確率様相論理による秘匿性の証明

竹内泉　真野健

2010年3月8日

秘匿

ある1ビットの変数 x の値（ $x=0$ か $x=1$ か）が隠されている

●非確率論的議論

$x=0$ であるような可能世界と $x=1$ であるような可能世界があり
隠されている人にとって区別できない

●確率論的議論

隠されている人がどんなに努力して予想 $\bar{x}$ を立てても
$x=\bar{x}$ となる確率を $1/2$ より大きくすることが出来ない

目標

確率論的議論を形式化して秘匿性を証明できるような論理体系を提案する

例題：〈暗号学者の会食〉問題

(Dining Cryptgrapher Protocol, D. Chaum, J. Cryptgraphy, 1988)

● A、B、C が三人で店で食事をした

●会計をしょうとした所、既に済んでいた

●三人の内の誰かがこっそり全額支払ったか、あるいは三人以外の人が全額支払ったかの
いずれかである

（三人の性格からして、二人で支払うということはありえない）

●支払ったのが三人の中にいるのか否かだけを知りたい
三人の内の誰かが支払った場合でも支払ったのが誰かは秘密にしておきたい

●硬貨を三枚振って、それをそれぞれ違った二人だけが見る

・硬貨 1 は A と B だけが見る

・硬貨 2 は B と C だけが見る

・硬貨 3 は C と A だけが見る

●三人はそれぞれ、自分の見た硬貨の表だった数と、
自分が支払ったか否かの真偽値を合計したパリティーだけを皆に知らせる
例：見た硬貨が一枚表であり、自分が支払っている場合は 1+1 で 0 と言う
例：見た硬貨が両方表であり、自分が支払っていない場合は 2+0 で 0 と言う

p_A ···· A が支払った　q_1 ···· 硬貨 1 は表だった
p_B ···· B が支払った　q_2 ···· 硬貨 2 は表だった
p_C ···· C が支払った　q_3 ···· 硬貨 3 は表だった

A の申告　$r_A = p_A + q_1 + q_3$
B の申告　$r_B = p_B + q_1 + q_2$
C の申告　$r_C = p_C + q_2 + q_3$　$\pmod 2$

$$r_A + r_B + r_C = p_A + p_B + p_C + 2q_1 + 2q_2 + 2q_3$$
$$= p_A + p_B + p_C \pmod 2$$

三人の申告の和のパリティーによって、三人の中に支払った人がいるのか否かが分かる

A が支払った場合に、C には A が支払ったのか B が支払ったのかは分からない
例：硬貨が 3 枚とも裏だった場合

		p_A	p_B	p_C	q_1	q_2	q_3	
A の申告	$r_A =$	1			$+0$	$+0$		$=1$
B の申告	$r_B =$		0		$+0$	$+0$		$=0$
C の申告	$r_C =$			0		$+0$	$+0$	$=0$

しかし、C には第一硬貨の裏表が分からないので、B が支払った場合と区別が付かない

		p_A	p_B	p_C	q_1	q_2	q_3	
A の申告	$r_A =$	0			$+1$	$+0$		$=1$
B の申告	$r_B =$		1		$+1$	$+0$		$=0$
C の申告	$r_C =$			0		$+0$	$+0$	$=0$

これには第一硬貨の裏表の確率が $1/2$ ずつであることが重要である

第一硬貨の表の確率が $p > 1/2$ である場合、A が支払っていても、B が支払っていても、
確率 p で支払った人を言い当てる戦略が C には存在する

$p_C = 0$ (C は支払っていない)
$r_A + r_B + r_C = 1 \pmod 2$ (A か B が支払った) という前提はその侭
この前提から $r_A + r_B + q_2 + q_3 = 0$ が得られる

C の戦略：
– $r_A + q_2 = r_B + q_3 = 0 \pmod 2$ の時、A が支払ったと推測する
– $r_A + q_2 = r_B + q_3 = 1 \pmod 2$ の時、B が支払ったと推測する
　→ $q_1 = 1$ と仮定して推測する

A が支払った場合でも、B が支払った場合でも、
$q_1 = 1$ であれば推測は当たり、$q_1 = 0$ であれば推測は外れる

この戦略は、A が支払うか B が支払うかを確率過程と見做していない

第一硬貨の裏表の確率が $1/2$ ずつである場合、
$1/2$ より大きい確率で A が支払ったか B が支払ったかを C が言い当てる戦略は存在しない
　→確率論的な秘匿性

この秘匿性を演繹する論理体系を設計する

確率を表す様相記号
　AF ……　確率が 1 である、必ず成り立つ
　MF ……　確率が $1/2$ より大きい
　HF ……　確率が丁度 $1/2$ である
　EF ……　確率が 0 ではない

確率量化命題論理

命題変数 $\boldsymbol{V} = \boldsymbol{V_N} \cup \boldsymbol{V_P} \cup \boldsymbol{V_D}$

$\boldsymbol{V_N}$ …… **非決定性変数** $\boldsymbol{V_P}$ …… **確率変数** $\boldsymbol{V_D}$ …… **補助変数**

論理式 $\boldsymbol{F} := \boldsymbol{V} \mid \top \mid \neg \boldsymbol{F} \mid \boldsymbol{F} \wedge \boldsymbol{F} \mid \forall \boldsymbol{V_N} \boldsymbol{F} \mid \forall \boldsymbol{V_D} \boldsymbol{F} \mid \mathsf{A}\boldsymbol{F} \mid \mathsf{M}\boldsymbol{F}$

A と M は確率変数を全て束縛する

$\mathsf{A}\boldsymbol{F}$ と $\mathsf{M}\boldsymbol{F}$ では、$\boldsymbol{F}$ には補助変数は自由に現れない

略記法

$\boldsymbol{F} \supset \boldsymbol{G} \equiv \neg(\boldsymbol{F} \wedge \neg \boldsymbol{G})$

$\boldsymbol{F} \vee \boldsymbol{G} \equiv \neg \boldsymbol{F} \supset \neg \boldsymbol{G}$

$\boldsymbol{F} \leftrightarrow \boldsymbol{G} \equiv (\boldsymbol{F} \supset \boldsymbol{G}) \wedge (\boldsymbol{G} \supset \boldsymbol{F})$

$\boldsymbol{F} \oplus \boldsymbol{G} \equiv (\neg \boldsymbol{G} \wedge \boldsymbol{F}) \vee (\neg \boldsymbol{F} \wedge \boldsymbol{G}) \equiv \neg(\boldsymbol{F} \leftrightarrow \boldsymbol{G})$

$\bot \equiv \neg \top$

$\mathsf{E}\boldsymbol{F} \equiv \neg \mathsf{A} \neg \boldsymbol{F}$,

$\mathsf{H}\boldsymbol{F} \equiv \neg \mathsf{M} \boldsymbol{F} \wedge \neg \mathsf{M} \neg \boldsymbol{F}$

意味論

各変数への割当の集合 $\boldsymbol{W_N},\ \boldsymbol{W_P}, \boldsymbol{W_D}$

$\boldsymbol{W_N} = \{0,1\}^{\boldsymbol{V_N}},\ \boldsymbol{w} \in \boldsymbol{W_N} \iff \boldsymbol{w} : \boldsymbol{V_N} \to \{0,1\}$

$\boldsymbol{W_P} = \{0,1\}^{\boldsymbol{V_P}},\ \boldsymbol{w} \in \boldsymbol{W_P} \iff \boldsymbol{w} : \boldsymbol{V_P} \to \{0,1\}$

$\boldsymbol{W_D} = \{0,1\}^{\boldsymbol{V_D}},\ \boldsymbol{w} \in \boldsymbol{W_D} \iff \boldsymbol{w} : \boldsymbol{V_D} \to \{0,1\}$

確率 $\boldsymbol{\mu} : \boldsymbol{V_P} \to [0,1]$

$\boldsymbol{w} \in \boldsymbol{W_P}$ **に対して** $\mathsf{Pr}^{\boldsymbol{\mu}}(\boldsymbol{w}) = \left(\prod_{\{\boldsymbol{x} \mid \boldsymbol{w}(\boldsymbol{x})=1\}} \boldsymbol{\mu}(\boldsymbol{x})\right) \times \left(\prod_{\{\boldsymbol{x} \mid \boldsymbol{w}(\boldsymbol{x})=0\}} (1 - \boldsymbol{\mu}(\boldsymbol{x}))\right)$

……各確率変数は独立

$\boldsymbol{E} \subset \boldsymbol{W_P}$ **に対して** $\mathsf{Pr}^{\boldsymbol{\mu}}(\boldsymbol{E}) = \sum_{\boldsymbol{w} \in \boldsymbol{E}} \mathsf{Pr}^{\boldsymbol{\mu}}(\boldsymbol{w})$

意味論　$w = (w_N, w_P, w_D) \in W_N \times W_P \times W_D,\ \mu$ **に対して**

$(w, \mu) \models x \iff w_N(x) = 1$ ... $x \in V_N$

$(w, \mu) \models x \iff w_P(x) = 1$ ... $x \in V_P$

$(w, \mu) \models x \iff e(x) = 1$ ... $x \in V_D$

$(w, \mu) \models \top$ **は常に成り立つ**

$(w, \mu) \models \neg F \iff (w, \mu) \not\models F$

$(w, \mu) \models F \wedge G \iff (w, \mu) \models F$ & $(w, \mu) \models G$

$(w, \mu) \models \forall x F \iff (w, \mu) \models F[\top/x] \wedge F[\bot/x]$

$(w, \mu) \models \mathsf{A}F \iff \mathsf{Pr}^{\mu, w_N}(F) = 1$

$(w, \mu) \models \mathsf{M}F \iff \mathsf{Pr}^{\mu, w_N}(F) > 1/2$

但し $\mathsf{Pr}^{\mu, w_N} = \mathsf{Pr}^{\mu}(\{w | (w_N, w, w_D) \models F\})$

$\models F \iff$ **任意の** (w, μ) **に対して** $(w, \mu) \models F$

公理化

分離規則　$\vdash F \supset G, \vdash F \implies \vdash G$

必然性規則　$\vdash F \implies \vdash \mathsf{A}F$

始式

1. **トートロジー**
2. $\forall$ **に関する始式**　…　$\forall x F \leftrightarrow F[\top/x] \wedge [\bot/x]$
3. **確率に関する始式**

3.1 $x \leftrightarrow \mathsf{A}x$ $(x \in V_N)$,　　**3.2** $\mathsf{A}F \leftrightarrow \mathsf{AA}F$,　　**3.3** $\mathsf{M}F \leftrightarrow \mathsf{AM}F$

3.4 $\mathsf{A}(F \supset G) \supset \mathsf{A}F \supset \mathsf{A}G$,　　**3.5** $\mathsf{A}(F \supset G) \supset \mathsf{M}F \supset \mathsf{M}G$

3.6 $\mathsf{A}F \supset \mathsf{M}F$　　**3.7** $\mathsf{M}F \supset \mathsf{M}G \supset \mathsf{E}(F \wedge G)$

3.8 $\mathsf{H}F \supset (\mathsf{M}((F \wedge G) \vee (\neg F \wedge H)) \leftrightarrow \mathsf{M}((F \wedge H) \vee (\neg F \wedge G)))$

但し $V_P \cap FV(F) \cap FV(G, H) = \emptyset$, $V_D \cap FV(F, G, H) = \emptyset$

完全な公理化は困難である

不完全だが必要な定理は得られる、というような公理化ならば出来る

〈暗号学者の会食〉問題の形式化

非決定性変数

p_A … A が支払った、p_B … B が支払った、p_C … C が支払った

確率変数

q_1 … 第一硬貨が表、q_2 … 第二硬貨が表、q_3 … 第三硬貨が表

補助変数

r_A … A の報告、r_B … B の報告、r_C … C の報告

共通理解

$$P_0 \equiv (p_A \wedge \neg p_B \wedge \neg p_C) \vee (\neg p_A \wedge p_B \wedge \neg p_C) \vee (\neg p_A \wedge \neg p_B \wedge p_C) \vee (\neg p_A \wedge \neg p_B \wedge \neg p_C)$$

……三人の内の誰かが一人で全部支払ったか、三人以外の誰かが支払った

$$P_1 \equiv r_A \leftrightarrow p_A \oplus q_1 \oplus q_2$$

$$P_2 \equiv r_B \leftrightarrow p_B \oplus q_2 \oplus q_3$$

$$P_3 \equiv r_C \leftrightarrow p_C \oplus q_3 \oplus q_1$$

……三人の報告の内容

〈暗号学者の会食〉問題の形式化

C の知識 …… p_C, q_2, q_3, r_A, r_B のそれぞれの真偽値

確率を使わずに得られること

$$\vdash P_0 \wedge P_1 \wedge P_2 \wedge P_3 \wedge \neg p_C \supset ((p_A \vee p_B) \leftrightarrow r_A \oplus r_B \oplus r_C)$$

$$\vdash P_0 \wedge (p_A \vee p_B) \supset (p_A \leftrightarrow \neg p_B)$$

$$\vdash \forall r_A (P_1 \supset F) \leftrightarrow F[p_A \oplus q_1 \oplus q_2 / r_A]$$

r_B、r_C についても同様

準備

任意のブール函数 $F(\ )$ に対してあるブール函数 $F'(\ )$ があって

$$\vdash (p_A \vee p_B) \wedge P_0 \wedge P_1 \wedge P_2 \wedge P_3 \supset (F(p_C, q_2, q_3, r_A, r_B) \leftrightarrow F'(p_C, q_2, q_3, p_A \oplus q_1))$$

論理式 F_0、F_1 があって

$$\vdash F'(p_C, q_1, q_3, p_A \oplus q_1) \leftrightarrow ((p_A \oplus q_1) \wedge F_1) \vee (\neg(p_A \oplus q_1) \wedge F_0)$$

但し $FV(F_0) \subset \{p_C, q_2, q_3\},\ FV(F_1) \subset \{p_C, q_2, q_3\}$

準備（続き）

$$\vdash (p_A \leftrightarrow F'(p_C, q_2, q_3, p_A \oplus q_1)) \leftrightarrow (p_A \wedge q_1 \wedge F_1) \vee (\neg p_A \wedge \neg q_1 \wedge \neg F_1) \vee (p_A \wedge \neg q_1 \wedge F_0) \vee (\neg p_A \wedge q_1 \wedge \neg F_0)$$

$$\vdash \forall p_A \mathsf{M}(p_A \leftrightarrow F'(p_C, q_2, q_3, p_A \oplus q_1)) \leftrightarrow \mathsf{M}((q_1 \wedge F_1) \vee (\neg q_1 \wedge F_0)) \wedge \mathsf{M}((q_1 \wedge \neg F_0) \vee (\neg q_1 \wedge \neg F_1))$$

確率に関する規則

$$\vdash \mathsf{H} q_1 \supset \mathsf{M}((q_1 \wedge F_1) \vee (\neg q_1 \wedge F_0)) \leftrightarrow \mathsf{M}((q_1 \wedge F_0) \vee (\neg q_1 \wedge F_1))$$

故に

$$\vdash \mathsf{H} q_1 \supset \forall p_A (\mathsf{M}(p_A \leftrightarrow F'(p_C, q_2, q_3, p_A \oplus q_1)) \leftrightarrow \mathsf{M}((q_1 \wedge F_0) \vee (\neg q_1 \wedge F_1)) \wedge \mathsf{M}((q_1 \wedge \neg F_0) \vee (\neg q_1 \wedge \neg F_1)))$$

確率に関する規則 $\quad \mathsf{M}G \wedge \mathsf{M}H \supset \mathsf{E}(G \wedge H)$

故に

$$\vdash \mathsf{H} q_1 \supset \forall p_A (\mathsf{M}(p_A \leftrightarrow F'(p_C, q_2, q_3, p_A \oplus q_1)) \supset \mathsf{E}\bot)$$

即ち

$$\vdash \mathsf{H} q_1 \supset \neg \forall p_A \mathsf{M}(p_A \leftrightarrow F'(p_C, q_2, q_3, p_A \oplus q_1))$$

結論

任意のブール函数 $F(\ )$ に対して

$$\vdash \mathsf{H} q_1 \supset \neg \forall p_A \forall p_B \forall p_C P_0 \wedge (p_A \vee p_B) \supset \mathsf{M}(p_A \leftrightarrow \forall r_A \forall r_B \forall r_C P_1 \wedge P_2 \wedge P_3 \supset F(p_C, r_A, r_B, q_1, q_3))$$

議論

確率過程と非決定性過程は区別する

→確率過程は確率変数で、非決定性過程は非決定性変数で表現

受動的攻撃者は形式化できる

→能動的攻撃者は、このままでは形式化できない

今後の課題

●条件付き確率

●能動的攻撃者