

2. 多項式時間計算量

来嶋 秀治

滋賀大学 データサイエンス学部

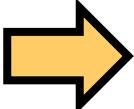
“Valiant計画” (since 1979)

#P困難な $A \in \mathbb{R}$ に対して、近似解 $Z \in \mathbb{R}$ を精度

$$\Pr[(1 - \epsilon)A \leq Z \leq (1 + \epsilon)A] \geq 1 - \delta$$

で多項式時間($\text{poly}(\text{input}, \epsilon^{-1}, \log \delta^{-1})$)で求められるか？

多項式時間(polynomial time)とは何が多項式なのか？

 「演算」の回数

「計算量」(決定性 Turing machine)

通常(形容詞のない場合)は
worst case time complexityを指す

□ 計算量 = 演算回数(有限回に限る)

- 読み込み, 書き出し, 代入, 比較: $O(\text{行数})$
- 四則演算(+, -, ×, /) $O(\text{行数}) \sim O(\text{行数}^2)$
- 論理演算($\neg, \wedge, \vee, \Rightarrow$) $O(1)/1$ 演算
- 繰り返し(for, while)は繰り返し中の演算の総数
- 「パラメータ」
 - 固定(定数)なら $O(1)$
 - 可変なら四則演算に準ずる
- 「関数(ライブラリ)」
 - 計算量が解明されていれば, それに準拠
 - オラクル計算量では, 通常の演算数とは別に数える

「計算」を掘り下げる

若干(?) 嘘を含むので注意

Turing machine

□ できること

- 有理数の四則演算
- 論理演算 ($\Rightarrow, \wedge, \vee, \neg, T, \perp$; 例: $1 \vee 0 = 1, 1 \wedge 0 = \perp$)
- 受理、非受理の判定 (If文)
- 大きな数が数えられる (=メモリがある: While文、For文)
- 配列

□ できないこと

- 実数 (無理数一般) の計算 (二次方程式の解の公式とか)
- 「難しい」関数の計算: $\sin, \cos, \tan, \exp, \log, \text{etc.}$
- 微分、積分 (一般に)
- 二階述語論理 (停止性問題)

➤ 何をどこまで計算可能か都度確認。

Pythonではmathをimportしてexp(x)は計算できる!?

$$\exp(3) \simeq 2.718 * 2.718 * 2.718$$

$$\exp(1.5) \simeq \sqrt{2.718 * 2.718 * 2.718} \text{ (開平根)}$$

$$\exp(1.7) \simeq \sqrt[10]{\left(\left((2.718^2)^2\right)^2\right)^2 * 2.718}$$

$$\exp(x) = 1 + \frac{1}{2}x^2 + \frac{1}{3!}x^3 + \dots$$

「計算」を掘り下げる

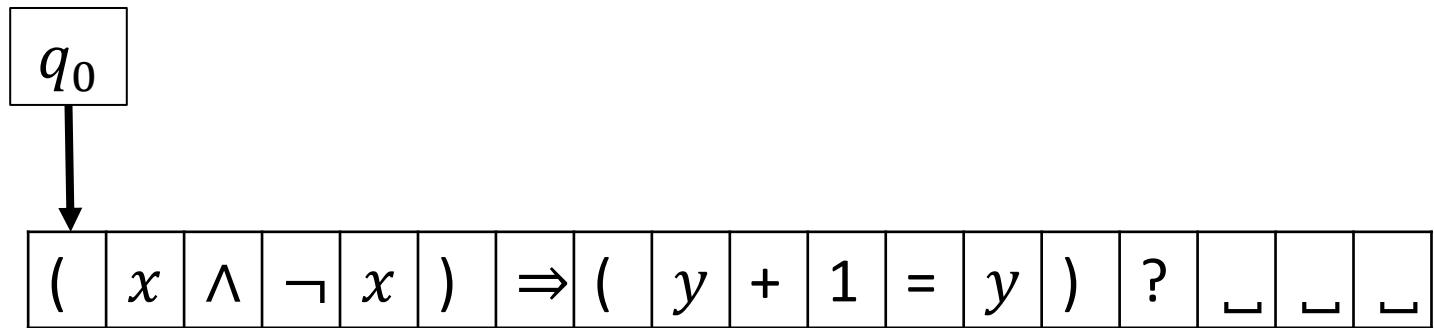
□ 計算 = accept-rejectの決定

□ 入力 = 文字列

□ なぜ「多項式」時間？

➤ 等価性、帰着

計算機科学における計算: Turing machine



Turing machine

- headerとtapeで構成された機械
 - 決められた規則に従って動作する
- headerは有限個の演算規則集(有限オートマトン)
- tapeはメモリ
 - 文字を読んだり書いたり(書き換えたり)できる。長さに上限がない
- 文字は有限種類
- 最終的に、accept(正しい) or reject(間違い)を判断して停止
 - 判断できない計算問題が存在する(Turingの停止問題)

計算機科学の歴史 (NP以前)

1874, Cantor, $\infty^n \neq 2^\infty$, 対角線論法

1900, Hilbert, 算術の無矛盾性 (23問題)

1931, Gödel, 不完全性定理

1936, Turing, Turing機械 + 停止問題

1936, Church, ラムダ計算

1945, von Neumann, ノイマン型コンピュータ(ENIAC)

1956, Kleene, regular language = finite automaton判定

1956, Chomsky, Chomsky階層

1971, Cook, NP完全の提案

Turing machineの先祖は論理学

Hilbert計画(1900)

数学が正しいことを証明せよ

- 形式証明: 論理演算規則による変形

(例) 命題: $\forall x, \forall y, [\text{even}(x) \wedge \neg\text{even}(y) \rightarrow \text{even}(x + y)]$ (偶数+奇数=偶数)

証明:

$$\text{even}(x) \Rightarrow \exists a(x = 2a)$$

$$\neg\text{even}(y) \Rightarrow \exists b(y = 2b + 1)$$

$$(x = 2a) \wedge (y = 2b + 1) \Rightarrow (x + y = 2(a + b) + 1)$$

$$\exists c(x + y = 2c + 1) \Rightarrow \neg\text{even}(x + y)$$

$$\neg\text{even}(x + y) \wedge \text{even}(x + y) = \perp$$

- 証明できればaccept (=定理), 矛盾が出ればreject

Gödel(1931):

証明とは数字(Gödel数)の計算である. 計算できない命題が存在する.

計算機科学(Turing(1936), Kleene(1956), Chomsky(1956), ...?):

計算とは文字列のaccept-rejectの決定である. 決定できない文字列が存在する.

「計算」を掘り下げる

- 計算 = accept-rejectの決定
- 入力 = 文字列
- なぜ「多項式」時間 ?
 - 等価性、帰着

言語の認識

- Σ : 文字の集合(alphabet)
- Σ^k : 長さ k の文字列の集合. $\Sigma^* = \bigcup_{k=0}^{\infty} \Sigma^k$
- $\mathcal{L} \subseteq \Sigma^*$: 言語(language)
- $w \in \mathcal{L}$: 語(word)
- $w \in \mathcal{L}$ を accept し, $w \notin \mathcal{L}$ を reject できることを recognition という.

定理 (Kleene 1956)

正規言語であることの必要十分条件は**有限オートマトン**で recognize できる言語

$\Sigma = \{0,1\}$ とする.

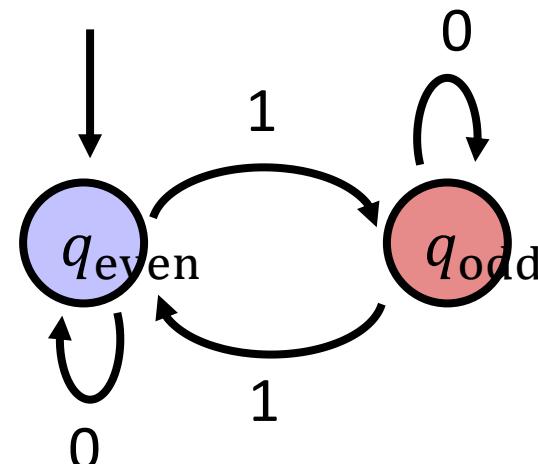
□ 正規言語の例

- $\{w | w \text{の最初と最後は同じ文字}\} = 0\Sigma^*0 \cup 1\Sigma^*1 \cup 0 \cup 1$
- $\{w | w \text{の長さは3の倍数}\} = (\Sigma\Sigma\Sigma)^*$
- $\{w | w \text{は1を偶数個もつ}\}$

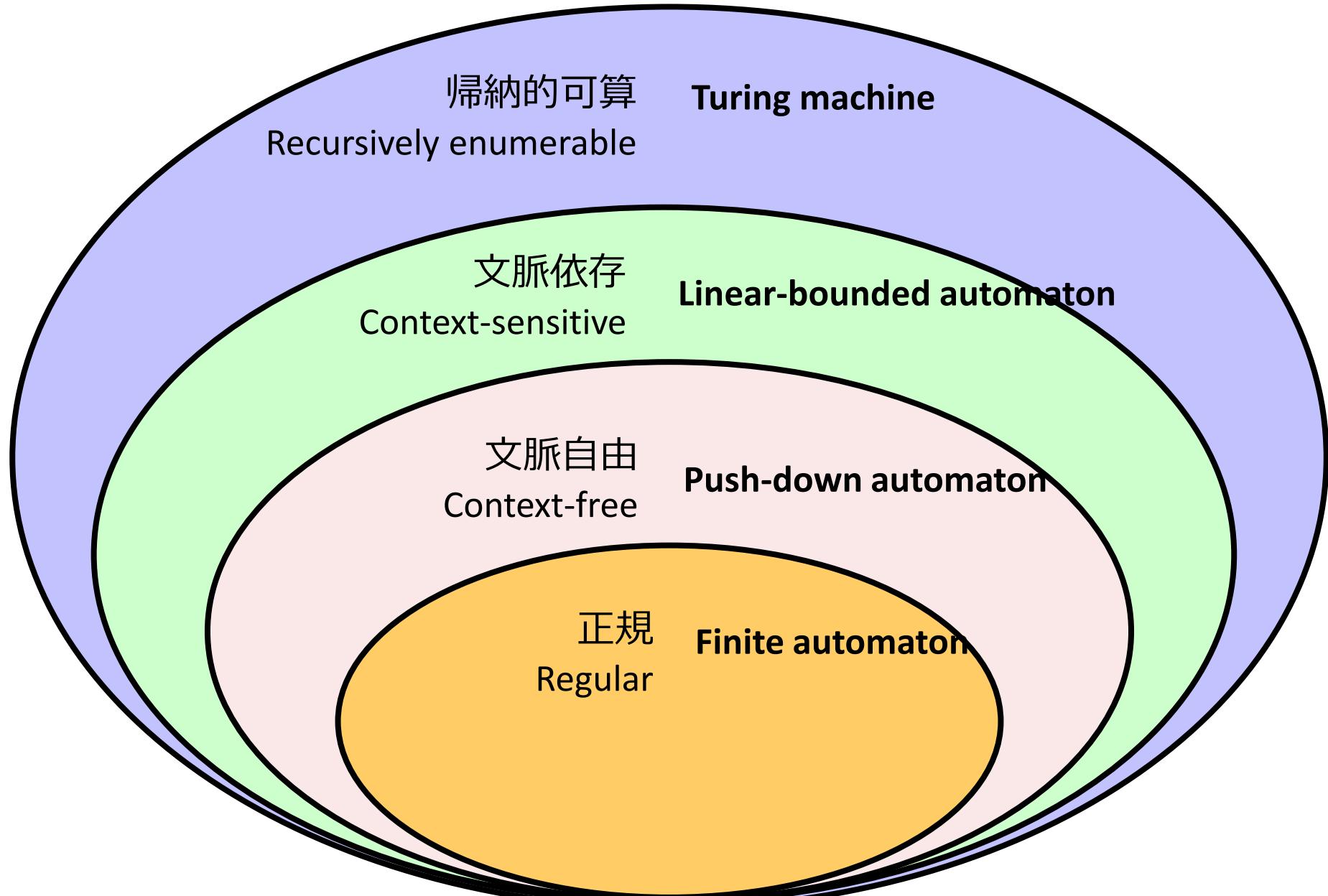
□ 正規言語でない例

- $\{0^n 1^n | n \geq 0\}$
- $\{w | w \text{は0と1を同数もつ}\}$

有限オートマトンは
大きな数を数えられない



Chomsky hierarchy



決定問題(decision problem)

例1. グラフ3彩色

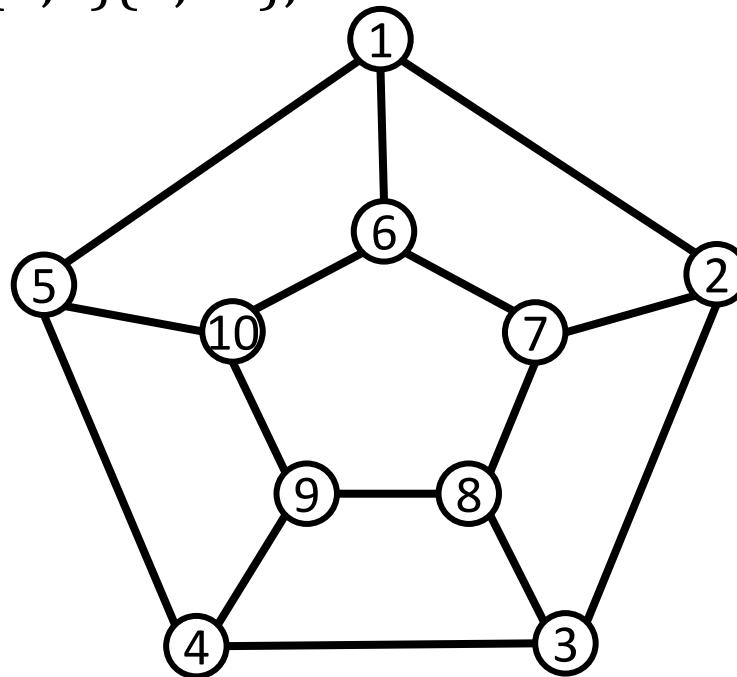
入力: $G = (V, E)$

問題: G は3色で塗り分けられるか ?

$\mathcal{L} \subseteq \Sigma^* = \{0, \dots, 9, \{, \}, :, ;\}$: グラフ3彩色言語

$w = 10: \{1,2\}\{1,5\}\{1,6\}\{2,3\}\{2,7\}\{3,4\}\{3,8\}\{4,5\}\{4,9\}\{5,10\}$
 $\{6,7\}\{6,10\}\{7,8\}\{8,9\}\{9,10\};$

$w \in \mathcal{L}$



決定問題(decision problem)

例1. グラフ3彩色

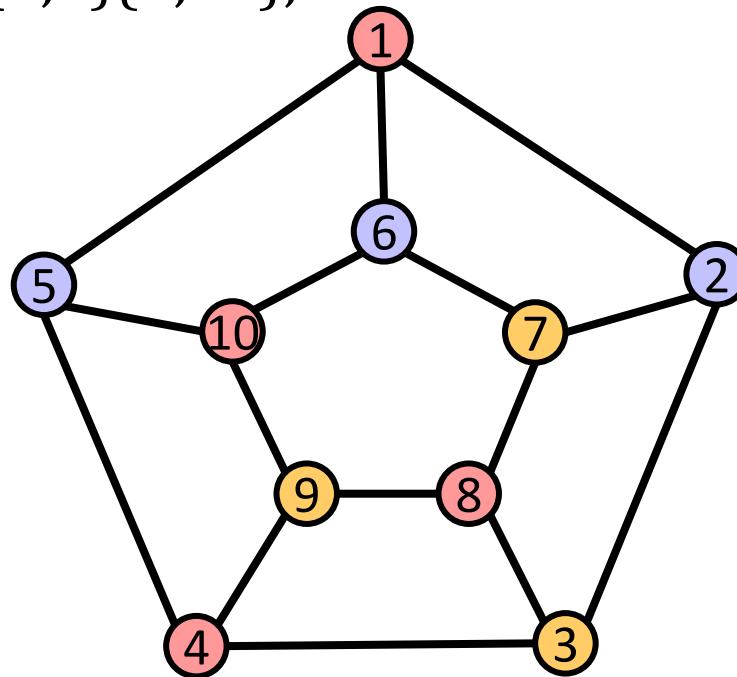
入力: $G = (V, E)$

問題: G は3色で塗り分けられるか ?

$\mathcal{L} \subseteq \Sigma^* = \{0, \dots, 9, \{, \}, :, ;\}$: グラフ3彩色言語

$w = 10: \{1,2\}\{1,5\}\{1,6\}\{2,3\}\{2,7\}\{3,4\}\{3,8\}\{4,5\}\{4,9\}\{5,10\}$
 $\{6,7\}\{6,10\}\{7,8\}\{8,9\}\{9,10\};$

$w \in \mathcal{L}$



決定問題(decision problem)

例1. グラフ3彩色

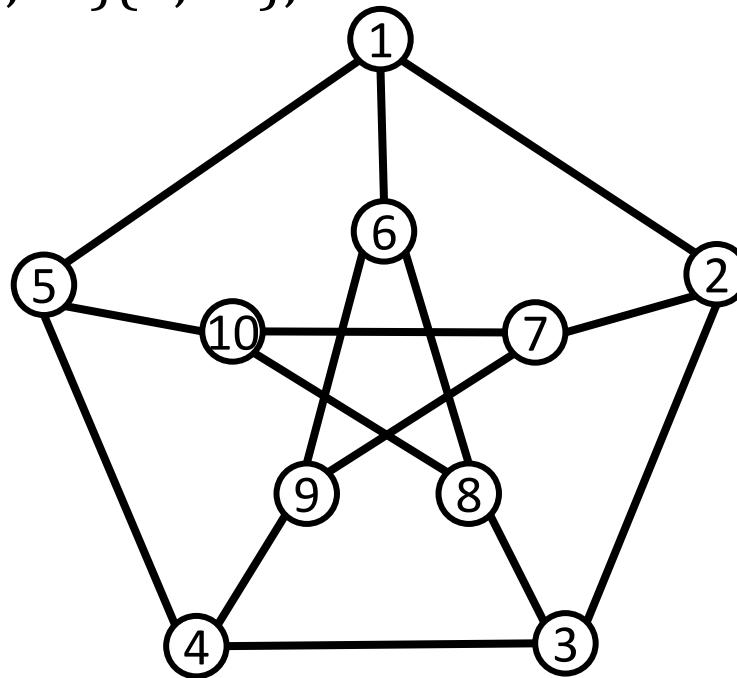
入力: $G = (V, E)$

問題: G は3色で塗り分けられるか ?

$\mathcal{L} \subseteq \Sigma^* = \{0, \dots, 9, \{, \}, :, ;\}$: グラフ3彩色言語

$w = 10: \{1,2\}\{1,5\}\{1,6\}\{2,3\}\{2,7\}\{3,4\}\{3,8\}\{4,5\}\{4,9\}\{5,10\}$
 $\{6,8\}\{6,9\}\{7,9\}\{7,10\}\{8,10\};$

$w \notin \mathcal{L}$



例2. Partition (cf. 0-1ナップサック問題)

入力: 整数 $z_1, z_2, \dots, z_n; k$.

問題: 合計が k となる組合せは存在するか?

例: 2,3,5,7,11,13,17,19; 38.

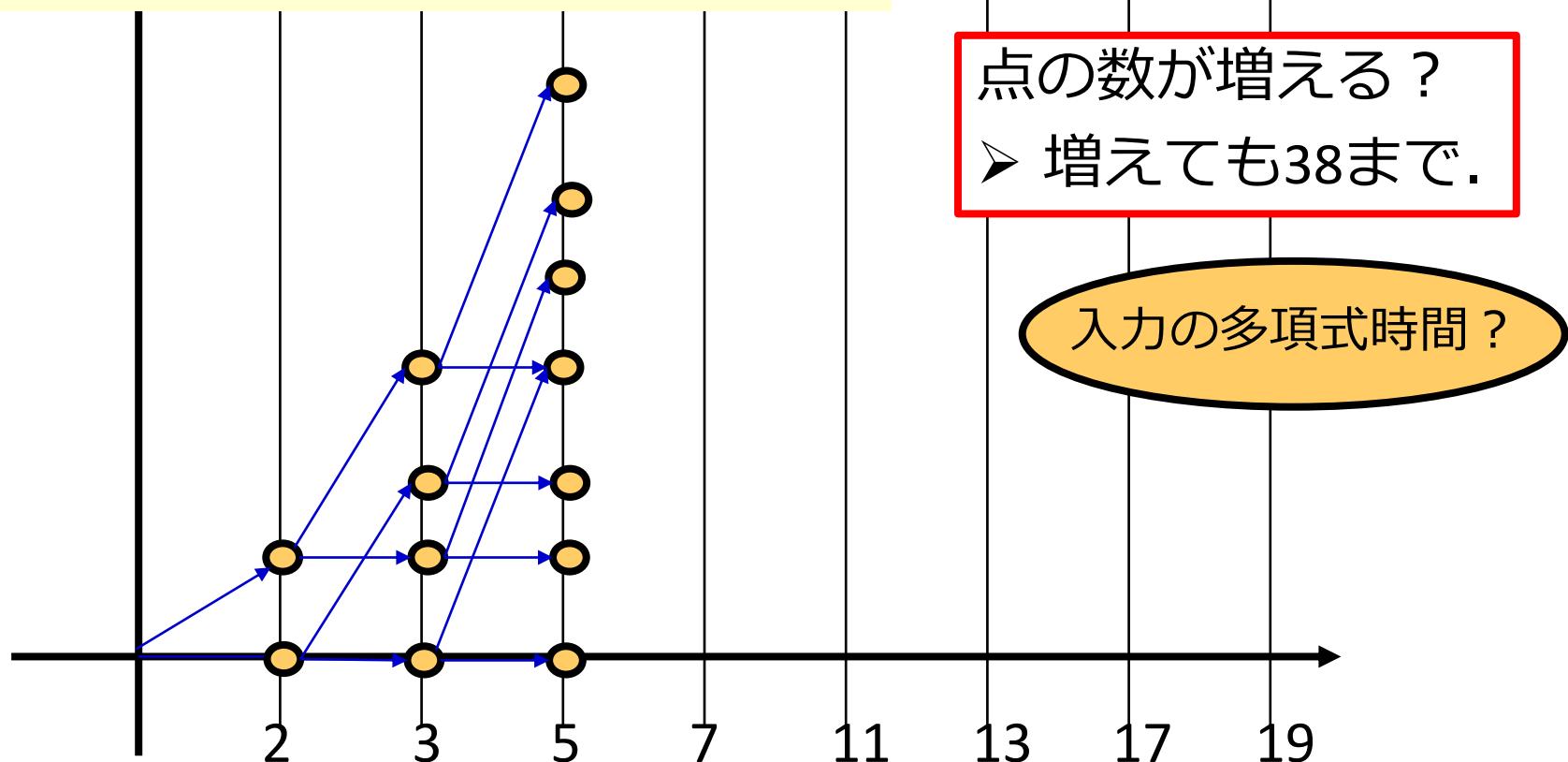
例2. Partition (cf. 0-1ナップサック問題)

入力: 整数 $z_1, z_2, \dots, z_n; k$

問題: 合計が k となる組合せは存在するか?

例: 2,3,5,7,11,13,17,19; 38.

動的計画法(dynamic programming; DP)



例2. Partition (cf. 0-1ナップサック問題)

入力: 整数 $z_1, z_2, \dots, z_n; k$

問題: 合計が k となる組合せは存在するか?

例: 271,314,141,200,223,264,316,331; 1008.

動的計画法(dynamic programming; DP)

点の数が増える?

➤ 増えても1008まで.

入力の多項式時間?

例2. Partition (cf. 0-1ナップサック問題)

入力: 整数 $z_1, z_2, \dots, z_n; k$

問題: 合計が k となる組合せは存在するか?

例,

27493847264785763747,
11048534940392845843,
24349209340394059321,
14330594095049538497,
19134704294349044340,
19417344368134910019,
22233434958080520924,
17000000000000000000;
74076491623349079329.

点の数が増える?

➤ 増えても 74076491623349079329まで.

入力の多項式時間?

入力サイズは桁数で数える.

数え上げ問題 [Valiant 79]

決定問題の特に計算量の議論は多分に組合せ論的である.

- たとえばNP完全問題の難しさは、膨大な組合せの中から条件に合う解を見つける難しさに起因する.

組合せ論の興味の中心は、すばり、組合せの個数である.

決定問題の解の個数は数えられるのであろうか？

$w \in \mathcal{L}$ に対し、

$$\mathcal{C}(w) \subseteq \Sigma^*$$

を w の“解”の集合とする.

計算量理論の枠組みでは
Certificateとかwitness
と呼ばれる.

Q. $w \in \mathcal{L}$ が与えられた時、 $|\mathcal{C}(w)|$ を求めよ.

数え上げ問題 (counting problem)

例1. グラフ3彩色

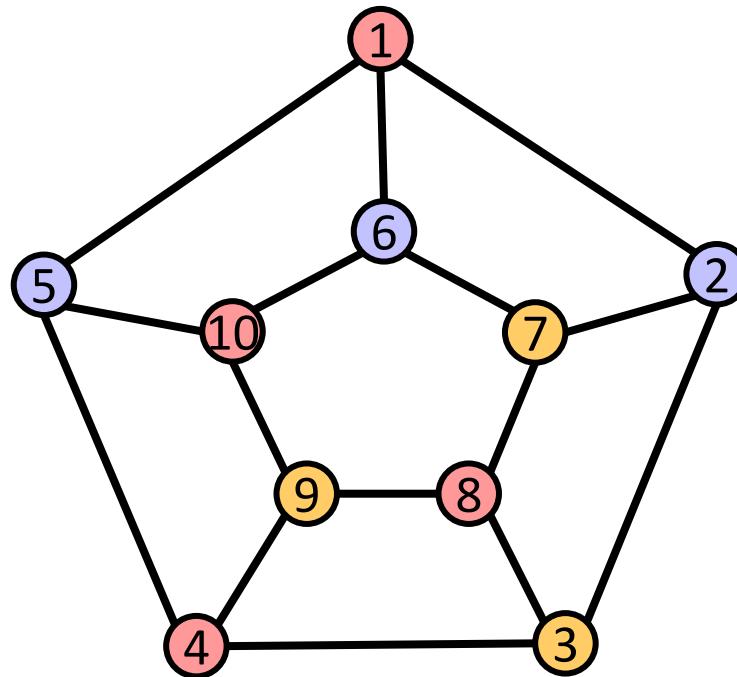
入力: $G = (V, E)$

問題: G は3色で塗り分けられるか?

$$\mathcal{C}(w) \subseteq \{r, b, y\}^{10}$$

$$rbryrbbyryrc \in \mathcal{C}(w)$$

計算量理論の枠組みでは
Certificateとかwitness
と呼ばれる.



数え上げ問題 (counting problem)

例1. グラフ3彩色

入力: $G = (V, E)$

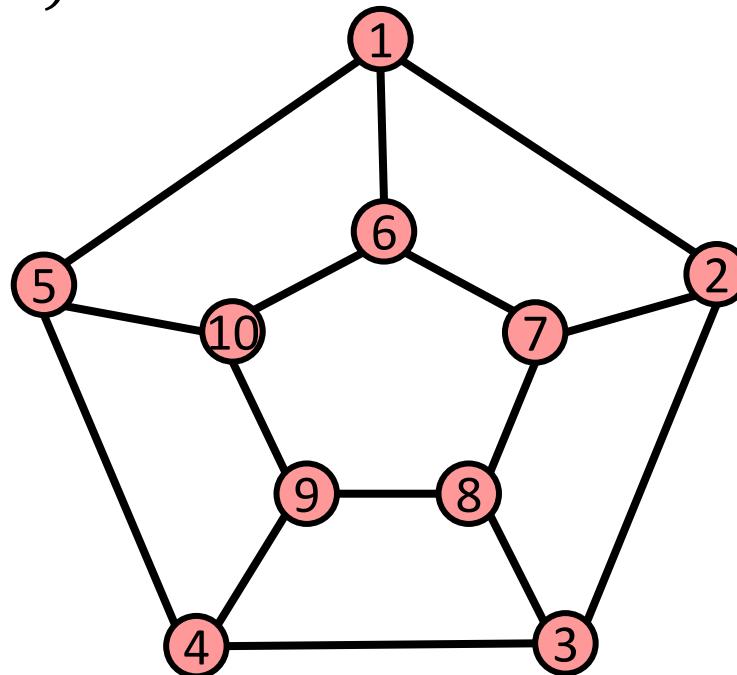
問題: G は3色で塗り分けられるか?

$$\mathcal{C}(w) \subseteq \{r, b, y\}^{10}$$

$$rbryrbbyryrc \in \mathcal{C}(w)$$

$$rrrrrrrrrrrr \notin \mathcal{C}(w)$$

計算量理論の枠組みでは
Certificateとかwitness
と呼ばれる.



計算機科学のMCMC法

計算量クラス #P [Valiant '79]

\mathcal{L} がNPに属するとき, $w \in \mathcal{L}$ に対し,
 $\mathcal{C}(w) \subseteq \Sigma^*$ を w のcertificateの集合とする.
 $|\mathcal{C}(w)|$ を求める問題のクラスを#Pと呼ぶ.

1998年Gödel prize

Cf. 定理 [戸田1991]
 $P^{\#P} = PH$

“Valiant計画” (since 1979)

#P問題 $|\mathcal{C}(w)| \in \mathbb{R}$ に対して, 近似解 $Z \in \mathbb{R}$ を精度

$$\Pr[(1 - \epsilon)|\mathcal{C}(w)| \leq Z \leq (1 + \epsilon)|\mathcal{C}(w)|] \geq 1 - \delta$$

で多項式時間($\text{poly}(\text{input}, \epsilon^{-1}, \log \delta^{-1})$)で求められるか?



Fully Polynomial-time Randomized Approximation Scheme (FPRAS)

$A \in \mathbb{R}$ に対して, 近似解 $Z \in \mathbb{R}$ を精度

$$\Pr[(1 - \epsilon)A \leq Z \leq (1 + \epsilon)A] \geq 1 - \delta$$

で多項式時間($\text{poly}(\text{input}, \epsilon^{-1}, \log \delta^{-1})$)で求めるアルゴリズム.

「計算」を掘り下げる

- 計算 = accept-rejectの決定
- 入力 = 文字列

□ なぜ「多項式」時間？

➤ 等価性、帰着

P ≠ NP予想

「言語 \mathcal{L} が**非**決定性Turing機械で多項式**時間**で判定可能
⇒ 言語 \mathcal{L} は決定性Turing機械で多項式**時間**で判定可能」

(⇐は定義から導かれる)

Cf. Savitchの定理

「言語 \mathcal{L} が**非**決定性Turing機械で多項式**領域**で判定可能
⇒ 言語 \mathcal{L} は決定性Turing機械で多項式**領域**で判定可能」

(⇐は定義から導かれる)

そもそも、Turing machineにはたくさん種類がある

- ◆ 有限オートマトン
- ◆ プッシュダウンオートマトン
- ◆ 2スタックプッシュダウンオートマトン
- ◆ 決定性Turing machine
 - 1テープ1ヘッド
 - 多テープマシン
 - 多ヘッドマシン
 - 万能Turing machine
- ◆ 非決定性Turing machine
- ◆ オラクルTuring machine
- ◆ 確率的Turing machine

- 1回の演算にかかる時間が異なる。
 - 例: n 桁 + m 桁
 - 1テープ1ヘッドだと $O((n+m)^2)$
 - 多ヘッドだと $O(n+m)$
- 「多項式」のくくりにすると
どの決定性TMでも等価.

Cf. Cantorの定理 $\infty^n \neq 2^\infty$

等価性

Reduction (還元, 帰着) : simulateできるか?

□ 計算可能性の等価性

- Turing完全
 - 例: 2-stack push-down automaton

□ 多項式領域計算量の等価性

- PSPACE完全
- NL完全
- Cf. Savitchの補題 : $\text{NSPACE}(f(n)) \subseteq \text{SPACE}(f(n)^2)$

□ 多項式時間計算量の等価性

- NP完全
- P完全

本講義の計算機モデル

非決定性Turing machineとは異なる
(cf. $RP \neq NP$ 予想)

□ 確率的Turing machine

- ・ 決定性Turing machine + random **bit** (0 or 1)生成
 - n bits生成は $O(n)$ 時間
 - $[0,1]$ 実数乱数は生成できない

けっこう不便. たとえば,

命題

確率的Turing Machineでは「確率 $1/3$ 」を有限時間停止では実現不可能.

命題

確率的Turing Machineでは「確率 $1/3$ 」を $O(1)$ 期待時間で実現不可能.

このくらいの精度で議論を進める.

まとめ

Turing machine

□ できること

- 有理数の四則演算
- 論理演算 ($\Rightarrow, \wedge, \vee, \neg, T, \perp$; 例: $1 \vee 0 = 1, 1 \wedge 0 = \perp$)
- 受理、非受理の判定 (If文)
- 大きな数が数えられる (=メモリがある: While文、For文)
- 配列

□ できないこと

- 実数 (無理数一般) の計算 (二次方程式の解の公式とか)
- 「難しい」関数の計算: $\sin, \cos, \tan, \exp, \log, \text{etc.}$
- 微分、積分 (一般に)
- 二階述語論理 (停止性問題)

➤ 何をどこまで計算可能か都度確認。

四則演算の計算量

- 整数 x はおよそ $\log x$ 桁
- p 桁と q 桁の和は $\max\{p, q\} + 1$ 桁以下
 - 計算時間もそれくらい
- p 桁 $-q$ 桁は符号込みで $\max\{p, q\} + 2$ 桁以下
 - 計算時間もそれくらい
- p 桁と q 桁の積は $n + m$ 桁以下
 - 計算時間もまあそれくらい
- 有理数 $\frac{x}{y}$ は $n + m$ 桁以下
 - 整数のペア (x, y) として表される（分数）

「計算量」(決定性 Turing machine)

通常(形容詞のない場合)は
worst case time complexityを指す

□ 計算量 = 演算回数(有限回に限る)

- 読み込み, 書き出し, 代入, 比較: $O(\text{行数})$
- 四則演算(+, -, ×, /) $O(\text{行数}) \sim O(\text{行数}^2)$
- 論理演算($\neg, \wedge, \vee, \Rightarrow$) $O(1)/1$ 演算
- 繰り返し(for, while)は繰り返し中の演算の総数
- 「パラメータ」
 - 固定(定数)なら $O(1)$
 - 可変なら四則演算に準ずる
- 「関数(ライブラリ)」
 - 計算量が解明されていれば, それに準拠
 - オラクル計算量では, 通常の演算数とは別に数える

計算機科学のMCMC法

計算量クラス #P [Valiant '79]

\mathcal{L} がNPに属するとき, $w \in \mathcal{L}$ に対し,
 $\mathcal{C}(w) \subseteq \Sigma^*$ を w のcertificateの集合とする.
 $|\mathcal{C}(w)|$ を求める問題のクラスを#Pと呼ぶ.

1998年Gödel prize

Cf. 定理 [戸田1991]
 $P^{\#P} = PH$

“Valiant計画” (since 1979)

#P問題 $|\mathcal{C}(w)| \in \mathbb{R}$ に対して, 近似解 $Z \in \mathbb{R}$ を精度

$$\Pr[(1 - \epsilon)|\mathcal{C}(w)| \leq Z \leq (1 + \epsilon)|\mathcal{C}(w)|] \geq 1 - \delta$$

で多項式時間($\text{poly}(\text{input}, \epsilon^{-1}, \log \delta^{-1})$)で求められるか?



Fully Polynomial-time Randomized Approximation Scheme (FPRAS)

$A \in \mathbb{R}$ に対して, 近似解 $Z \in \mathbb{R}$ を精度

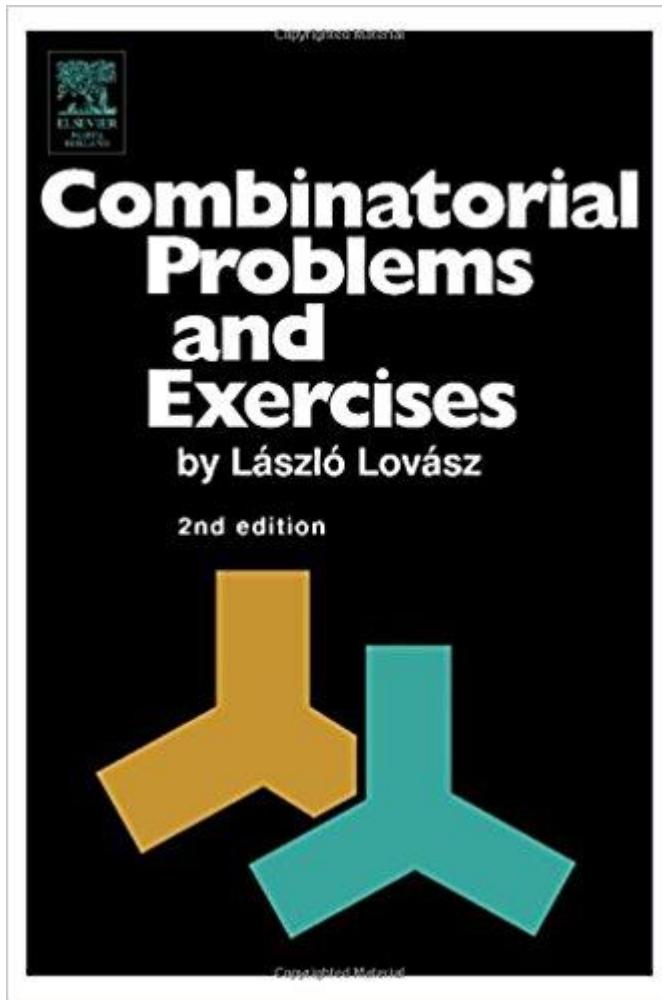
$$\Pr[(1 - \epsilon)A \leq Z \leq (1 + \epsilon)A] \geq 1 - \delta$$

で多項式時間($\text{poly}(\text{input}, \epsilon^{-1}, \log \delta^{-1})$)で求めるアルゴリズム.

次の時間の導入

組合せの数

Counting is a foundation of Combinatorics



Combinatorial Problems and Exercise [Lovasz 1979]

§1. Basic Enumeration

1. In a shop there are k kinds of postcards. We want to send postcards to n friends.

(i) How many different ways can this be done?



(ii) What happens if we want to send them different cards?



(iii) What happens if we want to send two different cards to each of them (but different persons may get the same card)?



Combinatorial Problems and Exercise [Lovasz 1979]

§1. Basic Enumeration

1. In a shop there are k kinds of postcards. We want to send postcards to n friends.

(i) How many different ways can this be done?

➤ k^n

(ii) What happens if we want to send them different cards?

➤

(iii) What happens if we want to send two different cards to each of them (but different persons may get the same card)?

➤

Combinatorial Problems and Exercise [Lovasz 1979]

§1. Basic Enumeration

1. In a shop there are k kinds of postcards. We want to send postcards to n friends.

(i) How many different ways can this be done?

➤ k^n

(ii) What happens if we want to send them different cards?

➤ $\frac{k!}{(k-n)!}$ (which is 0 if $n > k$)

(iii) What happens if we want to send two different cards to each of them (but different persons may get the same card)?

➤

Combinatorial Problems and Exercise [Lovasz 1979]

§1. Basic Enumeration

1. In a shop there are k kinds of postcards. We want to send postcards to n friends.

(i) How many different ways can this be done?

➤ k^n

(ii) What happens if we want to send them different cards?

➤ $\frac{k!}{(k-n)!}$ (which is 0 if $n > k$)

(iii) What happens if we want to send two different cards to each of them (but different persons may get the same card)?

➤ $\binom{k}{2}^n$

Combinatorial Problems and Exercise [Lovasz 1979]

§1. Basic Enumeration

2. We have k distinct post cards and want to send them all to our n friends (a friend can get any number of post cards, including 0).
- (i) How many ways can this be done?



- (ii) What happens if we want to send at least one card to each friend?



Combinatorial Problems and Exercise [Lovasz 1979]

§1. Basic Enumeration

2. We have k distinct post cards and want to send them all to our n friends (a friend can get any number of post cards, including 0).
- (i) How many ways can this be done?

➤ n^k

- (ii) What happens if we want to send at least one card to each friend?

➤

Combinatorial Problems and Exercise [Lovasz 1979]

§1. Basic Enumeration

2. We have k distinct post cards and want to send them all to our n friends (a friend can get any number of post cards, including 0).
- (i) How many ways can this be done?

➤ n^k

- (ii) What happens if we want to send at least one card to each friend?

➤ $n! \cdot \left\{ \begin{matrix} k \\ n \end{matrix} \right\}$

Stirling number of the second kind $\left\{ \begin{matrix} k \\ n \end{matrix} \right\}$ counts the number of ways to partition a set of k elements into n nonempty subsets.

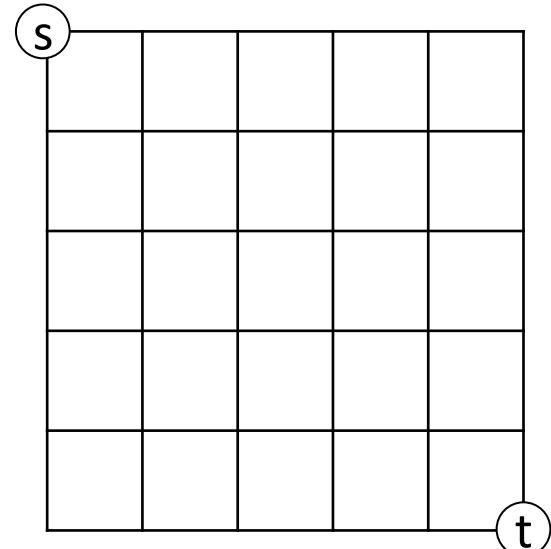
$$\left\{ \begin{matrix} k \\ n \end{matrix} \right\} = \left\{ \begin{matrix} k - 1 \\ n - 1 \end{matrix} \right\} + n \left\{ \begin{matrix} k - 1 \\ n \end{matrix} \right\}$$

holds. [Wikipedia “Stirling number”]

Another interesting counting problem in [Lovasz 1979]

§1. Basic Enumeration

32. How many shortest paths from s to t in the $n \times n$ grid?



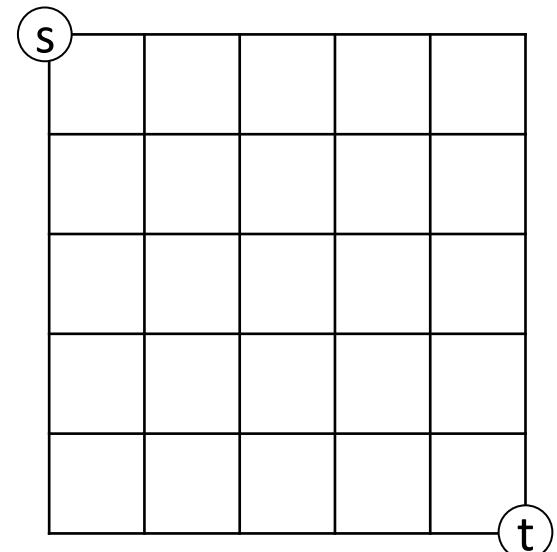
5×5 grid

Another interesting counting problem in [Lovasz 1979]

§1. Basic Enumeration

32. How many shortest paths from s to t in the $n \times n$ grid?

➤ $\binom{2n}{n}$



5×5 grid

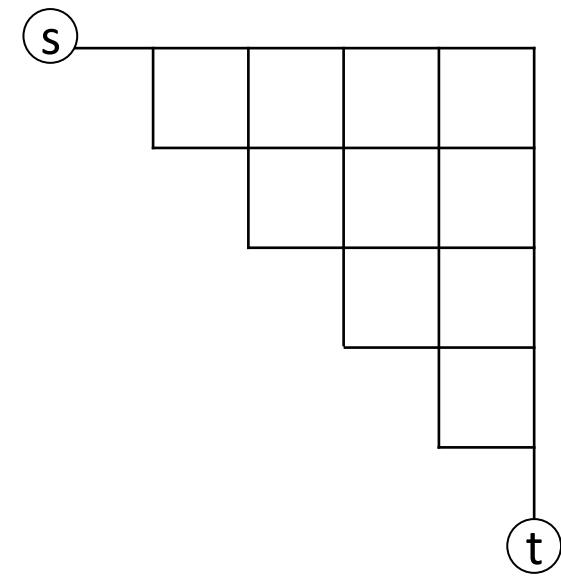
Another interesting counting problem in [Lovasz 1979]

§1. Basic Enumeration

32. How many shortest paths from s to t in the $n \times n$ grid?

➤ $\binom{2n}{n}$

33. How many shortest paths from s to t in the $n \times n$ grid upper than diagonal?



5×5 grid

Another interesting counting problem in [Lovasz 1979]

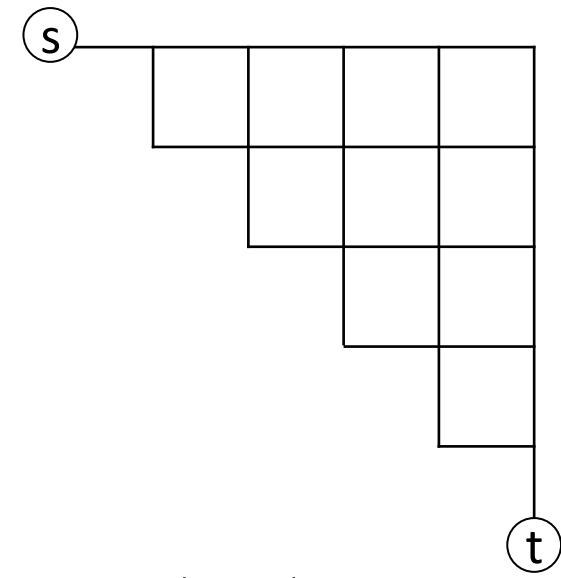
§1. Basic Enumeration

32. How many shortest paths from s to t in the $n \times n$ grid?

➤ $\binom{2n}{n}$

33. How many shortest paths from s to t in the $n \times n$ grid upper than diagonal?

➤ $\binom{2n}{n} - \binom{2n}{n-1} = \frac{2n!}{n!(n+1)!}$ (Catalan number)



5 × 5 grid

Counting is a foundation of Combinatorics

#permutations of n elements is $n!$

k combinations of n elements is $\binom{n}{k} = \frac{n!}{(n-k)!k!}$

#Dyck path = #binary trees = #proper parentheses = ...

is known as Catalan number = $\binom{2n}{n} - \binom{2n}{n-1} = \frac{2n!}{n!(n+1)!}$

spanning trees \Rightarrow Matrix tree theorem

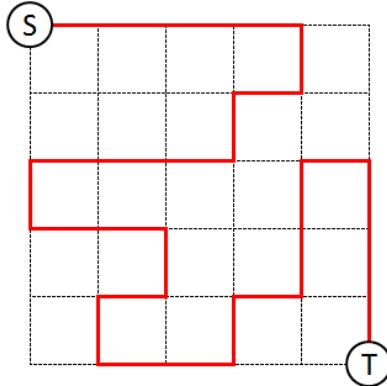
Many known formula for counting combinatorial objects
(while some of them do not have an “explicit form”
...such as Stirling number)

... And, many more combinatorial objects

for which efficient way to count is not known.

おねえさん問題

*n × n*格子グラフ上で、左上(s)から右下(t)を結ぶ、
*s-t*単純経路の総数を求めよ。



画像引用：日本科学未来館、『フカシギの考え方』おねえさんといっしょ！

みんなで数えてみよう！, YouTube, 2012/9/10公開,

<https://www.youtube.com/watch?v=Q4gTV4r0zRs>

おねえさん問題 youtube

search

01

12

212

3184

48512

51262816

6175780564

7789360633252

83266598486981642

941044208702632496804

10156875603064750013214100

1118241329151424804924470885236

1264528039343270018963357185158482118

1369450654761523136166427470154890735996488

142274497146768127396318654592798983387613232440

1522674556881267274634567396713098334866324585408319028

16687454456091499311587631563124898233824587945968099457285419306

17634814611237639713102975805244094439868648693646389387855336

1817821184084206512988384946623235271678380657047676559331452474605826692782532

19152334497104679993087428103192296908994542553223455577602986673735506029877569255844

203962892199823037560207299517133362502106333970573946337715152271133771068264035706704472064940398

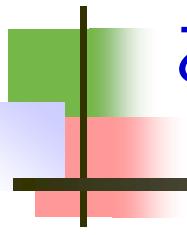
213137475105137102720420538122145131033121936872365306135191346433373989385793965576992246021316463868

227755970286667345339661549123315222619353103720724094811675914104795179257927436312349877634987271171404439792

2355435429555374770099143184890614379306913797990709644331332569586466484098407334885544569362402088571124206085409513482933945720

24132171722312070647583397448626735708349989012045996782270804495619955159300856413945507971130371918580282152280960212126562506027316549718402106494049978375604247408

2584029748578811334710070837454366809122729605429957759982152569291785770839709660121649718402134762789218193498006107082296223143380491348276721931129627708739880353908108906396



おわり