ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր 106 2006 № 2

ПРИКЛАДНАЯ МАТЕМАТИКА

УДК 512.62; 519.711

В. П. Габриелян

Линеаризированные покрытия одного типа уравнений высших степеней над конечным полем

(Представлено академиком Ю.Г. Шукуряном 14/IX 2005)

Ключевые слова: *конечное поле, размерность смежного класса, линеаризированные покрытия, длина или сложность покрытия*

В работе получены оценки сложности минимального покрытия множества решений уравнения $x_1y_1^{k_1}+x_2y_2^{k_2}+\cdots+x_ny_n^{k_n}=b$ над произвольным конечным полем F_q смежными классами линейных подпространств, где $k_1,k_2,\ldots,k_n$ — произвольные ненулевые натуральные числа. Для произвольного ненулевого элемента $b\in F_q$ построено минимальное покрытие. При $b=0$ сложность построенного покрытия близка к минимальной.

Пусть F_{q^n} конечное поле из q^n элементов [1] (q — степень простого числа). Рассмотрим это поле как n-мерное линейное пространство над полем F_q и представим его в следующем виде: $F_{q^n}\equiv\{(\alpha_1,\alpha_2,\ldots,\alpha_n)|\ \alpha_i\in F_q,\ i=1,2,\ldots,n\}$. Далее, если L — линейное подпространство в F_{q^n} и $\alpha\in F_{q^n}$, тогда множество $\alpha+L=\{\alpha+x|\ x\in L\}$ называется *смежным классом* (сдвигом) линейного подпространства L, размерность которого определяется как $\dim L$. Согласно эквивалентному определению подмножество $H\subseteq F_{q^n}$ является смежным классом, если для любых $h_1,h_2,\ldots,h_m\in H$ и $\lambda_1,\lambda_2,\ldots,\lambda_m\in F_q$ таких, что $\sum\limits_{i=1}^{m}\lambda_i=1$, сумма $\sum\limits_{i=1}^{m}\lambda_ih_i$ (аффинная комбинация векторов $h_1,h_2,\ldots,h_m$) лежит в H. Легко проверить, что существует взаимно однозначное соответствие между множеством m-мерных смежных классов в F_{q^n} и множеством классов эквивалентности всех систем линейных уравнений ранга $n-m$ относительно n неизвестных над полем F_q.

Определение 1. Пусть $N\subseteq F_{q^n}$. Если $H_1,H_2,\ldots,H_s$ суть смежные классы в N и $H_1\cup H_2\cup\ldots\cup H_s=N$, то совокупность смежных классов

$\{H_1, H_2, \ldots, H_s\}$ называется *линеаризированным покрытием* множества N. Количество смежных классов в покрытии называется его длиной.

Проблема минимального покрытия множества решений полиномиального уравнения над конечным полем смежными классами линейных подпространств впервые исследована в работах [2,3] для простого поля F_2.

Некоторые метрические характеристики линеаризированных покрытий подмножеств конечного поля исследованы в [4]. Задача линеаризированного покрытия симметрических подмножеств конечного поля решена в [5], а для множеств решений квадратичных и некоторых уравнений более высших степеней над конечным полем — в работах [6-8].

В настоящей работе задача минимального линеаризированного покрытия исследована для множества решений уравнения $x_1y_1^{k_1} + x_2y_2^{k_2} + \cdots + x_ny_n^{k_n} = b$ над произвольным конечным полем F_q, где $k_1, k_2, \ldots, k_n$ — произвольные ненулевые натуральные числа.

Для ненулевых натуральных чисел $k_1, k_2, \ldots, k_n$ рассмотрим уравнение

$$x_1y_1^{k_1} + x_2y_2^{k_2} + \cdots + x_ny_n^{k_n} = b \tag{1}$$

над конечным полем F_q. Множество решений уравнения (1) обозначим через N, а длину минимального линеаризированного покрытия множества N — через $L(n, k_1, k_2, \ldots, k_n)$. Ясно, что $N \subseteq F_{q^{2n}}$.

Теорема 1. *Для ненулевых натуральных чисел* $k_1, k_2, \ldots, k_n$

$$L(n, k_1, k_2, \ldots, k_n) = q^n - 1, \quad \textit{при } b \neq 0;$$
$$q^{n-1} + 1 - q^{-1} \leqslant L(n, k_1, k_2, \ldots, k_n) \leqslant q^n, \quad \textit{при } b = 0.$$

Доказательство. Верхняя оценка. Для всех ненулевых векторов $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in F_{q^n}$ построим следующую систему линейных уравнений:

$$\begin{cases} y_i = \alpha_i, & i = 1, 2, \ldots, n \\ \alpha_1^{k_1}x_1 + \alpha_2^{k_2}x_2 + \cdots + \alpha_n^{k_n}x_n = b, \end{cases} \tag{2}$$

а при $b = 0$ к системам типа (2) добавим линейную систему

$$y_i = 0, \qquad i = 1, 2, \ldots, n. \tag{3}$$

Очевидно, что множества решений построенных выше систем линейных уравнений являются смежными классами, лежат в N и попарно не пересекаются, следовательно, образуют линеаризированное непересекающееся покрытие множества N, которое назовем *каноническим покрытием*.

Ранги систем типа (2) и (3) равны соответственно $n+1$ и n, поэтому системы (2) и (3) имеют соответственно q^{n-1} и q^n решений в $F_{q^{2n}}$. Учитывая вышесказанное, получаем:

$$|N| = \begin{cases} q^{2n-1} - q^{n-1} & , \text{ при } b \neq 0 \\ q^{2n-1} - q^{n-1} + q^n & , \text{ при } b = 0 \end{cases}$$

и

$$L(n, k_1, k_2, \ldots, k_n) = \begin{cases} q^n - 1 & , \text{ при } b \neq 0 \\ q^n & , \text{ при } b = 0, \end{cases}$$

где $|N|$ — количество решений уравнения (1).

Нижняя оценка.

Определение 2. Если H является m-мерным смежным классом в F_{q^n}, тогда $(q^m \times n)$-матрица, в которой строки суть векторы из H, называется *матрицей смежного класса* H.

Для m-мерного смежного класса H в F_{q^n} рассмотрим его $(q^m \times n)$-матрицу [5]. Отождествим H с $(q^m \times n)$-матрицей. Очевидно, что всякая аффинная комбинация строк H также является строкой этой матрицы и любая перестановка строк матрицы H не изменяет свойства матрицы быть смежным классом. К линейной системе, которая определяет смежный класс H, добавим линейно независимое линейное уравнение $\ell(x_1, \ldots, x_n) = \alpha$, где $\alpha \in F_q$. Строки H, которые удовлетворяют новой удлиненной системе, образуют смежный класс размерности $m-1$ для каждого $\alpha \in F_q$. Следовательно, H можно представить как объединение в точности q попарно непересекающихся подсмежных классов размерности $m-1$, каждый из которых является сдвигом некоторого другого. Из вышесказанного также следует, что каждый столбец в H либо состоит из одних и тех же элементов поля F_q, либо содержит в точности q^{m-1} копий элемента α, для всех $\alpha \in F_q$. Столбец матрицы H, состоящий из одинаковых элементов, называется *постоянным*.

Условимся, что если $\mathcal{A} = (\alpha_{ij})$ — матрица размера $(m \times n)$ над полем F_q, то для любых натуральных чисел $k_1, k_2, \ldots, k_n$ через $\mathcal{A}^{k_1,k_2,\ldots,k_n}$ обозначим матрицу $\left(\alpha_{ij}^{k_j}\right)$ размера $(m \times n)$, т.е. $\mathcal{A}^{k_1,k_2,\ldots,k_n} = \left(\alpha_{ij}^{k_j}\right)$.

Лемма. *Пусть строки матрицы H образуют смежный класс m-мерного линейного подпространства L в F_{q^n}. Тогда для любых натуральных чисел $k_1, k_2, \ldots, k_n$:*

(i) если $H = L$, то $rank H^{k_1,k_2,\ldots,k_n} \geqslant m$;

(ii) если $H \neq L$, то $rank H^{k_1,k_2,\ldots,k_n} \geqslant m+1$.

Доказательство. Применим индукцию по m. Пусть $m = 0$. Тогда матрица H содержит в точности одну строку. Если эта строка нулевая (т.е. $H = L$), то единственная строка матрицы $H^{k_1,k_2,\ldots,k_n}$ также нулевая и $rankH^{k_1,k_2,\ldots,k_n} = rankH = 0$, а в противном случае (когда $H \neq L$) очевидно, что $rankH^{k_1,k_2,\ldots,k_n} = rankH = 1$.

Теперь предположим, что $m \geqslant 1$ и утверждение леммы справедливо для всех смежных классов, размерность которых меньше m. Поскольку $\dim H = m \geqslant 1$, то в $(q^m \times n)$-матрице смежного класса H существует непостоянный столбец. Без потери общности предположим, что это первый столбец. Тогда, если к линейной системе, которая определяет смежный класс H, добавим линейно независимое уравнение $x_1 = \alpha$, $\alpha \in F_q$, то все строки H, начинающиеся с α (и только они), удовлетворяют новой системе линейных уравнений и образуют $(m-1)$-мерный подсмежный класс H_α. Согласно индуктивному предположению для элемента $0 \in F_q$ имеем, что $rankH_0^{k_1,k_2,\ldots,k_n} \geqslant m-1$ (когда $H = L$) и $rankH_0^{k_1,k_2,\ldots,k_n} \geqslant m$ (когда $H \neq L$). Для каждого ненулевого элемента $\alpha \in F_q$ любая строка подматрицы $H_\alpha^{k_1,k_2,\ldots,k_n}$ линейно независима от строк подматрицы $H_0^{k_1,k_2,\ldots,k_n}$, следовательно, $rankH^{k_1,k_2,\ldots,k_n} \geqslant m$ (когда $H = L$) и $rankH^{k_1,k_2,\ldots,k_n} \geqslant m+1$ (когда $H \neq L$).

Рассмотрим теперь каноническое линеаризированное покрытие уравнения (1). Смежный класс, соответствующий вектору $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in F_{q^n}$ из канонического покрытия, обозначим через $N(\alpha)$. Тогда ясно, что $N = \cup N(\alpha)$. С другой стороны, если через $E(\alpha)$ обозначим множество решений линейной системы

$$\begin{cases} y_i = 0, & i = 1, 2, \ldots, n \\ \alpha_1^{k_1} x_1 + \alpha_2^{k_2} x_2 + \cdots + \alpha_n^{k_n} x_n = 0, \end{cases} \tag{4}$$

то очевидно, что $N(\alpha)$ является сдвигом линейного подпространства $E(\alpha)$.

Определение 3. Пусть $M \subseteq F_{q^n}$. Тогда смежный класс $H \subseteq M$ называется максимальным для множества M, если в M не существует смежного класса H^*, для которого $H \subset H^*$.

Пусть $H \subseteq N$, H является смежным классом линейного подпространства L в $F_{q^{2n}}$ и $\dim H = \dim L = m$. Так как $N = \cup N(\alpha)$, то H можно представить как объединение непустых смежных классов $H \cap N(\alpha)$, т.е. $H = \cup(H \cap N(\alpha))$. Учитывая вышесказанное, получаем, что каждый непустой смежный класс $H \cap N(\alpha)$ является сдвигом подпространства $L \cap E(\alpha)$.

Обозначим $S \equiv \{\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) |\ \alpha \in F_{q^n},\ H \cap N(\alpha) \neq \emptyset\}$. Рассмотрим $(q^m \times 2n)$-матрицу смежного класса H. Столбцы этой матрицы, которые соответствуют переменным $y_1, y_2, \ldots, y_n$, образуют подматрицу, строки которой в свою очередь образуют смежный класс и являются элементами множества S. Следовательно, S — смежный класс. Далее, пусть $\alpha =$

$(\alpha_1, \alpha_2, \ldots, \alpha_n) \in S$. В этом случае, добавляя к линейной системе, которая соответствует смежному классу H, всевозможные линейно независимые уравнения

$$\begin{cases} y_{i_1} = \alpha_{i_1} \\ \vdots \\ y_{i_r} = \alpha_{i_r}, \end{cases} \tag{5}$$

где $0 \leqslant r \leqslant n$ и $i_s \neq i_t$, когда $s \neq t$, имеем, что новой полученной линейной системе будут удовлетворять векторы смежного класса $H \cap N(\alpha)$ и только они. Ясно, что если в системе (5) элементы $\alpha_{i_1}, \ldots, \alpha_{i_r} \in F_q$ заменить элементами $\beta_{i_1}, \ldots, \beta_{i_r} \in F_q$, где $\beta = (\beta_1, \ldots, \beta_n) \in S$, то в результате получим смежный класс $H \cap N(\beta)$. Далее, если через E обозначим линейное подпространство решений системы

$$\begin{cases} y_{i_1} = 0 \\ \vdots \\ y_{i_r} = 0, \end{cases}$$

то очевидно, что каждый непустой $H \cap N(\alpha)$ является сдвигом подпространства $L \cap E$ и $\dim(H \cap N(\alpha)) = \dim(L \cap E) \equiv p$. С другой стороны, как отметили выше, $H \cap N(\alpha)$ — также сдвиг подпространства $L \cap E(\alpha)$. Следовательно, $L \cap E(\alpha) = L \cap E$ для всех $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in S$, и $L \cap E$ удовлетворяет следующей системе:

$$\begin{cases} y_i = 0, \qquad i = 1, 2, \ldots, n \\ \alpha_1^{k_1} x_1 + \alpha_2^{k_2} x_2 + \cdots + \alpha_n^{k_n} x_n = 0, \quad (\alpha_1, \alpha_2, \ldots, \alpha_n) \in S. \end{cases} \tag{6}$$

Так как H представляется как объединение непустых p-мерных смежных классов $H \cap N(\alpha)$ и $\dim H = m$, то $\dim S = m - p$. Продолжая, согласно лемме имеем, что для матрицы $S^{k_1, k_2, \ldots, k_n}$ (ее строками являются вектора $(\alpha_1^{k_1}, \alpha_2^{k_2}, \ldots, \alpha_n^{k_n})$, где $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in S$) $rank S^{k_1, k_2, \ldots, k_n} \geqslant m - p$, если она содержит нулевую строку, и $rank S^{k_1, k_2, \ldots, k_n} \geqslant m - p + 1$ в противном случае.

Теперь мы можем оценить размерность смежного класса H. Очевидно, что $\dim(L \cap E) \equiv p \leqslant 2n - rank(6) = 2n - \left(n + rank S^{k_1, k_2, \ldots, k_n}\right)$. Последовательно получаем, что $p \leqslant 2n - (n + m - p + 1)$, когда $b \neq 0$ (в этом случае $(0, 0, \ldots, 0) \notin S$), и $p \leqslant 2n - (n + m - p)$, когда $b = 0$. Наконец имеем:

$$m \leqslant n - 1 \quad \text{при } b \neq 0,$$

$$m \leqslant n \qquad \text{при } b = 0.$$

Отметим, что максимальные значения $n-1$ и n размерностей смежных классов достижимы на смежных классах канонического покрытия.

Используя оценку $L(n, k_1, k_2, \ldots, k_n) \geqslant \frac{|N|}{q^{\max \dim H}}$, где H — смежный класс в N, получаем:

$$L(n, k_1, k_2, \ldots, k_n) \geqslant q^n - 1 \qquad \text{при } b \neq 0;$$
$$L(n, k_1, k_2, \ldots, k_n) \geqslant q^{n-1} + 1 - q^{-1} \qquad \text{при } b = 0.$$

Теорема полностью доказана.

Ереванский государственный университет

Վ. Պ. Գաբրիելյան

Որոշակի տիպի բարձր կարգի հավասարումների գծայնացված ծածկույթները վերջավոր դաշտի վրա

Հոդվածում գնահատված է F_q վերջավոր դաշտում $x_1 y_1^{k_1} + x_2 y_2^{k_2} + \cdots + x_n y_n^{k_n} = b$ հավասարման լուծումների բազմության՝ գծային ենթատարածությունների հարակից դասերով կարճագույն ծածկույթի երկարությունը, որտեղ $k_1, k_2, \ldots, k_n$ ոչ զրոյական բնական թվեր են: Կամայական ոչ զրոյական $b \in F_q$ դարրի դեպքում կառուցված է կարճագույն ծածկույթ: Երբ $b = 0$, կառուցված ծածկույթի երկարությունը մոտ է նվազագույնին:

V. P. Gabrielyan

Linearized Coverings of One Type Equations of Higher Degree over Finite Fields

The complexity of minimal covering with cosets of linear subspaces is estimated for the set of solutions of the equation $x_1 y_1^{k_1} + x_2 y_2^{k_2} + \cdots + x_n y_n^{k_n} = b$ over an arbitrary finite field, where $k_1, k_2, \ldots, k_n$ are non-zero natural numbers. A covering with minimum complexity is constructed for any $b \in F_q$, $b \neq 0$. When $b = 0$ then the complexity of *constructed covering is almost minimum.*

Литература

1. *Лидл Р., Нидеррайтер Г.*. Конечные поля. В 2-х томах. М. Мир. 1988.

2. *Алексанян А. А.* - ДАН СССР. 1989. Т. 304. N4.

3. *Алексанян А. А.* Дизъюнктивные нормальные формы над линейными функциями. Теория и приложения. Ереван. Изд. ЕГУ. 1990.

4. *Габриелян В.* - Препринт НАН РА. 04-0603. Ереван. 2004.

5. *Alexanian A., Gabrielyan V.* - Algebra, Geometry & Their Applications, Seminar Proceedings. 2004. V. 3-4. Yerevan State University. P. 110-124.

6. *Алексанян А. А., Серобян Р. К.* - ДАН Армении. 1992. Т. 93. N1.

7. *Aleksanyan A., Papikian M.* - The Electronic Journal of Combinatorics. 2001. V. 8. R22. P. 1-9.

8. *Габриелян В.* - Препринт НАН РА. 04-0602. Ереван. 2004.