報告番号	※甲　　第　　号

主　論　文　の　要　旨

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)

氏　名　Yiling Lin

論　文　内　容　の　要　旨

離散数学の研究分野は広く、その応用範囲は情報科学を含む様々な分野に及んでいる。本学位論文で扱う組合せデザイン、符号理論、暗号の理論は組合せ構造を研究する離散数学の一分野であり、統計学、情報通信、遺伝子情報、オペレーションズ・リサーチなどの分野に多くのアプリケーションがある。

また、数学的には、代数、数論、有限幾何などと深い関係があり、理論、応用の両方の側面から研究が発展してきた。組合せデザインの研究は、1920 年代に R. A. Fisher により統計学の一分野である実験計画法の研究として始まり、統計的最適性を持つ組合せ構造に関する研究が行われてきた。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、符号化方式や情報セキュリティなど情報通信分野での重要性が高まり、それに関連する組合せデザインや組合せ符号の研究が進展した。組合せデザイン・符号の研究は、最適な組合せ構造の特徴付け、存在性の証明、効率的な構成法の導出、非同型な構造の数え上げなどのテーマに分けられる。

本論文では、組合せデザイン・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する研究結果をまとめる。具体的には、量子ジャンプ符号から導出された t-spontaneous emission error design （t-SEED と略す）と呼ばれる組合せデザインと、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、構成法について論じる。

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るとともに、必要な概念と用語、記号を定義し、既知の結果をまとめる。

第 2 章では、与えられたパラメータを持つ最適な t-SEED の組合せ的特徴付けを行い、t-SEED の構成法およびその暗号への応用について議論する。t-SEED は t-

デザインあるいは partial t-デザインと呼ばれる組合せデザインの族である。Beth ら (2003) は、量子コンピュータの記憶素子において、自然減衰と量子ジャンプにより記憶情報に生じた誤りを訂正するために、量子ジャンプ符号 (quantum jump codes) と呼ばれる一種の量子誤り訂正符号を導入した。さらに、彼らは t-SEED を用いて、量子ジャンプ符号を実現する方法を示した。量子ジャンプ符号に応用する場合、t-SEED に含まれる排反なデザインの数は符号の次元に対応しているため、排反なデザインを多く持つ t-SEED が望ましい。本論文では、含まれるデザインの数が最大となる最適な t-SEED の組合せ的特徴付けを行い、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証明する。さらに、その特徴付けを用いて、最適な t-SEED の非存在に関する結果を示す。

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 の再帰的な構成法を与える。さらに、組合せ的な均衡性を用いて、秘密分散暗号への応用を提案する。組合せデザインを用いた秘密分散暗号については、Stinson-Vanstone (1988) およびそれに続く研究で、$(t-1)$-デザインに分解できる t-デザイン、あるいはある種のハイパーグラフによる手法が提案されている。本論文では、提案する t-SEED を用いた秘密分散暗号と彼らの暗号を 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す。

第 3 章では、組合せ符号の 1 つである衝突回避符号について、与えられたパラメータに対する最大符号語数とそれを達成する符号長系列について論じる。衝突回避符号は、フィードバックのない多元接続通信チャンネルにおいて、一定のユーザ数まではチャンネル内のすべてのユーザに対して通信の成功を保証し、それを超えたユーザ数の場合にも高い確率で通信を成功させる通信プロトコル系列の集合である。衝突回避符号はある条件を満たす 0, 1 の 2 値ベクトルの集合であり、与えられた条件の下でできるだけ多くの符号語を持つ符号が望ましい。衝突回避符号において、すべてのベクトルの重みが 3 の場合、偶数符号長については 2010 年までに最大符号語数は完全に明らかにされているが、奇数符号長については未解決である。また、重み 4 の場合には、符号長の偶奇に関わらず、最大符号語数についてはほとんど知られていない。

本論文では、衝突回避符号に等差性を仮定し、重み 3 で未解決な奇数符号長の場合および重み 4 の場合に、最大符号語数が厳密に決定可能な符号長の系列を求める。まず、重み 3 の場合に剰余環における 2 の位数 (order, suborder) に関する数論的な性質を調べ、ある種の符号長を持つ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、符号語数の上限界を達成するタイト (tight) な衝突回避符号の存在を示す。また、符号長 n が円分多項式を用いて $n = \Phi_{4m}(2)$ と表せる場合にも、タイトな衝突回避符号が存在することを明らかにする。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る。

重み 4 の場合については、符号長を $n = 2^a 3^b m$（m は 6 と素）と表し、等差ベクトルを頂点とみなして、共通の差を持つ頂点間に有向辺を持つグラフを定義し、パラメータ a, b, m に注目して、そのグラフ構造を明らかにする。この有向グラフと剰余環における 2 と 3 の位数に関する性質を用いて、a, b に関する最大符号語数の漸化式を求め、一般の n に対する最大符号語数の問題が $n = m$, $2m$, $3m$, $6m$, $12m$, $24m$ の場合に帰着できることを示す。さらに、$n = 3m$, $12m$ と一部の $n = 24m$ の場合には一般に最大符号語数が決定できることを証明し、その構成法を与える。

本論文で得られた結果と今後の課題は該当する各章の最後に述べるとともに、第 4 章にまとめる。