Tutorial 10

10 May 2023 14:06

Algebraic techniques (fingerprinting) 1

→ Frievald's technique for matrix multiplication

→ Polynomial comparison: Schwartz - Zippel thm

→ SZ thm. ⇒ Frievald's technique

Matrix multiplication

Given $n \times n$ matrices A, B and C over a finite field $\mathbb{F}_p$.

Verify whether $A \cdot B = C$

Naive solution:

Multiply $\underbrace{A \cdot B}_{O(n^3)}$ and $\underbrace{\text{compare element by element to } C}_{O(n^2)}$

→ $O(n^{2.373})$

Can we compare $A \cdot B$ with C for smaller price?

1.) Choose $\boxed{\vec{v} \in \{0,1\}^n}$ at random and calculate

$\underbrace{A \underbrace{(B \cdot \vec{v})}_{O(n^2)}}_{O(n^2)}$ and $\underbrace{C \cdot \vec{v}}_{O(n)^2}$ and compare the results $O(n)$

2.) If results are equal Alg. outputs 'YES'

—— " —— different A's. outputs 'NO'

3.) output NO $\Rightarrow$ $A \cdot B \neq C$ w.p. 1

output YES $\Rightarrow$ $A \cdot B \neq C$ w.p. $\leq 1/2$

ANALYSIS:

$\rightarrow$ We can reduce the problem to finding whether $D = A \cdot B - C$ is identically 0 $D = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \end{pmatrix}$

$\rightarrow$ $D \cdot \vec{r} = \vec{0}$ for all strings $\vec{r}$

$\rightarrow$ $D \neq 0 \Rightarrow D$ has a non-zero element

$$P_r(\text{Algorithm outputs 'YES'} \mid D \neq 0)$$

WLOG we assume that d_{00} is non-zero.

Let's calculate the first element of $\vec{e} = D \cdot \vec{r}$

$\vec{e} = (e_0, \dots, e_{n-1})$

$$e_0 = d_{00} \cdot r_0 + d_{01} \cdot r_1 + \dots + d_{0n-1} \cdot r_{n-1} \stackrel{?}{=} 0$$

$$r_0 = \frac{d_{01} \cdot r_1 + \dots + d_{0n-1} \cdot r_{n-1}}{-d_{00}}$$

for all $(r_1, \dots, r_{n-1})$ R.H.S. is a fixed value in $\{0, \dots, p-1\}$

r_0 is chosen from $\{0,1\}$

$$Pr(e_0 = 0 \mid D \neq 0) \leq 1/2 .$$

Is the choice of $\vec{v} \in \{0,1\}^n$ special?

How about $\vec{v} \in (S)^n_i ; S \subseteq \mathbb{F}_p$ $|S| = 2$

$|S| = k$ $Pr(\text{error}) \leq 1/k$

Polynomials

$p(x) \in \mathbb{F}_p[x]$ (set of all polynomials over $\mathbb{F}_p$)

$$p(x) = \sum_{i=0}^{\infty} a_i x^i \mod p \quad \forall_i \; a_i \in \mathbb{F}_p$$

$$\boxed{\begin{array}{l} 3x^2 + 7x + 782x^2 + 3 \\ + 9 + 8 \mod 3 \end{array}}$$

- Is polynomial $p(x)$ identically 0?
- Are $p_1(x)$ and $p_2(x)$ equal?

$$p_1(x) - p_2(x) \equiv 0 \; ?$$

- $P_1(x) \cdot P_2(x) \stackrel{?}{=} P_3(x)$

$$P_1(x) \cdot P_2(x) - P_3(x) \equiv 0$$

$\rightarrow$ if $p(x) \equiv 0$, then $\forall a \in \mathbb{F}_p$ $P(a) = 0 \mod p$

$\rightarrow$ if $p(x) \equiv 0$, then $\forall a \in \mathbb{F}_p \quad P(a) = 0 \mod p$

if $p(x) \not\equiv 0$, then how many $a \in \mathbb{F}_p$ give $P(a) = 0$?

number of roots $\leq$ $\boxed{\text{degree of } p(x) = \text{highest exponent}}$

$\boxed{\text{Algorithm}}$

Choose $r \in S \subseteq \mathbb{F}_p$ at random and evaluate $P(r)$

if $P(r) = 0$ then say $P(x) \equiv 0$ otherwise $P(x) \not\equiv 0$.

$$P_r(\text{error}) \leq \frac{\#\text{roots}}{|S|} = \frac{\text{degree}(P(x))}{|S|}$$

Similar claim exists for multivariate polynomials = Schwartz-Zippel thm

$P[x_1, \dots, x_n] \in \mathbb{F}_p[x_1, \dots, x_n]$

$$p[x_1 \dots, x_n] = a_{\underbrace{000\,000}_{r}} + a_{1000\dots} x_1 + a_{0100\dots} x_2 + \dots$$

$$\dots + a_{11000}(x_1 \cdot x_2) + \dots \quad a_{e_1 e_2 \dots e_n} \cdot x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$$

$a_{e_1 \dots e_n} \in \mathbb{F}_p$

$x_1^2 x_2^3 x_3 x_n \rightsquigarrow$ polynomial terms

$x_1^2 x_2^3 x_3 x_7$ ⇝ polynomial terms

$$\deg(x_1^2 x_2^3 x_3 x_7) = 7$$

Total degree $P(x_1, \dots, x_n)$ = the largest degree over all it's terms.

Schwartz-Zippel thm.

Let $Q[x_1, \dots, x_n] \in \mathbb{F}_p[x_1, \dots, x_n]$ of total degree d.

Fix any $S \subseteq \mathbb{F}_p$ and let $r_1, \dots, r_n$ be chosen at random from S.

then:

$$\boxed{\Pr\left(Q(r_1, \dots, r_n) = 0 \mid Q(x_1, \dots, x_n) \not\equiv 0 \right) \leq \frac{d}{|S|}}$$

Proof by induction in the number of variables

I.B. done above

I.H. this holds for $n-1$ variables

I.S. show that this also holds for n variables

$$Q(x_1, \dots, x_n) = \sum_{i=0}^{k} Q_i(x_1, \dots, x_{n-1}) \cdot x_n^i$$

$Q(x_1, x_2) = x_1 x_2 + 3x_1 x_2^7 + 5x_1 x_2^3$
$+ x_1^2 x_2 + 7 \cdot x_1^2 x_2^4 + 3x_1^2 x_2^3$

$$Q(x_1, \dots, x_n) = \sum_{i=0} Q_i(x_1, \dots, x_{n-1}) \cdot x_n^i$$

Principle of deferred decision allows us to choose $\boxed{r_1, \dots, r_{n-1}}$ before choosing r_n.

$$+ x_1^2 x_2 + 7 \cdot x_1^2 x_2^4 + 3 x_1^2 x_2^3 + x_2 + x_2^3$$

$$= x_1 \cdot \underbrace{\left(x_2 + 3x_2^7 + 4x_2^3\right)}_{Q_1} + x_1^2 \cdot \underbrace{\left(x_2 + 7x_2^4 + 3x_2^3\right)}_{Q_2}$$

$$\underbrace{x_2 + x_2^3}_{Q_0}$$

$$q(x_n) = Q(r_1, \dots, r_{n-1}, x_n) = \sum_{i=0}^{k} x_n^i \, Q_i(r_1, \dots, r_{n-1})$$

if $Q \not\equiv 0$ there is at least one value i, such that $Q_i \not\equiv 0$

Let k be largest such i

$$\boxed{P_r\left(q(r_n) = 0 \mid Q_k\{r_1, \dots, r_n\} \not\equiv 0, Q \not\equiv 0\right] < \frac{k}{|S|}}$$

From I.H.

$$\boxed{P_r\left[Q_k\{r_1, \dots, r_{n-1}\} = 0 \mid Q \not\equiv 0\right] \leq \frac{d-k}{|S|}}$$

This implies the S.Z. thm

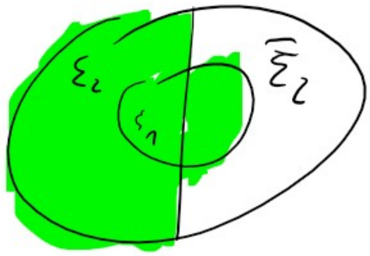
For two events

$$\mathcal{E}_1 = \left[q(r_n) = 0 \mid Q_k(r_1, \dots, r_n) \not\equiv 0, Q \not\equiv 0\right]$$

$$\mathcal{E}_2 = \left[Q_k(r_1, \dots, r_n) = 0 \mid Q \not\equiv 0\right]$$

$$\frac{k}{|S|} + \frac{d-k}{|S|} = \frac{d}{|S|}$$

$$\Pr[\mathcal{E}_1] \le \Pr[\mathcal{E}_1 \mid \bar{\mathcal{E}}_2] + \Pr[\mathcal{E}_2]$$



if in $Q[x_1, \dots, x_n]$ $\deg(x_i) = d_i$

and $r_i \in S_i \subseteq \mathbb{F}$

$$\Pr[Q[x_1, \dots, x_n] = 0 \mid Q \not\equiv 0] \le \frac{d_1}{|S_1|} + \frac{d_2}{|S_2|} + \dots + \frac{d_n}{|S_n|}$$

if all $|S_i|$ are identical $\frac{\sum_i d_i}{|S|} \ge \frac{d}{|S|}$

SZ $\Rightarrow$ Frievald's technique

F.t. $Q\begin{pmatrix} a_{00} & \dots & a_{0n-1} \\ & & \\ a_{n-1\,0} & \dots & a_{nn} \end{pmatrix}$ is identically 0

$Q[x_0, \dots, x_{n-1}]$ $\quad Q\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}$

$= a_{00}x_0 + a_{01}x_1 + \dots + a_{0n-1}x_{n-1}$

$\cdot \left(\right. + a_{10}x_0 + a_{11}x_1 + \dots +$

$+$

for $Q \equiv 0 \implies Q\{x_0 \cdots x_{n-1}\} \equiv 0$

from S-Z

$$\Pr\{Q\{r_0, \dots, r_{n-1}] \mid Q[x_1, \dots, x_{n-1} \not\equiv 0]\} \leq \frac{\deg Q}{|S|} = \frac{1}{2}$$