Proceedings of the Twenty-Sixth RAMP Symposium
Hosei University, Tokyo, October 16-17, 2014

新学術領域「計算限界解明」について

On the Project ELC, Exploring the Limits of Computation

渡辺　治[1*]

Osamu Watanabe

概要　H24 年度採択の新学術領域の 1 つとして開始した「多面的アプローチの統合による計算限界の解明」（略称，「計算限界解明」）についての紹介をさせて頂く．本領域は，計算複雑さの理論は，様々な計算に対し，それに対する計算手法の限界を研究する学問分野で，アルゴリズムや情報セキュリティ技術の基礎理論に位置する．実際，計算複雑さの理論を発端に，公開鍵暗号，計算論的学習理論（← データマイニングの基礎理論）等々，社会を変えるような情報科学技術が誕生してきた．しかし，その一方で，P≠NP 予想に代表されるように，未解決の課題も非常に多い．このような，まだまだ未開拓で魅力的な分野に対し，本領域では，幅広い関連分野からの研究者集団が，複数の観点から，新たな解析手法や自然で強力な切り口を提案する研究を行う．それにより，計算限界の完全解明へ向けての将来性の高い研究の道筋を構築することを目指す．現在，2 年ほど経過して，いくつか手ごたえのある成果も得られつつある．こうした進捗状況や今後の研究課題について述べる．

キーワード　計算複雑さの理論，P≠NP 予想，計算の理解，革新的アルゴリズムの基盤社会に変革をもたらすような計算の基盤

1　東京工業大学 数理・計算科学専攻, 〒152-8552 東京都目黒区大岡山
Department of Mathematical and Computing Science, Tokyo Institute of Technology, Meguro-ku Ookayama, Tokyo 152-8552, Japan

∗　E-mail address: watanabe@is.titech.ac.jp

2014.10.17
OR学会 RAMP

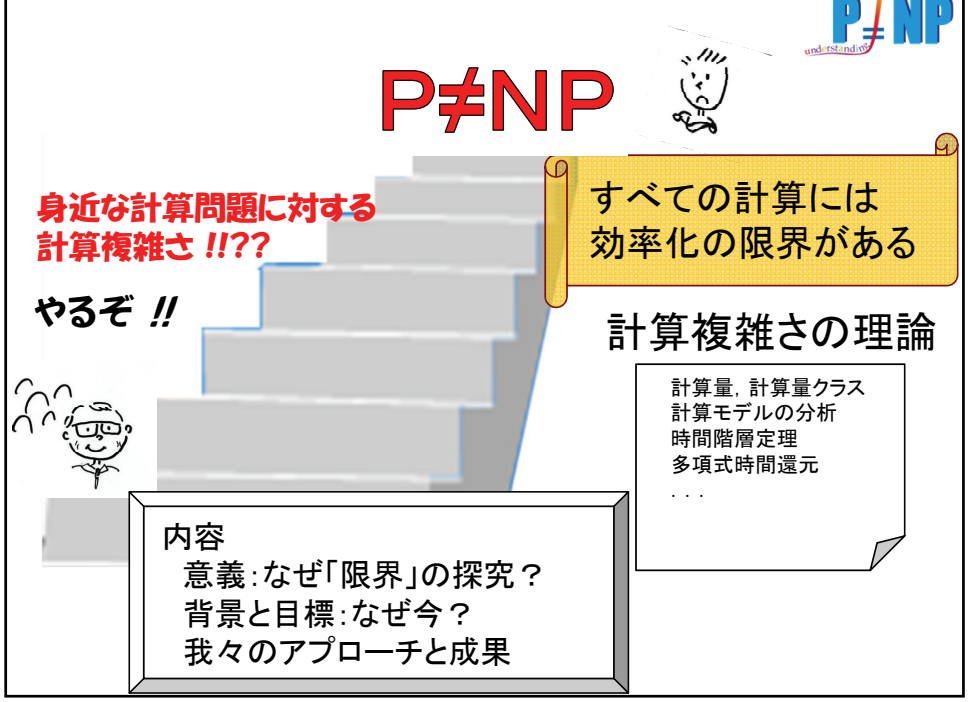
領域の概要・成果の概観

新学術領域「計算限界解明」

科研費新学術領域 H24 ～ H28
多面的アプローチの統合による計算限界の解明

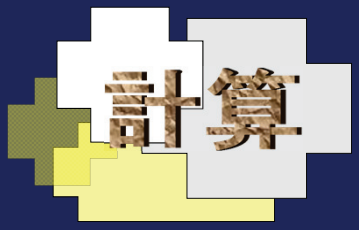
P≠NP understanding

領域代表
渡辺　治（東京工業大学）



なぜ「計算限界」？

なぜ計算？
　情報を形にできるから



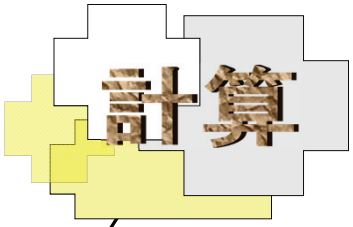
コンピュータに載せる

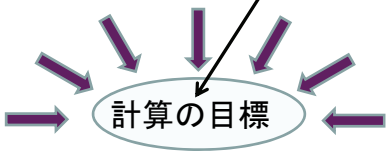
人類が初めて「情報」を様々な角度から見ることが可能となった

なぜ「計算限界」？

なぜ計算？
　情報を形にできるから

なぜ計算**限界**？
　計算を
　　真に理解するため





様々なアルゴリズム

スパコン「京」

スパコンあれば必要ない！

良 ← 1000 倍 → 悪

アルゴリズム

- コンピュータを生かすも殺すもアルゴリズム次第
- コンピュータの性能 ↗
  ⇒ アルゴリズムの重要性 ↗
  ∵高度なアルゴリズムが使える

計算を知るべし

それは大きな勘違い !!

アルゴリズム仙人

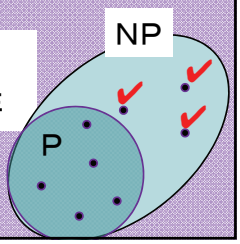
なぜ P ≠ NP 予想？

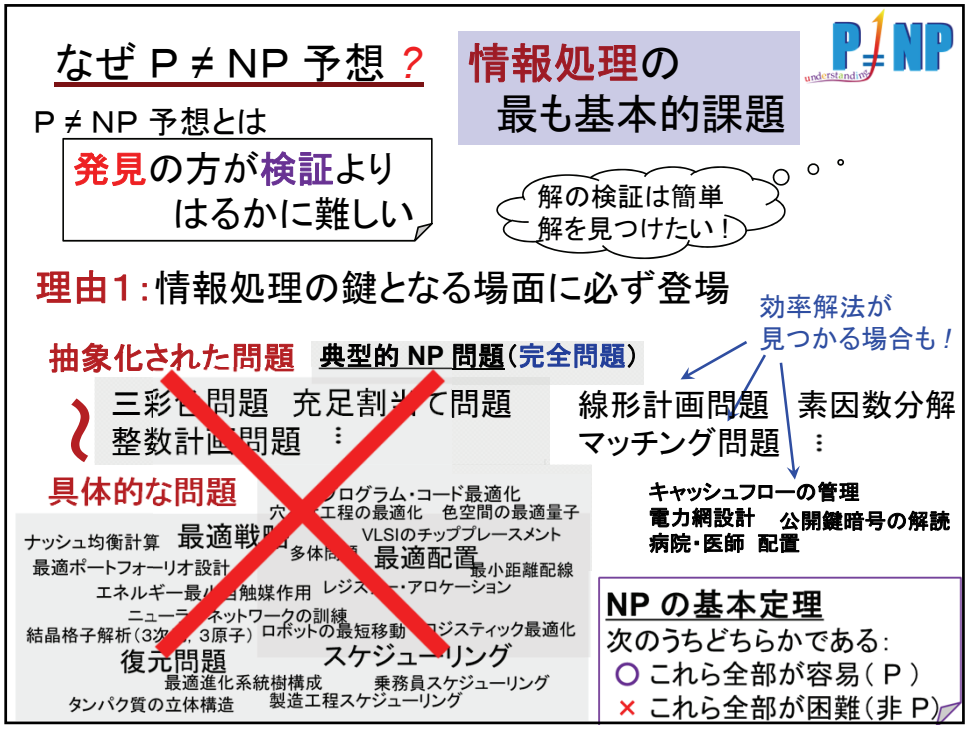
P≠NP予想

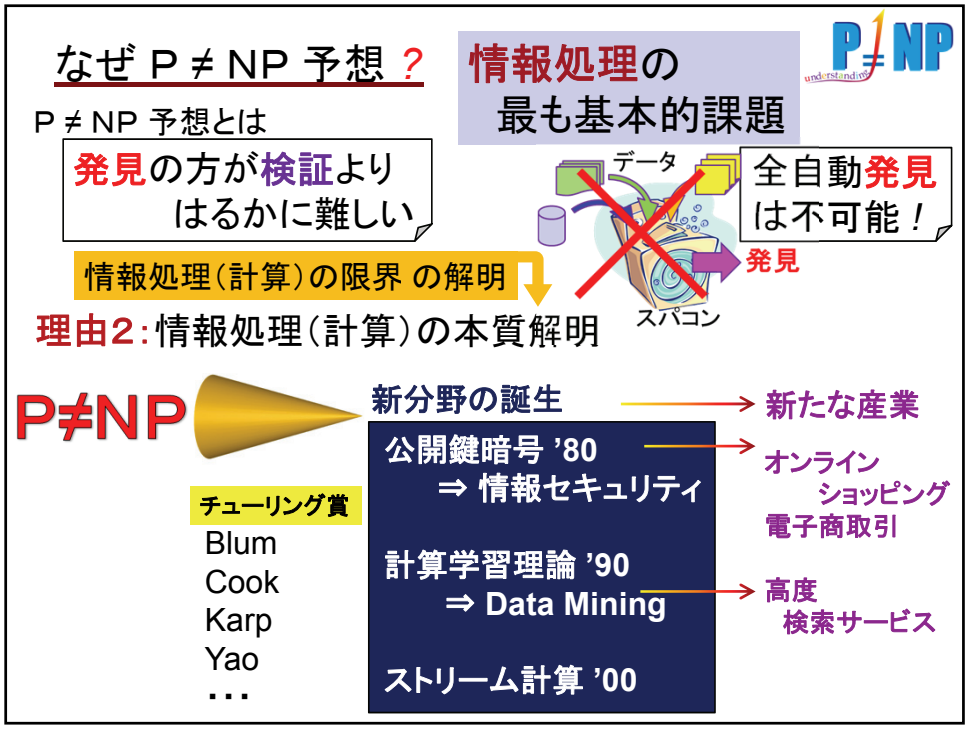
P ≠ NP予想とは

解を発見は解の検証よりはるかに難しい.

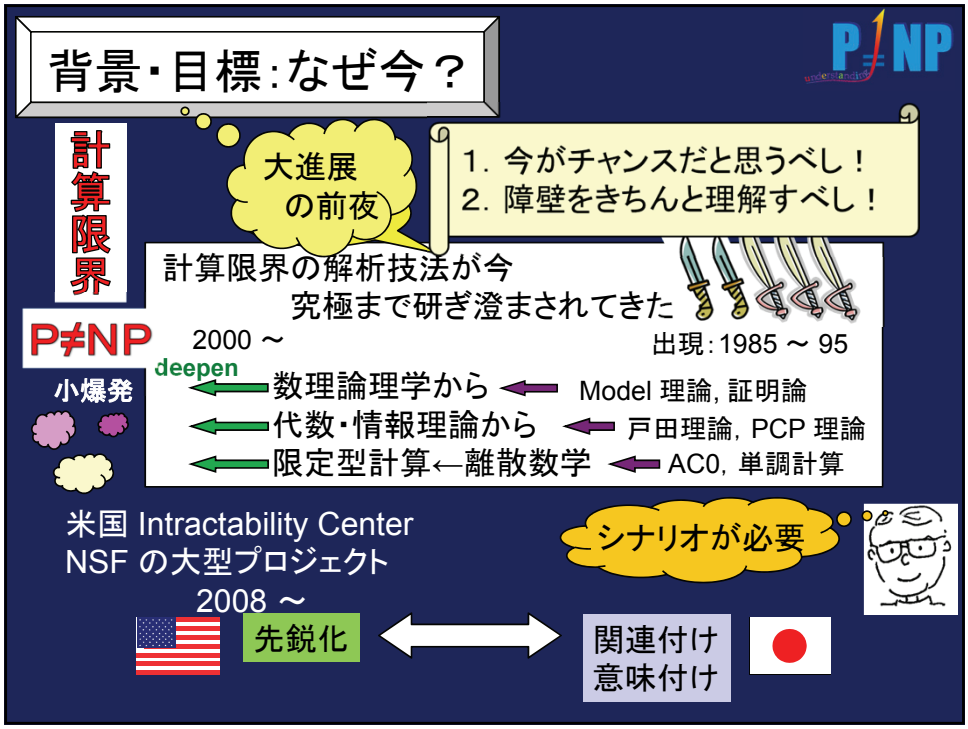
P ⇔ 解の発見の計算が容易な問題群
NP ⇔ 解の検証の計算が容易な問題群




なぜ P ≠ NP 予想 ？
情報処理の
最も基本的課題
P ≠ NP 予想とは
発見の方が検証より
はるかに難しい
解の検証は簡単
解を見つけたい！
理由1：情報処理の鍵となる場面に必ず登場
効率解法が
見つかる場合も！
抽象化された問題
典型的 NP 問題（完全問題）
三彩色問題　充足割当て問題
整数計画問題　⋮
線形計画問題　素因数分解
マッチング問題　⋮
具体的な問題
プログラム・コード最適化
穴あけ工程の最適化　色空間の最適量子
VLSIのチッププレースメント
ナッシュ均衡計算　最適戦略
最適ポートフォーリオ設計
多体問題　最適配置
最小距離配線
エネルギー最小化　触媒作用　レジスター・アロケーション
ニューラルネットワークの訓練
結晶格子解析（3次元, 3原子）　ロボットの最短移動　ロジスティック最適化
復元問題
スケジューリング
最適進化系統樹構成　乗務員スケジューリング
タンパク質の立体構造　製造工程スケジューリング
キャッシュフローの管理
電力網設計　公開鍵暗号の解読
病院・医師　配置
NP の基本定理
次のうちどちらかである：
○ これら全部が容易（P）
× これら全部が困難（非 P）

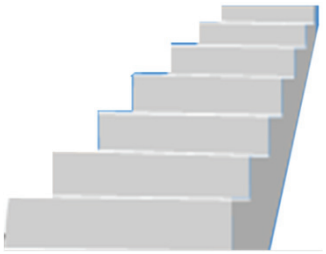

なぜ P ≠ NP 予想 ？
情報処理の
最も基本的課題
P ≠ NP 予想とは
発見の方が検証より
はるかに難しい
データ
全自動発見
は不可能！
発見
スパコン
情報処理（計算）の限界 の解明
理由2：情報処理（計算）の本質解明
P≠NP
チューリング賞
Blum
Cook
Karp
Yao
・・・
新分野の誕生
新たな産業
公開鍵暗号 ’80
⇒ 情報セキュリティ
オンライン
ショッピング
電子商取引
計算学習理論 ’90
⇒ Data Mining
高度
検索サービス
ストリーム計算 ’00


なぜ「計算限界」？
P≠NP
understanding
P≠NP予想
ほんの一例
様々な計算
Complexity Zoo
交替計算
対話計算
計算限界の解明
論理式
省スペース計算
乱択計算
計算の理解
量子計算
単調回路計算
非一様回路計算


背景・目標：なぜ今？
P≠NP
understanding
計算限界
大進展の前夜
1. 今がチャンスだと思うべし！
2. 障壁をきちんと理解すべし！
計算限界の解析技法が今
究極まで研ぎ澄まされてきた
出現：1985 ～ 95
P≠NP
2000 ～
小爆発
deepen
数理論理学から ← Model 理論，証明論
代数・情報理論から ← 戸田理論，PCP 理論
限定型計算←離散数学 ← AC0，単調計算
米国 Intractability Center
NSF の大型プロジェクト
2008 ～
シナリオが必要
先鋭化
関連付け
意味付け

目標：大理論の構築へ

計算限界



解析技法が究極まで
研ぎ澄まされ
てきた今

解決への道筋を
示す指導原理の構築
を目指す

百年の計

如何に？

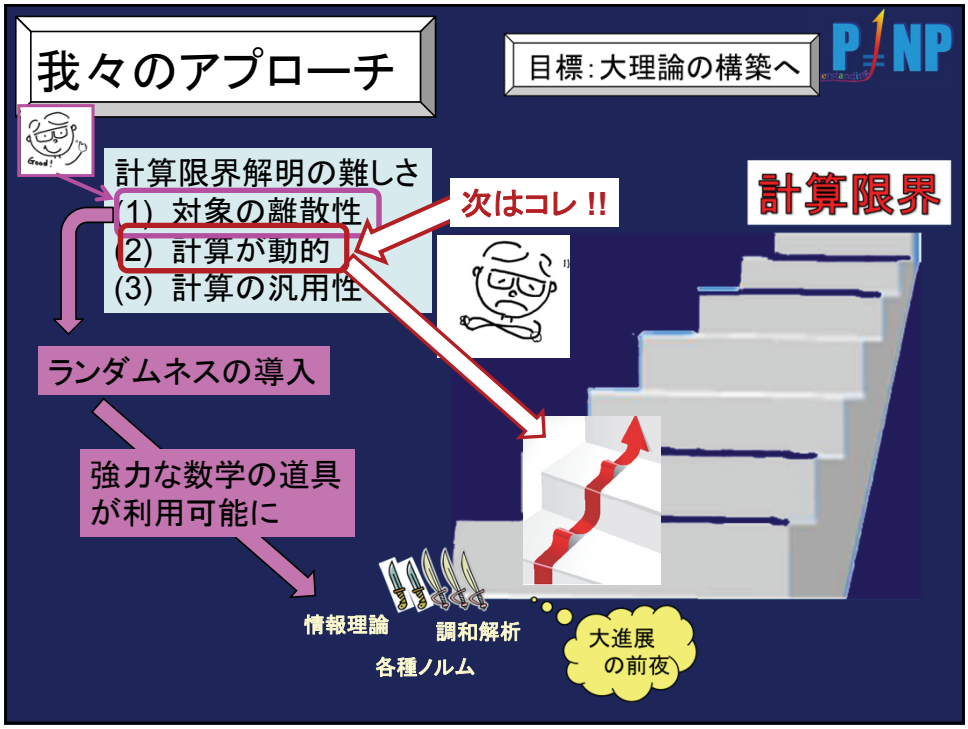
我々のアプローチ

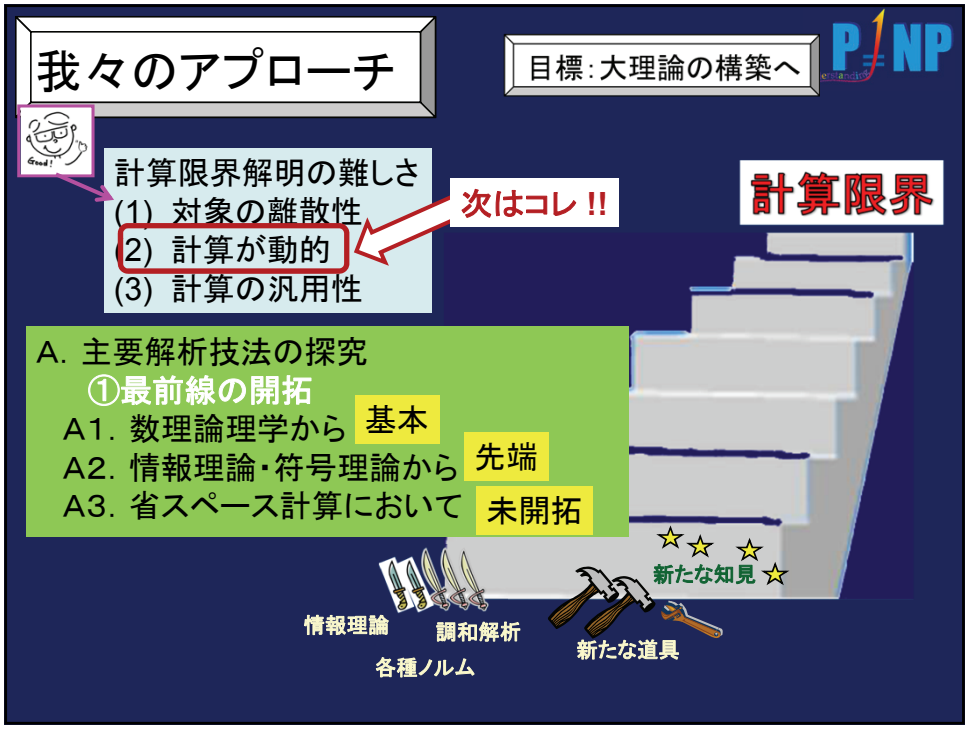
多面的アプローチの統合

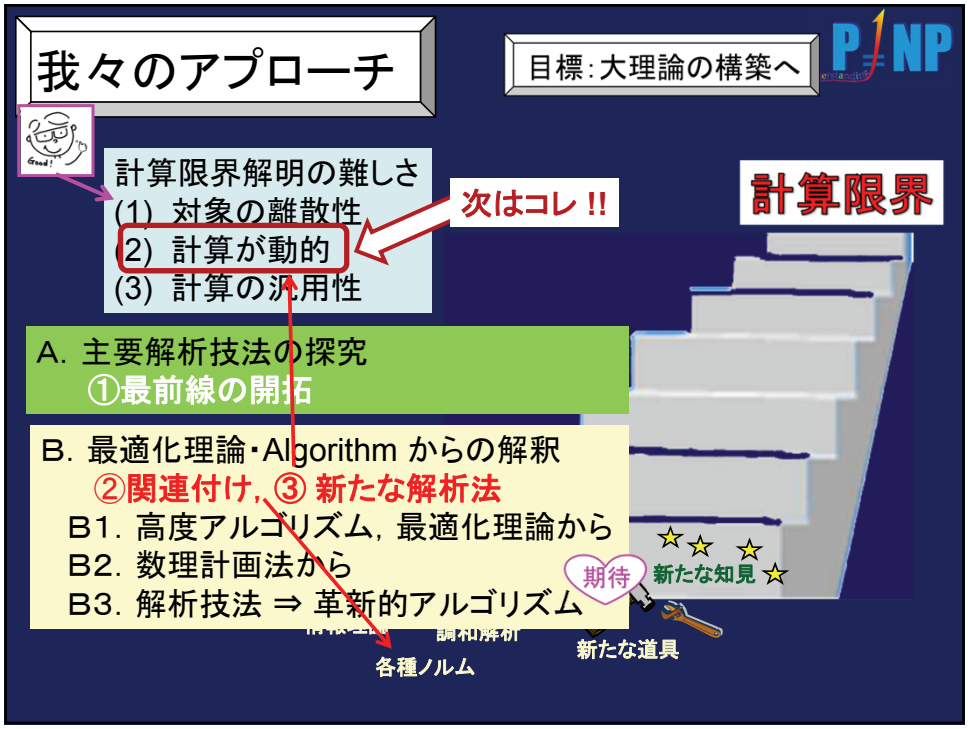
A. 主要解析技法の探究：さらに極める
- A1. 数理論理学から　牧野，河村，垣村，小林，ロスマン
- A2. 情報・符号理論から　河原林，伊藤，玉置，吉田
- A3. 領域限定計算の解析　浅野，垂井，上原，清美，小野

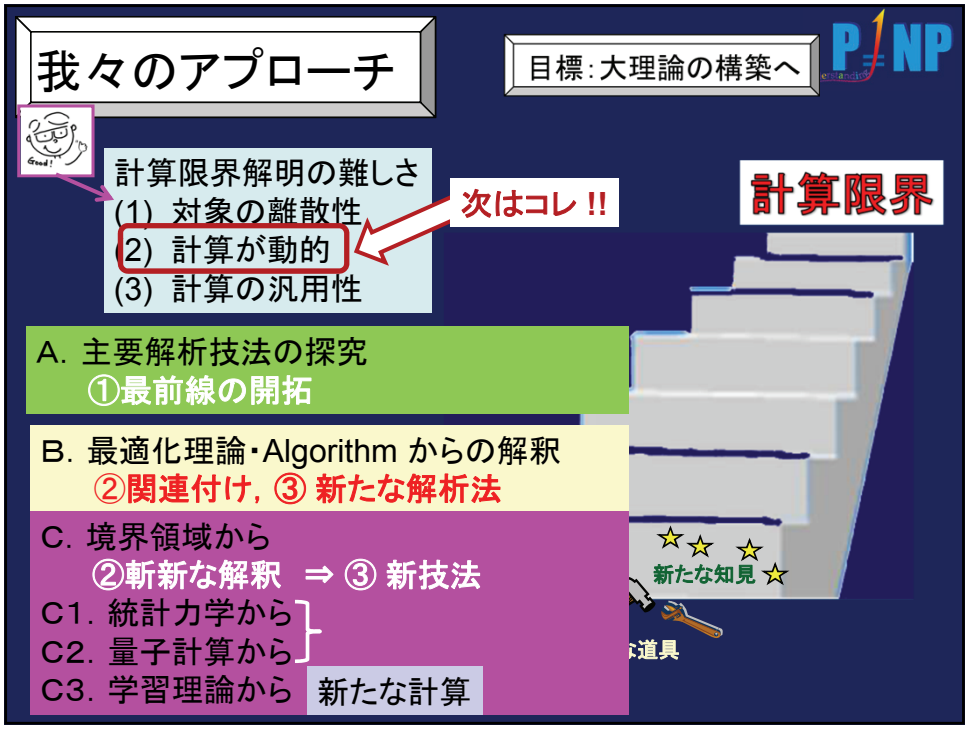
B. 上界からの解釈：新技法の開拓
- B1. 最適化理論から　加藤，神山，岩田，岡本，来嶋
- B2. 数理計画法から　エイビス，天野，上野
- B3. 解析技法 ⇒高速算法　徳山，堀山，渋谷，宇野

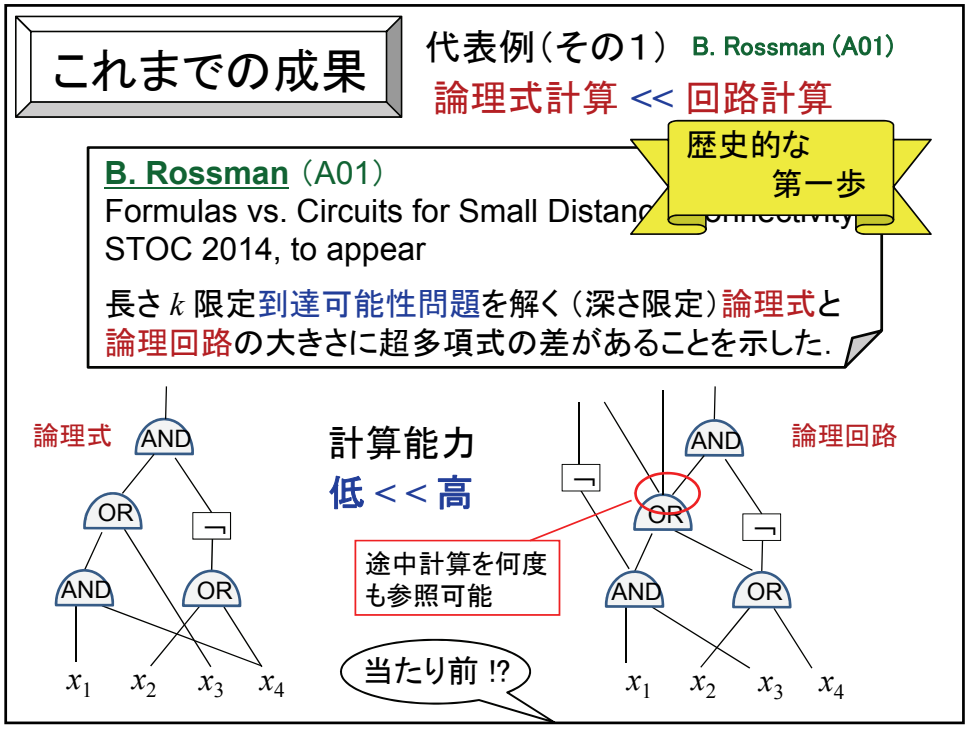
C. 境界領域から：　新解釈・新技法の導入
- C1. 統計力学から　渡辺，小柴，安藤，伊東，山本
- C2. 量子計算から　山下，西村，河内，ルガル，中西
- C3. 学習理論から　瀧本，内沢，畑埜，正代，篠原

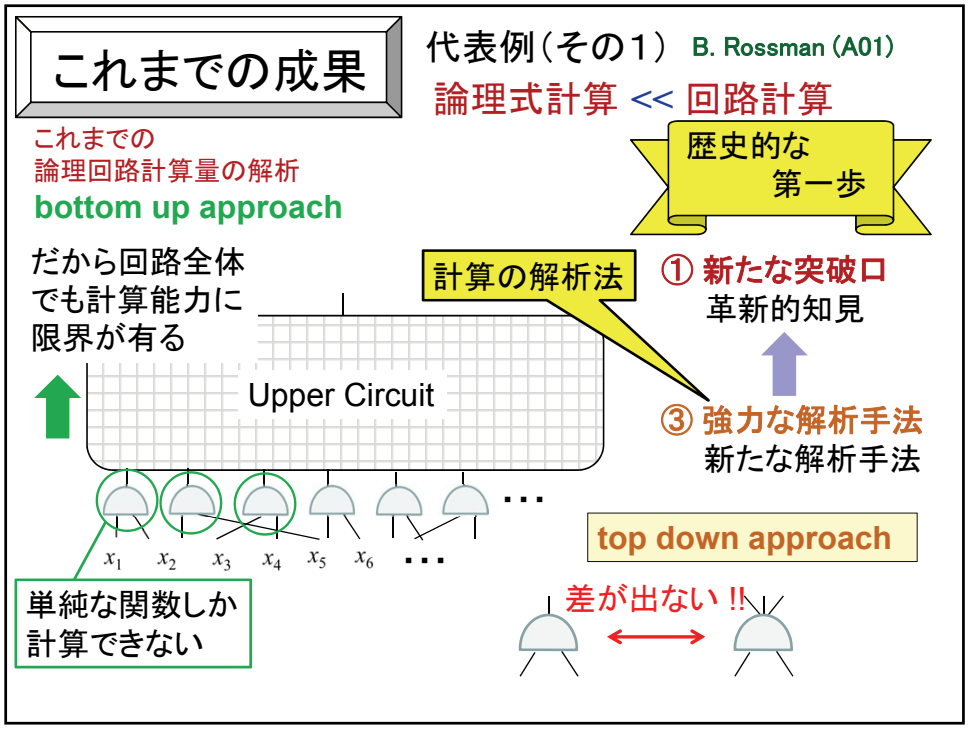

我々のアプローチ
目標：大理論の構築へ
PJNP
計算限界解明の難しさ
(1) 対象の離散性
(2) 計算が動的
(3) 計算の汎用性
次はコレ !!
計算限界
ランダムネスの導入
強力な数学の道具
が利用可能に
情報理論
調和解析
各種ノルム
大進展
の前夜


我々のアプローチ
目標：大理論の構築へ
PJNP
計算限界解明の難しさ
(1) 対象の離散性
(2) 計算が動的
(3) 計算の汎用性
次はコレ !!
計算限界
A. 主要解析技法の探究
①最前線の開拓
A1. 数理論理学から 基本
A2. 情報理論・符号理論から 先端
A3. 省スペース計算において 未開拓
新たな知見
情報理論
調和解析
各種ノルム
新たな道具


我々のアプローチ
目標：大理論の構築へ
P ≠ NP
計算限界解明の難しさ
(1) 対象の離散性
(2) 計算が動的
(3) 計算の汎用性
次はコレ !!
計算限界
A. 主要解析技法の探究
①最前線の開拓
B. 最適化理論・Algorithm からの解釈
②関連付け, ③ 新たな解析法
B1. 高度アルゴリズム, 最適化理論から
B2. 数理計画法から
B3. 解析技法 ⇒ 革新的アルゴリズム
期待
新たな知見
新たな道具
各種ノルム


我々のアプローチ
目標：大理論の構築へ
P ≠ NP
計算限界解明の難しさ
(1) 対象の離散性
(2) 計算が動的
(3) 計算の汎用性
次はコレ !!
計算限界
A. 主要解析技法の探究
①最前線の開拓
B. 最適化理論・Algorithm からの解釈
②関連付け, ③ 新たな解析法
C. 境界領域から
②斬新な解釈 ⇒ ③ 新技法
C1. 統計力学から
C2. 量子計算から
C3. 学習理論から
新たな計算
新たな知見


これまでの成果
代表例（その１） B. Rossman (A01)
論理式計算 << 回路計算
歴史的な
第一歩
B. Rossman（A01）
Formulas vs. Circuits for Small Distanc
STOC 2014, to appear
長さ k 限定到達可能性問題を解く（深さ限定）論理式と
論理回路の大きさに超多項式の差があることを示した.
論理式
AND
OR
¬
AND
OR
x1 x2 x3 x4
計算能力
低 << 高
途中計算を何度
も参照可能
当たり前 !?
論理回路
AND
¬
OR
AND
OR
x1 x2 x3 x4


これまでの成果
代表例（その１） B. Rossman (A01)
論理式計算 << 回路計算
歴史的な
第一歩
これまでの
論理回路計算量の解析
bottom up approach
だから回路全体
でも計算能力に
限界が有る
計算の解析法
① 新たな突破口
革新的知見
Upper Circuit
③ 強力な解析手法
新たな解析手法
x1 x2 x3 x4 x5 x6
top down approach
単純な関数しか
計算できない
差が出ない !!

これまでの成果

代表例（その2） F. LeGall（C02）

行列乗算 世界最速

新世界記録！

F. LeGall（C02）
Powers of Tensors and Fast Matrix Multiplication
preprint, arXiv:1401.7714, 2014.

行列積の計算の世界最速アルゴリズムの提案

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{22} & \cdots & a_{2n} \\ \vdots & & & & \\ \vdots & & & & \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} & b_{13} & \cdots & b_{1n} \\ b_{21} & b_{22} & b_{22} & \cdots & b_{2n} \\ \vdots & & & & \\ \vdots & & & & \\ b_{n1} & b_{n2} & \cdots & \cdots & b_{nn} \end{pmatrix}$$

$O(n^3) \longrightarrow O(n^{2.3755}) \longrightarrow O(n^{2.3729})$

[Coppersmith-Winograd,1987] [LeGall 2014]

これまでの成果

代表例（その2） F. LeGall（C02）

行列乗算 世界最速

新世界記録！

F. LeGall（C02）
Powers of Tensors and Fast Matrix Multiplication
preprint, arXiv:1401.7714, 2014.

行列積の計算の世界最速アルゴリズムの提案

LeGall, 西村らの C02 班での研究

異なる視点

Stothers [2010]
V. Williams の解析
指数関数時間

② 意味・関係
量子計算からの解釈

③ 強力な解析手法
新たな解析手法
⇒ スパコン利用も

$O(n^3) \longrightarrow O(n^{2.3755}) \longrightarrow O(n^{2.3729})$

[Coppersmith-Winograd,1987] [LeGall 2014]

これまでの成果

代表例（その z）

期待

革新的アルゴリズムの素 ??

吉田（A02）

A characterization of locally testable affine
propertiesvia decomposition theorem
STOC 2014, to appear

可能・不可能の確定

アフィン変換に関して閉じた関数の性質の中で
定数時間で検査可能な性質の特徴付け.

計算の理解

より基本的な側面を
より深く理解できる
ようになったか？

常識を覆すアルゴリズム
高度な誤り訂正符号

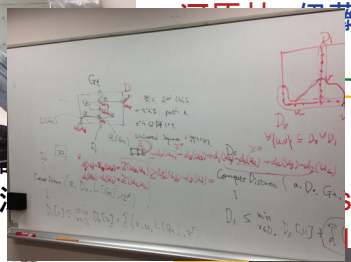
② 意味・関係
手法の理解・新たな解釈

③ 強力な解析手法
新たな解析手法

B3. 解析技法
⇒ アルゴリズム

これまでの成果

領域横断研究



ELC 計算量理論秋学校

ELC チュートリアル

ELC 暗号理論学校

サイエンスカフェ

ELC Seminars

≧ 50

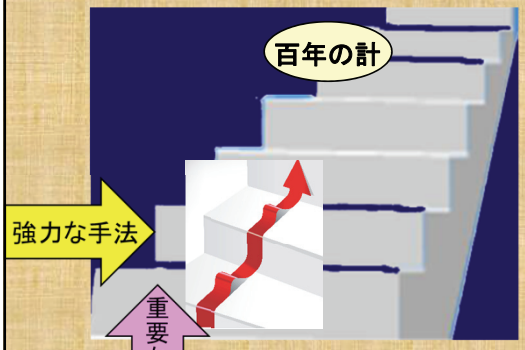
学生自主ゼミ@田町

ELC Tokyo Complexity Workshop

今後の計画

情報処理技術への展開

目　標	意　義
P≠NP予想をはじめとする計算の効率限界の謎解明への新たな道筋の構築	計算の理解の深化 ➡ 革新的アルゴリズム ➡ 斬新な計算利用法



波及活動

理論 ⇒ アルゴリズム

B03 アルゴリズム開発

C03 学習理論

関連プロジェクトとの連携

・河原林 ERATO

・岡田新学術領域