

Тотально парастрофно-ортогональные квазигруппы и полные графы

Г. Б. БЕЛЯВСКАЯ

*Институт математики и информатики
АН Республики Молдова
e-mail: gbell@rambler.ru*

Т. В. ПОПОВИЧ

*Институт математики и информатики
АН Республики Молдова
e-mail: tanea-popovici@mail.ru*

УДК 512.548+519.11+519.17

Ключевые слова: квазигруппа, латинский квадрат, Т-квазигруппа, парастрофно-ортогональная (сопряжённо-ортогональная) квазигруппа, спектр, граф.

Аннотация

В статье изучается спектр квазигрупп, все парастрофы которых различны и попарно ортогональны. Такие квазигруппы мы называем тотально парастрофно-ортогональными (или тотально сопряжённо-ортогональными) квазигруппами, кратко — totCO-квазигруппами. Каждая totCO-квазигруппа определяет полный граф K_6 сопряжённо-ортогонального латинского квадрата. Приводятся примеры totCO-квазигрупп различных порядков.

Abstract

G. B. Belyavskaya, T. V. Popovich, Totally conjugate orthogonal quasigroups and complete graphs, Fundamentalnaya i prikladnaya matematika, vol. 16 (2010), no. 8, pp. 17–26.

In this article, we study the spectrum of quasigroups all conjugates of which are distinct and pairwise orthogonal. We call such quasigroups totally conjugate orthogonal quasigroups (for brevity, totCO-quasigroups). Every totCO-quasigroup defines the complete conjugate orthogonal Latin square graph K_6 . Examples of totCO-quasigroups of different orders are given.

1. Введение

Квазигруппа — это упорядоченная пара (Q, A) , где Q — множество, а A — бинарная операция, определённая на Q и такая, что каждое из уравнений $A(a, y) = b$, $A(x, a) = b$ однозначно разрешимо для любой пары элементов a, b из Q . Известно, что мультипликативная таблица конечной квазигруппы определяет латинский квадрат и что с каждой квазигруппой (латинским квадратом)

Фундаментальная и прикладная математика, 2010, том 16, № 8, с. 17–26.

© 2010 Центр новых информационных технологий МГУ,
Издательский дом «Открытые системы»

связана система из шести (не обязательно различных) сопряжённых операций (или парастрофов) [1, 11].

Две квазигруппы (Q, A) и (Q, B) ортогональны, если система уравнений $\{A(x, y) = a, B(x, y) = b\}$ однозначно разрешима для всех элементов a, b из Q .

Множество $\Sigma = \{A_1, A_2, \dots, A_n\}$ квазигрупп, определённых на одном и том же множестве, ортогонально, если любые две квазигруппы этого множества ортогональны.

Понятие ортогональности играет важную роль в теории латинских квадратов, в теории квазигрупп и в различных приложениях, в частности в теории кодирования и криптографии. При этом значительный интерес представляют квазигруппы, ортогональные некоторым их парастрофам, и квазигруппы, два парастрофа которых ортогональны (они известны как сопряжённо-ортогональные или парастрофно-ортогональные квазигруппы).

Исследованию различных аспектов сопряжённо-ортогональных квазигрупп посвящено много статей. Напомним некоторые из них.

В [5—8, 10, 17] изучался спектр сопряжённо-ортогональных квазигрупп (латинских квадратов).

Различные тождества и комбинаторные схемы, связанные с такой ортогональностью, рассмотрены в [3, 7, 12].

В [9] рассмотрена проблема, относящаяся к спектру латинских квадратов, когда требуется, чтобы каждый парастроф латинского квадрата был ортогонален своему транспонированному (только своему транспонированному среди других пяти парастрофов) латинскому квадрату.

В [4, 16] установлены некоторые квазитожества в конечных парастрофно-ортогональных примитивных квазигруппах.

В [5], в частности, показано, что для всех n , больших 5594, за исключением, возможно, $n = 6810$, существует латинский квадрат со всеми различными и попарно ортогональными парастрофами. Доказательство основано на нескольких конструкциях попарно уравновешенных схем индекса 1. В [6] Ф. Беннет улучшил этот результат, доказав, что такие идемпотентные латинские квадраты существуют для любого порядка $n > 5074$.

В [8, 9, 14] рассматривается связь между сопряжённо-ортогональными латинскими квадратами и графами. Граф ортогональности латинских квадратов — это граф, вершинами которого являются латинские квадраты одинакового порядка из одних и тех же символов, а две вершины являются смежными тогда и только тогда, когда латинские квадраты ортогональны.

В этой статье изучается спектр квазигрупп, все парастрофы которых различны и попарно ортогональны. Такие квазигруппы мы назвали тотально сопряжённо-ортогональными, сокращённо — totCO-квазигруппами. Устанавливаются необходимые и достаточные условия, чтобы T-квазигруппа была totCO-квазигруппой (теорема 2), а в основной теореме 3 доказывается, что для любого целого числа $n \geq 11$, взаимно простого с 2, 3, 5 и 7, существует totCO-квазигруппа порядка n . В качестве следствия получаем информацию о спектре

латинских квадратов, реализующих полный граф K_6 сопряжённо-ортогонального латинского квадрата (следствие 5). Приводятся примеры totCO-квазигрупп различных порядков.

2. Предварительные сведения

Напомним некоторые необходимые понятия и результаты.

Квазигруппа (Q, A) называется Т-квазигруппой, если существуют абелева группа $(Q, +)$, её автоморфизмы φ, ψ и элемент $c \in Q$, такие что $A(x, y) = \varphi x + \psi y + c$ для любых $x, y \in Q$ [13].

Операция A вида $A(x, y) = ax + by \pmod n$, $n \geq 2$, является Т-квазигруппой тогда и только тогда, когда числа a, b по модулю n взаимно просты с n . В этом случае $\varphi = L_a$, $\psi = L_b$, где $L_a x = ax \pmod n$, $x \in Q = \{0, 1, 2, \dots, n-1\}$, являются подстановками (автоморфизмами аддитивной группы по модулю n).

С любой квазигруппой (Q, A) связана система Σ из шести (не обязательно различных) *парастрофов (сопряжённых операций)*:

$$\Sigma = \{A, A^{-1}, {}^{-1}A, {}^{-1}(A^{-1}), ({}^{-1}A)^{-1}, A^*\},$$

где

$$A(x, y) = z \iff A^{-1}(x, z) = y \iff {}^{-1}A(z, y) = x \iff A^*(y, x) = z.$$

Известно [15], что число различных парастрофов в Σ может быть 1, 2, 3 или 6.

Используя удобное обозначение В. Д. Белоусова парастрофов квазигруппы (Q, A) из [3], получаем следующую систему Σ парастрофов:

$$\Sigma = \{A, {}^rA, {}^lA, {}^{lr}A, {}^{rl}A, {}^sA\},$$

где

$${}^1A = A, \quad {}^rA = A^{-1}, \quad {}^lA = {}^{-1}A, \quad {}^{lr}A = {}^{-1}(A^{-1}), \quad {}^{rl}A = ({}^{-1}A)^{-1}, \quad {}^sA = A^*.$$

Заметим, что

$$\begin{aligned} ({}^{-1}(A^{-1}))^{-1} &= {}^{rl}A = {}^{-1}({}^{-1}A)^{-1} = {}^{lr}A = {}^sA, \\ {}^{rr}A &= {}^{ll}A = A, \quad {}^{\sigma\tau}A = {}^\sigma({}^\tau A). \end{aligned}$$

Пусть Q — конечное или бесконечное множество, A, B — операции на Q . Тогда правое и левое умножения $A \cdot B$ и $A \circ B$ Манна определяется следующим образом [2]:

$$(A \cdot B)(x, y) = A(x, B(x, y)), \quad (A \circ B)(x, y) = A(B(x, y), y).$$

Если (Q, A) и (Q, B) — квазигруппы, то операция $A \cdot B$ ($A \circ B$) всегда *обратима справа (слева)*, т. е. уравнение $(A \cdot B)(a, y) = b$ ($(A \circ B)(x, a) = b$) имеет единственное решение для любых $a, b \in Q$.

Согласно *критерию Белоусова* [2] две квазигруппы (Q, A) и (Q, B) ортогональны ($A \perp B$) тогда и только тогда, когда операция $A \cdot {}^rB$ (или $A \circ {}^lB$) является квазигруппой.

3. Тотально парастрофно-ортогональные квазигруппы

Ниже мы рассмотрим квазигруппы (Q, A) , все парастрофы которых различны и попарно ортогональны, и изучим спектр таких квазигрупп. Для этих квазигрупп множество всех парастрофов $\Sigma = \{A, {}^rA, {}^lA, {}^{lr}A, {}^{rl}A, {}^sA\}$ является ортогональным.

Определение 1. Квазигруппа (Q, A) называется тотально парастрофно-ортогональной или тотально сопряжённо-ортогональной (кратко — totCO-квазигруппой), если все её парастрофы различны и попарно ортогональны.

Очевидно, что любая totCO-квазигруппа инвариантна относительно преобразования парастрофии, т. е. если квазигруппа (Q, A) — totCO-квазигруппа, то квазигруппа $(Q, {}^\sigma A)$ также является totCO-квазигруппой для любого её парастрофа ${}^\sigma A$.

Известно, что конечные totCO-квазигруппы существуют (см., например, [5, 6]). В [3] В. Д. Белоусов отметил, что существуют бесконечные квазигруппы, все парастрофы которых попарно ортогональны, и привёл следующий пример такой квазигруппы: $A(x, y) = 2x + 3y$, где $(Q, +, \cdot)$ — поле рациональных чисел.

Для того чтобы получить некоторую информацию относительно спектра totCO-квазигрупп, установим критерий ортогональности различных пар парастрофов T-квазигрупп.

Сначала укажем вид парастрофов (которые также являются T-квазигруппами) T-квазигруппы $A(x, y) = \varphi x + \psi y + c$:

$$\begin{aligned} {}^sA(x, y) &= \psi x + \varphi y + c, & {}^rA(x, y) &= I\psi^{-1}\varphi x + \psi^{-1}y + I\psi^{-1}c, \\ {}^lA(x, y) &= \varphi^{-1}x + I\varphi^{-1}\psi y + I\varphi^{-1}c, & {}^{rl}A(x, y) &= \psi^{-1}x + I\psi^{-1}\varphi y + I\psi^{-1}c, \\ {}^{lr}A(x, y) &= I\varphi^{-1}\psi x + \varphi^{-1}y + I\varphi^{-1}c, \end{aligned}$$

где $Ix = -x$ (см., например, [16]).

Пусть $\sigma \perp \tau$ означает, что ${}^\sigma A \perp {}^\tau A$, в $\sigma\tau$ сначала берётся парастроф τ , затем парастроф σ , $(\varphi + \psi)x = \varphi x + \psi x$, а ε является тождественной подстановкой. Очевидно, что если ${}^\sigma A \perp {}^\tau A$, то ${}^{s\sigma}A \perp {}^{s\tau}A$.

Теорема 1. Пусть (Q, A) — конечная или бесконечная T-квазигруппа вида $A(x, y) = \varphi x + \psi y$. Тогда два её парастрофа ортогональны тогда и только тогда, когда соответствующие этим парастрофам отображения

$$\begin{aligned} (1 \perp l \text{ или } s \perp lr) &\rightarrow \varphi + \varepsilon, & (r \perp rl) &\rightarrow \varphi + \varepsilon \text{ и } \varphi - \varepsilon, \\ (1 \perp r \text{ или } s \perp rl) &\rightarrow \psi + \varepsilon, & (l \perp lr) &\rightarrow \psi + \varepsilon \text{ и } \psi - \varepsilon, \\ (1 \perp lr \text{ или } s \perp l) &\rightarrow \varphi + \psi^2, & (1 \perp rl \text{ или } s \perp r) &\rightarrow \varphi^2 + \psi, \\ (r \perp lr \text{ или } rl \perp l) &\rightarrow \varphi - \psi, & (1 \perp s) &\rightarrow \varphi - \psi \text{ и } \varphi + \psi, \\ (l \perp r \text{ или } lr \perp rl) &\rightarrow \psi\varphi - \varepsilon \end{aligned}$$

являются подстановками.

Доказательство. Условия для ортогональности $A \perp {}^{\sigma}A$, т. е. для $1 \perp r$, $1 \perp l$, $1 \perp lr$, $1 \perp rl$ и $1 \perp s$ установлены в [16, теорема 17]. Заметим, что

$$1 \perp r \iff s \perp rl, \quad 1 \perp l \iff s \perp lr, \quad 1 \perp lr \iff s \perp l, \quad 1 \perp rl \iff s \perp r.$$

Аналогично

$$r \perp lr \iff rl \perp l, \quad l \perp r \iff lr \perp rl.$$

Проверим остальные случаи, используя критерий Белоусова ортогональности двух квазигрупп ($A \perp B$ тогда и только тогда, когда операция $A \cdot {}^rB$ (или $A \circ {}^lB$) является квазигруппой) и вид парастрофов Т-квазигруппы с элементом $c = 0$. При этом примем во внимание, что все эндоморфизмы абелевой группы образуют ассоциативное кольцо с единицей относительно операций сложения и умножения эндоморфизмов.

Рассмотрим случай $r \perp rl$. Имеем

$$C(x, y) = {}^rA(x, A(x, y)) = \psi^{-1}x + I\psi^{-1}\varphi(\varphi x + \psi y) = \psi^{-1}(\varepsilon - \varphi^2)x + I\psi^{-1}\varphi\psi y.$$

Отсюда следует, что операция C является квазигруппой тогда и только тогда, когда отображение $\varphi^2 - \varepsilon$ является подстановкой (автоморфизмом группы $Q(+)$). Но

$$\varphi^2 - \varepsilon = (\varphi + \varepsilon)(\varphi - \varepsilon) = (\varphi - \varepsilon)(\varphi + \varepsilon),$$

и если $\varphi^2 - \varepsilon$ — подстановка, то отображения $(\varphi + \varepsilon)$ и $(\varphi - \varepsilon)$ сюръективны и инъективны, т. е. являются подстановками.

Обратно, если оба эти отображения являются подстановками, то отображение $\varphi^2 - \varepsilon$ также подстановка.

Доказательство для случая $l \perp lr$ аналогично, если $C(x, y) = {}^lA(A(x, y), y)$.

Рассмотрим случаи $r \perp lr$ и $rl \perp l$. Имеем

$$C(x, y) = {}^lrA(x, A(x, y)) = I\varphi^{-1}\psi x + \varphi^{-1}(\varphi x + \psi y) = \varphi^{-1}(\varphi - \psi)x + \varphi^{-1}\psi y,$$

откуда следует, что операция $C(x, y)$ является квазигруппой тогда и только тогда, когда отображение $\varphi - \psi$ — подстановка.

Рассмотрим случаи $l \perp r$ и $lr \perp rl$. Имеем

$$C(x, y) = {}^lA(x, A(x, y)) = \varphi^{-1}x + I\varphi^{-1}\psi(\varphi x + \psi y) = I\varphi^{-1}(\psi\varphi - \varepsilon)x + I\varphi^{-1}\psi^2y,$$

и операция $C(x, y)$ — квазигруппа тогда и только тогда, когда отображение $\psi\varphi - \varepsilon$ является подстановкой. $\square$

Замечание. Легко проверить, что для Т-квазигруппы вида $A(x, y) = \varphi x + \psi y + c$, где $c \neq 0$, условия теоремы 1 те же самые, так как они не зависят от элемента c . Поэтому если Т-квазигруппа (Q, A) с $A(x, y) = \varphi x + \psi y$ является totCO-квазигруппой, то Т-квазигруппа (Q, B) с $B(x, y) = \varphi x + \psi y + c$ также totCO-квазигруппа для любого элемента $c \in Q$.

Из теоремы 1 и этого замечания сразу вытекают следующие связи между ортогональностью парастрофов Т-квазигрупп.

Следствие 1. Для любой T -квазигруппы (Q, A) с $A(x, y) = \varphi x + \psi y + c$

$$r \perp rl \implies 1 \perp l, \quad s \perp lr,$$

$$l \perp lr \implies 1 \perp r, \quad s \perp rl,$$

$$1 \perp s \implies r \perp lr, \quad l \perp rl.$$

Из всех условий теоремы 1 вытекает теорема 2.

Теорема 2. T -квазигруппа (Q, A) с $A(x, y) = \varphi x + \psi y + c$ является totCO -квазигруппой тогда и только тогда, когда все отображения

$$\varphi + \varepsilon, \quad \varphi - \varepsilon, \quad \psi + \varepsilon, \quad \psi - \varepsilon, \quad \varphi^2 + \psi, \quad \psi^2 + \varphi, \quad \varphi - \psi, \quad \varphi + \psi, \quad \psi\varphi - \varepsilon$$

являются подстановками.

Следствие 2. T -квазигруппа (Q, A) с $A(x, y) = ax + by \pmod{n}$ является totCO -квазигруппой тогда и только тогда, когда все элементы

$$a + 1, \quad a - 1, \quad b + 1, \quad b - 1, \quad a^2 + b, \quad b^2 + a, \quad a - b, \quad a + b, \quad ab - 1$$

по модулю n взаимно просты с n .

Доказательство. В самом деле, в этом случае отображения

$$(\varphi + \varepsilon): (\varphi + \varepsilon)x = (L_a + \varepsilon)x = (a + 1)x,$$

$$(\varphi - \varepsilon): (\varphi - \varepsilon)x = (L_a - \varepsilon)x = (a - 1)x,$$

$$(\psi + \varepsilon): (\psi + \varepsilon)x = (L_b + \varepsilon)x = (b + 1)x,$$

$$(\psi - \varepsilon): (\psi - \varepsilon)x = (L_b - \varepsilon)x = (b - 1)x,$$

$$(\varphi^2 + \psi): (\varphi^2 + \psi)x = (L_a^2 + L_b)x = (a^2 + b)x,$$

$$(\psi^2 + \varphi): (\psi^2 + \varphi)x = (L_b^2 + L_a)x = (b^2 + a)x,$$

$$(\varphi - \psi): (\varphi - \psi)x = (L_a - L_b)x = (a - b)x,$$

$$(\varphi + \psi): (\varphi + \psi)x = (L_a + L_b)x = (a + b)x,$$

$$(\psi\varphi - \varepsilon): (\psi\varphi - \varepsilon)x = (L_b L_a - \varepsilon)x = (ab - 1)x$$

являются подстановками тогда и только тогда, когда соответствующие элементы по модулю n взаимно просты с n . Заметим, что элементы a, b также взаимно просты с n , так как (Q, A) — квазигруппа. $\square$

Из следствия 2 вытекают следующие необходимые условия для tot -квазигрупп рассматриваемого вида.

Следствие 3. Если T -квазигруппа (Q, A) с $A(x, y) = ax + by \pmod{n}$ является totCO -квазигруппой, то $a \neq -1, 1, b, -b, -b^2$, $b \neq -1, 1, -a^2$, $ab \neq 1$ по модулю n .

Доказательство. Эти условия исключают случаи, когда элементы из следствия 2 равны 0 по модулю n , и поэтому соответствующие отображения не являются подстановками. $\square$

Ниже мы рассмотрим некоторые Т-квазигруппы конечного порядка и используем следствие 2, чтобы получить следующую информацию относительно спектра totCO-квазигрупп.

Теорема 3. Для любого целого числа $n \geq 11$, взаимно простого с 2, 3, 5 и 7, существует totCO-квазигруппа порядка n .

Доказательство. Пусть $\bar{a}$ — элемент a по модулю n , (m, n) — наибольший общий делитель m и n . Рассмотрим квазигруппу (Q, A) с $A(x, y) = 2x + 5y \pmod{n}$, где $(2, n) = 1$ и $(5, n) = 1$. Проверим условия следствия 2 для этой квазигруппы:

$$\begin{aligned}(a+1)x &= 3x, & (a-1)x &= x, & (b+1)x &= 6x, & (b-1)x &= 4x, & (a^2+b)x &= 9x, \\ (b^2+a)x &= 27x, & (a-b)x &= -3x, & (a+b)x &= 7x, & (ab-1)x &= 9x.\end{aligned}$$

Так как $n \geq 11$, то отображения $3x, 4x, 6x, -3x, 7x, 9x$ являются подстановками, если число n взаимно просто с 2, 3 и 7. Заметим, что если $(3, n) = 1$, то $(-3, n) = (n-3, n) = 1$. Пусть число n взаимно просто с 2, 3, 5 и 7. Тогда $n \neq 27$ и $n < 27$ только для $n = 11, 13, 17, 19, 23$. Все эти числа являются простыми, поэтому $(\overline{27}, n) = 1$ для каждого из этих чисел. Если $n > 27$, то $\overline{27} = 27$ и $(27, n) = 1$, так как число n взаимно просто с 3. Следовательно, по следствию 2 квазигруппа $A(x, y) = 2x + 5y \pmod{n}$ является totCO-квазигруппой для любого n , взаимно простого с 2, 3, 5 и 7. $\square$

Следствие 4. Для любого $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, где p_i — простое число, $p_i \neq 2, 3, 5, 7$, $k_i \geq 1$, $i = 1, 2, \dots, s$, $s \geq 1$, существует totCO-квазигруппа порядка n .

Кроме квазигруппы, использованной при доказательстве теоремы 3, существуют и другие квазигруппы с аналогичными свойствами.

Предложение 1. Квазигруппы

$$A_1(x, y) = 2x + 4y \pmod{n}, \quad A_2(x, y) = 3x + 5y \pmod{n}$$

являются totCO-квазигруппами тогда и только тогда, когда число n взаимно просто с 2, 3, 5 и 7.

Квазигруппы

$$\begin{aligned}A_3(x, y) &= 2x + 3y \pmod{n}, & A_4(x, y) &= 2x + 8y \pmod{n}, \\ A_5(x, y) &= 5x + 10y \pmod{n}, & A_6(x, y) &= 5x + 11y \pmod{n}\end{aligned}$$

являются totCO-квазигруппами тогда и только тогда, когда число n взаимно просто с 2, 3, 5, 7 и 11.

Квазигруппы

$$A_7(x, y) = 3x + 7y \pmod{n}, \quad A_8(x, y) = 3x + 9y \pmod{n}$$

являются totCO-квазигруппами тогда и только тогда, когда число n взаимно просто с 2, 3, 5, 7 и 13.

Доказательство. Это предложение доказывается аналогично теореме 3 с использованием следствия 2. Дополнительно заметим, что среди чисел из следствия 2 (при обычном умножении) наибольшим является число $b^2 + a$ для всех квазигрупп из предложения 1. Этим числом является число $m_1 = 18$ ($m_2 = 28$, $m_3 = 11$, $m_4 = 66$, $m_5 = 105$, $m_6 = 126$, $m_7 = 52$, $m_8 = 84$) для квазигруппы A_1 (для квазигрупп $A_2, A_3, A_4, A_5, A_6, A_7, A_8$ соответственно). Но если число n взаимно просто с 2, 3, 5, 7, то наименьшим непростым числом является $n = 121$, и $(126, 121) = (5, 121) = 1$. Остальные числа m меньше числа $b^2 + a$ в каждой из рассматриваемых квазигрупп, и поэтому тем более $(m, n) = 1$, если число n взаимно просто с 2, 3, 5, 7 для квазигрупп A_1 и A_2 (с 2, 3, 5, 7, 11 для квазигрупп A_3, A_4, A_5, A_6 и с 2, 3, 5, 7, 13 для квазигрупп A_7, A_8). $\square$

Компьютерное исследование показало, что totCO-квазигрупп порядка $n \leq 7$ среди Т-квазигрупп вида $A(x, y) = ax + by \pmod{n}$ не существует. Но среди квазигрупп этого вида существуют идемпотентные ($A(x, x) = x$ для любого x) totCO-квазигруппы различных порядков. Некоторые из таких квазигрупп приведены в следующем предложении.

Предложение 2. Квазигруппы

$$\begin{aligned} A(x, y) &= 3x + 9y \pmod{11}, & A(x, y) &= 6x + 8y \pmod{13}, \\ A(x, y) &= 6x + 12y \pmod{17}, & A(x, y) &= 7x + 11y \pmod{17}, \\ A(x, y) &= 8x + 10y \pmod{17}, & A(x, y) &= 9x + 11y \pmod{19} \end{aligned}$$

являются идемпотентными totCO-квазигруппами.

Доказательство. Это предложение также доказывается аналогично теореме 3 с использованием следствия 2. Нужно учесть, что во всех указанных квазигруппах n — простое число, $a + b = 1 \pmod{n}$, а Т-квазигруппа $A(x, y) = \varphi x + \psi y$ идемпотентна тогда и только тогда, когда $\varphi + \psi = \varepsilon$. $\square$

Как было отмечено выше, любой парастроф $(Q, {}^\sigma A)$ totCO-квазигруппы (Q, A) также является totCO-квазигруппой. Определим парастрофы Т-квазигруппы вида $A(x, y) = ax + by \pmod{n}$, используя вид парастрофов Т-квазигрупп, указанный выше:

$$\begin{aligned} {}^s A(x, y) &= bx + ay \pmod{n}, & {}^r A(x, y) &= IL_b^{-1} L_a x + L_b^{-1} y \pmod{n}, \\ {}^l A(x, y) &= L_a^{-1} x + IL_a^{-1} L_b y \pmod{n}, & {}^{rl} A(x, y) &= L_b^{-1} x + IL_b^{-1} L_a y \pmod{n}, \\ {}^{lr} A(x, y) &= IL_a^{-1} L_b x + L_a^{-1} y \pmod{n}, \end{aligned}$$

где $Ix = -x$, L_a^{-1} — подстановка, обратная к подстановке L_a .

Пусть $n = p$, где p — простое число, $L_a^{-1}x = L_{a^{-1}}x \pmod{p}$, где a^{-1} — элемент, обратный к a в мультипликативной группе $(Q', \cdot)$ по модулю p , $Q' = Q \setminus 0$. В этом случае $-a = p - a$, $a^{-1} = (k_0 p + 1)/a$, где k_0 — наименьшее число, такое что a делит $k_0 p + 1$. Учитывая это, можно получить все попарно ортогональные парастрофы totCO-квазигруппы (Q, A) с $A(x, y) = ax + by \pmod{p}$. Например,

для totCO-квазигруппы $A(x, y) = 2x + 4y \pmod{17}$ (см. предложение 1) мы находим следующее ортогональное множество из шести парастрофов:

$$\Sigma = \{A(x, y) = 2x + 4y, {}^sA(x, y) = 4x + 2y, {}^rA(x, y) = 8x + 13y, {}^{rl}A(x, y) = 13x + 8y, {}^lA(x, y) = 9x + 15y, {}^{lr}A(x, y) = 15x + 9y\} \pmod{17}.$$

Квазигруппа (Q, A) называется *самоортогональной*, если $A \perp A^* = {}^sA$. В [9] изучаются латинские квадраты порядка n , для которых каждый парастроф ортогонален своему транспонированному. Такие латинские квадраты называют сопряжённо-самоортогональными и обозначают CSOLS(n). CSOLS*(n) — это CSOLS(n) со свойством, что каждый парастроф ортогонален только своему транспонированному. В [9] (лемма 4.1 и теорема 4.12) доказано следующее.

Лемма 1 [9]. Для всех простых степеней $n \neq 2, 3, 5$ существует CSOLS(n).

Теорема 4 [9]. CSOLS*(n) существует тогда и только тогда, когда $n \geq 8$, за исключением, возможно, $n = 10, 11$.

Как отмечается в [9], компьютерное исследование подтвердило, что CSOLS*(n) не существуют для $n \leq 7$.

Очевидно, что CSOLS(n) соответствует квазигруппе (Q, A) порядка n с самоортогональными парастрофами, т. е. ${}^\sigma A \perp {}^s({}^\sigma A)$ для любого парастрофа ${}^\sigma A$. В [16] такие квазигруппы называются SOC-квазигруппами и доказывается, что Т-квазигруппа вида $A(x, y) = \varphi x + \psi y + c$ является SOC-квазигруппой (SOC-Т-квазигруппой) тогда и только тогда, когда все отображения

$$\varphi - \psi, \quad \varphi + \psi, \quad \varepsilon - \psi, \quad \varepsilon + \psi, \quad \varepsilon - \varphi, \quad \varepsilon + \varphi -$$

подстановки [16, теорема 20]. Там же приводятся следующие примеры SOC-Т-квазигрупп: $A(x, y) = 3x + 5y \pmod{7}$, $A(x, y) = 3x + 9y \pmod{11}$ и $A(x, y) = ax + by + c$ над полем рациональных чисел, где $a \neq 0, 1, b, b \neq 0, 1$.

Очевидно, что класс totCO-квазигрупп содержится в классе SOC-квазигрупп и totCO-квазигруппа не может соответствовать CSOLS*. Из теоремы 2 и [16, теорема 20] следует, что SOC-Т-квазигруппа (Q, A) с $A(x, y) = \varphi x + \psi y + c$ является totCO-квазигруппой тогда и только тогда, когда отображения $\varphi^2 + \psi$, $\varphi + \psi^2$ и $\psi\varphi - \varepsilon$ — подстановки.

В [8, 9] рассматривается представление ортогональных связей парастрофов латинского квадрата L графом, в котором вершинами являются парастрофы, а две вершины соединены тогда и только тогда, когда соответствующие парастрофы ортогональны. Такой граф называется графом сопряжённо-ортогонального латинского квадрата L . Проблема описания полного спектра латинских квадратов, реализующих полный граф K_6 сопряжённо-ортогонального латинского квадрата, ещё остаётся открытой.

Очевидно, что любая конечная totCO-квазигруппа соответствует полному графу K_6 сопряжённо-ортогонального латинского квадрата, поэтому из следствия 3 вытекает следствие 5.

Следствие 5. Для каждого $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, где p_i — простое число, $p_i \neq 2, 3, 5, 7$, $k_i \geq 1$, $i = 1, 2, \dots, s$, $s \geq 1$, существует латинский квадрат порядка n , реализующий полный граф K_6 сопряжённо-ортогонального латинского квадрата.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (грант 08.820.08.08).

Литература

- [1] Белоусов В. Д. Основы теории квазигрупп и луп. — М.: Наука, 1967.
- [2] Белоусов В. Д. Системы ортогональных операций // Мат. сб. — 1968. — Т. 77 (119), № 1. — С. 38–58.
- [3] Belousov V. D. Parastrophic-orthogonal quasigroups // Quasigroups Relat. Syst. — 2005. — Vol. 13, no. 1. — P. 25–72.
- [4] Belyavskaya G. B., Diordiev A. D. On some quasi-identities in finite quasigroups // Bul. Acad. Ştiinţe Repub. Mold. Mat. — 2005. — No. 3 (49). — P. 19–32.
- [5] Bennett F. E. Latin squares with pairwise orthogonal conjugates // Discrete Math. — 1981. — Vol. 36. — P. 117–137.
- [6] Bennett F. E. On conjugate orthogonal idempotent Latin squares // Ars Combinatoria. — 1985. — Vol. 19. — P. 37–50.
- [7] Bennett F. E. The spectra of a variety of quasigroups and related combinatorial designs // Discrete Math. — 1989. — Vol. 77. — P. 29–50.
- [8] Bennett F. E., Mendelsohn N. S. Conjugate orthogonal Latin square graphs // Congr. Numer. — 1979. — Vol. 23. — P. 179–192.
- [9] Bennett F. E., Zhang H. Latin squares with self-orthogonal conjugates // Discrete Math. — 2004. — Vol. 284. — P. 45–55.
- [10] Chaffer R. A., Lieberman D. J., Smith D. D. The number of orthogonal conjugates of a quasigroup // Congr. Numer. — 1982. — Vol. 35. — P. 169–180.
- [11] Déneš J., Keedwell A. D. Latin Squares and Their Applications. — Budapest: Akadémiai Kiadó; New York: Academic Press, 1974.
- [12] Evans T. Algebraic structures associated with Latin squares and orthogonal arrays // Congr. Numer. — 1975. — Vol. 13. — P. 31–52.
- [13] Kepka T., Nemec P. T-quasigroups. I // Acta Univ. Carolin. Math. Phys. — 1971. — Vol. 12, no. 1. — P. 39–49.
- [14] Lindner C. C., Mendelsohn E., Mendelsohn N. S., Wolk B. Orthogonal Latin square graphs // J. Graph Theory. — 1973. — Vol. 3. — P. 325–328.
- [15] Lindner C. C., Steedly D. On the number of conjugates of a quasigroup // Algebra Universalis. — 1975. — Vol. 5. — P. 191–196.
- [16] Mullen G., Shcherbacov V. On orthogonality of binary operations and squares // Bul. Acad. Ştiinţe Repub. Mold. Mat. — 2005. — No. 2 (48). — P. 3–42.
- [17] Phelps K. T. Conjugate orthogonal quasigroups // J. Combin. Theory Ser. A. — 1978. — Vol. 25. — P. 117–127.