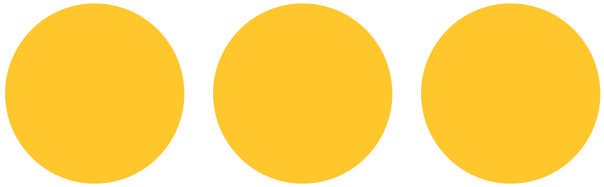
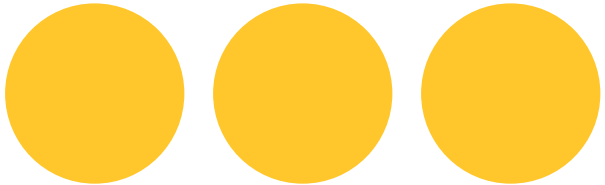


猫にもわかるP≠NP予想

@xharaken



今日の話の流れ

目標:

- P≠NP予想とは何なのかを理解する
- なぜP≠NP予想が重要なのかを理解する

今日の話の流れ

- P≠NP予想は、とても理論的な話です

- コンピュータサイエンス系の講義のなかでも、理解するのがもっとも難しい話題のひとつです

- 今日は、できるかぎりわかりやすく解説します

ざっくり言って、P≠NP予想とは何なのか

- コンピュータが解くことができる問題（グラフ探索、ソーティング、巡回セールスマン問題、etc）の「難しさ」に関するひとつの予想

- あとで説明しますが、問題の「難しさ」には、Pという概念とNPという概念があって、「P＝NPなのかP≠NPなのか」を議論するのがP≠NP予想
    - 「予想」という名のとおり、どっちなのかはまだ証明されていない
    - 多くの研究者がP≠NPだと予想している

なぜP≠NP予想が重要なのか

重要性1：計算機科学の未解決問題のなかで最重要な問題のひとつだから

- クレイ数学研究所のミレニアム懸賞問題として、100万ドルの懸賞金がかけられている
- 「コンピュータサイエンスを修めた」というからには、教養として知っておくことは重要
- 未解決問題にはロマンがある

なぜP≠NP予想が重要なのか

重要性2：現代暗号の安全性はP≠NPであることを仮定しているから

- 万が一P＝NPであることが証明されてしまえば、現代暗号が破綻する
    - たとえば素因数分解も簡単に計算できてしまうことになる
- インターネットのセキュリティモデルが根幹から崩れる可能性がある

なぜP≠NP予想が重要なのか

重要性3：PやNPの概念を理解していると、問題を解くときに適切なアルゴリズムを選べるようになるから

- もしP≠NPであることが証明されれば、巡回セールスマン問題に対して「O(N^3)以下のアルゴリズムはあるかな？」と考えることは無意味
  - 存在しないことが理論的に言える
  - 最初から、ヒューリスティクスなりの近似解法を考えるべきだとわかる

さて、そろそろ本題に入りましょう

- Pとは何なのか
- NPとは何なのか
- P≠NP予想とは何なのか

P≠NP予想が対象にする問題

- さっきも言ったように、P≠NP予想とは、「コンピュータが解くことができる問題」の「難しさ」に関するひとつの予想
    - 「コンピュータが解くことができる問題」とは何か？

- いろんな定義があるが、ここでは決定問題（decision problem）を対象にする
    - 決定問題 ＝ 答えが1か0で決まる問題のこと

決定問題の例

- 文字列AとBが与えられたとき、BはAの部分文字列か？

- 与えられた数Aには、B以下の約数があるか？

- 与えられたグラフに閉路があるか？

決定問題の例

- 巡回セールスマン問題は、そのままでは決定問題ではない
  - 「すべての都市を1回ずつ通る最短経路はどれか？」
    - 答えが1か0かで決まらない

- こう言い換えれば決定問題になる：
  - 「すべての都市を1回ずつ通る長さ*X*以下の経路が存在するか？」

易しい問題と難しい問題

- さて、世の中には「易しい」問題もあれば「難しい」問題もある
    - 正確な定義は後述

- ソーティング：O(N log N)で解けるから、まぁ易しい

- 巡回セールスマン問題：O(N!)通りの経路を調べないと解けそうにないから、まぁ難しい

易しい問題の定義

- 多項式時間（polynomial time） ＝ *N*の多項式で表される時間
  - O(*N*^5)は多項式時間
  - O(*N* log *N*)も多項式時間（O(*N*^2)で抑えられるから）
  - O(2^*N*)は多項式時間ではない

-「易しい問題」＝ 多項式時間で解ける問題
  - ソーティングは「易しい問題」
  - 文字列検索も「易しい問題」

Pとは何なのか

- クラスP ＝ 多項式時間で解ける問題の集合（＝「易しい問題」の集合）
    - ソーティングも文字列検索もクラスPに属する
    - “P”は“polynomial”の“p”

- これで「PとNP」のうち「P」のほうはわかりました
    - ではNPとは何なのか？

NPとは何なのか

- クラスNP ＝ 多項式時間で解けない問題の集合？
    - 巡回セールスマン問題は多項式時間では解けないからクラスNPに属する？
    - “NP”って“non polynomial”の略？

- 実はそうじゃないんだな…
    - ここを理解できるかどうかが、P≠NP予想を理解できるかどうかの鍵

NPとは何なのか

- もし仮に、
    - クラスP ＝ 多項式時間で解ける問題の集合
    - クラスNP ＝ 多項式時間で解けない問題の集合

だとしたら、定義からして、P≠NPであることは（「予想」するまでもなく）明らか

- クラスNPの定義がそうではないから、P≠NPかどうかが問題になっている

NPとは何なのか

- 「巡回セールスマン問題は多項式時間で解けない」というのも誤り

- 「巡回セールスマン問題を解く多項式時間アルゴリズムはまだ知られていない」というだけであって、ないかどうかは証明されていない

- ではNPとは何なのか？

NPとは何なのか

- クラスNP（Non-deterministic polynomial time）＝ ある解候補が与えられたとき、それが本当に解であるかどうかを多項式時間で確認できる問題の集合

NPとは何なのか

- 巡回セールスマン問題＝「すべての都市を1回ずつ通る長さX以下の経路が存在するか？」
    - ある都市の列が与えられたときに、それが長さX以下の経路になっているかどうかを確認することは$O(N)$でできる
    - よって、巡回セールスマン問題はNPに属する

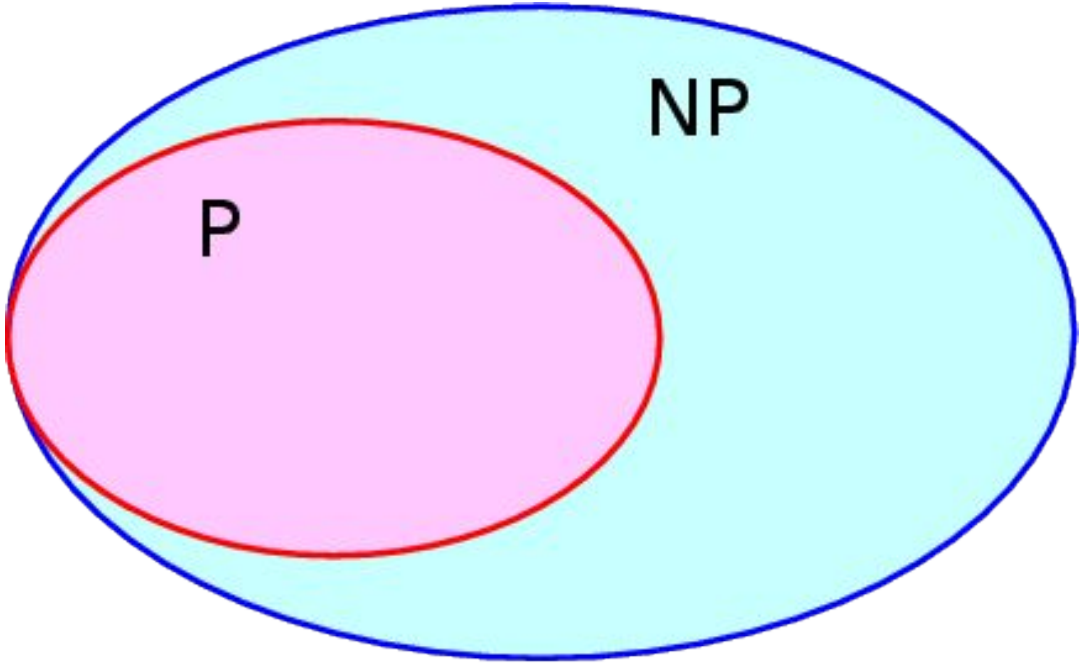
PとNPの関係

- 定義を比べてみよう
  - クラスP ＝ 多項式時間で解ける問題の集合
  - クラスNP ＝ 与えられた解候補が本当に解であるかどうかを多項式時間で確認できる問題の集合

- 当然、Pに属する問題はNPにも属する
  - ソーティングはPでもあるし、NPでもある
  - 巡回セールスマン問題はNPであるが、Pであるかどうかはわかっていない

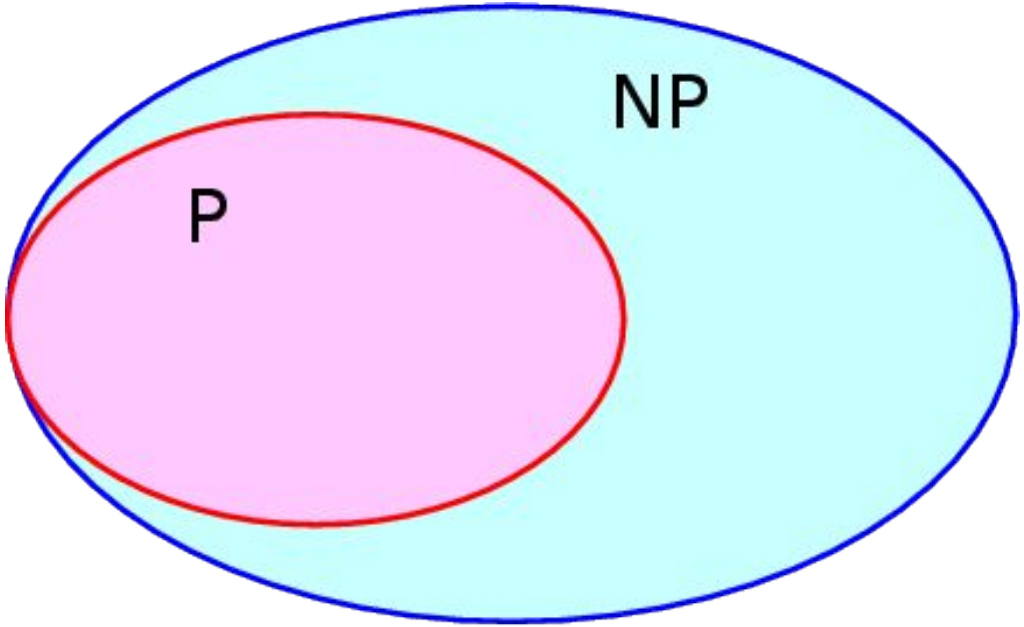
PとNPの関係

- PはNPの部分集合



それで、P≠NP予想とは何なのか

- まさしく「このPの集合とNPの集合が一致しているかどうか」を考えるのがP≠NP予想



それで、P≠NP予想とは何なのか

- 正確な言い方：

「多項式時間で解ける問題の集合と、与えられた解候補が本当に解であるかどうかを多項式時間で確認できる問題の集合は一致しているかどうか？」

- もっとわかりやすい言い方：

「自分で考えて答えを出すのと（＝クラスP）、他人から聞いた答えが正しいかどうかを確認するのとでは（＝クラスNP）、どちらが簡単か？」（東野圭吾「容疑者Xの献身」より抜粋）

もしP＝NPだとわかると何が起きるか

- 万が一、P＝NPが証明されたとすると、それはつまり、「NPに属する問題は多項式時間で解けてしまう」ことになる
    - 巡回セールスマン問題も多項式時間で解ける
    - 素因数分解問題も多項式時間で解ける
    - ハッシュ関数の結果を元に戻すのも多項式時間で解ける
    - その他、現代暗号理論が「多項式時間では解けないから安全」だと仮定しているいろんな問題も多項式時間で解けてしまう

もしP≠NPだとわかると何が起きるか

- 現代暗号理論の安全性が保証される

- ある問題がPでないとわかっていれば、「効率の良い多項式時間アルゴリズムを考えよう」などという実らない努力をする必要がなくなる
    - そんなものは存在しない
    - 最初から、近似解法で解くべきだ（解くしかない）とわかる

多くの研究者の予想

- 多くの研究者は、P≠NPだと予想している
  - 「さすがに巡回セールスマン問題は多項式時間では解けないでしょ」
  - 一方で、P＝NPを証明しようとしている人たちもたくさんいる

- いずれにせよ、P≠NPかどうかで計算機科学の世界は大きく変わる

PとNPの関係を掘り下げる

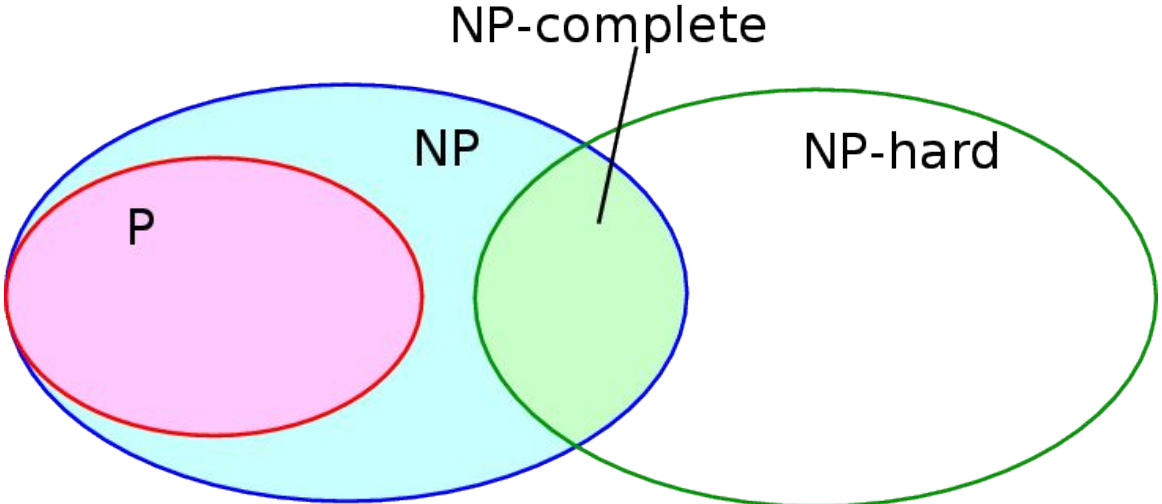
- ところで、「P＝NPであること」あるいは「P≠NPであること」を示すには、具体的には何を示せばよいのか？

- 理解を深めるために、もう少しPとNPの関係を掘り下げてみよう

- 大切な概念：
    - NP困難
    - NP完全

NP困難とNP完全

- NP困難（NP-hard）な問題 ＝ NPに属するどの問題よりも同程度以上に難しい問題のこと
- NP完全（NP-complete）な問題 ＝ NP困難であって、かつNPに属する問題のこと（＝NPのなかでいちばん難しい問題のこと）



NP困難とNP完全

- 話が抽象的になってきました

- 問題Aが問題B「よりも難しい」って、具体的にはどういうこと？
    - 巡回セールスマン問題はソーティング「よりも難しい」気はする
    - 巡回セールスマン問題と素因数分解問題はどっちが難しいのか？
- 「よりも難しい」の意味をはっきりさせることが必要

「よりも難しい」の直観的な理解

- 問題Aが問題B「よりも難しい」とはどういうことか？

- 「問題Aが解けたと仮定するなら、問題Bも解ける」とき、「問題Aは問題Bよりも同程度以上には難しい」と言う
    - 例：「オムライスを作れるなら、オムレツも作れるに決まっている」ならば、「オムライスを作るのは、オムレツを作るよりも同程度以上には難しい」

「よりも難しい」の定義

- 問題Aへの任意の入力xを、多項式時間で問題Bへの入力x'に変換できて、かつ、「xに対する問題Aの答え＝x'に対する問題Bの答え」になっているとき、問題Aは問題Bへ多項式時間還元できる（polynomial time reducible）と言う
    - 要するに「問題Bが解ければ問題Aが解ける」

- 問題Aが問題Bに多項式時間還元できるとき、問題Bは問題A「よりも同程度以上に難しい」と言う

多項式時間還元の例

- ハミルトン閉路問題:「あるグラフが与えられたとき、すべての頂点を1度ずつたどる巡回路が存在するか？」

- 巡回セールスマン問題:「あるグラフが与えられたとき、すべての頂点を1度ずつたどる長さX以下の巡回路が存在するか？」

- どっちが難しいか？

多項式時間還元の例

- 直観的な理解：
  - 見るからに、巡回セールスマン問題のほうが、ハミルトン閉路問題よりも一般的な問題を解いている
  - 「巡回セールスマン問題が解ければ、ハミルトン閉路問題も解ける」
  - 「巡回セールスマン問題は、ハミルトン閉路問題よりも同程度以上に難しい」

多項式時間還元の例

- 正確な理解：
  - ハミルトン閉路問題の任意の入力をそのまま巡回セールスマン問題の入力にして（この操作は明らかに多項式時間で可能）、$X=\infty$として巡回セールスマン問題を解けば、ハミルトン閉路問題の答えが得られる
  - 「ハミルトン閉路問題は巡回セールスマン問題に多項式時間還元できる」
  - 「巡回セールスマン問題は、ハミルトン閉路問題よりも同程度以上に難しい」

NP困難とNP完全を振りかえってみよう

- NP困難（NP-hard）な問題 ＝ NPに属するどの問題よりも同程度以上に難しい問題のこと（＝NPに属するすべての問題から多項式時間還元できる問題のこと）

- NP完全（NP-complete）な問題 ＝ NP困難であって、かつNPに属する問題のこと（＝多項式時間還元という尺度で難しさを測ったときに、NPのなかで「いちばん難しい」問題のこと）

ある問題がNP完全であることを示すには

- NP困難かつNPであることを言えばよい
  - 「NPであること」を言うのはたいてい簡単
    - 与えられた解候補が本当に解になっているかどうかを多項式時間で確認できることを言えばよいだけ
  - 「NP困難であること」を言うのは大変
    - NPに属するすべての問題がその問題に多項式時間還元できることを言わなければならない

ある問題がNP困難であることを示すには

- 1971年にCookさんというすごい人が、NPに属するすべての問題が、SATという問題に多項式時間還元できることを示してくれた

- SAT（充足可能性問題）:
  - 入力：N変数（$X1, X2, \ldots, XN$）を¬、∨、∧でつなげた命題論理式
    - 例：$X1 \vee X2 \wedge (\neg X3 \vee X1)$
  - 出力：その命題論理式を真にする0-1変数の割り当てがあれば1、なければ0

ある問題がNP困難であることを示すには

- Cookさんのおかげで、話はずいぶん楽になった

- ある問題AがNP困難であることを示すのに、「NPに属するすべての問題がその問題Aに多項式時間還元できること」を示す必要はもはやなく、「SATから問題Aに多項式時間還元できること」さえ言えばよい
    - SATがNPに属するすべての問題よりも同程度以上に難しいことは既知
    - ならば、問題AがSATよりも同程度以上に難しいことさえ言えばよい

ある問題がNP困難であることを示すには

- かくして、数千以上の問題がNP困難であることが示されてきた（これらの問題はNPに属するので、さらにNP完全でもある）
    - ハミルトン閉路問題
    - 巡回セールスマン問題
    - ナップザック問題
    - ぷよぷよ全消し可能判定
    - マインスイーパ
    - …

巡回セールスマン問題が NP完全なことの証明

(0) SATはNP困難（Cookさんが示してくれた）

(1) SATがハミルトン閉路問題に多項式時間還元可能（ちょっと難しいが示せる）

(2) ハミルトン閉路問題が巡回セールスマン問題に多項式時間還元可能（さっき示した！）

(3) したがって、巡回セールスマン問題はNP困難

(4) 巡回セールスマン問題はNP（さっき示した！）

(5) したがって、巡回セールスマン問題はNP完全

補足

- ところで、論理が循環してない？
    - SATは、NPに属するすべての問題よりも同程度以上に難しい
    - ハミルトン閉路問題はSATよりも同程度以上に難しい
    - 巡回セールスマン問題はハミルトン閉路問題よりも同程度以上に難しい

- ん？？でも、SATは巡回セールスマン問題よりも同程度以上に難しいはず…

補足

- この論理の循環が意味すること:
    - 結局のところ、「すべてのNP完全な問題は同程度の難しさを持っている」ということを意味している

- SATも、巡回セールスマン問題も、ぷよぷよも、「同程度に難しい」

補足

- 見るからに、巡回セールスマン問題はハミルトン閉路問題よりも一般的な問題なので、この2つの問題が「同程度に難しい」というのは直観には反するかもしれない

- しかし、「多項式時間還元できるかどうか」という尺度で測った場合には、この2つの問題は「同程度に難しい」ことになる
    - 実際に、巡回セールスマン問題とハミルトン閉路問題の多項式時間還元は双方向に可能（でないと矛盾する）

話をまとめます

- ここまでの議論で、PやNPの世界で「難しさ」がどう測られているかはわかりました
  - 「多項式時間還元できるかどうか」が難しさの尺度
  - 問題Aが問題Bに多項式時間還元できるならば、問題Bは問題A「よりも同程度以上に難しい」
  - NP困難な問題は、NPに属するすべての問題「よりも同程度以上に難しい」
  - NP完全な問題は、NPのなかで「いちばん難しい」
  - NP完全な問題は、すべて「同程度の難しさ」を持っている

P≠NP予想が解かれるために必要なこと

- ここまでわかると、P≠NP予想が解かれるためには何が示される必要があるのかわかるはずです

- P≠NP予想の可能な帰結：
  - 「P＝NPであること」が示される
  - 「P≠NPであること」が示される

- それぞれ何が示されればよいのか？

P=NPを示すためには

- P＝NPを示すには、ひとつでよいから、NP完全な問題のうち多項式時間で解けるものを見つければよい
  - NP完全な問題はNPのなかでいちばん難しいのだから、それさえ多項式時間で解ければ、P＝NPを示すのに十分
  - 例：巡回セールスマン問題を多項式時間で解く方法を見つければ、P＝NPが示せたことになる

P≠NPを示すためには

- P≠NPを示すには、ひとつでよいから、NPに属する問題のうち多項式時間で解けないものを見つければよい
    - NPに属する問題であればよく、NP完全な問題である必要はない
    - 例：巡回セールスマン問題を多項式時間で解く方法がないことが言えれば、P≠NPを示せたことになる

まとめ

- このスライドで説明したこと
  - P、NP、NP困難、NP完全とは何なのか
  - P≠NP予想とは何なのか、なぜそれが重要なのか
  - P≠NP予想が解かれるためには、具体的に何が示されれる必要があるのか

- 理論の詳細はともかく、コンピュータサイエンスを修めたというからには議論の大筋を把握しておくことは重要

理解を深めるための確認クイズ

- 正しければ○、正しくなければ×と答えてください！

(1) NPとは、多項式時間では解けない問題の集合である

(2) Pには属するがNPには属さない問題が存在する

(3) 文字列検索問題（文字列Aが文字列Bに含まれているかどうか）はPであり、かつNPである

理解を深めるための確認クイズ

(4) SATを巡回セールスマン問題に多項式時間還元することもできるし、逆に、巡回セールスマン問題をSATに多項式時間還元することもできる
(5) 問題AをNP困難な問題に多項式時間還元できれば、問題AがNP困難であることを示せたことになる
(6) NP完全な問題Aと問題Bがあったとき、問題Aから問題Bへ多項式時間還元できないことがありうる
(7) NP困難な問題Aと問題Bがあったとき、問題Aから問題Bへ多項式時間還元できないことがありうる

理解を深めるための確認クイズ

(8) ひとつでよいから、「NPに属する問題であって、多項式時間で解けないもの」を見つければ、P≠NPを示したことになる
(9) ひとつでよいから、多項式時間で解けるNPな問題を見つければ、P＝NPを示したことになる
(10) ひとつでよいから、多項式時間で解けるNP完全な問題を見つければ、P＝NPを示したことになる
(11) ひとつでよいから、多項式時間で解けるNP困難な問題を見つければ、P＝NPを示したことになる

理解を深めるための確認クイズ

(12) 巡回セールスマン問題を多項式時間で解く方法を見つければ、P＝NPを示したことになる

(13) 巡回セールスマン問題を多項式時間で解けないことを示せば、P≠NPを示したことになる