論文審査の結果の要旨

氏名　濱野 健二

本論文は「Analysis and Applications of the T-complexity (T-complexity の解析と応用)」と題し、７章から構成されている。多くの情報セキュリティシステムでは、その安全性が暗号鍵などの２値系列のランダム性に基づいているため、系列に何らかの偏りがないかを調べる乱数検定が、情報セキュリティシステムの安全性に非常に重要となる。その乱数検定においては、系列のランダム性を測るための指標としての複雑度(Complexity)が重要な役割を果たしている。本論文では、そのような複雑度として T-complexity を取り上げ、理論およびシミュテーションによりその特性を解析すると共に、データ圧縮や乱数検定への実用的な応用法を提案している。

第１章「Introduction」では、乱数検定や複雑度に対する研究の背景, 目的および従来研究に対する本研究の位置付けを述べている。さらに、T-complexity の基になっている T-code や関連する LZ-complexity, 統計的乱数検定法などの基本概念をまとめている。

第２章「Forward T-decomposition」では、T-complexity を求めるための系列の新しい分解アルゴリズムを提案している。従来の分解アルゴリズムは、全系列が揃って初めて開始できるオフラインアルゴリズムであったのに対し、本章で提案された分解アルゴリズムは逐次的に処理できる特徴がある。さらに、数値実験により従来のものより、高速に T-complexity が求められることを実証している。

第３章「Differential Equation Method for Derivation of the Formulas of the T-complexity and the LZ-complexity」では、微分方程式を用いて T-complexity のプロファイルを導出する新しい方法論を提案している。従来、T-complexity 最大系列のプロファイルが対数積分関数（li 関数)で表現できることが実験的に予想され理論的に証明されていたが、li 関数が現れる本質的な理由が分かっていなかった。しかし、本章の解析により、T-complexity 最大系列のプロファイルが必然的に li 関数で表されることが明らかにされている。また、同様の手法により、一般系列の T-complexity や、LZ-complexity のプロファイルも導出できることも示されている。

第４章「Properties of the Maximum T-complexity Sequences」では、T-complexity 最大系列がどのような特性を持つかを，乱数検定などを適用することにより解析している。その結果、T-complexity 最大系列は LZ-complexity 最大系列よりもランダム性が少ないことを明らかにすると共に、T-complexity 最大系列の非ランダム性の原因を定性的、定量的に考察している。

第５章「Application of the forward T-decomposition to Data Compression」では、３章で提案した系列分解法(forward T-decomposition)のデータ圧縮への応用を取り扱っている。系列の分解法とデータ圧縮符号は密接に関係しており、LZ-complexity の分解法を利用した Unix の compress は比較的性能のよいデータ圧縮符号として知られている。

しかし、T-complexity に対応した性能のよいデータ圧縮法は今まで知られていなかった。本章では、辞書式データ圧縮法において、辞書に登録されるフレーズを forward T-decomposition を利用して登録するデータ圧縮法を提案している。さらに、それらが従来知られていた T-decomposition を利用したデータ圧縮法や compress などより性能がよいことを、実際のファイル圧縮性能を比較することにより実証している。この成果は、T-complexity が系列のランダム性を検出するよい能力を持っていることの傍証となっている。

第 6 章「Application of the T-complexity to Randomness Testing for Cryptography」では、T-complexity を用いた新しい乱数検定法(T-complexity 検定)を提案している。T-complexity 検定の具体的な構成法を示すと共に、その検定が性能のよい検定法となっていることを実証している。乱数検定としては，NIST（米国国立標準技術研究所）の乱数検定ツールが世界的によく用いられている。しかし、それに含まれていた LZ-complexity に基づく LZ 検定に問題があり、排除された状況になっている。これに対して、本章で提案された T-complexity 検定では、そのような問題がないことを明らかにすると共に、従来の LZ 検定やそれを改良した修正 LZ 検定よりも検定能力が高いことを示している。さらに、NIST 乱数検定ツールではほとんど検出できないが、T-complexity 検定で検出可能な非乱数系列が存在し、T-complexity 検定は NIST 乱数検定の弱点を補完できる検定法であることが示されている。

第 7 章「Conclusions」では、本論文の成果をまとめると共に、今後の研究課題を示している。

なお，本論文の成果は、山本博資との共同研究であるが、論文提出者が主体となって新しいアルゴリズムの提案、解析、シミュレーションを行なったものであり、論文提出者の寄与が十分であると判断する。

したがって、博士（科学）の学位を授与できると認める。