arXiv:2301.00633v1 [cs.IT] 2 Jan 2023

嵌套完美环面数组

VER´ONICA BECHER 和 OLIVIER CARTON

Abstract. 我们介绍一种二维环面数组，它是 de Bruijn 环面的一种变体。我们称之为嵌套完美环面数组。我们不再要求给定大小的每个数组恰好出现一次，而是将各个位置划分为同余类，并要求每个同余类中恰好出现一次。我们还要求这一性质递归地适用于每个子数组。我们提出一种基于模 2 帕斯卡三角形矩阵构造嵌套完美环面数组的方法。对于二元字母表，当 n 为 2 的幂时，我们的方法可生成 2^{n^2+n-1} 种不同的嵌套完美环面数组，在每个同余类中分配所有不同的 $n \times n$ 数组；这些同余类由行号模 n 和列号模 n 得到。

关键词：de Bruijn 环面、嵌套完美项链、帕斯卡三角形 数学主题分类：05B05、11C20 计算机分类系统：计算数学、离散数学、组合问题

Contents

1. 引言与结果陈述 1 2. 定理1的证明 4 3. 定理2的证明 9 致谢。17 参考文献 17

1. Introduction and statement of results

大小为 $n \times n$ 的环面数组是指将行号视为模 n、列号视为模 n 的数组。在本文中，我们研究由有限字母表中的符号构成的环面数组。构造大小最小且能容纳给定一族较小数组的环面数组这一问题可追溯至20世纪60年代，例如参见 [8, 15]。对于这类环面数组，其中每个族成员恰好出现一次；其构造将经典一维德布鲁因序列推广到二维数组，称为 de Bruijn 环面或完美映射。人们为确定不同子数组尺寸下这类环面数组是否存在，并提出相应的构造方法，付出了大量努力，例如 [12, 6, 16, 10, 5, 14, 4] 的研究。早期成果主要关注由 0 和 1 构成的数组。后续研究解决了任意字母表下的存在性问题和构造问题。如何高效地恢复任意给定子数组也备受关注 [13]。此外，还有关于三维数组构造的研究 [9]。

Date：2023年1月3日。

本文介绍 de Bruijn 环面的一种变体，称之为嵌套完美环面数组。我们不再要求给定大小的每个数组恰好出现一次，而是将位置划分为同余类，并要求每个同余类中恰好出现一次。我们还要求这一性质递归地适用于子数组。

嵌套完美环面数组是作者在一维情形下工作的二维版本，他们将其称为嵌套完美项链 [3]。嵌套完美项链是完美项链 [1] 的一种特殊情形。

在下文中，我们将行和列从 0 开始编号（而不是从 1 开始）。对于任意二维环面数组 A，位置为 (k,ℓ)、大小为 $n \times n$ 的子数组，是由从 k 到 $k+n-1$ 的行以及从 ℓ 到 $\ell+n-1$ 的列组成的数组，其中所有这些索引均分别对 A 的行数和列数取模。请注意，由于行和列从 0 开始编号，因此 (0, 0) 是每个数组左上角的位置。

模是一个由两个正整数构成的对，写作 (p,q)。任意给定数组的位置会按照各自对 p 和 q 取模所得的剩余类，划分为 pq 个剩余类：因此，模 (1, 1) 产生一个包含所有位置的单一类，而模 (2, 2) 则将这些位置划分为四类。

大小为 $n \times n$ 的数组在数组中位置 (k,ℓ) 处出现，当且仅当它等于位置 (k,ℓ) 处大小为 $n \times n$ 的子数组。

定义 1（完美环面数组）。若环面数组 A 对于窗口大小 $s \times t$ 和模 (p,q) 是完美的，简称为 (s,t,p,q)-完美，则每个 $s \times t$ 数组在 A 中的每个模 (p,q) 剩余类里恰好出现一次。

因此，在 $(s,t,1,1)$-完美环面数组中，每个 $s \times t$ 数组恰好出现一次。图1给出了一个 (2, 2, 1, 1)完美环面数组和两个 (2, 2, 2, 2)-完美环面数组的示例。在最左侧的数组中，每个 2×2 数组恰好出现一次。在另外两个数组中，每个2×2 数组恰好出现四次，并且在模 (2, 2) 的每个剩余类中恰好出现一次。

定义2（对齐子数组）。给定一个数组 A，大小为 $k \times \ell$ 的子数组若其在 A 中的位置 (i,j) 满足 k 整除 i 且 ℓ 整除 j，则称其为对齐子数组。

定义3（细分）。若 k 和 ℓ 均整除 n，则数组 $n \times n$ 的 $k \times \ell$-细分会产生 $k\ell$ 个对齐子数组，每个子数组的大小为 $n/k \times n/\ell$。

定义4（嵌套完美环面数组）。设字母表含有 b 个符号。若完美环面数组 A 对窗口大小 $s \times t$ 和模 (p,q) 是嵌套的，简称嵌套 (s,t,p,q)-完美，则对于每个 $k = 0,\ldots,s-1$，A 的 $b^{kt/2} \times b^{kt/2}$- 细分中的每个对齐子数组都是 $(s-k,t,p,q)$ - 完美的。

请注意，(f,g,p,q)-完美意味着当 $1 \le f' \le f$ 和 $1 \le g' \le g$ 时 (f',g',p,q)-完美。反向推论未必成立。定义4要求细分产生 $(s-k,t,p,q)$-完美子数组，而非可能预期的 $(s-k,t-k,p,q)$-完美子数组。我们的动机是，我们有一种构造方法可以确保这一更强的性质。

对于嵌套完美数组的定义，还有其他自然的选择。对于非方形数组，这些定义彼此并不等价，但对于方形数组，它们都一致。在本文中，我们关注方阵情形。

考虑一个在含有 b 个符号的字母表上的 (n,n,n,n)-完美环面数组。其大小为 $nb^{n^2/2} \times nb^{n^2/2}$，其中 n 为偶数。对于 $k = 0,\ldots,n-1$，其 $b^{kn/2} \times b^{kn/2}$ 细分的每个部分大小为 $nb^{n(n-k)/2} \times nb^{n(n-k)/2}$。

对于方形数组，嵌套完美环面数组的定义可以改述如下。

定义5（方形嵌套完美环面数组）。设字母表包含 b个符号。若一个(n,n,n,n)完美环面数组满足：对于 $k = 1,\ldots,n$，每个大小为$nb^{nk/2} \times nb^{nk/2}$的对齐子数组都是$(k,n,n,n)$完美的，则称其为嵌套的。

对于 $b = 2$ 和 $n = 4$：大小为 1024×1024 的数组 A 是嵌套的(4, 4, 4, 4)完美环面数组，当且仅当

- A 是一个(4, 4, 4, 4)完美环面数组；
- 每个 256×256 对齐子数组都是一个(3, 4, 4, 4)完美环面数组；
- 每个 64×64 对齐子数组都是一个(2, 4, 4, 4)完美环面数组；
- 每个 16×16 对齐子数组都是一个(1, 4, 4, 4)完美环面数组。

				0	0	0	0	0
				0	1	0	1	0
				0	0	0	1	1
0	1	0	0	1	0	1	0	1
0	1	1	1	0	0	0	1	1
1	1	1	0	1	1	1	1	1
0	0	1	0	0	0	0	1	1

(a) 非嵌套
(2, 2, 1, 1)完美

0	0	0	0	0	0	0	0	
0	0	0	1	1	0	1	1	
0	1	0	1	0	1	0	1	
0	0	0	1	1	0	1	1	
1	0	1	0	1	0	1	0	
0	0	0	1	1	0	1	1	
1	1	1	1	1	1	1	1	
0	0	0	1	1	0	1	1	

(b) 非嵌套
(2, 2, 2, 2)-完美

0	0	0		1	0	1	0	0
0	0	0	1	0	0	0	1	
1	0	1	1	1	1	1	0	
1	0	1	1	1	0	1	1	
1	0	1	1	1	1	1	0	
0	0	0	1	0	0	0	1	
0	0	0	1	0	1	0	0	
1	0	1	1	1	0	1	1	

(c) 嵌套
(2, 2, 2, 2)-完美

FIGURE 1. 完美环面数组示例

嵌套（n,n,n,n）完美数组的数组大小，$n = 2^d$	窗口大小	模
$(b^{n\times n/2} \times n) \times (b^{n\times n/2} \times n)$	$n \times n$	(n,n)
$(b^{n/2\times n/2} \times n) \times (b^{n/2\times n/2} \times n)$	$(n/2) \times n$	(n,n)
$(b^{n/2^2\times n/2} \times n) \times (b^{n/2^2\times n/2} \times n)$	$(n/2^2) \times n$	(n,n)
$\vdots$	$\vdots$	$\vdots$
$(b^{1\times n/2} \times n) \times (b^{(1\times n/2} \times n)$	$1 \times n$	(n,n)

FIGURE 2. 细分大小和窗口大小

上方图1中最左侧的两个环面数组不是嵌套完美数组：最左侧的数组之所以不是嵌套的，是因为其左上方的 2×2 子数组中有 2 次 1×2 数组$[0,1]$ 出现，但没有 1×2 数组 $[0,0]$出现。图1中的中间数组不是嵌套（2, 2, 2, 2）-完美数组，因为其左上方的 4×4 子数组中 0 的数量多于 1 的数量。最右侧的环面数组是嵌套（2, 2, 2, 2）-完美环面数组。

以下是本文的主要结果。该结果说明：当所有参数都等于同一个 2 的幂时，存在由 0 和 1 组成的嵌套完美环面数组。

定理 1. 对于每个为 2 的幂的整数 $n \geqslant 2$，都存在由 0 和 1 构成的嵌套（n, n, n, n）完美环面数组。

我们的构造方法并非只产生一个实例，而是能产生许多个。下一个结果——定理 2——给出了用我们的方法能够得到的不同实例的确切数量。

定理 2. 存在一种构造方法，对于每个为 2 的幂的整数 n，都能产生 2^{n^2+n-1} 个由 0 和 1 构成的不同嵌套（n, n, n, n）完美环面数组。

我们不知道是否还有更多。

2. 定理 1 的证明

我们假设字母表是二元域 $\mathbb{F}_2 = \{0, 1\}$。我们将使用由 $\mathbb{F}_2 = \{0, 1\}$ 中元素组成的矩阵，进行矩阵乘法和矩阵求和。$\mathbb{F}_2$ 中元素的逐分量和用符号 $\oplus$ 表示。矩阵用字母 M、N、P、Q 加上下标和上标命名。绘制矩阵时，我们会在外侧画上黑色括号。每种情况下，构造的结果都是一个由 $0s$ 和 1 组成的环面数组，通过用上述矩阵铺砌得到。数组用字母 A、B、C 命名，绘制时不在外侧加黑色括号。

我们首先定义以下矩阵族。

定义6. 我们通过归纳定义矩阵 M_d，它由 $\mathbb{F}_2$ 中的元素组成，大小为 $2^d \times 2^d$，对每个 $d \geq 0$，定义如下：

$$M_0 = (1) \quad and \quad M_{d+1} = \begin{pmatrix} M_d & M_d \\ 0 & M_d \end{pmatrix}.$$

因此，矩阵 M_1 和 M_2 是

$$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

对于每个 d，矩阵 M_d 都是上三角矩阵，即 $(M_d)_{i,\,j} = 0$ 对于 $0 \leqslant j < i < 2^d$。下面的引理指出，矩阵 M_d 的上半部分也是模 2 的帕斯卡三角形的开头，该图形也称为谢尔宾斯基三角形。证明可通过对 d进行简单归纳得到，详见 [3, 引理 3]。

矩阵 M_d 与 M. Levin 在 [11, 定理 2] 中使用的矩阵几乎相同，因为我们颠倒了各列的顺序。H. Faur´e [7] 此前曾使用帕斯卡三角形矩阵来构造实数的均匀分布序列。

引理 1（[3, 引理 3]）。对于满足 $d \geqslant 0$、$0 < i < 2^d$ 和 $0 \leqslant j < 2^d - 1$ 的所有整数 d、i、j，有 $(M_d)_{i,\,j} = (M_d)_{i-1,\,j} \oplus (M_d)_{i,\,j+1}$。

证明。为便于审阅，我们纳入了 [3, 引理 3]中已经给出的证明。证明通过对 d 使用归纳法完成。对于 $d = 0$，结论显然成立，因为不存在这样的 i 和 j。对于 $d = 1$，结论显然成立。假设结论对M_d 成立，并令 i、j 为满足 $0 < i < 2^{d+1}$ 和 $0 \le j < 2^{d+1} - 1$ 的整数。如果 $i \neq 2^d$ 且$j \neq 2^d - 1$，则三个元素（M_{d+1}）$_{i,\ j}$ （M_{d+1}）$_{i-1,\ j}$ 和（M_{d+1}）$_{i,\ j+1}$ 位于矩阵 M_{d+1} 的同一象限内，结论由归纳假设得出。否则，结论是以下事实的结果：对于每个整数 $d \ge 1$，元素（M_d）$_{i,\ j}$ 在 $i = 0$ 或 $j = 2^d - 1$ （第一行和最后一列）时等于 1，在 $i = 2^d - 1$ 或 $j = 0$ （最后一行和第一列）时等于 0，而（M_d）$_{0,\ 0}$ = （M_d）$_{2^d-1,\ 2^d-1} = 1$ （前述两种情况的交集）。这些事实很容易通过对 d 使用归纳法证明。□

Bacher 和 Chapman [2, 定理 1 及 3] 证明了：对于每个非负整数 d以及满足 $1 \le k \le 2^d$的每个整数 k，由 k 个连续行和最后的 k 列，或由顶部的 k 个连续行和任意 k 个连续列构成的每个 M_d 子矩阵 $k \times k$ 都是可逆的。在 $k = 2^d$ 的情况下，这说明整个矩阵 M_d 是可逆的。下一节的引理 2 和 3 中给出了这一结果更一般形式的证明。

现在我们定义所有 $n \times n$ 矩阵在 $\mathbb{F}_2$上的一个枚举。假设整数 n 已固定。令 N_0、...、$N_{2^{n^2}-1}$ 为按如下方式定义的这些矩阵的枚举。非正式地说，对于 $0 \leqslant k < 2^{n^2}$，矩阵 N_k 由 k的二进制展开中的各位填充：最 n高有效的二进制位放在第一行，接下来的 n 个位放在第二行，依此类推，直到最后一行。

定义 7（矩阵枚举）。固定一个正整数整数 n。我们定义所有 $\mathbb{F}_2$上的 $n \times n$ 矩阵的一个枚举 $N_0, \ldots, N_{2^{n^2}-1}$。设 k为一个非负整数，其二进制展开为 $a_{n^2-1} \cdots a_0$（最低有效位为 a_0）。对于每个 i, j，满足 $i, j = 0, \ldots, n-1$，矩阵 N_k的第（i, j）个元素为 $a_{n^2-1-in-j}$。因此， N_k的（0, 0）元素是第一位数字 a_{n^2-1}，而第（$n-1, n-1$）个元素是最后一位数字 a_0。

例如， $\mathbb{F}_2$ 上大小为 2×2 的 16 个矩阵的枚举 $N_0, \ldots, N_{15}$ 为

$$\begin{matrix}\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right),\\ \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)\end{matrix}$$

对于任意给定的非负整数 k，我们将其二进制表示视为比特序列 $a_n \ldots a_0$。我们用 even(k) 表示这样一个整数，其二进制表示为子序列 $a_m \ldots a_2 a_0$，该子序列由 k的表示中处于偶数位置的比特组成，因此，若 n 为偶数，则 $m = n$；否则为 $m = n - 1$。类似地，odd(k) 是由奇数索引确定的子序列所定义的整数。

定义 8（帕斯卡环面数组）。设 d 为正整数，并设 $n = 2^d$。我们通过用所有 $n \times n$ 个 $\mathbb{F}_2$ 上的矩阵铺砌，定义一个大小为 $n2^{n^2/2} \times n2^{n^2/2}$、取值于 $\mathbb{F}_2$ 的环面数组 A_d。由于共有 2^{n^2} 个这样的矩阵，放置的单元格总数恰好等于 A_d的大小。对于每个满足 $0 \leqslant k < 2^{n^2}$ 的 k，将矩阵 $M_d N_k$ 放置在 A_d 中的位置 (odd(k)n, even(k)n)。

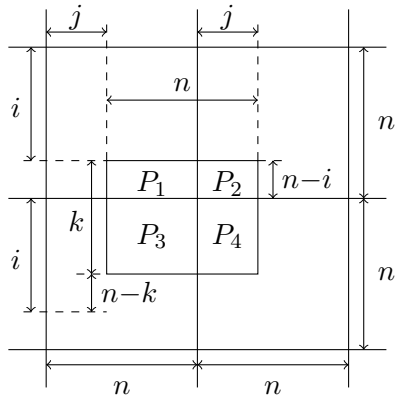


FIGURE 3. 数组 B 在 A_d, $n = 2^d$ 中的一次出现。

由于每个矩阵 M_d 都是对角线上为 1 的上三角矩阵，因此它是可逆的。由于 N_0，...，N_{n^2-1} 是所有 $n \times n$ 个矩阵的枚举，因此 M_dN_0，...，$M_dN_{n^2-1}$ 也是所有 $n \times n$ 个矩阵的枚举，只是顺序不同。这意味着每个 $n \times n$矩阵都恰好使用一次来铺砌数组 A_d。

我们以 $d = 1, n = 2$ 为例说明 A_d 的构造。上面列出了矩阵 $N_0, \ldots, N_{15}$。矩阵 M_1N_k（$k = 0, \ldots, 15$）在数组 A_1 中的排列如下：

$$\begin{array}{cccc} M_1N_0 & M_1N_1 & M_1N_4 & M_1N_5 \\ M_1N_2 & M_1N_3 & M_1N_6 & M_1N_7 \\ M_1N_8 & M_1N_9 & M_1N_{12} & M_1N_{13} \\ M_1N_{10} & M_1N_{11} & M_1N_{14} & M_1N_{15} \end{array}$$

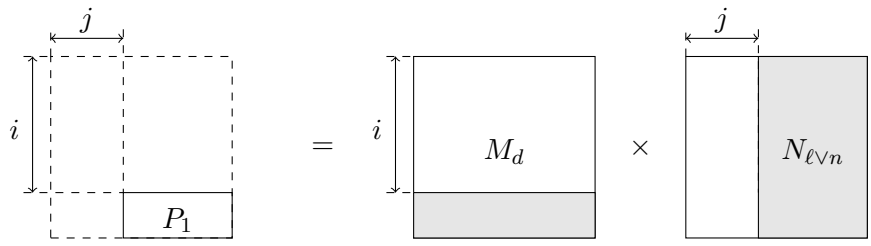
由于每个矩阵 M_1N_k 的大小为 2×2，数组 A_1 的大小为 8×8。图1右侧给出的嵌套 (2, 2, 2, 2)-完美数组实际上就是数组 A_1。

命题1. 设 d 为非负整数，且令 $n = 2^d$。设 k 为满足 $1 \leqslant k \leqslant n$ 的整数。A_d 的每个 $n2^{kn/2} \times n2^{kn/2}$ 对齐子数组都是一个嵌套 (k, n, n, n)-完美环面数组。

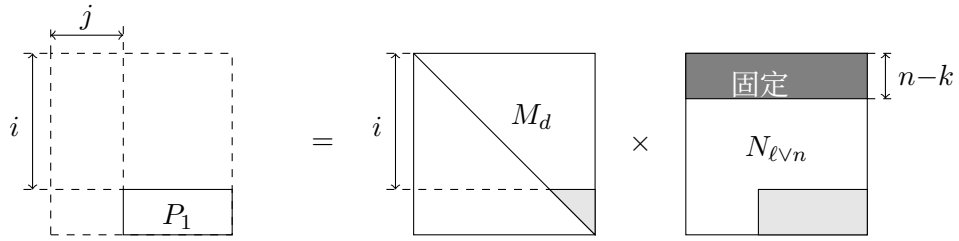
证明。假设 k 固定，$1 \leqslant k \leqslant n$，并令 B 为 A_d 的一个大小为 $n2^{kn/2} \times n2^{kn/2}$ 的对齐子数组。由于 B 对齐，其左上角的坐标形式为 $pn2^{kn/2}$ 和 $qn2^{kn/2}$，其中 p 和 q 为满足 $0 \leqslant p$、$q < 2^{(n-k)n/2}$ 的两个整数。这意味着子数组 B 可由矩阵 $M_dN_{\ell \vee m}$ 平铺，其中整数 ℓ 和 m 满足

$$p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2} \text{ and } q2^{kn/2} \leqslant m < (q+1)2^{kn/2}.$$

注意，因子 n 消失了，因为它表示各个矩阵的大小$M_dN_{\ell \vee m}$。所有满足 $p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2}$ 的整数 ℓ 的二进制展开都以相同的（$n-k$）$n/2$ 个二进制位开头；所有满足 $q2^{kn/2} \leqslant m < (q+1)2^{kn/2}$. 的整数 m 也同样如此。这意味着，$\ell \vee m$ 的二进制展开也以相同的（$n-k$）n个二进制位开头。由于 $\ell \vee m$的前几个二进制位被放在矩阵 $N_{\ell \vee m}$的前几行中，而这些行的长度为 n，因此，对于各自区间内的 ℓ 和 m，所有矩阵 $N_{\ell \vee m}$ 的前 $n - k$ 行都相同。

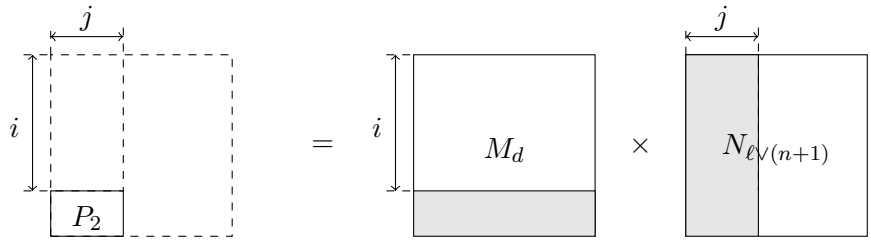


(a) 用于计算 P_1 的 M_d 和 $N_{\ell\vee n}$ 部分

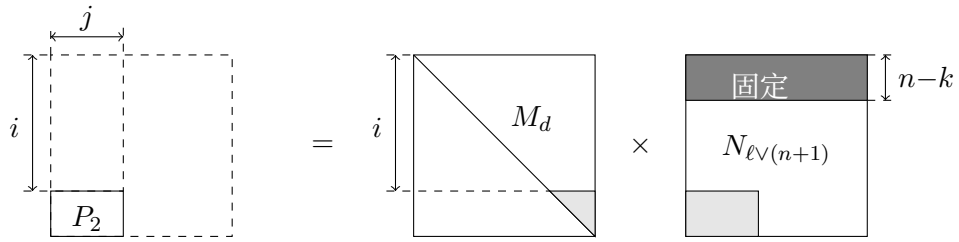


(b) 考虑到 M_d 是上三角的

FIGURE 4. 命题1的证明，使用 P_1



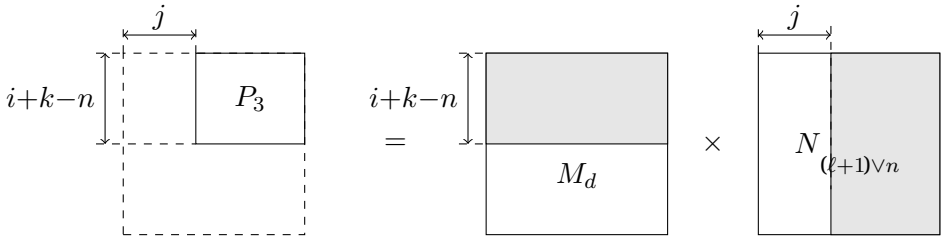
(a) 用于计算 P_2 的 M_d 和 $N_{\ell\vee n}$ 部分



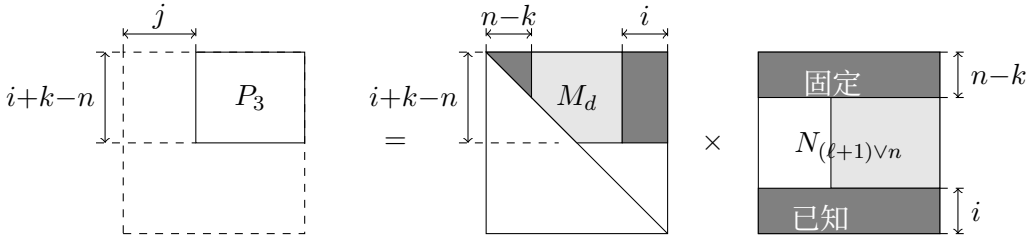
(b) 考虑到 M_d 是上三角的

FIGURE 5. 命题1的证明，使用 P_2

设（i，j）为一对整数，满足 $0 \leqslant i, j < n$，并设 P为大小为 $k \times n$的数组。我们断言，P在 B中恰好出现一次，且该位置与（i，j）模（n，n）同余。为证明这一点，我们证明，当且仅当某个线性方程组有解时，P才恰好有这样一次出现。此外，该方程组的这个解给出矩阵 $N_{\ell\vee m}$，进而确定整数 ℓ 和 m；这些整数又给出 P 在子数组 B中的出现位置。

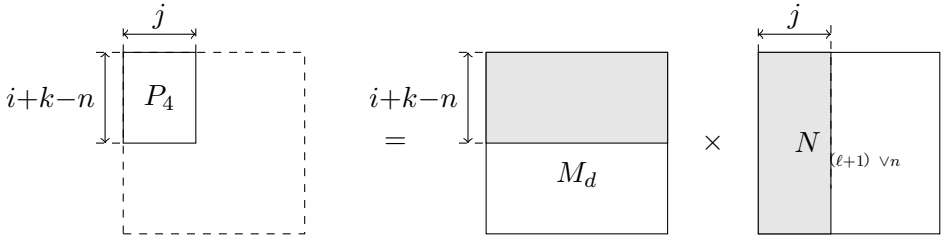


(a) 用于计算 P_3 的 M_d 和 $N_{\ell\vee n}$ 部分

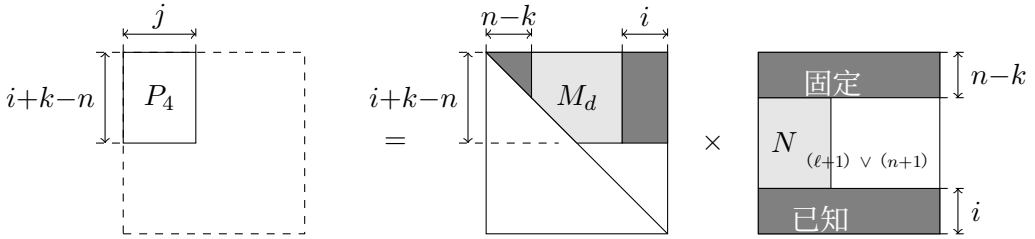


(b) 考虑到 M_d 是上三角矩阵

FIGURE 6. 命题1的证明，使用 P_3



（a）用于计算 P_4的 M_d 和 $N_{\ell\vee n}$ 部分



（b）考虑到 M_d 是上三角矩阵

FIGURE 7. 命题1的证明，使用 P_4

一次出现 P 最多可以与铺砌子数组 B的四个矩阵重叠。假设 P 的一次出现的左上角位于某个矩阵 $M_dN_{\ell\vee m}$ 中，其中整数ℓ 和 m 满足 $p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2}$ 以及 $q2^{kn/2} \leqslant m < (q+1)2^{kn/2}$。 $M_dN_{\ell\vee m}$ 右侧的矩阵和其下方的矩阵分别为 $M_dN_{(\ell+1)\vee m}$ 和 $M_dN_{\ell\vee(m+1)}$，其中 $\ell+1$ 和 $m+1$ 必须按模 $2^{kn/2}$ 理解，才能使其落在正确的区间内。设 P 中分别与矩阵$M_dN_{\ell\vee m}$、 $M_dN_{\ell\vee(m+1)}$、 $M_dN_{(\ell+1)\vee m}$ 和 $M_dN_{(\ell+1)\vee(m+1)}$重叠的部分为 P_1、 P_2、 P_3 和 P_4 。它们如图 10 所示。

若 $j = 0$，则该次出现的部分 P_2和 P_4为空。若 $i+k \leqslant n$，则该次出现的部分 P_3和 P_4也为空。最简单的情况是方程组 $M_d N_{\ell\vee m} = P$，其中 $i = j = 0$ 且 $k = n$。现在我们处理各部分均非空的一般情况；其他情况类似且更简单。

现在陈述方程组。未知数是矩阵 $N_{\ell\vee m}$ 中的元素。我们声称，可以根据矩阵 A_d 、数对 (i, j) 以及数组 P_1、 P_2、 P_3和 P_4 求出这些元素。如前所述，由于 $k = \ell \vee m$，矩阵 $N_{\ell\vee m}$ 的前 $n - k$ 行由子数组 B 固定。这部分在图4中以深灰色标出。

P_1 的高和宽分别为 $n - i$ 和 $n - j$。部分 P_1 是通过将矩阵 M_d 的最后 $n - i$ 行与矩阵 $N_{\ell\vee m}$ 的最后 $n - j$ 列相乘得到的（见图4a中的灰色部分）。现在我们利用矩阵 M_d 是上三角矩阵这一事实。这使得用于计算 P_1 的 M_d 和 $N_{\ell\vee m}$ 部分得以缩减（见图4b中的灰色部分）。此外，在 M_d 中使用的部分是一个对角线上为 1 的上三角矩阵。因此，该矩阵可逆。这意味着，可以将该三角矩阵的逆矩阵与 P_1 相乘，从而得到 $N_{\ell\vee m}$ 中的灰色部分。

P_2 的高度和宽度分别为 $n - i$ 和 j。部分 P_2 由矩阵 M_d 的最后 $n - i$ 行与矩阵 $N_{\ell\vee(m+1)}$ 的前 j 列相乘得到（见图5a中的灰色部分）。至于 P_1，由于矩阵 M_d 是上三角矩阵，因此用于计算 P_2 的 M_d 和 $N_{\ell\vee(m+1)}$ 部分得以缩减（见图5b中的灰色部分）。此外，M_d 中使用的部分再次是可逆的。这意味着 $N_{\ell\vee(m+1)}$ 中的灰色部分可以通过将该三角矩阵的逆矩阵与 P_2相乘得到。

我们断言， $N_{\ell\vee m}$ 的 $n - i$ 行由 $N_{\ell\vee m}$ 和 $N_{\ell\vee(m+1)}$中已知的部分确定。这是因为，对于整数 r 和 s， s 的最后 r 个二进制位决定了 $s+1$ 的最后 r 个二进制位；反过来， $s+1$ 的最后 r 个二进制位也决定了 s的最后 r 个二进制位。由此可知，四个矩阵 $N_{\ell\vee m}$、 $N_{\ell\vee(m+1)}$、 $N_{(\ell+1)\vee m}$ 和$N_{(\ell+1)\vee(m+1)}$ 的最后 i 行是已知的。这些部分在图5中以深灰色标出。

P_3 的高度和宽度分别为 $i + k - n$ 和 $n - j$。部分 P_3 由矩阵 M_d 的前 $i + k - n$ 行与矩阵 $N_{(\ell+1)\vee m}$ 的最后 $n - j$ 列相乘得到（见图6a中的灰色部分）。现在利用这样一个事实：$N_{(\ell+1)\vee m}$ 的前 $n-k$行和最后 i 行已知。这些行中的元素可视为方程组中的常数。结合这一结果，以及图6b中灰色的 M_d 的方形（$i + k - n$） $\times$ （$i + k - n$）子矩阵可逆这一事实，便可求出 $N_{(\ell+1)\vee m}$ 最后 $n - j$ 列中仍未知的元素。

P_4 的高度和宽度分别为 $i + k - n$ 和 j。采用与 P_3中非常相似的推理，可以求出矩阵 $N_{(\ell+1)\vee(m+1)}$ 的其余元素，见图7a和图7b。□

在命题1中，情形 $k = n$ 指出， $n = 2^d$ 的帕斯卡环面数组是一个嵌套的（n, n, n, n）-完美环面数组。这证明了定理 1。

3. Proof of Theorem 2

我们考虑一族最早在 [3] 中定义的矩阵。这些矩阵是通过对定义6中给出的矩阵 M_d 的列进行若干旋转得到的。

令 σ 为一个函数，它将每个字 $a_1 \cdots a_n$ 映射到通过将最后一个符号移至最前面而得到的 $a_n a_1 a_2 \cdots a_{n-1}$。由于 $\mathbb{F}_2$ 上的字被视为列向量，因此函数 σ 也可以应用于列向量。

定义 9（帕斯卡型矩阵）。令 d 为一个非负整数，并令 $n = 2^d$。令$m_0,\dots,m_{n-1}$为整数，使得 $m_{n-1} = 0$，且对于每个整数$0 \le i < n$， $m_{i+1} \le m_i \le m_{i+1} + 1$。令 $C_0,\dots,C_{n-1}$为 M_d的列，即 $M_d = (C_0,\dots,C_{n-1})$。定义

$$M_d^{m_0,\dots,m_{n-1}} = \big(\sigma^{m_0}(C_0),\dots,\sigma^{m_{n-1}}(C_{n-1})\big).$$

以下是八个可能的矩阵 $M^{m_0,\dots,m_{n-1}}_d$，对应于 $d = 2$ 和 $n = 2^2$。

$$M_2^{0,0,0,0} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M_2^{1,0,0,0} \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M_2^{1,1,0,0} \quad \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M_2^{2,1,0,0} \quad \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M_2^{1,1,1,0} \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad M_2^{2,1,1,0} \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad M_2^{2,2,1,0} \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \qquad M_2^{3,2,1,0} \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

矩阵 $M^{0,\dots,0}_d$正是定义6中的矩阵 M_d。不仅 $M^{0,\dots,0}_d$，定义 9 中的所有矩阵 $M^{m_0,\dots,m_{n-1}}_d$也具有这样的性质：顶部和右侧的所有方形子矩阵都是可逆的。

该结果的证明见 [3, 引理 4 和 5]。我们在下面列出它们。

引理 2（[3, 引理 4]）。设 d 为一个非负整数，且设 $n = 2^d$。令矩阵 M 为 $M^{m_0,\dots,m_{n-1}}_d$中的一个。设 ℓ 和 k 为两个整数，满足 $0 \le \ell < \ell + k \le n$。由 k 行 $\ell, \ell+1, \dots, \ell+k-1$ 以及 M的最后 k列 $n-k,\dots,n-1$ 构成的子矩阵是可逆的。

证明。注意，对于 $k = n$ 和 $\ell = 0$，引理陈述中的子矩阵就是整个矩阵 $M^{m_0,\dots,m_{n-1}}_d$，显然它是可逆的。根据引理 1，矩阵 M 的每个元素 $M_{i,j}$（其中 $0 < i < n$ 和 $0 \le j < n-1$）满足以下条件之一：若 $m_j = m_{j+1}$（列 C_j 的旋转次数与列 C_{j+1} 相同），则有 $M_{i,j} = M_{i-1,j} \oplus M_{i,j+1}$；若 $m_j = m_{j+1} + 1$（列 C_j 的旋转次数比列 C_{j+1} 多一次），则有 $M_{i,j} = M_{i-1,j} \oplus M_{i-1,j+1}$。

令 P 为引理陈述中的子矩阵：

$$M = \begin{pmatrix} \ell & \\ k & \boxed{P} \\ n-k & k \end{pmatrix} \begin{matrix} \updownarrow n \\ \\ \updownarrow n \end{matrix}$$

为了证明 P 可逆，我们应用变换将其化为三角形。注意，最后一列的所有元素都是 1。对 P 应用的第一个变换如下。行L_0 保持不变，而对于 $1 \le i < k$，将行 L_i 替换为 $L_i \oplus L_{i-1}$。除最上方的元素外，最后一列的所有元素都变为零。此外，每个元素 $P_{i,j}$ 都会根据数值 $m_j - m_{j+1}$被替换为 $P_{i,j+1}$ 或 $P_{i-1,j+1}$。还需注意，根据数值 $m_j - m_{j+1}$，新元素的值仍满足 $P_{i,j} = P_{i-1,j} \oplus P_{i,j+1}$ 或 $P_{i,j} = P_{i-1,j} \oplus P_{i-1,j+1}$。

对 P 应用的第二个变换如下。行 L_0 和 L_1 保持不变，对于 $2 \le i < k$，将每一行 L_i 替换为 $L_i \oplus L_{i-1}$。倒数第二列中，除最上方的两个元素外，其余元素现在都为零。在步骤 t 中，对于 $0 \le t < k$，行$L_0, \ldots, L_t$保持不变，对于 $t+1 \le i < k$，将每一行 L_i替换为 $L_i \oplus L_{i-1}$。对 $0 \le t < k$ 应用所有这些变换后，对于 $i + j = k - 1$，每个元素 $P_{i,j}$ 都满足 $P_{i,j} = 1$；对于 $i+j > k-1$，每个元素 $P_{i,j}$都满足 $P_{i,j} = 0$。由此可得，P 的行列式为 $\mathbf{1}$，且矩阵 P 可逆。□

设 $n = 2^d$，其中 $d \geqslant 1$，并令 M为矩阵 $M^{m_0,\ldots,m_{n-1}}_d$ 中的一个矩阵。我们引入此类矩阵 $M^{m_0,\ldots,m_{n-1}}_d$ 的上边界和下边界的概念。若元素 $M_{i,j}$满足 $0 \leqslant i$、$j < n$，则称其位于 M 的上边界（分别为下边界）中；如果对于所有 $k = 0$、...、$i-1$，都有 $M_{i,j} = 1$ 和 $M_{k,j} = 0$（分别对于所有 $k = i+1$、...、$n-1$）。例如，矩阵 $M^{0,\ldots,0}_d = M_d$ 的上边界是第一行，其下边界是主对角线。第 i 列中的上边界和下边界分别位于第 m_i 行和第 $m_i + i$ 行。

$$M_3^{3,3,2,1,1,1,0,0} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \underline{\mathbf{1}} & \mathbf{1} \\ 0 & 0 & 0 & \underline{\mathbf{1}} & \mathbf{1} & \mathbf{1} & 0 & 1 \\ 0 & 0 & \underline{\mathbf{1}} & 1 & 0 & 1 & 1 & 1 \\ \underline{\mathbf{1}} & \mathbf{1} & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & \underline{\mathbf{1}} & \mathbf{1} & \mathbf{1} & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & \underline{\mathbf{1}} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \underline{\mathbf{1}} & \mathbf{1} & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \underline{\mathbf{1}} \end{pmatrix}$$

FIGURE 8. M^3 的上边界和下边界以粗体显示,30 3 21110,,,,,。

Column i	0	1	2	3	4	5	6	7
Upper border m_i	3	3	2	1	1	1	0	0
Lower border $m_i + i$	3	4	4	4	5	6	6	7

矩阵 $M^{m_0,\ldots,m_{n-1}}_d$ 的两条边界都从第一列中唯一的元素 $\mathbf{1}$ 出发。上边界终止于最后一列最上方的元素，下边界终止于最后一列最下方的元素。上边界仅由向东步或东北步构成，下边界仅由向东步或向东南步构成。当 $m_j = m_{j+1}$ 时，上边界包含一条从第 C_j 列到第 C_{j+1} 列的向东步；当 $m_j = m_{j+1} + 1$时，则包含一条东北步。此外，每当上边界使用向东步（分别为东北步）从一列移至其右侧相邻列时，下边界就使用向东南步（分别为向东步）。这是因为第 i 列中，上边界与下边界之间的距离恰好为 i。由此，我们可以定义一个从 $\{0, \ldots, n-1\}$ 到 $\{0, \ldots, n-1\}$ 的函数 τ，如下所示。

$$\tau(i) = \begin{cases} m_i & \text{if either } i = 0 \text{ or } m_{i-1} = m_i + 1 \\ m_i + i & \text{otherwise, that is, } i > 0 \text{ and } m_{i-1} = m_i \end{cases}$$

$\tau(i)$ 的值是第 i 列上边界或下边界的行索引。根据函数 τ 的定义可得，$M_{\tau(i),i} = 1$ 和 $M_{\tau(i),j} = 0$ 对每个 $0 \leqslant j < i$ 均成立。

图8所示矩阵的函数 τ 的值如下。在图8中，与 τ 的值对应的边界上的 1 均已加下划线。注意，每行和每列中恰好各有一个带下划线的 1。

i	0	1	2	3	4	5	6	7
$\tau(i)$	3	4	2	1	5	6	0	7

函数 τ 是满射，因此也是双射，因为每一行中最左侧的 1 都位于上边界或下边界。因此，$\{0,\ldots,n-1\}$ 中的每个 j 都等于 $\tau(i)$，其中 i 是第 j 行中最左侧的 1 所在的列。

由于矩阵 $M^{0,\ldots,d}{}^{0}=M_d$具有对称性，引理 2 也适用于通过选取第一行从 $M^{0,\ldots,d}{}^{0}$ 中得到的子矩阵。由于其他矩阵 $M^{m_0,\ldots,d}{}^{m_{n-1}}$不再具有这种对称性，我们需要考虑对 $M^{0,\ldots,d}{}^{0}$中的列进行的旋转，以得到 $M^{m_0,\ldots,d}{}^{m_{n-1}}$。

引理 3（[3, 引理5]）。设 d 为非负整数，且设 $n=2^d$。令矩阵 M 为 $M^{m_0,\ldots,d}{}^{m_{n-1}}$ 中的一个。设 k 为满足 $1\le k\le n$的整数。由 k 个连续行和 k 个连续列构成、且右上角元素位于 M 上边界的 M的 $k\times k$-子矩阵是可逆的。

证明。设 P 为引理陈述中的子矩阵 M：

$$M=\left(\begin{array}{c} \begin{array}{cc} & \begin{array}{c}0\\0\\1\end{array}\\ k\updownarrow & \boxed{P} \\ & \underset{k}{\longleftrightarrow} \end{array} \\ \underset{n}{\longleftrightarrow} \end{array}\right)\updownarrow n$$

我们对子矩阵 P 进行变换，使其成为一种便于计算行列式的形式。为固定记号，假设子矩阵 P 是通过选取行 L_r、...、L_{r+k-1} 以及列 C_s、...、C_{s+k-1} 得到的。假设 $M_{r,s+k-1}$ 这一元素位于 M 的上边界上。注意，M 和 P 的上边界在 P 内重合。我们用 j_0、...、j_t 表示 P 中原先由上边界的东北步确定的、取值为 0、...、$k-1$ 的那些列的索引。这意味着 j_0、...、j_t 是满足 $m_{s+j-1}=m_{s+j}+1$ 的索引序列 j。按照惯例，令 $j_0=0$，即 P 第一列的索引。

对矩阵 P施加的第一个变换如下。列 $C_0,\ldots,C_{j_t-1}$和 C_{k-1} 保持不变，并将每一列 C_j（其中 $j_t\le j<k-1$）替换为 $C_j\oplus C_{j+1}$。除最右侧元素外，第一行的所有元素都变为零。此外，将每个元素 $P_{i+1,\ j}$（其中 $j_t\le j<k-1$）替换为 $P_{i,\ j}$。对矩阵 P施加的第二个变换如下。列 $C_0,\ldots,C_{j_{t-1}-1}$和 C_{k-2},C_{k-1} 保持不变，并将每一列 C_j（其中 $j_{t-1}\le j<k-2$）替换为 $C_j\oplus C_{j+1}$。第一行保持不变，第二行除最后两个元素外的所有元素都变为 0。我们依次使用 $j_t,j_{t-1},\ldots,j_0$，总共施加 $t+1$次这样的变换。随后再进行 $k-t$ 步，得到对于每一行 i，除最后 i 个元素外，其余元素都变为 0。

应用所有这些变换后，对于 $i+j=k-1$，每个元素 $P_{i,\ j}$ 都满足 $P_{i,\ j}=1$；对于 $i+j<k-1$，每个元素 $P_{i,\ j}$ 都满足 $P_{i,\ j}=0$。由此可知，P的行列式为 1，且矩阵 P 可逆。□

我们通过考察类帕斯卡矩阵族来定义仿射环面数组 es.

定义 10（仿射环面数组）。设 d 是一个非负整数，并设 $n = 2^d$。设 M 是任意一个大小为 $n \times n$ 的帕斯卡型矩阵（定义 9）。设 N_0、……、$N_{2^{n^2}-1}$ 是 $\mathbb{F}_2$（定义 7）上所有 $n \times n$ 矩阵的枚举，并设 Z 是 $\mathbb{F}_2$ 上任意一个 $n \times n$ 矩阵。

大小为 $n2^{n^2/2} \times n2^{n^2/2}$ 的数组 A 若满足以下条件，则称其为（n，n，n，n）-仿射：对于每个满足 $0 \leqslant k < 2^{n^2}$ 的整数 k，矩阵 $MN_k \oplus Z$ 都放置在 A 中，且其左上角单元格位于位置 (odd(k)n, even(k)n)。

由于每个矩阵 $M = M^{m_0, \ldots\ldots, m_{n-1}}_d$ 都是可逆的，因此每个矩阵 Z 都等于某个矩阵 Z' 的 MZ'。

对于数组 Z，我们用 $(Z)^{(n\times n)}$ 表示由 n^2 个 Z、n 行和 n 列组成的数组。下一个结果表明，任何嵌套完美数组都可以转换为另一个大小相同、但上角的矩阵为 0 的嵌套完美数组。

在下文中，我们对 $\mathbb{F}_2$ 中的子数组使用运算 $\oplus$，表示元素矩阵的通常的和。

引理 4。设 d 为非负整数。固定 $n = 2^d$。设 A 为大小为 $n2^{n^2/2} \times n2^{n^2/2}$ 的数组，设 Z 为大小为 $n \times n$ 的数组。那么，当且仅当 $A \oplus (Z)^{2^{n^2/2}\times 2^{n^2/2}}$ 是嵌套（n，n，n，n）-完美环面数组时，A 是嵌套（n，n，n，n）-完美环面数组。

证明。设 $A' = A \oplus (Z)^{2^{n^2/2}\times 2^{n^2/2}}$。设 ℓ 为满足 $1 \leq \ell \leq n$ 的整数，并设 L 是 A 的一个大小为 $n2^\ell \times n2^\ell$、起始位置与 (0, 0) 同余的对齐子数组。A' 在相同位置处的对应子数组 L' 为 $L' = L \oplus (Z)^{(2^\ell \times 2^\ell)}$。

首先，假设 A 是嵌套的 (n,n,n,n)-完美数组。那么，L 是嵌套的 (ℓ,ℓ,n,n)-完美数组。设 i，j 满足 $0 \leq i,j < n$，并设 T 是 $(Z)^{(2\times 2)}$ 中一个大小为 $\ell \times \ell$、起始位置为 (i,j) 的子数组。令 U' 为任意一个大小为 $\ell \times \ell$ 的数组。那么，数组 $U = U' \oplus T$ 在数组 L 中恰好出现一次，其位置 (i',j') 模 (n,n) 与 (i,j) 同余。因此，$U' = U \oplus T$ 在 L' 中的同一位置 (i',j') 出现。由于每个矩阵 U 对于每个可能的 (i,j) 都有这样的出现。由于 L' 的大小为 $n2^\ell \times n2^\ell$，L'，它是一个嵌套的 (ℓ,ℓ,n,n)-完美数组。

如果 A 不是嵌套(n,n,n,n)-完美的，则存在一个见证 ℓ，$1 \leq \ell \leq n$，以及一个大小为 $n2^\ell \times n2^\ell$ 的子数组 L，它在同一同余类中的位置出现两次。用与前一种情况类似的论证，很容易验证 A' 中存在一个子数组 L'，它在 A' 中同一同余类的位置出现两次。□

现在我们可以证明仿射数组是嵌套完美数组。

命题 2. 设 d 为一个非负整数，且设 $n = 2^d$。每个(n,n,n,n)-仿射数组都是一个嵌套(n,n,n,n)-完美数组。

证明。根据引理 4，可以假设仿射数组的定义中的数组 Z 是零矩阵。设 M 是矩阵 $M^{m_0,\ldots,m_{n-1}}_d$ 之一。假设 A 是由 M 和零矩阵定义的 (n,n,n,n)-仿射数组。命题的证明沿用命题1的证明，但此处考虑矩阵 $M = M^{m_0,\ldots,m_{n-1}}_d$，而不是帕斯卡矩阵 $M^{0,\ldots,0}_d$。设 k 是一个满足 $1 \leq k \leq n$ 的整数。设 B 是 A 的一个大小为 $n2^{kn/2} \times n2^{kn/2}$ 的对齐子数组。B 的左上角坐标为 $pn2^{kn/2}$ 和 $qn2^{kn/2}$ 的形式，其中 p 和 q 是满足 $0 \leqslant p, q < 2^{(n-k)n/2}$ 的两个整数。这意味着

子数组 B 被矩阵 $MN_{\ell\vee m}$ 平铺，其中 ℓ 且 t 满足

$$p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2} \text{ and } q2^{kn/2} \leqslant t < (q+1)2^{kn/2}.$$

所有满足条件的整数 ℓ 的二进制展开

$$p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2}$$

以相同的 $2^{n(n-k)/2}$ 个二进制位开头；对于所有满足条件的整数 t，情况也相同

$$q2^{kn/2} \leqslant t < (q+1)2^{kn/2}.$$

这意味着 $\ell \vee m$ 以相同的 n（$k-n$）位开头。由于 $\ell \vee m$ 的前几位放在长度为 n 的 $N_{\ell\vee m}$ 的前几行中，因此对于各自区间内的 ℓ 和 t，所有矩阵 $N_{\ell\vee m}$ 的前 $n-k$ 行都相同。

设 (i,j) 为一对满足 $0 \leqslant i,j < n$ 的整数，并设 P 为一个大小为 $k \times n$ 的数组。我们断言， P 在 B 中恰好出现一次，且该出现位置与 (i,j) 模 (n,n) 同余。为证明这一点，我们说明， P 恰好出现一次，当且仅当某个线性方程组有解。此外，该方程组的解给出矩阵 $N_{\ell\vee m}$，进而确定整数 ℓ 和 m，它们又给出 P 在子数组 B 中出现的位置。一次出现 P 最多可以与铺砌子数组 B 的四个矩阵重叠。

假设 P 的出现的左上角位于某个矩阵 $MN_{\ell\vee m}$ 中，其中整数 ℓ 和 m 满足 $p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2}$ 且 $q2^{kn/2} \leqslant m < (q+1)2^{kn/2}$。 $MN_{\ell\vee m}$ 右侧的矩阵和其下方的矩阵分别为 $MN_{(\ell+1)\vee m}$ 和 $MN_{\ell\vee(m+1)}$，其中 $\ell+1$ 和 $m+1$ 必须按模 $2^{kn/2}$ 理解，才能使其保持在正确的区间内。设 P_1、 P_2、 P_3 和 P_4 是 P 中分别与矩阵 $MN_{\ell\vee m}$、 $MN_{\ell\vee(m+1)}$、 $MN_{(\ell+1)\vee m}$ 和 $MN_{(\ell+1)\vee(m+1)}$ 重叠的部分。如图 10 所示。

若 $j=0$，则该出现中的部分 P_2 和 P_4 为空。这是一个退化情形，因此我们只处理 $j \geqslant 1$ 的情形。根据 $i+k \leqslant n$ 是否成立，分为两种主要情形。

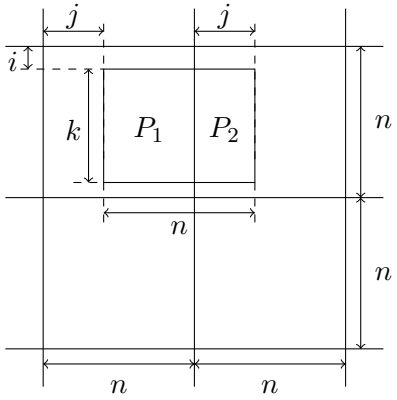


FIGURE 9. 数组 B 在 A 中的一次出现，具有 $i+k \leqslant n$。

假设 $i+k \leqslant n$。那么，部分 P_3 和 P_4 不存在，而 P的出现可化简为 P_1 和 P_2。考虑 P_1 中出现的一列，也就是矩阵 $MN_{\ell\vee m}$ 中索引为 s 且大于 j 的那一列，该列从第 $i+1$ 行到第 $i+k$ 行。这一列由 M中从 $i+1$ 行到 $i+k$ 行的各行与 $N_{\ell\vee m}$中索引为 s的列相乘得到。

注意，后者的前 $n-k$ 个元素已知，可以视为常数。因此，矩阵 $N_{\ell\vee m}$ 中列 s 的其余 k 个元素就是下列方程组的解： $y = Mx$，其中 y 是 P_1的列， M 是由 M 中从 i 行到 $i+k-1$ 行以及从第 $n-k$ 列到第 $n-1$ 列构成的 $k\times k$ 矩阵，而 x 是 $N_{\ell\vee m}$的 k 个元素。根据引理 2，矩阵 M可逆，因此该方程组有唯一解。这意味着可以求出 $N_{\ell\vee m}$ 中索引为 s 的列的 k 个元素。对 P_2中的一列进行类似推理，可以求出一列 s，其具有 $N_{\ell\vee(m+1)}$ 的 $s\leqslant j$，因而也具有 $N_{\ell\vee m}$的 $s\leqslant j$。

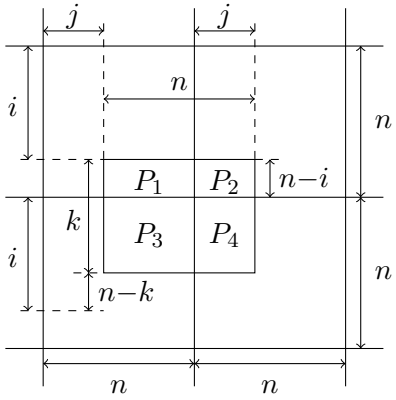


FIGURE 10. 数组 B 在 A 中出现，且具有 $i+k>n$。

现在假设 $i+k>n$，并进一步明确如何从 P在模 (i,j) 下的出现计算矩阵 $N_{\ell\vee m}$。回顾一下， $N_{\ell\vee m}$的顶部 $n-k$ 行，即第 0 行至第 $n-k-1$ 行，由子数组 B确定。设 $N_{\ell\vee m}$ 中尚未知的行的索引为 $n-k,\dots,n-1$。这 k 个剩余行的计算分两个阶段进行。第二阶段和第一阶段分别计算第 $n-k,\dots,r-1$ 行和第 $r,\dots,n-1$ 行，其中满足 $n-k\leqslant r\leqslant n-1$ 的切割索引 r 定义如下。整数 r 是使得所有整数 $\tau(r)\dots,\tau(n-1)$ 都属于 $\{0,\dots,i+k-n-1\}\cup\{i,\dots,n-1\}$ 的最小整数。注意， $\{0,\dots,i+k-n-1\}$ 是穿过 P_3P_4 的行的索引，而 $\{i,\dots,n-1\}$ 是穿过 P_1P_2 的行的索引。如果 $r=n-k$，则所有 k 行 $n-k,\dots,n-1$ 都由第一阶段计算，第二阶段为空。

我们更精确地描述第一阶段。设 s是满足 $r\leqslant s\leqslant n-1$的整数，并假设行 $s+1,\dots,n-1$已知，而行 s仍未知。行 s的元素按索引从最右侧的 $n-1$到最左侧的 0 依次计算。考虑矩阵 M中的行 $\tau(s)$。根据 τ的定义，元素 $M_{\tau(s),\,s}$等于 1，而对于 $s'<s$，元素 $M_{\tau(s),\,s'}$ 等于 0。根据 $\tau(s)$属于 $\{0,\dots,i+k-n-1\}$还是 $\{i,\dots,n-1\}$，我们分两种情况讨论。

假设 $\tau(s)$ 属于 $\{i,\dots,n-1\}$。设 t为一个整数，使得 $j\leqslant t\leqslant n-1$。将 M 中的行 $\tau(s)$与 $N_{\ell\vee m}$ 的列 t 相乘，得到 P_1 中的元素 $(\tau(s)\ t)$，也就是 P 中的元素 $(\tau(s)-i,t-j)$。M 中行 $\tau(s)$ 的性质，以及 $N_{\ell\vee m}$ 中行 r 以下的各行均已知这一事实，使我们能够计算 $N_{\ell\vee m}$ 中的元素 (s,t)。设 t 为一个整数，使得 $0\leqslant t<j$。将 M 中的行 $\tau(s)$与 $N_{\ell\vee m+1}$ 的列 t 相乘，得到 P_2 中的元素 $(\tau(s)\ t)$，也就是 P 中的 $(\tau(s)-i,t+n-i)$。

M 中行 $\tau(s)$ 的性质，以及 $N_{\ell\vee m}$ 中行 s 以下的各行均已知这一事实，使我们能够求出 $N_{\ell\vee(m+1)}$ 中的元素 (s,t)。由于对于 $N_{\ell\vee m}$ 的 $j \leqslant t \leqslant n-1$，所有元素 (s,t) 均已知；对于 $N_{\ell\vee(m+1)}$ 的 $0 \leqslant t < j$，所有元素 (s,t) 均已知；而且 $N_{\ell\vee m}$ 中行 s 以下的各行也都已知，因此 $N_{\ell\vee m}$ 的第 s 行已知。

现在假设 $\tau(s)$ 属于 $\{0,\dots,i+k-n-1\}$。使用矩阵$N_{(\ell+1)\vee m}$ 和 $N_{(\ell+1)\vee(m+1)}$ 以及 P 的部分 P_3 和 P_4，通过相同的推理，我们可以计算出 $N_{(\ell+1)\vee m}$的第 s 行，从而得到 $N_{\ell\vee m}$的第 s 行。

最后，我们描述第二阶段。子数组 B确定了第 0 至 $n-k-1$ 行，而第一阶段已计算出第 r 至 $n-1$ 行。第 $n-k$ 至 $r-1$ 行仍然未知。我们假设 $n-k<r$，否则就没有未知行。根据 r 的定义，整数 $\tau(r-1)$ 因而只能是 $i+k-n$ 或 $i-1$。假设 $\tau(r-1) = i-1$，另一种情况类似。考虑矩阵 M'，它是一个 $(k+r-n)\times(k+r-n)$ 矩阵，由矩阵 M 中第 $i-r$ 至 $i+k-n-1$ 行和第 $n-k$ 至 $r-1$ 列选取得到。M' 的右上角元素是 M 的元素 $(i-r,r-1)$。由于 $\tau(r-1) = i-1$，且第 $r-1$ 列中上边界与下边界之间的距离为 $r-1$，元素 $(i-r,r-1)$ 位于 M 的上边界上。根据引理3，矩阵 M' 可逆。注意，M' 中选取的行仍是 P 中尚未使用的行，而选取的列对应于 $N_{\ell\vee m}$ 中仍然未知的行。M' 的可逆性使我们能够计算出 $N_{\ell\vee m}$的第 $n-k$ 至 $r-1$ 行。至此，定理得证。□

下一个引理计算 (n,n,n,n)-仿射数组的数量。

命题 3. 设 d 是非负整数，并设 $n = 2^d$。那么，存在 2^{n^2+n-1} 个 (n,n,n,n)-仿射数组。

证明。恰好有 2^{n-1} 个矩阵 $M^{m_0,\dots,m_{n-1}}$。事实上，序列 $m_0,\dots,m_{n-1}$ 完全由序列 $m_0-m_1,\dots,m_{n-2}-m_{n-1}$ 决定，其中包含取值于 $\{0,1\}$ 的 $n-1$ 个差。矩阵 Z 在 $\mathbb{F}_2^{n\times n}$ 中也有 2^{n^2} 个可能的取值。这证明了 (n,n,n,n)-仿射数组的数量至多为 2^{n^2+n-1}。

剩下的工作是证明：由不同的两对 (M,Z) 和 (M',Z') 得到的两个 (n,n,n,n)-仿射数组确实不同。设 $N_0,\dots,N_{2^{n^2}-1}$ 是在 $\mathbb{F}_2$ 上的所有 $n\times n$ 个矩阵的枚举。设 M 和 M' 是形如 $M^{m_0,\dots,m_{n-1}}$ 的两个矩阵。设 Z 和 Z' 是两个 $n\times n$ 矩阵 $\mathbb{F}_2$。设 $U_i = N_i \oplus Z$ 和 $U_i' = N_i \oplus Z'$ 满足 $i = 0,\dots,2^n-1$。设 W 和 W' 是两个放置，定义如下：对于满足 $0 \leqslant i \leqslant 2^{2^n}-1$ 的每个整数 i，将矩阵 MU_k 放置在 W 中，使其左上角单元格位于位置（odd(i)n, even(i)n）。类似地，对于 W'，用 U_i' 替代 U_i。我们声称，如果 $W = W'$，那么 $M = M'$ 和 $Z = Z'$。假设 $W = W'$。由于根据引理 2，矩阵 M 和 M' 都是可逆的，因此 MU_i（分别为 $M'U_i'$）是零向量，当且仅当 U_i（分别为 U_i'）是零向量，也就是说，$Z = W_i$（分别为 $Z' = W_i$）。这意味着 $Z = Z'$，从而对于 $i = 0,\dots,2^n-1$，有 $U_i = U_i'$。注意，矩阵 U_i 遍历所有可能的 $n\times n$ 个矩阵。如果对于所有 $i = 0,\dots,2^n-1$ 都有 $MU_i = M'U_i$，那么 $M = M'$。□

对于 d 一个非负整数以及 $n = 2^d$ 定义 10 给出了一种（n，n，n，n）-仿射数组的构造方法。命题 3 计算了可以构造出的数组数量，并证明它们各不相同。由此完成了定理 2 的证明。

Acknowledgements.

两位作者均为 SINFIN实验室的成员，该实验室隶属于巴黎大学/法国国家科学研究中心—布宜诺斯艾利斯大学/CONICET。本研究获得阿根廷国家科学技术促进局资助，项目编号为 PICT 2018-2315。

References

[1] N. Alvarez、V. Becher、P. A. Ferrari 和 S. Yuhjtman。完美项链。 *Adv. in Appl. Math.*，80 61，2016 48：–。[2] Roland Bacher 和 Robin Chapman。模

p European Journal of 对称 *Combinatorics* 25 4 459 473, 2004
帕斯卡矩阵。，( )：–。算术与组合。[3] V. Becher 和 O. Carton。正规数与完美项链。 *Journal of Complexity*，54，2019。[4] F.R.K Chung、P Diaconis 和 R.L Graham。组合结构的通用循环。 *Discrete math.*，110 43 59，1992：–。[5] T. Etzion。完美映射和伪随机阵列的构造。 *IEEE Trans. Inform. Theory*，34(5, part 2):1308–1316，1988。[6] C. T. Fan、S. M. Fan、S. L. Ma 和 M. K. Siu。关于德布鲁因阵列。 *Ars Combin.*，19(A):205–213，1985。[7] H. Faure。与 ′数列 ′相 `关的`差异估计（在 ′维 *s*中）。 *Acta Arithmetica*，41 1982，。[8] B. Gordon。关于完美映射的存在性（通信）。 *IEEE Transactions on Information Theory*，12 4 486 487，1966 ( )：–。[9] M. Horv ′áth 和 A. Iv ′anyi。构造不断增大的完美立方体。 *Discrete Math.*，308(19):4378–4388，2008。[10] G. Hurlbert 和 G. Isaak。关于德布鲁因环面问题。 *J. Comb. Theory, Ser. A*，64(1):50–62，1993。[11] M. B. Levin。关于正规数的差异估计。 *Acta Arithmetica*，88(2):99–111，1999。[12] S. L. Ma。关于具有某种窗口性质的二进制阵列的注记。 *IEEE Trans. Inform. Theory*，30(5):774–775，1984。[13] D. A. Makarov 和 A. D. Yashunski

˘ *Diskretn.* ı。 *Anal. Issled. Oper.* 26 2 98 114, 2019
关于易解码子德布鲁因阵列的一种构造。，( )：–。[14] K. Paterson。完美映射。 *IEEE Trans. Inform. Theory*，40(3):743–753，1994。[15] I. S. Reed 和 R. M. Stewart。关于完美映射存在性的注记。 *IRE Trans. on Information Theory*，IT-8:10–12，1962。[16] J. H. van Lint、F. J. MacWilliams 和 N. J. A. Sloane。关于伪随机阵列。 *SIAM Journal on Applied Mathematics* 36 1 62 72, 1979 ，( )：–。

Ver ′onica Becher 计算系，精确与自然科学学院 & ICC 布宜诺斯艾利斯大学 & CONICET，阿根廷 vbecher@dc.uba.ar

Olivier Carton 基础计算机科学研究所 巴黎西岱大学，法国 Olivier.Carton@irif.fr