А К А Д Е М И Я Н А У К С С С Р
СИБИРСКОЕ ОТДЕЛЕНИЕ
А В Т О М Е Т Р И Я

№ 5 1968

УДК 621.317.7+681.142.621

В. В. ЕФИМЕНКО, Б. В. КАРПЮК, Ю. А. СТУКАЛИН

(Новосибирск)

ОБ ОДНОМ АЛГОРИТМЕ СИНТЕЗА КВАЗИЭКВИДИСТАНТНЫХ ДВОИЧНЫХ КОДОВ*

Подобно квазиэквидистантным двоично-десятичным кодам с заданным расстоянием $d>1$, двоичные квазиэквидистантные коды обеспечивают минимальную вероятность появления ошибок считывания в цифраторах перемещения. Поэтому для цифровой измерительной техники несомненный интерес представляет задача синтеза таких кодов. Ниже приводится одно из возможных решений этой задачи.

Постановка задачи. Поставим в соответствие N числам натурального ряда $0, 1, 2, \ldots, N-1$ наборы двоичных символов $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_n$ так, что $m = \sum_{j=1}^{n} \gamma_j 2^{n-j}$, где $m \in \{\overline{0, N-1}\}$. Код, построенный по такому правилу, называется нормальным кодом $X_н$ [2]. Все другие возможные двоичные коды можно представить в виде таблиц подстановок. Наша задача найти подстановку

$$\begin{pmatrix} x_1, & x_2, & \ldots, & x_N \\ y_1, & y_2, & \ldots, & y_N \end{pmatrix} = \begin{pmatrix} X_н \\ X_н A \end{pmatrix} = \begin{pmatrix} X_н \\ Y \end{pmatrix}, \tag{1}$$

для которой $\| y_i \oplus y_{i\,н} \| = d$ при любом $i=1, 2, \ldots, N$ и $1 \leqslant d < n$.

Когда $d=1$, последовательность Y есть код Грея. При решении этой задачи отдельно рассмотрим два случая: 1) d — нечетное число; 2) d — четное число.

1-й случай. Следуя [2], кодовые символы (наборы двоичных переменных) будем рассматривать как векторы n-мерного пространства Хэмминга, над которыми можно производить линейные преобразования вида $y=xA$, где x — исходный вектор; y — вектор, полученный из x преобразованием, заданным матрицей A.

При помощи матрицы A можно составить подстановку

$$\begin{pmatrix} X_н \\ X_н A \end{pmatrix} = \begin{pmatrix} x_1, & x_2, & \ldots, & x_N \\ x_1 A, & x_2 A, & \ldots, & x_N A \end{pmatrix}, \tag{1a}$$

и, следовательно, задача в этом случае сводится к нахождению такой матрицы A ($\det \neq 0$), чтобы $\| x_i A \oplus x_{i+1} A \| = d$, где d — нечетное число.

* Мы пользуемся терминологией и обозначениями, принятыми в [1] и [2].

Легко видеть [2], что сумма $x_i \oplus x_{i+1}$ может принимать n различных значений: 00 . . . 01, 00 . . . 11, . . . , 11 . . . 11— и существует n различных значений сумм $x_i A \oplus x_{i+1} A = e_s$ $(s = 1, 2, \ldots, n)$. Учитывая, что $x_i A \oplus x_{i+1} A = (x_i \oplus x_{i+1}) A$, можно записать следующую систему уравнений:

$$
\begin{aligned}
(00\ldots01)\,A &= e_1 = \gamma_{11}\gamma_{12}\ldots\gamma_{1n};\\
(00\ldots11)\,A &= e_2 = \gamma_{21}\gamma_{22}\ldots\gamma_{2n},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
(11\ldots11)\,A &= e_n = \gamma_{n1}\gamma_{n2}\ldots\gamma_{nn},
\end{aligned}
\tag{2}
$$

где

$$
A = \begin{Vmatrix} a_{11} & a_{12} \ldots a_{1n} \\ a_{21} & a_{22} \ldots a_{2n} \\ \ldots & \ldots \\ a_{n1} & a_{n2} \ldots a_{nn} \end{Vmatrix}.
$$

Записывая (2) через элементы матрицы A, получаем систему из $n \times n$ уравнений:

$$
\begin{aligned}
&a_{11}\cdot 0 \oplus a_{21}\cdot 0 \oplus \ldots \oplus a_{n-1,1}\cdot 0 \oplus a_{n1}\cdot 1 = \gamma_{11};\\
&a_{12}\cdot 0 \oplus a_{22}\cdot 0 \oplus \ldots \oplus a_{n-1,2}\cdot 1 \oplus a_{n2}\cdot 1 = \gamma_{12};\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a_{1n}\cdot 1 \oplus a_{2n}\cdot 1 \oplus \ldots \oplus a_{n-1,n}\cdot 1 \oplus a_{nn}\cdot 1 = \gamma_{nn}.
\end{aligned}
\tag{3}
$$

Из (3) непосредственно находим:

$$
\begin{aligned}
&a_{n1} = \gamma_{11},\ a_{n-1,1} = a_{n1} \oplus \gamma_{21},\ a_{n-2,1} = a_{n1} \oplus a_{n-1,1} \oplus \gamma_{31};\\
&a_{n2} = \gamma_{12},\ a_{n-1,2} = a_{n2} \oplus \gamma_{22},\ a_{n-2,2} = a_{n2} \oplus a_{n-1,2} \oplus \gamma_{32};\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a_{nn} = \gamma_{1n},\ a_{n-1,n} = a_{nn} \oplus \gamma_{2n},\ a_{n-2,n} = a_{nn} \oplus a_{n-1,n} \oplus \gamma_{3n};\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a_{11} = a_{n1} \oplus a_{n-1,1} \oplus \ldots \oplus a_{21} \oplus \gamma_{n1};\\
&a_{12} = a_{n2} \oplus a_{n-1,2} \oplus \ldots \oplus a_{22} \oplus \gamma_{n2};\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a_{1n} = a_{nn} \oplus a_{n-1,n} \oplus \ldots \oplus a_{2n} \oplus \gamma_{nn}.
\end{aligned}
\tag{4}
$$

Таким образом, по известным числам e_s из (4) легко определяются элементы матрицы A. В качестве векторов (двоичных чисел) e_s должны быть взяты линейно независимые векторы (чтобы выполнялось условие $\det A \neq 0$), причем такие, для которых $\|e_s\| = d$. Для рассматриваемого случая (d — число нечетное) можно рекомендовать следующие алгоритмы нахождения n линейно независимых векторов e_s.

1. Выбирается вектор, у которого первые d координат равны 1, а все остальные — нулю:

$$
\overbrace{1\,1\,1\ldots1}^{d}\ \ \overbrace{00\ldots00}^{n-d}.
$$

Остальные $n-1$ векторы находятся по схеме

$$
\left.\begin{array}{l}
0111\ldots1100\ldots0\\
0011\ldots1110\ldots0\\
0001\ldots1111\ldots0\\
\ldots\ldots\ldots\ldots\\
0000\ldots0011\ldots1
\end{array}\right\}\ \text{Циклический сдвиг исходного вектора вправо } n-d \text{ раз.}
$$

$$
\begin{array}{c}
d-1\\
\text{перестановка значения } (d+1)\text{-й координаты исходного вектора последовательно со всеми значениями координат, начиная со второй и кончая } d\text{-й координатой.}
\end{array}
\left\{\begin{array}{l}
1011\ldots1100\ldots0\\
1101\ldots1100\ldots0\\
1110\ldots1100\ldots0\\
\ldots\ldots\ldots\ldots\\
1111\ldots1010\ldots0
\end{array}\right.
$$

Покажем, что полученные n векторов e_s линейно независимы. Для этого перепишем эти векторы в порядке

$$
\begin{array}{l}
\overbrace{011\ldots110}^{d}\ \ldots0\\
d\left\{\begin{array}{l}
101\ldots110\ \ldots0\\
1101\ldots110\ldots0\\
\ldots\ldots\ldots\ldots\\
111\ldots1010\ldots0\\
111\ldots1100\ldots0
\end{array}\right.\\
\left.\begin{array}{l}
001\ \ldots1110\ \ldots0\\
0001\ldots11110\ldots0\\
\ldots\ldots\ldots\ldots\\
000\ \ldots01111\ldots1
\end{array}\right\}\ n-d-1
\end{array}
$$

Используя теорему Лапласа [3], можно найти, что

$$
\begin{vmatrix}
011 & \ldots & 110\ldots0\\
101 & \ldots & 110\ldots0\\
1101 & \ldots & 110\ldots0\\
\ldots & \ldots & \ldots\\
111 & \ldots & 1010\ldots0\\
111 & \ldots & 1100\ldots0\\
001 & \ldots & 11110\ldots0\\
0001 & \ldots & 11110\ldots0\\
\ldots & \ldots & \ldots\\
000 & \ldots & 011\ldots1
\end{vmatrix}
\bmod 2 =
\overbrace{\begin{vmatrix}
0 & & & 1\\
 & 0 & & \\
 & & \ddots & \\
 & & & 0\\
1 & & & 0\ \ 0
\end{vmatrix}}^{d}
\cdot
\begin{vmatrix}
1 & & & 0\\
 & 1 & & \\
 & & \ddots & \\
B & & & 1\ \ 1
\end{vmatrix}
\bmod 2 = 1
$$

Следовательно, указанная система векторов линейно независима.

2. Для случая, когда d и n — числа взаимно простые, можно предложить более простой алгоритм получения n независимых векторов e_s, для которых $\| e_s \| = d$, а именно: выбирается, как и прежде, в качестве исходного вектор, у которого первые d координат равны 1, а остальные $(n - d)$ координат равны 0, и путем циклического сдвига вправо (влево) получаются все другие $(n - 1)$ векторы:

$$\begin{array}{c} \overbrace{}^{d} \\ 11\ \ldots\ 1100 \ldots 00 \\ 01\ \ldots\ 1110 \ldots 00 \\ 001 \ldots 11110 \ldots 00 \\ \ldots\ldots\ldots\ldots \\ 111 \ldots\ 1000 \ldots 01 \end{array} \tag{6}$$

Докажем, что система векторов (6) при взаимно простых d и n линейно независима. Для этого покажем, что определитель матрицы, составленной из координат системы векторов (6) при числах n и d взаимно простых, отличен от нуля. Итак, определитель наш имеет вид

$$D = \begin{vmatrix} 11 \ldots\ 1100 \ldots 00 \\ 01 \ldots\ 1110 \ldots 00 \\ 001 \ldots 11110 \ldots 00 \\ \ldots\ldots\ldots\ldots \\ 11 \ldots\ \ \ 10 \ldots 01 \end{vmatrix} \tag{7}$$

Определитель (7) относится к типу определителей, которые называются циркулянтами [4]. Они (при арифметических операциях сложения и умножения) вычисляются по формуле

$$D = f(\varepsilon_0) f(\varepsilon_1) \ldots f(\varepsilon_{n-1}),$$

где $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ — корни n-й степени из 1, а $f(x)$ в нашем случае равно $\sum_{n=1}^{d-1} x^n$. Совершая очевидные алгебраические преобразования и используя свойства корня n-й степени из 1 [3], получаем $D = (-1)^d d$ или 0, если n и d не взаимно простые числа. Но так как нахождение определителя (в общем случае) связано лишь с операциями умножения и сложения, то поэтому [5] при нечетном d

$$D \overset{\text{mod } 2}{=} \begin{cases} 1, \text{ если } n \text{ и } d \text{ взаимно простые;} \\ 0, \text{ если } n \text{ и } d \text{ не взаимно простые,} \end{cases}$$

что и требовалось доказать.

Из изложенного выше для нечетного d вытекает следующий алгоритм синтеза квазиэквидистантных двоичных кодов с заданным расстоянием:

1. Исходя из количества N кодовых символов нормального двоичного кода $X_н$, выбираем значность кода $n = \log_2 N$.

$$e_1 = \gamma_{11}\,\gamma_{12}\,\gamma_{13}\,\ldots\,\gamma_{1n};$$

$$e_2 = \gamma_{21}\,\gamma_{22}\,\gamma_{23}\,\ldots\,\gamma_{2n};$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$e_n = \gamma_{n1}\,\gamma_{n2}\,\gamma_{n3}\,\ldots\,\gamma_{nn}.$$

3. По соотношениям (4) находим элементы матрицы A.

4. Умножая векторы x_i на матрицу A, находим векторы y_i, являющиеся кодовыми символами квазиэквидистантного двоичного кода с заданным нечетным значением d.

Пример. Имеется нормальный двоичный код: $N=32$. Найти квазиэквидистантный двоичный код с $d=3$ при $N=32$.

1. Определяем, что $n=\log_2 32=5$.

2. Выбираем в качестве e_s $(s = 1, 2, \ldots, 5)$ числа:

$$e_1=11100; \quad e_2=01110; \quad e_3=00111; \quad e_4=10011; \quad e_5=11001.$$

При данных значениях n и d для получения e_s мы воспользовались лишь циклическим сдвигом, поскольку числа 5 и 3 взаимно простые. Если $n=6$, $d=3$, то этим способом векторы e_s получить нельзя, а необходимо сочетать циклический сдвиг с перестановками, согласно способу 2, например:

$$e_1=111000; \quad e_2=011100; \quad e_3=001110; \quad e_4=000111; \quad e_5=101100;$$
$$e_6=110100.$$

3. По (4) находим, что

$$A = \begin{Vmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{Vmatrix}$$

4. Умножая векторы x_i $(i=0, 1, 2, \ldots, N-1)$ нормального кода $X_н$ на A, получаем код Y:

i	$X_н$	Y
0	00000	00000
1	00001	11100
2	00010	10010
3	00011	01110
4	00100	01001
.	...	...
28	11100	10111
29	11101	01011
30	11110	00101
31	11111	11001

2-й случай: d — четное число.

В данном случае не удается построить матрицу A, для которой $\det A \neq 0$, так как при $d=2k$ $(k=1, 2, \ldots)$ в n-мерном пространстве Хэмминга нельзя найти n линейно независимых векторов e_s, для которых $\| e_s \| = d$.

В самом деле, рассматривая матрицу, построенную из n любых векторов e_s n-мерного пространства Хэмминга, для которых $\| e_s \| = 2k$ $(k=1, 2, \ldots)$, убеждаемся, что ее определитель равен 0, так как сумма по mod 2 всех столбцов этой матрицы есть нулевой столбец. Это означает, что любые n векторов с четной нормой в указанном пространстве являются линейно зависимыми. Следовательно, непосредственно найти код с четным значением d, используя линейное преобразование двоичного нормального кода $X_н$, невозможно.

Известно, что для того чтобы $\| x \oplus y \| = 2k$, значения $\| x \|$ и $\| y \|$ одновременно должны быть четными либо нечетными числами. Это означает, что если кодовые символы $X_н$ суть векторы n-мерного пространства, то кодовые символы кода Y с четным значением d суть векторы пространства Хэмминга размерности $n+1$ или большей. Поэтому можно предложить следующий алгоритм синтеза квазиэквидистантных двоичных кодов с заданным четным значением d:

1) построить квазиэквидистантный двоичный код с нечетным значением $d'=d-1$;

2) увеличить на единицу размерность векторов, использующихся в качестве кодовых символов, полученного кода с расстоянием d', приписывая справа или слева значение новой координаты вектора (0 или 1) таким образом, чтобы, кроме возрастания размерности пространства, значение $\| y_i \oplus y_{i+1} \|$ также возросло* на 1.

Пример 2. Имеется нормальный двоичный код: $N=32$. Найти квазиэквидистантный двоичный код с $d=4$ при $N=32$.

1. Находим код Y' с $d'=d-1=3$ (см. пример 1).

2. Увеличиваем размерность векторов y_i кода Y', приписывая 0 или 1, и получаем искомый код Y с $d=4$ при $N=32$:

0	00000	000000
1	11101	111001
2	10010	100100
3	01110	011101
4	01001	010010
.	. . .	. . .
28	10111	101110
29	01011	010111
30	00101	001010
31	11001	110011

В заключение следует отметить, что для обратного преобразования квазиэквидистантного кода с нечетным d в нормальный двоичный код

* Для выполнения этого условия необходимо приписывать 0 и 1 так, чтобы в итоге значения $\| y_i \|$ для всех i были либо все четными, либо все нечетными числами.

необходимо найти матрицу, обратную A, и умножить векторы (кодовые комбинации) y_i на эту матрицу. Для четного d сначала необходимо от кода Y перейти к коду Y', а далее действовать как в случае кода с нечетным d.

ЛИТЕРАТУРА

1. В. В. Ефименко, Б. В. Карпюк. Квазиэквидистантные двоично-десятичные коды для цифраторов перемещения.— Автоматический контроль и методы электрических измерений. Тезисы докладов и сообщений. Новосибирск, 1966.
2. Н. Я. Матюхин. Линейные преобризования двоичных кодов.— Автоматика и телемеханика, 1958, № 8.
3. А. Г. Курош. Курс высшей алгебры. М., Физматгиз, 1959.
4. А. П. Мишина, И. В. Проскуряков. Высшая алгебра. СМБ. М., Физматгиз, 1962.
5. Ш. X. Михелович. Теория чисел. М., «Высшая школа», 1962.

Поступила в редакцию
25 января 1968 г.