報告番号	※甲　　　第　　　号

主　論　文　の　要　旨

論文題目　Combinatorial Designs with Certain Inner Structures and Number Theoretic Approaches to Their Existence
（特定の内部構造をもつ組合せデザインおよびその存在性に対する数論的アプローチ）

氏　　名　盧　暁南

論　文　内　容　の　要　旨

組合せデザインは，離散数学の一分野であり,「バランスの良い」組合せ構造の存在・構成・代数構造などの問題を主に扱う．1930 年代の農業実験計画において統計的視点で釣合い型不完備ブロックデザイン（BIB デザインと略す）や格子方陣デザインの研究が始まり，理論的・実用的側面の両面から盛んに研究が発展してきた．同時に，数学的に有限群論や有限幾何の問題と関連しながら深く研究されてきた．また，情報通信やセキュリティ分野で、種々の符号を構成する上での重要性が認識され，現在でも幅広い研究が進展している．本論文では，特定の内部代数的構造と幾何的構造をもつ組合せデザインの最適構造とその存在性・構成法に焦点を絞り，幾つかの代数的，数論的アプローチを通じて，剰余環 $\mathbb{Z}_v = \mathbb{Z}/v\mathbb{Z}$ 上のアフィン不変な四重系，有限体 $\mathbb{F}_q$ 上の grid-block 差族および最適な grid-block 被覆デザインと呼ばれる 3 種類の組合せ構造に関する研究成果をまとめる．

ここで，本論文における幾つかの用語の定義を行う．

V を要素数 v の有限集合とし，V の各要素を点と呼ぶ．$\mathcal{B}$ を V の k 元部分集合の集合族とし，各部分集合をブロックと呼ぶ．組合せ構造 $(V,\mathcal{B})$ に対して，V の任意の t 元部分集合はちょうど λ 個のブロックに現れるとき，$(V,\mathcal{B})$ を t-(v,k,λ) デザインと呼ぶ．特に，3-$(v,4,1)$ デザインは Steiner 四重系（SQS と略す）と呼び，3-$(v,4,2)$ デザインは two-fold 四重系（TQS と略す）と呼ぶ．

また，$\mathcal{A}$ を V の元を要素にもつ $r\times k$ 配列の集合とする．$\mathcal{A}$ の各配列に同じ点が 2 回以上現われないとする．V の任意の異なる 2 点を含む配列の行数と列数の合計がちょうど 1 となるとき，組合せ構造 $(V,\mathcal{B})$ を $r\times k$ grid-block デザインと呼ぶ．

本論文は 5 章で構成される．

第 1 章では，導入として組合せデザイン理論の発展の歴史や，本論文の研究背景と本論文で扱う様々な組合せデザインを紹介し，それらの先行結果を概説する．

初めに，t デザインとその自己同型群の定義を与え，多重アクセス通信における光直交符号との関連性について述べる．t デザインの研究においては，$t \geq 3$ の t デザインに関する問題が非常に困難である．特に Steiner 四重系（SQS）は最も重要な構造の一つであり，巡回的な SQS の存在性・構成問題は特に難しく現在でも未解決である．その強い対称性をもつ SQS とその関連する組合せデザインは本論文の前半の主題である．

次に，BIB デザイン（すなわち，2 デザイン）の構成法で最も重要である差集合族などの組合せ構造を紹介し，その一般化として grid-block 差族を導入する．一方，遺伝子情報解析に応用することを目的として，格子方陣デザインや BIB デザインは grid-block デザインに拡張されてきた．それらの構成には，grid-block 差族が用いられ，その「配列型」の組合せ構造は本論文のもう一つの主題である．

第 2 章では，アフィン不変な SQS と TQS の構成法とその応用を主に扱う．すなわち，巡回群を含む一般アフィン群を自己同型群に持つデザインを中心として考える．まず，アフィン不変な SQS の構成法を直接的構成法と再帰的構成法をそれぞれ二つ提案し，構成法 A と構成法 B と呼ぶことにする．直接的構成法 A では，位数 p の有限体 $\mathbb{F}_p$ における射影直線上の点への射影特殊線型群 $\mathrm{PSL}(2,p)$ による作用を考え，新たに LG グラフと CG グラフと呼ばれる代数的グラフを定義し，そのグラフの 1 因子が存在するとき，要素数が $2p$ であるアフィン不変な SQS の構成法を与える．また，直接的構成法 B では，位数 p の有限体の要素を頂点とみなして，特殊な超グラフを定義し，その超グラフの 1 因子を利用して，要素数が $2p$ であるアフィン不変な SQS の構成法を与える．再帰的構成法 A と B では，ともに剰余環 $\mathbb{Z}_{2p^m}$ の乗法群 $\mathbb{Z}_{2p^m}^\times$ の巡回性と $\mathbb{Z}_{2p^m} \setminus \mathbb{Z}_{2p^m}^\times$ の構造を利用して，具体的な構成法を与える．また，それぞれの構成法 B を用いることにより，組合せデザインの難しい問題の一つである着色問題に対して，新たな 2 色で点彩色可能な SQS の系列を与える．さらに，アフィン不変な TQS を検討し，SQS の構成法 A と類似な条件を満たすとき，同様の手法を適用し，アフィン不変な TQS に対しても直接的構成法と再帰的構成法を提案する．応用として，アフィン不変性を用いることにより，計算機のファイリング・システムや統計的グループ検査への有用性を示す．

第 3 章では，差集合族の一般化として，$r \times k$ grid-block 差族を考えることにより，有限体 $\mathbb{F}_q$ 上の radical $r \times k$ grid-block 差族の構成法を提案し，代数的整数論の手法を用いて，その無限系列の存在を証明する．特に (radical) $1 \times k$ grid-block 差族は，最も重要な組合せデザインの一種であるブロックのサイズが k である (radical) 差集合族と同値である．本論文では，解析的密度である Kronecker 密度の概念を用いて，組合せデザインの「スパース性」を評価し，その構成法の「存在比率」も明らかにする．さらに，Kronecker 密度の計算により，k が素数のとき，$2 \times k$ grid-block 差族の無限存在性を証明する．

差集合族・grid-block 差族およびその類似の代数的性質をもつ組合せ構造における漸近存在性を証明するとき，対象となる集合が有限体の乗法群の剰余類の代表系であるという制限条件が付けられることが多い．組合せデザイン論では，有限体上の乗法指標和に関する Weil の定理の帰結である Buratti-Pasotti の定理がよく使われる．本論文では，Weil の定理を直接用いることにより，より一般の制限条件の下で，差集合族と類似の代数的内部構造をもつ組合デザインへ応用しやすい定理を与え，Buratti-Pasotti の定理を改良する．さらに，その grid-block 差族の存在性限界の改良効果も示す.

第 4 章では，分解可能性という幾何的性質をもつ $r \times k$ grid-block デザインに注目する．しかし，$k \geq 3$ のとき，分解可能な $2 \times k$ grid-block デザインは存在しないため，分解可能な grid-block 被覆デザインという組合せ構造を導入する．初めに，各 grid-block が互いに素である grid-block 差族を利用して，分解可能な grid-block（被覆）デザインを構成する定理を証明する．さらに，$2 \times k$ grid-block の数が最小となる最適かつ分解可能な grid-block 被覆デザインの組合せ論的特徴付けを行い，再帰的構成法を与え，分解可能な最適 2×3 grid-block 被覆デザインの存在性に関する必要十分条件を与える．また，再帰的構成法では，小さいパラメータをもつデザインに対して，ソフトウェア・アルゴリズムの分野で最近盛んに研究がなされている SAT ソルバーが組み込まれた SUGAR を用いて，効率的に見出すこが可能であることを示す.

第 5 章では，本論文で得られた結果のまとめと今後の更なる研究課題に対して各章ごとに記述する.