
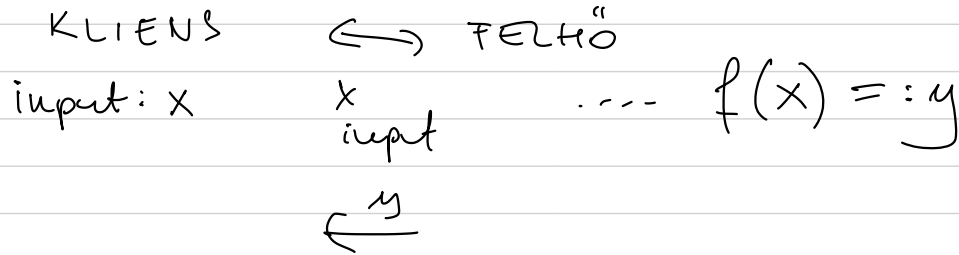


POLINOMOK + KÓDOLÁIS / KRIPTOGRÁFIA



KRIPTO FELADAT

f fu.

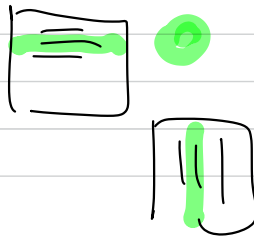


CE: ellenőrizni, hogy $f(x) = y$

VERIFIABLE COMPUTATION

SPEC. ESET: $A \cdot B = C$

$(n \times n$ mátrixok
 n nag)



NAIV $A \cdot B$: $O(n)$ elemenként
 Σ : $O(n^3)$

CEL: igazoljuk $O(n^2)$ lépésben, hogy $A \cdot B == C$

RÖKÖN FELADAT:

A

B

$$\underline{a} = [a_0, a_1, \dots, a_{n-1}]$$

$$b = [b_0, b_1, b_2, \dots, b_n]$$

n nagy

KÉRDÉS:

$$\underline{a} == \underline{b} \quad ??$$

CHECKSUM

$$f := a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$$

$$g := b_0 + b_1 x + \dots + b_{n-1} x^{n-1}$$

$$f(x) == g(x)$$

(+tipikusan mod p
p nagy)

r : véletlen $\in 0, 1, 2, \dots, p-1$

ELLENŐRZÉS: $f(r) == g(r)$??

IGEN

NEM: $f \neq g$

$f = g$
✓

$f \neq g$, csak
véletlenül

$$(f-g)(r) = 0$$

FALS POSITIV : valsz. : $\frac{\text{gyökök száma}}{p} \leq \frac{n}{p}$

EMELK: n -edfokú pol. gyökei száma $\leq n$

↓
Kicsi
 10^{-100}
akár

VISZTA: $A \cdot B \stackrel{?}{=} C$

FREIVALD-ALGO
 $n \times n \quad n \times n$

mod p

r : véletlen szám:

$$A \cdot B \cdot \underline{r} \stackrel{?}{=} C \cdot \underline{r}$$

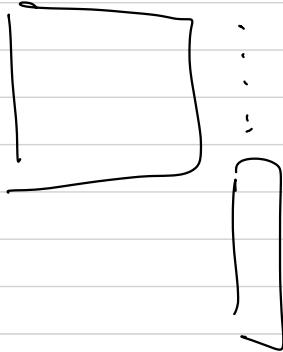
$$\underline{r} : (1, r, r^2, r^3, \dots, r^{n-1})$$

$$\downarrow$$

$$A \cdot (\underline{B \cdot r})$$

$$\uparrow$$

$$O(n^2)$$



AU: Ha $A \cdot B \neq C$

akkor $\text{Prob}(A \cdot B \cdot r = C \cdot r)$

$$\leq \frac{n}{p}$$

FI:

$$2^{10} = 10^3$$

$$\pi \text{ sec} = 1 \text{ nanocentury}$$

$$1 \text{ eV} \approx 3.14 \cdot 10^7 \text{ sec} \left(\frac{30}{\text{millis}} \right)$$

KICS: (2^{100})

Gráfok kérdés megválaszolása polinomiálisan

LEMMA: SCHWARTZ-ZIPPEL LEMMA

TÖBBVÁRTÓZÓS POLINOM: $f(x_1, x_2, \dots, x_n) \pmod{p}$

r_1, r_2, \dots, r_n : véletlen input:

$$\text{Prob} \left[f(r_1, r_2, \dots, r_n) = 0 \right] \leq \frac{d}{p} \quad d: \text{fok}$$

ALK: G gráfban van-e TELJES PÁROSÍTÁS

(EGYIK LEHETSÉGES) VÁLTOZAT:

$$A = \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix}$$

$$a_{ij} = \begin{cases} x_{ij} & \text{ha } i-j \text{ él, } i < j \\ -x_{ji} & \text{ha } i-j \text{ él, } i > j \\ 0 & \text{amúgy} \end{cases}$$

x_{ij} : polinom változó

$$\begin{vmatrix} x & y & z \\ x & y & w \\ y & z & x \end{vmatrix}$$

áll: $\det A = 0 \Leftrightarrow$ nincs párosítás



TESTELHETŐ RANDOM elemek behelyettesítésével.

$$A_{n \times n} = B_{n \times n}$$

$$A \cdot \begin{pmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{n-1} \end{pmatrix} = B \cdot \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{n-1} \end{pmatrix}$$

HIBAFAVÍTÓ KÓDOLÁS EGYIK FÁJTÁJA

Cél: n hosszú üzenet $\longrightarrow n+k$ hosszú üzenet,

ha néhány hiba van,
akkor még el tudjuk olvasni

mod 5, 3 kosziár

Pl. :

(0, 1, 4) \rightarrow

(2, 3, 1)

⋮

$5^3 = 125$ -féle

ELSŐ PRÓBA: $(a, b, c) \mapsto (a, b, c, a+b+c)$

BAZ: $(0, 1, 1) \mapsto (\underline{0}, 1, 1, 2) \overset{?}{\rightarrow} (1, 1, 1, 2)$

$(1, 0, 1) \mapsto (1, \underline{0}, 1, 2) \overset{?}{\rightarrow}$ látom,
hogyan

És : 1-hibajavító: $(a, b, c) \mapsto (a, b, c, a+b+c, a+2b+3c)$

EGY 26 #BAGAVITO KOD OTETE;

äussert: $f(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$ in $\mathbb{R}[x]$



Kód : $\tau_1, \tau_2, \tau_3, \dots, \tau_{n+k}$: $f(r_1), f(r_2), \dots, f(r_{n+k})$
 publikus. helyettesítési értékek

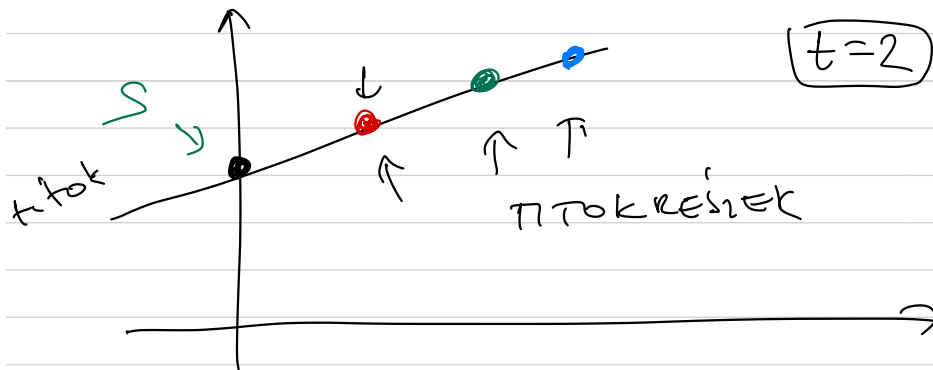
ALAPÖTLET. $(n-1)$ -edfokú polinom kitalálása
 n db helyettesítési értékből (interpoláció)

minden, am melyik a db értéket ismerem, az eredeti polinom kiment.

~~~~~) REED-SOLOMON-COD

$\frac{k-1}{2}$  hiba javítható

TITOKMEGOSZTÁS: CEI: adjak titokrészeket :  $\geq t$  ember : tudja a titkot



$(x_1, f(x_1))$        $(x_2, f(x_2))$        $(x_3, f(x_3))$   
 A                                  B                                  C

$\geq 2$  szereplő összejött: s kitalálható.

$t \geq 2$  :  $(t-1)$ -ed fokú polinom:  $t$  db ( legkevesebb  $t$  db )

