Tutorial 12

12 May 2022 09:02

Algebraic techniques (fingerprinting)

- Frievald's technique for matrix multiplication ✓
- Polynomial comparison: Schwartz-Zippel thm
- SZ thm. $\Rightarrow$ Frievald's technique. ✓

Matrix multiplication

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

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

Verify whether $\boxed{A \cdot B = C}$

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 a new multiplication algorithm is correct. With randomized technique $A \cdot B \stackrel{?}{=} C$ can be done in $O(n^2)$.

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

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

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

2.) If the results are equal alg. outputs 'YES' &
if not alg. 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 $\quad D \stackrel{?}{=} \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$

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

$\rightarrow$ $D \not\equiv 0 \Rightarrow D$ has an non-zero element

$\Pr(\text{Algorithm outputs 'YES'} \mid D \not\equiv 0)$

WLOG assume that the non-zero element of D is the element d_{00}.

Let's calculate the first element of $\vec{e} = D \cdot \vec{r}$ $\quad \vec{e}\,(e_0, e_1, \dots, e_{n-1})$

$$e_0 = \boxed{\begin{matrix}\not\phi \\ d_{00}\end{matrix}} \cdot r_0 + d_{01} \cdot r_1 + d_{02} \cdot r_2 + \dots + d_{0n-1}\, r_{n-1} \stackrel{?}{=} 0$$

$$r_0 = \frac{d_{01} \cdot r_1 + d_{02} \cdot r_2 + \dots + d_{0n-1} \cdot r_{n-1}}{-d_{00}}$$

for all $(r_0 \dots r_{n-1})$ R.H.S is a fixed value in $\{0, \dots, p-1\}$ $\mathbb{F}_p$

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

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

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

How about $\vec{r} \in S \subseteq \mathbb{F}_p^n$ $\{1,3\}^n$ $|S| = 2$

How about $\vec{r} \in S \subseteq \mathbb{F}_p^n$ $|S| = k \Rightarrow \Pr(\text{error}) \leq 1/k$

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

Polynomials

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

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

$3x^2 + 7x + 78x^3 + 3 \cdot c$

$3x^2 + 7x + 78x^2 + 3x + 9 + 8 \mod 3$

- Is polynomial $p(x)$ identically 0?
- Are $P_1(x)$ and $P_2(x)$ equal?

$$P_1(x) - P_2(x) \equiv 0 \; ? \quad ✓$$

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

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

→ 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 $P_r(0) = 0$ say $P(x) \equiv 0$, otherwise $P(x) \not\equiv 0$.

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

Similar argument for multivariate polynomials exists: Schwartz-Zippel thm

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

$$P\{x_1, \dots x_n\} = \underbrace{c_{0000}}_{n} + \underbrace{c_{1000}}_{n} x_1 + \underbrace{c_{0100}}_{n} x_2 + \dots + \underbrace{c_{0001}}_{n} x_n$$
$$+ c_{1100}(x_1 \cdot x_2) - - - c_{a_1 a_2 \dots a_n} x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$$

$c_{a_1 \dots a_n} \in \mathbb{F}_p$

$x_1^2 x_2^3 x_3 x_7 \rightsquigarrow$ 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:
$$\Pr\left(Q(r_1, \dots, r_n) = 0 \mid Q(x_1, \dots, x_n) \not\equiv 0\right) \leq \frac{d}{|S|}$$

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 holds for n variables

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

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

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

$= x_1 \cdot \boxed{(x_2 + 3x_2^7 + 4x_2^3)}\ Q_1$
$+ x_1^2 \boxed{(x_2 + 7x_2^4 + 3x_2^3)}\ Q_2$
$+ (x_2 + x_2^3)\ Q_0$

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

If $Q \not\equiv 0$ then there is at least one value i, such that $Q_i \not\equiv 0$. Let k be largest such i

$$\boxed{\Pr(q(r_n) = 0 \mid Q_k[r_1, \dots, r_{n-1}] \neq 0, Q \not\equiv 0) < \frac{k}{|S|}}$$

from I.H.

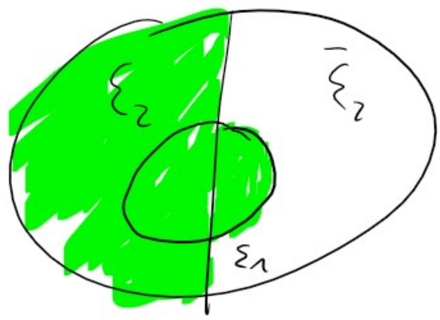
$$\boxed{\Pr[Q_k[r_1, \dots r_{n-1}] = 0 \mid Q \not\equiv 0] \leq \frac{d-k}{|S|}}$$

This implies the result.

For two events $\mathcal{E}_1 = (q(r_n) = 0 \mid Q \not\equiv 0)$

$\mathcal{E}_2 = (Q_k(r_1, \dots, r_{n-1}) = 0 \mid Q \not\equiv 0)$

$$\Pr\{\mathcal{E}_1\} \leq \Pr\{\mathcal{E}_1 \mid \overline{\mathcal{E}_2}\} + \Pr\{\mathcal{E}_2\}$$



$\boxed{\text{QED}}$

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

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

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

if all $|S_i|$ are identical $= \frac{\sum_i d_i}{|S|} \geq \frac{d}{|S|}$ ↯

SZ ⇒ Frievald's matrix equality

F.t. $Q\begin{pmatrix} a_{00} & \dots & a_{1n} \\ \vdots & & \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ is identically 0?

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

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

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

$$+ a_{10} x_0 + a_{11} x_1 + \cdots a_{1\,n-1} x_{n-1}$$

$$\vdots$$

$$a_{n-1\,0} x_0 + \cdots \quad \cdots \quad a_{n-1\,n-1} x_{n-1}$$

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

From S-Z

$$\Pr\left[Q[r_1, \ldots, {}_n] = 0 \,/\, Q[x_1, \ldots, x_n] \neq 0 \right] \leq \frac{\deg Q}{|S|} = \frac{1}{2}.$$