

# Kody korekcyjne: Lista 13

10 stycznia 2020

**Zadanie 1.** Niech  $D \geq 1$ ,  $k \geq 2$  będą liczbami naturalnymi; zdefiniujmy

$$N_{k,D} = |\{(i, j) : i + (k-1)j \leq D, i, j \in \mathbb{N}\}| .$$

Pokaż, że

$$N_{k,D} > \frac{D(D+2)}{2(k-1)} .$$

Czy potrafisz (i jak bardzo) poprawić to oszacowanie?

**Zadanie 2.** Pokaż, że stopień ważony  $\deg_{(x,y)}$  dla naturalnych  $x, y \geq 0$  zachowuje się jak prawdziwy stopień wielomianów, tzn.

$$\deg_{(x,y)}(PQ) \leq \deg_{(x,y)}(P) + \deg_{(x,y)}(Q), \quad \deg_{(x,y)}(P+Q) \leq \max(\deg_{(x,y)}(P), \deg_{(x,y)}(Q))$$

Co więcej, jeśli  $\deg_{(1,w)}(Q) = D$  a  $P(X)$  jest wielomianem, takim że  $\deg(P) \leq w$  to

$$\deg(Q(X, P(X))) \leq D .$$

**Zadanie 3.** Pokaż, że podana na wykładzie definicji pierwiastka  $r$ -krotnego dla wielomianu wielu zmiennych (wielomian  $Q$  ma pierwiastek  $r$ -krotny w  $(0,0)$ ), jeśli każdy jego jednomian ma stopień przynajmniej  $r$ ) *nie implikuje*, że wielomian można przedstawić jako iloczyn  $r$  wielomianów, które mają pierwiastek w  $(0,0)$ .

*Wskazówka:* Można rozważyć możliwość rozkładu

wielomianu. Wskazówka: Można rozważyć możliwość rozkładu wielomianu. Można również rozważyć możliwość rozkładu wielomianu.

**Zadanie 4.** Pokaż, że Algorytm Guruswaniego-Sudana (czyli najlepszy dla dekodowania RS do listy) można uogólnić tak, by przydzielał różne krotności  $r_i$  każdemu z pierwiastków  $(\alpha_i, y_i)$  wielomianu  $Q$ . Algorytm powinien zwracać wszystkie wielomiany  $P$  spełniające warunek

$$\sum_{i:P(\alpha_i)=y_i} r_i > \left\lceil \sqrt{(k-1) \sum_{i=1}^n r_i(r_i+1) + 1} \right\rceil - 1$$

**Zadanie 5.** Pokaż, że Algorytm Guruswaniego-Sudana można też rozszerzyć do przypadku, kiedy podajemy parę możliwych wartości w punkcie  $\alpha_i$ . Dokładniej: niech  $w_{i,\alpha}$  dla  $i = 1, \dots, n$  oraz  $\alpha \in \mathbb{F}_q$  możemy w wielomianowym czasie podać wszystkie wielomiany  $P(X)$  spełniające warunek

$$\sum_i r_{i,P(\alpha_i)} > \left\lceil \sqrt{(k-1) \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} r_{i,\alpha}(r_{i,\alpha}+1) + 1} \right\rceil - 1$$

Celem kilku poniższych zadań jest pokazanie, jak można faktoryzować wielomiany dwóch zmiennych (nad  $\mathbb{F}_q$ ).

**Zadanie 6.** Niech  $Q_0(X, Y)$  będzie niezerowym wielomianem dwóch zmiennych niepodzielnym przez  $X$ . Niech  $F_0(X) = \sum_{i \geq 0} f_i X^i \in \mathbb{F}_q[X]$  będzie wielomianem spełniającym

$$Q(X, F_0(X)) \equiv 0 .$$

Niech

$$Q_1(x, y) = Q_0(X, XY + f_0)$$

Wtedy  $f_0$  jest pierwiastkiem wielomianu

$$Q_0(0, Y)$$

a  $F_1(x) = \sum_{i \geq 0} f_{i+1} X^i \in \mathbb{F}_q[X]$  spełnia

$$Q_1(X, F_1(X)) \equiv 0$$

**Zadanie 7.** Niech  $Q_0(X, Y) \in \mathbb{F}_q[X, Y]$  będzie wielomianem dwóch zmiennych niepodzielnym przez  $X$  oraz niech  $\alpha \in \mathbb{F}_q$  będzie (dokładnie)  $h$ -krotnym pierwiastkiem  $Q_0(0, Y)$ . Zdefiniujmy  $Q_1(X, Y) = Q_0(X, XY + \alpha)$  i niech  $Q_1^*(X, Y) = Q_1(X, Y)/X^\sigma$ , gdzie  $\sigma$  jest największą liczbą taką że  $X^\sigma | Q_1$ . Wtedy  $\deg(Q_1^*(0, Y)) \leq h$ .

$$Q_1^*(X, Y) = \frac{Q_1(X, Y)}{X^\sigma} = \frac{Q_0(X, XY + \alpha)}{X^\sigma}$$

**Zadanie 8.** Używając dwóch poprzednich zadań podaj algorytm, który dla danego  $Q(X, Y) \in \mathbb{F}_q[X][Y]$  znajduje wszystkie  $P$  takie że  $Y - P(X) | Q(X, Y)$ . Czas działania ma zależeć wielomianowo od stopnia  $Q$ , liczby współczynników  $Q$  oraz  $q$ ; w szczególności możesz faktoryzować wielomian jednej zmiennej w czasie zależnym od  $q$ .