

Kody korekcyjne: Lista 5

31 października 2019

Zadanie 1. Pokaż, że w ciele \mathbb{F}_q dla $\beta \in \mathbb{F}_q^*$ zachodzi:

$$\frac{x^{q-1} - 1}{x - \beta} = \sum_{i=0}^{q-2} \beta^i x^{q-2-i} .$$

Zadanie 2. Pokaż, że znając error locator polynomial oraz syndrom $[s_0, \dots, s_{n-k-1}]^T$ można obliczyć wielomian $\varphi^{\vec{e}} = E^{\vec{e}} s^{\vec{e}} / (x^n - 1)$.

Wskaźnik: Policz stopnie wielomianów. Pokaż, wielomiany $\varphi^{\vec{e}}$ oraz $x^n - 1$ nie mierzonych współczynników przy jednej potędze. Jeden z nich da się wyliczyć z z $E^{\vec{e}} s^{\vec{e}}$.

Zadanie 3. Zróżniczkuj obustronnie równanie

$$E^{\vec{e}} s^{\vec{e}} = \varphi^{\vec{e}}(x^n - 1)$$

i oblicz wartość obu stron w γ^j , gdzie $e_j \neq 0$. Wyprowadź z tego zależność

$$e_j = \frac{\varphi^{\vec{e}}(\gamma^j)}{(E^{\vec{e}})'(\gamma^j)} .$$

Zadanie 4 (2 punkty). Rozszerz algorytm Berlekamp-Massey tak aby obliczał on też wielomian ewaluujący $\varphi^{\vec{e}}$.

Wskaźnik: Samemu może być ciężko. <https://mosullivan.sdsu.edu/Teaching/Coding04/RScodes.pdf>, strony 19-21.

Zadanie 5. Pokaż, że znając error locator polynomial $E^{\vec{e}}$ dla wektora błędów \vec{e} oraz mając dostęp do syndromu $[s_0, \dots, s_{n-k-1}]^T$ można bezpośrednio obliczyć wartości s_{n-k}, \dots, s_{n-1} (i tym samym wielomian syndromu $s^{\vec{e}}$).

Wskaźnik: Error locator polynomial daje zależność rekurencyjną na kolejne syndromy, wykorzystujemy to wprost w algorytmie Peterson-Gorenstein-Zierler.

Zadanie 6. Pokaż poprawność algorytmu Peterson-Gorenstein-Zierler, tj. dla wektora błędów \vec{e} o wadze $t = \|\vec{e}\|_1 \leq \frac{n-k}{2}$ pokaż, że

- dla $m > t$ macierz syndromów S , gdzie $(S)_{ij} = s_{i+j-2}$, nie jest odwracalna;
- dla $m = t$ macierz syndromów jest odwracalna.

Zadanie 7. Pokaż, jak zaimplementować algorytm Peterson-Gorenstein-Zierler w czasie $\mathcal{O}(n^3)$.