PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Xxxx XXXX, Pages 000–000
S 0002-9939(XX)0000-0

ON FINITE SUBSETS OF NONABELIAN GROUPS WITH SMALL DOUBLING

GREGORY A. FREIMAN

(Communicated by Matthew A. Papanikolas)

Abstract. We give a detailed and clear exposition of the basic result describing the structure of a finite subset A of a nonabelian group G with a small doubling $|A^2| < 1.5|A|$.

1. Introduction

Let G be a group, A be a finite subset of G, $|A|$ be the number of elements in A, $|A| = k$,

$$\begin{aligned} A &= \{a_0, a_1, ..., a_{k-1}\}\ , \\ A^2 &= \{x : \quad x = a_i a_j;\ \ 0 \le i, j \le k-1\}\ . \end{aligned}$$

Definition. The quotient $\frac{|A^2|}{|A|} = C(A)$ is said to be the doubling coefficient of A.

The structure of a finite subset A of a nonabelian group G with a small doubling of $|A^2| < 1.6|A|$ was found in 1973 in [5]. These results were published in a provincial Russian edition. The proofs were too short and the exposition was far from clear (for example, the size of the proof of the main result of this note was less than 1 page). We now see a renewed interest in the study of sets with small doubling in groups (see [1]-[4],[6]-[8], where a very natural concept of an "approximate group" was introduced which, roughly speaking, is a symmetric subset of a group with a small doubling). We feel therefore that a detailed presentation and continuation of the study which we began in [1] would be desirable. In this paper we begin with the case $C(A) < 1.5|A|$.

2. Formulation of the main result

Theorem. *If*

$$|A^2| < 1.5|A|\ , \tag{1}$$

then the following assertions hold:

(a) *The set $H = A^{-1}A = AA^{-1}$ is an A-invariant subgroup of G, $H \le G$.*
(b) *If $A^2 \cap H \ne \emptyset$, then $A^2 = H$.*
(c) *If $A^2 \cap H = \emptyset$, then the set A^2 is a coset of H.*

Received by the editors May 18, 2010 and, in revised form, March 27, 2011.
1991 *Mathematics Subject Classification.* Primary 20-XX; Secondary 11P70.

3. The set $H = A^{-1}A$ is a subgroup of G

We will show now that for any two elements of $a_\alpha \in A$ and $a_\beta \in A$ we have

$$|a_\alpha A \cap a_\beta A| > \frac{k}{2} \ . \tag{2}$$

Indeed

$$a_\alpha A \cup a_\beta A \subseteq A^2 \tag{3}$$

and

$$a_\alpha A \cup a_\beta A = [a_\alpha A \setminus (a_\alpha A \cap a_\beta A)] \cup a_\beta A \tag{4}$$

and the last union is a partition.

Therefore in view of $|A| = k$, $|A|^2 < 1.5|A|$, (1), (3) and (4) we have

$$|a_\alpha A \setminus (a_\alpha A \cap a_\beta A)| < \frac{k}{2}$$

so that $|a_\alpha A \cap a_\beta A| > \frac{k}{2}$; i.e., (2) is valid.

Let

$$a_\alpha A \cap a_\beta A = \{x_1, x_2, ..., x_s\}, \tag{5}$$

where, because of (2), $s > \frac{k}{2}$.

In view of (5) we have, for each $1 \leq i \leq s$,

$$x_i = a_\alpha d_i = a_\beta f_i \ , \tag{6}$$

where $d_i, f_i \in A$ for all $i \in \{1, \dots, s\}$. Note that if $i \neq j$, then $d_i \neq d_j$ and $f_i \neq f_j$.

From (6) we obtain

$$a_\alpha^{-1} a_\beta = d_i f_i^{-1}, \ i = 1, 2, ..., s \ . \tag{7}$$

As we have noticed, all d_i in these s representations are different and all f_i are different.

Let us now take any other pair $a_\gamma \in A$ and $a_\delta \in A$. We would have as in (2)-(5),

$$|a_\gamma A \cap a_\delta A| > \frac{k}{2} \ ,$$

$$a_\gamma A \cap a_\delta A = \{y_1, y_2, ..., y_p\}, \ p > \frac{k}{2}; \tag{8}$$

and now as in (6) we have

$$y_j = a_\gamma e_j = a_\delta g_j \ ,$$

where $e_j, g_j \in A$ for each $1 \leq j \leq p$, and finally

$$a_\gamma^{-1} a_\delta = e_j g_j^{-1} \ , \ j = 1, 2, ..., p \ . \tag{9}$$

As above, we have $|\{e_1, \dots, e_p\}| = p = \{g_1, \dots, g_p\}|$.

From (7) and (9) we get the equalities

$$a_\alpha^{-1} a_\beta a_\gamma^{-1} a_\delta = d_i f_i^{-1} e_j g_j^{-1} \tag{10}$$

for each i, j, where $1 \leq i \leq s$ and $1 \leq j \leq p$.

Now look at the product $f_i^{-1} e_j$. Here $f_i \in \{f_1, f_2, ..., f_s\} = F$ and $e_j \in \{e_1, e_2, ..., e_p\} = E$. We have $F \subset A, E \subset A$, where because of (2), (5), (8) we have $|F| > \frac{k}{2}$ and $|E| > \frac{k}{2}$ and therefore $F \cap E \neq \emptyset$. This means that there exist two values i_0 and j_0 for which $f_{i_0} = e_{j_0}$ and therefore $f_{i_0}^{-1} e_{j_0} = e$, where e is the identity element of G.

From (10), taking $i = i_0$ and $j = j_0$, we get

$$a_\alpha^{-1} a_\beta a_\gamma^{-1} a_\delta = d_{i_0} g_{j_0}^{-1} \ . \tag{11}$$

We see that for every choice of $1 \le \alpha \le k, 1 \le \beta \le k, 1 \le \gamma \le k$ and $1 \le \delta \le k$, there exist two elements $d_{i_0} \in A$ and $g_{j_0} \in A$ for which (11) is valid, which means that

$$(A^{-1}A)^2 \subseteq AA^{-1} \tag{12}$$

since $a_\alpha, a_\beta, a_\gamma, a_\delta$ run over the set A independently.

Let us now begin the same proof in a different way, taking any two elements $a_{\alpha'} \in A$ and $a_{\beta'} \in A$ and looking at the intersection of the sets $Aa_{\alpha'}$, and $Aa_{\beta'}$ instead of $a_\alpha A \cap a_\beta A$. Instead of the left side in (7) we would obtain the term $a_{\alpha'} a_{\beta'}^{-1}$ and further the equality

$$a_{\alpha'} a_{\beta'}^{-1} a_{\gamma'} a_{\delta'}^{-1} = d_{j'_0}^{-1} g_{j'_0}$$

instead of (11), which means instead of (12),

$$(AA^{-1})^2 \subseteq A^{-1}A \ . \tag{13}$$

Remembering that the identity element $e \in AA^{-1}$, from (13) we obtain

$$AA^{-1} \subseteq A^{-1}A \ . \tag{14}$$

In the same way we obtain from (12),

$$A^{-1}A \subseteq AA^{-1} \ . \tag{15}$$

Thus, in view of (14) and (15),

$$H = AA^{-1} = A^{-1}A \ . \tag{16}$$

This equality together with (12) gives

$$H^2 = (A^{-1}A)^2 \subseteq A^{-1}A = H \ .$$

We see that H is a finite subset of a group G closed under multiplication; i.e., H is a (finite) subgroup of G. The main part of (a) is proved.

4. The order of H is small, $|H| \le |A^2| < 1.5k$

There are k^2 products of the form $a_i a_j, a_i \in A, a_j \in A$. These products are elements of the set A^2 of cardinality $|A^2| < \frac{3}{2}k$. Thus, by Dirichlet's principle, there exists an element $z \in A^2$ which has u different representations in the form $a_i a_j$, $a_i, a_j \in A$:

$$z = a_{i_s} a_{j_s}, \qquad 1 \le s \le u, \tag{17}$$

where

$$u > \frac{k^2}{\frac{3}{2}k} = \frac{2}{3}k \ . \tag{18}$$

Now choose two elements a_α and a_β where $1 \le \alpha, \beta \le k$ and, in the same way as for (2), we show that

$$v = |Aa_\alpha \cap Aa_\beta| > \frac{k}{2} \ . \tag{19}$$

This set may be described in two ways:

$$\begin{aligned} Aa_\alpha \cap Aa_\beta &= \{c_1a_\alpha, c_2a_\alpha, ..., c_va_\alpha\} \\ &= \{q_1a_\beta, q_2a_\beta, ..., q_va_\beta\}, \end{aligned}$$

where

(20) $$c_ma_\alpha = q_ma_\beta \ , \ c_m \in A \ , \ q_m \in A \ , \ 1 \leq m \leq v,$$

and therefore

(21) $$a_\alpha a_\beta^{-1} = c_m^{-1}q_m \in H$$

(recall that H is a subgroup of G).

Each element of the coset zH, because of (17) and (21), may be written in the form

(22) $$a_{i_s}a_{j_s}c_m^{-1}q_m \in zH \ .$$

Because of (17), $a_{i_s}a_{j_s}$ is equal to each of the u products in which a_{j_s} takes u different values. Because of (20), $c_m^{-1}q_m$ is equal to v different products, and therefore c_m takes v different values. From (18) and (19) we see that $u \geq \frac{2}{3}k$ and $v > \frac{k}{2}$, and therefore we can find $j_s = j_{s_0}$ and $m = m_0$ so that $a_{s_0} = c_{m_0}$. It then follows from (22) that

(23) $$a_{i_s}a_{j_s}c_m^{-1}q_m = a_{i_{s_0}}q_{m_0} \ .$$

It follows from (22) and (23) that

(24) $$zH \subseteq A^2,$$

and from here we get

(25) $$|H| \leq |A^2| < 1.5k \ .$$

5. A^2 is a left coset of a subgroup H

Take any two elements a_α and a_β from A. We have

$$a_\alpha a_\beta \in A^2 \ .$$

In the same way as for (2), we can show that for two sets $A^{-1}a_\alpha$ and Aa_β^{-1} we get

(26) $$t = |A^{-1}a_\alpha \cap Aa_\beta^{-1}| > \frac{k}{2} \ .$$

Indeed, $A^{-1}a_\alpha$ and Aa_β^{-1} are both of cardinality k and both are subsets of H, in view of (16). Using $|H| < \frac{3}{2}k$, we obtain (26).

This set may be described in two ways:

$$\begin{aligned} A^{-1}a_\alpha \cap Aa_\beta^{-1} &= \{b_1^{-1}a_\alpha, b_2^{-1}a_\alpha, ..., b_t^{-1}a_\alpha \\ &= \{h_1a_\beta^{-1}, h_2a_\beta^{-1}, ..., h_ta_\beta^{-1}\}, \end{aligned}$$

where

$$b_l^{-1}a_\alpha = h_la_\beta^{-1} \ , \ b_l \in A, \ h_l \in A \ ,$$

and therefore

(27) $$a_\alpha a_\beta = b_lh_l \ , \ 1 \leq l \leq t.$$

Now take the set

$$a_\beta^{-1}a_\alpha^{-1}A^2 \ . \tag{28}$$

Now take one more pair a_γ and a_s, elements from A. As in (27) we have

$$a_\gamma a_\delta = l_n r_n, \quad 1 \le n \le u \ , \tag{29}$$

where $u > \frac{k}{2}$, i.e. u representations of $a_\gamma a_\delta$ as products of pairs of elements from A.

Taking an element $a_\beta^{-1}a_\alpha^{-1}a_\gamma a_\delta$ from the set (28), we have, using (27) and (29), tu representations

$$a_\beta^{-1}a_\alpha^{-1}a_\gamma a_\delta = h_l^{-1}b_l^{-1}l_n r_n \ ,$$

where $1 \le l \le t$, $1 \le n \le u$.

Because we have $t > \frac{k}{2}$ and $n > \frac{k}{2}$ we can find $l = l_0$ and $n = n_0$ such that $b_{l_0} = l_{n_0}$ and so

$$h_{l_0}^{-1}b_{l_0}^{-1}l_{n_0}r_{n_0} = h_{l_0}^{-1}r_{n_0}. \tag{30}$$

From (30) it follows that

$$a_\beta^{-1}a_\alpha^{-1}A^2 \subset H;$$

further

$$A^2 \subset a_\alpha a_\beta H \ , \tag{31}$$

and in view of (25),

$$|A^2| = |H| \ . \tag{32}$$

6. End of the proof

We have two possibilities:

(d) $A^2 \cap H \neq \emptyset$,

(e) $A^2 \cap H = \emptyset$.

In the case (d) there exists an element $a_\alpha a_\beta \in A^2 \cap H$, and from (31) it follows that $A^2 \subseteq H$. However, $|H| = |A^2|$ by (32), and we conclude that $H = A^2$. The proof of (b) is complete. In this case, H is A-invariant.

In case (e) from (31) and (32) we see that $A^2 = a_\alpha a_\beta H$ for some α and β; i.e., A^2 is a coset of H, completing the proof of (c). It remains to show that H is A-invariant. By (16), $a_\alpha^{-1}a_\beta \in A^{-1}A = H$ for all $a_\alpha, a_\beta \in A$. If, in addition, $a_\gamma \in A$, then

$$a_\gamma a_\alpha^{-1}a_\beta a_\gamma^{-1} \in (AA^{-1})^2 = H,$$

and thus

$$a_\alpha^{-1}a_\beta \in a_\gamma^{-1}Ha_\gamma = H \tag{33}$$

for all $\alpha, \beta, \gamma \in \{1, \dots, k\}$. It follows from (33) that $A^{-1}A \subseteq a_\gamma^{-1}Ha_\gamma$. Since, by (16), $A^{-1}A = H$, we get $H = a_\gamma^{-1}Ha_\gamma$, completing the proof of (a).

Acknowledgements

The author is deeply grateful to Prof. Y. Berkovich for his advice and help in the course of writing this paper. He thanks the referee for pointing out a paper of Y. O. Hamidoune; see [9]. This preprint contains several related results and also some references, such as L. Husbands's master's thesis and Terence Tao's blog.

References

1. E. Breuillard, B. Green, Approximate groups, I: The torsion-free nilpotent case, preprint arXiv: 0906. 3598vl [mathCO] 19 June 2009.
2. E. Breuillard, B. Green, Approximate groups, II: The solvable linear case, preprint arXiv: 0907.0927.
3. E. Breuillard, B. Green, T. Tao, Approximate subgroups of linear groups, preprint.
4. D. Fisher, N.H. Katz, I. Peng, On Freiman's theorem in nilpotent groups, preprint arXiv: 0901.1409vl [mathCO] 11 Jan. 2009.
5. G. A. Freiman, Groups and the inverse problems of additive number theory. Kalinin Gos. Univ. Moskow (Russian) (1973) 175-183. MR0435006 (55:7968)
6. E. Hrushovski, Stable group theory and approximate subgroups, preprint arXiv: 0909.2190, 2009
7. B. Green, Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak, preprint arXiv: 0911.335vl (mathNT] 17 Nov. 2009.
8. T. Tao, Product set estimates for non-commutative groups. Combinatorica 28(5) (2008) 547-594. MR2501249 (2010b:11017)
9. Y. O. Hamidoune, Two inverse results, preprint arxiv: 1006.5074v1, 25 June 2010.

Department of Mathematics, Tel Aviv University, Ramat Aviv, Tel Aviv, Israel