Kody korekcyjne: Lista 4

23 października 2019

Zadanie 1. Udowodnij, że niezmiennik w algorytmie BM działa tuż po tym, kiedy g stanie się niezerowy.

Zadanie 2. Udowodnij, że niezmienniki w algorytmie BM są zachowywane też w przypadku, gdy $r > c$.

Zadanie 3. Udowodnij, że jeśli $\deg(g) \leq \mathrm{span}(f) < \infty$ to $\mathrm{span}(g) \leq \deg(f)$.

Wskazówka: Rozważ najpierw przypadek $\deg(g) \leq \mathrm{span}(f)$, w drugim przypadku przemnóż g przez odpowiedni jednomian.

Zadanie 4 (Nie takie trudne, ale trochę długie — 2 punkty)**.** Algorytm BM w niektórych kręgach podawany jest jako algorytm rozwiązujący następujący problem:
Dane na wejściu liczby $a_1, \ldots, a_n$. Podaj najmniejsze możliwe ℓ oraz liczby $\alpha_0, \ldots, \alpha_{\ell-1}$, takie że

$$a_{i+\ell} = \sum_{j=0}^{\ell-1} \alpha_j a_{i+j}$$

Wskazówka: Zauważ, że nasza definicja $\langle \vec{e}, \cdot \rangle$ mnoży liczby "po współrzędnych". Liczby $a_1, \ldots, a_n$ będą odpowiadać $e_1, \ldots, e_n$, zaś α_i wartości $E(\gamma^i)$.

Zadanie 5. Jak wygląda macierz odwrotna do macierzy Vandermonde'a rozmiaru $n \times n$ nad $\mathbb{F}_q$ dla $n = q - 1$ (bzo. możesz odpowiednio uszeregować wiersze, tj. i-ty wiersz to potęgi γ^{i-1}, gdzie γ to generator $\mathbb{F}_q$. Ale możesz też inaczej, jeśli Ci wygodniej.).

Zadanie 6. Pokaż, jak policzyć szybko konwolucję dwóch ciągów liczb naturalnych, :
Dane są dwa ciągi $a_0, \ldots, a_{n_a}$ oraz $b_0, \ldots, b_{n_b}$. Chcemy policzyć ciąg $c_0, \ldots, c_{n_a+n_b}$, gdzie $c_k = \sum_{i,j:i+j=k} a_i b_j$.

Zadanie 7. Rozpatrujemy problem policzenia FFT (szybka transformata Fouriera), dla ciała skończonego. Dokładniej, dla ciała $\mathbb{F}_m$ rozpatrzmy jego dowolny element γ, przez d oznaczmy rząd γ. Dla danego wektora $\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{bmatrix}$ chcemy obliczyć wektor $\begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{d-1} \end{bmatrix}$ zadany przez

$$\begin{bmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{d-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \gamma & \gamma^2 & \ldots & \gamma^{d-1} \\ 1 & \gamma^2 & \gamma^4 & \ldots & \gamma^{2(d-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma^{d-1} & \gamma^{2(d-1)} & \ldots & \gamma^{(d-1)^2} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{d-1} \end{bmatrix} .$$

Innymi słowy

$$A_j = \sum_{i=0}^{d-1} a_i \gamma^{ji} \qquad (*)$$

Rozważ dwa przypadki:

- Jeśli d jest parzyste, to pokaż, że można ten problem sprowadzić do dwóch wywołań rekurencyjnych dla $d/2$ (oraz dodatkowych liniowych obliczeń).
- Jeśli d jest nieparzyste, to pokaż, że istnieje α taka że $\gamma = \alpha^2$. Przepisz równanie $(*)$ do postaci

$$A_j = \sum_{i=0}^{d-1} a_i \alpha^{2ji} \ .$$

Przedstaw $2ij = -i^2 - j^2 + (i+j)^2$ i zredukuj problem do Zadania 6, nawet jeśli nie umiesz go policzyć.

Zadanie 8. Podaj algorytm w modelu adaptacyjnym, który znajduje jedną chorą osobę używając $\mathcal{O}(\log N)$ testów. Uogólnij wynik tak, aby znajdować d osób przy użyciu $\mathcal{O}(d \log N)$ testów.

Popraw algorytm tak, aby używał $\mathcal{O}\left(d \log_2 \frac{N}{d}\right)$ testów.

Wskazówka: Pierwszy sposób: podziel N na mniejsze grupy i sprawdź osobno, oszacuj czas. Drugi: uszeregуj wszystkie osoby, pokaż jak znaleźć chorego o najmniejszym numerze N' w czasie $\mathcal{O}(\log N')$. Iterуj, oszacuj sumaryczny czas (nierówność Jensena, być może też jakieś podchodne).

Zadanie 9. Macierz M rozmiaru $t \times N$ jest *d-separowalna*, jeśli dla $J, J' \subseteq \{1, \ldots, N\}$, $|J|, |J'| \leq d$ zachodzi

$$\bigvee_{j \in J} M^j \neq \bigvee_{j \in J'} M^j \ ,$$

gdzie M^j to j-ta kolumna M zaś $\bigvee$ to alternatywa logiczna po współrzędnych.

Pokaż, że macierz M rozmiaru $t \times N$ użyta jako macierz testów do nieadaptacyjnego group testing dla N osób wykrywa chorych (o ile jest ich nie więcej niż d) wtedy i tylko wtedy, gdy jest d-separowalna.

Zadanie 10. Macierz M rozmiaru $t \times N$ jest d-rozłączna wtedy i tylko wtedy, gdy dla każdego $S \subseteq \{1, \ldots, N\}$, $|S| \leq d$ oraz dla każdego $j \notin S$, istnieje $i \in \{1, \ldots, t\}$ takie, że $M_{ij} = 1$ oraz dla wszystkich $k \in S$, $M_{ik} = 0$; równoważnie

$$M^j \not\subseteq \bigvee_{k \in S} M^k \ .$$

Pokaż, że macierz d-rozłączna jest też d-separowalna. Podaj algorytm dla problemu group testing używający tej macierzy i odtwarzający zbiór chorych w czasie $\mathcal{O}(tN)$ (czasu mnożenia macierzy i wektora chorych nie liczymy).

Wskazówka: Intuicja definicji: jeśli S to zbiór chorych, to test i jak z definicji daje wynik 0, czyli jest świadkiem tego, że i jest zdrowy.
Algorytm: $i \in \{1, 2, \ldots, N\}$ można rozpatrzyć oddzielnie stаtus chory/zdrowy rozpatrywać tylko na podstawie testów, w których brał udział.

Zadanie 11. Pokaż, że każda macierz d-separowalna jest też $(d-1)$-rozłączna.