# 計算量理論特論 2 レポート課題

251903014 社会情報学専攻 川嶋 康太

本レポート課題では，問題 3,5,7 を選択した．

## 問題 3

**問題** $PERM \in \#P$

問題 $PREM$ が $\#P$ に属することを講義プリントの定義 16 に基づいて証明せよ．

*Proof.* $PERM \in \#P$ となることを示すためには，任意の $n$ 次行列 $A = (a_{i,j})$ に対して，$perm(A) = \#ACC(M(A))$ となるような非決定性多項式時間チューリング機械 $M$ が存在することを示す必要がある．ここで，$S_n$ を $n$ 次置換の集合とし，任意の入力 $A$ に対して，$M$ の手続きを以下のように定義する：

1. $\sigma \in S_n$ をランダムに選択する．
2. 「$a_{i,\sigma_i} = 0$ の時には拒否をし，$a_{i,\sigma_i} = k(k \neq 0)$ の時には $k$ だけパスを分岐させる」という操作を $i = 1$ から $i = n$ まで繰り返す．
3. $i = n$ まで拒否が出なかった場合は，そのパスを受理する．

このように定義された $M$ において，任意の入力 $A$ に対し，明らかに以下のことが成立する：

$$\#ACC(M(A)) = \Sigma_{\sigma \in S_n} \Pi_i^n a_{i,\sigma(i)} = perm(A)$$

というのも，選ばれた $\sigma$ に対して，受理するパスの数は 2,3 の手続きによって $\Pi_i^n a_{i,\sigma(i)}$ 個であるからである．

□

## 問題 5

**問題** $NP = \bigcup_{k>0} PCP[\mathcal{O}(\log n), n^k]$

講義プリントの命題 21（$NP = \bigcup_{k>0} PCP[\mathcal{O}(\log n), n^k]$）を証明せよ（定理 27 を使わずに証明すること）．

*Proof.* $NP = \bigcup_{k>0} PCP[\mathcal{O}(\log n), n^k]$ を示すことは，$NP = PCP[\mathcal{O}(\log n), poly(n)]$ を示すことと同値である．また，$NP$ と $PCP$ の定義から $NP \subseteq PCP[\mathcal{O}(\log n), poly(n)]$ は自明に成り立つ．よって，$PCP[\mathcal{O}(\log n), poly(n)] \subseteq NP$ を示すだけで十分である．

$L \in PCP[\mathcal{O}(\log n), poly(n)]$ とし，$V$ を $L$ に対する検証者とする．この時，与えられた $x \in L$ に対して，$L \in NP$ が成立することを言うために必要な多項式時間アルゴリズム $V'$ を構成すれば良い．しかし，$x \in L$（$|x| = n$）であることにより，$L \in PCP[\mathcal{O}(\log n), poly(n)]$ なることを保証する良い証明（ビット列）$\pi_x$ は単純には使うことができないことに注意しなければならない．なぜなら，定義から $\pi_x$ の長さは指数長でもあり

うるからである．そこで，$x$ を $|\varphi_x| = \mathcal{O}(\log n)$ となるような $\varphi_x$ に圧縮することを考える．すると，このようにして得られた $\varphi_x$ に対して，$|\pi_{\varphi_x}| = 2^{\mathcal{O}(\log n)} = poly(n)$ が成立する．

ここで，多項式時間アルゴリズム $V'$ を，$V(x, \pi_x, z) = 1$ の時に $V'(\varphi_x, \pi_{\varphi_x}) = 1$，$V(x, \pi_x, z) = 0$ の時に $V'(\varphi_x, \pi_{\varphi_x}) = 0$ となるものとして定義する（$|\pi_{\varphi_x}| = poly(n)$ であるので，この定義は well-defined である）．すると，以下が成立する：

$$\begin{aligned}\varphi_x \in L &\iff x \in L \\ &\iff \exists \pi_x \in \{0,1\}^*[V(x, \pi_x, z) = 1] \\ &\iff \exists \pi_{\varphi_x} \in \{0,1\}^{poly(n)}[V'(\varphi_x, \pi_{\varphi_x}) = 1]\end{aligned}$$

よって，$L \in NP$ である．ゆえ，$PCP[\mathcal{O}(\log n), poly(n)] \subseteq NP$ が成立する． □

## 問題 7

**問題**

計算量理論特論 1,2 で扱っていない計算量クラスを 1 つ選んで A4 用紙 1 2 枚で紹介せよ

量子計算量理論おける計算クラスである「$QCPH$」と「$QPH$」を紹介する．これら計算クラスはどちらも計算量理論特論 1 の方で紹介された「$PH$」というクラスの量子的一般化（quantum generaization）となっている．これらのクラスは，2018 年の論文 [2] で定式化された新しいクラスのようである．

私は，これらのクラスをわかりやすく紹介するための量子計算量理論の十分な知識を持ち合わせていないので，まず [2] のアブストラクトを紹介する（そして，簡単にでもこのクラスの意義を理解していただけると幸いである）．その後，クラスを定義（実際の定義はもう少し複雑であることに注意する必要がある．完全性と健全性の条件を定式化することを省いている.）をして，興味深い結果を述べる．最後に，論理学と計算量理論の関係を網羅的に示してくれている興味深い図を見つけたので，その図を掲載して終わることにする（$QCPH$ や $QPH$ の立ち位置を知るのに便利）．

**アブストラクト [2]**

多項式時間階層 ($PH$) は，計算複雑性理論における分割を証明するための強力な道具であることを証明した．ここでは，二つの $PH$ の量子的一般化が，（$PH$ と同様に）量子状態における分割を証明しうるかどうかを確認する．一つ目の一般化は $QCPH$ といい，これは古典的証明を用いる．そして，二つ目の一般化は $QPH$ といい，これは量子証明を用いる．前者については，Karp-Lipton 定理と戸田の定理の量子版を示す．後者に関しては，半正定値プログラムを効率的に解くための楕円法を使用して，その 3 階目である $Q\Sigma_3$ を $NEXP$ へ位置づける．これらの結果は，$QMA(2)$（二つのエンタングル証明を伴った Quantum Merlin-Arthur($QMA$)）に対する 2 つの意味ある結果を与える．一つ目は，もし $QCPH = QPH$ が成立するならば，この時 $QMA(2)$ は数え上げ階層 (特に，$P^{PP^{PP}}$) に属するというものである．二つ目は，$QMA(2) = Q\Sigma_3$ 出ない限り，$QMA(2)$ は $NEXP$ に厳密含意されるというものである．

**定義 0.1** $PH$

言語 $L$ が $\Sigma_i$（PH の i 階目）に属するとは，多項式時間非決定性チューリング機械 $M$ が存在し，以下の条件を満たすことをいう：

1. $x \in L \implies \exists y_1 \forall y_2 ... Q_k y_k [M(x, y_1, ..., y_k) = 1]$

2. $x \notin L \implies \forall y_1 \exists y_2 ... \bar{Q}_k y_k [M(x, y_1, ..., y_k) = 1]$

$QCPH$ も $QPH$ も $PH$ の定義からのアナロジーによって定式化されるに至った [2].

**定義 0.2** $QCPH$**(簡略 ver)**

約定問題 (promise problem)$A = (A_{yse}, A_{no})$ が $QCPH$ の i 階目 $QC\Sigma_i$ に属するとは，一様多項式サイズ生成された量子回路 $V$ が存在し，以下の条件を満たすことをいう：

1. $x \in A_{yes} \implies \exists y_1 \forall y_2 ... Q_k y_k [Pr[V(x, y_1, ..., y_k) = 1] \geq 2/3]$
2. $x \in A_{no} \implies \forall y_1 \exists y_2 ... \bar{Q}_k y_k [Pr[V(x, y_1, ..., y_k) = 1] \leq 1/3]$

$QCPH$ それ自体は，以下のように定義される．

$$QCPH = \bigcup_i QC\Sigma_i = \bigcup_i QC\Pi_i$$

$QCPH$ は $QCMA$ の一般化となっており，$QC\Sigma_1 = QCMA$ が成立する．

また，$QCPH$ は以下の事実にあるように，$PH$ の一般化でもある．

**事実 0.3**

任意の $i$ に対して，$\Sigma_i \subseteq QC\Sigma_i$ と $\Pi_i \subseteq QC\Pi_i$ が成立する．よって，$PH \subseteq QCPH$ が成立する．

**定義 0.4** $QPH$**(簡略 ver)**

約定問題 (promise problem)$A = (A_{yse}, A_{no})$ が $QPH$ の i 階目 $Q\Sigma_i$ に属するとは，一様多項式サイズ生成された量子回路 $V$ が存在し，以下の条件を満たすことをいう：

1. $x \in A_{yes} \implies \exists \rho_1 \forall \rho_2 ... Q_k \rho_k [Pr[V(x, \rho_1, ..., \rho_k) = 1] \geq 2/3]$
2. $x \in A_{no} \implies \forall \rho_1 \exists \rho_2 ... \bar{Q}_k \rho_k [Pr[V(x, \rho_1, ..., \rho_k) = 1] \leq 1/3]$

ここで，$\rho_j$ は多項式回キュービット上の量子状態のことである．
$QPH$ それ自体は，以下のように定義される．

$$QPH = \bigcup_i Q\Sigma_i = \bigcup_i Q\Pi_i$$

$QMA = Q\Sigma_1$ と $QMA(2) \subseteq Q\Sigma_3$ となることに注意せよ．

以下が興味深い結果である．

**定理 0.5 A quantum-classical analogue of Toda' s theorem**

$QCPH \subseteq P^{PP^{PP}}$

さらに，上記定理と $QMA(2) \subseteq QPH$ から，以下のことが系として得られる．

**定理 0.6**

$QCPH = QPH$ が成立するならば，$QMA(2) \subseteq P^{PP^{PP}}$ が成立する．

**定理 0.7 インフォーマル版**

$Q\Sigma_2 \subseteq EXP$ と $Q\Pi_2 \subseteq EXP$ が成立する．

**定理 0.8　インフォーマル版**

$QMA(2) \subseteq Q\Sigma_3 \subseteq NEXP$ と co-$QMA(2) \subseteq Q\Pi_3 \subseteq NEXP$ が成立する．

**定理 0.9　A quantum-classical Karp-Lipton theorem**

Precise-$QCMA \subseteq BQP_{/mpoly}$ が成立するならば，$QC\Pi_2 = QC\Sigma_2$ が成立する．

このように，二つの $PH$ の量子的一般化のクラスである $QCPH$ と $QPH$ についてはたくさんの有意義な結果が示されている．私は最近，圏論的論理学に興味を持っているので，圏論的には $PH$ のみならず，$QCPH$ や $QPH$ はどのように定式化されるのか調査してみるのは面白いことだと思う．

最後に，論理学と計算量理論の関係を網羅的に示してくれている興味深い図を掲載する．

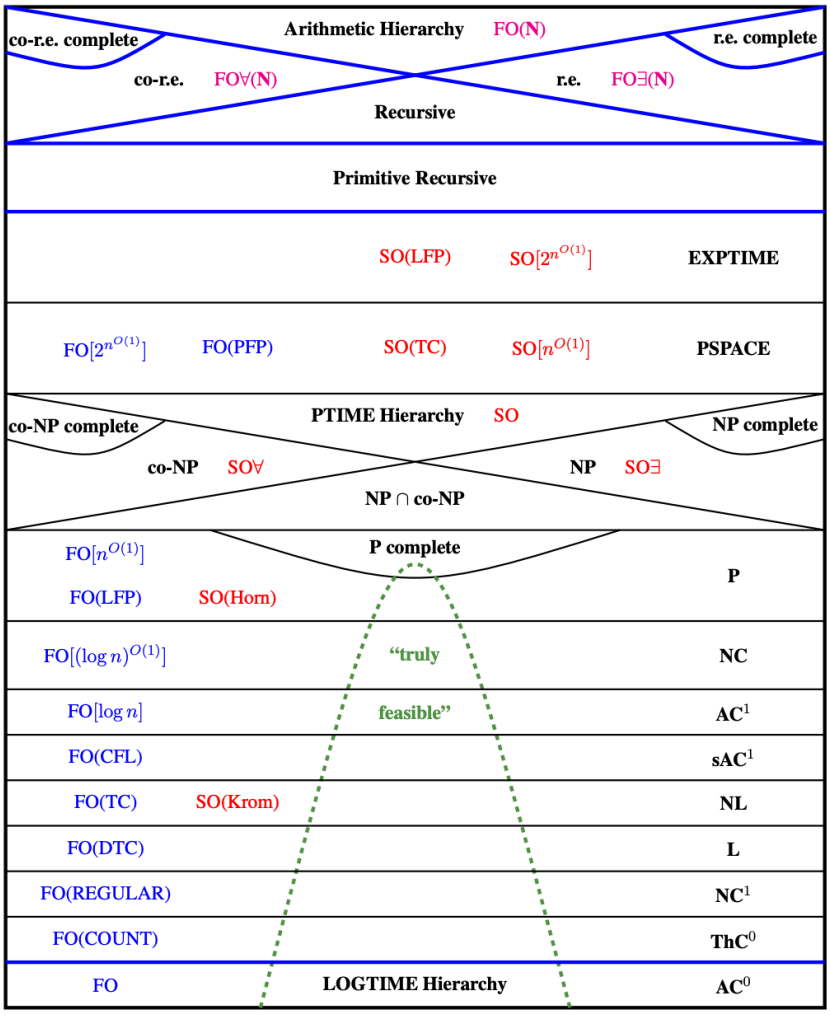


図 1　計算量クラスの階層 [3]

## 参考文献

[1] Notes on Complexity Theory Lecture 21, Jonathan Katz , 2011

[2] Quantum generalizations of the polynomial hierarchy with applications to QMA(2), Sevag Gharibian Miklos Santha Jamie Sikora Aarthi Sundaram Justin Yirka, 2018

[3] Descriptive Complexity, Neil Immerman, 2015