Mathematical Problems of Computer Science 42, 5–16, 2014.

Zero-Free Sets in Abelian Groups

Vahe G. Sargsyan

Institute for Informatics and Automation Problems of NAS RA
e-mail: vahe_sargsyan@ymail.com, vahe_sargsyan@ipia.sci.am

Abstract

The subset A of the group G is called *zero-free* if the equation $x+y+z=0$ has no solutions in the set A. The upper and lower estimates were obtained for the maximum cardinality of the zero-free set in an Abelian group, and the asymptotic behavior of the logarithm of the number of zero-free sets in an Abelian group was established.

Keywords: Sum-free set, Characteristic function, Group, Progression, Coset.

1. Introduction

Let G be a set with a certain addition operation on it. The subset $A \subseteq G$ is called *sum-free* (SFS) if the equation $x+y=z$ has no solutions in the set A. The family of all SFS in G we denote by $SF(G)$. For natural numbers m and n the set of natural numbers x, such that $m \leq x \leq n$, we denote by $[m,n]$.

In 1988, P. Cameron and P. Erdös [1] assumed that $SF([1,n]) = O(2^{n/2})$. In particular, they proved that there exist constants c_0 and c_1 such that $|SF([[n/3],n])| \sim c_0 2^{n/2}$ for even n, and $|SF([[n/3],n])| \sim c_1 2^{n/2}$ for odd n.

N. Calkin [2] and, independently, N. Alon [3] proved that[1] $\log |SF([1,n])| \leq (n/2)(1+\bar{o}(1))$.

The proof of the Cameron-Erdös hypothesis and the asymptotic behavior of the number of SFS in the interval $[1,n]$ were found by Sapozhenko [4] and, independently, by B. Green [5]. It is proved that $|SF([1,n])| \sim c(n)2^{n/2}$, where the constant $c(n)$ depends on the parity of n.

In 1991, N. Alon [3] proved that the number of SFS of an arbitrary finite group does not exceed $2^{n/2+\bar{o}(n)}$. Further, the given result became more accurate for different subclasses of finite Abelian groups.

In 2002, A. A. Sapozhenko [6] and, independently, Lev-Luczak-Schoen [7] obtained the asymptotics of maximum possible number of SFS for finite Abelian groups containing at least one subgroup of index 2. The group of residues modulo n is denoted by Z_n.

In 2002 V. Lev and T. Schoen [8] proved that if p is a sufficiently large prime number, then the following estimates are true:

$$2^{\lfloor (p-2)/3 \rfloor}(p-1)(1+O(2^{-\varepsilon_1 p})) \leq |SF(Z_p)| \leq 2^{p/2-\varepsilon_2 p},$$

[1] hereinafter $\log x = \log_2 x$

where ε_1 and ε_2 are positive constants.

In 2005, B. Green and I. Ruzsa [9] using the Fourier transform, obtained the asymptotics of the logarithm of the number of SFS in finite Abelian groups. They proved that for any finite G Abelian group $\log|SF(G)| \sim \lambda(G)$ is true, where $\lambda(G)$ is the maximum cardinality SFS in G.

In 2009, A.A. Sapozhenko [10] obtained the asymptotic behavior of the number of SFS in the groups of prime order.

Theorem 1: *For any $\alpha \in \{-1, 1\}$ there exists a constant c_α, such that for any $\varepsilon > 0$ there exists a natural number N, such that for any simple p of the form $p \equiv \alpha \pmod 3$, such that $p > N$, the following inequalities are performed:*

$$1 \le \frac{|SF(Z_p)|}{c_\alpha (p-1) 2^{\lfloor (p-2)/3 \rfloor}} < 1 + \varepsilon.$$

As to the problem of finding the maximum cardinality SFS in an Abelian group, it is finally resolved.

In 1969 H. P. Yap and P. Diananda [11] got the upper and lower estimates of maximum cardinality SFS in an Abelian group, showing that

Theorem 2: *Let G be an Abelian group of the order n. Then the following statements are true:*

(i) *if n has a prime divisor comparable with 2 modulo 3, then*

$$\lambda(G) = \frac{n}{3} \cdot \left(1 + \frac{1}{p}\right),$$

where p is the smallest prime divisor of n, comparable to 2 modulo 3,

(ii) *if it does not have prime divisors comparable with 2 modulo 3, but $3|n$, then*

$$\lambda(G) = \frac{n}{3},$$

(iii) *if all prime divisors of n have the form $p \equiv 1 \pmod 3$, then*

$$\frac{n}{3} \cdot \left(\frac{\nu - 1}{\nu}\right) \le \lambda(G) \le \frac{n-1}{3},$$

where ν is the exponent of the group G.

The final solution of the problem of finding the maximum cardinality SFS in an Abelian group was obtained in [9] by B. Green and I. Ruzsa in 2005.

Theorem 3: *Let G be an Abelian group of the order n. If n is divided only into prime $p \equiv 1 \pmod 3$, then the following equality holds:*

$$\lambda(G) = \frac{(\nu - 1)n}{3\nu},$$

where ν is the exponent of the group G.

The subset A of the group G is called *zero-free* (ZFS), if it has no solutions to the equation

$$x + y + z = 0. \tag{1}$$

The family of all ZFS in G is denoted by $ZF(G)$, and by $\mu(G)$ the maximum cardinality ZFS in G. In case ZFS are missing in an Abelian group, then either the exponent of the group is equal to 3 (item (iii) of Theorem 5), or the group consists only of a zero element (item (iv) of Theorem 5 for $n = 1$). In these cases it is supposed that $|ZF(G)| = 0$ and $\mu(G) = 0$. In this paper, using the methods of [9] the asymptotic behavior of the logarithm of the number of ZFS is set in an Abelian group, and also obtained the upper and lower bounds of maximum cardinality ZFS in an Abelian group. In particular, the following two theorems are proved:

Theorem 4: *Let G be an Abelian group of the order n. Then the following equality is true:*

$$\log |ZF(G)| = \mu(G) + \bar{o}(n).$$

Theorem 5: *Let G be an Abelian group of the order n with the exponent ν. Then the following statements are true:*

(i) *if n has a prime divisor comparable with 2 modulo 3, then*

$$\mu(G) = \frac{n}{3} \cdot \left(1 + \frac{1}{p}\right),$$

where p is the smallest prime divisor of n, comparable to 2 modulo 3;

(ii) *if n has no prime divisors $p \equiv 2 \pmod 3$, but $3|n$ and $\nu > 3$, then*

$$\frac{n}{3} \cdot \left(\frac{\nu - 3}{\nu}\right) \le \mu(G) \le \frac{n}{3};$$

(iii) *if $\nu = 3$, then*

$$\mu(G) = 0;$$

(iv) *if all prime divisors of n have the form $p \equiv 1 \pmod 3$, then*

$$\frac{n}{3} \cdot \left(\frac{\nu - 1}{\nu}\right) \le \mu(G) \le \frac{n - 1}{3}.$$

2. The Asymptotics of the Logarithm of the Number of Zero-free Sets in an Abelian Group

2.1 Definitions and Auxiliary Statements

Let G be an Abelian group of the order n. *The character* of the group G is called a mapping $\gamma : G \to C$ such, that for any $x \in G$ holds $|\gamma(x)| = 1$ and $\gamma(x + y) = \gamma(x)\gamma(y)$. The set of all characters of the group G is denoted by Γ. Note that Γ forms a group with the operation $(\gamma_1 * \gamma_2)(x) = \gamma_1(x)\gamma_2(x)$. Let $f : G \to R$. *The Fourier transform* f is the function $\widehat{f} : G \to C$, defined by the equality $\widehat{f}(\gamma) = \sum_{x \in G} f(x)\gamma(x)$.

For the proof of Theorem 4 use the method of granularization. The essence of this method is that for the evaluation of the cardinality of the set $ZF(G)$ the family $\mathcal{F}$, of the so called "grains" $F \in \mathcal{F}$ is constructed, such that every element of the set $ZF(G)$ is contained in some grain F of the constructed family $\mathcal{F}$, wherein $\log|\mathcal{F}| = \bar{o}(n)$, and in each grain $F \in \mathcal{F}$ there are $\bar{o}(n^2)$ solutions of the equation (1), that is, a family of subsets of the group G is constructed having the following properties:

- $\log|\mathcal{F}| = \bar{o}(n)$,
- for any $A \in ZF(G)$ there exists a grain $F \in \mathcal{F}$ such that $A \subseteq F$,
- in each grain $F \in \mathcal{F}$ there exist $\bar{o}(n^2)$ solutions of the equation (1).

There are two types of a granular structure that we will consider.

The union of cosets of the group G of some subgroup of order not less than L is called *L-granular of coset type.*

Let L be an integer and $d \in G$, wherein $ord(d) \geq L$, where $ord(d)$ is the order of the element d. Consider the subgroup G, generated by the element d, and divide each of its cosets into $\lfloor ord(d)/L \rfloor$ progressions of the form $\{x + id \mid 0 \leq i \leq L-1\}$ and one "residual" set of the cardinality less than L. For each $d \in G$ fix one such partition. The union of the obtained progressions is called *L-granular of progression type.*

The proofs of the following two lemmas are available in [9].

Lemma 1: *Suppose that n is larger than some absolute constant and that $L \leq \sqrt{n}$. Then the number of subsets of an Abelian group G of the order n, which are L-granular (of either coset or progression type) is at most $2^{3n/L}$.*

Lemma 2: *Suppose that ρ is smaller than some absolute positive constant, and that n is sufficiently large. Then the number of subsets of an n-element set of cardinality at most ρn is not more than $2^{n\sqrt{\rho}}$.*

The proof of the following lemma can be found in [12].

Theorem 6: *Let $m \geq 3$ be a fixed integer, and suppose that $A_1, \ldots, A_m$ are subsets of an Abelian group G of the order n, such that there are $\bar{o}(n^{m-1})$ solutions to the equation $a_1 + \ldots + a_m = 0$ with $a_i \in A_i$ for all i. Then we may remove $\bar{o}(n)$ elements from each A_i so as to leave sets A'_i, such that there are no solutions to $a'_1 + \ldots + a'_m = 0$ with $a'_i \in A'_i$ for all i.*

2.2 Granularization

The essence of the following lemma is that for every $A \in ZF(G)$ "a suitable" grain is constructed.

Lemma 3: (Granularization) *Let G be an Abelian group of the order n, and $A \in ZF(G)$, $\varepsilon \in \left(0, \frac{1}{2}\right)$, L and L' be positive numbers satisfying the inequality*

$$n > L' (4L/\varepsilon)^{9 \cdot 2^{14} \cdot \varepsilon^{-8}}.$$

Then there is a subset $A' \subseteq G$ such that

(i) *A' is either L-granular of progression type, or it is L'-granular of coset type,*

(ii) $|A \setminus A'| \le \varepsilon n$*,*

(iii) *A' contains not more than εn^2 solutions of the equation (1).*

Proof: Assume $\delta = \varepsilon^4/192$. First prove that there is a subset $P \subseteq G$, satisfying the following conditions:

(A) P is either a progression of the form $\{id \mid L-1 \le i \le L-1\}$, and $ord(d) \ge 2L/\varepsilon$, or a subgroup of the group G of an order not less than L',

(B) for any $B \subseteq G$ and $\gamma \in \Gamma$ the inequality $|\widehat{B}(\gamma)(1-g(\gamma))| \le \delta n$ holds, where $g(\gamma) = |P|^{-1} \sum\limits_{p \in P} \gamma(p)$, and $B(x)$ is the characteristic function of the subset B.

Let R_1 be the set of characters γ such that $|\widehat{B}(\gamma)| > \delta n/2$, and Γ_1 be the subgroup of the group Γ, generated by the set R_1. Consider the subgroup G_1 of the group G

$$G_1 = \{x \in G \mid \gamma(x) = 1 \text{ for any } \gamma \in \Gamma_1\}.$$

Consider two cases:

1) Let $|G_1| \ge L'$. Assume $P = G_1$. Since $g(\gamma) \in [-1,1]$ for $\gamma \in \Gamma \backslash \Gamma_1$ obtain that $|\widehat{B}(\gamma)(1-g(\gamma))| \le 2|\widehat{B}(\gamma)| < 2\delta n/2 = \delta n$, and for $\gamma \in \Gamma_1$ the equality $|\widehat{B}(\gamma)(1-g(\gamma))| = 0$ is true.

2) Let $|G_1| < L'$. Choose such d, that if the progression $P = \{id \mid L-1 \le i \le L-1\}$, is taken as P then the requirements of the items (A) and (B) will be satisfied. Note that when $\gamma \in \Gamma \backslash \Gamma_1$, the item (B) is executed. Now estimate the value of $1 - g(\gamma)$. Fix $\gamma \in \Gamma$ and denote $\arg \gamma(d) \in [-\pi, \pi)$ by β. Thus, we have

$$0 \le 1 - g(\gamma) = 1 - \frac{1}{2L-1} \sum_{j=-L-1}^{L-1} (\cos j\beta + i \sin j\beta) =$$

$$= 1 - \frac{1}{2L-1} - \frac{2}{2L-1} \sum_{j=1}^{L-1} \cos j\beta = \frac{2L-2}{2L-1} - \frac{2}{2L-1} \sum_{j=1}^{L-1} \cos j\beta =$$

$$= \frac{2}{2L-1} \sum_{j=1}^{L-1} (1 - \cos j\beta) \le \frac{1}{2L-1} \sum_{j=1}^{L-1} (j\beta)^2 = \frac{L(L-1)}{6} \beta^2 \le \frac{(L\beta)^2}{6}.$$

Note that if for all $\gamma \in R_1$ there occurred $|\arg \gamma(d)| \le L^{-1}\sqrt{6\delta n/|\widehat{B}(\gamma)|}$, then the fulfillment of the item (B) was completed. Also note that to satisfy the condition $ord(d) \ge 2L/\varepsilon$ it is sufficient that for some $\gamma \in \Gamma$ there occurred

$$0 < |\arg \gamma(d)| < 2\pi \cdot \frac{\varepsilon}{2L} = \frac{\pi\varepsilon}{L}.$$

Show that such $d \notin G_1$ can be chosen that for all $\gamma \in R_1$ the following is true:

$$|\arg \gamma(d)| \le \frac{1}{L} \min\left(\pi\varepsilon, \sqrt{\frac{6\delta n}{|\widehat{B}(\gamma)|}}\right).$$

Note that if $d_1, d_2 \in G$ belong to different cosets of G on G_1, then there exists a character $\gamma \in R_1$ such that $\gamma(d_1) \neq \gamma(d_2)$. Thus, for the existence of $d = d_1 - d_2 \notin G_1$, with the restriction $|arg(\gamma(d))| < \eta_\gamma$ it is enough that the amount of cosets with respect to G_1 exceeds $\prod\limits_{\gamma\in R_1} (1 + \lfloor 2\pi/\eta_\gamma \rfloor)$, that is

$$|G/G_1| > \prod_{\gamma\in R_1} \left(1 + L \max\left(\frac{2}{\varepsilon}, \sqrt{\frac{2\pi|\widehat{B}(\gamma)|}{6\delta n}}\right)\right).$$

Note that the following inequalities are true:

$$\prod_{\gamma\in R_1} \left(1 + L \max\left(\frac{2}{\varepsilon}, \sqrt{\frac{2\pi|\widehat{B}(\gamma)|}{6\delta n}}\right)\right) \le \prod_{\gamma\in R_1} \left(1 + 2L \max\left(\frac{1}{\varepsilon}, \sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}}\right)\right) \le$$

$$\le (4L)^{|R_1|} \prod_{\gamma\in R_1} \max\left(\frac{1}{\varepsilon}, \sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}}\right).$$

By the Parsevals identity, we have

$$\sum_{\gamma\in\Gamma} |\widehat{B}(\gamma)|^2 = n \sum_{x\in G} |B(x)|^2 = n|B| \le n^2.$$

Hence, from the definition of the set R_1 it follows $|R_1| \le 4\delta^{-2}$. Also note that the following inequality $\max(x, y) \le x^y$ is true for $x \ge 1$ and $y \ge e^{1/e}$. Thus, we obtain

$$(4L)^{|R_1|} \prod_{\gamma\in R_1} \max\left(\frac{1}{\varepsilon}, \sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}}\right) \le (4L)^{4\delta^{-2}} \left(\prod_{\gamma\in R_1} \max\left(\frac{1}{\varepsilon^4}, \left(\frac{|\widehat{B}(\gamma)|}{\delta n}\right)^2\right)\right)^{1/4} \le$$

$$\le (4L)^{4\delta^{-2}} \left(\varepsilon^{-4}\right)^{(4\delta^2 n^2)^{-1} \sum\limits_{\gamma\in\Gamma} |\widehat{B}(\gamma)|^2} \le (4L)^{4\delta^{-2}} \varepsilon^{-\delta^{-2}} \le (4L/\varepsilon)^{4\delta^{-2}} < \frac{n}{L'} \le |G/G_1|.$$

Thus, the existence of the subset $P \subseteq G$, satisfying the requirements of the items (A) and (B), is proved. Also note that since by construction P is either a subgroup or a progression symmetric with respect to 0, then $g(\gamma) = |P|^{-1} \sum\limits_{p\in P} \gamma(p)$ is a real number in the interval $[-1, 1]$.

Now construct a set A'. Consider two cases:

1) If P is a subgroup, then as A' take the union of cosets G on P, containing at least $\varepsilon|P|$ elements of the set A. Then we have

$$|A \setminus A'| \le \varepsilon|P| \cdot \frac{n}{|P|} = \varepsilon n.$$

2) If P is a progression with the difference d, then consider the granular structure of progression type with the difference d, and as A' take the union of progressions containing not less than $\varepsilon L/2$ elements A. Note that not more than $nL/ord(d)$ elements of "residual" sets are not included in any of the grains. Then, considering that $ord(d) \ge 2L/\varepsilon$ obtain

$$|A \setminus A'| \le \frac{\varepsilon L}{2} \cdot \frac{n}{L} + \frac{nL}{ord(d)} \le \varepsilon n.$$

The requirements (i) and (ii) of the lemma are satisfied in both cases.

Let us prove the point (iii). Consider the function $a_1(x) = |P|^{-1}|A \cap (P + x)|$. By $A(x)$ denote the characteristic function of the subset A of the group G. Note that for the Fourier transform of the function $a_1(x)$ the following correlation is true $\widehat{a}_1(\gamma) = g(\gamma)\widehat{A}(\gamma)$. Indeed, considering that $P = -P$ we have

$$\widehat{a}_1(\gamma) = \sum_{x\in G} a_1(x)\gamma(x) = \frac{1}{|P|}\sum_{x\in G}|A\cap(P+x)|\gamma(x) = \frac{1}{|P|}\sum_{a\in A}\sum_{p\in P}\gamma(a-p) =$$

$$= \frac{1}{|P|}\left(\sum_{a\in A}\gamma(a)\right)\left(\sum_{p\in P}\gamma(-p)\right) = \frac{1}{|P|}\left(\sum_{a\in A}\gamma(a)\right)\left(\sum_{p\in P}\gamma(p)\right) = g(\gamma)\widehat{A}(\gamma).$$

Also note that if $f : G \to R$, and $\widehat{f}$ is a Fourier transform of the function f, then the following equality is true:

$$\sum_{x_1+x_2+x_3=0} f(x_1)\cdot f(x_2)\cdot f(x_3) = \frac{1}{n}\sum_{\gamma\in\Gamma}\left(\widehat{f}(\gamma)\right)^3.$$

Indeed, considering that

$$\sum_{\gamma\in\Gamma}\gamma(x) = \begin{cases} 0, & \text{if } x \neq 0 \\ n, & \text{if } x = 0, \end{cases}$$

we have

$$\sum_{x_1+x_2+x_3=0} f(x_1)\cdot f(x_2)\cdot f(x_3) = \frac{1}{n}\sum_{x_i\in G, i\in[1,3]}\sum_{\gamma\in\Gamma}\Big(\gamma\left(x_1+x_2+x_3\right) f(x_1)\cdot f(x_2)\cdot f(x_3)\Big) =$$

$$= \frac{1}{n}\sum_{\gamma\in\Gamma}\left(\Big(\sum_{x_1\in G}\gamma(x_1)f(x_1)\Big)\cdot\Big(\sum_{x_2\in G}\gamma(x_2)f(x_2)\Big)\cdot\Big(\sum_{x_3\in G}\gamma(x_3)f(x_3)\Big) = \frac{1}{n}\sum_{\gamma\in\Gamma}\left(\widehat{f}(\gamma)\right)^3.\right.$$

Consider two cases: $x \in A'$ and $x \notin A'$.

Let $x \in A'$. If P is a subgroup, then $x + P$ contains at least $\varepsilon|P|$ elements of the set A, and if P is a progression, then $x + P$ contains the grain of A', comprising x, and therefore $|(x + P) \cap A| \geq \varepsilon|P|/4$. In both cases $a_1(x) \geq \varepsilon/4 = \varepsilon A'(x)/4$.

In case if $x \notin A'$, then $a_1(x) \geq 0 = \varepsilon A'(x)/4$.

Thus, considering that $|\widehat{A}(\gamma)| \leq \sum_{x\in A}|\gamma(x)| = |A| \leq n$, and $A \in ZF(G)$ we have

$$\#\{\text{solutions of the equation (1) in } A'\} =$$

$$= \sum_{x_1+x_2+x_3=0} A'(x_1)\cdot A'(x_2)\cdot A'(x_3) \leq \frac{4^3}{\varepsilon^3}\cdot\sum_{x_1+x_2+x_3=0} a_1(x_1)\cdot a_1(x_2)\cdot a_1(x_3) =$$

$$= \frac{4^3}{\varepsilon^3}\cdot\sum_{x_1+x_2+x_3=0}\Big(a_1(x_1)\cdot a_1(x_2)\cdot a_1(x_3) - A(x_1)\cdot A(x_2)\cdot A(x_3)\Big) =$$

$$= \frac{4^3}{\varepsilon^3}\cdot\frac{1}{n}\cdot\sum_{\gamma\in\Gamma}\Big((\widehat{a}_1(\gamma))^3 - (\widehat{A}(\gamma))^3\Big) = \frac{4^3}{n\varepsilon^3}\cdot\sum_{\gamma\in\Gamma}(\widehat{A}(\gamma))^3\Big((g(\gamma))^3 - 1\Big) \leq$$

$$\leq \frac{4^3}{n\varepsilon^3}\cdot\sum_{\gamma\in\Gamma}|\widehat{A}(\gamma)|^3|1-(g(\gamma))^3| \leq \frac{4^3}{n\varepsilon^3}\cdot 3\cdot\max_{\gamma\in\Gamma}|\widehat{A}(\gamma)||1-g(\gamma)|\cdot\sum_{\gamma\in\Gamma}|\widehat{A}(\gamma)|^2 \leq$$

$$\leq \frac{192}{n\varepsilon^3} \cdot \delta n \cdot n|A| \leq \frac{192}{\varepsilon^3} \cdot \delta \cdot n^2 = \varepsilon n^2.$$

Lemma 3 is proved. ■

The existence of a family of grains is proved in the following theorem.

Theorem 7: *Let G be an Abelian group of the order n, and n be sufficiently large. Then there exists the family $\mathcal{F}$ of subsets of the group G, satisfying the following conditions:*

(i) $\log|\mathcal{F}| \leq \sqrt{2}n(\log n)^{-1/18}$,

(ii) *for each $A \in ZF(G)$ there exists $F \in \mathcal{F}$ such that $A \subseteq F$,*

(iii) *every $F \in \mathcal{F}$ contains not more than $n^2(\log n)^{-1/9}$ solutions of the equation (1).*

Proof: Assume that $L = L' = \lfloor \log n \rfloor$ and $\varepsilon = (\log n)^{-1/9}/4$. Note that for sufficiently large n such a choice of parameters satisfies the condition of Lemma 3. Thus, for every set $A \in ZF(G)$, applying Lemma 3, construct the set A'. Assume that $\mathcal{F} = \{A \cup A' \mid A \in ZF(G)\}$. The item (ii) is executed by construction.

Hence and from the item (ii) of Lemma 3 it follows that the cardinality of the family $\mathcal{F}$ does not exceed the number of sets that are the union of L-granular with some subset of the group G, of size at most εn. Thus, from Lemmas 1 and 2 it implies that $\log|\mathcal{F}| \leq 3n/L + n\sqrt{\varepsilon}$, which for sufficiently large n does not exceed $2n\sqrt{\varepsilon}$.

Also note that while adding an element to the set, there can be formed not more than $3n$ new solutions of the equation (1). From this it follows that in each set $F \in \mathcal{F}$ there exist not more than $\varepsilon n^2 + 3\varepsilon n^2 = n^2(\log n)^{-1/9}$ solutions of the equation (1).

Theorem 7 is proved. ■

2.3 Proof of Theorem 4

Let G be an Abelian group of the order n. By Theorem 7 there exists a family $\mathcal{F}$ of subsets (grains) of the group G, satisfying the conditions (i)-(iii). Let $F \in \mathcal{F}$. Fixing F and applying Theorem 6 at $A_1 = A_2 = A_3 = F$ we obtain that there exists $F' \subseteq F$ such that $|F \backslash F'| = \bar{o}(n)$ $F' \in ZF(G)$. Hence, it follows that $|F| \leq \mu(G) + \bar{o}(n)$, where $\mu(G)$ is the maximum size of the set from $ZF(G)$. The fact that $\log|\mathcal{F}| = \bar{o}(n)$ (item (i) of Theorem 7) we find that the number of subsets of all the sets of the family $\mathcal{F}$, does not exceed $2^{\mu(G)+\bar{o}(n)}$.

By virtue of item (ii) of Theorem 7 all the sets from $ZF(G)$ are subsets of some set of the family $\mathcal{F}$. Hence it follows that

$$\log|ZF(G)| = \mu(G) + \bar{o}(n).$$

Theorem 4 is proved.

3. The Upper and Lower Estimates for the Maximum Size of a Zero-free set in an Abelian Group

3.1 Definitions and Auxiliary Statements

In this section we find the upper and lower estimates of the value $\mu(G)$. For this the following auxiliary results are needed.

Let G be an Abelian group and A, B be non-empty subsets of the group G. Assume that $A+B=\{a+b \mid a \in A, b \in B\}$, $2A=A+A$, and $-A=\{-a \mid a \in A\}$. Let $A \in ZF(G)$. The subset A is called *maximal,* if it is maximal by inclusion, i.e., for every $x \in G \setminus A$ the set $(A \cup \{x\}) \notin ZF(G)$.

Definition 1: *Let A be a non-empty subset of an Abelian group G. The subgroup $H(A)=\{g \in G \mid g+A=A\}$ is called a stabilizer of the set A.*

Theorem 8: (Kneser, [13]) *Let A, B be non-empty subsets of an Abelian group G, and H be a stabilizer of the set $A+B$. Then*

$$|A+B| \geq |A+H|+|B+H|-|H|.$$

Lemma 4: *Let G be an Abelian group, $A \in ZF(G)$, and H be a stabilizer of the set $2A$. Then $(A+H) \in ZF(G)$.*

Proof: Assume the contrary, and let $a_1+h_1+a_2+h_2+a_3+h_3=0$ for some $a_1, a_2, a_3 \in A$, and $h_1, h_2, h_3 \in H$. Since $2A+H=2A$, then obtain $0=a_1+h_1+a_2+h_2+a_3+h_3=a_1+a_2+a_3+(h_1+h_2+h_3)=a_1+a_2+a_3+h_4=a_1+(a_2+a_3+h_4)=a_1+a_4+a_5$, where $a_4, a_5 \in A$, and $h_4 \in H$. The latter contradicts the fact that $A \in ZF(G)$, i.e., the set $(A+H) \in ZF(G)$.

Lemma 4 is proved. ■

Lemma 5: *Let G be an Abelian group and the subset A of the group G be a maximal ZFS, and H be a stabilizer of the set $2A$. Then the set A is a union of cosets of the subgroup H.*

Proof: Since the subset A of the group G is a maximal ZFS, then by Lemma 4: we have $A=A+H$, that is the subset A is a union of cosets of the subset H.

Lemma 5 is proved. ■

Lemma 6: *Let G be an Abelian group. Then the following statements are equivalent:*

(i) *the exponent of the group G is divided into d;*

(ii) *there exists a subgroup H of the group G such that the quotient group G/H is isomorphic to the cyclic group Z_d.*

Lemma 7: *Let G be an Abelian group of the order n, and d is a divisor of the exponent group G. Then the following inequality holds:*

$$\mu(G) \geq \mu(Z_d) \cdot \frac{n}{d}.$$

Proof: Since d is an exponent divisor of the group G, then by Lemma 6: there exists a subgroup H of the group G such that the quotient group G/H is isomorphic to the cyclic group Z_d. Let $\psi\colon G \to G/H$ be a canonical homomorphism, and $K \in ZF(G/H)$. It is easy to see that the set $\psi^{-1}(K) \in ZF(G)$, and $|\psi^{-1}(K)|=|K| \cdot \frac{n}{d}$. Assume that $K=\{a_1+H, a_2+H, \ldots, a_k+H\}$, where $a_1, \ldots, a_k \notin H (H \notin K)$, and $k=|K|$. Let $\psi^{-1}(K) \notin ZF(G)$. Without loss of generality assume that for some $h_1, h_2, h_3 \in H$ the following equality holds: $a_1+h_1+a_2+h_2+a_3+h_3=0$. From this equality it follows that $a_1+a_2+a_3 \in H$, i.e., for elements $(a_1+H), (a_2+H), (a_3+H) \in K$ the following correlation holds: $(a_1+H)+(a_2+H)+(a_3+H)=H$. The latter contradicts the fact that $K \in ZF(G/H)$, i.e., the set $\psi^{-1}(K) \in ZF(G)$.

Lemma 7 is proved. ■

3.2 Proof of Theorem 5

First prove the upper estimates. Let $A \subseteq G$ be a maximal ZFS. Since $2A \cap (-A) = \emptyset$ (follows from the fact that $A \in ZF(G)$), then we obtain

$$|2A| + |A| \leq n. \tag{2}$$

From Theorem 8, Lemma 5 and the inequality (2) it follows that

$$3|A| - |H| \leq n, \tag{3}$$

where H is the stabilizer of the set $2A$.

From the last inequality and the fact that $|A|$ is divided into $|H|$ (follows from Lemma 5) we find that

$$|A| \leq |H| \cdot \Big\lfloor \frac{1}{3}\Big(\frac{n}{|H|} + 1\Big) \Big\rfloor. \tag{4}$$

Thus, we have

$$\mu(G) \leq \max_{d|n} \left(\left\lfloor \frac{d+1}{3} \right\rfloor \cdot \frac{n}{d} \right). \tag{5}$$

It is easy to see that the last inequality is equivalent to

$$\mu(G) \leq \begin{cases} \frac{n}{3}(1 + \frac{1}{p}), & \text{the least prime divisor } n \text{ of the form } p \equiv 2 \pmod 3; \\ \frac{n}{3}, & \text{no prime divisor } n \text{ of the form } p \equiv 2 \pmod 3\text{, but } 3|n; \\ \frac{1}{3}(n-1), & \text{all prime divisors } n \text{ have the form } p \equiv 1 \pmod 3. \end{cases}$$

The upper estimates are proved. Now prove the lower estimates.

(i) Let p be the least prime divisor n, of the form $p \equiv 2 \pmod 3$. Then there exist a subgroup H of the order n/p, and the element g of the order p such that

$$G = H \cup (H + g) \cup \ldots \cup (H + (p-1)g).$$

Define the set A by the equation

$$A = (H + g) \cup (H + 4g) \cup (H + 7g) \cup \ldots \cup (H + (p-1)g). \tag{6}$$

It is easy to see that the set A is a ZFS in the group G, and $|A| = \frac{p+1}{3} \cdot \frac{n}{p}$. By definition ZFS $A \in ZF(G)$ if $0 \notin A + A + A$, which is equivalent to $2A \cap (-A) = \emptyset$. Considering that $A = -A$ it is sufficient to show that $2A \cap A = \emptyset$. Indeed, from (6) we have $2A \subseteq \bigcup_i (ig + H)$, where $i \not\equiv 1 \pmod 3$, but since $A = \bigcup_j (jg + H)$, where $j \equiv 1 \pmod 3$, then it follows that $2A \cap A = \emptyset$.

(ii) Note that for any integer $m > 1$ the interval $[1, m-1]$ is a ZFS in the cyclic group Z_{3m}. Hence and from Lemma 7 the lower estimate follows.

(iii) Let the exponent of the Abelian group G be equal to 3. Since for any $g \in G$ the following equality holds $g + g + g = 0$, then in the group G the ZFS are missing. Therefore, one can assume that $\mu(G) = 0$.

(iv) Let ν be an exponent of the Abelian group G of the order n. Then there exists a subgroup H of the order n/ν, and an element g of the order ν such that

$$G = H \cup (H + g) \cup \ldots \cup (H + (\nu - 1)g).$$

Define the set A by the equation

$$A = (H + 2g) \cup (H + 5g) \cup (H + 8g) \cup \ldots \cup (H + (\nu - 2)g). \quad (7)$$

It is easy to see that the set A is a ZFS in the group G, and $|A| = \frac{\nu-1}{3} \cdot \frac{n}{\nu}$. Considering that $A = -A$ it is sufficient to prove that $2A \cap A = \emptyset$. From (7) we have $2A \subseteq \bigcup_i (ig + H)$, where $i \neq 2 \pmod 3$. And since $A = \bigcup_j (jg + H)$, where $j \equiv 2 \pmod 3$, then we find that $2A \cap A = \emptyset$.

Theorem 5 is proved.

References

[1] P.J. Cameron and P. Erdös, "On the number of sets of integers with various properties", *Journal of Number Theory (Bnaff,AB,1988)*, Berlin, de Gruyter, pp. 61-79, 1990.

[2] N.J. Calkin, "On the number of sum-free set", *Bull. London Mathematical Society*, vol. 22, pp. 140-144, 1990.

[3] N. Alon, "Independent sets in regular graphs and sum-free subsets of Abelian groups", *Israel Journal of Mathematics*, vol. 73, pp. 247-256, 1991.

[4] A.A. Sapozhenko, "The Cameron-Erdös conjecture", *Dokl. Akad. Nauk*, vol. 393, no. 6, 749-752, 2003.

[5] B. Green, "The Cameron-Erdös conjecture", *Bull. London Mathematical Society*, vol. 36, no. 6, pp. 769-778, 2004.

[6] A.A. Sapozhenko, "On the number of sum-free sets in Abelian groups", *Vestnik Moskovskogo Universiteta. Matematika i Mexanika*, vol. 4, pp. 14-17, 2002.

[7] V.F. Lev, T. Luczak and T. Schoen, "Sum-free sets in Abelian groups", *Israel Journal of Mathematics*, vol. 125, pp. 347-367, 2001.

[8] V.F. Lev and T. Schoen, "Cameron-Erdös modulo a prime", *Finite Fields and their Applications*, vol. 8, no. 1, pp. 108-119, 2002.

[9] B. Green and I. Ruzsa, "Sum-free sets in Abelian groups", *Israel Journal of Mathematics*, vol. 147, pp. 157-188, 2005.

[10] A.A. Sapozhenko, "Solution of the Cameron-Erdös problem for groups of prime order", *Computational Mathematics and Mathematical Physics*, vol. 49, no. 8, pp. 1435-1441, 2009.

[11] P.H. Diananda and H.P. Yap, "Maximal sum-free sets of elements of finite groups", *Proc. Japan Acad.*, vol. 45, no. 1, pp. 1-5, 1969.

[12] B. Green, "A Szemerédi-type regularity lemma in Abelian groups", *Journal Geometric and Functional Analysis (GAFA)*, vol. 15, no. 2, pp. 340-376, 2005.

[13] M.B Nathanson, "Additive number theory: Inverse problems and the geometry of sumsets", *Graduate Texts in Mathematics*, Berlin, Heidelberg, New York Springer-Verlag., p. 312, 1996.

Submitted 27.03.2014, accepted 01.08.2014.

Զրոյից ազատ բազմությունները Աբելյան խմբերում

Վ. Սարգսյան

Ամփոփում

G խմբի A ենթաբազմությունը կոչվում է զրոյից ազատ, եթե $x+y=z=0$ հավասարումը չունի լուծում A բազմության մեջ:

Աշխատանքում ստացվել են Աբելյան խմբի զրոյից ազատ բազմության առավելագույն հզորության վերին և ստորին գնահատականները, ինչպես նաև Աբելյան խմբի զրոյից ազատ բազմությունների քանակի լոգարիթմական ասիմպտոտիկ գնահատականը:

Множества, свободные от нуля, в абелевых группах

В. Саргсян

Аннотация

Подмножество A элементов группы G называется свободным от нуля, если уравнение $x+y+z=0$ не имеет решений в множестве A. В работе получены верхние и нижние оценки максимальной мощности множества, свободного от нуля, в абелевой группе, и установлена асимптотика логарифма числа множеств, свободных от нуля, в абелевой группе.