計算の複雑さと力学系

東大院総合 佐藤 譲, 池上 高志

ysato@sacral.c.u-tokyo.ac.jp, ikeg@sacral.c.u-tokyo.ac.jp

Abstract

命題論理式の充足可能性問題 (Satisfiability problem, 以下 SATと表記する.) は数理論理学を背景に持つ代表的な NP完全問題であり, 計算の複雑さの理論においては「実際的計算可能性」を考える上で重要な研究対象になっている. 近年, この SATは数値計算を用いる実験数学的な手法によって研究されており, 計算の複雑さの現実的な性質が明らかになっている. 本論文では力学系の理論に基づき計算理論に新たな視点を導入する.

SATのうちで, 節に含まれるリテラルの数が k個である和積標準型の論理式 ($kCNF$) の充足可能性を判定する問題を特に $kSAT$という. 本稿では主にこの $kSAT$を取り上げる. $kSAT$は与えられた $kCNF$を満たす解が存在するかどうかを判定する決定問題であり, $k=1,2$ のときは多項式時間で解ける問題クラス (class P), $k \geq 3$ のときは多項式時間では解けないと予想されている問題クラス (class NP) に属することが知られている.

先行研究によると, 計算コストのかかる問題の分布は一様なものではないことが示唆される. この分布の幾何学的側面を考察するために, ここでは $kCNF$を k次元の単位区間内にコードし, 充足可能式をプロットするという方法をとった. このとき $3CNF$の充足可能式の集合は 3 次元の単位立方体内部に, $2CNF$の充足可能式の集合はその原点を通る平面での切断面に埋め込まれることになる. 結果として, この $kCNF$の充足可能式の集合は, $k=2$ のとき完全な自己相似集合 (フラクタル), $k \geq 3$ のとき部分自己相似集合 (準フラクタル) となると予想された. 自己相似集合は単純な入れ子構造をもつ縮小写像系, 部分自己相似集合は互いに他に含まれるような入れ子構造をもつ縮小写像系で表現される. したがってここでは, このような縮小写像系の再構成が重要な意味を持つ.

$k=2$ の場合, 充足可能式の集合を縮小写像系で再構成することができたが, $k \geq 3$ の場合は再構成が困難だった. このため Box-counting 法で数値的に Hausdorff 次元を求めたところ, $k=2$ の場合は理論値に良く一致したが, $k \geq 3$ の場合は (自己相似集合を仮定した場合の) 理論値からややずれるという結果を得た.

$3SAT$が class NPに属するのは何故かという論点に戻ると, 相互に他に含まれる入れ子構造をもつ縮小写像系によって生成される準フラクタルの性質により, NPの言語を認識することのできる離散力学系 (アルゴリズム) において初期入力が不変集合に到達する時間 (計算時間) が単純な入れ子構造をもつ縮小写像系によって生成される Pのそれよりも長くなるという説明がつく.

以上を考察して, 以下の予想を得た.

$$\begin{aligned} \textit{class } P &\iff \textit{Self similar set} \\ \textit{class } NP &\iff \textit{Partially self similar set} \end{aligned}$$

この予想の検証は今後の課題である.

命題論理式はそれを真にするような変数の真偽値の割り当てが存在するとき, 充足可能であるという. 任意の命題論理式は簡単な変換操作により, k和積標準形 (以下 $kCNF$) に変換できるので, 命題論理式のうち $kCNF$だけを考えても一般性を失わない. 与えられた $kCNF$が充足可能かどうかを判定する問題を $kSAT$とよぶ. 例えば $k=3$ ($3SAT$) の場合

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

に対して $x_1 = x_2 = true$, $x_3 = x_4 = false$ とすれば $F = true$ となるので, Fは充足可能である.

$kSAT$に関しては, $k = 1,2$ のときは問題のサイズに対して多項式時間で解ける計算量クラス (class P), $k \geq 3$ のときは多項式時間では解けないと予想されている計算量クラス (class NP) に属することが知られている. $P = NP$, $P \subset NP$のどちらが成り立つかに関しては不明であり, これを検証する問題は「$P =?NP$」問題とよばれる計算機科学における重要な未解決問題である.

さて n 変数の $kCNF$を $\mathbf{R}^k$上の単位立方体 $I_k = [-\frac{1}{2}, \frac{1}{2}]^k$ に対応させる区間コードを下図のように与える. 図の各区間をさらに小区間に分割し, 対応する節を積として式に加えていく. 無限長の節をもつ論理式を I^kに埋め込んだ上で, そのうちの充足可能式の全体を $S^k(n)$ とおくと, この I^k上での $S^k(n)$ の幾何学的な複雑さが $kSAT$ の計算の複雑さを反映していることになる. ここでとくに S^2と S^3の構造的差異は class P, class NP の差異と直接に関係することになる.

図 2に $S^2(n), S^3(n)$ を示した. 充足可能式は I^k上で fractal 状に分布しているが, S^2と比較して S^3の分布には異方性がみられる.

				$\vdots$				
	$(\overline{x_3}+x_3)$	$(\overline{x_2}+x_3)$	$(\overline{x_1}+x_3)$	x_3	(x_1+x_3)	(x_2+x_3)	(x_3+x_3)	
	$(\overline{x_3}+x_2)$	$(\overline{x_2}+x_2)$	$(\overline{x_1}+x_2)$	x_2	(x_1+x_2)	(x_2+x_2)	(x_3+x_2)	
	$(\overline{x_3}+x_1)$	$(\overline{x_2}+x_1)$	$(\overline{x_1}+x_1)$	x_1	(x_1+x_1)	(x_2+x_1)	(x_3+x_1)	
$\cdots$	$\overline{x_3}$	$\overline{x_2}$	$\overline{x_1}$	ϵ	x_1	x_2	x_3	$\cdots$
	$(\overline{x_3}+\overline{x_1})$	$(\overline{x_2}+\overline{x_1})$	$(\overline{x_1}+\overline{x_1})$	$\overline{x_1}$	$(x_1+\overline{x_1})$	$(x_2+\overline{x_1})$	$(x_3+\overline{x_1})$	
	$(\overline{x_3}+\overline{x_2})$	$(\overline{x_2}+\overline{x_2})$	$(\overline{x_1}+\overline{x_2})$	$\overline{x_2}$	$(x_1+\overline{x_2})$	$(x_2+\overline{x_2})$	$(x_3+\overline{x_2})$	
	$(\overline{x_3}+\overline{x_3})$	$(\overline{x_2}+\overline{x_3})$	$(\overline{x_1}+\overline{x_3})$	$\overline{x_3}$	$(x_1+\overline{x_3})$	$(x_2+\overline{x_3})$	$(x_3+\overline{x_3})$	
				$\vdots$				

図 1: 命題論理式の埋め込み (k=2 のとき)

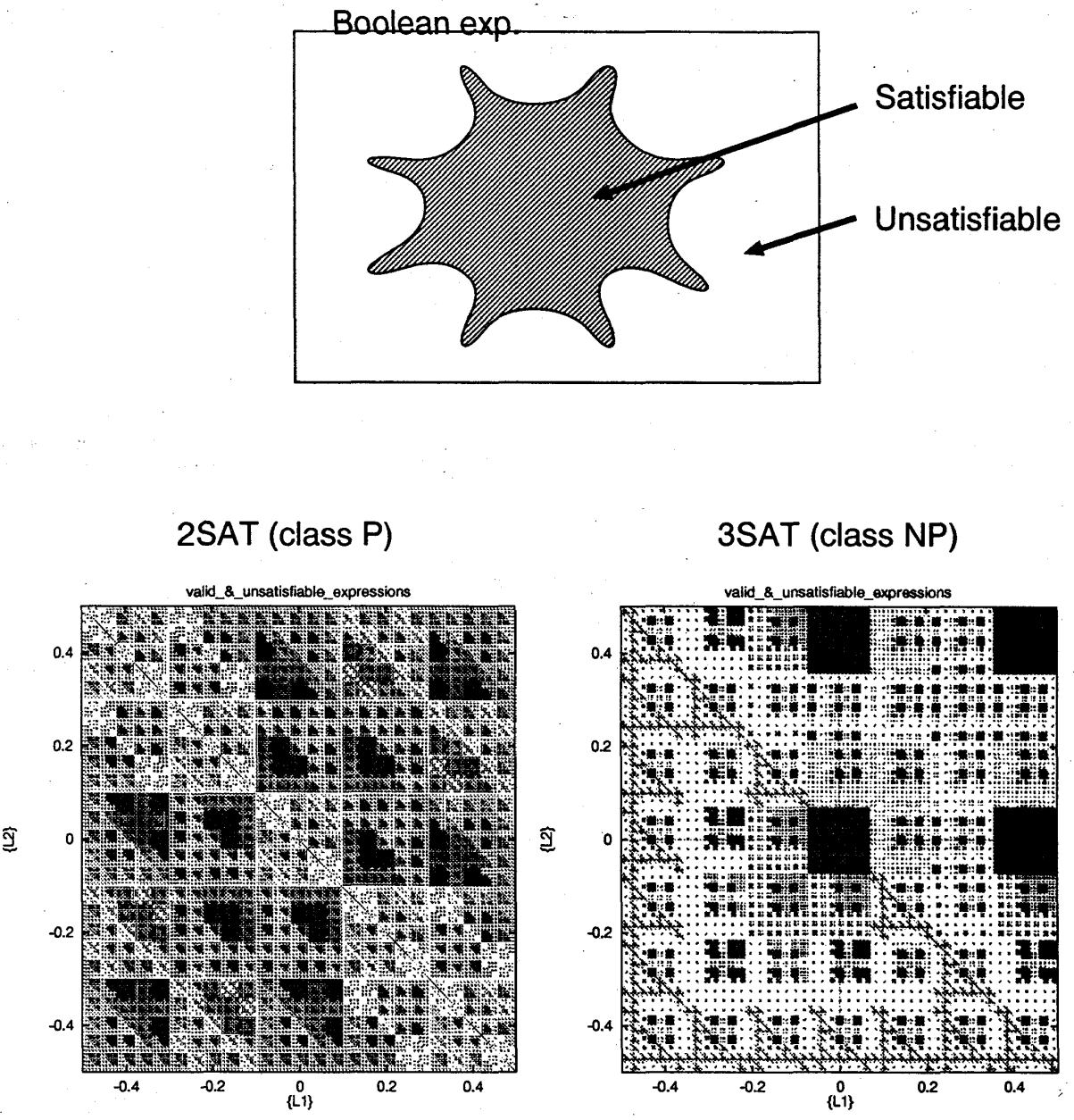

図 2: 単位区間上での充足可能式の分布

次に $S^k(n)$ を極限集合とする IFS(Iterated Functional System) を具体的に与えることを考える. この IFS は L_{kSAT} の Generator となる. 区間コードの定義から, $S^k(n)$ を極限集合とする IFS は全て縮小率が $\frac{1}{2n+1}$ でかつ開集合条件を満たすような縮小写像の組からなる IFS であることがわかる. IFS を構成するために分割された区間を領域とよび, IFS $F = f_1 \cup f_2 \cup \cdots \cup f_n$ を構成するのに必要な領域を $D_{f_1}, D_{f_2}, \cdots, D_{f_n}$ とする. また領域 D' が領域 D を構成要素として含むとき, $D \sqsubseteq D'$ で関係 $\sqsubseteq$ をいれる. IFS F について, $(D_{f_i}, \sqsubseteq)$ が半順序集合となるとき, F を Monotone IFS,$(D_{f_i}, \sqsubseteq)$ が (反対称律を満たさず), 半順序集合とならないとき, F を Recurrent IFS とよぶ. (つまり, 領域間の入れ子の関係が一方向的である IFS を Monotone IFS, 2 つ以上の領域が互いに他と入れ子の関係になっている IFS を Recurrent IFS とよぶ.) Monotone IFS, Recurrent IFS の極限集合はそれぞれ自己相似集合, 部分自己相似集合とよばれる affine fractal となる.

$S^2(1)$ (1 変数の $2CNF$の充足可能式の集合) は以下の Monotone IFS の極限集合となる.

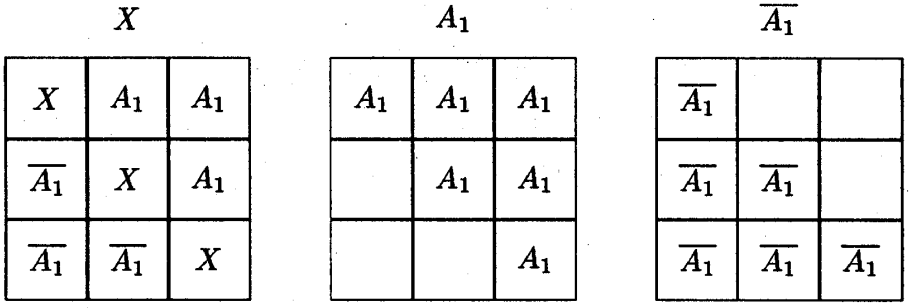

図 3: $S^2(1)$ の IFS

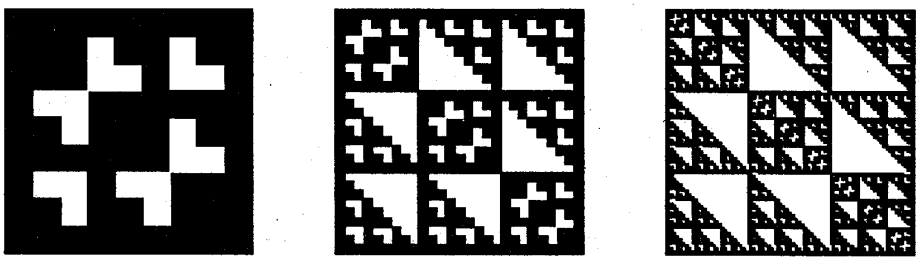

図 4: $S^2(1)$ の生成

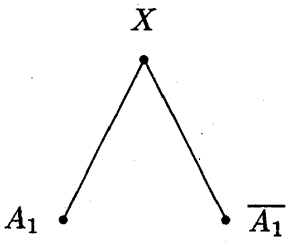

図 5: $S^2(1)$ の IFS の構成領域の Hasse 図

$S^2(2)$ (2 変数の $2CNF$の充足可能式の集合) は以下の Monotone IFS の極限集合となる. ここで, $\overline{A_{(\cdot)}}$は $A_{(\cdot)}$の反転である.

X

X	$A_{\bar{1}+2}$	A_2	A_{1+2}	A_2
$\overline{A_{\bar{1}+2}}$	X	A_1	A_1	A_{1+2}
$\overline{A_2}$	$\overline{A_1}$	X	A_1	A_2
$\overline{A_{1+2}}$	$\overline{A_1}$	$\overline{A_1}$	X	$A_{\bar{1}+2}$
$\overline{A_2}$	$\overline{A_{1+2}}$	$\overline{A_2}$	$\overline{A_{\bar{1}+2}}$	X

A_1

A_1	$A_{1\cdot 2}$	$A_{1\cdot 2}$	A_1	$A_{1\cdot 2}$
A_1	A_1	A_1	A_1	A_1
$\overline{A_{\bar{1}\cdot 2}}$		A_1	A_1	$A_{1\cdot 2}$
$\overline{A_{\bar{1}\cdot 2}}$			A_1	$A_{1\cdot 2}$
$\overline{A_{\bar{1}\cdot 2}}$	$\overline{A_{\bar{1}\cdot 2}}$	$\overline{A_{\bar{1}\cdot 2}}$	A_1	A_1

A_2

A_2	A_2	A_2	A_2	A_2
$A_{1\cdot 2}$	A_2	$A_{1\cdot 2}$	$A_{1\cdot 2}$	A_2
	$A_{\bar{1}\cdot 2}$	A_2	$A_{1\cdot 2}$	A_2
$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	A_2	A_2
	$A_{\bar{1}\cdot 2}$		$A_{1\cdot 2}$	A_2

A_{1+2}

A_{1+2}	A_2	A_2	A_{1+2}	A_2
A_1	A_{1+2}	A_1	A_1	A_{1+2}
$\overline{A_{\bar{1}\cdot 2}}$	$A_{\bar{1}\cdot 2}$	A_{1+2}	A_1	A_2
$A_{1\oplus 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	A_{1+2}	A_2
$\overline{A_{\bar{1}\cdot 2}}$	$A_{1\oplus 2}$	$\overline{A_{\bar{1}\cdot 2}}$	A_1	A_{1+2}

$A_{1\cdot 2}$

$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$
$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$
		$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$
			$A_{1\cdot 2}$	$A_{1\cdot 2}$
			$A_{1\cdot 2}$	$A_{1\cdot 2}$

$A_{\bar{1}\cdot 2}$

$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$
	$A_{\bar{1}\cdot 2}$			$A_{\bar{1}\cdot 2}$
	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$		$A_{\bar{1}\cdot 2}$
$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$	$A_{\bar{1}\cdot 2}$
	$A_{\bar{1}\cdot 2}$			$A_{\bar{1}\cdot 2}$

$A_{\bar{1}+2}$

$A_{\bar{1}+2}$	$A_{\bar{1}+2}$	A_2	A_2	A_2
$A_{1\otimes 2}$	$A_{\bar{1}+2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$	A_2
$\overline{A_{1\cdot 2}}$	$\overline{A_1}$	$A_{\bar{1}+2}$	$A_{1\cdot 2}$	A_2
$\overline{A_1}$	$\overline{A_1}$	$\overline{A_1}$	$A_{\bar{1}+2}$	$A_{\bar{1}+2}$
$\overline{A_{1\cdot 2}}$	$\overline{A_1}$	$\overline{A_{1\cdot 2}}$	$A_{1\otimes 2}$	$A_{\bar{1}+2}$

$A_{1\oplus 2}$

$A_{1\oplus 2}$	$A_{\bar{1}+2}$	$A_{\bar{1}+2}$	$A_{1\oplus 2}$	$A_{\bar{1}+2}$
$\overline{A_{\bar{1}\cdot 2}}$	$A_{1\oplus 2}$	$\overline{A_{\bar{1}\cdot 2}}$	$\overline{A_{\bar{1}\cdot 2}}$	$A_{1\oplus 2}$
$\overline{A_{\bar{1}\cdot 2}}$	$A_{\bar{1}+2}$	$A_{1\oplus 2}$	$\overline{A_{\bar{1}\cdot 2}}$	$A_{\bar{1}+2}$
$A_{1\oplus 2}$	$A_{\bar{1}+2}$	$A_{\bar{1}+2}$	$A_{1\oplus 2}$	$A_{\bar{1}+2}$
$\overline{A_{\bar{1}\cdot 2}}$	$A_{1\oplus 2}$	$\overline{A_{\bar{1}\cdot 2}}$	$\overline{A_{\bar{1}\cdot 2}}$	$A_{1\oplus 2}$

$A_{1\otimes 2}$

$A_{1\otimes 2}$	$A_{1\otimes 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$
$A_{1\otimes 2}$	$A_{1\otimes 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$
$\overline{A_{1\cdot 2}}$	$\overline{A_{1\cdot 2}}$	$A_{1\otimes 2}$	$A_{1\cdot 2}$	$A_{1\cdot 2}$
$\overline{A_{1\cdot 2}}$	$\overline{A_{1\cdot 2}}$	$\overline{A_{1\cdot 2}}$	$A_{1\otimes 2}$	$A_{1\otimes 2}$
$\overline{A_{1\cdot 2}}$	$\overline{A_{1\cdot 2}}$	$\overline{A_{1\cdot 2}}$	$A_{1\otimes 2}$	$A_{1\otimes 2}$

図 6: $S^2(2)$ の IFS

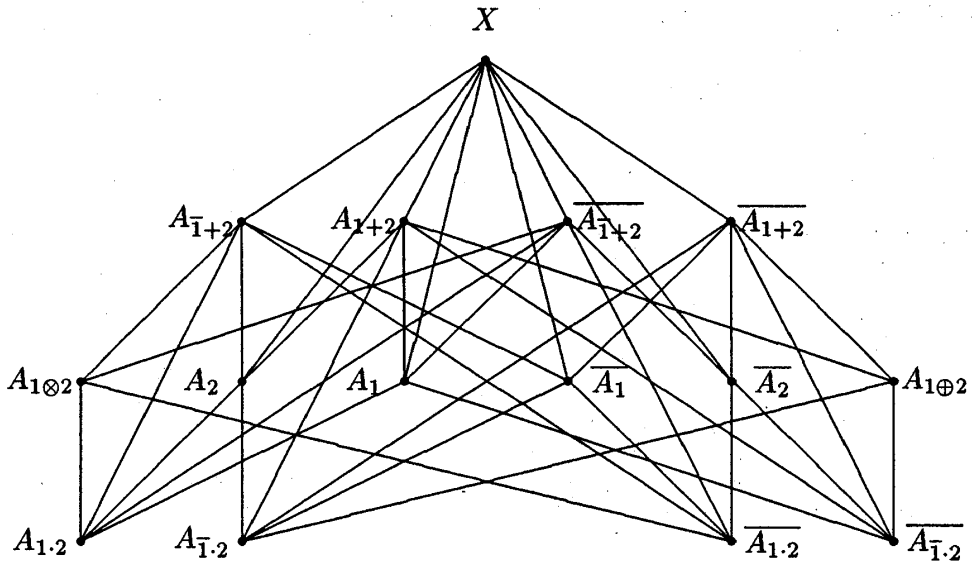

図 7: $S^2(2)$ の IFS の構成領域の Hasse 図

同様にして $S^2(n)$ を極限集合とする Monotone IFS が構成できる. 以上の IFS の構造は一見複雑そうにみえるが, 実際には Bool 演算則に基づき容易に決定できる. 分割された領域の図は Bool 演算表そのものである.

極めて trivial な場合以外, $S^3(n)$ (n 変数の $3CNF$の充足可能領域) を極限集合とする Monotone IFS の構成は困難である. この IFS の構成が困難であるということ自体, $3SAT$の intractability と本質的に関係していると思われる.

以上を考察して, やや強い主張をすると

$$S^1(n),\ S^2(n) \in P \implies Monotone\ IFS\text{で生成可能.}$$
$$S^3(n) \in NP \implies Monotone\ IFS\text{では生成不可能.}$$

となり, この結果から以下のような対応付けが可能となる.

$$class\ P \iff Self\ similar\ set$$
$$class\ NP \iff Partially\ self\ similar\ set$$

この予想の検証は今後の課題である.