QUOTIENT SETS IN NONABELIAN GROUPS

VSEVOLOD F. LEV

ABSTRACT. We show that for a finite, nonempty subset A of a group, the quotient set $A^{-1}A := \{a_1^{-1}a_2 \colon a_1, a_2 \in A\}$ has size $|A^{-1}A| \geq \frac{5}{3}|A|$, unless A is densely contained in a coset, or in a union of two cosets of a finite subgroup.

1. Introduction: Background and the Main Result

One of the cornerstones of the additive combinatorics is Kneser's theorem [Kn53, Kn55] relating the size of a sumset in an abelian group to the sizes of the set summands. As shown by Olson [O84], a straightforward, simple-minded analogue of Kneser's theorem for nonabelian groups fails to hold. Many partial extensions of the theorem in the nonabelian settings are known, however; see, for instance, [F73, O84, O86, SW, T13, Z94, H13]. Particularly relevant in our present context are the papers by Freiman [F73], Olson [O86], and Hamidoune [H13].

In [F73], Freiman classified finite, nonempty subsets A of a group with the product set $A^2 := \{a_1a_2 \colon a_1, a_2 \in A\}$ satisfying $|A|^2 < \frac{8}{5}|A|$.

Olson has extended Freiman's result onto products with distinct set factors; namely, as shown in [O84, Theorem 1], if A and B are finite, nonempty subsets of a group, then "normally" the product set $AB := \{ab \colon a \in A, b \in B\}$ has size $|AB| \geq |A| + \frac{1}{2}|B|$.

Improving the *doubling coefficients* $\frac{8}{5}$ and $\frac{1}{2}$ in the Freiman-Olson estimates is a fascinating, mostly open, problem.

Addressing the case where $B = A^{-1}$, Hamidoune [H13] has established some properties of the quotient set $A^{-1}A := \{a_1^{-1}a_2 \colon a_1, a_2 \in A\}$ assuming that $|A^{-1}A| < \frac{5}{3}|A|$.

In this note, under the same assumption $|A^{-1}A| < \frac{5}{3}|A|$, we completely determine the structure of the set A itself, with an if-and-only-if-type classification.

For a subgroup H of a group G, let $N(H)$ denote the normalizer of H in G.

2020 *Mathematics Subject Classification.* Primary 11B75.

Key words and phrases. Small doubling, Sumset, Kneser's theorem.

Theorem 1. *Let A be a finite subset of a group G. Then $|A^{-1}A| < \frac{5}{3}|A|$ if and only if one of the following holds:*

(i) *there is a finite subgroup $H \le G$ such that A is contained in a left H-coset and $|A| > \frac{3}{5}|H|$;*
(ii) *there is a finite subgroup $H \le G$ and elements $a, b \in G$ with $(a^{-1}b)^2 \notin H$ and $a^{-1}b \in N(H)$ such that $A \subseteq aH \cup bH$ and $|A| > \frac{9}{5}|H|$.*

Moreover, in the case (i) we have $A^{-1}A = H$, while in the case (ii) the set $A^{-1}A$ is a disjoint union of H and two double H-cosets of size $|H|$ each.

The coefficient $\frac{5}{3}$ corresponds to a structure threshold: say, if H is a finite subgroup, and $g \in N(H)$ is an element with $g^i \notin H$ for $i \in [1,4]$, then the set $A := g^{-1}H \cup H \cup Hg$ satisfies $|A^{-1}A| = \frac{5}{3}|A|$, while A does not have the structure described in the theorem.

We remark that the ostensible lack of symmetry in the statement of the theorem clears off once we notice that any left coset is a right coset of a conjugate subgroup, and vice versa.

With the exception of Section 5, the rest of the paper is devoted to the proof of Theorem 1. In the next section we formally introduce the notation used and gather some basic facts needed for the proof. In Section 3 we show that conditions (i) and (ii) of Theorem 1 are sufficient for $|A^{-1}A| < \frac{5}{3}|A|$ to hold, and also that they imply the last assertion of the theorem (concerning the structure of the quotient set). Additionally, in Section 3 we prove a lemma that will be used in the course of the proof of necessity in Section 4. Finally, in the concluding Section 5 we state and briefly discuss a conjectural extension of Theorem 1 onto the sets A satisfying $|A^{-1}A| < 2|A|$.

2. Preliminaries: notation and tools

For subsets A and B of a group, we denote by A^{-1} the set of inverses of the elements of A, and by AB the product set:

$$A^{-1} := \{a^{-1} \colon a \in A\} \quad \text{and} \quad AB := \{ab \colon a \in A, b \in B\}.$$

Thus, for instance, $A^{-1}A = \{a^{-1}b \colon a, b \in A\}$.

The subgroup generated by A is denoted by $\langle A \rangle$, and the identity element of the group by 1. A left (right) coset of a subgroup H is a set of the form gH (Hg), where g is an element of the group. A *double* H-coset if a set of the form HgH.

The following lemma summarizes the basic properties of double cosets.

Lemma 1. *If H is a subgroup of a group G, then G is a disjoint union of double H-cosets. A set $S \subseteq G$ is a union of double H-cosets if and only if it is stable under both left and right multiplication by H; that is, if and only if $HS = SH = S$; alternatively, if and only if there is a set $T \subseteq G$ such that $S = HTH$. For $a, b \in G$, we have $HaH = HbH$ if and only if there exist $h_1, h_2 \in H$ such that $b = h_1 a h_2$.*

The *normalizer* of a subgroup H, denoted $N(H)$, is the subgroup consisting of all those group elements g satisfying $gH = Hg$.

Given a finite subset A of a group, and a group element g, by $r(g)$ we denote the number of representations of g in the form $g = a^{-1}b$ with $a, b \in A$. Clearly, r is supported on the quotient set $A^{-1}A$, and $r(g^{-1}) = r(g) \le r(1) = |A|$ for any element g. Moreover, $r(g) = |A|$ if and only if $Ag = A$. Therefore, the number of elements $g \in G$ satisfying $Ag = A$ is the size of the maximal subgroup H such that A is a union of left H-cosets.

For a real x, the largest integer not exceeding x and the smallest integer not smaller than x are denoted $\lfloor x \rfloor$ and $\lceil x \rceil$, respectively.

Lemma 2. *For any finite subgroup H and any group elements a and b, either $aH = Hb$, or $|aH \cap Hb| \le \frac{1}{2}|H|$.*

Proof. Assuming that $aH \cap Hb$ is nonempty, fix an element $g \in aH \cap Hb$. Then $a \in gH$ and $b \in Hg$, whence $|aH \cap Hb| = |gH \cap Hg| = |H \cap g^{-1}Hg|$. The result follows since the intersection in the right-hand side is a subgroup of H. □

Lemma 3. *Suppose that H is a finite subgroup, and a, b are elements of a group. For $aH = Hb$ to hold, it is necessary and sufficient that $a, b \in N(H)$ and $aH = bH$.*

Proof. If $aH = Hb$, then $b \in aH$ whence $a^{-1}b \in H$; equivalently, $b^{-1}a \in H$, or $a \in bH$. As a result, $aH = bH$, and, consequently, $Hb = bH$, so that $b \in N(H)$. In a similar way we get $a \in N(H)$. The opposite direction is trivial: if $a, b \in N(H)$ and $aH = bH$, then $aH = bH = Hb$. □

Lemma 4. *Suppose that H is a subgroup, and $g \notin H$ is an element of a group. For the union $H \cup gH$ to be a subgroup, it is necessary and sufficient that $g^2 \in H$.*

Proof. If $H \cup gH$ is a subgroup, then $g^{-1} \in H \cup gH$ whence, indeed, $g^{-1} \in gH$, and then $g^2 \in H$. Conversely, if $g^2 \in H$, then $H \cup gH$ is easily seen to be closed under the "skew multiplication" $(a, b) \mapsto a^{-1}b$. □

Lemma 5. *Suppose that H is a finite subgroup of a group G. For an element $g \in G$, the double H-coset HgH has size $|HgH| = |H|$ if and only if $g \in N(H)$.*

Proof. Write $S = HgH$. Then $gH \subseteq S$ and $Hg \subseteq S$. Hence, $|S| = |H|$ if and only if $gH = Hg$; that is, if and only if $g \in N(H)$. $\square$

We will use the box principle in the following form.

Lemma 6. *Suppose that A is a finite, nonempty subset of a group G. If $g_1, g_2 \in G$ are group elements with $r(g_1) + r(g_2) > |A|$, then $g_1^{-1}g_2 \in A^{-1}A$.*

Proof. For $i \in \{1, 2\}$, let A_i be the set of all those elements $a \in A$ the inverse of which appears as the first factor in some representation $g_i = a^{-1}b$ with $b \in A$. Thus, $|A_i| = r(g_i)$, and from $r(g_1) + r(g_2) > |A|$ and $A_1, A_2 \subseteq A$ it follows that A_1 and A_2 have a common element; that is, there are $a, b_1, b_2 \in A$ such that $g_1 = a^{-1}b_1$ and $g_2 = a^{-1}b_2$. Consequently, $g_1^{-1}g_2 = b_1^{-1}aa^{-1}b_2 = b_1^{-1}b_2 \in A^{-1}A$. $\square$

We need the following result of Kemperman and Wehn.

Theorem 2 (Kemperman-Wehn)**.** *If A and B are finite, nonempty subsets of a group, then $|AB| \ge |A| + |B| - r(g)$ for any element $g \in AB$.*

Quoting from [O84],

> "Theorem 2 goes back to results of L. Moser and P. Scherk in the case of abelian groups, and was proved for nonabelian groups by J. H. B. Kemperman and (independently) D. F. Wehn. For proof see Kemperman's paper [K56]."

3. Proof of Theorem 1: sufficiency

If G is a group, H is a finite subgroup of G, and A is a subset of G contained in an H-coset and satisfying $|A| > \frac{3}{5}|H|$, then $A^{-1}A = H$ by the box principle, whence $|A^{-1}A| < \frac{5}{3}|A|$. Thus, condition (i) of the theorem is sufficient for A to satisfy $|A^{-1}A| < \frac{5}{3}|A|$, and it also implies the corresponding part of the last assertion of the theorem. We now prove a similar result for condition (ii).

Proposition 1. *Let H be a finite subgroup of a group G, and suppose that $A \subseteq aH \cup bH$ where $a, b \in G$ are elements with $a^{-1}b \in N(H)$ and $(a^{-1}b)^2 \notin H$. If $|A| > \frac{9}{5}|H|$, then $|A^{-1}A| < \frac{5}{3}|A|$; moreover, in this case $A^{-1}A$ is a disjoint union of H and two double H-cosets of size $|H|$ each.*

Proof. The assumption $|A| > \frac{9}{5}|H|$ implies that the cosets aH and bH are disjoint. We write $A = aX \cup bY$ with $X, Y \subseteq H$ and notice that

$$A^{-1}A = (X^{-1}a^{-1} \cup Y^{-1}b^{-1})(aX \cup bY) \\ = ((X^{-1}X) \cup (Y^{-1}Y)) \cup (X^{-1}a^{-1}bY) \cup (Y^{-1}b^{-1}aX). \quad (1)$$

Since $|X| + |Y| = |A| > |H|$, we have either $|X| > \frac{1}{2}|H|$, or $|Y| > \frac{1}{2}|H|$; accordingly, by the box principle, either $X^{-1}X = H$, or $Y^{-1}Y = H$. Thus, $(X^{-1}X) \cup (Y^{-1}Y) = H$. Furthermore, since $a^{-1}b \in N(H)$, we have $a^{-1}bY \subseteq a^{-1}bH = Ha^{-1}b$; consequently, there is a subset $Y' \subseteq H$ such that $a^{-1}bY = Y'a^{-1}b$, and then $X^{-1}a^{-1}bY = X^{-1}Y'a^{-1}b = Ha^{-1}b$, as $X^{-1}Y' = H$ in view of $|X^{-1}|+|Y'| = |X|+|Y| > |H|$. Therefore $|X^{-1}a^{-1}bY| = |H|$. Taking the inverses, we get $|Y^{-1}b^{-1}aX| = |H|$. Hence, $|A^{-1}A| \le 3|H| < \frac{5}{3}|A|$. Next, $X^{-1}a^{-1}bY = Ha^{-1}b = a^{-1}bH$ shows that $X^{-1}a^{-1}bY$ is a double H-coset, and so is its inverse $Y^{-1}b^{-1}aX = Hb^{-1}a = b^{-1}aH$. Finally, the two double H-cosets are disjoint from H and from each other thanks to the assumption $(a^{-1}b)^2 \notin H$. □

Next, we prove a lemma that provides a simple criterion for a given set to satisfy conditions (i) and (ii) of Theorem 1; this lemma will be used in the proof of necessity in the next section.

Lemma 7. *Let H be a finite subgroup of a group G, and suppose that $A \subseteq aH \cup bH$ where $a, b \in G$. If $|A| > \frac{9}{5}|H|$ and $|A^{-1}A| \le 3|H|$, then A satisfies either condition (i), or condition (ii) of Theorem 1, according to whether $(a^{-1}b)^2 \in H$ or $(a^{-1}b)^2 \notin H$.*

Proof. As in the proof of Proposition 1, we write $A = aX \cup bY$ with $X, Y \subseteq H$, and use (1). If $a^{-1}b \notin N(H)$, then $Ha^{-1}b \ne a^{-1}bH$ by the definition of the normalizer subgroup; hence,

$$|X^{-1}a^{-1}b \cap a^{-1}bY| \le |Ha^{-1}b \cap a^{-1}bH| \le \frac{1}{2}|H|$$

by Lemma 4. Without loss of generality, we assume $a, b \in A$ whence $1 \in X \cap Y$. Consequently, both $X^{-1}a^{-1}b$ and $a^{-1}bY$ lie in $X^{-1}a^{-1}bY$, and we conclude that

$$|X^{-1}a^{-1}bY| \ge |X^{-1}a^{-1}b \cup a^{-1}bY| = |X| + |Y| - |X^{-1}a^{-1}b \cap a^{-1}bY| > |H|.$$

Taking the inverses, we get $|Y^{-1}b^{-1}aX| > |H|$, and then from (1) we obtain $|A^{-1}A| > 3|H|$, contradicting the assumptions. Thus, $a^{-1}b \in N(H)$. By Lemma 3, the set $F := H \cup (a^{-1}b)H$ is a subgroup if and only if $(a^{-1}b)^2 \in H$. In this case $A \subseteq aF$ and $|A| > \frac{9}{5}|H| = \frac{9}{10}|F| > \frac{3}{5}|F|$ so that A satisfies condition (i). Finally, if $(a^{-1}b)^2 \notin H$, then A satisfies condition (ii). □

4. Proof of Theorem 1: necessity

Let $A \subseteq G$ be a finite subset with $|A^{-1}A| < \frac{5}{3}|A|$, and suppose that the assertion is true for all sets $\mathcal{A} \subseteq G$ satisfying either $|\mathcal{A}^{-1}\mathcal{A}| < |A^{-1}A|$, or $|\mathcal{A}^{-1}\mathcal{A}| = |A^{-1}A|$ and $|\mathcal{A}| > |A|$. We show that A is contained ether in a coset, or in a union of two cosets, as specified in the conditions (i) and (ii) of the theorem.

We write $Q := A^{-1}A$; thus, $|A| > \frac{3}{5}|Q|$.

Recall, that for an element $g \in G$, we have denoted by $r(g)$ the number of representations $g = a^{-1}b$ with $a, b \in A$. By Theorem 2,

$$r(g) \ge 2|A| - |Q|, \quad g \in Q.$$

Let $Q^+ := \{g \in Q\colon r(g) > |Q| - |A|\}$. We notice that Q^+ is nonempty as, for instance, it contains the identity element. Also, Q^+ is stable under inversion.

For any $g \in Q$ and $g_0 \in Q^+$ we have

$$r(g) + r(g_0) > (2|A| - |Q|) + (|Q| - |A|) = |A|.$$

Hence, $g_0^{-1}g \in Q$ by Lemma 6, implying $g \in g_0Q$. It follows that $g_0Q = Q$ for any $g_0 \in Q^+$. Therefore, $Q^+Q = Q$ and, considering the inverses, $QQ^+ = Q$. Letting $F := \langle Q^+ \rangle$, we furthermore conclude that $QF = FQ = Q$. As a result,

$$(AF)^{-1}(AF) = FA^{-1}AF = FQF = FQ = Q = A^{-1}A. \tag{2}$$

From these equalities and by the choice of A, either $AF = A$, or there is a finite subgroup $H \le G$ such that one of the following holds:

- AF is contained in a left H-coset, $|AF| > \frac{3}{5}|H|$, and $(AF)^{-1}(AF) = H$;
- AF meets exactly two left H-cosets, $|AF| > \frac{9}{5}|H|$, and $(AF)^{-1}(AF)$ is a disjoint union of H and two double H-cosets of size $|H|$ each.

In the first case, recalling (2) we get $Q = (AF)^{-1}(AF) = H$; as a result, A is contained in a single left H-coset, and $|A| > \frac{3}{5}|Q| = \frac{3}{5}|H|$; thus, A satisfies condition (i).

In the second case, with (2) in mind, $|Q| = |(AF)^{-1}(AF)| = 3|H|$ showing that $|A| > \frac{3}{5}|Q| = \frac{9}{5}|H|$. By Lemma 7, the set A satisfies condition (i) or condition (ii).

Having ruled out the exceptional cases where AF is contained in a single coset, or in a union of two cosets, we proceed with the proof using the additional assumption

$$AF = A, \quad F = \langle Q^+ \rangle. \tag{3}$$

Thus, A is a union of left F-cosets, and so is $Q = \cup_{a\in A} a^{-1}A$. It follows that $F \subseteq Q$. Indeed, we have $F = Q^+$: here the inclusion $Q^+ \subseteq F$ is trivial, while $F \subseteq Q^+$ follows by observing that if $g \in F$, then $r(g) = |A| > |Q| - |A|$ by (3), whence $g \in Q^+$.

As we have just observed, if $g \in F$, then $r(g) = |A|$. Conversely, if $g \in Q$ is an element with $r(g) = |A|$, then $r(g) > |Q| - |A|$ showing that $g \in Q^+ = F$. As a bottom line, $r(g) = |A|$ if and only if $g \in F$.

If $g \in G$ is an element with $r(g) > |Q| - |A|$, then $g \in Q^+ = F$, whence, indeed, $r(g) = |A|$. Thus, we have

$$2|A| - |Q| \le r(g) \le |Q| - |A|$$

for all elements $g \in Q$ with $r(g) < |A|$. We remark that the first of the two inequalities is just Theorem 2, but the second one is new and, in our view, is quite amazing.

We write $k := |A|/|F|$. If $k = 1$, then A is a single left F-coset; therefore A satisfies condition (i). If $k = 2$, then A is a union of two left F-cosets and $|A^{-1}A| < \frac{5}{3}|A| < 4|F|$; therefore, applying Lemma 7, we conclude that A satisfies condition (ii). Suppose thus that $k \ge 3$.

Since A and Q are unions of left F-cosets, both $|A|$ and $|Q|$ are divisible by $|F|$. From this observation and $|Q| < \frac{5}{3}\,|A| = \frac{5}{3}\,k|F|$, we get

$$|Q| \le \left(\left\lceil \frac{5}{3}\,k \right\rceil - 1 \right) |F|. \tag{4}$$

Furthermore, to any representation $g = a^{-1}b$ with $a, b \in A$ there correspond $|F|$ representations $g = (fa)^{-1}(fb),\ f \in F$. (Notice that these representations are "legal" in the sense that both af and bf lie in A.) Therefore, also $r(g)$ is divisible by $|F|$, for any $g \in G$. Moreover, since g is constant on any left F-coset, for any given positive integer m, the number of elements $g \in Q$ with $r(g) = m$ is divisible by $|F|$;

Let Q_0 and Q_1 denote the sets of all those elements $g \in Q$ with $r(g) \le \frac{1}{2}\,|A|$ and with $r(g) > \frac{1}{2}\,|A|$, respectively. We write $N_0 := |Q_0|$ and $N_1 := |Q_1|$ and define

$$\sigma_0 := \sum_{g\in Q_0} r(g) \text{ and } \sigma_1 := \sum_{g\in Q_1} r(g);$$

thus, $N_0 + N_1 = |Q|$, $\sigma_0 + \sigma_1 = |A|^2$, and N_0, N_1, σ_0, and σ_1 are all divisible by $|F|$. The sum σ_0 has N_0 terms, each of them divisible by $|F|$ and not exceeding $\frac{1}{2}\,|A| = \frac{1}{2}\,k|F|$; therefore, $\sigma_0 \le \left\lfloor \frac{1}{2}\,k \right\rfloor |F| N_0$. The sum σ_1 has N_1 terms, of them $|F|$ are equal to $|A|$, and each of the remaining $N_1 - |F|$ terms does not exceed $|Q| - |A|$. Therefore,

$$\sigma_1 \le |F||A| + (N_1 - |F|)(|Q| - |A|) = 2|F||A| - |Q||F| + N_1|Q| - N_1|A|.$$

Letting $n := N_1/|F|$ and $q := |Q|/|F|$, we obtain

$$\begin{aligned} |A|^2 &\le \left\lfloor \frac{1}{2}\,k \right\rfloor |F|N_0 + 2|F||A| - |Q||F| + N_1|Q| - N_1|A|, \\ k^2|F| &\le \left\lfloor \frac{1}{2}\,k \right\rfloor (N_0 + N_1) + 2|A| - |Q| + \left(q - \left\lfloor \frac{1}{2}k \right\rfloor \right) N_1 - kN_1, \\ k^2 &\le \left(\left\lfloor \frac{1}{2}\,k \right\rfloor - 1 \right) q + 2k + \left(q - k - \left\lfloor \frac{1}{2}\,k \right\rfloor \right) n. \end{aligned}$$

Since $q \le \left\lceil \frac{5}{3}\,k \right\rceil - 1$ by (4), we derive that

$$k^2 \le \left(\left\lfloor \frac{1}{2}\,k \right\rfloor - 1 \right) \left(\left\lceil \frac{5}{3}\,k \right\rceil - 1 \right) + 2k + \left(\left\lceil \frac{5}{3}\,k \right\rceil - 1 - k - \left\lfloor \frac{1}{2}\,k \right\rfloor \right) n.$$

A routine analysis shows that for $k \ge 3$, the last inequality is false if $n \le k$. (Hint: exact computation for $3 \le k \le 6$, substituting $n = k$ and using the crude estimates $\lfloor k/2 \rfloor \le k/2$ and $\lceil 5k/3 \rceil \le (5k+2)/3$ for $k \ge 7$.) Therefore $n \ge k + 1$; that is,

$$|Q_1| = N_1 \ge |A| + |F| \quad (k \ge 3). \tag{5}$$

From Lemma 6 and the definition of the set Q_1, we have $g_1^{-1}g_2 \in Q$ for any $g_1, g_2 \in Q_1$. Consequently, $Q_1^{-1}Q_1 \subseteq Q$ whence, by the choice of A, there is a finite subgroup $H \le G$ such that one of the following holds:

1. Q_1 is contained in a left H-coset and $|Q_1| > \frac{3}{5}\,|H|$;
2. Q_1 meets exactly two left H-cosets and $|Q_1| > \frac{9}{5}\,|H|$.

We investigate these two cases separately.

Case 1: There is a finite subgroup $H \le G$ such that Q_1 is contained in a left H-coset and $|Q_1| > \frac{3}{5}\,|H|$. We have

$$|A| < |Q_1| \text{ and } Q_1 \subseteq H = Q_1^{-1}Q_1 \subseteq Q; \tag{6}$$

here the inequality follows from (5), the first inclusion from $1 \in Q_1$, the equality from $|Q_1| > \frac{3}{5}\,|H|$ and the box principle, and the second inclusion from Lemma 6.

Consider the coset decomposition $A = A_1 \cup \dots \cup A_n$ where $n = |AH|/|H|$ and $A_1, \dots, A_n$ are nonempty and reside in pairwise distinct left H-cosets. We number the sets A_i so that $|A_1| = \min\{|A_i| \colon 1 \le i \le n\}$. Fix $a_1 \in A_1$. In view of $a_1^{-1}A_2 \cup \dots \cup a_1^{-1}A_n \subseteq Q \setminus H$ and (6),

$$|Q| \ge |H| + (|A_2| + \dots + |A_n|) > |A| + \left(1 - \frac{1}{n}\right) |A| = \left(2 - \frac{1}{n}\right) |A|.$$

Since $|Q| < \frac{5}{3}\,|A|$, we conclude that $n = 1$ or $n = 2$. If $n = 1$, then A resides in a single H-coset; moreover, $|A| > \frac{3}{5}\,|Q| > \frac{3}{5}\,|H|$, showing that A satisfies condition (i).

Suppose now that $n = 2$. Fix $a_1 \in A_1$ and $a_2 \in A_2$. Then

$$\frac{5}{3}\,|A| > |Q| = |H| + |Q \setminus H| \ge |H| + |a_1^{-1}A_2| = |H| + (|A| - |A_1|)$$

whence $|A_1| > |H| - \frac{2}{3}\,|A| \ge \frac{1}{3}\,|A|$. Similarly, from

$$\frac{5}{3}\,|A| > |Q| = |H| + |Q \setminus H| \ge |H| + |a_1^{-1}A_2| = |H| + |A_2|$$

we obtain $|A_2| < \frac{2}{3}\,|A|$. Therefore,

$$\frac{1}{3}\,|H| < |A_1| \le \frac{1}{2}\,|A| \le |A_2| < \frac{2}{3}\,|A|. \tag{7}$$

Consider the set $S := (A_1 \times A_2) \cup (A_2 \times A_1)$ and the mapping $\varphi \colon S \to Q$ defined by $\varphi(a,b) := a^{-1}b$. Since the image $\mathrm{Im}(\varphi)$ is disjoint from H, we have $\mathrm{Im}(\varphi) \subseteq Q \setminus Q_1$. By the definition of the set Q_1, every element of $\mathrm{Im}(\varphi)$ has at most $\frac{1}{2}\,|A|$ inverse images in S. As a result,

$$|Q| - |Q_1| \ge \mathrm{Im}(\varphi) \ge \frac{|S|}{|A|/2} = 4\frac{|A_1||A_2|}{|A|}.$$

Comparing this estimate with (5) and with the assumption $|Q| < \frac{5}{3}\,|A|$, we obtain $|A|^2 > 6|A_1||A_2|$. This leads to $|A_2| > (2 + \sqrt{3})|A_1|$, contradicting (7).

Case 2: There is a finite subgroup $H \le G$ such that Q_1 meets exactly two left H-cosets and $|Q_1| > \frac{9}{5}\,|H|$. Since $1 \in Q_1$, we can write $Q_1 = B_0 \cup B_1$ where $B_0 \subseteq H$ and $B_1 \subseteq gH$ with some $g \in G \setminus H$. From $B_1 = Q_1 \setminus H$ and $Q_1^{-1} = Q_1$ we get $B_1^{-1} = Q_1^{-1} \setminus H = Q_1 \setminus H = B_1 \subseteq gH$. Thus, $B_1 \subseteq gH \cap Hg^{-1}$. By Lemma 2, and in view of

$$|B_1| = |Q_1| - |B_0| \ge |Q_1| - |H| > \frac{4}{5}\,|H|$$

we have $gH = Hg^{-1}$; that is, $H = gHg$, and it is easily seen that $H \cup gH$ is a subgroup. Moreover, $Q_1 = B_0 \cup B_1 \subseteq H \cup gH$ and $|Q_1| > \frac{9}{5}\,|H| > \frac{3}{5}\,|H \cup gH|$. This takes us back to the Case 1 considered above.

5. Concluding remarks

What is the structure of a finite set A with $\frac{5}{3}|A| < |A^{-1}A| < 2|A|$? We make the following conjecture.

Conjecture 1. *Let A be a finite subset of a group G, and let n be a positive integer. If*

$$|A^{-1}A| < \left(2 - \frac{1}{n+1}\right) |A|,$$

then there are a finite subgroup $H \le G$ and a subset $A_0 \subseteq A$ of size $|A_0| \le n$ contained in a single left $N(H)$-coset such that $A \subseteq A_0H$, $|A_0H| = |A_0||H|$, and $|A| > \left(2 - \frac{1}{n+1}\right)^{-1} (2|A_0| - 1)|H|$.

Moreover, $A^{-1}A = A_0^{-1}A_0H$ and $|A^{-1}A| = (2|A_0| - 1)H$.

The inequality $|A| > \left(2 - \frac{1}{n+1}\right)^{-1} (2|A_0| - 1)|H|$ is worth commenting on. It can be shown that, along with other conclusions of the conjecture, it implies $|A| \le |A_0H| < |A| + \frac{n}{2n+1} |H|$. Thus, this inequality ensures that A is a *dense* subset of the set A_0H.

The particular case $n = 1$ of the conjecture follows from Olson's theorem, while the case $n = 2$ is the main result of this paper.

As the following proposition shows, in the appropriate range, Conjecture 1 gives a necessary and sufficient condition for A to satisfy $|A^{-1}A| < \left(2 - \frac{1}{n+1}\right) |A|$.

Proposition 2. *Let A be a finite subset of a group G, and let n be a positive integer. Suppose that there are a finite subgroup $H \le G$ and a subset $A_0 \subseteq A$ of size $|A_0| \le n$ contained in a single left $N(H)$-coset such that $A \subseteq A_0H$, $|A_0H| = |A_0||H|$, and $|A| > \left(2 - \frac{1}{n+1}\right)^{-1} (2|A_0| - 1)|H|$. If, in addition, $|A^{-1}A| < 2|A|$ then, indeed, $|A^{-1}A| < \left(2 - \frac{1}{n+1}\right) |A|$.*

We omit the proof since, anyway, Proposition 2 is not of much importance as long as Conjecture 1 remains open.

References

[F73] G. Freiman, Groups and the inverse problems of the additive number theory (Russian), *Number-theoretic studies in the Markov spectrum and in the structural theory of set addition (Russian)*, 175–183, Kalinin. Gosudarstv. Univ., Moscow, 1973.

[H13] Y.O. Hamidoune, Two inverse results, *Combinatorica* **33** (2) (2013), 217–230.

[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.

[K56] J.H.B. Kemperman, on complexes in a semigroup, *Indag. Math.* **18** (1956), 247–254.

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

[O86] ———, On the symmetric difference of two sets in a group, European J. Combin. **7** (1) (1986), 43–54.

[SW] O. Serra and M. Wötzel, On a nonabelian Kneser theorem, *preprint*.

[T13] T. Tao, Noncommutative sets of small doubling, *European Journal of Combinatorics* **34** (8) (2013), 1459–1465.

[Z94] G. Zemor, A generalization to noncommutative groups of a theorem of Mann, *Discrete Mathematics* **126** (1994), 365–372.

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

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