Kody korekcyjne: Lista 7

10 grudnia 2023

Zadanie 1. Pokaż, że wymiar kodu q-arnego kodu BCH o długości $q^m - 1$ generowanego przez $g(X) = \mathrm{nww}(M^{(a)}(X), M^{(a+1)}(X), \ldots, M^{(a+\delta-2)}(X))$ jest niezależny od wybór elementu pierwotnego α.

Zadanie 2. Udowodnij, że odległość binarnego ścisłego kodu BCH (czyli dla $a = 1$) jest zawsze nieparzysta.

Jedna z możliwych dróg: traktujemy $\vec{c}$ jako indeksy niezerowych elementów z ciała $\mathbb{F}_{n+1}$ i myślimy o nim jako podzbiorze $C \subseteq \mathbb{F}_{n+1}^*$.

Korzystając z pseudo-macierzy parzystości, jeśli C należy do kodu, to dla $1 \leq j \leq \delta - 2$ zachodzi

$$\sum a \in C a^j = 0$$

Co umiesz powiedzieć więcej, jeśli C ma parzystą wagę (parzystą liczbę elementów)?

Rozważ zbiór

$$C + a = \{c + a \,:\, c \in C\}$$

Udowodnij, że on też spełnia powyższy warunek.

Wybierz odpowiednio element a, tak żeby C zawierał 0.

Zadanie 3. Udowodnij, że ścisły binarny kod BCH (czyli dla $a = 1$) o długości $n = 2^m - 1$ i projektowanej odległości $2t + 1$ ma odległość $2t + 1$, jeśli

$$\sum_{i=0}^{t+1} \binom{2^m - 1}{i} > 2^{mt} \quad .$$

Wskazówka: Liczby po prawej i lewej stronie mają dobrze zdefiniowany sens. Skorzystaj też z Zadania 2.

Zadanie 4. Niech C będzie kodem RS (w sensie BCH) generowanym przez wielomian $g = \prod_{i=1}^{\delta-1}(X - \alpha^i)$. Rozważmy kod rozszerzony $\overline{C}$, czyli powstały przez dodanie cyfry kontrolnej do słów kodowych (patrz lista 2). Pokaż, że $\overline{C}$ również jest kodem MDS, tzn. dla $\overline{C}$ zachodzi $n - k + 1 = d$.

Wskazówka: Dla słowa kodowego $c = fg$ rozważ $c(1) = f(1)g(1)$; osobno rozważ przypadki $c(1) \neq 0$ i $c(1) = 0$. W drugim przypadku rozważ kod generowany przez $(X - 1)g$, który też jest kodem BCH.

Zadanie 5. Używając wielomianów generujących pokaż, że kod dualny do kodu RS (w sensie BCH) też jest kodem RS (w sensie BCH).

Algorytm PGZ: Dane $s_0, \ldots, s_{n-k-1}$. Znajdź największe $m \leq \frac{n-k}{2}$, takie że równanie

$$\begin{bmatrix} s_0 & s_1 & \cdots & s_{m-1} \\ s_1 & s_2 & \cdots & s_m \\ \vdots & \vdots & \ddots & \vdots \\ s_{m-1} & s_m & \cdots & s_{2m-2} \end{bmatrix} \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{m-1} \end{bmatrix} = - \begin{bmatrix} s_m \\ s_{m+1} \\ \vdots \\ s_{2m-1} \end{bmatrix} \tag{PGZ}$$

ma jedno rozwiązanie. Wtedy m: liczba błędów, oraz $E = x^m + \sum_{i=0}^{m-1} \lambda_i x^i$.

Zadanie 6. Pokaż (częściową) 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 $m > t$ układ równań (PGZ) ma więcej niż jedno rozwiązanie oraz dla $m = t$ współczynniki $\lambda_0, \ldots, \lambda_{t-1}1$ prawdziwego error locator polynomial faktycznie są rozwiązaniem (PGZ).

(Brakuje pokazać, że jest to rozwiązanie jedyne, ale to wymaga jeszcze pewnych faktów.)

Wskazówka: Rozważ E oraz XE. Co umiesz powiedzieć o $S_e(E)$ i $S_e(XE)$?

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