February 14, 2023 1:50 PM

Knapsack

Given n items where item i has weight w_i ← assume integers
& value v_i

and number W (capacity),

find $I \subseteq \{1, \dots, n\}$ s.t. $\sum_{i \in I} w_i \le W$

maximizing $\sum_{i \in I} v_i$.

0/1 Version: each item used at most once (I is a set)

Unbounded version: each item may be used more than once (I is a multiset)

both (weak) NP-complete!

but if W is not too big, can use DP.

Define subproblems:

for each $i = 0, \dots, n$, $j = 0, \dots, W$,

let $C(i,j) = \max \sum_{i \in I} v_i$ s.t. $\sum_{i \in I} w_i \le j$, $I \subseteq \{1, \dots, i\}$

Want $C(n, W)$.

Recursive formula: (0/1 Version)

$$\boxed{C(i,j) = \max \{ \underbrace{C(i-1, j)}_{\text{not use } i},\ \underbrace{C(i-1, j-w_i) + v_i}_{\text{use } i} \}}$$

$C(0,j) = 0$.

increas. i

$\Rightarrow \boxed{O(nW)}$ time

Unbdd version: $C(i,j) = \max\{ C(i-1,j),\ C(i, j-w_i) + v_i \}$

$\Rightarrow O(nW)$ time

Alternate DP for unbdd:

let $C(j) = C(n,j)$

$$\boxed{C(j) = \max_{i : w_i \le j} \left(C(j - w_i) + v_i \right)}$$

$\Rightarrow O(nW)$ time

Rmk - V = opt total value

$O(nV)$ time

Rmk - space reduced to $O(W)$

Rmk - Chan, He '20: for unbounded vers.

$\tilde{O}(nU)$ where $U = \max_i w_i$.

(very simple modified DP)

$\tilde{O}(nU)$ where $U = \max_i w_i$.

(very simple modified DP
$O(U^2 \log U + W)$)

Midterm I

Feb 20 Mon 7pm–9pm Loomis 141

* Conflict: fill form by tomorrow

Cheat sheet

everything up to Feb 9 lecture

Short Qs + 3 or 4 Long Qs

my extra OH: Fri 2–3

RANDOMIZED ALG'MS

an algm that can make random choices
i.e. access to rand. number generator

rand_bit() ⟶ 0 or 1
rand(a,b) ⟶ a or a+1 or ... or b

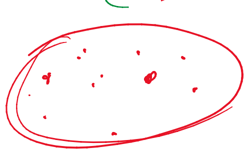
It's **Las Vegas** if it's always correct
runtime depends on rand choices.
⟵ analyze expected time

note: still worst-case input
(e.g. randomized quicksort)

It's **Monte Carlo** if correctness depends on rand. choices
⟵ analyze probability of error

(probability space is over the sequence of rand bits/numbers)

assume uniform & independent



Quick Probability Review:

event E, E'

$$\Pr(E \cup E') \leq \Pr(E) + \Pr(E')$$

(equal if disjoint)

$$\Pr(E^c) = 1 - \Pr(E)$$

$$\Pr(E \cap E') = \Pr(E)\Pr(E') \quad \text{if } \underline{\text{independent}}$$

$$\Pr(E \mid E') = \frac{\Pr(E \cap E')}{\Pr(E')}.$$

conditional prob.

random var. X, Y

$$E[X] = \sum_x x \cdot \Pr(X = x)$$

(integral if continuous)

$$E[X+Y] = E(X) + E[Y] \quad \text{always}$$

$$E[cX] = c\,E(X)$$

$$E(XY) = E(X) \cdot E(Y) \quad \text{if } \underline{\text{independent}}$$

---

e.g. Markov's ineq: If $X \geq 0$ and $E(X) = \mu$,

$$\Pr(X \geq c\mu) \leq \frac{1}{c}.$$

Pf: $\mu = E(X) \geq \sum_{x \geq c\mu} x \cdot \Pr(X = x) \geq c\mu \sum_{x \geq c\mu} \Pr(X = x) = c\mu \Pr(X \geq c\mu)$ $\square$

Problem

Given n-bit (large) number N,

is N prime or composite?

Trivial Alg'm:

for $a = 2$ to ~~$N-1$~~ $\sqrt{N}$

if $\underline{N}$ is divisible by $\underline{a}$ then return "composite" return "prime"

$N = ab \quad a \leq b$

$a^2 \leq N, \quad a \leq \sqrt{N}$

$$\Rightarrow \quad O(\sqrt{N}\, n^2) = O(2^{n/2} n^2)$$
$$\leq O(1.415^n)$$

exponential!

Rmk - factoring is probably hard
but not necessarily primality testing

Wilson's Thm (17??)

N is prime iff $(N-1)! \equiv -1 \pmod{N}$

$\#$ mults $= O(N) = O(2^n)$

Computationally useless

Fermat's Little Thm (16??)

N is prime $\iff$ $\forall a \in \{1, \ldots, N-1\}$, $a^{N-1} \equiv 1 \pmod{N}$

Can be computed quickly
repeated square

$\#$ mult $= O(\log N) = O(n)$