Zbornik radova Prirodno-matematičkog fakulteta—Univerzitet u Novom Sadu, knjiga 9 (1979)
Ежегодник Естественно-математического факультета — Университет в Новом Саде, Том 9 (1979)

Янез Ушан, Райко Тошич, Душан Сурла

ОДИН СПОСОБ ПОСТРОЕНИЯ СИСТЕМ ОРТОГОНАЛЬНЫХ ЛАТИНСКИХ ПРЯМОУГОЛЬНИКОВ, КОДОВ И к-СЕМИСЕТЕЙ

В настоящей работе рассматривается один способ построения систем ортогональных латинских прямоугольников, кодов исправляющих или обнаруживающих ошибки, и к-семисетей.

Теорема 1. Если существует подстановка $(a_0, a_1, \ldots, a_{q-1})$ чисел $0,1, \ldots, q-1$, которая для некоторого натурального числа $m<q$ удовлетворяет условию

(*) для каждого $k \in \{1, \ldots, m\}$, все члены последовательности

$$b_i^k = \sum_{j=i}^{k} c_{j+1} \pmod q, \; i=0,1, \ldots, q-(k+1),$$

попарно не сравнимые по модулю q, где для $r \in \{1, \ldots, q-1\}$

$$c_r = a_r - a_{r-1} \pmod q,$$

тогда существует система мощности $m+1$ попарно ортогональных латинских прямоугольников $q \times (q-m)$.

Доказательство

Условие (*) является конъюкцией m условий (k) — для каждого $k \in \{1, \ldots, m\}$ одно условие. Первым из этих условий (для $k=1$) является следующее условие:

(1) все разности $c_1=a_1-a_0, \ldots, c_{q-1}=a_{q-1}-a_{q-2}$, попарно не сравнимые по модулю q.

По Гаустону [1], если существует подстановка чисел $0,1, \ldots, q-1$, удовлетворяющая условию (1), тогда существует горизонтально полный латинский квадрат порядка q, т.е. латинский квадрат, для которого справедливо: для любого $(\alpha, \beta) \in \{0, \ldots, q-1\}^2$ существует строка квадрата, в которой α и β, в том же порядке, являются соседними координатами. Упомянутый квадрат получается следующим образом: 1. если $(a_0, a_1, \ldots a_{q-1})$ подстановка, удовлетворяющая условию (1), то последовательность $a_0, a_1, \ldots, a_{q-1}$ является первой строкой латинского квадрата; и 2.

$$u_{st} = u_{s-1,\, t+1} \pmod q$$

для каждого $s \in \{2, \ldots, q\}$ и каждого $t \in \{1, \ldots, q\}$. (Горизонтальная полность сохраняется при перестановке строк.)

Пусть L—латинский квадрат, полученный только что описанным способом.

Для фиксированного $\kappa \in \{1, \ldots, m\}$, члены последовательности

$$(\overline{k}) \qquad b_i^k = \sum_{j=i}^{k} c_{j+i} \pmod q, i=0, \ldots, q-(k+1),$$

являются следующими разностями по модулю q:

$$b_i^k = a_{i+k} - a_i; \qquad i=0, \ldots, q-(k+1).$$

Справедливо: упорядоченные пары $(u_{st}, u_{s,\, t-k})$ для любого $(s, t) \in \{1, \ldots, q\} \times \{k+1, \ldots, q\}$ являются между собой не равными, т. е. множество

$$\{(u_{st}, u_{s,\, t-k}) \mid (s, t) \in \{1, \ldots, q\} \times \{k+1 \ldots, q\}\}$$

имеет мощность $q.(q-k)$. Именно, разности $u_1\, t - u_{1,\, t-k}$ по модулю q, $q-k$ пар координат первой строки, на основании условий (k), между собой попарно не сравнимые по модулю q. Учитывая способ построения s-строк для $s \in \{2, \ldots, q\}$, получаем, что это справелдиво для всех s-строк квадрата L. Разность $u_{st} - u_{s,\, t-k}$ является независимой от s. Так как каждого $h \in \{0, 1, \ldots, q-1\}$ в каждом столбце находится точно по одному, то из $h = u_{st} = u_{s'\, t'}$ следует, что

$$u_{st} - u_{s,\, t-k} \neq u_{s'\, t'} - u_{s',\, t'-k},$$

и потому, что $u_{s,\, t-k} \neq u_{s',\, t-k}$.

Из L получаем $m+1$ попарно ортогональных латинских прямоуглольников $P_0, P_1, \ldots, P_m$ следующим образом: i-той $(i=1, \ldots, q-m)$ столбец прямоуглольника P_k $(k=0, \ldots, m)$ и $(k+i)$ - той столбец квадрата L являются равными (как q—последовательности). Пусть Pi и Pj, где $i \neq j$—только что построенные латинские прямоугольники. Пусть далее d_{st} и d'_{st} — элементы, принадлежащие сразу s-той строке и t-тому столбцу прямоугольников Pi и Pj в том же порядке. Таким образом получаем $q \cdot (q-m)$ упорядоченных пар (d_{st}, d'_{st}). Справедливо: если $(\bar{s}, \bar{t}) \neq (s, t)$, то $(d_{st}, d'_{st}) \neq (d_{\bar{s}\bar{t}}, d'_{\bar{s}\bar{t}})$. Учитывая способ построения квадрата L и прямоугольников P_k, получаем, что

$$d_{st} = u_{s,\, t+t} \text{ и } d'_{st} = u_{s,\, j+t} = u_{s,\, (t+t)+e} \quad (e=j-i).$$

Учитывая этот факт, получаем, что из

$$h = d_{st} = d_{\bar{s}\bar{t}} = u_{s,\, t+t} = u_{\bar{s},\, t+\bar{t}}$$

следует

$$d'_{st} = u_{s,\, (t+t)+e} \text{ и } d'_{\bar{s}\bar{t}} = u_{\bar{s},\, (t+\bar{t})+e}.$$

Отсюда, так как $i+t \neq i+\bar{t}$, находим, что $d'_{st} - d_{st} \neq d'_{\bar{s}\bar{t}} - d_{\bar{s}\bar{t}}$, и потому, что $d'_{st} \neq d'_{\bar{s}\bar{t}}$. Теорема доказана.

Теорема 2. Если существует подстановка $(a_0, a_1, \ldots, a_{q-1})$ чисел $0,1, \ldots, q-1$ которая для некоторого $m<q (m, q \in N)$ удовлетворяет условию (*) из теоремы 1, то существует код из, по меньшей мере, $q\cdot(q-m)>q^{1})(m+3)$ -последовательностей кодного расстояния $m+2$, построенного над альфавитом $\{0, 1, \ldots, q-1\}$.

Доказательство

Каждый латинский прямоугольник $q\times(q-m)$ определяет частичную квазигруппу на множестве из q элементов, определенном для $q\cdot(q-m)$ упорядоченных пар. F и E, где

$$F(x, y) \stackrel{\text{def}}{=} x \qquad \text{и} \qquad E(x, y) \stackrel{\text{def}}{=} y$$

называются левой и правой частичной единичной операцией. Множество из F, E и P_k, $\kappa \in \{0,1, \ldots, k\}$, где $\mathcal{D}F=\mathcal{D}E=\mathcal{D}P_k$, определяет ортогональную систему частичных операций (квазигрупп) — *ОСЧО* [4]. Учитывая теорему 2. из [4], находим, что предложение доказано. (Описанный код существует и для $q\cdot(q-m)=q$.)

Известно, что существуют конечные множества, не обладающие подстановками, удовлетворящие условию (1); таким образом — условию (κ). Для $q=4, 6, 8, 10$, используя *ЭВМ* Математического института в Новом Саде, мы получили результаты, приведенные в таблице 1. В таблице 1. приведены числа между собой не эквивалентных подстановок, удовлетворяющих условию (*) из теоремю 1. Эквивалентными считаются подстановки, которые в отношении „циклического сдвига".

q/m	1	2	3	4	5	6	7	8	9	10
4	1	1	1	–	–	–	–	–	–	–
6	4	2	2	2	2	–	–	–	–	–
8	24	–	–	–	–	–	–	–	–	–
10	288	8	4	4	4	4	4	4	4	–

Особо интересным является случай $q=6$ и случай $q=10$. Как известно, для $q=6$ не существуют пары ортогональных квазигрупп, а для $q=10$ до сих пар не построена тройка попарно ортогональных квазигрупп. Таким образом, не существует код из 36 4-последовательностей кодного расстояния 3 над альфавитом мощности 6. Также неизвестен код из 100 5-последовательностей кодного расстояния 4 над алфавитом мощности 10.

1) $q\cdot(q-m)\leq q^2$; см. [4].

Помощью предлагаемого нами способа над упомянутыми алфавитами можно построить коды κ-последовательностей и для $k>4$ (-для алфавита мощности 6) и для $k>5$ (-для алфавита мощности 10), у которых число κ-последовательностей меньше, чем 36, и меньше, чем 100, но обладающих кодным расстоянием больше, чем 4 и больше, чем 5, в том же порядке.

Пример 1.

Подстановка 021453 ($h=6$) удовлетворяет условию (*) для $m=1, 2, 3, 4, 5$. Здесь последовательности b_i^1, b_i^2, b_i^3, b_i^4, b_i^5, (в том же порядке) являются следующими последовательностями: 2, 5, 3, 1, 4; 1, 2, 4, 5; 4, 3, 2; 5, 1; 2. Соответствующий квадрат L представлен табл. 2. Прямоугольники 6x5 P_0 и P_1 представлень в таблицах 3a и 3b. Соответствующие частичные квазигруппы представлены в таблицах 4a и 4б. Соответствующий код построен на основании теоремы 2 — ($K1$).

0	2	1	4	5	3
1	3	2	5	0	4
2	4	3	0	1	5
3	5	4	1	2	0
4	0	5	2	3	1
5	1	0	3	4	2

Табл. 2.

0	2	1	4	5
1	3	2	5	0
2	4	3	0	1
3	5	4	1	2
4	0	5	2	3
5	1	0	3	4

Табл. 3a.

2	1	4	5	3
3	2	5	0	4
4	3	0	1	5
5	4	1	2	0
0	5	2	3	1
1	0	3	4	2

Табл. 3b.

	0	1	2	3	4	5	
0	0	2	1	4	5		
1	1	3	2	5	0		
2	2	4	3	0	1		
3	3	5	4	1	2		
4	4	0	5	2	3		
5	5	1	0	3	4		

Табл. 4a.

	0	1	2	3	4	5	
0	2	1	4	5	3		
1	3	2	5	0	4		
2	4	3	0	1	5		
3	5	4	1	2	0		
4	0	5	2	3	1		
5	1	0	3	4	2		

Табл. 4b.

0002	1013	2024	3035	4040	5051
0121	1132	2143	3154	4105	5110
0214	1225	2230	3241	4252	5203
0345	1350	2301	3312	4323	5334
0453	1404	2415	3420	4431	5442

(K1)

Так как рассматриваемая подстановка удовлетворяет условию (*) и для $m=2$, то, исходя из L, получаем и попарно ортогональные латинские прямоугольники P_0, P_1, P_2, представленные в табл. 5. Отвечающий код (из 24 5-последовательностей кодного расстояния 4 над алфавитом {0, 1, 2, 3, 4, 5}) —($K2$).

0	2	1	4
1	3	2	5
2	4	3	0
3	5	4	1
4	0	5	2
5	1	0	3

2	1	4	5
3	2	5	0
4	3	0	1
5	4	1	2
0	5	2	3
1	0	3	4

1	4	5	3
2	5	0	4
3	0	1	5
4	1	2	0
5	2	3	1
0	3	4	2

Табл. 5.

00021	10132	20243	30354	40405	50510
01214	11325	21430	31541	41052	51103
02145	12250	22301	32412	42523	52034
03453	13504	23015	33120	43231	53342

(*K*2)

Таким же образом, для $m=3$ и $m=4$, получается код из 18 6-последовательностей кодного расстояния 5 и код из 12 7-последовательностей кодного расстояния 6 над алфавитом {0, 1, 2, 3, 4, 5}.

Пример 2.

Подстановка 0764839125 является одной из 4 подстановок, удовлетворяющих условию (*) для $m=1, 2, \ldots, 9$. Как и в примере 1, исходя из этой подстановки, можно получить коды из 10. $(10-m)$ $(m+3)$- последовательностей кодного расстояния $m+2$ над алфавитом $\{0, 1, \ldots, 9\}$. Соответствующий квадрат L представлен в таблице 6. Прямоугольники P_0, P_1, P_2 (для $m=2$) приведены на таблицах 7. Соответствующий код (из 80 5-последовательностей кодного расстояния 4 над алфавитом {0, 1, . . .9}) — (*K*3).

0	7	6	4	8	3	9	1	2	5
1	8	7	5	9	4	0	2	3	6
2	9	8	6	0	5	1	3	4	7
3	0	9	7	1	6	2	4	5	8
4	1	0	8	2	7	3	5	6	9
5	2	1	9	3	8	4	6	7	0
6	3	2	0	4	9	5	7	8	1
7	4	3	1	5	0	6	8	9	2
8	5	4	2	6	1	7	9	0	3
9	6	5	3	7	2	8	0	1	4

Табл. 6.

0	7	6	4	8	3	9	1
1	8	7	5	9	4	0	2
2	9	8	6	0	5	1	3
3	0	9	7	1	6	2	4
4	1	0	8	2	7	3	5
5	2	1	9	3	8	4	6
6	3	2	0	4	9	5	7
7	4	3	1	5	0	6	8
8	5	4	2	6	1	7	9
9	6	5	3	7	2	8	0

7	6	4	8	3	9	1	2
8	7	5	9	4	0	2	3
9	8	6	0	5	1	3	4
0	9	7	1	6	2	4	5
1	0	8	2	7	3	5	6
2	1	9	3	8	4	6	7
3	2	0	4	9	5	7	8
4	3	1	5	0	6	8	9
5	4	2	6	1	7	9	0
6	5	3	7	2	8	0	1

6	4	8	3	9	1	2	5
7	5	9	4	0	2	3	6
8	6	0	5	1	3	4	7
9	7	1	6	2	4	5	8
0	8	2	7	3	5	6	9
1	9	3	8	4	6	7	0
2	0	4	9	5	7	8	1
3	1	5	0	6	8	9	2
4	2	6	1	7	9	0	3
5	3	7	2	8	0	1	4

Табл. 7.

00076	20298	40410	60632	80854	
01764	21986	41108	61320	81542	
02648	22860	42082	62204	82426	
03483	23605	43827	63049	83261	
04839	24051	44273	64495	84617	
05391	25513	45735	65957	85179	
06912	26134	46356	66578	86790	
07123	27347	47569	67781	87903	
10187	30309	50521	70743	90965	(*K*3)
11875	31097	51219	71431	91653	
12759	32971	52193	72315	92537	
13594	33716	53938	73150	93372	
14940	34162	54384	74506	94728	
15402	35624	55846	75068	95280	
16023	36245	56467	76689	96801	
17236	37458	57670	77892	97014	

Учитывая определение регулярной частичной квазигруппы [3], находим, что справедлива

Лемма 1. Латинский прямоугольник $q\times(q-m)$, $m<q$, определен на множестве $\{0, 1, \ldots, q-1\}$, определяет регулярную частичную квазигруппу, если $q-m\geq 2$.

Далее, учитывая определение регулярно ортогональных частичных операций [3], находим, что справедлива и

Лемма 2. Ортогональные латинские прямоугольники $q\times(q-m)$, $m<q$, определенные на множестве $\{0, 1, \ldots, q-1\}$, определяют регулярно ортогональные частичные квазигруппы если $q-m\leq 2$.

Учитывая теорему 1, леммы 1-2 и теорему 4. из [3], находим, что справедлива.

Теорема 3. Если существует натуральное число $m<q$, $q\in N$, где $q-m\geq 2$ и подстановка $(a_0, a_1, \ldots, a_{q-1})$ чисел $0,1, \ldots, q-1$, удовлетворяющая условию (*) из теоремы 1, тогда существует $(m-3)$-семисеть из $q\cdot(q-m)$ точек, в которой справедливо L-порядок[1)] $=T$-порядок[1)] $=q$.

На рис. 2. в [3] представлена 4-семисеть из 18 точек, в которой L-порядок $=$ T-порядок $=6$. Учитывая пример 1, находим, что существует 4-семисеть из 30 точек, в которой справедливо L-порядок$=$ T-порядок$=6$.

[1)] см [5]

ЛИТЕРАТУРА

[1] Houston T. R., *Sequential Counterbalancing in Latin Squres*, Ann. Math. Statist., 37 (1966), 741—743.

[2] Dénes J., Keedwell A. D., *Latin Squares and their Applications*, Akadémiai Kiado, Budapest, 1974.

[3] Ušan J., *k-Seminets*, Mat. Bilten, 1977, 41—46.

[4] Ušan J., Stojaković Z., *Orthogonal Systems of Partial Operations*, Zbornik radova PMF u Novom Sadu, 8, 1978,

Janez Ušan
Ratko Tošić
Dušan Surla

JEDAN NAČIN ZA KONSTRUKCIJU ORTOGONALNIH SISTEMA LATINSKIH PRAVOUGAONIKA, KODOVA I k-SEMIREŠETAKA

Rezime

U radu je dat jedan postupak za konstrukciju sistema ortogonalnih latinskih pravougaonika, kodova koji ispravljaju ili otkrivaju greške i k-semirešetaka. Postupak se zasniva na tri teoreme koje se dokazuju u radu.

Rezultati su ilustrovani primerima koji su dobijeni korišćenjem računara Instituta za matematiku PMF-a u Novom Sadu.