氏名（本籍）	菱田隆彰（愛知県）
学位の種類	博士（工学）
学位記号番号	甲第 126 号
学位授与年月日	平成 12 年 3 月 24 日
専攻	電子情報システム工学専攻
学位論文題目	Theoretical and Computer Aided Constructions of Balanced Incomplete Block Designs with Nested and Resolvable Structures （巣型構造あるいは分解可能性を持つブロック計画の理論的および計算機支援構成法）
学位論文審査委員	（主査） 教授 後藤宗弘 （副査） 教授 田中嘉津夫　教授 岸田邦治 助教授 寒河江雅彦　助教授 金子美博 教授 神保雅一

論文内容の要旨

1. BIB 計画の実験計画及び情報通信への応用

釣り合い型不完備ブロック計画(Balanced Incomplete Block Design, 以下 BIB 計画と略す)は、もともと統計学の一分野である実験計画法において Fisher の 3 原則（反復、無作為化、局所管理）を満たし、与えられた実験回数のもとで推定の精度を上げることを目的として、1936 年に Yates によって導入された。BIB 計画は実験計画において、ある条件のもとで常に統計的な最適性が得られる事が知られており、農場実験などの分野において各処理の主効果の推定を行う際、すべての要因の組合せに対して実験を行うよりはるかに少ない実験回数でありながら高い精度で推定を行うことができる。

BIB 計画はもともと、農場実験及び、工業分野における品質管理の分野に利用されてきたが、情報通信の発達と共に符号理論との関連がブロック計画の重要なテーマの一つとなっている。さらに近年では、BIB 計画はその組合せ的なバランスの良さから、暗号の分野にも利用されている。BIB 計画の暗号への応用の例としては鍵共有暗号システムや認証暗号システムなどが挙げられる。また符号理論の分野においては、従来からブロック符号との関連が研究されているが、最近、次期デジタル移動通信方式である CDMA(Code Division Multiple Access：広帯域符号分割多元接続方式)の通信情報の符号化に BIB 計画を利用する研究も進められている。

BIB 計画は一般に任意のパラメータについて存在するとは限らず、多くの研究者が BIB

計画 の存在性、構成法等に関して研究を続けている。本論文では BIB 計画の巡回的分解可能性および巣型構造を持つ BIB 計画に対する存在性や構成法に関する研究を行っている。

2. BIB 計画の定義

Vを v個の元からなる有限集合とし Vの各元を処理と呼ぶ。例えば処理は農場実験では実験対象となる品種等を表し、暗号の分野では配布する鍵等を意味する。k個の処理からなる部分集合をブロックと呼び、b個のブロックの集まり(族)を Bとする。このとき kをブロックサイズと呼ぶ。処理とブロックの組(V, B) が以下の条件を満たすとき、(V, B)を BIB 計画と呼ぶ。

i. 各処理があるブロックに現れる回数は高々1回。

ii. 各処理は必ずそれぞれ r個のブロックに含まれる。

iii. 異なる二つの処理の組は必ずそれぞれλ個のブロックに含まれる。

このとき基本となる各パラメータ v, b, r, k, λは独立ではなく $vr=bk$, $r(k-1)=\lambda(v-1)$ なる関係が成り立つ。したがって BIB 計画は 3 つのパラメータ v, k, λを用いて、$B(v, k, \lambda)$と記される。

3. 巣型構造を持つ BIB 計画 (nested BIB design)の構成と非存在性

ある計画において各ブロックが小さな部分ブロックに分割され、元のブロックの族に関しても、部分ブロックの族に関しても BIB 計画であるとき、この計画を巣型 BIB 計画と呼ぶ。このような巣型 BIB 計画を実際の統計解析に利用するために、実用的な範囲で、与えられたパラメータを持つ BIB 計画の存在証明や系統的な構成法が必要である。

学位論文第 2 章ではより複雑な行列型の巣型構造をもつ BIB 計画の再帰的な構成法、及び直接的な構成法を理論的に導出し、過去の他の構成法との比較を行い、その有効性を示した。また、学位論文第 3 章 では $v \leq 14, r \leq 30$ の範囲で唯一存在性が明らかにされていないパラメータを持つ巣型 BIB 計画の存在性を 2 つの異なる効果的なアルゴリズムを用いて計算機により調べ、その非存在を示した。

4. 分解可能性を持つ BIB 計画 (resolvable BIB design)の存在性

BIB 計画のブロックの集合が、すべての処理が一度ずつ現れるようなブロックの組に分解できるとき、その BIB 計画は分解可能性を持つと呼ばれる。分解可能性を持つ BIB 計画は前述した巣型 BIB 計画のより特殊な概念と考えることができる。

分解可能性を持つ BIB 計画はブロック実験の解析だけでなく、鍵共有暗号システムと呼ばれる暗号の構成にも応用可能である。各処理を共有鍵の番号とみなし、分割された各組にはそれぞれ秘密鍵の番号を割り当てることで、鍵共有暗号が構成可能となる。暗号システムに応用するにはその安全性の面から非常に大きな v (例えば、10 進 100 桁程度)を持つ計画が必要とされ、そのためには有限体の巡回性などを用いた系統的な構成法が必要不可欠である。

従来より、有限射影幾何を用いて BIB 計画を構成する方法が知られているが、その巡回的分解可能性についてはほとんど未解決であり、有限射影幾何 PG(5,2)上で、直線からなる巡回的分解可能な BIB 計画の存在性が Sarmiento (1997)により示されているのみである。学位論文第 4 章では有限射影幾何 PG(7,2)上の直線からなる BIB 計画の巡回的分解可能性

を調べた。ここでは、まず理論的に不可能なパターンを排除することにより、計算量を削減した後、計算機を用いて 4 つの巡回的な分解パターンが存在することを示した。また、射影幾何 PG(5,2)上の平面からなる BIB 計画は 2 種類の異なる自己同型変換(Cyclic, 2-rotational)により巡回的に分解可能であることを計算機と理論を併用して示した。射影幾何上の平面から構成される BIB 計画の巡回的分解可能性を示したのは本研究が初めてである。

論文審査結果の要旨

本論文では釣合い型不完備ブロック計画(以下 BIB 計画と略す)と呼ばれる組合せ構造に巡回的分解可能性および巣型構造などの条件を付加した構造を持つ BIB 計画の存在性および構成法に関する研究を行っている．BIB 計画はもともと，農場実験，品質管理，医学・薬学などの分野の実験データの収集法として用いられてきたが，情報通信の発達と共にブロック符号，たたみ込み符号，鍵共有暗号システム，認証暗号システム，CDMA 通信などの分野などにも利用されている．本論文により得られた結果は以下のとおりである．

（1）BIB 計画では，局所管理の原則のもとにブロックと呼ばれる小区画に分割して実験を行い，誤差変動を小さくするが，本論文では，各ブロックがさらに小さな部分ブロックに分割され，元のブロック，部分ブロックのいずれに関しても BIB 計画である巣型 BIB 計画あるいは行列型の巣構造を持つ BIB 計画について存在性・構成法の研究を行っている．まず，行列型の巣構造を持つ BIB 計画の再帰的あるいは直接的ないくつかの構成法を理論的に導出し，他の構成法との比較を行い，その有効性を示した．さらに，公表されている巣型 BIB 計画の表の中で唯一存在性が明らかにされていなかったパラメータを持つ巣型 BIB 計画の存在性を効果的なアルゴリズムにより調べ，その非存在を示した．

（2）従来より，有限射影幾何を用いて BIB 計画を構成する方法が知られているが，その巡回的分解可能性についてはほとんど未解決である．本論文では，有限射影幾何 PG(5,2), PG(7,2)上の直線あるいは平面からなる BIB 計画について，存在しない組合せ構造を理論的に排除することにより，大幅に計算量を削減した後，計算機を用いて巡回分解可能性を示した．射影幾何上の平面から構成される BIB 計画の巡回的分解可能性を示したのは本研究が初めてである．本研究は，BIB 計画の存在，構成問題に対して，理論的にも実用面においても新しい知見を得たものであり，工学的に有意義である．よって，本論文は博士(工学)の学位論文として価値あるものと認める．

最終試験結果の要旨

公聴会後に，学位論文に関する口頭試問を行い，これを最終試験に代え，合格と判定した．