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

110 2010 № 3

ПРИКЛАДНАЯ МАТЕМАТИКА

УДК 512.62; 519.711

В. П. Габриелян

Кубическое диагональное уравнение над конечным полем характеристики 2

(Представлено академиком Ю.Г. Шукуряном 18/II 2010)

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

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 $\alpha \in F_{q^n}$, то 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 $\sum_{i=1}^{m} \lambda_i = 1$, сумма $\sum_{i=1}^{m} \lambda_i h_i$ (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 $H_1 \cup H_2 \cup \cdots \cup H_s = N$, тогда 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_q.

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 [6-9].

В настоящей работе задача минимального линеаризированного покрытия исследована для множества решений уравнения $x_1^3 + x_2^3 + \cdots - x_n^3 = b$ над конечным полем F_q характеристики 2. Когда $q = 2$, указанное уравнение, учитывая равенство $\alpha^3 = \alpha$ для всех $\alpha \in F_2$, принимает следующий вид: $x_1 + x_2 + \cdots - x_n = b$, для которого исследуемая задача имеет тривиальное решение.

Над конечным полем F_q, где $q \geq 4$ и $q \equiv 0 \ mod\ 2$, рассмотрим уравнение

$$x_1^3 + x_2^3 + \cdots + x_n^3 = b. \qquad (1)$$

Множество решений уравнения (1) обозначим через N, а длину минимального линеаризированного покрытия множества N – через $L(q,n)$. Ясно, что $N \subseteq F_q^n$.

Теорема 1. *Если $q = 4$, то длина $L(q,n)$ кратчайшего линеаризированного покрытия множества решений уравнения (1) удовлетворяет следующим неравенствам:*

$$2q^{n/2-1} + 1 \leq L(q,n) \leq 2q^{n/2} - 1, \text{ при } n \equiv 0 \ mod\ 2 \text{ и } b = 0,$$

$$L(q,n) = 2\left(q^{n/2} - 1\right), \text{ при } n \equiv 0 \ mod\ 2 \text{ и } b = 1,$$

$$2q^{(n-1)/2} - 1 \leq L(q,n) \leq 2q^{(n-1)/2+1} - 2q + 1, \text{ при } n \equiv 1 \ mod\ 2 \text{ и } b = 0,$$

$$2q^{(n-1)/2} + 1 \leq L(q,n) \leq 2q^{(n-1)/2+1} - 2q + 3, \text{ при } n \equiv 1 \ mod\ 2 \text{ и } b = 1.$$

Теорема 2. *Если $q > 4$ и $q \equiv 0 \ mod\ 2$, то длина $L(q,n)$ кратчайшего линеаризированного покрытия множества решений уравнения (1) удовлетворяет следующим неравенствам:*

- $$L(q,n) \le \begin{cases} (q^{n/2}-1)q+1, & \text{при } n \equiv 0 \bmod 2 \text{ и } b=0, \\ (q^{n/2}-1)q, & \text{при } n \equiv 0 \bmod 2 \text{ и } b \neq 0, \\ (q^{(n-1)/2}-1)q^2+3, & \text{при } n \equiv 1 \bmod 2. \end{cases}$$

- Когда $q \equiv 1 \bmod 3$, то

$$L(q,n) \ge \begin{cases} q^{n/2-1} - \dfrac{(q-1)(4^{n/2}-1)}{3q}+1, & \text{при } n \equiv 0 \bmod 2 \text{ и } b=0, \\ q^{n/2} - \dfrac{(q-1)(4^{n/2}-1)}{3}-1, & \text{при } n \equiv 0 \bmod 2 \text{ и } b \neq 0, \\ q^{(n-1)/2} - \dfrac{(q-1)(4^{(n-1)/2}-1)}{3}-1, & \text{при } n \equiv 1 \bmod 2 \text{ и } b=\beta^3, \beta \in F_q, \\ q^{(n-1)/2+1} - \dfrac{q(q-1)(4^{(n-1)/2}-1)}{3}-q, & \text{при } n \equiv 1 \bmod 2 \text{ и } b \neq \beta^3, \forall \beta \in F_q. \end{cases}$$

- Когда $q \not\equiv 1 \bmod 3$, то

$$L(q,n) \ge \begin{cases} q^{n/2-1}, & \text{при } n \equiv 0 \bmod 2 \text{ и } b=0, \\ q^{n/2}, & \text{при } n \equiv 0 \bmod 2 \text{ и } b \neq 0, \\ q^{(n-1)/2}, & \text{при } n \equiv 1 \bmod 2 \text{ и } b=\beta^3, \beta \in F_q, \\ q^{(n-1)/2+1}, & \text{при } n \equiv 1 \bmod 2 \text{ и } b \neq \beta^3, \forall \beta \in F_q. \end{cases}$$

Доказательство теорем. *Верхняя оценка теоремы 1.* Порядок ненулевых элементов поля F_q в мультипликативной группе $F_q^* \equiv F_q \setminus \{0\}$ равен 3, когда $q=4$, т. е. $\alpha^3 \in F_2 = \{0,1\}$ для всех $\alpha \in F_q$. Это значит, что если $b \neq 0$ и $b \neq 1$, то уравнение (1) в поле F_{q^n} не имеет решений. Следовательно, мы предполагаем, что $b=0$ или $b=1$. Пусть $n=2k+1$. Тогда уравнение (1) можно записать в виде

$$(x_1+x_2)(x_1^2+x_1x_2+x_2^2)+\cdots+(x_{2k-1}+x_{2k})(x_{2k-1}^2+x_{2k-1}x_{2k}+x_{2k}^2)+x_{2k+1}^3=b. \quad (2)$$

Для каждого ненулевого вектора $(\alpha_1,\ldots,\alpha_k) \in F_{q^k}$ и каждого $\beta \in F_q$ построим систему

$$\begin{cases} x_{2i-1}+x_{2i}=\alpha_i, \ i=1,2,\ldots,k, \\ x_{2k+1}=\beta, \\ \sum_{i=1}^{k}(\alpha_i x_{2i}^2+\alpha_i^2 x_{2i})=b+\beta^3+\sum_{i=1}^{k}\alpha_i^3. \end{cases} \quad (3)$$

Если $b=0$, то к системам (3) добавляем одну линейную систему вида

$$\begin{cases} x_{2i-1}+x_{2i}=0, \ i=1,2,\ldots,k, \\ x_{2k+1}=\beta. \end{cases} \quad (4)$$

Если же $b=1$, то добавляем ровно три системы вида (4). Последнее уравнение системы (3) можно переписать в следующем виде:

$$(\alpha_1^2 x_2 + \cdots + \alpha_k^2 x_{2k})^2 + \alpha_1^2 x_2 + \cdots + \alpha_k^2 x_{2k} = b + \beta^3 + \sum_{i=1}^k \alpha_i^3,$$

так как $q = 4$ и $\alpha^q = \alpha$, $(\alpha + \beta)^2 = \alpha^2 + \beta^2$ для всех $\alpha, \beta \in F_q$.

Многочлен $y^2 + y + a$, где $a \in F_2$, приводим в кольце $F_q[y]$ [1], и поскольку $b + \beta^3 + \sum_{i=1}^k \alpha_i^3 \in F_2$, то существуют элементы $\gamma_1, \gamma_2 \in F_q$ такие, что $\gamma_1 \neq \gamma_2$ и $\gamma_1^2 + \gamma_1 = \gamma_2^2 + \gamma_2 = b + \beta^3 + \sum_{i=1}^k \alpha_i^3$. Поэтому из каждой системы (3) мы строим линейные системы

$$\begin{cases} x_{2i-1} + x_{2i} = \alpha_i, i = 1,2,\ldots,k, \\ x_{2k+1} = \beta, \\ \sum_{i=1}^k \alpha_i^2 x_{2i} = \gamma_1 \end{cases} \quad \text{и} \quad \begin{cases} x_{2i-1} + x_{2i} = \alpha_i, i = 1,2,\ldots,k, \\ x_{2k+1} = \beta, \\ \sum_{i=1}^k \alpha_i^2 x_{2i} = \gamma_2. \end{cases} \tag{5}$$

Множества решений систем типа (4) и (5) попарно не пересекаются. Объединение этих множеств (смежных классов) в точности совпадает с множеством N, следовательно, является непересекающимся линеаризированным покрытием множества N, которое назовем *каноническим*. Очевидно, что длина канонического покрытия равна

$$\begin{cases} 2(q^k - 1)q + 1, & \text{при } n = 2k + 1 \text{ и } b = 0, \\ 2(q^k - 1)q + 3, & \text{при } n = 2k + 1 \text{ и } b = 1 \end{cases}$$

и является верхней оценкой для $L(q, n)$.

Нетрудно проверить, что

$$|N| = \begin{cases} 2(q^k - 1)qq^{k-1} + q^k, & \text{при } n = 2k + 1 \text{ и } b = 0, \\ 2(q^k - 1)qq^{k-1} + 3q^k, & \text{при } n = 2k + 1 \text{ и } b = 1. \end{cases}$$

Пусть теперь $n = 2k$. В этом случае линейные системы типа (4) и (5) (канонического покрытия) не содержат уравнения $x_{2k-1} = \beta$, а система типа (4) строится только тогда, когда $b = 0$. Поэтому длина канонического покрытия равна

$$\begin{cases} 2q^k - 1, & \text{при } n = 2k \text{ и } b = 0, \\ 2(q^k - 1), & \text{при } n = 2k \text{ и } b = 1, \end{cases}$$

а мощность множества N равна $\begin{cases} 2(q^k - 1)q^{k-1} + q^k, & \text{при } n = 2k \text{ и } b = 0, \\ 2(q^k - 1)q^{k-1}, & \text{при } n = 2k \text{ и } b = 1. \end{cases}$

Верхняя оценка теоремы 2. Предположим $n \equiv 0 \bmod 2$. В этом случае уравнение (1) можно написать следующим образом:

$$(x_1 + x_2)(x_1^2 + x_1x_2 + x_2^2) + \cdots + (x_{n-1} + x_n)(x_{n-1}^2 + x_{n-1}x_n + x_n^2) = b.$$

Для каждого ненулевого вектора $(\alpha_1, \ldots, \alpha_{n/2}) \in F_q{}^{n/2}$ составляем систему

$$\begin{cases} x_{2i-1} + x_{2i} = \alpha_i, \ i = 1,2, \ldots, n/2, \\ \sum_{i=1}^{n/2} (\alpha_i x_{2i}^2 + \alpha_i^2 x_{2i}) = b + \sum_{i=1}^{n/2} \alpha_i^3 . \end{cases} \quad (6)$$

Когда $b = 0$, к системам (6) добавляем систему

$$x_{2i-1} + x_{2i} = 0, \ i = 1,2, \ldots, n/2. \quad (7)$$

Для последнего уравнения системы (6) справедлива также следующая запись:

$$\left(\alpha_1^{q/2} x_2 + \cdots + \alpha_{n/2}^{q/2} x_n\right)^2 + \alpha_1^2 x_2 + \cdots + \alpha_{n/2}^2 x_n = b + \sum_{i=1}^{n/2} \alpha_i^3.$$

Тогда для произвольного элемента $\gamma \in F_q$ рассмотрим линейную систему

$$\begin{cases} x_{2i-1} + x_{2i} = \alpha_i, \ i = 1,2, \ldots, n/2, \\ \sum_{i=1}^{n/2} \alpha_i^{q/2} x_{2i} = \gamma, \\ \sum_{i=1}^{n/2} \alpha_i^2 x_{2i} = b + \gamma^2 + \sum_{i=1}^{n/2} \alpha_i^3. \end{cases} \quad (8)$$

Ненулевые векторы $\left(\alpha_1^{q/2}, \ldots, \alpha_{n/2}^{q/2}\right)$ и $\left(\alpha_1^2, \ldots, \alpha_{n/2}^2\right)$ линейно зависимы тогда и только тогда, когда ненулевые координаты вектора $(\alpha_1, \ldots, \alpha_{n/2})$ равны, при условии НОД$(q-1, q/2-2) = 1$. Если же НОД$(q-1, q/2-2) = 3$, то эти векторы линейно зависимы в том и только том случае, когда для любых различных ненулевых координат α_i и α_j вектора $(\alpha_1, \ldots, \alpha_{n/2})$ порядок элемента $\alpha_i \alpha_j^{-1}$ в группе $F_q^* \equiv F_q \setminus \{0\}$ равен 3.

Количество ненулевых векторов $(\alpha_1, \ldots, \alpha_{n/2}) \in F_{q^{n/2}}$, для которых векторы $\left(\alpha_1^{q/2}, \ldots, \alpha_{n/2}^{q/2}\right)$ и $\left(\alpha_1^2, \ldots, \alpha_{n/2}^2\right)$ линейно зависимы, равно $\sum_{i=1}^{n/2} C_{n/2}^i (q-1) = (q-1)\left(2^{n/2} - 1\right)$ при НОД$(q-1, q/2-2) = 1$ и $\sum_{i=1}^{n/2} C_{n/2}^i (q-1)3^{i-1} = (q-1)\left(4^{n/2} - 1\right)/3$ при НОД$(q-1, q/2-2) = 3$.

Система (8), когда векторы $\left(\alpha_1^{q/2}, \ldots, \alpha_{n/2}^{q/2}\right)$ и $\left(\alpha_1^2, \ldots, \alpha_{n/2}^2\right)$ линейно зависимы, совместна тогда и только тогда, когда многочлен $x^2 + \alpha_j^{2-q/2} x + b + \sum_{i=1}^{n/2} \alpha_i^3 \in F_q[x]$ приводим над полем F_q для всех элементов $\alpha_j \neq 0$, $1 \leq j \leq n/2$.

Смежные классы, соответствующие системам (7) и (8), не пересекаются и образуют непересекающееся линеаризированное покрытие множества решений уравнения (1) в поле F_{q^n}. Это покрытие называется *каноническим*.

Очевидно, что длина канонического покрытия не больше, чем величина

$$\begin{cases}(q^{n/2}-1)q+1, & \text{при } n \equiv 0 \bmod 2 \text{ и } b = 0,\\ (q^{n/2}-1)q, & \text{при } n \equiv 0 \bmod 2 \text{ и } b \neq 0.\end{cases}$$

Последнее является верхней оценкой сложности $L(q,n)$ – минимального линеаризированного покрытия множества решений уравнения (1) при $n \equiv 0 \bmod 2$.

Как в случае $n \equiv 0 \bmod 2$, так и при $n \equiv 1 \bmod 2$ аналогично строится каноническое линеаризированное покрытие множества решений уравнения (1) (единственное отличие в том, что системы (6), (7) и (8) содержат одно добавочное уравнение), длина которого не превосходит величины $(q^{(n-1)/2}-1)q^2+3$, так что

$$L(q,n) \le (q^{(n-1)/2}-1)q^2+3 \text{ при } n \equiv 1 \bmod 2.$$

Далее, если $q \not\equiv 1 \bmod 3$, то для каждого элемента $\alpha \in F_q$ существует единственный элемент $\beta \in F_q$ такой, что $\beta^3 = \alpha$. Следовательно, когда $q \not\equiv 1 \bmod 3$, то мощность множества N – всех решений уравнения (1) равна $|N| = q^{n-1}$.

Пусть теперь $q \equiv 1 \bmod 3$. Нетрудно проверить, что

$$|N| \ge \begin{cases}\left[q^{n/2} - \dfrac{(q-1)(4^{n/2}-1)}{3} - 1\right]q^{n/2-1} + q^{n/2}, & \text{при } n \equiv 0 \bmod 2 \text{ и } b = 0,\\ \left[q^{n/2} - \dfrac{(q-1)(4^{n/2}-1)}{3} - 1\right]q^{n/2-1}, & \text{при } n \equiv 0 \bmod 2 \text{ и } b \neq 0,\\ \left[q^{(n-1)/2} - \dfrac{(q-1)(4^{(n-1)/2}-1)}{3} - 1\right]q^{(n-1)/2}, & \text{при } n \equiv 1 \bmod 2.\end{cases}$$

Нижние оценки теорем.

Лемма 1. *Пусть H является смежным классом в множестве N. Тогда*

- *если* $q = 4$, *то* $\dim H \le \begin{cases} n/2, & \text{когда } n \equiv 0 \bmod 2 \text{ и } b = 0,\\ n/2-1, & \text{когда } n \equiv 0 \bmod 2 \text{ и } b = 1,\\ (n-1)/2, & \text{когда } n \equiv 1 \bmod 2 \text{ и } b = 0,\\ (n-1)/2, & \text{когда } n \equiv 1 \bmod 2 \text{ и } b = 1; \end{cases}$
- *если* $q > 4$, *то* $\dim H \le \begin{cases} n/2, & \text{когда } n \equiv 0 \bmod 2 \text{ и } b = 0,\\ n/2-1, & \text{когда } n \equiv 0 \bmod 2 \text{ и } b \neq 0,\\ (n-1)/2, & \text{когда } n \equiv 1 \bmod 2 \text{ и } b = \beta^3, \beta \in F_q,\\ (n-1)/2-1, & \text{когда } n \equiv 1 \bmod 2 \text{ и } b \neq \beta^3, \forall \beta \in F_q. \end{cases}$

Отметим, что максимальные значения размерностей смежных классов в множестве N достижимы на смежных классах канонического покрытия. Имея максимально возможную размерность смежного класса H в множестве N, с

помощью формулы $L(q,n) \geq \frac{|N|}{q^{\max \dim H}}$ получаем нижние оценки, отмеченные в теоремах.

Ереванский государственный университет

В. П. Габриелян

Кубическое диагональное уравнение над конечным полем характеристики 2

Для уравнения $x_1^3 + x_2^3 + \cdots + x_n^3 = b$ над конечным полем F_q характеристики 2 получена оценка минимального покрытия смежными классами линейных подпространств.

Վ. Պ. Գաբրիելյան

Խորանարդային անկյունագծային հավասարումը 2 բնութագրիչի վերջավոր դաշտում

Գնահատված է 2 բնութագրիչի F_q վերջավոր դաշտի վրա $x_1^3 + x_2^3 + \cdots + x_n^3 = b$ հավասարման լուծումների բազմության գծային ենթատարածությունների հարակից դասերով կարճագույն ծածկույթի երկարությունը:

V. P. Gabrielyan

Cubical Diagonal Equation over Finite Fields of Characteristic 2

The complexity of the minimal covering with cosets of linear subspaces is estimated for the set of solutions of the equation $x_1^3 + x_2^3 + \cdots + x_n^3 = b$ over finite fields of characteristic 2.

Литература

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х томах. М. Мир. 1988.
2. *Алексанян А. А.* – ДАН СССР. 1989. Т. 304. №4.

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. №1. С. 6-10.
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.
9. *Габриелян В. П.* - ДНАН РА. 2006. Т. 106. №2. С. 101-107.