Limits of Minimum Circuit Size Problem as Oracle (CCC 2016)

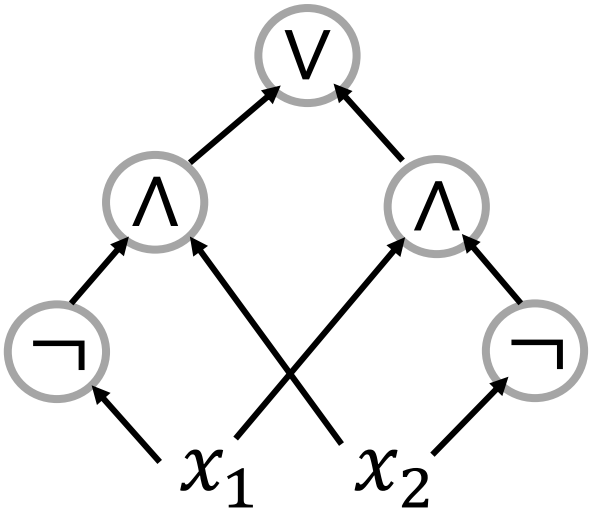
平原 秀一（東京大学、ERATO研究協力者）
渡辺 治（東京工業大学）

概要: 回路最小化問題はNP完全か？

(Minimum Circuit Size Problem; *MCSP*)

入力　真理値表　→　出力　回路サイズ＝5

x_1	x_2	x_1 xor x_2
0	0	0
0	1	1
1	0	1
1	1	0



我々の貢献

“現在の帰着手法”では回路最小化問題のNP完全性を示せない、ということに対して強い証拠を与えた。

目次

1. 問題設定・重要性
2. 背景・先行研究
   - MCSPの二つの側面
3. “オラクル独立”帰着
   - なぜ現在の帰着手法はオラクル独立なのか
4. 結果・まとめ

目次

1. 問題設定・重要性
2. 背景・先行研究
   - MCSPの二つの側面
3. “オラクル独立”帰着
   - なぜ現在の帰着手法はオラクル独立なのか
4. 結果・まとめ

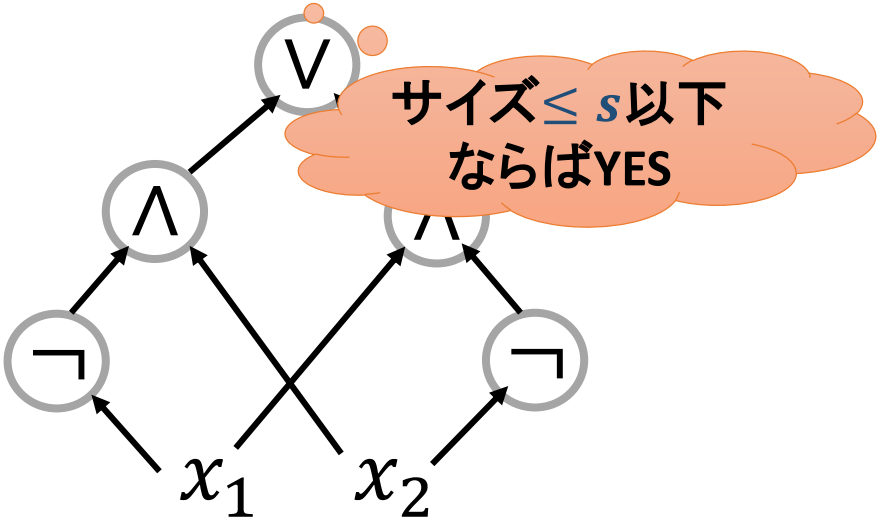
回路最小化問題(MCSP)

入力　真理値表T　→　出力　回路サイズ＝5

加えて、サイズパラメタ $s \in \mathbb{N}$

x_1	x_2	x_1 xor x_2
		0
		1
1	0	1
1	1	0

$= T$

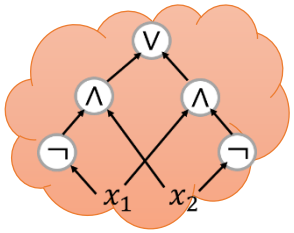


<u>定義</u> (回路最小化問題; Minimum Circuit Size Problem; MCSP)

入力: 真理値表 $T \in \{0,1\}^{2^n}$ とサイズパラメタ $s \in \mathbb{N}$
出力: 真理値表を実現するサイズs以下の回路が存在するか？

注意: 入力に対して多項式時間 $\Leftrightarrow 2^{O(n)}$時間

MCSPはNPに属する



- NPの証拠: サイズs以下の回路C
- 証拠の正しさのチェック:
  - ✓全てのありうる入力$x_1, \ldots, x_n$を試して真理値表Tと一致するか確かめる。

- $2^{O(n)}$時間　　・・・　入力長2^nについて多項式時間

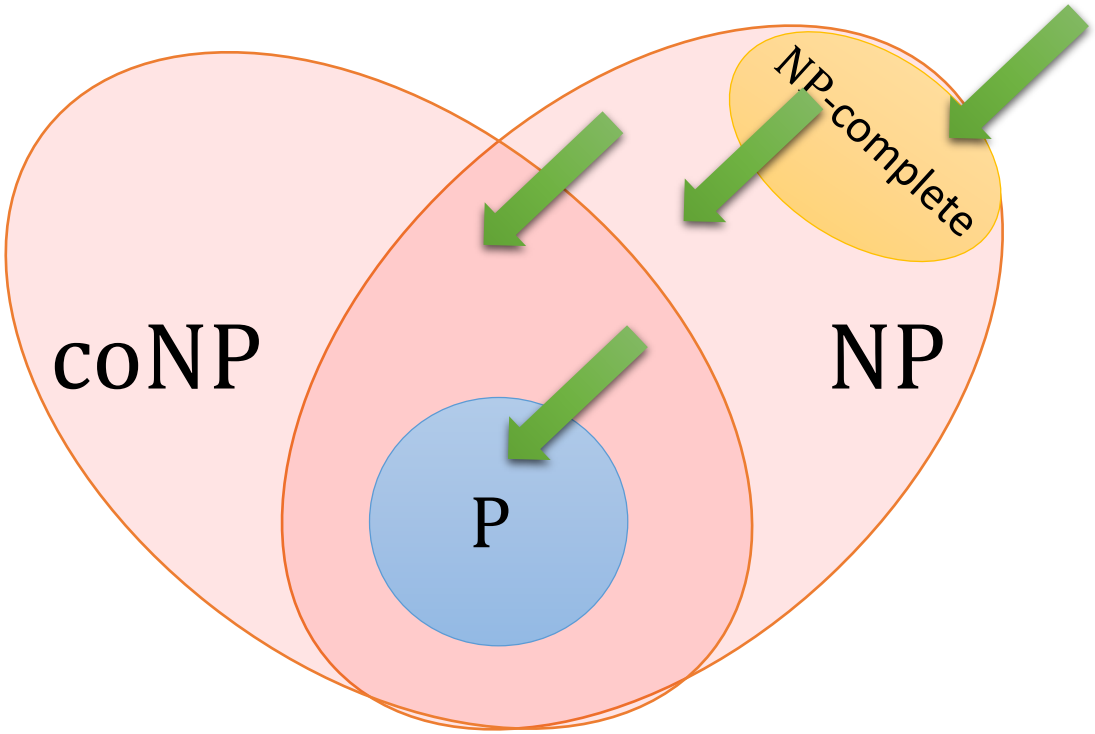
定義 (回路最小化問題; Minimum Circuit Size Problem; MCSP)

入力: 真理値表 $T \in \{0,1\}^{2^n}$ とサイズパラメタ $s \in \mathbb{N}$
出力: 真理値表を実現するサイズs以下の回路が存在するか？

注意: 入力に対して多項式時間 ⇔ $2^{O(n)}$時間

問 MCSPはどのくらい難しいのか？

- NP完全か？
  MCSPが解ける ⟹ SATが解ける？
- MCSP ∈ coNPか？



重要性 MCSPの計算量理論的側面

- NPに対する回路下界

計算量理論のゴールのひとつ:

$$\mathrm{NP} \not\subseteq \mathrm{SIZE}(n^{O(1)}) \implies \mathrm{P} \neq \mathrm{NP}$$

多項式サイズの回路
で解ける問題全体

- MCSPと回路下界は深く関連している。

$$\mathrm{MCSP} \in \mathrm{P} \implies \mathrm{EXP}^{\mathrm{NP}} \not\subseteq \mathrm{SIZE}(n^{O(1)})$$

[Kabanets & Cai (2000)]

もし示せれば大きな
ブレークスルー

重要性 MCSPの計算量理論的側面

- NPに対する回路下界

計算量理論のゴールのひとつ:

$$\mathrm{NP} \not\subseteq \mathrm{SIZE}(n^{O(1)}) \implies \mathrm{P} \neq \mathrm{NP}$$

多項式サイズの回路
で解ける問題全体

- MCSPと回路下界は深く関連している。

$$\mathrm{MCSP} \in \mathrm{P} \implies \mathrm{EXP}^{\mathrm{NP}} \not\subseteq \mathrm{SIZE}(n^{O(1)})$$

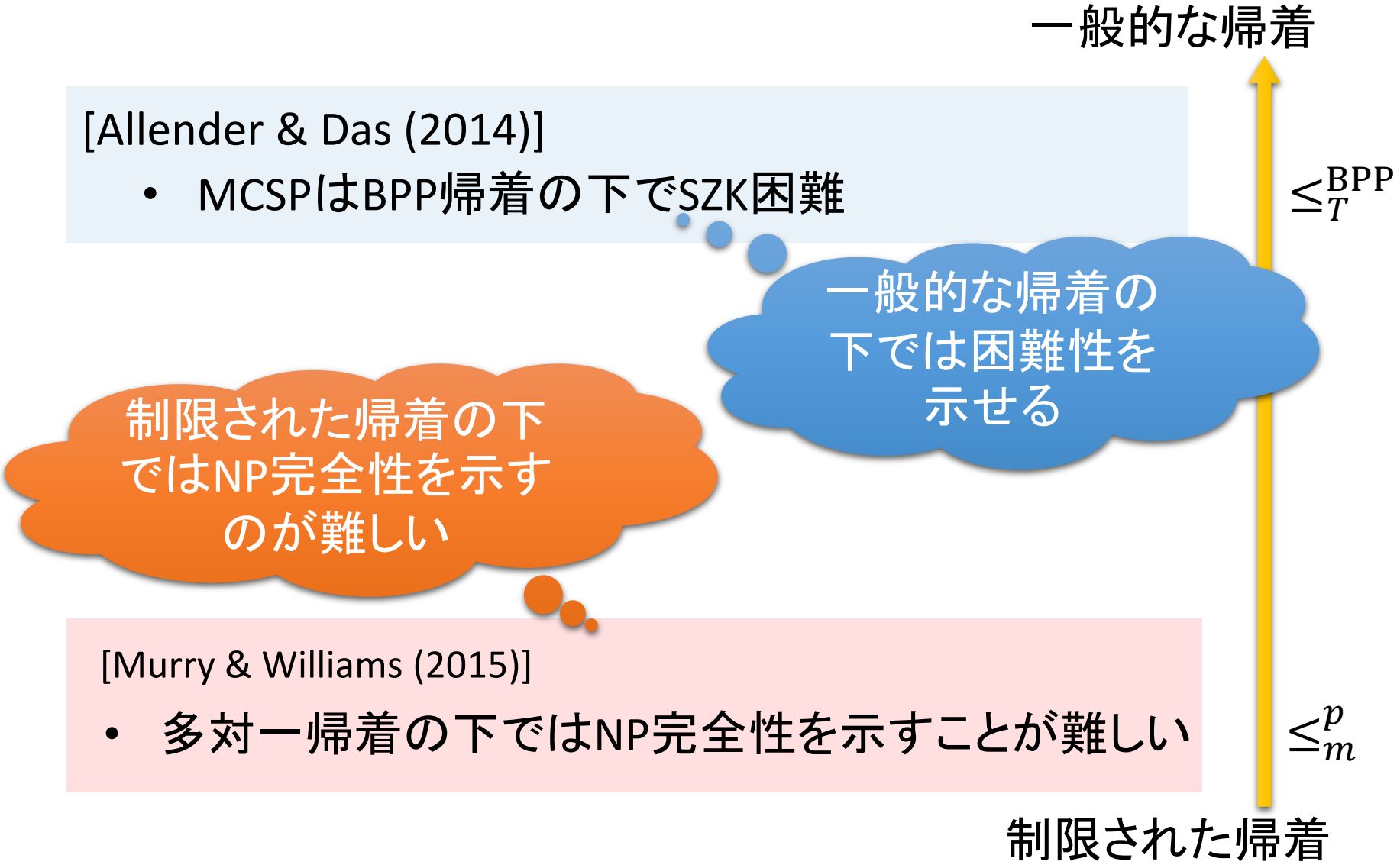
[Kabanets & Cai (2000)]

$$\mathrm{MCSP} \in \mathrm{coNP} \implies \mathrm{EXP}^{\mathrm{NP}} \not\subseteq \mathrm{SIZE}(n^{O(1)})$$

目次

1. 問題設定・重要性
2. 背景・先行研究
   - MCSPの二つの側面
3. “オラクル独立”帰着
   - なぜ現在の帰着手法はオラクル独立なのか
4. 結果・まとめ

背景: MCSPの二つの側面



帰着の種類 (1/3)

<u>定義</u> (多対一帰着; カープ帰着)

SATがMCSPに多対一帰着できる
⇔ ある多項式時間機械Mがあって、$\mathrm{MCSP}\big(M(\varphi)\big) = \mathrm{SAT}(\varphi)$.

<u>機械Mで多項式時間で変換可能</u>

SATのインスタンス 論理式φ	$\longmapsto$	MCSPのインスタンス (T, s)
φが充足可能	$\Leftrightarrow$	真理値表Tを実現する サイズs以下の回路が存在する

- NP完全性を議論するときの普通の帰着の概念

帰着の種類 (2/3)

定義 (P帰着;多項式時間チューリング帰着; クック帰着)

SATがMCSPにP帰着できる $(\mathrm{SAT} \in \mathrm{P}^{\mathrm{MCSP}})$
⇔ ある多項式時間オラクル機械Mがあって、

$$M^{\mathrm{MCSP}}(\varphi) = \mathrm{SAT}(\varphi).$$

つまり、

MCSPが単位時間で解ける $\Longrightarrow$ SATが多項式時間で解ける

対偶をとると

SATが難しい $\Longrightarrow$ MCSPも難しい

- 多対一帰着の一般化

帰着の種類 (3/3)

(Bounded-error Probabilistic Polynomial)

定義 (BPP帰着)

SATがMCSPにBPP帰着できる $(\mathrm{SAT} \in \mathrm{BPP}^{\mathrm{MCSP}})$
⇔ ある多項式時間乱択オラクル機械Mがあって、

$$M^{\mathrm{MCSP}}(\varphi) = \mathrm{SAT}(\varphi)$$

が99%以上で成立する。

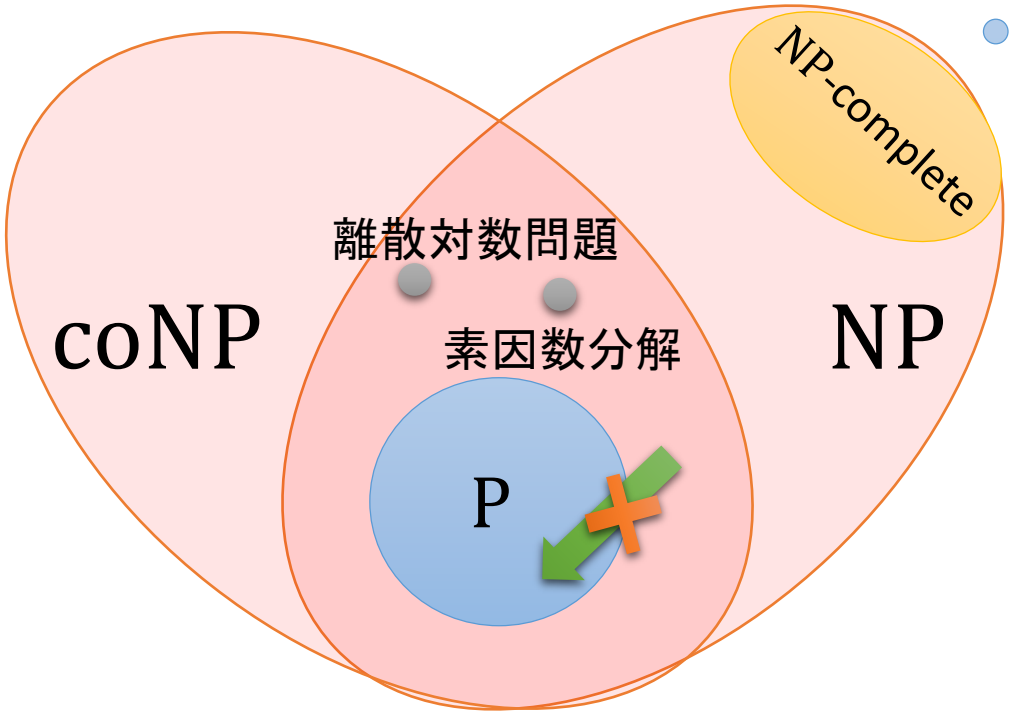
つまり、

MCSPが単位時間で解けると仮定して、SATが乱択アルゴリズムで多項式時間で計算できる。

背景: MCSPの困難性

[Allender, Buhrman, Koucký, van Melkebeek and Ronneburger (2006)]

- 素因数分解がMCSPにBPP帰着できる　（素因数分解$\in \mathrm{BPP}^{\mathrm{MCSP}}$）
- 離散対数問題がMCSPにBPP帰着できる　（離散対数問題 $\in \mathrm{BPP}^{\mathrm{MCSP}}$）

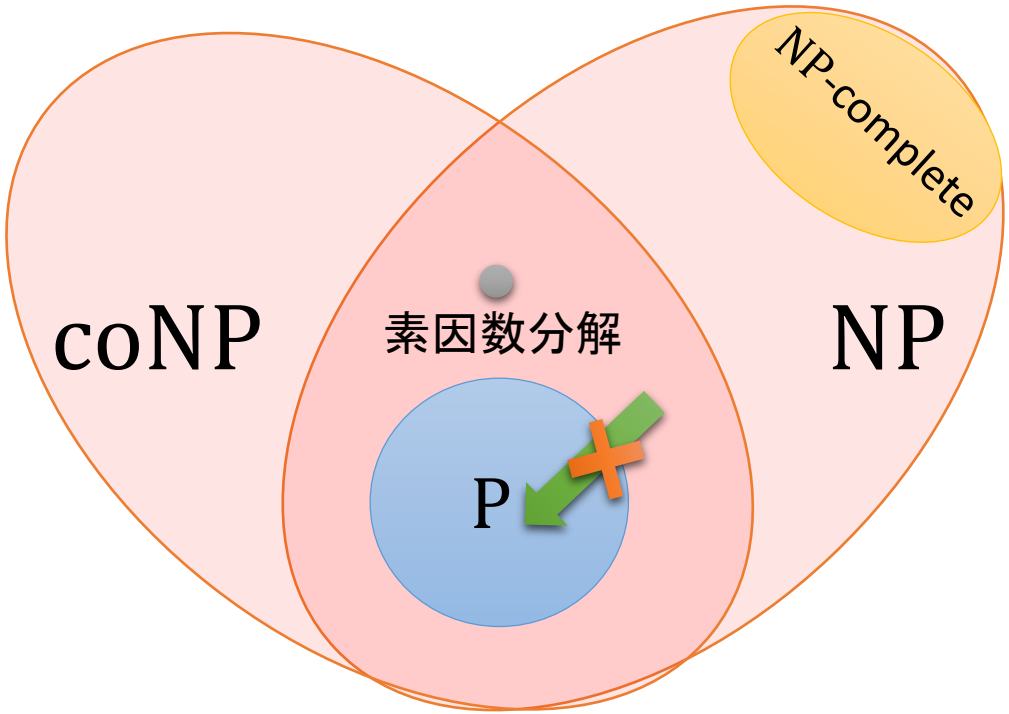


NPの中間の問題より困難

問 MCSPはどのくらい難しいのか？

- MCSPはPには属さない（素因数分解が簡単でない限り）

（注）素因数分解 ∈ NP ∩ coNP

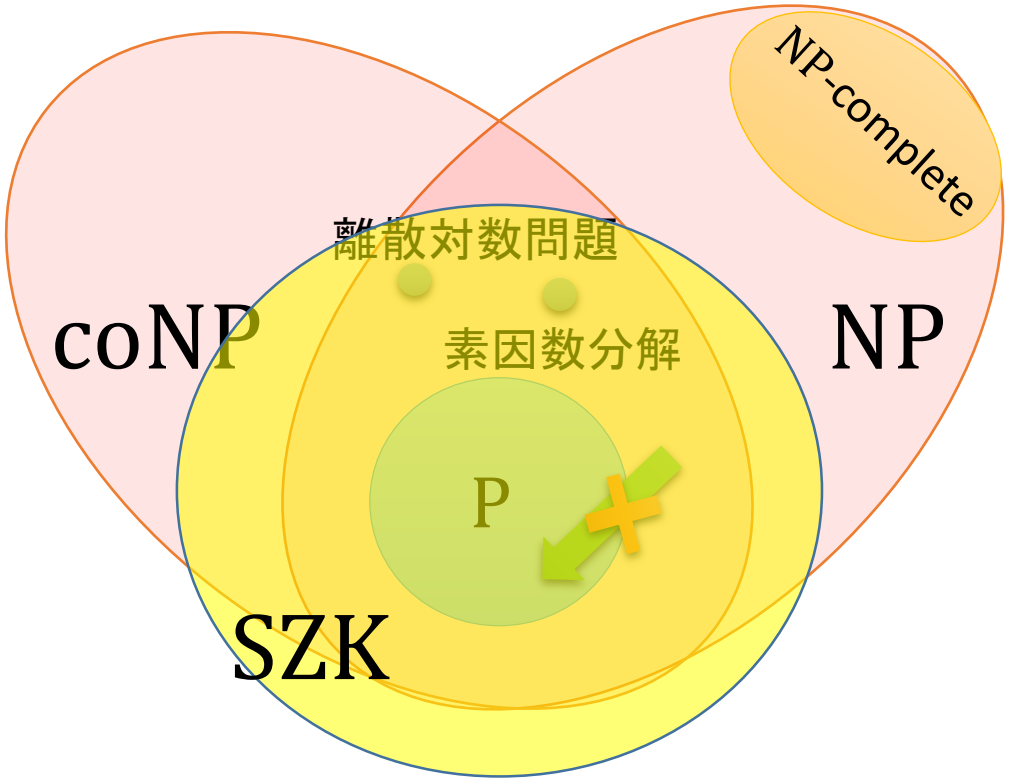


背景: MCSPの困難性

[Allender & Das (2014)]

統計的ゼロ知識証明(SZK)の任意の問題がMCSPにBPP帰着できる。
(Statistical Zero Knowledge)

つまり、 $\mathrm{SZK} \subseteq \mathrm{BPP}^{\mathrm{MCSP}}$



MCSPは
SZK困難

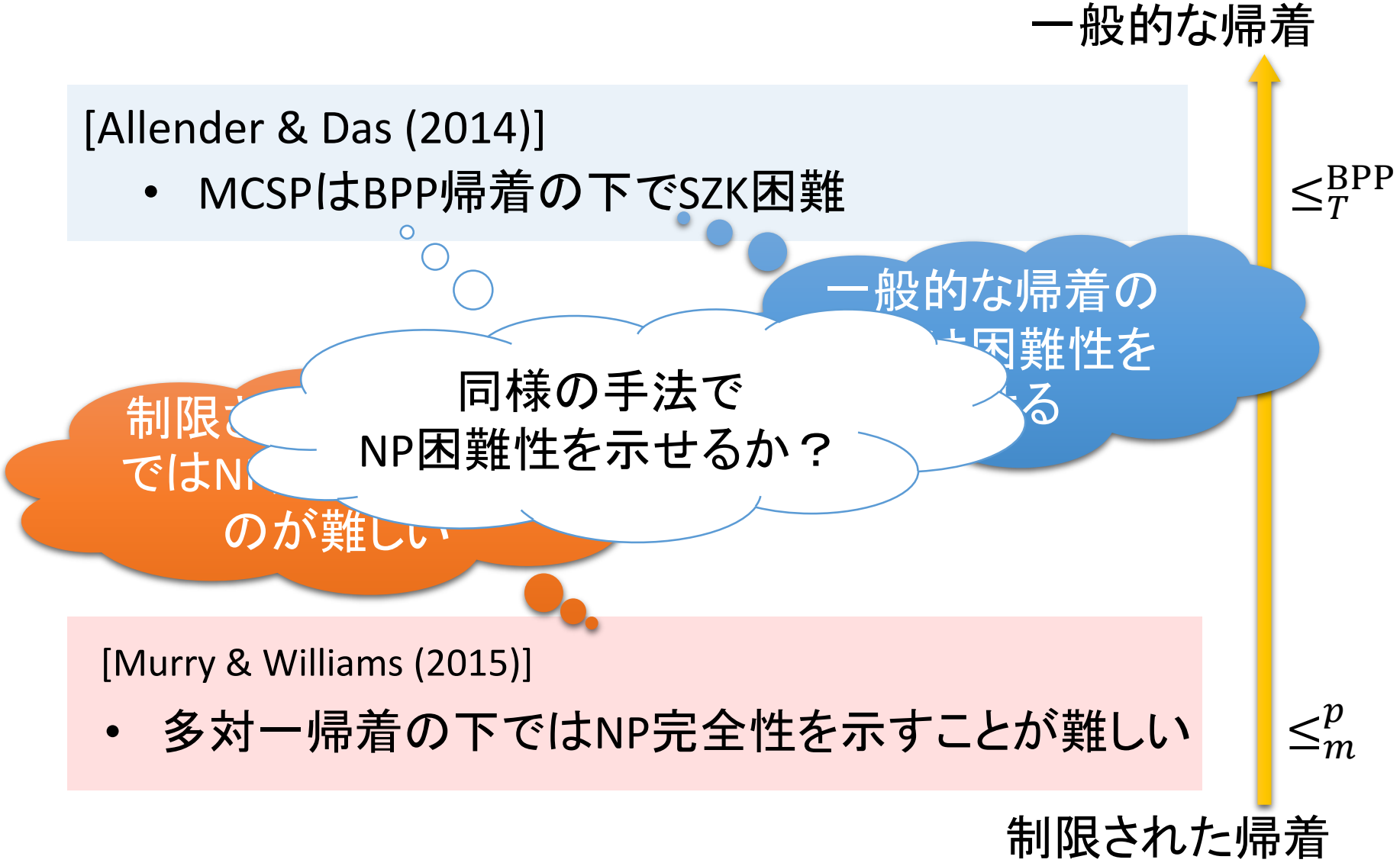
制限された帰着では困難性を示すことは難しい

[Murray & Williams (CCC 2015)]

- 多対一帰着の下でNP完全性を示せたとすると、重要な未解決問題($\mathrm{ZPP} \neq \mathrm{EXP}$)が従う。

多対一帰着の下でNP完全性を示すのは難しい。

背景: MCSPの二つの側面



背景: MCSPの二つの側面

一般的な帰着

[Allender & Das (2014)]

- MCSPはBPP帰着の下でSZK困難

$\leq_T^{\mathrm{BPP}}$

我々の結果

1. 「現在の帰着手法」ではP帰着の下でもNP完全性を示せない。
2. 同様に(クエリが一回の)BPP帰着の下でも示せない。

$\leq_m^{\mathrm{BPP}}$

$\leq_T^p$

[Murry & Williams (2015)]

- 多対一帰着の下ではNP完全性を示すことが難しい

$\leq_m^p$

制限された帰着

目次

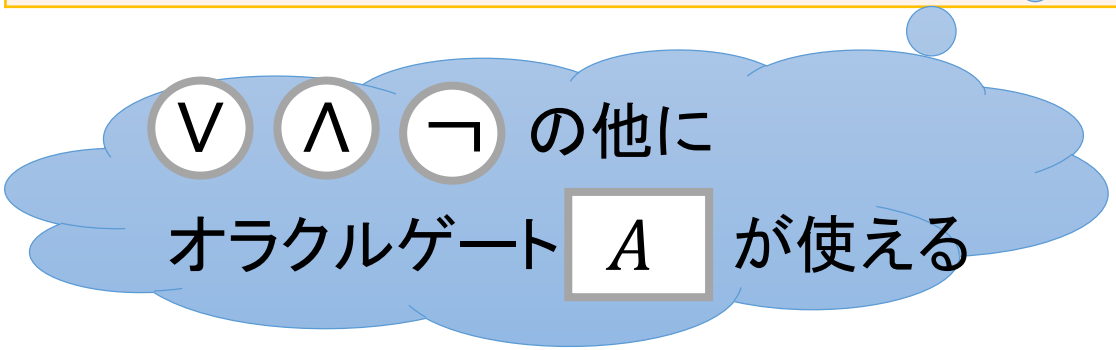
1. 問題設定・重要性
2. 背景・先行研究
   - MCSPの二つの側面
3. “オラクル独立”帰着
   - なぜ現在の帰着手法はオラクル独立なのか
4. 結果・まとめ

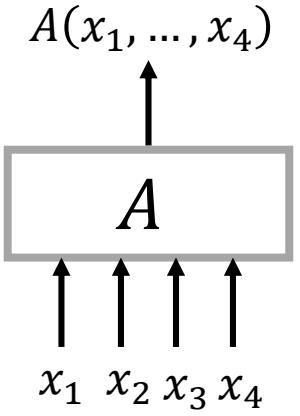
オラクル回路最小化問題

- Aをオラクルとする。 $A : \{0,1\}^* \to \{0,1\}$

定義 (Aオラクル回路最小化問題; $\mathbf{MCSP}^A$)

入力: 真理値表 $T \in \{0,1\}^{2^n}$ とサイズパラメタ $s \in \mathbb{N}$
出力: 真理値表を実現するサイズs以下のAオラクル回路が存在するか？





オラクル独立帰着

アイディア:

帰着が（MCSPの性質というよりも）全てのMCSP^Aに共通の性質だけしか使っていない。

定義 (オラクル独立帰着)

問題Lが、任意のオラクルAに対して、MCSP^Aへ帰着できるとき、LはMCSPにオラクル独立帰着できるという。

例えば:　　問題LがMCSPにオラクル独立P帰着できる

$$\overset{\text{def}}{\Leftrightarrow} \quad \text{任意のオラクル} A \text{に対して} L \in \mathrm{P}^{\mathrm{MCSP}^A}$$

$$\Leftrightarrow \quad L \in \bigcap_A \mathrm{P}^{\mathrm{MCSP}^A} .$$

現在の帰着手法は全てオラクル独立

- Allender & Das (2014)の結果はオラクル独立帰着になっている

  MCSPはBPP帰着の下でSZK困難:

$$\mathrm{SZK} \subseteq \mathrm{BPP}^{\mathrm{MCSP}}$$

（一般化）

  MCSPはオラクル独立BPP帰着の下でSZK困難:

$$\mathrm{SZK} \subseteq \bigcap_{A} \mathrm{BPP}^{\mathrm{MCSP}^{A}}$$

Let’s look at it.

- 他の帰着も全てオラクル独立

MCSPを用いてSZKを解く

主張: $\mathrm{SZK} \subseteq \mathrm{BPP}^{\mathrm{MCSP}}$ [Allender & Das (2014)]

重要な観察

任意の疑似乱数生成器がMCSPを用いて破れる。

⇓ [Hastad, Impagliazzo, Levin & Luby (1999)]

任意の一方向性関数が破れる

⇓ [Allender & Das (2014)]

SZKが多項式時間で解ける

MCSPを用いて疑似乱数生成器を破る

重要な観察

任意の疑似乱数生成器がMCSPを用いて破れる。

（出力を真理値表だとみなすと）

疑似乱数生成器の出力 $G(r)$ ← 回路計算量が低い

MCSPを用いると二つの文字列を区別できる

一様ランダムに選ばれた文字列 ← 回路計算量は高い

MCSPを用いて疑似乱数生成器を破る

重要な観察

任意の疑似乱数生成器がMCSPを用いて破れる。

（出力を真理値表だとみなすと）

疑似乱数生成器の出力 $G(r)$ ← 回路計算量が低い

- 疑似乱数生成器は“効率的に”計算可能なので、回路計算量も低い

一様ランダムに選ばれた文字列 ← 回路計算量は高い

- 数え上げの議論より、高い確率で回路計算量は高い

  サイズs以下の回路は高々$s^{O(s)}$個程度
  一方、長さ2^nの真理値表は2^{2^n}程度

MCSP^Aを用いて疑似乱数生成器を破る

重要な観察

任意の疑似乱数生成器がMCSP^Aを用いて破れる。

（出力を真理値表だとみなすと）

疑似乱数生成器の出力 $G(r)$ ← 回路計算量が低い

- 疑似乱数生成器は“効率的に”計算可能なので、回路計算量も低い

オラクルゲートが使える状況でも
回路サイズは小さいまま

一様ランダムに選ばれた文字列 ← 回路計算量は高い

- 数え上げの議論より、高い確率で回路計算量は高い

サイズs以下の

一方、長さ2^nの

数え上げの議論はそのまま成立

MCSP^Aを用いて疑似乱数生成器を破る

重要な観察

任意の疑似乱数生成器がMCSP^Aを用いて破れる。

（出力を真理値表だとみなすと）

疑似乱数生成器の出力 $G(r)$ ← 回路計算量が低い

- 疑似乱数生成器は“効率的に”計算可能なので

系 [Allender & Das (2014)]

$$\mathrm{SZK} \subseteq \bigcap_{A} \mathrm{BPP}^{\mathrm{MCSP}^A}.$$

- 数え上げの議論より、高い確率で回路計算量は高い

サイズs以下の

一方、長さ2^nの

数え上げの議論はそのまま成立

なぜオラクル独立帰着しか知られていないのか？

- 一般に、具体的な関数の回路下界を得るのは非常に難しい。
  - 例えば、$\mathrm{EXP}^{\mathrm{NP}} \not\subseteq \mathrm{SIZE}(n^{O(1)})$かどうかは未解決。

- 回路下界として数え上げの議論しか使っていない

  「一様ランダムに選んだ(具体的でない)関数は高い回路計算量を持つ。」

  → 任意のオラクルAをつけても成立する議論

目次

1. 問題設定・重要性
2. 背景・先行研究
   - MCSPの二つの側面
3. “オラクル独立”帰着
   - なぜ現在の帰着手法はオラクル独立なのか
4. 結果・まとめ

我々の結果 (1/2)

定理 1. (オラクル独立P帰着の限界)

問題LがMCSPにオラクル独立P帰着したとすると、
LはPに属する。別の言い方をすると、

$$\bigcap_{A} \mathrm{P}^{\mathrm{MCSP}^{A}} = \mathrm{P}.$$

特に、MCSPはその帰着の下ではNP困難ではない。
（P = NPでない限り）

我々の結果 (2/2)

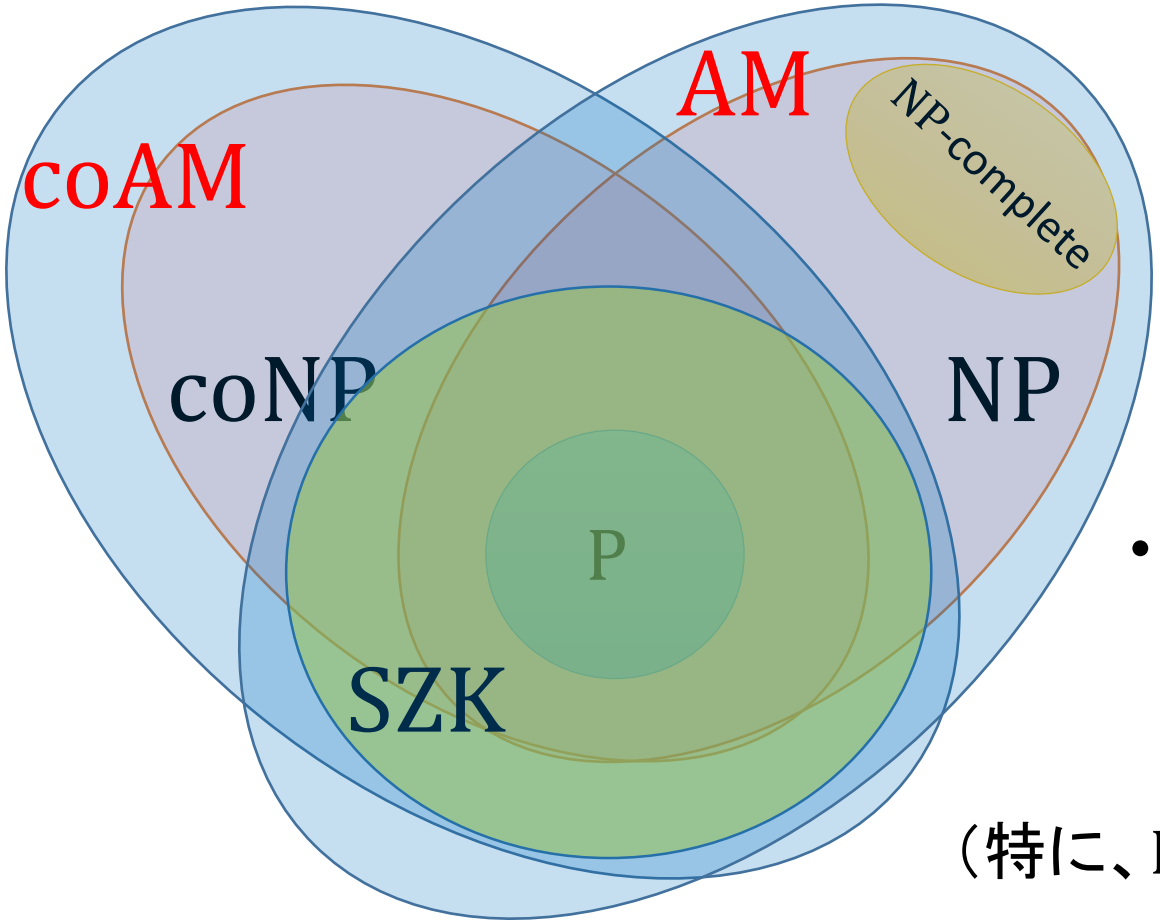
定理 2. (オラクル独立BPP帰着の限界)

問題LがMCSPに(クエリが一回の)オラクル独立BPP帰着したとすると、LはAM ∩ coAMに属する。
別の言い方をすると、

$$\bigcap_{A} \mathrm{BPP}^{\mathrm{MCSP}^{A}[1]} \subseteq \mathrm{AM} \cap \mathrm{coAM}.$$

特に、MCSPはその帰着の下ではNP困難ではない。
(多項式階層がつぶれないかぎり)

AMとは（Arthur-Merlin）



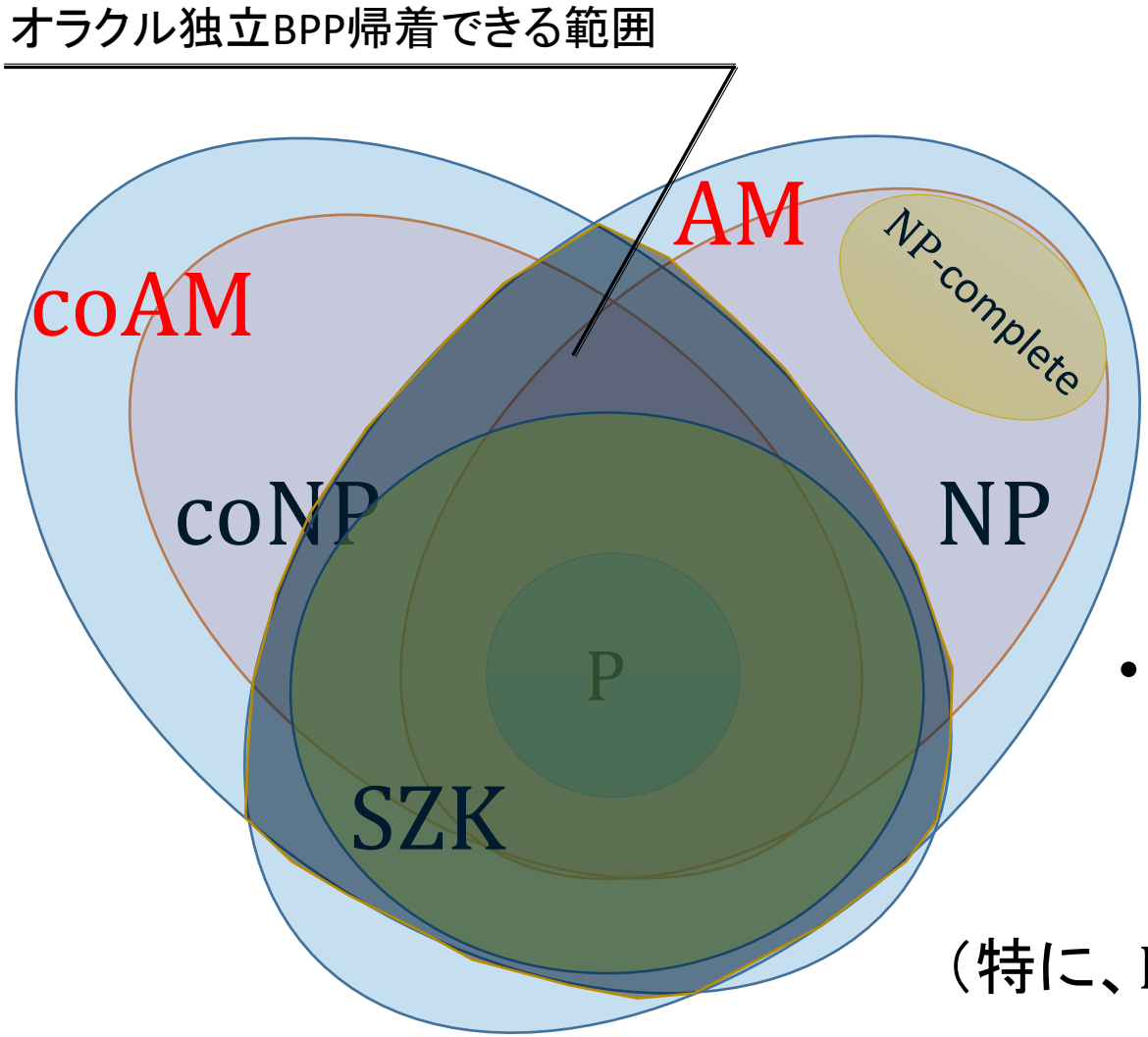
- $\mathrm{AM} = \mathrm{BP} \cdot \mathrm{NP}$
- $\mathrm{SZK} \subseteq \mathrm{AM} \cap \mathrm{coAM}$

  [Fortnow ’87]
  [Aiello & Hastad ‘91]

- 多項式階層がつぶれないかぎり、$\mathrm{NP} \not\subseteq \mathrm{coAM}$

（特に、$\mathrm{NP} \not\subseteq \bigcap_A \mathrm{BPP}^{\mathrm{MCSP}^A[1]}$）

AMとは（Arthur-Merlin）



- $\mathrm{AM} = \mathrm{BP} \cdot \mathrm{NP}$
- $\mathrm{SZK} \subseteq \mathrm{AM} \cap \mathrm{coAM}$

  [Fortnow ’87]
  [Aiello & Hastad ‘91]

- 多項式階層がつぶれないかぎり、$\mathrm{NP} \not\subseteq \mathrm{coAM}$

（特に、$\mathrm{NP} \not\subseteq \bigcap_A \mathrm{BPP}^{\mathrm{MCSP}^A[1]}$）

まとめ

- 我々の貢献
  1. MCSPの帰着の限界を議論する枠組みを導入（オラクル独立帰着）
  2. P帰着でも（クエリが一回の）BPP帰着でもNP完全性を示せないことを示した。
  - ➢難しさの本質 = 回路下界を得るのが難しい。
    - 数え上げの議論だけの回路下界ではオラクル独立帰着になってしまう。
- 未解決問題
  - ➢より強い帰着ではどうか？$\mathrm{NP} \subseteq \mathrm{coNP}^{\mathrm{MCSP}}$ ？
  - ➢複数回のクエリがあったときにも限界を示せるか？