УДК: 51
DOI: 10.30987/2658-6436-2020-2-4-10

С.А. Алешина, И.В. Вьюгин

ПОЛИНОМИАЛЬНЫЙ ВАРИАНТ ЗАДАЧИ СУММ-ПРОИЗВЕДЕНИЙ

В работе рассматривается обобщение задачи сумм-произведений. Обобщённый принцип данной проблемы сформулирован в гипотезе Эрдёша-Семереди. Вместо суммы Минковского множеств рассматривается множество значений f(x,y) однородного полинома f от двух переменных x и y, принадлежащих подгруппе мультипликативной группы G of F_p^* поля положительной характеристики. В работе получена нижняя оценка мощности такой полиномиальной суммы. Данная тема имеет прикладное значение в теории информации и динамике при расчете вероятностей событий, а также в различных методах кодирования и декодирования информации.

Ключевые слова: *задача сумм-произведений, поле вычетов, мультипликативная группа, подгруппа.*

S.A. Aleshina, I.V. Vyugin

POLYNOMIAL VERSION ON THE SUM-PRODUCT PROBLEM

This work is about the generalization of sum-product problem. The general principle of it was formulated in the Erdos-Szemeredi's hypothesis. Instead of the Minkowski sum in this hypothesis, the set of values f(x,y) of a homogeneous polynomial f lin two variables, where x and y belong to subgroup G of F_p^* is considered. The lower bound on the cardinality of such set is obtained. This topic has an applied value in the theory of information and dynamics in calculating the probabilities of events, as well as in various methods of encoding and decoding information.

Keywords: *sum-product problem, residue field, multiplicative group, subgroup.*

Introduction

This work touches upon questions of arithmetic combinatorics, which studies simultaneously additive and multiplicative operations on sets. One of the most fundamental questions is the problem of sum-product subsets. The detailed description of it can be found in the paper [1]. The problem below has numerous applications in several branches of mathematics, such as cryptography for codes and dynamical systems. The results associated with the problem of sum-product type in a field of positive characteristic enable us to solve the problem of estimating trigonometrical sums over subgroups, which is particularly important for number theory. These estimates make it possible to describe the distribution of the elements of a multiplicative subgroup in a field of positive characteristic.

Let A be a finite non-empty set of elements of a ring K (for example, a finite set of integers). Consider the sum and product of A with itself:

$$A + A := \{a + b : a, b \in A\} \quad (1)$$

$$A \cdot A := \{a \cdot b : a, b \in A\} \quad (2)$$

Obviously, the cardinality of both these sets is at least $|A|$, and in general the expectation is that it to be close to $|A|^2$. However, if A is closed under addition and multiplication (A is closed to a subring), then the cardinality of both sets $A + A$ and $A \cdot A$can be comparable to $|A|$. For the ring of integers, the Erdos - Szemeredi's hypothesis says that there exists a positive number ε for which the following inequality holds:

$$max(|A + A|, |A \cdot A|) \gg |A|^{2-\varepsilon} \qquad (3)$$

for any finite subset $|A|$ of a ring. The inequality means that there exists a positive number$C$ such that $max(|A + A|, |A \cdot A|) > C|A|^{2-\varepsilon}$. This is the sum-product phenomenon: if the finite set A is not close to a real ring, then the sum $A + A$ or the product $A \cdot A$must be considerably larger than $A$and close to $|A|^2$.

This phenomenon was not proved, however, there is Erdos - Szemeredi's theorem for finite set of integers which states:

$$max(|A + A|, |A \cdot A|) \gg |A|^{1+c},$$

where c – positive constant.

Estimates for the constant ^{c} were constantly improved. If the set $A \subset R$, then best result was proved by Solymosi based on the Szemeredi-Trotter theorem:

$$max(|A + A|, |A \cdot A|) \gg |A|^{4/3-\varepsilon}. \qquad (4)$$

Remark: Consider the analogous problem of estimating the cardinality of the set $|A + A \cdot A|$. In the construction of this problem both additive and multiplicative operations are applied. It is known that $|A + A \cdot A| \gg |A|^{4/3}$.

In 1999 Tom Wolf (see [1]) raised the idea of looking for the phenomenon of sum-product type in finite fields $F_p$of prime order (such fields do not have non-trivial subrings). In particular, the inequality (3) holds if $A \subset F_p$and ^{A} does not coincide with the entire field F_p, in the sense that $|A| \leq p^{1-\delta}$ for some $\delta > 0$ (it is reasonable that ε should depend on δ), which was subsequently resolved positively. Now the corresponding result is known as the theorem on estimates of sums of products for F_p (later he had new proofs and refinements).

It follows from the sum-product phenomenon that if the set $A \subset F_p$of medium size $p^\delta < |A| < p^{1-\delta}$has a multiplicative structure (for example, is a geometric progression or multiplicative subgroup), then it cannot have an additive structure: the sum $A + A$is more larger than the original set A. Further, it is concluded that sets with multiplicative structure are uniformly distributed in the additive sense.

There are some modern results in the sum-product problem:

Theorem (Konyagin-Shkredov, Rudnev-Steven-Shkredov, 2016 - 2017)

Let $A \subset R$. Then

$$max(|A + A|, |A \cdot A|) \gg |A|^{\frac{4}{3}+c},$$

where $|A|$ is infinite, $c > 0$ is an absolute constant.

Theorem (Roche-Newton-Rudnev-Shkredov, 2016, Askoy-Yazici-Murphy-Rudnev-Shkredov, 2017)

Let $A \subset F_p$, $|A| < p^{5/8}$. Then

$max(|A + A|, |A \cdot A|) \gg |A|^{1+1/5}$.

Additive shifts of multiplicative subgroups

This problem is widely applicable in algebra, for example, in the study of additive shifts of multiplicative subgroups.

GarciaandJ. Volochin 1988 [7],using some algebraic ideas, provedthat for any multiplicative subgroup $G \subset F_p^*, G < \frac{(p-1)}{(p-1)^{\frac{1}{4}+1}}$ and any $\mu \neq 0$:

$$|G \cap (G+\mu)| \le 4|G|^{\frac{2}{3}}. \tag{5}$$

D. Heath – Brown and S. Konyagin [4] simplified the proof of this fact and improved the constants in 2000 with the help of method of S. Stepanov [6], that is extremely popular in number theory. After that in 2012 I. Vyugin and I. Shkredov [3] generalize this fact for the number of additive shifts:

Let $G \subset F_p^*$ - multiplicative subgroup, $k \ge 1$ – an integer, $|G| > k \cdot 2^{2k+4}$. Let $\mu_1, \dots \mu_k$ - different non-zero residues and $Q = GQ$ – an invariant set such as:

$$0 \notin Q;\ |Q| < \left(\left(\frac{|G|}{k}\right)^{\frac{1}{2k}} - 1\right)^{2k+1};\ p \ge 4k|G|\left(|Q|^{\frac{1}{2k+1}} + 1\right).$$

Then

$$\sum_{\lambda \in Q} |G \cap (G+\lambda\mu_1) \cap \dots \cap (G+\lambda\mu_k)| \le 4(k+1)\left(|Q|^{\frac{1}{2k+1}} + 1\right)^{k+1} |G|.$$

This theorem leads to the statement about the maximum of the cardinality of the intersection of k additive shifts of subgroup:

Let

$$32k \cdot 2^{20k\log(k+1)} \le |G|, p \ge 4k|G|\left(|G|^{\frac{1}{2k+1}} + 1\right).$$

Then

$$|G \cap (G+\mu_1) \cap \dots \cap (G+\mu_k)| \le 4(k+1)\left(|G|^{\frac{1}{2k+1}} + 1\right)^{k+1}.$$

In other words,

$$|G \cap (G+\mu_1) \cap \dots \cap (G+\mu_k)| \le k|G|^{\frac{1}{2}+\alpha_k}.$$

If $1 \ll k|G| \ll kp^{1-\beta_k}$, where $\{\alpha_k\},\{\beta_k\}$ – some sequences of positive numbers and $\alpha_k, \beta_k \to 0, k \to \infty$.

Also, in that work another additive characteristic of multiplicative subgroups is considered, namely, the cardinality of its sum and difference. The estimate (5) leads to

$$|G+G| \gg |G|^{\frac{4}{3}}.$$

For any G, for which $|G| \ll p^{\frac{3}{4}}$. Indeed, considering the cardinality of union of group G with some k elements of group G

$$|G \cup (G+\mu_1) \cup \dots \cup (G+\mu_k)|,$$

then it equals to

$$k|G| - |G \cap (G+\mu_1) \cap \dots \cap (G+\mu_k)| \ge k|G| - \frac{4n(n+1)|G|^{\frac{2}{3}}}{2}$$

from (5). If taking $k = C|G|^{\frac{1}{3}}$, where C – some constant, then the previous inequality will look like:

$$(C - 2C^2)|G|^{\frac{4}{3}} + 2C|G|.$$

The last part of the sum is linear, that can be omitted, so:

$$|G \cup (G+\mu_1) \cup \dots \cup (G+\mu_k)| \ge (C - 2C^2)|G|^{\frac{4}{3}},$$

that means that

$$|G+G| \gg |G|^{\frac{4}{3}},$$

since

$$|G \cup (G+\mu_1) \cup \dots \cup (G+\mu_k)| \le |G+G|.$$

This result will be generalized for polynomials in Theorem 2(trivial bound).

D. Heath – Brown and S.Konyagin proved the inequality

$$|G \pm G| \gg |G|^{\frac{4}{3}}$$

for all subgroup G, for which $|G| \ll p^{\frac{2}{3}}$. Using the combinatorial idea, I. Vyugin and I. Shkredov made the previous inequality stronger:

$$|G \pm G| \gg \frac{|G|^{\frac{5}{3}}}{\log^{\frac{1}{2}}|G|}$$

for all subgroup G, for which $|G| \ll p^{\frac{1}{2}}$.

In this work the problem of the sum-product type for multiplicative subgroups is extended, and the lower bound of the number of solutions for the set $P(G, G)$ where G is a multiplicative subgroup, is obtained. The obtained estimate generalizes the earlier ones (see [1, 2]). These estimates are a corollary of author's result if the linear polynomial $P(x, y)$ is considered.

Preliminaries

Definition 1. Let us call the polynomial $P \in F_p[x, y]$good if it is homogeneous with respect to x,y and $P(x, y) - 1$is absolutely irreducible (it is irreducible over the algebraic closure of F_p).

Definition 2. For a prime number p and a natural number n, let us call a group$G$ (n, p)– admitted if$G \subset F_p^*$ and $100n^3 < |G| < \frac{1}{3}p^{3/4}$.

Theorem 1 (I. Vyugin, S. Makarychev). For any natural number n there exist constants $C_1, C_2 > 0$ such that for any prime number p, for any (n, p)– admitted group G, for any good polynomial P of degree n, for any natural $h < C_2|G|^{3/2}$ and numbers $\alpha_1, \ldots \alpha_h \in F_p^*$ in different G-cosets, there are at most

$$C_1 h^{2/3}|G|^{2/3}$$

pairs (x, y) for which $P(x, y) = \alpha_k$ for some k. Later one of the constants in the last theorem was found exactly: $C_1 = 32n^5$.

Main results

Let us begin with the supporting statement:

Lemma. Let $P(x, y) \in F_p$ be a homogeneous polynomial of degree n such that the polynomial $P(x, y) - 1$ is irreducible over algebraic closure of F_p. Then the polynomial $Q(x, y) = P(x, y) - \alpha$, where α is a constant in F_p^* is irreducible over the closure of F_p.

Proof. For any α from F_p^* there must be denoted by the root of the n – th power from $\frac{1}{\alpha}$ in the algebraic closure of F_p.The polynomial $P(ax, ay) - 1$ is irreducible because if

$$P(ax, ay) - 1 = P_1(x, y)P_2(x, y),$$

then substituting into this equality x/a and y/a instead of x and y, then

$$P(x, y) - 1 = P_1\left(\frac{x}{a}, \frac{y}{a}\right) P_2\left(\frac{x}{a}, \frac{y}{a}\right),$$

i.e. $P(x, y) - 1$ is reducible, that contradicts to the assumption. So,

$$P(ax, ay) - 1 = a^n P(x, y) - 1 = \frac{P(x, y)}{\alpha} - 1$$

is irreducible. Multiplication by the constant α does not change irreducibility.

Theorem 2 (trivial bound). For any n there exist $C > 0$ such that for any prime number p (n, p) – admitted group G and a good polynomial P of degree n:

$$|P(G,G)| > C|G|^{4/3}.$$

Here $P(G,G)$ is the set of all elements of F_p that can be obtained by substituting all possible elements of G as x, y.

Proof. Consider the equation $P(x,y) = \alpha$. There are two cases: $\alpha = 0$ and $\alpha \neq 0$.

1) For any $\alpha \neq 0$, the Theorem 1 can be applied (according to Lemma, $P(x,y) = \alpha$ is absolutely irreducible), taking $h = 1$ (that $P(x,y) = \alpha$ has at most $C_1|G|^{2/3}$solutions for a constant C_1 depending only on the polynomial P).
2) If $\alpha = 0$, then the number of pairs for which $P(x,y) = 0$ is at most $2n|G|$.

a) If $P(x,*) = 0$ (P vanishes when y is substituted), then there are no more than n values of y (for example, the leading coefficient of x must vanishes, and its degree in y is not greater than n). They give no more than $n|G|$ pairs for which the P vanishes.

b) If the polynomial does not vanish (the given y is substituted), then it turns into a nonzero polynomial in x of degree no greater than n. Therefore, this polynomial has no more than n roots. In total, this gives at most $|G|n$ pairs for which the polynomial vanishes. Now it is needful to estimate the number of values of good P on elements from the (n, p)–admitted group G.

As $|G| > 100n^3$ (see Definition 2), then

$$2n|G| < \frac{|G|^2}{50n^2}.$$

As it was proved above, there are at most $2n|G|$ solutions

$$P(x,y) = 0,$$

this means that there are smaller than one fiftieth of all possible pairs. Remaining at least $\frac{(50n^2-1)|G|^2}{50n^2}$ pairs must somehow be distributed among other values of P, but each of these values does not exceed $C_1|G|^{2/3}$ pairs. Hence, the number of values cannot be less than

$$\frac{\left(\frac{(50n^2-1)|G|^2}{50n^2}\right)}{(C_1|G|^{2/3})} = \left(\frac{50n^2-1}{50n^2C_1}\right)|G|^{4/3} \tag{5}$$

As $C_1 = 32n^5$ (see the Theorem 1), then

$$C = \frac{50n^2-1}{1600n^7}.$$

The goal of this paper is to improve the lower bound of the number of solutions of the set $P(G,G)$.

Theorem 3 (non-trivial bound). For any n there exist $C > 0$ such that for any prime number $p(n,p)$ – admitted group G and a good polynomial P of degree n:

$$|P(G,G)| > C|G|^{3/2}.$$

Proof. Suppose the contrary. Then there exists n, for which Theorem 3 is not correct. Then for any constant C there are the (n,p) –admitted group G and the good polynomial P such that

$$|P(G,G)| \leq C|G|^{3/2}.$$

To obtain a contradiction, Theorem 1 must be applied. Thus, for n it needs to be chosen some $C_1C_2 > 0$ satisfying the condition of Theorem 3. After this let us choose $C > 0$ such that

$$C < C_2, C_1C^{2/3} < \frac{50n^2-1}{50n^2}.$$

Take any bad pair (P, G) for the chosen C. All possible values of $P(G, G)$ that are not more than $C|G|^{3/2}$ can be arranged in the form of the Young tableau in such a way that each row contains values from one G -coset, and in different rows - from different G-cosets . Thus, each line of the resulting diagram has no more than $|G|$ elements. Let us estimate from above the number of pairs (x, y) for which the value lies into one or another column.

If some column has h elements, then it can be noted that $h \le |P(G, G)| \le C|G|^{3/2} \le C_2|G|^{3/2}$. Therefore, since all the elements of the column lie in different G- cosets, according to the Theorem 1, there exists at most $C_1h^{2/3}|G|^{2/3}$ pairs (x, y) for which $P(x, y)$ lies into this column. The number of pairs for which $P(x, y) = 0$ is at most $2n|G|$ (see the proof of Theorem 2).

Now it can be denoted the column lengths for $h_1h_2, \dots h_{|G|}$ and estimate the total number of pairs:

$$|G|^2 < 2n|G| + \sum_{k=1}^{|G|} C_1h_k^{2/3}|G|^{2/3}.$$

On the other hand, by the inequality on the power averages:

$$(\frac{1}{|G|}\sum_{k=1}^{|G|} h_k^{2/3})^{3/2} \le \frac{1}{|G|}\sum_{k=1}^{|G|} h_k.$$

The sum of all $h_k$is the total number of cells in the table, so it does not exceed $C|G|^{3/2}$, whence:

$$|G|^2 < 2n|G| + C_1|G|^{2/3}|G|(\frac{C|G|^{3/2}}{|G|})^{2/3} = 2n|G| + C_1C^{2/3}|G|^2 < 2n|G| + (\frac{50n^2-1}{50n^2})|G|^2.$$

As $|G| > 100n^3$(see Definition 2), it is a contradiction, and therefore, theorem is proved.

The constant

$$C = min\,((\frac{50n^2-1}{50n^2C_1})^{3/2};\ C_2) = (\frac{50n^2-1}{1600n^7})^{3/2};$$

as C_2 was not found yet.

Conclusion

In this paper, the sum-product problem for multiplicative subgroups is expanded, and the lower bound for the number of solutions for the set $P(G, G)$ is obtained. The received estimate generalizes the ones previously obtained (see [1,2]). These estimates are a consequence of the obtained result assuming that the polynomial $P(x, y)$ is linear. The results that are considered in this paper, are intricately connected to another problems in additive combinatorics, namely, the additive energy of two sets and the structure of sumset problem, which allows to obtain the improved estimates for the cardinality of such sets.

Список литературы:

1. Тао, Т. Структура и случайность - М: МЦНМО, 2013. - 360 с.

2. Corvaja, P. Greatest common divisor of u-1, v-1 in positive and rationalpoints on curves over finite fields / P. Corvaja, U. Zannie // L. Eur. Math. Soc., 15, 1927- 1942, (2013). - Pp.345-356.

References:

1. Tao, T. Struktura i sluchajnost' - M: MCNMO, 2013. - 360 p.

2. Corvaja, P. Greatest common divisor of u-1, v-1 in positive and rational points on curves over finite fields / P. Corvaja, U. Zannie // L. Eur. Math. Soc., 15, 1927-1942, (2013). - Pp.345-356.

3. Вьюгин, И.В. Об аддитивных сдвигах мультипликативных подгрупп / И.В. Вьюгин, И.Д. Шкредов // Матем. сб., 2012. - Т. 203, № 6. – С. 81–100.
4. Heath-Brown, D. R. New bounds for Gauss sums derived from k-thpowers, and for Heilbronn’s exponential sum / Heath-Brown, D. R. S. Konyagin // Q. J. Math., 51: 2 (2000). - Pp. 221-235.
5. Конягин, С. В. Оценки для тригонометрических сумм на подгруппы и для гауссовых сумм", IV интернац. конф. Современные проблемы теории чисел и ее приложения, Актуальные проблемы. Часть 3 (Тула, 2001). - Изд: Моск. ун-та. - 2002. - С. 86-114.
6. Степанов, С. А. О числе точек гиперэллиптической кривой над простым конечным полем / С. А. Степанов // Изв. АН СССР. - 1969. - С.1171-1181.
7. Garcia, A. Fermat curves over finite fields / A. Garcia, J. F. Voloch // Number Theory, 30: 3 (1988). - Pp. 345-356.
8. Katz, N. H. On additive doubling and energy / N. H. Katz, P. Koester. SIAM J. Discrete Math., 24:4 (2010). - Pp. 1684-1693.
9. Sanders, T. On a non-abelian Balog-Szemeredi-type lemma, arXiv: 0912.0306.
10. Sanders, T. Structure in sets with logarithmic doubling, arXiv: 1002.1552.

3. V'yugin, I.V. Ob additivnyh sdvigah mul'tiplikativnyh podgrupp / I.V. V'yugin, I.D. SHkredov // Matem. sb., 2012. - T. 203, № 6. – Pp. 81–100.
4. Heath-Brown, D. R. New bounds for Gauss sums derived from k-thpowers, and for Heilbronn’s exponential sum / Heath-Brown, D. R. S. Konyagin // Q. J. Math., 51: 2 (2000). - Pp. 221-235.
5. Konyagin, S. V. Ocenki dlya trigonometricheskih summ na podgruppy i dlya gaussovyh summ", IV internac. konf. Sovremennye problemy teorii chisel i ee prilozheniya, Aktual'nye problemy. CHast' 3 (Tula, 2001). - Izd: Mosk. un-ta. - 2002. - Pp. 86-114.
6. Stepanov, S. A. O chisle tochek giperellipticheskoj krivoj nad prostym konechnym polem / S. A. Stepanov // Izv. AN USSR. - 1969. - Pp. 1171-1181.
7. Garcia, A. Fermat curves over finite fields / A. Garcia, J. F. Voloch // Number Theory, 30: 3 (1988). - Pp. 345-356.
8. Katz, N. H. On additive doubling and energy / N. H. Katz, P. Koester. SIAM J. Discrete Math., 24:4 (2010). - Pp. 1684-1693.
9. Sanders, T. On a non-abelian Balog-Szemeredi-type lemma, arXiv: 0912.0306.
10. Sanders, T. Structure in sets with logarithmic doubling, arXiv: 1002.1552.

Статья поступила в редколлегию 24.04.2020.
Рецензент: канд. техн. наук, доцент,
Брянский государственный технический университет
Подвесовский А.Г.
Статья принята к публикации 30.04.2020.

Сведения об авторах

Алешина Софья Александровна
студентка программы MBA университета Бедфордшира,
E-mail: aleshina.sofia@mail.ru.

Вьюгин Илья Владимирович
кандидат физико-математических наук, доцент факультета математики Национального Исследовательского Университета “Высшая Школа Экономики”,
E-mail: vyugin@gmail.com.

Information about authors:

Sofia Aleshina
MBA student at University of Bedfordshire, UK,
E-mail: aleshina.sofia@mail.ru.

Ilya Vyugin
Candidate of Sciences* (PhD), docent of faculty of mathematics at National Research University “Higher School of Economics”,

E-mail: vyugin@gmail.com.