



列正交强正交阵列的构造

献给朱烈教授 80 华诞

包经俊¹, 季利均^{2*}, 潘元瑶²

1. 宁波大学数学与统计学院, 宁波 315211;

2. 苏州大学数学科学学院, 苏州 215006

E-mail: baojingjun@nbu.edu.cn, jilijun@suda.edu.cn, 2833807862@qq.com

收稿日期: 2022-04-17; 接受日期: 2022-06-18; 网络出版日期: 2022-08-17; * 通信作者
国家自然科学基金 (批准号: 11871363) 资助项目

摘要 在计算机试验中, 强正交阵列比一般的阵列具有更好的空间填充性质. 强度为 $2+$ 、 $2*$ 、 $3-$ 和 3 的强正交阵列可以改进低维的空间填充性质, 列正交性在计算机试验中起着重要作用. 本文利用差矩阵和线性码的生成矩阵构造强度为 $2+$ 、 $2*$ 、 $3-$ 和 3 的列正交强正交阵列. 与已知的结果相比, 本文构造的列正交强正交阵列具有更多的因子数.

关键词 正交阵列 差矩阵 空间填充设计

MSC (2020) 主题分类 05B15

1 引言

物理现象的确定性计算机模拟在科学和工程中得到了广泛的应用. 尤其是空间填充设计, 它在计算机试验中起着重要作用, 参见文献 [5, 12].

受计算机试验中的 (t, m, s) - 网格 (nets) 结构的启发, He 和 Tang^[7] 提出了强正交阵列 (strong orthogonal array, SOA) 的概念. 相较于强度为 t 的正交阵列 (orthogonal array, OA), 强度为 t 的强正交阵列在空间维度低于 t 时具有更好的填充性质, 同时还保留 t 维空间的填充性质. 为了实现强正交阵列的更好性质, 它的强度应当不小于 3. 给定因子数, 强度为 3 的强正交阵列通常需要更多的行数. 为了更经济且保持强度为 3 的强正交阵列的二维空间填充性质, He 等^[6] 提出了强度为 $2+$ 的强正交阵列.

在计算机试验设计中, 阵列的列正交性质起着重要作用. 列正交性质的优势在于列正交设计往往具有空间填充性质. 更具体地, 当考虑 Gauss 过程模型时, 列正交性质可以作为基础用于寻找空间填充设计, 详细的列正交性的优点参见文献 [1].

英文引用格式: Bao J J, Ji L J, Pan Y Y. Constructions of column-orthogonal strong orthogonal arrays (in Chinese). Sci Sin Math, 2023, 53: 233–248, doi: 10.1360/SSM-2022-0062

2021 年, Li 等^[10] 提出了强度为 2^* 的列正交强正交阵列. 与 Zhou 和 Tang^[13] 所定义的 $\text{OSOA}(N, m, s^2, 2+)$ 类似, $\text{OSOA}(N, m, s^3, 2^*)$ 也满足任意两列可以塌缩成一个 $\text{OA}(N, 2, s^2 \times s, 2)$ 和一个 $\text{OA}(N, 2, s \times s^2, 2)$, 且列具有正交性. 两者主要的差别在于水平数, 前者的水平数是 s^2 , 而后的水平数是 s^3 , 这蕴涵着后者在任何一维空间上都实现了更精细的分层, 同时后者比前者具有更好的二维平衡性^[10]. 从 Zhou 和 Tang^[13] 及 Li 等^[10] 获得的结果来看, 强度为 $2+$ 和 2^* 的列正交强正交阵列的因子数几乎相同, 强度为 $3-$ 和 3 的列正交强正交阵列的因子数也几乎相同. 与强度为 3 的列正交强正交阵列比较, 强度为 $2+$ 和 2^* 的列正交强正交阵列具有更大的因子数. 相较于强度为 3 的列正交强正交阵列, 强度为 $2+$ 、 2^* 和 $3-$ 的列正交强正交阵列还有其他好的性质 (参见文献 [10, 13]).

2019 年, Zhou 和 Tang^[13] 用一对具有额外性质的正交阵列构造了强度为 $2+$ 和 $3-$ 的列正交强正交阵列, 用正则的 2 水平饱和设计和 Hadamard 矩阵构造强度为 $3-$ 的 4 水平列正交强正交阵列, 并且还用饱和设计 $\text{OA}(s^k, (s^k - 1)/(s - 1), s, 2)$ 来构造 $\text{OSOA}(s^k, (s^{k-1} - 1)/(s - 1), s^2, 2+)$. Li 等^[10] 也用一对具有特殊性质的正交阵列构造强度为 2^* 和 3 的列正交强正交阵列, 还分别用 2 水平饱和设计 $\text{OA}(m, m - 1, 2, 2)$ 与饱和设计 $\text{OA}(s^k, (s^k - 1)/(s - 1), s, 2)$ 来构造 $\text{OSOA}(2m, m - 2, 8, 3)$ 与 $\text{OSOA}(s^k, 2 \lfloor \frac{s^{k-1} - 1}{2s - 2} \rfloor, s^3, 2^*)$.

本文用差矩阵和线性码的生成矩阵来构造强度为 $2+$ 、 2^* 、 $3-$ 和 3 的列正交强正交阵列, 所得到的列正交强正交阵列有更多的因子数. 本文也证明存在一个强度为 2^* 的强正交阵列当且仅当存在一个强度为 $2+$ 的强正交阵列, 存在一个强度为 $3-$ 的强正交阵列当且仅当存在一个强度为 3 的强正交阵列, 一定程度上解释了为何强度为 2^* 和 3 的列正交强正交阵列的因子数分别与强度为 $2+$ 和 $3-$ 的列正交强正交阵列的因子数几乎相同.

本文余下内容安排如下: 第 2 节介绍预备知识以及强度为 2^* 、 $2+$ 、 $3-$ 和 3 的强正交阵列之间的联系. 第 3 节利用差矩阵给出列正交强正交阵列的 3 个构造方法. 第 4 节利用线性码的生成矩阵获得列正交强正交阵列的 4 个构造. 第 5 节总结全文.

2 预备知识和强正交阵列等价刻画

一个强度为 t 、因子数为 m 的正交阵列是一个第 j 列元素取自于集合 $\{0, 1, \dots, s_j - 1\}$ 的 $N \times m$ 阵列, 满足: 对于它的任意 $N \times t$ 子阵列, 所有可能的 t 元组作为行在该子阵中出现相同的次数. 记此阵列为 $\text{OA}(N, m, s_1 \times \dots \times s_m, t)$. 当 $s_1 = \dots = s_m = s$ 时, 称此阵列是对称的, 并记为 $\text{OA}(N, m, s, t)$; 否则, 称此阵列是非对称的. 一个强度为 t 、因子数为 m 、水平数为 s^t 的强正交阵列 (记为 $\text{SOA}(N, m, s^t, t)$) 是一个元素取自于集合 $\{0, 1, \dots, s^t - 1\}$ 的 $N \times m$ 阵列, 满足: 对于任意满足 $u_1 + u_2 + \dots + u_g = t$ 和 $g \leq t$ 的正整数 g 与 $u_1, u_2, \dots, u_g$, 它的任意 $N \times g$ 子阵列可以塌缩成一个 $\text{OA}(N, g, s^{u_1} \times \dots \times s^{u_g}, g)$. 此处, 水平数 s^t 塌缩成水平数 s^{u_j} 的方式为: 对于 $a = 0, 1, \dots, s^t - 1$, 将 a 映射成 $\lfloor \frac{a}{s^{t-u_j}} \rfloor$, 其中 $\lfloor w \rfloor$ 表示不超过 w 的最大整数. 一个 $\text{SOA}(N, m, s^3, 3)$ 满足: 任意两列可以塌缩成一个 $\text{OA}(N, 2, s^2 \times s, 2)$ 和一个 $\text{OA}(N, 2, s \times s^2, 2)$, 且任意三列可以塌缩成一个 $\text{OA}(N, 3, s, 3)$.

一个强度为 $2+$ 的强正交阵列, 记为 $\text{SOA}(N, m, s^2, 2+)$, 是一个元素取自于集合 $\{0, 1, \dots, s^2 - 1\}$ 的 $N \times m$ 阵列, 满足: 任意两列可以塌缩成一个 $\text{OA}(N, 2, s^2 \times s, 2)$ 和一个 $\text{OA}(N, 2, s \times s^2, 2)$. 强度为 $2+$ 的强正交阵列不需要满足任意三列可以塌缩成一个 $\text{OA}(N, 3, s, 3)$ 的要求. 若一个 $\text{SOA}(N, m, s^2, 2+)$ 的任意三列可以塌缩成一个 $\text{OA}(N, 3, s, 3)$, 则称其是强度为 $3-$ 的强正交阵列, 记为 $\text{SOA}(N, m, s^2, 3-)$.

一个强度为 2^* 的强正交阵列, 记为 $\text{SOA}(N, m, s^3, 2^*)$, 是一个元素取自于集合 $\{0, 1, \dots, s^3 - 1\}$

的 $\text{OA}(N, m, s^3, 1)$ 且满足: 任意两列可以塌缩成一个 $\text{OA}(N, 2, s^2 \times s, 2)$ 和一个 $\text{OA}(N, 2, s \times s^2, 2)$.

Lawrence^[9] 于 1996 年提出了广义正交阵列的概念. He 和 Tang^[7] 于 2013 年推广了 Lawrence 的结果, 并证明存在一个强正交阵列等价于存在一个广义正交阵列. 一个强度为 t 、水平数为 s 、限制数为 m 的广义正交阵列 (generalized orthogonal array, GOA), 记为 $\text{GOA}(N, m, s, t)$, 是一个元素取自于集合 $\{0, 1, \dots, s-1\}$ 的 $N \times (mt)$ 阵列 $A = (A_{11}, A_{12}, \dots, A_{1t}; \dots; A_{m1}, A_{m2}, \dots, A_{mt})$, 此 mt 列分成每个都为 t 列的 m 个组 $A_1, A_2, \dots, A_m$, 使得对于任意满足 $t_1 + t_2 + \dots + t_m = t$ 的非负整数 $t_1, t_2, \dots, t_m$, 从每一个组 A_i ($1 \leq i \leq m$) 中取出它的前 t_i ($0 \leq t_i \leq t$) 列所组成的 $N \times t$ 子阵列是一个 $\text{OA}(N, t, s, t)$.

引理 2.1^[7] 设 $A = (A_{11}, A_{12}, \dots, A_{1t}; \dots; A_{m1}, A_{m2}, \dots, A_{mt})$ 是一个 $\text{GOA}(N, m, s, t)$. 令

$$B = (s^{t-1} \cdot A_{11} + s^{t-2} \cdot A_{12} + \dots + A_{1t}, \dots, s^{t-1} \cdot A_{m1} + s^{t-2} \cdot A_{m2} + \dots + A_{mt}).$$

则 B 是一个 $\text{SOA}(N, m, s^t, t)$. 反之, 若 B 是一个 $\text{SOA}(N, m, s^t, t)$, 将 B 中的每一行 $(b_1, b_2, \dots, b_m)$ 替换成 $(a_{11}, \dots, a_{1t}; \dots; a_{m1}, \dots, a_{mt})$, 则可得一个 $\text{GOA}(N, m, s, t)$, 其中 $a_{i1}, \dots, a_{it}$ 是 b_i 在 s 进制表示下的系数, 即 $b_i = a_{i1} \cdot s^{t-1} + a_{i2} \cdot s^{t-2} + \dots + a_{it}$ ($1 \leq i \leq m$).

对于 $\text{SOA}(N, m, s^3, 2^*)$ 中的每一行 $(x_1, x_2, \dots, x_m)$, 将每个分量 x_i 用 s 进制表示 $x_i = \alpha_i s^2 + \beta_i s + \gamma_i$ ($\alpha_i, \beta_i, \gamma_i \in \{0, 1, \dots, s-1\}$, $1 \leq i \leq m$), 可将此行向量写成 $(\alpha_1, \beta_1, \gamma_1; \alpha_2, \beta_2, \gamma_2; \dots; \alpha_m, \beta_m, \gamma_m)$. 则可得一个 $N \times (3m)$ 阵列 $M' = (a_1, b_1, c_1; \dots; a_m, b_m, c_m)$. 由于 $\text{SOA}(N, m, s^3, 2^*)$ 的任意两列组成的子阵列可以塌缩成一个 $\text{OA}(N, 2, s^2 \times s, 2)$ 和一个 $\text{OA}(N, 2, s \times s^2, 2)$, 所以对于任意 $i \neq j$, 每个 $N \times 3$ 子阵列 (a_i, b_i, a_j) 都是 $\text{OA}(N, 3, s, 3)$. 因此, 从一个 $\text{SOA}(N, m, s^3, 2^*)$ 可得一个 $\text{SOA}(N, m, s^2, 2+)$ $(s \cdot a_1 + b_1; \dots; s \cdot a_m + b_m)$. 反之, 利用 $\text{SOA}(N, m, s^t, t)$ 和 $\text{GOA}(N, m, s, t)$ 的等价性可得, 存在一个 $\text{SOA}(N, m, s^2, 2+)$ 当且仅当存在一个 $\text{GOA}(N, m, s, 2)$ $M = (a_1, b_1; a_2, b_2; \dots; a_m, b_m)$, 使对于任意 $i \neq j$, 每个 $N \times 3$ 子矩阵 (a_i, b_i, a_j) 都是 $\text{OA}(N, 3, s, 3)$. 令 $M' = (s^2 \cdot a_1 + s \cdot b_1 + a_2, s^2 \cdot a_2 + s \cdot b_2 + a_3, \dots, s^2 \cdot a_m + s \cdot b_m + a_1)$. 则 M' 是一个 $\text{SOA}(N, m, s^3, 2^*)$. 因此, 可得如下结论.

引理 2.2 存在一个 $\text{SOA}(N, m, s^3, 2^*)$ 当且仅当存在一个 $\text{SOA}(N, m, s^2, 2+)$.

因为 $\text{SOA}(N, m, s^2, 3-)$ 是一个 $\text{SOA}(N, m, s^2, 2+)$, 且满足任意 3 列可以塌缩成一个 $\text{OA}(N, 3, s, 3)$, 所以由 $\text{SOA}(N, m, s^t, t)$ 和 $\text{GOA}(N, m, s, t)$ 的等价性可得, 存在一个 $\text{SOA}(N, m, s^2, 3-)$ 当且仅当存在一个 $\text{GOA}(N, m, s, 2)$ $M = (a_1, b_1; \dots; a_m, b_m)$, 满足: 对于任意 $i \neq j$, 每个 $N \times 3$ 子阵列 (a_i, b_i, a_j) 都是 $\text{OA}(N, 3, s, 3)$, 且对于任意两两不同的 i, j 和 k , 每个 $N \times 3$ 子阵列 (a_i, a_j, a_k) 都是 $\text{OA}(N, 3, s, 3)$. 令 $\overline{M} = (a_1, b_1, a_2; a_2, b_2, a_3; \dots; a_{m-1}, b_{m-1}, a_m; a_m, b_m, a_1)$. 则 $\overline{M}$ 是一个 $\text{GOA}(N, m, s, 3)$. 反之, 若 $\overline{M} = (a_1, b_1, c_1; a_2, b_2, c_2; \dots; a_m, b_m, c_m)$ 是一个 $\text{GOA}(N, m, s, 3)$, 则 $(sa_1 + b_1, \dots, sa_m + b_m)$ 是一个 $\text{SOA}(N, m, s^2, 3-)$. 从而可得如下结论.

引理 2.3 存在一个 $\text{SOA}(N, m, s^2, 3-)$ 当且仅当存在一个 $\text{SOA}(N, m, s^3, 3)$.

定理 2.1^[6] 存在一个 $\text{SOA}(N, m, s^2, 2+)$ D 当且仅当存在两个 $N \times m$ 阵列 $A = (a_1, \dots, a_m)$ 和 $B = (b_1, \dots, b_m)$ 使得 $D = sA + B$, A 是一个 $\text{OA}(N, m, s, 2)$, B 是一个 $\text{OA}(N, m, s, 1)$ 且对于任意 $i \neq j$, 每个 (a_i, b_i, a_j) 都是 $\text{OA}(N, 3, s, 3)$.

注 2.1 对于任意 $i \neq j$, 由于每个 $N \times 3$ 子阵列 (a_i, b_i, a_j) 是 $\text{OA}(N, 3, s, 3)$, 所以阵列 A 必定是一个 $\text{OA}(N, m, s, 2)$, 且 B 是一个 $\text{OA}(N, m, s, 1)$. 因此, 可以省略定理中的两个条件: (i) A 是一个 $\text{OA}(N, m, s, 2)$; (ii) B 是一个 $\text{OA}(N, m, s, 1)$.

根据 $\text{SOA}(N, m, s^2, 3-)$ 与 $\text{GOA}(N, m, s, 2)$ 之间的联系, 可得如下类似于定理 2.1 的结论.

定理 2.2 存在一个 $\text{SOA}(N, m, s^2, 3-)$ D 当且仅当存在两个 $N \times m$ 阵列 $A = (a_1, \dots, a_m)$ 和

$B = (b_1, \dots, b_m)$ 使得 $D = sA + B$, A 是一个 $\text{OA}(N, m, s, 3)$ 且对于任意 $i \neq j$, 每个 (a_i, b_i, a_j) 都是 $\text{OA}(N, 3, s, 3)$.

一个阵列 D 称为是列正交的, 若中心化后阵列中任意两列的内积都为 0. 一个水平数为 s 的中心化是指将每个元素 $x = 0, 1, \dots, s-1$ 转化成 $x - \frac{s-1}{2}$, 用集合 $\Omega(s) = \{-(s-1)/2, -(s-3)/2, \dots, (s-3)/2, (s-1)/2\}$ 来标记. 一个列正交的 $\text{SOA}(N, m, s^2, 2+)$ 记为 $\text{OSOA}(N, m, s^2, 2+)$. 其他列正交的阵列用类似的方式来简记.

虽然 $\text{SOA}(N, m, s^3, 2^*)$ 的存在性等价于 $\text{SOA}(N, m, s^2, 2+)$ 的存在性, 但 $\text{OSOA}(N, m, s^3, 2^*)$ 的存在性和 $\text{OSOA}(N, m, s^2, 2+)$ 的存在性并不等价. 同样地, $\text{OSOA}(N, m, s^2, 3-)$ 的存在性和 $\text{OSOA}(N, m, s^3, 3)$ 的存在性也不等价.

下面列举由一对具有特殊性质的正交阵列来获得强度为 $2+$ 、 2^* 、 $3-$ 和 3 的列正交强正交阵列的构造方法.

定理 2.3 (参见文献 [13, 定理 1]) 若存在一对 $\text{OA}(N, m, s, 2)$, $A = (a_1, \dots, a_m)$ 和 $B = (b_1, \dots, b_m)$, 使对于任意 $i \neq j$, 每个 (a_i, a_j, b_j) 是 $\text{OA}(N, 3, s, 3)$, 则 $D = sA + B$ 是一个 $\text{OSOA}(N, m, s^2, 2+)$.

定理 2.4 (参见文献 [13, 定理 2]) 若 $A = (a_1, \dots, a_m)$ 是一个 $\text{OA}(N, m, s, 3)$ 且 $B = (b_1, \dots, b_m)$ 是一个 $\text{OA}(N, m, s, 2)$, 使对于任意 $i \neq j$, 每个 (a_i, a_j, b_j) 都是 $\text{OA}(N, 3, s, 3)$, 则 $D = sA + B$ 是一个 $\text{OSOA}(N, m, s^2, 3-)$.

Li 等^[10] 对 $\text{OSOA}(N, m, s^3, 2^*)$ 和 $\text{OSOA}(N, m, s^3, 3)$ 给出了一个递推构造, 构造过程如下:

步骤 1 设 $A = (a_1, \dots, a_m)$ 和 $B = (b_1, \dots, b_m)$ 是两个元素取自于集合 $\{0, 1, \dots, s-1\}$ 的 $N \times m$ 阵列.

步骤 2 设 $p = \lfloor m/2 \rfloor$, 对于 $j = 1, \dots, p$, 令 $C_j = (a_{2j-1}, b_{2j-1}, a_{2j}, b_{2j})$ 和 $C = (C_1, \dots, C_p)$.

步骤 3 对于 $j = 1, \dots, p$, 通过 $C_j^* = C_j - (s-1)/2$ 的方式将 s 元水平集 $\{0, 1, \dots, s-1\}$ 转化成 $\Omega(s) = \{-(s-1)/2, -(s-3)/2, \dots, (s-3)/2, (s-1)/2\}$. 令 $D^* = (D_1^*, \dots, D_p^*)$, 其中, $D_j^* = C_j^* V$ ($j = 1, \dots, p$) 和

$$V = \begin{pmatrix} s^2 & s & 1 & 0 \\ -1 & 0 & s^2 & s \end{pmatrix}^T,$$

这里上标符号 T 代表矩阵的转置.

步骤 4 通过

$$D = D^* + \frac{s^3 - 1}{2} \quad (2.1)$$

方式将 D^* 的水平集从 $\Omega(s^3)$ 变成 $\{0, 1, \dots, s^3 - 1\}$.

基于这个构造, Li 等获得如下 $\text{OSOA}(N, 2\lfloor m/2 \rfloor, s^3, 2^*)$ 和 $\text{OSOA}(N, 2\lfloor m/2 \rfloor, s^3, 3)$ 的构造.

定理 2.5 (参见文献 [10, 定理 2]) 若存在一对 $\text{OA}(N, m, s, 2)$, $A = (a_1, \dots, a_m)$ 和 $B = (b_1, \dots, b_m)$, 使得对于任意 $i \neq j$, 每个 (a_i, a_j, b_j) 都是 $\text{OA}(N, 3, s, 3)$, 则由 (2.1) 所得的阵列 D 是一个 $\text{OSOA}(N, 2\lfloor m/2 \rfloor, s^3, 2^*)$.

定理 2.6 (参见文献 [10, 定理 3]) 若 $A = (a_1, \dots, a_m)$ 是一个 $\text{OA}(N, m, s, 3)$ 且 $B = (b_1, \dots, b_m)$ 是一个 $\text{OA}(N, m, s, 2)$, 使得对于任意 $i \neq j$, 每个 (a_i, a_j, b_j) 都是 $\text{OA}(N, 3, s, 3)$, 则由 (2.1) 所得的阵列 D 是一个 $\text{OSOA}(N, 2\lfloor m/2 \rfloor, s^3, 3)$.

接下来两节利用差矩阵和线性码的生成矩阵来构造满足定理 2.3–2.6 中条件的一对正交阵列.

3 基于差矩阵的列正交强正交阵列构造

在构造强度为 2 的正交阵列中, 差矩阵起着重要作用, 参见文献 [2, 8]. 本节利用差矩阵构造出满足定理 2.3–2.6 中条件的一对正交阵列.

v 阶交换群 G 上的一个 (v, m, λ) -差矩阵 (difference matrix, DM) 是一个元素取自于 G 的 $(\lambda v) \times m$ 矩阵 $D = (d_{ij})$ ($1 \leq i \leq \lambda v, 1 \leq j \leq m$), 使得对于任意不同的两列 C_r 和 C_h , 向量差 $C_h - C_r$ 包含 G 中每个元素恰 λ 次. 显见, 若存在一个 (v, m, λ) -差矩阵, 则存在一个 $\text{OA}(\lambda v^2, m+1, v, 2)$ (参见文献 [2]).

定理 3.1 设 $D = (d_{ij})$ 是交换群 $G = \{g_1, g_2, \dots, g_v\}$ 上的一个 (v, m, λ) -DM. 则所有向量 $(d_{i1} + g_s, d_{i2} + g_s, \dots, d_{im} + g_s, g_{[i/\lambda]})$ ($1 \leq i \leq \lambda v, 1 \leq s \leq v$) 生成一个 $\text{OA}(\lambda v^2, m+1, v, 2)$.

显然, 一个差矩阵的任意一行或列加上 G 中的任意一元素所得到的矩阵还是一个差矩阵. 不失一般性, 可设第一列全为 0. 差矩阵已被深入研究, 在文献 [2] 中可以找到很多关于 $(v, m, 1)$ -DM 的存在性结果. 特别地, q 阶有限域的乘法表是一个 $(q, q, 1)$ -DM. 参数为 $(v, \lambda v, \lambda)$ 的差矩阵称为广义 Hadamard 矩阵.

定理 3.2 设 v 是一个奇数, 若在 v 阶交换群 G 上存在一个 (v, m, λ) -DM, 则存在一个 $\text{OSOA}(\lambda v^3, 2m, v^2, 2+)$ 和一个 $\text{OSOA}(\lambda v^3, 2m, v^3, 2*)$.

证明 设 $D = (d_{i,j})$ 是交换群 G 上的一个 (v, m, λ) -DM, 其第一列元素全为 0. 对于 $1 \leq i \leq \lambda v$ 和 $g, e \in G$, 定义如下两个向量:

$$\begin{aligned} A(i, g, e) &= (2g + e, d_{i,2}, d_{i,2} + g, \dots, d_{i,m} + g, d_{i,2} + e, \dots, d_{i,m} + e), \\ B(i, g, e) &= (e, g + e, d_{i,2} + g + e, \dots, d_{i,m} + g + e, d_{i,2} + 2g + e, \dots, d_{i,m} + 2g + e). \end{aligned}$$

设 A 和 B 分别是由全部向量 $A(i, g, e)$ 和 $B(i, g, e)$ ($1 \leq i \leq \lambda v, g, e \in G$) 按相同次序排成的两个 $(\lambda v^3) \times (2m)$ 阵列. 下面验证 A 和 B 满足定理 2.3 和 2.5 中的条件.

如注 2.1 中所指出的, 我们只需要证明对于任意 $j \neq \ell$, A 中第 j 和 ℓ 列以及 B 中第 j 列组成的子阵列是一个强度为 3 的正交阵列且 B 是一个强度为 2 的正交阵列.

由于 D 是一个 (v, m, λ) -DM, 所以由所有 $B(i, g, 0)$ 组成的矩阵是一个 $(v, 2m, \lambda v)$ -DM. 由定理 3.1 可知, B 是一个 $\text{OA}(\lambda v^3, 2m, v, 2)$.

对于任意 $j \neq \ell$, 计算任意三元组 (x, y, z) 在 A 中第 j 和 ℓ 列以及 B 中第 j 列组成的子阵列 (a_ℓ, a_j, b_j) 出现的次数. 下面根据 j 的取值分情形讨论.

情形 1 $j = 1$.

由 v 是奇数知, 存在唯一的元素 g 和 e 使得 $2g + e = y$ 和 $e = z$. 若 $\ell = 2$, 则由 D 是一个 (v, m, λ) -DM 知, 多重集 $\{d_{i,2}: 1 \leq i \leq \lambda v\}$ 包含 G 中每一个元素恰 λ 次, 从而恰存在 λ 个 i 使得 $d_{i,2} = x$. 若 $3 \leq \ell \leq m+1$, 则由 D 是一个 (v, m, λ) -DM 知, 恰存在 λ 个 i 使得 $d_{i,\ell-1} + g = x$. 若 $\ell > m+1$, 则由 D 是一个 (v, m, λ) -DM 知, 恰存在 λ 个 i 使得 $d_{i,\ell-m} + e = x$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 因此, 这个子阵列是一个强度为 3 的正交阵列.

情形 2 $j = 2$.

由差矩阵定义知, 恰存在 λ 个 i 使得 $d_{i,2} = y$. 若 $\ell = 1$, 则存在唯一的元素 g 和 e 满足 $2g + e = x$ 和 $g + e = z$. 对于每个固定的 i , 若 $3 \leq \ell \leq m+1$, 则存在唯一元素 g 满足 $d_{i,\ell-1} + g = x$, 从而存在唯一元素 e 满足 $g + e = z$. 若 $\ell > m+1$, 则存在唯一元素 e 满足 $d_{i,\ell-m} + e = x$, 从而存在唯一元素 g

满足 $g + e = z$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 因此, 这个子阵列是一个强度为 3 的正交阵列.

情形 3 $3 \leq j \leq m+1$.

存在唯一元素 e 满足 $e = z - y$. 若 $\ell = 1$, 则存在唯一元素 g 满足 $2g + e = x$. 由差矩阵定义知, 恰存在 λ 个 i 使得 $d_{i,j-1} + g = y$, 故三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 若 $\ell = 2$, 则由差矩阵定义知, 恰存在 λ 个 i 使得 $d_{i,2} = x$. 对于每一个 i , 存在唯一元素 g 使得 $d_{i,j-1} + g = y$, 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 若 $3 \leq \ell \leq m+1$, 则由 D 是一个 (v, m, λ) -DM 知, 多重集 $\{d_{i,\ell-1} - d_{i,j-1} : 1 \leq i \leq \lambda v\}$ 包含 G 中每一个元素恰 λ 次, 于是恰存在 λ 个 i 使得 $d_{i,\ell-1} - d_{i,j-1} = x - y$. 对于每个 i , 存在唯一元素 g 使得 $d_{i,j-1} + g = y$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 若 $\ell > m+1$, 则恰存在 λ 个 i 使得 $d_{i,\ell-m} + e = x$, 于是对于每个固定的 i , 存在唯一的 g 使得 $d_{i,j-1} + g = y$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 因此, 这个子阵列是一个强度为 3 的正交阵列.

情形 4 $j > m+1$.

由于 v 是奇数, 所以存在唯一元素 g 满足 $2g = z - y$. 若 $\ell = 1$, 则存在唯一元素 e 满足 $2g + e = x$. 再由差矩阵定义知, 恰存在 λ 个 i 使得 $d_{i,j-m} + e = y$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 若 $\ell = 2$, 则恰存在 λ 个 i 使得 $d_{i,2} = x$. 对于每个 i , 存在唯一元素 e 使得 $d_{i,j-m} + e = y$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 若 $3 \leq \ell \leq m+1$, 则恰存在 λ 个 i 使得 $d_{i,\ell-1} + g = x$. 对于每个 i , 存在唯一元素 e 使得 $d_{i,j-m} + e = y$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 若 $m+2 \leq \ell \leq 2m$, 则由多重集 $\{d_{i,\ell-m} - d_{i,j-m} : 1 \leq i \leq \lambda v\}$ 包含 G 中每一个元素恰 λ 次知, 恰存在 λ 个 i 使得 $d_{i,\ell-m} - d_{i,j-m} = x - y$. 对于每个 i , 存在唯一元素 e 使得 $d_{i,j-m} + e = y$. 由此可得三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λ 次. 因此, 这个子阵列是一个强度为 3 的正交阵列.

综上所述, A 和 B 满足定理 2.3 和 2.5 中的条件. 从而结论成立. $\square$

定理 3.3 若在 v 阶交换环 R 上存在一个 (v, m, λ) -DM 且 R 有单位 α 满足 $\alpha - 1$ 也是单位, 则存在一个 $\text{OSOA}(\lambda v^3, 2m, v^2, 2+)$ 和一个 $\text{OSOA}(\lambda v^3, 2m, v^3, 2*)$.

证明 设 $D = (d_{i,j})$ 是环 R 上的一个 (v, m, λ) -DM 且第一列元素全为 0. 对于 $1 \leq i \leq \lambda v$ 和 $g, e \in R$, 定义如下两个向量:

$$A(i, g, e) = (\alpha g + e, d_{i,2}, d_{i,2} + g, \dots, d_{i,m} + g, d_{i,2} + e, \dots, d_{i,m} + e),$$

$$B(i, g, e) = (e, g + e, d_{i,2} + g + e, \dots, d_{i,m} + g + e, d_{i,2} + \alpha g + e, \dots, d_{i,m} + \alpha g + e).$$

设 A 和 B 是分别由全部向量 $A(i, g, e)$ 和 $B(i, g, e)$ ($1 \leq i \leq \lambda v, g, e \in R$) 按相同次序排成的两个 $(\lambda v^3) \times (2m)$ 阵列. 类似于定理 3.2 的证明可证明得到 A 和 B 满足定理 2.3 和 2.5 中的条件. 因此, 结论成立. $\square$

由文献 [3, 表 5.10] 知, 对于任意的素数 $p, \lambda \in \{1, 2, 4\}$ 和非负整数 ℓ , 在 p^n 阶初等交换群 G 上存在一个 $(p^n, \lambda p^{n+\ell}, \lambda p^\ell)$ -DM. 当使用 p^n 阶有限域时, 它有 $p^n - 1$ 个单位, 应用定理 3.2 可得下面结论.

推论 3.1 对于任意奇素数 $p, \lambda \in \{1, 2, 4\}$ 、正整数 n 和非负整数 ℓ , 存在一个 $\text{OSOA}(\lambda p^{3n+\ell}, 2\lambda p^{n+\ell}, p^{2n}, 2+)$ 和一个 $\text{OSOA}(\lambda p^{3n+\ell}, 2\lambda p^{n+\ell}, p^{3n}, 2*)$.

注 3.1 当 q 为奇素数幂时, 推论 3.1 中获得的 $\text{OSOA}(\lambda q^k, 2\lambda q^{k-2}, q^2, 2+)$ 与 $\text{OSOA}(\lambda q^k, 2\lambda q^{k-2}, q^3, 2*)$ 分别比文献 [13, 命题 2] 和 [13, 定理 4] 中的 $\text{OSOA}(q^k, \frac{q^{k-1}-1}{q-1}, q^2, 2+)$ 和 $\text{OSOA}(2q^k, \frac{2(q^{k-1}-1)}{q-1})$

$-1, q^2, 2+)$ 与文献 [10, 定理 5] 和 [10, 应用 3] 中的 $\text{OSOA}(q^k, 2\lfloor \frac{q^{k-1}-1}{2(q-1)} \rfloor, q^3, 2*)$ 和 $\text{OSOA}(2q^k, \frac{2(q^{k-1}-1)}{q-1} - 2, q^3, 2*)$ 有更多的因子数.

定理 3.4 若在 v 阶交换环 R 上存在一个 (v, m, λ) -DM 且 R 有 t 个单位 $\alpha_1, \dots, \alpha_t$ 满足 $\alpha_i - \alpha_j$ ($i \neq j$) 也是单位, 则存在一个 $\text{OSOA}(\lambda v^4, (3t-2)m, v^2, 2+)$ 和一个 $\text{OSOA}(\lambda v^4, 2\lfloor (3t-2)m/2 \rfloor, v^3, 2*)$.

证明 设 $D = (d_{i,j})$ 是环 R 上一个 (v, m, λ) -DM. 对于 $1 \leq i \leq \lambda v$, $2 \leq s \leq t$ 和 $e_0, e_1, e_2 \in R$, 定义如下行向量:

$$\begin{aligned} \mathbf{a}_0(i, e_0, e_1, e_2) &= (d_{i,1} + \alpha_1 e_0 + \alpha_1 e_1, \dots, d_{i,m} + \alpha_1 e_0 + \alpha_1 e_1), \\ \mathbf{b}_0(i, e_0, e_1, e_2) &= (d_{i,1} + \alpha_1 e_0 + \alpha_1 e_1 + \alpha_1 e_2, \dots, d_{i,m} + \alpha_1 e_0 + \alpha_1 e_1 + \alpha_1 e_2), \\ \mathbf{a}_{r,s}(i, e_0, e_1, e_2) &= (d_{i,1} + \alpha_1 e_r + \alpha_s e_{r+1}, \dots, d_{i,m} + \alpha_1 e_r + \alpha_s e_{r+1}), \\ \mathbf{b}_{r,s}(i, e_0, e_1, e_2) &= (d_{i,1} + \alpha_1 e_r + \alpha_s e_{r+1} + \alpha_1 e_{r+2}, \dots, d_{i,m} + \alpha_1 e_r + \alpha_s e_{r+1} + \alpha_1 e_{r+2}), \end{aligned}$$

其中 $0 \leq r \leq 2$ 且 e_i 下标的加法按模 3 进行运算. 令

$$\begin{aligned} \mathbf{a}_1(i, e_0, e_1, e_2) &= (\mathbf{a}_{0,2}(i, e_0, e_1, e_2), \dots, \mathbf{a}_{0,t}(i, e_0, e_1, e_2), \dots, \mathbf{a}_{2,2}(i, e_0, e_1, e_2), \dots, \mathbf{a}_{2,t}(i, e_0, e_1, e_2)), \\ \mathbf{b}_1(i, e_0, e_1, e_2) &= (\mathbf{b}_{0,2}(i, e_0, e_1, e_2), \dots, \mathbf{b}_{0,t}(i, e_0, e_1, e_2), \dots, \mathbf{b}_{2,2}(i, e_0, e_1, e_2), \dots, \mathbf{b}_{2,t}(i, e_0, e_1, e_2)), \\ \mathbf{a}(i, e_0, e_1, e_2) &= (\mathbf{a}_0(i, e_0, e_1, e_2), \mathbf{a}_1(i, e_0, e_1, e_2)), \\ \mathbf{b}(i, e_0, e_1, e_2) &= (\mathbf{b}_0(i, e_0, e_1, e_2), \mathbf{b}_1(i, e_0, e_1, e_2)). \end{aligned}$$

设 A 和 B 分别是由全部向量 $\mathbf{a}(i, e_0, e_1, e_2)$ 和 $\mathbf{b}(i, e_0, e_1, e_2)$ ($1 \leq i \leq \lambda v$, $e_0, e_1, e_2 \in R$) 按相同次序排成的两个 $(\lambda v^4) \times (3tm - 2m)$ 阵列. 下面证明 A 和 B 满足定理 2.3 和 2.5 中的条件.

如注 2.1 中所指出的, 只需要证明对于任意 $j \neq \ell$, A 中第 j 和 ℓ 列以及 B 中第 j 列组成的子阵列是一个强度为 3 的正交阵列且 B 是一个强度为 2 的正交阵列.

对于任意 $j \neq \ell$, 计算任意三元组 (x, y, z) 在 A 中第 j 和 ℓ 列以及 B 中第 j 列组成的子阵列 (a_ℓ, a_j, b_j) 出现的次数. 下面根据 j 的取值分情形讨论.

情形 1 $1 \leq j \leq tm$. 由 α_1 是环 R 上的单位可得, 存在唯一的元素 e_2 满足 $e_2 = \alpha_1^{-1}(z - y)$. 对于这种情形, 下面分成 4 种情形来验证.

(1) 若 $cm < j, \ell \leq (c+1)m$, 其中 $t > c \geq 0$, 则由 D 是一个 (v, m, λ) -DM 可知, 多重集 $\{d_{i,j-cm} - d_{i,\ell-cm} : 1 \leq i \leq \lambda v\}$ 包含 R 中每一个元素恰 λ 次. 于是恰存在 λ 个 i 使得 $d_{i,j-cm} - d_{i,\ell-cm} = y - x$. 对于每个 i , 恰存在 v 对元素 (e_0, e_1) 使得

$$d_{i,j-cm} + \alpha_1 e_0 + \alpha_{c+1} e_1 = y.$$

(2) 若 $cm < j \leq (c+1)m$ 且 $c'm < \ell \leq (c'+1)m$, 其中 $t > c'$, $c \geq 0$ 且 $c' \neq c$, 则对于每个 i ($1 \leq i \leq \lambda v$), 因为 $\alpha_1, \alpha_{c+1} - \alpha_{c'+1}$ ($c \neq c'$) 都是环 R 上的单位, 所以根据 Cramer 法则可知, 线性方程组

$$\begin{cases} d_{i,j-cm} + \alpha_1 e_0 + \alpha_{c+1} e_1 = y, \\ d_{i,\ell-c'm} + \alpha_1 e_0 + \alpha_{c'+1} e_1 = x \end{cases}$$

存在唯一解

$$\begin{cases} e_0 = (\alpha_{c'+1}\alpha_1 - \alpha_{c+1}\alpha_1)^{-1}(\alpha_{c'+1}y + \alpha_{c+1}d_{i,\ell-c'm} - \alpha_{c+1}x - \alpha_{c'+1}d_{i,j-cm}), \\ e_1 = (\alpha_{c+1} - \alpha_{c'+1})^{-1}(y + d_{i,\ell-c'm} - x - d_{i,j-cm}). \end{cases}$$

(3) 若 $cm < j \leq (c+1)m \leq c'm < \ell \leq (c'+1)m$, 其中 $2t-1 > c' \geq t > c \geq 0$, 则对于每个 i ($1 \leq i \leq \lambda v$), 因为 α_1 和 α_c 都是环 R 上的单位且 $e_2 = \alpha_1^{-1}(z-y)$, 所以根据 Cramer 法则可知, 线性方程组

$$\begin{cases} d_{i,j-cm} + \alpha_1 e_0 + \alpha_{c+1} e_1 = y, \\ d_{i,\ell-c'm} + \alpha_1 e_1 + \alpha_{c'-t+2} e_2 = x \end{cases}$$

存在唯一解

$$\begin{cases} e_1 = \alpha_1^{-1}(x - d_{i,\ell-c'm} - \alpha_{c'-t+2} e_2), \\ e_0 = \alpha_1^{-1}(y - d_{i,j-cm} - \alpha_{c+1} e_1). \end{cases}$$

(4) 若 $cm < j \leq (c+1)m \leq c'm < \ell \leq (c'+1)m$, 其中 $3t-2 > c' \geq 2t-1, t > c \geq 0$, 则类似情形 1(3) 的证明也可得结论成立.

由此可知三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λv 次. 因此, 这个子阵列是一个强度为 3 的正交阵列.

情形 2 $tm < j \leq (2t-1)m$. 由 α_1 是环 R 上的单位可得, 存在唯一的元素 e_0 满足 $e_0 = \alpha_1^{-1}(z-y)$. 对于这种情形, 下面也分成 4 种情形来验证.

(1) 若 $c'm < \ell \leq (c'+1)m \leq cm < j \leq (c+1)m$, 其中 $2t-1 > c \geq t > c' \geq 0$, 则此情形可以通过类似上面情形 1(3) 的证明得到.

(2) 若 $cm \leq j, \ell < (c+1)m$, 其中 $2t-1 > c \geq t$, 则此情形可以通过类似上面情形 1(1) 的证明得到.

(3) 若 $cm < j \leq (c+1)m$ 且 $c'm < \ell \leq (c'+1)m$, 其中 $2t-1 > c, c' \geq t$ 且 $c' \neq c$, 则此情形可以通过类似上面情形 1(2) 的证明得到.

(4) 若 $cm < j \leq (c+1)m \leq c'm < \ell \leq (c'+1)m$, 其中 $3t-2 > c' \geq 2t-1 > c \geq t$, 则此情形可以通过类似上面情形 1(3) 的证明得到.

由此可知三元组 (x, y, z) 在子阵列 (a_ℓ, a_j, b_j) 中恰出现 λv 次. 因此, 这个子阵列是一个强度为 3 的正交阵列.

情形 3 $(2t-1)m < j \leq (3t-2)m$. 此情形可以通过类似上面情形 1 和 2 的证明得到.

接下来验证 B 是一个强度为 2 的正交阵列. 对于任意 $j \neq \ell$, 计算任意二元组 (x, y) 在 B 的第 j 和 ℓ 列组成的子阵列 (b_ℓ, b_j) 中出现的次数. 下面将根据 j 的取值分情形讨论.

情形 1 $1 \leq j \leq tm$. 对于这种情形, 下面分成 4 种情形来验证.

(1) 若 $cm < j, \ell \leq (c+1)m$, 其中 $t > c \geq 0$, 则由 D 是一个 (v, m, λ) -DM 可知, 多重集 $\{d_{i,j-cm} - d_{i,\ell-cm} : 1 \leq i \leq \lambda v\}$ 包含 R 中每一个元素恰 λ 次. 于是恰存在 λ 个 i 使得 $d_{i,j-cm} - d_{i,\ell-cm} = y - x$. 对于每个 i , 由 α_1 是环 R 上的单位可知, 恰存在 v^2 组 (e_0, e_1, e_2) 使得 $d_{i,j-cm} + \alpha_1 e_0 + \alpha_{c+1} e_1 + \alpha_1 e_2 = y$ (任意取定 e_1 和 e_2 , 方程都有唯一解 e_0).

(2) 若 $cm < j \leq (c+1)m$ 且 $c'm < \ell \leq (c'+1)m$, 其中 $t > c', c \geq 0$ 和 $c' \neq c$, 则对于每个 i ($1 \leq i \leq \lambda v$), 因为 α_1 和 $\alpha_{c+1} - \alpha_{c'+1}$ ($c \neq c'$) 都是环 R 上的单位, 所以由环上线性方程组理论可得非齐次线性方程组

$$\begin{cases} d_{i,j-cm} + \alpha_1 e_0 + \alpha_{c+1} e_1 + \alpha_1 e_2 = y, \\ d_{i,\ell-c'm} + \alpha_1 e_0 + \alpha_{c'+1} e_1 + \alpha_1 e_2 = x \end{cases}$$

恰有 v 组解 (e_0, e_1, e_2) (任意取定 e_2 , 方程都有唯一解 (e_0, e_1)).

(3) 若 $cm < j \leq (c+1)m \leq c'm < \ell \leq (c'+1)m$, 其中 $2t-1 > c' \geq t > c \geq 0$, 则由 $c'-t+2 \geq 2$ 可知, $\alpha_{c'-t+2} \neq \alpha_1$. 又因为 α_1 和 $\alpha_{c'-t+2} - \alpha_1$ 都是环 R 上的单位, 所以对于每个 i ($1 \leq i \leq \lambda v$), 由环上线性方程组理论可得非齐次线性方程组

$$\begin{cases} d_{i,j-cm} + \alpha_1 e_0 + \alpha_{c+1} e_1 + \alpha_1 e_2 = y, \\ d_{i,\ell-c'm} + \alpha_1 e_1 + \alpha_{c'-t+2} e_2 + \alpha_1 e_0 = x \end{cases}$$

恰存在 v 组解 (e_0, e_1, e_2) (任意取定 e_1 , 方程都有唯一解 (e_0, e_2)).

(4) 若 $cm < j \leq (c+1)m \leq c'm < \ell \leq (c'+1)m$, 其中 $3t-2 > c' \geq 2t-1$, $t > c \geq 0$, 则此情形可以通过类似上面情形 1(3) 的证明得到.

由此可知二元组 (x, y) 在子阵列 (b_ℓ, b_j) 中恰出现 λv^2 次. 因此, 这个子阵列是一个强度为 2 的正交阵列.

情形 2 $tm < j \leq (2t-1)m$ 或 $(2t-1)m < j \leq (3t-2)m$. 类似于前面的情形 1 的证明过程可得结论成立. 由此可知二元组 (x, y) 在子阵列 (b_ℓ, b_j) 中恰出现 λv^2 次. 因此, 这个子阵列是一个强度为 2 的正交阵列.

因此, A 和 B 满足定理 2.3 和 2.5 中的条件. 从而结论成立. $\square$

推论 3.2 对于任意的素数 p 、 $\lambda \in \{1, 2, 4\}$ 、正整数 n 和非负整数 ℓ , 存在一个 $\text{OSOA}(\lambda p^{4n+\ell}, \lambda(3p^n - 5)p^{n+\ell}, p^{2n}, 2+)$ 和一个 $\text{OSOA}(\lambda p^{4n+\ell}, 2\lfloor \frac{\lambda(3p^n - 5)p^{n+\ell}}{2} \rfloor, p^{3n}, 2*)$.

注 3.2 当素数幂 $q \geq 4$ 且 $k \geq 4$ 时, 推论 3.2 中获得的 $\text{OSOA}(\lambda q^k, \lambda(3q - 5)q^{k-3}, q^2, 2+)$ 与 $\text{OSOA}(\lambda q^k, 2\lfloor \frac{\lambda(3q-5)q^{k-3}}{2} \rfloor, q^3, 2*)$ 分别比文献 [13, 命题 2] 和 [13, 定理 4] 中的 $\text{OSOA}(q^k, \frac{q^{k-1}-1}{q-1}, q^2, 2+)$ 和 $\text{OSOA}(2q^k, \frac{2(q^{k-1}-1)}{q-1} - 1, q^2, 2+)$ 与文献 [10, 定理 5] 和 [10, 应用 3] 中的 $\text{OSOA}(q^k, 2\lfloor \frac{q^{k-1}-1}{2(q-1)} \rfloor, q^3, 2*)$ 和 $\text{OSOA}(2q^k, \frac{2(q^{k-1}-1)}{q-1} - 2, q^3, 2*)$ 有更多的因子数.

4 基于生成矩阵的列正交强正交阵列构造

将一个正交阵列 $\text{OA}(N, m, s, t)$ 的所有行取出, 则可获得一个码长为 m 、码字数为 N 、Hamming 距离为某正整数 d 的 s 元码, 记为 $(m, N, d)_s$ 码. 有关码的基本概念可参见文献 [8].

一个 q 阶有限域 $GF(q)$ 上的码长为 m 、维数为 ℓ 的线性码可以由 ℓ 个线性无关的行向量生成, 由这 ℓ 个线性无关的行向量构成的 $\ell \times m$ 矩阵称为这个线性码的一个生成矩阵. 如果一个正交阵列对应的码是线性码, 则称此阵列为线性的, 即该正交阵列全体行是一组行向量的全部线性组合.

定理 4.1 (参见文献 [8, 定理 3.27, 3.29]) 设 ℓ 和 m 是两个正整数, q 是一个素数幂. 设 M 是一个元素取自于 $GF(q)$ 上的秩为 ℓ 的 $\ell \times m$ 矩阵, 使得任意 t 列线性无关. 令 D 是一个 $q^\ell \times m$ 矩阵, 它的行由 M 的行向量的全部线性组合构成. 则 D 是一个线性的 $\text{OA}(q^\ell, m, q, t)$. 反之, 若 D 是一个线性的 $\text{OA}(q^\ell, m, q, t)$, 则这正交阵列关联的线性码的生成矩阵 G 满足任意 t 列线性无关.

定理 4.2 如果存在一个线性的 $\text{OA}(N, m, q, 3)$, 那么存在一个 $\text{OSOA}(N, m-1, q^2, 3-)$ 和一个 $\text{OSOA}(N, 2\lfloor \frac{m-1}{2} \rfloor, q^3, 3)$.

证明 设 G 是线性的 $\text{OA}(N, m, q, 3)$ 的生成矩阵, 则由定理 4.1 可知 G 中任意三列线性无关. 设 G_i 是 G 当中的第 i 列. 令 $A = (G_1, G_2, \dots, G_{m-1})$ 和 $B = (G_1 + G_m, G_2 + G_m, \dots, G_{m-1} + G_m)$. 显然, A 中任意三列线性无关且 B 中任意两列线性无关. 进一步, 对于任意 $i \neq j$, G_i 、 G_j 和 $G_i + G_m$

都线性无关. 故根据定理 4.1, 以 A 和 B 为生成矩阵分别获得线性的 $\text{OA}(N, m-1, q, 3)$ 和线性的 $\text{OA}(N, m-1, q, 2)$, 且满足定理 2.4 和 2.6 中条件. 因此, 存在一个 $\text{OSOA}(N, m-1, q^2, 3-)$ 和一个 $\text{OSOA}(N, 2\lfloor \frac{m-1}{2} \rfloor, q^3, 3)$. $\square$

Zhou 和 Tang^[13] 获得的一个 $\text{OSOA}(2^{k+1}, 2^k-1, 4, 3-)$ 和一个 $\text{OSOA}(2^{k+1}, 2^k-2, 8, 3)$ 也可利用线性的 $\text{OA}(2^{k+1}, 2^k, 8, 3)$ (参见文献 [8, 表 12.6(a)]) 和定理 4.2 得到. 因为对于任意素数幂 q 都存在一个线性的 $\text{OA}(q^3, q+1, q, 3)$, 也存在一个线性的 $\text{OA}(2^{3k}, 2^k+2, 2^k, 3)$ ^[8], 所以由定理 4.2 可得下述结论.

推论 4.1 对于任意素数幂 q , 存在一个 $\text{OSOA}(q^3, q, q^2, 3-)$ 和一个 $\text{OSOA}(q^3, 2\lfloor \frac{q}{2} \rfloor, q^3, 3)$. 进一步, 若 $q = 2^k$, 则存在一个 $\text{OSOA}(q^3, q+1, q^2, 3-)$ 和一个 $\text{OSOA}(q^3, q, q^3, 3)$.

通过直接构造一对线性正交阵列的生成矩阵, 上述推论可进一步改进如下.

定理 4.3 对于任意奇素数幂 q , 存在一个 $\text{OSOA}(q^3, q+1, q^2, 3-)$ 和一个 $\text{OSOA}(q^3, q+1, q^3, 3)$.

证明 设 $GF(q) = \{0, \alpha^0, \alpha^1, \dots, \alpha^{q-2}\}$, 其中 α 是本原元. 令

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} & 0 \\ 0 & \alpha^0 & \alpha^2 & \cdots & \alpha^{2q-4} & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 2\alpha^0 & 2\alpha^1 & \cdots & 2\alpha^{q-2} & 0 \end{pmatrix}.$$

易验证矩阵 A 的任意三列线性无关, 矩阵 B 的任意两列线性无关, 且对于 $1 \leq i, j \leq q+1, i \neq j$, 矩阵 A 的第 i 和 j 列与 B 的第 i 列构成的向量组线性无关. 故以 A 和 B 为生成矩阵获得的线性 $\text{OA}(q^3, q+1, q, 3)$ 和线性 $\text{OA}(q^3, q+1, q, 2)$ 满足定理 2.4 和 2.6 的条件. 因此, 结论成立. $\square$

在射影几何 (projective geometry, PG) $\text{PG}(3, q)$ 中大小为 q^2+1 的点集称为一个卵形, 如果任意三点不共线. 例如, 一个卵形可通过选取满足方程 $xy + z^2 + azw + w^2 = 0$ 的点 $(w, x, y, z) \in GF(q)^4$ 获得, 其中 $a \in GF(q)$ 使方程 $z^2 + az + 1 = 0$ 在有限域 $GF(q)$ 上没有根^[4]. 例如, Hedayat 等^[8] 指出, 用这些向量 $(w, x, y, z)^T$ 作为一个生成矩阵的列向量可得到一个线性的 $\text{OA}(q^4, q^2+1, q, 3)$. 由定理 4.2 可获得一个 $\text{OSOA}(q^4, q^2, q^2, 3-)$ 和一个 $\text{OSOA}(q^4, 2\lfloor \frac{q^2}{2} \rfloor, q^3, 3)$. 通过直接构造一对线性正交阵列的生成矩阵, 上述结论可进一步改进如下.

定理 4.4 对于任意素数幂 q , 存在一个 $\text{OSOA}(q^4, q^2+1, q^2, 3-)$ 和一个 $\text{OSOA}(q^4, 2\lfloor \frac{q^2+1}{2} \rfloor, q^3, 3)$.

证明 设 $GF(q) = \{0, \alpha^0, \alpha^1, \dots, \alpha^{q-2}\}$, 其中 α 是本原元. 选取 $a \in GF(q)$, 使方程 $z^2 + az + 1 = 0$ 在 $GF(q)$ 中没有根. 线性 $\text{OA}(q^4, q^2+1, q, 3)$ 的生成矩阵 A 由文献 [4] 中所构造的一个卵形获得. 该 $4 \times (q^2+1)$ 的矩阵 A 的列就是 $\text{PG}(3, q)$ 中满足方程 $xy + z^2 + azw + w^2 = 0$ 的 q^2+1 点 $(w, x, y, z)^T$, 即 $A = (A_0, A_{1,0}, A_{1,\alpha^0}, \dots, A_{1,\alpha^{q-2}})$, 其中

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & -\alpha^0 & -\alpha^2 & \cdots & -\alpha^{2q-4} \\ 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} \end{pmatrix}, \quad A_{1,z} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ -\alpha^0 & -\alpha^1 & \cdots & -\alpha^{q-2} \\ \frac{z^2+az+1}{\alpha^0} & \frac{z^2+az+1}{\alpha^1} & \cdots & \frac{z^2+az+1}{\alpha^{q-2}} \\ z & z & \cdots & z \end{pmatrix}, \quad z \in GF(q).$$

按 q 的奇偶性分别构造线性 $\text{OA}(q^4, q^2+1, q, 2)$ 的生成矩阵, 使其满足要求.

情形 1 q 为偶数.

构造如下的生成矩阵 $B = (B_0, B_{1,0}, B_{1,\alpha^0}, \dots, B_{1,\alpha^{q-2}})$:

$$B_0 = \begin{pmatrix} 0 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & a\alpha^0 & a\alpha^1 & \cdots & a\alpha^{q-2} \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad B_{1,z} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha \cdot \alpha^0 & \alpha \cdot \alpha^1 & \cdots & \alpha \cdot \alpha^{q-2} \\ \alpha \cdot \frac{z^2+az+1}{\alpha^0} & \alpha \cdot \frac{z^2+az+1}{\alpha^1} & \cdots & \alpha \cdot \frac{z^2+az+1}{\alpha^{q-2}} \\ z & z & \cdots & z \end{pmatrix}, \quad z \in GF(q).$$

易验证矩阵 B 的任意两列线性无关. 对于 $1 \leq i, j \leq q^2 + 1, i \neq j$, 下面验证矩阵 A 的第 i 和 j 列与 B 的第 i 列构成的向量组线性无关. 设矩阵 A 的第 i 和 j 列及 B 的第 i 列分别为 a_i, a_j 和 b_i . 下面根据 i 的取值分情形讨论.

- (1) 当 $i = 1$ 时, 由矩阵 A 中除第 1 列外其他所有列的第三分量都非零知, a_i, a_j 和 b_i 线性无关.
- (2) 当 $i = 2$ 时, 由矩阵 A 中除第 2 列外其他所有列的第二分量都非零知, a_i, a_j 和 b_i 线性无关.
- (3) 当 $3 \leq i \leq q + 1$ 时, 分成两种情形来验证.
 - (i) 若 $1 \leq j \leq q + 1$, 则由 a_i 和 a_j 第一分量为 0 且 b_i 的第一分量为 1 可知 $\text{rank}(a_i, a_j, b_i) = 1 + \text{rank}(a_i, a_j) = 3$.
 - (ii) 当 $2 + c(q - 1) < j \leq 2 + (c + 1)(q - 1)$ 且 $1 \leq c \leq q$ 时, 使用反证法证明

$$(a_i, b_i, a_j) = \begin{pmatrix} 0 & 1 & 1 \\ \alpha^{2i-6} & a\alpha^{i-3} & \alpha^{j-c(q-1)-3} \\ 1 & 0 & \frac{z_c^2+az_c+1}{\alpha^{j-c(q-1)-3}} \\ \alpha^{i-3} & 0 & z_c \end{pmatrix}$$

的秩等于 3, 其中当 $c = 1$ 时, $z_c = 0$; 当 $q \geq c \geq 2$ 时, $z_c = \alpha^{c-2}$. 假设这 3 个向量线性相关, 则存在 $x \in GF(q)$ 使得 $xa_i + b_i = a_j$. 从而可得

$$a\alpha^{i-3} + x\alpha^{2i-6} = \alpha^{j-c(q-1)-3}, \quad x\alpha^{i-3} = z_c, \quad x = \frac{z_c^2 + az_c + 1}{\alpha^{j-c(q-1)-3}}.$$

由前两个等式可得

$$\begin{aligned} x\alpha^{j-c(q-1)-3} &= x(a\alpha^{i-3} + x\alpha^{2i-6}) = ax\alpha^{i-3} + x^2\alpha^{2i-6}, \\ z_c^2 + az_c + 1 &= x^2\alpha^{2i-6} + ax\alpha^{i-3} + 1 = x\alpha^{j-c(q-1)-3} + 1. \end{aligned}$$

这与第三个等式 $x\alpha^{j-c(q-1)-3} = z_c^2 + az_c + 1$ 矛盾. 因此, a_i, a_j 和 b_i 线性无关.

- (4) 当 $2 + c'(q - 1) < i \leq 2 + (c' + 1)(q - 1)$ 且 $1 \leq c' \leq q$ 时, 分成两种情形来验证.

- (i) 当 $1 \leq j \leq q + 1$ 时, 令 $a_j = (0, x, y, z)^T$, 则矩阵

$$(a_i, b_i, a_j) = \begin{pmatrix} 1 & 1 & 0 \\ \alpha^{i-c'(q-1)-3} & \alpha \cdot \alpha^{i-c'(q-1)-3} & x \\ \frac{z_{c'}^2+az_{c'}+1}{\alpha^{i-c'(q-1)-3}} & \alpha \cdot \frac{z_{c'}^2+az_{c'}+1}{\alpha^{i-c'(q-1)-3}} & y \\ z_{c'} & z_{c'} & z \end{pmatrix}$$

的秩等于矩阵

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha^{i-c'(q-1)-3} & (\alpha-1) \cdot \alpha^{i-c'(q-1)-3} & x \\ \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} & (\alpha-1) \cdot \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} & y \\ z_{c'} & 0 & z \end{pmatrix}$$

的秩, 其中当 $c' = 1$ 时, $z_{c'} = 0$; 当 $q \geq c' \geq 2$ 时, $z_{c'} = \alpha^{c'-2}$. 因为 x 、 y 和 z 中恰有一个或三个非零, 所以上述矩阵的第 2 和 3 列线性无关. 因此, a_i 、 a_j 和 b_i 线性无关.

(2) 当 $2 + c(q-1) < j \leq 2 + (c+1)(q-1)$ 且 $1 \leq c \leq q$ 时, 矩阵

$$(a_i, b_i, a_j) = \begin{pmatrix} 1 & 1 & 1 \\ \alpha^{i-c'(q-1)-3} & \alpha \cdot \alpha^{i-c'(q-1)-3} & \alpha^{j-c(q-1)-3} \\ \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} & \alpha \cdot \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} & \frac{z_c^2 + az_c + 1}{\alpha^{j-c(q-1)-3}} \\ z_{c'} & z_{c'} & z_c \end{pmatrix}$$

的秩等于矩阵

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha^{i-c'(q-1)-3} & (\alpha-1) \cdot \alpha^{i-c'(q-1)-3} & \alpha^{j-c(q-1)-3} - \alpha^{i-c'(q-1)-3} \\ \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} & (\alpha-1) \cdot \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} & \frac{z_c^2 + az_c + 1}{\alpha^{j-c(q-1)-3}} - \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} \\ z_{c'} & 0 & z_c - z_{c'} \end{pmatrix}$$

的秩. 若 $z_c \neq z_{c'}$, 则上述矩阵的秩为 3. 若 $z_c = z_{c'}$, 则 $c = c'$ 且 $\alpha^{i-c'(q-1)-3} \neq \alpha^{j-c(q-1)-3}$. 上述矩阵通过初等列变换可得

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha^{i-c'(q-1)-3} & 1 & 1 \\ \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{i-c'(q-1)-3}} & \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{2i-2c'(q-1)-6}} & \frac{z_{c'}^2 + az_{c'} + 1}{\alpha^{j+i-(c+c')(q-1)-6}} \\ z_{c'} & 0 & 0 \end{pmatrix}.$$

由 $\alpha^{i-c'(q-1)-3} \neq \alpha^{j-c(q-1)-3}$ 可得上述矩阵的第 2 和 3 列线性无关. 因此, a_i 、 a_j 和 b_i 线性无关.

综上所述, 以 A 和 B 为生成矩阵获得的线性 $\text{OA}(q^4, q^2 + 1, q, 3)$ 和线性 $\text{OA}(q^4, q^2 + 1, q, 2)$ 满足定理 2.4 和 2.6 的条件. 因此, 结论成立.

情形 2 q 为奇数.

构造如下的生成矩阵 $B = (B_0, B_{1,0}, B_{1,\alpha^0}, \dots, B_{1,\alpha^{q-2}})$:

$$B_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & -2\alpha^0 & -2\alpha^1 & \cdots & -2\alpha^{q-2} \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}, \quad B_{1,z} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ -2\alpha^0 & -2\alpha^1 & \cdots & -2\alpha^{q-2} \\ 0 & 0 & \cdots & 0 \\ z & z & \cdots & z \end{pmatrix}, \quad z \in GF(q).$$

类似于偶数的情形, 可证明矩阵 B 的任意两列线性无关, 且对于 $1 \leq i, j \leq q^2 + 1, i \neq j$, 矩阵 A 的第 i 和 j 列与 B 的第 i 列构成的向量组线性无关. 故以 A 和 B 为生成矩阵获得的线性 $\text{OA}(q^4, q^2 + 1, q, 3)$ 和线性 $\text{OA}(q^4, q^2 + 1, q, 2)$ 满足定理 2.4 和 2.6 的条件. 因此, 结论成立. $\square$

注 4.1 推论 4.1、定理 4.3 和 4.4 中获得的 OSOA 比文献 [11, 定理 4] 中的 $\text{OSOA}(q^3, 2\lfloor \frac{q+1}{4} \rfloor, q^3, 3)$ 和 $\text{OSOA}(q^4, 2\lfloor \frac{q^2+1}{4} \rfloor, q^3, 3)$ 有更多的因子数.

定理 4.5 设 $q \geq 3$ 是一个素数幂, $k \geq 3$ 是一个正整数且满足 $q \geq k$, 则存在一个 $\text{OSOA}(q^k, m, q^2, 2+)$ 和一个 $\text{OSOA}(q^k, 2\lfloor \frac{m}{2} \rfloor, q^3, 2+)$, 其中

$$m = \begin{cases} q^{k-1} - (q-1)^{k-1}, & q \geq 2^{k-1}, \\ \sum_{i=1}^{k_0} \binom{k-1}{i} (q-1)^{k-1-i} + x(q-1)^{k-2-k_0}, & q-1 = \sum_{i=1}^{k_0} \binom{k-1}{i} + x, \quad 0 \leq x < \binom{k-1}{k_0+1}. \end{cases}$$

证明 设有限域 $GF(q) = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$, 其中 $\alpha_0 = 0, \alpha_{q-1} = 1$. 取集合 $\{1, 2, \dots, k-1\}$ 的所有非空子集并给它们一个序, 使得当 $|I_1| < |I_2|$ 时, 都有 I_1 排在 I_2 之前. 对于 $1 \leq \ell \leq q-1$, 令 C_ℓ 是由下标 $x_1, x_2, \dots, x_{k-1} \in \{0, 1, \dots, q-2\}$ 且满足 $x_1 + x_2 + \dots + x_{k-1} \equiv \ell \pmod{q-1}$ 的所有行向量 $(\alpha_{x_1}, \alpha_{x_2}, \dots, \alpha_{x_{k-1}})$ 组成. 由众所周知的正交阵列零和构造可得, 每个 C_ℓ 是元素取自于集合 $GF(q) \setminus \{\alpha_{q-1}\}$ 的一个 $\text{OA}((q-1)^{k-2}, k-1, q-1, k-2)$. 显然, 所有 C_ℓ ($1 \leq \ell \leq q-1$) 中的这 $(q-1)^{k-1}$ 个行向量互异.

设 $\{1, 2, \dots, k-1\}$ 的第 ℓ 个子集 I_ℓ 为 $I_\ell = \{i_1, i_2, \dots, i_t\}$, 其中 $i_1 < i_2 < \dots < i_t$. 取出 C_ℓ^T 中第 $i_1, \dots, i_{t-1}$ 个分量均为 α_0 的 $(q-1)^{k-1-|I_\ell|}$ 个列向量, 组成阵列 $\tilde{C}_\ell$. 将矩阵 $\tilde{C}_\ell$ 所有列向量的 I_ℓ 中分量全部替换成 α_{q-1} , 可得另一个新的矩阵 E_ℓ .

对于 $q \geq 2^{k-1}$, 令

$$A = \begin{pmatrix} E_1 & E_2 & \cdots & E_{2^{k-1}-1} \\ \mathbf{1}_{(q-1)^{k-1-|I_1|}} & \mathbf{1}_{(q-1)^{k-1-|I_2|}} & \cdots & \mathbf{1}_{(q-1)^{k-1-|I_{2^{k-1}-1}|}} \end{pmatrix},$$

$$B = \begin{pmatrix} \tilde{C}_1 & \tilde{C}_2 & \cdots & \tilde{C}_{2^{k-1}-1} \\ \mathbf{1}_{(q-1)^{k-1-|I_1|}} & \mathbf{1}_{(q-1)^{k-1-|I_2|}} & \cdots & \mathbf{1}_{(q-1)^{k-1-|I_{2^{k-1}-1}|}} \end{pmatrix},$$

其中 $\mathbf{1}_w$ 代表每个分量都为 1 的一个 w 维行向量. 则矩阵 A 和 B 的列数为 $\sum_{r=1}^{k-1} \binom{k-1}{r} (q-1)^{k-1-r} = q^{k-1} - (q-1)^{k-1}$. 下面证明这两个 $k \times (q^{k-1} - (q-1)^{k-1})$ 矩阵 A 和 B 满足: A 和 B 中任意两列线性无关, 且 A 中的第 i 和 j 列与 B 中的第 i 列也线性无关.

由 C_ℓ^T 中所有列向量不同且不同矩阵 C_ℓ^T 与 $C_{\ell'}^T$ 中取出的两列向量也不同可知, B 中任意两列线性无关. 显然, 从不同矩阵 E_ℓ 和 $E_{\ell'}$ 中取出的两列是不同的, 且由矩阵 E_ℓ 的选取可知, 从同一矩阵 E_ℓ 中取出的两列也是不同的. 因此, A 中的任意两列线性无关.

设 A 的第 i 列向量 β 属于 A 的第 ℓ 个子矩阵, A 的第 j 列向量 γ 属于 A 的第 ℓ' 个子矩阵. 设 B 的第 i 列向量是 η . 根据 ℓ 和 ℓ' 的关系, 分两种情形来验证 β, γ 和 η 线性无关. 下面设 $\beta|_I$ 为向量 β 限制在集合 I 分量上的向量且 $[k-1] = \{1, 2, \dots, k-1\}$.

情形 1 $\ell = \ell'$. 则有 $\beta|_{I_\ell} = \gamma|_{I_\ell}$, $\beta|_{[k-1] \setminus I_\ell} \neq \gamma|_{[k-1] \setminus I_\ell}$, $\beta|_{[k-1] \setminus I_\ell} = \eta|_{[k-1] \setminus I_\ell}$ 和 $\beta|_{I_\ell} \neq \eta|_{I_\ell}$. 将

这 3 个列向量构成的矩阵进行适当的初等行变换, 可得如下矩阵:

$$\begin{pmatrix} \beta|_{I_\ell} & \gamma|_{I_\ell} & \eta|_{I_\ell} \\ \beta|_{[k-1]\setminus I_\ell} & \gamma|_{[k-1]\setminus I_\ell} & \eta|_{[k-1]\setminus I_\ell} \\ 1 & 1 & 1 \end{pmatrix}.$$

再通过初等列变换可得如下矩阵:

$$\begin{pmatrix} \beta|_{I_\ell} & \mathbf{0} & \eta|_{I_\ell} - \beta|_{I_\ell} \\ \beta|_{[k-1]\setminus I_\ell} & \gamma|_{[k-1]\setminus I_\ell} - \beta|_{[k-1]\setminus I_\ell} & \mathbf{0} \\ 1 & 0 & 0 \end{pmatrix}.$$

由于 $\eta|_{I_\ell} - \beta|_{I_\ell} \neq \mathbf{0}$ 且 $\gamma|_{[k-1]\setminus I_\ell} - \beta|_{[k-1]\setminus I_\ell} \neq \mathbf{0}$, 所以此矩阵的秩为 3. 从而, 向量组 β 、 γ 和 η 线性无关.

情形 2 $\ell \neq \ell'$. 则有 $\beta|_{[k-1]\setminus I_\ell} = \eta|_{[k-1]\setminus I_\ell}$ 和 $\beta|_{I_\ell} \neq \eta|_{I_\ell}$. 将这 3 个列向量构成的矩阵进行适当的初等行变换, 可得如下矩阵:

$$\begin{pmatrix} \beta|_{I_\ell} & \gamma|_{I_\ell} & \eta|_{I_\ell} \\ \beta|_{[k-1]\setminus I_\ell} & \gamma|_{[k-1]\setminus I_\ell} & \eta|_{[k-1]\setminus I_\ell} \\ 1 & 1 & 1 \end{pmatrix}.$$

再通过初等列变换可得如下矩阵:

$$\begin{pmatrix} \beta|_{I_\ell} & \gamma|_{I_\ell} - \beta|_{I_\ell} & \eta|_{I_\ell} - \beta|_{I_\ell} \\ \beta|_{[k-1]\setminus I_\ell} & \gamma|_{[k-1]\setminus I_\ell} - \beta|_{[k-1]\setminus I_\ell} & \mathbf{0} \\ 1 & 0 & 0 \end{pmatrix}.$$

当 $I_{\ell'} \not\subset I_\ell$ 时, 由于 $\gamma|_{[k-1]\setminus I_\ell}$ 的某个分量是 α_{q-1} , 而 $\beta|_{[k-1]\setminus I_\ell}$ 的全部分量不为 α_{q-1} , 所以 $\gamma|_{[k-1]\setminus I_\ell} - \beta|_{[k-1]\setminus I_\ell} \neq \mathbf{0}$. 再由 $\eta|_{I_\ell} \neq \beta|_{I_\ell}$ 可得此矩阵的秩为 3. 当 $I_{\ell'} \subset I_\ell$ 时, 由 $\ell \neq \ell'$ 可知, $\gamma|_{I_\ell} - \beta|_{I_\ell}$ 不是零向量且 $\gamma|_{I_\ell} - \beta|_{I_\ell}$ 至少有一个分量等于 0. 由 $\eta|_{I_\ell}$ 的每个分量都不为 α_{q-1} 可得 $\eta|_{I_\ell} - \beta|_{I_\ell}$ 所有分量都不等于 0. 于是向量 $\gamma|_{I_\ell} - \beta|_{I_\ell}$ 和 $\eta|_{I_\ell} - \beta|_{I_\ell}$ 线性无关, 从而矩阵的秩为 3. 故向量组 β 、 γ 和 η 线性无关.

因此, 阵列 A 和 B 满足: A 和 B 中任意两列线性无关, 且 A 中的第 i 和 j 列与 B 中的第 i 列也线性无关. 应用定理 4.1, 由生成矩阵 A 和 B 得到的两个线性的 $\text{OA}(q^k, m, q, 2)$ 满足定理 2.3 和 2.5 中条件, 从而结论成立.

对于 $q < 2^{k-1}$, 令

$$A' = \begin{pmatrix} E_1 & E_2 & \cdots & E_{q-1} \\ \mathbf{1}_{(q-1)^{k-1}-|I_1|} & \mathbf{1}_{(q-1)^{k-1}-|I_2|} & \cdots & \mathbf{1}_{(q-1)^{k-1}-|I_{q-1}|} \end{pmatrix},$$

$$B' = \begin{pmatrix} \tilde{C}_1 & \tilde{C}_2 & \cdots & \tilde{C}_{q-1} \\ \mathbf{1}_{(q-1)^{k-1}-|I_1|} & \mathbf{1}_{(q-1)^{k-1}-|I_2|} & \cdots & \mathbf{1}_{(q-1)^{k-1}-|I_{q-1}|} \end{pmatrix}.$$

类似于 $q \geq 2^{k-1}$ 情形的证明, 这两个 $k \times m$ 矩阵 A' 和 B' 满足: A' 和 B' 中任意两列线性无关, 且 A' 中的第 i 和 j 列与 B' 中的第 i 列也线性无关, 其中 $m = \sum_{i=1}^{k_0} \binom{k-1}{i} (q-1)^{k-1-i} + x(q-1)^{k-2-k_0}$. 因此, 应用定理 4.1, 由生成矩阵 A' 和 B' 得到的两个线性的 $\text{OA}(q^k, m, q, 2)$ 满足定理 2.3 和 2.5 中条件, 从而结论成立. $\square$

注 4.2 Zhou 和 Tang^[13] 构造了一个 $\text{OSOA}(q^k, \frac{q^{k-1}-1}{q-1}, q^2, 2+)$, 定理 4.5 所得到的 $\text{OSOA}(q^k, m, q^2, 2+)$ 具有更多的因子数. Li 等^[10] 构造了一个 $\text{OSOA}(q^k, 2\lfloor \frac{q^{k-1}-1}{2q-2} \rfloor, q^3, 2*)$, 定理 4.5 所得到的 $\text{OSOA}(q^k, 2\lfloor m/2 \rfloor, q^3, 2*)$ 具有更多的因子数.

5 结论

列正交强正交阵列在计算机试验中有重要作用. Zhou 和 Tang^[13] 及 Li 等^[10] 通过构造一对正交阵列分别获得强度为 $2+$ 和 $3-$ 及 $2*$ 和 3 的列正交强正交阵列. 本文利用差矩阵和线性码的生成矩阵构造满足他们定理要求的一对正交阵列, 从而构造出强度为 $2+$ 、 $2*$ 、 $3-$ 和 3 的列正交强正交阵列. 相比之下, 本文构造的列正交强正交阵列具有更多的因子数.

当 $N < 300$ 时, 关于 $\text{OSOA}(N, m, s^2, 2+)$ 、 $\text{OSOA}(N, m, s^3, 2*)$ 和 $\text{OSOA}(N, m, s^3, 3)$ 因子数的改进如表 1.

对于强度为 $3-$ 的阵列, 除 Zhou 和 Tang 构造的 $\text{OSOA}(2^{k+1}, 2^k - 1, 4, 3-)$ 外, 没有相关结果, 本

表 1 $N < 300$ 的三类列正交强正交阵列

N	s	原来的 m 值和文献	新的 m 值	强度 p	依据
27	3	4 [13, 表 1]	6	$2+$	推论 3.1
54	3	7 [13, 表 1]	12	$2+$	推论 3.1
64	4	5 [13, 表 1]	8	$2+$	推论 3.1
81	3	13 [13, 表 1]	18	$2+$	推论 3.1
125	5	6 [10, 表 3]	10	$2+$	推论 3.1
250	5	11 [10, 表 3]	20	$2+$	推论 3.1
162	3	25 [10, 表 3]	36	$2+$	推论 3.1
243	3	40 [10, 表 3]	54	$2+$	推论 3.1
27	3	4 [10, 应用 2]	6	$2*$	推论 3.1
54	3	6 [10, 应用 2]	12	$2*$	推论 3.1
64	4	4 [10, 表 3]	8	$2*$	推论 3.1
81	3	12 [10, 应用 2]	18	$2*$	推论 3.1
125	5	6 [10, 表 3]	10	$2*$	推论 3.1
250	5	10 [10, 表 3]	20	$2*$	推论 3.1
162	3	24 [10, 表 3]	36	$2*$	推论 3.1
243	3	40 [10, 表 3]	54	$2*$	推论 3.1
27	3	2 [10, 表 3]	4	3	定理 4.3
64	4	3 [10, 表 3]	4	3	推论 4.1
81	3	5 [10, 表 3]	10	3	定理 4.4
125	5	3 [10, 表 3]	6	3	定理 4.3

文丰富此类阵列结果.

本文从差矩阵和生成矩阵来获得列正交强正交阵列, 利用其他正交阵列的构造方法获得具有更多因子数的列正交强正交阵列值得进一步探究.

致谢 感谢审稿人对本文提出宝贵意见.

参考文献

- 1 Bingham D, Sitter R R, Tang B. Orthogonal and nearly orthogonal designs for computer experiments. *Biometrika*, 2009, 96: 51–65
- 2 Colbourn C J. Difference matrices. In: *The CRC Handbook of Combinatorial Designs*. Boca Raton: CRC Press, 2007, 411–419
- 3 de Launey W. Generalized Hadamard matrices. In: *The CRC Handbook of Combinatorial Designs*. Boca Raton: CRC Press, 2007, 301–306
- 4 Dembowski P. *Finite Geometries*. New York: Springer, 1968
- 5 Fang K T, Li R, Sudjianto A. *Design and Modeling for Computer Experiments*. Boca Raton: Chapman & Hall/CRC, 2006
- 6 He Y, Cheng C S, Tang B. Strong orthogonal arrays of strength two plus. *Ann Statist*, 2018, 46: 457–468
- 7 He Y, Tang B. Strong orthogonal arrays and associated Latin hypercubes for computer experiments. *Biometrika*, 2013, 100: 254–260
- 8 Hedayat A S, Sloane N J A, Stufken J. *Orthogonal Arrays*. New York: Springer, 1999
- 9 Lawrence K M. A combinatorial characterization of (t, m, s) -nets in base b . *J Combin Des*, 1996, 4: 275–293
- 10 Li W, Liu M Q, Yang J F. Construction of column-orthogonal strong orthogonal arrays. *Stat Papers*, 2022, 63: 515–530
- 11 Liu H, Liu M Q. Column-orthogonal strong orthogonal arrays and sliced strong orthogonal arrays. *Stat Sinica*, 2015, 25: 1713–1734
- 12 Santner T J, Williams B J, Notz W I. *The Design and Analysis of Computer Experiments*. New York: Springer, 2003
- 13 Zhou Y, Tang B. Column-orthogonal strong orthogonal arrays of strength two plus and three minus. *Biometrika*, 2019, 106: 997–1004

Constructions of column-orthogonal strong orthogonal arrays

Jingjun Bao, Lijun Ji & Yuanyao Pan

Abstract Strong orthogonal arrays have better space-filling properties than ordinary orthogonal arrays for computer experiments. Strong orthogonal arrays of strength two plus, two star, three minus and three can improve the space-filling properties in low dimensions and column orthogonality plays a vital role in computer experiments. In this paper, we use difference matrices and generator matrices of linear codes to present several constructions of column-orthogonal strong orthogonal arrays of strength two plus, two star and three minus. Compared with the known results, our constructions can provide more factors.

Keywords orthogonal array, difference matrix, space-filling design

MSC(2020) 05B15

doi: 10.1360/SSM-2022-0062