

УДК 519.7+512.62

А. А. Алексанян, Р. К. Серобян

Покрытия, связанные с квадратичными над конечным полем уравнениями

(Представлено чл.-корр. АН Армении Ю. Г. Шукурьяном 3/IV 1991)

Настоящая работа посвящена исследованию следующей задачи о покрытии. Пусть в конечном поле из q элементов F_q задано квадратичное уравнение с n переменными. Задача состоит в определении наименьшего количества систем линейных над F_q уравнений, объединение множеств решений которых в точности совпадает с множеством решений исходного квадратичного уравнения. Иными словами, требуется оценить длину кратчайшего покрытия множества решений заданного квадратичного уравнения системой смежных классов по линейным над F_q подпространствам в F_q^n — n -мерном линейном над F_q пространстве. Для $q = 2$ эта задача решена одним из авторов в (1, 2). Ниже исследован случай произвольного $q > 2$.

Авторы следуют терминологии и обозначениям книги (3). Пусть F_q^n — n -мерное линейное пространство над F_q .

Определение. Подмножество N пространства F_q^n называется смежным классом, если N является сдвигом некоторого линейного подпространства $L \subseteq F_q^n$, т. е. найдется $a \in F_q^n$ такое, что $N = a + L$.

Иными словами, N содержит любую аффинную (или выпуклую) комбинацию своих элементов. Размерность $\langle \dim N \rangle$ определяется как размерность соответствующего линейного подпространства L .

Очевидно, что всякий смежный класс является множеством решений некоторой системы линейных уравнений. Верно и обратное.

Определим η -квадратичный характер поля F_q для $q \equiv 1 \pmod{2}$.

$$\eta(a) = \begin{cases} 0, & \text{если } a = 0 \\ 1, & \text{если } a \text{ является квадратом} \\ -1, & \text{если } a \text{ не является квадратом.} \end{cases}$$

Для четного q примем соглашение: $\eta \equiv 0$.

Определим функцию v на F_q формулой:

$$v(x) = \begin{cases} -1, & \text{если } x \neq 0 \\ q-1, & \text{если } x = 0. \end{cases}$$

Пусть $|A|$ обозначает мощность множества A , а $Tr_{F_q}(a)$ — функцию следа.

Через $\begin{bmatrix} n \\ m \end{bmatrix}_q$ обозначим коэффициент Гаусса — количество m -мерных линейных подпространств в F_q^n . Известно, что (см. (4)):

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-m+1} - 1)}{(q^m - 1)(q^{m-1} - 1) \dots (q - 1)}.$$

Покрывтия для канонических уравнений. Пусть задано квадратичное над F_q уравнение

$$\sum_{i,j=1}^n a_{ij} x_i x_j = b, \quad (1)$$

где левая часть — суть невырожденная квадратичная форма, а $N \subseteq F_q^n$ — множество решений этого уравнения. Далее приводится метод построения покрытия множества N системой смежных классов. Ввиду инвариантности длины покрытия (количества смежных классов) относительно действия полной аффинной группы преобразований, в дальнейшем рассматриваются квадратичные уравнения (1) с квадратичной формой, приведенной к каноническому виду (см. например (3)). Таким образом, рассмотрения подлежат следующие уравнения:

- I. $x_1 x_2 + x_3 x_4 + \dots + x_{n-1} x_n = b$, где $n \equiv 0 \pmod{2}$, q — произвольное;
- II. $x_1 x_2 + x_3 x_4 + \dots + x_{n-2} x_{n-1} + a x_n^2 = b$, где $0 \neq a \in F_q$, $n \equiv 1 \pmod{2}$, q — произвольное;
- III. $x_1 x_2 + x_3 x_4 + \dots + x_{n-3} x_{n-2} + x_{n-1}^2 + a x_n^2 = b$, где $0 \neq a \in F_q$, $n \equiv 0 \pmod{2}$, $q \equiv 1 \pmod{2}$, $\chi(-a) = -1$;
- IV. $x_1 x_2 + x_3 x_4 + \dots + x_{n-1} x_n + x_{n-1}^2 + a x_n^2 = b$, где $0 \neq a \in F_q$, $n \equiv 0 \pmod{2}$, $q \equiv 0 \pmod{2}$, $Tr_{F_q}(a) = 1$.

Далее перечисляются покрытия множества решений канонических уравнений. Смежные классы задаются системами линейных уравнений.

Случай I. Пусть $k \leftarrow n/2$. Для каждого ненулевого вектора $(a_1, \dots, a_k) \in F_q^k$ составим систему

$$\begin{cases} x_{2i} = a_i, & i = 1, \dots, k \\ \sum_{i=1}^k a_i x_{2i-1} = b. \end{cases} \quad (2)$$

При $b \neq 0$ требуемое покрытие состоит из всех смежных классов вида (2), а при $b = 0$ к ним добавляется система $x_{2i} = 0$, $i = 1, \dots, k$.

Длина покрытия L равна $\begin{cases} q^k - 1, & \text{при } b \neq 0 \\ q^k, & \text{при } b = 0. \end{cases}$

Случай II. Пусть $k = (n-1)/2$, $0 \neq (a_1, \dots, a_k) \in F_q^k$ и $\beta \in F_q$. Покрытие состоит из всех систем вида

$$\begin{cases} x_{2i} = a_i, & i = 1, \dots, k \\ x_{2k+1} = \beta, \\ \sum_{i=1}^k a_i x_{2i-1} = b - a\beta^2 \end{cases} \quad (3)$$

и

$$\begin{cases} x_{2i} = 0, & i = 1, \dots, k \\ x_{2k+1} = \beta, \end{cases} \quad \text{где } \beta^2 = ba^{-1}, \quad (4)$$

причем системы вида (4) добавляются при $q \equiv 0 \pmod{2}$ или при $q \equiv 1 \pmod{2}$ и $\eta(ba^{-1}) \neq -1$.

Длина покрытия L равна $q^{k+1} - q + \eta(ba^{-1}) + 1$.

Случай III. Пусть $k = n/2 - 1$, $0 \neq (a_1, \dots, a_k) \in F_q^k$ и $\beta, \gamma \in F_q$. Покрытие состоит из всех систем вида:

$$\begin{cases} x_{2i} = a_i, & i = 1, \dots, k \\ x_{2k+1} = \beta, \\ x_{2k+2} = \gamma, \\ \sum_{i=1}^k a_i x_{2i-1} = b - \beta^2 - a\gamma^2 \end{cases} \quad (5)$$

и

$$\begin{cases} x_{2i} = 0, & i = 1, \dots, k \\ x_{2k+1} = \beta, \\ x_{2k+2} = \gamma, \end{cases} \quad (6)$$

где для β и γ выполнено $\beta^2 + a\gamma^2 = b$. Длина покрытия равна $L = q^{k+2} - q^2 + q - v(b)$.

Случай IV. Пусть $k = n/2$, $0 \neq (a_1, \dots, a_{k-1}) \in F_q^{k-1}$ и $\beta, \gamma \in F_q$. Покрытие состоит из всех систем вида:

$$\begin{cases} x_{2i} = a_i, & i = 1, \dots, k-1 \\ x_{2k-1} = \beta, \\ x_{2k} = \gamma, \\ \sum_{i=1}^{k-1} a_i x_{2i-1} = b + \beta\gamma + \beta^2 + a\gamma^2 \end{cases} \quad (7)$$

и

$$\begin{cases} x_{2i} = 0, & i = 1, \dots, k-1 \\ x_{2k-1} = \beta, \\ x_{2k} = \gamma, \end{cases} \quad (8)$$

где для β и γ выполнено $\beta\gamma + \beta' + a\gamma^2 = b$. Длина покрытия равна $L = q^{n+1} - q^2 + q - v(b)$.

Основная теорема. Пусть $L(n, q)$ — наименьшая длина покрытия множества N решений квадратичного уравнения, а $m(n, q)$ — наибольшая размерность смежного класса, содержащегося в N . Тогда

в случае I:

$$m(n, q) = \begin{cases} n/2 - 1, & \text{при } b \neq 0 \\ n/2, & \text{при } b = 0, \end{cases}$$

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

в случае II:

$$m(n, q) = (n-1)/2 + \eta(1-\eta)/2,$$

$q^{\eta(\eta-1)/2} (q^{(n-1)/2} + \eta) \leq L(n, q) \leq q^{(n+1)/2} - q + \eta + 1$, где $\eta \equiv \eta(ba^{-1})$,
в частности, при $q \equiv 1 \pmod{2}$ и $\eta = -1$ имеем:

$$L(n, q) = q^{(n+1)/2} - q;$$

в случаях III и IV

$$m(n, q) = n/2 - 1 \text{ и } q^{n/2} - v(b) \leq L(n, q) \leq q^{n/2+1} - q^2 + q - v(b).$$

Верхние оценки для $L(n, q)$ получаются покрытиями из предыдущего пункта. Следует отметить, что количество смежных классов размерности $m(n, q)$, целиком содержащихся в N , может быть точно вычислено. Например, в случае I получается формула:

для $b \neq 0$

$$\sum_{p=0}^{k-1} \left[\begin{matrix} k \\ p+1 \end{matrix} \right]_q (q^{p+1} - 1) q^{\frac{(k-p)(k-p-1)}{2}} \quad \text{при } q > 2 \text{ и}$$

$$\sum_{p=0}^{k-1} \left[\begin{matrix} k \\ p+1 \end{matrix} \right]_q (q^{p+1} - 1) q^{\frac{(k-p-1)(k-p+2)}{2}} \quad \text{при } q = 2;$$

для $b = 0$

$$\sum_{p=0}^k \left[\begin{matrix} k \\ p \end{matrix} \right]_q q^{\frac{(k-p)(k-p-1)}{2}} \quad \text{при } q > 2 \text{ и}$$

$$1 + \sum_{p=0}^{k-1} \left[\begin{matrix} k \\ p \end{matrix} \right]_q q^{\frac{(k-p-1)(k-p+2)}{2}} \quad \text{при } q = 2. \text{ Здесь } k = n/2.$$

Во всех случаях I—IV получаются величины порядка $q^{(1+o(1))n/2}$.

Греванский государственный университет

Վերջավոր դաշտում բառակուսային հավասարումների ունե
կապված ծածկույթներ

Դիցուք F_q վերջավոր դաշտում տրված է n փոփոխականից կախված
 $\sum_{i,j=1}^n a_{ij} x_i x_j = b$ հավասարումը: Աշխատանքում ցուցանված է $L(n, q)$
մեծությունը—գծային համակարգերի նվազագույն քանակը, որոնց լուծում-
ների միավորումը համընկնում է բառակուսային հավասարման լուծումների
բազմության հետ:

ЛИТЕРАТУРА — ԿՐԿԱՆՈՒՄՆԵՐ

1 А. А. Алексанян Дизъюнктивные нормальные формы над линейными функциями. Изд. ЕГУ. 1990. 2 А. А. Алексанян ДАН СССР, т. 304, № 4, с. 781—784 (1989). 3 Р. Лидл, Г. Нидеррайтер, Конечные поля (в 2-х томах), Мир, М., 1988. 4 М. Адзнер Комбинаторная теория, Мир, М., 1982.