別紙１－１

論文審査の結果の要旨および担当者

報告番号	※　甲　第　　号

氏　　名　　林　怡伶

論　文　題　目　Combinatorial designs and codes related to information-communication

（情報通信に関連した組合せデザインと組合せ符号）

論文審査担当者

主　査　　名古屋大学教授　　神保　雅一

名古屋大学教授　　平田　富夫

名古屋大学教授　　柳浦　睦憲

名古屋大学准教授　　佐藤　潤也

別紙１－２

論文審査の結果の要旨

林怡伶氏提出の学位論文は「Combinatorial designs and codes related to information-communication」と題し，４章からなる．本学位論文は、離散数学に関連する組合せデザイン、符号理論、暗号の理論の境界分野の研究論文である。組合せデザインの研究は、1920 年代に統計学の一分野である実験計画法への応用が見出されて盛んになり、その後、コンピュータの発達やインターネットの普及に伴い、情報通信分野での重要性が高まり、関連する符号、暗号の研究と共に組合せデザインの研究が進展してきた。

本論文では、組合せデザイン・組合せ符号の情報通信への応用における最適構造とその存在性および構成法に焦点を絞って、これらの組合せ構造に関連する２つのテーマに関する研究成果をまとめている。１つは、量子ジャンプ符号への応用を目的として導入された t-spontaneous emission error design (t-SEED)と呼ばれる組合せデザインに関する成果であり、もう一つは、多元接続通信チャネルにおける通信プロトコルの１つである衝突回避符号(conflict-avoiding code, CAC)とよばれる組合せ符号の最適性、存在問題、構成法に関する結果である。

本論文は 4 章で構成される。第 1 章では、本研究の背景を述べ、必要な概念を定義して、既知の結果をまとめている。

第 2 章では、t-SEED と呼ばれる組合せ構造の組合せ的特徴付け、構成法およびその暗号への応用について議論している。t-SEED は t-デザインと呼ばれる古典的な組合せデザインの満たすべき条件を緩和した複数のデザインの集合として定義される。本論文では、それらのデザインの数が与えられたパラメータのもとで上限を達成する最適な t-SEED は会合数１の t-デザインの large set と呼ばれる組合せ構造と同値であることを明らかにした。さらに、その特徴付けを用いて、ある種の最適な t-SEED の非存在を示した。次に、2 つの t-SEED を合成して新たな t-SEED を構成する方法、および t-SEED と直交配列の large set を用いた、より点の数が多い t-SEED の再帰的な構成法などを与えた。さらに、t-SEED が持つ組合せ論的な均衡性を利用して、秘密分散暗号への応用を提案し、先行研究と本論文の結果を t-secure, perfect などの概念および鍵空間のサイズについて比較し、t-SEED による暗号の有効性を示した。

第 3 章では、衝突回避符号とよばれる組合せ符号について、重み 3 の場合に剰余環における 2 の位数に関する数論的な性質および円分多項式の性質を調べ、符号長が奇数の衝突回避符号の系列について、すべての差がちょうど１回ずつ現れ、符号語数の上限を達成するタイトな衝突回避符号の存在を明らかにした。さらに、タイトな符号が存在しない場合についても、$n \equiv 1 \pmod 8$ の場合に最大符号語数を持つ最適な等差衝突回避符号の構成法を与えた。重み 4 の場合については、衝突回避符号の構成問題を有向グラフにおけるある条件を満たす頂点の選択問題として表現し、剰余環における 2 と 3 の位数に関する性質を用いて最大符号語数の漸化式を求め、一般の符号

長 n に対する最大符号語数の問題を n=m, 2m, 3m, 6m, 12m, 24m (m は 6 と素な正整数) の場合に帰着できることを示した。特に、符号長が n = 3m, 12m と一部の n = 24m の場合は一般に最大符号語数が決定できることを証明し、その構成法を与えた。

第 4 章は、本論文で得られた成果と今後の課題のまとめである。

本論文では、組合せデザイン・組合せ符号の最適構造および構成法・存在問題に関する研究成果を通して、情報通信の数理的基礎に関する重要な知見を与えた。その研究成果は、３編の著名な国際誌に掲載され、離散数学および情報通信の研究者に注目されており、学術的価値は高い。よって審査委員は全員一致して、林怡伶君が博士（情報科学）の学位を授与されるに十分な資格を有するものと判定した。