報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題名　Existence and Construction of Difference Families and Their Applications to Combinatorial Codes in Multiple-Access Communications
(差集合族の存在性と構成およびその多重アクセス通信における組合せ符号への応用について)

氏名　　籾原　幸二

論　文　内　容　の　要　旨

組合せデザインは，組合せ論の主要な研究対象であり，有限群や有限幾何の問題と関連しながら発展してきた．また，その統計学や情報通信理論への応用的側面についても盛んに研究されており，その研究の重要性が再認識されている．中でも特に，多重アクセス通信で用いられる組合せ符号との関連性については近年非常に多くの研究がなされている．本論文では，差集合族と呼ばれる組合せデザインの存在性について議論し，その結果に基づき，多重アクセス通信で用いられる光直交符号や衝突回避符号の新しい構成法を与える．

Gを有限群とし，NをGの部分群とする．自然数k,λに対し，Gのk元部分集合(**ブロック**とよぶ)の部分族$\mathcal{F}$で，$G\setminus N$の任意の元がブロック内の差としてちょうどλ回被覆されるとき，$\mathcal{F}$を(G,N,k,λ)-**相対差集合族**という．$|N|=1$のとき，単に(G,k,λ)-**差集合族**とよぶ．本論文では，特に，Gが可換群もしくは巡回群である場合を扱う．

第1章では，組合せデザイン論における差集合族と多重アクセス通信の組合せ符号について概説する．通常の差集合族，相対差集合族，根差集合族などの種々の差集合族の定義を与え，それらの基本的性質と既存の結果，他の組合せデザインとの関連について述べる．また，多重アクセス通信で用いられる光直交符号や衝突回避符号の組合せ論的側面および差集合族との関係について述べる．

長さv，ハミング重みkの0,1列の集合Cが，与えられた正整数λ_aとλ_cに対し，以下の条件を満たすとき，Cを$(v,k,\lambda_a,\lambda_c)$-**光直交符号**とよぶ．

(i) (**自己相関性**) 任意の$X=(x_i)\in C$と任意の$1\le s\le v-1$に対し，$\sum_{i=0}^{v-1}x_ix_{i+s}\le\lambda_a$;

(ii) (**相互相関性**) 任意の異なる$X=(x_i),Y=(y_i)\in C$と任意の$0\le s\le v-1$に

対し，$\sum_{i=0}^{v-1} x_i y_{i+s} \leq \lambda_c$.

ここで，添え字$i+s$はvを法とする剰余である．vを**符号長**，kを符号の**重み**とよぶ．また，相互相関性(ii)のみを満たす集合Cを(v,k,λ_c)-**衝突回避符号**とよぶ．Cの各要素を**符号語**とよび，与えられたv,k,λ_a,λ_cに対し，符号語数最大の光直交符号および衝突回避符号を構成することが本論文の主題である．

第2章では，$\lambda_c=1$の光直交符号を各ブロックに現れる差の数によって分類するために，既存の差集合族の概念を包含する新たな差集合族を定義する．また，巡回群上で定義された4元部分集合Xを，Xの差集合$\Delta X=\{a-b|a,\in X;a\neq b\}$に現れる元の最大重複数および$X$の差集合に現れる差の種類の数(**差数**とよぶ)の双方で分類することにより，$(v,4,2,1)$-光直交符号の最大符号語数に関する上限式を得る．また，この上限式の上限を達成する**最適な**$(v,4,2,1)$-光直交符号について，有限体を利用した直接的構成法と再起的構成法を与え，多くの無限系列を得る．

第3章では，符号語数最大の$(v,k,1)$-衝突回避符号の構成と存在問題を扱う．特に，vを法とする整数の剰余環$\mathbb{Z}_v=\mathbb{Z}/v\mathbb{Z}$の非零元を差数$2(k-1)$を持つブロックの差集合の台集合の元としてちょうど1回被覆する差集合族の存在性を調べる．素数pと一般のkに対して，そのような差集合族が存在するための条件を巡回群上の**完全パッキング**の言葉を用いて記述し，特に$k=3,4,5$の場合に対する必要十分条件を，$\mathbb{Z}_p$の乗法部分群とそのコセットへの$\mathbb{Z}_p$の特定の元の配置として特徴づけ，その条件を満たす素数pの無限存在性を証明している．

第4章では，有限群N上のk元部分集合(multiset)族$\mathcal{E}$でNの零元も含めたすべての元が，差としてちょうどμ回被覆されるという条件を持つ(N,k,μ)-**強差集合族**($|\mathcal{E}|=1$のとき$D\in\mathcal{E}$を(N,k,μ)-**差被覆集合**とよぶ)を導入し，そのような差集合族について，平方和，cyclotomic数，部分差集合などの概念を利用し，種々の構成法と存在定理および非存在定理を与える．また，強差集合族と相対差集合族との関連性についても調べており，「$k\leq 5$のとき，(N,k,μ)-強差集合が存在するならば，ある自然数$q_{k,\mu}$が存在し，$q>q_{k,\mu}$なる任意の素数ベキ$q\equiv 1\,(\mathrm{mod}\ \mu)$に対し，$(N\times\mathbb{F}_q, N\times\{0\},k,1)$-相対差集合族が存在する」という定理を証明する．ここで，$\mathbb{F}_q$は位数qの有限体を意味する．$k\geq 6$の場合も，$q\equiv\mu+1\,(\mathrm{mod}\ 2\mu)$として同様の主張が成立する．この結果は，Wilsonによる有限体上の差集合族の漸近存在定理の相対差集合族への一般化を与えている．また，$\lambda=1$かつ$|N|\leq k(k-1)$の巡回群上の相対差集合族が符号語数最大の$(|G|,k,1,1)$-光直交符号を与えるということに注意すると，この定理は，1つの強差集合族が符号語数最大の光直交符号を無限個与えるという点で非常に重要である．

第5章では，Gが巡回群である場合の相対差集合族の一般化として，ブロックのサイズが一定であるという条件を除いた差集合族を定義し，そのような差集合族の構成法を提示する．この章では，「qを素数ベキとし，e,m,nを$\gcd(n,m)=1$,

$n|q-1$，$\gcd(e,n)=1$を満たす正整数とする．このとき，位数$(q^m-1)/n$の巡回群上で，位数$(q-1)/n$の部分群の元を被覆しない$\lambda=q^{m-2}(q-1)/en$の相対差集合族が存在する．特に，ブロック数は$(q-1)/e$で，各ブロックのサイズは下から$\frac{1}{n}(q^{m-1}-(n-1)q^{(m-1)/2})$，上から$\frac{1}{n}(q^{m-1}+(n-1)q^{(m-1)/2})$で抑えられる」という主定理を示す．この差集合族は有限体上のトレース関数と離散対数関数を用いて構成される．この結果の系として，符号語数n，符号長$v=(q^2-1)/n$，重み$k=\lceil\frac{1}{n}(q-(n-1)\sqrt{q})\rceil$の$(v,k,1,1)$-光直交符号の新しい無限系列を得ることができる．この系列は，$n\geq 3$かつ$q\geq 4(n-1)^2(n+1)^2$のとき符号語数最大であり，パラメータqとnを自由に選ぶことができるという意味で，既存の光直交符号の中でも広いクラスを与える．

第6章では，この論文で提示した結果についてのまとめと今後の更なる研究課題について，それぞれの章ごとに記述する．