А. Е. Т р и ш и н (Москва, ТВП)**. Способ построения ортогональных латинских квадратов на основе подстановочных двучленов конечных полей.**

Латинским квадратом порядка n называется квадратная матрица, каждая строка и каждый столбец которой являются перестановкой элементов конечного множества A, состоящего из n элементов.

Два латинских квадрата (b_{ij}), (c_{ij}) порядка n называются *ортогональными*, если для любой упорядоченной пары $(a_1, a_2) \in A^2$ найдутся такие $i, j \in \{1, 2, \ldots, n\}$, что $b_{ij} = a_1$, $c_{ij} = a_2$.

Можно рассматривать системы из r попарно ортогональных латинских квадратов порядка n. Известно, что $r \leqslant n-1$, и при $r = n-1$ такая система называется *полной*.

Известны методы построения полных систем попарно ортогональных латинских квадратов (см. [2], [4]). Напомним *метод Боуза*. Пусть $n = p^t$, где p — простое число, $t \in \mathbf{N}$, $n \geqslant 3$. Рассмотрим конечное поле $\mathrm{GF}(p^t) = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{n-1}\}$, где 0 и 1, соответственно, — нуль и единица этого поля. Тогда множество таблиц $L^{(l)} = (a_{ij}^{(l)})$, $a_{ij}^{(l)} = a_l a_t + a_j$, $i, j = 1, 2, \ldots, n$, $l = 1, 2, \ldots, n-1$, образует полное множество попарно ортогональных латинских квадратов порядка n.

Многие способы построения ортогональных латинских квадратов используют идею метода Боуза. Пусть $(A, +)$ — абелева группа порядка n, и π, σ — подстановки на множестве A. *Разностью подстановок* π и σ называется такое отображение $\pi - \sigma$: $A \to A$, что $(\pi - \sigma)(a) = \pi(a) - \sigma(a)$ для всех $a \in A$.

Теорема 1 (см. [4])**.** *Латинские квадраты* $(\pi(a_i) + a_j)_{i,j=1,2,\ldots,n}$ *и* $(\sigma(a_i) + a_j)_{i,j=1,2,\ldots,n-1}$ *ортогональны в том и только в том случае, если отображение* $\pi - \sigma$ *является подстановкой.*

Для построения ортогональных латинских квадратов можно использовать подстановочные двучлены над конечными полями. Напомним, что многочлен над конечным полем называется *подстановочным*, если он задает подстановку на множестве элементов этого поля (ср. [1]).

Пусть многочлен $x^u + \alpha x^v$ над полем $\mathrm{GF}(q)$ является подстановочным для всех элементов $\alpha \in \{\alpha_1, \ldots, \alpha_k\} \subset \mathrm{Gf}(q0 \setminus \{0\}$, и числа u и v различны и взаимно просты с числом $q-1$. Тогда из теоремы 1 следует, что набор $\pi, \sigma_1, \ldots, \sigma_k$ таких подстановок поля $\mathrm{GF}(q)$, что $\pi(x) = x^u$, $\sigma_l(x) = \alpha x^v$, $l = 1, 2, \ldots, k$, задает систему из $k+1$ попарно ортогональных латинских квадратов.

Теорема 2 (см. [1]). *Многочлен* $x^{p^m} + \alpha x$ *над полем* $\mathrm{GF}(p^t)$ *является подстановочным в том и только в том случае, если* $(-\alpha)^{(p^t-1)/d}$, *где* $d = \mathrm{НОД}(p^m - 1, p^t - 1)$.

П р и м е р 1. Пусть число $t \in \mathbf{N}$ четно, $t \geqslant n$. Тогда многочлен $x^4 + \alpha x$ является подстановочным многочленом поля $\mathrm{GF}(2^t)$, если $\alpha \neq \gamma^3$ для некоторого $\gamma \in \mathrm{GF}(2^t)^*$. Рассмотрим случай $t = 4$. Пусть ξ — первообразный элемент поля $\mathrm{GF}(16)$. Тогда многочлены $\xi^{3k} x^4$, $\xi^{3k+1} x$, $\xi^{3k+2} x$, $k = 0, 1, \ldots, 4$, являются подстановочными и задают полную систему попарно ортогональных латинских квадратов порядка 16.

П р и м е р 2. Пусть $t = 6$. Многочлен $x^{13} + \alpha x^4$ является подстановочным многочленом поля $\mathrm{GF}(64)$, если α — корень из 1 степени 3 или 21 (ср. [3]). Тогда подстановочные многочлены x^{13} и αx^4 задают пару ортогональных латинских квадрата порядка 64.

Пусть $\mathrm{GF}(q)$ — конечное поле и $\pi_1, \ldots, \pi_{q-1}$ — набор различных подстановок поля $\mathrm{GF}(q)$, удовлетворяющих условию $\pi_l(0) = 0$, $l = 1, 2, \ldots, q-1$, и для любых различных индексов $i, j \in \{1, 2, \ldots, q-1\}$ найдется такой индекс $k \in \{1, 2, \ldots, q-1\}$, что $\pi_i + \pi_j = \pi_k$. Тогда этот набор задает полную систему попарно ортогональных латинских квадратов порядка q. Известны отдельные примеры таких наборов подстановок (см. [5], [6]).

Работа выполнена при поддержке гранта Президента РФ (НШ–4.2008.10)

СПИСОК ЛИТЕРАТУРЫ

1. *Лидл Р.*, *Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988.
2. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, 1982.
3. *Тришин А. Е.* Двучленные подстановки конечных полей характеристики 2. — Вестник Томского гос. ун-та, 2007, приложение № 23, с. 64–65.
4. *Denes J.*, *Keedwell A. D.* Latin squares and their applications. London: English Univ. Press, 1975.
5. *Laywin C.*, *Mullen G.* Discrete Mathematics Using Latin Squares. Chichester etc.: J. Wiley, 1998.
6. *Nyberg K.* Perfect nonlinear S-boxes. — Lecture Notes Comput. Sci., 1999, v. 1440, p. 378–385.