СВОЙСТВА БИНАРНЫХ МАТРИЦ И ЭЛЕМЕНТОВ КОНЕЧНОГО ПОЛЯ, РЕАЛИЗУЮЩИХ ДРУГ ДРУГА

Барашко А.С.

Кафедра ПМИ ДонГТУ

Abstract

Barashko Л..S". Properties ***of binary matrices and finite field elements which realize one another.*** *The criterions of the possibility realization of binary matrices by finite field elements are found. It is showed that the set ofbinary matrices, realized by field elements, is isomorphic to this field. The finding methods of matrix, realized by the given field element, and conversely offield element, which realize the given matrix of some type, are proposed.*

В данной работе продолжены исследования, результаты которых опубликованы в [1]. В [2] показано, что многоканальные сигнатурные анализаторы (СА) типа MISR (multiple input signature register) удобно описывать линейными полиномами над расширениями поля Галуа *GFß).* Схема СА типа MISR, задаваемого полиномом $g(x) = x^r+g>\_i/^{\wedge}+...+gix+go$ степени r над *GFfl),* и схема СА, задаваемого линейным полиномом $x+a$, где *a eGFft'),* показаны на рисунках 1 и 2 соответственно.

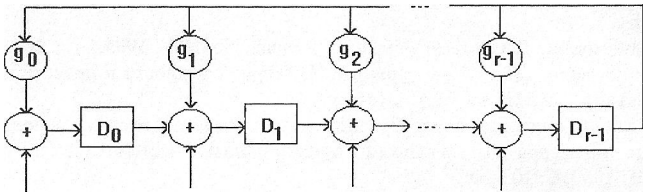

Рис. 1. СА типа MISR, задаваемый полиномом *g(x)* степени r.

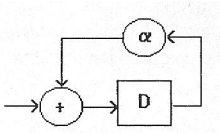

Рис. 2. СА, задаваемый полиномомх+α над *GF(.I').*

Сигнатурный анализатор, показанный на рис. 1, является частным случаем СА C= *(A, I),* определяемого бинарной *rxr-* матрицей *A* (/ - единичная *rxr-* матрица). В случае, изображенномнарисунке 1 *,A= Mg^,r%e*

$$M_{g(x)} = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & g_0 \\ 1 & 0 & 0 & \dots & 0 & g_1 \\ 0 & 1 & 0 & \dots & 0 & g_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & g_{r-1} \end{bmatrix}$$

транспонированная сопровождающая матрица полинома *g(xj* [3]. СА, показанный на рис. 2, определяется только элементом *a eGFft'(.* Поэтому отождествим его с этим элементом. Определим, в каком смысле будем считать СА Ci= *(A, I)* и *Ci=a* одинаковыми. Для $r > 1$ введем в рассмотрение векторное пространство E_r бинарных векторов-столбцов размерности r с покомпонентной операцией сложения по модулю 2. Операции сложения в E_r и *GFft')* будем обозначать одинаково +.

Определение 1. СА *C=(A, I),* где *A* - бинарная *rxr-* матрица, и *a eGFft')* изоморфны (обозначение С = а), если существует такое линейное взаимно однозначное отображение (л.в.о.о.) *f. E_r ^> GFft'),* что *f(As+y) = f(y)+ af(s)* для всех *s, ye E_r.*

Определение 2. Бинарная *rxr-* матрица *A* и элемент *a eGFft!)* реализуют друг друга, если существует такое л.в.о.о./ *E_r ^> GFft'),* что *f(As)= af(s)* для всех *s* є *E_r.*

СА C=(A, I) является линейной последовательностной машиной без выходов с начальным состоянием 0 (0 - вектор-столбец, все компоненты которого есть 0). Поэтому его можно представить в виде инициального автомата без выходов *C=(E_r, E_r, δ* Q), где первое E_r - множество состояний, второе E_r - входной алфавит, *δ* - функция переходов, 0 - начальное состояние. Для любых *s, ye E_r δ'(s, y)=As+y.* Для произвольного конечного алфавита *X* обозначим *X* множество всех слов над этим алфавитом конечной длины, включая пустое слово е длины 0. СА С характеризуется множеством необнаружимых им ошибок, которое задается выражением *Vc={ue E_r \ δ(0, u)*= 0 }. Сигнатурой слова *ue* E_r в СА С называют *sc(it)= 5*(0, *u).*

Аналогичные понятия можно ввести и для СА, изображенного на рис. 2. Любое слово w= W_1 ... *w,, є X* (w, *eX)* можно представить в виде полинома*p,, (x)= w\x"~'+* vi'2x" *" [2]+ ... + w_n .\+w,,* (если *w=e,* то *$p_w(x)$*= 0). Для *a eGFft')* положим *V_a={ve (GFft'))* I *(x+a)* I *$p_v(x)$},* где *(x+a)* | *p,(x)* означает деление полинома *$p_v(x)$* на полином *x+a* без остатка. Сигнатура *$s_a(v)$* слова *ve(GFft'))* в СА, определяемом элементом *a &GFft'),* задается равенством *$s_a(v)=R_{x+a}$ [p/xJ],* где *R_{x+a}* [*p,(x)]* - остаток от деления полинома *$p_v(x)$* на полином *x+a* . Л.в.о.о. *f. E_r ~^ GFft')* можно расширить до отображения *f.* £*-> *(GFft'))*,* положив *f(e)=e* и, если *u=u\ ... u,,* , где u,e E_r , то *f(u)=f(u\) ...J(U_n).* Отметим также, что любое л.в.о.о./определяется заданием базы пространства *GFft')* [1]. Базу в пространстве *GFft')* будем задавать в виде вектора *b=(βi ,..., β_r),* где *β\ ,..., β_r-* линейно независимые элементы поля *GFft').*

Основываясь нарезультатах [1], можно сформулировать следующую теорему.

Теорема 1 *.Для СА C=(A, I) и a eGF(2^r) следующиеутвержденияравносильны:*

1. С= а.

2. А и а реализуют друг друга.

3.Wc)= У_адля некоторогол.в.о.о./·. E_r ^> GFft').

4. $\wedge_{u\&E}{}^{t}(f\{s_{c}\{u) = s_{a}\{f\{u))) \quad npuHeKotopoMn.e.o.o.f.E_{r}\wedge GF\beta^{r}).$

5. bA=ab для некоторой базы b пространства GFft').

Оставшаяся часть статьи будет посвящена анализу матричного уравнения

$$bA=\alpha b, \tag{1}$$

где *b* - база *GFft'), a eGF(2')* и *A* - бинарная *rxr*- матрица.

Отметим, что если *b* - база *GFft'),* то любая другая база *b'* этого же пространства может быть получена из *b* путем ее умножения на некоторую неособенную бинарную *rxr*- матрицу *Q,* т.е. *b' = bQ.* Справедлива следующая цепочка равносилыюстей:

$$bA=ab<t> \quad b' \quad Q\text{-}^{i}A=Ub' \quad Q\wedge<=>b' \quad Q \quad {}^{i}AQ=Ub' \quad ,$$

где $Q\text{-}^{i}AQ$ - матрица, подобная матрице *A.* В результате получаем следующее утверждение.

Теорема *2. Если бинарная rxr-матрица A и элемент a є GF(2') реализуют друг друга в базе b, то любая подобная A матрица и этот оіce элемент a реализуют друг друга в некоторой базе b'* .

Из уравнения (1) и единственности представления элемента через базу следует, что при фиксированном элементе *a* и базе *b* существует единственная матрица *A* такая, что *A* и *a* реализуют друг друга в базе *b.* Обозначим эту единственную бинарную *rxr*-матрицу Ag и покажем, как ее найти по *a* и *b.*

Если *a* = 0, то Ад = 0, так как *b0 = 0b.* Если *a* = 1, то *A^* =/, так как *bl* = 1 *b.* Таким образом, элементы 0 и 1 реализуют матрицы 0 и I в любой базе.

Пусть *b* - база *GF(I')* и *a є GF(I')* - ненулевой элемент. Поскольку *b A^ =ab,* то I *Aβ* I * 0, т.е. *Aд* - неособенная матрица. Поэтому *a' '& = b(A„)* $^{\prime 1}$ и, значит, матрица $(\mathrm{A}д)'^{1}$ и элемент a'^{1} реализуют друг друга в базе *b.* Из уравнения (1) следует, что элементы, реализующие в фиксированной базе одну и ту же матрицу, одинаковы, а матрицы, реализуемые одним и тем же элементом (в различных базах), подобны. В фиксированной базе *GF(2')* существует в точности 2^{Γ} бинарных *rxr*- матриц, реализуемых элементами поля *GFQ').* В любой другой базе это множество из 2^{Γ} бинарных матриц будет преобразовано в множество подобных им матриц, причем матрица подобия будет равна матрице перехода от первой базы ко второй. Поэтому достаточно получить общий вид матриц, реализуемых элементами поля в какой-либо одной базе.

При нахождении общего вида матрицы А% будут использоваться некоторые понятия теории конечных полей [4]. Следом произвольного элемента */є GFQ')* называют $T,(/)=y + y^{2} + y^{2} + \ldots + \gamma^{2}$. При этом *Tr(y)e GF(2).* Базы *b =(β\ , ... , βr)* и *I=(λι,..., λ,)* пространства *GF(2')* называются дополнительными (двойственными), если

$$T_r(\beta_i\lambda_j)=\begin{cases}0, \text{если } i\neq j,\\ 1, \text{если } i=j.\end{cases}$$

Для любой базы существует единственная дополнительная база. Следующая формула дает представление элемента *γ* в базе *b:*

$$\gamma=\sum_{i=1}^{r}T_r(\gamma\lambda_i)\beta_i,$$

где $T,(\gamma\lambda O,\sim\cdot$, $T,(\gamma\lambda,)$ - координаты элемента γ в базе b. Пусть Tj - вектор-столбец координат элемента γ в базе b, т.е. $\gamma = b\,Tj$. Тогда $a\beta, = b\,T'''^{\wedge'}$. Определим бинарную rxr- матрицу $T\,\wedge = \{\ T\,f\ \backslash\ .\ .\ .\ j\,f\ '\ \backslash$. Поскольку $bT^{\wedge}=(bT^{\wedge}\backslash...$, $bT_r^{a\beta'})=(a\beta,,....$, $a\beta_r) = ab$, *то* $A^b_a = T_r^{ab}$.

Теперь рассмотрим способ вычисления матрицы $A^{\wedge}$ в одной конкретной базе b пространства $GF(2^r)$. Для произвольного $\gamma\varepsilon\ GF(2^r)$ через y^b обозначим вектор-столбец бинарных координат элемента yъ базе b. Пусть M_r - множество полиномов над $GF(2)$, степень которых не превышает r - 1, и φ: $E_r \wedge M_r$ - взаимно однозначное отображение, которое для произвольного 5 $=(so,\ s\text{i},\ \ldots\ ,\ \boldsymbol{S_r}\ .\ \iota)'\ \epsilon\ E_r$ (здесь ' обозначает операцию транспонирования) определяется равенством $\varphi(\varsigma)= s_r.\ /x^{\mathrm{r}}\ \wedge\ '+S_{\tau} - 2^{*r}\ ^2+...+\ \mathrm{siJt}+\ \mathrm{So}\ \cdot$ Предположим $GF(2^r)$ - расширение поля $GF(2)$ по модулю $p(x)$, где $p(x)$ - примитивный полином степени r над $GF(2)$. Тогда, считая элементами $GF(T)$ полиномы из M_r , получим, что χ - примитивный элемент $GF(2^r)$. Зафиксируем базу $b=(l,\ x,\ x^2,\ ...,\ x\ '\ ')$ поля $GF(2^r)$. Полагая $a = x$, любой ненулевой элемент поля можно представить в виде ot, где $0< k < 2^r$ - 2. Матрица $A^b_{a\ i}$, реализуемая элементом ot в базе b, определяется равенствами

$$A^b_{\alpha^k} =[(\alpha^k)^b,\ (\alpha^{k+1})^b,...,(\alpha^{k+r-1})^b]=$$

$$[\varphi^{-1}(R_{p(x)}[x^k]),\varphi^{-1}(R_{p(x)}[x^{k+1}]),\ldots,\varphi^{-1}(R_{p(x)}[x^{k+r+1}])].$$

Пример. Пусть $GF(\backslash 6)$- расширение поля $GF(2)$ по примитивному полиному$p(x)= x^4+x+\backslash$ и $a = \chi$ - примитивный элемент этого поля. Найдем матрицу A^b_{a},, реализуемую элементом a^5 в базе $b=(\backslash,\ x,\ x^2,\ x^3)$. Поскольку $Яp\wedge[x\wedge] = x^2+x$, $«P(x)\ [*^6] = *^3\ + *^2$, $Rp(X)\ [*^7] = X^3\ + *\ + 1$ и $R_{p(x)}[x^8] = *^2\ + 1$, ТО

$$A^b_{\alpha^5} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Рассмотрим множество бинарных rxr- матриц, реализуемых в базе b всеми элементами поля $GF(1)$, т. е. $Q^b = \{A^b{}_a \backslash a\ \epsilon\ GF(I^r)\}$. В качестве операции сложения + и умножения • матриц из этого множества примем расширенные на матрицы операции сложения и умножения поля $GF(2)$.

Теорема 3. *Тройка* $< \mathbf{\Omega}^{\wedge},\ +,\ - >$ *изоморфна полю* $GF(2')$.

Доказательство. Пусть $a,\ \beta e\ GF(2')$ и b - база $GF(2^r)$. Тогда $b(A^{\wedge} + A^{\wedge}) = ab+\beta b= (a\ +\beta\ )b$ и $b(A^b\text{-}A^b) = (bA^b)A^b{}_{,,} = abA^b = a\beta b$. Отсюда следует, что

сложению и умножению матриц в Ω, в поле $GF(2^r)$ соответствует сложение и умножение реализующих их элементов. Теорема доказана.

Теперь рассмотрим вопрос, как по бинарной квадратной матрице найти базу и элемент поля, реализующий данную матрицу в этой базе. Ясно, что не всякая матрица может быть реализована элементом поля в некоторой базе. В [1] установлено, что бинарная *rxr*- матрица A реализуема элементом поля в некоторой базе тогда и только тогда, когда ее минимальный полином $m_A(x)$ прост.

Пусть бинарная *rxr*- матрица A такова, что полином *m^(x)* прост. Ограничимся нахождением базы и элемента поля, реализующего естественную нормальную форму [3] M матрицы A в этой базе. Известно, что M подобна A, т. е. $M= QAQ'$, где Q - некоторая бинарная неособенная матрица. Если $bM= ab$, то $bQA= abQ$. Полагая $b' = bQ$, получаем $b'A = ab'$, т. е. матрица^ реализуемаэлементом a в базе b' .

Если *тл(х)* - прост, то, как следует из [1], матрицаМимеет вид

$$M=\begin{bmatrix} M_{d(x)} & & & \\ & M_{d(x)} & & \\ & & \ddots & \\ & & & M_{d(x)} \end{bmatrix},$$

где *mj(x)= тм(x')- d(x)* $=x^k+a_{k-1}x^{k-1}+\ldots+a_1x+a_0$ и число блоков

$$Md(x) = \begin{vmatrix} 0 & 0 & 0 & \ldots & 0 & d_0 \\ 1 & 0 & 0 & \ldots & 0 & d_1 \\ 0 & 1 & 0 & \ldots & 0 & d_2 \\ & & & & & \\ 0 & 0 & 0 & \ldots & 1 & d_{r\_} \end{vmatrix}$$

равно $w = r/k$. Из результатов [1] следует существование таких базы $b=(\beta_1,\ldots, \beta_r)$ и элемента $a\in GF(2^r)$, что $bM= ab$. Остановимся на способе вычисления b и a . Распишем матричное равенство $bM= (a\beta_1,\ldots, a\beta_r)$ в виде системы равенств элементов поля

$$\left.\begin{array}{l} \alpha\beta_1=\beta_2,\alpha\beta_2=\beta_3,\ldots,\alpha\beta_{k-1}=\beta_k,\alpha\beta_k=\sum\limits_{i=1}^{k}\beta_i d_{i-1}, \\ \alpha\beta_{k+1}=\beta_{k+2},\alpha\beta_{k+2}=\beta_{k+3},\ldots,\alpha\beta_{2k-1}=\beta_{2k},\alpha\beta_{2k}=\sum\limits_{i=k+1}^{2k}\beta_i d_{i-k-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha\beta_{r-k+1}=\beta_{r-k+2},\alpha\beta_{r-k+2}=\beta_{r-k+3},\ldots,\alpha\beta_{r-1}=\beta_r,\alpha\beta_r=\sum\limits_{i=r-k+1}^{r}\beta_i d_{i-r+k-1}. \end{array}\right\} \quad (2)$$

Из (2) следует, что $\alpha^k=\sum\limits_{i=0}^{k-1}\alpha^i d_i$, т. е. α - корень полинома $d(x)$. Кроме того,

$$\left.\begin{aligned}
&\alpha\beta_1=\beta_2,\alpha^2\beta_1=\beta_3,\ldots,\alpha^{k-1}\beta_1=\beta_k,\\
&\alpha\beta_{k+1}=\beta_{k+2},\alpha^2\beta_{k+1}=\beta_{k+3},\ldots,\alpha^{k-1}\beta_{k+1}=\beta_{2k},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\alpha\beta_{r-k+1}=\beta_{r-k+2},\alpha^2\beta_{r-k+1}=\beta_{r-k+3},\ldots,\alpha^{k-1}\beta_{r-k+1}=\beta_r.
\end{aligned}\right\} \qquad (3)$$

Поскольку полином *d(x)* имеет *к* различных корней, то в случае, когда $\kappa > 1$, существует несколько элементов поля, реализующих матрицуМи, стало быть, матрицу^.

Положим $\gamma_1 = \beta\backslash, Y_2$ - *ßk+\>--->Yw* = *Pr-k+\-* Тогда из (3) следует, что база *b,* в которой а реализует матрицу М, может быть представлена в виде

$$b = (r\backslash, a Y_X, \ldots, a^{k\sim x} y_x, y2, a Y2, \sim, a^{k\sim X} Y2, \ldots, r_w, a r_w, \ldots, a^{k\sim l} y_w). \qquad (4)$$

Поскольку *d(x)* - прост и *а* - корень *d(x),* то *d(x)* - минимальный полином степени *к* элемента а . Поэтому 1, а, a^2,..., $a^{\kappa'}$ '- линейно независимые элементы и согласно доказательству теоремы 1.84 [4] всегда можно найти такие элементы $\gamma\backslash,\ldots,y_w$, которые совместно со степенями *а* определят базу (4). Элементы $Y\backslash,\cdots,\gamma_v$ определяются не единственным способом. Поэтому для выбранного элемента *а* существует несколько баз, в которых ареализует *М.*

Рассмотрим случай, когда *w*=1, т. е. степень *d(x)* равна *r.* В этом случае матрица *Md(x)* задает СА типа MISR, регистр сдвига которого описывается полиномом *d(x).* Пусть *а* - корень *d(x),* тогда 1, *а,* o^2,..., $a'\sim^x$ - база $GF(2^r)$ и элемент *а* реализует М^ в любой базе вида *b=(y, αγ , o?γ, ... a ' ' ' γ),* где *γ* - произвольный ненулевой элемент поля *GF(2').* Заметим, что число различных элементов, реализующих матрицу *Md(x>,* равно *r* (всевозможные корни *d(x)).*

Пусть матрица M_p^, где$p(x)=x^r+p_{r-1}x^{r-1}+\ldots+p_1x+p_0$, реализуется некоторым элементом $x\in GF(2')$ в базе $b=(\beta_1,\ldots,\beta_r)$. Принимая во внимание (3), получаем, что

$b=(\beta i,a\beta\backslash,\ldots,a^{r\sim x}\beta i)$ и $a^z = \sum_{i=0}^{r-1} a'p_i$. Поэтому *а* - корень полинома$p(x)$ и $b' =(l, a, a^2,\ldots, a^{z\sim'})$ - база $GF(2^r)$. Значит, *а* не может быть корнем никакого полинома меньшей степени. Следовательно,^&} - минимальный полином элемента *а* и, стало быть, прост.

Обратно, пусть $a\in GF(2^r)$ такой элемент, что $b=(\beta, a, o^2,\ldots, a^{r\sim l}J$ - база $GF(2^r)$. Покажем существование такого простого полинома$p(x)$ степени *r*, что $bM_{p(x)}\sim ab$, т. е. *а* реализует M_p^ в базе *b.* Так как *b* - база, то существуют такие $p_0, p\backslash,\ldots, p_{r-1}\in\{0,1\}$,что $a^r = \sum_{i=0}^{r-1} a' p_j$ и,значит,а-кореньполинома$x^r+p_{r-1}x^{r-1}+\ldots+p\backslash x+p_0$, который прост в силу того, что *b* - база. Непосредственным вычислением убеждаемся в справедливости равенства $b\ M_p^{\wedge} = ab$.

Итак, доказана следующая теорема.

Теорема 4. *Если матрица вида M_p^, где p(x) - полином степени r, реализуема элементомаеСР(2^z),тор(х)-минимальныйполиномэлементаииЬ = (l, а, a^2,..., $a^{r\sim'}$)-баЗаGF(2^r). Обратно, еспиаеGF(2^r)таКОЧЗ.пеМеит. чтоЪ= (\, а, o^2,..., $a^{z\sim}$)*

- база ***GF(2^r), то а реализует в базе b матрицу M_p^, где p(x) - минимальный полином элемента а.***

Следствие. ***Матрица M_p^, где p(x) - полином степени r, реализуема элементом ае GF(/) тогда и только тогда, когдар(х) - минимальный полином элемента а.***

Литература

1. Барашко А. С. О возможности представления многоканальных сигнатурных анализаторов линейными полиномами над конечными полями // Кибернетика и системный анализ. - 1997. - № 5. - С. 142 -151.
2. Pradhan D. K., Gupta S. K., Karpovsky M. G. Aliasing probability for multiple input signature analyzer // IEEE Trans. Comput.- 1990.-C - 39,№4.-P. 586 - 591.
3. Гилл А. Линейные последовательностные машины. М.: Наука, 1971. - 287 с.
4. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. - Т.1,2. - 820 с.