An Approach to Studying Periods of Binary Digit-position Sequences over Prime Rings

Kuzmin S.A.

TVP Laboratories

CTCrypt'17

VI Workshop on Current Trends in Cryptology

Closest aspects

- level sequences and k-linear recurring sequences (Bylkov D.V., Kamlovskiy O.V., Kurakin V.L., Kuzmin A.S., Kozlitin O.A., Nechaev A.A.)
- modular reductions of linear recurring sequences over $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_{pq}$ where p and q are different prime numbers (Xuan-Yong Zhu, Wen-Feng Qi)
- digit-position sequences over fields and rings (Kuzmin A.S., Kuzmin S.A.)

Introduction

Let $\mathbb{Z}_{p^n}$, be a primary ring with the generator polynomial $F(x)$, $\deg F(x) = m$, notably $u(i) = (u(i))_{i=0}^{\infty}$ is LRS MP over this ring. Period $T(u)$ of LRS MP u equals $p^{n-1}(p^m - 1)$.
Every element $u(i)$ of some LRS MP u over prime ring can be uniquely represented as follows

$$u(i) = \sum_{t=0}^{k} u_t(i) 2^t,$$

where $k = [\log_2 p^n]$.
Sequence $u_t, t = \overline{1, k}$ is called t^{th} binary digit-position sequence.
The following property holds $T(u_t) | T(u)$.

Approach

Multiplier of sequence u is an element $c \in \mathbb{Z}_{p^n}^*$, for which exists $q \in \mathbb{N}$ with property $x^q u = cu$.

Let $c \in \mathbb{Z}_{p^n}$ be a multiplier of sequence u over $\mathbb{Z}_{p^n}$. Let $M(u)$ be a set of all of multipliers of u. $M(u)$ forms subgroup in $\mathbb{Z}_{p^n}^*$.

Let $H = \{1, \beta, \beta^2, \ldots, \beta^{2d-1}\}$ be a subgroup of $M(u)$, here β is a forming element of group H, value $2d$ satisfies condition

$$2d | GCD(T(u), |\mathbb{Z}_{p^n}^*|) = p^{n-1}(p-1).$$

The set of $\mathbb{Z}_{p^n} \setminus \{0\}$ can be represented as a decomposition of non-intersecting classes $g_j H$ for some $g_j \in \mathbb{Z}_{p^n} \setminus \{0\}$

Result

Theorem

Let $\boldsymbol{u}$ be an LRS MP over $\mathbb{Z}_{p^n}$ with generator polynomial $F(x)$, $degF(x) = m$, all the elements of $\mathbb{Z}_{p^n}$ occure in the cycle of $\boldsymbol{u}$, $\boldsymbol{u}_s$ be the s^{th} digit-position sequence of $\boldsymbol{u}$, where s satisfies conditions $p^n = a(s)2^{s+1} + 2^s - 1$, for some $a(s) \geq 0$, $s \geq 1$. Let $H < M(u)$, $|H| = 2d$, $p \geq 3$. Then the following expression holds

$$T(u_s) \nmid \frac{T(u)}{2d}.$$

Thank you for attention.