ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXIV 1982 2

УДК 519.1

МАТЕМАТИКА

Л. Г. Хачатрян

Таблицы, обладающие свойством «окна»

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 14/IX 1981)

Работа посвящена построению таблиц, обладающих свойством „окна", которые являются обобщением последовательностей максимальной длины и циклов де Брейна на плоскости. Дается новый метод построения таких таблиц. С помощью предложенного метода, в частности, получен класс таблиц, являющийся улучшением результата работы ([1]). Для получения новых классов таблиц в работе рассматривается также проблема разбиения последовательностей максимальной длины и циклов де Брейна.

1. Пусть $A=a_1a_1\ldots a_{t^m-2}$ последовательность длины t^m-1 из элементов алфавита $T=\{0, 1, \ldots, t-1\}$. A называется последовательностью максимальной длины (п. м. д.), если среди m-наборов $(a_0, \ldots, a_{m-1})$, $(a_1\ldots a_m), \ldots (a_{t^m-2}a_0\ldots a_{m-2})$ встречаются всевозможные ненулевые комбинации над алфавитом T. Аналогичную последовательность длины t^m с нулевым набором обозначим через (п. м. д.) 0. (П. м. д.) 0 называется также полным циклом или последовательностью де Брейна. (П, м. д.) над конечными полями хорошо изучены. Они существуют над любым конечными полем $GF(q)$, относительно любого натурального числа m и строятся следующим образом. Рассмотрим рекуррентные соотношения или разностные уравнения над полем $GF(q)$

$$\sum_{j=0}^{m} h_j a_{i+j}=0 \qquad (1)$$

или

$$a_{i+m}=-\sum_{j=0}^{m-1} h_j a_{i+j}, \qquad (2)$$

где $h_0\neq 0$, $h_m=1$, каждое $h_i\in GF(q)$ и $\exists a_i\neq 0$ $(0\leqslant i<m)$. Тогда решение этих уравнений описывается следующей теоремой.

Теорема 1 ([2]). *Пусть* $h(x)=\sum_{j=0}^{m} h_j x^j$, $h_0\neq 0$, $h_m=1$ *и* n *— наименьшее натуральное число, для которого многочлен* x^n-1 *делится на* $h(x)$. *Тогда решение рекуррентных соотношений* (1) *периодично с периодом* n. *Если* $h(x)$ *— примитивный полином степени* m, *то период последовательности равен* q^m-1.

Естественным обобщением (п. м. д.) и (п. м. д.) 0 является построение таблиц, обладающих свойством „окна".

Определение 1 [1]. Пусть D таблица размера $a\times b$, где $a\cdot b=t^{mk}-1$, из элементов алфавита $T=(0, 1, \ldots, t-1)$. Таблица D обладает свойством $m\times k$ „окна", если при перемещении прямоугольника $m\times k$ по таблице D в клетках прямоугольника встречаются всевозможные ненулевые $t^{mk}-1$ комбинации над алфавитом T.

Определение 1*. Таблица D размера $a\times b$, где $a\cdot b=t^{mk}$, обладает свойством $m\times k$ „окна" над алфавитом T, если при перемещении прямоугольника $m\times k$ по таблице D в клетках прямоугольника встречаются всевозможные t^{mk} комбинации над алфавитом T.

Заметим, что в отличие от (п. м. д.) и (п. м. д.) 0 таблицы со свойством „окна" с нулевым набором и без нулевого набора существенно различаются, хотя бы размерами.

2. Пусть $A=a_0a_1\ldots a_{q^k-2}$ (п. м. д.) из элементов поля $GF(q)$. Через $A_i(i=0, 1, \ldots, q^k-2)$ обозначим последовательность, которая получается из A циклическим сдвигом на i позиций. Через A_y обозначим нулевой вектор длины q^k-1. Рассмотрим m-наборы из множества $L=\{F(0, 1, \ldots, q^k-2), y\}$, где $F(0, 1, \ldots, q^k-2)$ кольцо целых чисел по модулю q^k-1, а „y" элемент, для которого по определению $y+\delta=y$ для всех $\delta\in L$.

Определение 2. Скажем, что набор $(i_1, \ldots, i_m)$ эквивалентен набору $(j_1, \ldots, j_m)$, если существует $\delta\in L$ такой, что

$$(i_1, \ldots, i_m)=(j_1+\delta, \ldots, j_m+\delta).$$

Пусть M все m-наборы над множеством L, у которых есть хотя бы один элемент из кольца F и первый из них O. Легко убедиться, что мощность M

$$|M|=C_m^0(q^k-1)^{m-1}+C_m^1\cdot(q^k-1)^{m-2}+\ldots+C_m^{m-1})^0=\frac{q^{km}-1}{q^k-1}$$

и любая пара из M неэквивалентна.

Рассмотрим ленты $B_i\left(i=1, \ldots, \dfrac{q^{km}-1}{q^k-1}\right)$ размеров $q^k-1\times m$ со столбцами $(A_{i_1}, \ldots, A_{i_m})$, где $(i_1, \ldots, i_m)-i$-ый набор множества M. (У ленты, в отличие от таблицы, циклически замкнута только одна сторона). Тогда можно убедиться, что, если прямоугольник $k\times m$ пробегает все ленты B_i, то в клетках прямоугольника встречаются все $q^{km}-1$ ненулевые комбинации над полем $GF(q)$. Поэтому, если возможно построить последовательность $C=c_0c_1\ldots c_{\frac{q^{km}-1}{q^k-1}-1}$ длины $\dfrac{q^{km}-1}{q^k-1}$ над множеством L такую, что среди m-наборов $(c_0c_1\ldots$ $\ldots c_{m-1})$; $\ldots(c_1, \ldots, c_m), \ldots (c_{\frac{q^{km}-1}{q^k-1}-1}, c_0, \ldots, c_{m-2})$ нет набора $(y,$

$y, \ldots, y$) и любая пара наборов неэквивалентна, то таблица размера $q^k-1 \times \dfrac{q^{km}-1}{q^k-1}$, столбцы которой состоят из A_i, где i пробегает последовательность C, обладает свойством $k \times m$ „окна“. Назовем C порождающей последовательностью таблицы.

Используя некоторые свойства рекуррентных соотношений, построена порождающая последовательность C и тем самым доказана теорема.

Теорема 2. *Для любых натуральных чисел k и m можно построить таблицу размера $q^k-1 \times \dfrac{q^{km}-1}{q^k-1}$ из элементов поля $GF(q)$, обладающих свойством $k \times m$ „окна“.*

Это является улучшением результата Мак-Вильямса и Слоэна, где требуется дополнительное условие $\left(q^k-1, \dfrac{q^{km}-1}{q^k-1}\right)=1$.

Примеры. а) $q=2$, $k=m=2$. Порождающая последовательность имеет вид (y 0020). Таблица 3×5 со свойством 2×2 „окна“ в качестве первого столбца имеет нулевой набор, а остальные столбцы состоят из сдвигов (п. м. д.)$=011$.

$D_1=$

0	0	0	1	0
0	1	1	1	1
0	1	1	0	1

б) $q=2$, $k=2$, $m=3$. Порождающая последовательность равна:

$$(yy00y2011121 10y1y1020)$$

$D_2=$

0	0	0	0	0	1	0	1	1	1	1	1	1	0	0	1	0	1	0	1	0
0	0	1	1	0	1	1	0	0	0	1	0	0	1	0	0	0	0	1	1	0
0	0	1	1	0	0	1	1	1	1	0	1	1	1	0	1	0	1	1	0	1

Таблица D_2 обладает свойством 2×3 „окна“

3. Метод построений таблиц $t^k \times t^{k(m-1)}$ со свойством $k \times m$ „окна“ аналогичен методу, описанному в пункте 2. Для построения таблиц со свойством „окна“ с нулевым набором строятся порождающие последовательности, m-наборы которых неэквивалентны. Однако построения этих последовательностей существенно отличаются.

Сначала рассмотрим случай, когда $t=q$ — степень простого числа. Для построения порождающей последовательности доказаны следующие леммы.

Лемма 1. *Пусть $N=n_0 n_1 \ldots n_{q^{m-1}-2}$ (п. м. д.) длины $q^{m-1}-1$, которая задается решением рекуррентных соотношений (1) с помощью примитивного полинома $h(x)$, степени $m-1$, над полем $GF(q)$ и $m \geqslant 2$. Тогда все m-наборы при $q \geqslant 3$ $(n_0 n_1 \ldots n_{m-1}), \ldots$ $\ldots (n_{q^{m-1}-2}, n_0, \ldots, n_{m-2})$ неэквивалентны над полем $GF(q)$. Для $q=2$ это имеет место при $m \geqslant 3$.*

Лемма 2. *Пусть $N=n_0 n_1 \ldots n_{q^{m-1}-2}$ (п. м. д.), определен-*

ная в лемме 1, и N_j—последовательность, полученная из N циклическим сдвигом на j позиции так, что первые $(m-1)$ элементы N_j—единицы. Обозначим через $\hat{N}=(\hat{n}_0\,\hat{n}_1\ldots\hat{n}_{q^{k(m-1)}-1})$ последовательность длины $q^{k(m-1)}$, у которой первые $q^{(k-1)(m-1)}$ элементы единицы, а остальная часть состоит из $q^{(k-1)(m-1)}$ последовательностей N_j. Тогда для каждого $i=0, 1, \ldots, q^{(k-1)(m-1)}-1$ среди наборов вида

$$(\hat{n}_{i+jq^{(k-1)(m-1)}}, \hat{n}_{i+1+jq^{(k-1)(m-1)}}, \ldots, \hat{n}_{i+m-1+jq^{(k-1)(m-1)}}),\ j=0, \ldots, q^{m-1}-1$$

встречаются всевозможные неэквивалентные наборы.

С помощью этих лемм доказана следующая теорема.

Теорема 3. *Пусть $q=p^n$ — степень простого числа. Тогда для каждых k и $m\neq 2$ можно построить последовательность длины $q^{k(m-1)}$ из элементов $(0, 1, \ldots, q^k-1)$, которая содержит все неэквивалентные наборы над кольцом $F(0, 1, \ldots, q^k-1)$. Если $p\geqslant 3$, то такую последовательность можно построить и для $m=2$.*

Перейдем к построению таблиц над любым конечным алфавитом, обладающих свойством „окна“.

Пусть V_1 и V_2 таблицы размеров $n_1^{t_1}\times n_2^{t_2}$ и $n_1^{t_1'}\times n_2^{t_2'}$ над алфавитами $(0, 1, \ldots, n_1-1)$ и $(0, 1, \ldots, n_2-1)$ соответственно и $t_1+t_2=t_1'+t_2'=km$. Имеет место следующее утверждение.

Теорема 4. *Если таблицы V_1 и V_2 обладают свойством $k\times m$ „окна“ и $(n_1, n_2)=1$, то существует таблица V размера $n_1^{t_1}\cdot n_2^{t_1'}\times n_2^{t_2}\cdot n_2^{t_2'}$, обладающая свойством $k\times m$ „окна“ над алфавитом $(0, 1, \ldots, n_1\cdot n_2-1)$.*

Следствие. Для любых натуральных чисел t и m существует последовательность максимальной длины $(t^m-1$ или $t^m)$ над алфавитом из t элементов.

Из теорем 3 и 4 следует

Теорема 5. *Для любых натуральных чисел $k, t\geqslant 2$, $m\neq 2$ можно построить таблицу размера $t^k\times t^{k(m-1)}$, обладающую свойством $k\times m$ „окна“. Если t—нечетное число, то такую таблицу можно построить и для $m=2$.*

Пример. $t=2$, $k=2$, $m=3$. Порождающая последовательность имеет вид: $C^*=0003020320010023$

$\hat{D}=$

0	0	0	0	0	1	0	0	1	0	0	1	0	0	1	0
0	0	0	1	0	1	0	1	1	0	0	0	0	0	1	1
1	1	1	1	1	0	1	1	0	1	1	0	1	1	0	1
1	1	1	0	1	0	1	0	0	1	1	1	1	1	0	0

Таблица D обладает свойством 2×3 „окна“ В последовательности C^* все 3-наборы неэквивалентны над кольцом по модулю 4. Таблица $\hat{D}$ состоит из (п. м. д.)0 $A=0011$ и ее сдвигов, которые соответствуют C^*.

4. Пусть $A=a_0a_1 \dots a_{q^m-2}$ (п. м. д.) над полем $GF(q)$ и $q^m-1=$ $=M \cdot T$, $M>m$.

Определение 3. Последовательности $A^{(0)}=(a_0^{(0)}, a_1^{(0)}, \dots, a_{M-1}^{(0)}), \dots$ $\dots A^{(T-1)}=(a_0^{(T-1)}, a_1^{(T-1)}, \dots, a_{M-1}^{(T-1)})$ называются разбиением последовательности A, если среди m-наборов

$$(a_i^{(j)}, a_{i+1}^{(j)}, \dots, a_{i+m-1}^{(j)}),\ i=0, \dots, M-1;\ j=0, 1, \dots, T-1$$

встречаются всевозможные q^m-1 ненулевые комбинации над полем $GF(q)$.

Доказан следующий результат.

Теорема 6. *Пусть $M \cdot T=q^m-1$. Если существует разбиение (п. м. д.) $A=a_0a_1 \dots a_{q^m-2}$ на T частей, то всегда можно построить таблицу размера $M\times \dfrac{q^{km}-1}{M}$, обладающую свойством $m\times k$ „окна“.*

Определение 3*. Пусть $E=e_0e_1 \dots e_{q^m-1}$ (п. м. д.) 0.

$$q^r\times q^{m-r}=q^m,\ q^r>m$$

Последовательности

$$E^{(0)}=(e_0^{(0)}, e_1^{(0)}, \dots, e_{q^r-1}^{(0)}), \dots, E^{(q^{m-r}-1)}=(e^{(q^{m-r}-1)}, \dots, e_{q^r-1}^{(q^{m-r}-1)})$$

называются разбиением E, если среди наборов

$$(e_i^{(j)}, e_{i+1}^{(j)}, \dots, e_{i+m-1}^{(j)}),\ i=0, \dots, q^r-1;\ j=0, \dots, q^{m-r}-1$$

встречаются всевозможные q^m комбинации над полем $GF(q)$.

Доказана следующая теорема.

Теорема 7. *Пусть существует разбиение (п. м. д.) 0 $E=$ $=e_0 \cdot e_{q^m-1}$; $E^{(0)}, \dots, E^{(q^{m-r}-1)}$, которые содержат всевозможные m-наборы над полем $GF(q)$. Тогда можно построить таблицу размера $q^r\times q^{mk-r}$, обладающую свойством $m\times k$ „окна“.*

Лемма 3. *(П. м. д.) 0 $E=e_0e_1 \dots e_{q^m-1}$ над полем $GF(q)$ всегда можно разбить на q частей, кроме случая, когда $E=0011$.*

Из теоремы и леммы 3 получаем следующий результат.

Теорема 8. *Для любых натуральных чисел k, m можно построить таблицу размера $q^{m-1}\times q^{mk-m+1}$ над полем $GF(q)$, обладающую свойством $m\times k$ „окна“ с исключением, когда $q=m=2$.*

Пример. (П. м. д.)0 длины 9 над полем $GF(3)$ можно разбить на 3 части: $(001)=v$, $(112)=u$, $(220)=w$. Используя теорему 8, можно построить таблицу размера 3×27 со свойством 2×2 „окна“ над алфавитом (0, 1, 2). Порождающая последовательность состоит из трех переменных v, u, w и имеет вид:

$$w_0u_0u_1v_0v_0v_1v_0u_0w_1w_0v_0w_1u_0u_0v_1u_0w_0w_1v_0w_0u_1u_0v_0u_1w_0w_0v_1$$

$D^*=$

0	2	1	1	1	0	1	2	2	0	1	2	2	2	0	2	0	2	1	0	1	2	1	1	0	0	0
2	1	2	0	0	1	0	1	0	2	0	0	1	1	1	1	2	0	0	2	2	1	0	2	2	2	1
2	1	1	0	0	0	0	1	2	2	0	2	1	1	0	1	2	2	0	2	1	1	0	1	2	2	0

Таблица D^* обладает свойством 2×2 „окна“.

Вычислительный центр Академии наук Армянской ССР и
Ереванского государственного университета

Լ. Հ. ԽԱՉԱՏՐՅԱՆ

«Լուսամուտի» հատկությամբ օժտված աղյուսակներ

Աշխատանքը նվիրված է «լուսամուտի» հատկությամբ օժտված աղյուսակների կառուցմանը, որոնք հանդիսանում են մաքսիմալ երկարության հաջորդականությունների և դե Բրեյնի ցիկլերի ընդհանրացումը հարթության վրա։ Տրված է նոր մեթոդ այդպիսի աղյուսակների կառուցման համար։ Նոր մեթոդի օգնությամբ, մասնավորապես, կառուցված է աղյուսակների դաս, որոնք (¹) աշխատանքի արդյունքի ընդհանրացումն են կազմում։ Աղյուսակների նոր դասեր ստանալու համար աշխատանքում դիտարկված է նաև մաքսիմալ երկարության հաջորդականությունների և դե Բրեյնի ցիկլերի տրոհման պրոբլեմը։

ЛИТЕРАТУРА—ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *F. J. MacWilliams, N. J. A. Sloane*, IEEE, vol. 64, № 12 (1976). [2] *У. Питерсон, Э. Уэлдон*, Коды, исправляющие ошибки. Мир, М., 1976.