数学と情報科学で解き明かす多様な対象の数理構造と活用　　2022 年度
2020 年度採択研究代表者　　年次報告書

平原 秀一

情報・システム研究機構 国立情報学研究所
准教授

メタな視点に基づく計算量理論の新展開

研究成果の概要

2022 年度の主要な成果として、部分関数版回路最小化問題（MCSP*）の NP 完全性の解決をした（原著論文 1）。この研究成果は理論計算機科学のトップ会議である FOCS に採択されたうえ、Complexity Result of the year 2022 に選出された。以下に研究成果の概要を述べる。

回路最小化問題（Minimum Circuit Size Problem; MCSP）の歴史は古く、少なくとも NP 完全性の理論が創始された 1970 年代までさかのぼる。計算量理論の根源的な定理である Cook―Levin の定理は、いくつかの自然な問題が NP 完全であることを示した。この定理は、冷戦の時代に独立に Cook と Levin に証明されたが、Cook（1971 年）よりも Levin は2年遅く論文を出版した。というのも、Levin は回路最小化問題の NP 完全性を示すために出版を遅らせたといわれている。結局、回路最小化問題が NP 完全かどうかは今でも未解決であるが、1973 年の Levin の論文では部分関数版の DNF 式最小化問題（DNF-MCSP*）の NP 完全性を証明している。この論文以来、DNF 式（＝深さ2段に制限された回路）ではなく一般の回路に関する部分関数版回路最小化問題（MCSP*）の NP 完全性は長い間未解決であった。原著論文 1 では、この未解決問題を解決した。

また、 この成果は「Heuristica の除外」という重要な未解決問題に対する進展でもある。Heuristica の除外とは、NP の平均時・最悪時計算量が同等に困難であるかを問う未解決問題である。この未解決問題を解決することは、暗号の安全性の解析にとって重要なステップである。FOCS 2018 の研究成果では、回路最小化問題の近似問題が NP 完全であるということを証明できれば、Heuristica を除外できる、ということを示している。原著論文 1 では、部分関数版回路最小化問題の NP 完全性を示している。従って、部分関数ではなく全域関数版について NP 完全性を示すことができれば、Heuristica の除外も可能となる。

【代表的な原著論文情報】

1) “NP-Hardness of Learning Programs and Partial MCSP.” In Proceedings of the Symposium on Foundations of Computer Science (FOCS 2022).
2) “Hardness Self-Amplification from Feasible Hard-Core Sets.” In Proceedings of the Symposium on Foundations of Computer Science (FOCS 2022).
3) “Symmetry of Information from Meta-Complexity.” In Proceedings of Computational Complexity Conference (CCC 2022)