Kody korekcyjne: Lista 5

8 listopada 2023

Zadanie 1. Naturalne kodowanie wiadomości w kodzie cyklicznym generowanym przez $g(X)$ to zinterpretowanie jej jako wielomianu $w(X)$ i zakodowanie jako $w(X)g(X)$. To kodowanie nie jest jednak systematyczne. Pokaż „naturalne” kodowanie systematyczne.

Wskazówka: Najprościej jest zakodować wiadomość jako współczynniki przy najwyższych potęgach X a cyfry kontrolne na mniej znaczących.

Zadanie 2. Pokaż, że jeśli $C \leq \mathbb{F}_q^n$ jest cyklicznym kodem samodualnym, czyli $C^\perp = C$, to q jest parzyste (innymi słowy: charakterystyki 2) oraz $g_0 \in \{1, -1\}$, gdzie g jest wielomianem generującym.

Wskazówka: Rozważ własności współczynników g.

Zadanie 3. Pokaż, że jeśli $\alpha \neq 0$ jest pierwiastkiem k-krotnym g, to α^{-1} jest pierwiastkiem k-krotnym g_R.

Zadanie 4. Udowodnij, że jeśli $g(X)|(X^n - 1)$ to również $g_R(X)|(X^n - 1)$.

Zadanie 5. Niech $C_i \leq \mathbb{F}_q^n$ będą kodami cyklicznymi o generatorach $g_i(X)$, dla $i \in \{1, 2\}$. Pokaż, że $C_1 \leq C_2$ wtedy i tylko wtedy, gdy $g_2(X)|g_1(X)$.

Zadanie 6. Niech $C_i \leq \mathbb{F}_q^n$ będą kodami cyklicznymi o generatorach $g_i(X)$, dla $i \in \{1, 2\}$. Pokaż, że $C_1 \cap C_2$ oraz $C_1 + C_2$ (w sensie sumy przestrzeni liniowych, t.j. $\{v_1 + v_2 : v_1 \in C_1, v_2 \in C_2\}$) są kodami cyklicznymi. Jak ich wielomiany generujące wyrażają się przez g_1, g_2?

Zadanie 7. Niech $\vec{v} \in \mathbb{F}_q^n$. Pokaż, że wielomian generujący najmniejszy kod cykliczny zawierający $\vec{v}$ jest równy $\mathrm{nwd}(v(X), X^n - 1)$, gdzie $v(X)$ jest wielomianem odpowiadającym $\vec{v}$.

Zadanie 8. Dany jest $[n, k]_2$ kod cykliczny poprawiający 2 błędy, przy czym $n \geq 2k$. Pokaż, że algorytm error trapping poprawnie poprawia do 2 błędów w tym kodzie.

Czy jest to prawda dla $n < 2k$?

Zadanie 9. Niech $g(x)$ będzie wielomianem generującym binarny kod cykliczny C. Pokaż, że C_E wektorów z C o parzystej wadze (Hamminga) również jest kodem cyklicznym. Wyznaczy jego wielomian generujący (wyraź go przez $g(X)$).