HONORS ALGORITHMS

2024-02-14

FAST MULTIPLICATION OF POLYNOMIALS

CONVOLUTION OF SEQUENCES

$$(a_0 \dots a_{n-1}) * (b_0 \dots b_{n-1}) = (c_0 \dots c_{n-1})$$

$$c_k = \sum_{i=0}^{n-1} a_i \, b_{k-i \bmod n}$$

via DISCRETE FOURIER TRANSFORM

DFT discrete Fourier transform

$$(a_0, \dots, a_{n-1}) \underset{\text{lin. trf.}}{\longmapsto} (b_0, \dots, b_{n-1})$$

n^{th} roots of unity

$$1, \omega, \omega^2, \dots, \omega^{n-1}$$

$$f(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$$

$$\omega = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}.$$

$$\boxed{b_j = f(\omega^j)}$$

$$\underline{b} = F \cdot \underline{a}$$

$$\boxed{F = (\omega^{ij})_{n \times n}}$$

$$\underline{b} = \underline{\hat{a}}$$

DEF z is a n^{th} root of unity if $z^n = 1$

DEF —"— primitive n^{th} root of unity if $(\forall k)(1 \le k \le n-1)(z^k \ne 1)$

EX: z is a prim. n^{th} root of unity $\iff$ $\{1, z, z^2, \dots, z^{n-1}\}$ is ALL n^{th} roots of unity

If z is a pr n^{th} root of unity then which powers of z are — " —

z^k is a pr. n^{th} root of unity $\iff \gcd(n,k)=1$

$F = (\omega^{ij})_{n\times n}$ Fourier matrix

$F \cdot F^* = nI$ $\qquad F^{-1} = \frac{1}{n} F^*$

$\underline{a} = (a_0 \ldots a_{n-1}) \longmapsto \hat{\underline{a}}$

$\widehat{a * b} = \hat{a} \cdot \hat{b}$

convolution

pointwise product

FFT fast Fourier transform

$$n = 2^k$$

$a_0 \; \cdots \; a_{n-1}$

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

D & C by Karatsuba

$$\hat{a} = (f(1), f(\omega), f(\omega^2), \ldots, f(\omega^{n-1}))$$

FFT

$$f(x) = g(x^2) + x\, h(x^2)$$

ω^2: $\left(\frac{n}{2}\right)^{th}$ pr root of unity

$$T(n) = 2 \cdot T\left(\frac{n}{2}\right) + O(n)$$

Ex. $\boxed{T(n) = O(n \log n)}$

FINITE PROBABILITY SPACES

Ω "sample space"
non-empty finite set

outcomes of experiment

k coin flips HTTHHHTH

$|\Omega| = 2^k$

poker hand: 5 out of 52 cards
standard deck

$|\Omega| = \binom{52}{5}$

STUDY

DEF: Ω finite set
$f : \Omega \to \mathbb{R}$
is a probability distribution
if $\begin{cases} (\forall a \in \Omega)(f(a) \geq 0) \\ \sum_{a \in \Omega} f(a) = 1 \end{cases}$

uniform distrib
$(\forall a \in \Omega)\left(f(a) = \frac{1}{|\Omega|}\right)$

"probabilities of outcomes"

DEF finite prob. space: $(\Omega, \Pr)$
$\Pr$ is a prob. distr on Ω

Event: $A \subseteq \Omega$

extend $\Pr : \Omega \to \mathbb{R}$

to $\mathcal{P}(\Omega) \to \mathbb{R}$

set of all subsets of Ω

power set of Ω

"# heads is 17"

"full house" 3+2

3 of a kind

2 " "

KKK99

DEF $\Pr(A) := \sum_{a \in A} \Pr(a)$

$\Pr(\{a\}) = \Pr(a)$

"elementary event"

COR $0 \le \Pr(A) \le 1$

EX MODULAR EQUATION

$\Pr(A \cup B) + \Pr(A \cap B) = \Pr(A) + \Pr(B)$

EX $\Pr\left(\bigcup_{i=1}^{t} A_i\right) \le \sum_{i=1}^{t} \Pr(A_i)$

Equality holds $\iff$ $(\forall i \ne j)\left(\Pr(A_i \cap A_j) = 0\right)$

~~"independent"~~

~~pairwise disjoint~~

$\Updownarrow$

[all elementary events in $A_i \cap A_j$ have $\Pr = 0$]

DEF A is a trivial event if $\Pr(A) = 0$ or 1

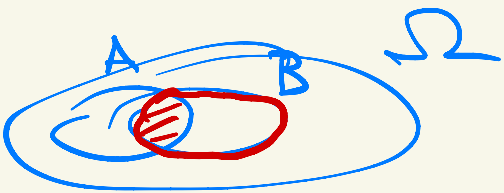
Examples: $\Pr(\emptyset) = 0$, $\Pr(\Omega) = 1$

$\boxed{\text{HW}}$ # trivial events is a power of 2

DEF events $A, B \subseteq \Omega$ are INDEPENDENT
if $Pr(A \cap B) = Pr(A) \cdot Pr(B)$

DEF conditional probability $Pr(A \mid B) = \dfrac{Pr(A \cap B)}{Pr(B)}$

"given"



define prob. space
$(B, Pr(\cdot \mid B))$

NEED
$Pr(B) \neq 0$

EX If $Pr(B) \neq 0$
then A, B indep.
$\iff P(A \mid B) = P(A)$

A, B <u>positively correlated</u> if

$$\Pr(A \cap B) > \Pr(A) \cdot \Pr(B)$$

in case $\Pr(B) \neq 0$ this means $P(A|B) > P(A)$

<u>negatively correl</u> if

$$P(A \cap B) < \Pr(A) \cdot \Pr(B)$$

DEF A, B, C are indep if

(i) pairwise indep

(iii) $\Pr(A \cap B \cap C) = \Pr(A) \cdot \Pr(B) \cdot \Pr(C)$

DEF $A_1 \dots A_k$ are indep if

$$(\forall I \subseteq [k])\left(\Pr\left(\bigcap_{i\in I} A_i\right) = \prod_{i\in I} P(A_i)\right)$$

automatically true if $I=\emptyset$

$$\bigcap_{i\in\emptyset} A_i = \Omega \quad \Big| \quad \prod_{i\in\emptyset} x_i = 1$$

— " — true if $|I|=1$

$2^k - k - 1$ conditions