Problem 6. «Sylvester matrices»

Special Prize from the Program Committee!

Sylvester matrices play a role in security since they are connected with topics like secret sharing and MDS codes constructed with cellular automata.

Consider two univariate polynomials over the 2-element field, $P_1(x)$ of degree m and $P_2(x)$ of degree n where $P_1(x) = a_m x^m + \ldots + a_0$ and $P_2(x) = b_n x^n + \ldots + b_0$. The *Sylvester matrix* is an $(m+n) \times (m+n)$ matrix formed by filling the matrix beginning with the upper left corner with the coefficients of $P_1(x)$, then shifting down one row and one column to the right and filling in the coefficients starting there until they hit the right side. The process is then repeated for the coefficients of $P_2(x)$. All the other positions are filled with zero.

Let $n > 0,\ m > 0$. Prove whether there exist $(m+n) \times (m+n)$ invertible Sylvester matrices whose inverse are Sylvester matrices as well.

Example. For $m = 4$ and $n = 3$, the Sylvester matrix is the following:

$$\begin{pmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \end{pmatrix}$$