コンプ研＠法政大学

2012.9.3

新学術領域

多面的アプローチの統合による計算限界の解明

東京工業大学
情報理工学研究科
渡辺　治

内容　Ⅰ ヒヤリングより
- 目標と背景
- 研究体制

Ⅱ 目指すもの

多面的アプローチの統合による計算限界の解明

東京工業大学　情報理工学研究科
渡辺　治

東北大学　徳山　豪
東京大学　牧野　和久

内容
- Ⅰ　研究の意義
- Ⅱ　目標と背景
- Ⅲ　研究戦略
- Ⅳ　研究体制
- Ⅴ　まとめ

Ⅰ 研究の意義

大目標

P≠NP予想

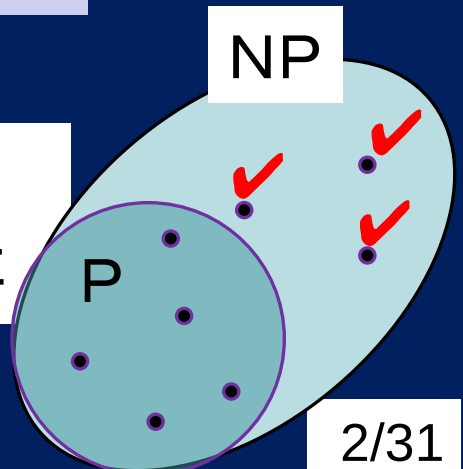
情報の処理に関する
最も基本的問題

コンピュータ出現時からの
未解決問題

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

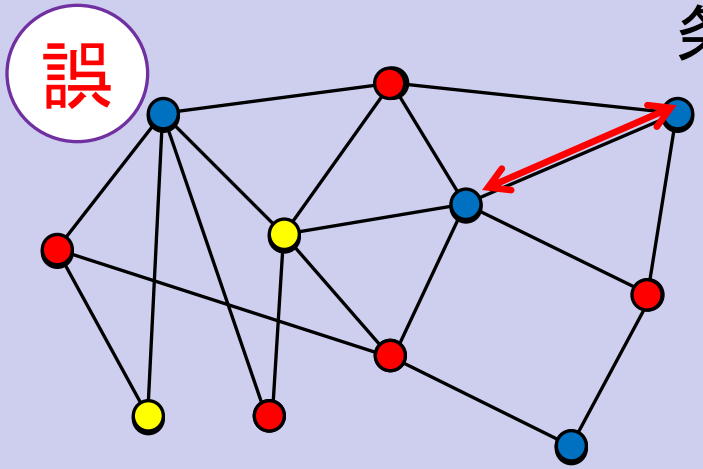


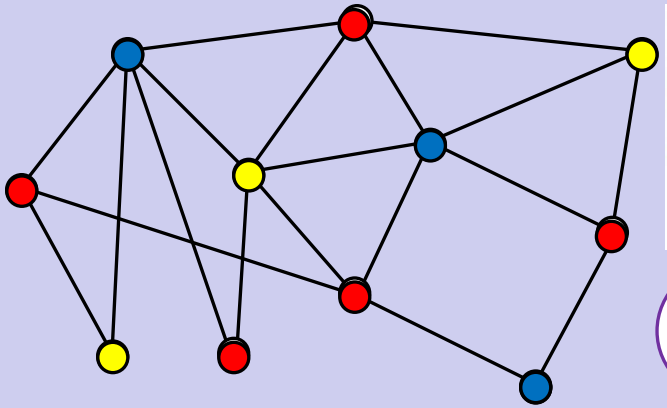
P ≠ NP 予想とは

例: 三彩色問題

「与えられたグラフの頂点を三色で塗り分けよ」

条件：全ての辺の両端は異なる色で





失礼！

要するに

発見の方が**検証**より
はるかに難しい

頂点数 n のグラフでは
解の候補（色の塗り方）
は 3^n 通り

↑ 3^{80} = スパコン「京」でも
＞400兆年

組合せ爆発

この計算法しかないのか？!

計算限界の解明

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

ナッシュ均衡計算　最適戦略
最適ポートフォリオ設計
エネルギー最小自触媒作用
ニューラルネットワークの訓練
結晶格子解析（3次元結晶）
復元問題
最適進化系統樹
タンパク質の立体構造

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
最適配置問題
最小距離配線
ロボットの最短移動　ロジスティック最適化
スケジューリング
乗務員スケジューリング
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：

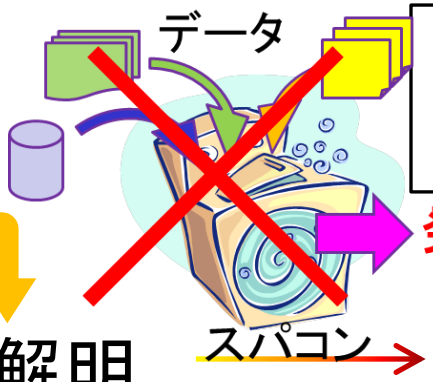
○ これら全部が容易（P）
× これら全部が困難（非 P）

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



全自動**発見**は不可能！

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

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

フィールズ賞	チューリング賞
Tao	Blum
Gowers	Cook
…	Karp
	Yao
	…

Ⅱ 目標と背景

なぜ今？ 何を目指す？

大進展
の前夜

P≠NP

計算限界の解析技法が今
究極まで研ぎ澄まされてきた

2000 ～　　出現：1985 ～ 95

小爆発

deepen

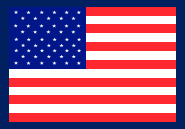
数理論理学から ← Model 理論，証明論

代数・情報理論から ← 戸田理論，PCP 理論

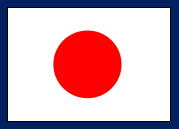
限定型計算←離散数学 ← AC0，単調計算

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



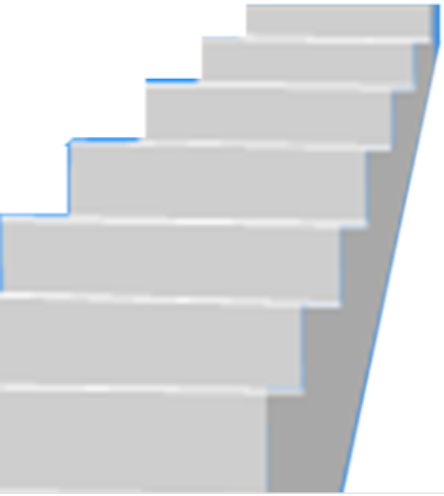
Ⅱ 目標と背景

なぜ今？ 何を目指す？

大進展の前夜

大進展を巻き起す「指導原理」

P≠NP



限界の解析技法が今
究極まで研ぎ澄まされてきた

解決への道筋を示す指導原理

＝

P≠NP理論

百年の計

例えば

フェルマの定理

類体論 ⇧

岩澤理論

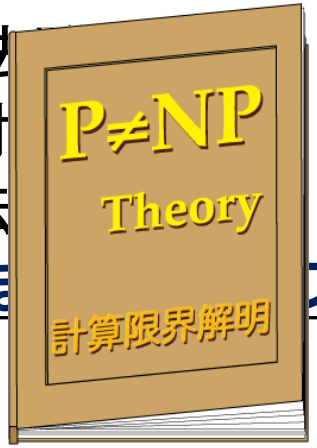
解析技法

・意味付 け

・適用法

体系化

⇒ 解決 プログラム



目標

派生新分野

・解の特質の利用技術
Semantic Coding
Ultra Compression

・情報の価値の科学
＝ 計算情報理論

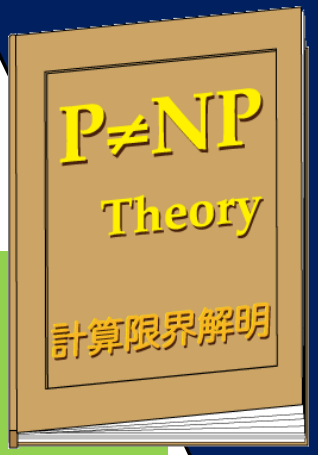
Ⅲ 研究戦略

P≠NP

現状

計算限界の解析技法の多くが究極まで研ぎ澄まされた.

しかし，まだ先が見えない

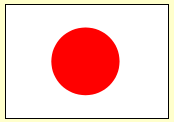


A. 主要解析技法の探究

さらに極める ⇒ 最前線の開拓

- A1. 数理論理学からの解析
- A2. 情報理論・符号理論からの解析
- A3. 省スペース計算，限定計算の解析

B. 上界からの解析技法



新たな解析技法の開拓

- B1. 最適化理論から
- B2. 数理計画法・大規模計算から
- B3. 解析技法 ⇒ 革新的アルゴリズム

C. 境界領域から

新解釈・新技法の導入

- C1. 統計力学から
- C2. 量子計算から
- C3. 学習理論から

Ⅳ 研究体制

A. 主要解析技法の探究：さらに極める　Rossman

A1. 数理論理学から　牧野，河村，垣村，小林

A2. 情報・符号理論から　河原林，伊藤，玉置，吉田

A3. 限定計算の解析　浅野，垂井，上原，清美，小野

B. 上界からの解析技法：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・大規模計算から　Avis，天野，上野

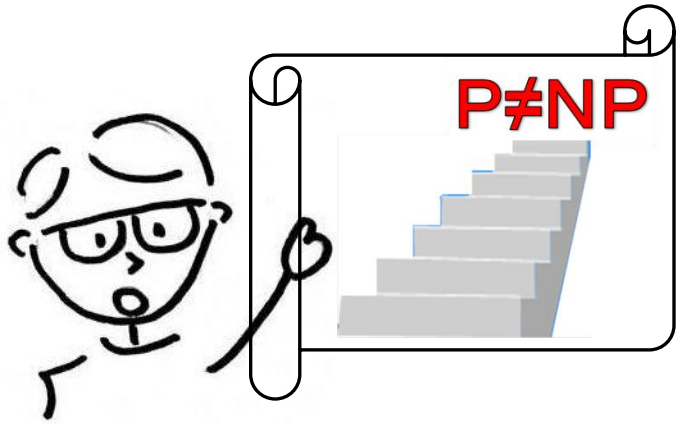
B3. 解析技法 ⇒ アルゴリズム　徳山，堀山，渋谷，宇野

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，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



というようなことを
説明しました. . .

審査員の先生方

で. . .

いいでしょう
やってみなさい！

晴れて
旗揚げです

計算限界解明
ELC

Exploring the
Limits of
Computation

年次計画

東工大 CIC
田町駅前
Center
for ELC

PD, 客員研究員
セミナー

H24 年度

- **計算限界研究センター**設立
- PD 雇用，研究者招聘
- 短期集中チュートリアル　⇒　公募研究へのいざない

▷ A チームを中心とした解析技法の見直し

↑ C チームの立場からの解釈やシナリオの提供

→ 解析技法のアルゴリズム応用への展開（B3 班）

▷ B チームを中心とした新技法の開拓

↑ 既存の技法との関連（A チーム）

☆ 未解決問題の解決例
☆ 各種解析技法の
- 使用レシピ
- 特徴分析レシピ

H25 年度以降

- 公募研究募集・審査 H25, H27
- 各種国際ワークショップの開催
- IEEE CCC（この分野のトップ会議）の開催

以上が発足までの経緯でした

新学術領域

多面的アプローチの統合による
計算限界の解明

第二部

計算限界解明　ELC
何をめざすか？

世界最強の
アルゴリズム軍団

本日のメッセージ

☆ 計算限界解明をやってみませんか？

変なアルゴリズムの構築

☆ 目標：あらたなステップを踏み出すこと

うまいストーリーを作り出そう !!

1. 研ぎ澄まされた解析技法

現状

- 様々な解析技法 1980 ～
- それらが究極まで研ぎ澄まされてきている

⇔ 限界 !?

例）Derandamization

ランダムネスは計算の効率化に本質的か？

P = BPP 予想と，その解明への道のり

- Shamir, Blum, Micali p.r.g. の導入
- Nisan-Wigderson の p.r.g
- hard core predicate の発見 Goldreich-Levin
- worst-case ⇒ average-case hardness

そして ….

1. 研ぎ澄まされた解析技法

例）Derandamization

P = BPP 予想

定理. [Impagliazzo-Wigderson (1997)]

$$E \not\subseteq SIZE[\,2^{o(n)}\,] \Rightarrow P = BPP$$

$$\uparrow$$

$$SAT \notin SIZE[\,2^{o(n)}\,]$$

ある意味限界 ***!?***

定理. [Kabanets-Impagliazzo (2002)]

$$P = BPP \Rightarrow \text{either } NEXP \not\subseteq P/poly$$

$$\text{or } Perm \notin AlgP/poly$$

1. 研ぎ澄まされた解析技法

例）Derandamization

P = BPP 予想

定理. [Impagliazzo-Wigderson (1997)]

$$E \not\subseteq SIZE[2^{o(n)}] \Rightarrow P = BPP$$

$$\uparrow$$

$$SAT \not\in SIZE[2^{o(n)}]$$

ある意味限界 ***!?***

定理. [Aydinlioglu-Gutfreund-Hitchcock-Kawachi (2011)]

$$AM \subseteq P(NP) \Rightarrow E(NP) \not\subseteq SIZE[2^{o(n)}]$$

$$\boxed{BPP(NP) \subseteq P(NP)}$$

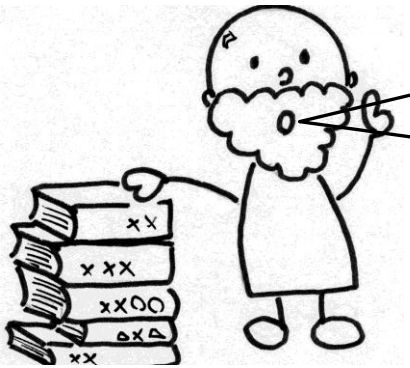
1. 研ぎ澄まされた解析技法

現状

- 様々な解析技法 1980 ～
- それらが究極まで研ぎ澄まされてきている

⇔ 限界 !?

行き詰り



諦めるのは
早すぎる !!

M. Agrawal

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！

PRIME is in P [2004]
P-Isomorphism Conjecture w.r.t. uniform AC0-red [2001]

2. 目指すところ: 今がチャンス

現状

- 様々な解析技法 1980 ～
- それらが究極まで研ぎ澄まされてきている

まだまだ使いきれていない

使いこなすには良いアルゴリズムが必要

例）ACC0 の計算限界 ← 30 年級未解決問題

定理. [Williams (2011)]

$$\mathrm{NEXP} \not\subseteq \mathrm{ACC0}$$

※ poly. size ACC0

2. 目指すところ: 今がチャンス

使いこなすには良いアルゴリズムが必要

定理. [Williams (2011)]

$$\mathrm{NEXP} \not\subseteq \mathrm{ACC0}$$

証明の鍵となったのは次のアルゴリズム

与えられた変数毎線形, |ai| < s, 項数 < 2^n

P(x1,…,xn) = a1･x1･x3 + a2･x2･x5･x8 + ….

に対し, その 2^n 個通りの入力に対する値を求める

多項式全入力評価
高速アルゴリズム

これを 2^n × poly(n, log s) 時間で行う

2. 目指すところ: 今がチャンス

NEXP ⊆ ACC0 ⇒ NTIME[2^n] ⊆ NTIME[2^n/n] 矛盾

補題0. NTIME[2^n] → SUCCINCT-SAT

補題1. NEXP ⊆ ACC0 ⊆ P/poly [IKW02]
⇒ SUCCINCT-SAT が「圧縮版証拠」を持つ

補題2. ⇒ NTIME[2^n] → 2^{o(n)}-size ACC0 版-SAT

補題3. ACC0 は変数毎線形多項式＋で計算できる
[Y-Tarui-B91]

補題4. ⇒ 2^{o(n)}-size ACC0 版-SAT の充足可能性は
2^n/n 時間でチェックできる

多項式全入力評価
高速アルゴリズム

2. 目指すところ: 今がチャンス

使いこなすには良いアルゴリズムが必要

うまい使い場所を見つけることが必須

計算複雑さ博物学

Complexity Zoo

A A0PP - AC - AC0 - AC0[m] - AC1 - ACC0 - AH - AL - ALL - ALOGTIME - AlgP/poly - Almost-NP - Almost-P - Almost-PSPACE - AM - AMEXP - AM ∩ coAM - AM[polylog] - AmpMP - AmpP-BQP - AP - APP - APX - ATIME - AUC-SPACE(f(n)) - AuxPDA - AVBPP - AvgE - AvgP - AW[P] - AWPP - AW[SAT] - AW[*] - AW[t] - AxP - AxPP

B βP - BH - BPd(P) - BPE - BPEE - BPHSPACE(f(n)) - BPKT - BPP//log - BPP/rlog - BPP-OBDD - BPPpath - BPQP - BPSPACE(f(n)) - BQP/log - BQP/mpoly - BQP/qlog - BQP/qpoly - BQP-OBDD - BPP(f(n)) - k-BPP

C C=AC0 - C=L - C=P - CC - CC0 - CFL - CLOG - CP - cofrIP - coMA - coModkP - compIP - compNP - coNE - coNEXP - coNL - coNP - coNPcc - coSL - coSPARSE - coUCC - coUP - CP - CSIZE(f(n)) - CSL - CSP - CZK

D D#P - DCFL - Δ2P - δ-BPP - δ-RP - DET - DiffAC - DTIME(f(n)) - DTISP(t(n),s(n)) - Dyn-FO - Dyn-ThC0

E E - EE - EEE - EESPACE - EEXP - EH - ELEMENT - EQPK - EQTIME(f(n)) - ESPACE - ∃BPP - ∃NISZK - EXP - EXP/poly - EXPSPACE

F FBQP - Few - FewEXP - FewP - FH - FIXP - FNL - FO(PFP) - FO(TC) - FO(t(n)) - FOLL - FP - FPNP[log] - FPR - FPRAS - FPT - FPTnu - FPTsu - FP(n))

G GA - GAN-SPACE(f(n)) - GapAC0 - GapL - GapP(n)) - G[t]

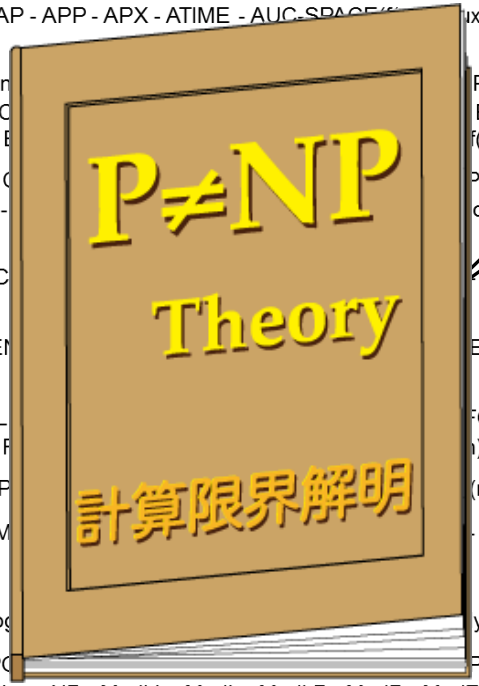
H HalfP - HeurBPP - HeurBPTIME(f(n)) - HeurDTIME - HkP - HVSZK

I IC[log,poly] - IP - IPP - IP[polylog]

L L - LC0 - LH - LIN - LkP - LOGCFL - LogFew - LogNP - LWPP

M MA - MA' - MAC0 - MAE - MAEXP - mAL - MAPCP0 - mcoNL - MinPB - MIP - MIP*[2,1] - MIPEXP - (Mk)P - mL - MM - MMSNP - mNC1 - mNL - mNP - ModkL - ModL - ModkP - ModP - ModZkL - mP - MP - MPC - mP/poly - mTC0

N NAuxPDAp - NC - NC0 - NC1 - NC2 - NE - NE/poly - Nearly-P - NEE - NEEE - NEEXP - NEXP - NEXP/poly - NIPZK - NIQSZK - NISZK - NISZKh - NL - NL/poly - NLIN - NLOG - NONE - NNC(f(n)) - NP - NPC - NPC - NPcc - NPkcc - NPI - NP ∩ coNP - (NP ∩ coNP)/poly - NP/log -



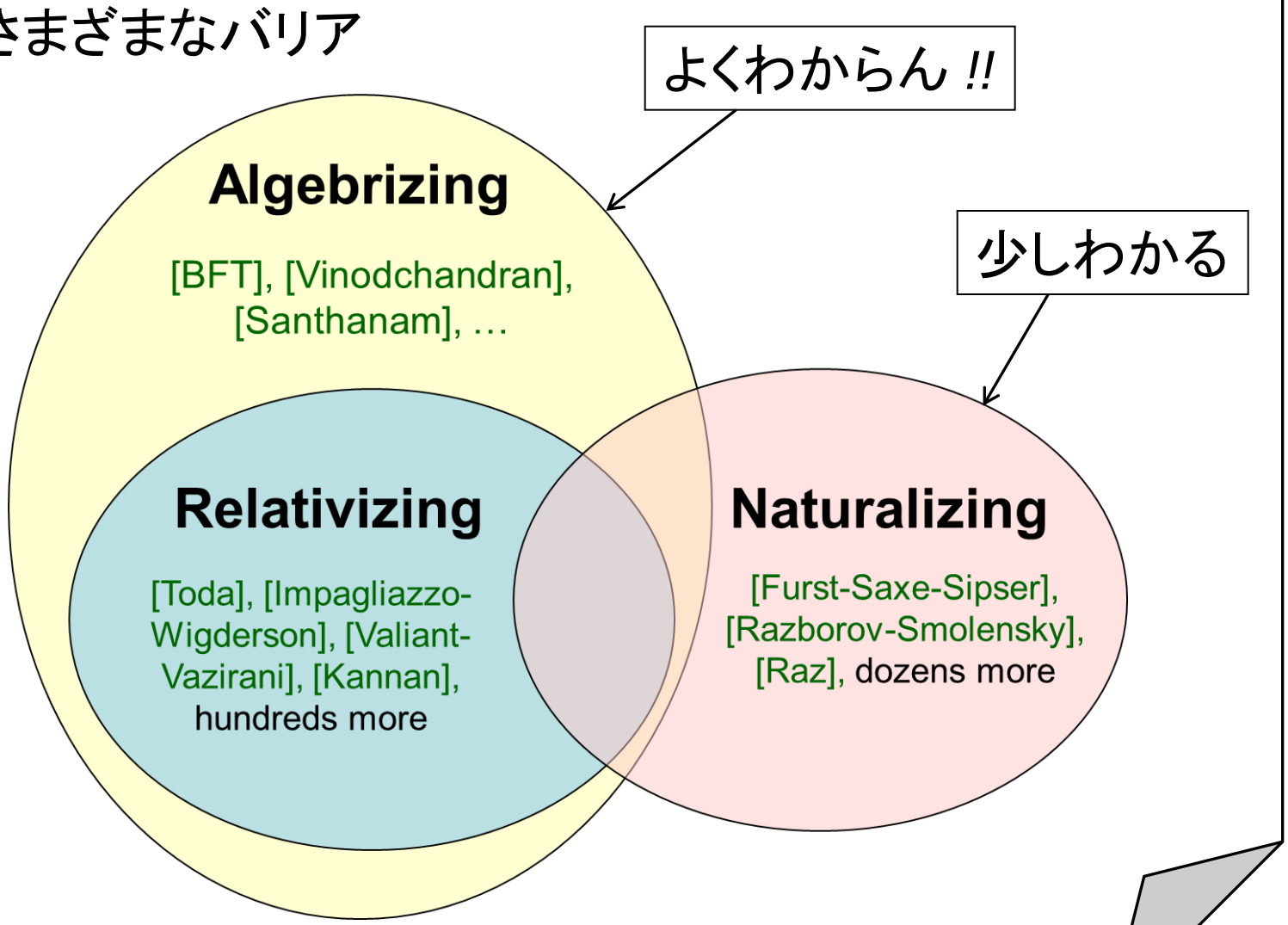
レシピ

L. Fortnow
wizard

皆の力で

2. 目指すところ: 障壁の理解

例）さまざまなバリア



[Aaronson の講演スライドより]

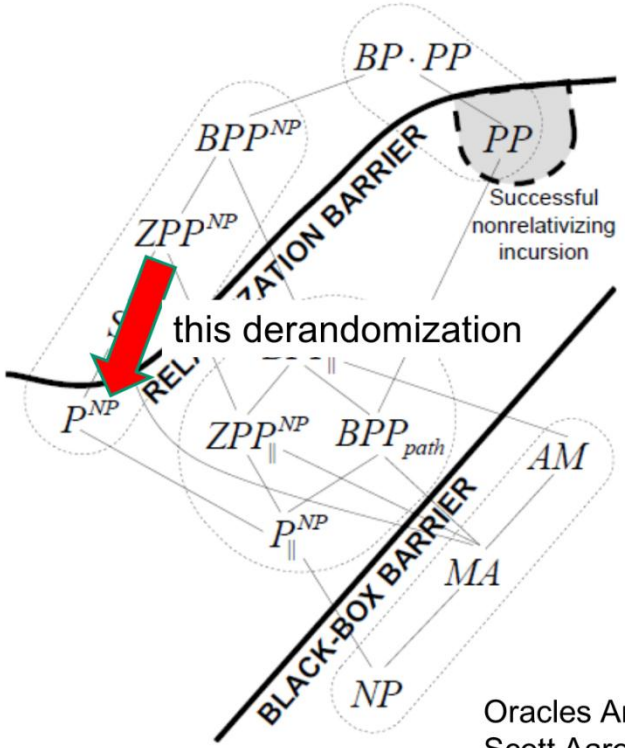
3. 目標とする技術課題

単に渡辺の好み

(1) algorithmic approach
to nonlinear size circuit lower bounds

- 非線形下界を持つ計算問題をアルゴリズム的に構成する手法
- 計算論的学習理論の技法の応用
- relativization barrier

なぜなの ??



Oracles Are Subtle But Not Maliciou
Scott Aaronson, ECCC 2005

- 近似数え上げ approximate counting が must か？

3. 目標とする技術課題

単に渡辺の好み

(2) use comp. power for exploring lower bounds

・計算問題を解くことで下界を解析する

なぜ？

有限の問題に落とし込むことが可能な場合がある

[天野さんの EATCS 解説記事]

例）ビット毎内積の
限定版 depth2 threshold circuits による計算

定理. $\mathrm{size}(\mathrm{IP}_n) \geqq \mathrm{size}(\mathrm{IP}_{n-4}) \times$ ▨

ここを計算する

3. 目標とする技術課題

単に渡辺の好み

(3) search for good target hard problems

- 目標として適切な問題を探り出す
- NP-完全問題ならばよい，という訳ではない
- 平均時で難しい問題，分布を探り出す
  なぜ，その分布で難しいのか？
  例）3SAT の phase transition threshold
- Unique Game Conjecture でいいのか？

3. 目標とする技術課題

単に渡辺の好み

(4) more techniques!

- 情報理論的な解析手法をうまく生かす

  例）communication complexity
  sublinear time algorithm

- 量子計算の論法，解析手法
- 代数幾何，表現論，．．．！？

4. さらにマニアックに ;-)

Relativization Barrier とは何なのか？

定理. [Baker-Gill-Solvay]

$P(X) = NP(X)$ となるオラクル X
$P(Y) \neq NP(Y)$ となるオラクル Y

⇒ 相対化できるような論法では $P \neq NP$ は示せない

だからどうなの？
何がバリアなの？

通常の algorithm 的手法の限界

generic algorithm framework

4. さらにマニアックに ;-)

generic algorithm

肝となるところを blackbox にした計算で，どんな blackbox でもうまく働くアルゴリズム

通常の algorithm 的手法の限界

generic algorithm framework

witness finding problem

= a problem of computing a witness of a given NP problem instance x , that is, w such that witness of $R(x, w)$ holds

generic witness finding problem

= a problem of computing a witness w such that $R(w)$ holds for a given R as a blackbox function

Theorem of [BenDavid et al. 1997] :

$\exists$ $\mathrm{BPP}_{\|}^{\mathrm{NP}(\cdot)}$-machine that solves the witness finding problem by $O(n^2)$ queries

$\Uparrow$ 最適性

Theorem: [Kawachi-Rossman-Watanabe]

No $\mathrm{BPP}_{\|}^{\mathrm{NP}(\cdot)}$- machine exists that solves the generic witness finding problem with $o(n^2)$ queries (to its NP-machine)

4. さらにマニアックに ;-)

generic algorithm

通常の algorithm 的手法の限界

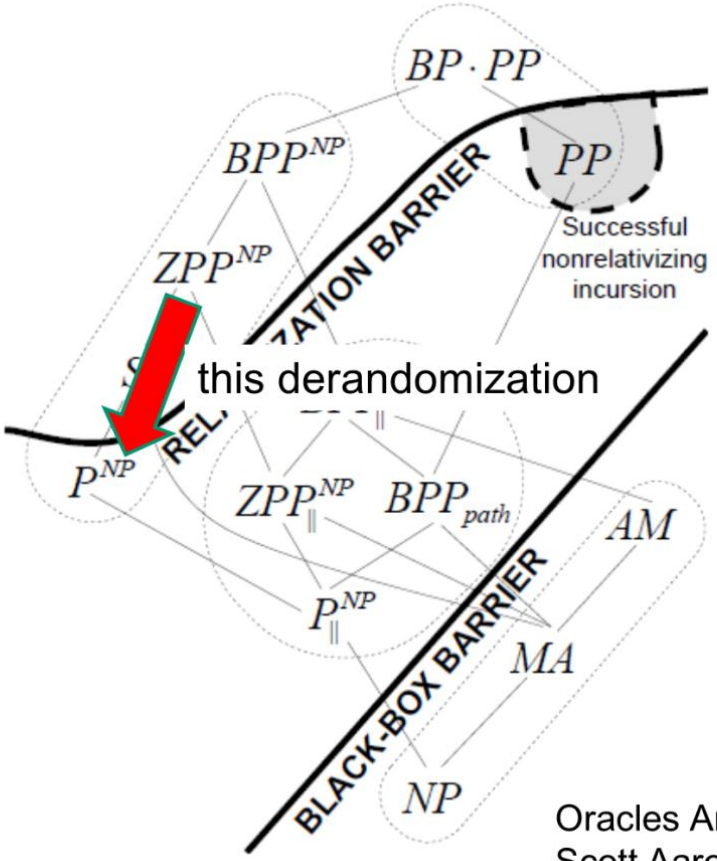
generic algorithm framework

肝となるところを blackbox にした計算で，どんな blackbox でもうまく働くアルゴリズム

非線形回路下界を持つ問題の設計

回路 Interprer I を blackbox とする

relativization barrier の重要な側面



Oracles Are Subtle But Not Malicious
Scott Aaronson, ECCC 2005

新学術領域

多面的アプローチの統合による計算限界の解明

計算限界解明　ELC
何をめざすか？

世界最強の
アルゴリズム軍団

本日のメッセージ

☆ 計算限界解明をやってみませんか？

変なアルゴリズムの構築

☆ 目標：あらたなステップを踏み出すこと

うまいストーリーを作り出そう!!

ありがとうございました