

УДК 519.8

МАТЕМАТИКА

А. К. Айдинян

Некоторые свойства кодов МДР

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 22/II 1983)

Известно, что для линейного кода над любым конечным полем выполняется неравенство $d \leq n - k + 1$, где n — длина кодового слова, k — число информационных символов, d — расстояние кода. Коды, у которых $d = n - k + 1$, называются разделимыми кодами с максимальным расстоянием или кодами МДР. Эти коды имеют систематический кодер, т. е. кодовые слова могут быть разделены на информационные и проверочные символы ^(1,2). Иногда эти коды также называют оптимальными. Основным из известных кодов МДР является код Рида — Соломона (РС) над полем $GF(q)$ ^(1,2). Из кода РС $[n = q - 1, k, n - k + 1]$ можно получить расширенный код РС $[n + 1, k, n - k + 2]$, который также является кодом МДР.

Задача построения кодов МДР наибольшей длины связана с рядом трудных комбинаторных задач, представляющих самостоятельный интерес, а также с вопросами построения конечных проективных геометрий.

Одна из основных задач теории кодов МДР формулируется следующим образом: для заданных k и q найти наибольшее значение n , для которого существует $[n, k, n - k + 1]$ -код над полем $GF(q)$. Обозначим это наибольшее значение через $n(k, q)$.

В работах ⁽³⁻⁵⁾ показано, что при $k \leq 5$ либо $q \leq 11$ имеет место соотношение

$$n(k, q) = \begin{cases} q + 1 & \text{для } 2 \leq k \leq q \\ k + 1 & \text{для } k > q, \end{cases}$$

кроме случая

$$n(3, q = 2^m) = q + 2.$$

Однако в общем случае эта задача остается нерешенной.

Целью настоящей работы является установление некоторых свойств кодов МДР, а также решение вышеприведенной задачи для некоторых новых частных случаев. При этом утверждается выводимость нескольких известных результатов из основных утверждений приводимой работы.

Хорошо известно ^(1,2), что $[n, k, d]$ -код является кодом МДР тогда и только тогда, когда любые k столбцов порождающей матрицы этого кода линейно-независимы.

Пусть задан $[n, k, d]$ -код МДР над полем $GF(q)$, порождающая матрица которого имеет вид $G=[I|A]$, где I —единичная матрица размерности $k \times k$, а A —матрица размерности $k \times (n-k)$ такая, что первый столбец и первая строка ее состоят из единичных элементов поля.

В книге Н. Дж. Слоэна и Ф. Дж. Мак-Вильямс доказывается Теорема ⁽¹⁾. Все квадратные подматрицы матрицы A невырождены.

Используя вышеприведенные обозначения, из этой теоремы можно получить

Следствие 1. Никакая строка (столбец) матрицы A , за исключением первой (первого), не содержит одинаковых элементов поля.

Приведем также вытекающую из этой теоремы оценку длины кода МДР над полем $GF(q)$.

Следствие 2. При $k \geq 2$ имеет место соотношение

$$n(k, q) \leq q + k - 1.$$

В этих же обозначениях верно

Следствие 3. При $k > q$ имеет место соотношение

$$n(k, q) = k + 1.$$

В ⁽¹⁾ доказывается следующий факт: пусть задан $[n, k, n-k+1]$ -код МДР. Тогда двойственный ему код также является кодом МДР с параметрами $[n, n-k, k+1]$. При помощи этого можно доказать нижеследующее утверждение:

Теорема 1. $n(k, q) = n(n(k, q) - k, q)$.

Из теоремы 1 и следствий 1, 2 можно получить утверждение о максимальных длинах кодов МДР над полем $GF(q)$ с двумя и с $q-1$ информационными символами:

Следствие 1.1. $n(2, q) = n(q-1, q) = q+1$ при нечетном q . Если же q есть степень двойки, то

$$n(3, q) = n(q-1; q) = q+2.$$

Теорема 2. Пусть t —такое целое число, что $1 \leq t \leq q-1$. Тогда для любого $k > t$ имеет место соотношение

$$n(t, q) = q+1 \Leftrightarrow n(k, q) \leq q+k-t+1.$$

Эта теорема позволяет улучшить границу для длины кодового слова. Очевидно, из теоремы 2 вытекает

Следствие 2.1. $n(k, q) \leq q+k-4$ для $4 < k < q$.

Приведенные в списке литературы работы содержат результаты по вычислению максимальной длины кодов МДР для конкретных числовых значений k при любом основании кода. Сформулируем результат, дающий точную оценку максимальной длины кодового слова для k таких, что $2k-1$ есть степень простого числа.

Теорема 3. При $2k-1=q$ имеет место равенство

$$n(k, q) = q+1.$$

Следствие 3.1. Если $q \leq 13$, то $n(k, q) = q + 1$ кроме случая $q = 4$ и 8.

Вычислительный центр
Академии наук Армянской ССР и
Ереванского государственного
университета

2. Կ. ԱՅԴԻՆՅԱՆ

ՄՀԱ-կոդերի որոշ հատկություններ

Գծային $[n, k, d]$ կոդերը (n -ը կոդային բառի երկարությունն է, k -ն ինֆորմացիոն նիշերի քանակը, d -ն կոդի մինիմալ հեմինգյան հեռավորությունը) բավարարում են $d \leq n - k + 1$ պայմանին: Այն կոդերը, որտեղ բավարարվում է $d = n - k + 1$ հավասարությունը, կոչվում են ՄՀԱ (մաքսիմալ հեռացված անջատելի), կամ Օպտիմալ կոդեր: Մինչ այժմ ՄՀԱ կոդերում չլուծված խնդիրներից մեկը հետևյալն է. տրված k -ի և q -ի համար գտնել ամենամեծ n -ը, որի համար գոյություն ունի $[n, k, n - k + 1]$ -կոդ $GF(q)$ դաշտի վրա:

Այս խնդիրը մինչ այժմ լուծված է $k \leq 5$ կամ $q \leq 11$ դեպքերում:

Հոգվածում բերվում են ՄՀԱ կոդերի որոշ հատկություններ և լուծվում վերոհիշյալ խնդիրը որոշ նոր մասնավոր դեպքերում:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

¹ Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, Теория кодов, исправляющих ошибки, Связь, М., 1979. ² У. Питерсон, Э. Уэлдон, Коды, исправляющие ошибки, Мир, М., 1976. ³ B. Segre, Lectures on Modern Geometry (Edizioni Cremonese). Rome, 1961. ⁴ L. R. A. Casse, Lincei-Ren. Sc. fis. mat. nat., 46 (1969). ⁵ C. Maneri, R. Silverman, J. Comb. Theory. 11A (1971).