

# 素因数分解問題とTFNPのサブクラス

手塚 真徹（東京科学大学）

田中 圭介（東京科学大学）

2025年5月13日

@CRESTクリプトマス 2025年度第1回全体会議

最終更新：2025年05月21日

- ・ 判定問題の計算量クラスと判定版素因数分解問題について
- ・ 探索問題とクラスFNPについて
- ・ クラスTFNPとそのサブクラスについて
- ・ TFNPのサブクラスと探索版素因数分解問題について
- ・  $\text{FACROOTMUL} \in \text{PWPP}$ の証明[Jer16]について
- ・ 暗号に関する探索問題とクラスPPP, PWPP
- ・  $\text{FACROOT} \in \text{PPA}$ の証明[Jer16]について
- ・ TNFPの困難性と暗号技術について

# 判定問題の計算量クラスと 判定版素因数分解問題について

# 判定問題

判定問題(Decision problem)

出力が1(Yes), 0(No)だけに限られる問題

判定問題の例: Composite

入力: 自然数  $n$

出力:  $n$ が合成数なら1, そうでないならば0を出力する.

判定問題は言語  $L \subseteq \{0, 1\}^*$  を用いて表すことができる.

$$L_{\text{composite}} = \{n \mid n \text{は合成数}\}$$

## クラスP

決定的多項式時間アルゴリズムで判定可能な言語  $L$  のクラス

## クラスNP

答えが Yes である入力  $x$  ( $x \in L$ ) に対し, 答えが Yes であることを証拠  $y$  (witness) を用いて多項式時間で検証できる言語のクラス

より正確には,

言語  $L$  が NP に属するとは, ある多項式時間検証可能な関係  $R$  が存在して,

$$x \in L \iff \text{ある } y \in \{0, 1\}^{\text{poly}(|x|)} \text{ が存在して } R(x, y) = 1 \text{ を満たすこと.}$$

# 判定問題の例

クラスPにもNPにも属する言語の判定問題

Composite

入力：自然数  $n \geq 2$

出力： $n$ が合成数なら1, そうでないならば0を出力

NPに属する言語の判定問題

INTEGER FACTORIZATION

$n$ を割り切る非自明な因子とは

$n$ を割り切る1と $n$ 以外の正の整数のこと.

入力： $(n, k)$

出力： $n$ を割り切る $k$ 以下の非自明な因子 $a$ があれば1を出力

そうでないならば0を出力

# 判定問題の多項式時間帰着とNP完全問題

探索問題の多項式時間帰着  $f$

問題Aの入力を問題Bの入力に変換する.

- $f$  は多項式時間で計算できる.
- $x$  が問題AのYes入力  $\iff f(x)$  が問題AのYes入力

問題PがNP完全問題

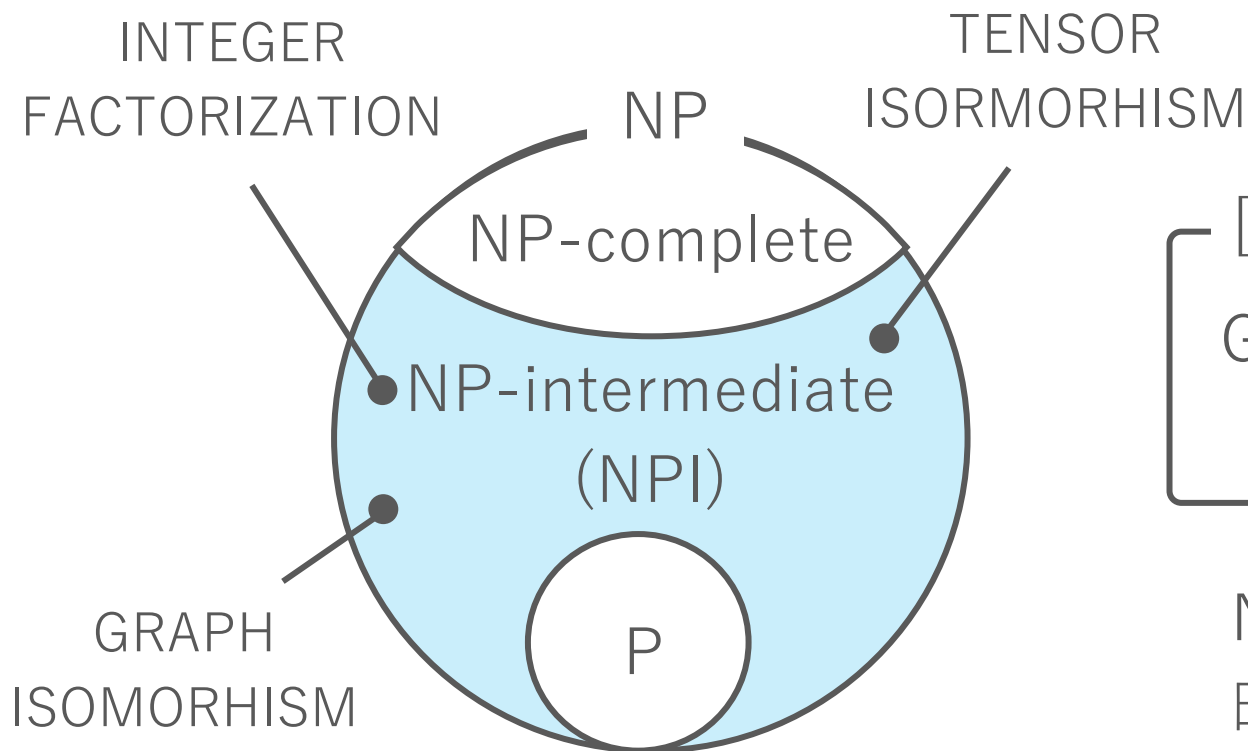
- すべてのNP問題が問題Pに多項式時間帰着する. (NP困難)
- 問題PがNP問題である.

NP完全問題はクラスNPに属する言語の判定問題の中で最も難しい.

# 判定版素因数分解問題の属する計算量クラス

素因数分解の判定問題 INTEGER FACTORIZATION はクラスNPに属する。

INTEGER FACTORIZATIONはNP問題だが、  
クラスPの問題に属さず、NP完全問題にも属さない。(NP-intermediate)



[BHZ87] —  
GRAPH ISOMORPHISMがNP完全問題  
⇒ 多項式階層PHが崩壊する

NP-intermediateの問題をベースに  
暗号方式が考案された例あり。



# 探索問題とクラスFNPについて

## 次の問題はクラスNPに属する？

FULLFAC

入力：自然数  $n \geq 2$

出力： $n$  の素因数分解

この問題はクラスNPか？

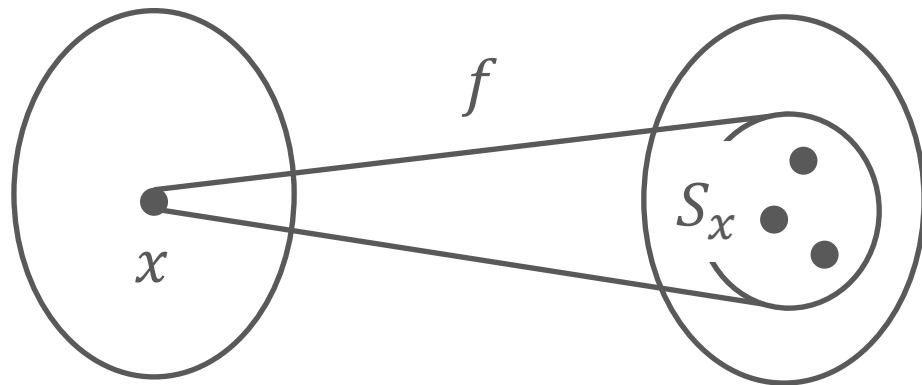
答えはNo!

クラスNPの問題の出力は0か1の2択のみであり、  
FULLFACの出力とは異なる。

この問題を捉えるためには、判定問題からのクラス拡張が必要である。

多価関数  $f$

入力  $x \in \Sigma^*$  から集合  $S_x \subseteq \Sigma^*$  を定める.



関数問題  $f$

入力  $x \in \Sigma^*$  対して  $y \in S_x = f(x)$  を計算する問題のこと.

関数  $f$  を一価に制限し, 集合  $S_x$  を  $\{0, 1\}$  に制限すれば判定問題を捉える.

関数  $f$  を一価に制限し,  $f(x)$  を解の個数とすれば,  
解の数え上げ問題を捉えることができる.

NP言語 $L$ に関連する関数問題  $f$  を定義したい.

言語 $L$ がNPに属するとは, ある多項式時間検証可能な関係 $R_L$ が存在して,

$x \in L \iff$  ある証拠  $y \in \{0, 1\}^{poly(|x|)}$  が存在して  $R_L(x, y) = 1$  を満たす.

$f$  を証拠(多価)関数として次のように定義する.

$$f(x) := \begin{cases} R_L(x, y) = 1 \text{ となる多項式長の証拠 } y \text{ の集合} & x \in L \\ \text{"No"} & x \notin L \end{cases}$$

クラスFunction NP (FNP) はNP言語に対する証拠関数  $f$  全体の関数クラス.

FNPに属する関数問題のみ扱うので,

以降, 関数問題を単に探索問題と呼ぶことにします.

## FULLFAC

$$R = \{(n, n \text{の素因数分解}) | n \geq 2\}$$

入力：自然数  $n \geq 2$

出力： $n$  の素因数分解（因子のリスト）

## FACTORING

$$R = \{(n, n \text{を割り切る非自明な因子}) | n \geq 2\}$$

入力：自然数  $n \geq 2$

出力： $n$ を割り切る非自明な因子  $a$  があれば  $a$  を出力  
そうでないならば "No" を出力

問題AがFNP完全問題

- ・すべてのFNPに属する問題が問題Aに多項式時間帰着する。(FNP困難)
- ・問題AがFNPに属する.

FNP完全問題の例

FSAT    入力：論理式  $\phi$

出力：  $\phi$  が充足可能であれば，充足割り当てを出力  
そうでないならば "No" を出力

FULLFAC, FACTORINGともにFNP完全問題ではなさそう.

これらの問題を捉えるFNPのサブクラスは？



クラスTFNPとそのサブクラスについて

探索問題 $\Pi_R$  がクラスTFNPであるとは.

すべての入力  $x \in \Sigma^*$  に対して, 必ず  $R(x, y) = 1$  となる  $y \in \Sigma^*$  が必ず存在する.

TFNPに属さない問題の例

FACTORING 入力: 自然数  $n \geq 2$

出力:  $n$  を割り切る非自明な因子  $a$  があれば  $a$  を出力  
そうでないならば "No" を出力

TFNPに属する問題の例

FULLFAC 入力: 自然数  $n \geq 2$

出力:  $n$  の素因数分解 (因子のリスト)



# クラスTFNPには完全問題が存在するのか？

17

TFNPは完全問題をもたないと信じられている。

$NP \neq coNP \iff$  TFNPに完全問題が存在しない [MP91]

※  $NP \neq coNP$  は重要な未解決問題

$NP \neq coNP$  が成り立つなら  $P \neq NP$  が成り立つ。

$NP \neq coNP$  の証明は  $P \neq NP$  を証明すること以上に難しい！

完全問題をもつTFNPのサブクラスを導入することにより、  
TFNPの問題の計算複雑性を詳細に捉える研究が行われている。

## 補足： クラスco-NP

言語  $L$  がco-NPに属するとは，補言語  $\bar{L} \in \text{NP}$  を満たすこと．

クラスco-NPの言語の例（co-NP完全問題）

$$L_{\text{tautology}} = \{\text{論理式 } \varphi \mid \varphi \text{ は恒真}\}$$

$\varphi$  が恒真であるとは，どの変数割り当てでも  $\varphi$  が充足される．

補言語  $\bar{L}_{\text{tautology}} = \{\text{論理式 } \varphi \mid \varphi \text{ を充足しない変数割り当てが存在}\} \in \text{NP}$  であるので， $L_{\text{tautology}} \in \text{co-NP}$  に属する．

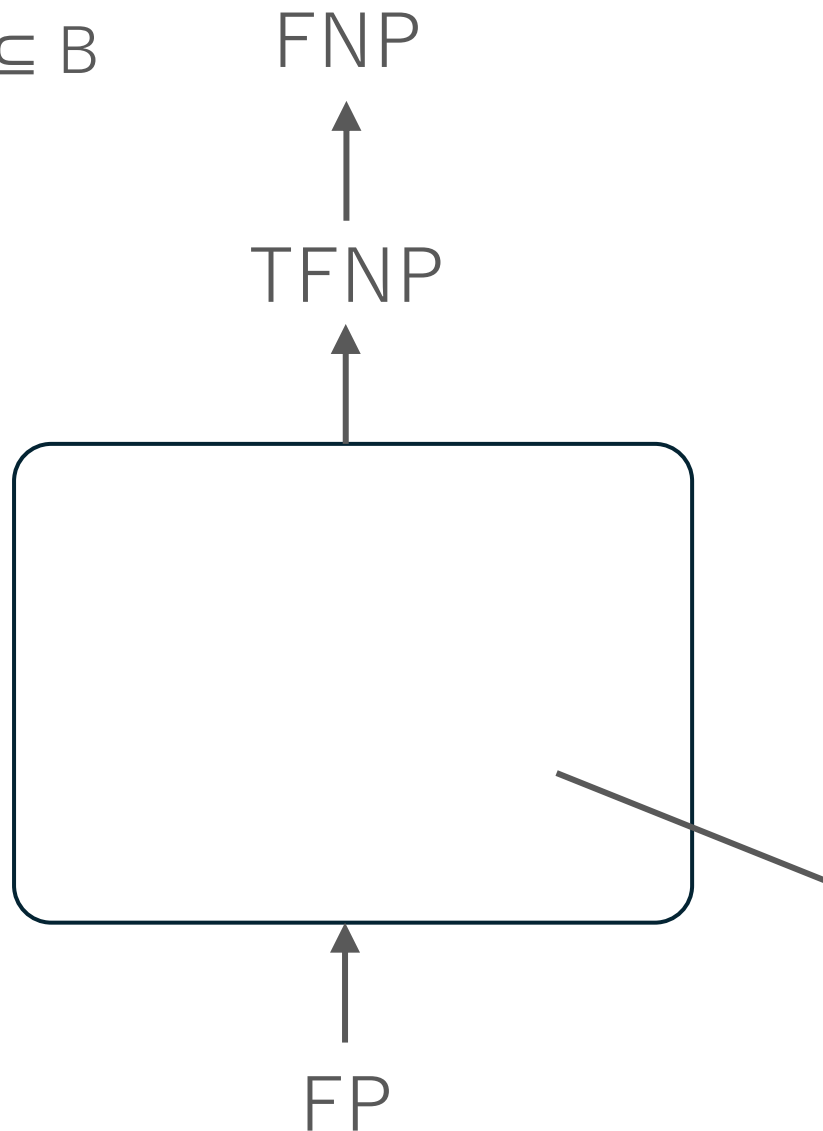
NP = coNP なら，

論理式  $\varphi$  が恒真であることの証拠が多項式長で与えられることになる．

# TNFPサブクラスの包含関係

19

$A \rightarrow B : A \subseteq B$



FNP : Function NP

TFNP : Total Function NP

FP : Function P

クラスFP

多項式時間で解くことができる

TFNPに属する関数問題  $f$  のクラス

この部分に存在するサブクラスは  
たくさんあります. . .

PLS : Polynomial Local Search [JPY85]

SOPL : Sink-Of-Potential-Line [GKRS19]

PPA : Polynomial Parity Arguments on graphs [Pap94]

PPADS : Polynomial Parity Arguments on Directed graphs, Sinks [Pap94]

PPAD : Polynomial Parity Arguments on Directed graphs [Pap94]

CLS : Continuous Local Search [DP11]

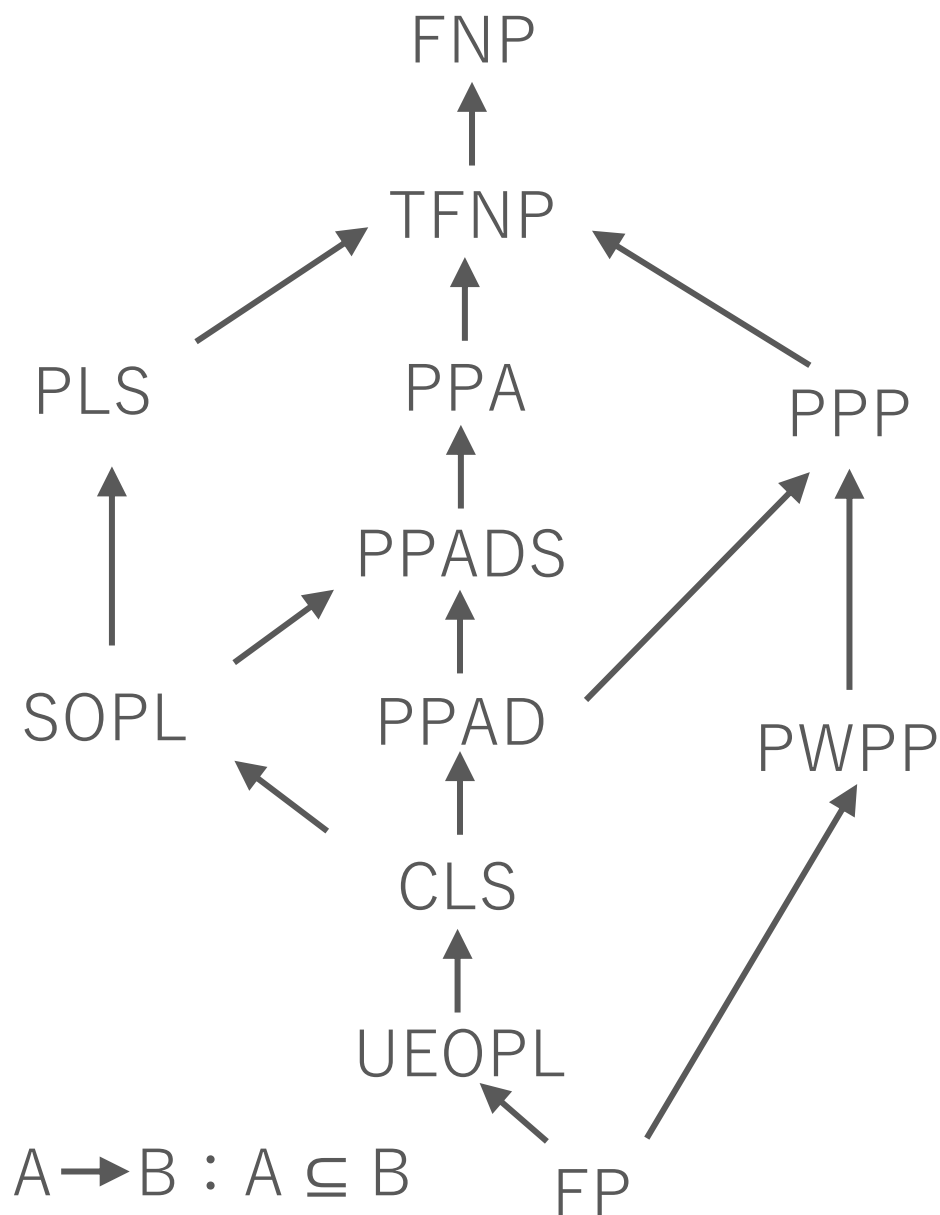
UEOPL : Unique End-Of-Potential-Line [FGMS19]

PPP : Polynomial Pigeonhole Principle [Pap94]

PWPP : Polynomial Weak Pigeonhole Principle [Jer16]

# TFNPサブクラスの包含関係

21



PLS : Polynomial Local Search

SOPL : Sink-Of-Potential-Line

PPA : Polynomial Parity Arguments on graphs

PPADS : Polynomial Parity Arguments on Directed graphs, Sinks

PPAD : Polynomial Parity Arguments on Directed graphs

CLS : Continuous Local Search

UEOPL : Unique End-Of-Potential-Line

PPP : Polynomial Pigeonhole Principle

PWPP : Polynomial Weak Pigeonhole Principle

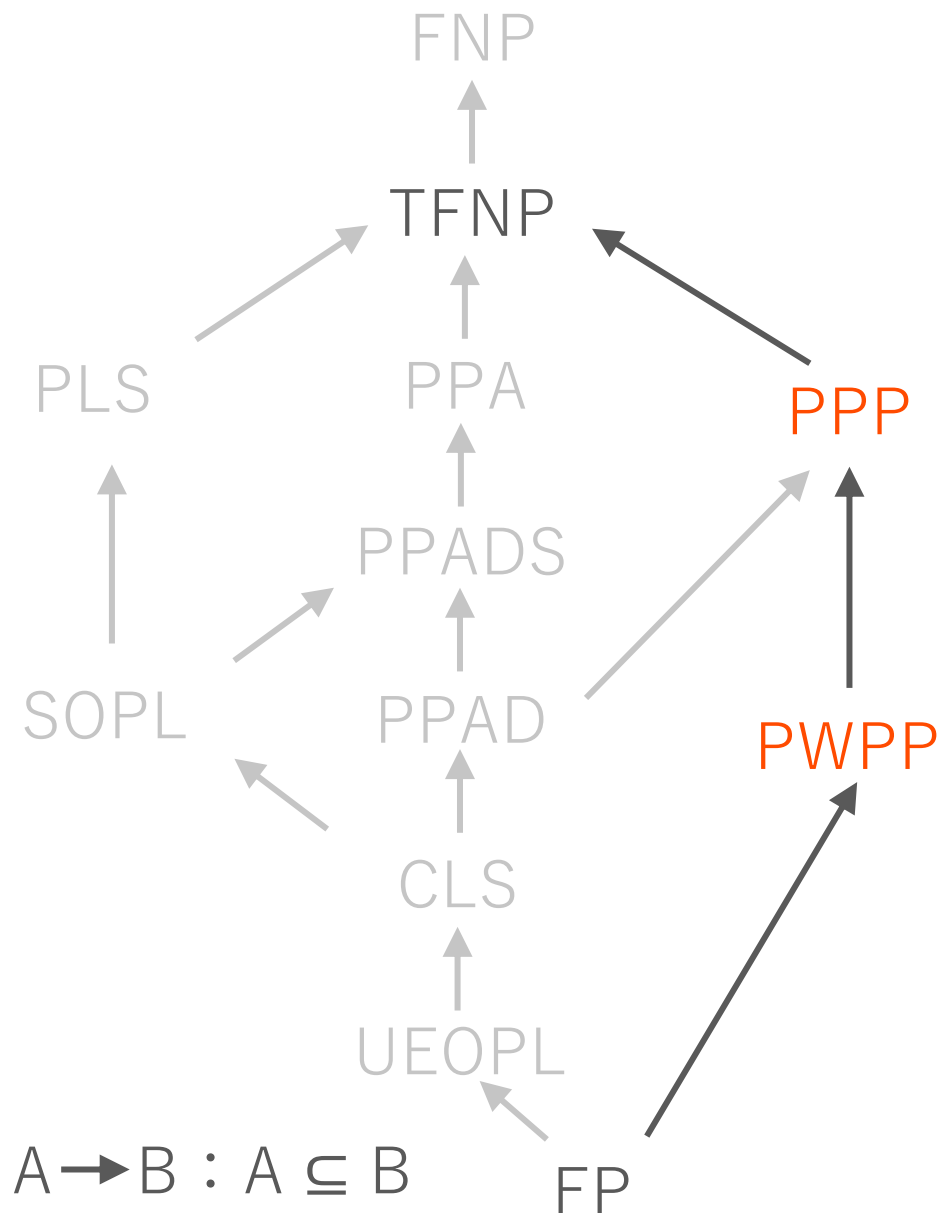
最近の結果

$\text{CLS} = \text{PLS} \cap \text{PPAD}$  [FGHS21](STOC21)

$\text{SOPL} = \text{PLS} \cap \text{PPADS}$  [GHJ+22] (CCC22)

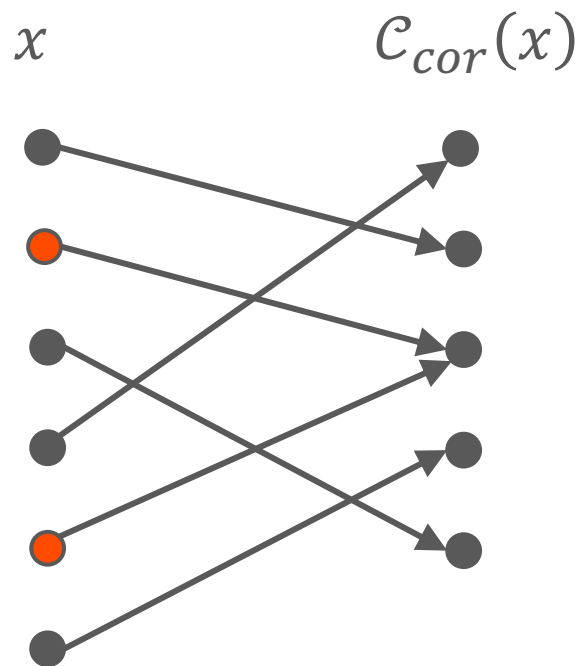
# サブクラスPPPとPWPP

22



PWPPとPPPは最悪ケースのハッシュ関数の衝突困難性を捉える探索問題計算量クラス.

COLLISION 入力： $n$  入力  $m$  出力回路  $\mathcal{C}_{cor}$  s.t.  $|\mathcal{C}_{cor}| = \text{poly}(n)$ ,  $m < n$   
出力： $(x, x')$  s.t.  $\mathcal{C}_{cor}(x) = \mathcal{C}_{cor}(x')$  かつ  $x \neq x'$

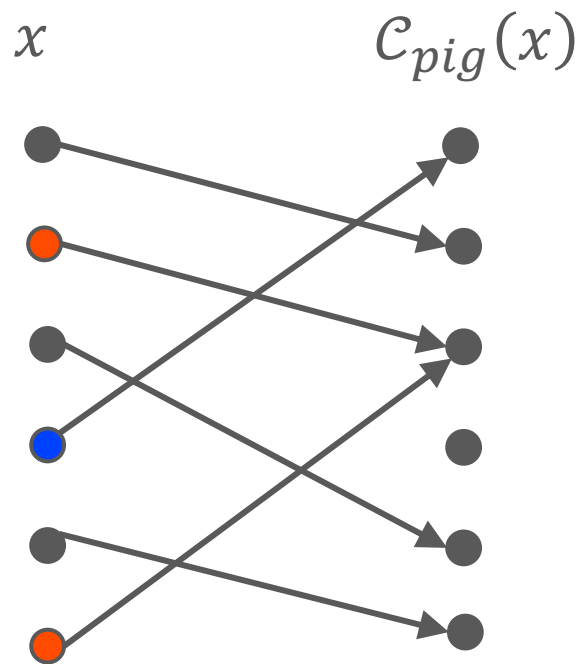


探索問題PがクラスPWPP問題に属するとは、  
問題Pから COLLISION問題への  
多項式時間帰着が存在する

## PIGONHOLE CIRCUIT

入力： $n$  入力  $n$  出力回路  $\mathcal{C}_{pig}$  s.t.  $|\mathcal{C}_{pig}| = \text{poly}(n)$

出力： $x$ , s.t.  $\mathcal{C}_{pig}(x) = 0^n$  または  $(x, x')$  s.t.  $\mathcal{C}_{pig}(x) = \mathcal{C}_{pig}(x')$  かつ  $x \neq x'$

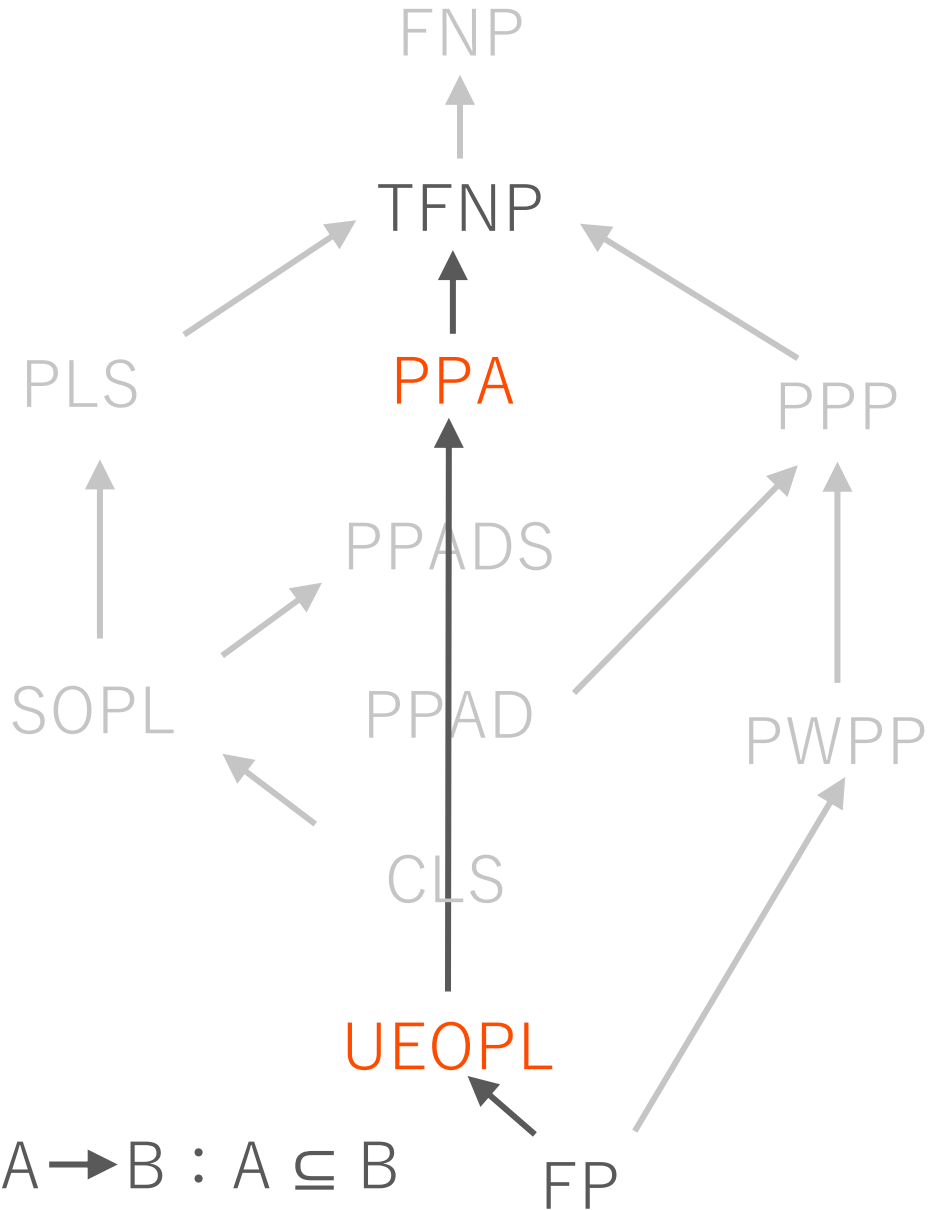


探索問題PがクラスPPPに属するとは,

問題Pから PIGEONHOLE CIRCUIT問題への  
多項式時間帰着が存在する.



# TNFPサブクラスの包含関係

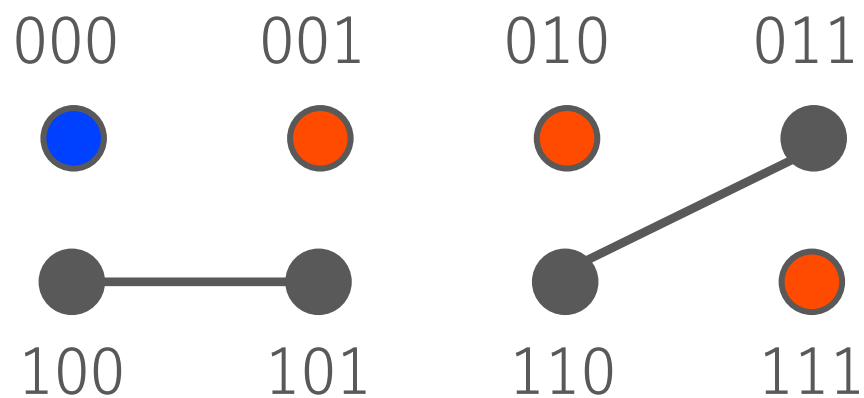


## クラスPPA, UEOPLを説明する.

# LONELY問題[BCE+95]とクラスPPA[Pap94]

26

LONELY 入力：無向グラフ  $G = (V, E)$  を表す回路  $\mathcal{C}_{lon}: \{0, 1\}^n \rightarrow \{0, 1\}^n$ ,  
 $|\mathcal{C}_{lon}| = \text{poly}(n)$ ,  $V = \{0, 1\}^n \setminus \{0^n\}$ ,  
 $(u, v) \in E$  iff  $u \neq v \wedge \mathcal{C}_{lon}(u) = v \wedge \mathcal{C}_{lon}(v) = u$   
出力：  $0^n$  以外のマッチングがない頂点



$$\mathcal{C}_{lon}(100) = 101, \mathcal{C}_{lon}(101) = 100$$

$$\mathcal{C}_{lon}(001) = 101, \mathcal{C}_{lon}(111) = 111$$

探索問題PがクラスPPAに属するとは,

頂点100 と101 はマッチする

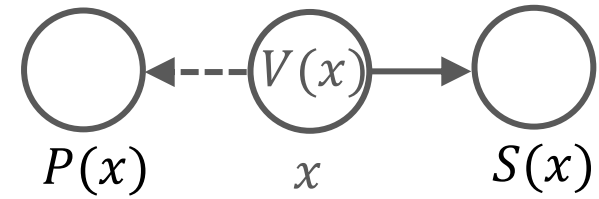
頂点101 と101 はマッチしない

問題PからLONELY問題への  
多項式時間帰着が存在する.

## UIQUE-END-OF-POTENTIAL-LINE (UEOPL)

入力：回路  $P, S: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $P(0^n) = 0^n$ ,  $S(0^n) \neq 0^n$

回路  $V: \{0, 1\}^n \rightarrow \{0, 1, \dots, 2^m - 1\}$  s.t.  $V(0^n) = 0^n$



出力：次のうちいずれかを出力

- I  $x$  s.t.  $P(S(x)) \neq x$
- II  $x$  s.t.  $S(x) \neq x$ ,  $P(S(x)) = x$ ,  $V(x) \geq V(S(x))$
- III  $x$  s.t.  $S(P(x)) \neq x$ ,  $x \neq 0^n$
- IV  $(x, y)$  s.t.  $x \neq y$ ,  $S(x) \neq x$ ,  $S(y) \neq y$ ,  $V(x) = V(y)$
- V  $(x, y)$  s.t.  $x \neq y$ ,  $S(x) \neq x$ ,  $S(y) \neq y$ ,  $V(x) < V(y) < V(S(x))$

探索問題PがクラスUEOPLに属するとは、

問題PからUEOPL問題への多項式時間帰着が存在する。

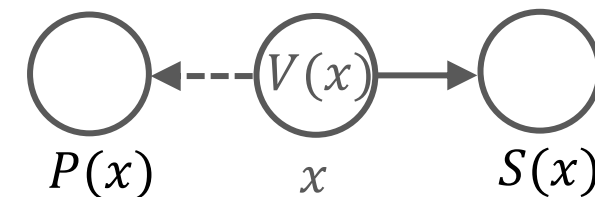
# UEOPL問題[FGMS19]

28

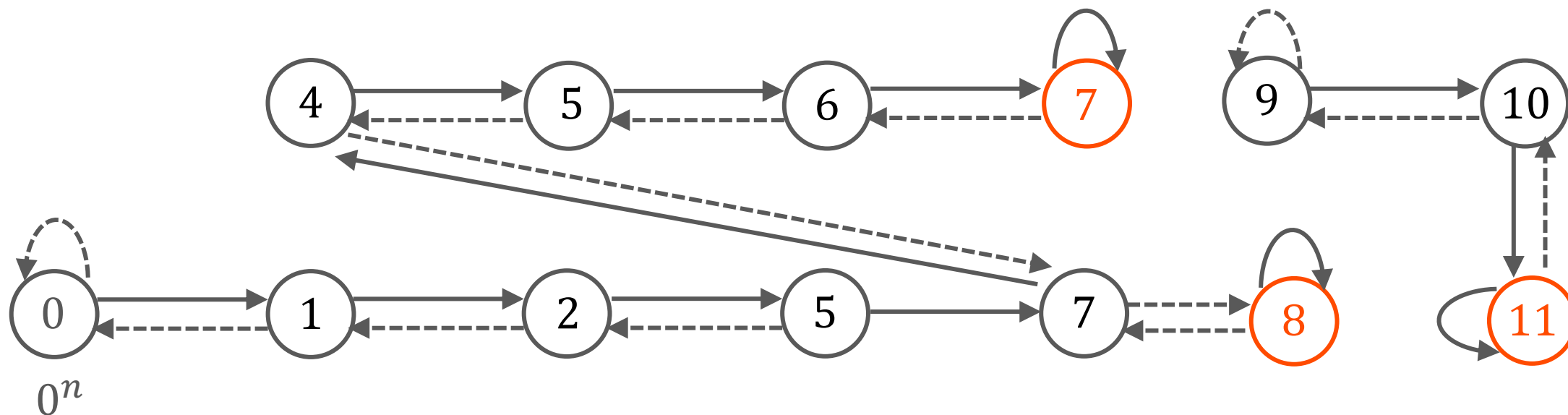
## UIQUE-END-OF-POTENTIAL-LINE (UEOPL)

入力：回路  $P, S: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $P(0^n) = 0^n$ ,  $S(0^n) \neq 0^n$

回路  $V: \{0, 1\}^n \rightarrow \{0, 1, \dots, 2^m - 1\}$  s.t.  $V(0^n) = 0^n$



出力：  $\mid x$  s.t.  $P(S(x)) \neq x$



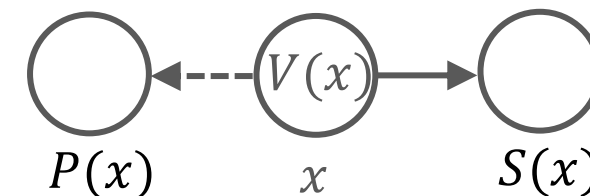
# UEOPL問題[FGMS19]

29

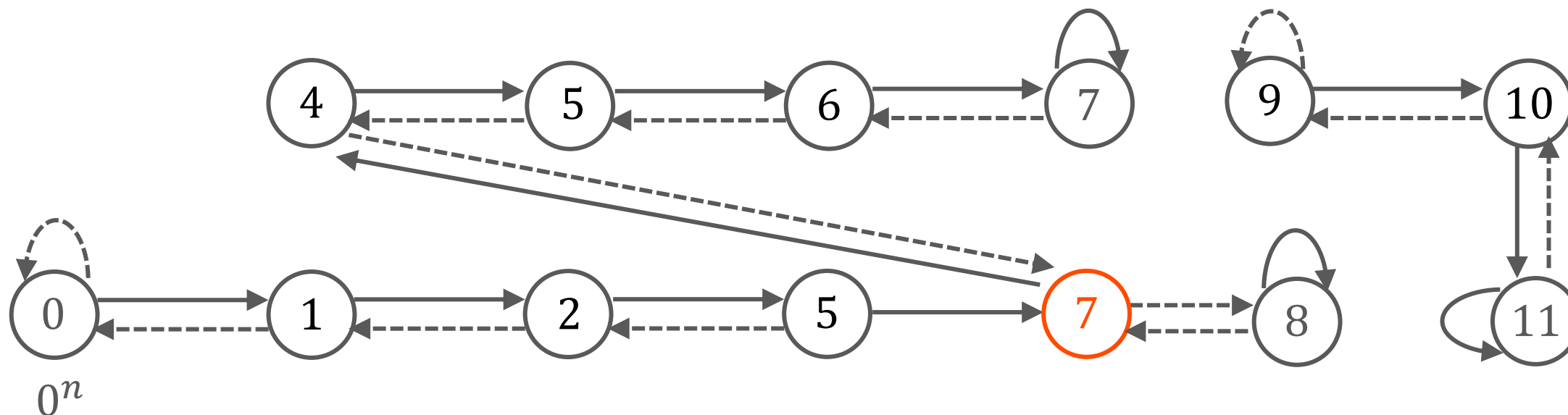
## UIQUE-END-OF-POTENTIAL-LINE (UEOPL)

入力：回路  $P, S: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $P(0^n) = 0^n$ ,  $S(0^n) \neq 0^n$

回路  $V: \{0, 1\}^n \rightarrow \{0, 1, \dots, 2^m - 1\}$  s.t.  $V(0^n) = 0^n$



出力： $\parallel \quad x$  s.t.  $S(x) \neq x$ ,  $P(S(x)) = x$ ,  $V(x) \geq V(S(x))$



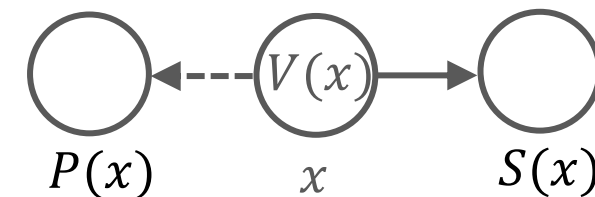
# UEOPL問題[FGMS19]

30

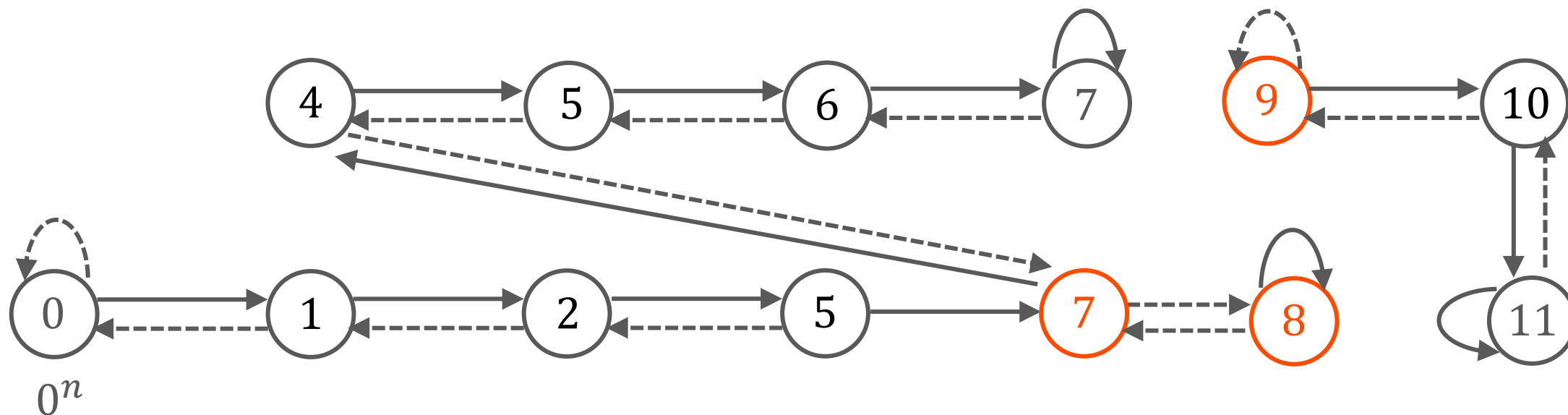
## UIQUE-END-OF-POTENTIAL-LINE (UEOPL)

入力：回路  $P, S: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $P(0^n) = 0^n$ ,  $S(0^n) \neq 0^n$

回路  $V: \{0, 1\}^n \rightarrow \{0, 1, \dots, 2^m - 1\}$  s.t.  $V(0^n) = 0^n$



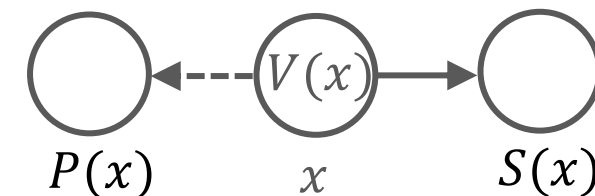
出力：III  $x$  s.t.  $S(P(x)) \neq x$ ,  $x \neq 0^n$



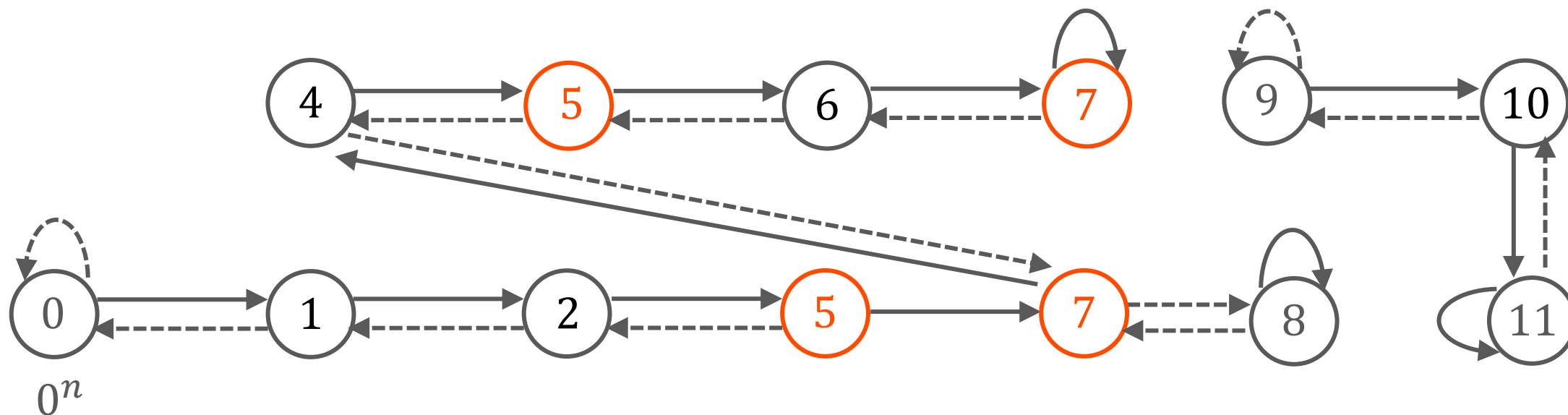
## UIQUE-END-OF-POTENTIAL-LINE (UEOPL)

入力：回路  $P, S: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $P(0^n) = 0^n$ ,  $S(0^n) \neq 0^n$

回路  $V: \{0, 1\}^n \rightarrow \{0, 1, \dots, 2^m - 1\}$  s.t.  $V(0^n) = 0^n$



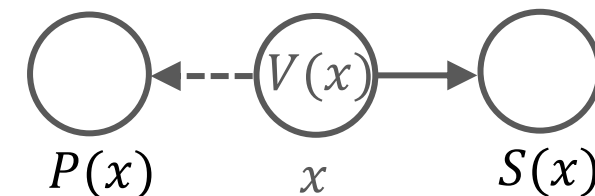
出力：  $\text{IV } (x, y) \text{ s.t. } x \neq y, S(x) \neq x, S(y) \neq y, V(x) = V(y)$



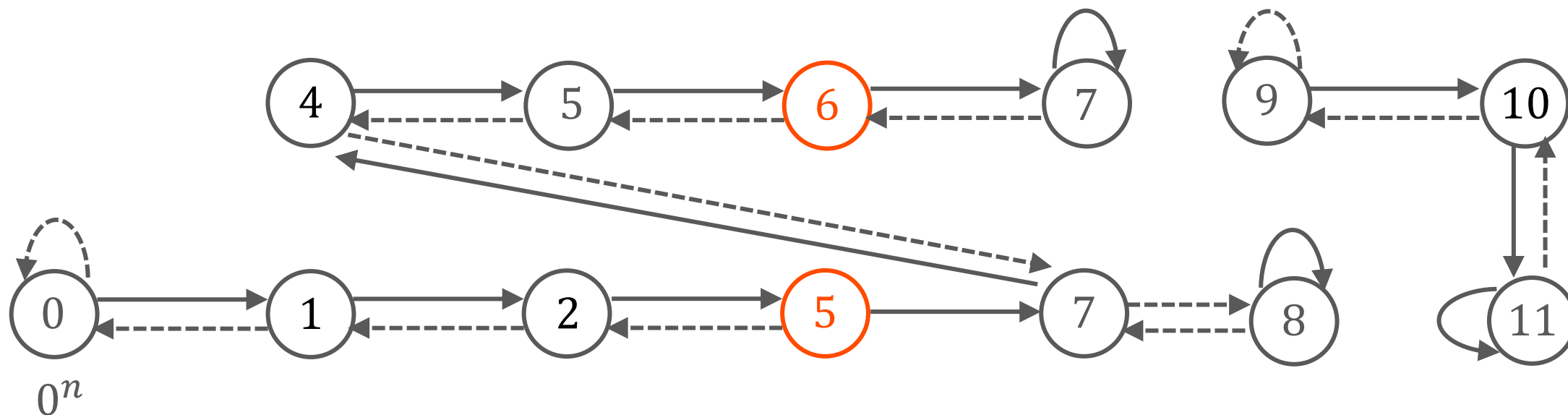
## UIQUE-END-OF-POTENTIAL-LINE (UEOPL)

入力：回路  $P, S: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $P(0^n) = 0^n$ ,  $S(0^n) \neq 0^n$

回路  $V: \{0, 1\}^n \rightarrow \{0, 1, \dots, 2^m - 1\}$  s.t.  $V(0^n) = 0^n$



出力：  $V$   $(x, y)$  s.t.  $x \neq y$ ,  $S(x) \neq x$ ,  $S(y) \neq y$ ,  $V(x) < V(y) < V(S(x))$

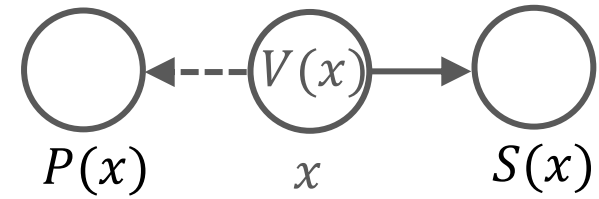




## UIQUE-END-OF-POTENTIAL-LINE (UEOPL)

入力：回路  $P, S: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $P(0^n) = 0^n$ ,  $S(0^n) \neq 0^n$

回路  $V: \{0, 1\}^n \rightarrow \{0, 1, \dots, 2^m - 1\}$  s.t.  $V(0^n) = 0^n$



出力：次のうちいずれかを出力

- I  $x$  s.t.  $P(S(x)) \neq x$
- II  $x$  s.t.  $S(x) \neq x$ ,  $P(S(x)) = x$ ,  $V(x) \geq V(S(x))$
- III  $x$  s.t.  $S(P(x)) \neq x$ ,  $x \neq 0^n$
- IV  $(x, y)$  s.t.  $x \neq y$ ,  $S(x) \neq x$ ,  $S(y) \neq y$ ,  $V(x) = V(y)$
- V  $(x, y)$  s.t.  $x \neq y$ ,  $S(x) \neq x$ ,  $S(y) \neq y$ ,  $V(x) < V(y) < V(S(x))$

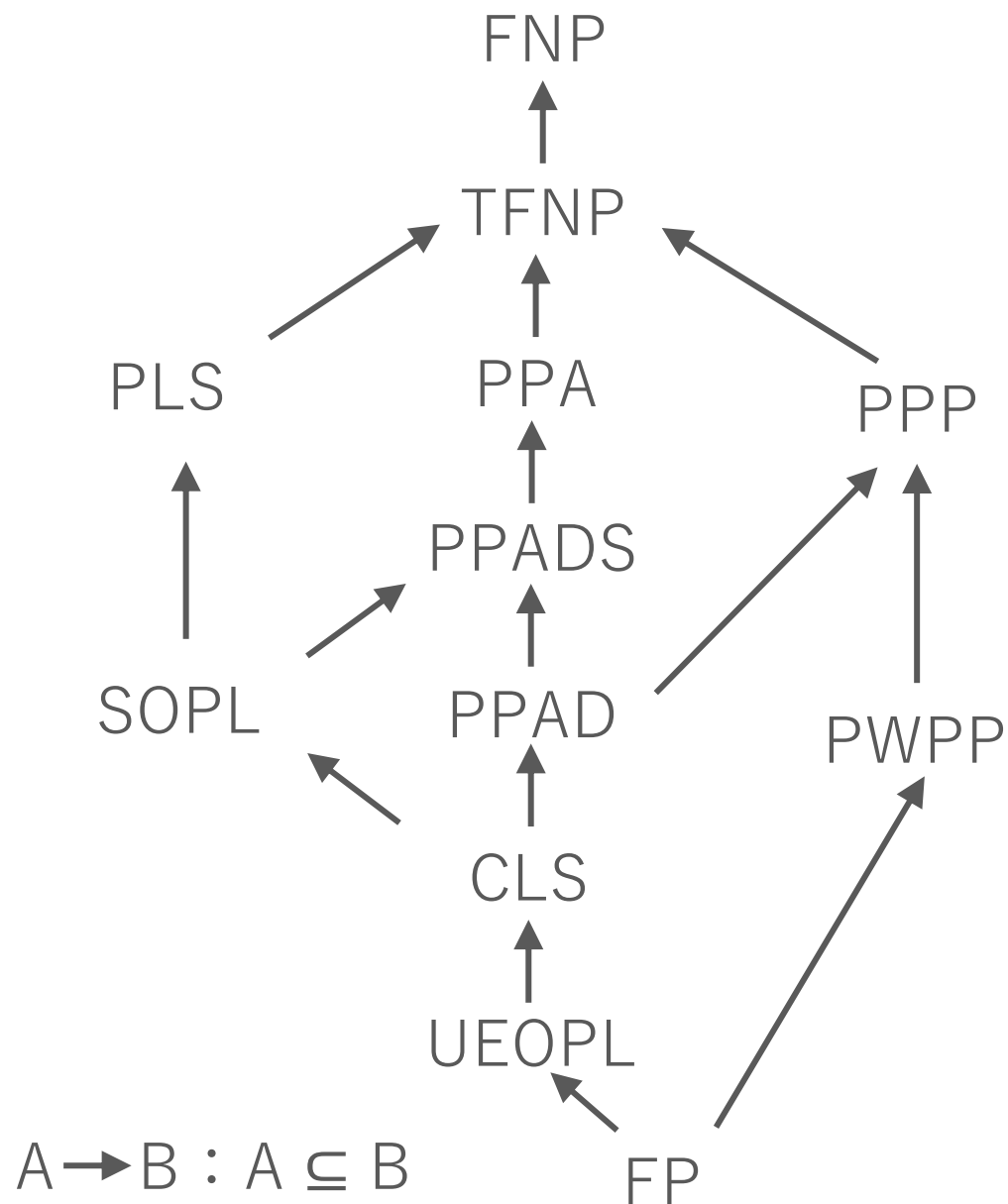
探索問題PがクラスUEOPLに属するとは,

問題PからUEOPL問題への多項式時間帰着が存在する.

# TFNPのサブクラスと 探索版素因数分解問題について

# 素因数分解問題はどのサブクラスに属するか？

35



# 探索版素因数分解問題のバリエーション

## FACTORING $\notin$ TFNP

入力：自然数  $n \geq 2$

出力： $n$ を割り切る非自明な因子  $a$  があれば  $a$  を出力  
そうでないならば "No" を出力

## C-FACTORING $\in$ TFNP

入力：合成数  $n$

出力： $n$ を割り切る非自明な因子  $a$  を出力

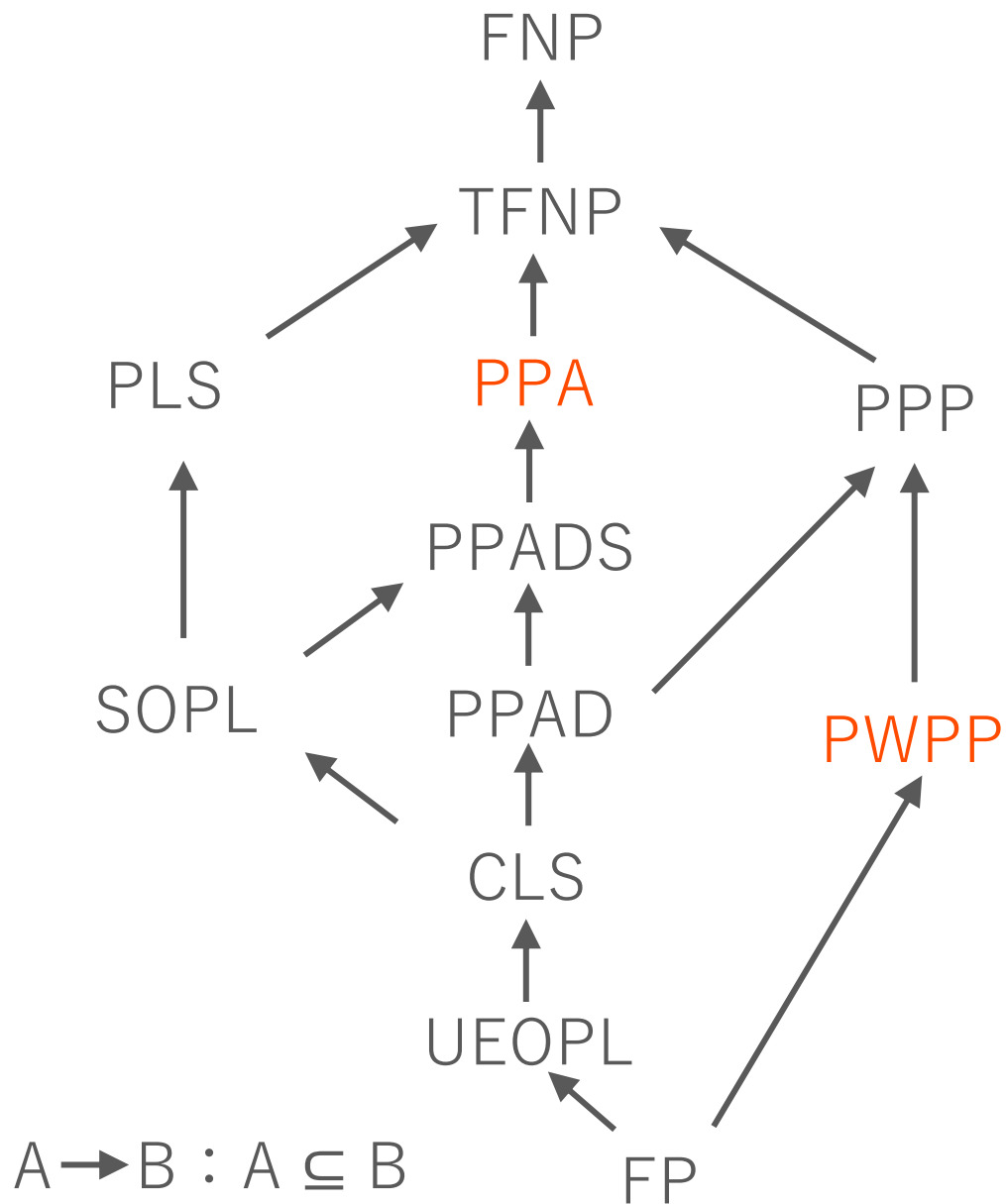
## FULLFAC $\in$ TFNP

入力：自然数  $n \geq 2$

出力： $n$  の素因数分解（因子のリスト）

# 素因数分解問題の計算量クラス

37



[Jer16]

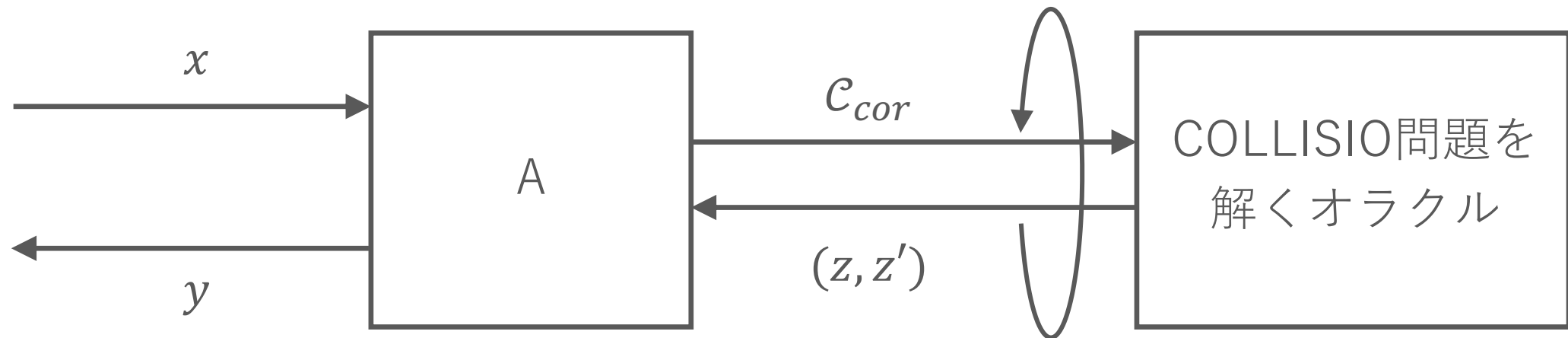
一般化されたリーマン予想GRHのもとで

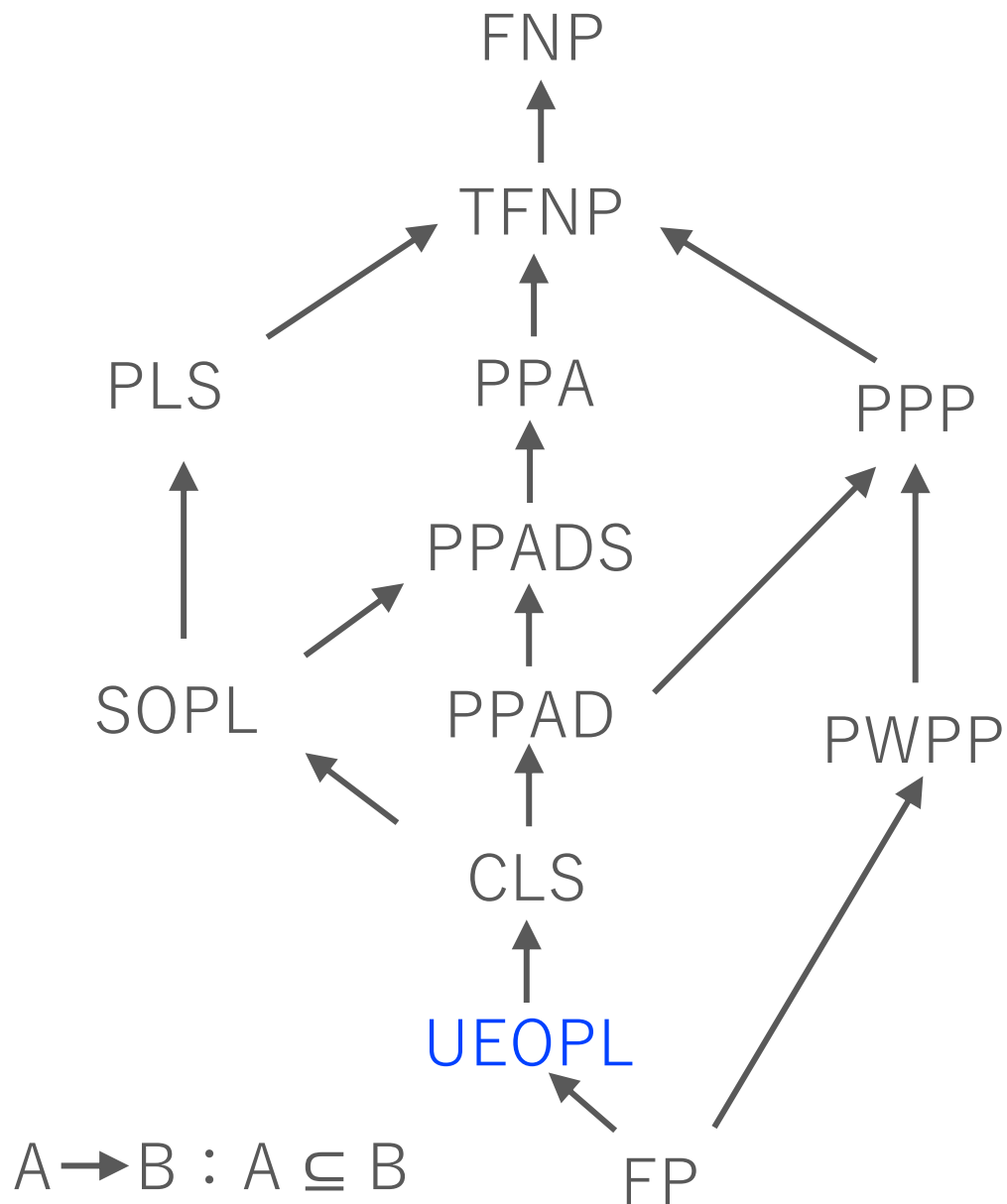
 $C\text{-FACTORING} \in PWPP \cap PPA$  $FULLFAC \in FP^{PWPP}$

探索問題  $P \in \text{FP}^{\text{PWPP}}$  とは、次の条件を満たす  
多項式時間オラクルアルゴリズム  $A$  が存在すること。

条件

オラクルはCOLLISION問題の回路  $\mathcal{C}_{cor}$  を受け取り、  
 $\mathcal{C}_{cor}(z) = \mathcal{C}_{cor}(z')$  かつ  $z \neq z'$  となる  $(z, z')$  を出力する。





[Jer16]

一般化されたリーマン予想GRHのもとで

$C\text{-FACTORING} \in \text{PWPP} \cap \text{PPA}$

$\text{FULLFAC} \in \text{FP}^{\text{PWPP}}$

[HMR23]

$\text{FULLFAC}$ が  
downward self-reducible であれば

$\text{FULLFAC} \in \text{UEOPL}$

※ $\text{FULLFAC}$ が  
downward self-reducibleであるかは未解決

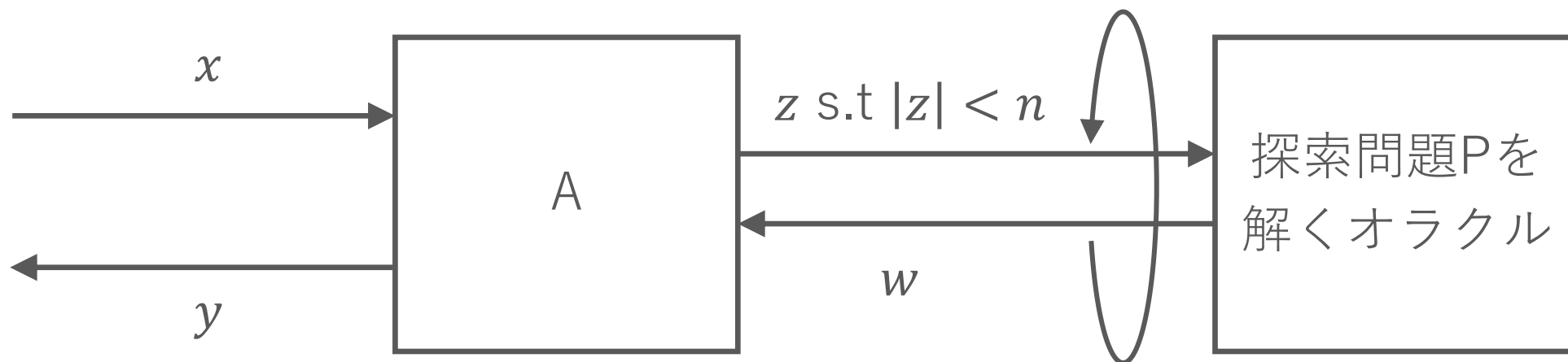
## 補足：Downward Self-Reducible

40

探索問題Pがdownward self-reducibleとは、次の条件を満たす多項式時間オラクルアルゴリズムAが存在すること.

条件

- ① オラクルは探索問題Pを解く.
- ② Aに与えられるインスタンス  $x \in \{0, 1\}^n$  に対し,  
オラクルにクエリできる入力長は  $n$  未満である.





# [HMR23]の結果概要

## クラスTFUP

TFNPの問題で入力  $x$  に対し, 解が唯一つの問題のクラス

## 主な結果

- ① TFNPの問題Pがdownward self-reducibleであれば, その問題PはPLSに属する
- ② TFUPの問題Pがdownward self-reducibleであれば, その問題PはUEOPLに属する

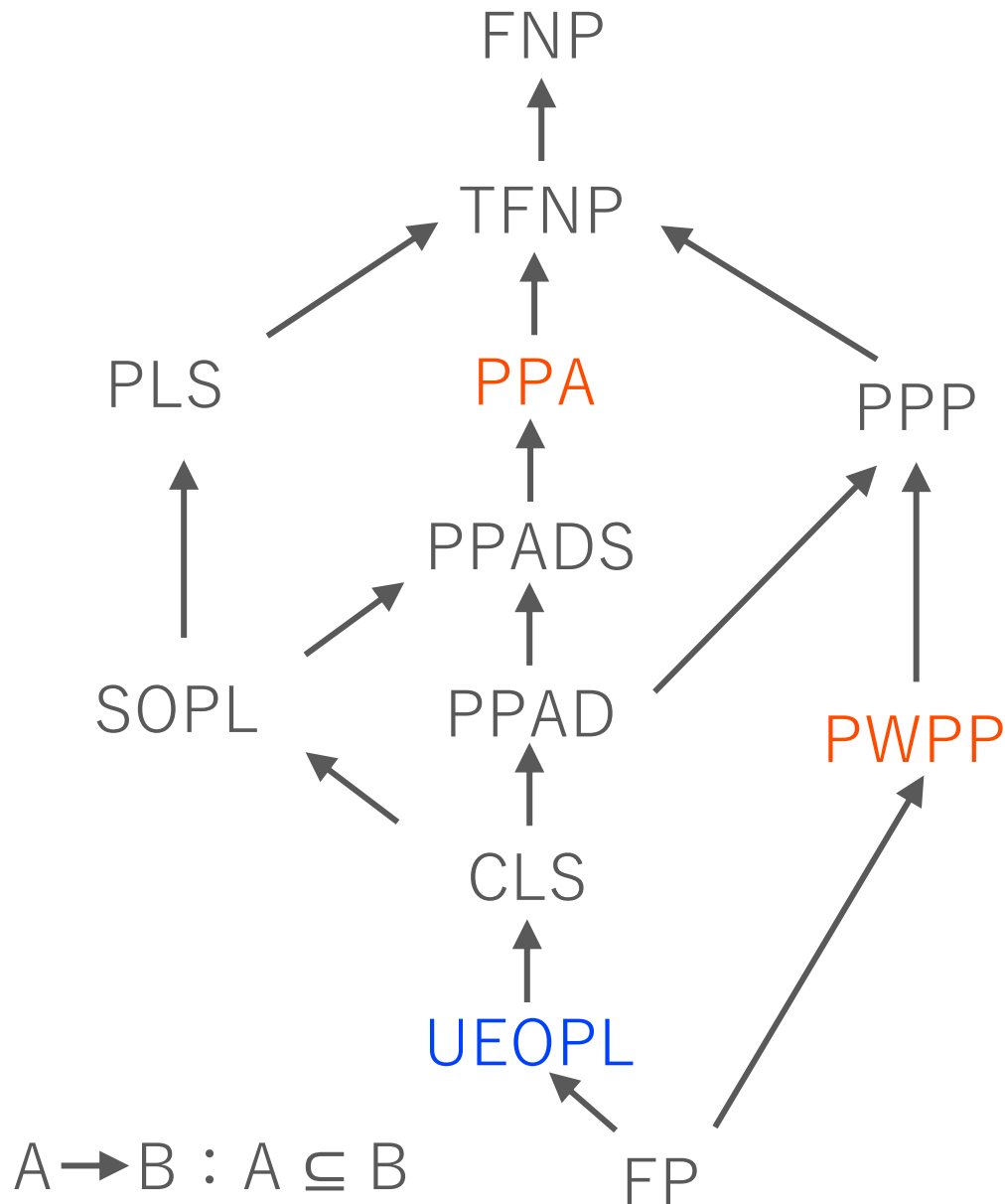


FULLFAC  $\in$  TFUPなので,

FULLFAC がdownward self-reducibleであれば, FULLFAC  $\in$  UEOPLTFUP

# 素因数分解問題の計算量クラス

42



[Jer16]

一般化されたリーマン予想GRHのもとで

 $C\text{-FACTORING} \in PWPPP \cap PPA$  $FULLFAC \in FP^{PWPPP}$ 

[HMR23]

FULLFACが  
downward self-reducible であれば $FULLFAC \in UEOPL$ 

※FULLFACが  
downward self-reducibleであるかは未解決

FACROOTMUL  $\in$  PWPP  
の証明[Jer16]について

C-FACTORING      入力：合成数  $n$   
出力： $n$  の非自明因子

ヤコビ記号  $(a|n)$

WEAKFACROOT    入力：奇数  $n$ ,  $a, b$  s.t.  $(a|n) = 1$ ,  $(b|n) = -1$   
出力： $n$  の非自明因子 or  $a$  の平方根

FACROOTMUL    入力：奇数  $n$ ,  $a, b$  s.t.  $(a|n) = 1$ ,  $(b|n) = -1$   
出力： $n$  の非自明因子 or  $a$  の平方根  
or  $b$  の平方根 or  $ab$  の平方根

FACROOT        入力：奇数  $n$ ,  $a$  s.t.  $(a|n) = 1$   
出力： $n$  の非自明因子 or  $a$  の平方根 $\approx$

## 補足：ルジャンドル記号とヤコビ記号

45

ルジャンドル記号

$p$  : 3以上の素数,  $a$  : 整数

$$(a|p) = \begin{cases} 0 & a = 0 \bmod p \\ 1 & a \neq 0 \bmod p \text{ かつ } x^2 = a \bmod p \text{ となる } x \text{ が存在する} \\ -1 & a \neq 0 \bmod p \text{ かつ } x^2 = a \bmod p \text{ となる } x \text{ が存在しない} \end{cases}$$

ヤコビ記号  $(a|n)$

$$n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_m^{\beta_m}$$

$$(a|n) = \underbrace{(a|p_1)^{\beta_1} \cdot (a|p_2)^{\beta_2} \cdot \dots \cdot (a|p_m)^{\beta_m}}$$

ルジャンドル記号の積

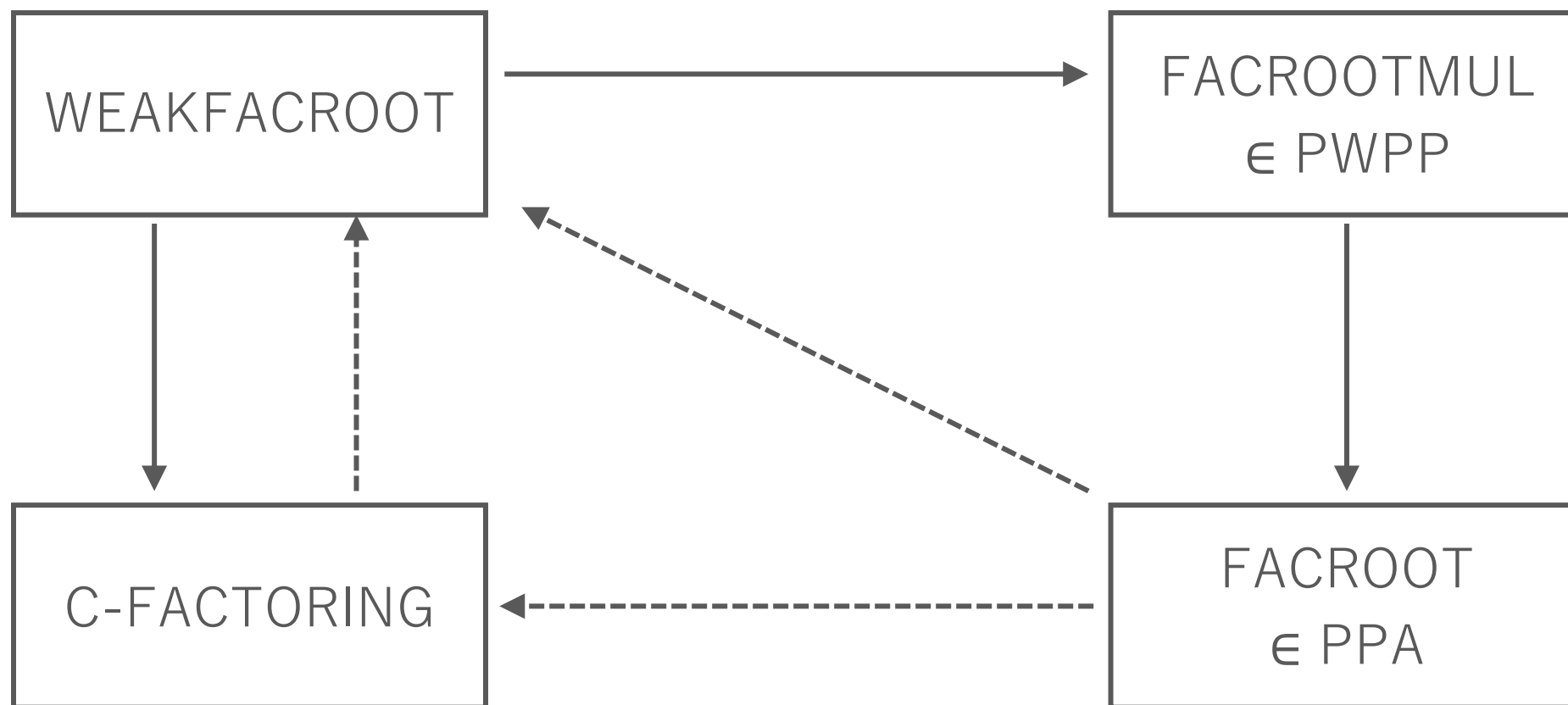
C-FACTORING      入力：合成数  $n$   
出力： $n$  の非自明因子

ヤコビ記号  $(a|n)$

WEAKFACROOT    入力：奇数  $n$ ,  $a, b$  s.t.  $(a|n) = 1$ ,  $(b|n) = -1$   
出力： $n$  の非自明因子 or  $a$  の平方根

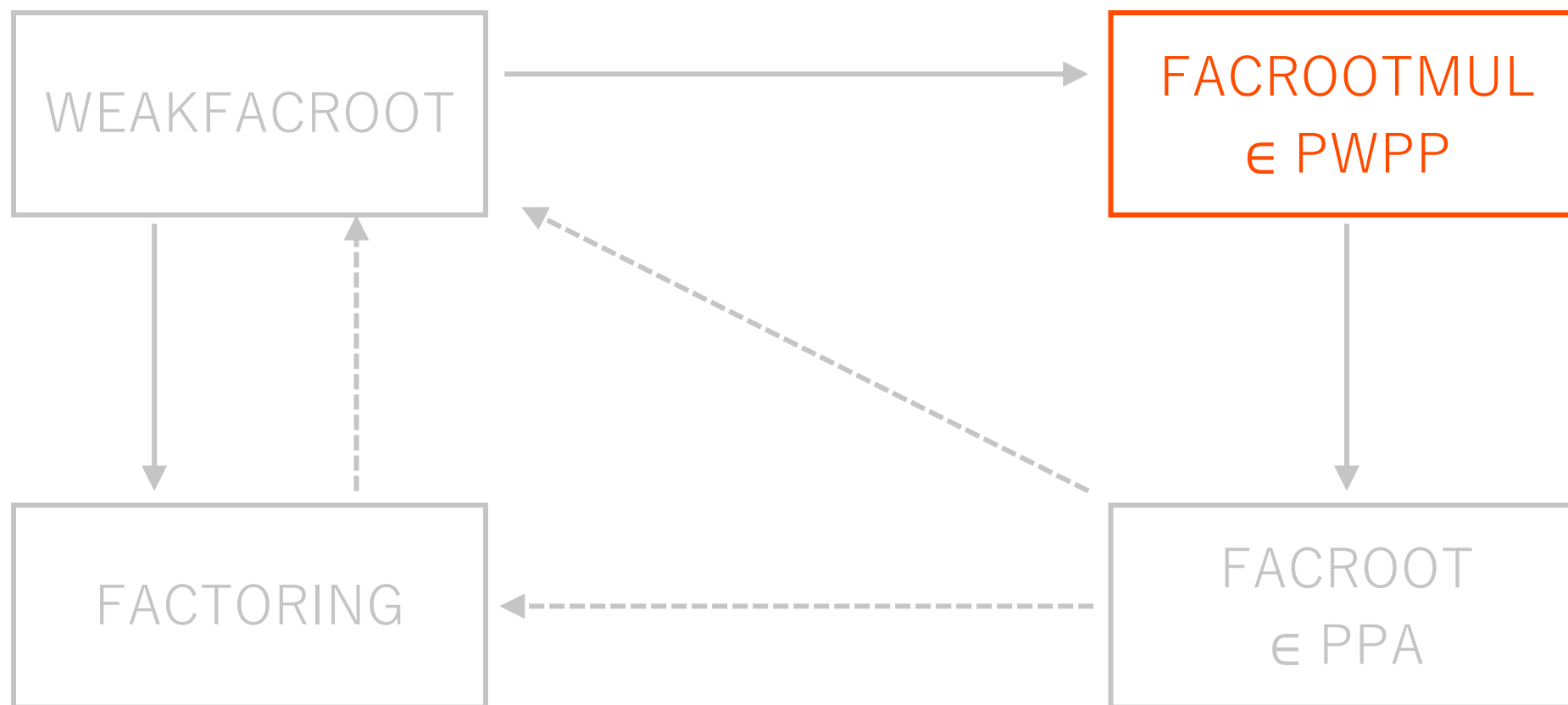
FACROOTMUL    入力：奇数  $n$ ,  $a, b$  s.t.  $(a|n) = 1$ ,  $(b|n) = -1$   
出力： $n$  の非自明因子 or  $a$  の平方根  
or  $b$  の平方根 or  $ab$  の平方根

FACROOT        入力：奇数  $n$ ,  $a$  s.t.  $(a|n) = 1$   
出力： $n$  の非自明因子 or  $a$  の平方根 $\approx$



$A \longrightarrow B$  :  $A$ から $B$ への多項式時間帰着が存在

$A \dashrightarrow B$  :  $A$ から $B$ への多項式時間乱択帰着が存在 (GRHで帰着を脱乱化できる)



$A \longrightarrow B$  :  $A$ から $B$ への多項式時間帰着が存在

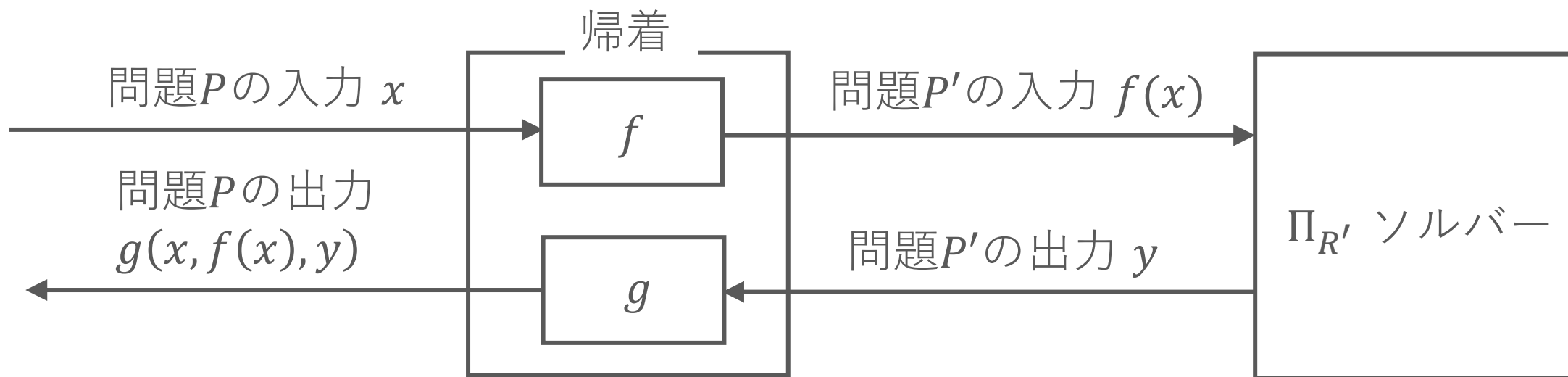
$A \dashrightarrow B$  :  $A$ から $B$ への多項式時間乱択帰着が存在 (GRHで帰着を脱乱化できる)



# TFNPの探索問題における多項式時間帰着

TFNPの探索問題 $P$ からTFNPの探索問題 $P'$ への多項式時間帰着  $(f, g)$  [SSZ18]

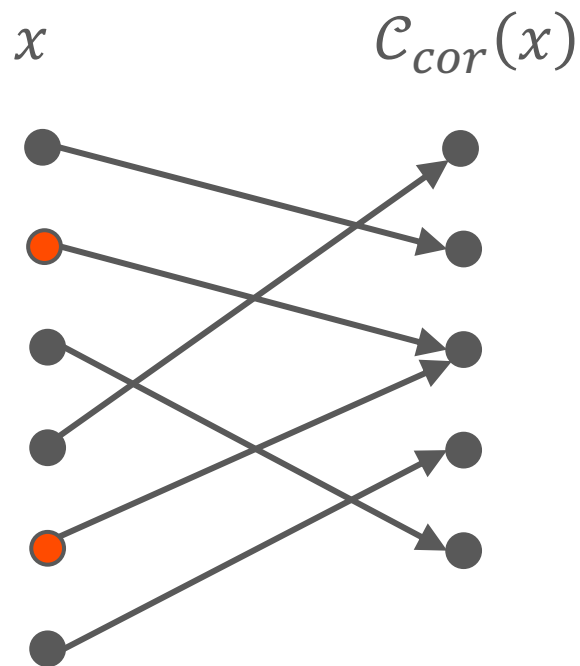
- $f, g$  は多項式時間で計算できる.
- $x$ が探索問題 $P$ の入力なら,  $f(x)$  は探索問題 $P'$ の入力である.
- $y$  が問題 $P'$ の入力  $f(x)$  の解なら,  $g(x, f(x), y)$  は問題 $P$ の入力  $x$ の解である.



# 再掲： COLLISIONとクラスPWPP

50

COLLISION 入力： $n$  入力  $m$  出力回路  $\mathcal{C}_{cor}$  s.t.  $|\mathcal{C}_{cor}| = \text{poly}(n)$ ,  $m < n$   
出力： $(x, x')$  s.t.  $\mathcal{C}_{cor}(x) = \mathcal{C}_{cor}(x')$  かつ  $x \neq x'$



探索問題PがクラスPWPPに属するとは、  
問題Pから COLLISION問題への  
多項式時間帰着が存在する

## FACROOTMUL

入力：奇数  $n$ ,  $a, b$  s.t.  $(a|n) = 1$ ,  $(b|n) = -1$

出力： $n$  の非自明因子 or  $a$  の平方根 or  $b$  の平方根 or  $ab$  の平方根

FACROOTMULの入力  $(n, a, b)$  に対し

関数  $h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1]$  を定義する.

$$h: (i, x) = \begin{cases} x \mod N & \text{if } GCD(n, x) \neq 1 \\ x^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

帰着  $f$  :  $(n, a, b)$  から関数  $h$  を計算する回路  $\mathcal{C}$  を構成し,  $\mathcal{C}$  を出力する.

帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

- $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.
- $i = j$  であれば,  $GCD(n, x - y)$  を出力する.
- $a_0 = 1$ ,  $a_1 = a$ ,  $a_2 = b$  とする.
- $i < j$ ,  $i = 0$  であれば,  $xy^{-1}$  を出力する.
- $i < j$ ,  $i = 1$  であれば,  $axy^{-1}$  を出力する.
- $i > j$  のときも同様(略).

$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1] \quad h: (i, x) = \begin{cases} x \mod N & \text{if } GCD(n, x) \neq 1 \\ x^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

- $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.
- $i = j$  であれば,  $GCD(n, x - y)$  を出力する.
- $a_0 = 1$ ,  $a_1 = a$ ,  $a_2 = b$  とする.
- $i < j$ ,  $i = 0$  であれば,  $xy^{-1}$  を出力する.
- $i < j$ ,  $i = 1$  であれば,  $axy^{-1}$  を出力する.
- $i > j$  のときも同様(略).

$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1] \quad h: (i, x) = \begin{cases} x \mod N & \text{if } GCD(n, x) \neq 1 \\ x^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

•  $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.

•  $i = j$  であれば,  $GCD(n, x - y)$  を出力する.

•  $a_0 = 1$ ,  $a_1 = a$ ,  $a_2 = b$  とする.

$i = j$  より,  $x \neq y$  である.

•  $i < j$ ,  $i = 0$  であれば,  $xy^{-1}$  を出力する.

$i = j = 0$  のとき,  
 $x^2 \bmod N = y^2 \bmod N$  なので  
 $(x + y)(x - y) \bmod N = 0$

•  $i < j$ ,  $i = 1$  であれば,  $axy^{-1}$  を出力する.

•  $i > j$  のときも同様(略).

$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1]$$

$$h: (i, x) = \begin{cases} x \bmod N & \text{if } GCD(n, x) \neq 1 \\ x^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

•  $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.

•  $i = j$  であれば,  $GCD(n, x - y)$  を出力する.

•  $a_0 = 1$ ,  $a_1 = a$ ,  $a_2 = b$  とする.

$i = j$  より,  $x \neq y$  である.

•  $i < j$ ,  $i = 0$  であれば,  $xy^{-1}$  を出力する.

$i = j = 1$  のとき,  
 $ax^2 \bmod N = ay^2 \bmod N$  なので  
 $(x + y)(x - y) \bmod N = 0$

•  $i < j$ ,  $i = 1$  であれば,  $axy^{-1}$  を出力する.

•  $i > j$  のときも同様(略).

$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1]$$

$$h: (i, x) = \begin{cases} x \bmod N & \text{if } GCD(n, x) \neq 1 \\ x^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

•  $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.

•  $i = j$  であれば,  $GCD(n, x - y)$  を出力する.

•  $a_0 = 1$ ,  $a_1 = a$ ,  $a_2 = b$  とする.

$i = j$  より,  $x \neq y$  である.

•  $i < j$ ,  $i = 0$  であれば,  $xy^{-1}$  を出力する.

$i = j = 2$  のとき,

$bx^2 \bmod N = by^2 \bmod N$  なので  
 $(x + y)(x - y) \bmod N = 0$

•  $i < j$ ,  $i = 1$  であれば,  $axy^{-1}$  を出力する.

•  $i > j$  のときも同様(略).

$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1]$$

$$h: (i, x) = \begin{cases} x \bmod N & \text{if } GCD(n, x) \neq 1 \\ x^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 \bmod N & \text{if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$



帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

•  $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.

•  $i = j$  であれば,  $GCD(n, x - y)$  を出力する.

•  $a_0 = 1, a_1 = a, a_2 = b$  とする.

•  $i < j, i = 0$  であれば,  $xy^{-1}$  を出力する.

•  $i < j, i = 1$  であれば,  $axy^{-1}$  を出力する.

•  $i > j$  のときも同様(略).

$$a_0 x^2 \bmod N = a_j y^2 \bmod N \text{ より}$$

$$a_j = (xy^{-1})^2 \bmod N$$

$xy^{-1}$  は  $a$  or  $b$  の平方根

$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1]$$

$$h: (i, x) = \begin{cases} x & \bmod N \text{ if } GCD(n, x) \neq 1 \\ x^2 & \bmod N \text{ if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 & \bmod N \text{ if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 & \bmod N \text{ if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

•  $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.

•  $i = j$  であれば,  $GCD(n, x - y)$  を出力する.

•  $a_0 = 1$ ,  $a_1 = a$ ,  $a_2 = b$  とする.

•  $i < j$ ,  $i = 0$  であれば,  $xy^{-1}$  を出力する.

•  $i < j$ ,  $i = 1$  であれば,  $axy^{-1}$  を出力する.

•  $i > j$  のときも同様(略).

$$a_i x^2 \bmod N = a_j y^2 \bmod N \text{ より} \\ ba^{-1} = (xy^{-1})^2 \bmod N$$

$$ba^{-1}a^2 = (axy^{-1})^2 \text{ より} \\ axy^{-1} \text{ は } ab \text{ の平方根}$$

$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \\ \rightarrow [1, n-1]$$

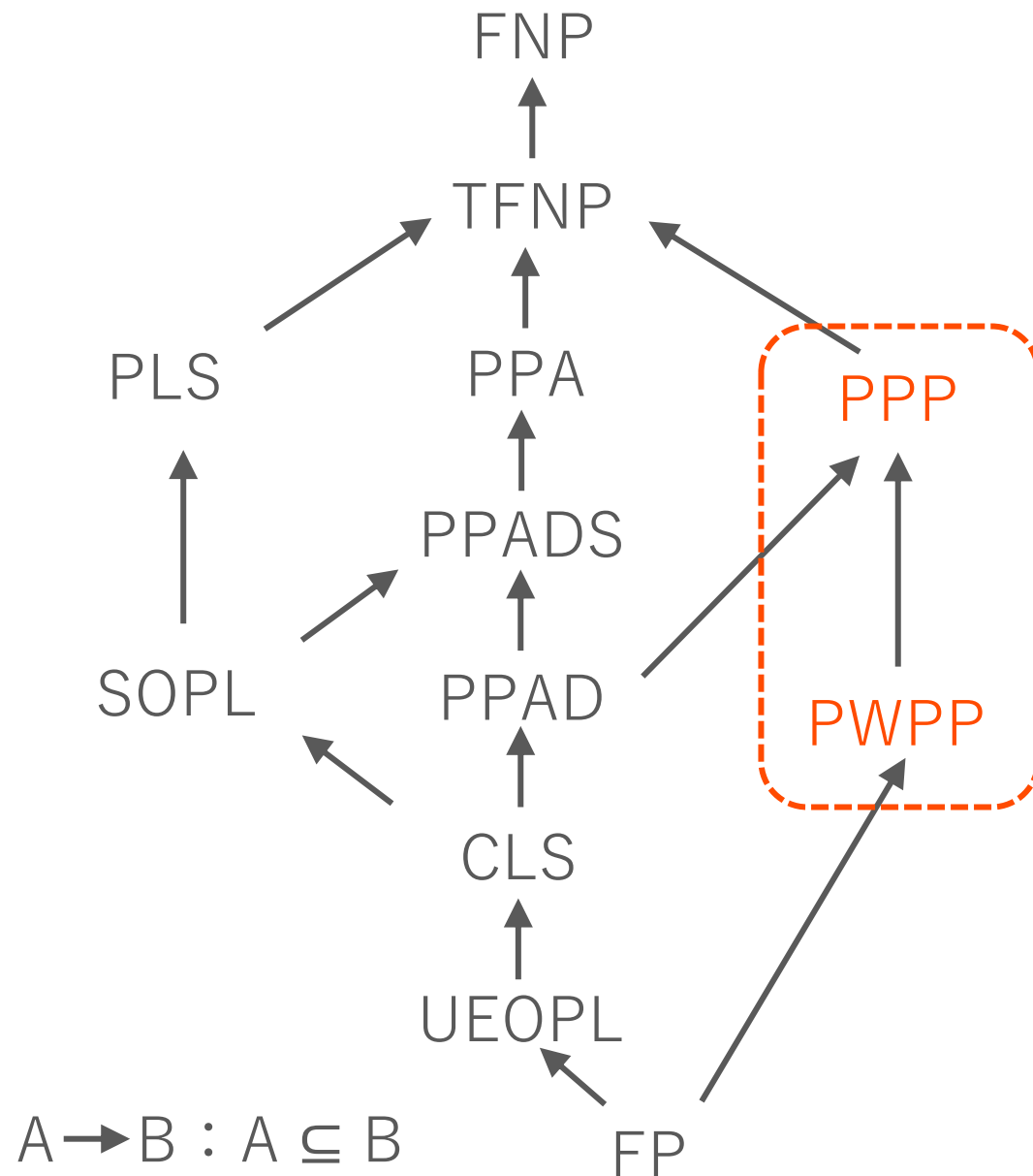
$$h: (i, x) = \begin{cases} x & \bmod N \text{ if } GCD(n, x) \neq 1 \\ x^2 & \bmod N \text{ if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 & \bmod N \text{ if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 & \bmod N \text{ if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

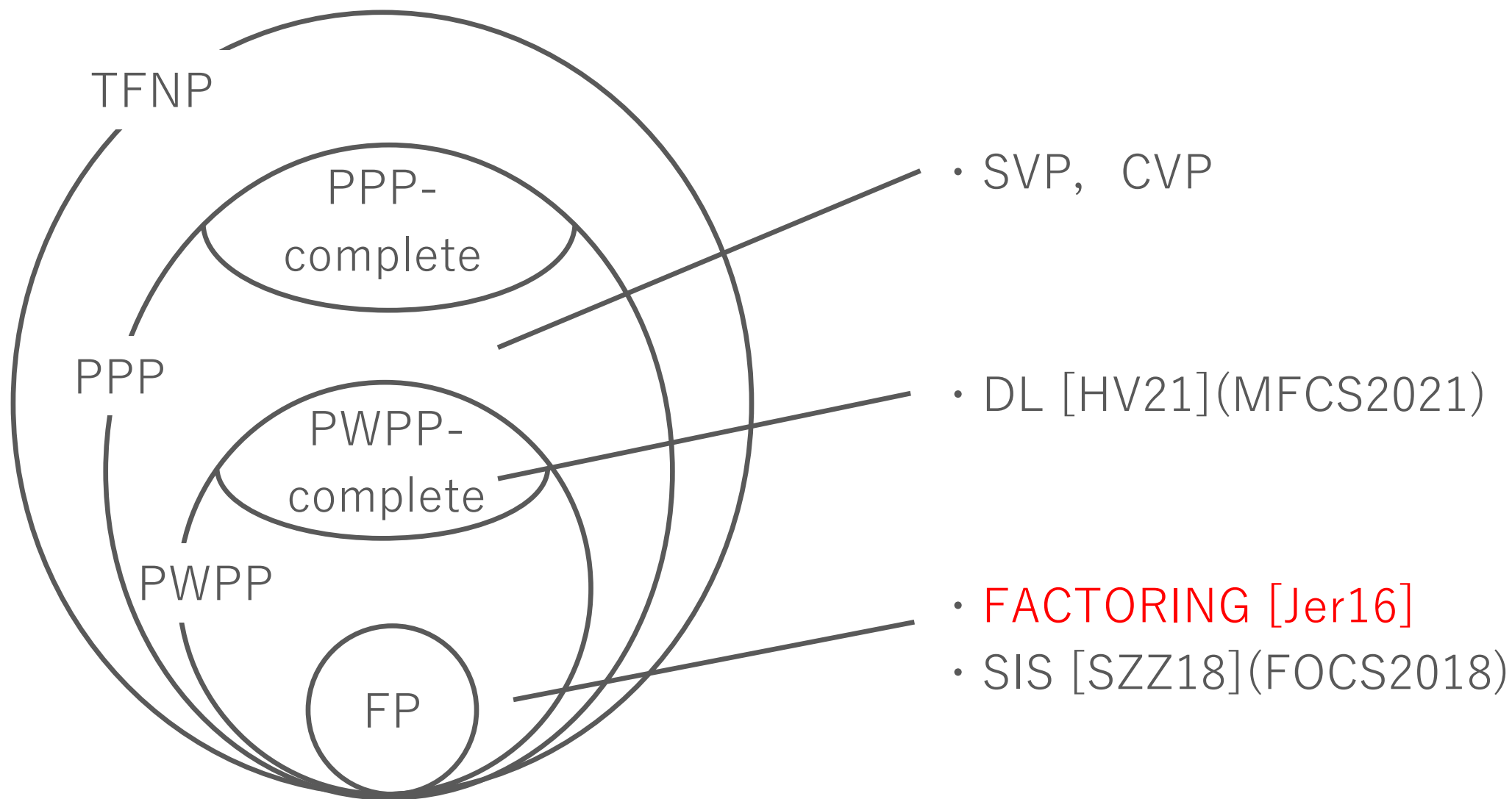
帰着  $g$  : 回路  $\mathcal{C}$  に対する solution  $((i, x), (j, y))$  s.t.  $(i, x) \neq (j, y)$  に対し,

- $GCD(n, x) \neq 1$  なら  $GCD(n, x)$ ,  $GCD(n, y) \neq 1$  なら  $GCD(n, y)$  を出力する.
- $i = j$  であれば,  $GCD(n, x - y)$  を出力する.
- $a_0 = 1$ ,  $a_1 = a$ ,  $a_2 = b$  とする.
- $i < j$ ,  $i = 0$  であれば,  $xy^{-1}$  を出力する.
- $i < j$ ,  $i = 1$  であれば,  $axy^{-1}$  を出力する.
- $i > j$  のときも同様(略).

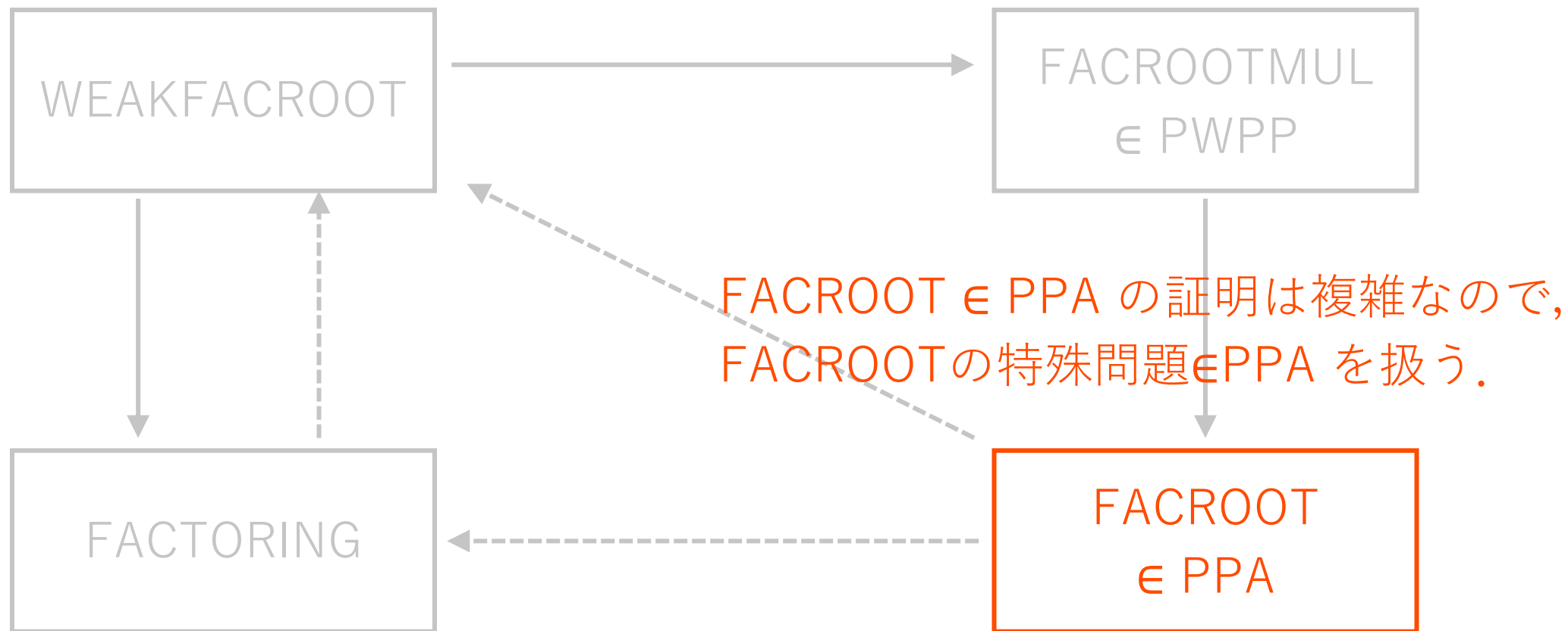
$$h: \{0, 1, 2\} \times \left[1, \frac{n-1}{2}\right] \rightarrow [1, n-1] \quad h: (i, x) = \begin{cases} x \mod N & \text{if } GCD(n, x) \neq 1 \\ x^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 0 \\ ax^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 1 \\ bx^2 \mod N & \text{if } GCD(n, x) = 1 \wedge i = 2 \end{cases}$$

# 暗号に関する探索問題と クラスPPP, PWPP





FACROOT  $\in$  PPAの証明[Jer16]について



$A \longrightarrow B$  :  $A$  から  $B$  への多項式時間帰着が存在

$A \dashrightarrow B$  :  $A$  から  $B$  への多項式時間乱択帰着が存在 (GRHで帰着を脱乱化できる)



# 再掲： LONELY問題[BCE+95]とクラスPPA[Pap94]

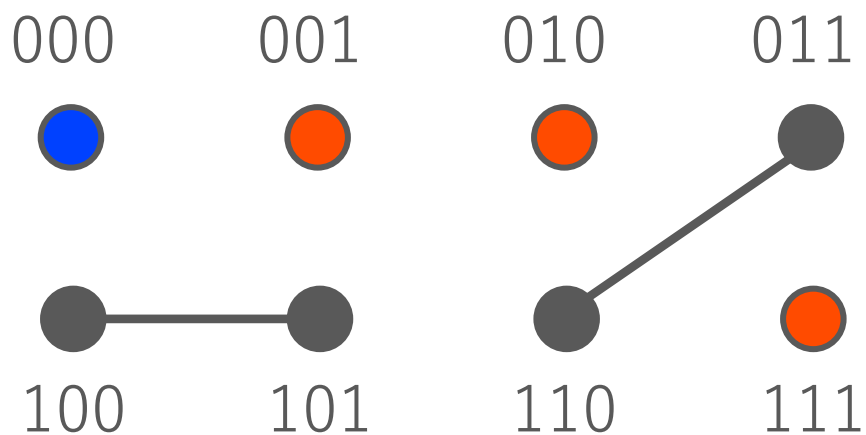
65

LONELY 入力：無向グラフ  $G = (V, E)$  を表す回路  $\mathcal{C}_{lon}: \{0, 1\}^n \rightarrow \{0, 1\}^n$ ,

$$|\mathcal{C}_{lon}| = \text{poly}(n), V = \{0, 1\}^n \setminus \{0^n\},$$

$$(u, v) \in E \text{ iff } u \neq v \wedge \mathcal{C}_{lon}(u) = v \wedge \mathcal{C}_{lon}(v) = u$$

出力：  $0^n$  以外のマッチングがない頂点



頂点100 と101 はマッチする

頂点101 と101 はマッチしない

頂点101 がない.

$$\mathcal{C}_{lon}(100) = 101, \mathcal{C}_{lon}(101) = 100$$

$$\mathcal{C}_{lon}(001) = 101, \mathcal{C}_{lon}(111) = 111$$

探索問題PがクラスPPAに属するとは,

問題PからLONELY問題への  
多項式時間帰着が存在する.

FACROOT<sub>a</sub>      入力：奇数  $n$ ,  $a$  s.t.  $(a|n) = 1$   
出力： $n$  の非自明因子 or  $a$  の平方根

以降は証明のための準備

$(\mathbb{Z}/n\mathbb{Z})^*$  の要素を  $N = \{x \mid |x| < n/2, \text{GCD}(n, x) = 1\}$

で一意に表現する.

$$N^+ = \{x \in N \mid x > 0\}, \quad N^- = \{x \in N \mid x < 0\}, \quad N_0 = N^+ \cup \{0\}$$

## 準備：対合写像 $s_{n,a}$

写像  $f: X \rightarrow Y$  が対合写像とは,

$$\forall x \in X \text{ に対し, } f(f(x)) = x \text{ が成り立つ.}$$

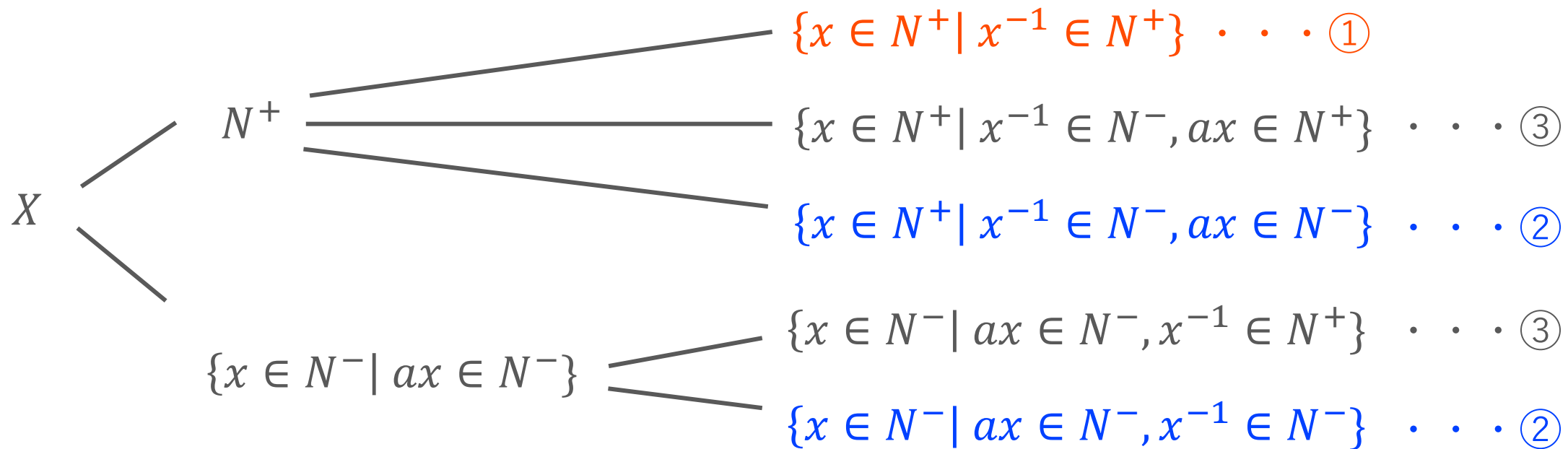
次の対合写像  $s_{n,a}(x)$   $X = \{x \in N^- \mid ax \in N^-\} \cup N^+$  を考える.

$$s_{n,a}(x) = \begin{cases} x^{-1} & x, x^{-1} \in N^+ \\ a^{-1}x^{-1} & ax, x^{-1} \in N^- \\ -x & (x, ax \in N^+ \wedge x^{-1} \in N^-) \vee (x, ax \in N^- \wedge x^{-1} \in N^+) \end{cases}$$

# 準備：対合写像 $s_{n,a}$

$$s_{n,a}(x) = \begin{cases} x^{-1} & \textcolor{red}{x, x^{-1} \in N^+} \cdots \textcircled{1} \\ a^{-1}x^{-1} & \textcolor{blue}{ax, x^{-1} \in N^-} \cdots \textcircled{2} \\ -x & (x, ax \in N^+ \wedge x^{-1} \in N^-) \vee (x, ax \in N^- \wedge x^{-1} \in N^+) \cdots \textcircled{3} \end{cases}$$

$X = \{x \in N^- \mid ax \in N^-\} \cup N^+$  は  $s_{n,a}$  によって3つに分割される.



## 準備：対合写像 $s_{n,a}$ の不動点

$$s_{n,a}(x) = \begin{cases} x^{-1} & \textcolor{red}{x, x^{-1} \in N^+} \cdots \textcircled{1} \\ a^{-1}x^{-1} & \textcolor{blue}{ax, x^{-1} \in N^-} \cdots \textcircled{2} \\ -x & (x, ax \in N^+ \wedge x^{-1} \in N^-) \vee (x, ax \in N^- \wedge x^{-1} \in N^+) \cdots \textcircled{3} \end{cases}$$

$s_{n,a}(x)$  の不動点  $x_{fix}$  は次の(1), (2)のうちどちらかの条件を満たす.

(1)  $\textcolor{red}{x_{fix} \in N^+ \setminus \{1\} \wedge x_{fix}^2 = 1}$       ① のときに対応する不動点

(2)  $\textcolor{blue}{x_{fix} \in N^- \wedge x_{fix}^2 = a^{-1}}$       ② のときに対応する不動点

③のときに対応する不動点は存在しない.

## 準備：対合写像 $t_{n,a}$

$s(x)$  の定義域は  $X = \{x \in N^- \mid ax \in N^-\} \cup N^+$

$t_{n,a}(x)$  を修正して，定義域が  $X \cup \{0\}$  の対合写像  $f_{n,a}(x)$  を構成する．

$$t_{n,a}(x) = \begin{cases} 1 & x = 0 \\ 0 & x = 1 \\ t_{n,a}(x) & x \neq 0, 1 \end{cases}$$

この関数を  $\text{FACROOT}_a$  から  $\text{LONELY}$  への帰着で用いる．

FACROOT2      入力：奇数  $n$ , s.t.  $(2|n) = 1$   
出力： $n$  の非自明因子 or  $a$  の平方根

平方剰余の法則

$$(2|n) = \begin{cases} 1 & n = \pm 1 \pmod{8} \\ -1 & n = \pm 3 \pmod{8} \end{cases}$$

以降  $n = \pm 1 \pmod{8}$  として考える.

$$n = \pm 1 \pmod{8}$$

$$(\mathbb{Z}/n\mathbb{Z})^* \text{ の要素を } N = \{x \mid |x| < n/2, \text{GCD}(n, x) = 1\}$$

$$N^+ = \{x \in N \mid x > 0\}, \quad N^- = \{x \in N \mid x < 0\}, \quad N_0 = N^+ \cup \{0\}$$

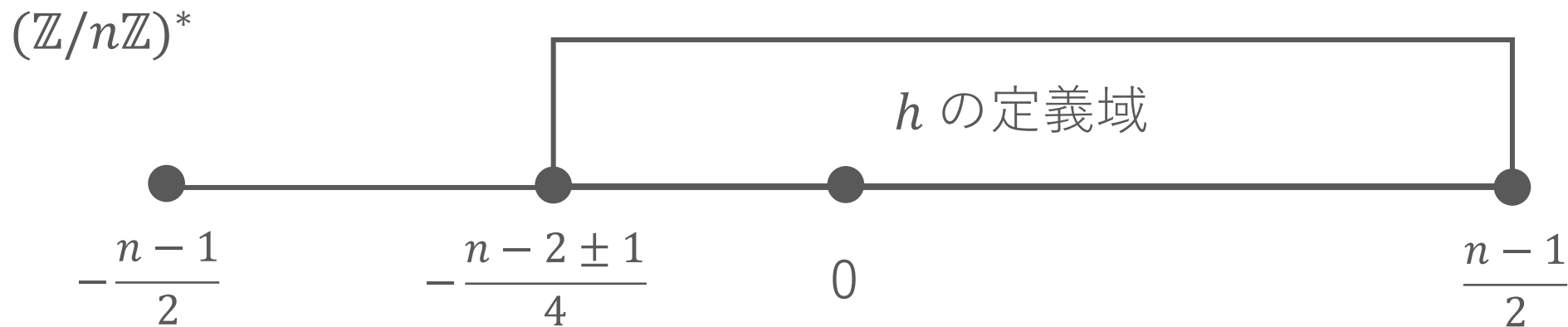
$$\{x \in N^- \mid 2x \in N^-\} = N \cap \left[ -\frac{n-2 \pm 1}{4}, \frac{n-1}{2} \right]$$

定義域が  $\left[ -\frac{n-2 \pm 1}{4}, \frac{n-1}{2} \right]$  の対合写像 $h(x)$ を次のように構成する.

$$h(x) = \begin{cases} x & x \neq 0 \wedge \text{GCD}(n, x) \neq 1 \\ f_{n,2}(x) & \text{Othwise} \end{cases}$$



$$h(x) = \begin{cases} x & x \neq 0 \wedge \text{GCD}(n, x) \neq 1 \\ f_{n,2}(x) & \text{Othrwise} \end{cases} \quad x \in \left[ -\frac{n-2\pm 1}{4}, \frac{n-1}{2} \right]$$



$h(x)$  の不動点  $x_{fix}$  は次の(1), (2), (3)のうちどちらかの条件を満たす.

$$h(x) = \begin{cases} x & x \neq 0 \wedge GCD(n, x) \neq 1 \cdots \textcircled{1} \\ t_{n,2}(x) & \text{Othrwise} \cdots \textcircled{2} \end{cases}$$

(1)  $x_{fix} \neq 0 \wedge GCD(n, x_{fix}) \neq 1$       ① のときに対応する不動点

(2)  $x_{fix} \in N^+ \setminus \{1\} \wedge x_{fix}^2 = 1$       ② のときに対応する不動点

(3)  $x_{fix} \in N^- \wedge x_{fix}^2 = 2^{-1}$       ② のときに対応する不動点

(1)または(2)の不動点が計算できれば $n$ の非自明因子が得られる.

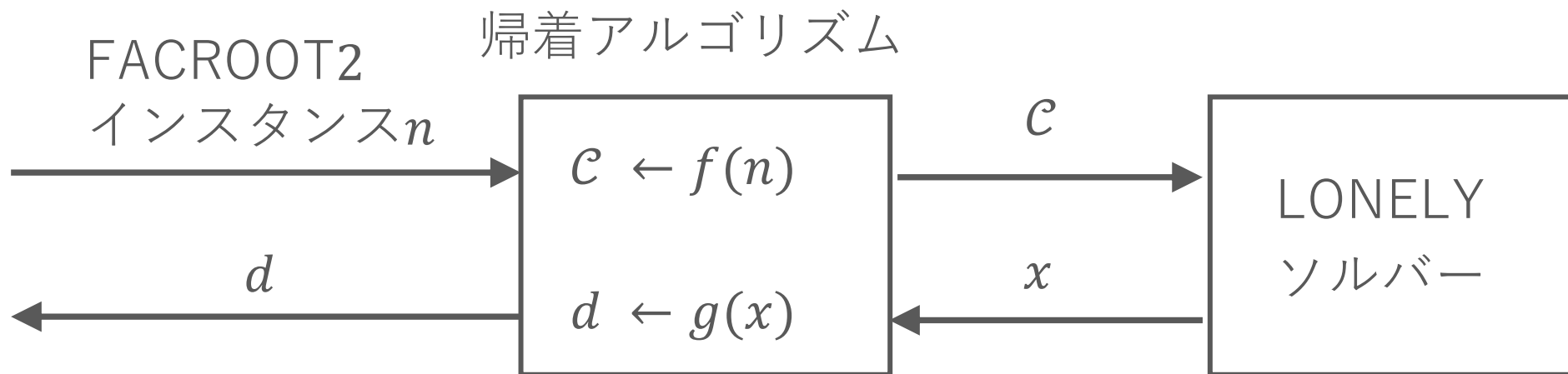
(3)の不動点が計算できれば,  $a = 2$  の平方根が得られる.

$h$ の不動点が計算できれば FACROOT2が解ける！

帰着  $f$  : 奇数  $n$  から関数  $h$  を計算する回路  $\mathcal{C}$  を出力する.

帰着  $g$  :  $x$  が不動点が (1) または (2) のタイプなら  
 $n$  の非自明因子を計算し出力する.

$x$  が不動点が (3) のタイプなら 2 の平方根を計算し出力する.



LONELYソルバーの出力が不動点であることを確認する必要あり.

$h(x)$  の定義域は  $\left[-\frac{n-2\pm 1}{4}, \frac{n-1}{2}\right]$ ,  $n = \pm 1 \pmod{8}$  であることに着目すると,

この区間に含まれる整数  $(3n \pm 1)/4$  個で奇数個.

さらに  $h(x)$  対合写像なので, マッチングがない点は  $h$  の不動点である.

FACROOT  $\in$  PPA の証明についても

帰着  $f$  は対合写像を構成し, 帰着  $g$  でその写像の不動点を解へ変換する.

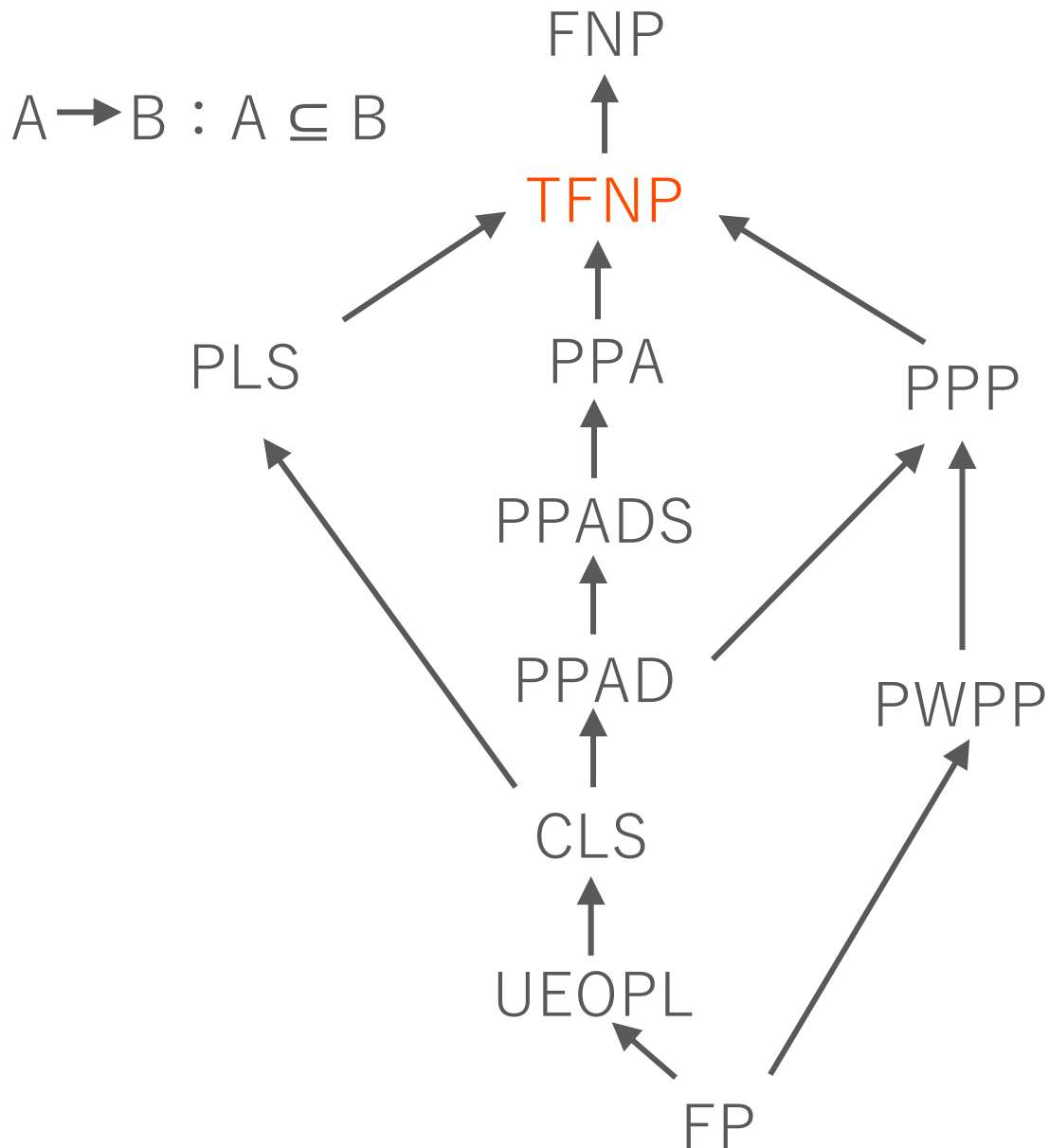
FACROOT では帰着  $f$  が構成する対合写像の構造は複雑である.

詳しい証明は [Jer16] を参照のこと.

# TNFPの困難性と暗号技術について

# TFNPに困難な問題が存在することの証明について

78



TNFPに解くことが難しい問題が存在することをどの仮定から証明できる？

[HNY17]

NPに平均ケースで解くことが難しい言語が存在 (Pessilandの世界)



TFNPに平均ケースで解くことが難しい問題が存在

# TFNPに困難な問題が存在することの証明について

79

Impagliazzoの5つの世界[Imp95]

Cryptomania：公開鍵暗号が存在する世界

Minicrypt：公開鍵暗号が存在しないが  
一方向性関数が存在する世界

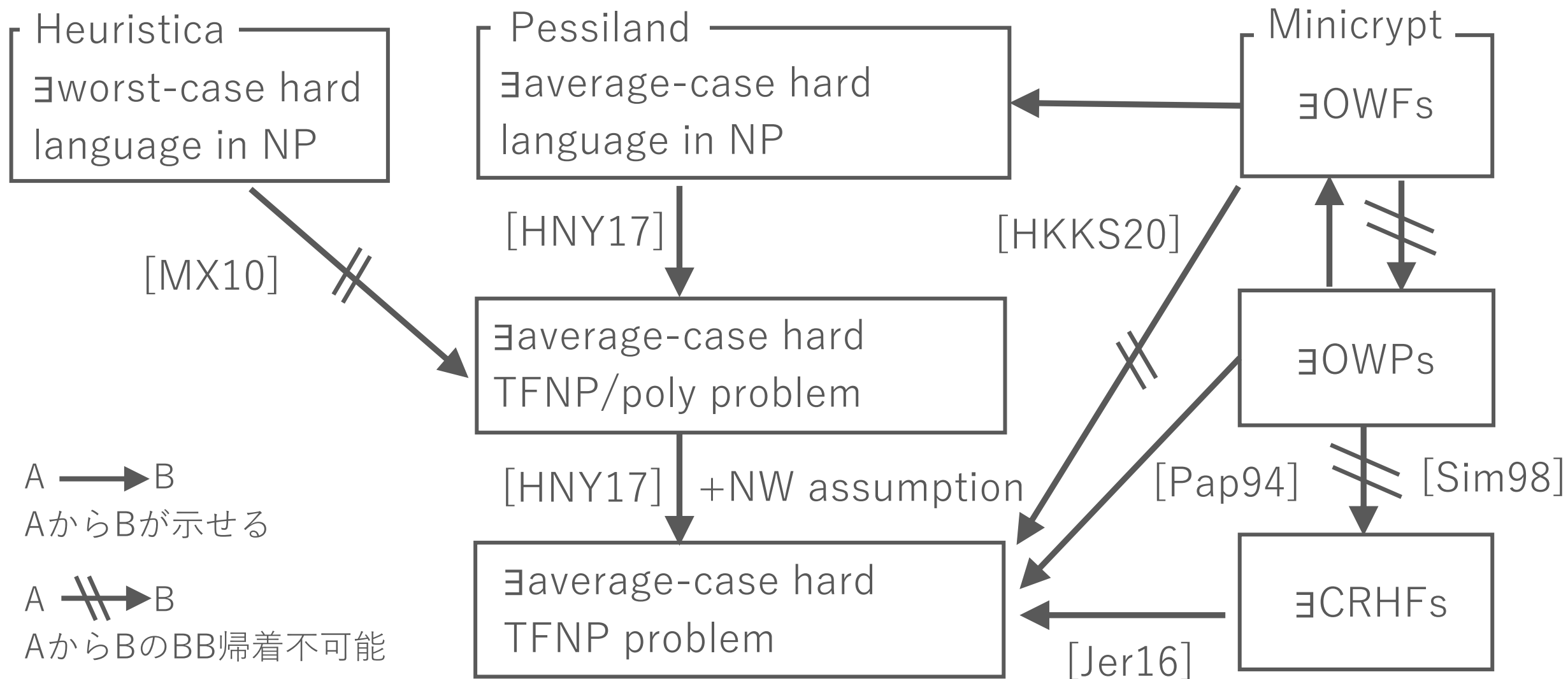
Pessiland：一方向性関数が存在しないが  
平均ケースで困難なNP言語が存在する世界

Heuristica：平均ケースで困難なNP言語が存在しないが  
 $P \neq NP$ が成り立つ世界

Algorithmica： $P = NP$ が成り立つ世界

# TFNPに困難な問題が存在することの証明について

80





# TFNPの困難性を用いて暗号技術は構成可能か？

TFNPから一方向性関数は構成可能か？

TFNPの平均ケース困難性を用いても  
一方向性関数をブラックボックス構成できない.

PPADの困難性(TFNPの困難性より強い仮定)から一方向性関数は構成可能か？

PPADの平均ケース困難性を用いても  
一方向性関数をブラックボックス構成できない. [RSS17]

暗号とTFNPに特化した講義（本スライド作成時にも参考にしました。）

COMS E6261: Advanced Cryptography Spring 2024: Cryptography  $\cap$  TFNP  
<https://dmitropolsky.github.io/teaching/6261/>

FNPの上位クラスPEPPに関連する話題

明示的構成の計算量と値域回避問題

Complexity of Explicit Constructions and Range Avoidance Problems  
[https://tcc.c.titech.ac.jp/yasunaga/talks/rangeavoidance\\_IMI202208.pdf](https://tcc.c.titech.ac.jp/yasunaga/talks/rangeavoidance_IMI202208.pdf)

- [BCE+95] Paul Beame, Stephen A. Cook, Jeff Edmonds, Russell Impagliazzo, Toniann Pitassi. The relative complexity of NP search problems (STOC1995).
- [BHZ87] Ravi B. Boppana, Johan Hastad, Stathis Zachos. Does co-NP Have Short Interactive Proofs? (Inf. Process. Lett. 1987).
- [DP11] Constantinos Daskalakis, Christos H. Papadimitriou. Continuous Local Search (SODA2011).
- [FGHS21] John Fearnley, Paul W. Goldberg, Alexandros Hollender, Rahul Savani. The complexity of gradient descent:  $\text{CLS} = \text{PPAD}_{\text{n}}\text{PLS}$  (STOC2021).
- [FGMS19] John Fearnley, Spencer Gordon, Ruta Mehta, Rahul Savani. Unique End of Potential Line. (ICALP2019)
- [GHJ+22] Mika Goos, Alexandros Hollender, Siddhartha Jain, Gilbert Maystre, William Pires, Robert Robere, Ran Tao. Further Collapses in TFNP (CCC22).
- [GKRS19] Mika Goos, Pritish Kamath, Robert Robere, Dmitry Sokolov. Adventures in Monotone Complexity and TFNP (ITCS2019).
- [HKKS20] Pavel Hubacek, Chethan Kamath, Karel Kral, Veronika Slivova. On Average-Case Hardness in TFNP from One-Way Functions (TCC2020).
- [HMR23] Prahladh Harsha, Daniel Mitropolsky, Alon Rosen. Downward Self-Reducibility in TFNP (ITCS2023).
- [HNY17] Pavel Hubacek, Moni Naor, Eylon Yogev. The Journey from NP to TFNP Hardness (ITCS2017).

- [HV21] Pavel Hubacek The Journey from NP to TFNP Hardness and Jan V�clavěk. On Search Complexity of Discrete Logarithm (MFCS2021).
- [Imp95] Russell Impagliazzo. A Personal View of Average-Case Complexity (SCT1995).
- [Jer16] Emil Jerabek. Integer factoring and modular square roots (J. Comput. Syst. Sci. 2016).
- [JPY85] David S. Johnson, Christos H. Papadimitriou, Mihalis Yannakakis. How Easy Is Local Search? (Extended Abstract) (FOCS1985).
- [MP91] Nimrod Megiddo and Christos H. Papadimitriou. On Total Functions, Existence Theorems and Computational Complexity (Theor. Comput. Sci. 1991).
- [MX10] Mohammad Mahmoody, David Xiao. On the Power of Randomized Reductions and the Checkability of SAT (CCC2010).
- [Pap94] Christos H. Papadimitriou. On the Complexity of the Parity Argument and Other Inefficient Proofs of Existence (J. Comput. Syst. Sci. 1994).
- [Sim98] Daniel R. Simon. Finding Collisions on a One-Way Street: Can Secure Hash Functions Be Based on General Assumptions? (EUROCRYPT1998).
- [SZZ18] Katerina Sotiraki, Manolis Zampetakis, Giorgos Zirdelis. PPP-Completeness with Connections to Cryptography (FOCS2018).
- [GQ21] Joshua A. Grochow and Youming Qiao. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials I: Tensor Isomorphism-Completeness (ITCS2021).