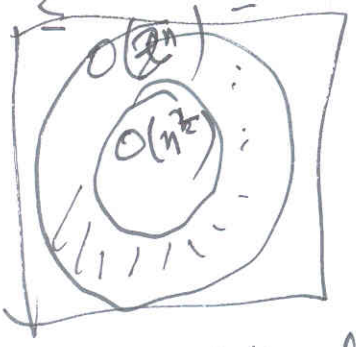
3/23 Complexity of alg. division... / Induction (?)

O, Θ, Ω

<, =, ≥



3.3 Computational complexity

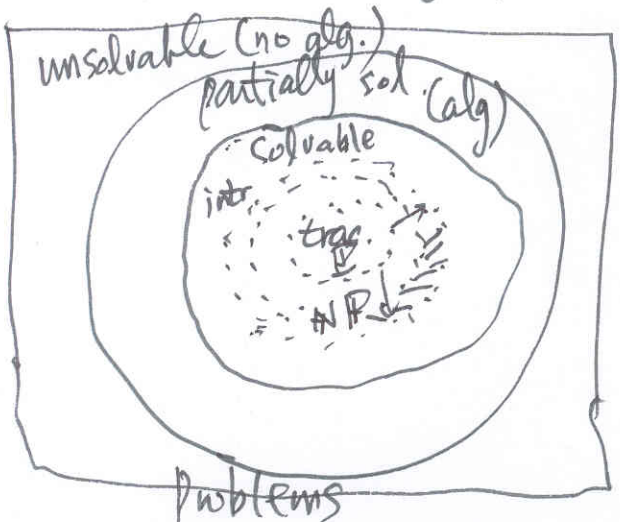
time complexity
space (memory) ∥ (↓)
(power consumption)
} → input data

[Worst-case analysis — theoritical
[Average-case ∥ — practical

linear search $\frac{n}{2}$ ~~n~~ $O(n)$

↑ average ↑ worst

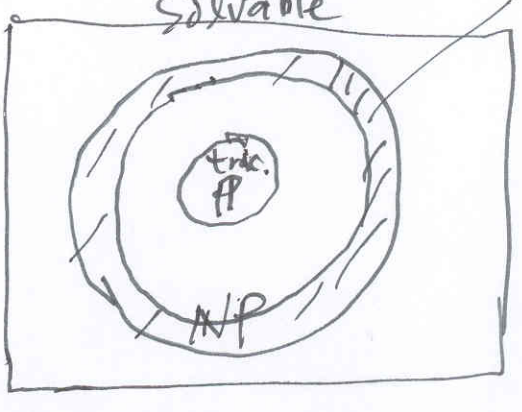
binary search $O(\log_2 n)$



$P \subseteq NP$ ⟨ $P = NP$ / $P \subsetneq NP$

[tractable = class P
→ poly ★
[intractable ~~class~~
→ exp. ↑

class NP
nondeterministic polynomial.



3

$|\mathbb{N}| = |\mathbb{N}^2| \cdots = |\mathbb{N}^k|$

$|2^{\mathbb{N}}| = (2) \times 2 \times \cdots$

infinite

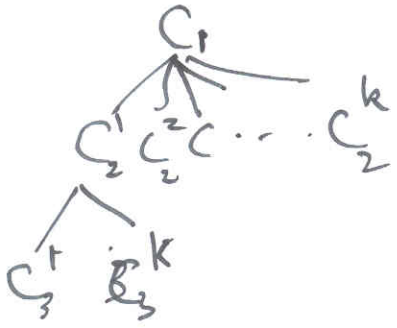
∞^k $\infty \times \infty \times \infty \cdots \times \infty$ (∞ finite)

3.4 The Integer and division

on data

$C_1 \to \cdots \to C_k$.

$k = O(n)$ "n^k" k can be expressed as polynomial ftn of n.



Computation

M, ... memory

ip ... instruction pointer

F_{in} ... input data

F_{out} ... output data

(M, ip, F_{in}, F_{out})

↓ Configuration of Computation

$C_0 = (M_0, ip_0, F_{in_0}, F_{out_0})$

initial cnf.

$C_0 \to C_1 \to C_2 \cdots \to C_n \to \cdots$

deterministic

$\forall C_i \; \exists! C_{i+1}$

Nondet. otherwise.

$\forall C_i$ C_{i+1}^1 ⋮ C_{i+1}^k

3.4. Integer and Division

$a, b \in \mathbb{Z}, \wedge a \neq 0$. a divides b, if $\exists c \in \mathbb{Z}$ s.t. $b = ac$

$a \mid b$ ($b \div a \in \mathbb{Z}$ → no remainder)

Ex) $3 \mid 6$, $3 \mid 3$, $5 \nmid 12$ $6 \nmid 3$

a는 b의 약수이다.

a is a divisor of b.

$a = ds$, $b = dt$ $s.t \in \mathbb{Z}$

$a + b = d(s+t)$

Theorem

i) $a \mid b \wedge a \mid c \rightarrow a \mid (b+c)$

ii) $a \mid b \rightarrow {}^{\forall} a \mid bc$

iii) $a \mid b \wedge b \mid c \rightarrow a \mid c$

Col. i) $a \mid b \wedge a \mid c \rightarrow a \mid (mb + nc)$ $^{\forall} m, n \in \mathbb{Z}$

Theorem 2 The division alg.

$^{\forall} a \in \mathbb{Z}, {}^{\forall} d \in \mathbb{Z}^+, \exists_1 q, \exists_1 r \in \mathbb{Z}: 0 \leq r < d$ s.t. $a = qd + r$.

$q = a \operatorname{div} d$, $r = a \bmod d$.

such that $\boxed{a \div d = q \cdots r}$ 초등학교

Modular arithmetic

Def. 3 $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

If $m \mid (a-b)$ then