Нулевые суммы векторов

Захаров Дмитрий

Берендеевы поляны, 17–23 августа 2019 г.

Теорема 1 (Эрдёш, Гинзбург, Зив, 1961). Пусть $A = a_1, a_2, \dots, a_{2n-1}$ и $a_i \in \mathbb{N}$. Тогда $\exists I \subset A: \ |I| = n, \sum I \vdots n$. *Примечание. При $|A| < 2n-1$ утверждение неверно, например, если в A $n-1$ единица и $n-1$ ноль.*

Лемма 2. Достаточно доказать 1 для $n \in \mathbb{P}$.

Доказательство. Пусть 1 доказана для чисел m и n. Докажем её для mn. Возьмём числа $a_1, a_2, \dots, a_{2mn-1}$. Рассмотрим первые $2n-1$ из них. Из них найдутся n, сумма которых кратна n. Уберём их из последовательности a_i и поставим в сторону. У нас останется последовательность, в которой на n меньше чисел. Так можно делать $2m-1$ раз, после чего у нас останутся $2m-1$ групп чисел, сумма в каждой из которых кратна n (и в каждой из которых n чисел). Тогда среди них найдутся m, общая сумма в которых делится на mn, что и доказывает теорему. ∎

Лемма 3. Пусть $p \in \mathbb{P}$. Тогда $\binom{2p-1}{p} \equiv 1 \mod p$ и $\binom{2p-1-j}{p-j} \vdots p$ для $0 < j < p$.

Доказательство. Первое утверждение:

$$1+\binom{2p}{p}+1 = \sum_k \binom{2p}{k} = 2^{2p} \equiv 4 \mod p \implies \binom{2p}{p} \equiv 2 \mod p \implies \binom{2p-1}{p} \equiv 1 \mod p.$$

Второе утверждение:

$$\binom{2p-1-j}{p-j} = \frac{(2p-1-j)!}{(p-j)!(p-1)!}$$ и числитель делится на p, а знаменатель нет. ∎

Доказательство теоремы 1 #1. Допустим, что $\forall I \subset A : \sum I \not\equiv 0 \mod p$. Рассмотрим S — сумму по всем множествам I выражения $\left(\sum I\right)^{p-1}$. Заметим, что $S \equiv \binom{2p-1}{p} \mod p$. С другой стороны, верно

$$S = \sum_{\sum k_i = p} \left(a_{i_1}^{k_1} \cdot a_{i_2}^{k_2} \cdot \ldots \cdot a_{i_t}^{k_t} \cdot \binom{2p-1-t}{p-t} \right).$$

Так как каждый такой биномиальный коэффициент кратен p по 3, то и вся сумма кратна, но она сравнима с 1 — противоречие.

Пусть $p \in \mathbb{P}$. Обозначим $\mathbb{F}_p$ — поле остатков по модулю p.

Лемма 4 (упражнение). Пусть $P(x) \in \mathbb{F}_p[x], \deg P < n, \forall x \in \mathbb{F}_p \ P(x) = 0$. Тогда $P(x) \equiv 0$. *Подсказка: используйте деление с остатком.*

Лемма 5 (упражнение). Придумайте контрпример к 4 при составном p и старшем коэффициенте 1.

Определение 1. Назовём многочлен $P \in \mathbb{F}[x_1, \dots, x_n]$ полилинейным, если в его мономах нет множителей вида x_i^α при $\alpha > 1$.

Лемма 6. Пусть $P \in \mathbb{F}[x_1, \dots, x_n]$ полилинейный и для каждого набора из n нулей и единиц $P(\text{набора}) = 0$. Тогда $P \equiv 0$.

Доказательство. Используем индукцию. При $n = 0$ очевидно.

Шаг индукции.

$$P(x_1, \dots, x_n, x_{n+1}) = Q(x_1, \dots, x_n) + x_{n+1} R(x_1, \dots, x_n).$$

Зафиксируем набор из n нулей и единиц. Для данного набора $P(x_1, \dots, x_{n+1}) = 0$ в нуле и единице, значит, Q и R удовлетворяют предположению индукции. ∎

Лемма 7 (понижение степеней). Пусть $P \in \mathbb{F}[x_1, \ldots, x_n]$ принимает нули во всех точках множества $\{0,1\}^n$. Тогда он равен тождественно нулю по модулю $x^2 - x$.

Доказательство теоремы 1 #2. Пусть $a_1, \ldots, a_{2p-1} \in \mathbb{F}_p$. Рассмотрим систему сравнений:

$$\begin{cases} a_1x_1 + a_2x_2 + \ldots + a_{2p-1}x_{2p-1} \equiv 0 \mod p \\ x_1 + x_2 + \ldots + x_{2p-1} \equiv 0 \mod p \end{cases} \quad (1)$$

Если существует решение системы 1 в полилинейных многочленах от x_i, то теорема доказана. Рассмотрим $P(v) = \left(1 - (\sum a_iv_i)^{p-1}\right)\left(1 - (\sum v_i)^{p-1}\right)$. Пусть теорема неверна. Тогда для любого ненулевого набора x сравнение не получится, т.е. $P(v) = \delta_{v,(0,0,\ldots)}$. Тогда по 7 верно $P(v) \equiv (1-v_1)(1-v_2)\ldots(1-v_{2p-1})$. Но степень левой части $2p-2$, а правой $2p-1$ — противоречие. ■

Обобщения ЭГЗ

. **Задача.** Найти $f(n,d)$ — наименьшее такое k, что для любого набора U из k векторов в $\mathbb{Z}^d$ найдётся такое множество I: $|I| = n, I \subset U, \forall j \leq d \sum\limits_{v \in I} v_j \vdots n$.

Теорема 8. $f(n,d) \geq 2^d(n-1)+1$.

Доказательство. Рассмотрим набор U такой, что каждая из строк из $\{0,1\}^d$ входит в него $n-1$ раз. Очевидно, что сумма любых n из них по каждой координате входит в интервал $[0, n-1]$ и все нули быть не могут, т.е. такого множества I нет.■

Лемма 9. Если для $n = n_1$ и $n = n_2$ верно $f(n,d) \leq c(n-1)+1$, то это верно и для $n = n_1n_2$, где c — константа, не зависящая от n (она может зависеть от d).

Доказательство. Аналогично 2. ■

Теорема 10 (Edel, Erscholz). $f(n,3) \geq 9n-8$ при нечётных n.

Набор точек плохой, если в нём нет подмножества I размера n, сумма координат которых делится на n (по каждой координате).

Лемма 11. Наборы: $\binom{0}{0}\binom{0}{2}\binom{2}{0}\binom{2}{2}$ (по $n-1$ штук) и $\binom{0}{1}\binom{1}{0}\binom{1}{2}\binom{2}{1}$ (тоже по $n-1$ штук) плохие.

Доказательство. Для первого набора это очевидно. Пусть мы взяли векторы второго набора с коэффициентами $\alpha, \beta, \gamma, \delta$. Заметим, что сумма первых координат взятых нами векторов равна n (не 0 и не $2n$), значит, $\alpha = \delta$. С другой стороны, сумма вторых координат тоже равна n, значит, $\beta = \gamma$. Тогда $n = \alpha + \beta + \gamma + \delta = 2\alpha + 2\beta$ — чётное — противоречие. ■

Доказательство теоремы 10. Рассмотрим набор по $n-1$ каждого из следующих векторов: $(1,0,0), (1,2,0), (1,0,2), (1,2,2), (2,0,1), (2,1,0), (2,1,2), (2,2,1), (3,1,1)$. Заметим, что последние две координаты первой четвёрки совпадают с первым набором из 11, а второй четвёрки — с вторым набором оттуда же. Пусть мы берём эти вектора с количествами $\alpha_1, \alpha_2, \ldots, \alpha_9$.

Лемма 12. $\alpha_9 \neq 0$.

Доказательство. Пусть $\alpha_9 = 0$. Тогда чтобы сумма x единиц и $n-x$ двоек делилась на n, x должно делиться на n, т.е. все вектора либо из первой четвёрки, либо из второй, что противоречит 11. ■

Лемма 13. Сумма по второй и третьей координатах равна n, а по первой — $2n$.

Доказательство. Сумма по второй и третьей координатах может быть либо 0, либо n, либо $2n$, причём у нас есть единица. Для первой координаты аналогично. ■

Конец доказательства. Заметим, что сумма координат каждого вектора нечётна, а т.к. n тоже нечётно, суммарная координата должна быть нечётной. С другой стороны, она равна $4n$ — противоречие. ■

Теорема 14. $f(n,d) \geq 2^d \left(\frac{9}{8}\right)^{\left[\frac{d}{3}\right]}$ для нечётных n.

Доказательство. Для $d \vdots 3$ доказательство аналогично 8. В противном случае добавим несколько пар $(0,1)$ в конце. ■

Теорема 15 (упражнение). При $n = 2^k$ оценка из 8 точная.

Лемма 16. Пусть сумма векторов $\binom{x_1}{y_1}, \ldots, \binom{x_{3n}}{y_{3n}}$ равна 0. Тогда множество этих векторов хорошее.

Доказательство. Рассмотрим систему сравнений от $3p-1$ переменной α_i:

$$\begin{cases} \sum \alpha_i x_i \equiv 0 \mod p \\ \sum \alpha_i y_i \equiv 0 \mod p \\ \sum \alpha_i \equiv 0 \mod p \end{cases} \tag{2}$$

Рассмотрим многочлен

$$P(\alpha_1, \ldots, \alpha_{3p-1}) = \left(1 - \left(\sum \alpha_i x_i\right)^{p-1}\right) \cdot \left(1 - \left(\sum \alpha_i y_i\right)^{p-1}\right) \cdot \left(1 - \left(\sum \alpha_i\right)^{p-1}\right).$$

Если ненулевых решений в $\alpha_n \in \{0,1\}$ у 2 нет, то по 7 верно $P(v) \equiv (1-v_1)(1-v_2)\ldots(1-v_{3p-1})$, но степень многочлена равна $3p-3 < 3p-1$. Следовательно, у системы есть решение. Тогда если в решении $\sum \alpha_i = p$, то задача решена, иначе $\sum \alpha_i = 2p$ и можно взять «дополнение». ■

Теорема 17 (Роньяи, 2007). $f(p,2) \leq 4p-2$ для $p \in \mathbb{P}$.

Доказательство. Пусть есть $4p-2$ вектора $\binom{x_1}{y_1}, \ldots, \binom{x_{4p-2}}{y_{4p-2}}$. Рассмотрим многочлен

$$P(\alpha_1, \ldots, \alpha_{4p-2}) = \left(1 - \left(\sum \alpha_i x_i\right)^{p-1}\right) \cdot \left(1 - \left(\sum \alpha_i y_i\right)^{p-1}\right) \cdot \left(1 - \left(\sum \alpha_i\right)^{p-1}\right) \cdot (\sigma_p(\alpha_i) - 2),$$

где $\sigma_n(v) = \sum\limits_{I \subset v, |I|=n} \prod\limits_{\alpha \in I} \alpha$. Если у P есть ненулевое решение в $\{0,1\}^{4p-2}$, то задача решена. Действительно, $\sum \alpha_i \in \{p, 2p, 3p\}$ из-за третьей скобки, $\sum \alpha_i \binom{x_i}{y_i} \equiv 0 \mod p$ из-за 1-й и 2-й скобки. Если $\sum \alpha_i = p$, то мы нашли сумму. Если $\sum \alpha_i = 3p$, то из-за 16 мы победили. Иначе $\sigma_p(\alpha_i) = \binom{2p}{p} \equiv 2 \mod p$, т.е. это не решение системы. Иначе этот многочлен (степени $4p-3$) по 7 тождественно равен многочлену степени $4p-2$ — противоречие. ■

Теорема 18 (Рейхер). $f(n,2) = 4n-3$.

Лемма 19. $f(3,d) \le 2 \cdot 3^d + 1$.

Доказательство. Если есть хотя бы столько векторов, то среди них будут 3 одинаковых по модулю 3 и их сумма даст 0. ■

Теорема 20. $f(3,d) \le 6 \sum\limits_{a+2b \le 2d/3} \binom{d}{a,\ b}$.

Теорема 21. Если 20, то для достаточно больших d выполняется $f(3,d) \le 2,752^d$.

Доказательство. Применим 20. Рассмотрим многочлен $P(x) = (1+x+x^2)^d = \sum C_k x^k$. Заметим, что $C_k = \sum\limits_{a+2b=k} \binom{d}{a,\ b}$. Мы знаем, что $f(3,d) \le 6 \sum\limits_{i \le 2d/3} c_i$.

Лемма 22. $c_k \le 2,7515^k$.

Доказательство. Если $x \ge 0$, то $P(x) \ge C_{2d/3} x^{2d/3}$, т.е. $C_{2d/3} \le x^{-2d/3}(1+x+x^2)^d$. Возьмём $x = 0,84^3$. Тогда $C_{2d/3} \le (0,84^{-2} + 0,84 + 0,84^4)^d < 2,7515^d$. Из этой формулы также видно, что предыдущие коэффициенты меньше. ■

Лемма 23. Пусть есть система $*$ из m линейных уравнений вида $\sum a_i x_i = 0$ и n неизвестных, причём $n > m$. Тогда существует решение с хотя бы $n-m$ ненулевыми неизвестными.

Доказательство. Рассмотрим решение системы $(x_1, \ldots, x_n)$ с максимальным числом ненулевых координат. Пусть их не больше, чем $n-m-1$. Для простоты можно считать, что это координаты $x_1, \ldots, x_{n-m-1}$. Рассмотрим такую систему:

$$\begin{cases} * \\ x_1 = 0 \\ x_2 = 0 \\ \vdots \\ x_{n-m-1} = 0 \end{cases} \tag{3}$$

У неё есть ненулевое решение $(y_1, \ldots, y_n)$. Тогда $z_i = x_i + y_i$ — тоже решение и у него меньше нулей — противоречие. ■

d-мерные матрицы. Ранг

Определение 2. d-мерная матрица $A = A(i_1, \ldots, i_d)$ имеет ранг 1, если есть такое t, что $A(i_1, \ldots, i_d) = B(i_t)C(i_1, \ldots, i_{t-1}, i_{t+1}, \ldots, i_d)$.

Определение 3. Ранг d-мерной матрицы A — наименьшее такое r, что A можно представить в виде суммы r матриц ранга 1.

Определение 4. Матрица называется диагональной, если все её ненулевые числа стоят на диагонали $i_1 = i_2 = \ldots = i_d$.

Лемма 24. Ранг диагональной матрицы равен числу ненулевых коэффициентов.

Доказательство теоремы 20. Пусть $X = \{x_1, \ldots, x_m\} \subset \mathbb{F}_3^d$. Допустим, что не существует таких i, j, k, что $x_i + x_j + x_k = 0$. Тогда каждый вектор повторяется не более двух раз. Также можно считать, что они все различны (после такого преобразования суммарное число векторов уменьшится не более чем в 2 раза). Рассмотрим такой многочлен от $3d$ переменных:

$$P(\vec{u}, \vec{v}, \vec{w}) = \prod_{i=1}^{d} ((u_i + v_i + w_i)^2 - 1).$$

По предположению, если u, v, w не все одинаковы и из множества x_i, то $P(u,v,w) = 0$. Действительно, $u + v + w \ne 0$ и $u + 2v = u - v \ne 0$, в обоих случаях произведение 0. Будем интерпретировать P как матрицу $3^d \times 3^d \times 3^d$. Оценим $rank\ P$.

Лемма 25. $rank\ P \geq \frac{m}{2}$.

Доказательство. Ранг матрицы не больше ранга подматрицы, а подматрица $P(u, v, w)$ при $u, v, w \in X$ диагональна. Значит, по 24 выполняется $rank\ P \leq \frac{m}{2}$. ■

Лемма 26. $rank\ P \leq 3 \sum\limits_{a+2b \leq 2d/3} \binom{d}{a,\ b}$.

Доказательство. Раскроем в многочлене скобки:

$$P(\vec{u}, \vec{v}, \vec{w}) = \prod_{i=1}^{d}((u_i + v_i + w_i)^2 - 1) = \sum \dots \overbrace{u_{\dots}^{\dots} v_{\dots}^{\dots} w_{\dots}^{\dots}}^{\leq 2d \text{ букв}}.$$

Заметим, что множителей с какой-то буквой (из u, v, w) не более $\frac{2d}{3}$. Поэтому

$$P(\vec{u}, \vec{v}, \vec{w}) = \sum u_{\dots}^{\dots} \cdot Q(\vec{v}, \vec{w}) + \sum v_{\dots}^{\dots} \cdot R(\vec{u}, \vec{w}) + \sum w_{\dots}^{\dots} \cdot S(\vec{u}, \vec{v}),$$

где в каждой сумме участвуют члены с достаточно малым кол-вом вынесенных переменных (например, в первой сумме количество u_i не больше $\frac{2d}{3}$). Заметим, что это представление P в виде суммы нужного количества матриц ранга не более 1. ■

Определение 5. Пусть A — d-матрица, $\vec{v}$ — вектор в $\mathbb{F}^n$, где n — размер каждого ребра A (считаем, что A кубическая). Определим свёртку $A \times v$ как $(d-1)$-матрицу такую, что $(A \times \vec{v})(i_1, \dots, i_{d-1}) = \sum\limits_{i_d=1}^{n} v_(i_d) A(i_1, \dots, i_d)$,

Доказательство леммы 24. Доказываем по индукции по количеству измерений. Пусть $A = A_1 + \ldots + A_r$, где у A_i ранг 1, и на диагонали ненулевые числа (иначе можно рассматривать подматрицу). Пусть для первых s матриц выполняется $A_i(\vec{j}) = B_i(j_1, \dots, j_{d-1}) C_i(j_d)$. Заметим, что по 23 существует вектор v такой, что:

- $(v, C_i) = 0\ \forall i = 1, \dots, s$ (скалярное произведение);
- v имеет хотя бы $n - s$ ненулевых координат.

Заметим, что $A \times v = A_{s+1} \times v + A_{s+2} \times v + \ldots + A_r \times v$, и все коэффициенты в этих слагаемых ненулевые. По предположению индукции лемма доказана. ■