Advanced Algorithms

南京大学

尹一通

Polynomial Identity Testing (PIT)

Input: two polynomials $f, g \in \mathbb{F}[x]$ of degree d

Output: $f \equiv g?$

$f \in \mathbb{F}[x]$ of degree d : $\quad f(x) = \sum_{i=0}^{d} a_i x^i$ for $a_i \in \mathbb{F}$

Input: a polynomial $f \in \mathbb{F}[x]$ of degree d

Output: $f \equiv 0?$

f is given as black-box

Input: a polynomial $f \in \mathbb{F}[x]$ of degree d

Output: $f \equiv 0?$

simple deterministic algorithm:

check whether $f(x)=0$ for all $x \in \{1, 2, \ldots, d+1\}$

Fundamental Theorem of Algebra:

A degree d polynomial has at most d roots.

pick a uniform random $r \in S$;

check whether $f(r) = 0$;

$S \subseteq \mathbb{F}$

pick a uniform random $r \in S$;

check whether $f(r) = 0$;

$S \subseteq \mathbb{F}$

$|S| = 2d$

if $f \not\equiv 0$

$$\Pr[f(r) = 0] \leq \frac{d}{|S|} = \frac{1}{2}$$

Fundamental Theorem of Algebra:

A degree d polynomial has at most d roots.

Checking Identity

北京

database 1

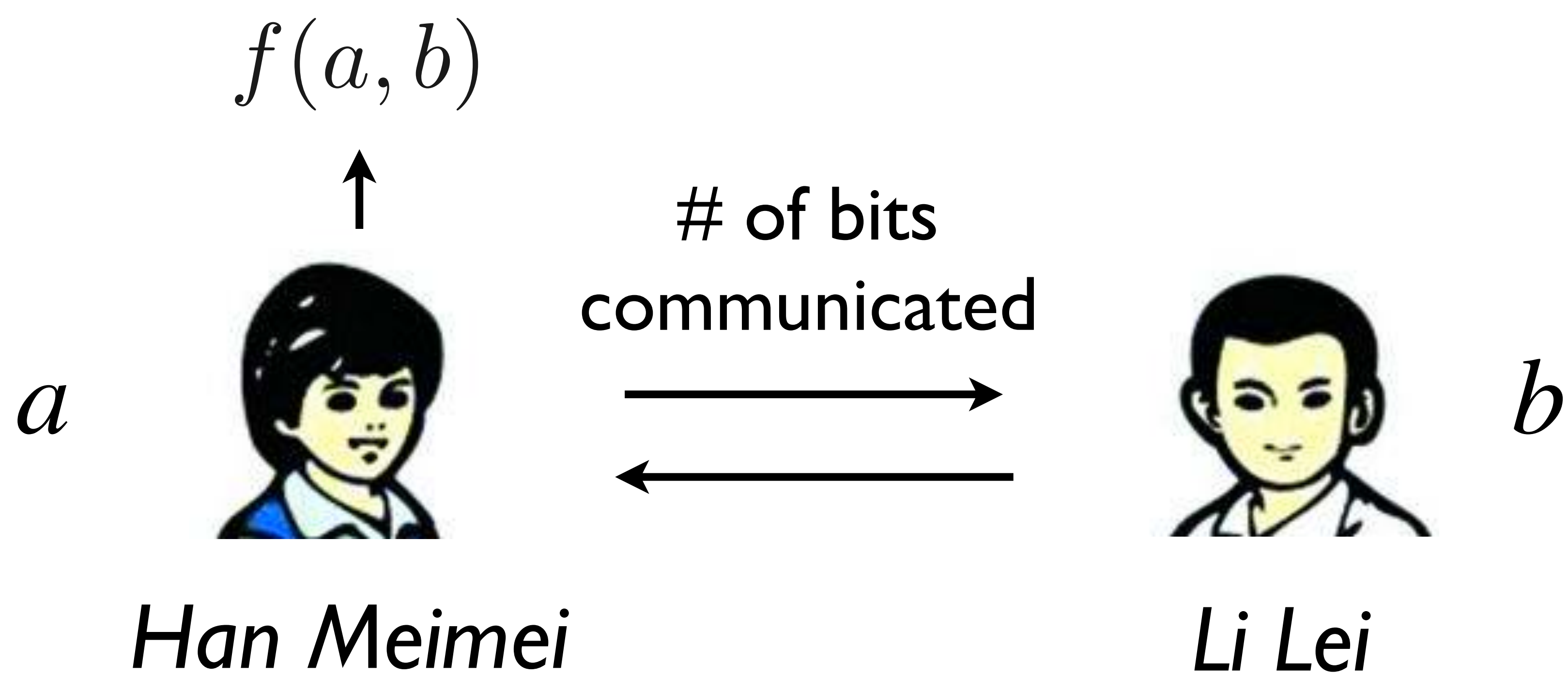
Are they identical?

南京

database 2

Communication Complexity

(Yao 1979)



$$\mathrm{EQ} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

Theorem (Yao, 1979)

There is no deterministic communication protocol solving EQ with less than *n* bits in the worst-case.

Communication Complexity

$$f = \sum_{i=0}^{n-1} a_i x^i$$

$f(r)=g(r)$?

$$g = \sum_{i=0}^{n-1} b_i x^i$$

$a \in \{0,1\}^n$

$r, g(r)$ ←

$b \in \{0,1\}^n$

Han Meimei

Li Lei

by PIT:

one-sided error $\leq \frac{1}{2}$

pick uniform random $r \in [2n]$

# of bit communicated: too large!

Communication Complexity

$f = \sum_{i=0}^{n-1} a_i x^i$

$f(r)=g(r)$?

$g = \sum_{i=0}^{n-1} b_i x^i$

$a \in \{0,1\}^n$

Han Meimei

$r, g(r)$ ←

O(log n) bits

Li Lei

$b \in \{0,1\}^n$

pick uniform
random $r \in [p]$

$k = \lceil \log_2(2n) \rceil$

choose a prime $p \in [2^k, 2^{k+1}]$

let $f, g \in \mathbb{Z}_p[x]$

Polynomial Identity Testing (PIT)

Input: $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv g$?

$\mathbb{F}[x_1, x_2, \ldots, x_n]$: ring of *n*-variate polynomials over field $\mathbb{F}$

$f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n \geq 0} a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

degree of f: maximum $i_1 + i_2 + \cdots + i_n$ with $a_{i_1, i_2, \ldots, i_n} \neq 0$

Input: $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv g?$

equivalently:

Input: $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv 0?$

$$f(x_1, x_2, \ldots, x_n) = \sum_{\substack{i_1, i_2, \ldots, i_n \geq 0 \\ i_1 + i_2 + \cdots + i_n \leq d}} a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

Input: $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv g?$

equivalently:

Input: $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv 0?$

f is given as block-box: given any $\vec{x} = (x_1, x_2, \ldots, x_n)$ returns $f(\vec{x})$

or as product form: e.g. Vandermonde determinant

$$M = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix} \qquad f(\vec{x}) = \det(M) = \prod_{j<i} (x_i - x_j)$$

PIT: Polynomial Identity Testing

Input: $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv 0?$

f is given as block-box or product form

if ∃ a poly-time deterministic algorithm for PIT:

⇒ either: **NEXP ≠ P/poly**

or: **#P ≠ FP**

Input: $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv 0$?

fix an arbitrary $S \subseteq \mathbb{F}$

pick random $r_1, r_2, \ldots, r_n \in S$;
uniformly and *independently* at random;
check whether $f(r_1, r_2, \ldots, r_n) = 0$;

$$f \equiv 0 \Rightarrow f(r_1, r_2, \ldots, r_n) = 0$$

Schwartz-Zippel Theorem

$$f \not\equiv 0 \Rightarrow \Pr[f(r_1, r_2, \ldots, r_n) = 0] \leq \frac{d}{|S|}$$

# of roots for any $f \not\equiv 0$ in any cube S^n is $\leq d \cdot |S|^{n-1}$

Schwartz-Zippel Theorem

$f \not\equiv 0 \Rightarrow \Pr[f(r_1, r_2, \ldots, r_n) = 0] \le \frac{d}{|S|}$

$$f(x_1, x_2, \ldots, x_n) = \sum_{\substack{i_1, i_2, \ldots, i_n \ge 0 \\ i_1 + i_2 + \cdots + i_n \le d}} a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

f can be treated as a single-variate polynomial of x_n:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{d} x_n^i f_i(x_1, x_2, \ldots, x_{n-1})$$

$$= g_{x_1, x_2, \ldots, x_{n-1}}(x_n)$$

$$\Pr[f(r_1, r_2, \ldots, r_n) = 0] = \Pr[g_{r_1, r_2, \ldots, r_{n-1}}(r_n) = 0]$$

$g_{r_1, r_2, \ldots, r_{n-1}} \not\equiv 0?$

done?

Schwartz-Zippel Theorem

$$f \not\equiv 0 \Rightarrow \Pr[f(r_1, r_2, \ldots, r_n) = 0] \leq \frac{d}{|S|}$$

induction on n :

basis: n=1 single-variate case, proved by the *fundamental Theorem of algebra*

I.H.: Schwartz-Zippel Thm is true for all smaller n

Schwartz-Zippel Theorem

$f \not\equiv 0 \Rightarrow \Pr[f(r_1, r_2, \ldots, r_n) = 0] \leq \frac{d}{|S|}$

induction step:

k: highest power of x_n in f $\Rightarrow \begin{cases} f_k \not\equiv 0 \\ \text{degree of } f_k \leq d - k \end{cases}$

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{k} x_n^i f_i(x_1, x_2, \ldots, x_{n-1})$$

$$= x_n^k f_k(x_1, x_2, \ldots, x_{n-1}) + \bar{f}(x_1, x_2, \ldots, x_n)$$

where $\bar{f}(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{k-1} x_n^i f_i(x_1, x_2, \ldots, x_{n-1})$

highest power of x_n in $\bar{f}$ $< k$

Schwartz-Zippel Theorem

$f \not\equiv 0 \Rightarrow \Pr[f(r_1, r_2, \ldots, r_n) = 0] \le \frac{d}{|S|}$

$$f(x_1, x_2, \ldots, x_n) = x_n^k f_k(x_1, x_2, \ldots, x_{n-1}) + \bar{f}(x_1, x_2, \ldots, x_n)$$

$\begin{cases} f_k \not\equiv 0 \\ \text{degree of } f_k \le d - k \end{cases}$

highest power of x_n in $\bar{f}$ $< k$

law of total probability:

$\Pr[f(r_1, r_2, \ldots, r_n) = 0]$

I.H. $\Rightarrow$ (blue) $\le \frac{d-k}{|S|}$

$$= \Pr[f(\vec{r}) = 0 \mid f_k(r_1, \ldots, r_{n-1}) = 0] \cdot \Pr[f_k(r_1, \ldots, r_{n-1}) = 0]$$

$$+ \Pr[f(\vec{r}) = 0 \mid f_k(r_1, \ldots, r_{n-1}) \ne 0] \cdot \Pr[f_k(r_1, \ldots, r_{n-1}) \ne 0]$$

(pink) $= \Pr[g_{r_1, \ldots, r_{n-1}}(r_n) = 0 \mid f_k(r_1, \ldots, r_{n-1}) \ne 0] \le \frac{k}{|S|}$

where $g_{x_1, \ldots, x_{n-1}}(x_n) = f(x_1, \ldots, x_n)$

Schwartz-Zippel Theorem

$$f \not\equiv 0 \quad \Rightarrow \quad \Pr[f(r_1, r_2, \ldots, r_n) = 0] \leq \frac{d}{|S|}$$

$$\Pr[f(r_1, r_2, \ldots, r_n) = 0] \leq \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}$$

Input: $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv 0$?

fix an arbitrary $S \subseteq \mathbb{F}$

pick random $r_1, r_2, \ldots, r_n \in S$;
uniformly and *independently* at random;
check whether $f(r_1, r_2, \ldots, r_n) = 0$;

$$f \equiv 0 \Rightarrow f(r_1, r_2, \ldots, r_n) = 0$$

Schwartz-Zippel Theorem

$$f \not\equiv 0 \Rightarrow \Pr[f(r_1, r_2, \ldots, r_n) = 0] \le \frac{d}{|S|}$$

# of roots for any $f \not\equiv 0$ in any cube S^n is $\le d \cdot |S|^{n-1}$

Fingerprinting

$$X \quad = \quad Y \quad ?$$

$$\downarrow \qquad\qquad \downarrow$$

$$\text{FING}(X) = \text{FING}(Y) \quad ?$$

- FING( ) is a function: $X = Y \Rightarrow \text{FING}(X) = \text{FING}(Y)$
- if $X \neq Y$, Pr[FING(X) = FING(Y)] is small.
- Fingerprints are easy to compute and compare.

Polynomial Identity Testing (PIT)

Input: $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d

Output: $f \equiv 0$?

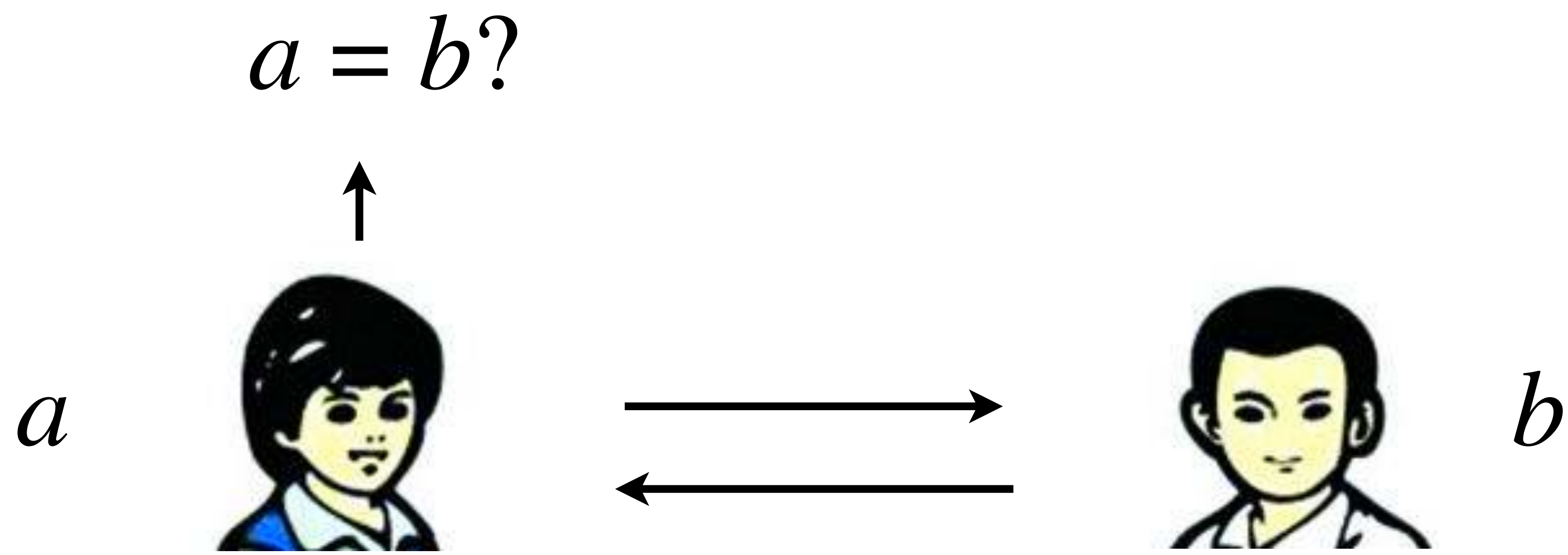
fix an arbitrary $S \subseteq \mathbb{F}$

pick random $r_1, r_2, \ldots, r_n \in S$;
uniformly and *independently* at random;
check whether $f(r_1, r_2, \ldots, r_n) = 0$;

polynomial f:

$\mathrm{FING}(f) = f(r_1, r_2, \ldots, r_n)$ for uniform&independent $r_1, \ldots, r_n \in S$

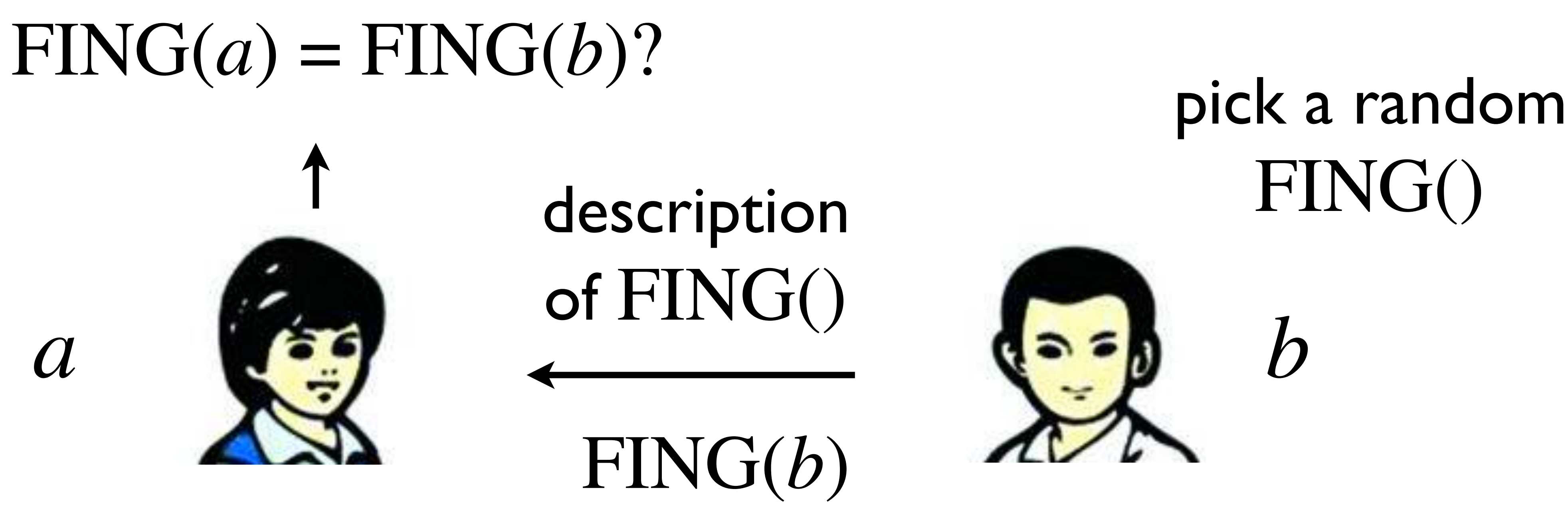
Communication Complexity



$$\mathrm{EQ} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

$$\mathrm{EQ}(a,b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

Fingerprinting



- FING( ) is a function: $a = b \Rightarrow$ FING(a) = FING(b)
- if $a \neq b$, Pr[FING(a) = FING(b)] is small.
- Fingerprints are easy to compute and compare.

$$f = \sum_{i=0}^{n-1} a_i x^i$$

$f(r)=g(r)$?

$$g = \sum_{i=0}^{n-1} b_i x^i$$

$a \in \{0,1\}^n$

$r, g(r)$ ←

$b \in \{0,1\}^n$

pick uniform
random $r \in [2n]$

$f, g \in \mathbb{Z}_p[x]$

prime $p \in [2^k, 2^{k+1}]$ for $k = \lceil \log_2(2n) \rceil$

$\mathrm{FING}(b) = \Sigma_i\, b_i\, r^i$ for random r

$a \equiv b \pmod{p}$?

uniform random prime $p \in [k]$

$\uparrow$

$a \in [2^n]$  $\xleftarrow[b \bmod p]{p}$  $b \in [2^n]$

$\mathrm{FING}(x) = x \bmod p$ for uniform random prime $p \in [k]$

communication complexity: $O(\log k)$

if $a = b$ $\Rightarrow$ $a \equiv b \pmod{p}$

if $a \neq b$: $\Pr[a \equiv b \pmod{p}] \leq ?$

for a $z = |a - b| \neq 0$: $\Pr[z \bmod p = 0] \leq ?$

uniform random prime $p \in [k]$

for a $z = |a - b| \neq 0$: $\Pr[z \bmod p = 0] \leq ?$

$\in [2^n]$

each prime divisor ≥ 2 } ⇨ # of prime divisors of $z \leq n$

$$\Pr[z \bmod p = 0] = \frac{\text{\# of prime divisors of } z \quad \leq n}{\text{\# of primes in } [k] \quad = \pi(k)}$$

$\pi(N)$: # of primes in $[N]$

Prime Number Theorem (PNT)

$$\pi(N) \sim \frac{N}{\ln N} \quad \text{as } N \longrightarrow \infty$$

$a \equiv b \pmod{p}$?

uniform random prime $p \in [k]$

$\uparrow$

$a \in [2^n]$ 

p

$\longleftarrow$

$b \bmod p$

 $b \in [2^n]$

for a $z = |a - b| \neq 0$: $\Pr[z \bmod p = 0] \leq ?$

$$\Pr[z \bmod p = 0] = \frac{\text{\# of prime divisors of } z}{\text{\# of primes in } [k]} \quad \begin{matrix} \leq n \\ = \pi(k) \end{matrix}$$

choose $k = n^2$ $\quad \leq \frac{n \ln k}{k} \quad = \frac{2 \ln n}{n}$

$a \equiv b \pmod{p}$?

uniform random prime $p \in [n^2]$

$a \in [2^n]$  $\xleftarrow[b \bmod p]{p}$  $b \in [2^n]$

$\mathrm{FING}(b) = b \bmod p$ for uniform random prime $p \in [n^2]$

communication complexity: $O(\log n)$

if $a = b$ ⇒ $a \equiv b \pmod{p}$

if $a \neq b$ ⇒ $\Pr[a \equiv b \pmod{p}] \leq (2 \ln n) / n$

Checking Distinctness

Input: n numbers $x_1, x_2, \ldots, x_n \in \{1, 2, \ldots, n\}$

Determine whether every number appears exactly once.

$A = \{x_1, x_2, \ldots, x_n\}$
$B = \{1, 2, \ldots, n\}$

Input: two multisets $A=\{a_1, a_2, \ldots, a_n\}$ and $B=\{b_1, b_2, \ldots, b_n\}$
where $a_1, \ldots, a_n, b_1, \ldots, b_n \in \{1, 2, \ldots, n\}$

Output: $A = B$? (as multisets)

$A = B$ ⟺ $\forall x$: # of times x appearing in A
= # of times x appearing in B

Input: two multisets $A=\{a_1, a_2, \ldots, a_n\}$ and $B=\{b_1, b_2, \ldots, b_n\}$ where $a_1, \ldots, a_n, b_1, \ldots, b_n \in \{1, 2, \ldots, n\}$

Output: $A = B$? (as multisets)

- naive algorithm: use $O(n)$ time and $O(n)$ space
- fingerprinting: random fingerprint function FING( )
  - check $\text{FING}(A) = \text{FING}(B)$?
  - time cost: time to compute and check fingerprints $O(n)$
  - space cost: space to store fingerprints $O(\log p)$

multisets $A=\{a_1, a_2, \ldots, a_n\}$ ⇒ $f_A(x) = \prod_{i=1}^{n}(x - a_i)$

$f_A \in \mathbb{Z}_p[x]$ for prime p (to be specified)

$\text{FING}(A) = f_A(r)$ for uniform random $r \in \mathbb{Z}_p$

multisets $A=\{a_1, a_2, \ldots, a_n\}$

$B=\{b_1, b_2, \ldots, b_n\}$

where $a_i, b_i \in \{1, 2, \ldots, n\}$

$$\begin{cases} f_A(x) = \prod_{i=1}^{n}(x - a_i) \\ f_B(x) = \prod_{i=1}^{n}(x - b_i) \end{cases}$$

$f_A, f_B \in \mathbb{Z}_p[x]$ for prime p (to be specified)

$$\left.\begin{array}{l} \mathrm{FING}(A) = f_A(r) \\ \mathrm{FING}(B) = f_B(r) \end{array}\right\}$$ for uniform random $r \in \mathbb{Z}_p$

$A \neq B$ ⇒ $f_A \not\equiv f_B$ on real field $\mathbb{R}$

(but possibly $f_A \equiv f_B$ on finite field $\mathbb{Z}_p$)

if $A = B$: $\mathrm{FING}(A) = \mathrm{FING}(B)$

if $A \neq B$: $\mathrm{FING}(A) = \mathrm{FING}(B)$

- $f_A \equiv f_B$ on finite field $\mathbb{Z}_p$ ⇒ in $f_A - f_B$ on $\mathbb{R}$: $\exists$ coefficient $c \neq 0$, $c \bmod p = 0$
- $f_A \not\equiv f_B$ on $\mathbb{Z}_p$ but $f_A(r) = f_B(r)$ ⇒ (Schwartz-Zippel) with probability $\leq n/p$

multisets $A=\{a_1, a_2, ..., a_n\}$

$B=\{b_1, b_2, ..., b_n\}$

where $a_i, b_i \in \{1, 2, ..., n\}$

$$\begin{cases} f_A(x) = \prod_{i=1}^{n}(x - a_i) \\ f_B(x) = \prod_{i=1}^{n}(x - b_i) \end{cases}$$

$f_A, f_B \in \mathbb{Z}_p[x]$ for uniform random prime $p \in [L, U]$

(L, U to be specified)

$$\left.\begin{aligned} \text{FING}(A) &= f_A(r) \\ \text{FING}(B) &= f_B(r) \end{aligned}\right\} \text{ for uniform random } r \in \mathbb{Z}_p$$

if $A \neq B$: $\text{FING}(A) = \text{FING}(B)$

- $f_A \equiv f_B$ on finite field $\mathbb{Z}_p$ → in $f_A - f_B$ on $\mathbb{R}$: $\exists$ coefficient $c \neq 0$, $c \bmod p = 0$

$$\Pr[\ c \bmod p = 0\ ] \leq \frac{\#\text{ of prime factors of } c}{\#\text{ of primes in } [L, U]}$$

$|c| \leq n^n$ → $\leq \frac{n \log_2 n}{\pi(U) - \pi(L)} \sim \frac{n \log_2 n}{U/\ln U - L/\ln L}$

- $f_A \not\equiv f_B$ on $\mathbb{Z}_p$ but $f_A(r) = f_B(r)$ → (Schwartz-Zippel) with probability $\leq n/p \leq n/L$

multisets $A=\{a_1, a_2, \ldots, a_n\}$

$B=\{b_1, b_2, \ldots, b_n\}$

where $a_i, b_i \in \{1, 2, \ldots, n\}$

$$\begin{cases} f_A(x) = \prod_{i=1}^{n}(x - a_i) \\ f_B(x) = \prod_{i=1}^{n}(x - b_i) \end{cases}$$

$f_A, f_B \in \mathbb{Z}_p[x]$ for uniform random prime $p \in [L, U]$

with $U = 2L = (n \log n)^2$

$$\left.\begin{aligned} \mathrm{FING}(A) &= f_A(r) \\ \mathrm{FING}(B) &= f_B(r) \end{aligned}\right\}$$ for uniform random $r \in \mathbb{Z}_p$

if $A \neq B$: $\mathrm{FING}(A) = \mathrm{FING}(B)$

- $f_A \equiv f_B$ on finite field $\mathbb{Z}_p$ → with probability $\leq \frac{n \log_2 n}{U/\ln U - L/\ln L} = O(1/n)$
- $f_A \not\equiv f_B$ on $\mathbb{Z}_p$ but $f_A(r) = f_B(r)$ → (Schwartz-Zippel) with probability $\leq n/p \leq n/L = O(1/n)$

Input: two multisets $A=\{a_1, a_2, \ldots, a_n\}$ and $B=\{b_1, b_2, \ldots, b_n\}$
where $a_1, \ldots, a_n, b_1, \ldots, b_n \in \{1, 2, \ldots, n\}$

Output: $A = B$? (as multisets)

Lipton 1989:

$$\mathrm{FING}(A) = \prod_{i=1}^{n}(r - a_i) \bmod p$$

$$\mathrm{FING}(B) = \prod_{i=1}^{n}(r - b_i) \bmod p$$

for uniform random prime $p \in [(n \log n)^2/2, (n \log n)^2]$ and uniform random $r \in \mathbb{Z}_p$

if $A \neq B$ as multisets:

$$f_A(x) = \prod_{i=1}^{n}(x - a_i) \bmod p \qquad f_B(x) = \prod_{i=1}^{n}(x - b_i) \bmod p$$

$$\Pr[\, \mathrm{FING}(A) = \mathrm{FING}(B) \,]$$

$$\leq \Pr[\, f_A \equiv f_B \,] + \Pr[\, f_A(r) = f_B(r) \mid f_A \not\equiv f_B \,] = O(1/n)$$

Input: n numbers $x_1, x_2, ..., x_n \in \{1, 2, ..., n\}$

Determine whether every number appears exactly once.

Lipton 1989:

$$\mathrm{FING}(A) = \prod_{i=1}^{n}(r - a_i) \bmod p$$

check if:

$$\mathrm{FING}(A) = \prod_{i=1}^{n}(r - i) \bmod p?$$

for uniform random prime $p \in [(n \log n)^2/2, (n \log n)^2]$ and uniform random $r \in \mathbb{Z}_p$

- time cost: $O(n)$
- space cost: $O(\log n)$
- error probability (false positive): $O(1/n)$
- data stream: input comes one at a time