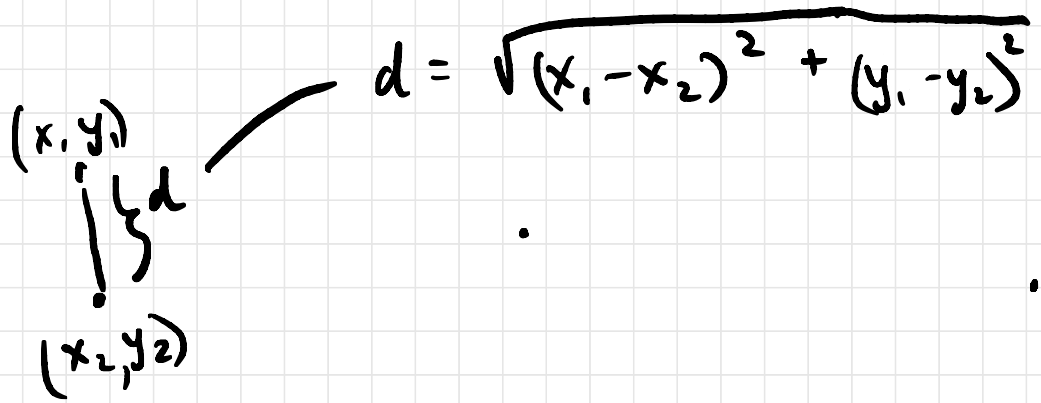
CSCE 310H - Fall 2021

Computer Science III - honors

Dr. Chris Bourke



Pairs = Combinations of size 2

given a set of n distinct elements,

how many combinations (order does not matter) of k elements are there?

n "choose" k

$$\binom{n}{k} = C(n,k) = C_k^n = {}_nC_k$$

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$$

ex:

$$\binom{n}{2} = \text{number of pairs}$$

$$= \frac{n!}{(n-2)!\,2!} = \frac{n(n-1)}{2} \in O(n^2)$$

$$= \frac{n^2}{2} - \frac{n}{2}$$

Input: A set of points $A = \{(x_1, y_1), \dots (x_n, y_n)\}$

Output: 2 closest points in A

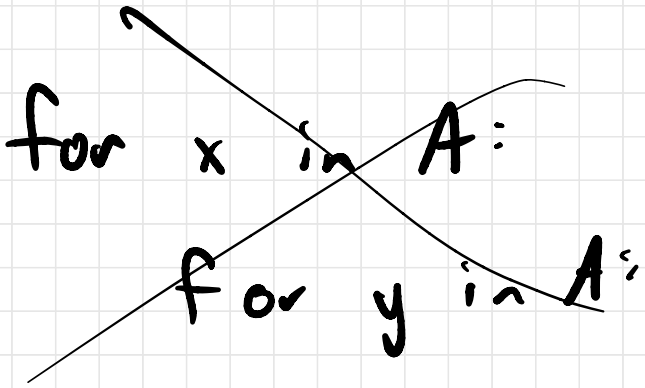
```
1  MinDist ← ∞
2  for each pair of points (x_a, y_a), (x_b, y_b) in A
3      d ← sqrt((x_a - x_b)^2 + (y_a - y_b)^2)
4      if d < MinDist
5          MinDist ← d
6          (p_a p_b) ← (p_1 p_2)
7  output (p_a p_b)
```

1) Input: A

2) Input size: n

3) Element Op: comp, line 4

4) $\binom{n}{2}$ 5) $\Theta(n^2)$



0 loose

$n \in \Theta(n)$

$n \in O(n^2)$

$n \in O(2^n)$

for $i = 0 \dots n-1$

for $j = i+1 \dots n$

$\dots$

1

$$\sum_{i=0}^{n-1} \sum_{j=i+1}^{n} 1 = \sum_{i=0}^{n-1} (n-i)$$

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Gauss's Formula

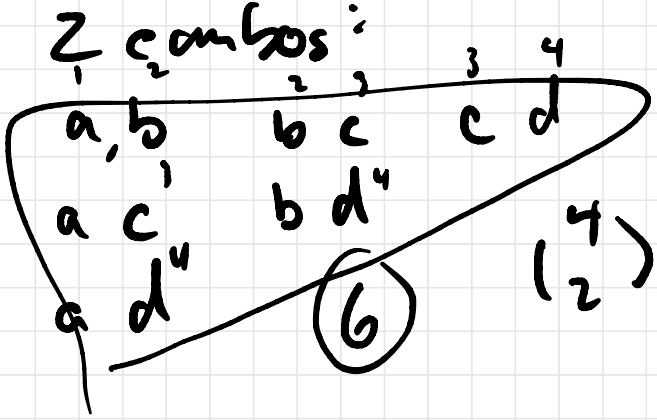
K-combinations

Given a set of n elements, $\{1, 2, 3, \dots n\}$

a k-combination is a subset of size k

↳ unordered

ex] $\{a, b, c, d\}$



$$\binom{4}{2} = \frac{4!}{(4-2)!\,(2!)} = \frac{4 \cdot 3}{2} = 6$$

3 - combos of a b c d ... n

```
for i = 1 .. 2^(n-2)
    for j = i+1 .. 3^(n-1)
        for k = j+1 .. 4^n
```

Want: generate every possible subset...

- how many subsets are there of a set of size n?

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} \cdots \binom{n}{n-1} + \binom{n}{n}$$

$$= 2^n$$

$O(2^n) \rightarrow$ exp.

$S = \{a, b, c \dots n\}$

$\mathcal{P}(S)$ = power set

0 if x is not in subset

1 if $x \in$ subset

$0 \dots 2^n - 1$

a, b, c	bit		
$\emptyset$	000	000	0
{a}	100	001	1
{b}	010	010	2
{c}	001	011	3
{a b}	110	100	4
{a c}	101	101	⋮
{b c}	011	110	
{a, b, c}	111	111	7

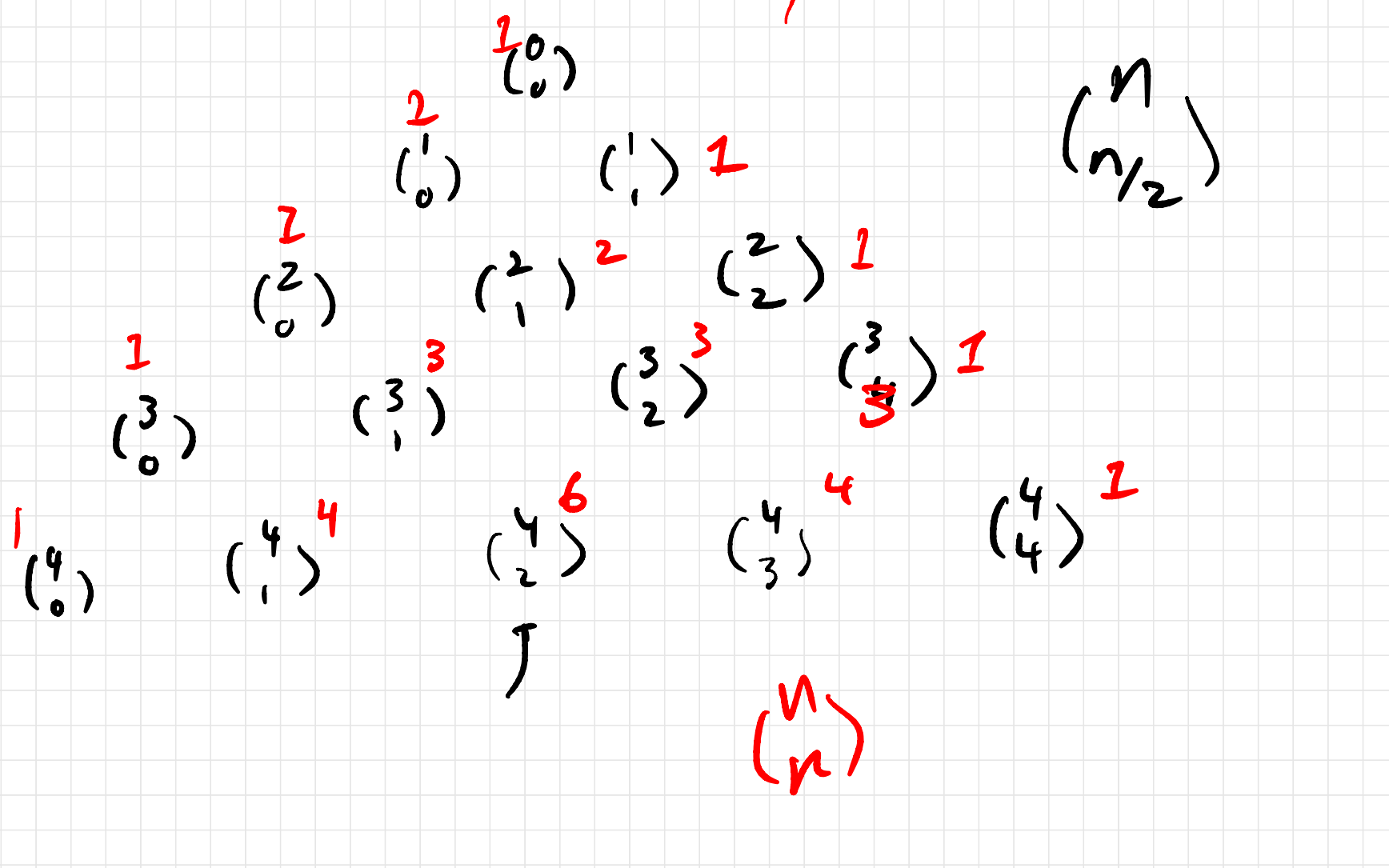
$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

$$\binom{n}{k} \in O(n^k)$$

$$\binom{n}{2} \in O(n^2)$$

$$\binom{n}{3} \in O(n^3)$$

$$\binom{n}{4} \in O(n^4)$$


1
$\binom{0}{0}$
2
$\binom{1}{0}$
$\binom{1}{1}$ 1
$\binom{n}{n/2}$
1
$\binom{2}{0}$
$\binom{2}{1}$ 2
$\binom{2}{2}$ 1
1
$\binom{3}{0}$
$\binom{3}{1}$ 3
$\binom{3}{2}$ 3
$\binom{3}{3}$ 1
1
$\binom{4}{0}$
$\binom{4}{1}$ 4
$\binom{4}{2}$ 6
$\binom{4}{3}$ 4
$\binom{4}{4}$ 1
$\binom{n}{r}$

$$\binom{n}{n/2} = \frac{n!}{(n-\frac{n}{2})!\,\frac{n}{2}!} \in O(2^n)$$

$\{2, 5, 6, 9, 10\}$

$n = 10$

$k = 5$

2 5 7 9 10

Algorithm 2: Next k-Combination

INPUT : A set of n elements and an k-combination, $a_1 \cdots a_k$.
OUTPUT : The next k-combination.

1 $i = k$
2 WHILE $a_i = n - k + i$ DO
3 $\quad i = i - 1$
4 $a_i = a_i + 1$
5 FOR $j = (i+1) \ldots k$ DO
6 $\quad a_j = a_i + j - i$

2) replace $a_i \rightarrow a_i + 1$

$a_2 : a_1 + j - i$

$2 + 2 - 1 = 3$

$a_3 : a_1 + j - i$

$2 + 3 - 1 = 4$

$n = 5$ {1 2 3 4 5}

$k = 3$

Next?

current:

a_1	a_2	a_3
1,	4,	5
↓	↓	↓
2	3	4

1) locate last a_i such that

$a_i \neq n - k + i$

$a_1 = 1 \stackrel{?}{=} 5 - 3 + 1$

$\neq 3$

$a_3 = 5 \stackrel{?}{=} n - k + i$

$= 5 - 3 + 3 = 5$

$a_2 = 4 \stackrel{?}{=} 5 - 3 + i$

$= 5 - 3 + 2 = 4$

Permutations

A permutation is an arrangement (order matters) of elements

---

abc	bac	cab	in general:
acb	bca	cba	$n!$

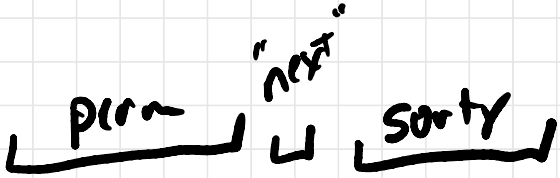
$n = 3$ 6

$n=6$

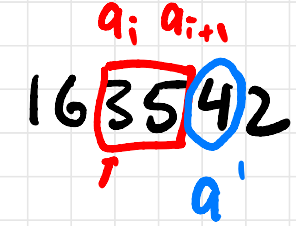
1 2 3 4 5 6

1 2 3 4 6 5

1 2 3 5 4 6



$n = 6$



↓

1 6 4 5 3 2

sort

↓

1 6 4 2 3 5 ✓

1) find last pair that is in order

2) find a': smallest element larger than a_i to the right

a) swap a_i a'

b) sort everything to the right of a'

1 6 4 2 3 5

swap

1 6 4 2 5 3

sort

⋮

6 5 4 3 2 1

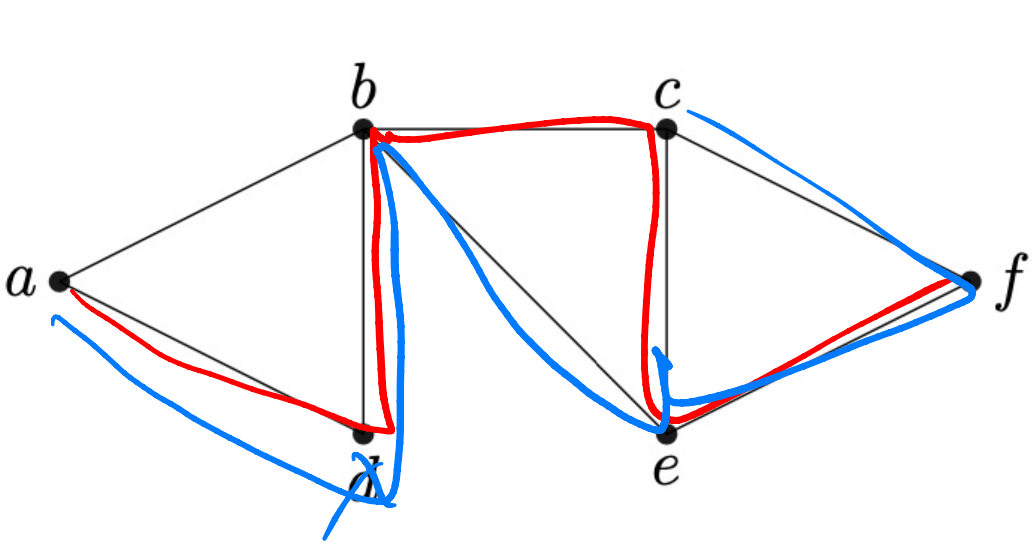
1) if, but most known pair

$n!$ permutations

$O(n!) = O(n^n)$

$0! = 1$

$, n$



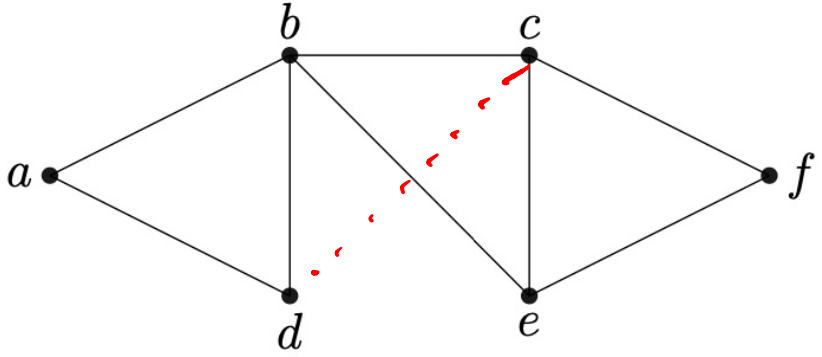
a d b c e f

a d b e f c

a b c e f d

```
for each permutation π of {v_1 ... v_n}:
    // verify π is a path:
    isValid ← true
    for i = 1 ... n-1:
        if (v_i v_{i+1}) ∉ E
            isValid ← false
    if isValid
        output Yes
output No
```

$O(n!)$



$n! = 6! = 720$

$\downarrow$

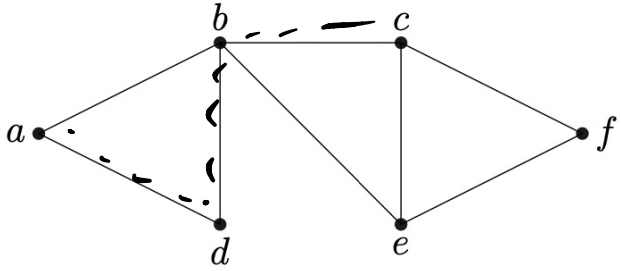
600

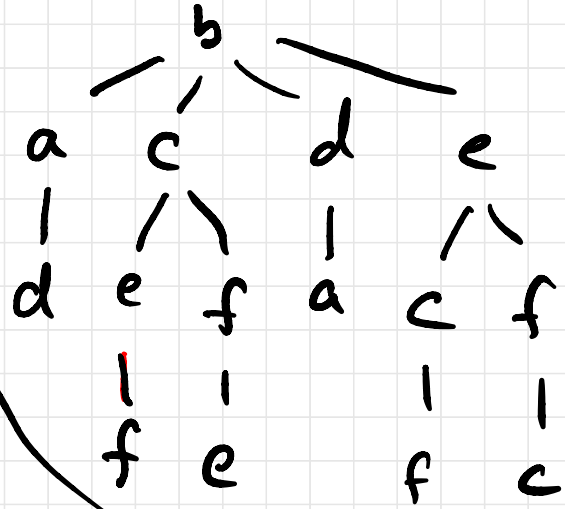
$\downarrow$

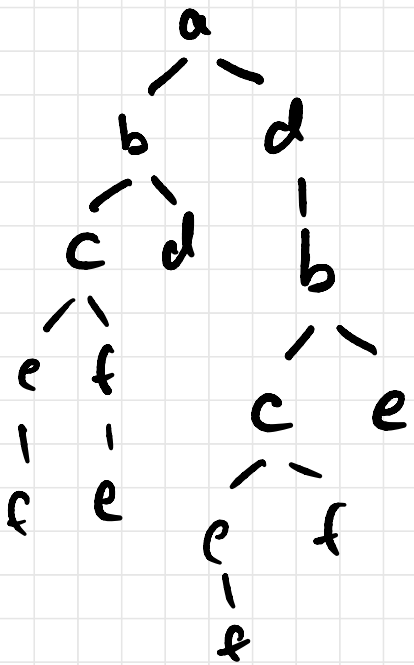
480

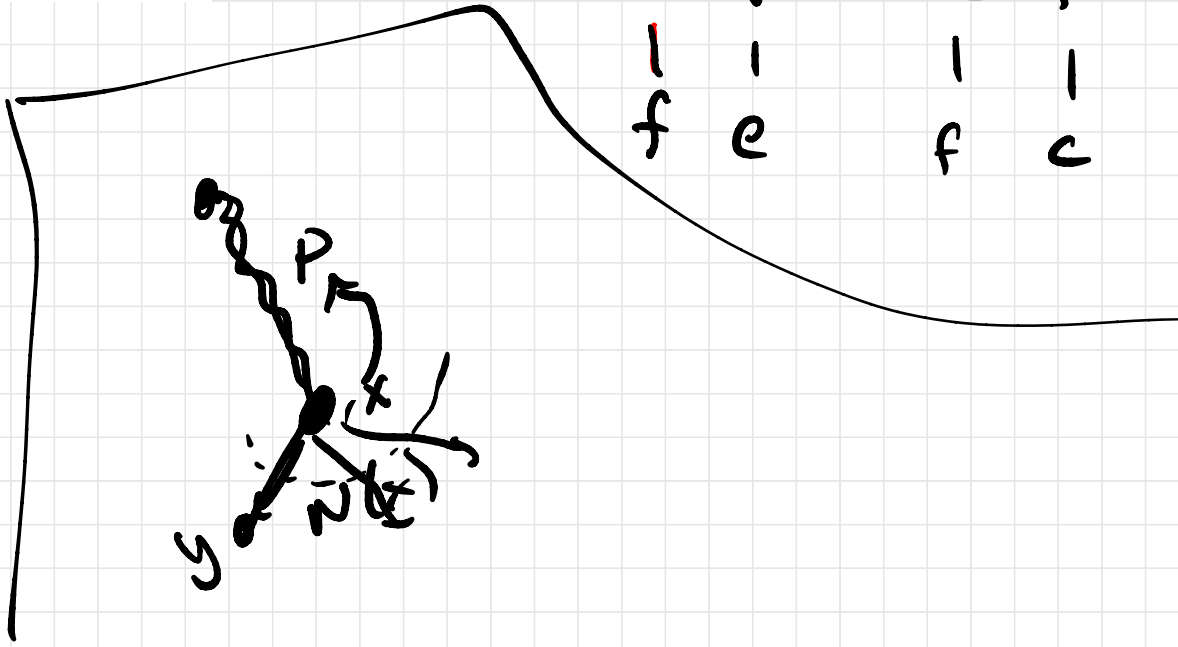
dc, a, b, e, f $\quad 5! = 120$

cd $\quad 5! \quad 120$


b
c
a
f
d
e


b
a
c
d
e
d
e
f
a
c
f
f
e
f
c


a
b
d
c
d
b
e
f
c
e
f
e
f
e


P
x
y

DFS Hamiltonian Walk – MAIN

Input: A graph $G = (V, E)$

Output: true if G contains a Ham. path

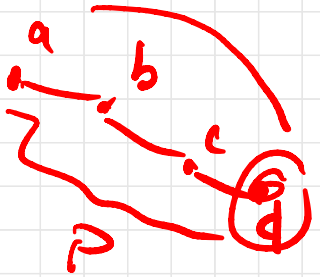
```
for each v ∈ V:
    path ← v
    if WALK(G, p):
        output true
output false
```

WALK(G, p):

Input: A graph $G = (V, E)$, a path p

Output true if G contains a Ham. path

```
if |p| = |V| - 1
    output true
x ← last vertex in p
for y ∈ N(x)
    if y ∉ p
        WALK(G, p + y)
output false
```



$N(x)$ = neighborhood of x

$|p|$ = length of the path p

$|V|$ cardinality of V

Item	Value	Weight
a_1	15	1
a_2	10	5
a_3	9	3
a_4	5	4

$W = 8$ max capacity

Knapsack

a_1	15	1	(7)
a_3	9	3	(4)
a_4	5	4	(0)
	29		

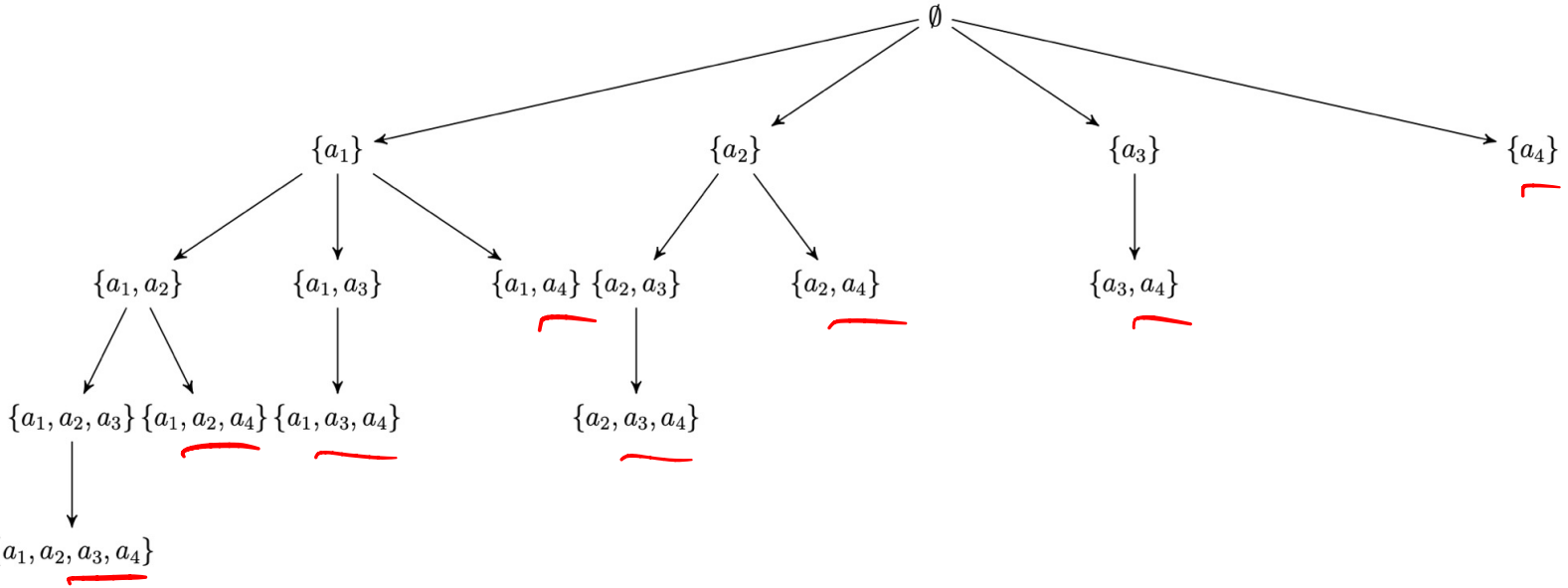
a_1	15	1
a_2	10	5
	25	6

a_2, a_4 → 9

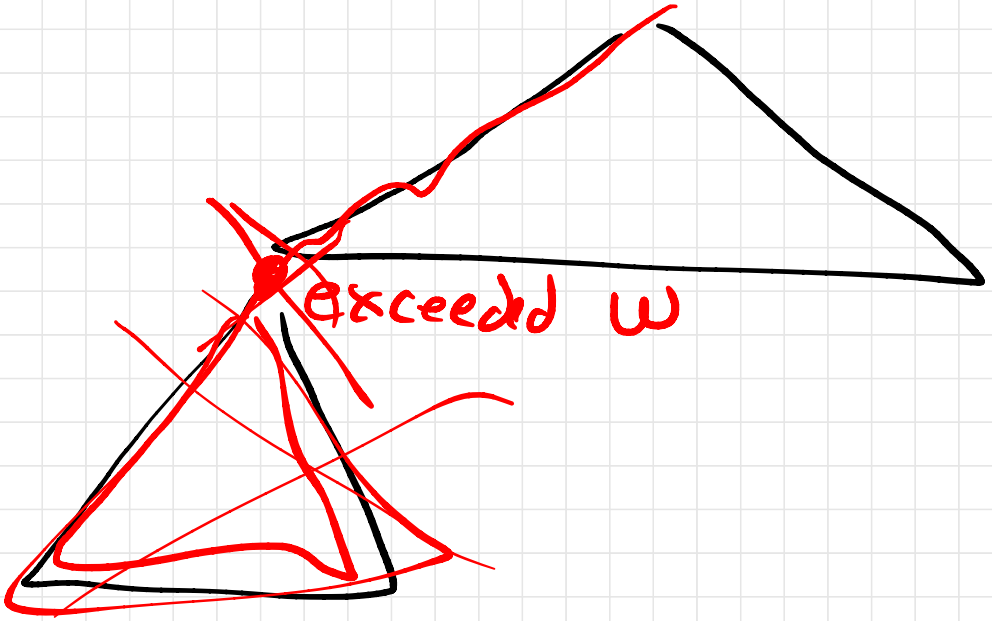
a_2, a_4, a_1

a_2, a_4, a_3

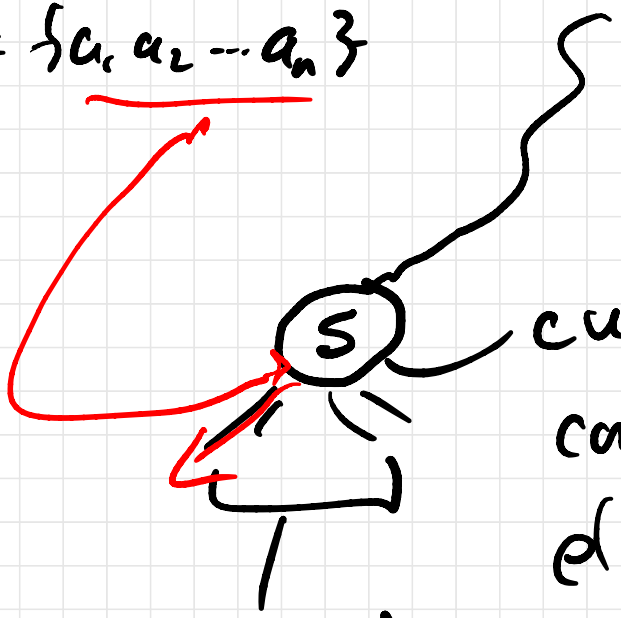
$n = 4$


∅
{a1}
{a2}
{a3}
{a4}
{a1, a2}
{a1, a3}
{a1, a4}
{a2, a3}
{a2, a4}
{a3, a4}
{a1, a2, a3}
{a1, a2, a4}
{a1, a3, a4}
{a2, a3, a4}
{a1, a2, a3, a4}

$\{a_1, a_2, a_3, a_4\}$

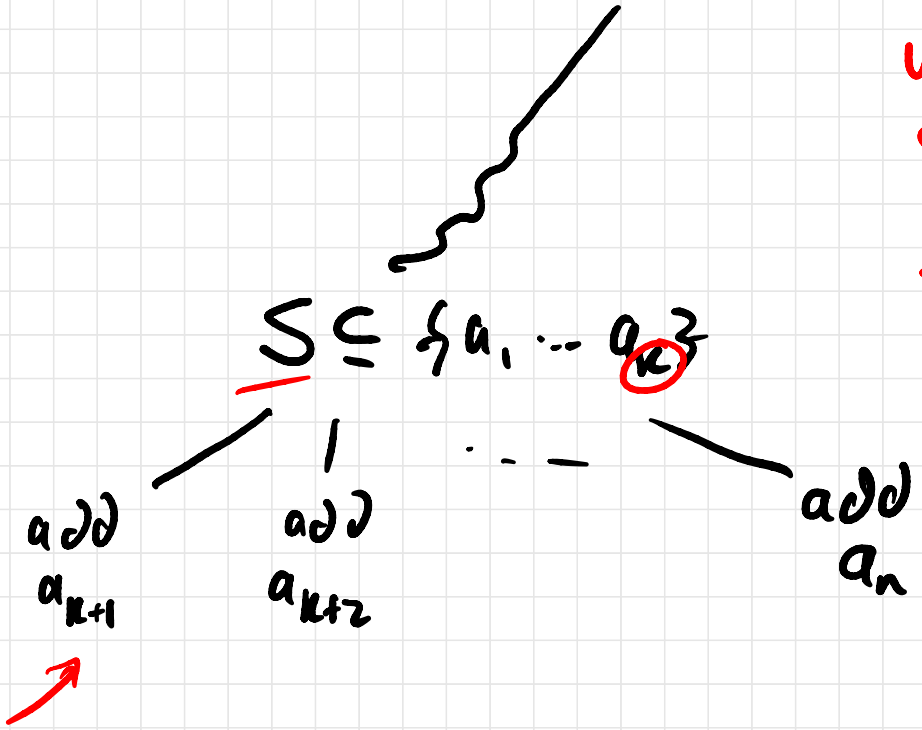

exceeded w

$A = \{a_1, a_2 \cdots a_n\}$



current subset consisting of some elements $a_1 \cdots a_k$

consider adding $a_{k+1}\ a_{k+2}\ a_{k+3} \cdots a_n$



we need:

S, the subset

A the original

k the index of elements you've considered

KNAPSACK(K, k, S)

Input: An instance of the 0-1 knapsack $K = (A, wt, val, W)$

An index k, a partial solution $S \subseteq A$ not consisting of elements indexed more than k

Output: A feasible solution <u>at least</u> as good as S

if $k = n$
  return S

$S_{best} \leftarrow S$

for $j = k+1 \dots n$

  $S' \leftarrow S \cup \{a_j\}$

  if $wt(S') \leq W$ // feasible

    $T \leftarrow$ KNAPSACK(K, j, S')

    if $val(T) > val(S_{best})$

      $S_{best} \leftarrow T$

return S_{best}

sum of vals of items in T

sum of wt's of items in S'

(if)

a b c d

{a} {b} {c}

{a b} {c}

{a c} {b}

{b, c} {a}

{a, b c}

Generalize Permutations

Ex: $P(4,2)$ permute 2 elements from a set of size 4

a b c d

a b	a c	a d	b c	b d	c d	(12)
b a	c a	d a	c b	d b	d c	

$P(n, r)$ $\quad P(n, n) = n!$

$P(n,r)$ = 1) Choose the r elements from n to arrange 2) arrange them

$$= \binom{n}{r} \times r!$$

$$= \frac{n!}{(n-r)!\,r!} \cdot r!$$

$$= \frac{n!}{(n-r)!}$$

How do you generate all possible permutations $P(n, r)$

for each r-combination C:

    output each permutation of C

Permutations with repetition:

- DNA: A G C T
- generate all DNA strings of length 3 trigrams

AAA
AAG
AAC
AAT
AGA
⋮
TTT

64

k

$d_1 d_2 \cdots d_k$

possible strings: 4^k

Symbols: $s_1\ s_2\ s_3 \cdots s_n$

$n = 2$

$s_1 = 0$

$s_2 = 1$

2^n

Given n symbols how many "strings" of length k are there?

$$\underbrace{n \cdot n \cdot n \cdots n}_{k} = n^k$$

Base 2

0000 0
0001 1
0010 2
0011 3
0100 4

Base 4

000
001
002
003
010
011
012
013
020
⋮

0 → A
1 → G
2 → C
3 → T

$d \times 10^k$

$$1874 = 1 \cdot 10^3 + 8 \times 10^2 + 7 \cdot 10^1 + 4 \cdot 10^0$$

$$\therefore \quad 2^3 \quad \downarrow \quad 2^2 \quad 2^1 \quad 2^0$$

SAT = Satisfiability

Given a typical predicate on n variables:

$P(x_1\ x_2 \cdots x_n)$ — boolean variables = 0 / 1

is there a truth setting to $\vec{x} = x_1 \cdots x_n$

such that $P(\vec{x}) \equiv 1$

1 1/0 1 1 1 0 0 0

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_3) \wedge (x_3 \vee \neg x_1) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3)$$

x_1	x_2	x_3	$P(\vec{x})$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

This is <u>not</u> satisfiable

$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee x_3)$$

x_1	x_2	x_3	$P(\vec{x})$
0	0	0	0
0	0	1	1

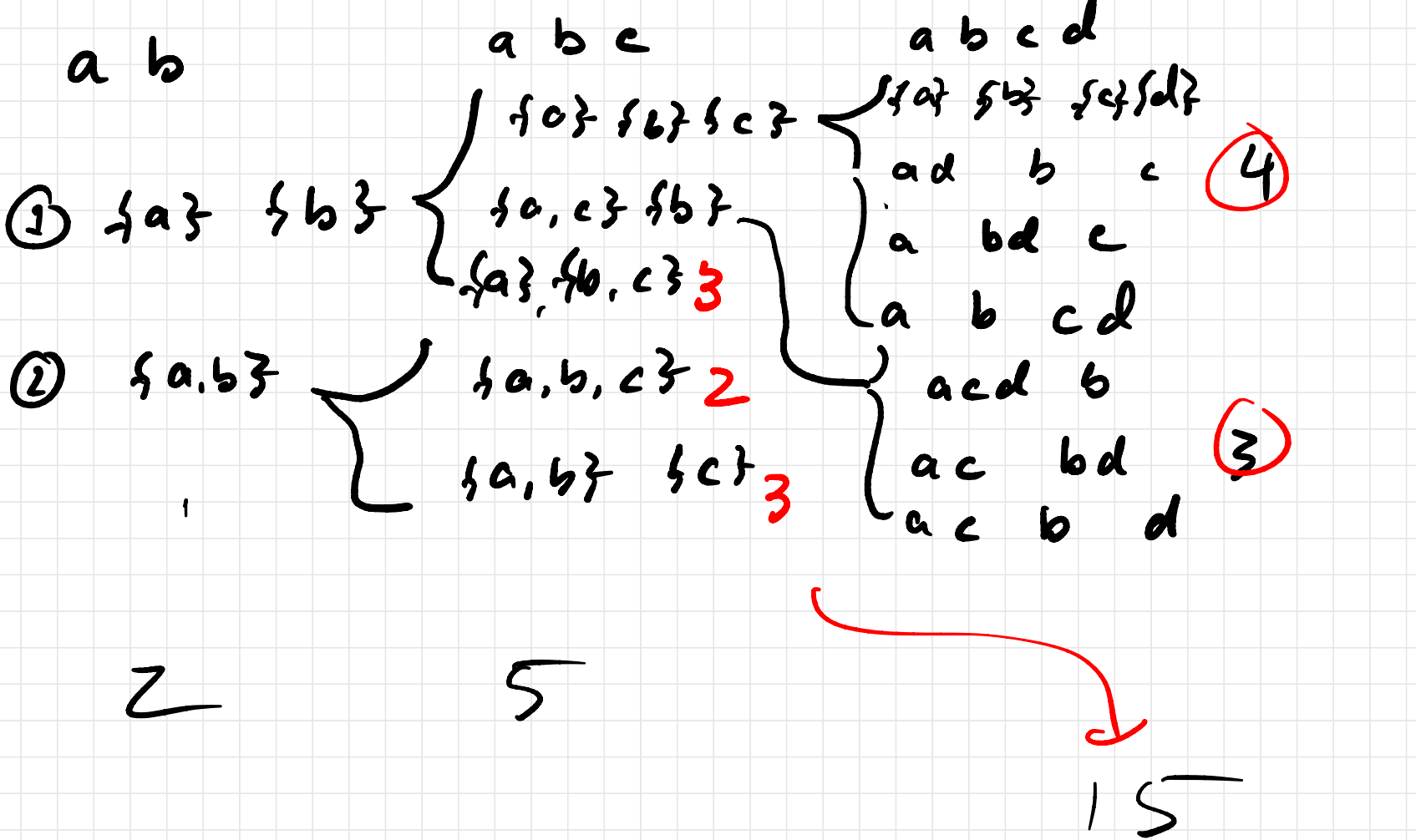
is satisfiable

If you have n variables, There are $\underline{2^n}$ possible truth assignments

$$O(2^n)$$

Set Partitions: Given n elements, $a_1 \cdots a_n$

How many ways are there to partition them into a set of subsets


a b
a b c
a b c d
{a} {b} {c} {d}
① {a} {b}
{a} {b} {c}
{a, c} {b}
{a} {b, c}
3
ad b c
4
a bd c
a b cd
② {a, b}
{a, b, c}
2
{a, b} {c}
3
acd b
ac bd
3
a c b d
2
5
15

The number of set partitions of $n+1$ elements is

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

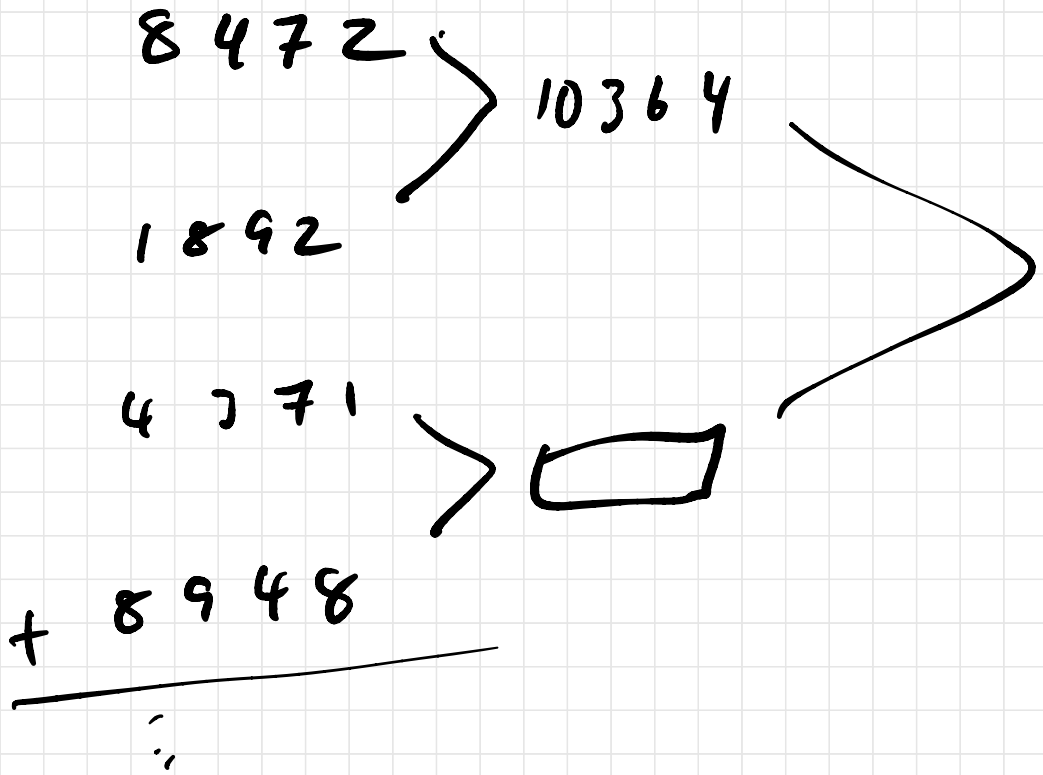
$\uparrow$

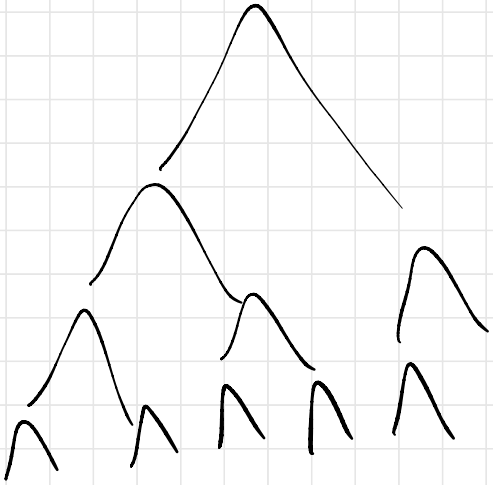
$n+1$th Bell Number

1 1 2 5 15 52 203 877

$\uparrow$ $\uparrow$ $\uparrow$ $\uparrow$

4140...


8472
1892
10364
4371
+ 8948



Theorem 4 (Master Theorem)**.** Let $T(n)$ be a monotonically increasing function that satisfies

$$\begin{aligned} T(n) &= aT(\tfrac{n}{b}) + f(n) \\ T(1) &= c \end{aligned}$$

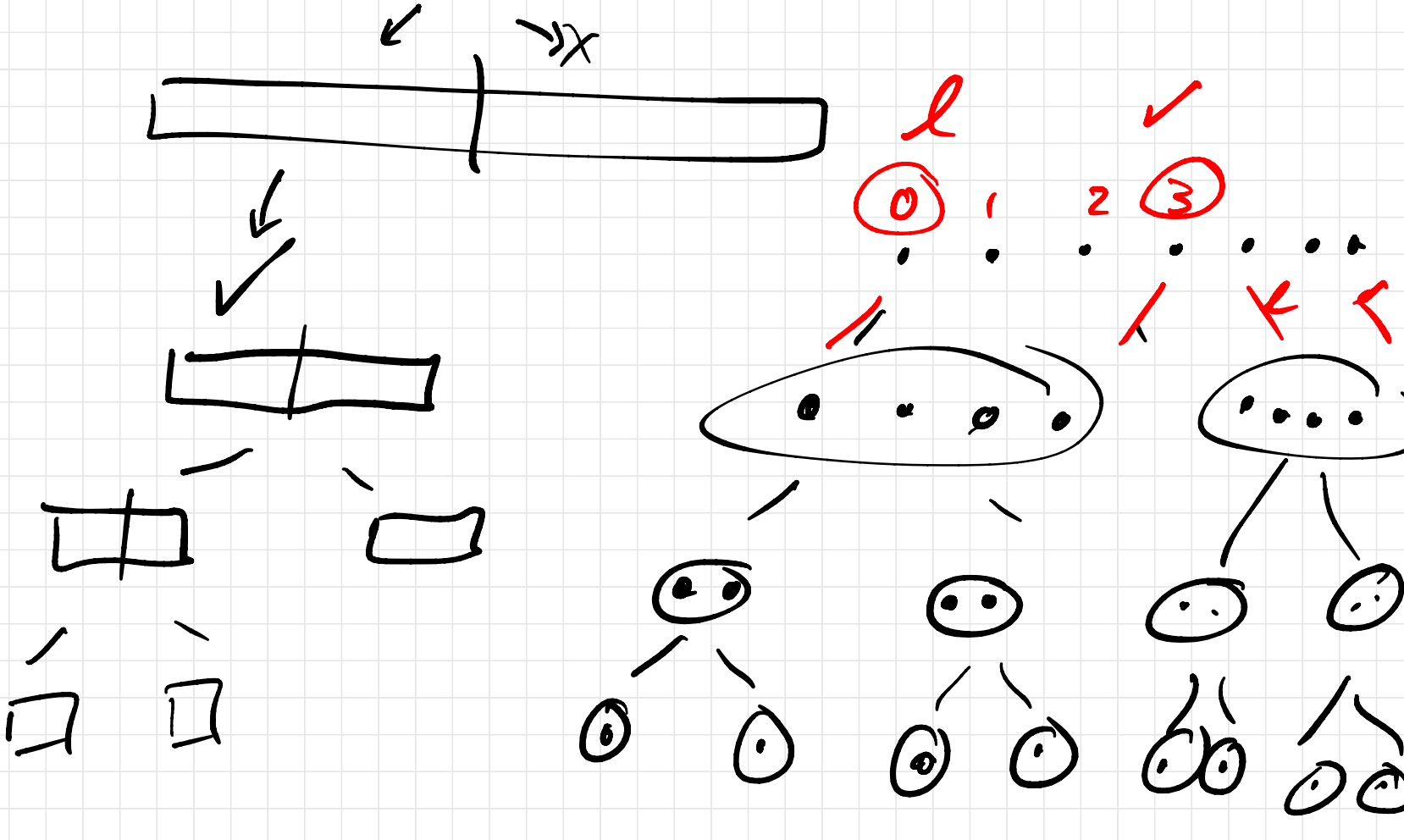
where $a \geq 1, b \geq 2, c > 0$. If $f(n) \in \Theta(n^d)$ where $d \geq 0$, then

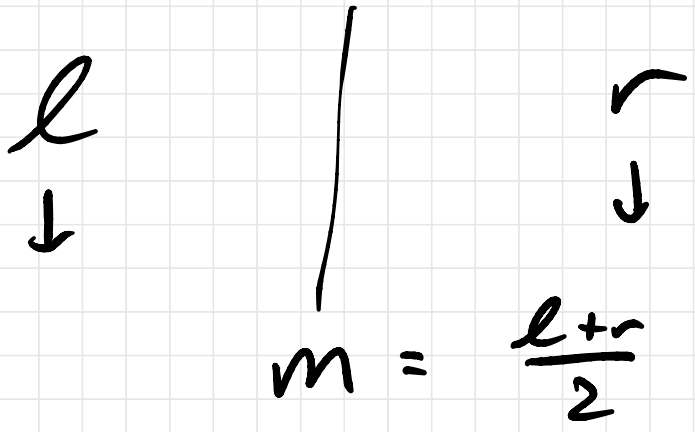
$$T(n) = \begin{cases} \Theta(n^d) & \text{if } a < b^d \\ \Theta(n^d \log n) & \text{if } a = b^d \\ \Theta(n^{\log_b a}) & \text{if } a > b^d \end{cases}$$

a: # of recursive calls

b: factor by which the input size is divided

$f(n)$ is the non-recursive code.


l
0
1
2
3



$l + \frac{r-l}{2}$

linear recursive search:

$$T(n) = \underbrace{2}_{\#\text{ of recursive calls}} T(\underbrace{n/2}_{\text{half as big}}) + \underbrace{\Theta(1)}_{f(n)}$$

$b = 2$ — $\Theta(1)$ or $O(1)$

$f(n) \in O(1)$

$T(1) = 1$

$O(1) = O(n^d)$

$d = 0$

$a = b^d$

$2 = 2^0$

$T(n) = O(n^{\log_2 2})$

$= O(n)$

Comput $a^n \bmod m$

for "very large" n

$12^{26} \bmod 17$

n is 2000 digits

$10 \bmod 3 = 1$

10 % 3

mod = modulo

= modules

$$n = \overbrace{26}^{2}$$

$$n = \overbrace{26784\cdots1872}^{100\ \text{digits}}$$

$\log_{10}(n)$ is the # of digits

$\downarrow$

$\log_2(n)$ # of bits

n is the input

$\log(n)$ is the input size

$$N = \log(n) \Rightarrow 2^N = n$$

$$O(n) = O(2^N)$$

$$a^{26} = a^{16} \cdot a^{8} \cdot a^{2}$$

a^1

$a \cdot a \cdot a \cdot a$

$a \cdot a = a^2$ 1 mult

$a^2 \cdot a^2 = a^4$ 1 mult.

$a^4 \cdot a^4 = a^8$ 1

$a^8 \cdot a^8 = a^{16}$ 1

2

6 mults

$O(\log_2(n))$ → ~~logarithmic~~? linear

Nope

n input

$N = \log_2(n)$ input size

$O(\log(n)) = O(N)$ linear

Binary Exponentiation or Repeated Squaring

Input: a, n, m;

Output $a^n \bmod m$

$n = b_k b_{k-1} \cdots b_0$ ← ↓

b_k: high order; b_0: lowest order bit.

term = a

if $b_0 = 1$

  product = a

else

  product = 1

for $i = 1 \ldots k$

  term = $term^2 \bmod m$

  if $b_i = 1$

    product = (product · term) mod m

output product

$12^{26} \bmod 17$

$26 = 11010$

16	8	4	2	1
1	1	0	1	0
b_4	b_3	b_2	b_1	b_0

$$12^{26} = 12^{2^4 \cdot b_4} \cdot 12^{2^3 \cdot b_3} \cdot 12^{2^2 \cdot b_2} \cdot 12^{2^1 \cdot b_1} \cdot 12^{2^0 \cdot b_0}$$

$b_4 = 1$, $b_3 = 1$, $b_2 = 0$, $b_1 = 1$, $b_0 = 0$

Square

Square and multiply

$12^{16} \cdot 12^{8} \cdot 12^{2}$

a >> 1 shifts bits of a left by 1 (divides by 2)

a & 1 → gives you the lowest order bit

60

$2 \cdot 2 \cdot 3 \cdot 5$

$2^2 \cdot 3 \cdot 5$

210

$2 \quad 3 \quad 5 \quad 7$

$2 \cdot 3 \cdot 5 \cdot 7$

$2 \cdot 3 \cdot 5 = 30$

$2 \cdot 5 \cdot 7 \cdot 11$

770

$3 \cdot 13 \cdot 17$

663

$$\gcd(770, 663) = 1$$

1768 184

a b

$1768 = 184 \cdot 9 + 112$

gcd must divide all 3

$\gcd(1768, 184) = \gcd(184, 112)$

$184 = 112 \cdot 1 + 72$

$112 = 72 \cdot 1 + 40$

$72 = 40 \cdot 1 + 32$

$40 = 32 \cdot 1 + 8$

$32 = 8 \cdot 4 + 0$

gcd of (184, 1768) has to divide both

Euclid - simple

Input: $a, b \in \mathbb{Z}^+$

Output: $\gcd(a, b)$

```
1  while b ≠ 0
2  |   t ← b
3  |   b ← a mod t
4  |   a ← t
5  output a
```

1) Input: WLOG $b > a$

2) size: $\log_2(b)$

3) Elem. op: line 3 division

// %

// remainder of a/t

4) how many times is line 3 executed?

- Worst case scenario:

  maximize the # of iterations

what "choice" of b keeps:

$$\frac{x}{b}$$

"big" $\Rightarrow$ make b as small as possible

$$\frac{\frac{\frac{b}{2}}{2}}{2} = 1$$

n = # of iterations

$$b \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} = 1$$

$$\frac{b}{2^n} = 1 \qquad b = 2^n$$

$$n = \log_2(b)$$

- #of iterations is <u>at most</u> $\log_2(b)$
  - input size is $\log_2(b) = N$
  - 5) Euclid is $O(\log_2(b)) = O(N)$ (linear)

Input: a, b

$a_0 = a,\ b_0 = b$

$t_0 = 0,\ t = 1$

$s_0 = 1,\ s = 0$

$q = \lfloor a_0 / b_0 \rfloor$

$r = a_0 - q \cdot b_0$

while $r > 0$

$\quad temp = t_0 - qt$

$\quad t_0 = t,\ t = temp$

$\quad temp = s_0 - qs$

$\quad s_0 = s,\ s = temp$

$\quad a_0 = b_0,\ b_0 = r$

$\quad q = \lfloor a_0 / b_0 \rfloor,\ r = a_0 - q b_0$

$\quad$ if $r > 0$

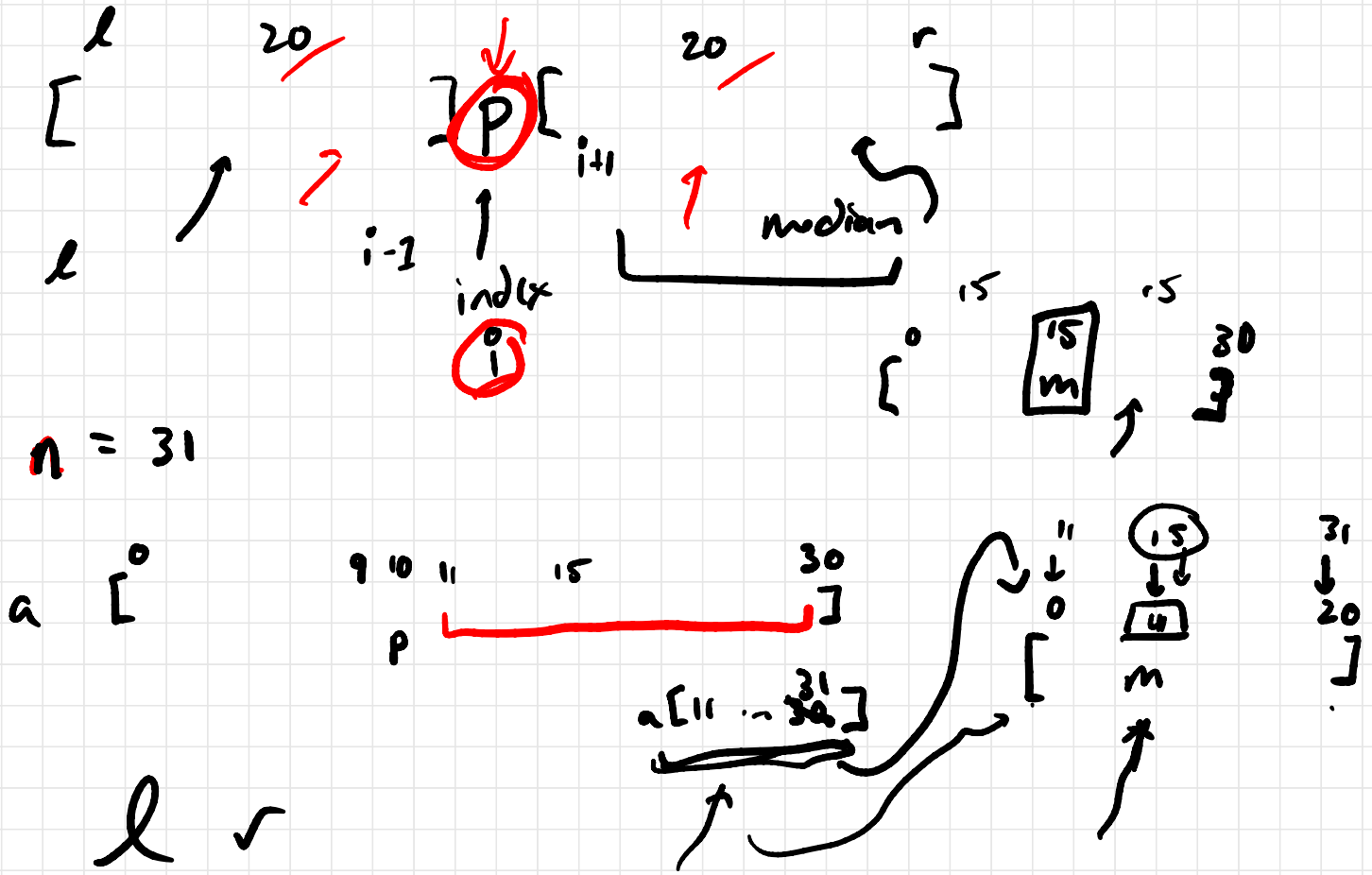
$\quad\quad g = r$

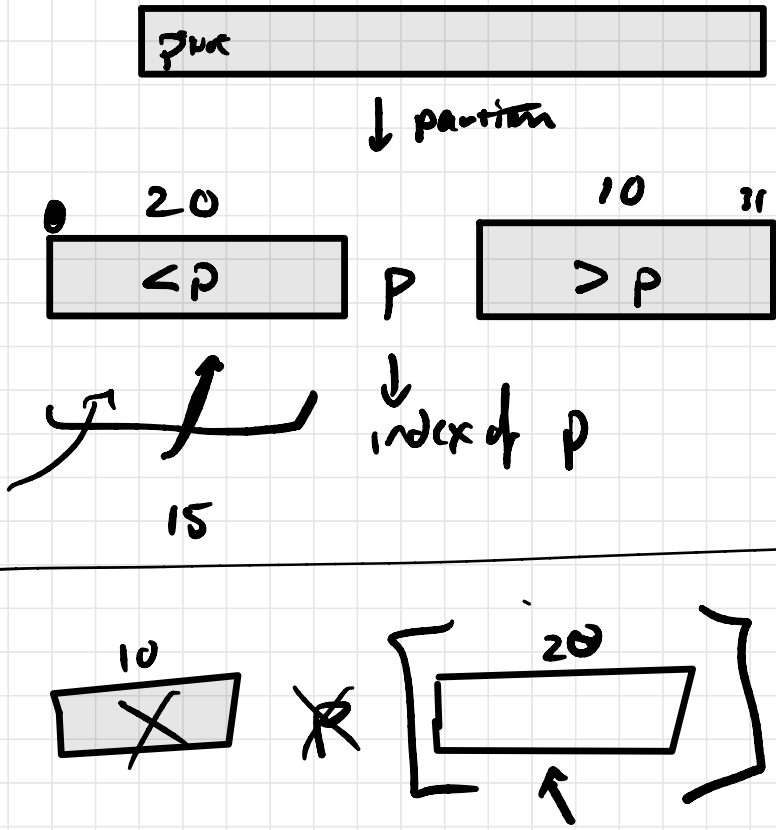
output g, s, t

Note:

$g = \underline{s} \cdot a + \underline{t} \cdot b$

gcd


l
20
p
20
r
i+1
i-1
median
index
0
i
n = 31
15
15
m
30
a
0
9 10 11 15 30
p
11
15
4
m
31
20
a[11 .. 31]
l r

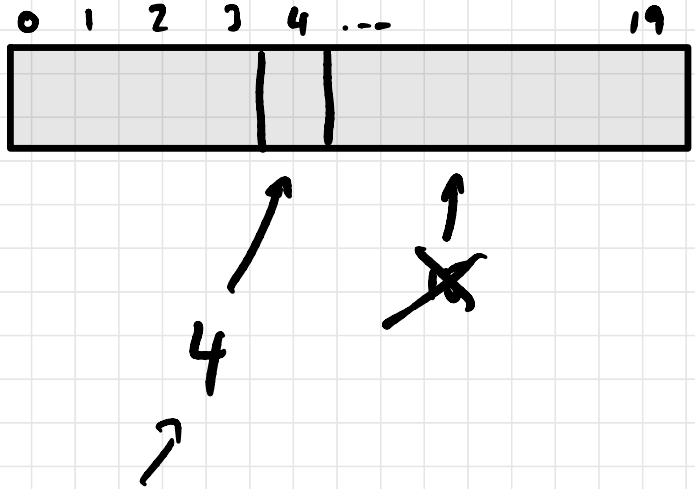


n = 31

index of median: if sorted

15

11



$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ ← integer remainders of mod m

Ex: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbb{Z}_m$ for any $m \geq 2$ is a ~~"ring"~~ "group"

Algebraic Structure:

- closure $x, y \in \mathbb{Z}_m$, $x + y \pmod m$ is in $\mathbb{Z}_m$

$x \cdot y \pmod m \in \mathbb{Z}_m$

$\mathbb{Z}_6$:

$2 + 5 \mod 6 = 1$

$2 \times 5 \mod 6 = 4$

- Addition identity: 0

$\forall a \in \mathbb{Z}_m, \quad 0 + a = a \in \mathbb{Z}_m$

- mult. identity: 1

$\forall a \in \mathbb{Z}_n \quad 1 \cdot a = a$

- Addition inverse:

$$\forall x \in \mathbb{Z}_m \; \exists y \quad x + y = 0$$

$\mathbb{Z}_m$:

x		y
0	$\longrightarrow$	0
1	$\longrightarrow$	5
2	$\longrightarrow$	4
3	$\longrightarrow$	3
4	$\longrightarrow$	2
5	$\longrightarrow$	1

- Multiplication Inverse? (x other than 0)

$x \in \mathbb{Z}_m$, $\exists^{?} x^{-1}$ such that $x \cdot x^{-1} = 1$

$\mathbb{Z}_6$

x	x^{-1}
1	1 ✓
2	DNE = Does not exist
3	DNE
4	DNE
5	$5 = 5^{-1}$

$3 \longrightarrow$ $2 \cdot 3 \bmod 6 = 0$ DNE

$3 \cdot 3 \bmod 6 = 3$

$3 \cdot 4 \bmod 6 = 0$

$3 \cdot 5 \bmod 6 = 3$

$25 \bmod 6 = 1$

$x^{-1} = \frac{1}{x}$ $\mathbb{Q}$ rationals

$\mathbb{Z}_m$

Fact: $x \in \mathbb{Z}_m$, a multiplicative inverse x^{-1} exists iff x and m are relatively prime: iff $\gcd(x, m) = 1$

$$x \cdot x^{-1} = 1$$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ $\mathbb{Z}_p$ is a "field"

$0 \longrightarrow$ no mult. inverse

$1 \longrightarrow 1$ is always its own inverse

$2 \longleftrightarrow 4$

$3 \longleftrightarrow 5$

$6 \longleftrightarrow 6$

$x \cdot y \rightarrow x \cdot y\, y^{-1} = x \cdot 1 = x$