Primitivity and Local Primitivity of Digraphs and Matrices

Authors: V.M. Fomichev, Y.E. Avezova,
A.M. Koreneva, S.N. Kyazhin

Introduction

A relevant direction in cryptology is a construction of vector space functions where each bit of output depends on all input bits.

A **matrix-graph approach** (further **MGA**) is used for solving the determination problem of a set of essential variables for a transformations' composition.

Let g be a transformation over V_n with a set of Boolean functions $\{g_1(x_1,\ldots,x_n),\ldots,g_n(x_1,\ldots,x_n)\}$. $\Gamma(g)$ denotes a **mixing digraph** of transformation g with vertex set $\{1,\ldots,n\}$.

A pair (i,j) is an arc in $\Gamma(g)$ $\Leftrightarrow$ x_i is an essential variable of g_j, $i,j\in\{1,\ldots,n\}$.

An adjacency matrix $M(g)$ associated with $\Gamma(g)$ is a **mixing matrix**.

Let $\Gamma(g)=\Gamma$ and $M(g)=M$.

Universal bounds

The main problem in the MGA context is to determine **conditions of primitivity** for M (for Γ) and estimate the **exponent** ($\exp\Gamma$) – the **smallest natural** t such that $M^t>0$. Let $Y=\{C_1,\ldots,C_m\}$ be a set of cycles of lengths $l_1,\ldots,l_m$ in Γ, $m\geq 1$, $l_1\leq\ldots\leq l_m$. Y is primitive if $\gcd(l_1,\ldots,l_m)=1$.

The criterion of primitivity. A strongly connected digraph Γ is primitive $\Leftrightarrow$ Γ contains a primitive set of cycles.

Universal bounds. [*Wielandt, 1950*]: $\exp\Gamma \leq n^2 - 2n + 2$;

[*Dulmage and Mendelsohn, 1964*]: $\exp\Gamma \leq n + l_1(n - 2)$.

[*Dulmage and Mendelsohn, 1964*]: $\exp\Gamma \leq F(l_1,\ldots,l_m) + r(\Gamma) + 1$,

where $\gcd(l_1,\ldots,l_m)=1$ and $F(l_1,\ldots,l_m)$ is a Frobenius number for arguments $l_1,\ldots,l_m$, $r(\Gamma)=\max\{r_{u,v}\}$, $r_{u,v}$ – the length of the shortest walk from vertex u to vertex v so that it contains a vertex of each cycle of Y.

[*Fomichev V.M., 2016*]: $\exp\Gamma \leq n(m+1) + F(l_1,\ldots,l_m) - l_1 - \ldots - l_m$; if subgraph $C_1\cup\ldots\cup C_m$ is strongly connected, then $\exp\Gamma \leq 2n - l_1 + F(l_1,\ldots,l_m)$.

Special bounds

Let Γ be a primitive digraph with a loop. It follows that $\exp\Gamma \le 2n-2$.

This estimate is improved in [*Fomichev V. M., 2010*]: $\exp\Gamma \le \max\limits_{i,j\in\{1,\ldots,n\}} \min\limits_{p\in\Pi} d_{i,p,j}$,

where $d_{i,p,j}$ – a length of the shortest walk from i to j in Γ going through vertex p, $i,j,p\in\{1,\ldots,n\}$, Π – a set of vertices with loops.

Let Γ contain the cycles C and C' of length l and λ with h common vertices, $(l,\lambda)=1$, $l>\lambda$. Then [*Fomichev V. M., 2011*]: $\exp\Gamma \le l\lambda - l - 3\lambda + h + 2n$.

Other special bounds:

- for digraphs with certain additional arcs and 3 cycles of lengths l, λ, μ, where $(l,\lambda,\mu)=1$ [*Fomichev V. M., 2014*];
- for tournaments [*Sachkov V.N., Tarakanov V.E., 2000*];
- for pseudosymmetric and dichotomic digraphs with limited in-degrees and out-degrees of vertices and limited digraph girth [*Knyazev A.V., 2002*];
- ...

Results for shift registers

Let $n,r,k \in N$, $k<n$. $R(n,r,k)$ denotes a class of k-feedback shift registers of length n over the set V_r ($R(2,r,1)$ – classic Feistel ciphers). Let $\Gamma(g)$ be an nr-vertex mixing digraph for $g \in R(n,r,k)$; $\Gamma_B(g)$ – n-vertex mixing digraph of blocks from V_r, i.e. (i,j) is an arc in $\Gamma_B(g) \Leftrightarrow$ some bits in j-th output block depend on some bits of i-th input block, $i,j \in \{1,\ldots,n\}$.

Results for shift registers.

[T. Suzaki, K. Minematsu, 2010]: for $g \in R(n,r,n/2)$, n is even, $\exp\Gamma_B(g) \le n$ and $\exp\Gamma_B(g) \le 2\log_2 n$ in case of the replacement of cyclic block shift by some permutation.

[*T.P. Berger, M. Minier, G. Thomas, 2013*]: for $g \in R(n,r,1)$, $\exp\Gamma_B(\varphi) \le (n-1)^2+1$ and $\exp\Gamma_B(\varphi) \le n(n+2)/2-2$ in case of the replacement of cyclic block shift by some permutation; for $g \in R(n,r,n-1)$ $\exp\Gamma_B(g) \le n$.

[*Fomichev V. M, Koreneva A. M., 2014*]: for $g \in R(n,r,1)$, $\exp\Gamma(g) \approx 2nr$ for certain feedback functions;

[*Fomichev V. M, Koreneva A. M., 2016*]: for $g \in R(n,r,1)$, based on modified additive generators $\exp\Gamma(g)=n-1$ for certain parameters; [*Koreneva A. M., 2017*]: for $g \in R(n,r,2)$ based on modified additive generators $\exp\Gamma(g)=\lceil n/2 \rceil+1$ for certain parameters.

Local primitivity of matrices and graphs

Let $I,J\subseteq\{1,\ldots,n\}$, $|I|=k>0$, $|J|=r>0$. Let $M(I\times J)$ be a $k\times r$ matrix obtained from M by removing the lines with numbers $i\notin I$ and columns with numbers $j\notin J$.

The matrix M is called $I\times J$-primitive (**local primitive**), if $M^t(I\times J)>0$ for all $t\geq\gamma$, where $\gamma\in N$. The smallest γ is denoted by $I\times J$-exp$M$ (also $\gamma_{I,J}$) and called $I\times J$-exponent (**local exponent**) of matrix M.

Let $P(i,j)$ be a set of all simple paths in a digraph Γ from i to j. The **Path Index** $w\in P(i,j)$ is the gcd of all simple cycles lengths inside a **SCC (Strong Connectivity Component),** so that w goes through some vertices in the SCC. The class of paths with index d is denoted by $P^{(d)}(i,j)$, taken from $P(i,j)$. Then, the following partition holds:

$$P(i,j)=P^{(d_1)}(i,j)\cup\ldots\cup P^{(d_k)}(i,j).$$

$\mathrm{spc}_d W=\{\mathrm{len}w\ (\mathrm{mod}\, d):\ w\in W\}$; $\overline{\mathrm{spc}}_d W=\{0,\ldots,d-1\}\backslash\mathrm{spc}_d W$; len$w$ is the length of path w;

$$H(P(i,j)) = \overline{\mathrm{spc}}_{d_1}\ P^{(d_1)}(i,j)\times\ldots\times\overline{\mathrm{spc}}_{d_k}\ P^{(d_k)}(i,j).$$

Local primitivity universal criterion: Let $\delta=\mathrm{lcm}\{d_1,\ldots,d_k\}$. Digraph Γ is $i\times j$-primitive $\Leftrightarrow$ system $\{x\equiv b_\theta \bmod d_\theta,\ \theta=1,\ldots,k\}$ has no solutions modulo δ for any $(b_1,\ldots,b_k)\in H(P(i,j))$.
If each path in $P^{(d)}(i,j)$ goes through some vertices in the SCC
with cycles of lengths $l_1,\ldots,l_m$, $\gcd(l_1,\ldots,l_m)=d$, then

$$\gamma_{i,j}\leq O(\max\{mn,\ dg(l_1/d,\ldots,l_m/d)\})\ \text{as}\ n\to\infty.$$

This results are improved in [*Fomichev V. M., Kyazhin S. N., 2017*] for different cases.

On primitivity of sets of nonnegative matrices (1)

Let $\mathcal{M}=\{M_1,\ldots,M_p\}$ be a set of 0,1-matrices and $\langle\mathcal{M}\rangle$ be a multiplicative semigroup generated by words over alphabet $\mathcal{M}$. **The word** $(M_{w_1},\ldots,M_{w_s})\in\langle\mathcal{M}\rangle$ (where $w=w_1\ldots w_s$ is a word over alphabet $\{1,\ldots,p\}$) **is called positive** (primitive) if the matrix $M(w)=M_{w_1}\ldots M_{w_s}$ is positive (primitive).

The set $\mathcal{M}$ **is** said to be **primitive** if the semigroup $\langle\mathcal{M}\rangle$ contains a positive word; the length of the shortest positive word over alphabet $\mathcal{M}$ is called an exponent of the set $\mathcal{M}$ (denoted by $\exp\mathcal{M}$).

Statement [*Fomichev V.M., Avezova Y.E., 2010*]**.** If the set $\mathcal{M}$ is primitive and $M(w)=M_{w_1}\ldots M_{w_s}$ is primitive, then $\exp\mathcal{M}\le s\cdot\exp M(w)$. Furthermore the matrix $M=M_1+\ldots+M_p$ is primitive as well and:

$$\exp M\le\exp\mathcal{M}\le\min\{\exp M_1,\ldots,\exp M_p\}.$$

On primitivity of sets of nonnegative matrices (2)

The set $\mathcal{M}$ corresponds to the set of digraphs $\widehat{\Gamma}=\{\Gamma_1,\ldots,\Gamma_p\}$; multigraph $\Gamma^{(p)}=\Gamma_1\cup\ldots\cup\Gamma_p$ in which the arc of digraph Γ_r is assigned the label r, $r=1,\ldots,p$. The walk is assigned the label w^t if it is a concatenation of t walks labeled w, the walk labeled w^0 is empty. Define w-strongly connected multigraph $\Gamma^{(p)}$ as strongly connected multigraph $\Gamma^{(p)}$ in which for all $i,j\in\{1,\ldots,n\}$ a walk labeled $w^{t_{ij}}$ exists from i to j for some $t_{ij}\in N$.

Criterion of primitivity for the digraph $\Gamma_{w_1}\ldots\Gamma_{w_s}$ [*Avezova Y.E., 2017*]. The digraph $\Gamma(w)=\Gamma_{w_1}\ldots\Gamma_{w_s}$, where $w=w_1\ldots w_s$, is primitive $\Leftrightarrow$ $\Gamma^{(p)}$ is w-strongly connected and has cycles labeled $w^{t_1},\ldots,w^{t_m}$, where $\gcd(t_1,\ldots,t_m)=1$.

The problem of recognizing primitivity for n-vertex digraphs is algorithmically decidable.

Example (*sufficient condition for one set of digraphs to be primitive*): let $\widehat{\Gamma}=\{\Gamma_0,\ldots,\Gamma_{n-1}\}$ be the set of digraphs, where Γ_i is Wielandt digraph with vertex set $\{0,\ldots,n-1\}$ and arc $(i,(i+2)\bmod n)$, $i=0,\ldots,n-1$, then $\exp\widehat{\Gamma}\le 2n-2$.

Further research directions

- Local primitivity and local exponent for special classes of matrices and digraphs (ex., shift registers of length n over V_r with several feedbacks)

- Design of cryptographic transformations with given limitations on the exponent or local exponent of a mixing digraph

Thank you!