Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Функциональные схемы, задающие семейства подстановок на пространстве $GF(2)^N$, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 3, 81–87

DOI: <https://doi.org/10.4213/mvk301>

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: 44.207.124.84

26 апреля 2023 г., 16:39:13

**Функциональные схемы,
задающие семейства подстановок
на пространстве $GF(2)^N$**

Ф. М. Малышев

*Математический институт им. В. А. Стеклова
Российской академии наук, Москва*

Получено 29.IV.2019

Аннотация. Рассматриваются семейства отображений булевых векторных пространств, задаваемых функциональными схемами, состоящими из линейных и нелинейных функциональных элементов. Приводятся условия на структуру соединений элементов схемы и линейные функциональные элементы, обеспечивающие биективность отображений при любом выборе нелинейных функциональных элементов.

Ключевые слова: функциональные схемы, регулярные регистры сдвига, схемы Фейстеля, линейная среда, биективные отображения

**Functional circuits defining families of permutations
of the space $GF(2)^N$**

F. M. Malyshev

Steklov Mathematical Institute of Russian Academy of Sciences, Moscow

Abstract. We consider families of mappings of Boolean vector spaces which are defined by functional circuits consisting of linear and nonlinear functional elements. Conditions on the structure of connections between circuit elements and on the linear functional elements which guarantee the bijectivity of mappings for any choice of nonlinear functional elements are given.

Keywords: functional circuits, regular shift registers, Feistel schemes, linear medium, bijective mappings

В статье описаны способы построения семейств функциональных схем, реализующих биективные отображения $F: V_N \rightarrow V_N$, $V_N = GF(2)^N$. Функциональные схемы состоят из нелинейных и линейных функциональных элементов. Совокупность последних задает линейную среду функциональной схемы [1]. Представляют интерес необходимые и достаточные условия на линейную среду, при которых биективность отображения F сохраняется после произвольных замен отображений, реализуемых нелинейными функциональными элементами (с сохранением их мест в функциональной схеме). Такие функциональные схемы (точнее, их линейную среду) будем называть устойчивыми. Примерами устойчивых функциональных схем являются регулярные регистры сдвига и их частный случай – схемы Фейстеля, широко используемые в криптографии [2].

Функциональная схема $\mathcal{F}$, задающая подстановку

$$F: V_N \rightarrow V_N, \quad V_N \ni a \mapsto b = F(a) \in V_N, \quad (1)$$

может представляться (см. [1]) последовательностью выполняемых в определенном порядке линейных и нелинейных отображений. Эту последовательность можно также рассматривать как схему компьютерной программы без циклов.

Пусть все нелинейные отображения содержатся среди отображений

$$f_i: V_{n_i} \rightarrow V_{m_i}, \quad x_i \mapsto y_i = f_i(x_i), \quad i = 1, \dots, k, \quad (2)$$

которые выполняются в этой программе в указанном порядке. Через $x_i \in V_{n_i}$ обозначено значение аргумента отображения f_i , которое в конечном счете выражается через $a \in V_N$ и является результатом выполнения некоторых предыдущих операций f_j , $j = 1, \dots, i-1$, и некоторых линейных операций, не числящихся среди f_i , $i = 1, \dots, k$. В промежутках между отображениями f_i , $i = 1, \dots, k$, выполняются линейные операции, каждая из которых является либо суммированием нескольких двоичных слагаемых, либо узлом размножения на несколько выходов: $x \mapsto (x, \dots, x)$.

Выписывать по отдельности линейные операции необходимости нет. Ограничимся тем, что для некоторых двоичных матриц c_{ij} размера $m_i \times n_j$, $i = 0, 1, \dots, k$, $j = 1, \dots, k, k+1$, $m_0 = N$, $n_{k+1} = N$, можно записать $x_j = ac_{0j} + \sum_{i=1}^{j-1} y_i c_{ij}$, $j = 1, \dots, k$, $b = ac_{0,k+1} + \sum_{i=1}^k y_i c_{i,k+1}$. Полагая $c_{ij} = 0$ при $i \geq j$, из блоков c_{ij} можно составить матрицу C размера $(N + \sum_{i=1}^k m_i) \times (\sum_{i=1}^k n_i + N)$, для которой

$$(a, y_1, \dots, y_k)C = (x_1, \dots, x_k, b). \quad (3)$$

Матрицу

$$C = C_{\mathcal{F}} = \begin{pmatrix} c_{01} & c_{02} & c_{03} & \dots & c_{0,k-1} & c_{0k} & c_{0,k+1} \\ 0 & c_{12} & c_{13} & \dots & c_{1,k-1} & c_{1k} & c_{1,k+1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & c_{k-1,k} & c_{k-1,k+1} \\ 0 & 0 & 0 & \dots & 0 & 0 & c_{k,k+1} \end{pmatrix} \quad (4)$$

будем называть матрицей линейной среды функциональной схемы $\mathcal{F}$. В ней аккумулированы линейные операции, не числящиеся среди f_i , $i = 1, \dots, k$. Линейная среда, состоящая из линейных преобразований и обозначаемая той же буквой C , сама является функциональной схемой. Она получается удалением из функциональной схемы $\mathcal{F}$ каждого функционального элемента f_i , $i = 1, \dots, k$, с сохранением n_i его двоичных входов, которые превращаются в выходы линейной среды C , и с сохранением m_i его двоичных выходов, которые становятся входами линейной среды C . Линейная среда задает линейное отображение $C : V_{N+\sum_{i=1}^k m_i} \rightarrow V_{\sum_{i=1}^k n_i+N}$ в соответствии с равенством (3).

Функциональная схема $\mathcal{F}$ тем самым представляется линейной средой C , в которую вживляются конкретные функциональные элементы $f_i : V_{n_i} \rightarrow V_{m_i}$, $i = 1, \dots, k$.

Определение. Линейную среду $C = C_{\mathcal{F}}$ функциональной схемы $\mathcal{F}$ называем *устойчивой*, если при замене отображений $f_i : V_{n_i} \rightarrow V_{m_i}$ любыми другими отображениями $f'_i : V_{n_i} \rightarrow V_{m_i}$, $i = 1, \dots, k$, реализуемое функциональной схемой отображение (1) остается биективным.

Теорема. Для устойчивости линейной среды, заданной матрицей (4), достаточно выполнения условий

$$c_{0,k+1} \in GL(N, 2), \quad (5)$$

$$c_{i,k+1}c_{0,k+1}^{-1}c_{0,i} = 0, \quad i = 1, \dots, k, \quad (6)$$

$$c_{i,k+1}c_{0,k+1}^{-1}c_{0,j} = c_{ij}, \quad 1 \leq i < j \leq k. \quad (7)$$

Условия (5) и (6) являются необходимыми для устойчивости линейной среды.

Примеры устойчивой линейной среды, для которой условие (7) не выполняется, строятся уже для $k = 2$ и $N = n_i = m_i = 1$, $i = 1, 2$. Тогда $x_1 = ac_{01}$, $x_2 = ac_{02} + y_1c_{12}$, $b = ac_{03} + y_1c_{13} + y_2c_{23}$, $y_1 = f_1(x_1) = \alpha x_1 + \gamma$, $y_2 = f_2(x_2) = \beta x_2 + \delta$, где константы $\alpha, \beta, \gamma, \delta \in GF(2)$ могут быть

произвольными, и при каждой их комбинации $(\alpha, \beta, \gamma, \delta) \in V_4$ зависящее от $(\alpha, \beta, \gamma, \delta)$ отображение $F: GF(2) \rightarrow GF(2)$, $a \mapsto b = F(a)$, $F(a) = a(c_{03} + \alpha c_{01}c_{13} + \beta c_{02}c_{23} + \alpha\beta c_{01}c_{02}c_{23}) + \varepsilon$, должно быть биективным. Здесь ε – не влияющий на биективность отображения F свободный член. В результате собственно биективность отображения F равносильна тождеству $c_{03} + \alpha c_{01}c_{13} + \beta c_{02}c_{23} + \alpha\beta c_{01}c_{02}c_{23} = 1$, которое должно выполняться для любых $(\alpha, \beta, \gamma, \delta) \in V_4$, поэтому $c_{03} = 1$ (необходимое условие (5)), $c_{01}c_{13} = c_{02}c_{23} = 0$ (необходимые условия (6)) и $c_{01}c_{12}c_{23} = 0$. Среди 17 решений последней системы из четырех равенств имеется 8 решений, для которых условие $c_{12} = c_{13}c_{02}$ (см. (7)) не выполняется. Например, $c_{01} = c_{23} = 0$, а c_{12}, c_{13}, c_{02} – любые, лишь бы $c_{12} \neq c_{13}c_{02}$. Кроме указанных 4 решений, имеются еще 4 таких решения: $c_{01} = c_{02} = 0$, $c_{12} = c_{23} = 1$, c_{13} – любое, и $c_{13} = c_{23} = 0$, $c_{01} = c_{12} = 1$, c_{02} – любое.

При доказательстве необходимости условия (6) теоремы будут использованы две приводимые ниже леммы, относящиеся к матрицам над полем $GF(2)$.

Лемма 1. Пусть $a_i, b_i \in GF(2)$, $i = 1, \dots, N$, $E_N \in GL(N, 2)$ – единичная матрица. Тогда

$$\det \left(E_N + \begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix} (b_1, \dots, b_N) \right) = 1 + (b_1, \dots, b_N) \begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix}. \quad (8)$$

Доказательство. Если $a_i = 0$, $i \in \{1, \dots, N\}$, то левая и правая части в (8) от b_i не зависят. Аналогично, если $b_i = 0$, $i \in \{1, \dots, N\}$, то левая и правая части в (8) от a_i не зависят. Пусть $a_i = b_i = 1$, $i = 1, \dots, k$, а для $i > k$ либо $a_i = 0$, либо $b_i = 0$. Тогда левая часть в (8) равна $\det(E_k + J_k)$, где J_k – матрица размера $k \times k$, все элементы которой равны $1 \in GF(2)$. Правая часть в (8) равна $1 + k$, поэтому для доказательства леммы 1 достаточно убедиться в равенстве

$$\det(E_k + J_k) = 1 + k. \quad (9)$$

При четном k равенство (9) следует из соотношения $(E_k + J_k)(E_k + J_k) = E_k$. При нечетном k имеем $(E_k + J_k)(E_k + J_k) = E_k + J_k$ и в справедливости равенства (9) убеждаемся от противного, так как при $\det(E_k + J_k) = 1$ получили бы противоречивое равенство $E_k + J_k = E_k$.

Лемма 1 доказана.

Лемма 2. Пусть над полем $GF(2)$ заданы: матрица A размера $N \times n$, матрица B размера $m \times N$. Тогда матрица $E_N + AXB$ невырождена для всех матриц X размера $n \times m$, если и только если $BA = 0$.

Доказательство. Если $BA = 0$, то $(E_N + AXB)(E_N + AXB) = E_N + AXBAXB = E_N + 0 = E_N$.

Обратно. Пусть $E_N + AXB \in GL(N, 2)$ для любой матрицы X над полем $GF(2)$ размера $n \times m$ и $BA = D = \|d_{ij}\|$, $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$. Выберем в качестве X матрицу с единственной единицей в строке $l \in \{1, \dots, n\}$ и столбце $s \in \{1, \dots, m\}$. Тогда

$$E_N + AXB = E_N + \begin{pmatrix} a_{1l} \\ \vdots \\ a_{Nl} \end{pmatrix} (b_{s1}, \dots, b_{sN})$$

и по лемме 1 (см. (8)) имеем:

$$\begin{aligned} 1 = \det(E_N + AXB) &= \det \left(E_N + \begin{pmatrix} a_{1l} \\ \vdots \\ a_{Nl} \end{pmatrix} (b_{s1}, \dots, b_{sN}) \right) = \\ &= 1 + (b_{s1}, \dots, b_{sN}) \begin{pmatrix} a_{1l} \\ \vdots \\ a_{Nl} \end{pmatrix} = 1 + d_{sl}. \end{aligned}$$

Откуда заключаем, что $d_{sl} = 0$ и $BA = 0$, так как номера $s \in \{1, \dots, m\}$ и $l \in \{1, \dots, n\}$ могут быть произвольными.

Лемма 2 доказана.

Доказательство теоремы. Вначале проверим, что при условиях (5), (6), (7) отображения (1) являются подстановками для любых отображений (2). Напомним, что имеет место равенство (3), которое можно записать в виде

$$\begin{aligned} x_1 &= ac_{01}, \\ x_2 &= ac_{02} + y_1c_{12}, \\ x_3 &= ac_{03} + y_1c_{13} + y_2c_{23}, \\ &\dots \\ x_i &= ac_{0i} + y_1c_{1i} + \dots + y_{i-1}c_{i-1,i}, \\ &\dots \\ x_k &= ac_{0k} + y_1c_{1k} + \dots + y_{k-1}c_{k-1,k}, \\ b &= ac_{0,k+1} + y_1c_{1,k+1} + \dots + y_{k-1}c_{k-1,k+1} + y_kc_{k,k+1}. \end{aligned} \tag{10}$$

Биективность отображения F равносильна тому, что по заданному $b \in V_N$ однозначно восстанавливается $a \in V_N$, для которого $b = F(a)$. Проверим это. С помощью равенств (10), (2) и условий (5), (6), (7) последовательно будем по известному b восстанавливать $x_k, y_k = f_k(x_k), x_{k-1}, y_{k-1} = f_{k-1}(x_{k-1}), \dots, x_1, y_1 = f_1(x_1), a$.

Умножая обе части последнего равенства в (10) на $c_{0,k+1}^{-1}c_{0k}$, получим

$$\begin{aligned} bc_{0,k+1}^{-1}c_{0k} &= ac_{0,k+1}c_{0,k+1}^{-1}c_{0k} + y_1c_{1,k+1}c_{0,k+1}^{-1}c_{0k} + \dots + \\ &+ y_{k-1}c_{k-1,k+1}c_{0,k+1}^{-1}c_{0k} + y_kc_{k,k+1}c_{0,k+1}^{-1}c_{0k} = \\ &= ac_{0k} + y_1c_{1k} + \dots + y_{k-1}c_{k-1,k} + y_k \cdot 0 = x_k. \end{aligned}$$

Предположим, что $x_k, y_k = f_k(x_k), x_{k-1}, y_{k-1} = f_{k-1}(x_{k-1}), \dots, x_{i+1}, y_{i+1} = f_{i+1}(x_{i+1})$ уже восстановлены. Восстановим x_i , а затем и $y_i = f_i(x_i)$. Умножая обе части последнего равенства в (10) на $c_{0,k+1}^{-1}c_{0i}$ и используя i -е равенство в (10), получим

$$\begin{aligned} bc_{0,k+1}^{-1}c_{0i} &= ac_{0,k+1}c_{0,k+1}^{-1}c_{0i} + y_1c_{1,k+1}c_{0,k+1}^{-1}c_{0i} + \dots + y_{i-1}c_{i-1,k+1}c_{0,k+1}^{-1}c_{0i} + \\ &+ y_ic_{i,k+1}c_{0,k+1}^{-1}c_{0i} + y_{i+1}c_{i+1,k+1}c_{0,k+1}^{-1}c_{0i} + \dots + y_kc_{k,k+1}c_{0,k+1}^{-1}c_{0i} = \\ &= ac_{0i} + y_1c_{1i} + \dots + y_{i-1}c_{i-1,i} + y_i \cdot 0 + \varphi_i(y_{i+1}, \dots, y_k) = \\ &= x_i + \varphi_i(y_{i+1}, \dots, y_k). \end{aligned}$$

Здесь φ_i – известная функция, поэтому x_i из последней цепочки равенств восстанавливается однозначно.

Продолжая этот процесс, восстановим $x_{i-1}, y_{i-1} = f_{i-1}(x_{i-1}), \dots, x_1, y_1 = f_1(x_1)$. Затем, прибегая к последнему равенству в (10), найдем a .

Осталось доказать необходимость условий (5) и (6). Отображение (1) должно быть биективным при всех отображениях (2), поэтому оно будет биективно и для тождественно нулевых отображений f_i при всех $i = 1, \dots, k$. Тогда в последнем равенстве системы (10) всегда $y_1 = y_2 = \dots = y_k = 0$, следовательно, подстановка F задается равенством $b = F(a) = ac_{0,k+1}$, поэтому $c_{0,k+1} \in GL(N, 2)$.

Для проверки необходимости условия (6) положим $f_i(x_i) = x_iX$, где X – произвольная булева матрица размера $n_i \times m_i$, и $f_j(x_j) = 0$ для всех $x_j \in V_{n_j}$ и для всех $j \in \{1, \dots, k\} \setminus \{i\}$. Тогда в последнем равенстве (10) имеем $y_j = 0$ для всех $j \in \{1, \dots, k\} \setminus \{i\}$, поэтому

$$\begin{aligned} b &= F(a) = ac_{0,k+1} + y_ic_{i,k+1} = ac_{0,k+1} + x_iXc_{i,k+1} = \\ &= ac_{0,k+1} + ac_{0i}Xc_{i,k+1} = a(E_N + c_{0i}Xc_{i,k+1}c_{0,k+1}^{-1})c_{0,k+1}. \end{aligned}$$

Коль скоро F – подстановка, а $c_{0,k+1} \in GL(N, 2)$, то $E_N + c_{0i} X c_{i,k+1} c_{0,k+1}^{-1} \in GL(N, 2)$, причем для произвольной булевой матрицы X размера $n_i \times m_i$. Теперь справедливость условия (6) устанавливается с помощью леммы 2.

Теорема доказана.

Список литературы

- [1] Малышев Ф. М., “Двойственность разностного и линейного методов в криптографии”, *Математические вопросы криптографии*, **5:3** (2014), 35–47.
- [2] Шнайер Б., *Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си*, М. : ТРИУМФ, 2002.