審 査 の 結 果 の 要 旨

氏　　名　平原　秀一

本論文は，計算量理論の中心的な問題の一つである回路最小化問題およびその変種を軸にして，平均時計算量と最悪時計算量との間の関係，回路最小化問題の困難性などに関する新しい結果を与えている．平均時計算量と最悪時計算量との間の関係は公開鍵暗号の安全性にも関連し，特にNP完全問題が平均時に多項式時間で解けるか否かは計算量理論における重要な未解決問題の一つである．本論文の主要成果の一つは，回路最小化問題とその変種である時間制限付きコルモゴロフ記述量最小化問題についての平均時計算量と最悪時計算量の同値性であり，これは上記の未解決問題に新たな進展を与えるものである．既存の平均時・最悪時計算量の同値性を示すための主な手法である「ブラックボックス帰着」には適用できる問題のクラスに限界があることが知られていたのに対し，提案手法では「非ブラックボックス帰着」を用いることによってその限界を突破している．この結果に基づき，本論文ではさらに，上記未解決問題に対する否定的結果を得るための道筋を示し，そのために必要となる回路最小化問題のNP困難性を示す上での障壁に関する結果，制限された回路クラスにおける回路の最小化問題のNP困難性など，様々な新しい結果を示している．

本論文は以下のように全１３章からなる．

第１章は序論である．

第２章は，前準備として，回路最小化問題や時間制限付きコルモゴロフ記述量最小化問題（以下，単にコルモゴロフ記述量最小化問題と記す）の定義などの予備知識を与えている．

第３章は，回路最小化問題やコルモゴロフ記述量最小化問題の困難性が，一方向関数の存在やランダム３SAT問題の困難性の仮定などから導かれることを示している．

第４章は，回路最小化問題とコルモゴロフ記述量最小化問題について，平均時計算量と最悪時計算量の同値性を，非ブラックボックス帰着を用いて証明している．

第５章は，第４章の帰着手法が本質的にブラックボックス帰着では置き換えられないことを示している．

第６章は，計算可能性版の回路最小化問題について新しい困難性を示し，Allenderの予想を否定する証拠を与えている．

第７章は，回路最小化問題のNP完全性を証明することは，回路下界を証明するよりも難しいことを，先行研究よりも一般的な帰着の下で証明している．

第８章も，回路最小化問題のNP完全性を示すことの難しさに関する結果である．第７章が決定的帰着による証明の難しさを示したのに対し，本章では，より一般的な乱択帰着の下でも回路最小化問題のNP完全性を証明することがある意味で難しいことを示している。具体的にはオラクル独立帰着という概念を提案することにより，既存の帰着手法ではNP完全性を示せないことを証明している．

第９章は，DNF-XOR回路という制限された回路クラスについて，回路最小化問題のNP完全性を示している．これは，1979年にDNF回路についてのNP完全性が示されて以来，より表現能力の高い回路クラスについてのNP完全性を示した初めての結果である．

第１０章は，コルモゴロフ記述量最小化問題の困難性を局所帰着に基づいて議論している．主要な結果の一つは非一様な局所帰着による行列式の計算問題からコルモゴロフ記述量最小化問題への帰着である．先行研究で一様な局所帰着ではそのような帰着が存在しないことが知られていたため，上述の結果は帰着の一様性が重要であることを示している．

第１１章は，NP完全ではないがPにも属さない「NP中間問題」について考察している．P≠NPならばNP中間問題が存在することは1975年にLadnerにより証明されていたが，これまでは人工的な問題しか知られていなかった．本章では，補助入力一方向性関数の存在という仮定のもとで回路最小化問題の一種がNP中間問題であることなどを示しており，そのような弱い仮定のもとでの自然なNP中間問題を与えた初めての結果である．

第１２章は，回路最小化問題の困難性のさらなる証拠として，同問題の回路下界を与えている．

第１３章は，結論を述べるとともに，未解決問題と今後の研究の展望について述べている．

以上要するに, 本論文は, 回路最小化問題に関して様々な新しい結果を与えるとともに, それを通じて最悪時計算量と平均時計算量の関係に関する重要な未解決問題の解決に向けての進展を与えるものであり、コンピュータ科学、特に計算量理論分野に対する貢献が大きいものと判断される.

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる.