DOI: 10.12386/A20210055 **文献标识码: A**

完美置换和空间均衡拉丁方

郑 豪

北京物资学院信息学院 北京 101149
E-mail: zhenghao20070826@163.com

曹海涛

南京师范大学数学科学学院 南京 210023
E-mail: caohaitao@njnu.edu.cn

摘 要 本文首次提出完美置换的概念并研究它的代数性质和构造方法,解决了 $2n+1$ 为素数时 n 阶完美置换的存在性. 我们还利用完美置换给出了循环空间均衡拉丁方和对称空间均衡拉丁方的构造方法, 它们在试验设计中有广泛的应用.

关键词 完美置换; 循环拉丁方; 对称拉丁方; 空间均衡拉丁方
MR(2010) 主题分类 05B05, 46B20
中图分类 O157.2

Perfect Permutations and Spatially Balanced Latin Squares

Hao ZHENG

School of Information, Beijing Wuzi University, Beijing 101149*, P. R. China*
E-mail: *zhenghao*20070826@163*.com*

Hai Tao CAO

School of Mathematical Sciences, Nanjing Normal University,
Nanjing 210023*, P. R. China*
E-mail: *caohaitao@njnu.edu.cn*

Abstract In this paper, a new conception called perfect permutation will be introduced. We focus on its algebraic properties and construction methods. The main result is that there exists a perfect permutation of order n when $2n+1$ is a prime. Furthermore, we use perfect permutations to construct cyclic spatially balanced Latin squares and symmetric spatially balanced Latin squares both of which are widely used in experimental designs.

Keywords perfect permutation; cyclic Latin square; symmetric Latin square; spatially balanced Latin square
MR(2010) Subject Classification 05B05, 46B20
Chinese Library Classification O157.2

收稿日期: 2020-04-02; 接受日期: 2021-08-30
基金项目: 国家自然科学基金 (12071226, 11931006); 国家自然科学青年基金 (11901039) 资助项目

1 引言

拉丁方的理论研究与实际应用是一个古老的经典问题, 文 [3] 中有大量关于拉丁方研究成果的综述. 本文主要研究在试验设计中有重要应用的空间均衡拉丁方 (spatially balanced Latin squares), 简记为 SBLS. 在农业试验中, 测试和比较重茬栽培的土壤大都是采用重复实验、分块实验以及随机安排等实验方法, 其中随机完全区组设计方法被广泛应用 [1, 4, 8]. 传统的随机分配栽培可能影响方差和变量的精度以及变量在空间上的相关性. 文 [9] 中指出空间均衡拉丁方可用来解决随机完全区组的这些局限性. 空间均衡拉丁方也被用在温室试验、多孔滴定板的化学分析及微阵列载玻片的基因组学研究中 [10].

SBLS 的构造是有趣且具有挑战的问题, 一直以来都是计算机领域的学者从算法和存在性的角度在研究. 2004 年, Gomes 等人使用模拟退火算法得到 12 阶以内的 SBLS. 文 [5] 中通过优化约束算法得到 18 阶以内的 SBLS. 2005 年, Smith 在文 [7] 中扩展了约束求解算法的思想, 得到 35 阶以内的 SBLS. Gomes 等人在文 [6] 中提出一种多项式算法且构造出一类 SBLS(n), 其中 $2n+1$ 是素数, 但证明非常复杂. Gomes 在文 [2] 中定义了循环的 SBLS, 构造出 14 阶以内的循环 SBLS, 提出以下公开问题: 给出循环 SBLS 的构造方法.

本文主要从数学的角度研究 SBLS 的构造, 我们首次提出 n 阶完美置换 (PP(n)) 的概念并研究它的构造方法和代数属性, 得到了一些小阶数的 PP(n) 及其性质, 主要解决了 $2n+1$ 为素数时 PP(n) 的存在性. 我们还利用完美置换构造了循环的 SBLS(n) 和对称的 SBLS(n).

文章组织结构如下: 第 2 节给出拉丁方的定义及相关结果; 第 3 节给出完美置换的定义, 应用完美置换构造循环的 SBLS(n) 和对称的 SBLS(n), 同时讨论了完美置换的一些代数性质; 最后一节证明了 $2n+1$ 为素数时 PP(n) 的存在性, 给出了文 [6] 中主要结果的简化证明, 同时也得到了一些新的循环的 SBLS(n) 和对称的 SBLS(n).

2 预备知识

记集合 $N=\{1,2,\ldots,n\}$. 一个 n 阶拉丁方是一个元素取自 N 的 $n\times n$ 阵列 L, 满足 N 中的每一个元素在 L 的每一行和每一列中都恰好出现一次. 设 $L=(l_{ij})$ 为 n 阶拉丁方, 若 $l_{ij}=l_{ji}$ 对任意的 $1\le i,j\le n$ 成立, 则称 L 是对称的. 一个 n 阶拉丁方的行 (列) 变换是指将它的行 (列) 作一次置换. 显然, 拉丁方经过行列变换后还是拉丁方.

设 $L=(l_{ij})$ 为 n 阶拉丁方, 其 x 行和 y 行在第 j 列的距离定义为 $R_j(L,x,y)=|l_{xj}-l_{yj}|$. L 的 x 行和 y 行的距离定义为 $R(L,x,y)=\sum_{j=1}^{n}R_j(L,x,y)$. 显然 $R(L,x,y)=R(L,y,x)$. 若 $R(L,x,y)=\frac{n(n+1)}{3}$ 对任意的 $1\le x<y\le n$ 成立, 则称 L 为行均衡的. 从 $R(L,x,y)$ 的定义可知, n 阶行均衡拉丁方作行列变换后, 得到的拉丁方仍然是一个行均衡的. 因此有下面的引理.

引理 2.1 设 L 是 n 阶行均衡的拉丁方, 则 L 经过行变换和列变换后得到的拉丁方也是行均衡的.

在 n 阶拉丁方 $L=(l_{ij})$ 中, 元素 x 和 y 在第 j 列的距离定义为 $D_j(L,x,y)=|s-k|$, 其中 $l_{sj}=x, l_{kj}=y$. 元素 x 和 y 在 L 中的距离定义为 $D(L,x,y)=\sum_{j=1}^{n}D_j(L,x,y)$. 若 $D(L,x,y)=\frac{n(n+1)}{3}$ 对任意的 $1\le x<y\le n$ 成立, 则称 L 为空间均衡拉丁方, 记为 SBLS(n). 因为 $D(L,x,y)$ 是一个正整数, 所以 SBLS(n) 存在时, $n\not\equiv 1\,(\mathrm{mod}\ 3)$.

下面引进 $(3,2,1)$- 共轭拉丁方的概念, 并用它给出一个判断拉丁方是否为 SBLS(n) 的新方法. 假设 $A=(a_{ij})$ 和 $B=(b_{kj})$ 均为 n 阶拉丁方, 若 $a_{ij}=k$ 当且仅当 $b_{kj}=i$, 则称 B 是 A 的 $(3,2,1)$- 共轭. 由定义可知, A 的 $(3,2,1)$- 共轭是 B 当且仅当 B 的 $(3,2,1)$- 共轭是 A.

引理 2.2 设 A 是一个 n 阶拉丁方, B 是 A 的 $(3,2,1)$- 共轭, 则对于任意两个元素 x,y,

$$D(A,x,y)=R(B,x,y). \tag{2.1}$$

证明 对任给的 $1\le j\le n$, 若 $a_{sj}=x$, $a_{kj}=y$, 则 $D_j(A,x,y)=|s-k|$. 由 B 是 A 的 $(3,2,1)$- 共轭可知 $b_{xj}=s$, $b_{yj}=k$. 所以 $D_j(A,x,y)=|s-k|=|b_{xj}-b_{yj}|$. 因此

$$D(A,x,y)=\sum_{j=1}^{n}D_j(A,x,y)=\sum_{j=1}^{n}|b_{xj}-b_{yj}|=R(B,x,y).$$

证毕.

若 A 是一个 SBLS(n), B 是 A 的 $(3,2,1)$- 共轭, 由引理 2.2 知, $R(B,x,y)=D(A,x,y)=\frac{n(n+1)}{3}$, 所以 B 是行均衡的. 反之, 若 B 是行均衡的, 则 $D(A,x,y)=\frac{n(n+1)}{3}$, $1\le x<y\le n$. 因此, 一个拉丁方是否为 SBLS(n) 等价于它的 $(3,2,1)$- 共轭是否行均衡. 由此可得以下引理.

引理 2.3 设 A 是一个 n 阶拉丁方, B 是 A 的 $(3,2,1)$- 共轭, 则 A 是 SBLS(n) 当且仅当 B 是行均衡的.

简洁起见, 下文中统一用 $x\,(\mathrm{mod}\ n)$ 来表示 x 模 n 后的最小非负剩余 t, 即 $x\equiv t\ (\mathrm{mod}\ n)$, $0\le t\le n-1$.

设 $L=(l_{ij})$ 是一个 n 阶拉丁方, 若对任意的 $2\le i<j\le n$, $l_{ij}=l_{i-1,j-1}$ 且 $l_{ji}=l_{j-1,n+1-i}$, 则称 L 是循环的. 容易看出, 循环拉丁方可由它的第一行元素生成. 在 n 阶循环拉丁方 $L=(l_{ij})$ 中, 若 $l_{1j}=a_{j-1}$, $1\le j\le n$, 则 $l_{ij}=a_{j-i\,(\mathrm{mod}\ n)}$, $1\le i\le n$. 从而

$$R_j(L,x,y)=|l_{xj}-l_{yj}|=|a_{j-x\ (\mathrm{mod}\ n)}-a_{j-y\ (\mathrm{mod}\ n)}|.$$

故

$$\begin{aligned}R(L,x,y)&=\sum_{j=1}^{n}R_j(L,x,y)\\&=\sum_{j=1}^{n}|a_{j-x\ (\mathrm{mod}\ n)}-a_{j-y\ (\mathrm{mod}\ n)}|\\&=\sum_{j=0}^{n-1}|a_{j+x-y\ (\mathrm{mod}\ n)}-a_j|.\end{aligned}\tag{2.2}$$

定义 2.4 若一个 n 阶空间均衡拉丁方 L 的 $(3,2,1)$- 共轭是循环的, 则称 L 为循环的空间均衡拉丁方, 简记为 CSBLS(n).

例 2.5 一个 CSBLS(5) A 和它的 $(3,2,1)$- 共轭 B.

$$A=\begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\\3&4&5&1&2\\4&5&1&2&3\\2&3&4&5&1\end{pmatrix},\quad B=\begin{pmatrix}1&2&4&3&5\\5&1&2&4&3\\3&5&1&2&4\\4&3&5&1&2\\2&4&3&5&1\end{pmatrix}.$$

3 完美置换

本文主要研究有限集 N 上的置换. 设 $P=(a_0,a_1,\ldots,a_{n-1})$ 是定义在 N 上的 n 阶置换. 对任意的正整数 t, 令 $P^t(a_j)=a_{j+t(\mathrm{mod}\ n)}$, $j\in\mathbb{Z}_n$, 定义 P 的 t- 段差如下

$$d_P(t)=\sum_{j=0}^{n-1}|a_{j+t\ \ (\mathrm{mod}\ n)}-a_j|. \tag{3.1}$$

容易看出

$$d_P(t)=\sum_{j=0}^{n-1}|P^t(a_j)-a_j|=\sum_{j=1}^{n}|P^t(j)-j|. \tag{3.2}$$

定义 3.1 给定 N 上的一个 n 阶置换 P, 若对任意的 $1\le t\le n-1$, $d_P(t)=\frac{n(n+1)}{3}$, 则称 P 是一个完美置换, 简记为 PP(n).

显然 $d_P(t)=d_P(n-t)$. 因此当验证置换 P 是否为完美置换时, 只需要验证

$$d_P(t)=\frac{n(n+1)}{3},\quad 1\le t\le\left\lfloor\frac{n}{2}\right\rfloor.$$

例 3.2 令 $n=5$, $P=(1,2,4,3,5)$, 则

$$d_P(1)=|2-1|+|4-2|+|3-4|+|5-3|+|1-5|=1+2+1+2+4=10,$$

$$d_P(2)=|4-1|+|3-2|+|5-4|+|1-3|+|2-5|=3+1+1+2+3=10.$$

故 $d_P(t)=n(n+1)/3$, $1\le t\le\lfloor\frac{n}{2}\rfloor$. 因此, P 是一个 PP(5).

下面给出利用 PP(n) 构造循环的 SBLS(n) 和对称的 SBLS(n) 的方法.

定理 3.3 若存在一个 PP(n), 则存在一个 CSBLS(n).

证明 设 $P=(a_0,a_1,\ldots,a_{n-1})$ 是一个 PP(n). 令 $L=(l_{ij})$ 是一个 n 阶循环拉丁方, 满足 $l_{1j}=a_{j-1}$, $1\le j\le n$. 设 B 是 L 的 $(3,2,1)$- 共轭. 下面证明 B 是一个 CSBLS(n).

因为 L 是循环拉丁方, 故由引理 2.3 可知只需证明 L 是行均衡的. 根据 (2.2) 和 (3.1) 可得

$$R(L,x,y)=\sum_{j=0}^{n-1}|a_{j+x-y\ \ (\mathrm{mod}\ n)}-a_j|=d_P(y-x). \tag{3.3}$$

由 P 是一个 PP(n) 可得 $d_P(y-x)=\frac{n(n+1)}{3}$. 所以 L 是行均衡的且 B 是一个 CSBLS(n). 证毕.

定理 3.4 若存在一个 PP(n), 则存在对称的 SBLS(n).

证明 设 $P=(p_0,p_1,\ldots,p_{n-1})$ 是一个 PP(n). 不失一般性, 可设 $p_0=1$. 令 $A=(a_{ij})$ 是一个循环拉丁方, $a_{ij}=p_{j-i(\mathrm{mod}\ n)}$. 根据定理 3.3 可知 A 是行均衡的. 令 B 是 A 经过一些行变换得到的拉丁方, 且满足 $b_{i1}=i$, $1\le i\le n$. 进一步, 令 C 是 B 经过一些列变换得到的拉丁方, 且满足 $c_{1,p_j}=p_{n-j(\mathrm{mod}\ n)}$, $0\le j\le n-1$. 令 $L=(l_{ij})$ 是 C 的 $(3,2,1)$- 共轭. 下面将证明 L 是一个对称的 SBLS(n). 根据引理 2.1 知 C 是行均衡的, 从而根据引理 2.3 可得 L 是一个 SBLS(n). 接下来, 只需证明 L 是对称的.

显然, C 的所有列的集合和 B 的所有列的集合相同, B 的所有行的集合和 A 的所有行的集合相同. 但是对于给定的行或者列的标号, 其在不同的拉丁方中的表示可能不同. 下面同样使用 $p_0,p_1,\ldots,p_{n-1}$ 作为行 (列) 的标号, 其中 $\{p_i:0\le i\le n-1\}=\{1,2,\ldots,n\}$. 根据构造, 对任意

的 $0 \le j \le n-1$, C 的第 p_j 列是 B 的第 q_j 列, B 的第 p_j 行是 A 的第 q_j 行, 其中 $q_0 = 1$ 且 $q_j = n - j + 1,\ 1 \le j \le n-1$.

下面证明 L 是一个对称的拉丁方, 即 $l_{p_i,p_j} = l_{p_j,p_i}$, $0 \le i, j \le n-1$. 设 $l_{p_i,p_j} = p_k$. 因为 L 是 C 的 $(3,2,1)$- 共轭, 则 $c_{p_k,q_j} = p_i$. 从而 $b_{p_k,q_j} = p_i$, $a_{q_k,q_j} = p_i$, 于是 $q_j - q_k \equiv i \pmod n$. 因为 $q_j \equiv 1 - j \pmod n$, 则 $q_j - q_k \equiv (1-j) - (1-k) \pmod n$, 即 $i \equiv k - j \pmod n$, $j \equiv k - i \pmod n$, 于是 $j \equiv q_i - q_k \pmod n$. 因此 $p_j = a_{q_k,q_i}$ 且 $c_{p_k,p_i} = b_{p_k,q_i} = a_{q_k,q_i} = p_j$. 因为 L 是 C 的 $(3,2,1)$- 共轭, 所以 $l_{p_j,p_i} = p_k$, 即 L 是对称的.

综上所述, L 是一个对称的 SBLS(n). 证毕.

下面给出 PP(n) 的一些基本性质.

定理 3.5 设 $P = (a_0, a_1, \dots, a_{n-1})$ 是一个 PP(n), 若 $\gcd(m,n) = 1$, $1 \le m \le n-1$, 则 P^m 也是一个 PP(n).

证明 令 $P^m = (b_0, b_1, \dots, b_{n-1})$, $b_i = a_{im \pmod n}$. 因为 $(m,n) = 1$, 所以 P^m 是 P 上的一个 n 阶置换. 对任意的 $1 \le t \le n-1$,

$$\begin{aligned} d_{P^m}(t) &= \sum_{j=0}^{n-1} |b_{j+t \pmod n} - b_j| \\ &= \sum_{j=0}^{n-1} |a_{(j+t)m \pmod n} - a_{jm \pmod n}| \\ &= \sum_{j=0}^{n-1} |a_{(jm \pmod n + tm \pmod n) \pmod n} - a_{jm \pmod n}| \\ &= \sum_{k=0}^{n-1} |a_{k+tm \pmod n} - a_k| \\ &= d_P(tm \pmod n) = \frac{n(n+1)}{3}. \end{aligned}$$

因此, P^m 是一个 PP(n). 证毕.

设 P 是一个 n 阶置换, 简洁起见, 以下用 $\mathscr{L}$ 表示 P 中 n 和 $n-1$ 对换, $\mathscr{S}$ 表示 P 中 1 和 2 对换, $\mathscr{F}$ 表示 i 和 $n+1-i$ 对换, $1 < i < n+1$, 即

$$\mathscr{L} = (n, n-1),\ \ \mathscr{S} = (1,2),\ \ \mathscr{F} = (1,n)(2,n-1)\cdots\left(\left\lfloor\frac{n}{2}\right\rfloor, n+1-\left\lfloor\frac{n}{2}\right\rfloor\right).$$

例 3.6 $P = (1,2,4,3,5)$, 则

$$\mathscr{L}(P) = (1,2,5,3,4),\ \ \mathscr{S}(P) = (2,1,4,3,5),\ \ \mathscr{F}(P) = (5,4,2,3,1).$$

定理 3.7 若 P 是一个 PP(n), 则 $\mathscr{L}(P)$, $\mathscr{S}(P)$ 和 $\mathscr{F}(P)$ 都是 PP(n).

证明 令 $A = \mathscr{L}(P)$, $B = \mathscr{S}(P)$, $C = \mathscr{F}(P)$. 首先证明 A 是一个 PP(n). 根据 (3.2) 任给

$$0 \le t \le n-1,\ \ d_P(t) = \sum_{j=1}^{n} |P^t(j) - j|.$$

在 n 个二元集合 $\{P^t(j), j\}$ 中, 至多有 4 个满足 $\{P^t(j), j\} \cap \{n-1, n\} \ne \emptyset$. 要证明 $d_A(t) = d_P(t)$, 只需要证明经过 n 和 $n-1$ 对换后, 原来的 n 个二元集合中至多有 4 个发生了变化, 并且发生变化后它们的绝对值之和保持不变.

下面分四种情况证明:

(1) $P^t(n)=n-1$ 且 $P^t(n-1)=n$.

此时, $|n-(n-1)|+|(n-1)-n|=|(n-1)-n|+|n-(n-1)|$.

(2) $P^t(n)=n-1$, $P^t(n-1)=k$ 且 $P^t(h)=n$, $k,h<n-1$.

此时, $|n-(n-1)|+|(n-1)-k|+|h-n|=2n-k-h=|(n-1)-n|+|n-k|+|h-(n-1)|$.

(3) $P^t(n-1)=n$, $P^t(n)=k$ 且 $P^t(h)=n-1$, $k,h<n-1$.

这种情况类似于 (2).

(4) $P^t(n-1)=r$, $P^t(n)=s$, $P^t(u)=n-1$ 且 $P^t(v)=n$, $r,s,u,v<n-1$.

此时 $|n-s|+|(n-1)-r|+|u-(n-1)|+|v-n|=4n-2-(s+r+u+v)=|(n-1)-s|+|n-r|+|u-n|+|v-(n-1)|$.

综上, A 是一个 PP(n). 类似可以证明 B 也是一个 PP(n).

下面证明 C 是一个 PP(n). 因为 $d_C(t)=\sum_{j=0}^{n-1}|C_{j+t}-C_j|=\sum_{j=0}^{n-1}|(n+1-P_{j+t})-(n+1-P_j)|=\sum_{j=0}^{n-1}|P_{j+t}-P_j|=d_P(t)$, 所以 C 是一个 PP(n). 证毕.

定理 3.8 若 $n\geq 5$, 则 PP(n) 所有解的个数是 8 的倍数.

证明 根据定理 3.7, 若 P 是一个 PP(n), 则 $\mathscr{L}(P)$, $\mathscr{S}(P)$ 和 $\mathscr{F}(P)$ 都是 PP(n). 令 T 是由 $\mathscr{L},\mathscr{S},\mathscr{F}$ 生成的变换群, 单位元记为 $\mathscr{E}$. 当 $n\geq 5$ 时, 容易验证

$$\mathscr{L}^2=\mathscr{S}^2=\mathscr{F}^2=\mathscr{E},\ \ \mathscr{S}\mathscr{F}=\mathscr{F}\mathscr{L},\ \ \mathscr{L}\mathscr{F}=\mathscr{F}\mathscr{S},\ \ \mathscr{S}\mathscr{L}=\mathscr{L}\mathscr{S},$$
$$\mathscr{L}\mathscr{F}\mathscr{L}=\mathscr{F}\mathscr{S}\mathscr{L}=\mathscr{S}\mathscr{F}\mathscr{S}=\mathscr{S}\mathscr{L}\mathscr{F}=\mathscr{L}\mathscr{S}\mathscr{F}=\mathscr{F}\mathscr{L}\mathscr{S},$$
$$\mathscr{L}\mathscr{F}\mathscr{S}=\mathscr{S}\mathscr{F}\mathscr{L}=\mathscr{F},\ \ \mathscr{S}\mathscr{L}\mathscr{S}=\mathscr{F}\mathscr{S}\mathscr{F}=\mathscr{L},\ \ \mathscr{L}\mathscr{S}\mathscr{L}=\mathscr{F}\mathscr{L}\mathscr{F}=\mathscr{S}.$$

不难验证, P, $\mathscr{L}(P)$, $\mathscr{S}(P)$, $\mathscr{L}\mathscr{S}(P)$, $\mathscr{F}(P)$, $\mathscr{F}\mathscr{L}(P)$, $\mathscr{F}\mathscr{S}(P)$ 和 $\mathscr{F}\mathscr{L}\mathscr{S}(P)$ 是 8 个不同的 PP(n). 对于 $n\geq 5$, 令 $T=\{\mathscr{E},\mathscr{L},\mathscr{S},\mathscr{L}\mathscr{S},\mathscr{F},\mathscr{F}\mathscr{L},\mathscr{F}\mathscr{S},\mathscr{F}\mathscr{L}\mathscr{S}\}$. 假设 A 和 B 是两个不同的 PP(n), 若存在某个 $\mathscr{T}\in T$, 使得 $\mathscr{T}(A)=B$, 则称 $A\sim B$. 容易证明 $\sim$ 是定义在 PP(n) 所有解上的等价关系. 因此, 利用上面定义的等价关系可以将 PP(n) 的所有解划分成等价类, 每个等价类含有 8 个等价的 PP(n). 所以 PP(n) 所有解的个数是 8 的倍数. 证毕.

下面三个表列出了当 $n=5,6,8$ 时 PP(n) 的等价类.

P	(1 2 4 3 5)	$\mathscr{F}(P)$	(1 5 4 2 3)
$\mathscr{L}(P)$	(1 2 5 3 4)	$\mathscr{F}\mathscr{L}(P)$	(1 3 2 5 4)
$\mathscr{S}(P)$	(1 4 3 5 2)	$\mathscr{F}\mathscr{S}(P)$	(1 4 5 2 3)
$\mathscr{L}\mathscr{S}(P)$	(1 5 3 4 2)	$\mathscr{F}\mathscr{L}\mathscr{S}(P)$	(1 3 2 4 5)

表 1 PP(5) 的 8 个解

P	(1 2 4 5 3 6)	$\mathscr{F}(P)$	(1 6 5 3 2 4)
$\mathscr{L}(P)$	(1 2 4 6 3 5)	$\mathscr{F}\mathscr{L}(P)$	(1 4 2 6 5 3)
$\mathscr{S}(P)$	(1 4 5 3 6 2)	$\mathscr{F}\mathscr{S}(P)$	(1 5 6 3 2 4)
$\mathscr{L}\mathscr{S}(P)$	(1 4 6 3 5 2)	$\mathscr{F}\mathscr{L}\mathscr{S}(P)$	(1 4 2 5 6 3)
P^5	(1 6 3 5 4 2)	$\mathscr{F}(P^5)$	(1 4 2 3 5 6)
$\mathscr{L}(P^5)$	(1 5 3 6 4 2)	$\mathscr{F}\mathscr{L}(P^5)$	(1 3 5 6 2 4)
$\mathscr{S}(P^5)$	(1 2 6 3 5 4)	$\mathscr{F}\mathscr{S}(P^5)$	(1 4 2 3 6 5)
$\mathscr{L}\mathscr{S}(P^5)$	(1 2 5 3 6 4)	$\mathscr{F}\mathscr{L}\mathscr{S}(P^5)$	(1 3 6 5 2 4)

表 2 PP(6) 的 16 个解

P	(1 3 8 7 4 5 2 6)	$\mathscr{F}(P)$	(1 2 5 4 7 3 8 6)
$\mathscr{L}(P)$	(1 3 7 8 4 5 2 6)	$\mathscr{F}\mathscr{L}(P)$	(1 5 4 7 3 8 6 2)
$\mathscr{S}(P)$	(1 6 2 3 8 7 4 5)	$\mathscr{F}\mathscr{S}(P)$	(1 2 5 4 8 3 7 6)
$\mathscr{L}\mathscr{S}(P)$	(1 6 2 3 7 8 4 5)	$\mathscr{F}\mathscr{L}\mathscr{S}(P)$	(1 5 4 8 3 7 6 2)
P^3	(1 7 2 3 4 6 8 5)	$\mathscr{F}(P^3)$	(1 4 8 2 7 6 5 3)
$\mathscr{L}(P^3)$	(1 8 2 3 4 6 7 5)	$\mathscr{F}\mathscr{L}(P^3)$	(1 7 6 5 3 2 4 8)
$\mathscr{S}(P^3)$	(1 3 4 6 8 5 2 7)	$\mathscr{F}\mathscr{S}(P^3)$	(1 4 7 2 8 6 5 3)
$\mathscr{L}\mathscr{S}(P^3)$	(1 3 4 6 7 5 2 8)	$\mathscr{F}\mathscr{L}\mathscr{S}(P^3)$	(1 8 6 5 3 2 4 7)
P^5	(1 5 8 6 4 3 2 7)	$\mathscr{F}(P^5)$	(1 3 5 6 7 2 8 4)
$\mathscr{L}(P^5)$	(1 5 7 6 4 3 2 8)	$\mathscr{F}\mathscr{L}(P^5)$	(1 8 4 2 3 5 6 7)
$\mathscr{S}(P^5)$	(1 7 2 5 8 6 4 3)	$\mathscr{F}\mathscr{S}(P^5)$	(1 3 5 6 8 2 7 4)
$\mathscr{L}\mathscr{S}(P^5)$	(1 8 2 5 7 6 4 3)	$\mathscr{F}\mathscr{L}\mathscr{S}(P^5)$	(1 7 4 2 3 5 6 8)
P^7	(1 6 2 5 4 7 8 3)	$\mathscr{F}(P^7)$	(1 6 8 3 7 4 5 2)
$\mathscr{L}(P^7)$	(1 6 2 5 4 8 7 3)	$\mathscr{F}\mathscr{L}(P^7)$	(1 2 6 8 3 7 4 5)
$\mathscr{S}(P^7)$	(1 5 4 7 8 3 2 6)	$\mathscr{F}\mathscr{S}(P^7)$	(1 6 7 3 8 4 5 2)
$\mathscr{L}\mathscr{S}(P^7)$	(1 5 4 8 7 3 2 6)	$\mathscr{F}\mathscr{L}\mathscr{S}(P^7)$	(1 2 6 7 3 8 4 5)

表 3 PP(8) 的 32 个解

从上表可以看出, 对 $n = 5, 6, 8$, 所有 PP(n) 解的个数不仅是 8 的倍数, 而且所有的解均可以由一个置换 P 生成. 如对于 $n = 5$, $\varphi(5) = 4$, 取 $P = (1, 2, 4, 3, 5)$, 由于 $P^2 = \mathscr{F}\mathscr{S}(P)$, $P^3 = \mathscr{F}\mathscr{L}(P)$, $P^4 = \mathscr{L}\mathscr{S}(P)$, 因此仅存在一个由 P 产生的等价类. 对于 $n = 6$, $\varphi(6) = 2$, 存在两个等价类, 分别由 $P = (1, 2, 4, 5, 3, 6)$ 和 $P^5 = (1, 6, 3, 5, 4, 2)$ 生成所有的解. 对于 $n = 8$, $\varphi(8) = 4$, 存在 4 个等价类, 分别由 $P = (1, 3, 8, 7, 4, 5, 2, 6)$, P^3, P^5 和 P^7 生成所有的解. 根据定理 3.5 可知一个 PP(n) 能够产生 $\varphi(n)$ 个 PP(n). 根据定理 3.8 可知 PP(n) 所有解的个数可以被 8 整除. 这两个结论有助于对所有 PP(n) 的解进行分类.

4 PP(n) 的一个无穷类

本节中假设 $n \geq 2$, $q = 2n + 1$ 是素数, ξ 是 $\mathbb{Z}_q$ 的一个本原元. 令 $a_i = \xi^i \pmod q$, $0 \leq i \leq q-2$. 由前面的约定知 $1 \leq a_i \leq q-1$. 我们还需要定义两个函数 f 和 g, 其中 $f : \mathbb{Z}_q \to \mathbb{Z}_q$ 满足:

$$f(i) = \min\{i, q-i\}. \tag{4.1}$$

$g : (\mathbb{Z}^+ \cup \{0\}, \mathbb{Z}^+ \cup \{0\}) \to \mathbb{Z}_q$ 满足: $g(i, j) = ij \pmod q$. 可以得出

$$g(i, j) = ij - \left\lfloor \frac{ij}{q} \right\rfloor q. \tag{4.2}$$

下面给出 f 和 g 的一些性质.

引理 4.1 函数 f 和 g 满足以下 4 条性质:

(1) $f(u) = f(q-u)$, $1 \leq u \leq q-1$.

(2) 若 $\gcd(t, q) = 1$, 则对任意的 $1 \leq j_1 < j_2 \leq n$, $f(g(t, j_1)) \neq f(g(t, j_2))$.

(3) $f(g(u, v)) = f(g(f(u), f(v)))$, $1 \leq u, v \leq q-1$.

(4) $f(a_{k+l \pmod n}) = f(g(f(a_k), f(a_l)))$, $1 \leq l \leq n-1$, $0 \leq k \leq n-1$.

证明 根据函数 f 的定义很容易得到性质 (1).

由于 q 是素数且 $\gcd(t, q) = 1$, 若 $1 \leq j_1 < j_2 \leq n$, 则 $tj_1 \not\equiv tj_2 \pmod q$ 且 $tj_1 \not\equiv -tj_2$

$(\mathrm{mod}\ q)$, 从而 $g(t,j_1)\neq g(t,j_2)$ 且 $g(t,j_1)+g(t,j_2)\neq q$. 因此, $f(g(t,j_1))\neq f(g(t,j_2))$. 于是 (2) 成立.

不难验证 $uv\equiv f(u)f(v)\ (\mathrm{mod}\ q)$ 或 $uv\equiv -f(u)f(v)\ (\mathrm{mod}\ q)$, 于是 $g(u,v)=g(f(u),f(v))$ 或 $g(u,v)=q-g(f(u),f(v))$. 对任给的 $1\leq u,\ v\leq q-1$, 可得 $f(g(u,v))=f(g(f(u),f(v)))$. 因此, 性质 (3) 正确.

因为 $a_i=\xi^i\ (\mathrm{mod}\ q)$, $a_{n+i}=-\xi^i\ (\mathrm{mod}\ q)$, 其中 $q=2n+1$, 所以当 $0\leq i\leq n-1$ 时, $a_i+a_{n+i}=q$. 因此, 当 $0\leq i\leq n-1$ 时, $f(a_{n+i})=f(q-a_i)=f(a_i)$. 对任给的 $1\leq l\leq n-1$, $0\leq k\leq n-1$, 可得

$$\begin{aligned}f(a_{k+l\ (\mathrm{mod}\ n)})&=f(a_{k+l})=f(\xi^{k+l}\ (\mathrm{mod}\ q))=f(\xi^k\times\xi^l\ (\mathrm{mod}\ q))\\&=f((\xi^k\ (\mathrm{mod}\ q))\times(\xi^l\ (\mathrm{mod}\ q))\ (\mathrm{mod}\ q))=f(a_k\times a_l\ (\mathrm{mod}\ q))\\&=f(g(a_k,a_l))=f(g(f(a_k),f(a_l))).\end{aligned}$$

由此可知, 性质 (4) 也成立. 证毕.

引理 4.2 记 $n\times n$ 阵列 $L=(l_{ij})$, 若 $l_{ij}=f(g(i,j))$, $1\leq i,\ j\leq n$, 则 L 是一个拉丁方.

证明 因为 q 是素数, 所以 $\gcd(t,q)=1$, $t\not\equiv 0\ (\mathrm{mod}\ q)$. 由引理 4.1 知, 对任给的 $1\leq j_1<j_2\leq n$, $f(g(t,j_1))\neq f(g(t,j_2))$. 因此, $f(g(t,1)),f(g(t,2)),\ldots,f(g(t,n))$ 是集合 N 上的一个置换. 又因为 $f(g(i,j))=f(g(j,i))$, 所以 $f(g(1,t)),f(g(2,t)),\ldots,f(g(n,t))$ 也是集合 N 上的一个置换. 因此, L 是一个拉丁方. 证毕.

引理 4.3 [6] 设 $(b_1,b_2,\ldots,b_n)$ 是 N 上的置换, 则

$$\sum_{j=1}^{n}|b_j-j|=n(n+1)-2\sum_{j=1}^{n}\min\{j,b_j\}. \tag{4.3}$$

在证明主要结论之前, 我们还需要下面的引理. 需要说明的是和下面引理类似的结论在文 [6] 中已经出现, 但没有用函数的语言叙述, 且结论的证明非常复杂, 需要分析 32 种不同的情况, 文 [6] 中只是证明了其中的两种情况.

引理 4.4 对于任给的 $2\leq t\leq n$, $1\leq j\leq n$,

$$|f(g(t,j))-j|=\min\{f(g(t-1,j)),f(g(t+1,j))\}. \tag{4.4}$$

证明 由 (4.1) 和 (4.2) 知

$$f(g(t,j))-j=\begin{cases}(t-1)j-\left\lfloor\dfrac{tj}{q}\right\rfloor q, & 1\leq g(t,j)\leq n,\\ \left(\left\lfloor\dfrac{tj}{q}\right\rfloor+1\right)q-(t+1)j, & n+1\leq g(t,j)\leq 2n.\end{cases}$$

以下分 4 种情形讨论:

情形 1 $f(g(t,j))-j>0$ 且 $1\leq g(t,j)\leq n$.

此时, $(t-1)j-\lfloor\frac{tj}{q}\rfloor q>0$, 即 $\frac{(t-1)j}{q}>\lfloor\frac{tj}{q}\rfloor$, 由此可得 $\lfloor\frac{tj}{q}\rfloor=\lfloor\frac{(t-1)j}{q}\rfloor$, 从而 $g(t,j)=g(t-1,j)+j$, 于是 $1\leq g(t-1,j)\leq n$, 因此, $f(g(t,j))-j=g(t,j)-j=g(t-1,j)=f(g(t-1,j))$, 即 $|f(g(t,j))-j|=f(g(t-1,j))$.

下面证明 $f(g(t+1,j))>f(g(t-1,j))$.

由 $1 \le g(t,j) \le n$ 且 $1 \le j \le n$ 可得 $g(t+1,j) = g(t,j) + j$, 从而 $\lfloor \frac{(t+1)j}{q} \rfloor = \lfloor \frac{tj}{q} \rfloor$. 若 $g(t+1,j) \le n$, 则 $f(g(t+1,j)) = (t+1)j - \lfloor \frac{(t+1)j}{q} \rfloor q = (t+1)j - \lfloor \frac{tj}{q} \rfloor q$, 从而 $f(g(t+1,j)) - f(g(t-1,j)) = (t+1)j - \lfloor \frac{tj}{q} \rfloor q - (t-1)j + \lfloor \frac{tj}{q} \rfloor q = 2j > 0$. 若 $g(t+1,j) > n$, 则 $f(g(t+1,j)) = (\lfloor \frac{(t+1)j}{q} \rfloor + 1)q - (t+1)j = (\lfloor \frac{tj}{q} \rfloor + 1)q - (t+1)j$. 所以

$$\begin{aligned} f(g(t+1,j)) - f(g(t-1,j)) &= \left(\left\lfloor \frac{tj}{q} \right\rfloor + 1 \right) q - (t+1)j - (t-1)j + \left\lfloor \frac{tj}{q} \right\rfloor q \\ &= \left(2 \left\lfloor \frac{tj}{q} \right\rfloor + 1 \right) q - 2tj > 0. \end{aligned}$$

情形 2 $f(g(t,j)) - j > 0$ 且 $n+1 \le g(t,j) \le 2n$.

此时, $(\lfloor \frac{tj}{q} \rfloor + 1)q - (t+1)j > 0$, 即 $\frac{(t+1)j}{q} - 1 < \lfloor \frac{tj}{q} \rfloor$, 又 $\frac{tj}{q} < \frac{(t+1)j}{q}$, 故 $\lfloor \frac{tj}{q} \rfloor = \lfloor \frac{(t+1)j}{q} \rfloor$. 于是 $g(t+1,j) = g(t,j) + j$, 从而 $n+1 \le g(t+1,j) \le 2n$. 因此, $f(g(t,j)) - j = (\lfloor \frac{tj}{q} \rfloor + 1)q - (t+1)j = (\lfloor \frac{(t+1)j}{q} \rfloor + 1)q - (t+1)j = f(g(t+1,j))$, 即 $|f(g(t,j)) - j| = f(g(t+1,j))$.

下面证明 $f(g(t+1,j)) < f(g(t-1,j))$.

由 $n+1 \le g(t,j) \le 2n$ 且 $1 \le j \le n$ 可得 $g(t-1,j) = g(t,j) - j$, 从而 $\lfloor \frac{tj}{q} \rfloor = \lfloor \frac{(t-1)j}{q} \rfloor$. 若 $1 \le g(t-1,j) \le n$, 则 $f(g(t-1,j)) = (t-1)j - \lfloor \frac{(t-1)j}{q} \rfloor q = (t-1)j - \lfloor \frac{tj}{q} \rfloor q$, 从而 $f(g(t-1,j)) - f(g(t+1,j)) = (t-1)j - \lfloor \frac{tj}{q} \rfloor q - (\lfloor \frac{tj}{q} \rfloor + 1)q + (t+1)j = 2tj - (2\lfloor \frac{tj}{q} \rfloor + 1)q > 0$. 若 $n+1 \le g(t-1,j) \le 2n$, 则

$$f(g(t-1,j)) = \left(\left\lfloor \frac{(t-1)j}{q} \right\rfloor + 1 \right) q - (t-1)j = \left(\left\lfloor \frac{tj}{q} \right\rfloor + 1 \right) q - (t-1)j > f(g(t+1,j)).$$

情形 3 $f(g(t,j)) - j < 0$ 且 $1 \le g(t,j) \le n$.

此时, $j > f(g(t,j)) = g(t,j)$, 于是 $g(t,j) = g(t-1,j) + j - q$, $n+1 \le g(t-1,j) \le 2n$, 从而 $\lfloor \frac{tj}{q} \rfloor = \lfloor \frac{(t-1)j}{q} \rfloor + 1$. 因此, $j - f(g(t,j)) = j - tj + \lfloor \frac{tj}{q} \rfloor q = (\lfloor \frac{(t-1)j}{q} \rfloor + 1)q - (t-1)j = f(g(t-1,j))$, 即 $|f(g(t,j)) - j| = f(g(t-1,j))$.

下面证明 $f(g(t+1,j)) > f(g(t-1,j))$.

由 $1 \le g(t,j) \le n$ 且 $1 \le j \le n$ 可得 $g(t+1,j) = g(t,j) + j$, 从而 $\lfloor \frac{(t+1)j}{q} \rfloor = \lfloor \frac{tj}{q} \rfloor$. 若 $g(t+1,j) \le n$, 则 $f(g(t+1,j)) = (t+1)j - \lfloor \frac{(t+1)j}{q} \rfloor q = (t+1)j - \lfloor \frac{tj}{q} \rfloor q$, 从而 $f(g(t+1,j)) - f(g(t-1,j)) = (t+1)j - \lfloor \frac{tj}{q} \rfloor q - (\lfloor \frac{tj}{q} \rfloor q - (t-1)j) = 2tj - 2\lfloor \frac{tj}{q} \rfloor q > 0$. 若 $g(t+1,j) > n$, 则 $f(g(t+1,j)) = (\lfloor \frac{(t+1)j}{q} \rfloor + 1)q - (t+1)j = (\lfloor \frac{tj}{q} \rfloor + 1)q - (t+1)j$, 因此

$$\begin{aligned} f(g(t+1,j)) - f(g(t-1,j)) &= \left(\left\lfloor \frac{tj}{q} \right\rfloor + 1 \right) q - (t+1)j - \left(\left\lfloor \frac{tj}{q} \right\rfloor q - (t-1)j \right) \\ &= q - 2j > 0. \end{aligned}$$

情形 4 $f(g(t,j)) - j < 0$ 且 $n+1 \le g(t,j) \le 2n$.

此时, $j > f(g(t,j)) = q - g(t,j)$, 即 $g(t,j) + j > q$, 于是 $1 \le g(t+1,j) \le n$, 从而 $\lfloor \frac{tj}{q} \rfloor = \lfloor \frac{(t+1)j}{q} \rfloor - 1$, 因此 $j - f(g(t,j)) = j - (\lfloor \frac{tj}{q} \rfloor + 1)q + tj = (t+1)j - \lfloor \frac{(t+1)j}{q} \rfloor q = f(g(t+1,j))$, 即 $|f(g(t,j)) - j| = f(g(t+1,j))$.

下面证明 $f(g(t+1,j)) < f(g(t-1,j))$.

由 $n+1 \le g(t,j) \le 2n$ 且 $1 \le j \le n$ 可得 $g(t-1,j) = g(t,j) - j$, 从而 $\lfloor \frac{tj}{q} \rfloor = \lfloor \frac{(t-1)j}{q} \rfloor$. 若 $1 \le g(t-1,j) \le n$, 则 $f(g(t-1,j)) = (t-1)j - \lfloor \frac{(t-1)j}{q} \rfloor q = (t-1)j - \lfloor \frac{tj}{q} \rfloor q$, 从而

$f(g(t-1,j))-f(g(t+1,j))=(t-1)j-\lfloor\frac{tj}{q}\rfloor q+(\lfloor\frac{tj}{q}\rfloor+1)q-(t+1)j=q-2j>0$. 若 $n+1\le g(t-1,j)\le 2n$, 则 $f(g(t-1,j))=(\lfloor\frac{(t-1)j}{q}\rfloor+1)q-(t-1)j=(\lfloor\frac{tj}{q}\rfloor+1)q-(t-1)j$, 因此

$$\begin{aligned}f(g(t-1,j))-f(g(t+1,j))&=\left(\left\lfloor\frac{tj}{q}\right\rfloor+1\right)q-(t-1)j+\left(\left\lfloor\frac{tj}{q}\right\rfloor+1\right)q-(t+1)j\\&=2\left(\left\lfloor\frac{tj}{q}\right\rfloor+1\right)q-2tj>0.\end{aligned}$$

综上可得 $|f(g(t,j))-j|=\min\{f(g(t-1,j)),f(g(t+1,j))\}$, $2\le t\le n$, $1\le j\le n$. 证毕.

根据前面的引理, 下面证明本文的主要结论.

定理 4.5 对任意 $n\ge 2$, 若 $q=2n+1$ 是素数, 则存在 PP(n).

证明 设 ξ 是 GF(q) 的本原元, $a_i=\xi^i$, $0\le i\le n-1$. 令 $\alpha=(f(a_0),f(a_1),\dots,f(a_{n-1}))$. 下证 α 是一个 PP(n).

由 $\xi^n\equiv -1\pmod q$ 可得 $a_i+a_{n+i}\equiv\xi^i+\xi^{n+i}\equiv 0\pmod q$. 任给 $0\le i<j\le n-1$, 若 $a_i+a_j\not\equiv 0\pmod q$, 则 $f(a_i)\ne f(a_j)$, 从而 α 是集合 N 上的一个轮换. 任给 $1\le l\le n-1$,

$$\begin{aligned}d(l)&=\sum_{k=0}^{n-1}|f(a_{k+l\pmod n})-f(a_k)|\\&=\sum_{k=0}^{n-1}|f(g(f(a_l),f(a_k)))-f(a_k)|\quad\text{(根据引理 4.1)}\\&=\sum_{j=1}^{n}|f(g(f(a_l),j))-j|.\end{aligned}$$

根据 (4.3) 可得

$$d(l)=n(n+1)-2\sum_{j=1}^{n}\min\{j,f(g(f(a_l),j))\}.\tag{4.5}$$

设存在 $0\le s\le n-1$, 使得 $g((f(a_l)-1)^{-1},f(a_l)+1)=a_s$, 或者 $g((f(a_l)-1)^{-1},f(a_l)+1)=q-a_s$. 从而 $a_s(f(a_l)-1)\equiv f(a_l)+1\pmod q$), 或者 $-a_s(f(a_l)-1)\equiv f(a_l)+1\pmod q$). 为统一两种情况证明, 设 $x(f(a_l)-1)\equiv f(a_l)+1\pmod q$), $x\in\{a_s,q-a_s\}$, 于是

$$\begin{aligned}d(l)&=\sum_{j=1}^{n}|f(g(f(a_l),j))-j|\\&=\sum_{j=1}^{n}\min\{f(g(f(a_l)-1,j)),f(g(x(f(a_l)-1),j))\}\quad\text{(根据 (4.4))}\\&=\sum_{j=1}^{n}\min\{f(g(f(a_l)-1,j)),f(g(x,f(g(f(a_l)-1,j))))\}\\&=\sum_{t_{l,j}=1}^{n}\min\{t_{l,j},f(g(x,t_{l,j}))\}\quad\text{(令 }t_{l,j}=f(g(f(a_l)-1,j))\text{)}\\&=\sum_{j=1}^{n}\min\{j,f(g(x,j))\}\quad\text{(根据引理 4.1)}\\&=\sum_{j=1}^{n}\min\{j,f(g(f(x),j))\}.\end{aligned}$$

当 $x \in \{a_s, q-a_s\}$ 时, $f(x) = f(a_s)$. 于是 $d(l) = \sum_{j=1}^{n} \min\{j, f(g(f(a_s), j))\}$. 根据 (4.5) 可得, $d(l) = \frac{n(n+1)}{2} - \frac{1}{2}d(s)$.

下面证明 $d(s) = \frac{n(n+1)}{2} - \frac{1}{2}d(l)$. 由前可知 $x(f(a_l)-1) \equiv f(a_l)+1 \pmod q$, $x \in \{a_s, -a_s\}$. 显然 $f(x) = f(a_s)$. 若 $1 \le x \le n$, 则 $x = f(x) = f(a_s)$. 从而 $f(a_l)(f(a_s)-1) \equiv f(a_s)+1 \pmod q$; 若 $1+n \le x \le 2n$, 则 $x = q - f(a_s)$. 从而 $f(a_s)(f(a_l)-1) \equiv -a_s(f(a_l)-1) \equiv -(f(a_l)+1) \pmod q$, 即 $f(a_l)^{-1}(f(a_s)-1) \equiv f(a_s)+1 \pmod q$. 设 $x(f(a_s)-1) \equiv f(a_s)+1 \pmod q$, $x \in \{f(a_l), f(a_l)^{-1}\}$. 类似 $d(l)$ 的推导, 可得 $d(s) = \frac{n(n+1)}{2} - \frac{1}{2}d(l)$.

由 $d(l) = \frac{n(n+1)}{2} - \frac{1}{2}d(s)$ 和 $d(s) = \frac{n(n+1)}{2} - \frac{1}{2}d(l)$, 可得

$$d(l) = \frac{n(n+1)}{3}, \quad 1 \le l \le n-1.$$

因此, α 是一个 PP(n). 证毕.

根据定理 3.3 和定理 4.5, 我们可得以下推论, 部分回答了文 [2] 中关于 CSBLS(n) 构造方法的公开问题.

推论 4.6 对任意 $n \ge 2$, 当 $2n+1$ 是素数时, 存在 CSBLS(n).

由定理 3.4 和定理 4.5 可得关于对称空间均衡拉丁方的一个推论.

推论 4.7 对任意 $n \ge 2$, 当 $2n+1$ 是素数时, 存在对称的 SBLS(n).

最后, 我们利用函数 f 和 g 给出 SBLS(n) 的一个简单构造方法. 在给出具体的构造方法之前, 我们先给两个引理.

引理 4.8 设 $n \ge 2$, $q = 2n+1$ 是素数. 若 $L = (l_{ij})$, 其中 $l_{ij} = f(g(i,j))$, $1 \le i, j \le n$, 则 L 是一个行均衡的 n 阶拉丁方.

证明 设 ξ 是 GF(q) 的一个本原元. 根据引理 4.2 知 L 是一个 n 阶拉丁方. 根据定理 4.5 知 $P = (f(a_0), f(a_1), \ldots, f(a_{n-1}))$ 是一个 PP(n). 对任给的两个不同的元素 $1 \le x, y \le n$, 不失一般性, 设 $x = f(a_i)$, $y = f(a_j)$, $1 \le j < i \le n$, 则

$$\begin{aligned}
R(L,x,y) &= \sum_{j=1}^{n} |l_{xj} - l_{yj}| \\
&= \sum_{j=1}^{n} |f(g(x,j)) - f(g(y,j))| \\
&= \sum_{j=1}^{n} |f(g(yy^{-1}x, j)) - f(g(y,j))| \\
&= \sum_{j=1}^{n} |f(g(g(y,j), g(y^{-1},x))) - f(g(y,j))| \\
&= \sum_{j=1}^{n} |f(g(f(g(y,j)), f(g(y^{-1},x)))) - f(g(y,j))| \quad \text{(根据引理 4.1)} \\
&= \sum_{j=1}^{n} |f(g(f(g(y^{-1},x)),j)) - j| \quad \text{(根据引理 4.1)} \\
&= \sum_{j=1}^{n} |f(g(f(a_{i-j}),j)) - j| = d_P(i-j).
\end{aligned}$$

因为 P 是一个 PP(n), 所以 $R(L,x,y)=d_P(i-j)=\frac{n(n+1)}{3}$. 因此, L 是行均衡的. 证毕.

引理 4.9 设 $n\geq 2$, $q=2n+1$ 是素数. 令 $L=(l_{ij})$, 其中 $l_{ij}=f(g(i,j))$, $1\leq i,j\leq n$. 若拉丁方 $B=(b_{ij})$ 是 L 的 $(3,2,1)$- 共轭, 则对任意 $1\leq j\leq n$, B 的第 j 列是 L 的第 b_{1j} 列.

证明 对任意 $1\leq j\leq n$, 只需要证明对所有的 $1\leq i\leq n$, $b_{ij}=l_{i,b_{1j}}$. 因为 B 是 L 的一个 $(3,2,1)$- 共轭, 于是 $l_{k_i,j}=i$, 从而 $f(g(k_i,j))=i$, 故

$$\begin{aligned} l_{i,b_{1j}} &= f(g(i,b_{1j}))\\ &= f(g(f(g(k_i,j)),b_{1j}))\\ &= f(g(g(k_i,j),b_{1j})) \quad (\text{根据引理 4.1})\\ &= f(g(k_i,g(j,b_{1j})))\\ &= f(g(k_i,f(g(j,b_{1j})))) \quad (\text{根据引理 4.1}). \end{aligned}$$

进一步, 因为 B 是 L 的 $(3,2,1)$- 共轭, 所以 $l_{b_{1j},j}=1$. 于是可得 $f(g(j,b_{1j}))=1$. 从而 $l_{i,b_{1j}}=f(g(k_i,f(g(j,b_{1j}))))=f(g(k_i,1))=k_i$. 因此, 对所有的 $1\leq i\leq n$, $b_{ij}=l_{i,b_{1j}}$. 证毕.

定理 4.10 设 $n\geq 2$, $q=2n+1$ 是素数. 若 $L=(l_{ij})$, 其中 $l_{ij}=f(g(i,j))$, $1\leq i,j\leq n$, 则 L 是一个 SBLS(n).

证明 令 B 是 L 的一个 $(3,2,1)$- 共轭. 我们由引理 4.9 可知 L 经过列变换可以得到 B. 再由引理 4.8 可知 L 是一个行均衡的拉丁方, 于是由引理 2.1 可得 B 也是一个行均衡的拉丁方. 最后根据引理 3.5 就可以得出结论. 证毕.

致谢 感谢苏州大学朱烈教授建议我们研究此问题, 感谢他和上海师范大学范金萍博士在本文形成过程中的有益的讨论. 感谢匿名审稿人提出高质量的评论和建议.

参 考 文 献

[1] Atkinson A. C., Bailey R. A., One hundred years of design of experiments on and off the pages of biometrika, *Biometrika*, 2001, **88**(1): 53–97.

[2] Bras R. L., Gomes C. P., Selman B., From streamlined combinatorial search to efficient constructive procedures, In: Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence, 2012: 499–506.

[3] Colbourn C. J., Dinitz J. H., Handbook of Combinatorial Designs (2nd ed.), Chapman & Hall/CRC, New York, 2007.

[4] Cochran W. G., Cox G. M., Experimental designs, John Wiley & Sons, Oxford, 1957.

[5] Gomes C. P., Sellmann M., Streamlined constraint reasoning, In: Lecture Notes in Computer Science, Springer, Berlin, 2004, Vol. 3258: 274–289.

[6] Le Bras R., Perrault A., Gomes C. P., Polynomial time construction for spatially balanced Latin squares, Technical report, Cornell University Library, 2012, http://hdl.handle.net/1813/28697.

[7] Smith C., Gomes C. P., Fernández C., Streamlining local search for spatially balanced Latin squares, In: International Joint Conference on Artificial Intelligence, Morgan Kaufmann, 2005, 1539–1541 (https://www.ijcai.org/Proceedings/05/Papers/post-0460.pdf).

[8] Van Es H. M., Sources of soil variability, In: Methods of Soil Analysis: Part 4 Physical Properties (5.4), 2002: 1–13.

[9] Van Es H. M., Van Es C. L., Spatial nature of randomization and its effect on the outcome of field experiments, *Agronomy Journal*, 1993, **85**(2): 420–428.

[10] Van Es H. M., Gomes C. P., Sellmann M., et al., Spatially-balanced complete block designs for field experiments, *Geoderma*, 2007, **140**(4): 346–352.