УДК 513.6:517.1:519.48

РАСШИРЕННЫЕ ПОЛЯ, ПОРОЖДАЕМЫЕ ПРИМИТИВНЫМИ ПРОСТРАНСТВЕННЫМИ МАТРИЦАМИ ГАЛУА

Анатолий Белецкий

В статье рассмотрены вопросы формирования расширенных полей, элементами которых являются матрицы Галуа G, синтезируемые на основе образующих элементов ω и неприводимых полиномов f_n степени n. Суть алгоритма синтеза сводится к размещению ω в нижних строках матриц G, в последующие строки которых (снизу вверх) вписываются сдвинутые на один разряд влево векторы, находящиеся в предыдущих строках. В том случае, когда при сдвиге строки длина вектора оказывается превышающей порядок n матрицы G, то этот вектор приводится к остатку по модулю f_n. Вводятся сопряженные матрицы Галуа и однозначно связанные с ними правосторонним транспонированием базовые и сопряженные матрицы Фибоначчи. Обсуждаются возможности построения расширенных полей Галка на основе пространственных матриц, изоморфных примитивным элементам ω.

Ключевые слова: *неприводимые и примитивные полиномы, базовые и сопряженные матрицы Галуа и Фибоначчи, пространственные матрицы, расширенные поля Галуа.*

Введение и постановка задачи. В классической теории конечных полей Галуа принято считать, что элементами ω расширенных полей $GF(p^n)$, порождаемых неприводимыми полиномами (НП) f_n степени n, являются *исключительно* полиномы $(n-1)$–й степени над простым полем $GF(p)$ [1-3]. Поэтому на первый взгляд может показаться несколько сомнительной возможность построения расширенных полей, компоненты которых представляют собой конечную совокупность двумерных матриц и тем более – так называемых r–мерных, $r \geq 3$, *пространственных матриц* [4, 5]. Однако проблема становится вполне разрешимой, если принять во внимание такие соображения.

Представим полное множество Ω_ω элементов ω поля $GF(p^n)$ как объединение, состоящее из нулевого элемента $\omega_0 = 0$ и $p^n - 1$ ненулевых элементов $\omega_k \neq 0$, $k = \overline{1, p^n - 1}$, составляющих мультипликативную группу максимального порядка $GF^*(p^n)$, то есть пусть $\Omega_\omega = 0 \cup GF^*(p^n)$. Группа $GF^*(p^n)$ образуется последовательным возведением в степень по модулю f_n (начиная с нулевой степени) любого примитивного элемента θ поля $GF(p^n)$, порождаемого НП f_n.

А теперь предположим, что существует некоторое множество $\mathfrak{M}$ в общем случае пространственных r–мерных, $r \geq 2$, матриц M_ω n–го порядка с элементами $m_{i,j,\ldots,r} \in Z_p$, $i, j, \ldots, r = \overline{1, n}$, которому (множеству) присущи следующие свойства. Во-первых, множество $\mathfrak{M}$ содержит нулевую матрицу $M_0 = 0$. Во-вторых, подмножество всех ненулевых матриц замкнуто относительно операций умножения и сложения. В-третьих, каждая матрица M_ω множества $\mathfrak{M}$ изоморфна соответствующему элементу ω множества Ω_ω. И, наконец, в–четвертых, существует подмножество примитивных матриц M_θ, последовательность степеней каждой из которых над полем $GF(p)$ образует мультипликативную группу максимального порядка, изоморфную соответствующей группе $GF^*(p^n)$, порождаемую примитивным элементом θ поля $GF(p^n)$ над НП f_n.

Если все же существуют множества $\mathfrak{M}$ матриц M_ω, обладающие перечисленными выше свойствами, то тем самым приоткрывается перспектива построения конечных полей, которые назовем *матричными расширенными полями* (МРП) Галуа. Обозначим МРП через $GF(p_r^n)$, где p есть характеристика поля, а нижний индекс r указывает на то, что элементами поля являются r–мерные объекты, в частном случае которых выступают обычные двумерные, $r = 2$, матрицы n–го порядка.

Таким образом, главная задача данной статье состоит в разработке методов формирования конечных матричных расширенных полей Галуа $GF(p_r^n)$ на основе синтеза пространственных r– мерных матриц M_ω, изоморфных элементам ω поля $GF(p^n)$.

1. Матрицы Галуа и Фибоначчи. Термины «матрица Галуа» и «матрица Фибоначчи» заимствованы из теорий кодирования и криптографии, в которых широко используются генераторы псев-

дослучайных последовательностей (ПСП) в конфигурации Галуа или Фибоначчи [6-8], основанные на линейных регистрах сдвига (ЛРС) с линейными обратными связями. Каждому такому генератору ставится в соответствие однозначно с ним связанная матрица Галуа G (или Фибоначчи F), посредством которой можно вычислить ту же самую последовательность кодовых комбинаций, что и последовательность, формируемую генератором ПСП.

Известно [6], что для того чтобы ЛРС являлся регистром максимального периода, соответствующий полином обратной связи должен быть примитивным полиномом (ПрП). На рис. 1 представлена структурная схема генератора (регистра) в конфигурации Галуа, линейные обратные связи которого образованы ПрП $f_8 = 101001101$.

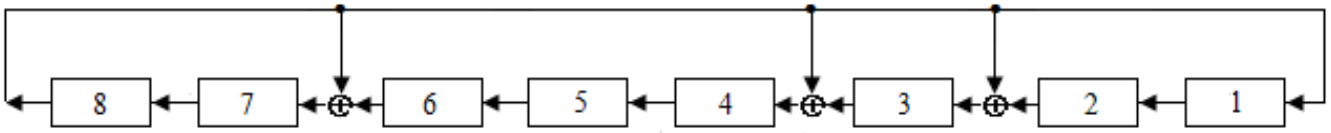

Рис 1. Структурная схема генератора Галуа над полиномом $f_8 = 101001101$

Классический генератор Галуа, показанный на рис. 1, сопоставляет каждому ненулевому элементу поля $GF(2^8)$ соответствующую степень примитивного элемента $\omega = 10$ по модулю $f_8 = 101001101$. В качестве элементов памяти разрядов ЛРС используются, как правило, D - триггеры, уровень сигнала на выходе которых (0 или 1) после подачи синхроимпульса повторяет уровень сигнала, подведенного к входу триггера. Элемент $\oplus$ в ЛРС осуществляет операцию сложения по модулю 2 (операцию XOR).

Как следует из структурной схемы генератора (на примере схемы, приведенной на рис. 1) обратные связи в простых (классических) генераторах (регистрах) Галуа однозначно определяются выбранным ПрП f_n и формируются таким способом: отклики каждого разряда поступают на входы последующих разрядов, являясь для них функциями возбуждения. Кроме того, отклик старшего разряда регистра подается (по схеме XOR) на входы тех и только тех разрядов регистра, номера которых совпадают с ненулевыми номерами мономов примитивных полиномов. При этом младшему моному, расположенному справа полинома f_n, зададим номер 1, как и младшему (правому) разряду (D - триггеру) регистра на рис. 1.

Обозначим $G_f^{[n]}$ двумерную матрицу Галуа $n-$ го порядка над неприводимым полиномом f_n, с помощью которой введем рекуррентное вычисление состояний $S(t)$ регистра в момент времени t по формуле

$$S(t) = S(t-1) \cdot G_f^{[n]}, \; S(0) = 00000001$$
$$t = 1, 2, \cdots . \qquad (1)$$

Вектором $S(0)$ выделяется нижняя строка (припишем ей номер 1) матрицы $G_f^{[n]}$. Следовательно, в нижней строке матрицы $G_f^{[n]}$ необходимо записать значение $S(1)$, совпадающее с минимальным образующим элементом (ОЭ) $\omega = 10$ поля $GF(2^8)$ над ПрП $f_8 = 101001101$. Продолжая операции преобразования (1), приходим к матрице

$$G_f^{[8]} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (2)$$

В соответствии с (2) алгоритм синтеза матриц Галуа может быть сформулирован следующим образом. Пусть f_n - векторная форма примитивного полинома степени n такая, что $f_n = \{1, u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1\}$, $u_i \in \{0,1\}, i = \overline{1, n-1}$, и $\omega = 10$ – минимальный ОЭ поля $GF(2^n)$, порождаемого ПрП f_n. Поместим образующий элемент 10 справа в нижней строке матрицы Галуа и заполним элементы матрицы, придерживаясь простого правила. Поставим единицы в элементах диагонали, расположенной ниже главной диагонали матрицы, а в оставшихся элементах матрицы $G_f^{[n]}$, кроме верхней строки, запишем нули. В верхней $n-$ й строке матрицы Галуа следует ожидать появления $(n+1)-$ битного вектора $100\ldots0$. Но это недопустимо, так как порядок матрицы равен n. Приведя этот $(n+1)-$ битный вектор к остатку по модулю f_n, приходим к тому, что в верхней строке матрицы $G_f^{[n]}$ следует разместить ПрП f_n,

исключая его старшую единицу, то есть n – битный вектор $u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1$.

На основании предложенного правила, назовем его *правилом простого диагонального заполнения*, получим общую форму *классической матрицы Галуа* n – го порядка:

$$G_f^{[n]} = \begin{pmatrix} u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \qquad (3)$$

В дополнении к матрицам Галуа можно ввести также *матрицы Фибоначчи* $F_f^{[n]}$ над ПрП f_n, отвечающие ЛРС по схеме Фибоначчи. Матрицы Фибоначчи $F_f^{[n]}$ взаимно–однозначно связаны с матрицами Галуа *оператором правостороннего транспонирования* $\perp$ [9] (транспонирования относительно вспомогательной диагонали), т. е.

$$F_f^{[n]} \xleftrightarrow{\perp} G_f^{[n]}. \qquad (4)$$

К общей форме матрицы Фибоначчи n – го порядка можно прийти, согласно (4), в результате правостороннего транспонирования матрицы (3). Имеем

$$F_f^{[n]} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & u_1 \\ 0 & 1 & \cdots & 0 & 0 & u_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & u_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & u_{n-1} \end{pmatrix}. \qquad (5)$$

Матрицы (3) и (5) как раз и являются *классическими примитивными матрицами* Галуа и Фибоначчи, но только лишь при условии, что f_n - примитивные НП. «Примитивными» такие матрицы названы на том основании, что последовательность степеней этих матриц в кольце вычетов по модулю 2 образует последовательность максимальной длины $L = 2^n - 1$ (или m - последовательность).

2. Сопряженные матрицы Галуа и Фибоначчи. В теории групп элемент x^* некоторой группы X является *сопряженным* элементу x той же группы [10], если существует некоторый элемент $z \in X$ такой, что

$$x^* = z^{-1} \cdot x \cdot z. \qquad (6)$$

По аналогии с (6) введем формальное определение *сопряженных матриц* Галуа и Фибоначчи по форме

$$M^* = P^{-1} \cdot M \cdot P, \qquad (7)$$

где M есть матрица G или F, а P - матрица, которую назовем *матрицей перехода* от M к M^* или *матрицей преобразования подобия*. Для простоты индекс f и порядок n в матрицах G и F иногда будем опускать. Как следует из соотношения (7), матрицы M^* являются матрицами, *подобными* M и, в силу этого, сохраняющими основные свойства матриц M.

Отметим, что матрицы G^* и F^* названы *сопряженными матрицам* G и F соответственно на основании лишь формального сходства преобразований (6) и (7).

В качестве матрицы P выбрана *матрица инверсной перестановки* (ИП), являющаяся одним из вариантов *перестановочной матрицы*, называемая также *обменной матрицей* [11], которую условно обозначим цифрой 1 (как элемент группы простых кодов Грея [12]).

Приведем, в качестве примера, матрицу ИП четвертого порядка

$$1 := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Матрица ИП является *инволютивной*, то есть обратной самой себе. Это означает, что $1^{-1} = 1$ и $1 \cdot 1 = 1^2 = E$. Таким образом,

$$\begin{aligned} G^* &= 1 \cdot G \cdot 1, \qquad G = 1 \cdot G^* \cdot 1; \\ F^* &= 1 \cdot F \cdot 1, \qquad F = 1 \cdot F^* \cdot 1. \end{aligned} \qquad (8)$$

Умножение квадратной матрицы M на матрицу ИП слева эквивалентно инверсии строк матрицы M, а справа – инверсии столбцов этой матрицы. Следовательно, сопряженная матрица M^* может быть получена из матрицы M в результате совместной инверсии ее строк и столбцов, выполняемых в любой последовательности, что эквивалентно, как это легко проверить, левостороннему и правостороннему транспонированию, также выполняемых в любой последовательности, т. е.:

$$M^* = 1 \cdot M \cdot 1 = M^{\perp T} = M^{T \perp}. \qquad (9)$$

Общие формы двоичных классических сопряженных матриц $n-$го порядка, в соответствии с соотношениями (3), (5) и (8), имеют вид:

$$G^* = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & u_1 & u_2 & \cdots & u_{n-2} & u_{n-1} \end{pmatrix};$$

$$F^* = \begin{pmatrix} u_{n-1} & 1 & 0 & \cdots & 0 & 0 \\ u_{n-2} & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ u_2 & 0 & 0 & \cdots & 1 & 0 \\ u_1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Согласно (9) любая из рассматриваемых матриц Галуа и Фибоначчи (базовая M или сопряженная M^*) может быть получена, как показано в табл. 1, в результате *преобразования подобия* другой матрицы.

Таблица 1

Операторы преобразование матриц

	G	F	G^*	F^*
G	—	$\perp$	T$\perp$	T
F	$\perp$	—	T	T$\perp$
G^*	T$\perp$	T	—	$\perp$
F^*	T	T$\perp$	$\perp$	—

3. Обобщенные матрицы Галуа над полем $GF(p)$. Для решения задачи синтеза обобщенных матриц Галуа воспользуемся *обобщенным правилом диагонального заполнения*, суть которого состоит в следующем. Первоначально в нижней строке матрицы $n-$го порядка $G_{f,\omega}$ записывается произвольный образующий элемент ω, являющийся элементом поля $GF(p^n)$ над выбранным НП f_n (совсем не обязательно примитивными). Элементы строки, расположенные левее ω, заполняются нулями. Последующие строки матрицы (по направлению снизу вверх) образуются сдвигом предыдущей строки на один разряд влево. Если при этом старший ненулевой разряд строки выходит за пределы матрицы, то векторы, отвечающие таким строкам, приводятся к остатку по модулю НП f_n и, тем самым, строчка также становятся $n-$разрядной.

Пусть, для примера, $p=3$, $n=8$, $f_8=102011122$ и $\omega=12112$. Воспользовавшись обобщенным правилом диагонального заполнения, приходим к матрице Галуа

$$G = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 2 \\ 2 & 0 & 1 & 0 & 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\ 1 & 2 & 1 & 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 2 \end{pmatrix}. \qquad (10)$$

Операторами табл. 1 матрица (10) легко преобразуется в обобщенную матрицу Фибоначчи F или обобщенные сопряженные матрицы G^* и F.

4. Изоморфизм матриц Галуа. На основании обобщенного правила диагонального заполнения матриц Галуа $G_{f,\omega}$ легко приходим к следующему утверждению.

Утверждение 1. *Матрица Галуа* $G_{f,\omega}$ $n-$*го порядка над неприводимым полиномом* f_n *изоморфна ее образующему элементу* ω, *принадлежащему полю* $GF(p^n)$, *порожденному полиномом* f_n, *т. е.*

$$G_{f,\omega} \leftrightarrow \omega. \qquad (11)$$

Другими словами, между матрицей $G_{f,\omega}$ и ее ОЭ ω существует биективное (взаимно–однозначное) соответствие, которое отображается отношением изоморфизма (11).

Доказательство. Образующий $(k+1)$–разрядный элемент $\omega \in GF(p^n)$ матрицы Галуа $G_{f,\omega}$, можно представить в виде полинома $k-$й степени одной переменной x, то есть в виде $\omega_k(x)$. Из теории многочленов (полиномов) одной переменной известно, что умножение произвольного полинома $\omega_k(x)$ степени k на x эквивалентно сдвигу полинома на один разряд влево и, соответственно, увеличению на 1 степени полинома. Или

$$x \cdot \omega_k(x) \to \omega_{k+1}(x). \qquad (12)$$

Воспользовавшись соотношением (12), представим матрицу Галуа $G_{f,\omega}$ порядка n выражением

$$G_{f,\omega} \Rightarrow \begin{pmatrix} x^{n-1}\cdot\omega \\ x^{n-2}\cdot\omega \\ \cdots \\ x\cdot\omega \\ \omega \end{pmatrix} (\mathrm{mod}\, f) = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} (\mathrm{mod}\, f). \quad (13)$$

Элементы x^l правого вектор-столбца в соотношении (13) являются полиномами $l-$й степени одной переменной, векторная форма которых имеет вид

$$x^l \to \underbrace{1, 0, \cdots 0, 0}_{(l+1)}, \quad l = \overline{1, n-1}. \quad (14)$$

С учетом замены (14) приходим к такому представлению правого вектор-столбца формулы (13)

$$\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = E, \quad (15)$$

где $E-$ единичная матрица $n-$го порядка.

Соотношения (13)-(15) дают возможность сформулировать вывод: *матрица Галуа* $G_{f,\omega}$ *порядка* n *над НП* f_n *однозначно определяется своим образующим элементом* ω.

Следовательно, матрица Галуа $G_{f,\omega}$ порядка n над $GF(p)$ изоморфна ее ОЭ ω, принадлежащему полю $GF(p^n)$ над выбранным неприводимым полиномом f_n. Это означает, в частности, что между матрицей $G_{f,\omega}$ и ее образующим элементом ω существует взаимно–однозначное соответствие (11).

Кроме того, следует иметь в виду, что образующий элемент ω не может быть меньше характеристики p НП ω, т. е. $\omega \geq p = 10$, так как в противном случае ОЭ становится одноразрядным, занимая при синтезе матрицы Галуа самую правую ячейку нижней строки матрицы. При этом матрица $G_{f,\omega}$ вырождается в диагональную матрицу, не зависящую от НП f_n, что недопустимо. Минимальное значение, равное 10, ОЭ ω принимает, как это имеет место в классических матрицах Галуа, если только НП является примитивным.

Из отношения изоморфизма (11) вытекают вполне очевидные следствия:

Следствие 1.1. *Для того чтобы возвести матрицу* $G_{f,\omega}$ *в степень* k *достаточно вычислить* $\omega_k = \omega^k (\mathrm{mod}\, f_n)$ *и по методу диагонального заполнения составить матрицу Галуа, образующим элементом которой является элемент* ω_k.

Следствие 1.2. *Минимальное ненулевое значение степени* e, *обеспечивающее равенство* $G^e_{f,\omega}$ *совпадает с порядком* e *элемента* ω, *образующего матрицу* $G_{f,\omega}$.

Следствие 1.3. *Матрица Галуа* $G_{f,\omega}$ *примитивна, если примитивным является образующий ее элемент* ω.

Следствие 1.4. Матрицы Галуа G_{f,ω_1} и G_{f,ω_2}, $\omega_1 \neq \omega_2$ коммутативны, поскольку являются элементами одной и той же мультипликативной группы GF^* максимального порядка, составленной из степеней матрицы $G_{f,\theta}$, произвольный примитивный образующий элемент которой θ принадлежит полю $GF(p^n)$, порожденному НП f_n.

Следствие 1.5. Произвольные алгебраические преобразования (суммирования, вычитания, умножения или деления) над матрицей Галуа, или совокупностью матриц Галуа, изоморфны таким же преобразованиям над образующими элементами этих матриц.

Следствие 1.6. Произведение вектора $n-$го порядка V на матрицу Галуа $G^{(n)}_{f,\omega}$ совпадает с произведением (*в кольце вычетов по модулю НП* f_n) этого вектора на образующий элемент ω матрицы G, т.е.:

$$V \cdot G^{(n)}_{f,\omega} = (V \cdot \omega) \bmod f_n.$$

Таким образом, на основании изоморфизма, существующего между обобщенными матрицами Галуа $G_{f,\omega}$ и образующими их элементами ω, принадлежащими полю $GF(p^n)$, приходим к заключению о возможности построения конечных расширенных матричных полей Галуа $GF(p_2^n)$ с элементами $G_{f,\omega}$.

Более того, поскольку матрицы Фибоначчи $F_{f,\omega}$ и сопряженные матрицы $G^*_{f,\omega}$ и $F^*_{f,\omega}$ подобны матрицам $G_{f,\omega}$, то из этого следует, что матричные поля Галуа могут быть построены также и на основании матриц $F_{f,\omega}$, $G^*_{f,\omega}$ и $F^*_{f,\omega}$.

5. Аксиомы расширенных полей Галуа. Для конечных полей Галуа, образуемых примитивными матрицами Галуа, должны соблюдаться

ряд условий (аксиом). Проверку выполнимости аксиом будем осуществлять на примере расширенного поля, элементы которого составляют полное множество матриц Галуа, порождаемых двоичным НП четвертой степени $f_4 = 11111$, не являющееся, кстати, примитивным. Образующими элементами множества матриц Галуа служат 16 двоичных векторов 0, 1, 10, …, 1111. Все эти матрицы показаны в табл. 2, причем жирными цифрами в нижних строчках выделены ОЭ, формирующие соответствующие матрицы Галуа.

Таблица 2

Полное множество матриц Галуа, образуемых НП $f_4 = 11111$

0 0 0 0	1 0 0 0	1 1 1 1	0 1 1 1
0 0 0 0	0 1 0 0	1 0 0 0	1 1 0 0
0 0 0 0	0 0 1 0	0 1 0 0	0 1 1 0
0 0 0 **0**	0 0 0 **1**	0 0 **1** **0**	0 0 **1** **1**
0 0 0 1	1 0 0 1	1 1 1 0	0 1 1 0
1 1 1 1	1 0 1 1	0 1 1 1	0 0 1 1
1 0 0 0	1 0 1 0	1 1 0 0	1 1 1 0
0 **1** **0** **0**	0 **1** **0** **1**	0 **1** **1** **0**	0 **1** **1** **1**
0 0 1 0	1 0 1 0	1 1 0 1	0 1 0 1
0 0 0 1	0 1 0 1	1 0 0 1	1 1 0 1
1 1 1 1	1 1 0 1	1 0 1 1	1 0 0 1
1 **0** **0** **0**	**1** **0** **0** **1**	**1** **0** **1** **0**	**1** **0** **1** **1**
0 0 1 1	1 0 1 1	1 1 0 0	0 1 0 0
1 1 1 0	1 0 1 0	0 1 1 0	0 0 1 0
0 1 1 1	0 1 0 1	0 0 1 1	0 0 0 1
1 **1** **0** **0**	**1** **1** **0** **1**	**1** **1** **1** **0**	**1** **1** **1** **1**

Полное множество примитивных элементов поля $GF(2^4)$ над НП $f_4 = 11111$, представлено в табл. 3.

Таблица 3

Множество примитивных элементов поля $GF(2^4)$ над НП $f_4 = 11111$

11	101	110	**111**	1001	1010	1011	1110

Выберем, для примера, примитивный элемент $\theta = 111$, выделенный в табл. 3 затенением, а из таблицы 2 – соответствующую этому элементу примитивную матрицу Галуа, обозначив ее как G_θ. Имеем

$$G_\theta = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix}. \qquad (16)$$

Согласно следствию 1.3 матрица G_θ, заданная соотношением (16), примитивна, поскольку примитивным над НП $f_4 = 11111$ является образующий ее элемент $\theta = 111$. Последовательно возводя матрицу G_θ в степень s, начиная с $s = 0$, приходим к мультипликативной группе 15-го порядка, сведенную в табл. 4.

Совокупность двоичных матриц четвертого порядка, представленных в табл. 4, дополненная нулевой матрицей составляет множество элементов поля $GF(2_2^4)$, формируемое НП $f_4 = 11111$ и примитивным элементом $\theta = 111$. В данной таблице, как и в табл. 2, в нижних строках матриц выделены образующие их элементы.

Таблица 4

Мультипликативная группа поля Галуа над НП $f_4 = 11111$, порождаемая матрицей G_θ, $\theta = 111$

–	1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 **1**	0 1 1 0 0 0 1 1 1 1 1 0 0 **1** **1** **1**	1 1 0 1 1 0 0 1 1 0 1 1 **1** **0** **1** **0**
0 0 1 0 0 0 0 1 1 1 1 1 **1** **0** **0** **0**	1 1 1 0 0 1 1 1 1 1 0 0 0 **1** **1** **0**	1 0 1 1 1 0 1 0 0 1 0 1 **1** **1** **0** **1**	1 1 1 1 1 0 0 0 0 1 0 0 0 0 **1** **0**
1 1 0 0 0 1 1 0 0 0 1 1 **1** **1** **1** **0**	0 1 0 1 1 1 0 1 1 0 0 1 **1** **0** **1** **1**	0 1 0 0 0 0 1 0 0 0 0 1 **1** **1** **1** **1**	0 0 1 1 1 1 1 0 0 1 1 1 **1** **1** **0** **0**
1 0 0 1 1 0 1 1 1 0 1 0 0 **1** **0** **1**	0 0 0 1 1 1 1 1 1 0 0 0 0 **1** **0** **0**	0 1 1 1 1 1 0 0 0 1 1 0 0 0 **1** **1**	1 0 1 0 0 1 0 1 1 1 0 1 **1** **0** **0** **1**

Проверим выполнение основных аксиом полей Галуа для поля $GF(p_2^4)$, выбрав за основу двоичное поле $GF(2_2^4)$. Введем обозначение $GF.k$ для $k-$й аксиомы.

GF.1. Из двух операций поля Галуа над элементами a и b одна операция называется *сложением* и обозначается как $a+b$, а другая – *умножением* и обозначается как $a \cdot b$ или ab.

Пусть

$$A=\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&1&0&0\\0&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{bmatrix},\quad B=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{bmatrix},\quad C=\begin{bmatrix}1&0&1&1\\1&0&1&0\\0&1&0&1\\\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{bmatrix}. \qquad (17)$$

есть выбранные элементы поля $GF(2_2^4)$. Имеем, для примера,

$$A+B=\begin{bmatrix}0&1&1&1\\1&1&0&0\\0&1&1&0\\0&0&\mathbf{1}&\mathbf{1}\end{bmatrix} \text{ и } A\cdot B=\begin{bmatrix}1&0&0&1\\1&0&1&1\\1&0&1&0\\0&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{bmatrix}. \qquad (18)$$

Соотношения (18) подтверждают нижеследующую аксиому полей Галуа.

GF.2. Результатом сложения и умножения двух элементов поля является третий элемент из того же поля.

В самом деле, как сумма $A+B$, так и произведение $A\cdot B$ элементов поля $GF(2_2^4)$ принадлежат этому же полю, что следует из табл. 2 и 4, т. е. элементы поля $GF(2_2^4)$ замкнуты относительно операций сложения и умножения.

GF.3. Поле Галуа всегда содержит мультипликативную единицу 1, в качестве которой в $GF(2_2^n)$ выступает единичная матрица $n-$го порядка, и аддитивную единицу 0 (в поле $GF(2_2^n)$ таковой является нулевая матрица), такие что $a\cdot 1=a$, и $a+0=a$ для произвольного элемента a поля.

GF.4. Для любого элемента a существует обратный элемент по сложению $(-a)$ и обратный элемент по умножению a^{-1} (если $a\neq 0$) такие, что $a+(-a)=0$ и $a\cdot a^{-1}=1$.

Например, элементам (17) отвечают обратные элементы обладающие тем свойством, что, во–первых, принадлежат, как и элементы (17), полю $GF(2_2^4)$ и, во-вторых, являются матрицами Галуа, образующие которых расположены в нижних строках матриц. Легко убедиться в том, что произведения матриц (17) на соответствующие обратные матрицы (19) равны единичным матрицам, как и должно быть.

$$A^{-1}=\begin{bmatrix}1&0&0&1\\1&0&1&1\\1&0&1&0\\0&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{bmatrix},\quad B^{-1}=\begin{bmatrix}0&1&0&1\\1&1&0&1\\1&0&0&1\\\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}\end{bmatrix},\quad C^{-1}=\begin{bmatrix}0&0&1&1\\1&1&1&0\\0&1&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}\end{bmatrix}. \qquad (19)$$

GF.5. Для операций сложения и умножения в поле $GF(2_2^n)$ выполняются обычные правила *ассоциативности*

$$a+(b+c)=(a+b)+c,\quad a(bc)=(ab)c,$$

коммутативности

$$a+b=b+a,\quad ab=ba$$

и *дистрибутивности*

$$a(b+c)=ab+ac,$$

что однозначно можно установить на примере матриц (17*)*.

Приведенные аксиомы соблюдаются не только для двоичного поля $GF(2_2^n)$, но также и для любого поля $GF(p_2^n)$ характеристики p. Таким образом, можно считать доказанным, что полное множество элементов G_ω, принадлежащих $GF(p_2^n)$, удовлетворяет всем классическим аксиомам полей и, тем самым, завершается доказательство того, что множество $\{G_\omega\}$ образует матричное поле Галуа $GF(p_2^n)$.

6. Расширение класса матриц, образующих поле $GF(p_2^n)$. Примитивные элементы θ поля $GF(p^n)$ над неприводимыми полиномами f_n являются образующими не только примитивных матриц Галуа G_θ, но и связанных с ними правосторонним транспонированием примитивных

матриц Фибоначчи F_θ, а также примитивных сопряженных матриц Галуа G_θ^* и Фибоначчи F_θ^*.

Из этого следует, что мультипликативные группы $GF^*(p_2^n)$ матричных полей Галуа $GF(p_2^n)$ могут быть построены не только на основании матриц G_θ, но также с помощью матриц F_θ, G_θ^* и F_θ^*.

Взаимосвязь матриц Галуа, к которым будем относить все перечисленные выше матрицы, посредством операторов классического и правостороннего транспонирования отображена в табл. 1. Придадим матрицам тригонометрическую интерпретацию (рис. 2). С этой целью представим базовую матрицу Галуа G_θ в виде направленного вектора G, месторасположение которого в квадрате на рис. 2 соответствует нижней строке матрицы, содержащей ОЭ θ, а стрелка задает направление упорядочения θ от младших разрядов к старшим.

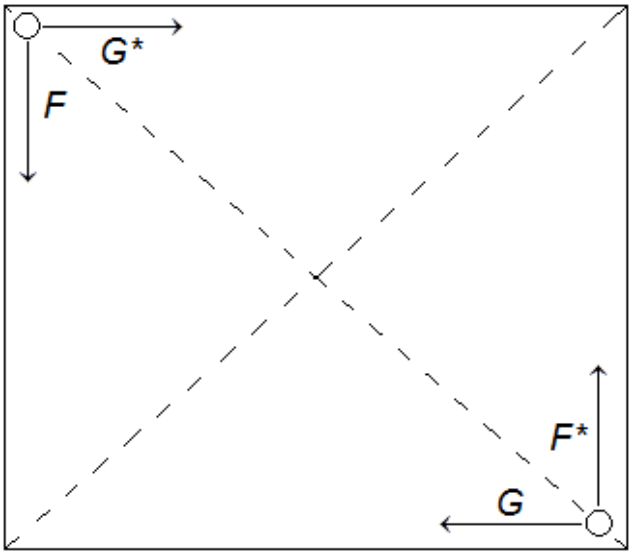

Рис. 2. Тригонометрическая интерпретация матриц Галуа

Правосторонним транспонированием (поворотом относительно вспомогательной диагонали квадрата) вектор G преобразуется в вектор F, символизирующий матрицу Фибоначчи F_θ, указывая, тем самым, что ОЭ θ располагается в левом столбце матрицы Фибоначчи, а младшие разряды ОЭ находятся сверху столбца.

Левостороннее транспонирование вектора G матрицы G_θ приводит к образованию вектора F^* сопряженной матрицы Фибоначчи F_θ^*, ОЭ которой занимает правый столбец матрицы, причем младший разряд θ, согласно направлению вектора F^*, находится внизу столбца. И, наконец, вектор G^* сопряженной матрицы G_θ^* может быть получен, согласно рис. 2, или правосторонним транспонированием вектора F^*, или классическим транспонированием вектора F. Образующий элемент θ сопряженной матрицы G_θ^* расположен в верхней строке матрицы, а разряды θ упорядочены слева направо. Отметим дополнительно, что место, которое занимает младший разряд образующих элементов матриц, условно обозначено на рис. 2 кружочком.

Тригонометрическая интерпретация матриц (рис. 2) дает возможность предложить способ прямого синтеза матриц G_θ^*, F_θ и F_θ^*, не прибегая к операторам транспонирования матрицы G_θ. Синтез данных матриц сводится к простейшей модификации разработанного выше алгоритма построения матрицы Галуа G_θ по методу обобщенного диагонального заполнения строк этой матрицы.

В частности, суть прямого метода синтеза матрицы Фибоначчи F_θ состоит в следующем. Пусть заданы НП f_n степени n с коэффициентами над $GF(p)$ и примитивный образующий элемент θ. Разместим разряды ОЭ θ в левом столбце матрицы $n-$го порядка F_θ таким образом, чтобы младший разряд θ оказался в верхней левой ячейке столбца, а в ячейки столбца, оставшиеся свободными, заносятся нули. Последующие столбцы матрицы, при заполнении слева направо, образуются в результате сдвига на один разряд вниз предыдущих столбцов, а в освобождающиеся верхние ячейки записываются нули. Если на каком–то шаге формирования матрицы F_θ ненулевой разряд столбца выходит за пределы матрицы, то этот столбец приводится к остатку по модулю f_n и, тем самым, возвращается в пределы матрицы.

Аналогичным образом могут быть сформулированы правила прямого синтеза матриц G_θ^* и F_θ^*. При этом следует иметь в виду, что младшие разряды НП f_n и ОЭ θ обязаны занимать одинаковые пространственные положения. Это означает, что указанные разряды должны находиться в правой или левой ячейках строк, при синтезе матриц G_θ и G_θ^* соответственно, а также в верхней или нижней ячейках столбцов, при синтезе матриц F_θ и F_θ^*.

7. Пространственные матрицы и поля Галуа. Понятие *пространственной матрицы*, т. е. матрицы трех и большего числа измерений обобщает понятие обычной, *двумерной (квадратной) матрицы* $n-$*го* порядка над полем $GF(p)$.

Любая система из n^3 элементов поля $GF(p)$, расположенных в точках трехмерного пространства, определяемых координатами i, j, k, называется *трехмерной (кубической) матрицей* $n-$*го* порядка над полем $GF(p)$.

В данном разделе статьи обсуждаются вопросы построения расширенных полей Галуа $GF(p_3^n)$, элементами которых являются трехмерные пространственные матрицы $n-$го порядка. Введем для этих матриц обозначение G_{ijk}. Пример кубической матрицы четвертого порядка показан на рис. 3.

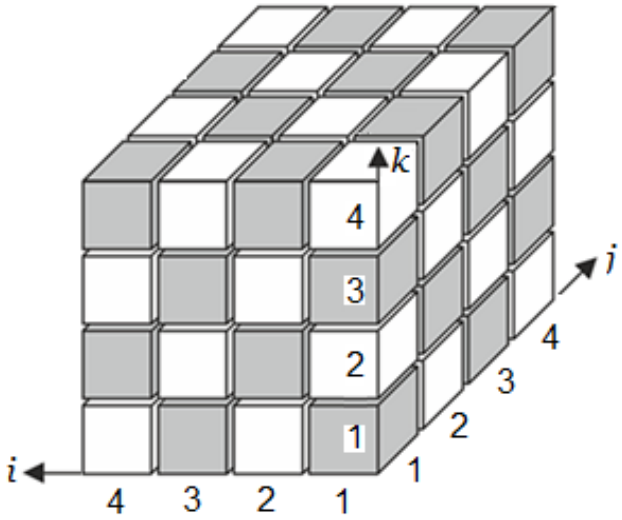

Рис. 3. Трехмерная матрица четвертого порядка

Совокупность элементов матрицы G_{ijk} с фиксированными значениями индексов i, j или k называются *сечениями ориентации* (i), (j) или (k) соответственно [4, 5]. Все n сечений в матрице G_{ijk} параллельны друг другу и являются обычными двумерными матрицами $n-$го порядка.

Один из возможных способов построения трехмерной матрицы Галуа над $GF(p)$, порождаемой НП f_n и изоморфной ОЭ ω, состоит в следующем. Пусть, для примера, $n=4$, как на рис. 3. Положим в *основание* куба четвертого порядка примитивную матрицу (17), обозначим ее G_{ij1},

$$G_{ij1}=\begin{bmatrix}0&1&1&0\\0&0&1&1\\1&1&1&0\\0&\mathbf{1}&\mathbf{1}&\mathbf{1}\end{bmatrix}, \qquad (20)$$

являющуюся (k) сечением, $k=1$, пространственной матрицы, показанной на рис. 3. Будем допускать, что все последующие сечения куба по направлению снизу вверх по оси k образуются из предыдущего сечения, умноженного на x. Это означает, в частности, что строки двумерной матрицы G_{ij2} являются результатом сдвига на один шаг влево соответствующих строк матрицы G_{ij1}, приведенных к остатку по модулю $f_4=11111$.

$$G_{ij2}=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{bmatrix}. \qquad (21)$$

Аналогично формируются матрицы G_{ij3} и G_{ij4}:

$$G_{ij3}=\begin{bmatrix}0&1&1&1\\1&1&0&0\\0&1&1&0\\0&0&\mathbf{1}&\mathbf{1}\end{bmatrix};$$

$$G_{ij4}=\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&1&0&0\\0&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{bmatrix}. \qquad (22)$$

Легко убедиться в том, что сечения куба G_{ik} совпадают с соответствующими сечениями G_{ij}, представленными системой матриц (20)–(22). Иными словами, все сечения куба, коллинеарные плоскости ij, совпадают с соответствующими сечениями, коллинеарными плоскости ik.

Также как и для двумерных матриц Галуа, справедливо следующее утверждение.

Утверждение 2. *Пространственные матрицы Галуа* $G_{ij\ldots r}$ *изоморфны образующим их элементам, являющихся элементами поля* $GF(p^n)$ *над НП* f_n.

Следствие 2.1. *Последовательность степеней пространственной* $r-$*мерной матрицы Галуа* $n-$*го порядка* G_θ, *образующий элемент которой является примитивным элементом* θ *поля* $GF(p^n)$, *порождаемого неприводимым над* $GF(p)$ *полиномом* f_n, *формирует*

мультипликативную группу максимального порядка $GF^*(p_r^n)$ *пространственного матричного поля* $GF(p_r^n)$.

Следствие 2.2. *Любые пары пространственных матриц Галуа, принадлежащих группе* $GF^*(p_r^n)$*, коммутативны.*

Следствием 2.2, являющимся, вообще говоря, аксиомой любой мультипликативной группы, подчеркивается та особенность матриц Галуа, что *произвольная пара* $r-$*мерных пространственных матриц Галуа* $G_{ij...r}$ *всегда коммутативна, тогда как в общем случае даже двумерные матрицы свойством коммутативности не обладают.*

И в заключение раздела отметим, что расширенные поля Галуа можно построить как на основании примитивных пространственных матриц Галуа G, так и пространственных матриц Фибоначчи F, а также их сопряженных вариантов G^* и F^*.

Выводы. Важнейшим научным результатом данной работы является подтверждение возможности построения матричных полей на основе пространственных матриц Галуа, изоморфных элементам поля $GF(p^n)$. Отличительная особенность матричных полей состоит в следующем. Если элементы ω классических полей $GF(p^n)$ инвариантны к неприводимым полиномам f_n, образующих поля, то элементы $G_{ij...r}$ матричных полей $GF(p_r^n)$ зависят от НП f_n. Следовательно, можно утверждать, что спектр разрабатываемых матричных полей Галуа $GF(p_r^n)$ гораздо богаче спектра классических полей $GF(p^n)$, которые являются частным случаем расширенных матричных полей, если положить в них параметр $r=1$.

Это, во–первых. И, во–вторых, не следует исключать того, что кроме $r-$мерных пространственных матриц G_ω $n-$го порядка, изоморфных элементам поля $GF(p^n)$, будут предложены и другие $r-$мерные объекты, отличные от матриц $G_{ij...r}$, но которые окажутся приемлемыми для построения полей $GF(p_r^n)$.

Однако многие важные вопросы, например, такие: как будут выглядеть и что представляют собой элементы $G_{ij...r}$ поля $GF(p_r^n)$, $r \geq 4$, и ряд др., в силу ограниченности объема статьи остались не раскрытыми и могут составить предмет отдельного исследования. Интересным для анализа остается также проблема выяснения правомочности применимости в полях $GF(p_r^n)$ пространственных матриц, образуемых из двумерных матриц G_ω не единственным преобразованием подобия на основе матриц ИП, как это предложено в данной статье, а произвольными матрицами перестановки.

ЛИТЕРАТУРА

[1]. Лидл Р. Конечные поля. Монография в 2-х томах. / Р. Лидл, Г. Нидеррайтер. Т. 1. – М.: Мир, 1988. – 432 с.

[2]. Постников М. М. Теория Галуа. / М. М. Постников. – Физматгиз, 1963. – 218 с.

[3]. Волкович С. Л. Вступ до алгебраїчної теорії перешкодостійкого кодування / С. Л. Волкович, В. О. Геранін, Т. В. Мовчан, Л. Д. Пісаренко. – Київ, ВПФ УкрІНТЕІ, 2002. – 236 с.

[4]. Соколов Н. П. Пространственные матрицы и их приложения. / Н. П. Соколов. – М.: ГИФМЛ, 1960. – 300 с.

[5]. Соколов Н. П. Введение в теорию многомерных матриц. / Н. П. Соколов. – К.: Наукова думка, 1972. – 176 с.

[6]. Поточные шифры. Результаты зарубежной открытой криптологии. – М., 1997. / [Электронный ресурс]. – Режим доступа: http//www/ssl/stu/neva/ru/psw/crypto/potok/str_ciph.htm

[7]. Асосков А. В. Поточные шифры. / А. В. Асосков, М. А. Иванов, А. А. Мирский и др. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

[8]. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

[9]. Муллажонов Р. В. Обобщенное транспо-нирование матриц и структуры линейных крупномасштабных систем. / Р. В. Муллажонов // Доповіді НАНУ, 2009, № 10. – С. 27-35.

[10]. Энциклопедия математики. Том 5. - М .: Изд-во "Советская энциклопедия", 1985. – 623 с.

[11]. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М.: Мир, 1986. – 576 с.

[12]. Белецкий А. Я. Обобщенные коды Грея. Научная монография. / А. Я. Белецкий. – Palmarium Academic Publishing, Germany, 2014. – 208 с. ISBN 978-3-639-68389-9

REFERENCES

[1]. Lidl R., Niederreiter H. Finite Fields T. 1. – M.: Mir, 1988., 432 p.

[2]. Postnikov M. M. Galois theory. - M .: Fizmatgiz, 1963., 218 p.

[3]. Volkovich S. A., Geranin V. O., Movchan T. V., Pisarenko L. D. Introduction to the algebraic theory of error-correcting coding. – Kiev, VPF UkrINTEI, 2002., 236 p.

[4]. Sokolov N. P. Spatial matrices and their applications. - M .: GIFML, 1960., 300 p.

[5]. Sokolov N. P. Introduction to the theory of multidimensional matrices. - K .: Naukova Dumka, 1972., 176 p.

[6]. Stream Ciphers. The results of the open foreign cryptology. – M., 1997. http//www/ssl/stu/neva/ru/psw/crypto/potok/str_ciph.htm

[7]. Asoskov A.V., Ivanov A. M., Mirskiy A. A. Stream ciphers. – M.: KUDIC-OBRAZ, 2003., 336 p.

[8]. Ivanov V., A., Chugunkov I., V. Theory, Appl. and Evaluation of the Quality of Pseudorandom Sequences. – M.: KUDIC-OBRAZ, 2003., 368 p.

[9]. Mullajonov R. V. Generalized transposition of matrices and linear structure of large-scale systems. - K .: Reports National Academy of Sciences, 2009, № 10., 27-35 p.

[10]. Encyclopedia of Mathematics. Volume 5 - M .: Publish. house "Soviet Encyclopedia", 1985. – 623 p.

[11]. Blahut R. Theory and practice off error control codes. – M.: Mir, 1986., 576 p.

[12]. Beletsky A. Ja. Generalized Gray codes. Monograph. – Palmarium Academic Publishing, Germany, 2014., 208 p. ISBN 978-3-639-68389-9

РОЗШИРЕНІ ПОЛЯ, ЩО ПОРОДЖУЮТЬСЯ ПРИМІТИВНИМИ ПРОСТОРОВИМИ МАТРИЦЯМИ ГАЛУА

У статті розглянуті питання формування розширених полів, елементами яких є матриці Галуа, що уявляють собою невироджені просторові матриці, синтезовані на основі утворюючих елементів ω - одновимірних векторів та незвідних поліномів f_n ступеня n за методом послідовного заповнення рядків матриць. Суть методу послідовного заповнення для варіанту двовимірних матриць G зводиться до розміщення елементів ω в нижніх рядках матриць, в наступні рядки яких (знизу вгору) вписуються зсунуті на один розряд вліво вектори, що знаходяться в попередньому рядку. У тому випадку, коли при зсуві вектора його довжина виявляється такою, що перевищує порядок n матриці G, то цей вектор приводиться до залишку за модулем f_n. Вводяться спряжені матриці Галуа і однозначно пов'язані з ними правостороннім транспонуванням базові й спряжені матриці Фібоначчі. Обговорюються можливості побудови розширених полів на основі просторових матриць, що утворюються двовимірними матрицями Галуа.

Ключові слова: Незвідні і примітивні поліноми, базові і спряжені матриці Галуа і Фібоначчі, просторові матриці, розширені поля Галуа.

EXTENSION OF THE FIELD, GENERATES A PRIMITIVE SPACE MATRIX GALOIS

The paper deals with the formation of extended fields, elements of which are Galois matrix representing the spatial non-degenerate matrix synthesized by forming elements ω – one-dimensional vectors and irreducible polynomials f_n of degree n by the method of successive rows of filling. The essence of the method of successive filling option for two-dimensional matrix G is reduced to the placement of elements in the lower row of the matrix in which the following lines (bottom to top) fit shifted by one bit to the left vectors lying in the previous line. In the case where a shift length of the vector is greater than the order n of the matrix G, this vector provides the residue modulo f_n. Introduced Galois conjugate matrix and unambiguously associated right-hand base and conjugate transpose matrix Fibonacci. Discussed the possibility of building advanced fields on the basis of spatial matrices formed by two-dimensional matrix Galois.

Keywords: irreducible and primitive polynomials, basic and conjugated matrix Galois and Fibonacci, spatial matrix, extended Galois field.

Білецький Анатолій Якович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки Національного авіаційного університету.
E-mail: abelnau@ukr.net

Белецкий Анатолий Яковлевич, доктор технических наук, профессор, заслуженный деятель науки и техники Украины, лауреат Государственной премии Украины в области науки и техники, профессор кафедры электроники Национального авиационного университета.

Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Professor of Department Electronics of National Aviation University.