**Pure Mathematics** 理论数学, 2018, 8(6), 656-661
Published Online November 2018 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2018.86088

Hans汉斯

# On the Construction of Several Types of BCCB Complex Hadamard Matrices of Order $n^2$

**Dengming Xu[1], Qianqian Yan[2]**

[1]Sino-European Institute of Aviation Engineering, Civil Aviation University of China, Tianjin
[2]College of Science, Civil Aviation University of China, Tianjin
Email: xudeng17@163.com, 1261916577@qq.com

Received: Oct. 24th, 2018; accepted: Nov. 5th, 2018; published: Nov. 16th, 2018

## Abstract

**In this note, we study how to construct BCCB complex Hadamard matrices. We first give a necessary and sufficient condition for a BCCB complex matrix of order $n^2$ to be Hadamard, and then use the condition to construct various types of BCCB complex Hadamard matrices. As an example, three new types of BCCB complex Hadamard matrices of order 16 are provided.**

## Keywords

**Circulant Matrices, Circulant Matrices with Circulant Blocks, Hadamard Matrices**

# 几类$n^2$阶BCCB哈达码矩阵的构造

**徐登明[1]，闫茜茜[2]**

[1]中国民航大学中欧航空工程师学院，天津
[2]中国民航大学理学院，天津
Email: xudeng17@163.com, 1261916577@qq.com

收稿日期：2018年10月24日；录用日期：2018年11月5日；发布日期：2018年11月16日

## 摘　要

**本文主要目的是构造BCCB复哈达码矩阵。首先，我们给出了$n^2$阶BCCB复矩阵是哈达码矩阵的一个充要条件，然后利用这个条件构造了几类BCCB复哈达码矩阵。最后，作为例子给出了三类16阶BCCB复哈达码矩阵。**

文章引用: 徐登明, 闫茜茜. 几类 $n^2$ 阶 BCCB 哈达码矩阵的构造[J]. 理论数学, 2018, 8(6): 656-661.
DOI: 10.12677/pm.2018.86088

## 关键词

**循环矩阵，循环块构成的循环矩阵，哈达码矩阵**



## 1. 引言

复哈达码矩阵在量子信息理论中有着重要作用。例如，它被用来解决最小路径覆盖问题[1] [2]，构造相互无偏基[3] [4] [5]，最大纠缠无偏基[6] [7] [8]等等；另一方面，复哈达码矩阵在理论物理的若干问题上有着大量应用[9]。然而，随着矩阵阶数的增加，复哈达码矩阵的结构变得越来越复杂，有关这方面工作的详细介绍读者可参考文[9]。

循环块组成的循环矩阵(BCCB 矩阵)作为循环矩阵的推广引起了人们的广泛关注。例如，文[10]作者利用 BCCB 复哈达码矩阵构造无偏基。文[11]作者研究 9 阶 BCCC 复哈达码矩阵，并利用这些矩阵构造了一个新的 9 维两体量子系统中的无偏基集。

到目前为止，对 BCCB 复哈达码矩阵分类的相关研究并不多，即使是 9 阶复哈达码矩阵的分类也没得以完全解决。本文目的是构造 BCCB 复哈达码矩阵。我们给出了 $n^2$ 阶 BCCB 复矩阵是哈达码矩阵的一个充要条件，并利用这个条件构造了几类 BCCB 复哈达码矩阵。

## 2. 预备知识

设 $n \geq 2$ 是自然数。

**定义 2.1 [12]**：设 $(a_0, a_1, \cdots, a_{n-1})$ 是环 $R$ 中的一个序列。

1) 对角阵 $D = diag(a_0, a_1, \cdots, a_{n-1})$ 定义如下：

$$\forall 1 \leq i, j \leq n,\ D_{jk} = \delta_{jk} a_{k-1}.$$

2) 循环阵 $C = Circ(a_0, a_1, \cdots, a_{n-1})$ 定义如下：

$$\forall 1 \leq j, k \leq n,\ C_{j,k} = a_{(n-1)j \oplus k}$$

其中，$(n-1)j \oplus k$ 是 $\mathbb{Z}_n$ 中的加法运算。因此 $C$ 可写成：

$$C = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \cdots & \cdots & \cdots & \ddots & \cdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

3) $n^2$ 阶方阵 $C$ 被称为由循环块组成的循环矩阵(BCCB 矩阵)是指它具有下面形式：

$$C = Circ(C_0, C_1, \cdots, C_{n-1})$$

其中 $C_0, C_1, \cdots, C_{n-1}$ 都是 $n$ 阶循环阵。

4) 一个 $n$ 阶方阵 $H$ 被称为复哈达码矩阵是指：方阵中每个元素的模都是 1，并且 $H^* H = I_n$，其中，$I_n$ 是 $n$ 阶单位阵，*是厄米特转置。

设 $\omega_n = \mathrm{e}^{\frac{2\pi i}{n}}$，傅立叶矩阵 $F_n$ 定义如下：

$$\forall 1 \le i, j \le n,\ \left(F_n\right)_{jk} = \omega^{(j-1)(i-1)}$$

众所周知，$U_n = \frac{1}{\sqrt{n}} F_n$ 是一个酉矩阵。记

$$D_n = diag\left(1, \omega_n, \omega_n^2, \cdots, \omega_n^{n-1}\right),\ J_n = Circ\left(0,1,0,\cdots,0\right)$$

由线性代数的基本知识，我们有

**命题 2.2：**保持上述记号不变，下列结论成立。

1) $U_n^{-1} J_n U_n = D_n$。

2) 若 $C = Circ\left(a_0, a_1, \cdots, a_{n-1}\right)$，$P_v = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$，则 $U_n^{-1} C U_n = diag\left(P_v\left(1\right), P_v\left(\omega_n\right), \cdots, P_v\left(\omega_n^{n-1}\right)\right)$。

## 3. 矩阵的构造及例子

下面这个定理给出了一个 $n^2$ 阶 BCCB 矩阵是哈达码矩阵的充要条件。

**定理 3.1：**设 $v_i = \left(a_{i,0}, a_{i,1}, \cdots, a_{i,n-1}\right) \in \mathbb{C}^n, 0 \le i \le n-1$，$A = \left(a_{i,j}\right)$，$C_i = Circ\left(v_i\right)$，且 $C = Circ\left(C_0, C_1, \cdots, C_{n-1}\right)$，将 $C$ 记为 BCCB($A$)。若 $A$ 中元素的模全为 1，则 $C$ 是一个哈达码矩阵当且仅当 $U_n C U_n$ 中元素的模全为 1。

**证明：**设 $U = U_n \otimes U_n$。易知

$$C = I_n \otimes C_0 + J_n \otimes C_1 + \cdots + J_n^{n-1} \otimes C_{n-1}.$$

于是有

$$U^{-1} C U = I_n \otimes U_n^{-1} C_0 U_n + D_n \otimes U_n^{-1} C_1 U_n + \cdots + D_n^{n-1} \otimes U_n^{-1} C_{n-1} U_n.$$

由命题 2.2 知，$U^{-1} C U$ 是 $n^2$ 阶对角阵。设 $0 \le k \le n-1$，记 $P_k = P_{v_k}$，

$$V_k = U_n^{-1} C_k U_n = diag\left(P_k\left(1\right), P_k\left(w_n\right), P_k\left(w_n^2\right), \cdots, P_k\left(w_n^{n-1}\right)\right),$$

$$W_k = V_0 + \omega_n^k V_1 + \omega_n^{2k} V_2 + \cdots + \omega_n^{k(n-1)} V_{n-1}.$$

则 $U^{-1} C U = diag\left(W_0, W_1, \cdots, W_{n-1}\right)$。易知对任意 $0 \le k \le n-1, 1 \le j \le n$ 有

$$\left(W_k\right)_{j,j} = \left(1, \omega_n^k, \omega_n^{2k}, \cdots, \omega_n^{k(n-1)}\right) A \left(1, \omega_n^{j-1}, \omega_n^{2(j-1)}, \cdots, \omega_n^{(j-1)(n-1)}\right)$$

故 $C$ 是哈达码矩阵当且仅当 $U^{-1} C U$ 是哈达码矩阵，当且仅当

$$\forall 0 \le k \le n-1, \forall 1 \le j \le n,\ \left|\left(W_k\right)_{j,j}\right| = n.$$

当且仅当 $F_n A F_n$ 中元素模全为 $n$，当且仅当 $U_n A U_n$ 中元素模为 1。□

**推论 3.2：**假设 $D$ 是元素模全为 1 的 $n$ 阶对角矩阵，则 BCCB$\left(DF_n^*\right)$ 和 BCCB$\left(F_n^* D\right)$ 都是哈达码矩阵。

**证明：**因为 $U_n$ 是酉矩阵，故 $U_n D F_n^* U_n = F_n D$ 和 $U_n F_n^* D U_n = D F_n$ 成立，故由定理 3.1 可知结论成立。

**例 3.1：**设 $\left(a,b,c\right) \in \mathbb{C}^3$ 且 $a$，$b$，$c$ 模全为 1。设 $\omega = \exp\left(\frac{2\pi i}{3}\right)$，$D = diag\left(a,b,c\right)$，则

$$F_3^* D = \begin{pmatrix} a & b & c \\ a & b\omega & c\omega^2 \\ a & b\omega^2 & c\omega \end{pmatrix}$$

由推论 3.2，我们得到一个 9 阶 BCCB 哈达码矩阵 $\mathrm{BCCB}\left(F_3^* D\right)$。

**推论 3.3**：设 $V$ 是元素模全为 1 的 $n$ 阶矩阵，则有

1) 若 $V$ 是对角矩阵，则 $\mathrm{BCCB}\left(VF_n\right)$ 和 $\mathrm{BCCB}\left(F_n V\right)$ 是哈达码矩阵。

2) 若 $U_n V U_n^*$ 中元素模全为 1，则 $\mathrm{BCCB}\left(V\right)$ 是哈达码矩阵。

3) 若 $F_n V = VF_n$，则 $\mathrm{BCCB}\left(V\right)$ 是哈达码矩阵。

**证明**：显然 $F_n^2 = nP$，其中 $P$ 是置换矩阵。

1) 因为 $U_n$ 是酉矩阵，故 $U_n VF_n U_n = \frac{1}{n} F_n VF_n^2 = F_n VP$。因此 $U_n VF_n U_n$ 中元素模全为 1。由定理 3.1 知 $\mathrm{BCCB}\left(VF_n\right)$ 是哈达码矩阵。同理可证 $\mathrm{BCCB}\left(F_n V\right)$ 也是哈达码矩阵。

2) 首先，$U_n VU_n = U_n VU_n^* U_n^2 = U_n VU_n^* P$。因为 $U_n VU_n^*$ 中元素模全为 1，故 $U_n VU_n$ 中元素模全为 1。由定理 3.1 知 $\mathrm{BCCB}\left(V\right)$ 是哈达码矩阵。

3) 由 $F_n V = VF_n$ 知 $U_n V = VU_n$，于是有 $U_n VU_n = VU_n^2 = VP$，故 $U_n VU_n$ 中元素模全为 1。由定理 3.1 知 $\mathrm{BCCB}\left(V\right)$ 是哈达码矩阵。□

因为 $F_n$ 是酉矩阵，所以存在对角矩阵 $D_n$ 和酉矩阵 $R_n$ 使得 $F_n = R_n D_n R_n^*$。假设 $D$ 是另一个对角矩阵且 $A = R_n DR_n^*$，则 $AF_n = F_n A$。作为前一推论的直接应用，我们有：

**命题 3.4**：设 $D_n, D$ 为 $n$ 阶对角方阵，$R_n$ 是酉矩阵且 $F_n = R_n D_n R_n^*$。假设 $R_n DR_n^*$ 中元素模全为 1，则 $\mathrm{BCCB}\left(R_n DR_n^*\right)$ 是哈达码矩阵。

**备注**：对比定理 3.1，命题 3.4 变量更少，更容易构造 BCCB 哈达码矩阵。

**例 3.2**：设 $D_4 = diag\left(2,2,-2,2i\right)$，设

$$R_4 = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 & 0 \\ 1 & 0 & -1 & \sqrt{2} \\ -1 & \sqrt{2} & -1 & 0 \\ 1 & 0 & -1 & -\sqrt{2} \end{pmatrix}$$

易验证 $R_4$ 是酉矩阵且 $F_4 = R_4 D_4 R_4^*$。设 $a,b,c,d \in \mathbb{C}^4, D = diag\left(a,b,c,d\right)$。经计算有

$$A = R_4 D_4 R_4^* = \frac{1}{4}\begin{pmatrix} 2b+a+c & a-c & 2b-\left(a+c\right) & a-c \\ a-c & a+c+2d & c-a & a+c-2d \\ 2b-\left(a+c\right) & c-a & 2b+a+c & c-a \\ a-c & a+c-2d & c-a & a+c+2d \end{pmatrix}$$

则 BCCB($A$)是哈达码矩阵当且仅当

$$\begin{cases} \left|a+c\pm 2b\right| = 4 \\ \left|a+c\pm 2d\right| = 4 \\ \left|a-c\right| = 4 \end{cases} \tag{1}$$

假设 $a+c=0$，则 BCCB($A$)是哈达码矩阵当且仅当 $a,b,c,d$ 的模都是 2，即对任意 $\left(\theta_1,\theta_2,\theta_3\right) \in \mathbb{C}^3$，BCCB($A$)是哈达码矩阵，其中

$$A = \begin{pmatrix} \mathrm{e}^{i\theta_1} & \mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_1} \\ \mathrm{e}^{i\theta_1} & \mathrm{e}^{i\theta_3} & -\mathrm{e}^{i\theta_1} & -\mathrm{e}^{i\theta_3} \\ \mathrm{e}^{i\theta_2} & -\mathrm{e}^{i\theta_1} & \mathrm{e}^{i\theta_2} & -\mathrm{e}^{i\theta_1} \\ \mathrm{e}^{i\theta_1} & -\mathrm{e}^{i\theta_3} & -\mathrm{e}^{i\theta_1} & \mathrm{e}^{i\theta_3} \end{pmatrix}$$

假设 $a+c\neq 0$。此时，有方程组(1)知 $b=\pm d$。故问题转化为求解方程组

$$\begin{cases} |a+c+2b|=4 \\ |a+c-2b|=4 \\ |a-c|=4 \end{cases} \tag{2}$$

i) 假设 $b=d$。由方程组(2)知，存在 $(\theta_1,\theta_2,\theta_3)\in\mathbb{R}^3$ 使得

$$\begin{cases} a+c+2b=4\mathrm{e}^{i\theta_1} \\ a+c-2b=4\mathrm{e}^{i\theta_2} \\ a-c=4\mathrm{e}^{i\theta_3} \end{cases}$$

显然，此时方程组总有解。因此，对任意 $(\theta_1,\theta_2,\theta_3)\in\mathbb{R}^3$，若取

$$A=\begin{pmatrix} \mathrm{e}^{i\theta_1} & \mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_3} & \mathrm{e}^{i\theta_2} \\ \mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_1} & -\mathrm{e}^{i\theta_2} & -\mathrm{e}^{i\theta_3} \\ \mathrm{e}^{i\theta_3} & -\mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_1} & -\mathrm{e}^{i\theta_2} \\ \mathrm{e}^{i\theta_2} & -\mathrm{e}^{i\theta_3} & -\mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_1} \end{pmatrix}$$

则 BCCB($A$)是哈达码矩阵。

ii) 假设 $b=-d$。同理，对任意 $(\theta_1,\theta_2,\theta_3)\in\mathbb{R}^3$，若取

$$A=\begin{pmatrix} \mathrm{e}^{i\theta_1} & \mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_3} & \mathrm{e}^{i\theta_2} \\ \mathrm{e}^{i\theta_2} & -\mathrm{e}^{i\theta_3} & -\mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_1} \\ \mathrm{e}^{i\theta_3} & -\mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_1} & -\mathrm{e}^{i\theta_2} \\ \mathrm{e}^{i\theta_2} & \mathrm{e}^{i\theta_1} & -\mathrm{e}^{i\theta_2} & -\mathrm{e}^{i\theta_3} \end{pmatrix}$$

则 BCCB($A$)是哈达码矩阵。

## 基金项目

感谢本文审稿人的宝贵意见，本论文由国家自然科学基金资助(编号：11501564)。

## 参考文献

[1] Caidman, L., Aharonov, Y. and Albert, D.Z. (1987) How to Ascertain the Values of σx, σy and σz of a Spin-1/2 Particle. *Physical Review Letters*, **58**, 1385-1387. https://doi.org/10.1103/PhysRevLett.58.1385

[2] Englert, B.G. and Aharonov, Y. (2001) The Mean King's Problem: Prime Degrees of Freedom. *Physics Letters A*, **284**, 1-5. https://doi.org/10.1016/S0375-9601(01)00271-7

[3] Bandyopadhyay, S., Boykin, P.O., Roychowdhury, V. and Vatan, F. (2002) A New Proof for the Existence of Mutually Unbiased Bases. *Algorithmica*, **34**, 512-528. https://doi.org/10.1007/s00453-002-0980-7

[4] Brierley, S. (2009) Mutually Unbiased Bases in Low Dimensions. PhD Thesis, University of York, York.

[5] Wootters, W.K. and Fields, B.D. (1989) Optimal State-Determination by Mutually Unbiased Measurements. *Annals of Physics*, **191**, 363-381. https://doi.org/10.1016/0003-4916(89)90322-9

[6] Liu, J.Y., Yang, M.H. and Feng, K.Q. (2017) Mutually Unbiased Maximally Entangled Bases in $\mathbb{C}^d\otimes\mathbb{C}^d$. *Quantum Information Processing*, **16**, 159. https://doi.org/10.1007/s11128-017-1608-9

[7] Tao, Y.H., Nan, H, Zhang, J. and Fei, S.M. (2015) Mutually Unbiased Maximally Entangled Bases in $\mathbb{C}^d\otimes\mathbb{C}^{kd}$. *Quantum Information Processing*, **14**, 2291-2300. https://doi.org/10.1007/s11128-015-0980-6

[8] Xu, D.M. (2017) Construction of Mutually Unbiased Maximally Entangled Bases through Permutations of Hadamard Matrices. *Quantum Information Processing*, **16**, 65. https://doi.org/10.1007/s11128-017-1534-x

[9] Tadej, W. and Zyczkowski, K. (2006) A Concise Guide to Complex Hadamard Matrices. *Open Systems and Informa-*

*tion Dynamics*, **13**, 133-177. https://doi.org/10.1007/s11080-006-8220-2

[10] Combescure, M. (2009) Block-Circulant Matrices with Circulant Blocks, Weil Sums, and Mutually Un-Biased Bases. II. The Prime Power Case. *Journal of Mathematical Physics*, **50**, Article ID: 032104. https://doi.org/10.1063/1.3078420

[11] Karlsson, B.R. (2016) BCCB Complex Hadamard Matrices of Order 9, and MUBs. *Linear Algebra and Its Applications*, **501**, 309-324. https://doi.org/10.1016/j.laa.2016.04.012

[12] Davis, P.J. (1979) Circulant Matrices. John Wiley and Sons, New York.