Math-Net.Ru

Общероссийский математический портал

М. М. Глухов, О 2-транзитивных произведениях трех регулярных групп подстановок конечного поля, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 1, 11–26

DOI: <https://doi.org/10.4213/mvk274>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 17:49:01

**О 2-транзитивных произведениях трех регулярных
групп подстановок конечного поля**

М. М. Глухов

Академия криптографии Российской Федерации, Москва

Получено 18.IV.2018

Аннотация. Рассматриваются группа $(GF(2^n), \oplus)$ и ее правое регулярное представление G_n . Приведены некоторые классы подстановок h поля $GF(2^n)$, для которых множество $(G_n h)^3$ является 2-транзитивным.

Ключевые слова: конечные поля, разностно равномерные подстановки, 2-транзитивность

**On 2-transitive products of three regular permutation groups
of a finite field**

M. M. Glukhov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. Let G_n be a right regular representation of the group $(GF(2^n), \oplus)$. We describe some classes of permutations h of the field $GF(2^n)$ such that the set $(G_n h)^3$ is 2-transitive.

Key words: finite fields, differentially uniform permutations, 2-transitivity

1. Введение

В работе используются следующие обозначения:

$P_n = GF(2^n)$ — расширение поля $GF(2)$ корнем θ неприводимого многочлена степени n ,

$(P_n, \oplus)$ — аддитивная группа поля P_n ,

P_n^* — мультипликативная группа поля P_n ,

$a = a_{n-1}\theta^{n-1} \oplus a_{n-2}\theta^{n-2} \oplus \dots \oplus a_0$ — элемент поля P_n , отождествляемый с числом $a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + \dots + a_0 \in \{0, 1, \dots, 2^n - 1\}$ и с двоичным вектором $(a_{n-1}, a_{n-2}, \dots, a_0)$,

$G_n = \{g_a: g_a(u) = u \oplus a; a, u \in P_n\}$ — правое регулярное представление группы $(P_n, \oplus)$,

$S(\Omega)$ — симметрическая группа подстановок конечного множества Ω ,

τ — подстановка обращения элементов поля P_n , $\tau(0) = 0$,

$a\psi = \psi(a)$ — образ элемента a при отображении ψ ,

$Q_{G_n h G_n}$ — матрица переходов ненулевых разностей элементов поля P_n при действии преобразований множества $G_n h G_n$,

$q_{a,b}(h)$ — элемент матрицы $Q_{G_n h G_n}$, равный числу решений уравнения

$$(a \oplus x)h \oplus xh = b, \quad a, b \in P_n^*, \quad (1)$$

T_n — подгруппа группы $(P_n, \oplus)$, состоящая из элементов с нулевым следом поля P_n в поле $GF(2)$, т.е. $T_n = \{a \in P_n: \text{tr}(a) = 0\}$,

$$T_n^* = T_n \setminus \{0\}.$$

Пусть $(\Omega, +)$ — конечная абелева группа, G — ее регулярное представление, h — подстановка из группы $S(\Omega)$ и Q_{Gh} — матрица переходов ненулевых биграмм под действием подстановок из Gh . Задача нахождения минимального значения k , при котором множество подстановок $(Gh)^k$ является 2-транзитивным, важно для криптографии, поскольку параметр k влияет на скорость стремления матрицы переходов ненулевых биграмм при итерациях преобразований из Gh к равномерной матрице, что существенно для оценок стойкости соответствующей шифрсистемы относительно разностного метода анализа. Заметим, что условие 2-транзитивности множества $(Gh)^k$ равносильно тому, что в матрице $(Q_{Gh})^k$ нет нулевых элементов, что далее будем записывать в виде неравенства $(Q_{Gh})^k > 0$. Очевидно, что это условие может выполняться лишь при $k > 1$. Минимальное значение k , при котором $(Q_{Gh})^k > 0$, называется показателем 2-транзитивности множества Gh .

В [1] доказано, что необходимые условия 2-транзитивности множества $(Gh)^2$ являются довольно жесткими.

С другой стороны, А. С. Амбросимовым доказано, что равномерно по всем регулярным группам порядка N вероятность 2-транзитивности множества $(Gh)^3$ при случайном выборе подстановки h стремится к 1 при $N \rightarrow \infty$. Однако каких-либо конкретных подстановок h поля P_n с 2-транзитивным множеством $(G_n h)^3$ до настоящего времени не было известно. Так, например, для аффинных подстановок абелевых групп порядка n известны варианты множеств Gh с показателем 2-транзитивности от 4 до $2^{n-2} + 3$ (см. [2]).

В данной работе приведены некоторые классы подстановок h поля P_n со свойством 2-транзитивности множества $(G_n h)^3$.

2. О разностно 2-равномерно нелинейных подстановках поля характеристики 2

В [10] было введено понятие разностно δ -равномерно нелинейного отображения конечного поля в себя. Так было названо отображение h , при котором уравнение

$$(a + x)h - xh = b$$

имеет не более δ решений для любых элементов поля $a, b, a \neq 0$. Ряд работ посвящен построению и исследованию разностно 4-равномерно нелинейных отображений (в частности, подстановок) полей, см. [12–14].

В случае поля характеристики 2 уравнению (1) наряду со значением $x = x_1$ удовлетворяет также $x_2 = x_1 \oplus a$. Поэтому для поля $P_n = GF(2^n)$ подстановка h является разностно 2-равномерно нелинейной, если элементами соответствующей матрицы $Q_{G_n h G_n}$ будут нули и двойки, а тогда в каждой строке будет $2^{n-1} - 1$ нулей и 2^{n-1} двоек. Для разностно 2-равномерно нелинейной подстановки h поля P_n неравенство

$$(Q_{G_n h G_n})^2 > 0$$

выполняется, поскольку в каждой строке и в каждом столбце матрицы $Q_{G_n h G_n}$ содержится более половины ненулевых элементов. Таким образом, справедливо следующее утверждение.

Утверждение 1. *Если подстановка h поля $P_n = GF(2^n)$ разностно 2-равномерно нелинейна, то множество подстановок $(G_n h)^3$ является 2-транзитивным.*

Замечание 1. В случае поля характеристики 2 разностно 2-равномерно нелинейные отображения называют также почти совершенно нелинейными функциями (короче, *APN*-функциями). Впервые примеры *APN*-функций были указаны В. А. Башевым и подробно исследованы Б. А. Егоровым в 1968–69 годах. Этими примерами были подстановки обращения ненулевых элементов полей P_n при любых нечетных n . В последующем было найдено много различных *APN*-функций (см. обзоры [4, 6], а также [12]). Однако в практически интересном случае четного n до 2009 г. *APN*-функции полей характеристики 2 не были найдены. Первый пример *APN*-подстановки при четном n для поля характеристики 2 приведен в [5], где построена *APN*-подстановка поля P_6 . Для других четных значений n вопрос о существовании *APN*-подстановок остается открытым.

3. О подстановках с нетривиальной линейной структурой

В [9] были введены понятия линейной и аддитивной структур отображения

$$f: V \rightarrow V,$$

где V — конечномерное линейное пространство над полем $GF(p^t)$ характеристики p . Отображение f имеет *аддитивную структуру*, если существует такое $a \in V$, что

$$f(x + a) = f(x) + f(a) + f(0) \quad \text{для любого } x \in V. \quad (2)$$

Отображение f имеет *линейную структуру*, если существуют такие $a, c \in V \setminus \{0\}$, что

$$f(x + ca) = f(x) + c(f(a) + f(0)) \quad \text{для любого } x \in V. \quad (3)$$

В [3] аналогичное понятие введено для отображений пространства V над полем $GF(p^t)$ на его подпространство над подполем $GF(p^s)$ поля $GF(p^t)$. Элемент a из (2), (3) называется соответственно *аддитивным* и *линейным транслятором* функции f . В [3, 9] изучаются свойства систем аддитивных и линейных трансляторов функций. В частности, доказано, что множество всех линейных трансляторов функции f является группой.

Понятия аддитивной структуры и аддитивного транслятора можно определить также для отображений произвольной группы $(\Omega, +)$ на ее подгруппу.

Утверждение 2. Пусть $(\Omega, +)$ — любая коммутативная группа порядка N , G — ее правое регулярное представление и h — подстановка из симметрической группы $S(\Omega)$ подстановок множества Ω . Если $h(0) = 0$ и функция h имеет по крайней мере два ненулевых аддитивных транслятора, то множество $(Gh)^3$ не является 2-транзитивным.

Доказательство. Допустим, что множество подстановок $(Gh)^3$ является 2-транзитивным, т.е. 2-транзитивно множество $GhGhG$. Это означает, что при любых таких ненулевых элементах $a, b, c, d \in \{\Omega\}$, что

$$a \neq b, \quad c \neq d,$$

система уравнений

$$\begin{aligned} ((a+x)h+y)h+z &= c, \\ ((b+x)h+y)h+z &= d \end{aligned} \tag{4}$$

имеет решение относительно неизвестных x, y, z со значениями в группе $(\Omega, +)$. Выберем в качестве a, b аддитивные трансляторы подстановки h , которые существуют по условию утверждения. Тогда, пользуясь определением аддитивного транслятора подстановки h , систему уравнений (4) можно будет преобразовать к равносильной ей системе уравнений вида

$$\begin{aligned} ah^2 + (xh+y)h+z &= c, \\ bh^2 + (xh+y)h+z &= d. \end{aligned}$$

Вычитая из первого уравнения второе и пользуясь коммутативностью группы G , получим равенство

$$ah^2 - bh^2 = c - d. \tag{5}$$

Таким образом, система уравнений (4) разрешима лишь при условии (5). А так как при фиксированных a, b элементы c, d могут быть любыми различными и ненулевыми, то существуют c, d , при которых равенство (5) не выполняется. Следовательно, множество подстановок $(Gh)^3$ не является 2-транзитивным, и утверждение доказано. $\square$

Следствие. Если в обозначениях утверждения подстановка h является автоморфизмом группы $(\Omega, +)$, то множество $(Gh)^3$ не является 2-транзитивным.

4. О подстановке обращения элементов поля P_n при четном n

В некоторых блочных шифрах, в частности в шифрсистеме AES, при задании подстановки h используются подстановки вида $\tau\varphi$, где φ — автоморфизм группы $(P_n, \oplus)$. Группу $(P_n, \oplus)$ можно рассматривать также как n -мерное линейное пространство над полем $GF(2)$. Поэтому будет корректно использовать как терминологию теории групп, так и терминологию теории линейных пространств. В частности, подгруппа порядка 2^k группы $(P_n, \oplus)$ является подпространством размерности k .

Рассмотрим сначала случай, когда φ — тождественная подстановка, т.е. $\tau\varphi = \tau$. При четном $n > 2$ подстановки поля P_n не являются APN -функциями. Для любой такой подстановки матрица $Q_{G_n\tau G_n}$ симметрична и в каждой ее строке содержится лишь $2^{n-1} - 1$ ненулевых элементов: $2^{n-1} - 2$ двоек и одна четверка. Следовательно, в каждой строке число ненулевых элементов меньше половины длины строки, и потому вопрос о 2-транзитивности множества $(G_n\tau G_n)^2$ не является очевидным. Для его решения нам понадобится вспомогательное утверждение.

Утверждение 3. *Множество элементов поля P_n , обратных к номерам столбцов матрицы $Q_{G_n\tau G_n}$, имеющих ненулевые элементы в строке с номером a , вместе с нулем является подгруппой порядка 2^{n-1} группы $(P_n, \oplus)$, причем эта подгруппа равна T_na .*

Доказательство. В соответствии с определением элементов матрицы $Q_{G_n\tau G_n}$ ее элемент $q_{a,b}(\tau)$ равен числу решений уравнения

$$(a \oplus x)\tau \oplus x\tau = b \quad (6)$$

для $a, b \in P_n^*$, которое при $x \neq 0$, а биективной заменой $x = ay$ неизвестного x приводится к уравнению

$$y^2 \oplus y \oplus (1/ab) = 0. \quad (7)$$

Заметим, что уравнение (6) имеет решения $x = 0$ и $x = a$ только при $b = a^{-1}$, и в этом случае для нахождения остальных решений необходимо решить уравнение

$$y^2 \oplus y \oplus 1 = 0.$$

Последнее уравнение при четном n имеет ровно 2 решения в поле P_n , отличные от 0, a . Это элементы $\varepsilon, \varepsilon^2$, где ε — отличный от 1 корень кубичный из 1 в поле P_n . Значит, в этом случае уравнение (2) имеет ровно 4 решения. В остальных случаях оно либо не имеет решений, либо имеет 2 решения. Выясним теперь условия, при которых уравнение (6) имеет решения.

По доказанному выше $q_{a,b}(\tau) \neq 0$ в том и только том случае, когда разрешимо уравнение (6). При этом $q_{a,b}(\tau) = 4$, если $b = a^{-1}$, и $q_{a,b}(\tau) = 2$ или 0, если $b \neq a^{-1}$. Теперь для доказательства утверждения достаточно воспользоваться известным критерием разрешимости уравнения (7) (см., например, [3]): уравнение (7), а потому и (6), разрешимо тогда и только тогда, когда $\text{tr}(1/ab) = 0$, т. е. $(ab)^{-1} \in T_n$, и потому $b^{-1} \in T_n^* a$, что и требовалось доказать. $\square$

Замечание 2. В группе $(P_n, \oplus)$ существует ровно $2^n - 1$ подгрупп порядка 2^{n-1} , и они исчерпываются подгруппами вида $T_n a$ при $a = 1, 2, \dots, 2^n - 1$.

Обозначим множество всех групп вида $T_n a$, $a = 1, 2, \dots, 2^n - 1$, через M_n .

Утверждение 4. Если $n > 2$, то множество подстановок $(G_n \tau)^3$ является 2-транзитивным.

Доказательство. Выше было отмечено, что множество $(G_n \tau)^3$ является 2-транзитивным тогда и только тогда, когда

$$Q_{G_n \tau G_n}^2 > 0.$$

Элемент строки с номером c и столбца с номером d матрицы $(Q_{G_n \tau G_n})^2$ получается умножением строки с номером c матрицы $Q_{G_n \tau G_n}$ на ее столбец с номером d , или, в силу симметрии матрицы $Q_{G_n \tau G_n}$, строки с номером c на строку с номером d .

Отсюда и из утверждения 1 следует, что $(Q_{G_n \tau G_n})^2 > 0$ в том и только том случае, когда для любых $c, d \in P_n^*$ выполняется условие

$$T_n c \cap T_n d \neq \{0\}.$$

Так как $T_n c, T_n d$ — подгруппы порядка 2^{n-1} и $n > 2$, то их пересечение является подгруппой порядка 2^{n-1} при их совпадении и подгруппой порядка 2^{n-2} в противном случае. Следовательно, всегда $T_n c \cap T_n d \neq \{0\}$, т. е. $(Q_{G_n \tau G_n})^2 > 0$. Значит, множество $(G_n \tau)^3$ является 2-транзитивным, и утверждение 4 доказано. $\square$

5. О подстановках $\tau\varphi$ с нетождественным автоморфизмом φ

Докажем предварительно несколько вспомогательных утверждений.

Лемма 1. Пусть A — произвольное непустое подмножество из P^* и его ранг (как системы n -мерных векторов над $GF(2)$) равен r . Если A содержит элемент, являющийся суммой четного числа других элементов из A , то $A \cap H \neq \{0\}$ для любой подгруппы $H \in M_n$. В противном случае M_n содержит ровно 2^{n-r} групп, не пересекающихся с множеством A .

Доказательство. Пусть $H = T_n a$ и $A \cap H = \emptyset$. Тогда, учитывая, что H — подгруппа индекса 2, получаем: $A \subset H \oplus c$, где $c \notin H$. Так как характеристика поля P равна 2, то множество $H \oplus c$ (а потому и A) не может содержать элемент, являющийся суммой четного числа других его элементов.

Пусть теперь выполнено последнее условие и $B = \{b_1, \dots, b_r\}$ — любой базис системы A . По условию каждый элемент из $A \setminus B$ является суммой нечетного числа элементов из B . Поэтому

$$A \cap H = \emptyset \Leftrightarrow B \cap H = \emptyset.$$

Найдем число всех групп $H \in M_n$, не пересекающихся с B . Обозначим через $M_n(X)$ множество всех групп $H \in M_n$, содержащих подмножество $X \in B$. Используя дополнения X до базисов групп порядка $2m-1$, нетрудно подсчитать, что

$$|M(X)| = 2^{n-|X|} - 1. \quad (8)$$

Для примера покажем, как это сделать в случае $n=4$. Возьмем $X = \{1, 2\}$ и выясним, сколько различных подгрупп из M_n можно получить, дополняя X до базиса из четырех элементов. Наименьший из элементов поля P_4 , которым можно дополнить X до линейно независимого подмножества, равен 4. К множеству $(1, 2, 4)$ нельзя добавлять 3, 5, 6, 7 и можно добавить 8, 9, 10, 11, 12, 13, 14, 15. Легко видеть, что добавление к $(1, 2, 4)$ любого из этих элементов приводит к базису одной и той же группы. Аналогично покажем, что к линейно независимым системам $(1, 2, 5)$ и $(1, 2, 6)$ можно путем дополнения до базиса получить лишь по одной группе. В результате будет получено три различных группы из M_n . Все другие дополнения множества $(1, 2)$ до базиса приводят к тем же трем группам.

Используя формулу (8) и метод включения-исключения, найдем число подгрупп, пересекающихся с B :

$$|M_n(b_1) \cup M_n(b_1) \cup \dots \cup M_n(b_r)| = 2^n - 2^{n-r} - 1. \quad (9)$$

Отсюда, учитывая, что общее число подгрупп порядка $2^n - 1$ группы $(P_n, \oplus)$ равно $2^n - 1$, получим требуемый результат 2^{n-r} . $\square$

Лемма 2. Для любого подмножества

$$A = \{a_1, a_2, \dots, a_k\} \subseteq P_n^*$$

имеет место равенство

$$|T_n a_1 \cap T_n a_2 \cap \dots \cap T_n a_k| = 2^{n-r},$$

где r — ранг системы элементов

$$a_1^{-1}, a_2^{-1}, \dots, a_k^{-1}. \quad (10)$$

Доказательство. Обозначим буквой B базис системы (10). Используя определение группы $T_n a$, свойство линейности функции tr и утверждение 3, получим:

$$\bigcap_{a \in A} T_n a = \bigcap_{b \in B} T_n b = \{b^{-1} \in P_n : \exists b_i \in B, \text{tr}(1/bb_i) = 0\} \cup \{0\}.$$

Следовательно, число $|\bigcap_{a \in A} T_n a|$ на единицу больше числа подгрупп $T_n b$, пересекающихся с множеством B . Отсюда и из формулы (9) для числа подгрупп при $X = B$ получаем требуемый результат 2^{n-r} . $\square$

Утверждение 5. Пусть $A = \{a_1, a_2, \dots, a_k\}$ — любая система различных элементов из P_n^* , r — ранг системы элементов (10) и $N(a_1, a_2, \dots, a_k)$ — число нулей в сумме строк с номерами $a_1, a_2, \dots, a_k$ матрицы $Q_{G_n \tau G_n}$. Тогда $N(a_1, a_2, \dots, a_k) = 0$ в том и только том случае, когда в системе (10) есть элемент, представимый в виде суммы четного числа других элементов из (10), и $N(a_1, a_2, \dots, a_k) = 2^{n-r}$ в противном случае.

Доказательство. Обозначим через $Q_{G_n \tau G_n}(a_1, a_2, \dots, a_k)$ подматрицу матрицы $Q_{G_n \tau G_n}$, составленную из ее строк с номерами $a_1, a_2, \dots, a_k$. Так как нуль является суммой лишь нулей, то искомое число $N(a_1, a_2, \dots, a_k)$ равно числу нулевых столбцов матрицы $Q_{G_n \tau G_n}(a_1, a_2, \dots, a_k)$.

Пусть в системе (10) существует элемент, являющийся суммой четного числа других элементов из (10). Не теряя общности, можно считать, что

$$a_i^{-1} = a_1^{-1} \oplus \dots \oplus a_{2s}^{-1}. \quad (11)$$

Допустим, что в матрице $Q_{G_n \tau G_n}(a_1, a_2, \dots, a_k)$ столбец с номером b нулевой. Тогда по утверждению 1 выполняются равенства

$$\text{tr}(1/ba_1) = \dots = \text{tr}(1/ba_k) = 1. \quad (12)$$

Полученное противоречие и доказывает, что в этом случае $N(a_1, \dots, a_k) = 0$.

Пусть в системе (10) нет элементов, являющихся суммой четного числа других элементов из (10). Зафиксируем любой базис системы (10). Не теряя общности, будем считать, что базисом системы (10) является ее подсистема $a_1^{-1}, a_2^{-1}, \dots, a_r^{-1}$.

Пусть матрица $Q_{G_n \tau G_n}(a_1, a_2, \dots, a_k)$ имеет нулевые столбцы с номерами $b_1, \dots, b_s$. Тогда $\{b_1, \dots, b_s\}$ есть максимальное подмножество элементов из P_n^* , удовлетворяющих условиям

$$\text{tr}(1/a_j b_i) = 1, \quad i = 1, \dots, s, \quad j = 1, \dots, k. \quad (13)$$

Так как каждый из элементов $a_{r+1}^{-1}, \dots, a_k^{-1}$ является суммой нечетного числа элементов системы (10), то равенства системы (13) выполняются тогда и только тогда, когда выполняются равенства

$$\text{tr}(1/a_j b_i) = 1, \quad i = 1, \dots, s, \quad j = 1, \dots, r.$$

По утверждению 3 условие $\text{tr}(1/a_j b_i) = 1$ означает, что

$$q_{a_j, b_i}(\tau) = 0, \quad (b_i^{-1} a_j^{-1}) \notin T_n \quad \text{и} \quad b_i^{-1} \notin T_n^* a_j.$$

Следовательно, b_i^{-1} не принадлежит пересечению групп $T_n^* a_j, j = 1, 2, \dots, r$. Значит, b_i^{-1} принадлежит пересечению смежных классов по подгруппам $T_n^* a_j, j = 1, 2, \dots, r$. Очевидно, что порядок пересечения этих смежных классов равен порядку пересечения соответствующих подгрупп и по лемме 2 равен 2^{n-r} . А так как все элементы $q_{a_j, b_i}(\tau) = 0$, то матрица $Q_{G_n \tau G_n}(a_1, a_2, \dots, a_r)$ содержит 2^{n-r} нулевых столбцов.

По условию элемент $a_t^{-1}, t = r + 1, \dots, k$, представляется через базис системы (10) в виде суммы нечетного числа слагаемых. Отсюда по свойству аддитивности функции tr имеет место равенство $\text{tr}(1/a_t b_i) = 1$. Следовательно, теми же рассуждениями получим аналогичный результат для матрицы $Q_{G_n \tau G_n}(a_1, a_2, \dots, a_r, a_{r+1}, \dots, a_k)$, т.е. эта матрица имеет 2^{n-r} нулевых столбцов. Утверждение полностью доказано. $\square$

Ранее мною было доказано, но не опубликовано, одно достаточное условие 2-транзитивности множества $(G_n \tau \varphi)^3$. Приведем здесь его формулировку.

Если $\varphi \in \text{Aut}(P, \oplus)$ и преобразование $\tau \varphi \tau$ действует линейно хотя бы на одной из подгрупп ранга 3 группы $(P_n, \oplus)$, то система подстановок $(G_n \tau \varphi)^3$ является 2-транзитивной.

Теперь укажем критерий 2-транзитивности множества $(G_n \tau \varphi)^3$.

Утверждение 6. *Если φ — автоморфизм группы $(P_n, \oplus)$ и $n > 2$, то множество подстановок $(G_n \tau \varphi)^3$ является 2-транзитивным тогда и только тогда, когда для любого элемента $a \in P_n^*$ множество $T_n a \tau \varphi^{-1} \tau$ содержит ненулевой элемент, равный сумме четного числа других ненулевых элементов.*

Доказательство. При тождественном отображении φ утверждение очевидно и доказано выше. Поэтому будем предполагать, что φ не является тождественным. По определению матрицы $Q_{G_n \tau \varphi G_n}$ ее элемент $q_{a,b}(\tau \varphi)$ равен числу решений уравнения

$$(a \oplus x) \tau \varphi \oplus x \tau \varphi = b, \quad (14)$$

которое в силу линейности отображения φ равносильно уравнению

$$(a \oplus x) \tau \oplus x \tau = b \varphi^{-1}. \quad (15)$$

Обозначим через $b_1, b_2, \dots, b_{2^{n-1}-1}$ номера столбцов матрицы $Q_{G_n \tau \varphi G_n}$, в которых элементы строки с номером a отличны от 0. По утверждению 2

$$\{b_1, b_2, \dots, b_{2^{n-1}-1}\} = (T_n a)^{-1} = T_n a \tau.$$

Тогда

$$\{b_1 \varphi^{-1} \tau, b_2 \varphi^{-1} \tau, \dots, b_{2^{n-1}-1} \varphi^{-1} \tau\} = (T_n a)^{-1} = T_n a \tau \varphi^{-1} \tau.$$

Таким образом, обратные к ненулевым элементам в строке с номером $a\tau\varphi^{-1}\tau$ матрицы $Q_{G_n\tau\varphi G_n}$ образуют множество $T_na\tau\varphi^{-1}\tau$. Тогда ненулевые элементы указанной строки образуют множество $T_na\tau\varphi^{-1}$. Поэтому в произведении матриц $Q_{G_n\tau\varphi G_n}$ и $Q_{G_n\tau\varphi G_n}$ строка с номером $a\tau\varphi^{-1}\tau$ равна сумме строк матрицы $Q_{G_n\tau\varphi G_n}$ с номерами из $T_na\tau\varphi^{-1}$. Тогда по леммам 1, 2 эта строка не будет содержать нулей в том и только том случае, когда множество $T_na\tau\varphi^{-1}\tau$ содержит ненулевой элемент, равный сумме четного числа других ненулевых элементов. Следовательно, множество подстановок $(G_n\tau\varphi)^3$ является 2-транзитивным тогда и только тогда, когда указанное условие выполняется для любого $a \neq 0$. Утверждение доказано. $\square$

В связи с утверждением 6 естественно возникают две задачи.

- 1) Выяснить, в каких случаях выполняется условие
 (*) множество $(T_na)\tau\varphi^{-1}\tau$ содержит отличный от нуля элемент, равный сумме четного числа других ненулевых элементов этого множества.
- 2) В каких из найденных в задаче 1) случаях преобразование φ является автоморфизмом группы $(P_n, \oplus)$?

Рассмотрим решения этих задач.

1) Для решения задачи 1) представим группу $(P_n, \oplus)$ в виде объединения множеств $T_na \cup K_a$, где K_a — смежный класс группы $(P_n, \oplus)$ по подгруппе T_na , а множество $(T_na)\tau\varphi^{-1}\tau$ — в виде объединения $A \cup B$, где $A \subseteq T_na, B \subseteq K_a$. Из условия видно, что

$$A \cap B = \emptyset \quad \text{и} \quad |A \cup B| = |(T_na)\tau\varphi\tau| = 2^{n-1}.$$

Если $B = \emptyset$, то $A = T_na$ — группа, и при $n > 2$ условие (*) выполняется.

Пусть $B \neq \emptyset$. Тогда ранг множества B как подмножества линейного пространства размерности n над полем $GF(2)$ не больше n .

Пусть $\text{rang } B = n$. Тогда в B существует $k_1 \leq 2^{n-1} - 1$ ненулевых элементов, представимых суммами с четным числом слагаемых, и $k_2 \leq 2^{n-1}$ элементов, представимых суммами с нечетным числом слагаемых из любого фиксированного базиса. Так как $B \subset K_a$, то первые суммы содержатся в A , а вторые суммы входят в B . Отсюда следует, что условие (*) может выполняться лишь при $A = \{0\}, |B| = 2^{n-1} - 1$. Но тогда в $A \cup B$ нет ненулевых элементов, представимых в виде суммы четного числа элементов, и потому условие (*) не выполняется.

Если $\text{rang } B = n - 1$, то, вычисляя суммы из четного числа слагаемых элементов базиса системы B , получим 2^{n-2} элементов, включая 0, которые входят в $T_n a$, и столько же элементов, представимых суммами с нечетным числом слагаемых. Следовательно, условие (*) выполняется только в том случае, когда A состоит из $k > 0$ ненулевых элементов, представимых суммами с нечетным числом слагаемых. Тогда

$$|A| = k + 1, \quad |B| = 2^{n-1} - k - 1, \quad A \cup B = (T_n a)\tau\varphi^{-1}\tau.$$

А так как $|T_n\tau\varphi^{-1}\tau| = 2^{n-1}$, то при условии (*) остается лишь одна возможность: $|A| = |B| = 2^{n-2}$. Следовательно, при любой фиксированной линейно независимой системе из $n - 1$ элементов множества K_a существует единственный вариант для множества $A \cup B = (T_n a)\tau\varphi^{-1}\tau$, при котором выполняется условие (*).

Пусть $\text{rang } B \leq n - 2$. Тогда в B содержится $k \leq 2^{n-2} - 1$ ненулевых элементов. А так как $|A \cup B| = 2^{n-1}$, то в A входит не менее $2^{n-2} + 1$ элементов, и потому в A есть ненулевой элемент, представимый суммой четного числа ненулевых элементов, т. е. условие (*) выполняется.

2) Выясним, для каких множеств $(T_n a)\tau\varphi\tau$, удовлетворяющих условию (*), отображение φ является автоморфизмом. Если $B = \emptyset$, то $(T_n a\tau)\varphi = T_n a\tau$. Так как множество $T_n a\tau$ не является группой и $|T_n a\tau| = 2^{n-1}$, то $\text{rang}(T_n a\tau) = n$. Взяв два базиса в $T_n a\tau$, построим линейное преобразование группы $(P_n, \oplus)$, переводящее $T_n a\tau$ в $T_n a\tau$. Пусть $\text{rang } B \leq n - 1$. По условию $A \cup B = (T_n a)\tau\varphi^{-1}\tau$, т. е.

$$(A \cup B)\tau\varphi = T_n a\tau.$$

Так как $|T_n\tau| = 2^{n-1}$ и $T_n\tau$ не является группой, то $\text{rang}(T_n\tau) = n$. Из аналогичных соображений следует также, что $\text{rang}((A \cup B)\tau) = n$. Тогда любое биективное отображение любого базиса системы $(A \cup B)\tau$ в любой базис системы $T_n a\tau$ можно по линейности продолжить до линейного отображения группы $(P_n, \oplus)$ так, чтобы $(A \cup B)\tau$ переходило в $T_n a\tau$. В итоге получим искомое отображение φ .

Пример. Рассмотрим случай, когда $n = 4$. Не теряя общности, можно положить, что a есть единица поля P_4 . При выполнении условия (*) возможен лишь случай $\text{rang } B = 3$. Выберем в B линейно независимую систему из трех элементов, например 8, 11, 13. Тогда их суммы с нечетным числом слагаемых образуют множество $B = \{8, 11, 13, 14\}$, а суммы с четным числом слагаемых из B образуют множество $A = \{0, 3, 5, 6\}$. Отсюда получаем:

$$T_4\tau = \{0, 1, 9, 14, 13, 11, 7, 6\}, \quad (A \cup B)\tau = \{0, 14, 11, 7, 3, 15, 5, 4\}.$$

Заметим, что в $T_4\tau$ есть соотношения

$$6 \oplus 1 = 7, \quad 9 \oplus 14 = 7, \quad 13 \oplus 11 = 6,$$

и в $(A \cup B)\tau$ есть соотношения

$$5 \oplus 14 = 11, \quad 15 \oplus 4 = 11, \quad 7 \oplus 3 = 4.$$

Так как искомое преобразование φ должно быть автоморфизмом группы $(P_4, \oplus)$, то оно сумму элементов из $T_4\tau$ должно переводить в сумму элементов из $(A \cup B)\tau$.

Учитывая соотношения в $T_4\tau$ и в $(A \cup B)\tau$, найдем отображение $T_4\tau$ в $(A \cup B)\tau$, которое по линейности дополним до преобразования поля P_4 . В итоге получим линейную подстановку φ^{-1} :

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 15 & 1 & 14 & 5 & 10 & 4 & 11 & 13 & 2 & 12 & 3 & 8 & 7 & 9 & 6 \end{pmatrix}.$$

Подстановка, обратная к построенной, и будет искомым автоморфизмом φ .

6. О биективных разностно 4-равномерно нелинейных преобразованиях поля P_n при четном n

Так как уравнение (1) над P_n может иметь лишь четное число решений, то по разностным свойствам ближайшими к APN-функциям являются разностно 4-равномерно нелинейные преобразования. Такие биективные преобразования поля P_n существуют при любом n . К ним относится, в частности, функция обращения τ ненулевых элементов поля P_n при любом четном n , $\tau(0) = 0$.

Известные разностно 4-равномерно нелинейные преобразования приведены, например, в [7, 10, 12–14]. Для этих функций найдены точные значения или оценки таких важных параметров, как нелинейность и алгебраическая степень. В [8] построен новый класс биективных разностно 4-равномерно нелинейных булевых функций поля P_n при четном n . Для этого выбирается некоторая система подмножеств U поля P_n , определяемых условиями

- 1) если $x \in U$, то и $x \oplus 1 \in U$,
- 2) $\text{tr } x = 1$ для любого $x \in U$,

и по каждому из этих подмножеств U определяется искомая функция F как разветвление функций $\tau(x)$ и $\tau(x \oplus 1)$ под управлением множества U , а именно:

$$F(x) = \begin{cases} \tau(x \oplus 1), & x \in U, \\ \tau(x), & x \notin U. \end{cases}$$

Полученные таким образом функции имеют максимальную степень, высокую нелинейность и при $n \geq 12$ не являются CCZ-эквивалентными известным разностно 4-равномерно нелинейным степенным и квадратичным функциям.

Рассмотрим подстановку более общего вида:

$$F_c(x) = \begin{cases} \tau(x \oplus c), & x \in U, \\ \tau(x), & x \notin U, \end{cases}$$

где U — любое подмножество, а c — любой элемент из P^* .

Утверждение 7. При указанной выше подстановке F_c множество подстановок $(G_n F_c)^3$ является 2-транзитивным.

Доказательство. Пусть

$$f_1(x) = \tau(x \oplus c),$$

$$f_2(x) = \tau(x).$$

Тогда

$$Q_{G_n f_2 G_n} = Q_{G_n \tau G_n} = (q_{a,b}(\tau)),$$

$$Q_{G_n f_1 G_n} = (q_{a,b}(f_1)),$$

где $q_{a,b}(\tau)$ — число решений уравнения

$$\tau(a \oplus x) \oplus \tau(x) = b, \quad (16)$$

$q_{a,b}(f_1)$ — число решений уравнения

$$\tau(a \oplus x \oplus c) \oplus \tau(x \oplus c) = b. \quad (17)$$

Очевидно, что уравнение (17) разрешимо тогда и только тогда, когда разрешимо уравнение (16). Следовательно, матрица $Q_{G_n F_c G_n}$ совпадает с матрицей $Q_{G_n \tau G_n}$.

Отсюда по утверждению 4 имеем: множество $(G_n F_c)^3$ является 2-транзитивным, и утверждение 7 доказано. $\square$

Список литературы

- [1] Глухов М. М., “О числовых параметрах, связанных с заданием конечных групп системами образующих элементов”, *Труды по дискретной математике*, **1** (1997), 43–66.
- [2] Глухов М. М., “О 2-транзитивных произведениях регулярных групп подстановок”, *Труды по дискретной математике*, **3** (2000), 37–52.
- [3] Сачков В. Н., “Трансляторы и трансляции дискретных функций”, *Труды по дискретной математике*, **9** (2006), 253–268.
- [4] Тужилин М. Э., “Почти совершенно нелинейные функции”, *Прикл. дискретн. матем.*, № 3 (2009), 14–20.
- [5] Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J., “An APN permutation in dimension six”, *Contemporary Mathematics*, **518**, Providence, RI: Amer. Math. Soc., 2010, 33–42.
- [6] Budaghyan L., Carlet C., Leander G., “Constructing new APN functions from known ones”, *Finite Field Appl.*, **15**:2 (2009), 150–159.
- [7] Carlet C., “On known and new differentially uniform functions”, *Lect. Notes Comput. Sci.*, **6812**, 2011, 1–15.
- [8] Charpin P., Kyureghyan G., “When does $G(x) + \gamma \text{Tr}(H(x))$ permute F_{p^n} ?”, *Finite Field Appl.*, **15**:5 (2009), 615–632.
- [9] Lai X., “Additive and linear structures of cryptographic function”, FSE 1994, *Lect. Notes Comput. Sci.*, **1008**, 1994, 75–85.
- [10] Nyberg K., “Differentially uniform mappings for cryptography”, EUROCRYPT’93, *Lect. Notes Comput. Sci.*, **765**, 1994, 55–64.
- [11] Nyberg K., “On the construction of highly nonlinear permutations”, EUROCRYPT-92, *Lect. Notes Comput. Sci.*, **658**, 1993, 92–98.
- [12] Tan Y., Qu L., Tan C., Li C., “New families of differentially 4-uniform permutations over $F_{2^{2k}}$ ”, SETA 2012, *Lect. Notes Comput. Sci.*, **7280**, 2012, 25–39.
- [13] Tang D., Carlet C., Tang X., “Differentially 4-uniform bijections by permuting the inverse function”, **639** (2013), <https://eprint.iacr.org/2013/639>.
- [14] Qu L., Tan Y., Tan C., Li C., “Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method”, *IEEE Trans. Inf. Theory*, **59**:7 (2013), 4675–4686.