**Lista 3, zadanie 7.** W AES S-boks oblicza wartość bajtu $b$ w ten sposób, że

- Jeśli $b \neq 0$, to $c = b^{-1}$ w ciele $F_{2^8}$, które jest ciałem wielomianów nad $\mathbb{Z}_2$ z działaniami modulo nierozkładalny wielomian ósmego stopnia. Jeśli $b = 0$, to $c = 0$.
- Niech $c = c_0c_1c_2c_3c_4c_5c_6c_7$. Wtedy $d_i = c_i \oplus c_{i+4} \oplus c_{i+5} \oplus c_{i+6} \oplus c_{i+7}$, gdzie indeksy dodawane są modulo 8.
- Wynikiem działania S-boksa jest $e = d \oplus 01100011$.

Jak wygląda przekształcenie odwrotne do tego S-boksa?

**Rozwiązanie.** Na początku odwrócimy dwa ostatnie kroki. Można je przestawić następująco jako operacje na macierzach modulo 2:

$$e = Ac + t,$$

gdzie $c = \begin{bmatrix} c_0 & c_1 & \cdots & c_7 \end{bmatrix}^T$, $t = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}^T$ oraz

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Odwracamy to przekształcenie:

$$\begin{aligned} e &= Ac + t \\ Ac &= e + t \\ c &= A^{-1}(e + t) \\ c &= A^{-1}e + A^{-1}t. \end{aligned}$$

Po odwróceniu macierzy $A$ modulo 2 otrzymujemy:

$$A^{-1} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix},$$

natomiast $A^{-1}t = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T$. Możemy to zapisać jako:

$$c_i = e_{i+2} \oplus e_{i+5} \oplus e_{i+7} \oplus 00000101.$$

Następnie musimy odwrócić pierwszy krok S-boksa, co nic w tym przypadku nie zmienia – szukamy odwrotności $c$ w $F_{2^8}$, jeśli $c \neq 0$, to $b = c^{-1}$, natomiast jeśli $c = 0$, to $b = 0$.