【43】

氏名（本籍）	篠原（しのはら）　聡（さとし）（千葉県）
学位の種類	博士（経営工学）
学位記番号	博甲第2239号
学位授与年月日	平成12年3月24日
学位授与の要件	学位規則第4条第1項該当
審査研究科	社会工学研究科
学位論文題目	New Applications of Algebraic Curves （代数曲線の新しい応用）

主査	筑波大学教授	工学博士	山本芳嗣
副査	筑波大学教授	Ph．D．（Combinatorics and Optimization）	藤原良叔
副査	筑波大学教授	工学博士	腰塚武志
副査	筑波大学助教授	工学博士	吉瀬章子
副査	筑波大学助教授	理学博士	安藤清

論文の内容の要旨

代数幾何と呼ばれる分野は数学に長い歴史を持つが，20年ほど以前より工学分野への応用が盛んに研究されるようになってきている。とくに複素数体上ではなく有限体上の代数曲線は情報科学への応用が広く，例えばGoppa（1981）による代数幾何符号，Koblitz（1987）やMiller（1986）による楕円曲線暗号，Lenstra Jr.（1987）による楕円曲線を用いた整数の因数分解法，XingとLam（1999）による擬似乱数列の生成などが挙げられる。

本論文では実験計画法などで用いられるbalanced array, balanced n-ary designと呼ばれる2種類の組合せ的デザインを有限体上の代数曲線を用いて構成する新しい方法を提案している。

balanced arrayは1956年にChakravartiによって，balanced n-ary designは1952年にTocherによって，いずれも実験計画法の配置問題に関連して提案されたものである。いずれも非負整数を要素とする配列であり，それぞれが満たすべき条件とはbalanced arrayについては“2行に列として現れる対(a.b)の個数が行に依存しない”，balanced n-ary designについては“列和一定で，どの2行の内積も等しい”と記述される。

有限体の元を係数に持つ多項式の根の集合として代数曲線を定義し，2つの代数曲線を定義している多項式の共通根を2曲線の交点と呼び，根の重複度を交点の重複度ということにする。以上の用語によれば，配列の各要素としてある条件を満たす非特異な曲線群の交点の重複度を用いることが，本論文で提案している構成法の基本的なアイデアである。

以下に本論文のアイデアをもう少し具体的に述べる。まず1つの曲線Cを固定し，その上の有限個の点を配列の行に対応させ，さらに新たに有限本の曲線群を配列の列に対応させる。そして曲線Cの第i点と第j列に対応する曲線の交点重複度をその配列の(i,j)-要素にすることによりbalanced arrayやbalanced n-ary designを構成するものである。この方法では曲線C，行に対応するC上の点，および列に対応する曲線群の三者を，要求された条件を満たすように選択する必要がある。そのため本論文では，固定された曲線C上の有限個の点それぞれに対して与えられた正整数以上の重複度でそれらと交わるすべての曲線群の集合は線型空間をなす，という事実を利用している。ただし，曲線Cを決める多項式の次数が3以上の場合にはこの条件を満たす曲線や交点の集合を簡単に得ることができない。そこで，次数が3の場合に対して明示的な方法を提案している。

本論文の構成は以下の通り。第1章で，有限体上の代数曲線の既存の応用，balanced array や balanced n-ary design の実験計画での応用例などについてまとめ，第2章で，本論文の以降の議論で必要となる代数曲線の理論に関する定義を与え，既存の定理や結果などを概観している。第3章，第4章では，それぞれbalanced arrayとbalanced n-ary designに対して新しい構成法を提案している。最後の第5章では提案した構成法に残された解決すべき問題点，将来の展望などについて述べている。

審 査 の 結 果 の 要 旨

2種類の組合せ的デザインを有限体上の代数曲線群の交点の重複度を用いて構成する新しい方法を提案したことは評価に値する。代数曲線を用いるこのような方法は理論的に新しく，デザインのみならず暗号やコードの開発に今後大きく貢献する可能性を持った成果である。ただし，提案した方法でどのようなパラメータを持つデザインが構成可能になったのか，それは既存の方法で構成できなかった新しいデザインを含んでいるのかについての言及が少ない点が惜しまれる。

以上より本論文は学位請求論文として十分な水準に達していると判断される。

よって，著者は博士（経営工学）の学位を受けるに十分な資格を有するものと認める。