

ingue: push na prvi

deque: če drugi prazen, vse iz prvega na drugega,
potem vrhnji iz 2. skla



potencialna:

$$\Phi(i) = |S_1| + |S_2|$$

$$\begin{cases} i & ; i = 2^k \\ 1 & ; \text{sicer} \end{cases}$$

$$C ; \sum_{i=1}^n C_i \leq nC(n)$$

$$\begin{aligned} \sum_{i=1}^n C_i &= \sum_{i=1}^k 2^i + (n - \log n) \cdot 1 = \frac{1-2^{k+1}}{1-2} + (n - \log n) \\ &= 2^{\log n + 1} - 1 + n - \log n \\ n = 2^k \Rightarrow k &= \log n \\ &= 2n - 1 + n - \log n = \\ &= 3n - \log n - 1 \end{aligned}$$

$$\Rightarrow C = 3 - \frac{\log n}{n} - \frac{1}{n} \quad o(1)$$

$$\omega = e^{\frac{2\pi i}{n}} \quad n \text{ s.d.o}$$

$$a) \quad \omega^{k+\frac{n}{2}} = -\omega^k$$

$$b) \quad \omega^a = \omega^b ; \quad a \equiv b \pmod{n}$$

$$c) \quad \frac{1}{\omega^k} = \overline{\omega^k}$$

$$a) \quad -1 = e^{\pi i}$$

$$-\omega^k = e^{\pi i} e^{\frac{(2\pi i)}{n}k} = e^{\frac{2\pi i}{n}k + \pi i}$$

$$\omega^{k+\frac{n}{2}} = \omega^k \omega^{\frac{n}{2}}$$

$$e^{\frac{2\pi i}{n} \frac{n}{2}} = e^{\pi i} = -1$$

$$b) \quad \omega^a = \omega^{a-nb}$$

$$c) \quad \frac{1}{\omega^k} = \overline{\omega^k} \quad \omega^{-k} = \overline{\omega^k}$$

$$\begin{aligned}
 p^*[j] &= \sum_k p[k] \omega_n^{jk} = \sum_{l=0}^{\frac{n}{2}-1} \left(p[2l] \omega_n^{2lj} + p[2l+1] \omega_n^{(2l+1)j} \right) = \\
 &= \sum_{l=0}^{\frac{n}{2}-1} p[2l] \omega_n^{2lj} + \omega_n^j p[2l+1] \omega_n^{2lj} \\
 &= \sum_{l=0}^{\frac{n}{2}-1} p[2l] \omega_{\frac{n}{2}}^{lj} + \omega_n^j p[2l+1] \omega_{\frac{n}{2}}^{lj} = p_s^*[j] + \omega_n^j p_l^*[j]
 \end{aligned}$$

$$[1 \ 2 \ 3 \ 1 \ 2]$$

$$[1, 2]$$

$$\omega = e^{\frac{2\pi i}{3}}$$

$$[\omega^0 + \omega^2 + \omega^3 + \omega^1 + \omega^2] \cdot [\omega^2 + \omega^1]$$

$$\begin{aligned}
 a_1 a_2 \dots &\rightsquigarrow [y_0 \ y_1 \ \dots \ y_{n-1}] \\
 b_1 \dots &\rightsquigarrow [z_0 \ y_1 \ \dots \ z_{n-1}]
 \end{aligned}$$

Množenje je $O(n \log n)$

dva vektorja dolžine n in ačunamo vse skalar. prod.

$$\langle a, b[i:] + b[i:] \rangle$$

$$p = \sum a_i x^i$$

$$q = \sum b_j x^j$$

$$1: a_0 b_0$$

$$x: a_0 b_1 + a_1 b_0$$

$$x^2: a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$\vdots$$

$$x^k = \sum_{i=0}^k a_i b_{k-i} = \langle a[k], b[n;k-1] \rangle$$

$$q(x) = \sum b_{n-1-j} x^j$$

$$p(x) = \sum a_i x^i$$

$$a_0 b_3$$

$$a_0 b_2 \quad a_1 b_3$$

$$a_0 b_1 \quad a_1 b_2 \quad a_2 b_3$$

$$a_0 b_0 \quad a_1 b_1 \quad a_2 b_2 \quad a_3 b_3 \leftarrow \langle a, b \rangle$$

$$a_0 b_3 \quad a_1 b_0 \quad a_2 b_1 \quad a_3 b_2$$

$$a_0 b_2 \quad a_1 b_2 \quad a_2 b_0 \quad a_3 b_1$$

$$a_0 b_1 \quad a_1 b_2 \quad a_2 b_3 \quad a_3 b_1$$

def f(a, b, i)

A = produkt_pd(a, b[i:-1])

n = len(a)

if i == 0: return A[n-1]

return A[n-1+i] + A[i-1]

```

def FFT(koef)
    n = len(koef)
    if n == 1: return koef
    assert n % 2 == 0
    sodi = koef[::2]
    lhi = koef[1::2]
     $\omega_n = e^{\frac{2\pi i}{n}}$ ,  $\omega = 1$ 
    sodi = FFT(sodi)
    lhi = FFT(lhi)
    rezultat = [0] * (2n)
    for k in range( $\frac{n}{2}$ ):
        rezultat[k] = sodi[k] +  $\omega$  lhi[k]
        rezultat[ $\frac{n}{2} + k$ ] = sodi[k] -  $\omega$  lhi[k]
         $\omega = \omega \cdot \omega_n$ 
    return rezultat

```

A, B množici

$$\max(A), \max(B) \leq M$$

$O(M \log M)$ algoritem, ki prešteje na koliko
možnih načinov dobimo vse možne
vsote

$$\begin{aligned} A &= \{0, 1, 2\} \\ B &= \{0, 2\} \end{aligned} \Rightarrow \begin{aligned} &\{0, 1, 2, 3, 4\} \\ &\quad 1 \quad 1 \quad 2 \quad 1 \quad 1 \end{aligned}$$

$$\begin{aligned} &1 + x + x^2 \\ &1 + x^2 \end{aligned}$$

$$|FFT \left(FFT_{2n}(a) \cdot FFT_{2n}(b) \right)|$$

$$\hat{f}(\hat{x}) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \hat{x}} dx$$

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\hat{x}) e^{2\pi i x \hat{x}} d\hat{x}$$

②

$$n = \max_{x \in B} |x|$$

for $x \dots$

for y

return $-x-y \in B - \{x, y\}$
hashtable

proving use of n in

when n is 0 or 1

in the recurrence relation

with n terms

$$h: N \rightarrow Y$$

$$v \in O(\sqrt{n}) \text{ trk}$$

$$|Y| = n$$

k elementen haben ~~keine~~ ~~größere~~ ~~oder~~
 keine ~~oder~~

$$1 - \frac{1}{n} \cdot \frac{1}{n-1} \cdots \frac{1}{n-k+1} = 1 - \frac{k!}{n!}$$

$$1 - \frac{\binom{n}{k}}{n^k}$$

$$1 \cdot (1 - \frac{1}{n}) (1 - \frac{2}{n}) \cdots = \frac{n!}{(n-k)! n^k} \leq e$$

$$\log \left(\frac{n!}{(n-k)! n^k} \right) = \log(n!) - \log((n-k)!) - k \log(n)$$

$$\leq \log(n^k) - k \log(n) = 0$$

$$1+x \leq e^x$$

$$* \leq e^{0 - \frac{1}{n} - \frac{2}{n} - \cdots} = e^{-\frac{1}{n} \left(\frac{k(k-1)}{2} \right)}$$

$$\text{ce je } k = \sqrt{n} = e^{-\frac{1}{n} \left(\frac{n - \sqrt{n}}{2} \right)} = e^{\left(-\frac{1}{2} + \frac{1}{\sqrt{n}} \right)} \leq \frac{1}{2}$$

$$e^{-1} e^{-2} \leq \frac{1}{2} \quad \therefore$$

- a) **odpornost prasl.ike** za dan y je težko najti $x \in X$, da $h(x) = y$
- b) **odpornost drage prasl.ike**: za dan $x \in X$ je težko najti $x' \in X$, da $h(x) = h(x')$
- c) **odpornost na tok** x, x' $x \neq x'$, da $h(x) = h(x')$

$$\textcircled{1} \quad n: a \Rightarrow n: b \quad (\Leftrightarrow b) \vee a) \checkmark$$

- x je dan iščemo x'
 - izračunamo $h(x)$
 - izračunamo z oraklom
 - ali $x \neq x'$?
- rjone $x = x'$ je majhno

$$h(x) = \begin{cases} x & ; 0 \leq x \leq 100 \\ \text{sha}_{256}(x) + 100 & ; \text{sicer} \end{cases} \quad \begin{matrix} h: a \\ \nwarrow \\ \text{memo } b \end{matrix}$$

$$h(x) = \begin{cases} \text{sha}_{256}(k) & ; x = 2k \\ \text{sha}_{256}(k) & ; x = 2k+1 \end{cases} \quad \text{je } a, n: b$$

② $h_1, h_2: \mathbb{N} \rightarrow n$ bitov

$$h_3(x) = (h_1(x) \oplus h_2(x))$$

← stik po bitih

$$h_4(x) = h_1(x) \oplus h_2(x)$$

bolj ali najn
odporna na trke?

h_3 : vse se ohrami

h_4 : lažje je slobo $h_1 > h_2 \Rightarrow$ vse je 0

③ h odporen na trke

Hočemo g , ki je odporna na trke in če
 g odlojemo zaradi bit, n: h odporna na trke

$$g(x) = \begin{cases} h(x) \gg 1 < 1 + 1 & x \in 2\mathbb{N} \\ h(x) \gg 1 < 0 & x \in 2\mathbb{N} + 1 \end{cases}$$