Kody korekcyjne: Lista 1

4 października 2023

Zadanie 1. Rozważmy następujący model powstania błędu: przesyłamy n-bitowy ciąg, dla każdego bitu z prawdopodobieństwem $\gamma < \frac{1}{2}$ zmieniamy bit na przeciwny.

Pokaż, że dla otrzymanego ciągu $\vec{v}$ najbardziej prawdopodobnym (czy ściślej: wiarygodnym) słowem kodowym $\vec{u}$ jest to o minimalnej odległości Hamminga od $\vec{v}$.

Co jeśli $\gamma = \frac{1}{2}$? Co jeśli $\gamma > \frac{1}{2}$?

Zadanie 2. Błędy zatarcia: w wynikowej wiadomości mogą być zarówno błędy polegające na zmianie symbolu jak i błędy zatarcia, to jest otrzymany symbol to $? \notin \Sigma$.

Podaj warunek dotyczący odległości kodu oraz korekcji k_1 błędów i k_2 błędów zatarcia (jednocześnie!).

Zadanie 3. Ile jest kodów korekcyjnych $C \subseteq \{0,1\}^n$, $|C| = 2$, $\Delta(C) = n$?

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. Nie używając macierzy parzystości pokaż, że kod Hamminga poprawia jeden błąd (lub prościej: pokaż, że ma odległość 3).

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

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

Zadanie 8. Pokaż, że dla kodu liniowego C istnieje podobny kod C', którego macierz generatorów jest systematyczna.

Zadanie 9. Pokaż, że jeśli macierz generatorów kodu C jest w postaci systematycznej $G_C = \begin{bmatrix} \mathrm{Id} \\ X \end{bmatrix}$ to macierz

$$[-X|\,\mathrm{Id}]$$

jest macierzą parzystości tego kodu.

Zadanie 10. Pokaż, że poniższa macierz jest macierzą parzystości kodu Hamminga.

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Używając jej udowodnij ponownie, że odległość kodu Hamminga wynosi 3.

Pokaż, że He_i, gdzie e_i jest i-tym wektorem standardowym, to zapis binarny i.

Zadanie 11. Używając poprzedniego zadania pokaż, że każde słowo $u \in \{0,1\}^7$ jest w odległości najwyżej 1 od jakiegoś słowa kodowego z kodu Hamminga.

W tym celu rozważ Hu.

Zadanie 12. 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.