Kody korekcyjne: Lista 8

9 grudnia 2023

Zadanie 1. Algorytm PGZ konstruuje E „od góry", tj. w pewnym sensie rozpatruje kolejne możliwe liczby błędów zaczynając od największej możliwej.

Zastanów się, czy można zmodyfikować algorytm PGZ by działał „od dołu": dla kolejnych $m = 0, 1, \ldots$ próbował wyliczyć rozwiązanie układu równań tj. wielomian E stopnia m.

Czy umiesz powtórzyć sposób z poprzedniej listy, by ten algorytm działał w czasie $\mathcal{O}(n^3)$? Jak dobrą złożoność jesteś w stanie uzyskać (t — faktyczna liczba błędów to lepiej niż n).

Wskazówka: Wierzę w $\mathcal{O}((n-k)t^2)$, gdzie t jest faktyczną liczbą błędów. Te modyfikacje PGZ raczej nie będą szybciej działały w praktyce. Co więcej, słabo nadają się do implementacji sprzętowej.

Zadanie 2. Pokaż kluczową część poprawności algorytmu Peterson–Gorenstein–Zierler, tj. dla wektora błędów $\vec{e}$ o wadze $t = \|\vec{e}\|_1 \leq \frac{n-k}{2}$ pokaż, że macierz syndromów S, gdzie $(S)_{ij} = s_{i+j-2}$, jest odwracalna dla $m = t$.

Zadanie 3. Udowodnij, że niezmiennik w algorytmie BM działa tuż po tym, kiedy g stanie się niezerowy.

Zadanie 4. Udowodnij, że niezmienniki w algorytmie BM są zachowywane też w przypadku, gdy $r > c$.

Zadanie 5 (Wyszukiwanie Chiena)**.** Chcemy sfaktoryzować wielomian $\sum_{i=0}^{t} \lambda_t x^i$ nad ciałem $\mathbb{F}_q$.

Ile operacji wykonuje naiwny algorytm ewaluacji w każdym punkcie?

Ile operacji wykonuje algorytm oparty na schemacie Hornera?

Zaprojektuj algorytm, który wykorzystuje fakt, że mnożenie przez stałe (tj. niezależne od danych) jest (sprzętowo) lepsze, niż mnożenie przez zmienne (tj. mnożenie przez liczby zależne od stałych).

Algorytm osobno sprawdza 0 (co jest łatwe).

Dla $i = 0, 1, \ldots$ algorytm przechowuje $(\lambda_0, \lambda_1 \cdot \alpha^i, \lambda_2 \cdot \alpha^{2i}, \ldots, \lambda_t \alpha^{ti})$ i sprawdza, czy

$$\sum_{j=0}^{t} \lambda_t \lambda^{ij} = 0$$

jeśli tak, to zwraca α^i jako pierwiastek.

Ile operacji wykonuje ten algorytm?

Zadanie 6. 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 7. 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 8 (FFT dla dowolnego ciała)**.** 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 7, nawet jeśli nie umiesz go policzyć.