Skew LRS of maximal period over Galois rings

Mikhail Goltvanitca, Alexandr Nechaev and Sergey Zaitcev

Let $R = GR(q^d, p^d)$ be a Galois ring of $q^d = p^{rd}$ elements and of characteristic p^d, $S = GR(q^{nd}, p^d)$ be extension of the ring R of the dimension n and $\check{S}$ be the ring of all linear transformations of the module ${}_RS$. We call a linear recurring sequence v over S with the law of recursion

$$\forall i \in \mathbb{N}_0 : \quad v(i+m) = \psi_{m-1}(v(i+m-1)) + ... + \psi_0(v(i)), \quad \psi_0, ..., \psi_{m-1} \in \check{S}$$

a *skew LRS over* S. It is known that the period $T(v)$ of such a sequence satisfies the inequality $T(v) \leq \tau = (q^{nm} - 1)p^{d-1}$. If $T(v) = \tau$ we call v a *skew LRS of maximal period* (*skew MP LRS*) *over* S.

Earlier such a sequences was studied by V. N. Tsypyschev, B. Tsaban, U. Vishne, G. Zeng, W. Han, K.C. He, S.R. Ghorpade, S.U. Hasan, M. Kumari, S. Ram, only for the case $R = \mathrm{GF}(q)$ as LRS of vectors $v^{\downarrow}(i) \in R^{(n)}$ with matrix recursion low: $v^{\downarrow}(i+m) = A_{m-1}v^{\downarrow}(i+m-1) + ... + A_0 v^{\downarrow}(i)$, where $A_0, ..., A_{m-1} \in R_{n,n}$ are fixed $n \times n$-matrices over R. Note that in works of the listed authors skew MP LRS where found mainly for some fixed parameters m, n only by brute force method.

Here a new general characterization of skew MP LRS in terms of coordinate sequences corresponding to some basis of a free module ${}_RS$ is given. For the first time simple constructive methods of creation of big enough classes of skew MP LRS for any values m and n are offered. Among these sequences are found such, at which linear complexity em (rank of linear recurring sequence) over the module ${}_SS$ is equal to mn, i.e. to the linear complexity over the module ${}_RS$.

Keywords: Galois Ring, Frobenius automorphism, Linear recurrence of maximal period, Linear complexity, Rank of a sequence.