

## 科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年 5 月 7 日現在

機関番号：17401

研究種目：基盤研究（C）

研究期間：2009～2011

課題番号：21540021

研究課題名（和文） $(u, \lambda)$ -型半正則相対差集合の研究研究課題名（英文）Research on semiregular relative difference sets of  $(u, \lambda)$ -type

研究代表者

平峰 豊（HIRAMINE YUTAKA）

熊本大学・教育学部・教授

研究者番号：30116173

研究成果の概要（和文）：

A. Blokhuis 等により  $\lambda=1$  のときアーベル群における半正則相対差集合はある素数  $p$  に対して  $p$  群となることが示された。この研究ではアーベル群  $G$  が  $\lambda=2$  の半正則相対差集合をもてば、特殊な例外は別として、 $G$  が 2-群になることを示した。また、 $Z_p \times Z_p \times Z_p$  における既知の半正則相対差集合を関数を利用して特長づけた。さらに半正則相対差集合に関係する一般アダマール行列を群環を利用して一般化して、それをを用いて spread に関係する新しい一般アダマール行列を構成した。

研究成果の概要（英文）：

A. Blokhuis et al. have shown that abelian semiregular relative difference sets with  $\lambda=1$  are  $p$ -groups for some prime  $p$ . In this research we study the case  $\lambda=2$  and show that the corresponding groups are 2-groups with some exceptions. Concerning the group  $G=Z_p \times Z_p \times Z_p$ , we characterize the known semiregular relative difference sets in  $G$  by using functions from  $Z_p$  to  $Z_p$ . We also consider generalized Hadamard matrices and give their modification. As an application we construct new generalized Hadamard matrices related to spreads.

交付決定額

（金額単位：円）

	直接経費	間接経費	合計
2009 年度	700,000	210,000	910,000
2010 年度	700,000	210,000	910,000
2011 年度	700,000	210,000	910,000
年度			
年度			
総計	2,100,000	630,000	2,730,000

研究分野：代数的組合せ論

科研費の分科・細目：数学・代数学

キーワード：差集合, デザイン, 有限幾何, 有限群

## 1. 研究開始当初の背景

位数  $u^2\lambda$  の群  $G$  の  $u\lambda$ -部分集合  $D$  が  $G$  の位数  $u$  の正規部分群  $U$  に関する  $(u\lambda, u, u\lambda, \lambda)$ -半正則相対差集合（以下  $(u, \lambda)$ -型半正則相対差集合）であるとは  $xy^{-1}$  ( $x, y \in D, x \neq y$ ) が  $G-U$

の各元をちょうど  $\lambda$  回重複して表すが  $U$  の元を全く表さないことをいう。  $U$  は禁止群と呼ばれる。  $\lambda=1$  のときつまり  $(n, n, n, 1)$ -半正則相対差集合は有限射影平面のなかで点集合上にもブロック集合上にも長さ  $n^2$  の軌道

をもつ半正則自己同型群に対応する．有限幾何の基本予想によりこのとき  $n$  は素数の累乗になると考えられている．この状況を一般化したものが位数  $u^2\lambda$  の群  $G$  における  $(u, \lambda)$ -型半正則相対差集合である．このことから  $G$  の位数が素数の累乗ではないにしても一般的に  $p$ -群と密接に関係していると考えられている．この観点から半正則相対差集合についての中心的な予想の一つとして，禁止群  $U$  はある素数  $p$  に対して  $p$ -群であるとされてい過去にもこれに関する研究が行われてきた．本研究の目標の一つは  $(u, \lambda)$ -型半正則相対差集合がどのくらい  $p$ -群と密接に結びついているかをさらに詳しく調べることである．

(1) Blokhuis-Jungnickel-Schidtにより群がアーベル群であるという条件のもとで  $\lambda=1$  であればある素数  $p$  があって  $G$  が  $p$ -群であることが示されたが，一般の  $\lambda$  では正しくなく  $((2n, 2, 2n, n)$ -半正則相対差集合，つまりアダマール群はもともと例外的なものとして除外したとしても) 実際にアーベル群のときでさえ Davis により構成された無限系列の反例が知られている．しかし  $\lambda$  が小さいときは反例は少ない．それは  $\lambda$  が小さいときはまだ有限射影平面的な状況が残存していることから，まだ群自体が  $p$ -群的なものだろうと考えられるからであると思われる．しかし，これに関する研究は十分にはされていなかった．

(2)  $(u, \lambda)$ -型半正則相対差集合は群により定義されるが，もともとの組合せ論的背景は射影平面の部分構造の一般化としての transversal design である．つまり，点集合  $P$ ，ブロック集合  $B$  のどちらもともに  $u^2\lambda$  個からなり，各ブロックのサイズは  $u\lambda$  で  $P$  は点クラスよばれる  $u$  点ずつからなる  $u\lambda$  個のクラス(各々は点クラスと呼ばれる)に分割されて，異なる 2 点を含むブロック数はその 2 点在同一クラスに属するかそうでないかによって 0 個または  $\lambda$  個であるという性質をもっている．

また，半正則相対差集合とこの transversal design の中間に位置する概念が一般アダマール行列であり，それは点クラス上に正則に作用する位数  $u$  ( $=$ 各点クラスのサイズ)の自己同型群をもつ transversal design と同値な概念である．この自己同型群はクラス正則群と呼ばれる．すなわち，群  $U$  上の  $u\lambda$  次行列  $[d_{ij}]$  ( $d_{ij} \in U$ ) が一般アダマール行列  $GH(u, \lambda)$  であるとは  $k=u\lambda$  とおくととき  $(\star) d_{i_1} d_{m_1}^{-1} + \dots + d_{i_k} d_{m_k}^{-1} = \lambda U$  ( $i \neq m$ ) が成り立つことをいう．

しかし，一般アダマール行列と半正則相

対差集合の中間に位置するものは過去に注目されることはなかった．従って研究されることはなかった．この方法を定式化すれば，これまでに構成されていない特別の性質をもつ transversal design, 一般アダマール行列，半正則相対差集合などの構成が期待される．

上記に関連して一般アダマール行列の別の視点からの一般化も考えられる．すなわち，成分は  $U$  を正規部分群として含む群の元からとることにして，上に述べた条件  $(\star)$  の右辺を  $G/U$  のいくつかの cosets の和集合であるとして一般化する．以下ではこれを coset 型の quasi-一般アダマール行列とよぶことにする． $G=U$  なら通常的一般アダマール行列に他ならない．この形での一般化はまだ試みられたことがなかった．

他の半正則相対差集合の直接的研究としては次を考える．位数  $p^3$  の群  $Zp^2 \times Zp$  における  $(p, p)$ -型半正則相対差集合は Ma-Pott により完全分類されたが，群が  $p$ -群  $Zp \times \dots \times Zp$  と同型である場合は未解決として残っていて，重要な問題と考えられている．

## 2. 研究の目的

(1) A. Blokhuis 等による  $\lambda=1$  の結果を群  $G$  がアーベル群であるという条件のもとで  $\lambda=2$  のときに拡張することを考えて，同じことが成り立つかどうかについて研究を行った．

(2) 一般アダマール行列と半正則相対差集合の中間に位置する概念を考えることが半正則相対差集合の研究には重要であると考えられる．行列の成分としては群環の元でよいとして考えることにすれば，もとの transversal design の半正則な自己同型群の各軌道が点クラスのユニオンになっているという設定にたどり着く．この視点から何がいえるかの研究を行う．また，この条件を群環の方程式で書き上げて，逆にそれをみたく群環での解を見つけることにより大きな半正則自己同型群をもつ transversal design の構成を試みる．さらにこの自己同型群の中から半正則相対差集合が取り出せないかを研究する．

(3) cosets を利用した一般アダマール行列の変形と半正則相対差集合を組合せて新しい変形一般アダマール行列が構成できないかについて研究する．

一方，これと平行して， $(p, p)$ -型半正則相対差集合の直接的研究としては次を考える．Ma-Pott による群  $Zp^2 \times Zp$  における  $(p, p)$ -型半正則相対差集合の分類の次のステップとして群が  $Zp \times Zp \times Zp$

のときについて半正則相対差集合を研究する。この場合は2つの無限系列が知られているが、この特徴付けが完全分類のためのステップとして重要と考えるのでこの研究を行う。

### 3. 研究の方法

上記(1)(2)(3)のうち、第一の研究についてはアーベル群であるから群の線形指標を駆使して素数べきでないときに同様なことが起きるかについて考察した。A. Blokhuis 等による $\lambda=1$ のときの方法も部分的に有効であった。

第二の研究については一般アダマール行列と半正則相対差集合の中間に位置するものを考える場合、一般アダマール行列の各成分は群の元であるがこれを一般化して群環の元まで条件をゆるめた状態で研究を行った。この際、有限幾何の手法も取り入れることが出来ることに気がついた。

第三の研究の前半部分については、変形一般アダマール行列の研究手法、すなわち群環の議論が有効に使えると予想された。後半の研究については素体から素体への関数を利用することで研究を進めること重要であることが分かり、群論の線形指標や群環の議論を使って研究を行った。

### 4. 研究成果

初年度： $\lambda=2$ のときの可換な半正則相対差集合については次の定理を得た。

定理. アーベル群  $G$  における  $\lambda=2$  の半正則相対差集合が存在すれば  $G$  は 2-群である。ただし、次の (i) (ii) を除く。

$$(i) \quad n=2^a 3^b, a, b > 0$$

$$(ii) \quad n=2^a 3^b p^c, p^c > 2^a 3^b > 1, (p > 3: \text{素数})$$

これは最初に予想しかつ期待した通りの結果であった。すなわち、基本的には  $\lambda=1$  のときの状態が  $\lambda=2$  でも引き継がれているということであるが、(i) (ii) を例外としたという点では  $\lambda=1$  のときの状態が  $\lambda=2$  では崩れ始めているということであると思われる。

この結果はアーベル群における半正則相対差集合の禁止部分群に関する予想を考える際に有効な方法を含んでいると考えられる。この点から今後の方向性を示す例となっていると思われる。また、残された (i) (ii) の case についても完全な分類が課題として残った形になったが今後解決を試みたい。この場合はどちらについても、これまでとはタイプの異なる無限系列が入っていると思われる。

次年度：

( $u, \lambda$ )-型半正則相対差集合の群の条件をゆるめると一般アダマール行列であり。一般アダマール行列にはしばしばよい半正則相対差集合が対応する。この意味でも一般アダマ

ール行列の研究は重要である。この一般アダマール行列を群  $G$  の群環の視点からその一般化の試みとして群  $G$  の  $s$ -部分集合を群環  $Z[G]$  の元とみて、それ成分にもつ  $t(=u\lambda/s)$  次の変形一般アダマール行列  $\text{GH}(s, u, \lambda) [D_{ij}] (1 \leq i, j \leq t)$  を次で定義した。

$$(\#) \quad D_{i1} D_{m1}^{(-1)} + D_{i2} D_{m2}^{(-1)} + \dots + D_{it} D_{mt}^{(-1)}$$

が  $i=m$  であるかないかによって  $u\lambda + \lambda (G-U)$  かまたは  $\lambda G$  となることをいう ( $1 \leq i, m \leq t$ )。

これは、特殊な半正則自己同型群をもつ transversal design に対応する概念となる。これを利用すると様々な transversal design を得ることが出来ることを示した。この  $\text{GH}(s, u, \lambda)$  行列を用いることにより得られる transversal design は  $G$  を半正則自己同型群として含むことを示して、実際にその例を構成した。次が得られた定理である。

定理. 位数  $us$  の群  $G$  において  $t$  次の  $\text{GH}(s, u, \lambda)$  行列  $[D_{ij}] (ts=u\lambda)$  が存在すれば点集合  $P$  とブロック集合  $B$  を  $P = \{1, 2, \dots, t\} \times G$ ,  $B = \{(1, D_{1j}h) \cup (2, D_{2j}h) \cup \dots \cup (t, D_{tj}h) \mid 1 \leq j \leq t, h \in G\}$  で定めれば  $(P, B)$  は  $G$  が自然に半正則自己同型群として作用する transversal design  $\text{TD}_\lambda(u\lambda, u)$  である。

この  $\text{GH}(s, u, \lambda)$  行列  $[D_{ij}]$  からは  $\text{GH}(u, \lambda)$  行列が次の定理により得られる。この意味で新しい一般アダマール行列の構成法が与えられたことになる。

定理. 位数  $us$  の群  $G$  位数  $u$  の正規部分群  $U$  に対して  $(\#)$  で定めた  $U$  に関する  $t$  次の  $\text{GH}(s, u, \lambda)$  行列  $[D_{ij}] (ts=u\lambda)$  が与えられたとする。このとき  $\{g_1, \dots, g_s\}$  を  $G/U$  の完全代表系として

$$C_{(i,n), (j,m)} = U \cap g_n^{-1} D_{ij} g_m \text{ と定めれば } [C_{(i,n), (j,m)}]$$

は  $U$  上の一般アダマール行列  $\text{GH}(u, \lambda)$  を与える。

さらに有限幾何との関連で次を考えた。  $p$  を素数として位数  $p^{2n}$  の基本可換群  $Z_{p^{2n}}$  のなかのどの2つについても単位元だけを共有する位数  $p^n$  の部分群  $p^{n+1}$  個は spread と呼ばれる。この spread を利用することで  $\text{GH}(s, u, \lambda)$  行列を定義して次の定理を得た。

定理. 位数  $q$  の任意の spread から得られる変形  $\text{GH}(q, q, q)$  行列は特別な場合を除けば全て class regular ではなくかつ対称な transversal design を与える。

この定理により一般アダマール行列からは得られることのない対称な transversal design (つまり、双対構造も transversal design となっているもの) を得ることができた。このような例の無限系列はこれまでに知られていなかったので価値があると思われる。さらに、この事実は、対称な transversal design を得るためには一般アダマール行列による構成は必ずしも万能ではないということの意味する点でも重要であるといつてよいと思われる。

今後の展望についてのべると、最初の定理はこれから様々な transversal design の構成、一般アダマール行列の構成、さらには半正則相対差集合の構成などに利用されていくであろうと確信している。2 番目の定理も有限幾何のこのような応用に留まらず、さらにもっと様々な利用の仕方を考える方向にいくと思われる。

最終年度：

coset 型の quasi-一般アダマール行列については、次の定理を得た。

定理. (i)  $G$  を位数  $u^2\mu$  の群,  $U$  を  $G$  の位数  $u$  の部分群で  $N(\geq U)$  を  $U$  の  $G$  における正規化群  $N_G(U)$  の部分群とする.  $[h_{ij}]$  を  $N/U$  に関する quasi-GH( $u, \lambda$ )-行列で  $\Delta = (D_1 \dots D_n)$  ( $n = u\lambda$ ) を  $G$  の禁止群  $U$  に関する ( $u, \mu$ )-半正則相対差集合の  $n$ -tuple とする. このとき  $n$  次正方行列  $M_{H\Delta}$  で  $[h_{ij} D_j]$  は変形一般アダマール行列 GH( $u\mu, u, u\mu\lambda$ ) である.

(ii) (i) でとくに  $U$  が  $G$  の正規部分群であるとして  $G=H$  のときは  $U$  に関する変形一般アダマール行列 GH( $u\mu, u, u\mu\lambda$ ) を得る.

この定理はある意味で内部に複数の半正則相対差集合をもっている変形一般アダマール行列の構成を述べたものであると言ってよいと思う. この定理を用いると Menon Hadamard 差集合 (つまり  $(4n^2, 2n^2-n, n^2-n)$ -差集合) から例えば GH( $4n^2, 2, 8n^2$ ) が得られる. さらに  $Z_p \times Z_p \times Z_p$  における  $(p, p)$ -型半正則相対差集合については次の結果を得た.

定理.  $r(x), s(x)$  を  $Z_p \rightarrow Z_p$  なる関数とする.  $D = \{(x, y, ay^2 + r(x)y + s(x)) : x, y \in Z_p\}$  が  $Z_p \times Z_p \times Z_p$  での  $(p, p)$ -型半正則相対差集合ならば次の (i) (ii) のいずれかが成り立つ.

- (i)  $r(x)$  は置換多項式で  $D$  は hyperplane 型
- (ii)  $\deg(r(x)) \leq 1$  かつ  $\deg(s(x)) = 2$  で  $D$  は product 型

今後の展望について述べると、

quasi-一般アダマール行列については、さらに多くの例が構成できるはずであるから最初の結果は  $(p, p)$ -型半正則相対差集合の完全分類に一步近づいたものと言ってよく、この完全分類の際にその役割を果たすと考えている. さらに未解決である planar 関数  $Z_p \times Z_p \rightarrow Z_p \times Z_p$  の研究にも役立つはずである. なぜなら、この場合は  $(p^2, 1)$ -差集合が対応するが、その禁止群の位数  $p$  の部分群による準同型像が  $(p, p)$ -差集合に他ならないからである. これは、可能な  $(p^2, 1)$ -差集合のあり方に制限をあたえるはずである.

その次の結果は群を利用した transversal design の構成やその自己同型群から新しい半正則相対差集合を得ることにつながることを期待している.

## 5. 主な発表論文等

[雑誌論文] (計 5 件)

- ① 平峰 豊, A construction for modified generalized Hadamard matrices using QGH matrices, Designs, Codes and Cryptography, 査読有, vol.62, 2012, 279-288
- ② 平峰 豊, On  $(p^2, p, p^2, p)$ -difference sets in  $Z_{p^3}$ , Journal of Statistical Theory and Practice, 査読有, vol.6, 2012, 88-96
- ③ 平峰 豊, A family of non class regular symmetric transversal designs of spread type, Designs, Codes and Cryptography, 査読有, Vol. 60 (2011) 91-99
- ④ 平峰 豊, Modified generalized Hadamard matrices and constructions for transversal designs, Designs, Codes and Cryptography, 査読有, Vol.56, 2010, 21-33
- ⑤ 平峰 豊, On abelian  $(2n, n, 2n, 2)$ -difference sets, Journal of Combinatorial Theory, Ser. A, 査読有, Vol.101, 2010, 281-284

[学会発表] (計 10 件)

- ① 平峰 豊, Modified difference matrices と Frobenius 群, 有限幾何とその周辺, H23 年 12 月 10 日, 大分大学 (大分)
- ② 平峰 豊, Cosets に関する difference matrices について (末竹千博との共同研究), 代数的組合せ論シンポジウム, H23 年 6 月 22 日, 大分大学 (大分)
- ③ 平峰 豊, On difference matrices with respect to cosets (joint work with C. Suetake), Institute of Mathematical Science of National University of Singapore, Coding, Cryptology and Combinatorial Designs, H23 年 6 月 1 日, (Singapore)
- ④ 平峰 豊, 変形一般アダマール行列を用いた GH( $q, 4m$ ) の構成について, Hadamard 行列とそれに関する代数的組合せ論, 平成 22 年 12 月 12 日, 神戸学院大学 (兵庫)
- ⑤ 平峰 豊, On  $TD_2(2n, n)$ 's admitting semiregular automorphism groups of order  $n^2$ , 2010 Algebraic and Geometric Combinatorics Conference, 平成 22 年 7 月 16 日, Gyeongju, South Korea (韓国)
- ⑥ 平峰 豊, On  $TD_2(2n, n)$ 's admitting semiregular automorphism groups of order  $n^2$ , 代数的組合せ論シンポジウム, 平成 22 年 6 月 22 日, 高知大学 (高知)
- ⑦ 平峰 豊, 位数  $n^2$  の半正則自己同型群をもつ  $TD_2(2n, n)$  について, 有限幾何とその周辺, 平成 22 年 5 月 9 日, 熊本大学教育学部 (熊本)
- ⑧ 平峰 豊, 成分が RDS である一般アダマール行列の構成, 代数的組合せ論および関連する群と代数, 平成 21 年 11 月 18 日, 信州大

学理学部（長野）

⑨平峰豊，RDS と一般変形アダマール行列，有限幾何とその周辺，平成21年8月7日，東京女子大学（東京）

⑩平峰豊，変形一般アダマール行列について，代数的組み合わせ論シンポジウム，平成21年6月5日，山形県生涯学習センター（山形）

## 6. 研究組織

### (1) 研究代表者

平峰 豊 (HIRAMINE YUTAKA)

熊本大学・教育学部・教授

研究者番号：30116173

### (2) 研究分担者

( )

研究者番号：

### (3) 連携研究者

千吉良 直紀 (CHIGIRA NAOKI)

熊本大学・自然科学研究科・准教授

研究者番号：40292073

渡辺 アツミ (WATANABE ATSUMI)

熊本大学・自然科学研究科・教授

研究者番号：90040120