Ортогональность обратимой тернарной операции и двух ее термальных операций

Н. А. Щучкин*

В работе рассматриваются обратимые справа тернарные операции. Для каждой такой операции строятся две ее термальные операции и утверждается ортогональность полученных трех операций. С помощью так построенных трех ортогональных операций преобразуются слова.

Ключевые слова: Тернарный группоид, ортогональность, обратимость, преобразование .

1. Введение

Мы используем тернарные ортогональные операции f, g, t для создания алгоритма шифрования, причем операция f однозначно разрешима справа, а операции g и t построены как термальные операции с использованием операции f. Процесс построения операций g и t описан в параграфе 3, там же приведена эквивалентность однозначной разрешимости справа операции f и ортогональности операций f, g, t в теореме 1. В параграфе 4 указаны два алгоритма шифрования с использованием тернарных ортогональных операций f, g, t, и найдены обратные к ним преобразования.

2. Предварительные сведения

Тернарная операция f на множестве Q называется i-обратимой для некоторого $i \in \{1, 2, 3\}$, если одно из трех уравнений (для $i = 1$ первое, для $i = 2$ второе, для $i = 3$ третье)

$$f(x, a, b) = c, f(a, y, b) = c, f(a, b, z) = c$$

имеет единственное решение для любых элементов a, b, c из Q.

Для i-обратимой тернарной операции f, $i = 1, 2, 3$, существует i-обратная тернарная операция ${}^{(i)}f$, определенная следующим образом:

$${}^{(1)}f(d, b, c) = a \Leftrightarrow f(a, b, c) = d;$$

* *Щучкин Николай Алексеевич* — профессор, ВГСПУ, г. Волгоград, e-mail: nikolaj_shchuchkin@mail.ru.

Shchuchkin Nikolai Alekseevich — Professor, VGSPU, Volgograd.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

$$^{(2)}f(a,d,c)=b \Leftrightarrow f(a,b,c)=d;$$
$$^{(3)}f(a,b,d)=c \Leftrightarrow f(a,b,c)=d.$$

3. Ортогональность тернарных операций

Определим ортогональность тернарных операций f,g,t, как это сделано С.К.Стейном в [1] для определения ортогональности бинарных операций. Тернарные операции f,g,t, определенные на одном и том же множестве Q, называются ортогональными, если отображение σ декартова произведения $Q\times Q\times Q$ на само себя, заданное по правилу $\sigma(x,y,z)=(f(x,y,z),g(x,y,z),t(x,y,z))$, является биективным.

Теорема 1. *Пусть (Q,f) – тернарный группоид. Определим еще две тернарные операции:*

1) $g(x,y,z)=f(f(x,y,z),x,y)$, $t(x,y,z)=f(f(x,y,z),g(x,y,z),x)$;
2) $g(x,y,z)=f(x,f(x,y,z),y)$, $t(x,y,z)=f(f(x,y,z),g(x,y,z),x)$;
3) $g(x,y,z)=f(f(x,y,z),x,y)$, $t(x,y,z)=f(g(x,y,z),f(x,y,z),x)$;
4) $g(x,y,z)=f(x,f(x,y,z),y)$, $t(x,y,z)=f(g(x,y,z),f(x,y,z),x)$;
5) $g(x,y,z)=f(f(x,y,z),y,x)$, $t(x,y,z)=f(f(x,y,z),g(x,y,z),y)$;
6) $g(x,y,z)=f(y,f(x,y,z),x)$, $t(x,y,z)=f(f(x,y,z),g(x,y,z),y)$;
7) $g(x,y,z)=f(f(x,y,z),y,x)$, $t(x,y,z)=f(g(x,y,z),f(x,y,z),y)$;
8) $g(x,y,z)=f(y,f(x,y,z),x)$, $t(x,y,z)=f(g(x,y,z),f(x,y,z),y)$.

Тернарная операция f является 3-обратимой тогда и только тогда, когда операции f,g,t ортогональны.

4. Преобразования слов

Выбираем конечное множество Q порядка m, на котором определены указанные операции f,g,t. Множество всех слов в алфавите Q обозначим

$$Q^{+}=\{x_1\dots x_s|x_i\in Q,s\geq 1\}.$$

Из множестве Q^{+} выбираем слово $x_1\dots x_s$. Предполагаем, что это слово содержит количество s символов, кратное трем, из алфавита Q. Если это не так, то добавляем в конец этого слова два пробела в случае, когда s при делении на 3 дает остаток 1, или один пробел в случае, когда s при делении на 3 дает остаток 2 (предполагается, что алфавит Q содержит символ "пробел"). Перед началом шифрования передается первоначальная длина слова, а затем отображается слово с дополнением нужного количества пробелов. Расшифровывать будем измененное слово, а затем, с учетом переданной информации о длине слова, восстановим исходное слово.

Случай 1. Преобразуем слова с помощью ортогональных тернарных операций f, g, t: f – 3-обратимая тернарная операция, $g(x,y,z) = f(\alpha(f(x,y,z)),\alpha(x),y)$, $t(x,y,z) = f(\beta(f(x,y,z)),\beta(g(x,y,z)),x)$, где α и β – перестановки на множествах $\{f(x,y,z),x\}$ и $\{f(x,y,z),g(x,y,z)\}$ соответственно, выбранные по одному из четырех вариантов: 1) α и β – диагонали; 2) α – транспозиция, β – диагональ; 3) α – диагональ, β – транспозиция; 4) α и β – транспозиции. Эти операции описывают 1)–4) из теоремы 1.

Отображаем слово $x_1 \dots x_s$ по правилу $\tau_1(x_1 \dots x_s) = y_1 \dots y_s$,

$$\text{где} \quad \begin{cases} y_i = f(x_i, x_{i+1}, x_{i+2}), \\ y_{i+1} = g(x_i, x_{i+1}, x_{i+2}) = f(\alpha(y_i), \alpha(x_i), x_{i+1}), \\ y_{i+2} = t(x_i, x_{i+1}, x_{i+2}) = f(\beta(y_i), \beta(y_{i+1}), x_i) \end{cases} \tag{1}$$

для всех $i = 3j-2$ при $j = 1, 2, \dots, s/3$.

Отображение τ_1, построенное по правилу (1), является биективным в силу ортогональности операций f, g, t.

На множестве слов, у которых длина кратна трем, строим отображение $\mu_1(y_1 \dots y_s) = z_1 \dots z_s$,

$$\text{где} \quad \begin{cases} z_i = {}^{(3)}f(\beta(y_i), \beta(y_{i+1}), y_{i+2}), \\ z_{i+1} = {}^{(3)}f(\alpha(y_i), \alpha(z_i), y_{i+1}), \\ z_{i+2} = {}^{(3)}f(z_i, z_{i+1}, y_i) \end{cases} \tag{2}$$

для всех $i = 3j-2$ при $j = 1, 2, \dots, s/3$.

Теорема 2. *Отображение μ_1, построенное по правилу (2), является обратным для отображения τ_1.*

Случай 2. Преобразуем слова с помощью ортогональных тернарных операций f, g, t: f – 3-обратимая тернарная операция, $g(x,y,z) = f(\alpha(f(x,y,z)),\alpha(y),x)$, $t(x,y,z) = f(\beta(f(x,y,z)),\beta(g(x,y,z)),y)$, где α и β – перестановки на множествах $\{f(x,y,z),y\}$ и $\{f(x,y,z),g(x,y,z)\}$ соответственно, выбранные по одному из четырех вариантов: 1) α и β – диагонали; 2) α – транспозиция, β – диагональ; 3) α – диагональ, β – транспозиция; 4) α и β – транспозиции. Эти операции описывают 5)–8) из теоремы 1.

Отображаем слово $x_1 \dots x_s$ по правилу $\tau_2(x_1 \dots x_s) = y_1 \dots y_s$,

$$\text{где} \quad \begin{cases} y_i = f(x_i, x_{i+1}, x_{i+2}), \\ y_{i+1} = g(x_i, x_{i+1}, x_{i+2}) = f(\alpha(y_i), \alpha(x_{i+1}), x_i), \\ y_{i+2} = t(x_i, x_{i+1}, x_{i+2}) = f(\beta(y_i), \beta(y_{i+1}), x_{i+1}) \end{cases} \tag{3}$$

для всех $i = 3j - 2$ при $j = 1, 2, \ldots, s/3$.

Отображение τ_2, построенное по правилу (3), является биективным в силу ортогональности операций f, g, t.

На множестве слов, у которых длина кратна трем, строим отображение $\mu_2(y_1 \ldots y_s) = z_1 \ldots z_s$,

$$\text{где} \quad \begin{cases} z_{i+1} = {}^{(3)}f(\beta(y_i), \beta(y_{i+1}), y_{i+2}), \\ z_i = {}^{(3)}f(\alpha(y_i), \alpha(z_{i+1}), y_{i+1}), \\ z_{i+2} = {}^{(3)}f(z_i, z_{i+1}, y_i) \end{cases} \tag{4}$$

для всех $i = 3j - 2$ при $j = 1, 2, \ldots, s/3$.

Непосредственной проверкой, как в теореме 2, доказывается, что отображение μ_2, построенное по правилу (4), является обратным для отображения τ_2.

5. Заключение

Для тернарной операции f по анлалогии, как описано выше, найдены по восемь пар тернарных операций g,t, с помощью которых устанавливается эквивалентность 1- и 2-обратимости операции f и ортогональности трех операций f,g,t. Имеются преобразования слов с помощью этих трех ортогональных операций и обратные к ним преобразования.

Список литературы

[1] S. K. Stein, “On the foundations of quasigroups”, *Trans. Amer. Math. Soc.*, **85**, 1957, 228–256.

Статья поступила 5 октября 2026 г.

The orthogonality of an invertible ternary operation and its two term operations

N. A. Shchuchkin

The paper deals with ternary operations that are right-invertible. For each such operation, two term operations are constructed, and the three resulting operations are shown to be orthogonal. These three orthogonal operations are then used to transform words.

Keywords: Ternary groupoid, orthogonality, reversibility, transformation .

Received on October 5, 2026