Kody korekcyjne: Lista 6

23 listopada 2023

Zadanie 1. (Trochę bez związku z kodami cyklicznymi)

Przeczytaj i opowiedz oryginalną konstrukcję kodów Golay'a `https://skos.ii.uni.wroc.pl/mod/resource/view.php?id=38620`.

Tylko jedna strona! Wspominana praca Shannona nie jest istotna, mowa jest o kodzie Hamminga i kodach optymalnych.

Zadanie 2. Niech $\alpha \in \mathbb{F}_{2^m}$ będzie generatorem $\mathbb{F}_{2^m}^*$ i niech $g(X) \in \mathbb{F}_2[X]$ będzie minimalnym wielomianem dla α nad $\mathbb{F}_2$ (czyli nierozkładalnym, którego α jest pierwiastkiem; zawsze taki wielomian istnieje). Pokaż, że kod cykliczny długości $2^m - 1$ generowany przez $g(X)$ jest w istocie kodem Hamminga.

Zadanie 3. 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 4. Niech $\mathbb{F} \leq \mathbb{F}'$ będą dwoma ciałami. Rozważmy wielomiany f, g, h, spełniające

$$\begin{aligned} fg &= h \\ f, h &\in \mathbb{F}[X] \\ g &\in \mathbb{F}'[X] \end{aligned}$$

Pokaż, że $g \in \mathbb{F}[X]$.

Innymi słowy: jeśli $f, h \in \mathbb{F}[X]$ i podzielność zachodzi w $\mathbb{F}'[X]$, to zachodzi też w $\mathbb{F}[X]$.

Zadanie 5. Pokaż, że dla generatora $\alpha \in \mathbb{F}_{2^m}$ wielomiany $M^{(i)}$ oraz $M^{(2i)}$ są równe.

Wskazówka: Co potrafisz powiedzieć o $M^{(i)}((\alpha^i)^2)$?

Zadanie 6. Niech $\mathbb{F} \leq \mathbb{F}'$, gdzie $|\mathbb{F}| = q, |\mathbb{F}'| = q^m$, weźmy $n = q^m - 1$. Niech α — generator $\mathbb{F}'$, oraz a oraz d — liczby naturalne. Pokaż że dla

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

zbiór

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

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 7. Dla kodu z poprzedniego zadania pokaż, że jego wymiar dla $n = q^m - 1$, a, d wynosi przynajmniej

$$q^m - 1 - (d-1)m$$

Wskazówka: Tu już trzeba przepisać warunki liniowe w $\mathbb{F}'$ na warunki liniowe $\mathbb{F}$.

Dla kodu z poprzdniego

Zadanie 8. Pokaż, że odległość kodu z Zadania 6 to przynajmniej d.

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