1. Summary

Let $A$ and $B$ be subsets of an elementary abelian 2-group $G$, none of which are contained in a coset of a proper subgroup. Extending onto potentially distinct summands a result of Hennecart and Plagne, we show that if $|A + B| < |A| + |B|$, then either $A + B = G$, or the complement of $A + B$ in $G$ is contained in a coset of a subgroup of index at least 8 (whence $|A + B| \geq \frac{7}{8}|G|$). We indicate conditions for the containment to be strict, and establish a refinement in the case where the sizes of $A$ and $B$ differ significantly.

2. Background and introduction

For subsets $A$ and $B$ of an abelian group, we denote by $A + B$ the sumset of $A$ and $B$:

$$A + B := \{a + b: a \in A, \ b \in B\}.$$  

We abbreviate $A + A$ as $2A$. By $\langle A \rangle$ we denote the affine span of $A$ (which is the smallest coset that contains $A$).

Pairs of finite subsets $A$ and $B$ of an abelian group with $|A + B| < |A| + |B|$ are classified by the classical results of Kneser and Kemperman \cite{Kne53, Kem60}. Recursive in its nature, this classification is rather complicated in general, but it has been observed that for the special case where the underlying group is an elementary abelian 2-group (that is, a finite abelian group of exponent 2), explicit closed-form results can be obtained. Particularly important in our present context is the following theorem due to Hennecart and Plagne.

**Theorem 1** (\cite[Theorem 1]{HP03}). Let $A$ be a subset of an elementary abelian 2-group $G$ such that $\langle A \rangle = G$. If $|2A| < 2|A|$, then either $2A = G$, or the complement of $2A$ in $G$ is a coset of a subgroup of index at least 8. Consequently, $|2A| \geq \frac{7}{8}|G|$.

\footnotesize

2010 Mathematics Subject Classification: Primary 11P70; Secondary 05D99.

Key words and phrases: sumset, abelian 2-group, affine span.
We mention two directions in which Theorem 1 was later developed. First, in connection with Freiman’s structure theorem, much attention has been attracted to the function $F$ defined by

$$F(K) := \sup \{ |\langle A \rangle|/|A| : |2A| \leq K|A| \}, \quad K \geq 1$$

where $A$ runs over non-empty subsets of elementary abelian 2-groups. It is not difficult to derive from Theorem 1 that

$$F(K) = \begin{cases} K & \text{if } 1 \leq K < \frac{7}{4} \\ \frac{5}{4} K & \text{if } \frac{7}{4} \leq K < 2 \end{cases}$$

This is, essentially, [HP03, Corollary 2]. A result of Ruzsa [Ruz99] shows that $F(K)$ is finite for each $K \geq 1$ and indeed, $F(K) \leq K^22^K$. Various improvements for $K \geq 2$ were obtained by Deshouillers, Hennecart, and Plagne [DHP04], Sanders [San08], Green and Tao [GT09], and Konyagin [Kon08], and the exact value of $F(K)$ was eventually established in [EZ11].

In another direction, [Lev06, Theorem 5] establishes the precise structure of those subsets $A$ satisfying $|2A| < 2|A|$, in contrast with Theorem 1 which describes the structure of the sumset $2A$ only.

The goal of the present paper is to extend Theorem 1 onto addition of two potentially distinct set summands. In this case the assumption $|A + B| < |A| + |B|$ does not guarantee any longer that the complement of $A + B$ is a coset of a subgroup of index at least 8, as evidenced, for instance, by the following construction: represent the underlying group $G$ as a direct sum $G = H \oplus F$ with $|H| = 8$, fix a generating set $\{h_1, h_2, h_3\} \subset H$ and an arbitrary proper subset $F_0 \subsetneq F$, and let

$$A := (\{h_1, h_2, h_3\} + F) \cup \{0\},$$
$$B := (\{h_1 + h_2, h_2 + h_3, h_3 + h_1, h_1 + h_2 + h_3\} + F) \cup F_0.$$ 

The complement of $A + B$ in $G$ is easily verified to be the complement of $F_0$ in $F$, which need not be a coset, and

$$|A + B| = |G| - (|F| - |F_0|) = |A| + |B| - 1.$$ 

It turns out, however, that while the complement of $A + B$ may fail to be a coset of a subgroup of index at least 8, it is necessarily contained in a such a coset — and indeed, in a coset of a subgroup of larger index if the summands differ significantly in size.

For subsets $A$ and $B$ of an abelian group and a group element $g$, let $\nu_{A,B}(g)$ denote the number or representations of $g$ in the form $g = a + b$ with $a \in A$ and $b \in B$, and let

$$\mu_{A,B} := \min \{ \nu_{A,B}(g) : g \in A + B \}.$$
The following theorem, proved in Section 4 is our main result.

**Theorem 2.** Let $A$ and $B$ be subsets of an elementary abelian 2-group $G$ such that $\langle A \rangle = \langle B \rangle = G$. If $|A + B| < \min\{|A| + |B|, |G|\}$, then the complement of $A + B$ in $G$ is contained in a coset of a subgroup of index 8. Moreover, if $\mu_{A,B} = 1$, then the containment is strict.

We could get a stronger conclusion in the “highly asymmetric” case.

**Theorem 2’.** Let $A$ and $B$ be subsets of an elementary abelian 2-group $G$ such that $\langle A \rangle = \langle B \rangle = G$. If $|A + B| < \min\{|A| + |B|, |G|\}$ and $|B| \geq \left(1 - \frac{k+1}{2^k}\right)|G|$ with integer $k \geq 4$, then the complement of $A + B$ in $G$ is contained in a coset of a subgroup of index $2^k$. Moreover, if $\mu_{A,B} = 1$, then the containment is strict.

Notice that in the statements of Theorems 2 and 2’, we disposed of the case where the sumset $A + B$ is the whole group by assuming from the very beginning that $|A + B| < |G|$.

The bounds on the subgroup index in Theorems 2 and 2’ are best possible under the stated assumptions. To see this, fix an integer $k \geq 3$ (the case $k = 3$ addressing Theorem 2), consider a decomposition $G = H \oplus F$ with $|H| = 2^k$, choose a generating set $\{0, h_1, \ldots, h_k\} \subset H$ and two arbitrary elements $g_1, g_2 \in G$, and let
\begin{align*}
A &= g_1 + \{0, h_1, \ldots, h_k\} + F, \\
B &= g_2 + (H \setminus \{0, h_1, \ldots, h_k\}) + F.
\end{align*}
Then $|B| = \left(1 - \frac{k+1}{2^k}\right)|G|$, the complement of $A + B$ in $G$ is $g_1 + g_2 + F$, and
\[|A + B| = |G| - |F| = |A| + |B| - |F|.
\]

Indeed, analyzing carefully the argument in Section 4, one can see that if $B$ is not of the form just described, then the containment in the conclusion of Theorem 2’ is strict.

An almost immediate corollary of Theorem 2 is that if $A$ and $B$ are subsets of an elementary abelian 2-group $G$ such that $\langle A \rangle = \langle B \rangle = G$ and $|A + B| < \frac{5}{4}(|A| + |B|)$, then $A + B = G$. In fact, Kneser’s theorem yields a stronger result: if $\langle A \rangle = \langle B \rangle = G$ and $|A + B| < \frac{3}{4}(|A| + |B|)$, then $A + B = G$. Omitting the proof, which is nothing more than a routine application of Kneser’s theorem, we confine ourselves to the remark that both assumptions $\langle A \rangle = G$ and $\langle B \rangle = G$ are crucial. This follows by considering the situation where $B$ is an index-8 subgroup of $G$, and $A$ is a union of 4 cosets of $B$ (which is not a coset itself), and that where $A$ is an index-4 subgroup, and $B$ is a union of three cosets of $A$.

We deduce Theorems 2 and 2’ from [Lev06, Theorem 2], quoted in the next section as Theorem 3. Based on the well-known Kemperman’s structure theorem, this result
3. Pairs of sets with a small sumset

The contents of this section originate from [Kem60] and [Lev06]. Our goal here is to introduce [Lev06, Theorem 2], from which Theorems 2 and 2′ will be derived in the next section.

For a subset $A$ of the abelian group $G$, the (maximal) period of $A$ will be denoted by $\pi(A)$; recall that this is the subgroup of $G$ defined by $\pi(A) := \{g \in G : A + g = A\}$, and that $A$ is called periodic if $\pi(A) \neq \{0\}$ and aperiodic otherwise.

By an arithmetic progression in the abelian group $G$ with difference $d \in G$, we mean a set of the form $\{g + d, g + 2d, \ldots, g + nd\}$, where $n$ is a positive integer.

Essentially following Kemperman’s paper [Kem60], we say that the pair $(A, B)$ of finite subsets of the 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, 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 where $H_1$ and $H_2$ 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, $c := g_1 + g_2$ is the unique element of $A + B$ with $\nu_{A,B}(c) = 1$;

(IV) $A = g_1 + H_1$ and $B = g_2 - H_2$, where $g_1, g_2 \in G$, and where $H_1$ and $H_2$ 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, $\mu_{A,B} \geq 2$.

Notice, that for elementary pairs of type (III) we have $|A| + |B| = |H| + 1$, whence $A + B = g_1 + g_2 + H$ by the box principle. Also, for type (IV) pairs we have $|A| + |B| = |H|$ and $A + B = g_1 + g_2 + (H \setminus \{0\})$; the reader can consider the latter assertion as an exercise or find a proof in [Lev06].

We say that the pair $(A, B)$ of subsets of an abelian group satisfies Kemperman’s condition if

\begin{equation}
\text{either } \pi(A + B) = \{0\}, \text{ or } \mu_{A,B} = 1. \tag{1}
\end{equation}

Given a subgroup $H$ of the abelian group $G$, by $\varphi_H$ we denote the canonical homomorphism from $G$ onto the quotient group $G/H$. 

We are at last ready to present our main tool.

**Theorem 3** ([Lev06 Theorem 2]). Let \( A \) and \( B \) be finite, non-empty subsets of the abelian group \( G \). A necessary and sufficient condition for \((A, B)\) to satisfy both

\[
|A + B| < |A| + |B|
\]

and Kemperman’s condition (1) is that either \((A, B)\) is an elementary pair, or there exist non-empty subsets \( A_0 \subseteq A \) and \( B_0 \subseteq B \) and a finite, non-zero, proper subgroup \( F < G \) such that

(i) each of \( A_0 \) and \( B_0 \) is contained in an \( F \)-coset, \(|A_0 + B_0| = |A_0| + |B_0| - 1\), and the pair \((A_0, B_0)\) satisfies Kemperman’s condition;

(ii) each of \( A \setminus A_0 \) and \( B \setminus B_0 \) is a (possibly empty) union of \( F \)-cosets;

(iii) the pair \((\varphi_F(A), \varphi_F(B))\) is elementary; moreover, \( \varphi_F(A_0) + \varphi_F(B_0) \) has a unique representation as a sum of an element of \( \varphi_F(A) \) and an element of \( \varphi_F(B) \).

4. **Proof of Theorems 2 and 2′**

We give Theorems 2 and 2′ one common proof.

If \(|G| \leq 4\), then the assumption \( \langle A \rangle = \langle B \rangle = G \) implies \( A + B = G \), and we therefore assume \(|G| \geq 8\) and use induction on \(|G|\).

If Kemperman’s condition (1) fails to hold, then, in particular, \( H := \pi(A + B) \) is a non-zero subgroup. In this case we observe that the assumptions \( \langle A \rangle = \langle B \rangle = G \) and \(|A + B| < |G|\) imply \( \langle \varphi_H(A) \rangle = \langle \varphi_H(B) \rangle = G/H \) and \( |\varphi_H(A) + \varphi_H(B)| < |G/H|\), respectively, and

\[
|B| \geq \left(1 - \frac{k + 1}{2^k}\right)|G| \tag{2}
\]

implies \( |\varphi_H(B)| \geq \left(1 - \frac{k + 1}{2^k}\right)|G/H|\). Hence, by the induction hypothesis, the complement of \( \varphi_H(A) + \varphi_H(B) = \varphi_H(A + B) \) in \( G/H \) is contained in a coset of a subgroup of index 8 and indeed, of index \( 2^k \) under the assumption (2), and so is the complement of \( A + B \) in \( G \).

From now on we assume that Kemperman’s condition (1) holds true, and hence Theorem 3 applies.

If \((A, B)\) is an elementary pair in \( G \), then it is of type III or IV, in view of the assumptions \(|G| \geq 8\) and \( \langle A \rangle = \langle B \rangle = G \). Moreover, by the same reason, the subgroup \( H \leq G \) in the definition of elementary pairs is, in fact, the whole group \( G \). We conclude that \((A, B)\) is actually of type IV: for, if it were of type III, we would have \( A + B = G \) (see a remark after the definition of elementary pairs). Consequently, \( \mu_{A,B} \geq 2 \) and the complement of \( A + B \) in \( G \) is a singleton; that is, a coset of the zero subgroup. To complete the treatment of the present case, we denote by \( n \) the rank of \( G \) and notice
that (2) implies $|A| = |G| - |B| \leq (k+1)2^{n-k}$, while $\langle A \rangle = G$ gives $|A| \geq n+1$. Hence, $(n+1)/2^n \leq (k+1)/2^k$. As a result, $n \geq k$, and therefore the zero subgroup has index $|G| \geq 2^k$.

Finally, consider the situation where $(A, B)$ is not an elementary pair in $G$, and find then $A_0 \subseteq A$, $B_0 \subseteq B$, and $F < G$ as in the conclusion of Theorem 3. Observe that $\langle \varphi_F(A) \rangle = \langle \varphi_F(B) \rangle = G/F$ yields $\min\{|\varphi_F(A)|, |\varphi_F(B)|\} \geq 2$, so that $(\varphi_F(A), \varphi_F(B))$ cannot be an elementary pair in $G/F$ of type I or II. Indeed, $(\varphi_F(A), \varphi_F(B))$ cannot be of type IV either, as in this case we would have $\mu_{\varphi_F(A), \varphi_F(B)} \geq 2$, contrary to Theorem 3(iii). Thus, $(\varphi_F(A), \varphi_F(B))$ is of type III, and $\langle \varphi_F(A) \rangle = \langle \varphi_F(B) \rangle = G/F$ implies that the subgroup of the quotient group $G/F$ in the definition of elementary pairs is actually the whole group $G/F$. As a result, we derive from Theorem 3 that the complement of $A + B$ in $G$ is the complement of $A_0 + B_0$ in the appropriate $F$-coset.

Write $|G/F| = 2^m$; to complete the proof it remains to show that $m \geq 3$, and if (2) holds then, indeed, $m \geq k$. To this end we notice that $\langle \varphi_F(A) \rangle = \langle \varphi_F(B) \rangle = G/F$ gives $\min\{|\varphi_F(A)|, |\varphi_F(B)|\} \geq m + 1$; compared to $|\varphi_F(A)| + |\varphi_F(B)| = 2^m + 1$, this results in $2m + 2 \leq 2^m + 1$, whence $m \geq 3$. Finally, $|\varphi_F(B)| \geq (1 - (k+1)/2^k)2^m$ gives $|\varphi_F(A)| \leq (k+1)2^{m-k} + 1$. Combined with $|\varphi_F(A)| \geq m + 1$ this leads to $m \leq (k+1)2^{m-k}$. As the right-hand side is a decreasing function of $k$, if we had $m < k$, the last inequality would yield $m \leq (m + 2)2^{m-(m+1)}$, which is wrong.

Note that the condition $\mu_{A,B} = 1$ can hold only under the last scenario (where $(A, B)$ is not an elementary pair in $G$). As we have shown, in this case the complement of $A + B$ is strictly contained in an $F$-coset, and the strict containment assertion follows.

\section*{Acknowledgment}

The first author would like to thank his thesis advisor, Professor Nati Linial, for a patient and helpful guidance.

\section*{References}

[DHP04] J.-M. Deshouillers, F. Hennecart, and A. Plagne, On small sumsets in $(\mathbb{Z}/2\mathbb{Z})^n$, Combinatorica 24 (2004), no. 1, 53–68.

[EZ11] C. Even-Zohar, On sums of generating sets in $\mathbb{Z}_2^n$, preprint \texttt{arXiv:1108.4902v1} (2011).

[GT09] B. Green and T. Tao, Freiman’s theorem in finite fields via extremal set theory, Combinatorics, Probability and Computing 18 (2009), no. 3, 335–355.

[HP03] F. Hennecart and A. Plagne, On the subgroup generated by a small doubling binary set, European Journal of Combinatorics 24 (2003), no. 1, 5–14.

[Kem60] J. H. B. Kemperman, On small sumsets in an abelian group, Acta Mathematica 103 (1960), no. 1, 63–88.

[Kne53] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, Mathematische Zeitschrift 58 (1953), no. 1, 459–484.
[Kon08] S.V. Konyagin, *On the Freiman theorem in finite fields*, Mathematical Notes 84 (2008), no. 3-4, 435–438.

[Lev06] V. F. Lev, *Critical pairs in abelian groups and Kemperman’s structure theorem*, Int. J. Number Theory 2 (2006), no. 3, 379–396.

[Ruz99] I. Z. Ruzsa, *An analog of Freiman’s theorem in groups*, Astérisque (1999), 323–326.

[San08] T. Sanders, *A note on Freiman’s theorem in vector spaces*, Combinatorics, Probability and Computing 17 (2008), no. 2, 297–305.

Einstein Institute of Mathematics, The Hebrew University, Jerusalem 91904, Israel
E-mail address: chaim.evenzohar@mail.huji.ac.il

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel
E-mail address: seva@math.haifa.ac.il