= n_2-1+\left(1-\frac{3}{n}\right)n_2 \\ &\geq 1+\left(1-\frac{3}{n}\right)n_2. \end{aligned}$$

Along with (17), this readily gives (16).

□

6. Proof of Theorem 2

We recall that A is a finite subset of the abelian group $G=\mathbb{Z}\oplus H$, where $H\leq G$ is finite. Assuming that $|2A|<3(1-\frac{1}{n})|A|$, where n is the number of elements in the image of A under the projection $G\to\mathbb{Z}$ along H, we want to show that there exist an arithmetic progression $P\subseteq G$ and a subgroup $K\leq H$ such that $A\subseteq P+K$ and $(|P|-1)|K|\leq|2A|-|A|$. As shown in Section 1, the estimates $3\leq|P|\leq(\tau-1)n+1$ and the equality $|P+K|=|P||K|$ follow automatically and we disregard them for the rest of the proof. Here and throughout the proof, τ is the doubling coefficient of A defined by $|2A|=\tau|A|$, so that $\tau<3(1-\frac{1}{n})$.

Let $\psi\colon G\to\mathbb{Z}$ be the projection mentioned in the previous paragraph. Without loss of generality we assume that $0\in A$ and $\min\psi(A)=0$, and we let $l:=\max\psi(A)$; thus, $A\cap(z+H)=\varnothing$ for $z<0$ and also for $z>l$, while the sets $A_0:=A\cap H$ and $A_l:=A\cap(l+H)$ are nonempty.

Fix arbitrarily an element $\delta\in A_l$, and let $A^*:=A_0\cap(A_l-\delta)$ and $\sigma:=|A_0|+|A_l|$. Notice that $0\in A^*$, $\sigma\geq 2|A^*|$, and $|A_0\cup(A_l-\delta)|=\sigma-|A^*|$.

For a subgroup $L\leq G$, by φ_L we denote the canonical homomorphism of G onto the quotient group G/L. Let $\Delta:=\langle\delta\rangle\leq G$. We adopt a special notation for the homomorphism φ_Δ, which plays a particularly important role in our argument: whenever g denotes an element of G, by $\overline{g}$ we denote the image of g under φ_Δ, and similarly for sets: $\overline{S}=\varphi_\Delta(S),\ S\subseteq G$. Thus, for instance, $\overline{A}=\varphi_\Delta(A)$ and $\overline{2A}=\varphi_\Delta(2A)=2\overline{A}$.

To make the proof easier to follow, we split it into several parts.

6.1. **Deficiency and the induction framework.** We use induction on $|H|$, the base case $|H|=1$ being Freiman's $(3n-3)$-theorem (see Section 1). Suppose that $|H|\geq 2$.

Given a subset $S\subseteq G$ and a subgroup $L\leq G$, both finite, we define the *deficiency* of S on a coset $g+L\subseteq G$ by

$$\mathsf{d}(S,g+L):=\begin{cases}|(g+L)\setminus S| & \text{if } S\cap(g+L)\neq\varnothing,\\ 0 & \text{if } S\cap(g+L)=\varnothing;\end{cases}$$

notice that in the first case we can also write $\mathsf{d}(S, g+L) = |L| - |(g+L) \cap S|$. The *total deficiency* of S with respect to L is

$$\mathsf{D}(S, L) := |(S+L) \setminus S|;$$

equivalently,

$$\mathsf{D}(S, L) = \sum_{g+L} \mathsf{d}(S, g+L),$$

where the sum extends over all L-cosets having a nonempty intersection with S.

Suppose that $L \le H$ is a nonzero subgroup with

$$\mathsf{D}(2A, L) \le \mathsf{D}(A, L). \tag{18}$$

Then

$$\begin{aligned} |2(A+L)| &= |2A| + \mathsf{D}(2A, L) \le |2A| + \mathsf{D}(A, L) \\ &= |A+L| + |2A| - |A| = |A+L| + (\tau-1)|A| \le \tau |A+L|; \end{aligned}$$

that is, writing $\widetilde{G} := G/L \cong (H/L) \oplus \mathbb{Z}$, $\widetilde{A} := \varphi_L(A)$, and $\widetilde{2A} := \varphi_L(2A)$, we have $|2\widetilde{A}| \le \tau|\widetilde{A}|$. Applying the induction hypothesis to the subset $\widetilde{A} \subseteq \widetilde{G}$, we conclude that there are an arithmetic progression $\widetilde{P} \subseteq \widetilde{G}$ and a subgroup $\widetilde{K} \le \widetilde{H} := H/L$ such that $\widetilde{A} \subseteq \widetilde{P} + \widetilde{K}$ and $(|\widetilde{P}|-1)|\widetilde{K}| \le |2\widetilde{A}| - |\widetilde{A}|$. Let $K := \varphi_L^{-1}(\widetilde{K})$; thus, $L \le K \le H$ and $|K| = |L||\widetilde{K}|$. Also, it is easily seen that $\varphi_L^{-1}(\widetilde{P}) = P + L$ where $P \subseteq G$ is an arithmetic progression with $|P| = |\widetilde{P}|$. From $\widetilde{A} \subseteq \widetilde{P} + \widetilde{K}$ we derive then that $A \subseteq P + K$, and from $(|\widetilde{P}|-1)|\widetilde{K}| \le |2\widetilde{A}| - |\widetilde{A}|$ we get

$$\begin{aligned} (|P|-1)|K| &\le (|\widetilde{P}|-1)|\widetilde{K}||L| \le (|2\widetilde{A}| - |\widetilde{A}|)|L| \\ &= |2A+L| - |A+L| = |2A| + \mathsf{D}(2A, L) - |A| - \mathsf{D}(A, L) \le |2A| - |A|, \end{aligned}$$

completing the induction step.

Consider the situation where $L \le H$ is a nonzero subgroup satisfying

$$\mathsf{D}(A, L) \le |L| - 1. \tag{19}$$

Let m be the number of L-cosets on which A has positive deficiency, and fix $a_1, \dots, a_m \in A$ such that $a_1 + L, \dots, a_m + L$ list all these cosets. It follows easily from (19) that there is at most one pair of indices $1 \le i \le j \le m$ such that $\mathsf{d}(A, a_i + L) + \mathsf{d}(A, a_j + L) \ge |L|$, and if such a pair exists, then in fact $i = j$. By the pigeonhole principle, we have then $\mathsf{d}(2A, g+L) = 0$ for every coset $g + L$, with the possible exception of one single L-coset which, if exists, is of the form $2a + L$, with some $a \in A$. This yields

$$\mathsf{D}(2A, L) = \mathsf{d}(2A, 2a+L) \le \mathsf{d}(A, a+L) \le \mathsf{D}(A, L).$$

Clearly, the resulting estimate

$$\mathsf{D}(2A, L) \le \mathsf{D}(A, L)$$

remains valid also if there are no exceptional L-cosets.

Thus, once we are able to find a nonzero subgroup $L \le H$ satisfying either (18) or (19), we can complete the proof applying the induction hypothesis.

As a result, we can assume that for any nonempty subsets $A', A'' \subseteq A$ with $A = A' \cup A''$,

$$|A' + A''| \ge |A'| + |A''| - 1;$$

for if this fails to hold, then letting $L := \pi(A' + A'')$, by Kneser's theorem we have $|L| \ge 2$ and $|A' + L| + |A'' + L| - |L| = |A' + A''| \le |A'| + |A''| - 2$, whence

$$\mathsf{D}(A, L) \le \mathsf{D}(A', L) + \mathsf{D}(A'', L) \le |L| - 2$$

(for the first inequality, notice that $\mathsf{d}(A, g + L) \le \mathsf{d}(A', g + L) + \mathsf{d}(A'', g + L)$ for any coset $g + L$, which follows from the assumption $A', A'' \subseteq A = A' \cup A''$).

In particular, we assume that $|A + S| \ge |A| + |S| - 1$ for any nonempty subset $S \subseteq A$.

As an important special case,

$$|A + A^*| \ge |A| + |A^*| - 1. \tag{20}$$

6.2. **The set $\overline{A}$ has small doubling.** For a set $S \subseteq G$ and an element $g \in G$, denote by $r_S(g)$ the number of representations of g as a difference of two elements of S; thus, for instance, $|A^*| = r_A(\delta)$. Clearly, every Δ-coset intersects A by at most two elements, and if the intersection contains *exactly* two elements, then the two elements differ by δ. It follows that

$$|A| = |\overline{A}| + r_A(\delta) = |\overline{A}| + |A^*|. \tag{21}$$

Similarly, since $\overline{s}_1 = \overline{s}_2$ for any $s_1, s_2 \in 2A$ with $s_2 - s_1 = \delta$, we have $|2A| \ge |2\overline{A}| + r_{2A}(\delta)$. Furthermore, $r_{2A}(\delta) \ge |A + A^*|$ as to any $a \in A$ and $a^* \in A^*$ there corresponds the representation $\delta = ((a^* + \delta) + a) - (a^* + a)$, and the sum $a + a^*$ is uniquely determined by this representation. Therefore,

$$|2A| \ge |2\overline{A}| + |A + A^*|. \tag{22}$$

We now claim that

$$|2\overline{A}| < 2|\overline{A}| - 1. \tag{23}$$

In view of $|2\overline{A}| \le |2A| - |A + A^*| \le \tau|A| - |A| - |A^*| + 1$ and $|\overline{A}| = |A| - |A^*|$ (following from (20)–(22)), to prove the claim it suffices to show that

$$\tau|A| - |A| - |A^*| + 1 < 2|A| - 2|A^*| - 1;$$

that is,

$$(3 - \tau)|A| > |A^*| + 2. \tag{24}$$

To this end we notice that, by (9) and in view of $|A^*| \le \min\{|A_0|, |A_l|\}$,

$$(3 - \tau)(\tau|A| + |A^*|) > 3(|A_0| + |A_l|) \ge 6|A^*|.$$

Consequently,

$$(3 - \tau)|A| > \left(\frac{3}{\tau} + 1\right)|A^*| > 2|A^*|,$$

which proves (24) in the case where $|A^*| \ge 2$. In the remaining case $|A^*| = 1$, we obtain (24) as an immediate corollary of $|A| \ge n$ and $\tau < 3\left(1 - \frac{1}{n}\right)$.

Thus, (23) is established, and from Kneser's theorem it follows that the period $\overline{F} := \pi(2\overline{A})$ is a nonzero subgroup of the quotient group G/Δ, and also, in view of $2|\overline{A}+\overline{F}| - |\overline{F}| = |2\overline{A}| \le 2|\overline{A}| - 2$, that

$$\mathsf{D}(\overline{A}, \overline{F}) \le \frac{1}{2}\,|\overline{F}| - 1. \tag{25}$$

We let $F := \varphi_\Delta^{-1}(\overline{F})$, so that $\overline{F} = \varphi_\Delta(F)$ and $\Delta \le F \le G$.

Observing that $0 \in A$ implies $\overline{A} + \overline{F} \subseteq 2\overline{A} + \overline{F} = 2\overline{A}$, we denote by N the number of $\overline{F}$-cosets contained in $2\overline{A}$, but not in $\overline{A} + \overline{F}$; that is,

$$N = (|2\overline{A}| - |\overline{A} + \overline{F}|)/|\overline{F}|.$$

Combining $|2\overline{A}| - |\overline{A} + \overline{F}| = N|\overline{F}|$ and $|2\overline{A}| = 2|\overline{A} + \overline{F}| - |\overline{F}|$, we get

$$|\overline{A} + \overline{F}| = (N+1)|\overline{F}| \quad \text{and} \quad |2\overline{A}| = (2N+1)|\overline{F}|. \tag{26}$$

6.3. **The intersection subgroup.** Let $K := F \cap H$. By Lemma 4, there is an element $f_0 \in F$ such that $F = \langle f_0 \rangle + K$. Notice that $f_0 \notin H$, as a result of $\delta \in F \setminus H$; it follows that, in fact, $F = \langle f_0 \rangle \oplus K$. This shows that all the elements of F sharing the same projection onto the torsion-free component of G reside in the same K-coset.

Since $\delta \in F$, there exist a nonzero integer m and an element $z \in K$ such that $\delta = mf_0 + z$, and then $l = \psi(\delta) = m\psi(f_0)$. Switching from f_0 to $-f_0$, if needed, we can assume that m and $\psi(f_0)$ are both positive.

From $K = F \cap H$ and $\Delta \le F$, in view of Lemma 3, we get $\overline{K} = \overline{F} \cap \overline{H}$, and by the isomorphism theorems

$$\overline{F}/\overline{K} = \overline{F}/(\overline{F} \cap \overline{H}) \cong (\overline{F} + \overline{H})/\overline{H} \cong (F+H)/(H+\Delta) = (\langle f_0 \rangle + H)/(H+\Delta).$$

It follows that $|\overline{F}|/|\overline{K}|$ is the order of f_0 in the quotient group $G/(H+\Delta)$; that is, the smallest integer $t > 0$ with $tf_0 \in H + \Delta$. Clearly, we have $t \le m$. On the other hand, if $tf_0 \in H + \Delta$, then $t\psi(f_0)$ is divisible by $\psi(\delta) = l$; therefore t is divisible by $l/\psi(f_0) = m$. Hence, $|\overline{F}|/|\overline{K}| = m$, implying $\overline{F} = \langle \overline{f_0} \rangle \oplus \overline{K}$.

6.4. **The case where $N = 0$.** If $N = 0$, then $\overline{A} + \overline{F} = 2\overline{A}$. Adding $\overline{A}$ to both sides we get $2\overline{A} = 2\overline{A} + \overline{A}$, showing that $\overline{A} \subseteq \pi(2\overline{A}) = \overline{F}$. Combining this with $\overline{A} + \overline{F} = 2\overline{A}$, we conclude that $2\overline{A} = \overline{F}$. Thus, $2A + \Delta = F$ and therefore

$$A \subseteq 2A + \Delta = F = \langle f_0 \rangle + K. \tag{27}$$

Let $P := \langle f_0 \rangle \cap \psi^{-1}\big([0,l]\big)$, so that $A \subseteq P + K$. Since $\psi^{-1}\big([0,l-1]\big)$ contains exactly one representative out of every Δ-coset, we have

$$\begin{aligned}
|2\overline{A}| &= |\varphi_\Delta(2A)| \\
&= |\varphi_\Delta(2A+\Delta)| \\
&= \big|(2A+\Delta) \cap \psi^{-1}\big([0,l-1]\big)\big| \\
&= \big|\big(\langle f_0 \rangle + K\big) \cap \psi^{-1}\big([0,l-1]\big)\big| \\
&= \big|\langle f_0 \rangle \cap \psi^{-1}\big([0,l-1]\big)\big||K| \\
&= \big|\langle f_0 \rangle \cap \psi^{-1}\big([0,l]\big)\big||K| - \big|\langle f_0 \rangle \cap \psi^{-1}(\{l\})|K| \\
&= (|P|-1)|K|,
\end{aligned}$$

the middle equality following from (27), and the last equality from

$$\varnothing \neq A \cap \psi^{-1}(\{l\}) \subseteq (\langle f_0 \rangle + K) \cap \psi^{-1}(\{l\}) = (\langle f_0 \rangle \cap \psi^{-1}(\{l\})) + K$$

and the resulting $\langle f_0 \rangle \cap \psi^{-1}(\{l\}) \neq \varnothing$. Consequently, (22) yields $(|P|-1)|K| \leq |2A|-|A|$, completing the proof in the case where $N = 0$.

We thus assume for the remaining part of the argument that $N > 0$; that is

$$\overline{A} + \overline{F} \subsetneq 2\overline{A}.$$

Therefore, $2\overline{A}$ is *not* a subgroup (if it were, we would have $\overline{F} = \pi(2\overline{A}) = 2\overline{A}$ implying $\overline{A} + \overline{F} \supseteq 2\overline{A}$).

6.5. **The case where** $N = 1$**.** If $N = 1$, then $\overline{A} + \overline{F}$ is a union of exactly two $\overline{F}$-cosets, and $2\overline{A}$ is a union of exactly three $\overline{F}$-cosets. Since $0 \in A$, we derive that $A = A_1 \cup (g + A_2)$, where $A_1, A_2 \subseteq F$ are nonempty, and where $g \in G$ satisfies $2g \notin F$, as a result of $2\overline{A}$ being a union of three $\overline{F}$-cosets. Write $n_i := |\psi^{-1}(A_i)|,\ i \in \{1,2\}$, so that $n := |\psi^{-1}(A)| \leq n_1 + n_2$. By Lemma 7, we have then

$$\begin{aligned}
|2A| &= |2A_1| + |A_1 + A_2| + |2A_2| \\
&\geq 3\Big(1 - \frac{1}{n_1+n_2}\Big)(|A_1| + |A_2|) \\
&\geq 3\Big(1 - \frac{1}{n}\Big)|A|,
\end{aligned}$$

a contradiction.

Let $\overline{H} := \varphi_\Delta(H)$ and $\overline{K} := \varphi_\Delta(K)$. We split the remaining case $N \geq 2$ into two further subcases: that where $\overline{K}$ is a proper subgroup of $\overline{F}$ (which, by Lemma 3 applied with $B = H$ and $C = F$, is equivalent to $\overline{F} \not\leq \overline{H}$ and thus to $F \not\leq H + \Delta$), and that where $\overline{K} = \overline{F}$ (equivalently, $\overline{F} \leq \overline{H}$, $F \leq H + \Delta$, or $F = K \oplus \Delta$).

6.6. **The case where $N \ge 2$ and $\overline{K} \subsetneq \overline{F}$.** We show that in this case

$$|2A \setminus A| \ge 2|\overline{A}|; \tag{28}$$

in view of (21) and (11), this will give

$$|2A| - |A| \ge 2|\overline{A}| = 2|A| - 2|A^*| > 2|A| - (3-\tau)|A| = (\tau - 1)|A|,$$

a contradiction.

To prove (28), we partition the elements $s \in 2A \setminus A$ into two groups, according to whether $\overline{s} := \varphi_\Delta(s)$ does or does not belong to $\overline{A} + \overline{F}$.

For the first group we have the estimate

$$|\{s \in 2A \setminus A \colon \overline{s} \in \overline{A} + \overline{F}\}| \ge |\overline{A} + \overline{F}|; \tag{29}$$

for, $\overline{A} + \overline{F} \subseteq 2\overline{A}$ shows that for every element $\overline{s} \in \overline{A} + \overline{F}$, the set $\{s \in 2A \colon \varphi_\Delta(s) = \overline{s}\}$ is nonempty, and the (unique) element of this set with the largest value of $\psi(s)$ does not lie in A as $s \in A$ implies $s + \delta \in 2A$, because of $\delta \in A$. (This argument shows that, indeed, for any subset $\overline{S} \subseteq 2\overline{A}$ there are at least $|\overline{S}|$ elements $s \in 2A \setminus A$ such that $\overline{s} \in \overline{S}$.)

Addressing the second group, we show that

$$T := |\{s \in 2A \setminus A \colon \overline{s} \notin \overline{A} + \overline{F}\}| \ge 2|\overline{A}| - |\overline{A} + \overline{F}|;$$

along with (29) this will prove (28), leading to a contradiction. (Notice that the trivial estimate would be $T \ge |2\overline{A}| - |\overline{A} + \overline{F}|$, in view of the parenthetical remark at the end of the previous paragraph.)

The set $(2\overline{A}) \setminus (\overline{A} + \overline{F})$ is a union of $\overline{F}$-cosets and, recalling (26), we find elements $a_1, \dots, a_N, b_1, \dots, b_N \in A$ such that the cosets are $\overline{a}_i + \overline{b}_i + \overline{F}$, $i \in [1, N]$.

Let

$$A_i := A \cap (a_i + F) \text{ and } B_i := A \cap (b_i + F), \quad i \in [1, N].$$

By Lemma 3 we have $\overline{A}_i = \overline{A} \cap (\overline{a}_i + \overline{F})$ and $\overline{B}_i = \overline{A} \cap (\overline{b}_i + \overline{F})$, and it follows that

$$|A_i| \ge |\overline{A}_i| = |\overline{F}| - \mathsf{d}(\overline{A}, \overline{a}_i + \overline{F}), \quad i \in [1, N] \tag{30}$$

and, similarly,

$$|B_i| \ge |\overline{B}_i| = |\overline{F}| - \mathsf{d}(\overline{A}, \overline{b}_i + \overline{F}), \quad i \in [1, N]. \tag{31}$$

Since $\varphi_\Delta(A_i + B_i) = \overline{A}_i + \overline{B}_i \subseteq \overline{a}_i + \overline{b}_i + \overline{F} \subseteq (2\overline{A}) \setminus (\overline{A} + \overline{F})$ by the choice of a_i and b_i, we have

$$T = \sum_{i=1}^N |\{s \in 2A \setminus A \colon \overline{s} \in \overline{a}_i + \overline{b}_i + \overline{F}\}| \ge \sum_{i=1}^N |A_i + B_i|. \tag{32}$$

By Lemma 2 applied to the subset $\widetilde{A} := (\overline{A} + \overline{F})/\overline{F}$ of the quotient group $\overline{G}/\overline{F}$, we can assume that each $\overline{F}$-coset from $\overline{A} + \overline{F}$ appears among the $2N$ cosets $\overline{a}_1 + \overline{F}, \dots, \overline{b}_N + \overline{F}$ at most N times, save for the following possible exceptions:

i) there is a subgroup $\widetilde{L} \le \overline{G}/\overline{F}$ and an element $\widetilde{c} \in \overline{G}/\overline{F}$ with $2\widetilde{c} \notin \widetilde{L}$ such that either $\widetilde{A} = \widetilde{L} \cup \{\widetilde{c}\}$, or $\widetilde{A} = (\widetilde{c} + \widetilde{L}) \cup \{0\}$;

ii) $N = 2$ and $\widetilde{A} = \{0, \widetilde{g}, 2\widetilde{g}\}$ where $\widetilde{g} \in \overline{G}/\overline{F}$ has order at least 5.

In the first exceptional case, A meets exactly two cosets of the subgroup $L = \varphi_F^{-1}(\widetilde{L})$, while $2A$ meets exactly three cosets of this subgroup. As a result, we can apply Lemma 7, exactly as in the case $N = 1$ considered above, to get a contradiction. In the second exceptional case there exists an element $g \in G$ such that $\overline{A} + \overline{F} = \{0, \overline{g}, 2\overline{g}\} + \overline{F}$ and $2\overline{A} = \{0, \overline{g}, 2\overline{g}, 3\overline{g}, 4\overline{g}\} + \overline{F}$, where $\overline{g} = \varphi_\Delta(g)$ and the five $\overline{F}$-cosets contained in $2\overline{A}$ are pairwise distinct. Letting $C_i := A \cap (ig + F),\ i \in \{0, 1, 2\}$, we have

$$2A \supseteq (2C_0) \cup (C_0 + C_1) \cup (2C_1) \cup (C_1 + C_2) \cup (2C_2),$$

where the union is disjoint. The set $\overline{C}_2 := \varphi_\Delta(C_2)$ hits at least two $\overline{H}$-cosets: otherwise $\overline{C}_2$ would be contained in a coset of the subgroup $\overline{H} \cap \overline{F} = \overline{K} \lneq \overline{F}$ leading to $\mathsf{D}(\overline{A}, \overline{F}) \geq |\overline{F}| - |\overline{C}_2| \geq |\overline{F}| - |\overline{K}| \geq \frac{1}{2}|\overline{F}|$, in a contradiction with (25). Therefore C_2 hits at least two H-cosets, and applying Lemma 8 we get an immediate contradiction.

We now address the "regular" situation where each $\overline{F}$-coset from $\overline{A}+\overline{F}$ appears among $\overline{a}_1 + \overline{F}, \dots, \overline{b}_N + \overline{F}$ not more than N times.

Since $A_i + B_i$ is contained in an F-coset, we have $\pi(A_i + B_i) \leq F$, and since $A_i + B_i$ is finite, $\pi(A_i + B_i) \leq H$; as a result, $\pi(A_i + B_i) \leq F \cap H = K$. Consequently, by (32), Kneser's theorem, (30), and (31),

$$T \geq 2N|\overline{F}| - \sum_{i=1}^{N} (\mathsf{d}(\overline{A}, \overline{a}_i + \overline{F}) + \mathsf{d}(\overline{A}, \overline{b}_i + \overline{F})) - |K|N.$$

Recalling that each $\overline{F}$-coset from $\overline{A}+\overline{F}$ appears at most N times among $\overline{a}_1+\overline{F}, \dots, \overline{b}_N+\overline{F}$, we get

$$T \geq 2N|\overline{F}| - N\mathsf{D}(\overline{A}, \overline{F}) - |K|N \geq \left(\frac{3}{2}\,|\overline{F}| - \mathsf{D}(\overline{A}, \overline{F})\right) N$$

(as $\overline{K} \lneq \overline{F}$ yields $|K| = |\overline{K}| \leq \frac{1}{2}|\overline{F}|$). Therefore, by (25), (26), and the definition of the total deficiency,

$$\begin{aligned} T &\geq (N+1)|\overline{F}| - 2\mathsf{D}(\overline{A}, \overline{F}) + (N-2)\left(\frac{1}{2}\,|\overline{F}| - \mathsf{D}(\overline{A}, \overline{F})\right) \\ &\geq (N+1)|\overline{F}| - 2\mathsf{D}(\overline{A}, \overline{F}) \\ &= 2|\overline{A}| - |\overline{A} + \overline{F}|. \end{aligned}$$

As shown at the beginning of this section, this leads to a contradiction.

6.7. **The case where $N \geq 2$ and $\overline{K} = \overline{F}$.** As shown above, in this case $\overline{F} \leq \overline{H}$, $F \leq H + \Delta$, and $F = K \oplus \Delta$; notice that this implies $|\overline{F}| = |\overline{K}| = |K|$.

Claim 1. *We have $A_0 \subseteq K$ and $A_l \subseteq \delta + K$; that is, each of the sets A_0 and A_l is contained in a single K-coset.*

Proof. From (22), Kneser's theorem, (20), and (21), we have

$$|2A| \ge (2|\overline{A}+\overline{F}| - |\overline{F}|) + (|A| + |A^*| - 1)$$
$$\ge 2|\overline{A}| - |\overline{F}| + |A| + |A^*| - 1 = 3|A| - |A^*| - |\overline{F}| - 1.$$

Combining this estimate with (10), we get

$$\sigma \le |A^*| + |\overline{F}|. \tag{33}$$

On the other hand,

$$|H \cap (A+\Delta)| \ge |\varphi_\Delta(H \cap (A+\Delta))| = |\varphi_\Delta(H) \cap \varphi_\Delta(A+\Delta)| = |\overline{H} \cap \overline{A}|$$

by Lemma 3. Observing that the left-hand side is

$$|(H \cap A) \cup (H \cap (A-\delta))| = |A_0 \cup (A_l - \delta)| = \sigma - |A^*|,$$

and using (33), we obtain

$$|\overline{H} \cap \overline{A}| \le \sigma - |A^*| \le |\overline{F}|. \tag{34}$$

Assuming now for a contradiction that, say, A_0 intersects nontrivially more than one K-coset, fix $a_1, a_2 \in A_0$ with $a_1 - a_2 \notin K$; hence, comparing the projections onto the torsion-free component, with $a_1 - a_2 \notin K + \Delta$. Since $\overline{a}_1, \overline{a}_2 \in \overline{H}$ are then distinct modulo $\overline{K} = \overline{F}$, in view of (25), the assumption $\overline{F} \le \overline{H}$, and (34), we get

$$\begin{aligned}
\frac12 |\overline{F}| &> \mathsf{D}(\overline{A}, \overline{F}) \\
&\ge \mathsf{d}(\overline{A}, \overline{a}_1 + \overline{F}) + \mathsf{d}(\overline{A}, \overline{a}_2 + \overline{F}) \\
&= 2|\overline{F}| - (|(\overline{a}_1 + \overline{F}) \cap \overline{A}| + |(\overline{a}_2 + \overline{F}) \cap \overline{A}|) \\
&\ge 2|\overline{F}| - |(\overline{H} + \overline{F}) \cap \overline{A}| \\
&= 2|\overline{F}| - |\overline{H} \cap \overline{A}| \\
&\ge |\overline{F}|,
\end{aligned}$$

the contradiction sought. $\square$

Let $A^\circ := A \setminus (A_0 \cup A_l)$ be the "middle part" of A.

Claim 2. *We have $2A^\circ + K = 2A^\circ$. Moreover, if $|A_0| \ge |A_l|$, then $A^\circ + K \subseteq 2A$, and if $|A_l| \ge |A_0|$, then $A^\circ + \delta + K \subseteq 2A$.*

Proof. To prove the first assertion, we fix $a_1, a_2 \in A^\circ$ and show that $a_1 + a_2 + K \subseteq 2A^\circ$. For $i \in \{1,2\}$, let $A_i := (a_i + F) \cap A$; notice that $A_i \subseteq a_i + F = a_i + K + \Delta$ whence, indeed, $A_i \subseteq a_i + K$. Write $S := A_1 + A_2 \subseteq a_1 + a_2 + K$ so that $\overline{S} = \overline{A}_1 + \overline{A}_2 = \overline{a}_1 + \overline{a}_2 + \overline{F}$ in view of (25). As a result, $|S| \ge |\overline{S}| = |\overline{a}_1 + \overline{a}_2 + \overline{F}| = |\overline{F}| = |\overline{K}| = |K|$, leading to $S = a_1 + a_2 + K$; thus, $a_1 + a_2 + K = A_1 + A_2 \subseteq 2A^\circ$.

Addressing the second assertion, we fix $a^\circ \in A^\circ$ and show that then either $a^\circ + K \subseteq 2A$, or $a^\circ + \delta + K \subseteq 2A$, according to the relation between $|A_0|$ and $|A_l|$. Write $B_0 := A \cap F$ and $B^\circ := A \cap (a^\circ + F)$; equivalently, $B_0 = A_0 \cup A_l$ by Claim 1, and $B^\circ = A \cap (a^\circ + K)$.

Letting $S := B_0+B^\circ$, in view of $B_0 \subseteq F$ and $B^\circ \subseteq a^\circ+F$ we have then $S \subseteq 2A\cap(a^\circ+F)$ and $\overline{S} = \overline{B}_0 + \overline{B}^\circ$. Furthermore, from

$$\mathsf{d}(\overline{A},\overline{F}) = |\overline{F}| - |\overline{A}\cap\overline{F}| = |\overline{F}| - |\overline{B}_0|$$

and

$$\mathsf{d}(\overline{A},\overline{a}^\circ+\overline{F}) = |\overline{F}| - |\overline{A}\cap(\overline{a}^\circ+\overline{F})| = |\overline{F}| - |\overline{B}^\circ|$$

recalling (25) we get

$$|\overline{B}_0| + |\overline{B}^\circ| = 2|\overline{F}| - (\mathsf{d}(\overline{A},\overline{F}) + \mathsf{d}(\overline{A},\overline{a}^\circ+\overline{F})) \ge 2|\overline{F}| - \mathsf{D}(\overline{A},\overline{F}) > \frac{3}{2}\,|\overline{F}|.$$

From $B_0 = A_0 \cup A_l$ we now derive

$$|A_0| + |A_l| + |B^\circ| \ge |B_0| + |B^\circ| \ge |\overline{B}_0| + |\overline{B}^\circ| > \frac{3}{2}\,|\overline{F}|.$$

Also, we have

$$|B^\circ| \ge |\overline{B}^\circ| = |\overline{A}\cap(\overline{a}^\circ+\overline{F})| = |\overline{F}| - \mathsf{d}(\overline{A},\overline{a}^\circ+\overline{F}) \ge |\overline{F}| - \mathsf{D}(\overline{A},\overline{F}) > \frac{1}{2}\,|\overline{F}|.$$

Therefore,

$$\max\{|A_0|,|A_l|\} + |B^\circ| \ge \frac{1}{2}(|A_0|+|A_l|+|B^\circ|) + \frac{1}{2}\,|B^\circ| > \frac{3}{4}\,|\overline{F}| + \frac{1}{4}\,|\overline{F}| = |\overline{F}| = |K|.$$

Since $B^\circ \subseteq a^\circ+K$, $A_0 \subseteq K$, and $A_l \subseteq \delta+K$, from the pigeonhole principle we conclude that if $|A_0| > |A_l|$, then $A_0+B^\circ = a^\circ+K$, while if $|A_l| \ge |A_0|$, then $A_l+B^\circ = a^\circ+\delta+K$. The assertion follows in view of $A_0+B^\circ \subseteq 2A$ and $A_l+B^\circ \subseteq 2A$. □

We can, eventually, complete the proof. Assuming $|A_0| \le |A_l|$ for definiteness, by Claim 2 we have $2A^\circ+K \subseteq 2A$ and also $A^\circ+A_l+K = A^\circ+\delta+K \subseteq 2A$; that is, the set $2A$ has zero deficiency on all K-cosets with the possible exception of the cosets contained in A_0+A+K; that is, cosets of the form $a+K$ with $a \in A$. On the other hand, in view of

$$A\cap(a+K) + A_0 \subseteq 2A\cap(a+K)$$

and $|2A\cap(a+K)| \ge |A\cap(a+K)|$ resulting from it, we have

$$\mathsf{d}(2A,a+K) \le \mathsf{d}(A,a+K).$$

Taking the sum over the elements $a \in A$ representing the K-cosets contained in $A+K$ we get

$$\mathsf{D}(A,K) = \sum_a \mathsf{d}(A,a+K) \ge \sum_a \mathsf{d}(2A,a+K) = \mathsf{D}(2A,K).$$

As noticed in Section 6.1, this completes the proof by appealing to the induction hypothesis.

Acknowledgement

I am grateful to the anonymous referee for the careful reading of the manuscript and useful suggestions and remarks.

References

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

[DF86] J-M. Deshouillers and G.A. Freiman, A step beyong Kneser's theorem for abelian finite groups, *Proc. London Math. Soc. (3)* **86** (1) (2003), 1–28.

[F62] G.A. Freiman, Inverse problems in additive number theory, VI. On the addition of finite sets, III, Izv.Vyssh. Uchebn. Zaved. Mat. 3 (1962), 151–157 (Russian).

[F73] ———, *Groups and the inverse problems of additive number theory, Number-theoretic studies in the Markov spectrum and in the structural theory of set addition* pp. 175–183. Kalinin. Gos. Univ., Moscow, 1973.

[G13] D.J. Grynkiewicz, *Structural additive theory*, Developments in Mathematics, **30**. Springer, Cham, 2013.

[Kn53] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.

[Kn55] ———, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.* **61** (1955), 429–434.

[L98] J. Losonczy, On matchings in groups, *Adv. in Appl. Math.* **20** (3) (1998), 385–391.

[N96] M. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics 165. Springer-Verlag, New York, 1996.

[O75] J.E. Olson, Sums of sets of group elements, *Acta Arith.* **28** (2) (1975/76), 147–156.

[TV06] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, **105**. Cambridge University Press, Cambridge, 2006.

Email address: seva@math.haifa.ac.il

Department of mathematics, the University of Haifa at Oranim, Tivon 36006, Israel