Kody korekcyjne: Lista 6

7 listopada 2019

Zadanie 1. Pokaż, że jeśli $r < q$ to

$$\dim(\mathrm{RM}(q, m, r)) = \binom{m+r}{r} \ .$$

Zadanie 2. Niech $0 \neq f \in \mathbb{F}_2[X_1, \ldots, X_m]$ będzie niezerowym wielomianem spełniającym $\deg_{X_i}(f) \leq 1$. Pokaż, że

$$|\{(a_1, \ldots, a_m) \in \mathbb{F}_2^m \ : \ f(a_1, \ldots, a_m) \neq 0\}| \geq 2^{m-\deg(f)} \ . \qquad (*)$$

Zadanie 3. Pokaż, że ograniczenie z Zadania 2 jest ścisłe, w tym sensie, że dla każdego m istnieje wielomian m zmiennych dla którego (*) jest spełniona z równością.

Zadanie 4. Pokaż, że dla każdej liczby pierwszej q oraz liczb całkowitych $m \geq 1$ i $1 \leq r \leq q-1$, istnieje wielomian z dokładnie $r \cdot q^{m-1}$ pierwiastkami.

Zadanie 5. Przypomnij (pokaż?), że dla $1 \leq d \leq q-1$

$$\sum_{\alpha \in \mathbb{F}_q} \alpha^d \neq 0 \qquad \iff d = q-1$$

Udowodnij, że dla $1 \leq d_1, \ldots, d_m \leq q-1$

$$\sum_{c_1, \ldots, c_m \in \mathbb{F}_q} \prod_{i=1}^{m} c_i^{d_i} \neq 0 \qquad \iff d_1 = d_2 = \cdots = q-1$$

Wywnioskuj z tego, że kody dualne do kodów $\mathrm{RM}(q, m, r)$ to kody $\mathrm{RM}(q, m, m(q-1) - r - 1)$.

Zadanie 6. Udowodnij, że r-ty kod Hadamarda $C_{\mathrm{Had}}^{(r)}$, czyli $[2^r, r, 2^{r-1}]_2$-kod, przekształca wiadomość $(m_1, \ldots, m_r) \in \{0,1\}^r$ w ewaluację wielomianu m zmiennych $\sum_{i=1}^{m} m_i X_i$ nad wszystkimi elementami $\{0,1\}^m$.

Wywnioskuj z tego, że kod $\mathrm{RM}(m, 1, 2)$ jest postaci $C_{\mathrm{Had}}^{(r)} \cup \overline{C_{\mathrm{Had}}^{(r)}}$, gdzie $\overline{C} = \{1 - v \ : \ v \in C\}$.

Zadanie 7. Udowodnij, że jeśli $g \in \mathbb{F}_q[X_1, \ldots, X_m]$ jest wielomianem m zmiennych oraz $\deg(g) < r$ to

$$\sum_{\vec{a} \in \mathbb{F}_2^r} g(\vec{a}) = 0 \ .$$

Zadanie 8. Pokaż, że algorytm Reed'a zdefiniowany na wykładzie działa w czasie $\mathcal{O}(n^2 poly(\log n))$.

Dla przypomnienia, jako wejście dostaje on f podaną jako ciąg wartości we wszystkich punktach $\mathbb{F}_2^m$, przy czym $n = 2^m$. Możesz założyć, że te wartości są właściwie uporządkowane, np. wartość dla podstawienia $X_i \leftarrow d_i$ d-ta w kolejności, gdzie d to liczba której zapis binarny to $d_m, \ldots, d_1$.)

Zadanie 9. Zaproponuj usprawnienia algorytmu Reeda, które pozwolą na zmniejszenie (asymptotycznego) czasu działania.

Wskazówka: Mam parę pomysłów, ale nie wiem, co i czy działa. Są też prace — często nazwa to „majority logic decoding".

Zadanie 10. Dla danego $q \geq 2$ (będącego potęgą liczby pierwszej, ale to bez znaczenia) oraz liczb naturalnej r niech s, t będą (jedynymi) nieujemnymi liczbami całkowitymi takimi że

$$0 \leq t \leq q-2 \text{ oraz } s(q-1) + t = r \ .$$

(tj. $t = r \bmod (q-1)$ i $s = (r-t)/(q-1)$). Pokaż że

$$(q-t) \cdot q^{m-s-1} \geq q^{m - \frac{r}{q-1}} \ .$$

Zadanie 11. Pokaż, jak z reprezentacji słowa kodowego kodu RM jako ciągu wartości P we wszystkich argumentach (dla znanej kolejności argumentów) odtworzyć współczynniki wielomianu P (innymi słowy: interpolacja).

Nie podaliśmy żadnego konkretnego kodowania, ale to jest pytanie o odtworzenie oryginalnej wiadomości z poprawnego kodu.

Zadanie 12. Pokaż, że w ciele $\mathbb{F}_{q^m}$ podciało $\mathbb{F}_q$ to dokładnie zbiór pierwiastków wielomianu

$$X^q - X$$

Zadanie 13. Używając Zadania 12 pokaż, że funkcja śladu

$$\mathrm{tr}(X) = \sum_{i=0}^{m-1} X^{q^i}$$

faktycznie przyjmuje tylko wartości w podciele $\mathbb{F}_q$.