MATEMATICKO-FYZIKÁLNY ČASOPIS SAV, 12. 3. 1962

ЗАМЕТКА ОБ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЯХ НАД КОНЕЧНЫМ ПОЛЕМ

ШТЕФАН ШВАРЦ (ŠTEFAN SCHWARZ), Братислава

Пусть

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \tag{1}$$

полином n-й степени над конечным полем $\boldsymbol{T} = GF(q)$, где $q = p^s$, $s > 1$ и p — простое число.

Пусть σ_k обозначает число различных неприводимых факторов полинома $f(x)$ k-й степени над полем $GF(q)$.

В работе [1] мы занимались взаимосвязью между числами $\sigma_1, \sigma_2, \ldots, \sigma_k$ и рангами некоторых циклических матриц, зависящих от коэффициентов полинома (1). Матрицы, которые там выступали, были порядка $q - 1$, $q^2 - 1, \ldots, q^k - 1$.

В этой заметке, которая не зависит от предыдущей работы, укажем на взаимное соотношение между числами $\sigma_1, \sigma_2, \ldots, \sigma_n$ и рангами некоторых матриц, зависящих от полинома (1), причем все рассматриваемые матрицы — порядка n.

Несмотря на то, что идет речь по существу о элементарных рассуждениях, нигде в литературе не нашел ссылку на такого рода соотношение, хотя вопросом определения числа σ_1 занимались в большом числе работ. (Смотри [2], стр. 223—262.)

Пусть k — целое число и пусть $k > k' > k'' > \ldots 1$ — все делители числа k. Если $\varphi(x)$ — какой-нибудь неприводимый полином k-й степени над полем $\boldsymbol{T} = GF(q)$ и $\varphi(j) = 0$, то известно, что в поле $\boldsymbol{T}(j) \simeq GF(q^k)$ лежат все нулевые точки всех неприводимых полиномов над $\boldsymbol{T}$ степени $k, k', k'', \ldots, 1$. Каждый элемент поля $\boldsymbol{T}(j)$ удовлетворяет уравнению $x^{q^k} - x = 0$.

В дальнейшем будем употреблять следующие обозначения. Если $\beta_1, \beta_2, \ldots, \beta_m$ элементы какого-нибудь поля, то через $\boldsymbol{V}(\beta_1, \beta_2, \ldots, \beta_m)$ и через $\boldsymbol{V}^*(\beta_1, \beta_2, \ldots, \beta_m)$ будем обозначать соответственно матрицы

$$\boldsymbol{V}(\beta_1, \beta_2, \ldots, \beta_m) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \beta_1 & \beta_2 & \ldots & \beta_m \\ \vdots & & & \\ \beta_1^{m-1} & \beta_2^{m-1} & \ldots & \beta_m^{m-1} \end{pmatrix},$$

$$\boldsymbol{V}^*(\beta_1, \beta_2, \ldots, \beta_m) = \begin{pmatrix} 1 & \beta_1 & \ldots & \beta_1^{m-1} \\ 1 & \beta_2 & \ldots & \beta_2^{m-1} \\ \vdots & & & \\ 1 & \beta_m & \ldots & \beta_m^{m-1} \end{pmatrix}.$$

Через $\boldsymbol{D}_l$ будем обозначать симметрическую матрицу n-го порядка

$$\boldsymbol{D}_l = \begin{pmatrix} s_l & s_{l+1} & \ldots & s_{l+n-1} \\ s_{l+1} & s_{l+2} & \ldots & s_{l+n} \\ \vdots & & & \\ s_{l+n-1} & s_{l+n} & \ldots & s_{l+2(n-1)} \end{pmatrix}, \tag{2}$$

где s_j — суммы j-ых степеней корней уравнения $f(x) = 0$. Наконец, если $\boldsymbol{B}$ — какая-нибудь матрица, то ранг матрицы $\boldsymbol{B}$ обозначим через $h(\boldsymbol{B})$.

Будем предполагать, что полином (1) *не имеет кратных факторов*. Пусть все корни уравнения $f(x) = 0$ (лежащие в каком-то расширении поля $\boldsymbol{T}$) — $\alpha_1, \alpha_2, \ldots, \alpha_n$. Корень α_i лежит в поле $GF(q^k)$ тогда и только тогда, если удовлетворяет уравнению

$$x^{q^k} - x = 0. \tag{3}$$

Из определения чисел σ_i и из введенного выше примечания следует, что между элементами $\alpha_1, \alpha_2, \ldots, \alpha_n$ существует точно $t = k\sigma_k + k'\sigma_{k'} + \ldots + \sigma_1$ элементов, которые удовлетворяют уравнению (3). Пусть этими элементами являются $\alpha_1, \alpha_2, \ldots, \alpha_t$.

Обозначим для простоты $p^k = r$ и рассмотрим матрицу

$$\boldsymbol{A}_k = \begin{pmatrix} \alpha_1^r - \alpha_1 & \alpha_2^r - \alpha_2 & \ldots & \alpha_n^r - \alpha_n \\ \alpha_1(\alpha_1^r - \alpha_1) & \alpha_2(\alpha_2^r - \alpha_2) & \ldots & \alpha_n(\alpha_n^r - \alpha_n) \\ \vdots & & & \\ \alpha_1^{n-1}(\alpha_1^r - \alpha_1) & \alpha_2^{n-1}(\alpha_2^r - \alpha_2) & \ldots & \alpha_n^{n-1}(\alpha_n^r - \alpha_n) \end{pmatrix}.$$

Первые t столбцов матрицы $\boldsymbol{A}_k$ состоят из одних нулей. Определитель матрицы, которая получается из матрицы $\boldsymbol{A}_k$ отбрасыванием первых t столбцов и последних t строк, равен, очевидно, элементу

$$(\alpha_{t+1}^r - \alpha_{t+1}) \ldots (\alpha_n^r - \alpha_n) \, | \, \boldsymbol{V}(\alpha_{t+1}, \ldots, \alpha_n)|.$$

Поскольку все элементы $\alpha_{t+1}, \ldots, \alpha_n$ различные между собой и ни один из них не лежит в поле $GF(q^k)$, то написанное выражение отличное от нуля. Поэтому ранг матрицы $\boldsymbol{A}_k$ равен числу $n - t = n - (k\sigma_k + k'\sigma_{k'} + \ldots + \sigma_1)$.

Если умножим матрицу $\mathbf{A}_k$ на матрицу $\mathbf{V}^*(\alpha_1, \ldots, \alpha_n)$, получим

$$\mathbf{A}_k\mathbf{V}^* = \begin{pmatrix} \alpha_1^r - \alpha_1 & \alpha_2^r - \alpha_2 & \ldots & \alpha_n^r - \alpha_n \\ \vdots & & & \\ \alpha_1^{n+r-1} - \alpha_1^n & \alpha_2^{n+r-1} - \alpha_2^n & \ldots & \alpha_n^{n+r-1} - \alpha_n^n \end{pmatrix} \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ & & & \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} s_r - s_1 & s_{r+1} - s_2 & \ldots & s_{r+n-1} - s_n \\ s_{r+1} - s_2 & s_{r+2} - s_3 & \ldots & s_{r+n} - s_{n+1} \\ \vdots & & & \\ s_{r+n-1} - s_n & s_{r+n} - s_{n+1} & \ldots & s_{r+2(n-1)} - s_{2n-1} \end{pmatrix} = \mathbf{D}_r - \mathbf{D}_1.$$

Поскольку матрицы $\mathbf{A}_k$ и $\mathbf{A}_k\mathbf{V}^*$ имеют одинаковый ранг, то имеет место

$$n - (k\sigma_k + k'\sigma_{k'} + \ldots + \sigma_1) = h(\mathbf{D}_{q^k} - \mathbf{D}_1).$$

Из соотношения

$$\sum_{i/k} i\sigma_i = n - h(\mathbf{D}_{q^k} - \mathbf{D}_1)$$

используя формулу Мебиуса для инверсии, вытекает:

$$k\sigma_k = \sum_{i/k} \mu\left(\frac{k}{i}\right)[n - h(\mathbf{D}_{q^i} - \mathbf{D}_1)].$$

Значит (ввиду известных свойств функции Мебиуса):

(4) $$\sigma_1 = n - h(\mathbf{D}_q - \mathbf{D}_1),$$

(5) $$\sigma_k = -\frac{1}{k}\sum_{i/k} \mu\left(\frac{k}{i}\right) \cdot h(\mathbf{D}_{q^i} - \mathbf{D}_1),$$

для $k > 1$.

Найденный результат можем сформулировать в виде такой теоремы:

Теорема. *Пусть (1) — полином n-й степени над полем $GF(q)$, который не имеет кратных факторов. Пусть $\mathbf{D}_l$ — матрица n-го порядка вида (2), где s_j — сумма j-ых степеней корней уравнения $f(x) = 0$. Если σ_k обозначает число неприводимых факторов полинома (1) степени k, а $h(\mathbf{B})$ ранг матрицы $\mathbf{B}$, то для числа σ_1 и σ_k $(k > 1)$ имеют место соответственно формулы (4) и (5).*

Примечание. В нашей теореме мы сделали ограничивающее предположение, что полином $f(x)$ не имеет кратных факторов. Интересно исследовать, как далеко можно дойти с помощью нашего метода в случае кратных факторов.

Пусть между корнями $\alpha_1, \alpha_2, \ldots, \alpha_n$ есть лишь ϱ взаимно различных. Эти различные корни обозначим через $\beta_1, \beta_2, \ldots, \beta_\rho$. Значит, $\varrho < n$ и каждое β_i равно некоторму (или нескольким) из чисел $\alpha_1, \alpha_2, \ldots, \alpha_n$.

В этом случае матрица $\mathbf{V}^*(\alpha_1, \ldots, \alpha_n)$ имеет ранг точно ϱ. Действительно, каждый минор этой матрицы порядка $> \varrho$ имеет по крайней мере две одинаковые строки, а, значит, равен нулю. Но минор ϱ-го порядка

$$\begin{vmatrix} 1 & \beta_1 & \ldots & \beta_1^{\varrho-1} \\ \vdots & & & \\ 1 & \beta_\varrho & \ldots & \beta_\varrho^{\varrho-1} \end{vmatrix},$$

очевидно, отличный от нуля.

Далее исследуем ранг матрицы $\mathbf{A}_k$. Прежде всего видно, что матрица $\mathbf{A}_k$ имеет самое больше ϱ разных столбцов, и именно столбцы вида

$$\begin{matrix} 1(\beta_1^r - \beta_1) & 1(\beta_2^r - \beta_2) & \ldots & 1(\beta_\varrho^r - \beta_\varrho) \\ \beta_1(\beta_1^r - \beta_1) & \beta_2(\beta_2^r - \beta_2) & \ldots & \beta_\varrho(\beta_\varrho^r - \beta_\varrho) \\ \vdots & & & \\ \beta_1^{n-1}(\beta_1^r - \beta_1) & \beta_2^{n-1}(\beta_2^r - \beta_2) & \ldots & \beta_\varrho^{n-1}(\beta_\varrho^r - \beta_\varrho). \end{matrix}$$

Если, далее, элементы $\beta_1, \beta_2, \ldots \beta_\tau$ все элементы среди элементов $\beta_1, \beta_2, \ldots, \beta_\rho$, которые лежат в поле $GF(q^k)$, то первые τ столбцов равны нулю. Поэтому матрица $\mathbf{A}_k$ имеет ранг, равный не более числа $\varrho - \tau$. (Это имеет место и в случае, когда $\tau = 0$, то есть никакой из элементов $\beta_1, \beta_2, \ldots, \beta_\rho$ не лежит в поле $GF(q^k)$.) Так как σ_i обозначает число различных неприводимых факторов полинома $f(x)$ степени i (и каждый такий фактор имеет точно i различных корней), то $\tau = k\sigma_k + k'\sigma_{k'} + \ldots + \sigma_1$. Чтобы доказать, что матрица $\mathbf{A}_k$ имеет ранг точно $\varrho - \tau$, достаточно ограничиться случаем $\varrho - \tau > 0$ и рассмотреть следующий минор порядка $\varrho - \tau$ матрицы $\mathbf{A}_k$

$$\begin{vmatrix} \beta_{\tau+1}^r - \beta_{\tau+1} & \ldots & \beta_\varrho^r - \beta_\varrho \\ \vdots & & \\ \beta_{\tau+1}^{\varrho-\tau-1}(\beta_{\tau+1}^r - \beta_{\tau+1}) & & \beta_\varrho^{\varrho-\tau-1}(\beta_\varrho^r - \beta_\varrho) \end{vmatrix}.$$

Этот определитель равен элементу

$$(\beta_{\tau+1}^r - \beta_{\tau+1}) \ldots (\beta_\varrho^r - \beta_\varrho) \begin{vmatrix} 1 & \ldots & 1 \\ \vdots & & \\ \beta_{\tau+1}^{\varrho-\tau-1} & \ldots & \beta_\varrho^{\varrho-\tau-1} \end{vmatrix},$$

который отличный от нуля, так как с одной стороны все элементы $\beta_{\tau+1}, \beta_{\tau+2}, \ldots, \beta_\rho$ разные между собой, с другой стороны никакой из них не лежит в поле $GF(q^k)$.

Так как матрица $\mathbf{A}_k$ имеет ранг $\varrho - \tau$, матрица $\mathbf{V}^*(\alpha_1, \ldots, \alpha_n)$ ранг ϱ, то матрица $\mathbf{A}_k\mathbf{V}^* = \mathbf{D}_r - \mathbf{D}_1$ имеет ранг равен не более числа $\varrho - \tau$. Значит, имеет место

$$h(\mathbf{D}_r - \mathbf{D}_1) \leqq \varrho - \tau,$$

то-есть в расписанном виде:

$$(6) \qquad \begin{aligned} \sigma_1 &\leqq \varrho - h(\mathbf{D}_q - \mathbf{D}_1) \\ 2\sigma_2 + \sigma_1 &\leqq \varrho - h(\mathbf{D}_{q^2} - \mathbf{D}_1) \\ 3\sigma_3 + \sigma_1 &\leqq \varrho - h(\mathbf{D}_{q^3} - \mathbf{D}_1) \\ &\vdots \end{aligned}$$

Однако, это все, что можем доказать, потому что на простых примерах можно показать, что в соотношениях (6) может на самом деле иметь место знак неравенства.

Рассмотрим, например, полином $f(x) = x^6 + 1 = (x^2 + 1)^3$ над полем $GF(3)$. Здесь $s_n = 0$ для каждого $n > 0$. Значит, $h(\mathbf{D}_3 - \mathbf{D}_1) = 0$. Далее $\varrho = 2$ и $\sigma_1 = 0$. Следовательно, действительно $\sigma_1 < \varrho - h(\mathbf{D}_3 - \mathbf{D}_1)$. Из соотношений (6), значит, не можно найти числа σ_i даже в случае, когда нам известно ϱ.

Интересно указать и на трудности, связанные с определением числа ϱ. Матрицы $\mathbf{V}(\alpha_1, \ldots, \alpha_n)$ и $\mathbf{V}^*(\alpha_1, \ldots, \alpha_n)$ имеют ранг ϱ. Поэтому матрица $\mathbf{V}\mathbf{V}^* = \mathbf{D}_0$ имеет ранг $\leqq \varrho$. Однако, в отличие от известного случая поля действительных чисел может иметь место и знак неравенства, то-есть $\mathbf{D}_0$ может иметь ранг меньший, чем число ϱ. Для этого достаточно рассмотреть, например, полином $f(x) = x^3 - 1 = (x - 1)^3$ над полем $GF(3)$. Здесь

$$\mathbf{V} = \mathbf{V}^* = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

и эта матрица имеет ранг 1. Но $\mathbf{V}\mathbf{V}^*$, очевидно, нулевая матрица (в поле $GF(3)$). Это дальнейший довод, почему попытка распространить результаты нашей теоремы на полиномы с кратными факторами не приводит к удовлетворительным результатам.

ЛИТЕРАТУРА

[1] Horáková K., Schwarz Š., *Циклические матрицы и алгебраические уравнения над конечным полем*, Matematicko-fyzikálny časopis SAV 12 (1962), 38—48.

[2] Dickson L. E, *History of the Theory of Numbers*, *Vol.* I, New York reprinted 1934.

[3] Dickson L. E., Mitchel H. H., Vandiver H. S., Wahlin G. E., *Report of the Committee on Algebraic Numbers*, National Research Council, New York 1923.

Поступило 15. 2. 1962 г.

Katedra matematiky
Elektrotechnickej fakulty
Slovenskej vysokej školy technickej
v Bratislave

A NOTE ON ALGEBRAIC EQUATIONS OVER FINITE FIELDS

Štefan Schwarz

Summary

The main result of this note is the following theorem: Let $f(x)$ be a polynomial of degree n without multiple factors over the finite field $GF(q)$. Let $\mathbf{D}_l$ be the matrix (2) of order n, where s_j is the sum of j-th powers of the roots of $f(x) = 0$. Denote by σ_k the number of (different) irreducible factors of $f(x)$ of degree k $(1 \leqq k \leqq n)$ and by $h(\mathbf{B})$ the rank of a matrix $\mathbf{B}$. Then the numbers σ_1 and σ_k $(k > 1)$ are given by the formulas (4) and (5) respectively. (Hereby $\mu(x)$ is the Möbius function.)

In the concluding remark the difficulties are shown which arise in attempting to extend this theorem to polynomials with multiple factors.