Math-Net.Ru

Общероссийский математический портал

Д. Р. Хис-Браун, К теоремам Шевалле–Варнинга, *УМН*,
2011, том 66, выпуск 2, 223–232

DOI: <https://doi.org/10.4213/rm9423>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.137.237

26 апреля 2023 г., 14:40:13

УДК 511

Памяти Анатолия Карацубы

К теоремам Шевалле–Варнинга

Д. Р. Хис-Браун

Пусть $f_1, \dots, f_r$ — многочлены от n переменных над полем $\mathbb{F}_q$ и пусть $d_1, \dots, d_r$ — их степени. В 1935 г. Э. Варнинг показал, что для числа $\mathcal{N}$ общих нулей многочленов f_i выполнено неравенство $\mathcal{N} \geq q^{n-d}$. Основная цель настоящей статьи — улучшить эту оценку. В предположении, что множество общих нулей не образует аффинного подпространства в $\mathbb{F}_q^n$, показывается, например, что $\mathcal{N} \geq 2q^{n-d}$, если $q \geq 4$, и что $\mathcal{N} \geq q^{n+1-d}/(n+2-d)$, если все многочлены f_i являются однородными.

Библиография: 5 названий.

Ключевые слова: теоремы Шевалле–Варнинга, многочлены, конечные поля, нули, оценка снизу, число нулей, аффинное подпространство.

Наиболее известный результат типа Шевалле–Варнинга утверждает, что если у многочлена над конечным полем характеристики p число переменных больше степени, то количество нулей многочлена кратно p . В частности, если многочлен однородный, то у него имеется хотя бы один нетривиальный нуль.

В литературе известен ряд утверждений, имеющих отношение к этому результату. В общей ситуации, пусть $\mathbb{F}_q$ — конечное поле, а $\mathbf{f} = (f_1(\mathbf{x}), \dots, f_r(\mathbf{x}))$ — набор из r многочленов $f_i(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$. Пусть d_i — (полная) степень f_i , а $d = d_1 + \dots + d_r$. Для подмножеств $S \subseteq \mathbb{F}_q^n$ положим

$$z(\mathbf{f}; S) = z(S) := \{\mathbf{x} \in S : f_i(\mathbf{x}) = 0 \ (1 \leq i \leq r)\}$$

и

$$\mathcal{N}(\mathbf{f}; S) = \mathcal{N}(S) := \#z(\mathbf{f}; S).$$

Тогда согласно оригинальному результату К. Шевалле [1] 1935 г., если $n > d$ и $z(\mathbb{F}_q^n)$ — непустое множество, то оно содержит не менее 2 точек. Вслед за тем Э. Варнинг [2] показал, что при $n > d$

$$p \mid \mathcal{N}(\mathbb{F}_q^n), \quad (1)$$

где p — характеристика $\mathbb{F}_q$. Фактически это следовало из несложной перекомпоновки доказательства Шевалле. В той же работе Варнинг доказал, что если $n \geq d$, а H_1 и H_2 — параллельные аффинные гиперплоскости в $\mathbb{F}_q^n$, то

$$\mathcal{N}(H_1) \equiv \mathcal{N}(H_2) \pmod{p}. \quad (2)$$

В качестве следствия он вывел следующее утверждение: если $z(\mathbb{F}_q^n)$ непусто, то

$$\mathcal{N}(\mathbb{F}_q^n) \geq q^{n-d} \quad (n > d). \quad (3)$$

Позже, в 1964 г., Дж. Экс [3] усилил (1) и продемонстрировал, что на самом деле

$$q \mid \mathcal{N}(\mathbb{F}_q^n) \quad (n > d). \quad (4)$$

Если n велико по сравнению с d , то результат можно усилить дальше, как было показано, например, Н. М. Катцем [4]. Эти уточнения утверждения (4) позволяют усилить все результаты, которые мы установим в настоящей работе. Однако в центре нашего внимания будет случай, когда n превосходит d не намного, так что нам хватит соотношения (4).

Наш первый результат показывает, что у (2) есть более сильный вариант, соответствующий уточнению Экса утверждения (1). Чтобы подчеркнуть, что возникающие аффинные подпространства не обязательно будут векторными подпространствами $\mathbb{F}_q^n$, мы будем действовать над $\mathbb{A}^n(\mathbb{F}_q)$, хотя множества $z(\mathbb{A}^n(\mathbb{F}_q))$ и $z(\mathbb{F}_q^n)$, разумеется, совпадают.

ТЕОРЕМА 1. *Во введенных выше обозначениях, для произвольной пары параллельных подпространств $L_1, L_2 \subseteq \mathbb{A}^n(\mathbb{F}_q)$ размерности не ниже d выполняется*

$$\mathcal{N}(L_1) \equiv \mathcal{N}(L_2) \pmod{q}. \quad (5)$$

На самом деле, из наших рассуждений будет видно, как можно вывести (5) из (4).

Далее мы попытаемся усилить (3). Рассмотрим в $K = \mathbb{F}_{q^k}$ базис $\omega_1, \dots, \omega_k$ над полем $F = \mathbb{F}_q$ и положим

$$N_k(x_1, \dots, x_k) := N_{K/F}(x_1\omega_1 + \dots + x_k\omega_k). \quad (6)$$

Мы получили форму степени k от k переменных со следующим свойством: $N_k(x_1, \dots, x_k) = 0$ для $x_i \in \mathbb{F}_q$, только если все x_i обращаются в нуль. В частности, если $\mathbf{f}$ состоит ровно из одного многочлена $f_1 = N_d$, то $z(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q))$ – подпространство размерности $n - d$ и в (3) имеет место равенство. Однако, с другой стороны, верны следующие результаты.

ТЕОРЕМА 2. *Предположим, что $n > d$, и пусть $z(\mathbb{A}^n(\mathbb{F}_q))$ – непустое множество, не являющееся подпространством $\mathbb{A}^n(\mathbb{F}_q)$. Тогда:*

- (i) *для любого q выполняется неравенство $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) > q^{n-d}$;*
- (ii) *для $q \geq 4$ выполняется $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq 2q^{n-d}$;*
- (iii) *в случае, когда $\mathbf{f}$ состоит из однородных многочленов, для любого q выполняется неравенство $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq q^{n+1-d}/(n+2-d)$.*

При доказательстве мы используем только комбинаторику $\mathbb{A}^n(\mathbb{F}_q)$, а также равенство (5) и его следствие (4). Таким образом, если вместо $z(\mathbb{A}^n(\mathbb{F}_q))$ рассмотреть произвольное множество, для которого свойство (5) выполнено для любой пары параллельных d -мерных подпространств $\Lambda_1, \Lambda_2 \subseteq \mathbb{A}^n(\mathbb{F}_q)$, то аналогичные результаты тоже верны. В частности, мы видим, что в этом смысле

результат в (ii) неулучшаем, поскольку (5) выполнено для $z(\mathbb{A}^n(\mathbb{F}_q))$, образованного двумя параллельными подпространствами размерности $n - d$.

Теперь будет поучительно разобрать два простых примера. Первый из них показывает, что не приходится надеяться на усиление части (iii) теоремы 2 до неравенства $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq q^{n+1-d}$. Действительно, рассмотрим $\mathbf{f}$, состоящее из одного полинома $Q(x_1, x_2, x_3, x_4)$, где

$$Q(x_1, x_2, x_3, x_4) = x_1x_2 + x_3^2 + x_3x_4 + cx_4^2,$$

а коэффициент $c \in \mathbb{F}_q$ выбран так, чтобы многочлен $x_3^2 + x_3x_4 + cx_4^2$ был неприводим над $\mathbb{F}_q$. Тогда уравнение $Q = 0$ имеет ровно $q^3 - q^2 + q$ решений $(x_1, x_2, x_3, x_4) \in \mathbb{F}_q^4$, и, поскольку $d = 2$, получаем, что в этом случае

$$\mathcal{N}(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q)) = q^{n+1-d}(1 - q^{-1} + q^{-2}) < q^{n+1-d}.$$

На самом деле это также показывает, что часть (ii) теоремы не распространяется на случай $q = 2$.

Второй пример демонстрирует, что если $\mathbf{f}$ содержит ровно один многочлен f_1 , то $z(\mathbb{A}^n(\mathbb{F}_q))$ может оказаться подпространством размерности $n - k$, даже когда f_1 не раскладывается на линейные сомножители. Положим $n = 4$ и выберем базис $1, \alpha$ в $\mathbb{F}_{q^2}$ над полем $\mathbb{F}_q$. Обозначим через N и N' норменные формы для $\mathbb{F}_{q^4}$ над $\mathbb{F}_{q^2}$ и в $\mathbb{F}_{q^2}$ над $\mathbb{F}_q$ соответственно, где во втором случае использован базис $1, \alpha$. Пусть σ – нетривиальный автоморфизм $\mathbb{F}_{q^2}$ над $\mathbb{F}_q$. Тогда $N(\mathbf{x}) = Q_1(\mathbf{x}) + \alpha Q_2(\mathbf{x})$ для некоторых квадратичных форм Q_1, Q_2 над $\mathbb{F}_q$. Ясно, что после линейной замены переменных над $\mathbb{F}_q$ мы можем записать $Q_1 + \alpha Q_2 = Y_1Y_2$ и $Q_1 + \alpha^\sigma Q_2 = Y_3Y_4$ для независимых переменных Y_1, Y_2, Y_3, Y_4 . Следовательно, если $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ отлочно от α и α^σ , то ранг $Q_1 + \beta Q_2$ равен 4. Разумеется, такое β существует всегда, за исключением случая $q = 2$. Теперь мы видим, что многочлен $f(\mathbf{x}) = (Q_1(\mathbf{x}) + \beta Q_2(\mathbf{x}))(Q_1(\mathbf{x}) + \beta Q_2(\mathbf{x}))^\sigma$ определен над $\mathbb{F}_q$ и не разлагается на линейные множители, но тем не менее $f(\mathbf{x}) = 0$ только при $\mathbf{x} = 0$.

Наконец, мы исследуем структуру $z(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q))$ с геометрической точки зрения.

ТЕОРЕМА 3. *Для любых фиксированных n и d существует константа $C(n, d)$ со следующим свойством. Произвольному набору полиномов $\mathbf{f}$ полной степени d соответствует такое множество абсолютно неприводимых многообразий $V_1, \dots, V_m$ над $\mathbb{F}_q$, для которого $z(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q))$ в точности равно множеству $\mathbb{F}_q$ -точек из $V_1 \cup \dots \cup V_m$. При этом степень каждого V_i не превосходит $C(n, d)$ и $m \leq C(n, d)$.*

Теперь оценка Ленга–Вейля [5] немедленно приводит к следующему результату.

СЛЕДСТВИЕ. *Пусть наибольшая размерность многообразий V_i равна D , и пусть k – число таких многообразий. Тогда (быть может, для большего значения константы $C(n, d)$)*

$$|\mathcal{N}(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q)) - kq^D| \leq C(n, d)q^{D-1/2}. \quad (7)$$

Таким образом, если $q \gg_{n,d} 1$, то $D \geq n - d$, а если $z(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q))$ не является подпространством размерности $n - d$, то $D \geq n + 1 - d$. В последнем случае

$$\mathcal{N}(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q)) \geq q^{n+1-d} - C(n, d)q^{n+1/2-d}$$

при $q \gg_{n,d} 1$.

Можно предположить, что $D \geq n - d$ вне зависимости от величины q , и было бы интересно получить прямое геометрическое доказательство этого результата. Разумеется, оценки D снизу получаются сравнением (7) с (3) и утверждением (iii) теоремы 2.

Теперь изложим доказательство теоремы 1. Пусть $f(x_1, \dots, x_n)$ – многочлен полной степени e . Имеется два разумных способа поставить ему в соответствие некоторую форму. Можно определить $f_-(x_1, \dots, x_n)$ как однородную компоненту степени e многочлена, а можно положить

$$f_+(x_0, \dots, x_n) = x_0^e f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

Для системы многочленов $\mathbf{f}$ зададим $\mathbf{f}_-$ и $\mathbf{f}_+$ описанными процедурами, где для многочлена f_i мы выбираем $e = d_i$. Ясно, что всякий нуль $\mathbf{f}$ порождает ровно $q - 1$ нулей $\mathbf{f}_+$ с $x_0 \neq 0$; а нули $\mathbf{f}_+$ с $x_0 = 0$ в точности соответствуют нулям $\mathbf{f}_-$. Таким образом,

$$\mathcal{N}(\mathbf{f}_+; \mathbb{F}_q^{n+1}) = (q - 1)\mathcal{N}(\mathbf{f}; \mathbb{F}_q^n) + \mathcal{N}(\mathbf{f}_-; \mathbb{F}_q^n).$$

В частности, если $n \geq d$, то из (4) следует, что $q \mid \mathcal{N}(\mathbf{f}_+; \mathbb{F}_q^{n+1})$ и потому

$$\mathcal{N}(\mathbf{f}; \mathbb{F}_q^n) \equiv \mathcal{N}(\mathbf{f}_-; \mathbb{F}_q^n) \pmod{q}.$$

Итак, мы видим, что по модулю q величина $\mathcal{N}(\mathbf{f}; \mathbb{F}_q^n)$ зависит только от старших однородных компонент многочленов $f_1, \dots, f_r$.

Пусть теперь заданы параллельные m -мерные подпространства L_1 и L_2 пространства $\mathbb{F}_q^n$. Ограничения форм из $\mathbf{f}$ на L_1 представляются набором многочленов $(g_1^{(1)}, \dots, g_r^{(1)})$ от m переменных; для L_2 ситуация аналогична. Поскольку L_1 и L_2 параллельны, старшие однородные компоненты у $g_i^{(1)}$ и $g_i^{(2)}$ одни и те же. Тем самым, мы пришли к теореме 1.

Наше доказательство теоремы 2 основано на следующих двух леммах, которые будут доказаны сразу после доказательства теоремы 2.

ЛЕММА 1. Пусть $L_0 \subseteq \mathbb{A}^n(\mathbb{F}_q)$ – подпространство. Выберем пространство L максимально возможной размерности k , для которого $L \supseteq L_0$ и $\mathcal{N}(L) = \mathcal{N}(L_0)$. Пусть $L' \supset L$ – пространство размерности $k + 1$ с минимальным $\mathcal{N}(L')$. Тогда

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq \mathcal{N}(L) + \frac{q^{n-k} - 1}{q - 1} (\mathcal{N}(L') - \mathcal{N}(L)). \quad (8)$$

ЛЕММА 2. Пусть $S \subseteq \mathbb{A}^t(\mathbb{F}_q)$ – множество, содержащее $t + 1$ точку в общем положении. Тогда:

- (i) если $q = 2$ и не существует двумерной плоскости $L \subseteq \mathbb{A}^t(\mathbb{F}_q)$, пересекающей S ровно в трех точках, то $S = \mathbb{A}^t(\mathbb{F}_q)$;
- (ii) если $q \geq 3$ и $\ell \subseteq S$ для всякой прямой ℓ , пересекающей S хотя бы в двух точках, то $S = \mathbb{A}^t(\mathbb{F}_q)$;
- (iii) если $q \geq 4$ и $\#(S \cap \ell) \geq q - 1$ для всякой прямой ℓ , пересекающей S не менее чем в двух точках, то $\mathbb{A}^t(\mathbb{F}_q) \setminus S$ лежит в гиперплоскости;
- (iv) если $m \geq 2$ – целое число и $\#(S \cap \ell) \geq m + 1$ для всякой прямой ℓ , пересекающей S не менее чем в двух точках, то

$$\#S \geq \frac{m^{t+1} - 1}{m - 1}.$$

Для вывода теоремы 2 предположим, что $z(\mathbb{A}^n(\mathbb{F}_q))$ содержит максимальное множество из $t \geq n + 1 - d$ точек в общем положении. Определим $\mathbb{A}^t(\mathbb{F}_q)$ как подпространство, натянутое на эти точки, и применим лемму 2 к множеству S нулей $\mathbf{f}$, лежащих в $\mathbb{A}^t(\mathbb{F}_q)$. По ходу дела мы приведем детали доказательства утверждений теоремы 2, но в общем наша стратегия будет следующей. С помощью леммы 2 мы либо получаем устраивающую нас оценку снизу для $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q))$, либо приходим к линейному пространству L_0 , к которому мы применим лемму 1. В случае, охватываемом частью (i) леммы 2, размерность этого пространства равна 2, а в противном случае оно одномерно. В силу нашего построения будет выполнено $\mathcal{N}(L_0) \leq q - 1$, а так как в лемме 1 $\mathcal{N}(L) = \mathcal{N}(L_0)$, то размерность k пространства L не превосходит d : в противном случае (5) приводит к противоречию. Если $k \leq d - 2$, то из (8) следует устраивающая нас оценка снизу

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq \frac{q^{n-k} - 1}{q - 1} \geq \frac{q^{n+2-d} - 1}{q - 1} \geq q^{n+1-d}.$$

Итак, можно предполагать, что L или L' имеет размерность d . Соответственно положим $L_1 = L$ или L' . Если $\mathcal{N}(L_1)$ принимает значение $v \leq q - 1$, то из (5) получаем, что $\mathcal{N}(L^*) \geq v$ для всякой аффинной d -плоскости L^* , параллельной L_1 . Покрыв $\mathbb{A}^n(\mathbb{F}_q)$ такими подпространствами, мы покажем, что $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq vq^{n-d}$. Подобные оценки будут достаточны для доказательства теоремы во всех случаях.

Начнем с доказательства части (i) теоремы 2. Из утверждений (i) и (ii) леммы 2 мы всегда можем вывести удовлетворяющую нас оценку $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq q^{n+1-d}$, за исключением случая, когда $q = 2$ и для некоторой двумерной плоскости $L_0 \subseteq \mathbb{A}^n(\mathbb{F}_q)$ выполнено $\mathcal{N}(L_0) = 3$, и случая, когда $q \geq 3$ и для некоторой прямой $L_0 \subseteq \mathbb{A}^n(\mathbb{F}_q)$ выполнено $2 \leq \mathcal{N}(L_0) \leq q - 1$. Применим теперь лемму 1. Как и выше, обязательно выполнено неравенство $k \leq d$. Более того, если $k \leq d - 1$, то (8) дает нам

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq \frac{q^{n+1-d} - 1}{q - 1} > q^{n-d},$$

чего вполне достаточно. Если же $k = d$ и $q = 2$, то (8) гарантирует, что

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq 3 + \frac{2^{n-d} - 1}{2 - 1} > 2^{n-d}.$$

Наконец, при $k = d$ и $q \geq 3$ имеем $2 \leq \mathcal{N}(L_0) = \mathcal{N}(L) \leq q - 1$ и проведенные выше рассуждения с $2 \leq v \leq q - 1$ показывают, что $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq 2q^{n-d}$. Итак, во всех случаях $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) > q^{n-d}$.

Обратимся к части (ii) теоремы 2. В силу утверждения (iii) леммы 2,

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq q^{n+1-d} - q^{n-d} \geq 2q^{n-d}$$

за исключением случая, когда $2 \leq \mathcal{N}(L_0) \leq q - 2$ для некоторой прямой $L_0 \subseteq \mathbb{A}^n(\mathbb{F}_q)$. Как и выше, используя лемму 1, мы можем считать, что $k = d - 1$ или d . Если $k = d$, то $2 \leq \mathcal{N}(L) \leq q - 2$ и, как и раньше, можно использовать (5) и заключить, что $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq 2q^{n-d}$. Аналогично, если $k = d - 1$ и $\mathcal{N}(L') - \mathcal{N}(L) = 1$, то $3 \leq \mathcal{N}(L') \leq q - 1$ и потому $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq 3q^{n-d}$. Наконец, при $k = d - 1$ и $\mathcal{N}(L') - \mathcal{N}(L) \geq 2$ из (8) следует, что

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq 2 \frac{q^{n+1-d} - 1}{q - 1} \geq 2q^{n-d}.$$

Тем самым искомая оценка доказана во всех случаях.

Для доказательства третьего утверждения теоремы 2 мы используем лемму 2 (часть (iv)), где целое число $m \leq q - 1$ будет выбрано по ходу дела. Итак,

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq \frac{m^{n+2-d} - 1}{m - 1} \geq m^{n+1-d},$$

если только не существует прямой с $2 \leq \mathcal{N}(L_0) \leq m$. А в этом последнем случае из леммы 1 выводим, что

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq \frac{q^{n-k} - 1}{q - 1} (\mathcal{N}(L') - m),$$

и в силу проведенных выше рассуждений достаточно рассмотреть значения $k = d - 1$ и $k = d$. Если $k = d - 1$, то можно показать, что $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq q^{n-d}(q - m)$ за исключением того случая, когда

$$m + 1 \leq \mathcal{N}(L') \leq q - 1.$$

Однако в последнем случае, используя (5), мы стандартным образом доказываем, что $\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq (m + 1)q^{n-d}$. В однородном случае равенство $k = d$ не может выполняться. Чтобы доказать это, рассмотрим два случая. Если $k = d$ и $\mathbf{0} \in L$, то $q - 1 \mid \mathcal{N}(L) - 1$, поскольку при $\mathbf{x} \in z(L)$ любой вектор, пропорциональный $\mathbf{x}$, тоже принадлежит $z(L)$. Однако это невозможно, поскольку $2 \leq \mathcal{N}(L_0) = \mathcal{N}(L) \leq m$. С другой стороны, при $\mathbf{0} \notin L$ рассмотрим $(d + 1)$ -мерное пространство $L' := \langle L, \mathbf{0} \rangle$. Тогда $\mathcal{N}(L') = 1 + (q - 1)\mathcal{N}(L)$. В силу (4) получаем, что $q \mid \mathcal{N}(L')$, и, значит, $\mathcal{N}(L) \equiv 1 \pmod{q}$. Это снова

невозможно, поскольку $2 \leq \mathcal{N}(L) \leq m$. Таким образом, должно выполняться или неравенство

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq m^{n+1-d},$$

или

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq q^{n-d}(q-m),$$

или

$$\mathcal{N}(\mathbb{A}^n(\mathbb{F}_q)) \geq (m+1)q^{n-d}.$$

Теперь мы получим требуемую оценку, если возьмем

$$m = \left\lfloor \frac{q(n+1-d)}{n+2-d} \right\rfloor$$

и заметим, что

$$\left\lfloor \frac{qv}{v+1} \right\rfloor^v \geq \frac{q^v}{v+1}$$

для любых натуральных $v \geq 2$ и $q \geq 2v+3$ за исключением $v=2$, $q=7$.

Оставшиеся случаи следуют из утверждений (i) и (ii) теоремы, а также из (4).

Докажем теперь леммы 1 и 2. Для доказательства леммы 1 достаточно заметить, что $\mathbb{A}^n(\mathbb{F}_q)$ – дизъюнктное объединение L с множествами $L^* \setminus L$, где L^* пробегает все $(k+1)$ -мерные подпространства, содержащие L . Всего таких подпространств $(q^{n-k}-1)/(q-1)$. Теперь лемма следует из неравенства $\mathcal{N}(L^* \setminus L) \geq \mathcal{N}(L') - \mathcal{N}(L)$.

Чтобы доказать лемму 2, придется заметно больше потрудиться. Четыре утверждения леммы будут доказаны отдельно, и в каждом случае мы используем индукцию по t . Все эти утверждения, очевидно, верны для $t=0$ и $t=1$. Для индуктивного перехода в случае (i) можно предположить, что S содержит подпространство L_0 размерности $t-1$, а также точку P_0 вне L_0 . Выберем теперь точку $P \notin L_0$, $P \neq P_0$, и покажем, что $P \in S$. Тогда мы сможем заключить, что действительно $S = \mathbb{A}^t(\mathbb{F}_q)$. Пусть P_1 – любая точка из L_0 . Рассмотрим двумерную плоскость, порожденную P , P_0 и P_1 . Поскольку $q=2$, она содержит три порождающие точки и какую-то четвертую точку P_2 , лежащую в L_0 . В силу нашей конструкции, P_0 , P_1 и P_2 лежат в S , так что по предположению $P \in S$, что и требовалось.

Чтобы доказать утверждение (ii), мы проведем такие же предварительные построения: мы предполагаем, что S содержит линейное пространство L_0 размерности $t-1$, а также точку P_0 вне L_0 . Выберем точку $P \notin L_0$, отличную от P_0 . Сначала допустим, что прямая ℓ , проходящая через P_0 и P , пересекает L_0 в какой-то точке P_1 . Тогда ℓ пересекает S не менее чем в двух точках, P_0 и P_1 . Значит, по предположению индукции, ℓ лежит в S , так что и P принадлежит S . Эти рассуждения годятся для всех точек P кроме тех, что лежат на гиперплоскости L_1 , параллельной L_0 и проходящей через P_0 . Для таких точек P мы зафиксируем произвольную точку P_1 из L_0 и рассмотрим прямую ℓ , проходящую через P и P_1 . Поскольку $q \geq 3$, эта прямая содержит еще хотя бы

одну точку P_2 , которая не может лежать на L_1 . Значит, $P_1 \in S$ в силу доказанного выше. Следовательно, ℓ пересекает S по меньшей мере в двух точках, P_1 и P_2 , и в силу наших предположений всякая точка ℓ лежит в S . В частности, $P \in S$, что и требовалось доказать.

Доказательство части (iii) леммы 2 самое сложное. Обозначим через S^c дополнение $\mathbb{A}^t(\mathbb{F}_q) \setminus S$ к S . Наш план – показать, что если S^c тоже содержит $t + 1$ точку в общем положении, то выполнено как неравенство $\#S > q^t/2$, так и $\#S^c > q^t/2$, что приводит к противоречию. Заметим, что условие утверждения (iii) симметрично относительно S и S^c , поскольку S пересекается с ℓ не меньше чем в двух точках тогда и только тогда, когда $\#(S^c \cap \ell) < q - 1$. Пусть R – это S или S^c и предположим, что R содержит $t + 1$ точку $P_0, \dots, P_t$ в общем положении. В качестве предположения индукции допустим, что для всякого $(t - 1)$ -мерного подпространства $L \subset \mathbb{A}^t(\mathbb{F}_q)$ либо $R \cap L$ не содержит t точек в общем положении, либо $L \setminus R$ лежит в собственном подпространстве L . Так что $L \cap R$ или $L \cap R^c$ лежит в собственном подпространстве L . Если $L = L_0$ натянуто на $P_1, \dots, P_t$, то реализуется вторая возможность. Для всякой точки $P \in L_0$ прямая ℓ , проходящая через P и P_0 , пересекает R не менее чем в двух точках (P и P_0), а значит, содержит не менее $q - 1$ точек из R . Выбирая разные P , мы получаем непересекающиеся множества $\ell \setminus \{P_0\}$, поэтому

$$\#R \geq 1 + (q - 2)\#(L_0 \cap R). \quad (9)$$

Допустим теперь, что для всякого $(t - 1)$ -мерного подпространства L , параллельного L_0 , но не совпадающего с ним, $L \cap R$ лежит в собственном подпространстве L . Поскольку $\mathbb{A}^t(\mathbb{F}_q)$ – дизъюнктное объединение L_0 и всевозможных подпространств L , получаем

$$\#R \leq \#(L_0 \cap R) + (q - 1)q^{t-2}.$$

Сравнивая это с (9), мы видим, что $(q - 3)\#(L_0 \cap R) < (q - 1)q^{t-2}$, а так как $\#(L_0 \cap R) \geq q^{t-1} - q^{t-2}$, то $q < 4$. Итак, при $q \geq 4$ должно существовать хотя бы одно подпространство L_1 , параллельное L_0 и не совпадающее с ним, для которого именно пересечение $L_1 \cap R^c$ содержится в собственном подпространстве L_1 . Если выбрать точку $Q \in L_1$ и сосчитать точки R , лежащие на прямых, соединяющих Q с L_0 , то, используя рассуждения из доказательства (9), мы получим по меньшей мере $(q - 2)\#(L_0 \cap R)$ точек из R , не лежащих на L_1 . Если теперь принять во внимание точки из $L_1 \cap R$, то мы увидим, что

$$\#R \geq (q - 2)\#(L_0 \cap R) + \#(L_1 \cap R).$$

Однако в нашем построении и $L_0 \cap R^c$, и $L_1 \cap R^c$ лежат в собственных подпространствах, так что $\#(L_0 \cap R) \geq q^{t-1} - q^{t-2}$ и аналогично для $\#(L_1 \cap R)$. Следовательно, $\#R \geq (q - 1)^2 q^{t-2} > q^t/2$ поскольку $q \geq 4$. Как мы уже объясняли, из этого неравенства следует утверждение (iii) леммы.

Наконец, перейдем к части (iv) леммы 2. Для индуктивного перехода будем предполагать, что имеются $(t - 1)$ -мерное пространство L_0 и точка P_0 вне L_0 ,

такие, что

$$\#(S \cap L_0) \geq \frac{m^t - 1}{m - 1}$$

и $P_0 \in S$. Для любой точки P из $S \cap L_0$ прямая ℓ , проходящая через P и P_0 , содержит не менее двух точек S , а значит, по предположению, она содержит не менее $m + 1$ таких точек. Для разных P множества $\ell \setminus \{P_0\}$ не пересекаются, так что

$$\#S \geq 1 + m\#(S \cap L_0) \geq 1 + m \frac{m^t - 1}{m - 1} = \frac{m^{t+1} - 1}{m - 1}.$$

Это завершает доказательство по индукции.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Если какой-то многочлен из $\mathbf{f}$ тождественно равен нулю, то очевидно, что его можно удалить из системы, а если какой-то из многочленов – ненулевая константа, то $z(\mathbf{f}; \mathbb{A}^n(\mathbb{F}_q))$ пусто и искомый результат тривиальным образом выполнен. Значит, мы можем считать, что степень каждого f_i положительна, так что r , число многочленов f_i , не превосходит d . Итак, множество нулей многочленов из $\mathbf{f}$ – алгебраическое многообразие V над $\overline{\mathbb{F}}_q$, размерность которого не превосходит n . Оно определено над $\mathbb{F}_q$, но может не быть абсолютно неприводимым. Мы назовем его неприводимые компоненты, не определенные над $\mathbb{F}_q$, “плохими” компонентами и зададимся целью заменить V многообразием V^* без плохих компонент, для которого $V(\mathbb{F}_q) = V^*(\mathbb{F}_q)$. Опишем общую “процедуру редукции” для наших многообразий. Чтобы держать под контролем число абсолютно неприводимых компонент многообразия и их степени, нам будет удобно ввести обозначение $\delta(X) = \sum \deg(X_i)$, где многообразие X является объединением абсолютно неприводимых компонент X_i . Тогда $\delta(V) \leq C_0(n, d)$ для некоторой величины $C_0(n, d)$, зависящей лишь от n и d , и мы хотим доказать аналогичную оценку $\delta(V^*) \leq C(n, d)$ для V^* .

Пусть у V есть хотя бы одна плохая компонента. Выберем плохую компоненту W максимальной размерности D . Рассмотрим множества $W_1 (= W)$, $\dots$, W_k , сопряженные с W относительно действия группы Галуа. Поскольку все они – неприводимые компоненты V , мы видим, что $k \leq C_0(n, d)$. Любая $\mathbb{F}_q$ -точка из W лежит в $W' := W_1 \cap \dots \cap W_k$. Так что, заменив компоненты $W_1, \dots, W_k$ многообразия V на W' и обозначив получившееся многообразие через V_1 , получаем равенство $V(\mathbb{F}_q) = V_1(\mathbb{F}_q)$. Вдобавок у V_1 нет плохих компонент размерности выше D , а так как $\dim(W') < \dim(W)$, то число плохих компонент размерности D уменьшилось на единицу. Заметим также, что мы можем оценить $\delta(W')$ сверху через n и $C_0(n, d)$, так что $\delta(V_1) \leq C_1(n, d)$ для подходящего целого $C_1(n, d)$. Теперь повторим процедуру редукции и перейдем от V_1 к V_2 и т.д. Поскольку на каждом шагу число плохих компонент максимальной размерности сокращается, а $\delta(V_i)$ остается под контролем, процесс рано или поздно завершится и даст нам многообразие V^* , у которого $\delta(V^*)$ оценивается через n и d . Отсюда вытекает теорема.

Эти исследования были начаты во время моего пребывания в Институте высших научных исследований в Принстоне. Я благодарен институту за гостеприимство и финансовую поддержку. Я также выражаю благодарность рецензенту за тщательное чтение первоначального варианта статьи, что позволило исправить две ошибки.

Список литературы

- [1] C. Chevalley, “Démonstration d’une hypothèse de M. Artin”, *Abh. Math. Sem. Univ. Hamburg*, **11** (1935), 73–75.
- [2] E. Warning, “Bemerkung zur vorstehenden Arbeit von Herrn Chevalley”, *Abh. Math. Semin. Hamb. Univ.*, **11** (1935), 76–83.
- [3] J. Ax, “Zeros of polynomials over finite fields”, *Amer. J. Math.*, **86**:2 (1964), 255–261.
- [4] N. M. Katz, “On a theorem of Ax”, *Amer. J. Math.*, **93**:2 (1971), 485–499.
- [5] S. Lang, A. Weil, “Number of points of varieties in finite fields”, *Amer. J. Math.*, **76**:4 (1954), 819–827.

Д. Р. Хис-Браун (D. R. Heath-Brown)
Mathematical Institute, University of Oxford, UK
E-mail: rhb@maths.ox.ac.uk

Поступила в редакцию
29.09.2010