Kody korekcyjne: Lista 9

28 listopada 2019

Zadanie 1. Niech $\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ zwraca dla liczby z $\mathbb{F}_{q^m}$ jej zapis q-arny z wiodącymi zerami, tj.

$$\varphi(c) = (c_{m-1}, \ldots, c_0) \quad \text{, gdzie } \sum_{i=0}^{m-1} c_i q^i = c \ .$$

Rozszerzamy φ do $\mathbb{F}_{q^m}^n$ w naturalny sposób, tzn. znak po znaku.

Rozważmy następujący kod C': dla kodu Reeda Solomona $C \leq \mathbb{F}_{q^m}^n$ wymiaru k (czyli wielomiany stopnia $< k$)

$$C' = \varphi(C) \ .$$

Jak długie błędy pęknięć potrafi poprawić kod C'?

Wskazówka: Skoro kod RS jest MDS, to jest też optymalny jako kod poprawiający błędy pęknięć.

Zadanie 2. Wiemy, że kody BCH są kodami liniowymi, bo są generowane przez wielomian. Podaj alternatywny dowód tego faktu, używający pseudo-macierzy parzystości: tzn. dla α — generatora $\mathbb{F}_{q^m}$, $n = q^m - 1$ oraz parametrów a oraz δ pokaż że dla

$$H' = \begin{bmatrix} 1 & \gamma^a & \gamma^{2a} & \ldots & \gamma^{(n-1)a} \\ 1 & \gamma^{a+1} & \gamma^{2(a+1)} & \ldots & \gamma^{(n-1)(a+1)} \\ \vdots & \vdots & \ldots & \vdots & \\ 1 & \gamma^{a+\delta-2} & \gamma^{2(a+\delta-2)} & \ldots & \gamma^{(n-1)(a+\delta-2)} \end{bmatrix}$$

kod BCH, czyli

$$\ker(H') \cap \mathbb{F}_q^n$$

jest kodem liniowym.

Wskazówka: Można na wiele sposobów: jako rzut, zamknięcie na operacje, czy też przez pokazanie, że warunki liniowe w $\mathbb{F}_{q^m}^n$ można przepisać jako warunki liniowe w $\mathbb{F}_q^n$.

Zadanie 3. Używając podejścia jak w poprzednim zadaniu podaj alternatywny dowód tego, że wymiar kodu BCH dla $n = q^m - 1$, a, δ wynosi przynajmniej

$$q^m - 1 - (\delta - 1)m$$

Wskazówka: Tu już trzeba przepisać warunki liniowe w $\mathbb{F}_{q^m}$ na warunki liniowe $\mathbb{F}_q$.

Zadanie 4. Pokaż, że odległość kodu BCH to przynajmniej δ.

Wskazówka: Użyj macierzy H' z Zadania 2. Jak warunek wiążący odległość kodu dla macierzy parzystości ogólnia się na H'?

Zadanie 5. 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 6. Udowodnij, że dla $f \in \mathbb{F}_2[X]$ jeśli α jest pierwiastkiem f, to również α^2 jest pierwiastkiem f. Wywnioskuj z tego, że wielomiany minimalne (dla generatora α ciała $\mathbb{F}_{2^m}$) $M^{(i)}$ oraz $M^{(2i)}$ są równe.

Zadanie 7. Udowodnij, że odległość binarnego ścisłego kodu BCH (czyli dla $a = 1$) jest zawsze nieparzysta.

Wskazówka: Użyj pseudo-macierzy parzystości. Zinterpretuj słowo kodowe $(c_1, \ldots, c_n)$ jako kombinację liniową $\sum_i c_i \beta_i$ dla pewnych elementów $\{\beta_1, \ldots, \beta_n\} = \mathbb{F}_{n+1}^*$. Rozważ sumę $\sum_i c_i(\beta_i + s)$ dla $s \in \mathbb{F}_{n+1}$.

Zadanie 8. 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

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

Wskazówka: Liczby po prawej i lewej stronie mają dobrze zdefiniowany sens. Skorzystaj też z Zadania 7.