回路最小化問題の平均計算量について (CCC 2017)

平原　秀一

東京大学 博士課程2年
ERATO研究協力者

共同研究者： Rahul Santhanam (University of Oxford)

目次

1. 回路最小化問題（MCSP）について
2. 平均計算量とは
3. 自然な証明について
4. MCSPの最悪計算量から平均計算量への帰着について（疑似ランダム自己帰着性）

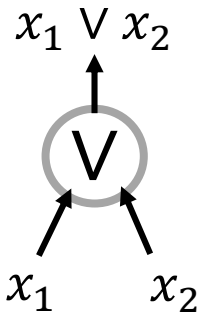
目次

1. 回路最小化問題（MCSP）について
2. 平均計算量とは
3. 自然な証明について
4. MCSPの最悪計算量から平均計算量への帰着について（疑似ランダム自己帰着性）

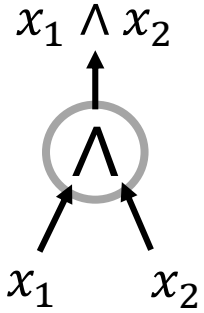
論理回路

- 論理回路は**論理ゲート**を組み合わせて構成される

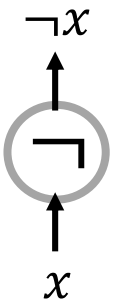
ORゲート



ANDゲート



NOTゲート

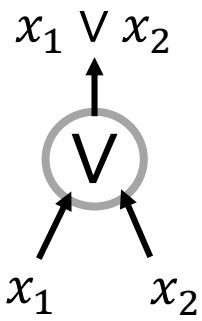


https://en.wikipedia.org/wiki/VLSI_Technology

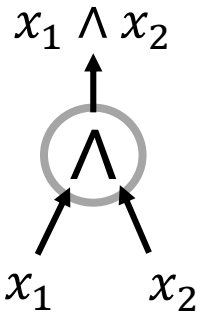
論理回路

- 論理回路は**論理ゲート**を組み合わせて構成される

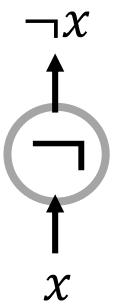
ORゲート



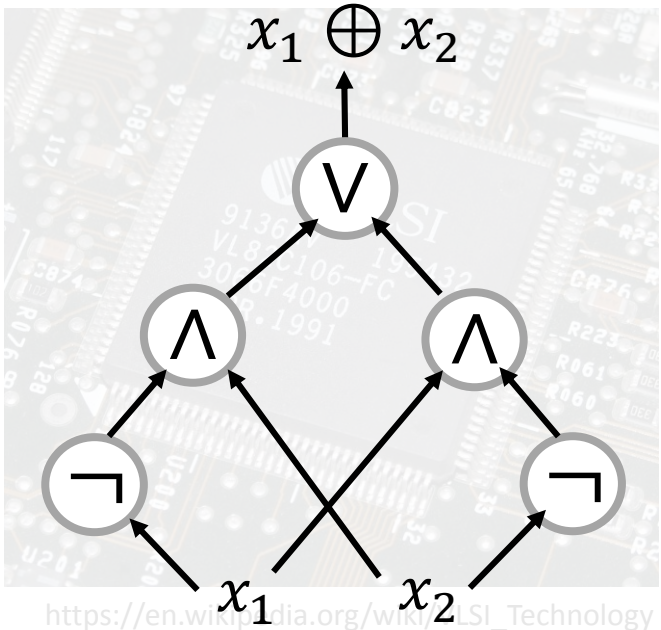
ANDゲート



NOTゲート



例: 2入力XORを計算する回路

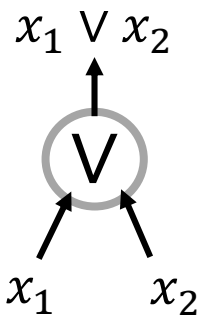


https://en.wikipedia.org/wiki/LSI_Technology

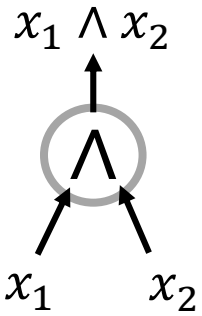
論理回路

- 論理回路は**論理ゲート**を組み合わせて構成される

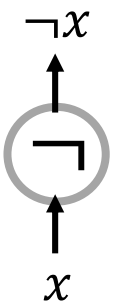
ORゲート



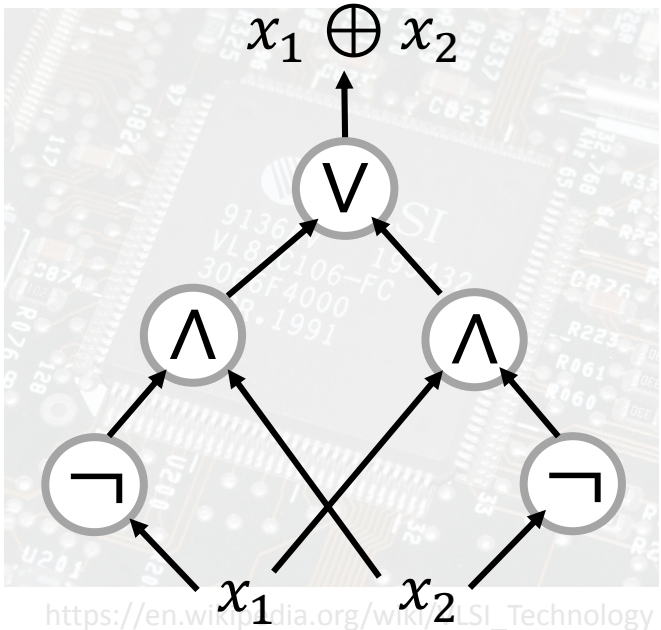
ANDゲート



NOTゲート



例: 2入力XORを計算する回路



https://en.wikipedia.org/wiki/LSI_Technology

- 出来る限り小さいサイズ（ゲート数）の回路を求めたい。
- コンピュータで自動的にそのような回路を求めたい。

回路最小化問題

（Minimum Circuit Size Problem; MCSP）

入力

実現したい関数

$$f:\{0,1\}^n \to \{0,1\}$$

の真理値表と自然数$s \in \mathbb{N}$

（入力例）

$s = 5$

$f =$

x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

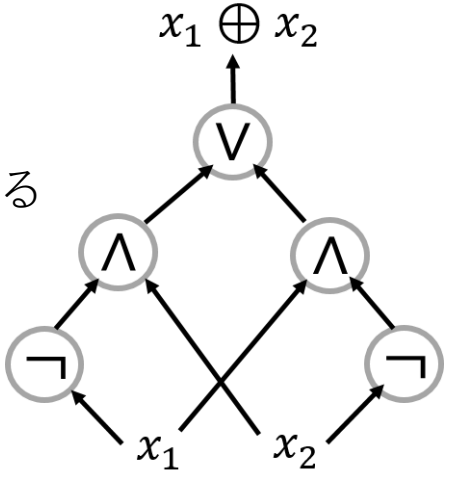
出力

関数fを計算するサイズs以下の回路が存在するか？

（出力）

“YES”

(実際にXORを計算する右図のような回路が存在するので。)



回路最小化問題

（Minimum Circuit Size Problem; MCSP）

入力

実現したい関数

$$f:\{0,1\}^n \to \{0,1\}$$

の真理値表と自然数$s \in \mathbb{N}$

（入力例）

$s = 5$

$f =$

x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

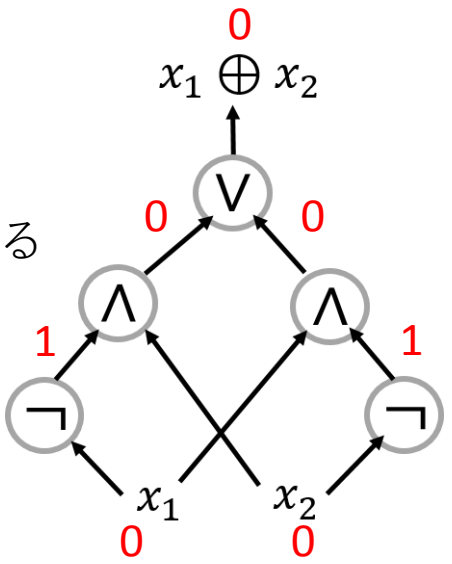
出力

関数fを計算するサイズs以下の回路が存在するか？

（出力）

“YES”

(実際にXORを計算する右図のような回路が存在するので。)



回路最小化問題

（Minimum Circuit Size Problem; MCSP）

入力

実現したい関数

$f: \{0,1\}^n \to \{0,1\}$

の真理値表と自然数$s \in \mathbb{N}$

（入力例）

$s = 5$

$f =$

x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

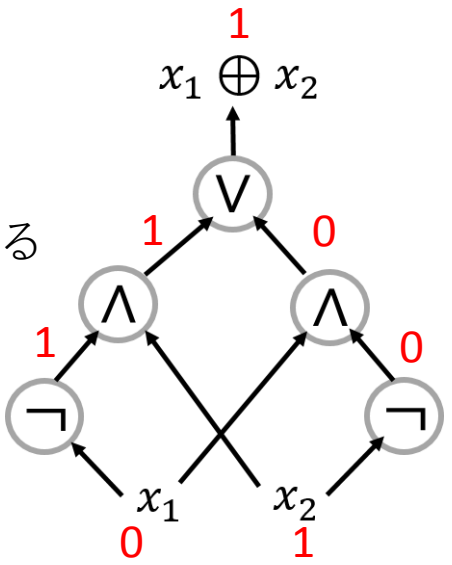
出力

関数fを計算するサイズs以下の回路が存在するか？

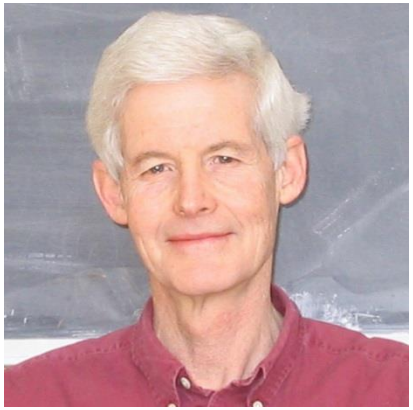
（出力）

“YES”

(実際にXORを計算する右図のような回路が存在するので。)



Cook-Levinの定理 (1970s)



Cook

Levin

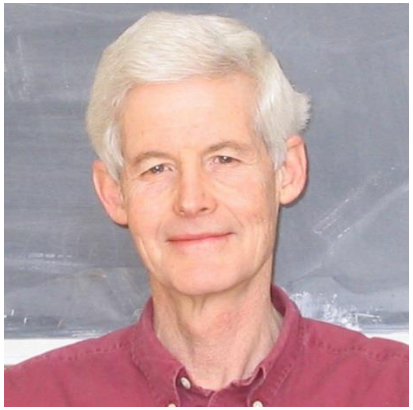
NPの問題の中で
最も難しい。

定理 (Cook-Levin)

充足可能性問題(SAT)は**NP**完全である。

- **P vs NP**問題の発端となった定理

Cook-Levinの定理 (1970s)



Cook

Levin

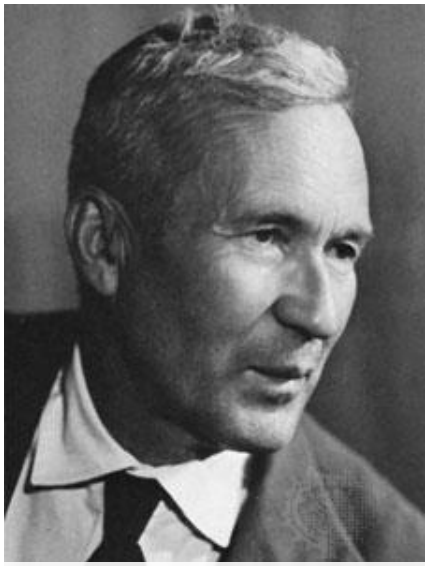
MCSPの計算量
について何かを
言いたいなあ…

定理 (Cook 1971, Levin 1973)

充足可能性問題(SAT)は**NP完全**である。

- **P vs NP**問題の発端となった定理

Cook-Levinの定理 (1970s)



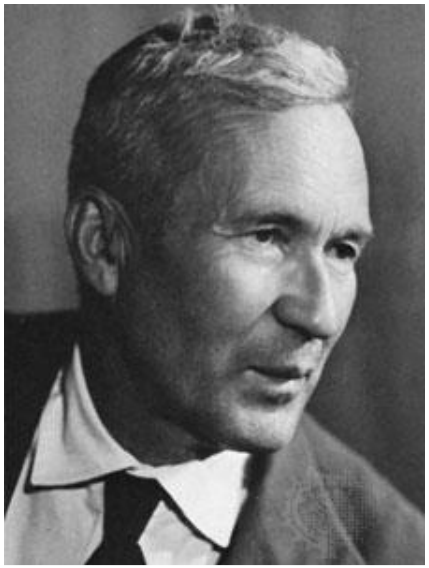
Kolmogorov
(指導教官)

Levin

早く結果を
出版しなさい！

- P vs NP問題の発端となった定理

Cook-Levinの定理 (1970s)



Kolmogorov
(指導教官)

Levin

早く結果を
出版しなさい！

わかりました。
でも2ページだけ
の論文で！

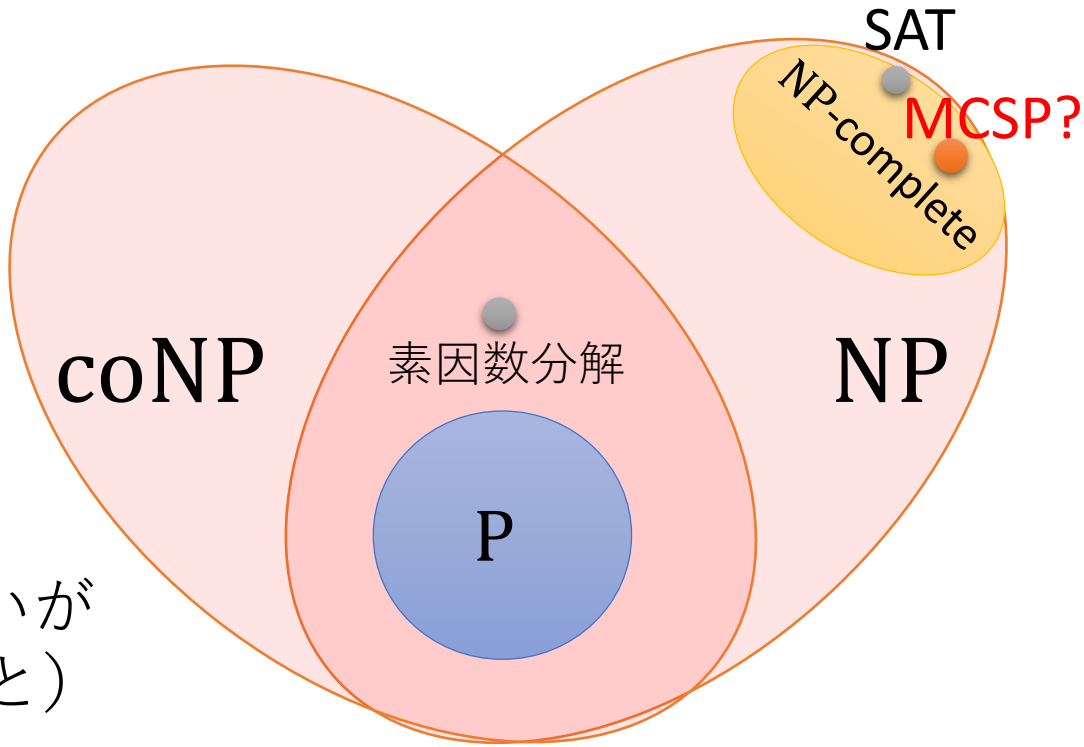
- P vs NP問題の発端となった定理

重要な未解決問題

MCSPは**NP**完全か？

- **NP**完全だと予想
  している人もいるし、

- **NP**の中間の問題だと
  予想している人もいる。
  （多項式時間では解けないが
NP完全でもない問題のこと）

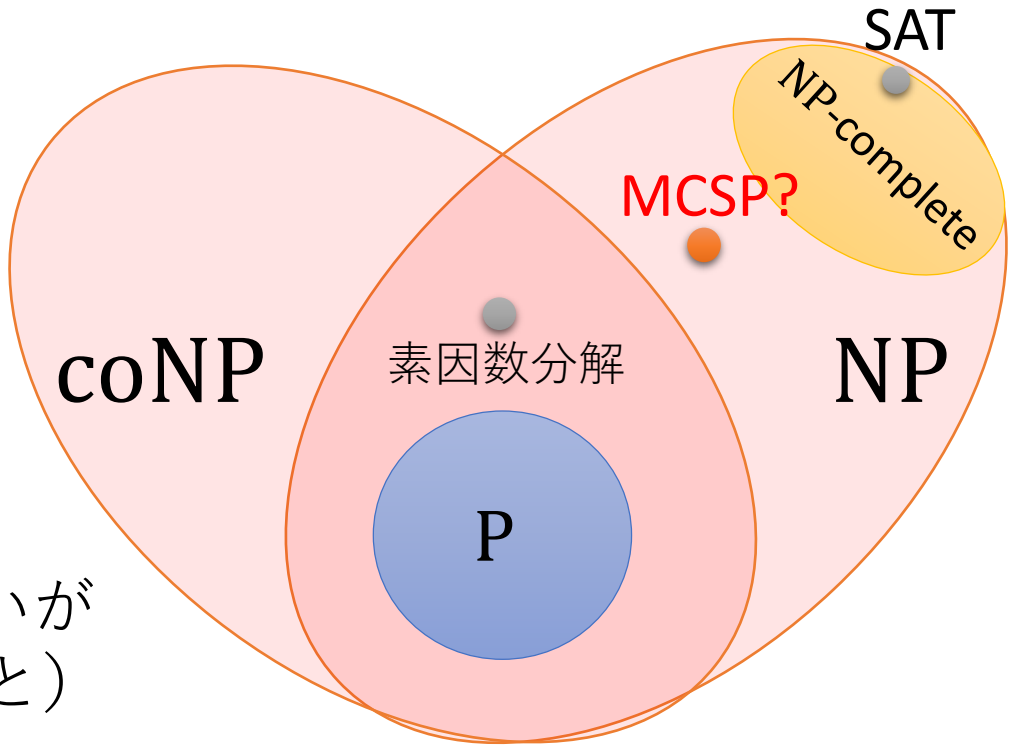


重要な未解決問題

MCSPは**NP**完全か？

- **NP**完全だと予想
  している人もいるし、

- **NP**の中間の問題だと
  予想している人もいる。
  （多項式時間では解けないが
NP完全でもない問題のこと）

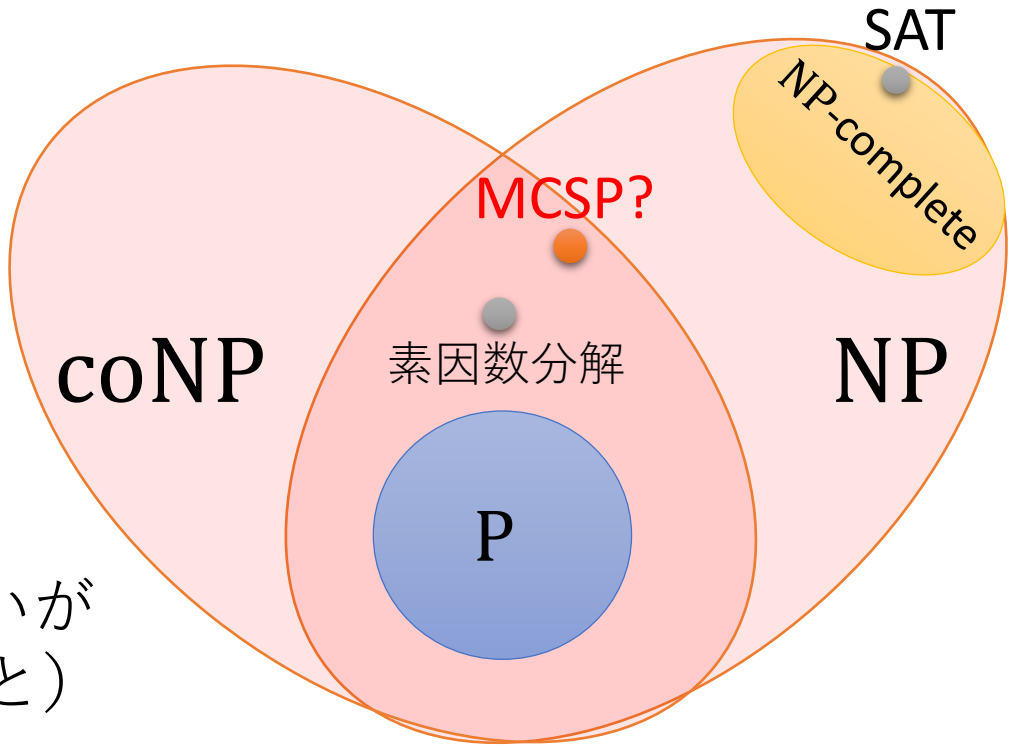


重要な未解決問題

MCSPは**NP**完全か？

- **NP**完全だと予想
  している人もいるし、

- **NP**の中間の問題だと
  予想している人もいる。
  （多項式時間では解けないが
  NP完全でもない問題のこと）



目次

1. 回路最小化問題（MCSP）について
2. 平均計算量とは
3. 自然な証明について
4. MCSPの最悪計算量から平均計算量への帰着について（疑似ランダム自己帰着性）

平均計算量とは

- 最悪計算量：

  アルゴリズムが最も悪く振る舞うような
  入力における計算量のこと。

- 平均計算量：

  入力がある分布から生成されているとしたときに、
  高い確率で正しく計算するアルゴリズムの計算量。
  （アルゴリズム自体は決定性でもよい）

例：Random 3SAT [Feige 2002]

- 3SATの平均計算量版
- 3CNF式の各節が一様ランダムに生成される。
  - 変数の数はn、節の数は$O(n)$。

$$\varphi = (x_1 \vee x_3 \vee \overline{x_4}) \wedge (\overline{x_2} \vee x_3 \vee \overline{x_4}) \wedge (x_1 \vee \overline{x_2} \vee x_4)$$

定義：~~Random~~ 3SATを解くアルゴリズム

~~Random~~ 3SATを解くアルゴリズムとは、
(1) 充足可能なすべての式を受理し、
(2) 充足不能なすべての式を拒否するようなもの。

例：Random 3SAT [Feige 2002]

- 3SATの平均計算量版
- 3CNF式の各節が一様ランダムに生成される。
  - 変数の数はn、節の数は$O(n)$。

$$\varphi = (x_1 \vee x_3 \vee \overline{x_4}) \wedge (\overline{x_2} \vee x_3 \vee \overline{x_4}) \wedge (x_1 \vee \overline{x_2} \vee x_4)$$

定義：Random 3SATを解くアルゴリズム

Random 3SATを解くアルゴリズムとは、
(1) 充足可能なすべての式を受理し、
(2) 充足不能な多くの式（例えば全体のうち50%の式）を拒否するようなもの。

回路最小化問題の平均計算量

- サイズパラメタ$s \in \mathbb{N}$を入力から除く。
- 代わりに、$s: \mathbb{N} \to \mathbb{N}$を事前に決めておき、MCSP[s]を考える。

定義：MCSP[s] (Parameterized version of MCSP)

入力

実現したい関数
$$f: \{0,1\}^n \to \{0,1\}$$
の真理値表（$=2^n$の長さの文字列）
~~と自然数$s \in \mathbb{N}$~~

出力

関数fを計算するサイズ$s(n)$以下の回路が存在するか？

- 入力の分布は$f: \{0,1\}^n \to \{0,1\}$の一様分布を考える。

回路最小化問題の平均計算量

- ただし、YESとなる入力はとても少ないので、ゼロ誤りアルゴリズムを考える。 $(\text{YESインスタンスの数}) = s^{O(s)} \ll (\text{全体のインスタンスの数}) = 2^{2^n}$

定義：ゼロ誤りアルゴリズム

ゼロ誤りアルゴリズムとは、
(1) “1”, “0”, “?”のどれかを出力し、
(2) “?”と出力する割合は全体の50%以下であって、
(3) YESの入力に対しては“1”か“?”と出力し、
(4) NOの入力に対しては“0”か“?”と出力するようなもの。

サイズ$s(n)$以下の回路で計算できない関数

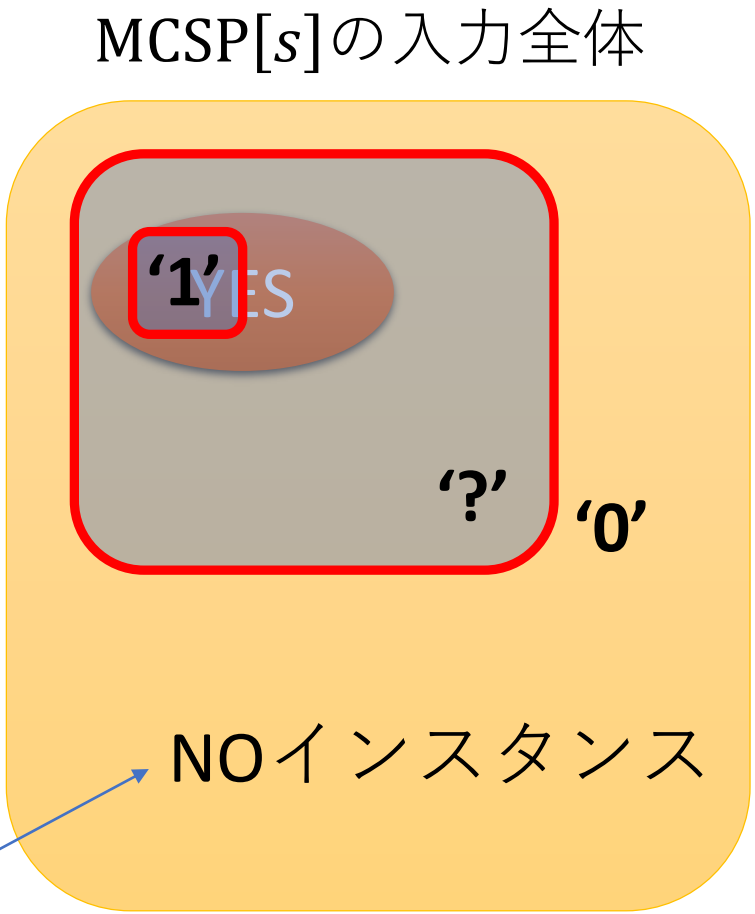
回路最小化問題の平均計算量

- ただし、YESとなる入力はとても少ないので、ゼロ誤りアルゴリズムを考える。 $(\text{YESインスタンスの数}) = s^{O(s)} \ll (\text{全体のインスタンスの数}) = 2^{2^n}$

定義：ゼロ誤りアルゴリズム

ゼロ誤りアルゴリズムとは、

(1) “1”, “0”, “?”のどれかを出力し、
(2) “?”と出力する割合は全体の50%以下であって、
(3) YESの入力に対しては“1”か“?”と出力し、
(4) NOの入力に対しては“0”か“?”と出力するようなもの。



サイズ$s(n)$以下の回路で計算できない関数

回路最小化問題の一種の困難性

- 時間制限付きコルモゴロフ記述量KTの最小化問題。
- 回路の代わりに、Random Access Machineの計算時間＋プログラムの長さを最小化する問題。

定理

$\mathrm{MKTP}[s]$（回路最小化問題MCSPの一種）は Random 3SAT困難。（$\exists s: \mathbb{N} \to \mathbb{N}$）

証明のアイディア：Identity Mapが帰着を与える。

Ryan O'Donnellの予想

Random 3SATは（多項式時間でも）coNPのアルゴリズムでさえ解けない。

➢特に、O'Donnellの予想の下で$\mathrm{MKTP} \notin \mathrm{coNP}$.

目次

1. 回路最小化問題（MCSP）について
2. 平均計算量とは
3. 自然な証明について
4. MCSPの最悪計算量から平均計算量への帰着について（疑似ランダム自己帰着性）

回路下界技法の発展 (1980s)

P ≠ NP に対するアプローチとして回路の表現力の限界を調べる技法が発展してきた。

定数段かつ多項式サイズの回路

$\mathrm{P} \not\subseteq \mathrm{AC}^0$ [Ajtai83, FSS84, Yao85, Hastad89]

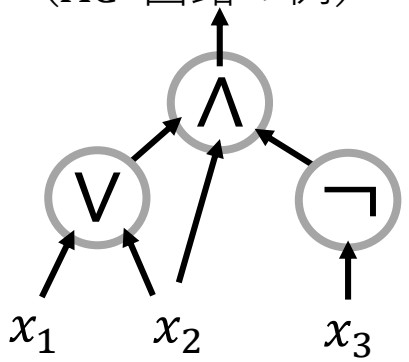
$\mathrm{P} \not\subseteq \mathrm{AC}^0[p]$ [Razborov87, Smolensky87]

未解決:

$\mathrm{NP} \not\subseteq \mathrm{TC}^0$

$\mathrm{NP} \not\subseteq \mathrm{P/poly}$

（AC^0回路の例）



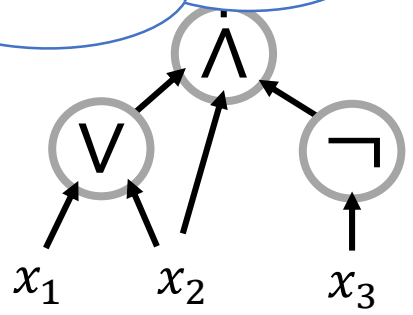
回路下界技法の発展 (1980s)

P ≠ NP に対するアプローチ
として回路の表現力の限界
を調べる技法が発展してきた。

$\mathrm{P} \not\subseteq \mathrm{AC}^0$ [Ajtai83, FSS84, Yao85, Hastad89]

$\mathrm{P} \not\subseteq \mathrm{AC}^0[p]$

多項式サイズの
回路



未解決:

$\mathrm{NP} \not\subseteq \mathrm{TC}^0$

$\mathrm{NP} \not\subseteq \mathrm{P/poly}$

回路下界技法の発展 (1980s)

P ≠ NP に対するアプローチとして回路の表現力の限界を調べる技法が発展してきた。

閾値ゲートからなる定数段の回路

$\mathrm{P} \not\subseteq \mathrm{AC}^0$ [Ajtai83, FSS84, Yao85, Hastad89]

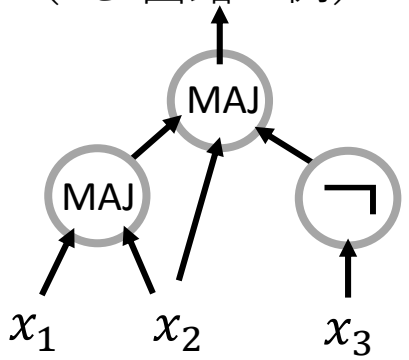
$\mathrm{P} \not\subseteq \mathrm{AC}^0[p]$ [Razborov87, Smolensky87]

未解決:

$\mathrm{NP} \not\subseteq \mathrm{TC}^0$

$\mathrm{NP} \not\subseteq \mathrm{P/poly}$

（TC^0回路の例）



自然な証明

[Razborov & Rudich 1997]

- **P vs NP**問題の難しさを示す一つのバリア

自然な証明が存在する ⇒ $\mathrm{P} \not\subseteq \mathrm{AC}^0$, $\mathrm{P} \not\subseteq \mathrm{AC}^0[p]$

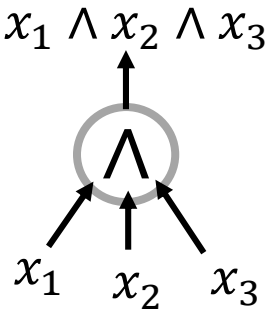
自然な証明が存在しない ⇒ $\mathrm{NP} \not\subseteq \mathrm{TC}^0$, $\mathrm{NP} \not\subseteq \mathrm{P/poly}$ (未解決)

自然な証明: MCSPの部分問題

- AC^0回路に対する**自然な証明**とは多項式時間アルゴリズムであって、

1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さいAC^0回路で実現できるときは“NO”と答える

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1



“NO”

（サイズ1のAC^0回路で実現できる）

自然な証明: MCSPの部分問題

- AC^0回路に対する**自然な証明**とは多項式時間アルゴリズムであって、

1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さいAC^0回路で実現できるときは“NO”と答える

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

“YES”

AC^0に対する自然な証明

- AC^0回路に対する自然な証明は存在するか？

- 回路下界の証明をアルゴリズム的に見直すと、
  存在することがわかる！

$$\mathrm{P} \not\subseteq \mathrm{AC}^0$$ [Ajtai83, FSS84, Yao85, Hastad89]

- 実はほとんど全ての回路下界の証明は
  自然な証明になっている。

自然な証明の存在について

自然な証明が存在する

- $\mathrm{P} \not\subseteq \mathrm{AC}^0$
- $\mathrm{P} \not\subseteq \mathrm{AC}^0[p]$

(解決済み)

自然な証明が存在しない

- $\mathrm{NP} \not\subseteq \mathrm{TC}^0$
- $\mathrm{NP} \not\subseteq \mathrm{P/poly}$

(未解決)

定理 [Razborov & Rudich (1997)]

（一方向性関数が存在するならば、）
P/polyに対する自然な証明は存在しない。

「回路最小化問題のゼロ誤りアルゴリズム」＝「自然な証明」

（$\mathrm{SIZE}(s)$に対する）
自然な証明

主張
$\Leftrightarrow$

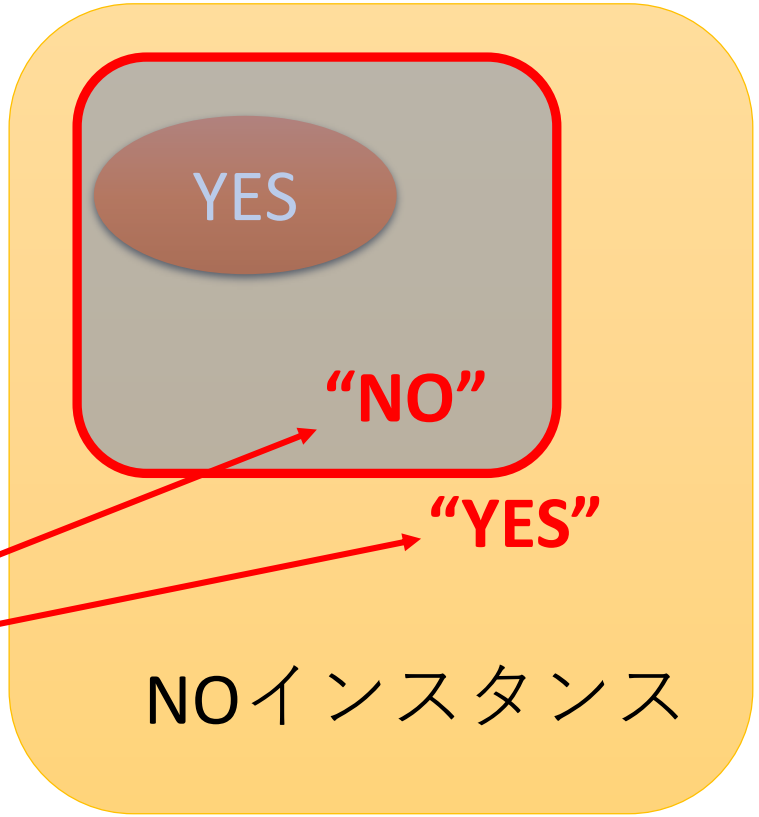
$\mathrm{MCSP}[s]$を解く
ゼロ誤りアルゴリズム

1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さい回路で実現できるときは“NO”と答える

「回路最小化問題のゼロ誤りアルゴリズム」＝「自然な証明」

（$\mathrm{SIZE}(s)$に対する）
自然な証明 ⇒ $\mathrm{MCSP}[s]$を解く
ゼロ誤りアルゴリズム

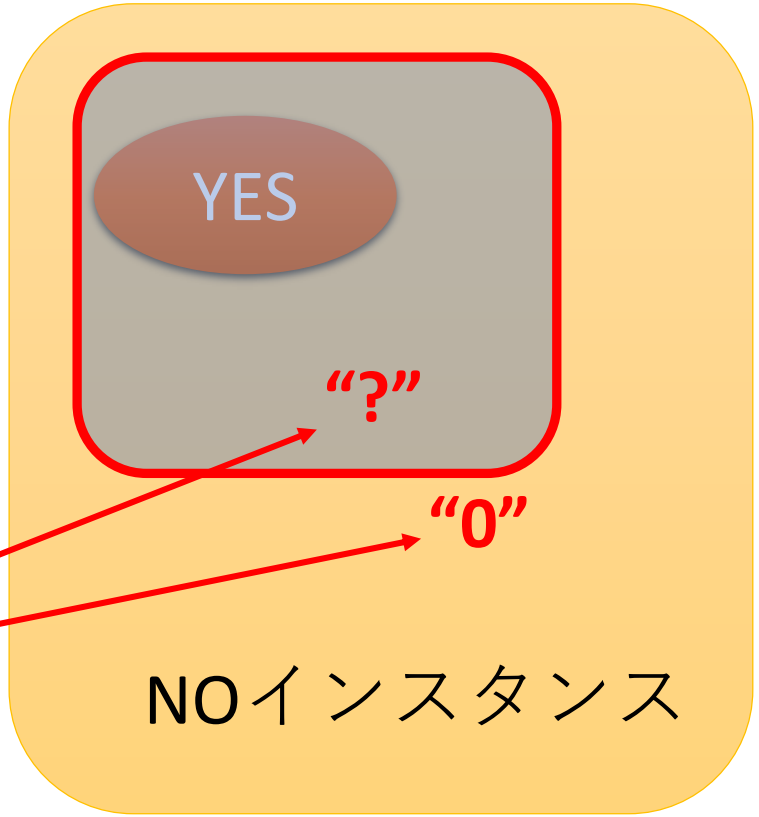
1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さい回路で実現できるときは“NO”と答える



「回路最小化問題のゼロ誤りアルゴリズム」＝「自然な証明」

（$\mathrm{SIZE}(s)$に対する）
自然な証明 $\Rightarrow$ $\mathrm{MCSP}[s]$を解く
ゼロ誤りアルゴリズム

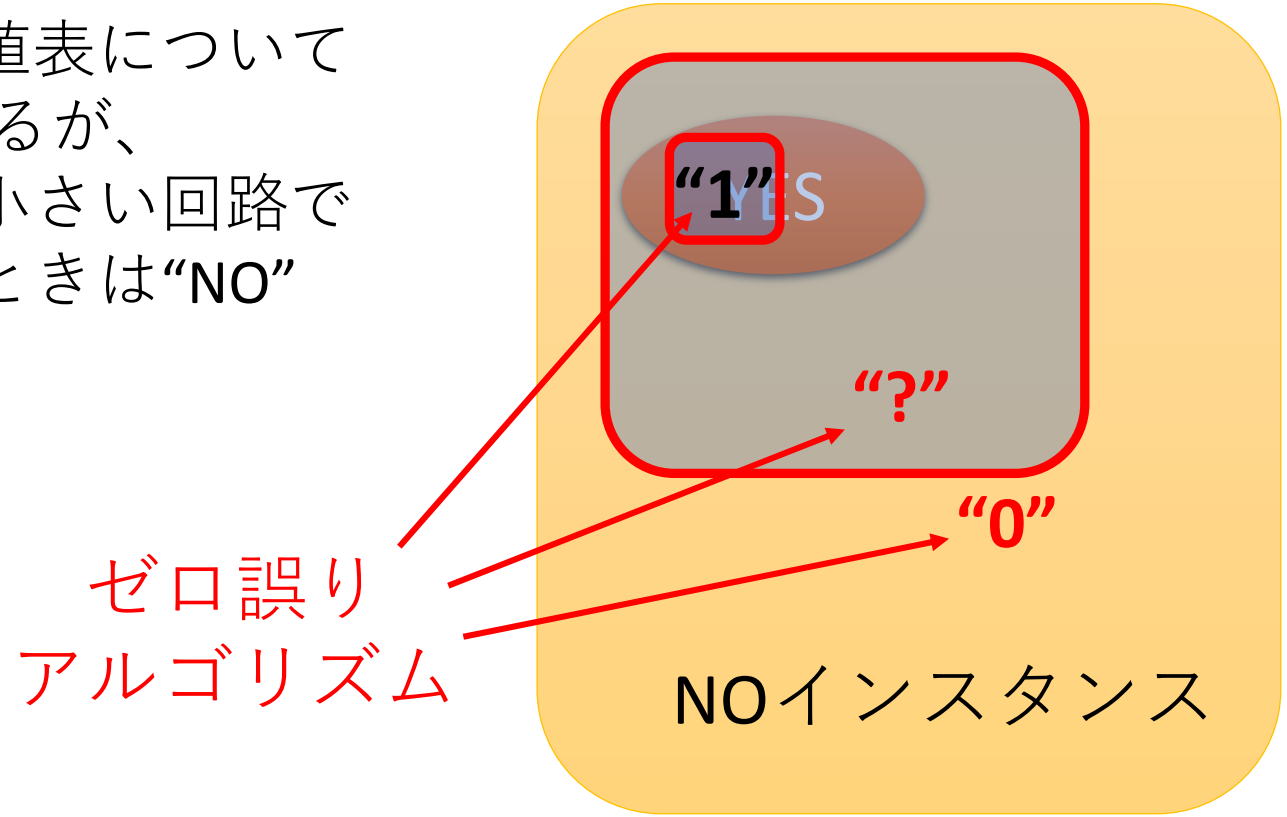
1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さい回路で実現できるときは“NO”と答える



「回路最小化問題のゼロ誤りアルゴリズム」＝「自然な証明」

（$\mathrm{SIZE}(s)$に対する）
自然な証明 ⇐ $\mathrm{MCSP}[s]$を解く
ゼロ誤りアルゴリズム

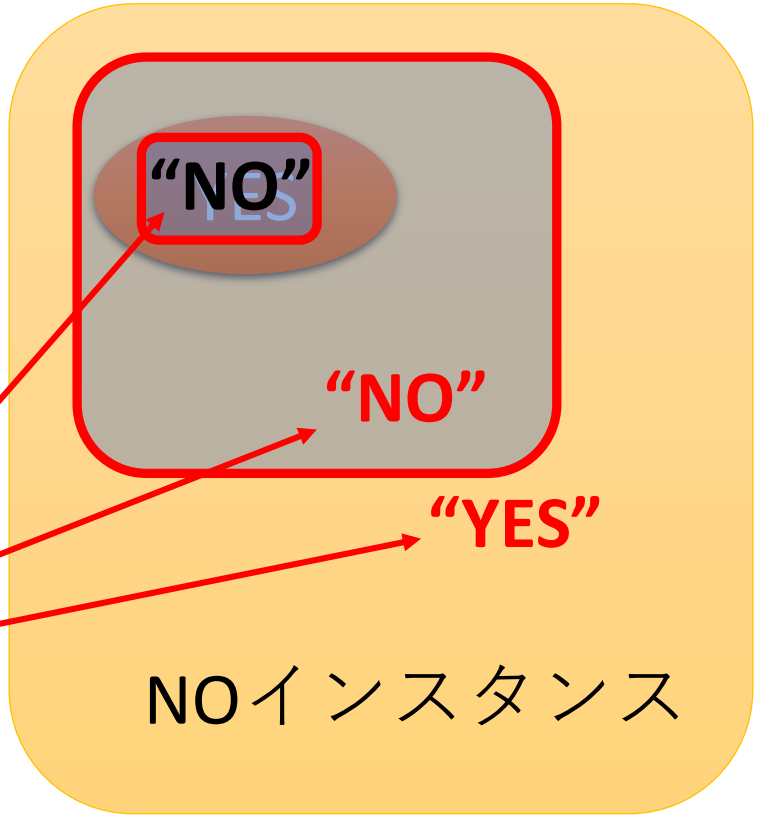
1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さい回路で実現できるときは“NO”と答える



「回路最小化問題のゼロ誤りアルゴリズム」＝「自然な証明」

（$\mathrm{SIZE}(s)$に対する）
自然な証明 ⇐ $\mathrm{MCSP}[s]$を解く
ゼロ誤りアルゴリズム

1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さい回路で実現できるときは“NO”と答える



(YESインスタンスの数) $= s^{O(s)}$
$\ll$ (全体のインスタンスの数) $= 2^{2^n}$

「回路最小化問題のゼロ誤りアルゴリズム」＝「自然な証明」

（$\mathrm{SIZE}(s)$に対する）
自然な証明

$\Leftrightarrow$

$\mathrm{MCSP}[s]$を解く
ゼロ誤りアルゴリズム

1. 多くの真理値表について“YES”と答えるが、
2. 真理値表が小さい回路で実現できるときは“NO”と答える

目次

1. 回路最小化問題（MCSP）について
2. 平均計算量とは
3. 自然な証明について
4. MCSPの最悪計算量から平均計算量への帰着について（疑似ランダム自己帰着性）

ランダム自己帰着 (Random self-reduction)

問題Lが（1回のクエリの）ランダム自己帰着できる

$\overset{\text{def}}{\Leftrightarrow}$ ∃ 乱択多項式時間機械

入力: $x \in \{0,1\}^N$

（ランダムな）クエリq

回答$L(q)$

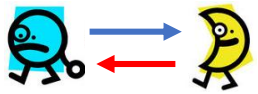
問題Lのオラクル

-  は問題の答え$L(x)$を高い確率で答える。
- qは$\{0,1\}^N$上で一様に分布する。

最悪計算量から平均計算量への帰着

- 問題Lがランダム自己帰着できる
- あるアルゴリズム  がLを**平均的に**解く

$\Rightarrow$ Lを**全ての入力で**解くアルゴリズムが存在する。



入力: $x \in \{0,1\}^N$

答え$L(x)$を出力

平均的に解くアルゴリズムで置き換える

クエリ$q \sim \{0,1\}^N$

回答$L(q)$

~~オラクルL~~

NP完全問題のランダム自己帰着性

定理 ([Feigenbaum & Fortnow 1993], [Bogdanov & Trevisan 2006])

（多項式階層がつぶれない限り）
NP完全問題はランダム自己帰着を持たない。

- もしもMCSPがランダム自己帰着性をもつならば、MCSPがNP完全でないことの強い証拠を与える。

疑似ランダム自己帰着

(Pseudorandom self-reduction)

問題Lが疑似ランダム自己帰着できる

$\overset{\text{def}}{\Longleftrightarrow}$ ∃ 乱択多項式時間機械

入力: $x \in \{0,1\}^N$

（ランダムな）

クエリq

回答$L(q)$

問題Lの

オラクル

-  は問題の答え$L(x)$を高い確率で答える。
- qと$\{0,1\}^N$上の一様分布は多項式時間で識別不可能。

我々の成果：回路最小化問題の疑似ランダム自己帰着性

定理

一方向性関数が存在するならば、
（約束付きの）回路最小化問題は疑似ランダム自己帰着性をもつ。

- 証明のアイディア：疑似乱数関数生成器とXORをとる

未解決問題

妥当な仮定の下でNP完全問題は疑似ランダム自己帰着性をもつか？

まとめ

- 疑似ランダム自己帰着性という、最悪計算量から平均計算量への弱い帰着の概念を導入
- （一方向性関数の存在の下で）MCSPはその性質を持つ。
- MKTP（MCSPの時間制限付きコルモゴロフ記述量版）はRandom 3SAT困難。特に、$\mathrm{MKTP} \notin \mathrm{coNP}$を示す初めての証拠を与えた。