Kody korekcyjne: Lista 9

13 grudnia 2023

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 stopnia r 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 stopnia r nad $\mathbb{F}_q$ z dokładnie $r \cdot q^{m-1}$ miejscami zerowymi, tj. spełniający z równością Lemat Schwartz-Zippel.

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 $\overline{C} = \{\vec{1} - \vec{v} \ : \ \vec{v} \in C\}$.

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

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

Zadanie 8. Pokaż, że dla $\mathbb{F}_q \neq \mathbb{F}_2$ i jednomianu $P = X_1 \cdots X_r$ zachodzi

$$\sum_{\vec{a} \in \mathbb{F}_q^r} P(\vec{a}) = 0$$

Dzięki tej obserwacji wytłumacz, dlaczego algorytm Reeda dla kodów RM nie działa dla ciała innego niż $\mathbb{F}_2$.

Wskazówka: Wystarczy dla $r = 1$, reszta przez proste sumowanie.
Dla q nie parzystego jest łatwo: jak się ma do siebie a i $-a$ w $\mathbb{F}_q$?
Dla q parzystego rozpatrz najpierw $\mathbb{F}_4$: bzo. jego elementy to wielomiany $0, 1, X, 1+X$ (mnożenie jest zdefiniowane modulo $X^2 + X + 1$, ale to nie będzie tutaj ważne). Jak to się uogólnia na większe ciała?

Zadanie 9. 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 10. Pokaż, że jeśli w multizbiorze S istnieje element $s \in S$ występujący w nim więcej niż $|S|/2$ razy, to Algorytm Majority go zwróci.

Algorytm 1 Algorytm Majority

```
    i, c ← 1
    s ← S[1]
    while i < |S| do
        i ← i + 1
 5:     if s = S[i] then
            c ← c + 1
        else
            c ← c − 1
            if c = 0 then
10:             i ← i + 1, c ← 1
                s ← S[i]
    if c > 0 then
        return s
    else
15:     return NULL
```

Zadanie 11. 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 12. Pokaż, że funkcja

$$r \mapsto q^m - (q-t)q^{m-s-1} \ ,$$

gdzie $r = s(q-1)+t$ dla $0 \leq t < q-1$, jest rosnąca jako funkcja r (przy ustalonych q, m).

Zadanie 13. 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.