Записки научных
семинаров ПОМИ
Том 432, 2015 г.

В. В. Волков, Ф. В. Петров

НЕКОТОРЫЕ ОБОБЩЕНИЯ ТЕОРЕМЫ КОШИ–ДЭВЕНПОРТА

Теорема Коши–Дэвенпорта [1] утверждает, что для непустых множеств A, B остатков по простому модулю p имеет место неравенство $|A+B| \geqslant \min(p, |A|+|B|-1)$. Начиная с середины 1990-х гг., когда появился полиномиальный метод, основанный на комбинаторной теореме о нулях [2], в этом круге вопросов было сделано многое, в том числе получены результаты для множеств точек в аффинных пространствах [3] и для общих групп [4, 5]. Мы приводим две простые теоремы на эту тему.

Первый результат позволяет заменить мощность подмножества поля K на наименьшую степень многочлена, обнуляющегося на множестве точек в K^n.

§1. Алгебраическая сложность

Пусть K – поле, A – непустое подмножество аффинного пространства K^n.

Определение 1. Назовем *алгебраической сложностью* множества A минимальную степень гиперповерхности H, содержащей A:

$$w(A) := \inf\{\deg H \mid H \supset A, H - \text{аффинная гиперповерхность в } K^n\}.$$

Алгебраическая сложность непустого множества принимает, таким образом, значения в множестве $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$.

Теорема 1. *Пусть $A_1 \subset K^{n_1}$, …, $A_m \subset K^{n_m}$ – конечные непустые множества, $x_i = (x_{i1}, \dots, x_{in_i})$ при $1 \leqslant i \leqslant m$ и $H(x_1, x_2, \dots, x_m)$ – многочлен от $n = n_1 + \dots + n_m$ переменных над K степени $\deg H = w(A_1) + \dots + w(A_m) - m$. Если коэффициент в H хотя бы при одном одночлене $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$, $|\alpha_i| = w(A_i) - 1$, не равен нулю, то H не покрывает $A_1 \times A_2 \times \dots \times A_m$.*

Ключевые слова: неравенство Коши–Дэвенпорта, полиномиальный метод, алгебраическая сложность.

Работа поддержана грантом РНФ 14-11-00581.

Доказательство. Индукция по m. База $m = 1$ тривиальна.

Разложим H по степеням x_m:

$$H(x_1, x_2, \ldots, x_m) = \sum_{|\alpha| \leqslant \deg H} H_\alpha(x_1, \ldots, x_{m-1}) x_m^\alpha.$$

Зафиксируем такой мультииндекс a, что $|a| = w(A_m) - 1$ и коэффициент в H_a при некотором одночлене $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{m-1}^{\alpha_{m-1}}$, где $|\alpha_i| = w(A_i) - 1$, не равен 0. Пусть $A_1 \times \cdots \times A_{m-1} = \{y_1, \ldots, y_s\}$. Пусть V – линейная оболочка в K^s всех векторов $(H_\alpha(y_1), \ldots, H_\alpha(y_s))$, $|\alpha| \geqslant w(A_m)$ (заметим, что в этом случае $\deg H_\alpha < w(A_1) + \cdots + w(A_{m-1}) - (m-1)$).

Рассмотрим два случая:

1. $(H_a(y_1), \ldots, H_a(y_s)) \in V$. Разложение этого вектора в линейную комбинацию векторов $(H_\alpha(y_1), \ldots, H_\alpha(y_s))$ с $|\alpha| \geqslant w(A_m)$ дает многочлен $G(x_1, \ldots, x_{m-1})$, нарушающий индукционное предположение для $m - 1$.

2. $(H_a(y_1), \ldots, H_a(y_s)) \notin V$. Предположим, что H покрывает $A_1 \times A_2 \times \cdots \times A_m$. Рассмотрим линейный функционал $L \in (K^s)^*$, обнуляющий V, но не обнуляющий $(H_a(y_1), \ldots, H_a(y_s))$. Тогда многочлен

$$G(x_m) = \sum_{|\alpha| \leqslant \deg H} L(H_\alpha(y_1), \ldots, H_\alpha(y_s)) \cdot x_m^\alpha$$

задает гиперповерхность степени меньше чем $w(A_m)$, покрывающую множество A_m. □

Следствие 1 (Неравенство Коши–Дэвенпорта для алгебраической сложности)**.** *Пусть $p(K)$ – аддитивный порядок единицы в поле K. Пусть A, $B \subset K^n$ – конечные непустые подмножества. Тогда*

$$w(A + B) \geqslant \min\{p(K), w(A) + w(B) - 1\}.$$

Доказательство. Заметим, что при удалении точки из множества A его алгебраическая сложность уменьшается не более чем на 1. Поэтому если $w(A) + w(B) > p(K) + 1$, то существуют непустые подмножества $A' \subset A$, $B' \subset B$, такие, что $w(A') + w(B') = p(K) + 1$. Это рассуждение сводит дело к случаю $w(A) + w(B) \leqslant p(K) + 1$.

Теперь предположим, что некоторый многочлен $H(z)$, $z \in K^n$, степени $w(A) + w(B) - 2 < p(K)$ обнуляется на $A + B$ (многочлен меньшей степени на что-нибудь домножим.) Тогда многочлен $F(x, y) :=$

$H(x+y)$ обнуляется на $A \times B$. Но если $z_1^{c_1} \dots z_n^{c_n}$ – некоторый одночлен в H старшей степени, то F содержит некоторый одночлен степени $w(A)-1$ по x и $w(B)-1$ по y (коэффициент не равен 0, поскольку соответствующие биномиальные коэффициенты не равны 0 в поле K). Это сразу противоречит теореме 1. □

§2. Мультипликативная группа поля

Обсудим алгебраические условия на множества A, B в мультипликативной группе поля K, гарантирующие выполнение неравенства типа Коши–Дэвенпорта $|A \cdot B| \geqslant |A|+|B|-1$. Используемый метод ранее применялся в [6] для нижних оценок полиномиальных выражений типа $|p(A,B)|$, $p \in K[x,y]$.

Теорема 2. *Пусть K – поле, A, B – непустые подмножества в $K \setminus 0$, $|A| = a$, $|B| = b$, $A = \{x_1, \dots, x_a\}$, $B = \{y_1, \dots, y_b\}$. Пусть $I = \{t_1 < \dots < t_a = a+b-2\}$, $J = \{s_1 < \dots < s_b = a+b-2\}$ – такие множества индексов, что $I \cap J = \{a+b-2\}$, $I \cup J = \{0, 1, \dots, a+b-2\}$. Рассмотрим $(a \times a)$-матрицу $Z(A,I) = (x_i^{t_j})$ и $(b \times b)$-матрицу $Z(B,J) = (y_i^{s_j})$. Если обе они невырождены, то $|A \cdot B| \geqslant a+b-1$.*

Доказательство. Если обе матрицы невырождены, то существуют (единственные) K-значные функции $f(x)$ на A и $g(y)$ на B, такие, что $\sum\limits_{x \in A} f(x) x^{t_i} = 0$ при $1 \leqslant i \leqslant a-1$, $\sum\limits_{x \in A} f(x) x^{t_a} = 1$; $\sum\limits_{y \in B} g(y) y^{s_i} = 0$ при $1 \leqslant i \leqslant b-1$, $\sum\limits_{y \in B} g(y) y^{s_b} = 1$. Предполагая, что $c := |A \cdot B| \leqslant a+b-2$, рассмотрим следующий многочлен от переменных x, y:

$$P(x,y) = (xy)^{a+b-2-c} \prod_{t \in A \cdot B} (xy - t).$$

Ясно, что P обнуляется на $A \times B$. Рассмотрим сумму

$$0 = \Sigma := \sum_{x \in A, y \in B} f(x) g(y) P(x,y).$$

Разлагая многочлен $P(x,y)$ по степеням xy мы видим, что каждая из сумм $\sum f(x)g(y)(xy)^m$ обнуляется при $m = 0, 1, \dots, a+b-3$ (такая сумма факторизуется как $(\sum f(x)x^m)(\sum g(y)y^m)$, и один из множителей обнуляется, поскольку $I \cup J \supset \{0, 1, \dots, a+b-3\}$). Но при $m = a+b-2$ соответствующая сумма $\sum f(x)g(y)(xy)^{a+b-2}$ равна 1. Значит, $\Sigma = 1$ – противоречие. □

Переформулировка. *Рассмотрим два матроида M_a, M_b на множестве $\{0,1,\dots,a+b-3\}$. Оба суть векторные матроиды над полем K, матроид M_a соответствует линейной зависимости векторов $v_i = (x_1^i,\dots,x_a^i)$ в K^a по модулю одномерного пространства $K\cdot v_{a+b-2}$, матроид M_b определим аналогично. Условия теоремы 2 на матроидном языке звучат так: объединение матроидов M_a, M_b имеет полный ранг $a+b-2$. Используя теорему Нэша–Уильямса для ранга объединения матроидов, получаем следующее эквивалентное условие: для любого множества $U\subset\{0,1,\dots,a+b-1\}$, содержащего $a+b-1$, имеет место неравенство на ранги матриц:*

$$\operatorname{rank}(x_i^u)_{1\leqslant i\leqslant a,\,u\in U} + \operatorname{rank}(y_i^u)_{1\leqslant i\leqslant b,\,u\in U} \geqslant |U|+1. \tag{1}$$

Условия теоремы выглядят несколько громоздко, поэтому приведем два более слабых, но более легко проверяемых условия, достаточных для неравенств типа Коши–Дэвенпорта.

Следствие 2. *Рассмотрим (в обозначениях теоремы 2) такую матрицу размера $(a+b)\times(a+b)$:*

при $i=0,1,\dots,a+b-3$ её $(i+1)$-я строка есть $(x_1^i,\dots,x_a^i,y_1^i,\dots,y_b^i)$; $(a+b-1)$-я строка есть $(x_1^{a+b-2},\dots,x_a^{a+b-2},0,\dots,0)$; $(a+b)$-я строка есть $(0,\dots,0,y_1^{a+b-2},\dots,y_b^{a+b-2})$. Если эта матрица невырождена, то $|A\cdot B|\geqslant a+b-2$.

Доказательство. Достаточно проверить условие (1). В самом деле, если оно нарушается для некоторого множества U, найдутся $|U|+1$ строк нашей матрицы (включающие $(a+b-1)$-ю и $(a+b)$-ю, а также строки, соответствующие элементам множества U), такие, что их линейная оболочка имеет размерность не больше $|U|$. □

Следующее следствие относится к специальному выбору множеств I, J. Обозначим через $h_N(x_1,\dots,x_a)$ полный однородный симметрический многочлен степени N от переменных $x_1,\dots,x_a$ (так, $h_2 = \sum\limits_i x_i^2 + \sum\limits_{i<j} x_ix_j$).

Следствие 3. *Предположим, что $h_{b-1}(x_1,\dots,x_a)\neq 0$. Тогда $|A\cdot B|\geqslant a+b-2$.*

Доказательство. Пусть

$$I=\{0,1,\dots,a-2,a+b-2\},\quad J=\{a-1,\dots,a+b-2\}.$$

Тогда если $W_A = \prod_{i<j}(x_j - x_i)$ и $W_B = \prod_{i<j}(y_j - y_i)$ обозначают определители Вандермонда для множеств A, B, имеем $\det Z(B, J) = W_B \cdot \prod y_i^{a-1} \neq 0$, $\det Z(A, I) = h_{b-1}(x_1, \ldots, x_a) \neq 0$ (это стандартный факт теории симметрических функций). □

Следствие 3 имеет следующий частный случай.

Следствие 4. *Предположим, что поле K имеет характеристику 0 и $x_i^{p^n} = 1$ при $i = 1, \ldots, a$, где p простое, n натуральное. Предположим также, что p не делит биномиальный коэффициент $\binom{a+b-2}{a-1}$. Тогда $h_{b-1}(x_1, \ldots, x_a) \neq 0$ и, следовательно, $|A \cdot B| \geqslant a + b - 2$.*

Доказательство. Пусть w – первообразный корень степени p^n из 1. Минимальный многочлен с рациональными коэффициентами, обнуляющий w, есть $\Phi_{p^n}(t) = 1 + t^{p^{n-1}} + \cdots + t^{(p-1)p^{n-1}}$. Заметим, что $h_{b-1}(x_1, \ldots, x_a)$ – многочлен от w с целыми коэффициентами, так что если его значение равно нулю, то он делится на $\Phi_{p^n}(w)$ как многочлен и по лемме Гаусса частное также имеет целые коэффициенты. Это означает, что если заменить w на 1, значение станет делиться на p, но $h_{b-1}(1, \ldots, 1) = \binom{a+b-2}{a-1}$, что по предположению не кратно p. Значит, $h_{b-1}(x_1, \ldots, x_a) \neq 0$, что и требовалось. □

Литература

1. H. Davenport, *On the addition of residue classes.* — J. London Math. Soc. **10** (1935), 30–32.
2. N. Alon, M. B. Natanson, I. Z. Ruzsa, *Adding distinct congruence classes modulo a prime,* Amer. Math. Monthly **102** (1995), 250–255.
3. S. Eliahou, M. Kervaire, *Sumsets in vector spaces over finite fields.* — J. Number Theory **71**, No. 1 (1998), 12–39.
4. G. Károlyi, *Cauchy–Davenport theorem in group extensions.* — L'Enseignement Mathematique **51** (2005), 239–254.
5. J. P. Wheeler, *The Cauchy–Davenport theorem for finite groups;* `arXiv:1202.1816`.
6. F. Petrov, *Combinatorial Nullstellensatz approach to polynomial expansion.* — Acta Arith. **165** (2014), 279–282.
7. `http://mathoverflow.net/questions/37044/cauchy-davenport-strengthening`.

Volkov V. V., Petrov F. V. Some generalizations of the Cauchy–Davenport theorem.

We investigate two possible generalizations of the Cauchy–Davenport inequality $|A + B| \geqslant \min(p, |A| + |B| - 1)$ for nonempty sets A, B of residues modulo a prime number p. The first one deals with another way

of measuring the size of a set of points in an affine space (rather than just taking the cardinality), namely, with algebraic complexity. The second one concentrates on the multiplicative group of a field.

Поступило 26 января 2015 г.

С.-Петербургский
государственный университет,
Университетский пр., д. 28, Старый Петергоф,
С.-Петербург 198504, Россия
E-mail: vladvolkov239@gmail.com

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
наб. р. Фонтанки, д. 27,
С.-Петербург 191023;
С.-Петербургский
государственный университет,
Уиверситетский пр., д. 28, Старый Петергоф,
С.-Петербург 198504, Россия
E-mail: fedyapetrov@gmail.com