Kody korekcyjne: Lista 3

17 października 2019

Zadanie 1. Załóżmy, że w przestrzeni $\mathbb{R}^n$ jest M różnych wektorów $v_1, \ldots, v_M$, z których każdy ma długość 1 oraz zachodzi

$$\langle v, v' \rangle \leq 0$$

dla $v \neq v'$ z tego zbioru, gdzie $\langle \cdot, \cdot \rangle$ jest standardowym iloczynem skalarnym w $\mathbb{R}^n$. Pokaż, że $M \leq 2n$. Udowodnij też, że to ograniczenie jest ścisłe.

Wskazówka: Indukcja. Obracanie przestrzeni jest izometrią, tj. nie zmienia iloczynu skalarnego, czyli możesz założyć, że jeden z wektorów jest jednostkowy.

Zadanie 2. Głównym problemem ograniczenia Plotkina jest to, że działa tylko dla kodów o dużych odległościach.

Udowodnij, że można z niego wywnioskować wersję, która działa też dla mniejszych odległości: Jeśli $d = \mathrm{d}(C) \leq \frac{q-1}{q} n$, gdzie n to długość kodu a q-rozmiar alfabetu, to

$$|C| \leq q^{n - \lceil d \frac{q}{q-1} \rceil} d \ .$$

Wskazówka: Podziel kod na wiele kodów, grupując wg. prefiksów odpowiedniej długości, tak aby móc dla każdego z nich zastosować ograniczenie Plotkina. Zsumuj ograniczenia i oszacuj.

Zadanie 3. 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 potęgi generatora, zastosuj wzory na sumę ciągu geometrycznego.

Zadanie 4. 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 $\mathrm{GRS}(\vec{\alpha}, n, k, \vec{\lambda})$

Wskazówka: Można próbować jak dla kodów RS, powinno wyjść. Prostszy sposób: najpierw dla maksymalnego k, czyli $n-1$. Potem indukcja w dół po k.

Zadanie 5. 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 6. 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 7. 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)