Tutorial XI

30 April 2020 14:02

Algebraic techniques

- → Freivald's technique for matrix multiplication
- → Polynomial comparison: Schwartz-Zippel theorem
- → 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. For prime p $\mathbb{F}_p = \{0, \dots, p-1\}$ and $+, \times$ mod p.

$\mathbb{F}_p$ exist only for prime power p.

Verify whether

$$A \cdot B = C$$

Multiply $A \cdot B$ and compare to C.

$O(n^3)$ $[O(n^{2.373})]$ ←

Suppose you want to check whether your matrix multiplication algorithm works correctly. With randomized technique we can solve the problem in $O(n^2)$.

Alg.

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

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

2.) • If the vectors are equal, alg. says matrices are equal $(A.B = C)$

• if not than $A \cdot B \neq C$

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

output YES $\Rightarrow$ 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 $\quad D = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$

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

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

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

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

$D = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 0 & \ddots & & \\ & & & 0 \end{pmatrix}$, $a_1 \neq 0$

The argument can be formulated for any position of non-zero element.

The argument can be formulated for any position of non-zero element.

lets calculate the first element of

$e = D.\vec{r}$ (if e is all zero's ALG says 'YES')

$e_1 = d_{11} \cdot v_1 + d_2 \cdot v_{2-1} \dots + d_n \cdot v_n$ (if equal to zero we get wrong answer)

$v_1 = \frac{d_2 v_2 + \dots + d_n v_n}{-d_1}$ (nonzero)

R.H.S is a fixed value (principle of delay (deffered decision))

v_1 is chosen from $\{0,1\}$.

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

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

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

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

$\Downarrow$

Pr of error $\leq \frac{1}{k}$

Note that this technique can be used for any matrix identity $X \stackrel{?}{=} Y$ if X and Y are given explicitly

Example:

$$\begin{pmatrix} 1237 & 4798 \\ 891 & 932 \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 8 & 7 \\ 14 & 98 \end{pmatrix}$$

mod 3

$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

mod 3

(0, 1, 2)

Example:

$$\begin{pmatrix} 1237 & 4798 \\ 891 & 932 \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 8 & 7 \\ 14 & 98 \end{pmatrix} \mod 3$$

$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

mod 3 (0,1,2)

$$4798 + 932 = 98 + 7 \mod 3$$

Polynomials

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

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

- Is polynomial $P(x)$ identically 0?

$3x^2 + 7x + x + 78x^2 + 3 + 9 + 8 + \ldots + \mod 3 \stackrel{?}{\equiv} 0$

- Are $P_1(x)$ and $P_2(y)$ equal?

  $P_1(x) - P_1(x) \stackrel{?}{\equiv} 0$

  $3x^2 + 7x^2 + \ldots$

  $4y^2 + 6y^2 + \ldots$

- verify whether $P_1(x) \cdot P_2(x) = P_3(x)$

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

→ if $P(x)$ is identically 0, then $\forall a,\ P(a) = 0$

→ if $P(x)$ is not identically 0? How many a give $P(a) = 0$?

↓ roots of polynomials?

$P(x)$ has exactly $\deg(P(x))$ → the highest exponent

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

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

Similar argument for multivariate polynomials

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

$$P[x_1, \dots, x_n] = C_{\underbrace{00000}_{n}} + C_{\underbrace{100\dots}_{n-1}} x_1 + C_{\underbrace{010\dots0}_{n-2}} x_2 + C_{110\cdots00}(x_1 \cdot x_2) + \dots + C_{a_1 \cdots a_n} x_1^{a_1} \cdots x_n^{a_n}$$

$x_1 x_2^2 x_3^3 x_7 \rightarrow$ this is a polynomial term

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

Total degree of $P[x_1, \dots, x_n]$ = the largest degree over all the 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 $r_1, \dots, r_n$ to be chosen at random from S. Then:

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

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

Let highest degree of x_n in Q be $k \le d$

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

Q_i contains all terms with x_n with power i

$$Q[x_1,x_2] = x_1x_2 + 3x_1x_2^7 + 4x_1x_2^3 + x_1^2x_2 + 7x_1^2x_2^4 + 3x_1^2x_2^3 + x_2 + x_2^3$$

$$= x_1[x_2 + 3x_2^7 + 4x_2^3] = Q_1[x_2]$$

$$+ x_1^2[x_2 + 7x_2^4 + 3x_2^3] = Q_2[x_2]$$

$$+ [x_2 + x_2^3] = Q_0[x_2]$$

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

$$\deg(q) = k$$

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

($\le k$ roots)

from IH

$$\Pr[Q_k[r_1,\dots,r_n] = 0] \le \frac{d-k}{|S|}$$

This implies the result.

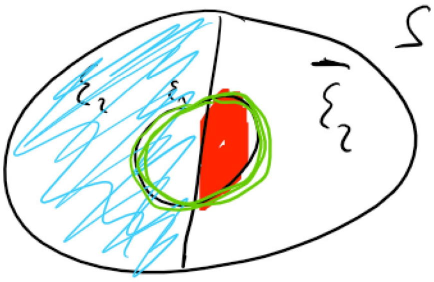
For two events $E_1 = q(r_n) = 0$, $E_2 = Q_k[r_1,\dots,r_n] = 0$

for an E_1 E_2

... [events] ε_1 : ... $= 0$ $\quad \varepsilon_2 : Q_2(r_1, \dots, r_n) = 0$

for any $\varepsilon_1, \varepsilon_2$

$$\Pr[\varepsilon_1] \leq \Pr[\varepsilon_1 \mid \bar{\varepsilon}_2] + \Pr[\varepsilon_2]$$



Homework

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

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

Probability that $Q[r_1, \dots, r_n] = 0$ given $Q \not\equiv 0$

is upper bounded by $\dfrac{d_1}{|S_1|} + \dfrac{d_2}{|S_2|} + \dots + \dfrac{d_n}{|S_n|}$

all S_i are identical

$= \dfrac{\sum_i d_i}{|S|} > \dfrac{d}{|S|}$ $\quad$ ↙ value from S-Z theorem

$x_1^2 x_2^1 + x_1^1 x_2^2$

total degree is 3

and $d_1 + d_2 = 4$

S-Z $\Rightarrow$ Freivald's technique

F.f. = decide whether an $n \times n$ matrix $Q = \begin{pmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & & \\ q_{n1} & \cdots & q_{nn} \end{pmatrix}$

is identically 0.

Define $Q[x_1, \dots, x_n] = Q \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$$= q_{11}x_1 + q_{12}x_2 + \dots + q_{1n}x_n$$
$$+ q_{21}x_1 + q_{22}x_2 + \dots + q_{2n}x_n$$
$$\vdots$$
$$+ q_{n1}x_1 + q_{n2}x_2 + \dots + q_{nn}x_n$$

for Q identically 0 matrix $\Leftrightarrow$ $Q[x_1, \dots, x_n]$ is a zero polynomial

Choose $v \in \{0,1\}^n$ and from S-Z theorem

$$\Pr\left[Q[v_1, \dots, v_n] = 0 \mid Q[x_1, \dots, x_n] \neq 0\right] \leq \frac{\deg Q}{|S|} = \frac{1}{2}$$