УДК 511.512:004:37

Белецкий А.Я., Белецкий Е.А.
Национальный авиационный университет, Киев, Украина

ПРИМИТИВНЫЕ МАТРИЦЫ И ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГАЛУА

DOI:10.14308/ite000463

В теории и практике криптографической защиты информации одной из ключевых проблем является проблема формирования двоичных псевдослучайных последовательностей (ПСП) максимальной длины $L = 2^n - 1$ с приемлемыми статистическими характеристиками. Генераторы ПСП реализуют, как правило, посредством линейных регистров сдвига (ЛРС) максимального периода с линейными обратными связями [1]. В данной статье мы расширим понятие ЛРС, полагая, что каждый его разряд (ячейка памяти) может находиться в одном из состояний $s \in GF(p)$, $p \geq 2$, назовем такие регистры «обобщенными линейными регистра сдвига».

Цель исследования состоит в разработке алгоритмов построения обобщенных матриц Галуа и Фибоначчи $n-$го порядка над полем $GF(p)$, $p \geq 2$, однозначно определяющих как структуру соответствующих обобщенных $n-$разрядных ЛРС максимального периода, так и формируемых на их основе генераторов ПСП Галуа максимальной длины.

Таким образом, в статье рассмотрены вопросы формирования обобщенных примитивных матриц Галуа и Фибоначчи произвольного порядка n над простым полем $GF(p)$. Синтез матриц базируется на использовании неприводимых полиномов f_n степени n и примитивных элементов расширенного поля $GF(p^n)$, порождаемого полиномом f_n. Предложены способы построения сопряженных примитивных матриц Галуа и Фибоначчи. Обсуждаются возможности применения таких матриц при решении задачи построения обобщенных генераторов псевдослучайных последовательностей Галуа..

Ключевые слова: *неприводимые полиномы, примитивные матрицы, поля Галуа, линейные регистры сдвига, генераторы последовательностей Галуа*.

1. Введение

В теории и практике криптографической защиты информации одной из ключевых проблем является проблема формирования двоичных псевдослучайных последовательностей (ПСП) максимальной длины $L = 2^n - 1$ с приемлемыми статистическими характеристиками. Генераторы ПСП реализуют, как правило, посредством линейных регистров сдвига (ЛРС) максимального периода с линейными обратными связями [1]. В данной статье мы расширим понятие ЛРС, полагая, что каждый его разряд (ячейка памяти) может находиться в одном из состояний $s \in GF(p)$, $p \geq 2$. Назовем такие регистры «обобщенными линейными регистра сдвига».

Цель исследования состоит в разработке алгоритмов построения обобщенных матриц Галуа и Фибоначчи $n-$го порядка над полем $GF(p)$, $p \geq 2$, однозначно определяющих как структуру соответствующих обобщенных $n-$разрядных ЛРС максимального периода, так и формируемых на их основе генераторов ПСП Галуа максимальной длины.

2. Понятийно-терминологические определения

Основными терминами, которые для определенности целесообразно уточнить, являются: «примитивный полином» и «примитивная матрица». Трактовки таким понятиям, как «сопряженные матрицы Галуа и Фибоначчи», «обобщенные генераторы псевдослучайных последовательностей Галуа» и ряду других, будут даны в последующих разделах работы.

В теории полей Галуа, составляющих основу алгебры помехоустойчивого кодирования, криптографии и построения современных электронных систем передачи информации,

ключевым является понятие неприводимого полинома (НП). Полином (или многочлен) одной переменной x степени n

$$f_n(x)=\sum_{i=0}^{n}u_{n-i}x^{n-i},\ \ u_i\in GF(p),\ \ u_n=1, \qquad (1)$$

называется *неприводимым над полем* $GF(p)$, если он не делится ни на какой полином меньшей степени над данным полем.

Полином (1) записан в так называемой *алгебраической форме*. Его можно также однозначно представить последовательностью своих коэффициентов

$$f_n=u_nu_{n-1}\ldots u_i\ldots u_0,\quad u_i\in GF(p),\quad u_n=1,$$

которую назовем *векторной формой* НП.

Важнейшее свойство конечных расширенных полей Галуа $GF(p^n)$, порождаемых НП f_n, как, в прочем, и простых полей $GF(p)$, состоит в том, что для любого его ненулевого элемента g должен существовать обратный элемент g^{-1} такой, что $g\cdot g^{-1}(\mathrm{mod}\ f_n)=1$. Сформулированное условие соблюдается, если только p является простым числом. Отсюда следует, что характеристика p поля Галуа, как простого $GF(p)$, так и расширенного $GF(p^n)$, должна быть простым числом.

Для удобства введем для полиномов понятие, которое назовем *характеристикой* p *полинома* f_n, совпадающее с характеристикой p простого поля Галуа $GF(p)$, которому принадлежат коэффициенты u_i, $i\in\overline{0,n}$, полинома f_n.

Множество НП содержит важное, например, для криптографических приложений, информатики, электроники и других направлений науки и техники, подмножество так называемых *примитивных полиномов* (ПрП). Существуют различные варианты определения понятия «примитивного полинома».

В алгебре, теории чисел и полей Галуа [2] неприводимый полином f_n степени n называется примитивным над $GF(p)$ в том и только в том случае, если он – нормированный полином, такой, что f_n не равен нулю и его *порядок*

$$\mathrm{ord}\,(f_n)=p^n-1.$$

В теории помехоустойчивого кодирования [3] неприводимый над $GF(p)$ полином f_n называется примитивным, если его корень α является примитивным элементом расширенного поля $GF(p^n)$.

И, наконец, в криптографии [4] примитивным считается такой неприводимый полином $f_n(x)$, который делит без остатка двучлен x^e-1, при условии, что минимальное e задано соотношением

$$e=p^n-1. \qquad (2)$$

Недостаток приведенных определений примитивного полинома состоит в том, что они не в полной мере раскрывают физический смысл данного термина, что затрудняет его инженерную интерпретацию. В этом плане, возможно, более подходящими могут оказаться такие определения ПрП.

Примитивным является неприводимый над $GF(p)$ полином f_n степени n (*необходимые условия*), порождающий расширенное поле Галуа $GF(p^n)$, минимальный примитивный элемент ω которого совпадает с характеристикой полинома p (*достаточные условия*).

Возможен другой вариант определения: примитивным над полем $GF(p)$ называется неприводимый полином f_n степени n, формирующий циклическую группу максимального

порядка p^n-1, минимальный образующий элемент которой ω совпадает с характеристикой поля p.

Полю $GF(p)$ принадлежат коэффициенты полинома f_n. Но для любого позиционного основания системы счисления (ОСС) m, в том числе и $m=p$, само основание, т.е. число m, записывается в виде 10. Тогда для любого $p-$ичного ОСС и, следовательно, любого поля $GF(p^n)$, порождаемого ПрП f_n, $(k+1)-$я степень минимального примитивного элемента $\omega=10$ поля можно представить соотношением $\omega^{k+1}=\omega^k\cdot\omega$, которое образуется смещением значения ω^k на один разряд влево (как результат умножения на $p-$ичное число 10). Если при этом окажется, что старшая ненулевая цифра числа ω^{k+1} смещается в $n-$й разряд (разряды нумеруются справа налево, начиная с нулевого разряда), то число ω^{k+1} приводится к остатку по $\bmod f_n$.

Перейдем к пояснению термина «примитивная матрица». Пусть $A=(a_{i,j})$ является положительной невырожденной матрицей порядка $n>1$ над полем целых неотрицательных чисел таких, что $a_{i,j}\in GF(p)$ для всех $i,j=\overline{1,n}$, и $E=(\delta_{i,j})$, где $\delta_{i,j}-$ символ Кронекера, есть единичная матрица того же порядка, что и A. Матрица A считается *невырожденной* в поле $GF(p)$, если ее определитель $\det A$ по модулю p не равен нулю, т.е. $\det A(\bmod p)\in\overline{1,p-1}$, где $p-$простое число. Операция возведения матрицы A в некоторую степень d выполняется в кольце вычетов по модулю p, при этом каждый элемент матрицы A^d приводится к неотрицательному остатку по модулю p. Последовательность степеней матрицы A, начиная с нулевой степени, для которой $A^0=E$, образует *циклическую группу* $\langle A\rangle$ порядка e. Матрицу A будем называть *примитивной*, если наименьшее натуральное e, при котором $A^e=E$, удовлетворяет соотношению (2). Суть термина «примитивная» матрица подобна, в определенной мере, сути термина «примитивный элемент» поля $GF(p^n)$.

3. Классические примитивные матрицы Галуа и Фибоначчи

Термины «матрица Галуа» и «матрица Фибоначчи» заимствованы из теории криптографии и кодирования [1, 4], в которых широко используются генераторы псевдослучайных последовательностей по схемам Галуа и Фибоначчи, основанные на линейных регистрах сдвига с линейными обратными связями. Будем называть такие генераторы ПСП генераторами Галуа и Фибоначчи соответственно.

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

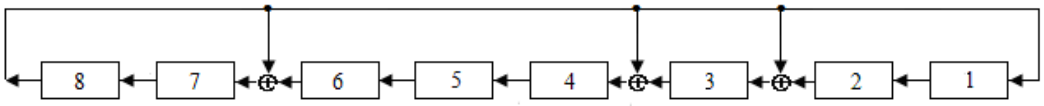

Рис. 1. Структурная схема генератора Галуа над ПрП $f_8=101001101$

Генератор Галуа 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 той, что показана на рис. 1) обратные связи в простых (классических) регистрах (генераторах) Галуа однозначно определяются выбранным ПрП f_n и формируются следующим образом: 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 ПрП. При этом младшему моному, расположенному справа полинома f_n, соответствует номер 1, как и младшему разряду ($D-$триггеру) регистра.

Обозначим G_f матрицу Галуа над НП f_n, с помощью которой введем рекуррентное вычисление состояний $S(t)$ регистра в момент времени t по формуле:

$$S(t) = S(t-1)\cdot G_f, \quad S(0) = 00000001, \; t = 1, 2, \cdots.$$

Вектором $S(0)$ выделяется нижняя строка (припишем ей номер 1) матрицы G_f. Следовательно, в нижней строке матрицы G_f необходимо записать значение $S(1)$, совпадающее с минимальным образующим элементом $\omega = 10$ поля $GF(2^8)$ над ПрП $f_8 = 101001101$. Продолжая подобным образом операции преобразований, приходим к окончательному выражению

$$G_f = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (3)$$

В соответствии с (3), алгоритм синтеза матриц Галуа G_f может быть сформулирован следующим образом. Пусть $f_n -$ векторная форма ПрП 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 образующий элемент поля $GF(2^n)$. Поместим ОЭ ω справа нижней строки матрицы G_f и заполним элементы матрицы, придерживаясь простого правила. Поставим единицы в элементах диагонали, расположенной ниже главной диагонали матрицы, а в оставшихся элементах матрицы G_f, кроме элементов верхней строки, запишем нули. В верхней строке матрицы G_f следует ожидать появления $(n+1)-$битного вектора 100…0. 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 следует разместить ПрП f_n, исключая его старшую единицу, т.е. $n-$битный вектор $u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1$.

На основании предложенного правила, назовем его *простым правилом диагонального заполнения*, получим общую форму матрицы Галуа $n-$го порядка:

$$G_f = \begin{pmatrix} u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \qquad (4)$$

Из сопоставления матрицы (3) и соответствующей ей структурной схемы ЛРС (рис. 1) легко приходим к значениям функций возбуждения $\nu_k(t)$ триггеров классических генераторов ПСП в конфигурации Галуа в любой момент времени t. Пусть $s_k(t) -$ состояние $k-$го разряда

($D-$триггера) регистра Галуа. Состояние регистра $S(t)=\{s_n(t), s_{n-1}(t), \cdots, s_2(t), s_1(t)\}$ в начальный момент времени $t=0$ таково: $S(0)=\{0,0,\cdots,0,1\}$. Тогда для каждого момента времени $t\geq 1$ функции возбуждения $\nu_k(t)$ $k-$го разряда регистра будут определяться выражениями

$$\nu_1(t)=s_n(t-1);\ \nu_k(t)=s_{k-1}(t-1)\oplus u_k\cdot s_n(t-1),\ k=\overline{2,n},\ t=1,2,\cdots.$$

В дополнении к матрицам Галуа можно ввести также *матрицы Фибоначчи* F_f над ПрП f_n, отвечающие ЛРС по схеме Фибоначчи (генераторы ПСП Фибоначчи). Матрицы Фибоначчи F_f взаимно-однозначно связаны с матрицами Галуа G_f *оператором правостороннего транспонирования* $\perp$ (транспонирования относительно вспомогательной диагонали), т.е.,

$$F_f \overset{\perp}{\longleftrightarrow} G_f. \tag{5}$$

К общей форме матрицы Фибоначчи $n-$го порядка можно прийти, согласно соотношению (5), в результате правостороннего транспонирования матрицы (4). Имеем

$$F_f=\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & u_1 \\ 0 & 1 & \cdots & 0 & 0 & u_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & u_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & u_{n-1} \end{pmatrix}. \tag{6}$$

Частным случаем (6) является матрица Фибоначчи над ПрП восьмой степени $f_8=101001101$, образуемая правосторонним транспонированием матрицы (3), т.е.,

$$F_f=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{7}$$

Структурная схема генератора ПСП в конфигурации Фибоначчи, соответствующая матрице (7), приведена на рис. 2.

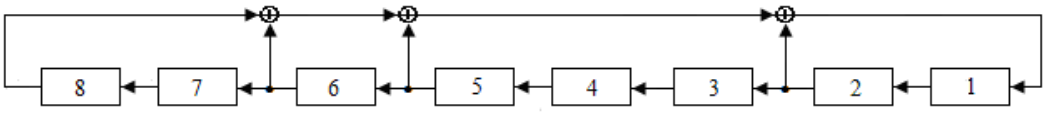

Рис. 2. Структурная схема генератора Фибоначчи над ПрП $f_8=101001101$

4. Сопряженные генераторы Галуа и Фибоначчи

В теории групп элемент x^* некоторой группы X является *сопряженным* элементу x той же группы, если существует некоторый элемент $z\in X$ такой, что

$$x^*=z^{-1}\cdot x\cdot z. \tag{8}$$

По аналогии с (8) введем формальное определение понятия *сопряженных матриц* Галуа и Фибоначчи по форме

$$M^*=P^{-1}\cdot M\cdot P, \tag{9}$$

где M есть матрица G или F, а $P-$ матрица, которая носит название *матрицы перехода* от M к M^*. Для простоты индекс f в матрицах G и F иногда будем опускать.

Как следует из соотношения (9), 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 (8) и (9). В качестве матрицы P в данной работе выбрана *матрица инверсной перестановки* (ИП), которую условно обозначим цифрой 1 (как элемент группы простых кодов Грея [5]). 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*, т.е. матрицей, обратной самой себе. Это означает, что $1\cdot 1=1^2=E$. Таким образом,

$$\begin{aligned}&G^*=1\cdot G\cdot 1, \qquad G=1\cdot G^*\cdot 1;\\&F^*=1\cdot F\cdot 1, \qquad F=1\cdot F^*\cdot 1.\end{aligned} \tag{10}$$

Следовательно,

$$M^*\overset{1}{\longleftrightarrow}M,\ \ M\in\{G,F\}. \tag{11}$$

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.

Согласно взаимно-однозначному соответствию (11) любая из рассматриваемых матриц Галуа и Фибоначчи (базовая M или сопряженная M^*) может быть получена в результате *преобразования подобия* из другой матрицы. Общие формы классических сопряженных матриц $n-$го порядка, в соответствии с (4), (6) и (10), имеют вид:

$$G_f^*=\begin{pmatrix}0&1&0&\cdots&0&0\\0&0&1&\cdots&0&0\\\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&1&0\\0&0&0&\cdots&0&1\\1&u_1&u_1&\cdots&u_{n-2}&u_{n-1}\end{pmatrix};\quad F_f^*=\begin{pmatrix}u_{n-1}&1&0&\cdots&0&0\\u_{n-2}&0&1&\cdots&0&0\\\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\u_2&0&0&\cdots&1&0\\u_1&0&0&\cdots&0&1\\1&0&0&\cdots&0&0\end{pmatrix}. \tag{12}$$

Согласно формам (12) для сопряженных матриц G_f^* и F_f^* над ПрП $f_8=101001101$ приходим к структурным схемам восьмиразрядных генераторов ПСП Галуа и Фибоначчи, представленных на рис. 3 и 4 соответственно.

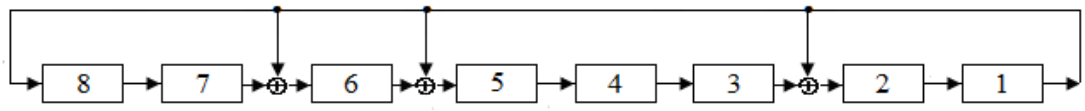

Рис. 3. Структурная схема сопряженного генератора Галуа над ПрП $f_8=101001101$

Рис. 4. Структурная схема сопряженного генератора Фибоначчи над ПрП $f_8=101001101$

Функции возбуждения $D-$триггеров классических $n-$разрядных сопряженных генераторов ПСП Галуа и Фибоначчи (начальные состояния регистров для обоих генераторов одинаковы и таковы: $s_1(0)=1$, $s_k(0)=0$, $k=\overline{2,n}$, при том, что $n=8$) определяются выражениями:

$$\nu_n(t)=s_1(t-1);\quad \nu_k(t)=s_{k+1}(t-1)\oplus u_{n-k}\cdot s_1(t-1),\quad k=\overline{1,n-1},\quad t=1,2,\cdots;$$

и

$$\nu_k(t)=s_{k+1}(t-1),\quad k=\overline{1,n-1};\quad \nu_n(t)=s_1(t-1)\overset{n}{\underset{k=2}{\oplus}} u_{k-1}\cdot s_k(t-1),\quad t=1,2,\cdots.$$

5. Линейные преобразования генераторов ПСП

Из сопоставления базовых матриц Галуа G_f (4) и Фибоначчи F_f (6), а также их сопряженных вариантов G_f^* и F_f^* (12) легко могут быть определены (табл. 1) операторы преобразования одной из известных матриц, в любую другую матрицу.

Таблица 1.

Операторы преобразование матриц

	G	F	G^*	F^*
G	—	$\perp$	$\mathsf{T}\perp$	T
F	$\perp$	—	T	$\mathsf{T}\perp$
G^*	$\mathsf{T}\perp$	T	—	$\perp$
F^*	T	$\mathsf{T}\perp$	$\perp$	—

В соответствии с табл. 1, если две матрицы принадлежат различным подгруппам (назовем их подгруппами Галуа и Фибоначчи), причем одна из них является сопряженной, то они связаны оператором классического транспонирования T.

Анализируя структурные схемы простых ЛРС частных генераторов ПСП над ПрП $f_8=101001101$, приведенных на рис. 1 – 4, приходим к общим правилам преобразования, сведенных в табл. 2, схем линейных обратных связей (ОС) известного генератора ПСП над заданным ПрП f_n к схемам ОС любого их оставшихся трех видов генераторов. В отличие от табл. 1, в которой символами G, F, G^* и F^* обозначены примитивные матрицы генераторов ПСП, в табл. 2 этими же символами условно обозначены *схемы обратных связей* в соответствующих генераторах.

Таблица 2.

Операторы преобразования обратных связей

	G	F	G^*	F^*
G	—	$1\circ 1$	$\circ 1$	$1\circ$
F	$1\circ 1$	—	$1\circ$	$\circ 1$
G^*	$\circ 1$	$1\circ$	—	$1\circ 1$
F^*	$1\circ$	$\circ 1$	$1\circ 1$	—

Смысл термина «схемы обратных связей» в G, F, G^* или F^* генераторах ПСП можно пояснить, обратившись к их стилизованному графическому отображению, показанному на рис. 5. Обратим внимание на такие особенности ОС. Если в базовых G и F генераторах ПСП обратные связи осуществляется по направлению часовой стрелки, то в сопряженных G^* и F^* генераторах – против часовой стрелки.

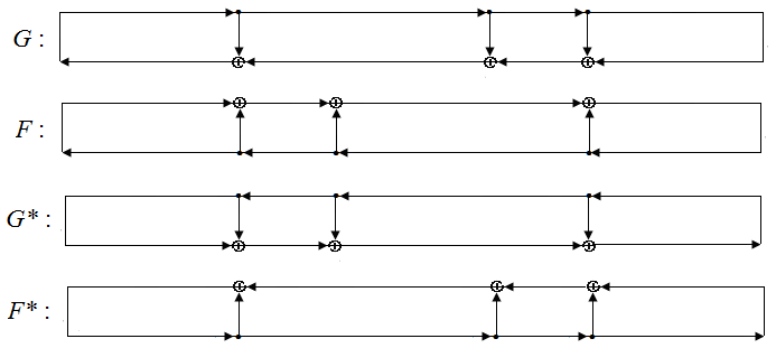

Рис. 5. Стилизованное представление обратных связей в генераторах ПСП

Уточним физический смысл операторов преобразования в табл. 2. Оператор $\circ 1$ означает, что схема ОС, обозначенная символом $\circ$, претерпевает *вращение* на 180° относительно вертикальной оси. Такие преобразования происходят, как это следует из рис. 5, в парах генераторов (G, G^*) или (F, F^*). Операция $\circ 1$ подобна операции инверсной перестановки столбцов матрицы M, которая реализуется, если умножить ее справа на матрицу инверсной перестановки 1. Оператором $1\circ$ осуществляется вращение схемы ОС относительно горизонтальной оси. Таким образом, операция $1\circ$ подобна операции инверсной перестановки строк матрицы M, если умножить ее слева на матрицу инверсной перестановки. Указанные преобразования обратных связей имеют место в парах генераторов (G, F^*) или (F, G^*). И, наконец, оператор $1\circ 1$ означает, что схема ОС претерпевает вращение на 180° относительно как вертикальной, так и горизонтальной осей. Такие преобразования схем ОС выполняются в парах генераторов (G, F) или (G^*, F^*).

6. Обобщенные примитивные матрицы Галуа над $GF(2)$

В данном разделе предлагается алгоритм построения примитивных матриц Галуа и других, связанных с ними матриц, в качестве образующих элементов которых применяются примитивные элементы $\omega > p = 2 = 10$ поля $GF(2^n)$ над произвольными неприводимыми двоичными полиномами f_n (совсем не обязательно примитивными) степени n.

Для решения задачи синтеза примитивных матриц воспользуемся *обобщенным правилом диагонального заполнения*, суть которого состоит в следующем. Первоначально в нижней строке матрицы G $n-$го порядка записывается ОЭ ω, являющийся примитивным элементом поля $GF(p^n)$ над выбранным НП f_n. 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 $n = 8$ и $f_8 = 101001101$. Выберем, для примера, ОЭ $\omega = 2D = 101101$. Приходим к примитивной матрице Галуа, представленной соотношением

$$G_f = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \qquad (13)$$

Обобщенной матрице Галуа G соответствует *обобщенная матрица Фибоначчи* F, образуемая оператором правостороннего транспонирования $\perp$ матрицы (13), т.е.

$$F_f = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}. \qquad (14)$$

Оператором $1 \circ 1$ матрицы (13) и (14) преобразуются в обобщенные сопряженные матрицы G^* и F^*, представленные соотношениями

$$G_f^* = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}; \quad F_f^* = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Рассмотрим пример синтеза обобщенных примитивных матриц и генераторов Галуа, выбрав в качестве неприводимого полином четвертой степени $f_n = 11111$, не являющийся примитивным, и примитивный ОЭ ω полинома f_n, равный 111. Матрицы, отвечающие выбранным параметрам генераторов, имеют вид:

$$G1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}; \quad F1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix};$$

$$G1^* = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}; \quad F1^* = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \qquad (15)$$

Структурная схема обобщенного базового четырехразрядного генератора Галуа, совпадающая с обобщенной схемой базового генератора Фибоначчи, показана на рис. 6. Вертикально расположенные регистры генераторов, отмеченные сверху символом $\otimes$, реализуют операцию поразрядного умножения, а регистры, отмеченные символом $\oplus$ – операцию сложения содержимого регистра по модулю 2.

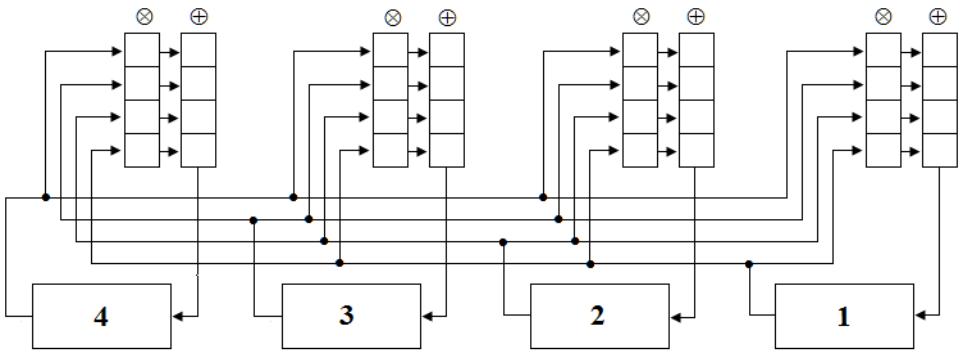

Рис. 6. Структурная схема обобщенных базовых генераторов ПСП Галуа/Фибоначчи

Если в регистрах умножения разместить элементы столбцов матрицы $G1$ системы (15), то получим генератор ПСП по схеме Галуа. В том случае, когда в тех же регистрах будут расставлены элементы матрицы $F1$, то образуется генератор ПСП в конфигурации Фибоначчи.

Схема сопряженных генераторов ПСП показана на рис. 7.

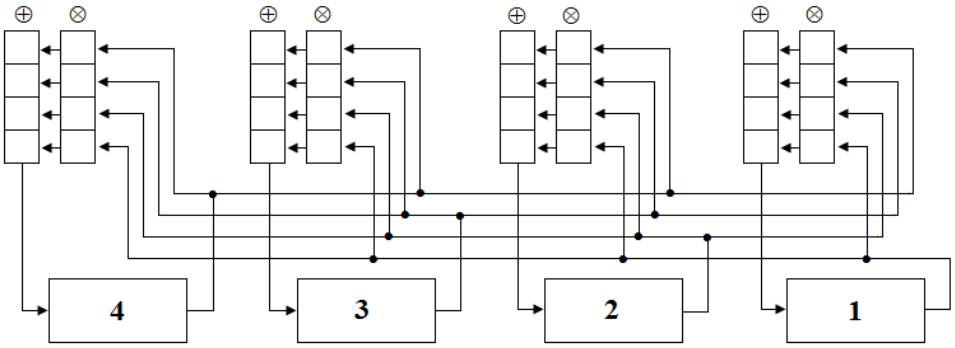

Рис. 7. Структурная схема обобщенных сопряженных генераторов ПСП Галуа/Фибоначчи

Аналогично базовым генераторам ПСП, если в регистрах умножения структурной схемы на рис. 7 разместить элементы столбцов матрицы $G1^*$, то получим обобщенный сопряженный генератор ПСП по схеме Галуа. В том случае, когда в тех же регистрах будут расставлены элементы матрицы $F1^*$, то образуется сопряженный генератор ПСП в конфигурации Фибоначчи.

Обобщенные примитивные матрицы, принадлежащие одной и той же группе (Галуа или Фибоначчи), обладают замечательным свойством *коммутативности*, суть которого поясняется ниже. Пусть ω_2=1011 – второй примитивный элемент поля $GF(2^4)$, отличный от ОЭ ω_1=111. Образующему элементу ω_2 отвечает такая совокупность примитивных матриц:

$$G2=\begin{pmatrix}0&1&0&1\\1&1&0&1\\1&0&0&1\\1&0&1&1\end{pmatrix};\qquad F2=\begin{pmatrix}1&1&1&1\\1&0&0&0\\0&0&1&1\\1&1&1&0\end{pmatrix};$$

$$G2^*=\begin{pmatrix}1&1&0&1\\1&0&0&1\\1&0&1&1\\1&0&1&0\end{pmatrix};\qquad F2^*=\begin{pmatrix}0&1&1&1\\1&1&0&0\\0&0&0&1\\1&1&1&1\end{pmatrix}. \tag{16}$$

Во множествах примитивных матриц (15) и (16) можно выделить коммутативные и не коммутативные матрицы. Коммутативными являются любые пары матриц, принадлежащие одной из двух групп *однородных примитивных матриц*. Первую однородную группу составляют матрицы Галуа (G – группа), в которую входят примитивные матрицы $G=\{G1,G2,G1^*,G2^*\}$. Во вторую (F – группу) входят примитивные матрицы Фибоначчи $F=\{F1,F2,F1^*,F2^*\}$. Таким образом, например, матрица $G1$ коммутативна с любой из трех матриц $G2$, $G1^*$ или $G2^*$, но не коммутативна ни с одной из примитивных матриц, входящих в F – группу.

Отметим, кроме того, такое интересное свойство примитивных базовых матриц Галуа G над НП f_n и ОЭ $\omega\geq 10$. Структура степеней G – матриц, т.е. матриц G^k, такая же, как и структура базовой матрицы G, т.е. подчинена принципу диагонального заполнения строк матриц. А из этого следует, что для того, чтобы вычислить матрицу G^k, достаточно возвести

в k – ю степень ОЭ ω, привести к остатку по модулю f_n значение ω^k и далее воспользоваться правилом диагонального заполнения матриц, используя в качестве образующего элемент $\omega_k = (\omega^k) \bmod f_n$. Эта особенность матриц будет учтена в последнем разделе, в котором устанавливается изоморфизм матриц Галуа.

8. Синтез примитивных матриц Галуа над $GF(p)$**,** $p > 2$

Примитивные матрицы над $GF(p)$, $p > 2$, синтезируются по тем же правилам (диагонального заполнения), что и матрицы над $GF(2)$. Выберем, для примера, $n = 4$, $p = 3$ и неприводимый над $GF(3)$ унитарный полином $f_4 = 12101$. Пусть $\omega = 1102$. Базовые G, F и сопряженные G^*, F^* обобщенные матрицы Галуа и Фибоначчи, соответствующие выбранным параметрам n, ω и f_4, имеют вид:

$$G = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 1 & 0 & 2 \end{pmatrix}; \quad F = \begin{pmatrix} 2 & 2 & 1 & 2 \\ 0 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 1 & 2 & 1 & 1 \end{pmatrix}; \tag{17}$$

$$G^* = \begin{pmatrix} 2 & 0 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 \end{pmatrix}; \quad F^* = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 2 & 0 \\ 2 & 1 & 2 & 2 \end{pmatrix}.$$

Структурные схемы обобщенных ЛРС инвариантны к характеристике поля p. В частности, структурная схема четырехразрядного Галуа ЛРС, обратные связи в котором заданы матрицей G системы (17), представлена на рис. 8, причем $\oplus$ есть оператор сложения по модулю $p = 3$.

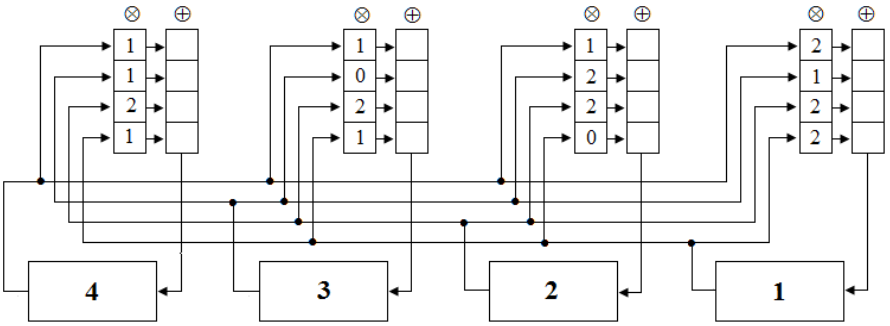

Рис. 8. Структурная схема обобщенного ЛРС Галуа

Структурная схема четырехразрядного сопряженного ЛРС Фибоначчи, обратные связи в котором заданы матрицей F^* системы (17), изображена на рис. 9.

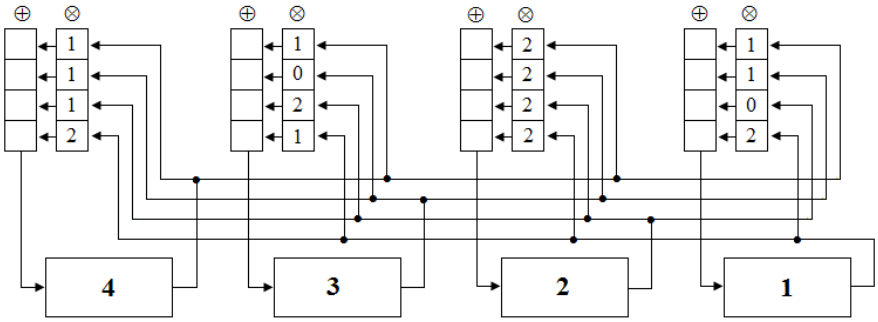

Рис. 9. Структурная схема обобщенного сопряженного ЛРС Фибоначчи

Из сопоставления рис. 6-9 следует, что структурные схемы базовых и сопряженных генераторов *инвариантны к операторам правостороннего транспонирования.*

И в заключение раздела обратим внимание на следующие факты. Во-первых, если хотя бы одна из обобщенных матриц над выбранным НП не примитивна (а это может произойти только в случае, если в качестве ОЭ матрицы выбран элемент поля Галуа, не являющийся примитивным), то свойство примитивности и коммутативности матриц утрачивается. И, во-вторых, согласно соотношениям (17) сопряженные матрицы Галуа и Фибоначчи являются матрицами, образуемыми преобразованием подобия исходных (базовых) матриц G и F. В качестве матриц преобразования P выступают матрицы инверсной перестановки 1. Как известно, подобные матрицы сохраняют все свойства исходных матриц. В силу указанной особенности, если матрицы G и F (простые или обобщенные) примитивны, то и соответствующие им сопряженные матрицы G^* и F^* также оказываются примитивными.

10. Изоморфизм матриц Галуа

Ранее было отмечено, что для того чтобы вычислить $k-$ю степень матрицы Галуа, достаточно возвести в $k-$ю степень ОЭ ω этой матрицы, вычислить остаток по модулю f_n значения ω^k и далее воспользоваться обобщенным правилом диагонального заполнения матриц, используя в качестве образующего элемент $\omega_k = (\omega^k) \bmod f_n$.

Рассмотрим другую интерпретацию правила «диагонального заполнения», используемого при синтезе матриц Галуа над полем $GF(p^n)$. Согласно предлагаемому правилу, на начальном этапе синтеза матрицы G_f, где $f = f_n -$неприводимый полином $n-$й степени, образующий ее элемент ω размещается в младших (правых) разрядах нижней строки матрицы $n-$го порядка. Последующие строки матрицы образуются сдвигом на один разряд влево предшествующей строки, причем после сдвига в освободившийся правый разряд записывается 0. В том случае, если ненулевой старший (левый) элемент сдвигаемой строки выходит за пределы матрицы, то этот $(n+1)-$разрядный $p-$ичный вектор приводится к остатку по $\bmod f_n$. Тем самым такая строка возвращается в границы матрицы и процесс заполнения ее оставшихся верхних строк продолжается по уже описанной схеме.

Образующий элемент ω матрицы Галуа G_f, содержащий $k+1$ разрядов, принадлежащих полю $GF(p)$, можно представить в виде полинома $k-$й степени одной переменной x, т.е. 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. Другими словами,

$$x \cdot \omega_k(x) \to \omega_{k+1}(x). \tag{18}$$

Воспользовавшись преобразованием (18), представим матрицу Галуа G_f порядка n выражением

$$G_f = \begin{pmatrix} x^{n-1} \cdot \omega \\ x^{n-2} \cdot \omega \\ \dots \\ x \cdot \omega \\ \omega \end{pmatrix} (\bmod f) = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \dots \\ x \\ 1 \end{pmatrix} (\bmod f), \tag{19}$$

Элементы x^l, $l = \overline{1, n-1}$, правого вектор-столбца в соотношении (19) являются полиномами $l-$й степени одной переменной, векторная форма которых имеет вид:

$$x^l \to \underbrace{1, 0, \cdots 0, 0}_{(l+1)}, \quad l = \overline{1, n-1}. \tag{20}$$

С учетом замены (20) приходим к такому представлению вектор-столбца:

$$\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = E, \qquad (21)$$

где E – единичная матрица n – го порядка.

Соотношения (19)-(21) дают возможность сформулировать заключение: матрица Галуа G_f порядка n над НП f_n однозначно определяется своим образующим элементом ω. Следовательно, матрица Галуа G_f 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 и ее образующим элементом ω существует взаимно-однозначное соответствие, т.е. $G_f \leftrightarrow \omega$.

Кроме того, следует иметь в виду, что образующий элемент ω не может быть меньше характеристики p НП f_n, 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 становится диагональной, не зависящей 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.

11. Характеристические полиномы матриц Галуа

Характеристическим полиномом (ХП) невырожденной квадратной матрицы A n – го порядка называется полином n – й степени

$$\chi(\lambda) = \det(A - \lambda E),$$

где E – единичная матрица того же порядка n, что и матрица A [6].

Замечательное свойство ХП матриц состоит в том, что если некоторые матрицы A и B подобны, то их ХП совпадают. Справедливо и обратное: если ХП матриц совпадают, то они являются подобными.

Обратимся к численному анализу характеристических полиномов матриц Галуа, Фибоначчи и сопряженным им матрицам. Справедливо следующее

***Утверждение*:** *Характеристические полиномы матриц Галуа и Фибоначчи (как базовых, так и сопряженных) над* $GF(p)$, $p \geq 2$, *с образующими элементами* $\omega = 10$ *совпадают с неприводимыми полиномами, порождающими данные матрицы.*

Суть утверждения состоит в том, что

$$\chi(x) = \det(M_{f_n} - xE) \equiv f_n(x), \qquad (22)$$

где M_{f_n} – матрицы G, F, G^* или F^*, порождаемые НП $f_n(x)$ и ОЭ $\omega = 10$.

Доказательство утверждения можно провести методом непосредственной проверки. В самом деле, выберем, для примера, ПрП третьей степени $f_3(x) = 1011$, $p = 2$, для которого

$$\chi_G(x) = \begin{vmatrix} -x & 1 & 1 \\ 1 & -x & 0 \\ 0 & 1 & -x \end{vmatrix}; \chi_F(x) = \begin{vmatrix} -x & 0 & 1 \\ 1 & -x & 1 \\ 0 & 1 & -x \end{vmatrix}; \chi_{G^*}(x) = \begin{vmatrix} -x & 1 & 0 \\ 0 & -x & 1 \\ 1 & 1 & -x \end{vmatrix}; \chi_{F^*}(x) = \begin{vmatrix} -x & 1 & 0 \\ 1 & -x & 1 \\ 1 & 0 & -x \end{vmatrix},$$

где $|A|$ – определитель матрицы A.

Легко убедиться в том, что для всех четырех матриц ХП являются одинаковыми, такими, что $\chi(x) = x^3 + x + 1$, совпадающими с ПрП $f_3(x)$.

Аналогичным образом осуществляется проверка равенства (22) также для матриц, порождаемых неприводимыми полиномами, не являющимися примитивными, но при условии, что образующие их элементы равны 10.

Вместе с тем, для обобщенных матриц G, F, G^* и F^*, т.е. таких, для которых ОЭ $\omega > 10$, утверждение не всегда выполняется. Рассмотрим пример. Пусть $p = 2$, $f_3(x) = 1011$ и $\omega = 101$. Имеем

$$G = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}; \quad \chi_G(x) = \begin{vmatrix} -x & 1 & 0 \\ 0 & -x & 1 \\ 1 & 0 & 1-x \end{vmatrix} = x^3 + x^2 + 1 \Rightarrow 1101,$$

т.е. $\chi_G(x)$ не совпадает с $f_3(x)$.

Выводы

Основным результатом данного исследования является разработка алгоритмов синтеза обобщенных базовых и сопряженных матриц Галуа и Фибоначчи, элементы которых принадлежат простому полю $GF(p)$ характеристики $p \geq 2$. Данные матрицы обладают замечательными свойствами, такими как примитивность и коммутативность, что дало возможность построить на их основе обобщенные линейные регистры сдвига максимального периода и соответствующие им генераторы псевдослучайных последовательностей. Структурные схемы обобщенных ЛРС оказались однородными и инвариантными как к порядкам регистров n, так и характеристикам p поля Галуа.

Вместе с тем следует отметить, что обобщенные ЛРС с линейными обратными связями не привносят каких-либо новых свойств последовательностям, формируемым обобщенными генераторами ПСП, поскольку для обобщенных генераторов ПСП постулаты Голомба соблюдаются точно так же, как и для классических генераторов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. / М. А.Иванов, И. В. Чугунков – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.
2. Лидл Р. Конечные поля. Монография в 2-х томах. / Р. Лидл, Г. Нидеррайтер – Т. 1. – М.: Мир, 1988. – 432 с.
3. 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. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. / М. А. Иванов– М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.
5. Белецкий А. Я. Преобразования Грея. / А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий – Монография в 2-х томах. – Т. 1. Основы теории. – К:. Кн. вид-во «НАУ-Друк», 2007. – 412 с.
6. Гантмахер Ф. Р. Теория матриц. / Ф. Р. Гантмахер – М.: Наука, 1968. – 576 с.