論 文 の 内 容 の 要 旨

論文題目　Worst-Case And Average-Case Complexity of Minimum Circuit Size Problem and Its Variants
（回路最小化問題とその変種の最悪時及び平均時計算量）

氏　名　平原　秀一

今日の情報通信社会の基盤技術として公開鍵暗号系が広く使われているが、その安全性は$P \neq NP$よりもはるかに強い仮定に基づいており未解決である。計算量理論の究極的な目標のひとつは数学的に証明された公開鍵暗号系を構成することにあるが、計算量理論には$P \neq NP$を始めとして未解決問題が山積している。Impagliazzo (1995)の分類に従うと、我々の現在の計算量理論の知識と一貫性のある5つの世界（Algorithmica, Heuristica, Pessiland, Minicrypt, Cryptomania）がある。これらは$P \neq NP$, $DistNP \not\subseteq AvgP$, 一方向性関数の存在, 公開鍵暗号の存在の4つの未解決問題が成立するか否かによって分類されており、どれか一つの世界が真の世界に対応している。これらの未解決問題は仮定の強い順に並んでおり、その逆を示すことは計算量理論における中心的な未解決問題である。つまり、$True \Longrightarrow P \neq NP \Longrightarrow DistNP \not\subseteq AvgP \Longrightarrow \exists$一方向性関数 $\Longrightarrow \exists$公開鍵暗号。ひとつの矢印「$\Longrightarrow$」を示すことはひとつのありうる世界を除外することに対応し、4つのすべての矢印を示すことによって安全な公開鍵暗号系の存在を示すことができる。

しかしながらそれら中心的な問題の解決には重大な障壁があることが知られている。例えば$P \neq NP \Longrightarrow DistNP \not\subseteq AvgP$を解決する（つまり、Heuristicaを除外する）ためには、**相対化する**証明技法では示せないし、多項式階層が潰れない限り**ブラックボックス帰着**の限界を突破する必要がある。

本論文では計算量理論における中心的な問題である**最小記述量問題**に着目し、その障壁のひとつを突破する。最小記述量問題とは、与えられた文字列を最小の「プログラム」へと圧縮したときの長さを問う問題である。プログラムが回路で表現される場合には回路最小化問題（Minimum Circuit Size Problem; MCSP）と呼ばれ、プログラムが効率的なチューリングマシンで表現される場合には最小時間制限付きコルモゴロフ記述量問題（MINKTまたはMKTP）と呼ばれる。これらの近似問題に関して、平均時計算量と最悪時計算量が同値になることを示す。これはブラックボックスでない帰着手法で証明されてお

り、適切な仮定の下でブラックボックス帰着を突破している初めての結果である。この結果はHeuristicaを除外するための新しいアプローチとしても見ることができる。すなわち、NPの最悪時・平均時計算量の同値性を示すためには、近似版最小記述量問題のNP完全性を解決すれば十分である。

次に、MCSPの様々な困難性を示す。埋め込みクリーク予想やランダム3SATなどに関する平均計算量の仮定の下でMCSPやMKTPが計算困難であることを示すことにより、$\mathrm{MCSP} \notin \mathrm{coNP}$であるというさらなる証拠を与える。また、MCSPオラクルの下で補助入力一方向性関数を破れることを示し、AllenderとDas (2017)による統計的ゼロ知識証明(SZK)の下でのMCSPの困難性を改善する。

ブラックボックス帰着の限界と同様に、SZK困難性をNP困難性に改善するためには現在の証明手法には限界があることを示す。具体的には**オラクル独立帰着**という概念を導入し、ほとんどのMCSPへの帰着手法はオラクル独立であり、そのような手法ではNP完全性を解決することができないという証拠を示す。

それゆえ、(一般の回路最小化問題ではなく）制限された回路クラスに関する回路最小化問題に着目する。Masek (1979)により$¥DNF$に対する回路最小化問題はNP完全だと知られていたが、DNFよりも表現能力の高い回路クラスに関する回路最小化問題についてのNP完全性は（重要性が認識されていたにも関わらず）約40年間未解決であった。本論文では$\mathrm{DNF} \circ \mathrm{XOR}$回路最小化問題のNP完全性を解決する。

さらにいくつかの追加の結果を示す。大雑把に言うと「計算可能性版のMCSPが非適応多項式時間帰着のもとでNP困難ではない」というAllenderの予想（2012）を否定する証拠を示す。弱い計算量理論の仮定に基づく初めての自然なNPの中間の問題を構成する。MCSPと回路下界の関係を改善する。仮定なしでのMCSPに対する回路下界を示す。