HONORS ALGORITHMS

2024-02-07

DESCRIPTION OF ALGORITHMS

~~JAVA~~

~~PYTHON~~

~~STORY~~

PSEUDOCODE

} INSUFFICIENT INFO TO JUDGE BIT-COMPLEXITY

PLEASE EXPLAIN the lines of code

BINARY OPERATION on set A:

$$f: A \times A \to A$$

examples: addition, multiplication } on $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/_{m}\mathbb{Z}$

mod m residue classes

EX: $(\forall a)(0 \cdot a = 0)$

COMMUTATIVE RING $(A, +, \times)$

addition		multiplication
$\forall a, b$ $a+b=b+a$	commutative	$ab=ba$
	associative	$(ab)c=a(bc)$
$\exists$ zero: $(\forall a)(0+a=a)$	
$\forall a \, \exists (-a)$ $a+(-a)=0$	
	distributive	$a(b+c)=ab+ac$

FIELD: commutative ring s.t.

$\exists$ identity element $(\forall a)(1 \cdot a = a)$

$(\forall a \neq 0)(\exists a^{-1})(a \cdot a^{-1} = 1)$

$1 \neq 0$ $\quad \therefore |F| \geq 2$

$\mathbb{Z}/_{m}\mathbb{Z}$ is a field $\Leftrightarrow$ m prime $\quad |\mathbb{F}_p| = p$

Examples: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}/_{p}\mathbb{Z} =: \mathbb{F}_p$

Ex $\underline{ab = 0 \Leftrightarrow a = 0 \vee b = 0}$

$\mathbb{Z}$ not a field

F field

$F[x]$ = ring of polynomials over F

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad \parallel$

formal lin. combinations of $1, x, x^2, \ldots$

coefficients from F

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

$(\forall a \in F)$ defines map $F[x] \longrightarrow F$

$f \longmapsto f(a)$ evaluation map

"polynomial
$\downarrow$ function"

$f \in F[x]$ $\quad \tilde{f} : F \to F \quad f \longmapsto \tilde{f}$

$f \mapsto \tilde{f}$ is injective $\Longleftrightarrow$ F is <u>infinite</u>

F finite $\quad f(x) = \prod_{a \in F}(x-a) \mapsto \tilde{f} = 0$

$f \neq 0$

__Lemma__ $\quad f \in F[x] \quad a \in F \implies$

$(\exists g \in F[x])(f(x) = (x-a)g(x) + f(a))$

__COR__. $\quad \underline{a}$ is a $\underset{f(a)=0}{\underline{\text{root}}}$ of $f \iff x-a \mid f$

divisor

i.e. $(\exists g)(f = (x-a) \cdot g)$

__COR__. If $f \neq 0$ then # roots of $f \leq \deg f$

multivariate polynomials

$$f(x_1, \dots, x_n)$$

monomial: product of variables

$$\prod x_i^{k_i}$$

polynomial: formal lin. combination of monomial

---

easy-to-evaluate poly. w exponentially many expansion terms ($\leftarrow$ monomials)

$$\prod_{i=1}^{n} (x_i - a_i)$$

PIT polynomial identity testing

deg(f) = max deg of its expansion terms

deg(0) = $-\infty$

degree $\left(\prod x_i^{k_i}\right) := \sum k_i$

$\deg(f) = 0 \iff f = a_0 \neq 0$ non-zero $\in F$ "constant"

$F^{\leq k}[x_1 \cdots x_n]$: each individual degree is $\leq k$

$\prod x_i^{k_i}$ $(\forall i)(k_i \leq k)$

EX. If $f \in F^{\leq k}[x_1 \cdots x_n]$ and $k < |F|$ order of field

then $f = 0 \iff \tilde{f} = 0$

EX. If F finite of order $q = |F|$ [q is necessarily a prime power]

then $(\forall a \in F)(a^q - a = 0)$

$x^q - x \mapsto 0$ function

(generalization of FERMAT's little theorem)

Polynomial Identity Lemma

Let $H \subseteq F$ $\quad$ $\underline{H \text{ finite}}$

$\underline{f \neq 0}$ $\quad$ not the zero poly.

Then

$$\operatorname*{Prob}_{a_i \in H}\left(f(a_1, \dots, a_n) = 0\right) \leq \frac{\deg(f)}{|H|}$$

witness of $f \neq 0$: $\underline{a} = (a_1 \cdots a_n)$ s.t. $f(\underline{a}) \neq 0$

$\therefore$ if $|H| \geq 2 \cdot \deg(f)$ then <u>witness</u> found w. prob $\geq \frac{1}{2}$

in k trials, witness found w. prob $\geq 1 - \frac{1}{2^k}$

POLYNOMIAL IDENTITY LEMMA

history

1979 Jacob Schwartz
Richard Zippel

1922 Øystein Ore