Kody korekcyjne: Lista 2

17 października 2023

Zadanie 1. Niech $\mathbb{F}_q$ będzie ciałem o q elementach. Udowodnij, że dla $0 < d < q-1$

$$\sum_{\alpha \in \mathbb{F}_q} \alpha^d = \sum_{\alpha \in \mathbb{F}_q^*} \alpha^d = 0 \ .$$

Wskazówka: Przedstaw α jako potęgę generatora, zastosuj wzory na sumę ciągu geometrycznego.

Zadanie 2. Niech $\mathrm{RS}_{\mathbb{F}_q}(n,k)$ oznacza kod Reeda-Solomona nad $\mathbb{F}_q$ z punktami ewaluacji $\mathbb{F}_q$, tj $n = q$. Pokaż, że

$$\mathrm{RS}_{\mathbb{F}_q}(n,k)^\perp = \mathrm{RS}_{\mathbb{F}_q}(n, n-k) \ .$$

Wskazówka: Zadanie 1.

Zadanie 3. Definiujemy *uogólnione kody Reeda Solomona* jako:

$$\mathrm{GRS}(\vec{\alpha}, n, k, \vec{\lambda}) = \{(\lambda_0 f(\alpha_0), \lambda_1 f(\alpha_1) \ldots, \lambda_{n-1} f(\alpha_{n-1}) \ : \ f \in \mathbb{F}[X], \deg(f) < k\} \ ,$$

gdzie $\alpha_0, \ldots, \alpha_{n-1}$ są parami różne.

Pokaż, że

$$\mathrm{GRS}(\vec{\alpha}, n, k, \vec{\lambda})^\perp = \mathrm{GRS}(\vec{\alpha}, n, n-k, \vec{\sigma})$$

dla pewnego $\vec{\sigma} \in \mathbb{F}^{n-k}$. W tym celu pokaż, jak wygląda macierz parzystości $\mathrm{GRS}(\vec{\alpha}, n, k, \vec{\lambda})$ najpierw dla maksymalnego k, czyli $n-1$. Potem indukcja w dół po k.

Wskazówka: Można próbować wprost, podobnie jak dla kodów $\mathrm{RS}_{\mathbb{F}_q}$, powinno wyjść. Prostszy sposób:

Zadanie 4. Udowodnij, że każda funkcja $f : \mathbb{F} \to \mathbb{F}$ jest wielomianem, tj. istnieje wielomian $p \in \mathbb{F}_q[X]$, taki że $\deg(p) < q$ oraz $f(\alpha) = p(\alpha)$ dla każdego $\alpha \in \mathbb{F}$. Uogólnij to twierdzenie na funkcje wielu zmiennych.

Zadanie 5. Wiemy, że każdy kod liniowy można przekształcić w kod z systematyczną macierzą generatorów. W szczególności jest to prawda dla kodów RS. Celem tego zadania jest skonstruowanie takiego przekształcenia.

Dla danego wektora punktów ewaluacji $\alpha_0, \ldots, \alpha_{n-1}$ podaj (jawnie) funkcję f z $\mathbb{F}_q^k$ w wielomiany stopnia $\leq k-1$, taką że dla każdej wiadomości $m_1, \ldots, m_k \in \mathbb{F}^k$ jeśli odpowiadającym wielomianem jest $f_m(X)$, to wektor $f_m(\alpha_0), \ldots, f_m(\alpha_{n-1})$ zawiera $m_1, \ldots, m_k$ na ustalonych współrzędnych (powiedzmy na pierwszych, ale nie jest to kluczowe).

Zadanie 6. To zadanie prezentuje kod będący „odpowiednikiem" kodu RS używającego teori liczb.

Niech $1 \leq k < n$ będzie liczbą całkowitą a $p_1 < p_2 < \cdots < p_n$ parami różnymi liczbami pierwszymi. Oznaczmy $K = \prod_{i=1}^k p_i$, $N = \prod_{i=1}^n p_i$. $\mathbb{Z}_m$ oznacza standardowo liczby modulo m.

Rozważmy Chiński kod reszt:

$$E : \mathbb{Z}_K \to \prod_{i=1}^n \mathbb{Z}_{p_i}$$

zadany jako

$$E(m) = (m \mod p_1, m \mod p_2, \ldots, m \mod p_n) \ .$$

Załóżmy, że $m_1 \neq m_2$. Dla $1 \leq i \leq n$ zdefiniujmy

$$b_i = \begin{cases} 1 & \text{jeśli } E(m_1)_i \neq E(m_2)_i \\ 0 & \text{jeśli } E(m_1)_i = E(m_2)_i \end{cases} \ .$$

Pokaż, że dla tak zdefiniowanych $b_1, \ldots, b_n$ zachodzi

$$\prod_{i=1}^n p_i^{b_i} > \frac{N}{K} \ .$$

Wywnioskuj z tego, że $m_1 \neq m_2$ implikuje, że kodowania $E(m_1)$ i $E(m_2)$ różnią się między sobą na co najmniej $n-k+1$ pozycjach.

(Drobna uwaga: formalnie to nie jest kod, bo na różnych pozycjach są symbole z różnych alfabetów, ale definicja odległości itp. się prosto uogólnia, pominiemy drobne komplikacje techniczne)

Zadanie 7. $[n, k, d]_q$ kod nazywamy *doskonałym*, jeśli każde słowo w $\mathbb{F}_q^n$ jest w odległości najwyżej $\left\lfloor \frac{d-1}{2} \right\rfloor$ od jakiegoś słowa kodowego.

Pokaż, że jeśli $[n, k, d]_q$-kod jest doskonały i nietrywialny (tj. nie jest całą przestrzenią, ani nie jest jednoelementowy), to d jest nieparzyste.

Zadanie 8. 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 generującą w postaci systematycznej.

Zadanie 9. Dla kodu liniowego C jego kod rozszerzony powstaje przez dopisanie bitu kontroli parzystości, formalnie:

$$\overline{C} = \{(c_1, \ldots, c_k, -\sum_{i=1}^{k} c_i) \ : \ c_1, \ldots, c_k \in C\} \ .$$

Pokaż, że jest to kod liniowy. Jak wygląda jego macierz parzystości? Pokaż też, że

$$\Delta(C) \leq \Delta(\overline{C}) \leq \Delta(C) + 1 \ .$$