Kody korekcyjne: Lista 1

2 października 2019

Zadanie 1. Rozważaliśmy symetryczny kanał komunikacji o prawdopodobieństwie błędu γ (w skrócie: BSC_γ) dla $\gamma < 1/2$. Co możesz powiedzieć o BSC_γ dla $\gamma = \frac{1}{2}$ oraz $\gamma < \frac{1}{2}$?

Zadanie 2. Co jeśli dopuścimy błędy zatarcia, tzn. wiemy, że bit był, ale nie potrafimy go odczytać.
Podaj warunek dotyczący odległości kodu oraz korekcji błędów zatarcia.
Co jeśli dopuścimy jednocześnie błędy zatarcia oraz błędy zmiany bitu?

Zadanie 3. Ile jest binarnych $(n, 2, n)_2$ kodów, dla $n \geq 2$?

Zadanie 4. Przypomnijmy, że (starsza wersja: dziesięciocyfrowy) kod ISBN definiowany jest jako ciąg cyfr $d_1, \ldots, d_{10}$ takich że $\sum_{i=1}^{10} i \cdot d_i \mod 11 = 0$. Cyfry $d_1, \ldots, d_9$ są od 0 do 9, zaś d_{10} może być równe 10 (i jest zapisane jako X).

Pokaż, że tak zdefiniowany kod pozwala wykryć jeden błąd oraz poprawić jedno wymazanie. Pokaż też, że potrafi wykryć zamianę sąsiednich cyfr.

Zadanie 5. Z dokładnością do permutowania cyfr, IBAN definiuje, iż do numeru rachunku bankowego należy dopisać (na dwóch najmniej istotnych pozycjach, czyli inaczej, niż to się robi przy zapisie) dwie wiodące cyfry kontrolne tak, aby wynik (przeczytany jako liczba dziesiętna) dawał resztę 1 modulo 97.

- Pokaż, że zawsze można dopisać takie cyfry kontrolne.
- Pokaż, że IBAN potrafi wykryć jeden błąd oraz jedną zamianę sąsiednich znaków.
- Co się stanie, jeśli procedurę generowania takiego kodu powtórzymy? Tj. dopiszemy cyfry kontrolne i następnie znów je dopiszemy. Co umiesz powiedzieć o tych drugich cyfrach? Jest to np. przypadek Portugalii.

Zadanie 6. Niech C będzie podprzestrzenią liniową przestrzeni $\mathbb{F}^n$, zaś G_C jej macierzą generującą. Pokaż, że:

- $C^\perp$ jest przestrzenią liniową;
- $v \in C^\perp \iff G_C^T v = \vec{0}$.
- $\dim(C^\perp) = n - \dim C$. (punkt drugi + wzór na wymiary jądra i obrazu)
- $(C^\perp)^\perp \geq C$.
- $C = (C^\perp)^\perp$ (punkt trzeci i czwarty).

Zadanie 7. Udowodnij, że dla kodu C o macierzy parzystości H_C odległość $\mathrm{d}_H(C)$ kodu C to najmniejsza liczba kolumn liniowo zależnych w H_C.

Wskazówka: i-ta kolumna to obraz i-tego wektora jednostkowego.

Zadanie 8. Pokaż równoważność warunków:

- H_C jest macierzą parzystości kodu C
- kolumny H_C^T są bazą $C^\perp$.

Pokaż też, że rząd macierzy H_C kodu C to $n - \dim C$, gdzie n: długość słów kodowych.

Możesz korzystać z poprzednich zadań.

Zadanie 9. Niech C_i będzie $[n_i, k_i, d_i]_2$-kodem, dla $i = 1, 2$. Rozpatrzmy zbiór macierzy, których wiersze są słowami kodowymi z C_1, zaś kolumny z C_2. Pokaż, że jest to $[n_1 n_2, k_1 k_2, d_1 d_2]_2$-kod.

Wskazówka: Macierze generujące w postaci systematycznej.

Zadanie 10. Pokaż, że kod Hamminga poprawia jeden błąd (lub prościej: pokaż, że jego dystans to 3).

Pokaż, że każde słowo długości 7 jest w odległości nie większej niż 1 od jakiegoś słowa kodowego z kodu Hamminga.