



Problem 9. «Vector LRS»

Problem for a special prize!

Definitions. Let $R = GF(2)$, $n \in \mathbb{N}$. We call subsequence of columns $v : \mathbb{N}_0 \rightarrow R^{(n)}$ *vector linear recurrent sequence* (LRS) of order m , if there exist matrices $A_0, \dots, A_{m-1} \in R_{n,n}$, such that for all $i \in \mathbb{N}_0$ it holds

$$v(i+m) = A_{m-1}v(i+m-1) + \dots + A_1v(i+1) + A_0v(i). \quad (1)$$

If there exists $T \in \mathbb{N}$, such that $v(i+T) = v(i)$ for all $i \in \mathbb{N}_0$, then the least such T is called *the period* of the sequence v and is denoted as $T(v)$. Considering the set of m -element items $\{(v(0), \dots, v(m-1)), (v(1), \dots, v(m)), \dots\}$, it is not difficult to show that the period of a vector LRS of order m does not exceed $\tau = 2^{mn} - 1$. In the case when $T(v) = \tau$, we will call the vector LRS v of order m a *vector LRS of maximum period*.

An example. Let $n = 2$, $m = 3$,

$$A_2 = A_1 = A_0 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

and initial columns are $v(0) = v(1) = (0, 0)^T$, $v(2) = (1, 0)^T$. Then it holds $v(3) = (0, 1)^T$, $v(4) = (1, 0)^T$, $v(5) = (1, 1)^T, \dots$. It is not difficult to check that v is a vector linear recurrent sequence of the maximum period $2^6 - 1 = 63$.

The problem. Let v be such a vector LRS of maximum period $\tau = 2^{mn} - 1$ of order m with the recursion law (1), such that for all $d \in \mathbb{N}$ coprime to τ , the sequence $w(i) = v(di)$ is also a vector LRS of maximum period of order m . Is it true that $A_k A_j = A_j A_k$ for all $k, j \in \{0, \dots, m-1\}$?