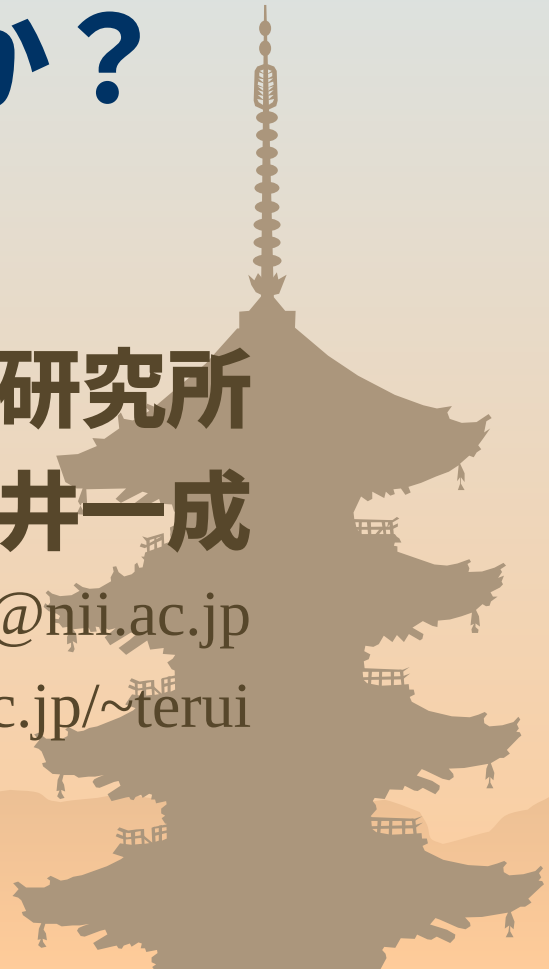
計算論の現在：
PvsNP問題とは何か？

国立情報学研究所
照井一成
terui@nii.ac.jp
http://research.nii.ac.jp/~terui



計算可能性理論初期の主要成果

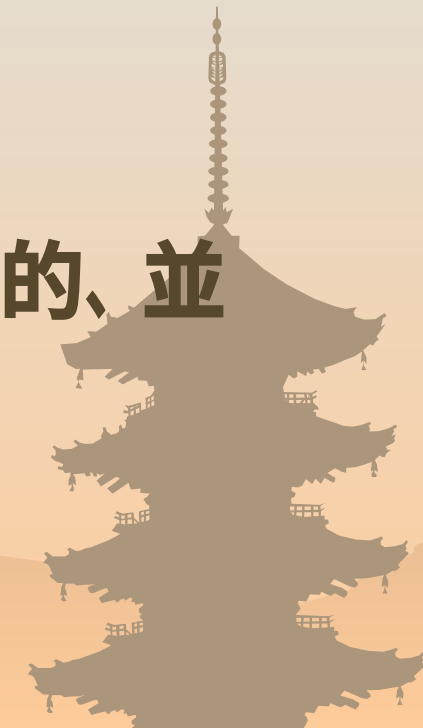
(1) 計算可能な関数 (決定可能な問題)
　　の定式化 (チャーチのテーゼ)
(2) 半決定可能かつ (全) 決定不能な問題の
　　発見 (チューリング機械停止問題)

計算可能性の概念だけで関数の計算論的性質
　を分析するのに十分か？

⇒もちろんNO。

計算の複雑さの理論

- １９６０年代～ (Hartmanis & Stearns1965)
- ある問題をある計算モデルで解くのにどの程度の計算量が必要か？
- 計算量：時間＝計算ステップ数、
  空間＝ 使用メモリ量
- 計算モデル：決定的/非決定的、確率的、並行的、ノンユニフォーム、量子的



計算の複雑さの研究の動機（1）

- コンピュータの実用化：大規模な計算を機械的に実行できる可能性

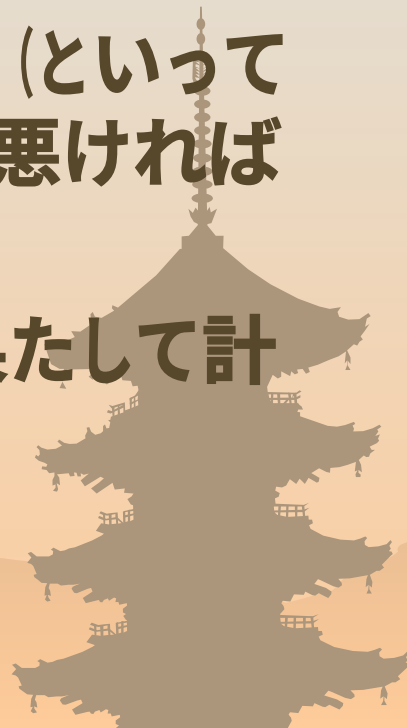
  ⇒理念としての計算から実用としての計算へ
- アルゴリズムを明示的に書き下し、評価することが頻繁に行われるようになった。

  ⇒評価基準の必要性
- 計算可能な関数が成す空間の階層性

  ⇒関数空間の計算論的見取り図の作成

計算の複雑さの研究の動機 (2)

- チャーチのテーゼにより計算可能性については一致をみたが、計算そのものについてまで一致をみたわけではない。いろいろな計算モデルがあってよいし、いろいろな複雑さの計算があってよい。
- (チューリング的) 計算概念：本性的に時間 (といって悪ければ計算ステップ数) と空間 (といって悪ければメモリ使用量) を伴う。
- 時間や空間に対する真摯な考察なくして果たして計算の全てが理解できるのか？



計算の複雑さの理論の主要課題

⑴ 実際的に計算可能 (feasibly computable)な関数、および実際的に決定可能な問題の定式化

⑵ 実際的に検証可能かつ実際的に決定不能な問題はあるか？

オイラー回路問題 (1)

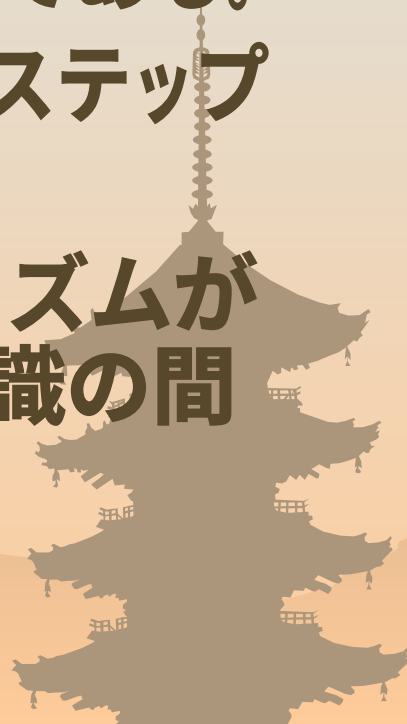
- 問題：グラフGが与えられたとき、各辺をちょうど一回ずつ通って出発点に戻ってくる道 (オイラー回路) は存在するか？
- 力づくの解法 (しらみつぶし、guess & check)：
  まず適当に道を書いてみて (guess)、それがオイラー回路になっているかどうか確かめる (check)。もしオイラー回路になっていればよし、さもなければ全ての可能な道の書き方についてこれを繰り返す (しらみつぶし)。

オイラー回路問題 (2)

- Guessが与えられたら、それが正しいかどうかを調べるのは簡単。
- しかし、グラフの点の個数がnのとき、2^n通りのguessについてcheckを行わなければならない (計算量の指数関数的爆発) 。

オイラー回路問題(3)

- うまい解法:各点の次数が偶数かどうかを調べる。
- 定理(オイラー):グラフGにオイラー回路が存在する⇔Gの全ての点の次数が偶数である。
- グラフの点の個数がnのとき、高々n^2ステップで判定は終了する。
- 定理を証明することで高速なアルゴリズムが得られる！命題的知識と手続き的知識の間の関係に対する一示唆



ハミルトン回路問題

- グラフGが与えられたとき、同じ辺を二回通ることなく各点をちょうど一回ずつ通って戻ってくる道（ハミルトン回路）は存在するか？
- しらみつぶし解法は存在する。しかしオイラー風のうまいアルゴリズムは存在するか？

課題

- オイラー回路問題に対する力づくの解法とうまい解法：後者の「うまさ」をどうやって表現すればよいか？
- ハミルトン回路問題はオイラー回路問題に比べて本質的に難しいように見える。このことをどうやって示せばよいか？
- もしハミルトン回路問題は本質的に難しい問題なのだということが言えれば、オイラー風の特徴づけを求めることは不毛だと言える。

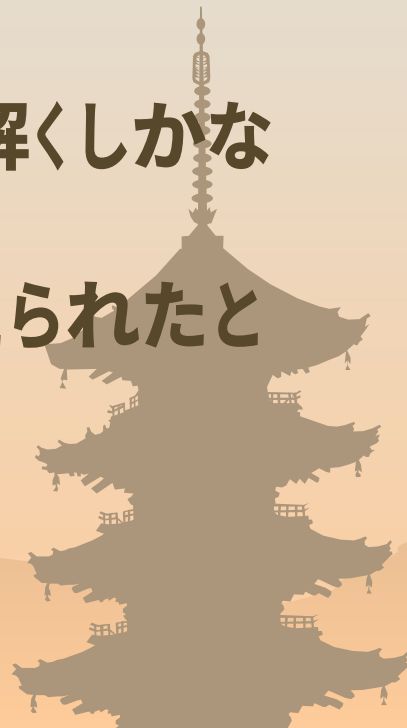
⇒グラフ論へのフィードバック

最大公約数

- 力づくの求め方：小学校算数の方法
- インプットがn桁ならば$2^{n/2}$ステップくらい必要
- うまい求め方：ユークリッド互除法
- インプットがn桁ならばn^2〜n^3ステップくらいで解ける

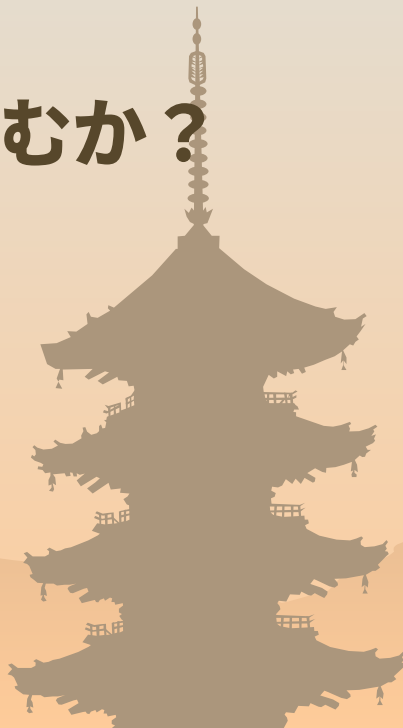
1次・2次ディオファントス方程式

- 自然数a,b,cが与えられたとき、$ax+by=c$を満たす自然数x,yは存在するか？
- 互助法を用いて簡単に解ける。
- 自然数a,b,cが与えられたとき、$ax^2+by=c$を満たす自然数x,yは存在するか？
- うまい方法は見つかっていない。力づくで解くしかないように見える。
- (参考) 13次ディオファントス方程式が与えられたとき、自然数解は存在するか？(決定不能)



問題

- 問題: INPUT, QUESTIONからなる。
- 例) ハミルトン回路
  - INPUT：グラフ G
  - QUESTION：Gはハミルトン回路を含むか？



問題の形式化

- INPUTは自然数でコード化されているものとする。
- 答えがyesとなるINPUTの集合はNの部分集合となる。
- 問題を自然数の部分集合$A \subseteq N$と同一視する。
- 例：ハミルトン回路問題＝
  {Gのコード｜Gはハミルトン回路を持つ}

INPUTのサイズ

- INPUT n のサイズ|n|：nを2進数で表したときのビット数。
- 別に10進数でもよい。グラフの場合は点の個数でもよい。LOGSPACE以上の計算量クラスに関する結果は、サイズのとり方に依存しない（reasonableなものであれば）。
- 例：Gがn個の点から成るグラフのとき

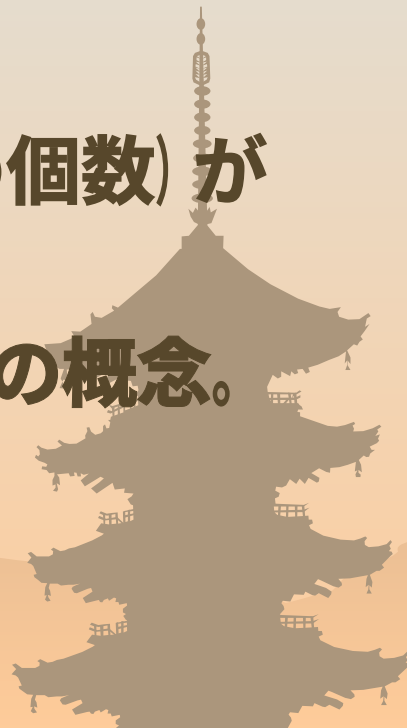
  $|G| \leqq c \cdot n^3$　（cは定数）

問題を解くチューリング機械

- チューリング機械Mが問題Aを解く
  ⇔INPUTwが与えられたとき、w∈Aの時に限りyesを出力する。
- 個々のINPUTについて解けることではない。
  全てのINPUTについて正しい答えが出せること。本質的に高次の概念。

「実際的計算可能性」の定式化 (feasible computability)

- ある関数（問題）が実際的に計算可能（実際的に決定可能）であるとはどういうことか？
- まずい定義：
  - 6時間で計算可能
  - 600000ステップで計算可能
- 着目点：INPUTのサイズ（例：グラフの点の個数）が大きくなればなるほど、多くの時間が必要。
- 計算時間の増加率に着目。本質的に高次の概念。
- 一つの境目：多項式と指数関数



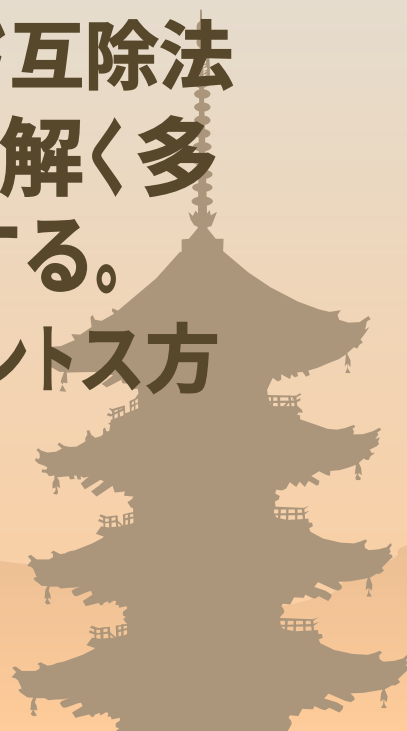
多項式 vs 指数関数

time complexity functions	Input Size n					
	1	10	100	1,000	10,000	100,000
n	1 μs	10 μs	100 μs	1ms	10ms	100ms
n^2	1 μs	100 μs	10ms	1sec	100sec	16.6min
n^3	1 μs	1ms	1sec	16.6min	11.6 days	317 years
2^n	1 μs	1ms	10^{14} years	10^{288} years	…	…

(Buss 2004)

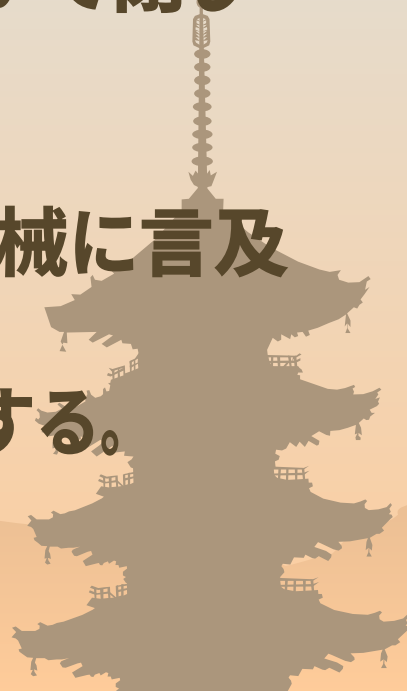
多項式時間計算量P

- 多項式時間チューリング機械：サイズnのINPUTが与えられたとき、$c \cdot n^k$ステップで停止する（ここでc,kは定数）。
  - 例：オイラーアルゴリズム、ユークリッド互除法
- 問題$A \subseteq N$がクラスPに属する⇔Aを解く多項式時間チューリング機械が存在する。
  - 例：オイラー回路問題、1次ディオファントス方程式問題
- (Cobham 1964), (Edmond 1965)



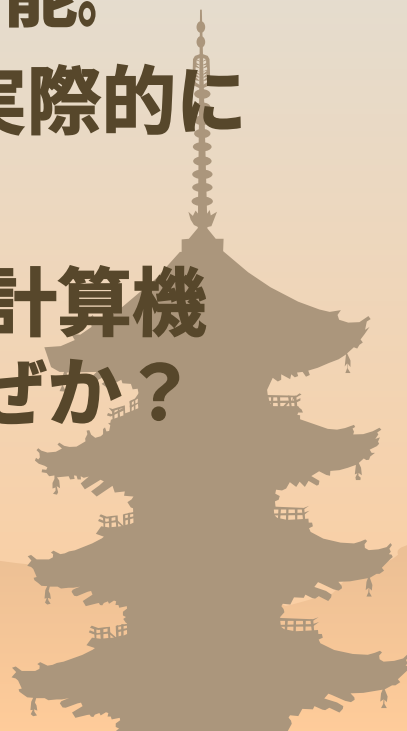
Pの定義の正当化

- 十分に安定している。定数の選び方や（現実性のあるものなら）計算モデルの選び方に依存しない。（量子コンピュータを除く）
- 多くのclosure propertyを持つ：∩、∪、補集合、合成について閉じている。（Pより上で合成について閉じている自然な時間計算量クラスはELEMENTARY！）
- 様々な非明示的（多項式やチューリング機械に言及しない）定義があり、それらが一致する。
- ある程度「実際に計算できること」とマッチする。



実際的計算可能性のテーゼ

- 問題Aが実際的に決定可能⇔A∈P
  - 多々の反例がある。この定義によれば---
  - n^{100000}時間かかっても実際的に決定可能。
  - $n^{0.00001 \log \log n}$ 時間しかかからなくても実際的に決定不能。
  - にもかかわらず、このテーゼは殆どの計算機科学者により受け入れられている。なぜか？

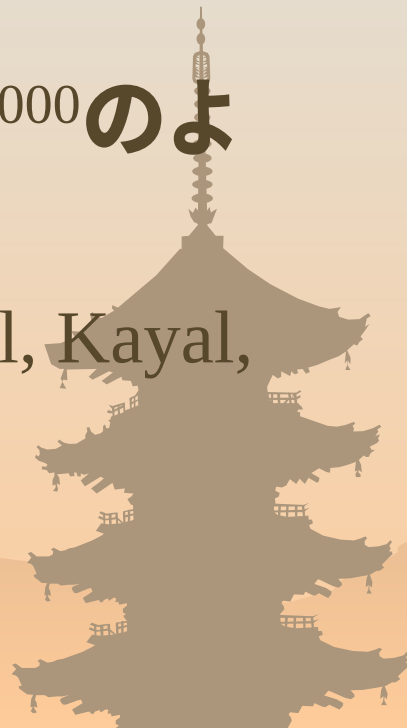


実際的計算可能性のテーゼのための弁明(1)

(1) 妥当な理論的抽象化：別に定式化自体が目的なのではなく、それについて数学的に研究したい。そのためにはたとえ近似的でも理論的に取り扱いやすいほうがよい。

(2) 経験則：自然な問題についてはn^{100000}のような大きな次数が表れることはない。

- 例：素数判定ですら$O(n^{7.5})$時間 (Agrawal, Kayal, Saxena 2002)



実際的計算可能性のテーゼのための弁明(2)

(3) 多項式時間vs指数関数時間という対立の図式の中で理解されるべき。$n^{\log \log n}$ などの緩衝地帯があってもよい。

(4) 本当はもっと別のことを言いたいのだ・・・

- 注意:量子コンピュータの実用化により、根本的に事情が変わる可能性がある。
  - 自然数の素因数分解は実際的には計算不可能と信じられているが、量子コンピュータを用いれば多項式時間で計算可能(Shor 1994)

非決定的多項式時間計算量NP

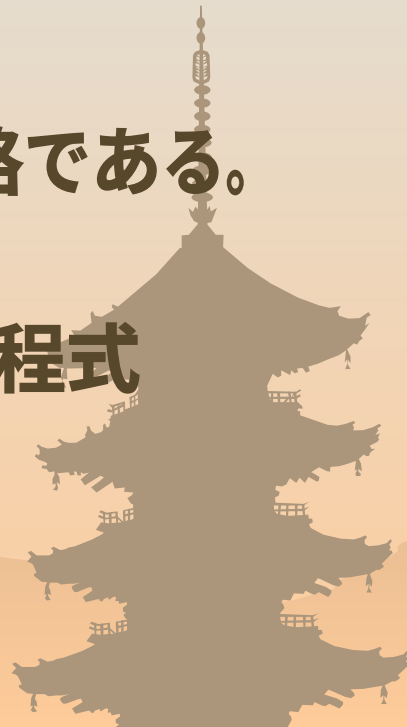
- 問題$A \subseteq N$がクラスNPに属する⇔ある$B \in P$、ある多項式pについて、

$$A(w) \Leftrightarrow \exists u.(|u| \leqq p(|w|) \wedge B(w,u))$$

  - 例1：ハミルトン回路問題

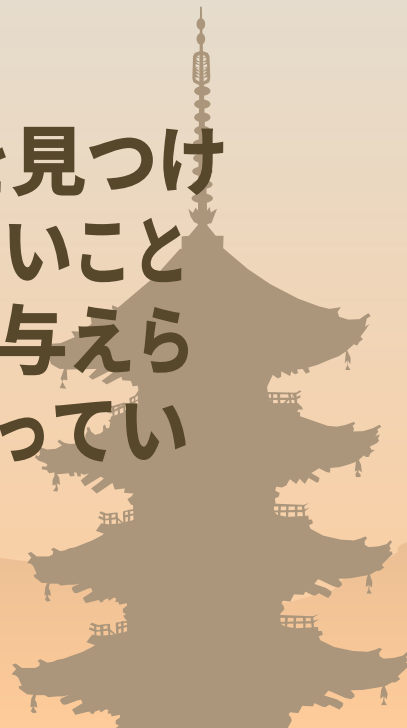
    $B(w,u)$⇔ 道uはグラフwのハミルトン回路である。
  - 例2：2次ディオファントス方程式問題

    $B(w,u)$⇔自然数uはディオファントス方程式(のコード) wの解である。
- 初出 (Cook 1971)



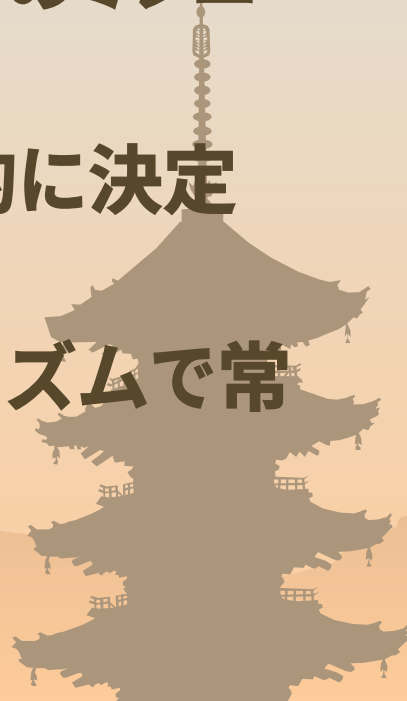
NP問題とは？

- しらみつぶしアルゴリズムにより、高々多項式サイズのguessを、それぞれ多項式時間でcheckすることにより解ける問題。
- 多項式時間検証可能問題
- 例）ハミルトン回路問題：ハミルトン回路を見つけるのは非常に難しい（ハミルトン回路がないことを示すのも非常に難しい）。しかし候補が与えられたとき、それがハミルトニアン回路になっているかどうかをcheckするのは非常に簡単。



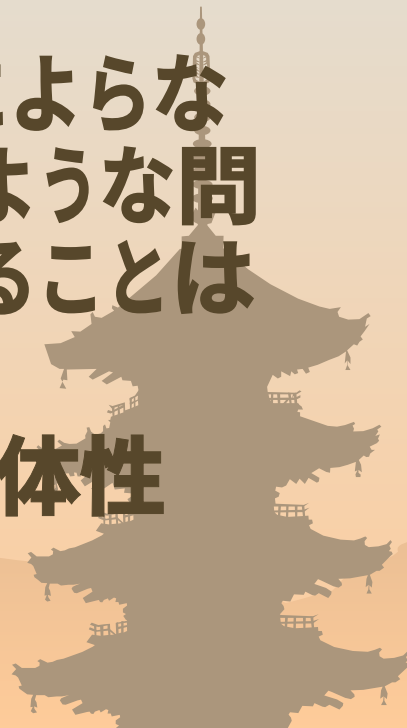
PとNP

- P⊆NPは明らか
- **根本問題：P＝NPか？**（Cook 1971）
- **計算機科学における最大の未解決問題**
- **クレイ数学研究所が2000年に提示した7つのミレニアム問題の一つ（賞金１００万ドル）**
- **「実際的に検証可能な問題は、常に実際的に決定可能か？」**
- **「力づく（しらみつぶし）は合理的なアルゴリズムで常に置き換えることが可能か？」**



PとNP (2)

- PvsNPの重要性：多くの重要な計算課題がNP問題。「しらみつぶしをすれば簡単なんだけど・・・」
- 大方の予想：P≠NP
- 「世の中には本質的にしらみつぶしによらなければ解けない問題が存在し、そのような問題に合理的なアルゴリズムを見つけることは不可能であろう。」
- 根拠：経験、NP完全問題の運命共同体性

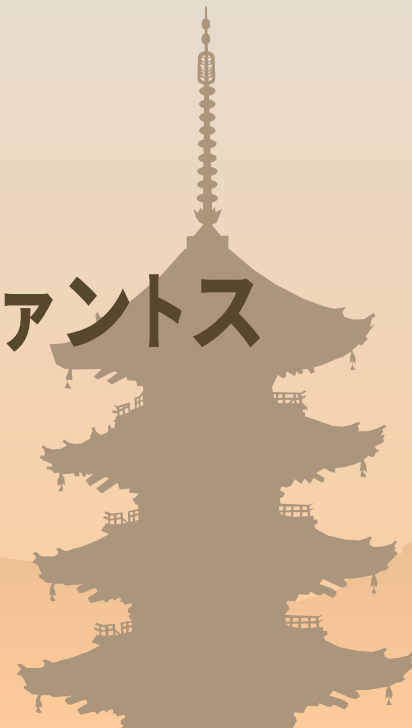


NP完全問題

- 問題Aが問題Bに還元可能である⇔ある多項式時間関数fが存在し、

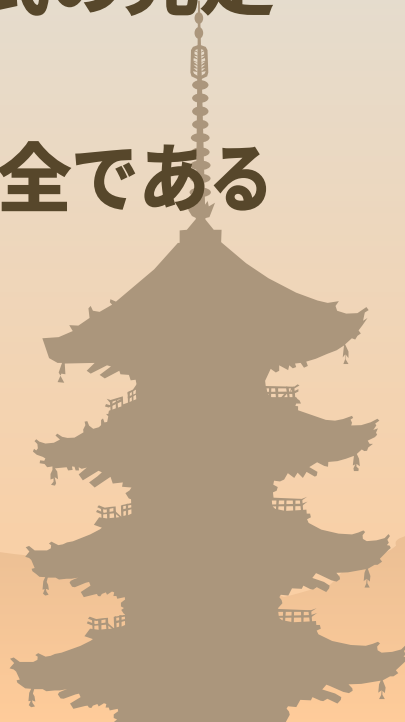
  $\forall w \ (\ w \in A \ \Leftrightarrow \ f(w) \in B \ )$

- 問題AがNP完全である⇔
  - $A \in NP$
  - 全てのNP問題がAに還元可能
- 例：ハミルトン回路問題、2次ディオファントス方程式問題…



NP完全問題とは？

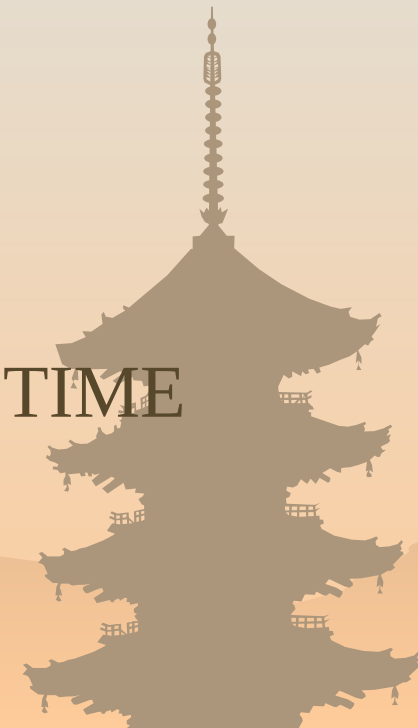
- 定理：もしもNP完全問題AがPに属するならばP=NP。
- NP問題の中で最も難しい問題。P≠NPという仮定の下では、NP完全問題は実際的には解けない。
- 最初に見つかったNP完全問題：命題論理式の充足可能性問題 (Cook 1971)
- 以後、何百以上もの興味深い問題がNP完全であることが判明した (see Garey, Johnson 1979)



その他の主な計算量クラス

- EXPTIME：**指数関数時間**
  - $2^{p(n)}$**時間で解ける問題（**p**は多項式）**
- PSPACE：**多項式空間**
  - p(n)**ビットのメモリを用いて解ける問題**
- LOGSPACE:**対数空間**
  - c・log n**ビットのメモリを用いて解ける問題**
- **定理**

$$\mathrm{LOGSPACE} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}$$



PvsNP：構造的アプローチ

- **様々な計算量クラスが成す空間の構造を探求**
- LOGSPACE≠PSPACE (**対角線論法**)
- P≠EXPTIME (**対角線論法**)
- PSPACE＝NPSPACE (**分割統治法**, Savitch 1970)
- EXP≠NEXP ⇒ P≠NP
  (**つけたし論法**, Hartmanis, Hunt 1974)
- LINSPACE⊆P ⇒ P＝NP＝PSPACE
  (**つけたし論法**, Book 1972)

構造的アプローチの一つの限界

- 対角線論法を用いて$P \neq NP$を示せるか？
- P^A：神託Aを用いて多項式時間で解ける問題
- 定理：ある神託A,Bが存在し、

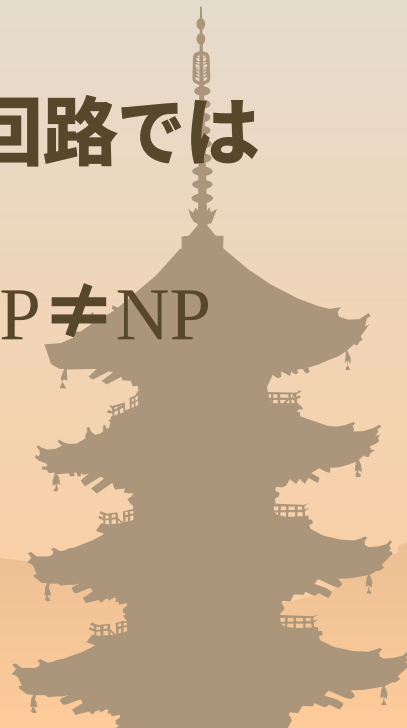
  $P^A = NP^A$　かつ　$P^B \neq NP^B$

  (Baker, Gill, Solovay 1975)
- 対角線論法は相対化する。もし$P \neq NP$が対角線論法で言えたならば、全ての神託Aについて$P^A \neq NP^A$が言えるだろう。これは上の定理に反する。

  ⇒対角線論法はその一般性ゆえに敗れる。

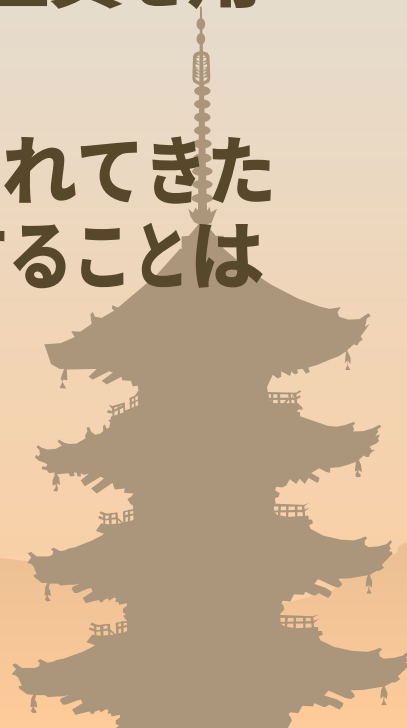
PvsNP:ブール回路アプローチ

- 具体的な関数に対して、それを計算するための最小のブール回路のサイズを見積もる。
- 定理：多項式サイズのブール回路では解けないNP問題が存在する ⇒ P≠NP
- Parity：少なくとも3n+k個のゲートが必要
- Parity：深さ固定の多項式サイズのブール回路では計算できない（Furst, Saxe, Sipser １９８４）
- mP≠mNP。単調なブール回路についてはP≠NP（Razborov １９８５）



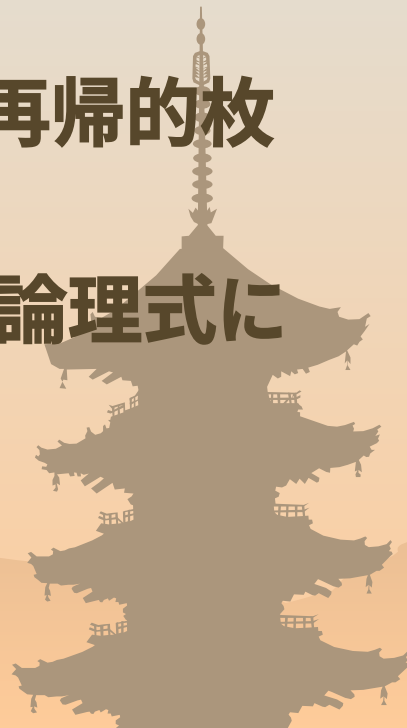
ブール回路アプローチの一つの限界

- P≠NPの「自然な」証明は存在しない（暗号学上のある仮定の下で）。(Razborov, Rudich 1994)
- 自然な証明：具体的な問題のsuper polynomialな下界を、容易に判定可能な組み合わせ論的性質を用いて示すような証明。
- 特に今までブール回路アプローチで用いられてきたような論法はそのままではP≠NPに応用することはできない。



算術階層

- Δ_0論理式：量化子は全て限定量化子 $\forall x \leqq t$、$\exists x \leqq t$の形の論理式。
- Σ_1論理式：$\exists x A$の形。ここでAは$\Delta 0$。
- Π_1論理式：$\forall x A$の形。ここでAは$\Delta 0$。
- 定理：Σ_1論理式により定義される集合＝再帰的枚挙可能集合
- 定理：Σ_1論理式により定義され、かつΠ_1論理式によっても定義される集合＝再帰的集合



ペアノ算術の部分体系

- $I\Sigma_1$：ペアノ算術において数学的帰納法の公理をΣ_1論理式に制限することにより得られる体系
- 定理：$I\Sigma_1$で$\forall x \exists ! y A(x,y)$が証明可能（Aは$\Sigma_1$⇔A(x,y)は原始再帰的関数を表現する（Parsons 1970)
- $I\Sigma_1 \subset I\Sigma_2 \subset I\Sigma_3 \cdots \subset PA$
- 同様な仕方でP、NP等の論理的特徴づけを与えることはできないか？

限定算術階層

- **言語**：0, S, +, ・, #, |x|, x/2, ≦
- **限定量化子**：∀x≦t、∃x≦t
- **sharply bounded量化子**：∀x≦|t|、∃x≦|t|
- **Δ^b_0論理式**：**量化子はすべて**sharply bounded**な論理式**
- **Σ^b_1論理式**：∃x≦t.A**の形。ここで**A**は**Δ^b_0
- **定理**：**Σ^b_1論理式により定義される集合＝**NP**集合**（Stockmeyer 1976, Wrathall 1976)

限定算術体系S^1_2

- 体系S^i_2:以下の公理から成る。
- BASIC公理群（0, S, +, ・, #, |x|, x/2, ≦の使用法を定めたもの）
- Σ^b_i-PIND：任意のΣ^b_i論理式Aについて

  $A(0) \wedge \forall x(A(x/2) \rightarrow A(x)) \rightarrow \forall x A(x)$
- S_2：BASIC公理に任意の限定論理式Aについてのの PINDを加えたもの
- 初出：　（Buss 1986）

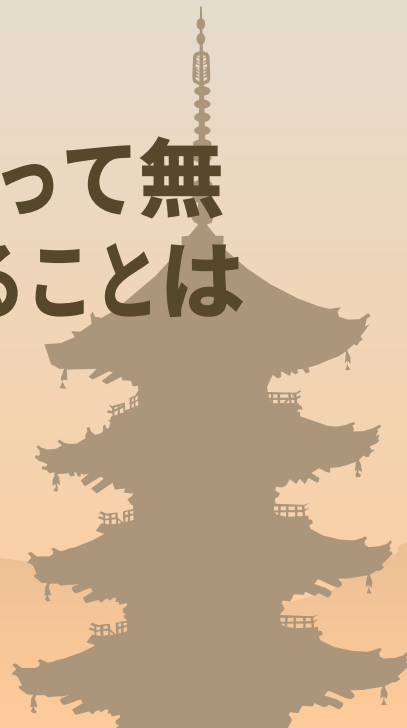
P,NPと限定算術

- **定理**：S^1_2で$\forall x \exists ! y A(x,y)$が証明可能（Aは$\Sigma^b_1$）⇔A(x,y)は多項式時間関数を表現する
- **定理**：S^2_2で$\forall x \exists ! y A(x,y)$が証明可能（Aは$\Sigma^b_2$）⇔A(x,y)は$FP^{NP}$関数を表現する

（Buss 1986）

限定算術と無矛盾性言明

- **定理：S^i_2はS^i_2の無矛盾性を証明しない。**
  (Buss 1986)
- **定理：S_2はQの無矛盾性を証明しない。**
  (cf. Wilkie, Paris 1987)
- **S^2_2はS^1_2の無矛盾性を証明しない。よって無矛盾性言明を用いてS^1_2とS^2_2 を分けることはできそうにない。**



多項式時間階層とS_2階層

- **定理：S_2が有限公理化可能**
  ⇔あるiについて$S_2 = S^i_2$
  ⇔ S_2は多項式時間階層が崩壊することを証明する。（Kreisel, Takeuti, Pudlak 1991, Buss 1993)

P=NP問題の行方 (1)

- **意見調査：100人の専門家に聞きました** (Gasarch 2002)
- **Q1**: PvsNP**問題はいつ解かれるか？**
  - **2071年 (100周年) まで：61人**
  - **3000年まで：13人**
  - **永遠に解けない：5人**

P=NP問題の行方 (2)

- Q2：どのような形で解決するか？
  - P≠NP：61人
  - P=NP：　9人
  - ZFCから独立：4人

まとめ

- 実際的計算可能性のテーゼ：多くの反例があるにもかかわらず、これだけ受け入れられているのはなぜか？
- PvsNP問題：実際的に検証可能な問題は常に実際的に計算可能か？「しらみつぶしは常に合理的なアルゴリズムで置き換えられるか？」
- 使い古された対角線論法ではなく、根本的に新しい手法が必要とされている。