

# Построение параметрического семейства многомерных латинских квадратов

И. А. Плаксина

В данной работе обобщается конструкция параметрического семейства латинских квадратов над прямым произведением абелевых групп, предложенная ранее в работе [2], на многомерный случай с целью увеличения количества параметров. Дается критерий реализуемости данной конструкции. Также рассмотрен вопрос о связи правильности и циклов в графе существенной зависимости для функций над кольцами вычетов.

**Ключевые слова:** правильное семейство функций, латинские квадраты, параметрическое семейство латинских квадратов, критерий для многомерного латинского квадрата, граф существенной зависимости семейства функций, связь правильности и циклов в графе существенной зависимости.

Латинским квадратом порядка  $n$  называют матрицу размера  $n \times n$ , заполненную элементами множества  $\Omega$ ,  $|\Omega| = n$ , таким образом, что в каждой из строк и каждом из столбцов ее элементы различны. Для практической применимости в сфере защиты информации требуются латинские квадраты достаточно больших размеров, что не позволяет хранить их в памяти поэлементно, такие квадраты необходимо задавать с использованием аналитических методов. Как правило, на практике они задаются функцией от двух переменных, определяющих значение элемента квадрата по номерам его координат, и в памяти требуется хранить не весь квадрат целиком, а только соответствующую функцию. Например, функция  $L(x, y) = x + y$ , где  $x, y$  — номера строк и столбцов соответствующей матрицы, будет задавать латинский квадрат. В данной работе продолжается рассмотрение параметрических семейств латинских квадратов, исследуемых в работах [2]–[5] для различных классов функций.

1. Пусть  $G$  — абелева группа. Рассмотрим прямое произведение  $n$  ее копий:

$$H = G^n = \underbrace{G \times G \times \dots \times G}_n.$$

Зададим над группой  $H$  латинский квадрат  $L$  порядка  $\underbrace{|H| \times |H| \times \dots \times |H|}_m$  следующим образом.

«Проиндексируем» каждое измерение  $L$  элементами группы  $H$ . Пусть  $x^1, x^2, \dots, x^m$ , где  $x^i = (x_1^i, x_2^i, \dots, x_n^i)$ ,  $i \in \overline{1, m}$ , — элементы группы  $H$ . Тогда элемент  $L(x^1, x^2, \dots, x^m) = (z_1, \dots, z_n)$  квадрата  $L$  определим формулами:

$$\begin{aligned} z_1 &= x_1^1 + \dots + x_1^m + f_1(p_1(x_1^1, \dots, x_1^m), \dots, p_n(x_n^1, \dots, x_n^m)) \\ z_2 &= x_2^1 + \dots + x_2^m + f_2(p_1(x_1^1, \dots, x_1^m), \dots, p_n(x_n^1, \dots, x_n^m)) \\ &\vdots \\ z_n &= x_n^1 + \dots + x_n^m + f_n(p_1(x_1^1, \dots, x_1^m), \dots, p_n(x_n^1, \dots, x_n^m)), \end{aligned} \quad (1)$$

где  $p_1, p_2, \dots, p_n$  — функции из  $G^m$  в  $G$ ,  $f_1, f_2, \dots, f_n$  — функции из  $G^n$  в  $G$ .

В работах [2, 3] был представлен такой способ введения параметра в семейство латинских квадратов в случае булевских функций и функций  $p$ -значной логики и  $m = 2$ .

Здесь и далее, для упрощения изложения, мы будем называть  $L$  — «латинским квадратом», хотя, в действительности, он представляет собой многомерное параметрическое семейство. Для перехода к параметрическому семейству латинских квадратов размерности 2 необходимо зафиксировать любые  $m - 2$  измерения и рассмотреть всевозможные значения параметров. В случае, если в качестве параметров берется семейство булевских функций, их число будет  $2^{2^n}$ .

Однако, не для всех функций  $f_1, f_2, \dots, f_n$   $L$  будет задавать латинский квадрат. Найдем условия на функции, при которых  $L$  будет таковым для произвольных  $p_1, p_2, \dots, p_n$ . Следующее свойство семейств функций было определено в работах [1, 2, 4] для булевских функций, функций  $p$ -значной логики и функций над абелевыми группами.

Будем говорить, что функции  $f_1, f_2, \dots, f_n$  от переменных  $p_1, p_2, \dots, p_n$  называется *правильным*, если для любых двух различных наборов значений переменных  $p' = (p'_1, p'_2, \dots, p'_n)$  и  $p'' = (p''_1, p''_2, \dots, p''_n)$  существует  $\alpha \in \overline{1, n}$  такое, что выполнено

$$p'_\alpha \neq p''_\alpha, \quad f_\alpha(p') = f_\alpha(p'').$$

Также в работе [1] приведены критерии правильности для булевского случая и доказано, что задача проверки правильности семейства функций является  $NP$ -трудной. В работе [3] даны несколько классов правильных семейств функций и представлен рекуррентный способ построения таких семейств для функций  $p$ -значной логики.

Следующая теорема была доказана в работе [4] для семейства функций над абелевыми группами и  $m = 2$ .

**Теорема 1.** *Формулы (1) определяют латинский квадрат для любых функций  $p_1, p_2, \dots, p_n$  тогда и только тогда, когда семейство функций  $f_1, f_2, \dots, f_n$  является правильным.*

**Доказательство.** 1. Достаточность.

Предположим,  $f_1, f_2, \dots, f_n$  — правильное семейство. Пусть  $z, \tilde{z}$  — два элемента, отличающиеся по одному измерению. Без ограничения общности будем считать, что этому измерению соответствует номер  $m$ :  $x^m \neq \tilde{x}^m$ . Тогда  $z = z(x^1, \dots, x^{m-1}, x^m)$ ,  $\tilde{z} = \tilde{z}(x^1, \dots, x^{m-1}, \tilde{x}^m)$  и верны следующие равенства:

$$\begin{aligned} z_1 &= x_1^1 + \dots + x_1^m + f_1(p_1(x_1^1, \dots, x_1^m), \dots, p_n(x_n^1, \dots, x_n^m)) \\ z_2 &= x_2^1 + \dots + x_2^m + f_2(p_1(x_1^1, \dots, x_1^m), \dots, p_n(x_n^1, \dots, x_n^m)) \\ &\vdots \\ z_n &= x_n^1 + \dots + x_n^m + f_n(p_1(x_1^1, \dots, x_1^m), \dots, p_n(x_n^1, \dots, x_n^m)) \\ \tilde{z}_1 &= x_1^1 + \dots + \tilde{x}_1^m + f_1(p_1(x_1^1, \dots, \tilde{x}_1^m), \dots, p_n(x_n^1, \dots, \tilde{x}_n^m)) \\ \tilde{z}_2 &= x_2^1 + \dots + \tilde{x}_2^m + f_2(p_1(x_1^1, \dots, \tilde{x}_1^m), \dots, p_n(x_n^1, \dots, \tilde{x}_n^m)) \\ &\vdots \\ \tilde{z}_n &= x_n^1 + \dots + \tilde{x}_n^m + f_n(p_1(x_1^1, \dots, \tilde{x}_1^m), \dots, p_n(x_n^1, \dots, \tilde{x}_n^m)) \end{aligned} \tag{2}$$

Рассмотрим 2 случая.

1). Если  $p_k(x_k^1, \dots, x_k^m) = p_k(x^1, \dots, \tilde{x}_k^m)$  для всех  $k \in \overline{1, n}$ , то функции  $f_l, l = 1, 2, \dots, n$  принимают одинаковые значения на наборах  $(x^1, \dots, x^m)$  и  $(x^1, \dots, \tilde{x}^m)$ . Поэтому правые части (2), (3) отличаются только в компонентах  $x^m$  и  $\tilde{x}^m$ . Так как все элементы одного измерения различны, получаем, что и  $z_i \neq \tilde{z}_i$  для всех  $i \in \overline{1, n}$ . Следовательно, для каждого из измерений элементы  $L$  будут различны. Отсюда заключаем, что  $L$  — латинский квадрат.

2). Пусть значения функций  $p_1, \dots, p_n$  на наборах  $(x^1, \dots, x^m)$   $(x^1, \dots, \tilde{x}^m)$  отличаются.

Из определения правильности семейства  $f_1, \dots, f_n$  следует, что  $\exists k$ :  $p_k(x_k^1, \dots, x_k^m) \neq p_k(x^1, \dots, \tilde{x}^m)$ ,  $f_k(p_1(x_1^1, \dots, x_1^m), \dots, p_n(x_n^1, \dots, x_n^m)) = f_k(p_1(x_1^1, \dots, \tilde{x}_1^m), \dots, p_n(x_n^1, \dots, \tilde{x}_n^m))$ .

Значит, правые части (2), (3) для строк с индексом  $k$  содержат одинаковые наборы  $x_k^1, \dots, x_k^{m-1}$  и  $f_k$ . Но, по построению  $x_k^m \neq \tilde{x}_k^m$ , откуда правые части (2), (3) не равны. Получаем, что и в этом случае элементы каждого из измерений  $L$  будут различны, откуда следует, что  $L$  — латинский квадрат.

2. Необходимость.

Пусть семейство функций  $f_1, \dots, f_n$  не является правильным.

Тогда существуют два различных набора  $t, \tilde{t}$ , таких что для всех  $\alpha$  выполнено:  $t_\alpha \neq \tilde{t}_\alpha$  и  $f_\alpha(t) \neq f_\alpha(\tilde{t})$ .

$L$  является латинским квадратом, поэтому существуют такие  $x^1, \dots, x^{m-1}$  и  $z = (z_1, \dots, z_n)$ , подставив которые в (1) вместе с наборами  $t$  и  $\tilde{t}$  получим значения  $x^m \neq \tilde{x}^m$ , при которых будет выполнено

$$\begin{aligned} z_1 &= x_1^1 + \dots + x_1^m + f_1(t_1, \dots, t_n) \\ z_2 &= x_2^1 + \dots + x_2^m + f_2(t_1, \dots, t_n) \\ &\vdots \\ z_n &= x_n^1 + \dots + x_n^m + f_n(t_1, \dots, t_n) \end{aligned} \quad (4)$$

$$\begin{aligned} z_1 &= x_1^1 + \dots + \tilde{x}_1^m + f_1(\tilde{t}_1, \dots, \tilde{t}_n) \\ z_2 &= x_2^1 + \dots + \tilde{x}_2^m + f_2(\tilde{t}_1, \dots, \tilde{t}_n) \\ &\vdots \\ z_n &= x_n^1 + \dots + \tilde{x}_n^m + f_n(\tilde{t}_1, \dots, \tilde{t}_n) \end{aligned} \quad (5)$$

Найдем  $p_1, \dots, p_n$ , удовлетворяющие условиям

$$\begin{aligned} p_1(x_1^1, \dots, x_1^{m-1}, x_1^m) &= t_1 \\ p_2(x_2^1, \dots, x_2^{m-1}, x_2^m) &= t_2 \\ &\vdots \\ p_n(x_n^1, \dots, x_n^{m-1}, x_n^m) &= t_n \end{aligned} \quad (6)$$

$$\begin{aligned} p_1(x_1^1, \dots, x_1^{m-1}, \tilde{x}_1^m) &= \tilde{t}_1 \\ p_2(x_2^1, \dots, x_2^{m-1}, \tilde{x}_2^m) &= \tilde{t}_2 \\ &\vdots \\ p_n(x_n^1, \dots, x_n^{m-1}, \tilde{x}_n^m) &= \tilde{t}_n \end{aligned} \quad (7)$$

Так выбрать данные функции нельзя только в случае, если  $\exists \alpha : x_\alpha^m = \tilde{x}_\alpha^m$  и  $t_\alpha \neq \tilde{t}_\alpha$ .

Но это бы означало, что  $f(t_\alpha) \neq f(\tilde{t}_\alpha)$ , а это несовместимо с  $x^m = \tilde{x}^m$  по (4), (5).

Следовательно, выбрать функции  $p_i, i \in \overline{1, n}$ , удовлетворяющие равенствам (6), (7) можно. Но, все элементы латинского квадрата должны быть различны по каждому из измерений, а мы получили, что элемент  $z$  по измерению с номером  $m$  повторяется. Значит, наше предположение о семействе функций  $f_1, f_2, \dots, f_n$  было неверным, что и доказывает необходимость условия правильности.

**Замечание 1.** Теорема 1 позволяет при помощи любого правильного семейства функций  $f_1, f_2, \dots, f_n$ , варьируя систему параметров  $p_1, p_2, \dots, p_n$ , получать различные латинские квадраты.

Рассмотрим число способов выбрать такую систему параметров. Функция  $p_i, i \in \overline{1, n}$  зависит от  $m$  аргументов, каждый из которых принимает  $|G|$  значений, из чего заключаем, что число способов выбрать одну функцию будет  $|G|^{|G|^m}$ . Отсюда, количество возможных систем параметров  $p_1, p_2, \dots, p_n$  равно  $|G|^{n|G|^m}$ . При фиксированных  $p_1, p_2, \dots, p_n$  число латинских квадратов размерности 2 составляет  $\frac{1}{2}m(m-1)|G|^{2n}$ .

Следовательно, общее число латинских квадратов размерности 2, которые можно получить, используя утверждение теоремы, составляет  $\frac{1}{2}m(m-1)|G|^{2n+n|G|^m}$ .

**Замечание 2.** Построенные таким способом латинские квадраты являются негрупповыми, то есть они не являются таблицей умножения (таблицей Кэли) конечной группы.

**Замечание 3.** Применение конструкции, предложенной выше, в шифровании позволяет увеличить число ключей при прежнем размере шифруемого текста, либо увеличить размер текста, оставив неизменным число ключей.

**2.** Рассмотрим граф существенной зависимости семейства функций.

Для семейства функций  $f_1, \dots, f_n$  от переменных  $x_1, \dots, x_n$  граф существенной зависимости  $G_f = (V, E)$ , где  $V = \{1, \dots, n\}$  строится следующим образом. Пара  $(i, j) \in E$  тогда и только тогда, когда  $f_j$  существенно зависит от  $x_i$ .

Простым элементарным циклом  $C$  в графе  $G_f$  будем называть цикл, никакое собственное подмножество вершин которого не образует цикл.

В работах [2, 3, 5] был рассмотрен вопрос о влиянии циклов графа  $G_f$  семейства функций на правильность этого семейства для булевых функций, функций  $p$ -значной логики и функций над абелевыми группами. Также, в работе [3] была доказана теорема о достаточности равенства произведения функций нулю на всех простых элементарных циклах графа  $G_f$  для того, чтобы соответствующее семейство функций являлось правильным.

Рассмотрим необходимость этого условия в случае, когда  $f_1, \dots, f_n$  — функции над кольцом вычетов.

**Теорема 2.** Пусть семейство функций  $f = f_1, \dots, f_n$  вида  $f_i = \prod_{j=1}^k \left( \sum_{i=1}^n S_i(x) \right)$ , где  $S_i(x)$  — биективны, правильно. Тогда для любого простого элементарного цикла  $C$  в  $G_f$  выполнено

$$\prod_{i \in C} f_i(x_1, \dots, x_n) \equiv 0. \quad (8)$$

**Доказательство.** Возьмем  $f_1, \dots, f_n$  — правильное семейство функций. Предположим, что существует такой простой элементарный цикл  $C = \{i_1, \dots, i_s\}$ ,  $i_k \in \{1, \dots, n\}$ , что (8) не выполнено. Из определения  $C$  следует, что  $f_{i_1}$  зависит от  $x_{i_2}$  существенно и не зависит существенно от  $x_{i_1}, x_{i_3}, \dots, x_{i_s}$ .

Аналогично,  $f_{i_2}$  зависит существенно только от  $x_{i_3}, \dots, f_{i_s}$  зависит существенно только от  $x_{i_1}$ .

Из нашего предположения следует, что  $\exists x^0 : \prod_{i \in \{i_1, \dots, i_n\}} f_i(x_1^0, \dots, x_n^0) = a \neq 0$

Следовательно,  $f_{i_1} = a_{i_1} \neq 0, \dots, f_{i_s} = a_{i_s} \neq 0$ .

Из того, что  $S_i(x)$  — биективны, получаем, что найдется такое  $\tilde{x}_{i_2} \neq x_{i_2}^0$ , что  $f_{i_1}(x_1^0, \dots, \tilde{x}_{i_2}, \dots, x_n^0) = 0$ . Аналогично подбираем  $\tilde{x}_{i_1}, \dots, \tilde{x}_{i_s}$ .

Рассмотрим  $\tilde{x} : (x_1^0, \dots, \tilde{x}_{i_1}, \dots, \tilde{x}_{i_s}, \dots, x_n^0)$ . Для этого набора будет выполнено:  $f_{i_1}(\tilde{x}) = \dots = f_{i_s}(\tilde{x}) = 0$ .

Следовательно,  $x^0 \neq \tilde{x}$ , но для всех  $j$ , таких, что  $x_j^0 \neq \tilde{x}_j$  будет верно  $f_j(x^0) \neq f_j(\tilde{x})$ , то есть условие правильности не выполняется. Теорема доказана.

Автор выражает благодарность своему научному руководителю к.ф.-м.н. Носову В. А. за постановку задачи и участие в обсуждении работы.

### Список литературы

- [1] Носов В. А. Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. — 1998. Т. 3, вып. 3–4. — С. 269–280.
- [2] Носов В. А. О построении классов латинских квадратов в булевой базе данных // Интеллектуальные системы. — 1999. Т. 4, вып. 3–4. — С. 307–320.
- [3] Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. — 2004. Т. 8, вып. 1–4. С. 517–528.
- [4] Носов В. А., Панкратьев А. Е. Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. — 2006. Т. 12, № 3. — С. 65–71.
- [5] Носов В. А., Панкратьев А. Е. О функциональном задании латинских квадратов // Интеллектуальные системы. — 2008. Т. 12, вып. 1–4. — С. 317–332.