行政院國家科學委員會補助專題研究計畫成果報告

環建構部分平衡不完全塊區設計
與結合方案之研究

計畫類別: 個別型計畫
計畫編號: NSC-91-2115-M-041-001
執行期間: 91 年 8 月 1 日至 92 年 7 月 31 日
計畫主持人: 孫新民

成果報告類型(依經費核定清單規定繳交): 精簡報告

執行單位: 嘉南藥理科技大學醫務管理系
中華民國 92 年 8 月 30 日

環建構部分平衡不完全塊區設計與結合方案之研究

孫新民

中英文摘要

(一) 中文摘要

關鍵詞: 結合方案; 部分平衡不完全塊區設計; 代數環; 定權碼

在最近, 孫氏發現可以有限代數環來建構結合方案 (association schemes) 與部分平衡不完全塊區設計 (partially balanced incomplete block designs). 我們研究此種建構方式的組合物件之結構, 以及與此相關的論題, 例如定權碼 (constant weight code) 上的應用. 同時考慮一些計算上問題.

(二) 英文摘要

Keywords: association scheme; partially balanced incomplete block design; PBIBD; ring; constant weight code

Recently, Sun constructs association schemes and PBIBDs (partially balanced incomplete block designs) by using finite rings. We study the structures of these combinatorial objects constructed by Sun's method and their related topics, such as the application to constant weight codes. Some computational approaches are considered.

1. 前言

結合方案 (association schemes) 之理論爲代數組合學的主要論題之一. 與其相關聯的有編碼理論 (coding theory), 設計理論 (design theory), 圖論 (graph theory) 和有限群論 (finite group theory).

Definition 1.1. Suppose V is a nonempty set. We need a partition of the collection of all two-element subsets of V as an association scheme is defined by a specific partition. Let $\mathcal{P}_2(V)$ be the collection of all two-element subsets, i.e., $\mathcal{P}_2(V) = \{A \subset V \mid |A| = 2\}$. Suppose $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ is a partition of $\mathcal{P}_2(V)$, so each A_j is a collection of two-element subsets of V, and for each x, $y \in V$ with $x \neq y$, there is exactly one $A_i \in \mathcal{A}$ such that $\{x, y\} \in A_i$. Let $I_m = \{1, 2, \ldots, m\}$ and $(h, i, j) \in I_m^3$. For any $x \in V$, let $A_i(x) = \{y \in V \mid \{x, y\} \in A_i\}$. Then for any $\{x, y\} \in A_h$, define $A_{ij}^h(x, y) = A_i(x) \cap A_j(y)$ and let $P_{ij}^h(x, y) = |A_{ij}^h(x, y)|$. If there is an integer p_{ij}^h so that $P_{ij}^h(x, y) = p_{ij}^h$ for every $\{x, y\} \in A_h$ and for every $(h, i, j) \in I_m^3$, then $\mathcal{A}$ is called a *(symmetric) association scheme* on V. The $A_1, A_2, \ldots, A_m$ are called the *associate classes* of the association scheme.

部分平衡不完全塊區設計 (partially balanced incomplete block designs, or PBIBDs) 被認爲是平衡不完全塊區設計 (balanced incomplete block designs, or BIBDs) 之一般化. PBIBD 的概念是由 Bose 及 Nair 所提出[7]. 他們的研究主要是在 PBIBDs with two associate classes[8].

Definition 1.2. Let V be a finite nonempty set of symbols, and suppose $\mathcal{B}$ is a nonempty collection of nonempty subsets of V. Then $(V, \mathcal{B})$ is called a *tactical configuration* if there are parameters $(v = |V|, b = |\mathcal{B}|, r, k)$ with the following properties: (1) $|B| = k$ for any $B \in \mathcal{B}$, and (2) $|\{B \in \mathcal{B} \mid x \in B\}| = r$ for any $x \in V$.

集合$\mathcal{B}$中的元素被稱爲塊區 (blocks).

Definition 1.3. Suppose $(V, \mathcal{B})$ is a tactical configuration with an association scheme $\mathcal{A}$ on V. Then $(V, \mathcal{B}, \mathcal{A})$ is a *PBIBD* (*partially balanced incomplete block design*) if the following two conditions are satisfied.

(1) To each $A_i \in \mathcal{A}$, there is an integer n_i so that for each $x \in V$ there are exactly n_i distinct $y \in V$ such that $\{x, y\} \in A_i$.
(2) To each $A_i \in \mathcal{A}$, there is an integer λ_i such that if $\{x, y\} \in A_i$, then x and y belong to exactly λ_i distinct blocks of $\mathcal{B}$.

一個 PBIBD 具有tactical configuration 之參數 (v, b, r, k), 結合方案 (association schemes) 之參數 p_{ij}^h, 及其它參數 n_i 與 λ_i.

Example 1.1. Let $V = \{0, 1, 2, 3, 4, 5\}$. The following is a partition $\mathcal{A} = \{A_1, A_2, A_3\}$ of $\mathcal{P}_2(V)$.

$A_1 = \{\{0,1\},\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,0\}\}$,
$A_2 = \{\{0,2\},\{1,3\},\{2,4\},\{3,5\},\{4,0\},\{5,1\}\}$,
$A_3 = \{\{0,3\},\{1,4\},\{2,5\}\}$.

One can check that $p^3_{12} = p^3_{21} = 2$, $p^2_{22} = p^1_{12} = p^1_{21} = p^2_{11} = p^1_{23} = p^1_{32} = p^2_{13} = p^2_{31} = 1$, and remaining $p^h_{ij} = 0$. Therefore $\mathcal{A}$ is an association scheme on V.

Let $\mathcal{B} = \{B_1, B_2, \ldots, B_6\}$, where

$$B_1 = \{0,1,5\}, \quad B_2 = \{0,1,2\}, \quad B_3 = \{1,2,3\},$$
$$B_4 = \{2,3,4\}, \quad B_5 = \{3,4,5\}, \quad B_6 = \{0,4,5\}.$$

Then $(V,\mathcal{B})$ is a tactical configuration with parameters $(v,b,r,k) = (6,6,3,3)$. Together with the above association scheme, we have that $(V,\mathcal{B},\mathcal{A})$ is a PBIBD with the additional parameters $(n_1,n_2,n_3) = (2,2,1)$ and $(\lambda_1,\lambda_2,\lambda_3) = (2,1,0)$.

2. 研究目的

我們研究此種建構方式的組合物件之結構, 以及與此相關的論題, 例如定權碼(constant weight code) 上的應用. 同時考慮一些計算上問題.

3. 文獻探討

有很多的結合方案已被發現. 請參考一些材料: [5], [10], [16], [31]. 較近的研究有一些放在分類上頭[17, 22]. 在應用方面已有許多領域, 例如在 Graph Theory 方面; 又例如在 Coding Theory 方面[9, 12].

雖然有很多的結合方案已被發現, 但是並沒有許多的 PBIBDs 被建構. 這部分請參考: [4], [15], [18], [20], [23], [24]. 大致的研究是著重在實驗設計方面 Two-Associate-Class PBIBDs 的性質, Most attention has been paid to PBIBDs with two associate classes[8]. Cheng and Bailey showed the optimality of some such PBIBDs[13].

4. 研究方法

We will focus on the structures of the constructions of PBIBDs. Most of the results concern with the size $b = \mu n$ of the PBIBD— directly or indirectly.

Theorem 4.1. *Let $(R,+,\cdot)$ be a finite ring with unit. Let $\mathcal{U}(R)$ denote the set of invertible elements and suppose Φ is a subgroup of $\mathcal{U}(R)$ with $-1 \in \Phi$. Also let S be a proper subset of R with $|S| \geq 2$. Define an equivalence relation $\sim$ on $R^* = R \setminus \{0\}$ by $s_1 \sim s_2$ if there is $b \in \Phi$ such that $bs_1 = s_2$. Let $s_1, s_2, \ldots, s_m$ be representatives of the distinct equivalence classes. Define $A_i = \{\{x,y\} \mid (y-x) \sim s_i\}$ for $i = 1,2,\ldots,m$. Let $\mathcal{A} = \{A_i \mid i = 1,2,\ldots,m\}$. Define $\mathcal{B} = \{bS +$*

$a \mid b \in \Phi,\ a \in R\}$. Then $(R, \mathcal{B}, \mathcal{A})$ is a PBIBD (partially balanced incomplete block design). Moreover, if S satisfies $S \neq -S + a$ for any a (i.e., $-1 \notin \overline{1}$), then the above PBIBD can be partitioned into two isomorphic PBIBDs; in this case each of the values b, r, and λ_i for these two PBIBDs is half of the corresponding one for $(R, \mathcal{B}, \mathcal{A})$.

Define $\sim_c$ on Φ by $b_1 \sim_c b_2$ if there is $a \in R$ such that $b_1 S = b_2 S + a$. Then $\sim_c$ is an equivalence relation on Φ. Define $\sim_r$ on R by $a_1 \sim_r a_2$ if $S + a_1 = S + a_2$. Then $\sim_r$ is an equivalence relation on R.

Let $n = |\Phi/\sim_c|$ and $\mu = |R/\sim_r|$. Let $T_c = \{b_1, b_2, \ldots, b_n\}$ be a set of representatives of the equivalence classes induced by $\sim_c$, and denote the equivalence class of b by $\overline{b}$. Also let $T_r = \{a_1, a_2, \ldots, a_\mu\}$ be a set of representatives of the equivalence classes induced by $\sim_r$, and denote the equivalence class of a by $\tilde{a}$.

Theorem 4.2. (1) *$\overline{1}$ is a subgroup of Φ.*

(2) *The equivalence classes induced by $\sim_c$ are exactly those left cosets of $\overline{1}$ in Φ; we have $\overline{b} = b\overline{1}$ for any $b \in \Phi$.*

(3) $\Phi = \bigcup_{k=1}^{n} \overline{b_k} = \bigcup_{k=1}^{n} b_k \overline{1} = T_c \overline{1} = \bigcup_{\beta \in \overline{1}} T_c \beta$.

(4) $n = |\Phi|/|\overline{1}|$.

Theorem 4.3. (1) *$\tilde{0}$ is a subgroup of R.*

(2) *The equivalence classes induced by $\sim_r$ are exactly those cosets of $\tilde{0}$ in R; we have $\tilde{a} = a + \tilde{0}$ for any $a \in R$.*

(3) $R = \bigcup_{k=1}^{\mu} \tilde{a_k} = \bigcup_{k=1}^{\mu} (a_k + \tilde{0}) = T_r + \tilde{0} = \bigcup_{\alpha \in \tilde{0}} (T_r + \alpha)$, *where $T_r + \tilde{0}$ means $\{a + x \mid a \in T_r,\ x \in \tilde{0}\}$.*

(4) $\mu = |R|/|\tilde{0}|$.

(5) *S is a union of some cosets of $\tilde{0}$, and $|\tilde{0}|$ divides $|S|$.*

(6) *If $\sim_r$ is nontrivial, that is, $|\tilde{0}| > 1$, then $\gcd(|S|, |R|) > 1$.*

Corollary 4.4. *If S is an additive subgroup of R, then $\tilde{0} = S$.*

One can see that $\mathcal{B}$ remains the same if S is replaced by any $\beta S + \alpha$ or $\beta(S + \alpha)$, where $\beta \in \Phi$ and $\alpha \in R$. This allows for some flexibility:

(1) If $\sum_{x \in S} x = 0$, we say that S is a *zero-sum generating block* (abbreviated as ZSGB). Especially when $\gcd(k, char R) = 1$, where $k = |S|$, we can assume S is a ZSGB. Why? If we let $s = \left(\sum_{x \in S} x\right) k^{-1}$ and $S' = S - s$, then the summation for S' is zero and S' generates the same $\mathcal{B}$ as S does.

(2) Sometimes we will choose S such that $0 \in S$, if this can make the discussion convenient.

(3) We can use another S with $1 \in S$ if there is $c \in S$ with $c \in \Phi$.

Proposition 4.5. *If S is a ZSGB and $\gcd(|S|, char R) = 1$, then $\overline{1} S = S$.*

Corollary 4.6. *If S is a ZSGB with $1 \in S$ and $\gcd(|S|, char R) = 1$, then*

(1) $\overline{1} \subseteq S$;
(2) $k = |S| \geq |\overline{1}|$; *and*
(3) $n \geq |\Phi|/|S| = n'/k$.

We conclude that $vn' \geq b = \mu n \geq [vn'/k^2]$ when S is a ZSGB with $1 \in S$ and $\gcd(k, char R) = 1$.

Proposition 4.7. *Let Z_n be the commutative ring of integers modulo n, where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$. Let $\Phi = \mathcal{U}(Z_n)$. Let s_i be the proper divisors of n. Also let $s_0 = n$. Then we have*

(1) $|\mathcal{A}| = m = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_\ell + 1) - 1$.
(2) $n_i = \phi(\frac{n}{s_i})$ *and* $n = \sum_{i=0}^{m} \phi\left(\frac{n}{s_i}\right) = \sum_{d|n} \phi(d)$, *which is a well-known result in number theory.*

5. 結果與討論

Definition 5.1. (1) Suppose S is a zero-sum generating block. Then it is *of the first type* if $0 \notin S$. If $0 \in S$, we say that S is *of the second type*. A ZSGB containing 1 is abbreviated as ZSGBO.
(2) For any nonempty subset S of R, define S to be a generating block *of the first type* if there exist $\beta \in \mathcal{U}(R)$ and $\alpha \in R$ such that $\beta S + \alpha$ is a ZSGB of the first type; if there exist $\beta \in \mathcal{U}(R)$ and $\alpha \in R$ such that $\beta S + \alpha$ is a ZSGB of the second type, we say that S is *of the second type*.
(3) For any PBIBD $(R, \mathcal{B}, \mathcal{A})$ constructed in Theorem 4.1, we say $\mathcal{B}$ (or the PBIBD) is *of the first type* if it is generated by a first-type block; $\mathcal{B}$ (or the PBIBD) is *of the second type* if it is generated by a second-type block.

Theorem 5.1. *Suppose $\gcd(k, char R)$=1. Then any generating block $S \subset R$ with $|S| = k$ is either of the first type or of the second type. Therefore any PBIBD with block size k is either of the first type or of the second type.*

Theorem 5.2. *Given a finite ring R with $|R| = v$ and block size $3 \leq k \leq v - 3$, let $\Phi = \mathcal{U}(R)$. Consider the action of $G = \{\tau_{b,a} \mid b \in \mathcal{U}(R), a \in R\}$ on the complete design $\binom{R}{k}$; each orbit is therefore a PBIBD. Then the number t_k of distinct simple PBIBDs with block size k is $\frac{\sum_{\tau_{b,a} \in G} |Fix(\tau_{b,a})|}{v|\mathcal{U}(R)|}$.*

Proof. The proof is by the Burnside Orbit Formula. □

Corollary 5.3. *Let $R = Z_v$, the commutative ring of integers modulo v. Let $G = \{\tau_{b,a} \mid b \in \mathcal{U}(Z_v), a \in R\}$. Then the number t_k of distinct simple PBIBDs with block size k is $\frac{\sum_{\tau_{b,a} \in G} |Fix(\tau_{b,a})|}{v\phi(v)}$.*

In the rest part, we consider the case when $R = Z_v$ and $\Phi = \mathcal{U}(Z_v)$.

First we want to construct certain kind of PBIBDs such that $\lambda_i = 0$ for any $i \neq \eta$. That is, we want to choose S so that $\{c, d\} \in A_\eta$ for any $c, d \in S$. Note that $A_\eta = \{(x, y) \mid y - x \in \mathcal{U}(Z_v)s_\eta\}$

Theorem 5.4. *Let $R = Z_v$, where $v = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell}$ and $p_1 < p_2 < \cdots < p_\ell$. Suppose $k \leq p_1$. Then $S = \{0, 1, \dots, k-1\}s_\eta$ generates a PBIBD with the following property: $\lambda_i = 0$ for any $i \neq \eta$.*

Proof. It is clear that $\{c, d\} \in A_\eta$ for any $c, d \in S$. We have $\lambda_\eta = \frac{2\mu n k(k-1)}{v\phi(v/s_\eta)}$. $\square$

For example, in Z_{25}, $S = \{0, 1, 2, 3, 4\}$ is such a set. It is also clear that for k greater than p_1, there is no PBIBD such that $\lambda_i = 0$ for any $i \neq \eta$. From the above result we obtain

$$p^2 \leq A(p^3(p-1), 2p(p-1)^2, p^2(p-1)).$$

For example, $4 \leq A(8, 4, 4)$ and $9 \leq A(54, 24, 18)$.

Next we give an algorithm for finding all the PBIBDs from the construction when $\gcd(k, v) = 1$.

Algorithm I.

1. Input: v, an integer, k, $3 \leq k \leq \frac{v}{2}$, $\gcd(k, v) = 1$
2. $S := \{1, 2, \dots, k\}$;
   $CountPBIBD := 0$;
3. if $\min S = v - k$ then goto Step 11
4. $S :=$ next generating block with higher *ord*
5. if $\sum_{x \in S} x \neq 0$ then goto Step 3
6. $|1| := 1$
7. for any $1 \neq x \in \mathcal{U}(Z_v)$ do
    if $ord(S) < ord(xS)$
    then goto Step 3
    else if $ord(S) = ord(xS)$
        then $|1| := |1| + 1$
8. $CountPBIBD := CountPBIBD + 1$;
   $n := \frac{\phi(v)}{|1|}$;
   $b := vn$, $r := kn$, $\lambda_i := \frac{vn \cdot |\{\{c,d\} \subseteq S \mid \{c,d\} \in A_i\}|}{|A_i|}$
9. Output: S, n, (v, b, r, k), λ_i
10. goto Step 3
11. end

Theorem 5.5. *If S is a zero-sum generating block and* $\gcd(k, v) = 1$, *where* $k = |S|$, *then*

(1) $\beta_1 \sim_c \beta_2 \Longleftrightarrow \beta_1 S = \beta_2 S$, *and so* $\overline{1} = Stab_{\mathcal{U}(Z_v)}(S)$*;*
(2) $|Stab_{F^*}(S)|$ *divides k if S is of the first type;*
(3) $|Stab_{F^*}(S)|$ *divides $(k-1)$ if S is of the second type;*
(4) $\{bS \mid b \in F^*\} = \{b_1 S, b_2 S, \ldots, b_n S\}$.

Therefore, when v is of the form p^α or $2p^\alpha$, and $\gcd(k, v) = 1$, given a generating block S, it is quite easy to compute the size of the PBIBD generated by S.

Algorithm II.

1. Input: v, of the form p^α or $2p^\alpha$, $S \subset Z_v$, $\gcd(|S|, v) = 1$
2. $g :=$ a primitive root of $\mathcal{U}(Z_v)$;
   $k := |S|$, $s := (\sum_{x \in S} x) k^{-1}$;
3. $S := S - s$
4. if $0 \in S$ then $t_0 := 1$ else $t_0 := 0$
5. $d := \gcd(k - t_0, \phi(v))$
6. factorize d
7. for $i \mid d$ from large to small do
   begin
     $q := g^{\frac{\phi(v)}{i}}$;
     if $qS = S$ then goto Step 8;
   end
8. $n := \frac{\phi(v)}{i}$;
   $T_c := \{1, g^1, \ldots, g^{n-1}\}$;
   $b := vn$, $r := kn$;
9. Output: S, n, T_c, (v, b, r, k)
10. end

6. 成果自評

所得到新的定理及計算結果將可以論文的方式發表呈現.

References

[1] P.P. Alejandro, R.A. Bailey, and P.J. Cameron, Association schemes and permutation groups, Discrete Math., Vol. 266, 2003, 47–67.

[2] R. J. R. Abel, Difference families, in:C. J. Colbourn and J. H. Dinitz, eds., The CRC Handbook of Combinatorial Designs (CRC Press, Boca Raton, 1996) 270–287.

[3] E. F. Assmus and J. D. Key, Designs and Their Codes (Cambridge University Press, Cambridge, 1992).

[4] R. A. Bailey, Association Schemes: Designed Experiments, Algebra and Combinatorics (Cambridge University Press, 2003)

[5] E. Bannai and T. Ito, Algebraic Combinatorics I: Association Schemes (Benjamin/Cummings, Menlo Park, 1984).

[6] T. Beth, D. Jungnickel, and H. Lenz, Design Theory, second ed. (Cambridge University Press, Cambridge, 1999).

[7] R. Bose and K. Nair, Partially balanced incomplete block designs, Sankhyā 4 (1939) 337–372.

[8] R. Bose and T. Shimamoto, Classification and analysis of partially balanced incomplete block designs with two associate classes, J. Amer. Statist. Ass. 47 (1952) 151–184.

[9] A. Brouwer, The linear programming bound for binary linear codes, IEEE Transactions on Information Theory 39 (1993) 677–680.

[10] A. Brouwer, A. Cohen, and A. Neumaier, Distance-Regular Graphs (Springer-Verlag, Berlin, 1989).

[11] A. E. Brouwer, J. B. Shearer, N.J.A. Sloane, and W. D. Smith, A new table of constant weight codes, IEEE Trans. Inform. Theory 36 (1990) 1334–1380.

[12] P. Camion, Codes and association schemes, in: V.S. Pless and W.C. Huffman eds., Handbook of Coding Theory (Elsevier, 1998) 1441–1566.

[13] C. S. Cheng and R. A. Bailey, Optimality of some two-associate-class partially balanced incomplete-block designs, Ann. Statist. 19 (1991) 1667–1671.

[14] C. J. Colbourn and J. H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs (CRC Press, Boca Raton, 1996).

[15] A. Dey, Theory of Block Designs (Wiley, New York, 1986).

[16] C. Godsil, Algebraic Combinatorics (Chapman & Hall, New York, 1993).

[17] A. Hanaki and I. Miyamoto, Classification of association schemes of small order, Discrete Math., Vol. 264, 2003, 75–80.

[18] P. W. John, Incomplete Block Designs (Marcel Dekker, New York, 1980).

[19] F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).

[20] D. Raghavarao, Constructions and Combinatorial Problems in Design of Experiments (Wiley, New York, 1971).

[21] E. M. Rains and N.J.A. Sloane, Table of Constant Weight Binary Codes, http://www.research.att.com/∼njas/codes/Andw/

[22] K. See and S. Y. Song, Association schemes of small order, J. Statist. Plann. Inference 73 (1998) 225–271.

[23] A. P. Street and D. J. Street, Combinatorics of Experimental Design (Oxford University Press, New York, 1987).

[24] D. J. Street and A. P. Street, Partially balanced incomplete block designs, in: C. J. Colbourn and J. H. Dinitz, eds., The CRC Handbook of Combinatorial Designs (CRC Press, Boca Raton, 1996) 419–423.

[25] H.-M. Sun, PBIB designs and association schemes obtained from finite rings, Discrete Math., Vol. 252, 2002, 267–277.

[26] H.-M. Sun, Explicit constructions of simple BIB designs, submitted.

[27] H.-M. Sun, The computation of simple BIBDs obtained from the action of the affine group of a finite field, preprint.

[28] V. D. Tonchev, Combinatorial Configurations: Designs, Codes, Graphs (Longman, England; Wiley, New York, 1988).

[29] V. D. Tonchev, Codes, in: C. J. Colbourn and J. H. Dinitz, eds., The CRC Handbook of Combinatorial Designs (CRC Press, Boca Raton, 1996) 517–543.

[30] V. D. Tonchev, Codes and designs, in: V. S. Pless and W. C. Huffman, eds.; R. A. Brualdi, assistant ed., Handbook of Coding Theory (Elsevier, New York, 1998) 1229–1267.

[31] P.-H. Zieschang, An Algebraic Approach to Association Schemes, Lecture Notes in Mathematics, Vol.1628 (Springer-Verlag, Berlin, 1996).

嘉南藥理科技大學醫務管理系
Current address: 國立台南師範學院數學教育學系暨應用數學研究所
E-mail address: sunhm@ipx.ntntc.edu.tw