Algebraic techniques
20 May 2021 16:09

ALGEBRAIC TECHNIQUES

→ Freivald's technique for matrix multiplication

→ Polynomial comparison: $\boxed{\text{Schwartz-Zippel thm}}$

→ SZ thm. ⇒ Freivald's technique

Matrix comparison

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

Finite fields are finite set of numbers with well defined multiplication and addition. They exist for all prime-power sizes. $\mathbb{F}_p$ for prime p. $\mathbb{F}_p = \{0, \dots, p-1\}$, and $\times$, $+$ mod p

Verify whether $A \cdot B = C$

Naive solution:

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

$[O(n^{2.373})]$

Suppose you want to check whether your matrix multiplication

Suppose you want to check whether your matrix multiplication alg. works correctly. With randomized techique $A \cdot B \overset{?}{=} C$ can be verified in $O(n^2)$

Alg.

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

$$\underbrace{A \cdot \underbrace{(B \cdot \vec{r})}_{O(n^2)}}_{O(n^2)} \quad \text{and} \quad \underbrace{C \cdot \vec{r}}_{O(n^2)}$$

$\overbrace{\text{and compare}}^{O(n)}$ the the results

$$(A \cdot B - C) \cdot \vec{r} \overset{?}{=} \vec{0}$$

2.) If the results are equal, alg. outputs "YES" if not then output "NO"

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

output YES $\Rightarrow A \cdot B \neq C$ w.p. smaller or equal to $1/2$.

ANALYSIS:

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

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

$\to D \neq 0 \Rightarrow D$ has a non-zero element $\qquad 0, p, 2p, \ldots, kp$

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

WLOG assume that non-zero element of D is in top left corner

$$D = \begin{pmatrix} \boxed{d_{00}}^{\neq 0} & d_{01} & \cdots & d_{0n-1} \\ d_{100} & & & \\ \cdot & & d_{ij} \neq 0 & \\ \cdot & & & d_{n-1,n-1} \end{pmatrix}$$

The argument can be formulated for all non-zero elements d_{ij}.

Let's calculate the first element of $e = (e_1, \ldots, e_n)$

$e = D \cdot \vec{r}$ (if e is all zero, alg. says 'YES')

$$e_1 = d_{00} r_0 + \underbrace{d_{02} r_2 + \cdots + d_{0n-1} r_{n-1}} = 0$$

$\Updownarrow$

$$\boxed{r_0} = \frac{d_{01} r_1 + d_{02} r_2 + \cdots + d_{0n-1} r_{n-1}}{-d_{00}} \bmod p$$

non-zero

$$r_j = \frac{d_0 v_0 \cdots + d_{j-1}}{d_{ij}}$$

for all $(r_1, r_2, \ldots r_{n-1})$ R.H.S is fixed value $\{0, 1, \ldots, p-1\}$

(principle of deffered decision)

r_0 is chosen from $\overset{S}{\{0, 1\}}$. $\qquad r_0 \in \{s_0, s_1, s_2\}$

$Pr(e = 0 \mid D \neq 0) \leq 1/$

$$\boxed{Pr(e_1 = 0 \mid D \neq 0) \leq 1/2.}$$

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

$\{2,3\}$

How about $r \in S \subseteq \mathbb{F}_p$ $|S| = 2$

How about $r \in S \subseteq \mathbb{F}_p$ $|S| = k$

$Pr(\text{error}) \leq \boxed{1/k}$

Note that this technique can be used for any matrix identity

$X \stackrel{?}{=} Y$ if X and Y are given explicitely

POLYNOMIALS

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

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

- $\boxed{\text{Is polynomial } p(x) \text{ identically } 0?}$

$3x^2 + 7x + x + 78x^2 + 3 + 5 + 8 + \dots$
$\dots \bmod 3$
$\equiv$
0 ?

- Are $P_1(x)$ and $P_2(x)$ equal?
  $P_1(x) - P_2(x) \equiv 0$?

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

  $P_1(x) \cdot P_2(x) - P_3(x) \overset{?}{\equiv} 0$

→ if $p(x) \equiv 0$, then $\forall a \; P(a) = 0$

→ if $p(x) \not\equiv 0$, how many a give $P(a) = 0$?

↓

roots of polynomial

$P(x)$ has at most $\deg(P(x))$ distinct roots.

↓

the highest exponent

Algorithm

↓

Choose $r \in S \subseteq \mathbb{F}$ at random and evaluate
$P(r)$. if $P(r) = 0$ say $P(x) \equiv 0$, otherwise $P(x) \not\equiv 0$.

$$\Pr(\text{error}) \leq \frac{\#\text{roots}}{|S|} = \frac{\deg(P(x))}{|S|} \leq \frac{n}{|S|} \quad \text{if } \deg(P(x)) = n)$$

$$\Pr(\text{error}) \le \frac{\#\text{roots}}{|S|} = \frac{\deg(P(x))}{|S|} \le \frac{n}{|S|} \qquad (\deg(P(x)) = n)$$

Similar argument for multivariate polynomials

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

$$P[x_1, \dots, x_n] = C_{\underbrace{0000}_{n}} + C_{10000}\, x_1 + C_{01000}\, x_2 + \dots + C_{000\dots1}\, x_n +$$
$$+ \, C_{1100\dots}(x_1 \cdot x_2) + \dots + C_{a_1 a_2, \dots a_n}\, x_1^{a_1} \cdot \dots \cdot x_n^{a_n}$$

$$C_{i \dots n} \in \mathbb{F}_p \qquad \bmod p$$

$x_1^2 x_2^3 x_3 x_7 \rightsquigarrow$ polynomial term

$\deg(x_1^2 x_2^3 x_3 x_7) = 7$ (sum of all exponents)

$\boxed{\text{Total degree of } P(x_1, \dots, x_2)}$ = the largest degree over all terms

Schwartz-Zippel thm

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

Fix any $S \subseteq \mathbb{F}$ and let $v_1, \dots, v_n$ to be chosen at random from S.

then:

$$\boxed{\Pr\left[Q(r_1,\dots,r_n)=0 \;\middle|\; Q(x_1,\dots,x_n)\not\equiv 0\right] \le \frac{d}{|S|}}$$

Proof by induction in the number of variables

I.B. done above

I.H. this holds for n-1 variables

I.S. show it holds for n variables

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

$$Q(x_1,x_2) = x_1x_2 + 3x_1x_2^7 + 4x_1x_2^3 + x_1^2x_2 + 7x_1^2x_2^4 + 3x_1^2x_2^3 + x_2 + x_2^3$$

$$= \underbrace{x_1\cdot(x_2+3x_2^7+4x_2^3)}_{Q_1[x_2]} + \underbrace{x_1^2(x_2+7x_2^4+3x_2^3)}_{Q_2[x_2]} + \underbrace{(x_2+x_2^3)}_{Q_0[x_2]}$$

$$q(x_n) = Q[r_1,\dots,r_{n-1},x_n]$$

$$\deg(q) = k \qquad = x_n^k \cdot Q_k(x_1,\dots,x_{n-1}) + x_n^{k-1} \cdot Q_{k-1}$$

$$\Pr\left[q(r_n)=0 \;\middle|\; Q_k[r_1,\dots,r_{n-1}]\neq 0\right] \le \boxed{\frac{k}{|S|}}$$

$$\Updownarrow$$

$$Q[x_1,\dots,x_n]\not\equiv 0$$

from I.H.

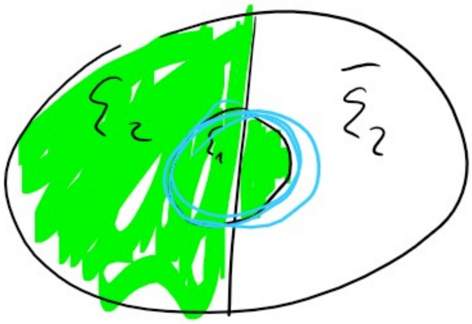
$$\Pr\left[Q_k[r_1,\dots,r_{n-1}]=0\right] \le \boxed{\frac{d-k}{|S|}}$$

This implies the result

For two events $\mathcal{E}_1 = [q(r_n) = 0]$

$$\mathcal{E}_2 = Q_2[r_1, \ldots, r_{n-1}] = 0$$

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



Pr{

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

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

$$\Pr[Q[r_1, \ldots, r_n] = 0 \mid Q \not\equiv 0] \le \frac{d_1}{|S_1|} + \frac{d_2}{|S_2|} + \cdots + \frac{d_n}{|S_n|}$$

if all $|S_i|$ are identical $= \dfrac{\sum_i d_i}{|S|} \ge \dfrac{d}{|S|}$ of SZ q

SZ => Freivald's matrix equality

SZ => Freivald's matrix equality

F.t. $Q = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$ is identically 0?

$Q[x_1, \ldots, x_n) = Q \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n$

$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n$

$\vdots$

$a_{n1}x_1 + \cdots \quad \cdots a_{nn}x_n$

for $Q \equiv 0 \iff Q[x_1, \ldots, x_n] \equiv 0$

Choose $r \in \{0,1\}^n$ $Q \cdot r = 0 \iff Q[r_1, \ldots, r_n] = 0$

From S-Z theorem

$$\Pr\{Q[r_1, \ldots, r_n] = 0 \mid Q[x_1, \ldots, x_n] \neq 0\} \leq \frac{\deg Q}{|S|} = \frac{1}{2}$$