コルモゴロフ複雑度と
そのアルゴリズム/暗号理論的恩恵

七島　幹人

(東京工業大学)

量子計算機暗号と量子情報の数理 @九州大

2022年 8月 3日

計算複雑性理論

どのような問題が困難か?

ある問題の困難性仮定

Ex. 離散対数,LWE,...

NP ⊈ BPP

暗号理論

$\Longrightarrow$

公開鍵暗号

共通鍵暗号

$\Longleftarrow$

$\overset{?}{\Longrightarrow}$

背景: メタ計算量理論 (Meta-Complexity)

TCS系会議: STOC, FOCS, Crypto, CCC, ITCS …
(Best/Best student: CCC16,20, FOCS18,20, Crypto21, ITCS20 …)
Invited talk/workshop: STOC2020, CCC21&22 …

計算量理論

= ある問題を解く計算量を知る

解きたい問題 $f\colon \{0,1\}^* \to \{0,1\}^*$

Ex. SAT,Factoring

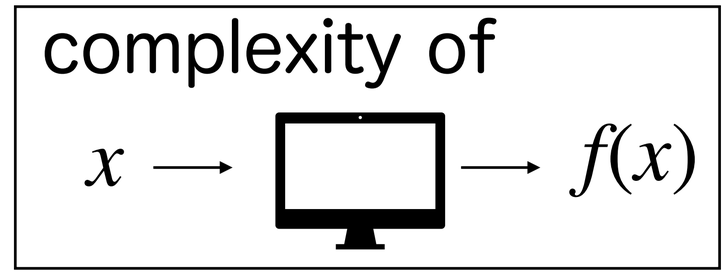
complexity of

Ex. time/space/size

メタ計算量理論

= 計算量を知る計算量を知る

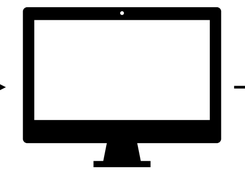
complexity of



Ex. 回路最小化問題(MCSP) [Kabanets & Cai, STOC00]

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

$tt(f) \in \{0,1\}^{2^n}$



f を計算する
最小の回路サイズ

背景: メタ計算量理論 (Meta-Complexity)

メタ計算量理論 = 計算量を知る計算量を知る

平均時計算量
[e.g. Hirahara, FOCS18]

暗号理論
[e.g. Liu&Pass, STOC20]

メタ計算量理論

学習理論
[e.g. Carmosino et al., CCC16]

証明複雑性理論
[e.g. Pich&Santhanam, FOCS19]

MINKT $x \in \{0,1\}^*$, $t \in \mathbb{N}$ →  → x の t 時間制限コルモゴロフ複雑度 $K^t(x)$

Q. コルモゴロフ複雑度とは? $K^t(x) \approx$ 決定的計算

Q. なぜ重要か? → $rKt, pK^t(x), rK^t(x) \approx$乱択計算
[Lu&Oliveira, ECCC TR22-081]

→ $KQ^t(x) \approx$量子計算 [?]

1. コルモゴロフ複雑度

2. アルゴリズム的恩恵

3. 暗号理論的恩恵

4. 将来展望: NPの困難性に基づく一方向性関数

1. コルモゴロフ複雑度

2. アルゴリズム的恩恵

3. 暗号理論的恩恵

4. 将来展望: NPの困難性に基づく一方向性関数

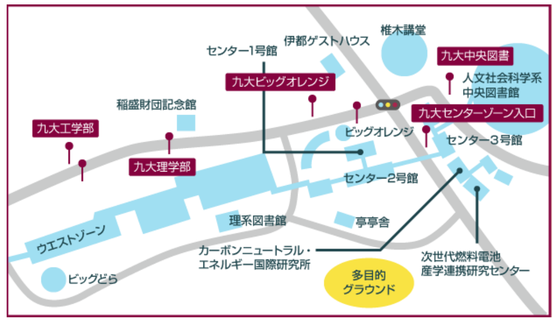
どちらがよりでたらめか ？

0100110110000001　　1111111111111111

どちらが多くの情報を持つか ？

トマトに含まれるリコピンには
抗酸化作用がある

レモン一個に含まれるビタミンCは
レモン一個分だぜ



情報量・エントロピー　　背景にある分布が必要

インスタンスごとに 情報量/でたらめさ を議論出来ないか?

コルモゴロフ複雑度 (Kolmogorov complexity)


A. Kolmogorov

= 文字列 x を出力するプログラムの最小記述量

= x をプログラムとしてどの程度圧縮できるか

$\overbrace{11111\cdots11111}^{n}$	“Print ‘1’ n times”	$O(\log n)$ bit
01001 ⋯ 00001	“??”	$\Omega(n)$ bit

Def. (コルモゴロフ複雑度)

U : Universal TM

$\forall M$: TM $\forall x \in \{0,1\}^*$

$M(x) = y$ in t steps $\Leftrightarrow$ $U(M, x) = y$ in $O(t^2)$ steps

$t \in \mathbb{N}$　時間制限

文字列 $x \in \{0,1\}^*$ の t-時間制限 コルモゴロフ複雑度 $K^t(x)$

$$K^t(x) := \min\{p \in \mathbb{N} : \exists \Pi \in \{0,1\}^p \text{ s.t. } U(\Pi) = x \text{ in } t \text{ steps}\}$$

コルモゴロフ複雑度 (Kolmogorov complexity)

Def. (コルモゴロフ複雑度)

$t \in \mathbb{N}$　時間制限

$x \in \{0,1\}^*$ の t-時間制限 コルモゴロフ複雑度 $K^t(x)$

$$K^t(x) := \min\{p \in \mathbb{N} : \exists \Pi \in \{0,1\}^p \text{ s.t. } U(\Pi) = x \text{ in } t \text{ steps}\}$$

Note. $\forall x \in \{0,1\}^n \quad K^{n^2}(x) \leq n + O(1)$ “Print x”

内 $\geq (7/8) \cdot 2^n$ 個　$K^{\infty}(x) \geq n - 3$

∵#長さ$n-3$未満のプログラム $= 2^0 + \cdots 2^{n-4} < 2^{n-3}$

MINKT　Input: $x \in \{0,1\}^*$, 1^t $(t \in \mathbb{N})$　Output: $K^t(x)$

(判定問題) Input $x \in \{0,1\}^*$, $1^s, 1^t$ $(s, t \in \mathbb{N})$　Determine $K^t(x) \overset{?}{\leq} s$

Note. MINKT $\in$ NP

NP完全かは

重要未解決問題

MINKT → Easy → アルゴリズム的恩恵

MINKT → Hard → 暗号理論的恩恵

1. コルモゴロフ複雑度

2. アルゴリズム的恩恵

3. 暗号理論的恩恵

4. 将来展望: NPの困難性に基づく一方向性関数

アルゴリズム的恩恵 (MINKTの困難性の根拠)

MINKT $\in$ P $\longrightarrow$ 与えられた x が圧縮できるか 判定

[Hirahara FOCS18, informal] Search-to-Decision 帰着　圧縮された表現を構成

[Hirahara&N FOCS21]　回路のAgonistic学習

Agnostic 学習

$\mathscr{C} \subseteq \{f\colon \{0,1\}^n \to \{0,1\}\}$

sample set

$(x^1, b^1), \ldots (x^m, b^m)$

n bitのデータ　1bitのラベル

unknown

$(x^i, b^i) \sim D$ over $\{0,1\}^n \times \{0,1\}$

D_x : example distribution

$\mathscr{C}$の中でbestな仮説と同等の仮説を出力

$\Pr_{(x,b)}[f^*(x) \neq b]$を最小化

$\mathrm{opt} = \min_{f \in \mathscr{C}} \Pr_{(x,b)}[f(x) \neq b]$

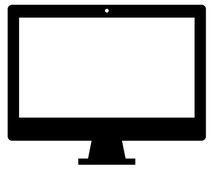
出力: 回路 h s.t. $\Pr_{(x,b)}[h(x) \neq b] \lesssim \mathrm{opt}$

サンプル数 $m = \mathrm{poly}(n)$ & $\mathrm{poly}(n)$ 時間

アルゴリズム的恩恵 (MINKTの困難性の根拠)

$\mathscr{C} \subseteq \{f\colon \{0,1\}^n \to \{0,1\}\}$

sample set
$(x^1, b^1), \ldots (x^m, b^m)$



回路 h s.t. $\Pr_{x,b}[h(x) \neq b] \lesssim$ opt

opt $= \min_{f \in \mathscr{C}} \Pr_{x,b}[f(x) \neq b]$

n bitのデータ　1bitのラベル

unknown

$(x^i, b^i) \sim D$ over $\{0,1\}^n \times \{0,1\}$　D_x : example distribution

Note.　$\mathscr{C}$ が大きくなるほど精度が良い学習アルゴリズム ⟶ 計算量 大

$\mathscr{C}$ = {線形関数}　example dist. D_x = 一様分布 (fix)

≒ Learning Parity with Noise (LPN)　暗号学的仮定

[FGKP09]

[Hirahara&N FOCS21]

MINKT ∈ P ⟹ (example dist D の計算量的仮定の元)

$\mathscr{C}$ = {多項式サイズ回路} が Agnostic 学習可能

強力な学習アルゴリズム　　MINKTの困難性の根拠

アルゴリズム的恩恵 (MINKTの困難性の根拠)

[Hirahara&N FOCS21]

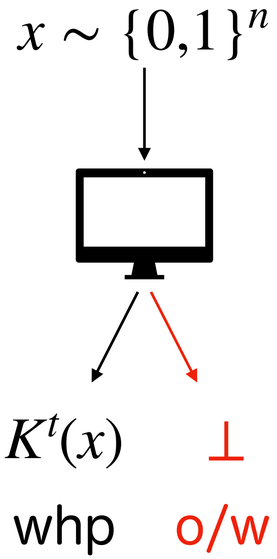
MINKT $\in$ P $\Longrightarrow$ example dist D が未知多項式サイズ回路でサンプル可能であれば

P = NP $\Longrightarrow$ $\mathscr{C}$ = {多項式サイズ回路} が Agnostic 学習可能

[BEHW87]

Note. $K^t(x)$の近似 で十分

GapMINKT $x, 1^t \longmapsto K^t(x) + o(K^t(x)) \cdot \mathrm{polylog}(|x|)$



[Hirahara FOCS18,CCC20] 最悪時-平均時 帰着

MINKTが平均時で解ける $\Longrightarrow$ GapMINKTは最悪時で解ける

(errorless) (=多くのインスタンス) (=全てのインスタンス)

$\Uparrow$ $\Downarrow$

NPが平均時で解ける $\Longrightarrow$ (example dist D_x の計算量的仮定の元)

(errorless) 多項式サイズ回路が Agnostic 学習可能

最悪時学習 - 平均時NP 帰着

GapMINKT ⇒ Learning [Hirahara & Nanashima 21]

STEP I GapMINKT ⟶ 弱学習アルゴリズム

$\mathrm{opt} \le 1/2 - 1/\mathrm{poly}(n)$
$\Rightarrow \Pr_{x,b}[h(x) \neq b] \le 1/2 - 1/\mathrm{poly}(n)$

STEP II 弱学習アルゴリズム ⟶ Agnostic学習アルゴリズム　Agnostic Boosting [Feldman ICS10]

入力 $\{(x^{(1)}, b^{(1)}), \ldots, (x^{(m)}, b^{(m)})\}$　$X := (x^{(1)}, \cdots, x^{(m)})^T$　$b := (b^{(1)}, \cdots, b^{(m)})^T$

Idea: $\Delta := K^{t+\delta}(X, b) - K^t(X)$ を近似 (for proper t and δ)

Goal: 次の2ケースを区別
→ hybrid argument

(i) sample　$\exists f^*$：$s(n)$ サイズ回路 $\Pr[f^*(x^{(i)}) \neq b^{(i)}] \le 1/2 - 1/\mathrm{poly}$

(ii) random　$b^{(i)} \leftarrow_u \{0,1\}$

$f^*(X) = (f^*(x^{(1)}), \ldots, f^*(x^{(m)}))^T$　$e = f^*(X) \oplus b$　(Bitwise XOR)

(i) sample　$b = f^*(X) \oplus e$　$\Delta \le |f^*| + |e| \le O(s(n)\log s(n)) + (1 - 1/\mathrm{poly}) \cdot m$

(ii) random　$b \sim \{0,1\}^m$　$\Delta \approx m$ ？ ⟶ m 十分大

D_x が多項式サイズ回路でsamplable ✓

1. コルモゴロフ複雑度

2. アルゴリズム的恩恵

3. 暗号理論的恩恵

4. 将来展望: NPの困難性に基づく一方向性関数

暗号理論的恩恵

メタ計算量による一方向性関数の特徴づけ

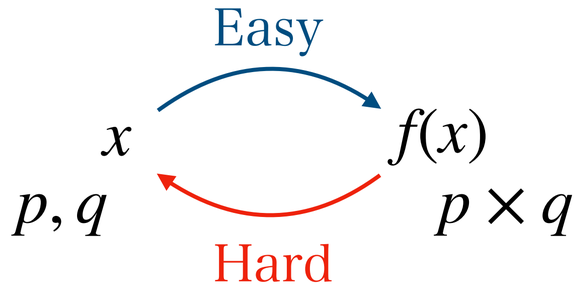
[Liu&Pass STOC20; Crypto21; CCC22; Allender et al. FSTTCS21, Ren&Santhanam CCC21, Ilango, Ren, and Santhanam, STOC22]

Def. (一方向性関数)

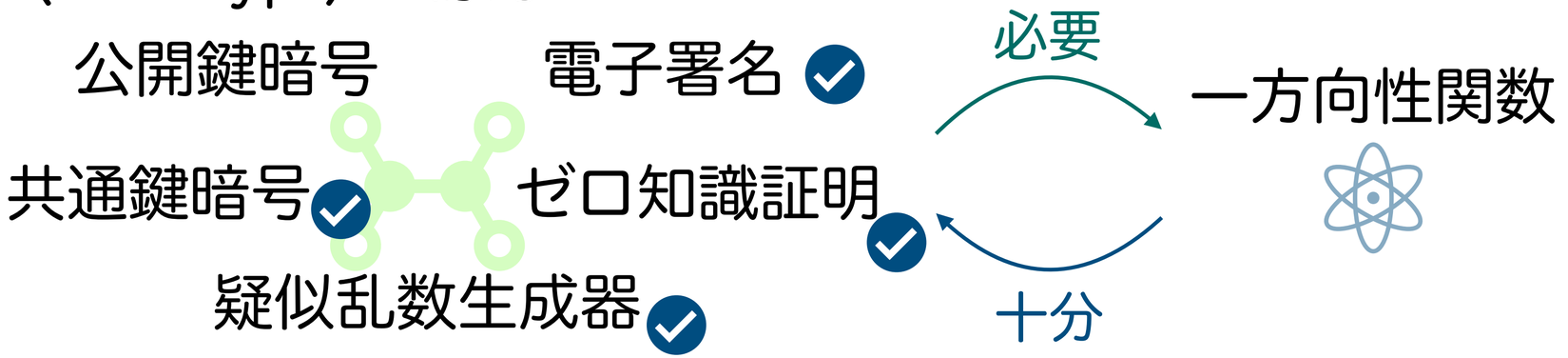
$f = \{f_n : \{0,1\}^{s(n)} \to \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ が一方向性関数 (OWF)

$\overset{\text{def}}{\iff}$ $\exists p$：多項式 $\forall I$ ：乱択多項式時間TM

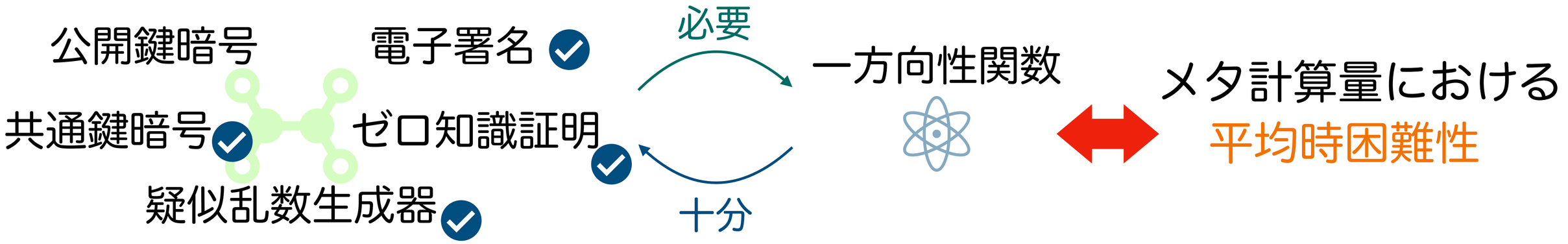
$$\Pr\left[I\left(1^n, f_n(U_{s(n)})\right) \in f_n^{-1}\left(f_n(U_{s(n)})\right)\right] < 1 - 1/p(n)$$



暗号の世界 (Minicrypt) の原子



暗号理論的恩恵



Thm. [Liu&Pass STOC20]

∃一方向性関数 $\iff$ MINKTが 一様分布上 平均時困難 (error-prone) for some sufficiently large $t(n) = \mathrm{poly}(n)$

f が D上平均時困難 (error-prone) $\overset{\text{def}}{\iff}$ $\exists p$:多項式 s.t. $\forall M$:多項式時間(乱択)TM

$$\Pr_{x \sim D}[M(x) \neq f(x)] \geq 1/p(|x|)$$

Thm. [Ilango, Ren, and Santhanam, STOC22]

∃一方向性関数 $\iff$ $\exists D$: 多項式時間samplable s.t. GapMINKTが D上 平均時困難 (error-prone)

一方向性関数の特徴付け (の片方向) [Liu&Pass 20]

MINKTが平均時間困難 $\Longrightarrow$ ∃ 一方向性関数

$t(n)$: 十分大きい任意の多項式 (時間制約)

$$f = \{f_n : \{0,1\}^{s(n)} \to \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$$

$$f_n(i,\Pi) = (i,x) \qquad i \sim [2n] \;\; \Pi \sim \{0,1\}^{2n} \;\; x = U(\Pi_{\leftarrow i}) \text{ in } t(n) \text{ steps}$$

Claim f が(弱)一方向性関数でない $\Longrightarrow$ $K^{t(n)}(x)$ が計算可能
w.p. $\geq 1 - 1/p(n)$ over $x \sim \{0,1\}^n$

I : inverter for f 失敗確率 $\leq 1/(n^2 p(n))$

if not 失敗確率 $> 1/p(n)$

$\longrightarrow$ A for computing $K^{t(n)}(x)$

入力 $x \in \{0,1\}^n$ 1. $\forall i \in [2n]$ で $I(i,x)$ を動かす 2. 成功した最小のiを出力

$\because$ $\Pr[f(U) = (K^{t(n)}(x), x)] \geq (1/2n) \cdot (1/2^{K^t(x)}) \geq 1/(2n2^{n+O(1)}) = (c/n) \cdot 2^{-n}$

A が $\geq 2^n/p(n)$ 個のxで失敗 $\Rightarrow$ I の 失敗確率 $\geq c \cdot 1/(np(n))$

失敗確率 $\leq 1/(n^2 p(n))$に矛盾 ∎

1. コルモゴロフ複雑度

2. アルゴリズム的恩恵

3. 暗号理論的恩恵

4. 将来展望: NPの困難性に基づく一方向性関数

まとめ

MINKT → Easy → アルゴリズム的恩恵
MINKT → Hard → 暗号理論的恩恵

Agnostic学習
最悪時-平均時帰着
一方向性関数
⇒ …

より強い安全性根拠に基づく暗号　　アルゴリズム vs. 暗号

MINKT → Easy → タスクXに対する強力なアルゴリズム
MINKT → Hard → 暗号プロトコルP

タスクX が困難 $\Longrightarrow$ MINKT が困難 $\Longrightarrow$ 暗号プロトコル P

暗号プロトコル Pに対する敵対者 $\Longrightarrow$ タスクXに対するアルゴリズム

Q. $\mathrm{NP} \not\subseteq \mathrm{BPP} \overset{?}{\Longrightarrow}$ 一方向性関数の存在

NPの困難性に基づくOWF

Q. $\mathrm{NP} \not\subseteq \mathrm{BPP} \overset{?}{\Longrightarrow}$ 一方向性関数の存在

∄一方向性関数 ⟷ ∀D:Psamp MINKTがD上平均時容易 (error-prone)
(inverterが存在) [LP20;IRS22]

? **Q.** errorless vs error-prone
barrier [RS21,HN22]

NPが平均時容易⟹ ∀D:Psamp MINKTがD上平均時容易 (errorless)

[Hir18,20]

Q. GapMINKTのNP完全性?
Q. MINKTのNP完全性?
Q. 学習のNP完全性?

GapMINKT

[HN21]

回路の学習

? **Q.** 仮説サイズの改善

? ?

NP ⊆ BPP ⟷ 弱学習

[Hirahara FOCS22] Upcoming!

Q. 他の問題 Ex. MINcKT [Liu&Pass CCC22] **Q.** 他の計算モデル Ex. 量子