

P 対 NP 問題（解決したら 100 万ドル）

奈良女子大学理学部情報科学科 鴨浩靖

2013 年 8 月 2 日

P 対 NP 問題とは？

強引な要約：

一般に、解が与えられたときにそれを十分に速く検算できる問題は、解が与えられなくても十分に速く解の有無を判定できるか？

未解決。答えが「はい」か「いいえ」か、わかっていない。

多くの研究者は、答えは「いいえ」だと思っている。

→ $P \neq NP$ 予想とも呼ばれる。

余談：P 対 NP 問題が出てくる作品

- 米国の TV ドラマ『NUMB3RS』（邦題：『NUMBERS 天才数学者の事件ファイル』）で、主人公の数学者が P 対 NP 問題に挑戦するシーンがある。
- 日本の推理小説『容疑者 X の献身』（東野圭吾）にも、登場人物が P 対 NP 問題について語るシーンがある。

ミレニアム懸賞問題

クレイ数学研究所が2000年に懸賞をかけた。
賞金は各100万ドル。

- P 対 NP 問題
- ホッジ予想
- リーマン予想
- バーチ・スウィナートン-ダイナー予想
- ★ ポアンカレ予想 (解決済み。賞金を辞退)
- ヤン・ミルズ理論と質量ギャップ
- ナビエ・ストークス方程式

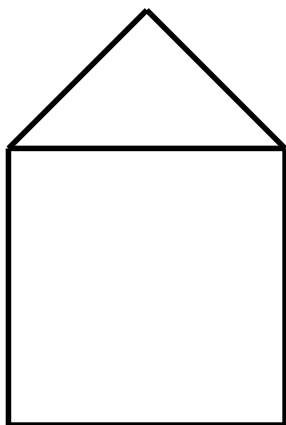
余談：100万ドルが受賞者に渡るまで

- (1) 解決した人の論文が、世界的に評価された査読付き数学専門雑誌に掲載される。
- (2) 2年待つ。
- (3) 2年経って、解決が数学界に受け入れられたとみなされるならば、クレイ数学研究所科学諮問会議が、その問題についての特別諮問委員会を設置する。
- (4) 特別諮問委員会の報告をもとに科学諮問会議がさらに検討を加え、研究所の理事会に勧告を出す。
- (5) 科学諮問委員会の勧告に基づき、理事会が授賞の決定をする。
- (6) 受賞者が賞金を受け取る。

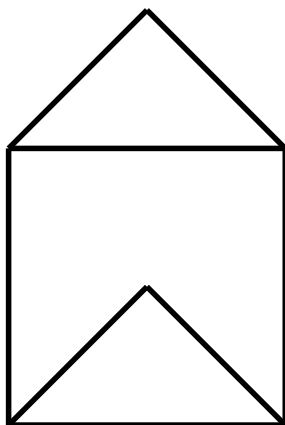
例：オイラー路（一筆書き）の有無を判定する

すべての辺をちょうど一度ずつ通る路は存在するか？

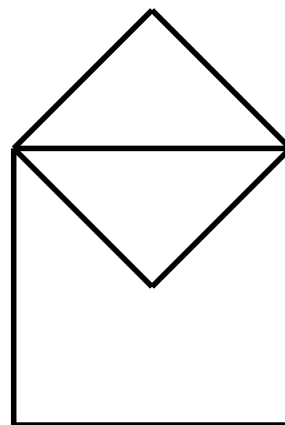
1.



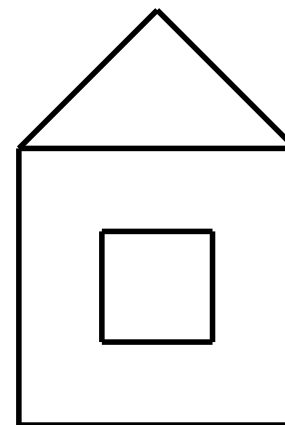
2.



3.



4.

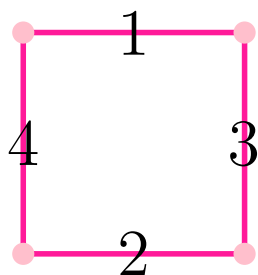


Leonhard Euler (1707–1783)



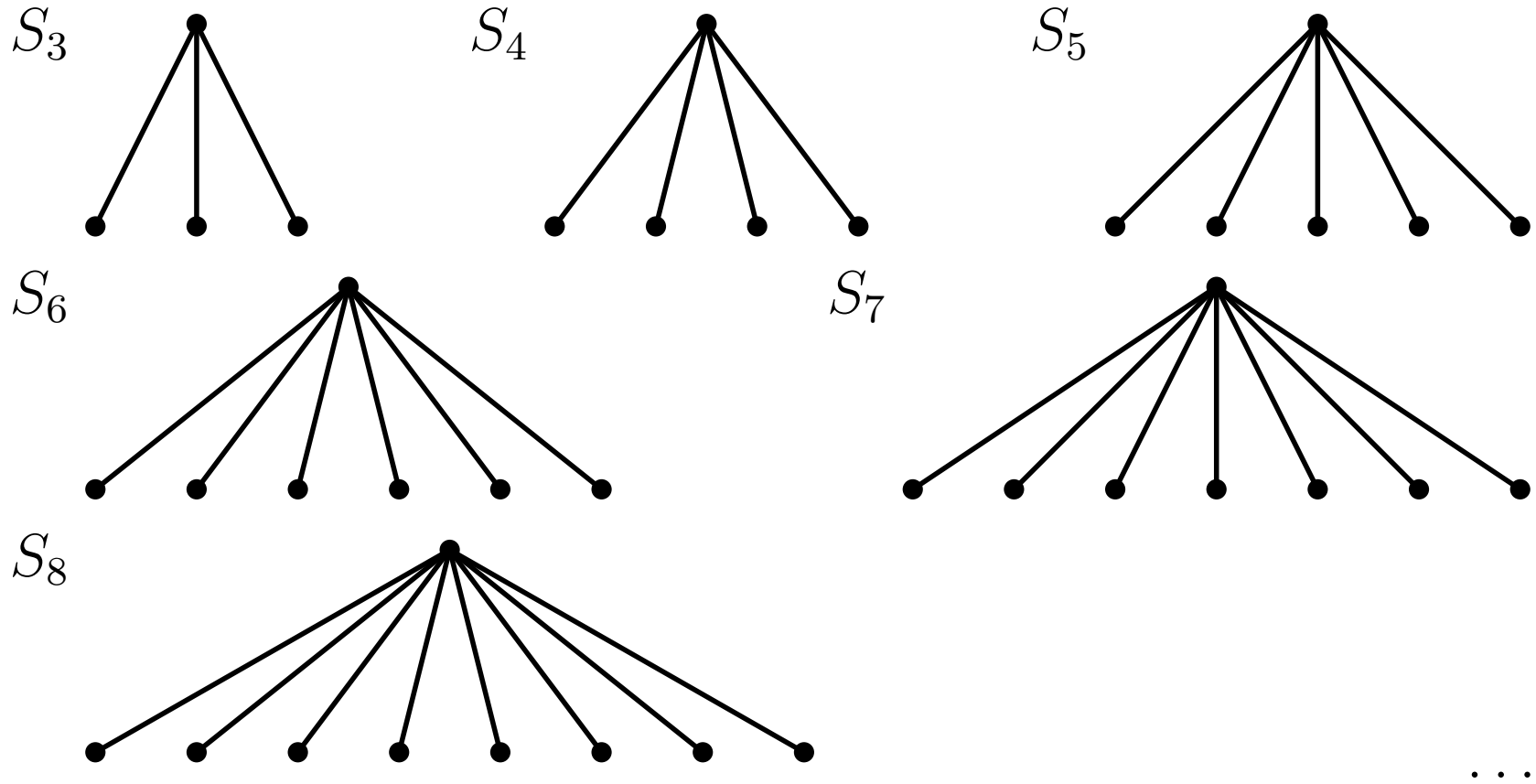
しらみつぶしでオイラー路の有無を判定する方法

辺の順列をすべて生成して、ひとつひとつ判定する。



1-2-3-4 ×	1-2-4-3 ×	1-3-2-4 ○
1-3-4-2 ×	1-4-2-3 ○	1-4-3-2 ×
2-1-3-4 ×	2-1-4-3 ×	2-3-1-4 ○
2-3-4-1 ×	2-4-1-3 ○	2-4-3-1 ×
3-1-2-4 ×	3-1-4-2 ○	3-2-1-4 ×
3-2-4-1 ○	3-4-1-2 ×	3-4-2-1 ×
4-1-2-3 ×	4-1-3-2 ○	4-2-1-3 ×
4-2-3-1 ○	4-3-1-2 ×	4-3-2-1 ×

判定してみる



これらを対象に実験する。

オイラー路の有無のしらみつぶし法での計算時間

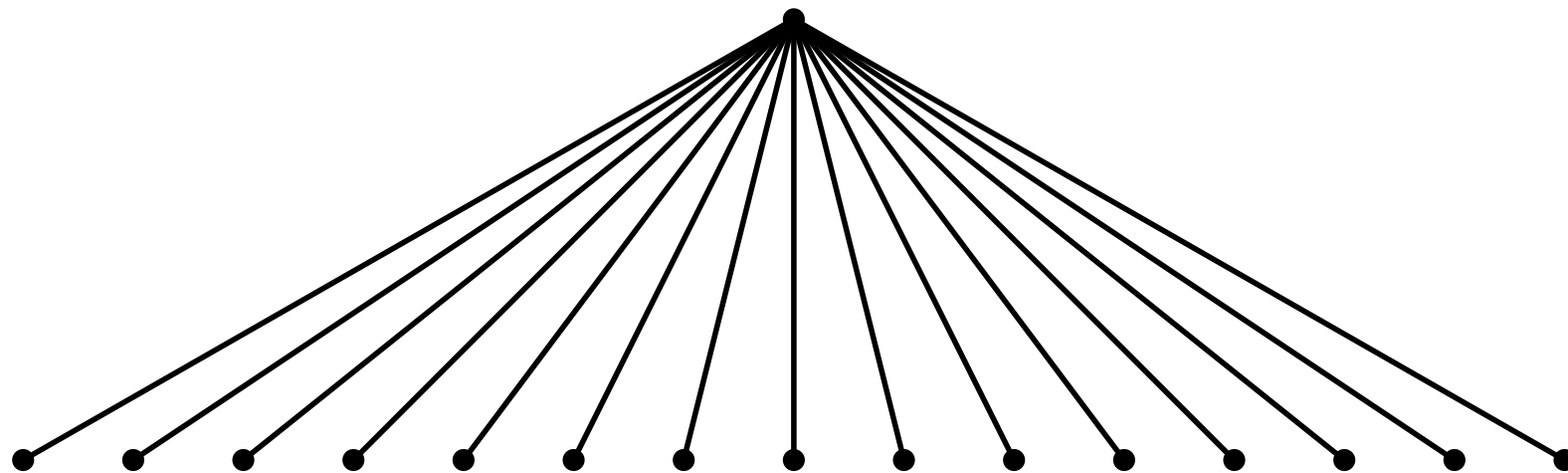
グラフ	辺の数	計算時間	
S_3	3	0.01 秒未満	(実測)
S_4	4	0.01 秒未満	(実測)
S_5	5	0.01 秒未満	(実測)
S_6	6	0.01 秒未満	(実測)
S_7	7	0.01 秒未満	(実測)
S_8	8	0.01 秒未満	(実測)
S_9	9	0.01 秒	(実測)
S_{10}	10	0.12 秒	(実測)

グラフ	辺の数	計算時間	
S_{11}	11	1.37秒	(実測)
S_{12}	12	16.57秒	(実測)
S_{13}	13	3分 32.98秒	(実測)
S_{14}	14	49分 39.97秒	(実測)
S_{15}	15	12時間 29分 26.99秒	(実測)
S_{16}	16	8.3日	(推計)
S_{17}	17	20週	(推計)
S_{18}	18	7.0年	(推計)

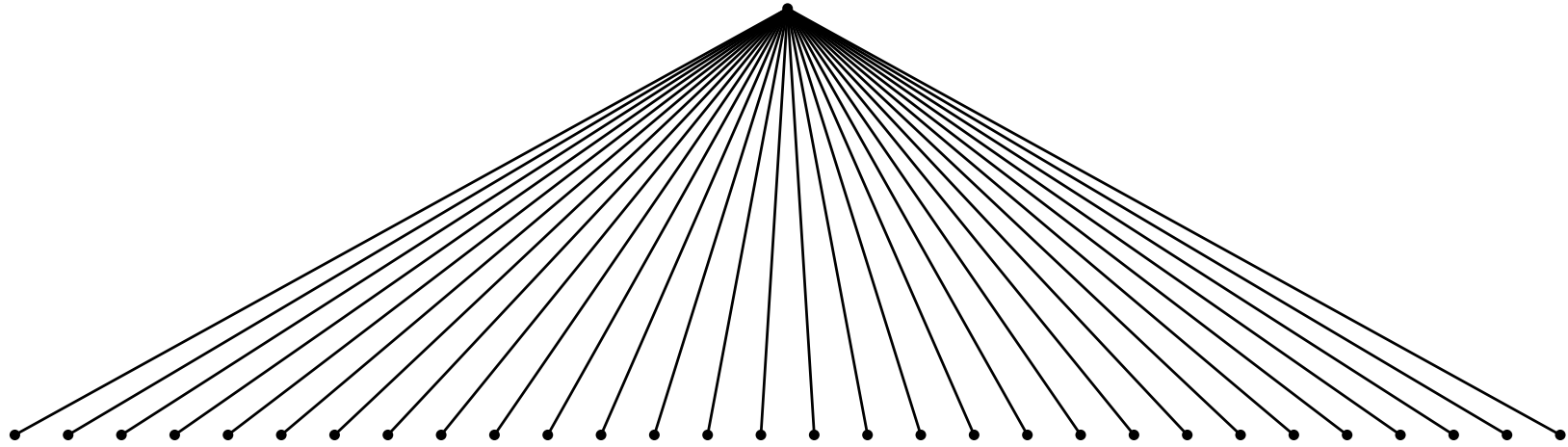
グラフ	辺の数	計算時間
S_{19}	19	130年 (推計)
S_{20}	20	2700年 (推計)
S_{21}	21	5 6000年 (推計)
S_{22}	22	120 0000年 (推計)
S_{23}	23	2800 0000年 (推計)
S_{24}	24	6 8000 0000年 (推計)
	(宇宙の年齢	137 0000 0000年)
S_{25}	25	170 0000 0000年 (推計)

グラフ	辺の数	計算時間
S_{26}	26	四千億年 (推計)
S_{27}	27	十兆年 (推計)
S_{28}	28	三百兆年 (推計)
S_{29}	29	一京年 (推計)
S_{30}	30	三十京年 (推計)
S_{31}	31	九百京年 (推計)
S_{32}	32	三垓年 (推計)
	⋮	⋮
S_{62}	62	三百無量大数年 (推計)
S_{63}	63	(ここから先、日本語がない)

辺の数 15 (約半日) が実用上の限界。



辺の数 30 (約三十京年) が実用的になるように高速化するには、計算機の性能を約一垓倍にしなければならない。



しらみつぶし法では無理！

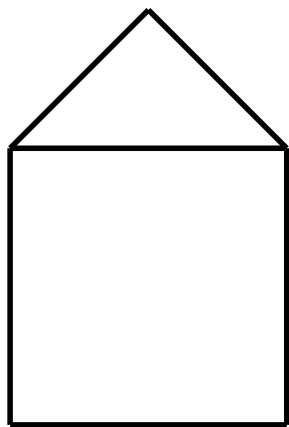
オイラー路の有無を判定する効率の良い方法

グラフがオイラー路を持つ必要十分条件は、以下の二つとも成り立つこと。

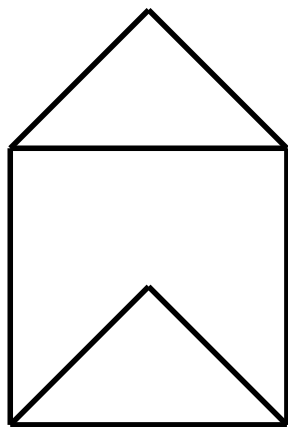
- 奇数本の辺が集まる頂点が0個か2個である。
- 全体が連結である。すなわち、どの二つの頂点も辺をたどって行き来できる。

この定理を利用すれば、効率の良い判定プログラムを書くことができる。

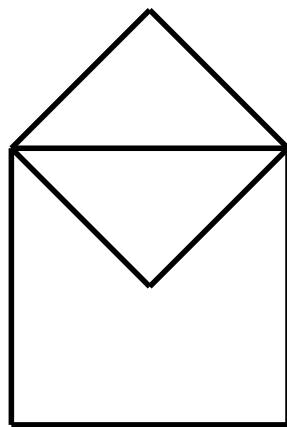
1.



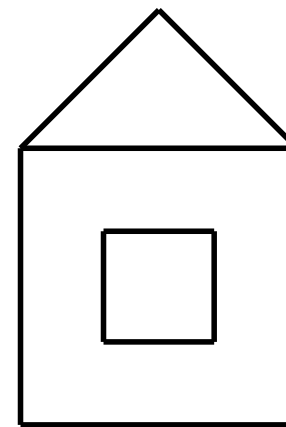
2.



3.



4.



奇点

2個

4個

0個

2個

連結性

連結

連結

連結

不連結

オイラー路

あり

なし

あり

なし

オイラー路の有無を判定する効率の良い方法の計算時間

グラフ	辺の数	計算時間	
S_3	3	0.01秒未満	(実測)
S_{30}	30	0.01秒未満	(実測)
S_{300}	300	0.01秒未満	(実測)
S_{3000}	3000	0.01秒未満	(実測)
S_{30000}	30000	0.04秒	(実測)
S_{300000}	300000	0.55秒	(実測)
$S_{3000000}$	3000000	6.20秒	(実測)
$S_{30000000}$	30000000	70.01秒	(実測)

疑い

早く計算が終わるデータを選んでいるのではないの？

釈明

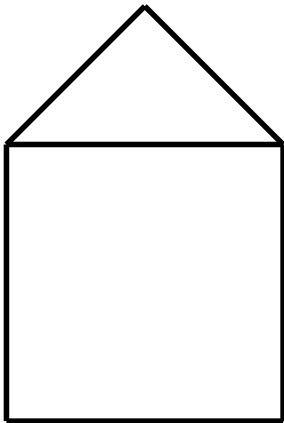
以下のことが数学的に証明できる。

計算機の性能によって決まる定数 a があって、
辺の本数が n であるグラフが入力されると
「効率の良いオイラー路判定プログラム」は
計算時間 an [秒] 以下でオイラー路の有無を判定で
きる

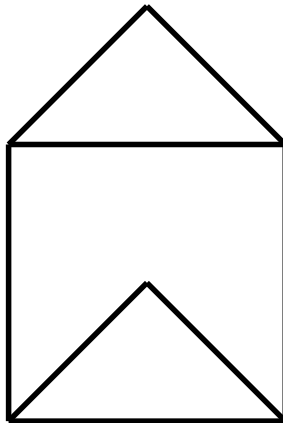
例：ハミルトン路（別種の一筆書き）
の有無を判定する

すべての頂点をちょうど一度ずつ通る路は存在するか？

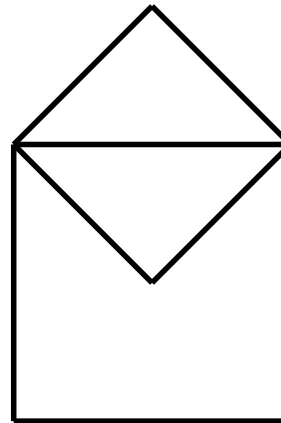
1.



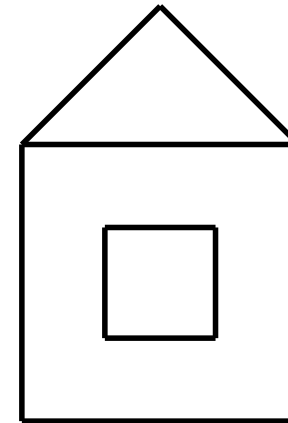
2.



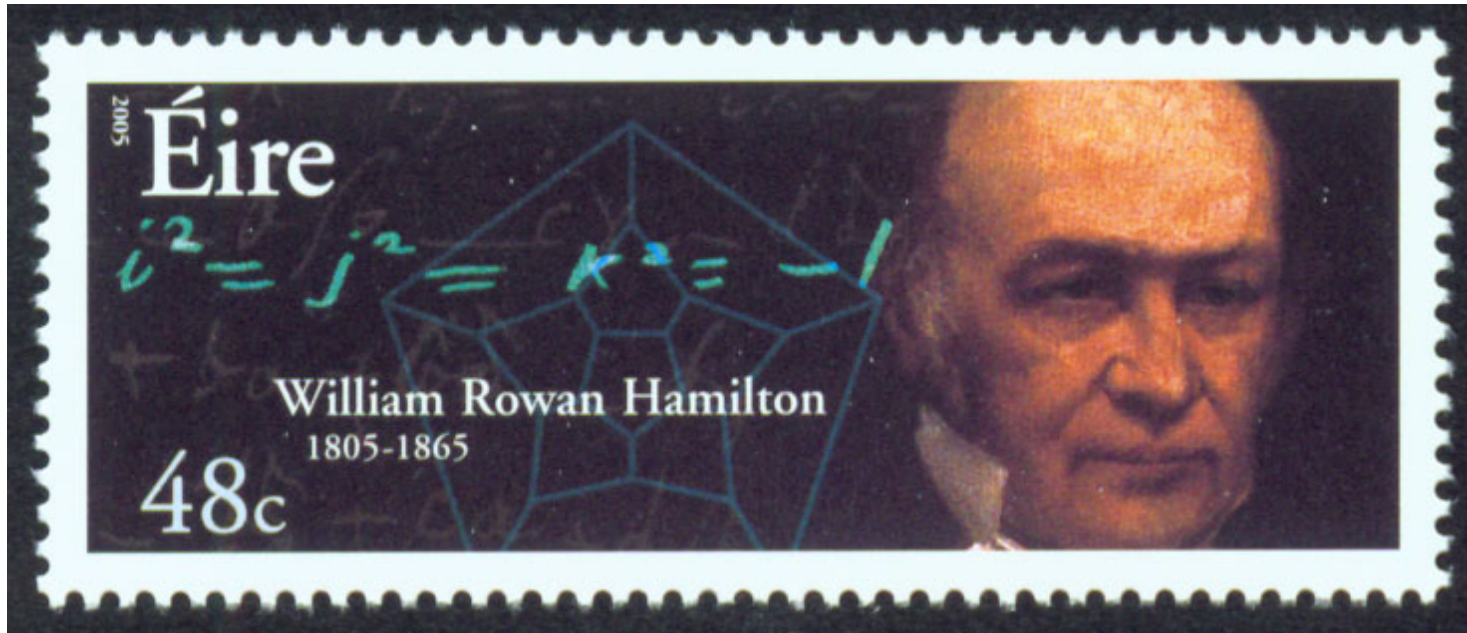
3.



4.

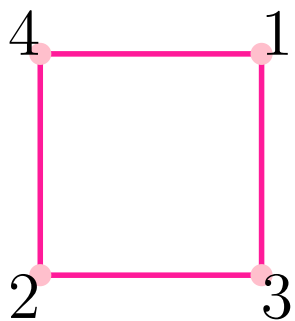


William Rowan Hamilton (1805–1865)



ハミルトン路の有無をしらみつぶしで判定する方法

頂点の順列をすべて生成し、ひとつひとつ判定する。



1-2-3-4 ×	1-2-4-3 ×	1-3-2-4 ○
1-3-4-2 ×	1-4-2-3 ○	1-4-3-2 ×
2-1-3-4 ×	2-1-4-3 ×	2-3-1-4 ○
2-3-4-1 ×	2-4-1-3 ○	2-4-3-1 ×
3-1-2-4 ×	3-1-4-2 ○	3-2-1-4 ×
3-2-4-1 ○	3-4-1-2 ×	3-4-2-1 ×
4-1-2-3 ×	4-1-3-2 ○	4-2-1-3 ×
4-2-3-1 ○	4-3-1-2 ×	4-3-2-1 ×

ハミルトン路の有無のしらみつぶし法での計算時間

グラフ	頂点の数	計算時間	
S_3	4	0.01 秒未満	(実測)
S_4	5	0.01 秒未満	(実測)
S_5	7	0.01 秒未満	(実測)
S_6	7	0.01 秒未満	(実測)
S_7	8	0.01 秒未満	(実測)
S_8	9	0.01 秒	(実測)
S_9	10	0.10 秒	(実測)
S_{10}	11	1.16 秒	(実測)

グラフ	頂点の数	計算時間	
S_{11}	12	13.80秒	(実測)
S_{12}	13	2分 52.30秒	(実測)
S_{13}	14	40分 8.24秒	(実測)
S_{14}	15	9時間 43分 1.21秒	(実測)
S_{15}	16	6.4日	(推計)
S_{16}	17	16週	(推計)
S_{17}	18	5.3年	(推計)
S_{18}	19	9.9年	(推計)
S_{19}	20	200年	(推計)

ハミルトン路の有無を判定する効率の良い方法
未発見。

しらみつぶしよりも多少はましな方法はみつかっている。
改良の研究は続行中

P 問題

計算機の性能に よって 決まる定数 a と
計算機の性能に よらずに 決まる定数 k があって、
大きさが n のデータが入力されると
計算時間 an^k [秒] 以下で解の有無を判定できるプログラム
を書くことができる問題を **P 問題** という。

- オイラー路問題は P 問題。

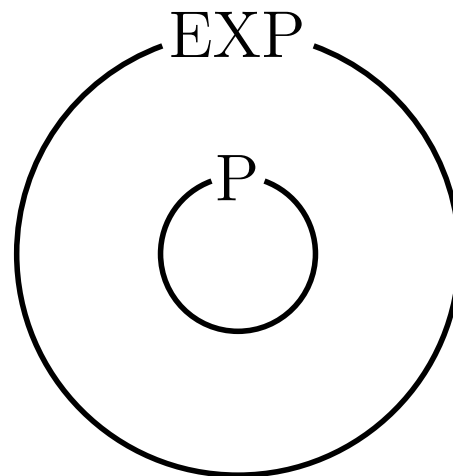
EXP 問題

計算機の性能に よって 決まる定数 a と
計算機の性能に よらずに 決まる定数 c と定数 k があって、
大きさが n のデータが入力されると
計算時間 ac^{n^k} [秒] 以下の解の有無を判定できるプログラム
を書くことができる問題を **EXP 問題** という。

- ハミルトン路問題は EXP 問題。

P 問題と EXP 問題の関係

- P 問題は EXP 問題でもある。
- EXP 問題であるが P 問題でない問題が存在することは証明済み。
- 計算可能であるが EXP 問題ではない問題が存在することは証明済み。



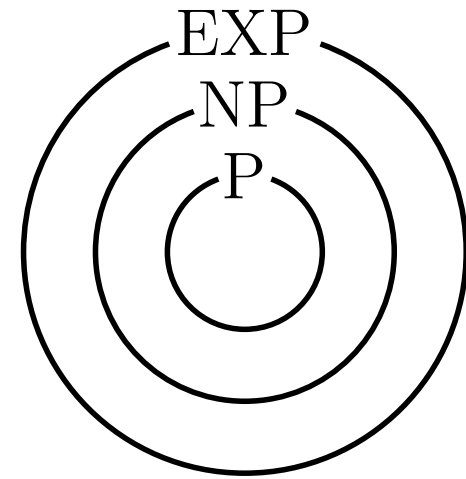
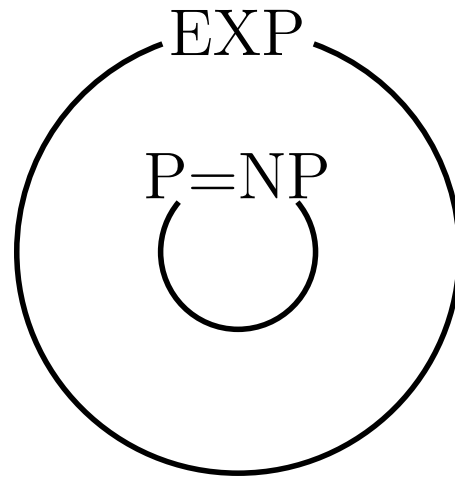
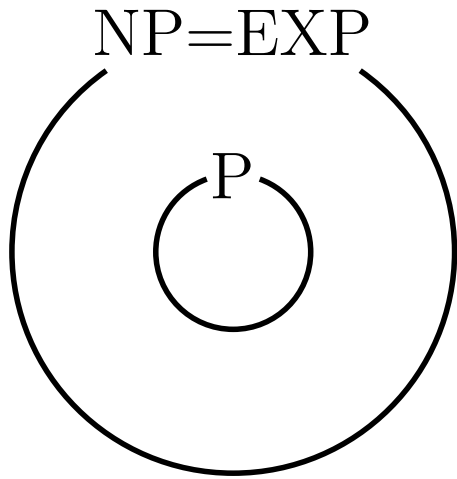
NP 問題

計算機の性能に よって 決まる定数 a と
計算機の性能に よらずに 決まる定数 k があって、
大きさが n のデータが入力され、
入力に加えて解も与えられると、
計算時間 an^k [秒] 以下で本当に解であると確認できるプログラムを書くことができる問題を **NP 問題** という。

- ハミルトン路問題は NP 問題。

P 問題と NP 問題と EXP 問題の関係

- P 問題は NP 問題でもある。
- NP 問題は EXP 問題でもある。
- EXP 問題であるが P 問題でない問題が存在することは、わかっている。(前述)
- EXP 問題であるが NP 問題でない問題が存在するかどうかは不明。
- NP 問題であるが P 問題でない問題が存在するかどうかは不明。← P 対 NP 問題



どれが正しい？

ちょっと一般的でない言葉の使い方に注意

難しい 計算に時間がかかる

易しい 計算に時間がかからない

手順が複雑／単純

理解が困難／容易

などの意味は含まない。

厳密な言葉の使い方に注意

(問題が) 解ける うまくプログラムを書けば、どんな入力データに対しても、かならず計算結果が出力されるようにできる。

「一部の例外的な入力データについては計算できません」
はダメ！

難しい問題を比較したい

難しい問題は、一様に難しいか？

たぶん、そんなことはない。

- 普通に難しい問題
- とても難しい問題
- 極めて難しい問題
- 著しく難しい問題

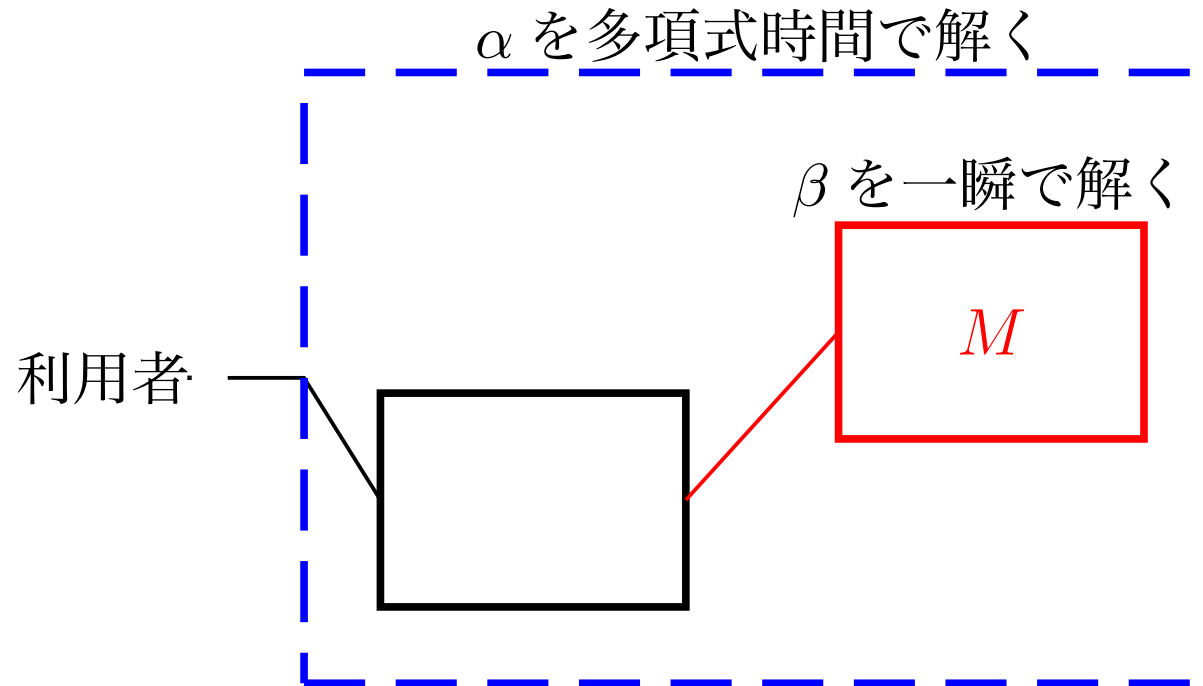
などなどがあると思う。

難しい問題の難しさの程度を比較したい！

難しい問題を比較する

問題 α も問題 β も難しい問題とする。

問題 β を一瞬で解くことのできる計算機 M が存在すると、**現実に反して** 仮定する。この仮定の下で、架空の計算機 M をうまく使ってやると、問題 α があたかも P 問題であるかのように解けるとする。



このような架空の計算機複合体を考えることができるとき、
問題 α の難しさは問題 β の難しさ以下である
(問題 β の難しさは問題 α の難しさ以上である)
と定義する。

問題 α の難しさが問題 β の難しさ以下であり、同時に、
問題 α の難しさが問題 β の難しさ以上であるとき、
問題 α は問題 β と同程度に難しい
と定義する。

問題 α の難しさが問題 β の難しさ以上であり、
問題 α は問題 β と同程度に難しくはないとき、
問題 α は問題 β より真に難しい
と定義する。

注意：難しさが比較不能な場合もある。

NP 困難

問題 φ の難しさが、
どんな NP 問題 α についてもその難しさ以上であるとき、
問題 φ を **NP 困難** な問題と呼ぶ。

NP 完全問題

NP 困難な NP 問題を、NP 完全問題と呼ぶ。

NP 完全問題

NP 完全問題は、いわば、NP 問題の頂点に君臨する難しさの問題。

1971 年に充足可能性問題（略称：SAT）が NP 完全であることが証明されて以来、NP 完全問題が続々と発見され続けている。

NP 完全な問題の例—SAT

変数 x_1, \dots, x_k から \neg と \wedge と \vee を使って作られた式が与えられたとき、 x_1, \dots, x_k のそれぞれに 0 か 1 をうまく割り当てて、式の値を 1 にできるか？

x	$\neg x$
0	1
1	0

x	y	$x \wedge y$	$x \vee y$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

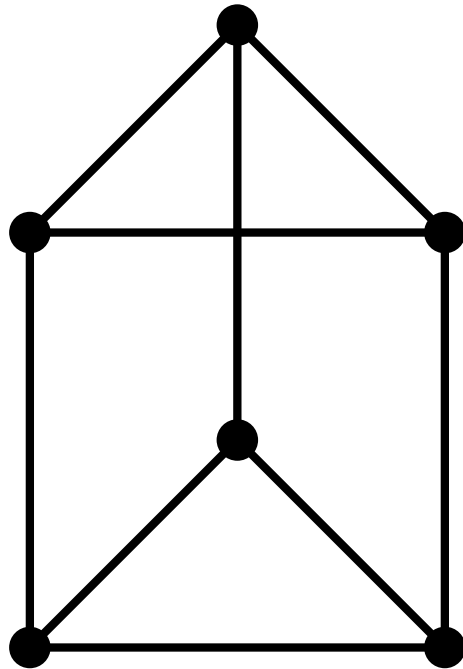
例 $x_1 \wedge \neg(\neg x_1 \vee x_2) \wedge (\neg x_1 \vee x_3)$ には、 $x_1 = 1$, $x_2 = 0$, $x_3 = 1$ と割り当てればよい。

NP 完全な問題の例—ハミルトン路

与えられたグラフに、すべての頂点をちょうど一度ずつ通る路は存在するか？

NP 完全な問題の例— k クリーク

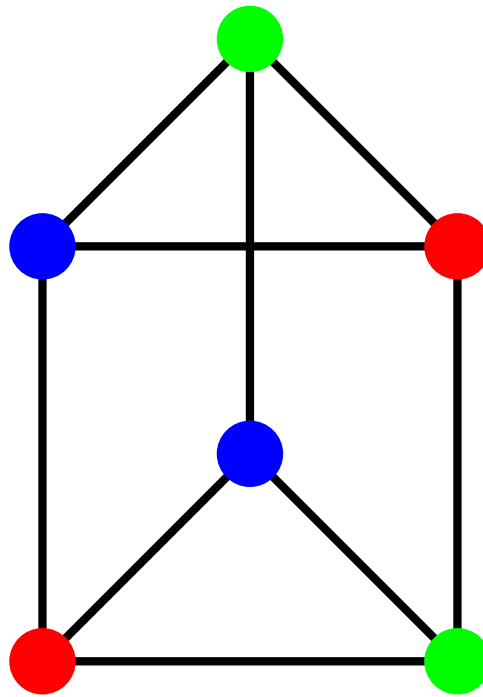
与えられたグラフから k 個の頂点を選び、その k 個のうち
のどの 2 個も結ばれているようにすることができるか？



3 クリークはあるが、
4 クリークはない。

NP 完全な問題の例—三色塗り分け

与えられたグラフのそれぞれの頂点を赤、緑、青のどれかの色に塗り、結ばれている頂点は必ず異なる色にすることが出来るか？



NP 完全な問題の例— 二次ディオファントス方程式

与えられた正整数 a, b, c について、未知数 x, y の方程式 $ax^2 + by = c$ は正整数解をもつか？

NP 完全な問題の例—その他

応用上、重要そうな問題も多い。

- 巡回セールスマン問題
- 各種の詰め込み問題
- 各種のスケジューリング問題
-

P 対 NP 問題の解決への見通し (否定的解決への道)

[証明済み] NP 完全問題の どれか一つ について、実は P 問題であることを、実際にプログラムを書く方法で証明できれば、 $P = NP$ と結論づけられる。

→ でも、たぶん、 $P \neq NP$ だろうから、この方向は無理筋だろうなあ。

P 対 NP 問題の解決への見通し

(初期の願望と挫折)

(既知の事実) $P \neq EXP$ は対角線論法を使って証明できる

(願望) $P \neq NP$ も対角線論法を使って証明したい

(挫折) 「 $P \neq NP$ も $P = NP$ も対角線論法を使う方法では証明できない」が証明された

(大団円ではない) 他の手法を模索中

P 対 NP 問題の解決への見通し (有力な候補)

- 代数幾何が役に立つのではないか？
- 論理体系に帰着させることはできないか？

P 対 NP 問題の解決への見通し（現状）

「○○の方法では証明できない」を着々と発見中。

おおざっぱな歴史 (1)

- 1936年 「計算」の定義が確立される
(チャーチ、チューリング、他多数)
- 1971年 P 対 NP 問題が定式化される
(クックとレビンが独立に発見)
- 2000年 P 対 NP 問題がミレニアム懸賞問題に選ばれる
- 2013年 P 対 NP 問題は未解決

おおざっぱな歴史 (2)

40000 年前? ヒトが何かを数えた痕跡が遺される。

5000 年前? 最古の数字? (メソポタミア文明)

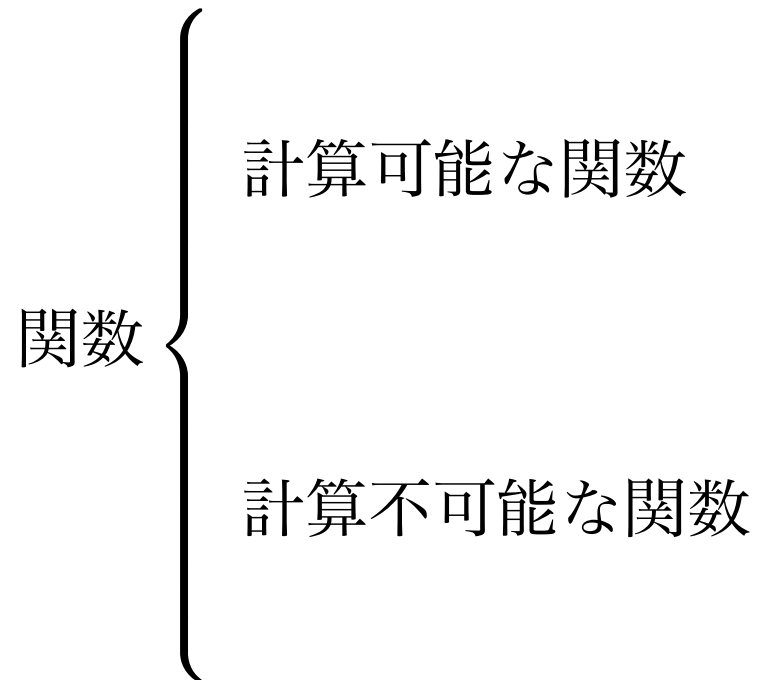
1500 年前? インドで0が発見され、位取り記数法による計算が可能になる。

77 年前 「計算」の定義が確立する。

現在

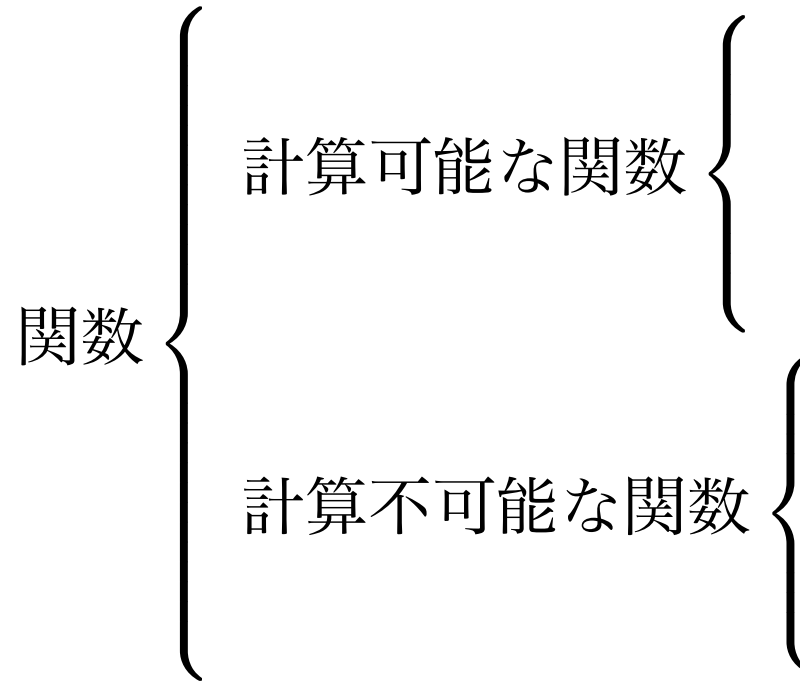
「計算」の定義が確立して、すぐにできたこと

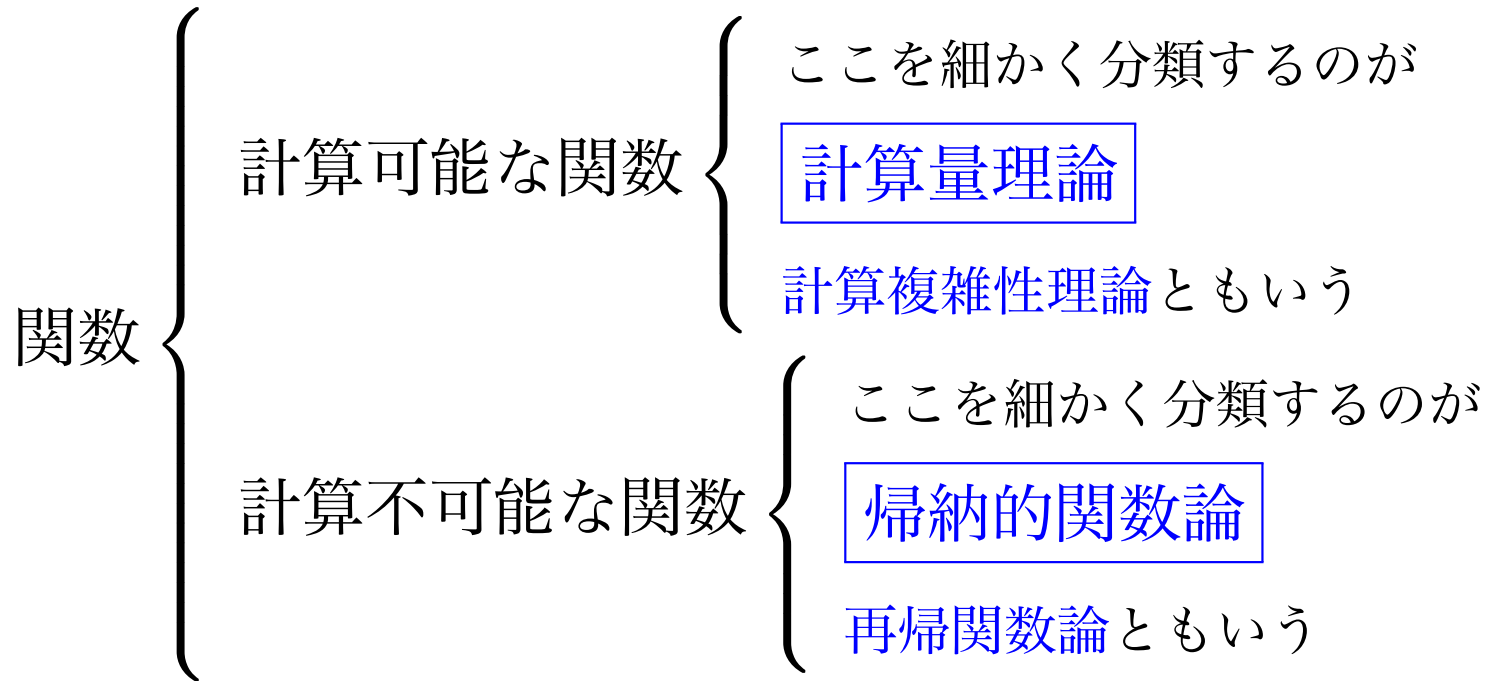
関数の分類



次にしたくなること

細かい分類





計算量クラス

P、NP、EXP の他にも、問題の難しさの分類はたくさんある。これらを計算量クラスという。

Complexity Zoo

https://complexityzoo.uwaterloo.ca/Complexity_Zoo

には 495 個掲載されている。

計算量クラスの包含関係については、未解決の問題が多数ある。P 対 NP 問題もそのひとつ。

まとめ

- P 対 NP 問題とは、

一般に、解が与えられたときにそれを十分に速く検算できる問題は、解が与えられなくても十分に速く解の有無を判定できるか？

- P 対 NP 問題は未解決。
- P 対 NP 問題は、壮大な問題

計算量クラスの階層構造を確定せよ

の一部。