УДК 621.391

Л. Х. Фам

Московский физико-технический институт (национальный исследовательский университет)

Алгоритм вычисления граничного ранга двоичной матрицы

Рассматриваются методы исправления ошибки в системе параллельных каналов, в которых действуют помехи. Предложено пространство квадратных матриц над конечным полем. Граничным рангом двоичной матрицы называется минимальное число строк и столбцов, в которых содержатся все ненулевые элементы матрицы. В данной работе речь пойдет о алгоритме вычисления граничного ранга матрицы.

Ключевые слова: граничный ранг, решетчатые конструкции, конечное поле, двоичные матрицы, кодовое расстояние, вектор сумм столбцов, вектор сумм строк.

L. H. Pham

Moscow Institute of Physics and Technology

Algorithm for computing term rank of binary matrices

We consider methods for correcting errors in the system of parallel channels with interference. The space of square matrices over a finite field is suggested. The term rank of the binary matrix A is defined to be a minimum number of rows and columns that contain all nonzero elements of the matrix. In this paper, we discuss the algorithm for computing the term rank of the matrix. Key words: term rank, lattice construction, finite field, binary matrices, distance of codes, row sum vector, column sum vector.

Key words: term rank, lattice construction, finite field, binary matrices, distance of codes, row sum vector, column sum vector.

1. Модель решетчатых ошибок

Рассмотрим процесс передачи дискретных сообщений от источника информации к получателю, который осуществляется по нескольким параллельным каналам. Каждый из каналов использует двоичные сигналы для передачи. Пусть количество каналов равно n_f, длительность передачи по каждому из каналов равна n_t. Тогда входные и выходные сигналы можно отождествить с матрицами (A_{ij}), $i = 1, ..., n_f; j = 1, ..., n_t$, где i означает номер канала, j означает номер временного интервала. Значения элементов равны 1 или 0.

В процессе передачи сообщений возникают различные специфические ошибки.

Когда действуют замирания сигнала, импульсные и узкополосные помехи, ошибки могут возникнуть в нескольких столбцах и нескольких строках матрицы. В таком случае ошибки называются решетчатыим.

Пусть задано множество матриц $(v_1, v_2, ..., v_M)$ на входе канала. Пусть передается матрица v_i, а на выходе получена матрица $y = v_i + e$, где e – матрица ошибок.

Пример. Матрица

$$e = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

есть ошибка решетчатой конфигурации с граничным рангом 3, так как искаженные символы сосредоточены в третьей строке и первом и четвертом столбцах.

Желательно правильно восстанавливать сообщение, если граничный ранг матрицы ошибок e не превосходит заранее заданной величины t. Нужен алгоритм вычисления граничного ранга двоичной матрицы.

2. Пространство квадратных двоичных матриц над конечным полем

Пусть $GF(2)$ – конечное поле, состоящее из $q = 2$ элементов. Пусть $GF(2^n)$ – расширение поля $GF(2)$ степени n, n – натуральное число. Поле $GF(2)$ будем назвать базовым полем, поле $GF(2^n)$ – расширенным полем.

Линейное пространство матриц A над полем $GF(2)$ с размерами $n \times n$ обозначается $GF(2)^{n\times n}$.

$$A = \begin{bmatrix} v_{0,0} & v_{0,1} & \dots & v_{0,n-1} \\ v_{1,0} & v_{1,1} & \dots & v_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n-1,0} & v_{n-1,1} & \dots & v_{n-1,n-1} \end{bmatrix}, \; v_{i,j} \in GF(2).$$

Ранг матрицы Rk(A) определяется как максимальное число линейно независимых над $GF(2)$ строк (или столбцов). Граничный ранг $\rho(A)$ двоичной матрицы определяется как минимальное число линий (строк и столбцов), в которых содержатся все ненулевые элементы матрицы [1+2].

Функция $\rho(A)$ удовлетворяет всем аксиомам нормы [1]:

1) $\rho(A) = 0 \leftrightarrow A = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix}$.

2) $\rho(A) > 0 \leftrightarrow A \neq 0$.

3) $|\rho(A) - \rho(B)| \leq \rho(A + B) \leq \rho(A) + \rho(B)$.

3. Гранично-ранговое расстояние. Примеры

Пример. Граничный ранг матрицы

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

равен 1, граничный ранг матрицы

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

равен 2, граничный ранг матрицы

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

равен 3.

Расстоянием между двумя матрицами A и B одинаковых размеров называется граничный ранг их разности:

$$d(A, B) = \rho(A - B). \tag{1}$$

Гранично-ранговое расстояние имеет все свойства обычного расстояния:

1) $d(A,B) = 0 \leftrightarrow A = B$.

2) $d(A,C) + d(C,B) \geq d(A,B)$ – неравенство треугольника.

3) $d(B,A) = d(A,B)$ – свойство симметричности.

Первое и третье свойства получены из отмеченного выше соотношения

$$d(A,B) = \rho(A-B) = \rho(B-A).$$

Аналогично

$$d(A,C) + d(C,B) =$$
$$= \rho(A-C) + \rho(C-B) \geq \rho((A-C)+(C-B)) =$$
$$= \rho(A-B) = d(A-B).$$

Таким образом, второе свойство расстояния доказано.

Гранично-ранговый код $\mathcal{V} \in GF(2)^{n_f \times n_t}$ – это любое подмножество пространства прямоугольных матриц с гранично-ранговой нормой.

Кодовое расстояние равно, по определению, минимальному из попарных расстояний между элементами кода [3]:

$$d = \min_{i \neq j} \rho(v_i - v_j).$$

Очевидно, для любого кода

$$d \leq D = \min(n_f, n_t).$$

4. Алгоритм вычисления граничного ранга двоичной матрицы

Этот алгоритм был предложен автором в 2018 г. Основная идея алгоритма заключается в том, что на основе сравнения между векторами сумм столбцов и векторами сумм строк можно вычислить максимальное значение элементов. Цель определения максимального значения элементов – управление процессом вычисления граничного ранга, то есть граничным рангом является минимальное число строк и столбцов, в которых содержатся все единицы матрицы.

Вход: A $= (A_{ij})$ – двоичная матрица с размером $m \times n$

Выход: $norm = \rho(A)$ – граничный ранг двоичной матрицы.

1) $y \leftarrow 0$.

2) Вычисление векторов $colum = (colum[1], colum[2], \ldots, colum[n])$ и $line = (line[1], line[2], \ldots, line[m])$. $colum[j]$ – это сумма элементов j-го столбца матрицы, $line[i]$ – это сумма элементов i-й строки матрицы:

$$colum[j] = \sum_{i=1}^{m} A_{ij}\, j = 1, \ldots, n,$$

$$line[i] = \sum_{j=1}^{n} A_{ij}\, i = 1, \ldots, m.$$

3) Вычисление $\max\_col\_var$ – максимальное значение элементов в векторе $colum$, $\max\_col\_index$ – индекс максимального значения элементов в векторе $colum$.

4) $\max\_line\_var$ – максимальное значение элементов вектора $line$, $\max\_line\_index$ – индекс максимального значения элементов в векторе $line$.

5) **While** $\max\_line\_var > 0$ **do**

6) $y \leftarrow y + 1$.

7) **If** $\max\_col\_var > \max\_line\_var$ **then** $A_{i,\max\_col\_index} \leftarrow 0$, где $i = 1 \ldots m$.

8) **Else** $A_{\max\_line\_index,j} \leftarrow 0$, где $j = 1 \ldots n$.

9) Вычисление векторов $colum$ и $line$.

10) Вычисление $\max\_col\_var$, $\max\_col\_index$.

11) Вычисление $\max\_line\_var$, $\max\_line\_index$.

12) **end while**.

13) $norm = \rho(A)$ – минимальное значение из трёх значений y, m и n.

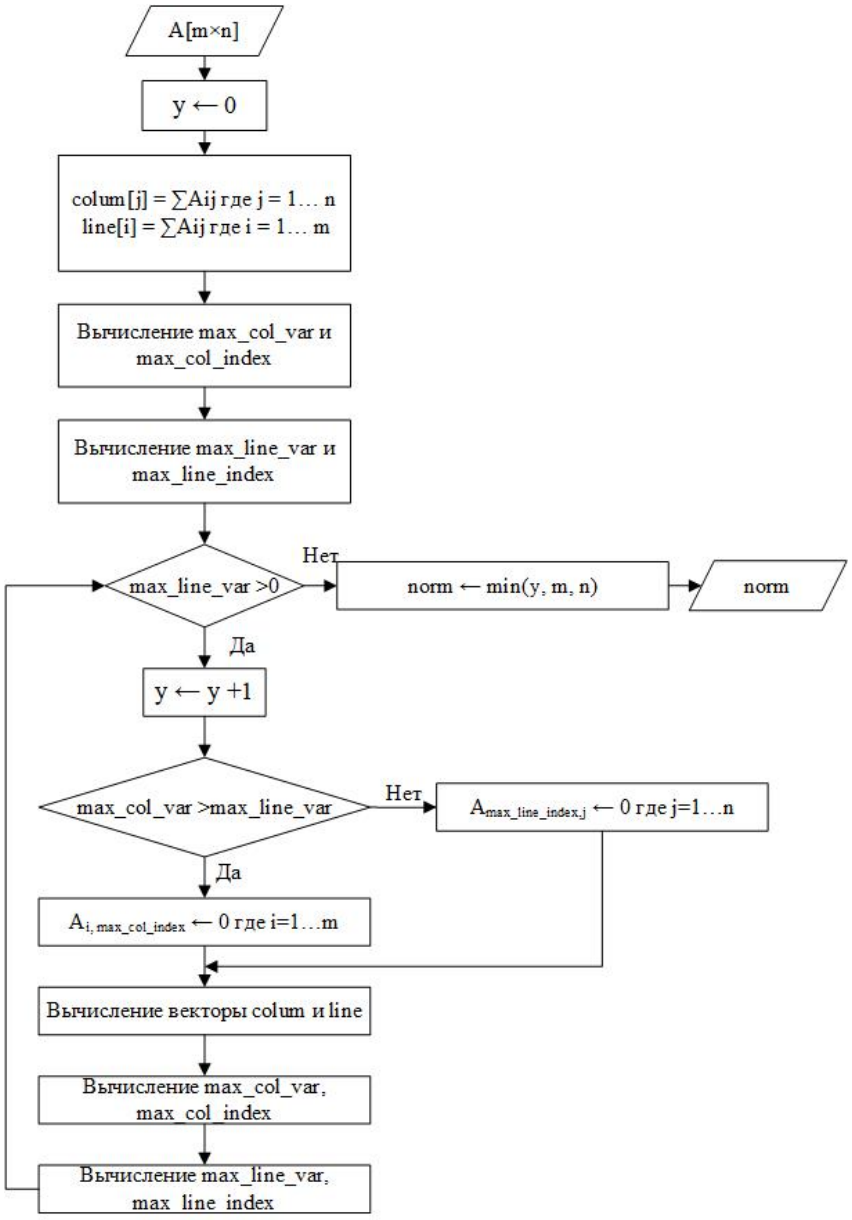

Рис. 1. Блок-схема алгоритма вычисления граничного ранга двоичной матрицы

Доказательство. Пусть A – двоичная матрица размером $m \times n$. Пусть y – количество разложенных матриц из A. Разложение матрицы A осуществляется в следующем порядке:

$\mathrm{A} = \mathrm{A}_1 + B_1$, где A_1 – двоичная матрица, у которой только одна строка (или столбец), в которой содержатся максимальное количество единиц из всех строк (или столбцов) матрицы A.

Пример

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = A_1 + B_1.$$

Аналогично для B_1: $B_1 = \mathrm{A}_2 + B_2$ и так далее.

В общем случае процесс разложения матрицы имеет следующий вид:

$$A = A_1 + B_1,$$

$$B_1 = A_2 + B_2,$$

$$\dots$$

$$B_{y-1} = A_y.$$

Таким образом, на конечном этапе получим $A = A_1 + A_2 + ... + \mathrm{A}_y$.

С учетом третьей аксиомы получаем

$$\rho(A) \le \rho(A_1) + \rho(A_2) + \dots + \rho(A_y) = 1 + 1 + \dots + 1 = y.$$

Матрицы A_i не зависят друг от друга. Поэтому если значение y больше, чем m или n, то граничный ранг матрицы A равен $\min(m, n)$. В противном случае, как легко увидеть, граничный ранг матрицы A равен y.

5. Пример. Код $(3, 1, 3)$. Дуальный код $(3, 2, 2)$

Пусть задан код (p, k, d), где $p = 3$ – размер квадратной матрицы, $k = p - 2 = 1$ – число информационных векторов (x, y, z), $d = 3$ – кодовое гранично-ранговое расстояние. Матрицей кода (3,1,3) является бинарная матрица размера 3×3. Код (3,1,3) имеет вид

$$\begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix}.$$

Пусть задано целое число элементов множества $L = 2^3 = 8$.

$$G_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, G_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, G_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

$$G_4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, G_5 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, G_6 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, G_7 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Легко заметить, что $\rho(G_0) = 0$ и $\rho(G_i) = 3$, где $i = 1 \dots 7$.

Рассматривается разность двух матриц $|G_i - G_j| \in G$. Поэтому гранично-ранговое расстояние равно 3.

Опишем данный код через G' матрицу дуального кода (3,2,2) из матрицы G. В результате получим

$$G = \begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix} \backsim \begin{pmatrix} a(x) & b(y) & c(z) \\ d(z) & g(x) & h(y) \\ b(y) + h(y) & c(z) + d(z) & a(x) + g(x) \end{pmatrix} \backsim$$

$$\backsim G' = \begin{pmatrix} a & b & c \\ d & g & h \\ b + h & c + d & a + g \end{pmatrix}.$$

Дуальный код $(3, 2, 2)$ имеет гранично-ранговое расстояние 2.

6. Код $(p, p-2, 3)$. Пример. Код $(4, 2, 3)$

Код $(p, p-2, 3)$ характеризуется параметрами (p, k, d), где p – размер квадратной матрицы, $k = p-2$ – число информационных векторов $(x_i, y_i, z_i, \ldots, k_i, e_i)$, где $i = 0, \ldots, p-1$, $d = p-k+1 = 3$ – кодовое гранично-ранговое расстояние.

Для построения кода $(p, p-2, 3)$ сначала определить сопровождающую матрицу F_n. Пусть $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ – примитивный многочлен над полем $GF(2)$.Тогда сопровождающая матрица F_n имеет вид

$$F_n = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ldots & 0 & 1 & \\ f_0 & f_1 & \ldots & \ldots & \ldots & f_{n-1} \end{pmatrix}.$$

Порождающая матрица кода имеет общую формулу:

$$G = \begin{pmatrix} x_0 + x_1 + \cdots + x_{n-3} \\ x_0 F_n + x_1 F_n^2 + \cdots + x_{n-3} F_n^{n-2} \\ \vdots \\ x_0 F_n^{n-1} + x_1 F_n^{2(n-1)} + \cdots + x_{n-3} F_n^{(n-1)(n-2)} \end{pmatrix}.$$

Здесь выберем сопровождающую матрицу F_n так, чтобы $\rho(G) \geq 3$. В этом случае код $(p, p-2, 3)$ является линейным. Поэтому гранично-ранговое расстояние $d(G_i - G_j) \geq 3$.

Код $(4, 2, 3)$ характеризуется параметрами (p, k, d), где $p = 4$ – размер квадратной матрицы, $k = p-2 = 2$ – число информационных векторов (x, y), $d = p-k+1 = 3$ – кодовое гранично-ранговое расстояние. Символы векторов представляют собой элементы поля $GF(2)$. Пусть G – (4×4)-матрица, которая состоит из информационных векторов. Матрица G имеет две информационные диагонали и две проверочные диагонали.

Код задается следующей порождающей матрицей:

$$G = \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \\ \mathbf{x}F_4 + \mathbf{y}F_4^2 \\ \mathbf{x}F_4^2 + \mathbf{y}F_4^4 \end{bmatrix},$$

где $\mathbf{x} = (x_0\ x_1\ x_2\ x_3), \mathbf{y} = (y_0\ y_1\ y_2\ y_3)$ – информационные вектор-строки длины 4. Здесь выберем сопровождающую матрицу F_4 так, чтобы $\rho(G) \geq 3$. А матрица F_4 – сопровождающая матрица многочлена $x^4 + x + 1$:

$$F_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix},$$

$$\mathbf{x}F_4 + \mathbf{y}F_4^2 = (x_0\ x_1\ x_2\ x_3) \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} + (y_0\ y_1\ y_2\ y_3) \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} =$$

$$= (x_3 + y_2\ x_0 + x_3 + y_2 + y_3\ x_1 + y_0 + y_3\ x_2 + y_1),$$

$$\mathbf{x}F_4^2 + \mathbf{y}F_4^4 = (x_0\ x_1\ x_2\ x_3) \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} + (y_0\ y_1\ y_2\ y_3) \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} =$$

$$= (x_2 + y_0 + y_3 \; x_2 + x_3 + y_0 + y_1 + y_3 \; x_0 + x_3 + y_1 + y_2 \; x_1 + y_2 + y_3).$$

Таким образом, получена общая формула:

$$G = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ x_3 + y_2 & x_0 + x_3 + y_2 + y_3 & x_1 + y_0 + y_3 & x_2 + y_1 \\ x_2 + y_0 + y_3 & x_2 + x_3 + y_0 + y_1 + y_3 & x_0 + x_3 + y_1 + y_2 & x_1 + y_2 + y_3 \end{bmatrix}.$$

Пусть задано целое число матриц множества $L = 2^8 = 256$. С помощью компьютера результат получен (табл. 1).

Таблица 1

Результат вычисления граничных рангов всех кодовых матриц G

Граничный ранг $\rho(\mathbf{G})$	0	1	2	3	4
Количество матриц	1	0	0	101	154

Из таблицы результата получено гранично-ранговое расстояние $d(G_i - G_j) \geq 3$.

7. Заключение

Представленный в статье алгоритм является новым. Алгоритм вычисления граничного ранга является основным результатом данной статьи, и с помощью этого алгоритма решалась задача построения кодов с расстоянием 3. Результат построения данных кодов представляет собой основу для решения последующих задач оптимальных кодов, исправляющих одиночные гранично-ранговые ошибки.

Автор выражает благодарность профессору Э. М. Габидулину и д.т.н Н. И. Пилипчук за замечания, которые способствовали улучшению статьи.

Литература

1. *Габидулин Э.М.* Лекции по алгебраическому кодированию. Москва : Наука, 2015. С. 62.
2. *Paterson M.B., Stinson D.R., Wei R.* Combinatorial batch codes // Adv. Math. Communications, 3. 2009. P. 13–17.
3. *Габидулин Э.М.* Оптимальные коды, исправляющие ошибки решетчатой конфигурации // Пробл. передачи информ. 1985. Т. 21, вып. 2. С. 103–108.

References

1. *Gabidulin E.M.* Lectures on algebraic coding. Moscow : Nauka, 2015. P. 62. (in Russian).
2. *Paterson M.B., Stinson D.R., Wei R.* Combinatorial batch codes. Adv. Math. Communications, 3. 2009. P. 13–17.
3. *Gabidulin E.M.* Optimal codes that correct lattice configuration errors. Prob. transfer infor. 1985. N 21. V. 2. P. 103–108. (in Russian).

Поступила в редакцию 10.02.2019