A-013

複雑性クラスの崩壊と関数の粒度

Complexity class collapse and function granularity

小林 弘二
Koji KOBAYASHI

1. 概要

本論文では ATM の交替回数の違いによる計算能力の違いを用いて複雑性クラスを分離する．特にPH, NCの階層が正当であることを示す．

TM で計算可能な決定問題全体と同じ複雑性クラスRに真に含まれるある複雑性クラスを計算する ATM を考える．その ATM と同じ計算資源（実行時間・記憶領域）を使用してより少ない交替回数でそのクラスの問題を計算できる ATM が存在すると仮定すると，いくつかの複雑性クラスが崩壊して 1 つのクラスになる．この ATM は入力の任意の$(\neg, \vee)$の組合せ（つまり回路族全体）を含むため，Rと同じクラスとなる．しかし仮定よりRはこのクラスを真に含む．つまりこの結果は仮定条件と矛盾する．よって，ATM の交替回数が異なる場合，同じ計算資源では計算できない問題が存在する．

この結果を用いることにより，PH, NCの正当性を示すことができる．

2. ATM の計算能力

まず始めに用語の定義を行う．

定義 1. “AC^i”, “NC^i”, “Δ_k”, “Σ_k”, “Π_k”,“R”をそれぞれの決定問題を集めたクラスとする．

本論文では計算資源を制限した ATM を用いる．参考文献[1]より，$NC^i \mid i \geq 2$は$O(\log n)$領域と$O\left((\log n)^i\right)$時間の ATM により計算できる．よって計算資源を限定した ATM を用いることは妥当である．

定義 2. “δ_k”， “σ_k”， “π_k”を，同じ制限した計算資源を使用するΔ_k．Σ_k．Π_kとする．

また．本論文では複数のδ_kをまとめてσ_k．π_kとするため，δ_kの開始状況からの最初の遷移を決定性の遷移に制限した部分集合を定める．

定義 3. “δ'_k”を，開始状況からの最初の遷移が必ず決定性の遷移となるδ_kの部分集合とする．

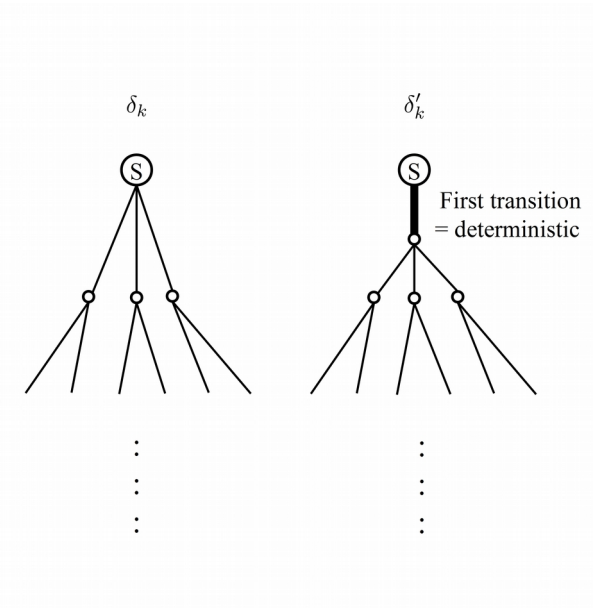

図 1: δ'_k

定理 4. $\forall A, B \in \delta'_k\,(A \vee B \in \sigma_k)$，$\forall A, B \in \delta'_k\,(A \wedge B \in \pi_k)$，$\forall A \in \delta'_k\,(\neg A \in \delta_k)$

証明. 本定理は自明である．

$A, B \in \delta'_k$は最初の遷移が決定性のため，（σ_k．π_kの計算の最初に非決定的に分岐することより）計算資源を追加することなくA, Bを同時に計算することができる．

またδ'_kを計算する ATM の受理状況と拒否状況を入れ替えることにより$co\delta'_k$を計算する ATM を構成できるため．
$\delta'_k = co\delta'_k$となる．

よって定理が成り立つ．□

σ_kとπ_kを組み合せることにより，任意の回路族を構成することができる．

定義 5. “p_k”を，始域のk桁目の値が 1 の時にのみ受理する射影関数の問題とする．“PFP”を，全てのp_kを集めた複雑性クラスとする．

定理 6. $PFP \subset NC^0$

証明. 本定理は自明である．$p^k \in PFP$は始域のk桁目の値を確認する問題であり，NC^0の回路で構成することができる．よって定理が成り立つ．□

定義 7. “WFF”を回路族の値判定問題に対応する複雑性クラスとする．

定理 8. $R = WFF$

証明. 本定理は自明である．WFFは決定問題であり明らかに$WFF \subset R$，またWFFは決定問題を計算する任意のDTM の遷移関数を模倣することが可能であり，$R \leq WFF$. よって定理が成り立つ．□

PFPは入力の任意の桁に対応するため，PFPを$(\neg, \vee, \wedge)$で組合せることによりWFF全体を構成することができる．

3. *ATM*の交替の正当性

上記の準備を元に，交替の回数により ATM の計算能力が真に異なることを示す．

仮に$PFP \subset \delta'_k \subsetneq R$の計算能力が$\sigma_k$と等しいとする．$\sigma_k$は組合せることにより$(\neg, \vee)$を実現することができる．また$PFP$は入力の任意の桁の値となり，また$(\neg, \vee)$は論理関数の完全系となるため，$\sigma_k$，$\delta'_k$，$PFP$を組合せることにより任意の$WFF$と等価な問題を構成することができる．任意の$WFF$の集合は$R$と等価になる．

しかし仮定より$\delta'_k \subsetneq R$のため，この結果は仮定と矛盾する．よってδ'_kとσ_kは等しくないという結論となる．

同様にしてδ'_kとπ_kの計算能力の違いを示すことができる．

定理 9. $\delta'_k \subsetneq \sigma_k, \delta'_k \subsetneq \pi_k \mid PFP \subset \delta'_k \subsetneq R$

証明. 背理法で$\delta'_k = \sigma_k \mid PFP \subset \delta'_k \subsetneq R$を証明する．簡単のため，$\delta'_k$は回路族に対応する TM とする．

この条件の元，

$\delta'_k = \sigma_k \mid PFP \subset \delta'_k \subsetneq R$

と仮定する．

仮定$\delta'_k = \sigma_k$と前述 4 より下記が成り立つ．

$\forall A, B \in \delta'_k \, (A \vee B \in \sigma_k = \delta'_k)$

$\forall A \in \delta'_k \, (\neg A \in \delta'_k)$

$PFP \subset \delta'_k$と上記の結果より，δ'_kは全てのPFPの$(\neg, \vee)$の組合せを含む．$(\neg, \vee)$は論理式の完全系のため，δ'_kは任意の論理式となる．よってδ'_kを回路族として考えるとWFFとなり下記が成り立つ．

$R = WFF \subset \delta'_k$

しかし，この結果は仮定$\delta'_k \subsetneq R$と矛盾する．

$\delta'_k \subset R = WFF \subsetneq \delta'_k$

よって背理法より$\delta'_k \subsetneq \sigma_k \mid PFP \subset \delta'_k \subsetneq R$が成り立つ．

$\delta'_k \subsetneq \pi_k \mid PFP \subset \delta'_k \subsetneq R$も同様に証明することができる．□

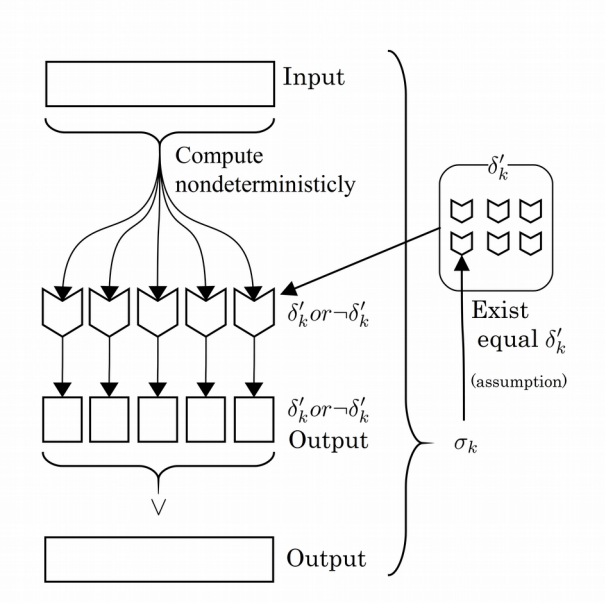

図 2: 交替回数の圧縮

系 10. $L \subsetneq NL, P \subsetneq NP, P \subsetneq coNP$

定理 11. $\delta'_k = \delta_k \mid NC^0 \subsetneq \delta_k$

証明. $\delta'_k \subset \delta_k$は定義より自明である．$\delta_k \leq_{NC^0} \delta'_k$を示すために，$\delta'_k$を計算する ATM:$M'_k$と$\delta_k$を計算する ATM:$M_k$を考える．$M'_k$と$M_k$は，計算開始状況からの最初の遷移が決定的であるかどうかのみの異なる．M_kからM'_kへの還元は高々 1 つの決定性の遷移関数を追加するのみで可能であり，M_kとM'_kの計算資源の違いは高々定数時間のみとなる．よって$NC^0 \subsetneq \delta_k$ならばδ_kに定数時間を追加したδ'_kもδ_kとなり，定理が成り立つ．□

系 12. $\delta_k \subsetneq \sigma_k \cup \pi_k \mid NC^0 \subsetneq \delta_k \subsetneq R$

上記の結果より，系としてNC, ACの各層の正当性，及びNL, Pの違いが示される．同様に$\Delta_k, \Sigma_k \cup \Pi_k$の違いも示される．

定理 13. $NC^i \subsetneq NC^{i+1}, \Delta_k \subsetneq \Sigma_k, \Delta_k \subsetneq \Pi_k$

証明. $\Delta_k \subsetneq \Sigma_k, \Delta_k \subsetneq \Pi_k$は明らかに成り立つ．

$NC^i \subsetneq NC^{i+1}$を示す．参考文献[1]より$NC^i \mid i \geq 2$は$O(\log n)$領域と$O\left((\log n)^i\right)$時間の ATM により計算できる．$PFP \subset NC^i \subsetneq R$のため，前述 9 より下記が成り立つ．

$NC^i = \delta_k \subsetneq \sigma_k \cup \pi_k \subset NC^{i+1} \mid i \geqq 2$

またNC^1, NC^2についても前述 10 より下記が成り立つ．

$NC^1 \subset L \subsetneq NL \subset NC^2$

よって定理が成り立つ．□

系 14. $AC^i \subsetneq AC^{i+1}, NL \subsetneq P$

定理 15. $NC \subsetneq P$

証明. 背理法を使用して証明する．

$NC = P$

と仮定する．仮定より$A \in P - Complete$を$B \in NC$に還元することができる．

しかしBはいずれかのNC^iに含まれる．よって$NC^i = NC^{i+1}$となるiが存在し，前述 13 と矛盾する．

よって背理法より定理が成り立つ．□

上記の結果を用いてPHの各層の正当性を示す．ただし証明の簡単化のため，参考文献[2]で示されている定理を用いる．

定理 16. $\Sigma_k \neq \Pi_k$

証明. 参考文献[2]定理 6.12 より

$\Sigma_k = \Pi_k \rightarrow \Sigma_k = \Pi_k = PH$

この対偶は下記のようになる．

$(\Sigma_k \subsetneq PH) \vee (\Pi_k \subsetneq PH) \rightarrow \Sigma_k \neq \Pi_k$

前述 13 より

$\Delta_k \subsetneq \Sigma_k \subset PH$

よって$\Sigma_k \neq \Pi_k$となる．□

系 17. $NP \neq coNP$

定理 18. $\Pi_k \nsubseteq \Sigma_k, \Sigma_k \nsubseteq \Pi_k$

証明. 背理法を使用して証明する．$\Pi_k \subset \Sigma_k$と仮定する．この仮定は$\overline{\Sigma_k} = \Pi_k \subset \Sigma_k$を意味する．よって

$\Pi_k \subset \Sigma_k$

$\rightarrow \forall A \in \Sigma_k \exists B \in \Sigma_k \left(\overline{A} = B\right)$

$\rightarrow \forall A \in \Sigma_k \exists B \in \Sigma_k \exists C \in \Pi_k \left(\overline{\overline{A}} = A = \overline{B} = C\right)$

これは$\Sigma_k \subset \Pi_k$を意味する．よって $\Sigma_k = \Pi_k$となる．

しかし，この結果は定理 16 と矛盾する．

よって背理法より $\Pi_k \nsubseteq \Sigma_k$となる．

$\Sigma_k \nsubseteq \Pi_k$も同様に証明することができる．□

定理 19. $\Sigma_k \subsetneq \Delta_{k+1}, \Pi_k \subsetneq \Delta_{k+1}$

証明. 背理法を使用して$\Sigma_k \subsetneq \Delta_{k+1}$を証明する．$\Sigma_k = \Delta_{k+1}$と仮定する．

参考文献[2]定理 6.10 より

$\forall k \geq 1 \left(\Delta_k \subset (\Sigma_k \cap \Pi_k) \subset (\Sigma_k \cup \Pi_k) \subset \Delta_{k+1}\right)$

よって

$\Sigma_k = \Delta_{k+1}$

$\rightarrow \Delta_k \subset (\Sigma_k \cap \Pi_k) \subset \Pi_k \subset (\Sigma_k \cup \Pi_k) \subset \Delta_{k+1} = \Sigma_k$

$\rightarrow \Pi_k \subset \Sigma_k$

しかし，この結果は前述 18 と矛盾する．

よって背理法より$\Sigma_k \subsetneq \Delta_{k+1}$となる．

$\Pi_k \subsetneq \Delta_{k+1}$も同様に証明することができる．□

定理 20. $PH \subsetneq PSPACE$

証明. 背理法を使用して証明する．$PH = PSPACE$と仮定する．仮定より$A \in PSPACE - Complete$を$B \in PH$に還元することができる．

しかしBはいずれかのΔ_kに含まれる．よって$\Delta_k = \Delta k + 1$となるkが存在し，前述 19 と矛盾する．

よって背理法より定理が成り立つ．□

4. 代数的構造の冪等性

上記の結果では，代数的構造の冪等性と関数合成の半順序性が重要な役割を果たす．代数的構造はある集合を渡る代数により構成される構造であり、代表的な例として普遍代数のクローンや群論のマグマなどを挙げることができる．代数的構造B°は基底集合Bと関数$\circ$から生成することができ

るが，この時，B°は冪等性$(B^{\circ})^{\circ} = B^{\circ}$という重要な性質を持つ．しかし，$B^{\circ}$の部分に着目すると，それぞれの元は関数の合成について半順序を構成し，冪等とならない．

この全体の冪等性と部分の半順序性を用いることによりPH, NCを分離することができる．もし半順序で鎖となる 2 つの部分集合が一致するのならば，冪等性よりその部分集合は半順序全体と等しくなる．また部分集合が半順序全体と等しくないのならば，その部分集合は鎖の関係となる他の部分集合と一致しない．

下記に代数的構造を用いて複雑性クラスを分離する証明図を示す．ここでは簡単のため$P \neq NP$に限定しているがこの手法は交替性 TM 全般に適用することができる．

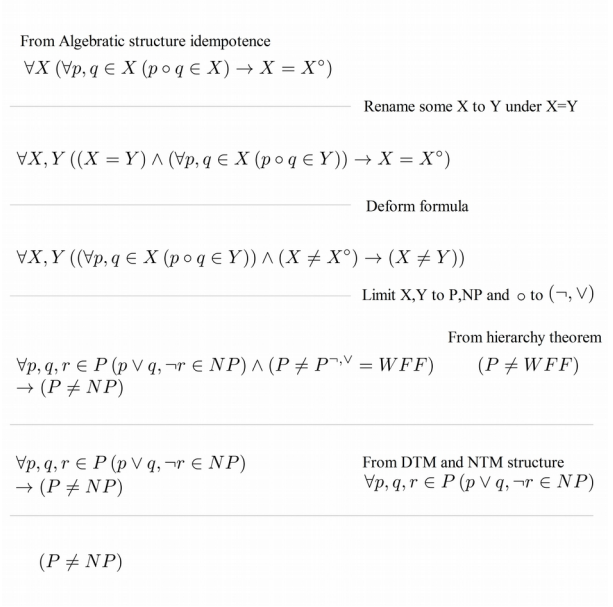

図 3: 証明図

参考文献

[1] W.L. Ruzzo, “On Uniform Circuit Complexity”, J. Comput. System Sci. 22 (3) 365–383 (1981)

[2] 荻原 光徳, “複雑さの階層” (2006)