Латинские квадраты над абелевыми группами

В. А. НОСОВ, А. Е. ПАНКРАТЬЕВ
Московский государственный университет им. М. В. Ломоносова

УДК 519.1+512.5

Ключевые слова: латинский квадрат, абелева группа, регулярное семейство функций.

Аннотация

В данной работе обобщается конструкция параметрического семейства латинских квадратов, предложенная ранее для булевой и векторной баз данных, на случай абелевых групп. Даются критерии реализуемости данной конструкции и приводятся некоторые классификационные результаты.

Abstract

V. A. Nosov, A. E. Pankratiev, Latin squares over Abelian groups, Fundamentalnaya i prikladnaya matematika, vol. 12 (2006), no. 3, pp. 65—71.

In this paper, parametric families of Latin squares over Boolean vectors and prime fields constructed earlier are generalized to the case of Abelian groups. Some criteria for realizability of this construction are presented. Some classification results are also given.

Латинские квадраты широко используются в кодировании, шифровании и в планировании эксперимента. В своей фундаментальной работе [4], посвящённой теоретическим основам связи в секретных системах, К. Шеннон показал, что шифры, построенные на латинских квадратах, обладают так называемым свойством совершенной секретности.

Для практической применимости в системах информационной безопасности требуются латинские квадраты достаточно больших размеров (порядка $10\ 000 \times 10\ 000$). Такие квадраты невозможно хранить в памяти поэлементно, для них необходимы аналитические методы задания. На практике латинские квадраты, как правило, задаются функцией от двух переменных, определяющей значение элемента квадрата по его координатам (номеру строки и столбца). В таком случае не требуется хранить в памяти весь квадрат целиком, достаточно хранить соответствующую функцию.

В данной работе мы рассматриваем прямое произведение нескольких (n) копий конечной абелевой группы G:

$$H = G^n = \underbrace{G \times G \times \ldots \times G}_{n}.$$

Фундаментальная и прикладная математика, 2006, том 12, № 3, с. 65—71.

Над группой H зададим латинский квадрат L порядка $|H| \times |H|$ следующим образом. Сначала «проиндексируем» строки и столбцы квадрата L элементами группы H. Пусть $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ — элементы группы H. Элемент $L(x, y) = (z_1, z_2, \ldots, z_n)$ квадрата L, находящийся на пересечении строки x и столбца y, определим формулами

$$\begin{aligned} z_1 &= x_1 + y_1 + f_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)), \\ z_2 &= x_2 + y_2 + f_2(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)), \\ &\vdots \\ z_n &= x_n + y_n + f_n(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)). \end{aligned} \tag{1}$$

Здесь $p_1, p_2, \ldots, p_n$ — функции из $G \times G$ в G, $f_1, f_2, \ldots, f_n$ являются функциями из G^n в G.

Нетрудно видеть, что матрица, задаваемая формулами (1), не всегда является латинским квадратом. К примеру, набор функций $f_1 = -y_1$, $f_2 = -y_2, \ldots$, $f_n = -y_n$ определяет квадрат с одинаковыми столбцами. Приведём условия на функции $f_1, f_2, \ldots, f_n$, при которых матрица $L = L(x, y)$, определённая формулами (1), является латинским квадратом при любых функциях $p_1, p_2, \ldots, p_n$.

Будем говорить, что функции $f_1, f_2, \ldots, f_n$ от переменных $p_1, p_2, \ldots, p_n$ образуют *правильное* семейство [1, 2], если для любых различных наборов $p' = (p'_1, p'_2, \ldots, p'_n)$ и $p'' = (p''_1, p''_2, \ldots, p''_n)$ найдётся индекс α, $1 \leqslant \alpha \leqslant n$, такой что $p'_\alpha \neq p''_\alpha$ и $f_\alpha(p') = f_\alpha(p'')$.

Проиллюстрируем введённое понятие замечаниями и примерами.

Замечание 1. Если функции $f_1, \ldots, f_n$ от переменных $p_1, \ldots, p_n$ образуют правильное семейство, то для любых констант $a_1, a_2, \ldots, a_n$ функции $g_1 = f_1(p_1, \ldots, p_n) + a_1, \ldots$, $g_n = f_n(p_1, \ldots, p_n) + a_n$ также образуют правильное семейство.

Замечание 2. Если функции $f_1, \ldots, f_n$ от переменных $p_1, \ldots, p_n$ образуют правильное семейство, то ни для какого α, $1 \leqslant \alpha \leqslant n$, функция f_α не может существенно зависеть от переменной p_α. В самом деле, в противном случае можно было бы найти наборы $p' = (p'_1, p'_2, \ldots, p'_n)$ и $p'' = (p''_1, p''_2, \ldots, p''_n)$, отличающиеся только компонентой с номером α и такие, что $f_\alpha(p') \neq f_\alpha(p'')$. Это означало бы, что семейство функций $(f_1, \ldots, f_n)$ не является правильным.

Замечание 3. Правильность семейства функций $(f_1, \ldots, f_n)$ от переменных $p_1, \ldots, p_n$ инвариантна относительно перестановок индексов в том смысле, что для любой перестановки $\pi \in S_n$ семейство функций $(g_1 = f_{\pi(1)}, g_2 = f_{\pi(2)}, \ldots, g_n = f_{\pi(n)})$ от переменных $s_1 = p_{\pi(1)}$, $s_2 = p_{\pi(2)}, \ldots$, $s_n = p_{\pi(n)}$ также является правильным.

Пример 1. Постоянные функции, очевидно, образуют правильное семейство.

Пример 2. Возьмём $f_1 = \mathrm{const}$, $f_2 = f_2(p_1)$, $f_3 = f_3(p_1, p_2), \ldots$, $f_n = f_n(p_1, \ldots, p_{n-1})$. Тогда эти функции, рассматриваемые как функции от n переменных $p_1, \ldots, p_n$, образуют правильное семейство. Такие семейства функций называются *треугольными*.

Можно показать, что класс правильных семейств функций содержит семейства, не приводимые к треугольному виду. Число правильных семейств функций (с точностью до перестановки индексов) остаётся неизвестным даже для малых размерностей.

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

Доказательство. Докажем достаточность. Предположим, что функции $f_1, f_2, \ldots, f_n$ образуют правильное семейство, и рассмотрим два элемента $z' = z'(x, y')$ и $z'' = z''(x, y'')$ в одной строке матрицы, заданной формулами (1):

$$\begin{aligned} z'_1 &= x_1 + y'_1 + f_1(p_1(x_1, y'_1), \ldots, p_n(x_n, y'_n)),\\ z'_2 &= x_2 + y'_2 + f_2(p_1(x_1, y'_1), \ldots, p_n(x_n, y'_n)),\\ &\vdots\\ z'_n &= x_n + y'_n + f_n(p_1(x_1, y'_1), \ldots, p_n(x_n, y'_n)), \end{aligned} \tag{2}$$

$$\begin{aligned} z''_1 &= x_1 + y''_1 + f_1(p_1(x_1, y''_1), \ldots, p_n(x_n, y''_n)),\\ z''_2 &= x_2 + y''_2 + f_2(p_1(x_1, y''_1), \ldots, p_n(x_n, y''_n)),\\ &\vdots\\ z''_n &= x_n + y''_n + f_n(p_1(x_1, y''_1), \ldots, p_n(x_n, y''_n)). \end{aligned} \tag{3}$$

Во-первых, если $p_k(x_k, y'_k) = p_k(x_k, y''_k)$ при всех k, $1 \leqslant k \leqslant n$, то каждая функция f_j, $1 \leqslant j \leqslant n$, принимает одинаковые значения на парах (x, y') и (x, y''). Это означает, что все правые части соответствующих равенств в системах (2) и (3) совпадают с точностью до y-компоненты. Но поскольку элементы y' и y'' различны (так как задают различные столбцы квадрата), то они отличаются по некоторой компоненте $y'_\alpha \neq y''_\alpha$, и следовательно, компоненты z'_α и z''_α также различны. Таким образом, все элементы в любой строке квадрата (1) различны. Абсолютно те же рассуждения верны и для любого столбца. Тем самым показано, что матрица (1) является латинским квадратом.

По определению правильного семейства для любых различных наборов $p' = p(x, y')$ и $p'' = p(x, y'')$ всегда найдётся индекс α, $1 \leqslant \alpha \leqslant n$, такой что $p'_\alpha \neq p''_\alpha$ и $f_\alpha(p') = f_\alpha(p'')$. Тогда правые части равенств с индексом α в системах (2) и (3) содержат один и тот же элемент x_α и одно и то же значение f_α. Однако из неравенства $p'_\alpha = p_\alpha(x_\alpha, y'_\alpha) \neq p''_\alpha = p_\alpha(x_\alpha, y''_\alpha)$ следует, что $y'_\alpha \neq y''_\alpha$. Отсюда получаем, что компоненты z'_α и z''_α различны. Таким образом, и в этом случае матрица (1) является латинским квадратом.

Докажем необходимость. Допустим, что семейство функций $(f_1, f_2, \ldots, f_n)$ не является правильным. Тогда найдутся два набора $t' = (t'_1, \ldots, t'_n)$ и $t'' = (t''_1, \ldots, t''_n)$ со свойством, что для любого $\alpha \in \overline{1, n}$ из неравенства $t'_\alpha \neq t''_\alpha$ следует неравенство $f_\alpha(t') \neq f_\alpha(t'')$.

Зафиксируем любые элементы $z = (z_1, \ldots, z_n)$ и $x = (x_1, \ldots, x_n)$. Так как L по условию является латинским квадратом, найдутся элементы $y' = (y'_1, \ldots, y'_n)$ и $y'' = (y''_1, \ldots, y''_n)$, такие что $z = x + y' + f(t')$ и $z = x + y'' + f(t'')$. Запишем эти равенства покомпонентно:

$$\begin{aligned} z_1 &= x_1 + y'_1 + f_1(t'_1, \ldots, t'_n), & z_1 &= x_1 + y''_1 + f_1(t''_1, \ldots, t''_n), \\ z_2 &= x_2 + y'_2 + f_2(t'_1, \ldots, t'_n), & z_2 &= x_2 + y''_2 + f_2(t''_1, \ldots, t''_n), \\ &\vdots & &\vdots \\ z_n &= x_n + y'_n + f_n(t'_1, \ldots, t'_n), & z_n &= x_n + y''_n + f_n(t''_1, \ldots, t''_n). \end{aligned} \tag{4}$$

Теперь выберем любые функции $p_1 = p_1(x_1, y_1), \ldots, p_n = p_n(x_n, y_n)$, удовлетворяющие условиям

$$\begin{aligned} p_1(x_1, y'_1) &= t'_1, & p_1(x_1, y''_1) &= t''_1, \\ p_2(x_2, y'_2) &= t'_2, & p_2(x_2, y''_2) &= t''_2, \\ &\vdots & &\vdots \\ p_n(x_n, y'_n) &= t'_n, & p_n(x_n, y''_n) &= t''_n. \end{aligned}$$

Такой выбор невозможен только в том случае, если для некоторого индекса α имеет место равенство $y'_\alpha = y''_\alpha$, тогда как $t'_\alpha \neq t''_\alpha$. Но в силу выбора наборов t' и t'' из неравенства $t'_\alpha \neq t''_\alpha$ следует неравенство $f_\alpha(t') \neq f_\alpha(t'')$, которое согласно условиям (4) несовместимо с равенством $y'_\alpha = y''_\alpha$.

Наконец, выбрав функции $p_1, \ldots, p_n$ с указанными свойствами, мы приходим к противоречию с тем, что L является латинским квадратом, поскольку элемент z дважды встречается в строке x: на пересечении со столбцами y' и y''. □

Теорема 1 является обобщением аналогичных результатов, полученных в [1, 2] для случаев булевских функций и векторов над простым полем (т. е. соответственно для прямых степеней групп $\mathbb{Z}_2$ и $\mathbb{Z}_p$).

Теорема 2. *Функции $f_1, f_2, \ldots, f_n$ образуют правильное семейство тогда и только тогда, когда для любого набора функций $\psi_1, \psi_2, \ldots, \psi_n$ (здесь $\psi_i \colon G \to G$) семейство функций $(x_1 + \psi_1(f_1(x)), x_2 + \psi_2(f_2(x)), \ldots, x_n + \psi_n(f_n(x)))$ является регулярным (т. е. определяет биективное отображение $G^n \to G^n$).*

Доказательство. Докажем необходимость. Пусть семейство функций $(f_1, f_2, \ldots, f_n)$ является правильным. Это означает, что для любых различных наборов $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ найдётся индекс $\alpha \in \overline{1, n}$, такой что $x'_\alpha \neq x''_\alpha$ и $f_\alpha(x') = f_\alpha(x'')$.

Зафиксируем произвольные функции $\psi_1, \psi_2, \ldots, \psi_n$ и рассмотрим наборы $x'_1 + \psi_1(f_1(x')), \ldots, x'_n + \psi_n(f_n(x'))$ и $x''_1 + \psi_1(f_1(x'')), \ldots, x''_n + \psi_n(f_n(x''))$. Нетрудно видеть, что $x'_\alpha + \psi_\alpha(f_\alpha(x')) \neq x''_\alpha + \psi_\alpha(f_\alpha(x''))$, поскольку в силу

выбора α выполнены равенство $f_\alpha(x') = f_\alpha(x'')$ (и, следовательно, $\psi_\alpha(f_\alpha(x')) = \psi_\alpha(f_\alpha(x''))$) и неравенство $x'_\alpha \neq x''_\alpha$. Тем самым доказана регулярность семейства $(x_1+\psi_1(f_1(x)), x_2+\psi_2(f_2(x)), \ldots, x_n+\psi_n(f_n(x)))$ для любых заданных функций $\psi_1, \psi_2, \ldots, \psi_n$.

Докажем достаточность. Предположим, что семейство $(f_1, f_2, \ldots, f_n)$ не является правильным. Тогда существуют различные наборы $x' \neq x''$, такие что для любого индекса $\alpha \in \overline{1,n}$ из неравенства $x'_\alpha \neq x''_\alpha$ следует неравенство $f_\alpha(x') \neq f_\alpha(x'')$.

Выберем функции $\psi_1, \psi_2, \ldots, \psi_n$ так, чтобы они удовлетворяли свойствам

$$\begin{aligned} x'_1 + \psi_1(f_1(x')) &= x''_1 + \psi_1(f_1(x'')),\\ x'_2 + \psi_2(f_2(x')) &= x''_2 + \psi_2(f_2(x'')),\\ &\vdots\\ x'_n + \psi_n(f_n(x')) &= x''_n + \psi_n(f_n(x'')) \end{aligned}$$

(такой выбор, очевидно, всегда возможен). Тогда каждая функция из семейства $(x_1 + \psi_1(f_1(x)), x_2 + \psi_2(f_2(x)), \ldots, x_n + \psi_n(f_n(x)))$ принимает одинаковые значения на различных наборах $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$, что противоречит регулярности этого семейства. Теорема доказана. □

Ряд классификационных теорем и результатов о построении классов правильных семейств функций [1, 2] легко переносятся на случай абелевых групп. В частности, справедливо следующее утверждение.

Теорема 3. *Пусть $F = (f_1, f_2, \ldots, f_n)$ — семейство линейных функций $G^n \to G$ вида*

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= a_{11}x_1 + \ldots + a_{1n}x_n,\\ f_2(x_1, \ldots, x_n) &= a_{21}x_1 + \ldots + a_{2n}x_n,\\ &\vdots\\ f_n(x_1, \ldots, x_n) &= a_{n1}x_1 + \ldots + a_{nn}x_n, \end{aligned}$$

где коэффициенты a_{ij} приведены по модулю экспоненты группы G. Определим ориентированный граф $\Gamma_F = (V, E)$ на множестве вершин $V = \{1, 2, \ldots, n\}$ по правилу $(i, j) \in E \iff a_{ji} \neq 0$. Тогда семейство функций $F = (f_1, f_2, \ldots, f_n)$ является правильным, если и только если граф Γ_F не содержит циклов.

Доказательство. Докажем необходимость. Допустим, что граф Γ_F содержит (ориентированные) циклы и рассмотрим кратчайший цикл $i_1 i_2 \ldots i_k$. Если $k = 1$, то цикл состоит из единственного ребра, начинающегося и заканчивающегося в одной и той же вершине i_1 (ориентированная петля). Это означает, что функция f_{i_1} существенным образом зависит от переменной x_{i_1}, что противоречит правильности семейства F в силу замечания 2.

Предположим теперь, что цикл $i_1 i_2 \ldots i_k$ проходит по крайней мере через две вершины. Обозначим соответствующее подмножество индексов через

$I = \{i_1, i_2, \ldots, i_k\}$. Тогда ни один из коэффициентов $a_{i_2 i_1}, a_{i_3 i_2}, \ldots, a_{i_1 i_k}$ не равен нулю. Заметим, что для любого $i \in I$ в точности один коэффициент $\{a_{ij}\}$, $j \in I$, не равен нулю. В самом деле, если $k = 2$, то наличие двух ненулевых коэффициентов a_{ij_1} и a_{ij_2} ($j_1 \neq j_2$), где $i, j_1, j_2 \in I$, означает, что один из них лежит на диагонали, и мы приходим к случаю петли, рассмотренному выше. В случае же $k \geqslant 3$ допустим, что (с точностью до циклической перестановки) существует индекс s, $1 \leqslant s \leqslant k-2$, такой что $a_{i_k i_s} \neq 0$. Тогда граф Γ_F содержит ребро $(i_s i_k)$ и, следовательно, имеется цикл $i_1 i_2 \ldots i_s i_k$, который является более коротким, чем цикл $i_1 i_2 \ldots i_{k-1} i_k$. Это противоречит выбору последнего как кратчайшего цикла в графе Γ_F.

Теперь возьмём $x' = (x'_1, \ldots, x'_n) = (0, \ldots, 0)$ и выберем $x'' = (x''_1, \ldots, x''_n)$ так, что $x''_j = 0$ при $j \notin I$ и $a_{i_2 i_1} x_1 \neq 0$, $a_{i_3 i_2} x_2 \neq 0, \ldots$, $a_{i_1 i_k} x_k \neq 0$ (здесь 0 обозначает тождественный элемент группы G). Тогда для любого индекса $i \in I$ имеем $x'_i \neq x''_i$ и $f_i(x'') \neq 0$, поскольку $f_i(x'') = a_{i1} x''_1 + a_{i2} x''_2 + \ldots + a_{in} x''_n$, где в точности одно слагаемое не равно нулю. В то же время $f_i(x') = 0$. Это противоречит определению правильного семейства функций.

Докажем достаточность. Допустим, что семейство $F = (f_1, f_2, \ldots, f_n)$ линейных функций не является правильным. Тогда найдутся различные наборы $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ со свойством, что для любого индекса $\alpha \in \overline{1,n}$ из неравенства $x'_\alpha \neq x''_\alpha$ следует неравенство $f_\alpha(x') \neq f_\alpha(x'')$.

Рассмотрим множество $I = \{i_1, i_2, \ldots, i_k\}$ всех индексов, по которым отличаются наборы x' и x''. Обозначим $s_1 = i_1$. Поскольку $f_{i_1}(x') \neq f_{i_1}(x'')$, функция f_{i_1} существенно зависит по крайней мере от одной из переменных $\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$. Это означает, что по крайней мере один из коэффициентов $a_{i_1 i_1}, a_{i_1 i_2}, \ldots, a_{i_1 i_k}$ отличен от нуля. Пусть этот коэффициент $a_{i_1 i_j}$. Обозначим $s_2 = i_j$.

Тогда имеем $a_{s_1 s_2} \neq 0$. Точно так же находим индекс $s_3 \in I$, для которого $a_{s_2 s_3} \neq 0$. Продолжая этот процесс, получаем последовательность индексов $s_1, s_2, \ldots$, принадлежащих множеству I и таких, что $a_{s_j s_{j+1}} \neq 0$. Но так как множество I содержит только k элементов, нам неминуемо попадётся индекс s_q, равный некоторому индексу s_p, полученному ранее ($p < q$). Это даёт цикл $s_p, s_{p+1}, \ldots, s_{q-1}$ в графе Γ_F. Теорема доказана. □

Замечание 4. В силу замечания 1 функции $f_1, f_2, \ldots, f_n$ в условии теоремы 3 могут также содержать нетривиальные свободные члены.

Литература

[1] Носов В. А. О построении классов латинских квадратов в булевой базе данных // Интеллект. сист. — 1999. — Т. 4, вып. 3—4. — С. 307—320.

[2] Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллект. сист. — 2004. — Т. 8, вып. 1—4. — С. 517—528.

[3] Носов В. А., Панкратьев А. Е. Латинские квадраты над абелевыми группами // Математические методы и приложения. Труды XIV математических чтений МГСУ (28—31 января 2005 г.). — М., 2005. — С. 72—76.

[4] Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. — М., 1963. — С. 333—369.

[5] Dénes J., Keedwell A. Latin Squares and Their Applications. — Budapest, 1974.