КОД БЕЗОПАСНОСТИ

SECURITY CODE

Matrix-graph approach for studying nonlinearity of transformations on vector spaces

Vladimir M. Fomichev,
Professor, Dr. Sci. (Phys.-Math.),
Scientific Advisor at "Security Code" LLC

Semigroups of ternary matrices

Let $G=\{0,1,2\}$ be a commutative semigroup, where $\tau 0=0$ for any $\tau \in G$, $\tau\sigma=\max\{\tau,\sigma\}$ for any $\tau,\sigma\neq 0$.

- An $n\times n$ matrix over G is called a **ternary matrix**.
- Denote by $\mathbf{(2)_n}$ the $n\times n$ matrix, each element of which equals 2.
- Define the **multiplication** of $n\times n$ ternary matrices $A=(a_{i,j})$ and $B=(b_{i,j})$:

$$AB=C=(c_{i,j}), \text{ where } c_{i,j}=\max\{a_{i,1}b_{1,j},\ldots,a_{i,n}b_{n,j}\}.$$

Matrix-graph approach for studying nonlinearity

Let f: $P^n \to P^n$ be a transformation represented by the coordinate polynomials $f=\{f_0(x_0,\dots,x_{n-1}),\dots,f_{n-1}(x_0,\dots,x_{n-1})\}$, where $n>1$ and P is a finite field.

- We consider the $n\times n$ ternary **matrix of nonlinearity** (denoted by $M_\Theta(f)$). For $0\le i,j<n$, the element $m_{i,j}$ in $M_\Theta(f)$ is equal to **0, 1 or 2**, if the function $f_j(x_0,\dots,x_{n-1})$ **fictitiously, linearly or nonlinearly** depends on the variable x_i, respectively. If $M_\Theta(f)=(2)_n$, then the transformation f is called **quite nonlinear**.
- Also, we consider the **digraph of nonlinearity** (denoted by $\Gamma_\Theta(f)$). For $0\le i,j<n$, $\Gamma_\Theta(f)$ is defined as the labelled n-vertex directed graph, whose arc (i,j) is labelled with $m_{i,j}$.

The basic theorem

Theorem 1. For any transformations $f^{(1)},\dots,f^{(t)}$ on P^n, $t\geq 1$, the following inequality is true:

$$M_\Theta(f^{(1)}\dots f^{(t)}) \leq M_\Theta(f^{(1)})\dots M_\Theta(f^{(t)})).$$

By Theorem 1 we can evaluate the elements of the matrix

$$M_\Theta(f^{(1)}\dots f^{(t)}).$$

⟨2⟩-primitivity of ternary matrices

- The matrix M (ternary matrix M) is called ***primitive*** (***⟨2⟩-primitive***), if $\exists\, t\in\mathbb{N} : M^t>0$ ($M^t=(2)_n$). The smallest t with this property we call ***exponent*** (***⟨2⟩-exponent***) of M, denoted by $\exp M$ ($\langle 2\rangle\exp M$)).
- For the matrices A,B it follows from $A\le B$ that $A^t\le B^t$, $t\in\mathbb{N}$.
  So, if A is ⟨2⟩-primitive, than B is ⟨2⟩-primitive too, and $\langle 2\rangle\exp A\ge\langle 2\rangle\exp B$.

Example 1. Let us calculate ⟨2⟩-exponent for the ternary matrix M:

$$M=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&2&0&0\end{pmatrix};\ M^2=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&2&0&0\\0&1&2&0\end{pmatrix};\ M^4=\begin{pmatrix}1&2&0&0\\0&1&2&0\\0&0&1&2\\2&2&0&1\end{pmatrix};\ \ldots\ M^{12}=\begin{pmatrix}1&2&2&2\\2&2&2&2\\2&2&2&2\\2&2&2&2\end{pmatrix};\ M^{13}=(2)_4.$$

Hence, $\langle 2\rangle\exp M=13$.

⟨2⟩-primitivity of labelled digraphs

- The labelled digraph Γ is called ***complete* ⟨2⟩-*digraph*** (denoted by $\Gamma_n^{\langle 2\rangle}$), if the matrix of labels $M(\Gamma)=(2)_n$. The **label of the path** in Γ is the largest of the labels of arcs that form this path.
- The labelled digraph Γ is called ***⟨2⟩-primitive***, if $\exists\ t\in\mathbb{N}:\ \Gamma^t=\Gamma_n^{\langle 2\rangle}$. The smallest t we call **⟨2⟩-exponent** of Γ (denoted by $\langle 2\rangle\exp\Gamma$). The value of $\langle 2\rangle\exp\Gamma$ equals the smallest $t\in\mathbb{N}$, such that for any pair (i,j) of vertices in Γ there is the path with the label "2" from i to j of length t.

The digraph Γ is ⟨2⟩-primitive ⇔ the matrix $M(\Gamma)$ is ⟨2⟩-primitive, so

$$\langle 2\rangle\exp\Gamma=\langle 2\rangle\exp M.$$

The criterion of ⟨2⟩-primitivity

Let Γ contains the arc labelled with “2”.

For $0 \le i < n$, we use the following notation:

- $l_i^{[2]}$ is the length of the shortest path from the vertex *i* to the nearest vertex, which is the start point of the arc with the label “2”;
- $d^{[2]} = \max\{l_0^{[2]}, \ldots, l_{n-1}^{[2]}\}$.

Theorem 2. The labelled digraph Γ is $\langle 2 \rangle$-primitive $\Leftrightarrow$ Γ is primitive and contains the arc with the label “2”. In this case we have

$$\exp\Gamma \le \langle 2 \rangle \exp\Gamma \le 1 + d^{[2]} + \exp\Gamma.$$

Bounds for $\langle 2 \rangle$-exponents of digraphs

1. **The universal bound**.

If the labelled digraph Γ is $\langle 2 \rangle$-primitive, then

$$\langle 2 \rangle \exp\Gamma \leq n^2-n+1.$$

2. If the $\langle 2 \rangle$-primitive digraph Γ contains the circuit of length $l>1$, then

$$\langle 2 \rangle \exp\Gamma \leq d^{[2]}+1+n+l(n-2).$$

3. If the circuit C of length l passes through the arc with label “2”, then

$$\langle 2 \rangle \exp\Gamma \leq n+l(n-1).$$

Bounds for $\langle 2 \rangle$-exponents of digraphs with loops

1. If $\langle 2 \rangle$-primitive digraph Γ has $p>0$ loops, then

$$\langle 2 \rangle \exp \Gamma \leq d^{[2]}+2n-p.$$

2. If $\langle 2 \rangle$-primitive digraph Γ has m loops with the label "2", $0<m \leq p$, then

$$\langle 2 \rangle \exp \Gamma \leq 2n-m.$$

Applications

Let g be a round transformation of block encryption algorithm.

Synthesis. The **$\langle 2 \rangle$-exponent** of ternary matrix of g may be considered as **the lower bound** for the number of encryption rounds. This value is a more accurate than the exponent of mixing matrix of g.

We apply this approach for evaluating the $\langle 2 \rangle$-exponents of ternary matrices, which correspond to the round transformations g and h of block ciphers DES and Magma, respectively (M.D. Sapegina, Diploma thesis at MEPhI, 2019).

The following values are obtained:

$$\langle 2 \rangle \exp M(g) = \exp M(g) = 5;$$

$$\langle 2 \rangle \exp M(h) = \exp M(h) = 6.$$

Thank you for your attention

Questions?