Tutorial XI

16 May 2019 12:04

Algorithmic techniques

- Freivald's technique for matrix identities
- Polynomial comparison Schwartz-Zippel theorem
- S-Z thm ⇒ Freivald's technique

Freivald's technique for matrix comparison

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

for prime p these are $\{0, \dots, p-1\}$ with operations $\times$ and $+$ mod p

Verify

$$A \cdot B = C$$

Multiplication of A and B takes $O(n^3)$ $\left[O(n^{2.373})\right]$

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

Alg.

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

$A \cdot (B\vec{r})$ and $C \cdot \vec{r}$ and compare the results

2.) Alg says no ⇒ $A \cdot B \neq C$ w.p. 1

2.) Alg says no $\Rightarrow A \cdot B \neq C$ w.p. 1

→ 3.) $A \cdot B \neq C$ and alg says 'yes' w.p. smaller or equal to $1/2$

(wrong answer)

Analysis:

→ We can reduce the problem to finding out whether

$D = A \cdot B - C$ is identically 0 $\quad D = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$

$D \cdot \vec{r}$ should be 0 for all strings

→ if $D \neq 0 \Rightarrow$ there is a non-element.

$Pr(\text{Algorithm gives answer 'equal'} \mid D \neq 0)$

WLOG assume that non-zero element of D is in top left corner. (the argument can be done for any position)

denote $\vec{d} = (d_1, \ldots, d_n)$ the first row of D.

this is the non-zero element.

$\begin{pmatrix} d_1 & \cdots & d_n \\ & & \\ & & \end{pmatrix}$

Take a look at the first element of

$\rho = D \cdot \vec{r}$

$\rho_1 = d_1 r_1 + d_2 r_2 + \cdots + d_n r_n$

$0 \stackrel{?}{=} d_1 r_1 + d_2 r_2 + \cdots + d_n r_n$

$r_1 = \dfrac{d_2 r_2 + \cdots + d_n r_n}{-d_1}$ → 0 non-zero

R.H.S is a fixed value.

r_1 is chosen randomly from $\{0,1\}$.

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

$P(\text{algorithm says yes} \mid A \cdot B \neq C)$

$P(A \cdot B \neq C \mid \text{algorithm says yes})$

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

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

How about $r \in S \subseteq \mathbb{F}$ $|S| = k \Rightarrow$ Pr of incorrect result is $\frac{1}{k}$

$r_1 \in S \subseteq \mathbb{F}$ and $r_2, \ldots, r_n \in \{0,1\}$

φ

Note that this technique can be used for any matrix identity $X \stackrel{?}{=} Y$. If X and Y are given explicitly this takes $O(n^2)$

Polynomials

$P(x) \in \mathbb{F}_p[x]$ (polynomial over a finite field $\mathbb{F}_p$)

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

Given three polynomials $P_1(x), P_2(x), P_3(x)$

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

$\deg(P_1(x)) \leq n$

$\deg(P_2(x)) \leq n$

choose $r \in S \subseteq \mathbb{F}_p$ and calculate

$P_1(r), P_2(r), P_3(r)$, verify whether $P_1(r) \cdot P_2(r) = P_3(r)$

Can be rephrased

$P_1(x) \cdot P_2(x) - P_3(x)$ identically 0?

Wrong answer if r is a root of $P_1(x) \cdot P_2(x) - P_3(x)$

$$P_r(\text{wrong answer}) = P_r(r \text{ is a root of } P_1(x) \cdot P_2(x) - P_3(x)) \leq \frac{\#\text{roots}}{|S|} = \frac{\deg(P_1(x) \cdot P_2(x) - P_3(x))}{|S|} \leq \frac{2n}{|S|}$$

Similar argument can be made for multivariable polynomials.

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

$$P[x_1, \dots, x_n] = c_{0000\dots0} + c_{100\dots0} x_1 + c_{010\dots0} x_2 + \dots + c_{110\dots0} x_1 \cdot x_2 + c_{a_1 \dots a_n} x_1^{a_1} \cdots x_n^{a_n}$$

$x_1^2 x_2^3 x_3 x_7$ → this is called a polynomial term

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

Total degree of $P(x_1 \dots x_n)$ = the largest degree over all terms.

Schwartz-Zippel thm

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

Let $Q(x_1, \dots, x_n)$ [illegible]

Fix any $S \subseteq F$ and let $r_1, \dots, r_n$ be chosen independently at random from S. Then:

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

Proof: Induction w. respect to the number of variables

I.B. - done above

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

I.S. - show for n variables.

Let highest degree of x_1 be $k \leq d$

$$Q[x_1, \dots, x_n] = \sum_{i=0}^{k} x_1^i Q_i(x_2, \dots, x_n)$$

Q_i contains all terms with x_1 with power i

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

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

$$= Q_1[x_2] + Q_2[x_2] + Q_0[x_2]$$

$$q[x_1] = Q[x_1, r_2, \dots, r_n]$$

$\deg[q] = k$

$$\Pr[q(r_1) = 0 \mid Q_k[r_2, \dots, r_n] \neq 0] \leq \frac{k}{|S|}$$

from IH

$$\Pr[Q_k[r_2, \dots, r_n] = 0] \leq \frac{d-k}{|S|}$$

implies the result because for 2 events $\mathcal{E}_1, \mathcal{E}_2$

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

Homework:

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

and $r_i \in S_i \subset F_i$

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

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

for all S_i identical

$$= \frac{\sum_i d_i}{|S|} > \frac{d}{|S|}$$

$x_1^2 x_2 + x_1 x_2^2$

total degree $= 3$

$d_1 + d_2 = 4$

S-Z thm. $\Rightarrow$ Frievald's technique

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

is identically 0.

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

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

$$= \begin{matrix} a_{11}x_1 + a_{12}x_2 + \cdots a_{1n}x_n \\ + a_{21}x_1 + a_{22}x_2 + \cdots a_{2n}x_n \\ \vdots \\ a_{n1}x_1 + \cdots a_{nn}x_n \end{matrix}$$

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

choose $r \in \{0,1\}^n$ $\leftarrow$

and from S-Z theorem

$$Pr\left[Q[r_1 \dots r_n] = 0 \;\middle|\; Q[x_1 \dots x_n] \not\equiv 0 \right] \leq \frac{\deg(Q)}{|S|} = \frac{1}{2}$$