Некоторые свойства перестановочной конструкции для параметрического задания квазигрупп

Пивень Н.А.

В работе исследуются свойства так называемой перестановочной конструкции, введенной ранее. Выясняется, что конструкция несколько избыточна, но в результате ее улучшения, она оказывается инъективной для случая линейных правильных семейств булевых функций, и, возможно, инъективной в общем.

Ключевые слова: квазигруппы, правильные семейства булевых функций, латинские квадраты, параметрическое задание

1. Введение

В наши дни разрабатываются различные способы защиты информации, использующие латинские квадраты. Это связано в частности с тем, что К. Шеннон показал, что шифры, построенные на латинских квадратах, обладают свойством "совершенной секретности" ([1]). Латинские квадраты естественным образом связаны с квазигруппами, а именно, в случае конечных квазигрупп, квазигрупповая операция может быть задана таблицей Кэли, являющейся латинским квадратом. Примеры использования квазигрупп для решения различных задач криптографии можно найти в работах [2, 3, 4, 5].

В. А. Носовым в работе [6] был предложен способ задания больших семейств латинских квадратов с помощью так называемых правильных семейств функций. В работе [7] предлагается усиление конструкции В. А. Носова, названное перестановочной конструкцией. При ее использовании удается получить большее количество различных латинских квадратов из того же набора правильных семейств, и более того, на практике было обнаружено, что больший процент из полученных с ее помощью квадратов обладает криптографически важным свойством полиномиальной полноты.

Дальнейшее изложение имеет следующую структуру. В разделе 2 даются основные определения. В разделе 3 анализируются избыточность текущей перестановочной конструкции. В разделе 4 вводится перестановочная конструкция с устранением обнаруженной избыточности и доказывается инъективность полученной конструкции для линейных правильных семейств.

2. Основные понятия

Определение 1. Конечной квазигруппой (Q, f_Q) называется множество Q, $|Q| < \infty$, на котором определена бинарная операция f_Q такая, что для любых элементов $a, b \in Q$ уравнения $f_Q(a, x) = b$ и $f_Q(y, a) = b$ однозначно разрешимы в Q.

В дальнейшем мы будем опускать слово "конечная".

Определение 2. Латинским квадратом порядка n называется матрица размера $n \times n$, заполненная элементами некоторого n–элементного множества таким образом, что в каждой её строке и в каждом столбце все элементы различны.

Квазигрупповую операцию можно задавать табличным способом: для множества элементов $\{q_1, \dots, q_m\}$, составляющих квазигруппу Q, выписывается квадратная таблица $m \times m$, такая что на пересечении i–ой строки и j–го столбца стоит $f_Q(q_i,\, q_j)$. Заметим, что построенная таким образом таблица, в связи с существованием и единственностью решения уравнений $f_Q(a, x) = b$ и $f_Q(y, a) = b$, является латинским квадратом, который мы и называем латинским квадратом, связанным с квазигруппой.

Определение 3. Семейство булевых функций $\mathrm{F}=\{f_i\}_{i=1}^n$, $f_i = f_i(x_1, \dots, x_n)$, называется правильным, если для любых различных значений аргументов $x' = (x'_1, \dots, x'_n)$ и $x'' = (x''_1, \dots, x''_n)$ найдется такой индекс $\alpha \in \{1, \dots, n\}$, что $x'_\alpha \neq x''_\alpha$, $f_\alpha(x'_1, \dots, x'_n) = f_\alpha(x''_1, \dots, x''_n)$

Правильные семейства функций были введены В. А. Носовым в работе [6] для построения латинских квадратов порядка 2^n. Занумеруем элементы множества Q, $|Q| = 2^n$, числами от 0 до $2^n - 1$. Таким образом, каждому элементу $a \in Q$ можно сопоставить n–битный вектор $(a_1, \dots, a_n)$, задающий двоичную запись номера. В результате квазигрупповая операция f_Q может быть представлена в векторной форме: записи

$z = f_Q(x, y)$ и

$$\begin{aligned} z_1 &= f_Q^1(x_1, \ldots, x_n, y_1, \ldots, y_n), \\ &\vdots \\ z_n &= f_Q^n(x_1, \ldots, x_n, y_1, \ldots, y_n), \end{aligned}$$

где $f_Q^1, \ldots, f_Q^n$ — булевы функции, являющиеся компонентами вектор–функции, порожденной f_Q, эквивалентны.

Пусть $f_1, \ldots, f_n$ — булевы функции от n переменных, $\pi_1, \ldots, \pi_n$ — булевы функции от двух переменных. Рассмотрим следующее семейство функций от $2n$ переменных:

$$\begin{aligned} g_1 &= x_1 \oplus y_1 \oplus f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ &\vdots \\ g_n &= x_n \oplus y_n \oplus f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \end{aligned} \tag{1}$$

где операция $\oplus$ означает сложение по модулю 2. В работе [6] показано, что семейство $G = \{g_1, \ldots, g_n\}$ задает латинский квадрат для любых функций $\pi_1, \ldots, \pi_n$ тогда и только тогда, когда семейство $F = \{f_1, \ldots, f_n\}$ правильное.

В работе [7] эта конструкция была усилена следующим образом. Пусть $n \in \mathbb{N}$, $F = \{f_1, \ldots, f_n\}$ — правильное семейство булевых функций, $\alpha, \beta, \gamma \in S_n$ — перестановки на множестве $\{1, \ldots, n\}$. Наложим перестановки α, β, γ на индексы переменных x и y и номера функций g в представлении (1):

$$\begin{aligned} g_{\gamma(1)} &= x_{\alpha(1)} \oplus y_{\beta(1)} \oplus f_1(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})), \\ &\vdots \\ g_{\gamma(n)} &= x_{\alpha(n)} \oplus y_{\beta(n)} \oplus f_n(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})). \end{aligned} \tag{2}$$

Это и было названо перестановочной конструкцией. Заметим, что исходное задание (1) получается из формул (2) при выборе тождественных перестановок в качестве α, β и γ. Также в работе [7] было показано, что после применения перестановочной конструкции к этим равенствам, семейство $G' = \{g_{\gamma(1)}, \ldots, g_{\gamma(n)}\}$ все еще задает латинский квадрат.

3. Избыточность перестановочной конструкции

В ходе практического применения введенной перестановочной конструкции было обнаружено, что, начиная с какого–то момента перебора перестановок, новых латинских квадратов уже не появлялось, что говорит об избыточности перестановочной конструкции. Для доказательства теоремы о ее избыточности, нам потребуется следующая лемма.

Лемма 1. *При согласованной перестановке индексов функций и переменных правильного семейства, полученное в результате семейство также является правильным.*

Доказательство. Предположим, мы применили перестановку α к индексам функций и переменных правильного семейства F и получили семейство функций F', не являющееся правильным. Тогда из определения правильного семейства, $\exists$ различные $y', y'' : \forall d \in 1 \dots n$ выполнено $y'_d \neq y''_d \implies f'_d(y') \neq f'_d(y'')$.
Пусть D – множество индексов, в которых отличаются y' и y'', тогда это можно переписать как $\exists$ различные $y', y'' : \forall d \in D\ f'_d(y') \neq f'_d(y'')$. (3)
Вернемся теперь к правильному семейству F. Опять же по определению правильного семейства, $\forall$ различных $x', x''\ \exists i \in 1 \dots n : x'_i \neq x''_i$ и $f_i(x') = f_i(x'')$ возьмем за эти x' и x'' выражения $\alpha^{-1}(y')$ и $\alpha^{-1}(y'')$ соответственно. Они различны, так как α перестановка, тогда $\alpha^{-1}(i) \in D$ и $f'_{\alpha^{-1}(i)}(y') = f'_{\alpha^{-1}(i)}(y'')$, что противоречит выражению (3) $\square$

Перейдем теперь к самой теореме.

Теорема 1. *Любой латинский квадрат, получаемый применением только перестановки γ в перестановочной конструкции, можно получить применением перестановок α, β, взятием другого правильного семейства и других функций π.*

Доказательство. Достаточно доказать утверждение для транспозиции. Без ограничения общности, возьмем транспозицию индексов 1 и 2. Таким образом,

$$\begin{aligned} g'_1 = g_2 &= x_2 \oplus y_2 \oplus f_2(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n)) \\ g'_2 = g_1 &= x_1 \oplus y_1 \oplus f_1(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n)) \\ &\vdots \\ g'_n = g_n &= x_n \oplus y_n \oplus f_n(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n)), \end{aligned}$$

Теперь вместо транспозиции по индексам g применим транспозицию по индексам 1 и 2 для x и y, возьмем правильное семейство, полученное согласованной перестановкой 1 и 2 индекса (такое правильное семейство существует согласно лемме) и возьмем функции π', такие, что $\pi'_1 = \pi_2$ и

$\pi'_2 = \pi_1$, остальные без изменений. Получим:

$$\begin{array}{rcl} g''_1 & = & x_2 \oplus y_2 \oplus f'_1(\pi'_1(x_2, y_2), \pi'_2(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ g''_2 & = & x_1 \oplus y_1 \oplus f'_2(\pi'_1(x_2, y_2), \pi'_2(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ & \vdots & \\ g''_n & = & x_n \oplus y_n \oplus f'_n(\pi'_1(x_2, y_2), \pi'_2(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \end{array}$$

Запишем это выражение через изначальные функции и получим:

$$\begin{array}{rcl} g''_1 & = & x_2 \oplus y_2 \oplus f_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ g''_2 & = & x_1 \oplus y_1 \oplus f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ & \vdots & \\ g''_n & = & x_n \oplus y_n \oplus f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \end{array}$$

Отсюда несложно заметить, что g'' совпадает с g', что завершает доказательство. □

4. Улучшение перестановочной конструкции

Для доказательства теоремы этого раздела нам потребуется утверждение из [8] о том, что граф существенной зависимости правильного семейства линейных функций не содержит циклов. Графом существенной зависимости семейства линейных функций F вида

$$\begin{array}{rcl} f_1 & = & a_{11}x_1 + \ldots + a_{1n}x_n; \\ & \vdots & \\ f_n & = & a_{n1}x_1 + \ldots + a_{nn}x_n \end{array}$$

назовем ориентированный граф $\Gamma_F(V, E)$ на множестве вершин $V = (1, .., n)$, составляемый по правилу $(i, j) \in E \iff a_{ji} \neq 0$.

В прошлом разделе мы показали избыточность перестановочной конструкции. Заменим ее на конструкцию того же вида, но без применения перестановки γ (ну или просто скажем, что перестановка γ должна быть тождественной, что одно и то же). Перестановочная конструкция такого вида оказалась инъективной для линейных правильных семейств, а именно, верна следующая теорема.

Теорема 2. *Пусть Q' и Q'' – два различных латинских квадрата одного порядка, порожденных линейными правильными семействами методом*

Носова. $S' = (\alpha', \beta', id)$ *и* $S'' = (\alpha'', \beta'', id)$ *– произвольные перестановочные конструкции с* $\gamma = id$*, где* id *– тождественная перестановка. Тогда* $S'(Q') \neq S''(Q'')$

Доказательство. Предположим, что различные квадраты Q' и Q'' перешли в один и тот же квадрат Q с помощью перестановок α', β' и α'', β'' соответственно. Тогда Q' можно перевести в Q'' соответствующей композицией этих перестановок. То есть Q' переходит в Q'' при применении неких перестановок α и β, хотя бы одна из которых нетождественна (Иначе эти квадраты одинаковые. Пусть нетождественна α), к индексам x и y соответственно. Запишем это в виде явных формул (одно из уравнений) учитывая, что функции из F линейны:

$x_1 \oplus y_1 \oplus a_{11}\pi_1(x_1, y_1) \oplus \ldots \oplus a_{1n}\pi_n(x_n, y_n) = x_{\alpha(1)} \oplus y_{\beta(1)} \oplus a'_{11}\pi'_1(x_{\alpha(1)}, y_{\beta(1)}) \oplus \ldots \oplus a'_{1n}\pi'_n(x_{\alpha(n)}, y_{\beta(n)})$

остальные уравнения аналогичны для всех индексов от 2 до n. Рассмотрим равенство, где в левой части первым слагаемым является x_1, то есть выписанное. оно верно для любых наборов x и y. Подставим все нули, кроме $x_{\alpha(1)}$ и соберем все константы в одну. (учитывая, что a_{11} и a'_{11} нулевые из правильности семейств – иначе бы был цикл–петля в графе существенной зависимости). Получим:

$a_{1\alpha(1)}\pi_{\alpha(1)}(x_{\alpha(1)}, 0) = x_{\alpha(1)} \oplus c$

Распишем функцию π как многочлен от 2 переменных с учетом второго аргумента–нуля и занесем константу так же в с:

$a_{1\alpha(1)}ax_{\alpha(1)} = x_{\alpha(1)} \oplus c_0$

Теперь если мы подставим сюда $x_{\alpha(1)} = 0$, то получим, что $c_0 = 0$, а исходя из этого, $a = a_{1\alpha(1)} = 1$

Т.е. в терминах графа существенной зависимости, в нем есть ребро $(\alpha(1), 1)$

Далее рассмотрим такое же равенство, только в котором первым слагаемым является $x_{\alpha(1)}$ и аналогичным образом получим, что в этом графе есть ребро $(\alpha(\alpha(1)), \alpha(1))$ и т.д.

Так как индексов конечное количество, рано или поздно один из них повторится, что означает, что в графе существенной зависимости есть цикл, что противоречит правильности семейства.

□

Из этой теоремы и количества перестановок порядка n очевидным образом получаем

Следствие 1. *Пусть* $(L_1, \ldots, L_k)$ *– множество латинских квадратов порядка* 2^n*, порожденных линейными правильными семействами буле-*

вых функций. Тогда перестановочная конструкция порождает из этого множества $n!^2k$ *попарно различных латинских квадрата.*

Замечание 1. *Во время практической работы с перестановочной конструкцией, было замечено, что это следствие верно вообще говоря для любых семейств булевых функций в случае квадратов порядка 8. В перспективе планируется доказать это утверждение для квадратов произвольного порядка.*

5. Заключение

В работе проведено исследование так называемой перестановочной конструкции, найдена избыточность в ее определении, в определение внесена корректировка для устранения обнаруженной избыточности и доказано, что для нового определения в случае линейности булевых функций, используемых для построения латинских квадратов, избыточность отсутствует.

Список литературы

[1] C. Shannon, "Communication theory of secrecy systems", *Bell System Techn. J.*, **28**:4 (1949), 656–715; имеется перевод: К. Шеннон, "Теория связи в секретных системах", *Работы по теории информации и кибернетике*, Издательство иностранной литературы, Москва, 1963, 333–369.

[2] М.М. Глухов, "О применениях квазигрупп в криптографии", *Прикладная дискретная математика*, 2008, №2, 28–32.

[3] S. Markovski, D. Gligoroski, V. Bakeva, "Quasigroup String Processing: Part 1", *Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci.*, **XX**:1–2 (1999), 13–28.

[4] S. Markovski, V. Kusacatov, "Quasigroup String Processing: Part 2", *Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci.*, **XXI**:1–2 (2000), 15–32.

[5] V. Shcherbacov, "Quasigroup based crypto-algorithms", arXiv: 1201.3016v1.

[6] В.А. Носов, "О построении классов латинских квадратов в булевой базе данных", *Интеллектуальные системы*, **4**:3–4 (1999), 307–320.

[7] Н.А. Пивень, "Исследование квазигрупп, получаемых с помощью правильных семейств булевых функций порядка 2", *Интеллектуальные системы. Теория и приложения*, **22**:1 (2018), 21–35.

[8] В. А. Носов, А. Е. Панкратьев, "Латинские квадраты над абелевыми группами", *Фундамент. и прикл. матем.*, **12**:3 (2006), 65–71; *J. Math. Sci.*, **149**:3 (2008), 1230–1234.

Some properties of permutation construction for parametric assignment of quasigroups

Piven N.A.

We analyse so–called permutation construction, introduced before. It turns out, that it's redundant, so we propose an improvement, which makes it injective for linear functions and possibly injective without conditions

Keywords: Quasigroup, Latin square, parametric assignment, proper families of functions