NESTED PERFECT ARRAYS

VERÓNICA BECHER AND OLIVIER CARTON

Abstract. We introduce two-dimensional periodic arrays that are a variant of the de Bruijn tori. We call them nested perfect arrays. Instead of asking that every array of a given size has exactly one occurrence, we partition the positions in congruence classes and we ask exactly one occurrence in each congruence class. We also ask that this property applies recursively to each of the subarrays. We give a method to construct nested perfect arrays based on Pascal triangle matrix modulo 2. For the two-symbol alphabet, and for n being a power of 2, our method yields 2^{n^2+n-1} different nested perfect arrays allocating all the different $n \times n$ arrays in each congruence class that arises from taking the line number modulo n and the column number modulo n.

Keywords: de Bruijn tori, nested perfect necklaces, Pascal triangle
Mathematics Subject Classification: 05B05, 11C20
CCS: Mathematics of computing, Discrete mathematics, Combinatorial problems

1. Introduction, definitions and statement of results

An array of size $n \times n$ is a periodic array where the line numbers are considered modulo n and the column numbers are considered modulo n. Here we consider arrays of symbols in a finite alphabet. The problem of constructing arrays of minimal size that allocate a given family of smaller arrays goes back to the 1960s, see for instance [9, 15]. The constructions of arrays where each member of the family occurs exactly once generalize the classical unidimensional de Bruijn sequences to two dimensional arrays, and they are known as de Bruijn tori or perfect maps. There has been significant effort in solving the problem of determining the existence of these arrays for the different subarrays sizes, and in giving construction methods, for instance the work of [13, 7, 11, 5, 14, 4]. The first achievements focus on arrays of 0s and 1s. Subsequent work solves the existence problem and the construction problem for arbitrary alphabets. There is also work on constructions for three dimensional arrays [10].

In this note we introduce a variant of the de Bruijn tori. We call them *nested perfect arrays.* Instead of asking that every array of a given size has exactly one occurrence, we partition the positions in congruence classes and we ask exactly one occurrence in each congruence class. We also ask that this property applies recursively to the subarrays.

Nested perfect arrays are the two-dimensional version of the work done by the authors in the unidimensional case, that they call *nested perfect necklaces* [3]. Their graph theoretic characterization uses graphs $G(n, k)$ which are the tensor product of the de Bruijn graph of order n and a simple cycle of length k. The *perfect necklaces* for blocks length n and k many congruence classes, called (n, k)-perfect necklaces [1], correspond to the Hamiltonian cycles in these graphs, which are exactly the Eulerian cycles in $G(n-1, k)$. Nested (n, k)-perfect necklaces are recursively defined as the concatenation of b many of nested $(n-1, k)$-perfect necklaces, unless $n = 1$, where b is the alphabet size. Thus, nested (n, k)-perfect necklaces

Date: May 28, 2024.

correspond to those Eulerian cycles in $G(n-1,k)$ which are the concatenation of b many Hamiltonian cycles. In turn, these Hamiltonian cycles satisfy the nesting property.

Here we present the definition of nested perfect arrays for arbitrary alphabets together with a method of constructing a large family of them for the binary alphabet. This is based on the method of constructing nested (n,n)-perfect necklaces, when n is a power of 2 and uses a simple $n \times n$ matrix related to Pascal triangle modulo 2. We require that n be a power of 2. The construction of nested perfect arrays for $n \times n$ matrices and $n \times n$ congruence classes is a tiling of an array of size $n2^{n^2/2} \times n2^{n^2/2}$ with all the different nested perfect $n \times n$ arrays. The technical challenge is to prove that such a tiling exists and to exhibit it. This is proved in Theorem 1 and the construction is very efficient. Theorem 2 gives a method of constructing 2^{n^2+n-1} many nested perfect arrays for for $n \times n$ matrices and $n \times n$ congruence classes.

The recent book [6] gives properties, constructions, and applications for one dimensional and two dimensional de Bruijn arrays. The ability to recover efficiently any given subarray receives special attention. With the exception of those applications where you need exactly one occurrence of each pattern such as coding, if you solve a problem with a two dimensional de Bruijn array you can also solve it with a nested perfect array. Locating a position in a large area given a window in the array and a congruence class can be done in time linear to the window size, because, as we show in the proof of Theorem 1, it is just to solve a linear system of equations. Also nested perfect arrays can be used for recovering the surface of objects by projecting structured-light patterns that are windows of the nested perfect array, adapting the work in [16].

There are advantages and disadvantages for using nested perfect arrays instead de Bruijn arrays. A disadvantage is that n must be a power of 2, while in the de Bruijn case it can be any number. An advantage is that nested perfect arrays have very low discrepancy, which means that the distribution of symbols and subarrays is close to uniform distribution. This is a distinctive feature of nested perfect arrays that makes them particularly well suited for structure-light-patterns.

In the one dimensional case the discrepancy of a sequence is the maximum, among all substrings of the sequence, of the difference between the number of occurrences of the symbol that occurs the most and the one that occurs the least. The block-discrepancy of a sequence is similar, but instead of considering symbols it considers all blocks of a given size, and the occurrences are computed in the circular sequence. The sequences with the least known block-discrepancy are the nested perfect necklaces [12, 3]. Discrepancy in two dimensions is defined similarly: the discrepancy of an array with respect to a size $p \times q$, is the maximum difference between the number of of occurrences of the $p \times q$ matrix that occurs the most and the one that occurs the least, in all subarrays of the array. Nested perfect arrays, for $n \times n$ matrices and $n \times n$ congruence classes, when n is a power of 2, have the distinctive property of having a very low discrepancy with respect to all square sizes.

1.1. **The definition of nested perfect arrays.** Along the sequel we number the lines and columns starting at 0 (instead of starting at 1). For any two-dimensional array A the subarray of size $n \times n$ at position (k,ℓ) is the array made of the lines from k to $k+n-1$ and the columns from ℓ to $\ell+n-1$ where all these indices are taken modulo the number of lines and columns of A. Note that $(0,0)$ is the position of the upper left corner of each array because lines and columns are numbered starting from 0.

A *modulo* is a pair of positive integers written (p,q). The positions of any given array are partitioned into pq residue classes according to their respective residue classes modulo p and modulo q: Thus, the modulo $(1, 1)$ yields a single class containing all the positions, and the modulo $(2, 2)$ partitions the positions in four classes.

An array of size $n \times n$ *occurs* at position (k, ℓ) in an array if it is equal to the subarray of size $n \times n$ at position (k, ℓ).

Definition 1 (Perfect array)**.** *An array A is* perfect *for window size $s \times t$ and modulo (p, q), abbreviated (s, t, p, q)-perfect, if each $s \times t$ array has exactly one occurrence in A in each residue class modulo (p, q).*

Then, in an $(s, t, 1, 1)$-perfect array each $s \times t$ array has exactly one occurrence. Figure 1 gives an example of a $(2, 2, 1, 1)$-perfect array and two $(2, 2, 2, 2)$-perfect arrays. In the leftmost, each 2×2 array occurs exactly once. In the other two, each 2×2 array occurs exactly four times, with one occurrence in each residue class modulo $(2, 2)$.

Definition 2 (Aligned subarray)**.** *Given an array A, a subarray of size $k \times \ell$ is* aligned *if its position (i, j) in A satisfies that k divides i and ℓ divides j.*

Definition 3 (Subdivision)**.** *If both k and ℓ divides n, a $k \times \ell$-*subdivision *of an array of size $n \times n$ yields $k\ell$ aligned subarrays, each of size $n/k \times n/\ell$.*

Definition 4 (Nested perfect array)**.** *Assume a b-symbol alphabet. A perfect array A is* nested *for window size $s \times t$ and modulo (p, q), abbreviated* nested (s, t, p, q)-perfect*, if for each $k = 0, \dots, s-1$, each aligned subarray of the $b^{kt/2} \times b^{kt/2}$ subdivision of A is $(s-k, t, p, q)$-perfect.*

Notice that (f, g, p, q)-perfect implies (f', g', p, q)-perfect for $1 \leq f' \leq f$ and $1 \leq g' \leq g$. The reverse implication may not be true. Definition 4 asks that the subdivisions yields $(s-k, t, p, q)$-perfect subarrays instead of $(s-k, t-k, p, q)$-perfect, as it could be expected. Our motivation is that we have a construction method that ensures the stronger property. There are other natural options for the definition of a nested perfect array. For non square arrays such definitions are not equivalent to each other, but they all coincide for square arrays. In this work we are interested in the square case.

Consider a (n, n, n, n)-perfect array in the b-symbol alphabet. Its size is $nb^{n^2/2} \times nb^{n^2/2}$ for n even. For $k = 0, \dots, n-1$, each part of its $b^{kn/2} \times b^{kn/2}$ subdivision has size $nb^{n(n-k)/2} \times nb^{n(n-k)/2}$.

For square arrays the definition of nested perfect arrays can be rephrased as follows.

Definition 5 (Square nested perfect array)**.** *Assume a b-symbol alphabet. An (n, n, n, n)-perfect array is* nested *if, for $k = 1, \dots, n$, each aligned subarray of size $nb^{nk/2} \times nb^{nk/2}$ is (k, n, n, n)-perfect.*

For $b = 2$ and $n = 4$: an array A of size 1024×1024 is a nested $(4, 4, 4, 4)$-perfect array if

- A is a $(4, 4, 4, 4)$-perfect array;
- each 256×256 aligned subarray is a $(3, 4, 4, 4)$-perfect array;
- each 64×64 aligned subarray is a $(2, 4, 4, 4)$-perfect array;
- each 16×16 aligned subarray is a $(1, 4, 4, 4)$-perfect array.

The leftmost two arrays in Figure 1 above are not nested perfect: The leftmost one is not nested because its left upper 2×2 subarray has 2 occurrences of the 1×2 array $[0, 1]$ but no occurrence of the 1×2 array $[0, 0]$. The middle array in Figure 1 is not a nested $(2, 2, 2, 2)$-perfect array because its left upper 4×4 subarray contains more 0s than 1s. The rightmost array is a nested $(2, 2, 2, 2)$-perfect array.

$$\begin{array}{cccc}
0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0
\end{array}$$

(a) Not nested
$(2,2,1,1)$-perfect

$$\begin{array}{cccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1
\end{array}$$

(b) Not nested
$(2,2,2,2)$-perfect

$$\begin{array}{cccccccc}
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1
\end{array}$$

(c) Nested
$(2,2,2,2)$-perfect

Figure 1. Examples of perfect arrays

Array size for nested (n,n,n,n)-perfect, $n = 2^d$	Window size	Modulo
$(b^{n\times n/2} \times n) \times (b^{n\times n/2} \times n)$	$n \times n$	(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. Subdivisions sizes and window sizes

1.2. **Two theorems.** The following is the main result in the present note. It states the existence of nested perfect arrays of 0s and 1s when all parameters are equal to the same power of 2.

Theorem 1. *For every integer $n \geqslant 2$ that is a power of 2, there exist nested (n,n,n,n)-perfect arrays of 0 and 1s.*

Our construction method does not yield just one instance, but many. The next result, Theorem 2, gives the exact number of different instances obtainable with our method.

Theorem 2. *There is a construction method that, for each integer n that is a power of 2, yields 2^{n^2+n-1} different nested (n,n,n,n)-perfect arrays of 0 and 1s.*

We do not know if there are more.

2. Proof of Theorem 1

We assume that the alphabet is the two element field $\mathbb{F}_2 = \{0,1\}$. We shall use matrices of elements in $\mathbb{F}_2 = \{0,1\}$, do matrix multiplication and matrix summation. The component-wise sum of elements in $\mathbb{F}_2$ is denoted by the symbol $\oplus$. Matrices are named with the letters M, N, P, Q with sub-indices and super-indices. When we depict a matrix we draw the surrounding black parenthesis outside. The outcome of the construction in each case is an array of $0s$ and 1s obtained by tiling with the above mentioned matrices. We name the arrays with letters A, B, C and when we draw them we do not put the surrounding black parenthesis outside.

We start by defining the following family of matrices.

Definition 6. *We give an inductive definition of the matrix M_d of elements in $\mathbb{F}_2$, of size $2^d \times 2^d$, for each $d \geq 0$ by*

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

Thus, the matrices M_1 and M_2 are

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

For every d, the matrix M_d is upper triangular, that is $(M_d)_{i,j} = 0$ for $0 \leqslant j < i < 2^d$. The following lemma states that the upper part of the matrix M_d is the beginning of the Pascal triangle modulo 2 also known as the Sierpiński triangle. The proof is a simple induction on d and can be found in [3, Lemma 3].

The matrix M_d is almost the one used by M. Levin in [12, Theorem 2] because we have reversed the order of the columns. The Pascal triangle matrix has been previously used by H. Fauré [8] for the construction of uniformly distributed sequences of real numbers.

Lemma 1 ([3, Lemma 3])**.** *For all integers d, i, j such that $d \geqslant 0$ and $0 < i < 2^d$ and $0 \leqslant j < 2^d - 1$, $(M_d)_{i,j} = (M_d)_{i-1,j} \oplus (M_d)_{i,j+1}$.*

Proof. To facilitate the review we include the proof already given in [3, Lemma 3]. The proof is carried out by induction on d. For $d = 0$, the result is trivially true because there are no such i and j. For $d = 1$, the result trivially holds. Suppose that the result holds for M_d and let i, j be integers such that $0 < i < 2^{d+1}$ and $0 \leq j < 2^{d+1} - 1$. If $i \neq 2^d$ and $j \neq 2^d - 1$, the three entries $(M_{d+1})_{i,j}$, $(M_{d+1})_{i-1,j}$ and $(M_{d+1})_{i,j+1}$ lie in the same quarter of the matrix M_{d+1} and the result follows from the inductive hypothesis. Otherwise, the result is a consequences the following facts. For each integer $d \geq 1$, the entry $(M_d)_{i,j}$ is equal to 1 if either $i = 0$ or $j = 2^d - 1$ (first row and last column) and it is equal to 0 if $i = 2^d - 1$ or $j = 0$ (last row and first column) and $(M_d)_{0,0} = (M_d)_{2^d-1,2^d-1} = 1$ (intersection of the two previous cases). These facts are easily proved by induction on d. □

Bacher and Chapman [2, Theorems 1 and 3] proved that for every non negative integer d and every integer k such that $1 \leq k \leq 2^d$, every $k \times k$ submatrix of M_d given by k consecutive rows and and the last k columns, or by the top k consecutive rows and any consecutive k columns, is invertible. In case $k = 2^d$ this says that the whole matrix M_d is invertible. A proof of this result in more general form appears in Lemmas 2 and 3 in the next section.

Now we define an enumeration of all $n \times n$ matrices over $\mathbb{F}_2$. Suppose that the integer n is fixed. Let $N_0, \ldots, N_{2^{n^2}-1}$ be the enumeration of these matrices defined as follows. Informally, for $0 \leqslant k < 2^{n^2}$, the matrix N_k is filled by the digits of the binary expansion of k: the most n significant binary digits are put in the first line, the following n digits are put in the second line and so on, until the last line.

Definition 7 (Matrices enumeration)**.** *Fix a positive integer integer n. We define an enumeration $N_0, \ldots, N_{2^{n^2}-1}$ of all the $n \times n$ matrices over $\mathbb{F}_2$. Let k be a non-negative integer* *and let $a_{n^2-1}\cdots a_0$ be its binary expansion (the least significant digit is a_0). For each i,j such that $i,j=0,\dots,n-1$ the (i,j)-entry of the matrix N_k is $a_{n^2-1-in-j}$. The $(0,0)$-entry of N_k is thus the first digit a_{n^2-1} and the $(n-1,n-1)$-entry is the last digit a_0.*

For example the enumeration $N_0,\dots,N_{15}$ of the 16 matrices over $\mathbb{F}_2$ of size 2 × 2 is

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

For any given non negative integer k we consider its binary representation as a sequence of bits $a_n\dots a_0$. We denote with $\operatorname{even}(k)$ the integer whose binary representation is the subsequence $a_m\dots a_2a_0$, made of the bits at even positions in the representation of k, so where $m=n$ in case n is even, otherwise $m=n-1$. Similarly, $\operatorname{odd}(k)$ is the integer defined from the subsequence determined by the odd indexes.

Definition 8 (Pascal array)**.** *Let d be a positive integer and let $n=2^d$. We define an array A_d of size $n2^{n^2/2}\times n2^{n^2/2}$ over $\mathbb{F}_2$ by tiling it with all the $n\times n$ matrices over $\mathbb{F}_2$. Since there are 2^{n^2} such matrices, the total number of placed cells is exactly the size of A_d. For each k such that $0\leqslant k<2^{n^2}$ the matrix M_dN_k is placed in A_d at position* $(\operatorname{odd}(k)n,\operatorname{even}(k)n)$.

Since each matrix M_d is upper triangular with 1s on the diagonal then it is invertible. Since $N_0,\dots,N_{n^2-1}$ is an enumeration of all $n\times n$ matrices, then $M_dN_0,\dots,M_dN_{n^2-1}$ is also an enumeration of all the $n\times n$ matrices, but in a different order. This implies that each $n\times n$ matrix is used exactly once to tile the array A_d.

We illustrate the construction of A_d for $d=1$, $n=2$. The 2 × 2 matrices $N_0,\dots,N_{15}$ are listed above. The matrices M_1N_k for $k=0,\dots,15$ are placed as follows in the array A_1:

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

Since each matrix M_1N_k has size 2 × 2, the array A_1 has size 8 × 8. The nested $(2,2,2,2)$-perfect array given in the right of Figure 1 is actually the array A_1.

Proposition 1. *Let d be a non-negative integer and let $n=2^d$. Let k be an integer such that $1\leqslant k\leqslant n$. Each $n2^{kn/2}\times n2^{kn/2}$ aligned subarray of A_d is a nested (k,n,n,n)-perfect array.*

Proof. Suppose that k is fixed, $1\leqslant k\leqslant n$, and let B be an aligned subarray of A_d of sizes $n2^{kn/2}\times n2^{kn/2}$. Since B is aligned, the coordinates of its upper left corner are of the form $pn2^{kn/2}$ and $qn2^{kn/2}$ for two integers p and q such that $0\leqslant p,q<2^{(n-k)n/2}$. This means that the subarray B is tiled by the matrices $M_dN_{\ell\vee m}$ for integers ℓ and m satisfying

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

Note that the factor n disappeared since it accounts for the sizes of each of the matrices $M_dN_{\ell\vee m}$. The binary expansions of all integers ℓ satisfying $p2^{kn/2}\leqslant\ell<(p+1)2^{kn/2}$ start with the same $(n-k)n/2$ binary digits and the same hold for all integers m satisfying $q2^{kn/2}\leqslant$

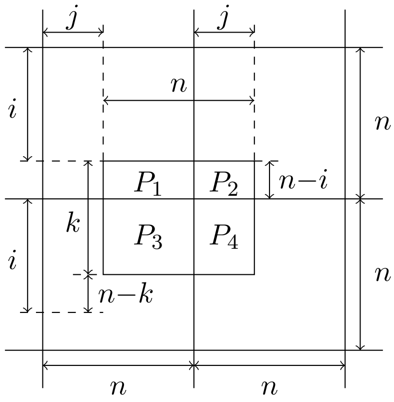


FIGURE 3. An occurrence of array B in A_d, $n = 2^d$.

$m < (q+1)2^{kn/2}$. This implies that the binary expansion of $\ell \vee m$ starts with the same $(n-k)n$ binary digits. Since the first binary digits of $\ell \vee m$ are put in the first rows of the matrix $N_{\ell\vee m}$ which have length n, all matrices $N_{\ell\vee m}$ for ℓ and m in their respective intervals have the same first $n-k$ rows.

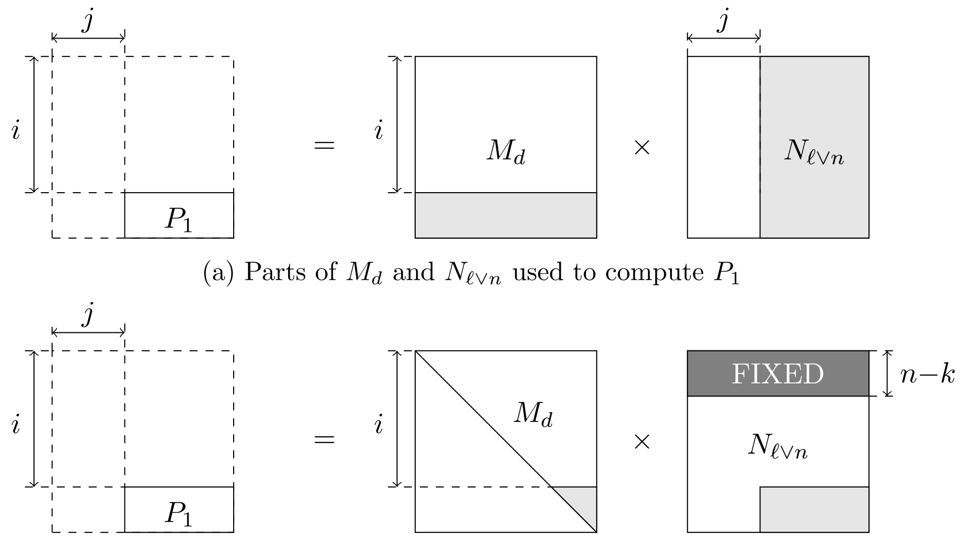
Let (i,j) be a pair of integers such that $0 \leqslant i,j < n$ and let P be an array of size $k \times n$. We claim that P has exactly one occurrence in B which is congruent to (i,j) modulo (n,n). To prove it, we show that P has a single such occurrence exactly when a certain system of linear equations has a solution. Furthermore, this solution of the system provides the matrix $N_{\ell\vee m}$ and thus the integers ℓ and m which, in turn, give the position of the occurrence of P in the subarray B.

An occurrence P can overlap at most four matrices tiling the subarray B. Suppose that the upper left corner of the occurrence of P lies in some matrix $M_dN_{\ell\vee m}$ where the integers ℓ and m such that $p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2}$ and $q2^{kn/2} \leqslant m < (q+1)2^{kn/2}$. The matrix on the right of $M_dN_{\ell\vee m}$ and the matrix below it are respectively $M_dN_{(\ell+1)\vee m}$ and $M_dN_{\ell\vee(m+1)}$ where $\ell+1$ and $m+1$ must be understood modulo $2^{kn/2}$ in order to remain in the right intervals. Let P_1, P_2, P_3 and P_4 be the parts of P that overlap respectively the matrices $M_dN_{\ell\vee m}$, $M_dN_{\ell\vee(m+1)}$, $M_dN_{(\ell+1)\vee m}$ and $M_dN_{(\ell+1)\vee(m+1)}$. They are pictured in Figure 10.

If $j = 0$, the parts P_2 and P_4 of the occurrence are empty. If $i+k \leqslant n$, the parts P_3 and P_4 of the occurrence are also empty. The simplest case is the system of equations $M_dN_{\ell\vee m} = P$ when $i = j = 0$ and $k = n$. We now treat the general case where none are empty, the other cases are similar and easier.

We state now the system of equations. The unknowns are the entries in the matrix $N_{\ell\vee m}$. We claim that they can be found from the matrix A_d the pair (i,j) and the arrays P_1,P_2,P_3 and P_4. As explained before, since $k = \ell \vee m$, the first $n-k$ rows of the matrix $N_{\ell\vee m}$ are fixed by the subarray B. This part is marked in dark grey in Figure 4.

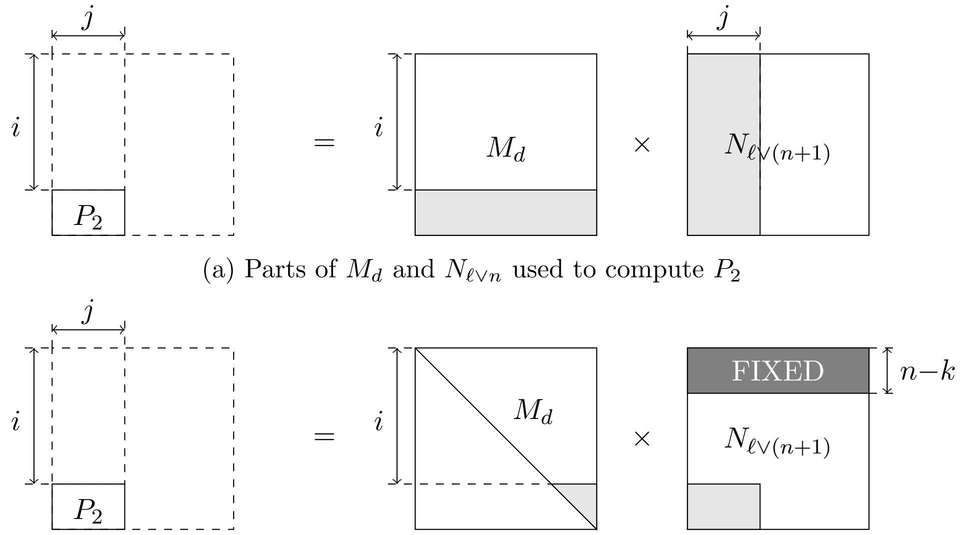
The height and width of P_1 are respectively $n-i$ and $n-j$. The part P_1 is obtained by the multiplication of the last $n-i$ rows of the matrix M_d and the last $n-j$ columns of the matrix $N_{\ell\vee m}$ (see grey parts in Figure 4a). Now we use the fact that the matrix M_d is upper triangular. This reduces the parts of M_d and $N_{\ell\vee m}$ used to compute P_1 (see grey parts in Figure 4b). Furthermore, the part used in M_d is upper triangular matrix with 1 on the



(a) Parts of M_d and $N_{\ell\vee n}$ used to compute P_1

(b) Taking into account that M_d is upper triangular

Figure 4. Proof of Proposition 1, using P_1



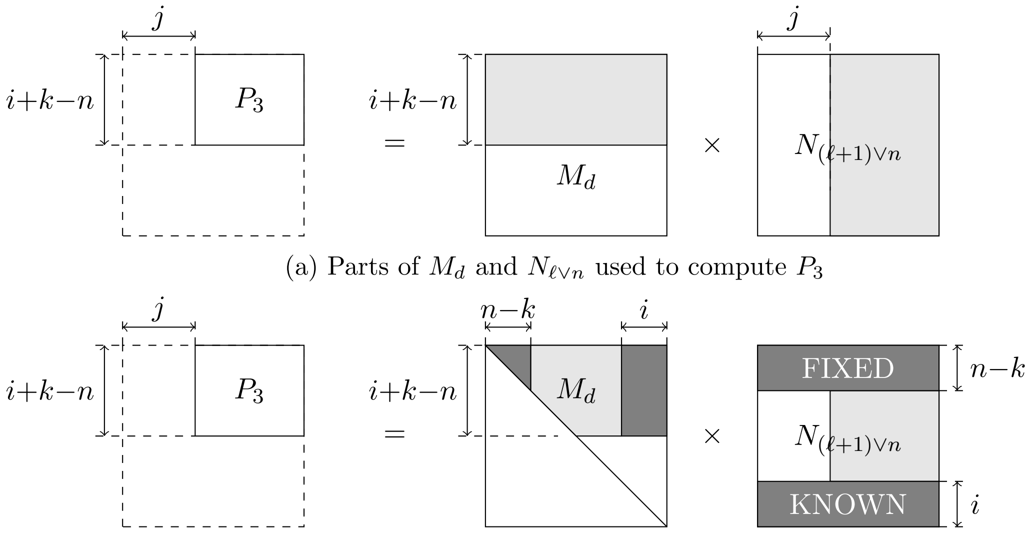
(a) Parts of M_d and $N_{\ell\vee n}$ used to compute P_2

(b) Taking into account that M_d is upper triangular

Figure 5. Proof of Proposition 1, using P_2

diagonal. This matrix is therefore invertible. This means that the grey part in $N_{\ell\vee m}$ can be obtained by multiplying the inverse of this triangular matrix with P_1.

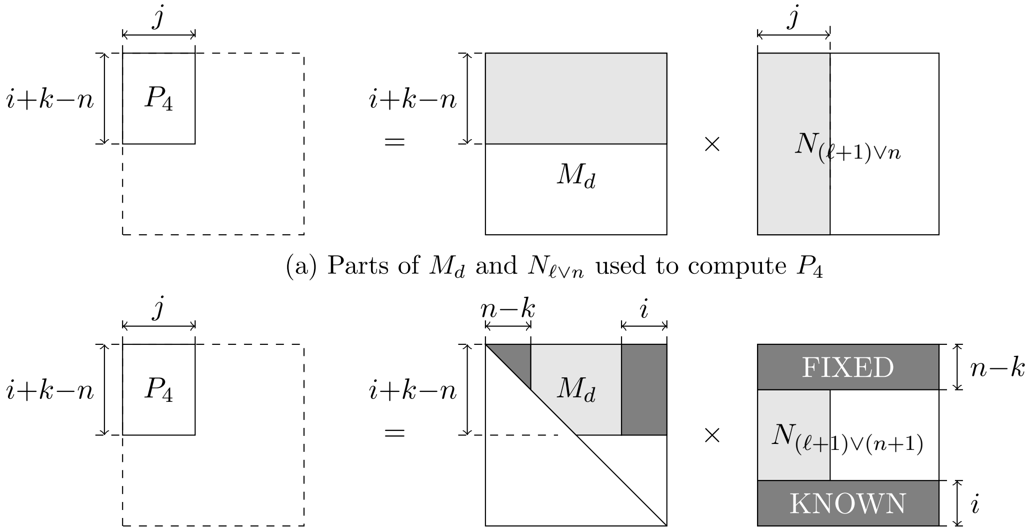
The height and width of P_2 are respectively $n-i$ and j. The part P_2 is obtained by the multiplication of the last $n-i$ rows of the matrix M_d and the first j columns of the matrix $N_{\ell\vee(m+1)}$ (see grey parts in Figure 5a). As for P_1, the fact that the matrix M_d is upper triangular reduces the parts of M_d and $N_{\ell\vee(m+1)}$ used to compute P_2 (see grey parts in Figure 5b). Furthermore, the part used in M_d is again invertible. This means that the



(a) Parts of M_d and $N_{\ell\vee n}$ used to compute P_3

(b) Taking into account that M_d is upper triangular

Figure 6. Proof of Proposition 1, using P_3



(a) Parts of M_d and $N_{\ell\vee n}$ used to compute P_4

(b) Taking into account that M_d is upper triangular

Figure 7. Proof of Proposition 1, using P_4

grey part in $N_{\ell\vee(m+1)}$ can be obtained by multiplying the inverse of this triangular matrix with P_2.

We claim that $n-i$ rows of $N_{\ell\vee m}$ are determined by part known in $N_{\ell\vee m}$ and $N_{\ell\vee(m+1)}$. This is because, for integers r and s, the last r binary digits of s determine the last r binary digits of $s+1$ and that conversely the last r binary digits if $s+1$ determine the last r binary digits of s. It follows that the last i rows of the four matrices $N_{\ell\vee m}$, $N_{\ell\vee(m+1)}$, $N_{(\ell+1)\vee m}$ and $N_{(\ell+1)\vee(m+1)}$ are known. These parts are marked in dark grey in the Figure 5.

The height and width of P_3 are respectively $i+k-n$ and $n-j$. The part P_3 is obtained by the multiplication of the first $i+k-n$ rows of the matrix M_d and the last $n-j$ columns of the matrix $N_{(\ell+1)\vee m}$ (see grey parts in Figure 6a). Now we use the fact that the first $n-k$ and the last i rows of $N_{(\ell+1)\vee m}$ are known. The elements of these rows can be considered as constants in the system of equations. Combining this latter result and the fact that the square $(i+k-n)\times(i+k-n)$ submatrix of M_d in grey in Figure 6b) is invertible the still unknown entries in the last $n-j$ columns of $N_{(\ell+1)\vee m}$ can be found.

The height and width of P_4 are respectively $i+k-n$ and j. By a reasoning very similar used with P_3, the remaining entries of the matrix $N_{(\ell+1)\vee(m+1)}$ can be found, see Figures 7a and 7b. □

In Proposition 1 the case $k=n$ states that the Pascal array for $n=2^d$ is a nested (n,n,n,n)-perfect array. This is proves Theorem 1.

3. Proof of Theorem 2

We consider a family of matrices that were first defined in [3]. These matrices are obtained by applying some rotations to columns of the matrices M_d given in Definition 6.

Let σ be the function which maps each word $a_1\cdots a_n$ to $a_na_1a_2\cdots a_{n-1}$ obtained by moving the last symbol to the front. Since words over $\mathbb{F}_2$ are identified with column vectors, the function σ can also be applied to a column vector.

Definition 9 (Pascal-like matrices)**.** *Let d be a non negative integer and let $n=2^d$. Let $m_0,\dots,m_{n-1}$ be integers such that $m_{n-1}=0$ and $m_{i+1}\le m_i\le m_{i+1}+1$ for each integer $0\le i<n$. Let $C_0,\dots,C_{n-1}$ be the columns of M_d, that is, $M_d=(C_0,\dots,C_{n-1})$. Define*

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

The following are the eight possible matrices $M_d^{m_0,\dots,m_{n-1}}$ for $d=2$ and $n=2^2$.

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

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

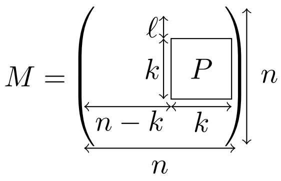
The matrix $M_d^{0,\dots,0}$ is exactly the matrix M_d of Definition 6. Not only $M_d^{0,\dots,0}$ but all the matrices $M_d^{m_0,\dots,m_{n-1}}$ of Definition 9 have the property that all the square submatrices on the top and on the right are invertible.

A proof of this result appears in [3, Lemmas 4 and 5]. We include them below.

Lemma 2 ([3, Lemma 4])**.** *Let d be a non negative integer and let $n=2^d$. Let matrix M be a one of $M_d^{m_0,\dots,m_{n-1}}$. Let ℓ and k be two integers such that $0\le\ell<\ell+k\le n$. The submatrix given by the k rows $\ell,\ell+1,\dots,\ell+k-1$ and the last k columns $n-k,\dots,n-1$ of M is invertible.*

Proof. Note that for $k = n$ and $\ell = 0$, the submatrix in the statement of the lemma, is the whole matrix $M_d^{m_0,\ldots,m_{n-1}}$, which is clearly invertible. By Lemma 1, each entry $M_{i,j}$ for $0 < i < n$ and $0 \leq j < n-1$ of the matrix M satisfies either $M_{i,j} = M_{i-1,j} \oplus M_{i,j+1}$ if $m_j = m_{j+1}$ (the column C_j has been rotated as much as the column C_{j+1}) or $M_{i,j} = M_{i-1,j} \oplus M_{i-1,j+1}$ if $m_j = m_{j+1} + 1$ (the column C_j has been rotated once more than the column C_{j+1}).

Let P be the submatrix in the statement of the lemma:



To prove that P is invertible we apply transformations to make it triangular. Note that all entries of the last column are 1. The first transformation applied to P is as follows. The row L_0 is left unchanged and the row L_i for $1 \leq i < k$ is replaced by $L_i \oplus L_{i-1}$. All entries of the last column but its top most one become zero. Furthermore, each entry is $P_{i,j}$ is replaced by either $P_{i,j+1}$ or $P_{i-1,j+1}$ depending on the value $m_j - m_{j+1}$. Note also that the new values of the entries still satisfy either $P_{i,j} = P_{i-1,j} \oplus P_{i,j+1}$ or $P_{i,j} = P_{i-1,j} \oplus P_{i-1,j+1}$ depending on the value $m_j - m_{j+1}$.

The second transformation applied to P is as follows. The rows L_0 and L_1 are left unchanged and each row L_i for $2 \leq i < k$ is replaced by $L_i \oplus L_{i-1}$. All entries of the second to last columns but its two topmost ones are now zero. At step t for $0 \leq t < k$, rows $L_0, \ldots, L_t$ are left unchanged and each row L_i for $t+1 \leq i < k$ is replaced by $L_i \oplus L_{i-1}$. After applying all these transformations for $0 \leq t < k$, each entry $P_{i,j}$ for $i + j = k - 1$ satisfies $P_{i,j} = 1$ and each entry $P_{i,j}$ for $i+j > k-1$ satisfies $P_{i,j} = 0$. It follows that the determinant of P is 1 and that the matrix P is invertible. □

Let $n = 2^d$ for some $d \geqslant 1$ and let M be one matrix $M_d^{m_0,\ldots,m_{n-1}}$. We introduce the notions of *upper* and *lower borders* of such a matrix $M_d^{m_0,\ldots,m_{n-1}}$. An entry $M_{i,j}$ for $0 \leqslant i, j < n$ is said to be in the *upper border* (respectively *lower border*) of M if $M_{i,j} = 1$ and $M_{k,j} = 0$ for all $k = 0, \ldots, i-1$ (respectively for all $k = i+1, \ldots, n-1$). For example, the upper border of the matrix $M_d^{0,\ldots,0} = M_d$ is the first row and its lower border is the main diagonal. The upper and lower borders in column i lie in lines m_i and $m_i + i$ respectively.

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

FIGURE 8. Upper and lower borders of $M_3^{3,3,2,1,1,1,0,0}$ are shown in boldface.

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

Both borders of matrix $M_d^{m_0,\dots,m_{n-1}}$ start in the unique entry 1 of the first column. The upper border ends in the top most entry of the last column and the lower border ends in the bottom most entry of the last column. The upper border is only made of either East or North-East steps and the lower border is only made of either East or South-East steps. The upper border contains an East step from column C_j to column C_{j+1} if $m_j = m_{j+1}$ and contains a North-East step if $m_j = m_{j+1} + 1$. Furthermore, whenever the upper border uses an East (respectively North-East) step to go from one columns to its right neighbour, the lower border uses a South-East (respectively East) step. This is because the distance from the upper border to the lower border in column i is exactly i. This allows us to define a function τ from $\{0,\dots,n-1\}$ to $\{0,\dots,n-1\}$ as follows.

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

The value of $\tau(i)$ is the line index of either the upper or the lower border in column i. It follows from the definition of the function τ that $M_{\tau(i),i} = 1$ and $M_{\tau(i),j} = 0$ for each $0 \leqslant j < i$. The values of the function τ for the matrix of Figure 8 are given below. In Figure 8, the 1s of the borders corresponding to values of τ are underlined. Note that there is exactly a single underlined 1 in each line and in each column.

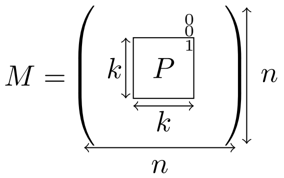
i	0	1	2	3	4	5	6	7
$\tau(i)$	3	4	2	1	5	6	0	7

The function τ is onto and thus bijective because each leftmost occurrence of 1 in each line belongs to either the upper or the lower border. It follows that each j in $\{0,\dots,n-1\}$ is equal to $\tau(i)$ where i is the column of the leftmost 1 in line j.

Due to the symmetry in the matrix $M_d^{0,\dots,0} = M_d$, Lemma 2 applies also to the submatrices of $M_d^{0,\dots,0}$ obtained by selecting the first row. Since this symmetry is lost in the other matrices $M_d^{m_0,\dots,m_{n-1}}$, we need to consider the rotations made to the columns in $M_d^{0,\dots,0}$ to obtain $M_d^{m_0,\dots,m_{n-1}}$.

Lemma 3 ([3, Lemma5])**.** *Let d be a non negative integer and let $n = 2^d$. Let matrix M be one of $M_d^{m_0,\dots,m_{n-1}}$. Let k be an integer such that $1 \leq k \leq n$. The $k \times k$-submatrix of M given by k consecutive rows and k consecutive columns with its top right entry on the upper border of M is invertible.*

Proof. Let P be the submatrix of M in the statement of the lemma:



We apply transformations to the submatrix P to put it in a nice form such that the determinant is easy to compute. To fix notation, suppose that the submatrix P is obtained by selecting rows $L_r, \dots, L_{r+k-1}$ and columns $C_s, \dots, C_{s+k-1}$. The hypothesis is that the entry $M_{r,s+k-1}$ is in the upper border of M. Note that the upper borders of M and P coincide inside P. We denote by $j_0, \dots, j_t$ the indices of the columns of P in $0, \dots, k-1$ originally defined by a North-East step of the upper border. This means that $j_0, \dots, j_t$ is the sequence of indices j such that $m_{s+j-1} = m_{s+j} + 1$. By convention, we set $j_0 = 0$, that is, the index of the first column of P.

The first transformation applied to the matrix P is the following. The columns $C_0, \dots, C_{j_t-1}$ and C_{k-1} are left unchanged and each column C_j for $j_t \leq j < k-1$ is replaced by $C_j \oplus C_{j+1}$. All entries of the first row but its right most one become zero. Furthermore, each entry $P_{i+1,j}$ for $j_t \leq j < k-1$ is replaced by $P_{i,j}$. The second transformation applied to the matrix P is the following. The columns $C_0, \dots, C_{j_{t-1}-1}$ and C_{k-2}, C_{k-1} are left unchanged and each column C_j for $j_{t-1} \leq j < k-2$ is replaced by $C_j \oplus C_{j+1}$. The first row remains unchanged and all entries of the second row but the last two become 0. We apply in total $t+1$ transformations like this one using successively $j_t, j_{t-1}, \dots, j_0$. Then $k-t$ further steps are made, obtaining that for each row i, all entries but the last i become 0.

After applying all these transformations, each entry $P_{i,j}$ for $i+j = k-1$ satisfies $P_{i,j} = 1$ and each entry $P_{i,j}$ for $i+j < k-1$ satisfies $P_{i,j} = 0$. It follows that the determinant of P is 1 and that the matrix P is invertible. □

We define the *affine arrays* by considering the family of Pascal-like matrices.

Definition 10 (Affine array)**.** *Let d be a non-negative integer and let $n = 2^d$. Let M be any Pascal-like matrix of size $n \times n$ (Definition 9). Let $N_0, \dots, N_{2^{n^2}-1}$ be the enumeration of all $n \times n$ matrices over $\mathbb{F}_2$ (Definition 7) and let Z be any $n \times n$ matrix over $\mathbb{F}_2$.*

An array A of size $n2^{n^2/2} \times n2^{n^2/2}$ is (n,n,n,n)-affine if for each integer k such that $0 \leqslant k < 2^{n^2}$, the matrix $MN_k \oplus Z$ is placed in A with its upper left corner cell at position $(\mathrm{odd}(k)n, \mathrm{even}(k)n)$.

Since each matrix $M = M_d^{m_0,\dots,m_{n-1}}$ is invertible, every matrix Z is equal to MZ' for some matrix Z'.

For an array Z we write $(Z)^{(n\times n)}$ to denote the array given by n^2 copies of Z, n rows and n columns. The next result states that any nested perfect array can be transformed into another one of the same size but having the matrix 0 in the upper corner.

In what follows we use the operation $\oplus$ on subarrays denoting the usual sum on matrices of elements in $\mathbb{F}_2$.

Lemma 4. *Let d be a non-negative integer. Fix $n = 2^d$. Let A be an array of size $n2^{n^2/2} \times n2^{n^2/2}$ and let Z be an array of size $n \times n$. Then A is a nested (n,n,n,n)-perfect array if and only if $A \oplus (Z)^{2^{n^2/2}\times 2^{n^2/2}}$ is a nested (n,n,n,n)-perfect array.*

Proof. Let $A' = A \oplus (Z)^{2^{n^2/2}\times 2^{n^2/2}}$. Let ℓ be an integer such that $1 \leq \ell \leq n$ and let L be an aligned subarray of A of size $n2^\ell \times n2^\ell$ starting at a position congruent to $(0,0)$. The corresponding subarray L' of A' at the same position is $L' = L \oplus (Z)^{(2^\ell \times 2^\ell)}$.

First suppose A is nested (n,n,n,n)-perfect. Then, L is a nested (ℓ,ℓ,n,n)-perfect array. Let i,j be such that $0 \leq i,j < n$ and T be the subarray of $(Z)^{(2\times 2)}$ of size $\ell \times \ell$ starting at position (i,j). Let U' be any array of size $\ell \times \ell$. Then, the array $U = U' \oplus T$ has exactly one occurrence in the array L at some position (i',j') congruent to (i,j) modulo (n,n). It follows that $U' = U \oplus T$ has an occurrence at the same position (i',j') in L'. Since each matrix U has such an occurrence for each possible (i,j).Since L' has size $n2^\ell \times n2^\ell$, L' it is a nested (ℓ,ℓ,n,n)-perfect array.

If A is not nested (n,n,n,n)-perfect, there is a witness ℓ, $1 \le \ell \le n$ and a subarray L of size $n2^\ell \times n2^\ell$ that occurs twice at positions in the same congruence class. With a similar argument as in the previous case it is easy to check that there is a subarray L' of A' with two occurrences in A' in the same congruence class. □

We can now prove that the affine arrays are nested perfect arrays.

Proposition 2. *Let d be a non negative integer and let $n = 2^d$. Every (n,n,n,n)-affine array is a nested (n,n,n,n)-perfect array.*

Proof. By Lemma 4, it may be assumed that the array Z in the definition of affine array is the zero matrix. Let M be one of the matrices $M_d^{m_0,\ldots,m_{n-1}}$. Suppose A is the (n,n,n,n)-affine array defined by M and the zero matrix. The proof of the Proposition follows that of Proposition 1, but now considering the matrix $M = M_d^{m_0,\ldots,m_{n-1}}$ instead of the Pascal matrix $M_d^{0,\ldots,0}$ Let k be an integer such that $1 \le k \le n$. Let B be an aligned subarray of A of sizes $n2^{kn/2} \times n2^{kn/2}$. The coordinates of the upper left corner of B are of the form $pn2^{kn/2}$ and $qn2^{kn/2}$ for two integers p and q such that $0 \leqslant p,q < 2^{(n-k)n/2}$. This means that the subarray B is tiled by the matrices $MN_{\ell\vee m}$ for ℓ and t satisfying

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

The binary expansions of all integers ℓ satisfying

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

start with the same $2^{n(n-k)/2}$ binary digits and the same hold for all integers t satisfying

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

This implies that $\ell \vee m$ start with the same $n(k-n)$ digits. Since the first digits of $\ell \vee m$ are put in the first rows of $N_{\ell\vee m}$ which have length n, all matrices $N_{\ell\vee m}$ for ℓ and t in their respective intervals have the same first $n-k$ rows.

Let (i,j) be a pair of integers such that $0 \leqslant i,j < n$ and let P be an array of sizes $k \times n$. We claim that P has exactly one occurrence in B which is congruent to (i,j) modulo (n,n). In order to prove it, we show that P has a single such occurrence exactly when a certain system of linear equations has a solution. Furthermore, this solution of the system provides the matrix $N_{\ell\vee m}$ and thus the integers ℓ and m which, in turn, give the position of the occurrence of P in the subarray B. An occurrence P can overlap at most four matrices tiling the subarray B.

Suppose that the upper left corner of the occurrence of P lies in some matrix $MN_{\ell\vee m}$ where the integers ℓ and m such that $p2^{kn/2} \leqslant \ell < (p+1)2^{kn/2}$ and $q2^{kn/2} \leqslant m < (q+1)2^{kn/2}$. The matrix on the right of $MN_{\ell\vee m}$ and the matrix below it are respectively $MN_{(\ell+1)\vee m}$ and $MN_{\ell\vee(m+1)}$ where $\ell+1$ and $m+1$ must be understood modulo $2^{kn/2}$ in order to remain in the right intervals. Let P_1, P_2, P_3 and P_4 be the parts of P that overlap respectively the matrices $MN_{\ell\vee m}$, $MN_{\ell\vee(m+1)}$, $MN_{(\ell+1)\vee m}$ and $MN_{(\ell+1)\vee(m+1)}$. They are pictured in Figure 10.

If $j = 0$, the parts P_2 and P_4 of the occurrence are empty. This is a degenerate case, so we only treat the case $j \geqslant 1$. Consider two main cases depending on whether $i + k \leqslant n$ or not.

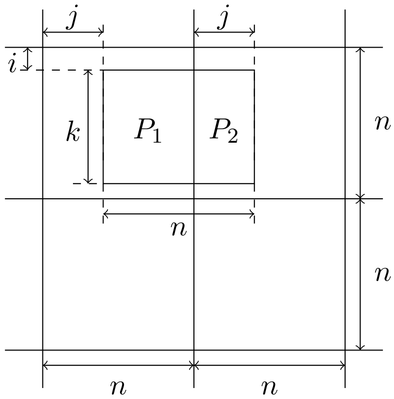


FIGURE 9. An occurrence of array B in A with $i + k \leqslant n$.

Suppose that $i + k \leqslant n$. Then, the parts P_3 and P_4 do not exist and the occurrence of P is reduced to P_1 and P_2. Consider a column of the occurrence in P_1, that is, a column of the matrix $MN_{\ell \vee m}$ with index s greater than j from line $i+1$ to line $i+k$. This column is obtained by multiplying the lines from $i+1$ to $i+k$ of M with the column of index s of $N_{\ell \vee m}$. Note that the first $n-k$ entries of this latter are known and can be considered as constant. The k remaining entries of the column s of $N_{\ell \vee m}$ are thus the solution of the system $y = Mx$ where y is the column of P_1, M is the $k \times k$ matrix made of lines from i to $i+k-1$ and columns $n-k$ to $n-1$ of M and x are the k entries of $N_{\ell \vee m}$. By Lemma 2, the matrix M is invertible and there is then a unique solution to the system. This means that the k entries of the column of index s of $N_{\ell \vee m}$ can be found. An similar reasoning with a column of P_2 allows us to find a column s with $s \leqslant j$ of $N_{\ell \vee (m+1)}$ and thus of $N_{\ell \vee m}$.

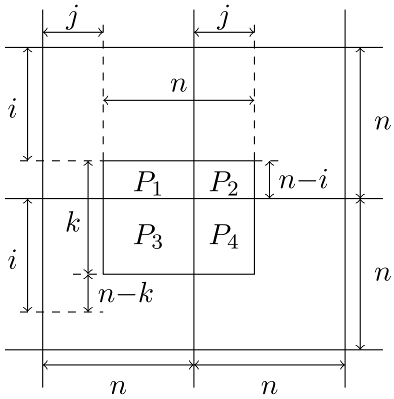


FIGURE 10. An occurrence of array B in A with $i + k > n$.

Now we suppose that $i + k > n$ and we make more explicit how the matrix $N_{\ell \vee m}$ can be computed from the occurrence of P modulo (i, j). Let us recall that the $n-k$ top lines of $N_{\ell \vee m}$, that is, lines $0, \ldots, n-k-1$ are fixed by the subarray B. Let $n-k, \ldots, n-1$ the indices of the lines of $N_{\ell \vee m}$ which are still unknown. The computation of these k remaining lines is carried out in two phases. The second and first phases respectively compute the lines $n-k,\dots,r-1$ and $r,\dots,n-1$ where the cutting index r satisfying $n-k \leqslant r \leqslant n-1$ is defined as follows. The integer r is the least integer such that all the integers $\tau(r),\dots,\tau(n-1)$ belong to $\{0,\dots,i+k-n-1\} \cup \{i,\dots,n-1\}$. Note that $\{0,\dots,i+k-n-1\}$ are the indices of the lines crossing P_3P_4 while $\{i,\dots,n-1\}$ are the indices of the lines crossing P_1P_2. If $r = n-k$, all k lines $n-k,\dots,n-1$ are computed by the first phase and the second phase is void.

We describe more precisely the first phase. Let s be an integer satisfying $r \leqslant s \leqslant n-1$ and let us suppose that lines $s+1,\dots,n-1$ are already known and that line s is still unknown. The entries of line s are computed from the rightmost one of index $n-1$ to the leftmost one of index 0. Let us consider the line $\tau(s)$ in the matrix M. By definition of τ, the entry $M_{\tau(s),s}$ is equal to 1 and entries $M_{\tau(s),s'}$ for $s' < s$ are equal to 0. We consider two cases depending on whether $\tau(s)$ belongs to $\{0,\dots,i+k-n-1\}$ or to $\{i,\dots,n-1\}$.

Assume $\tau(s)$ belongs to $\{i,\dots,n-1\}$. Let t be an integer such that $j \leqslant t \leqslant n-1$. The multiplication of the line $\tau(s)$ in M and the column t of $N_{\ell\vee m}$ gives the entry $(\tau(s),t)$ in P_1, that is, the entry $(\tau(s)-i, t-j)$ in P. The properties of the line $\tau(s)$ in M and the fact that lines below line r in $N_{\ell\vee m}$ are already known allow us to compute the entry (s,t) in $N_{\ell\vee m}$. Let t be an integer such that $0 \leqslant t < j$. The multiplication of the line $\tau(s)$ in M and the column t of $N_{\ell\vee m+1}$ gives the entry $(\tau(s),t)$ in P_2, that is, $(\tau(s)-i, t+n-i)$ in P.

The properties of the line $\tau(s)$ in M and the fact that lines below line s in $N_{\ell\vee m}$ are already known allow us to find the entry (s,t) in $N_{\ell\vee(m+1)}$. Since all entries (s,t) for $j \leqslant t \leqslant n-1$ of $N_{\ell\vee m}$ and all entries (s,t) for $0 \leqslant t < j$ of $N_{\ell\vee(m+1)}$ and all lines below line s in $N_{\ell\vee m}$ are known, line s of $N_{\ell\vee m}$ is known.

Now assume $\tau(s)$ belongs to $\{0,\dots,i+k-n-1\}$. The same reasoning with matrices $N_{(\ell+1)\vee m}$ and $N_{(\ell+1)\vee(m+1)}$ and parts P_3 and P_4 of P allows us to compute line s of $N_{(\ell+1)\vee m}$ and thus line s of $N_{\ell\vee m}$.

We finally describe the second phase. Lines $0,\dots,n-k-1$ are fixed by the subarray B and lines $r,\dots,n-1$ have been computed by the first phase. Lines $n-k,\dots,r-1$ are still unknown. We assume that $n-k < r$ since otherwise no line is unknown. It follows from the definition of r that the integer $\tau(r-1)$ is then either $i+k-n$ or $i-1$. Suppose $\tau(r-1) = i-1$, the other case is similar. Consider the $(k+r-n)\times(k+r-n)$ matrix M' obtained by selecting lines $i-r,\dots,i+k-n-1$ and columns $n-k,\dots,r-1$ from the matrix M. The upper right entry of M' is the entry $(i-r, r-1)$ of M. Since $\tau(r-1) = i-1$ and the distance between the upper and the lower borders in column $r-1$, is $r-1$, the entry $(i-r, r-1)$ lies on the upper border of M. By Lemma 3, the matrix M' is invertible. Note that selected lines of M' are still unused lines of P and that selected columns correspond to still unknown lines of $N_{\ell\vee m}$. Invertibility of M' allows us to compute lines $n-k,\dots,r-1$ of $N_{\ell\vee m}$. This completes the proof of the theorem. □

The next lemma computes the number of (n,n,n,n)-affine arrays.

Proposition 3. *Let d be a non-negative integer and let $n = 2^d$. Then,, there are 2^{n^2+n-1} (n,n,n,n)-affine arrays.*

Proof. There are exactly 2^{n-1} matrices $M_d^{m_0,\dots,m_{m-1}}$. Indeed, the sequence $m_0,\dots,m_{n-1}$ is fully determined by the sequence $m_0-m_1,\dots,m_{n-2}-m_{n-1}$ of $n-1$ differences which take their value in $\{0,1\}$. There are also 2^{n^2} possible values for the matrix Z in $\mathbb{F}_2^{n\times n}$. This proves that the number of (n,n,n,n)-affine arrays is at most 2^{n^2+n-1}.

It remains to show that two (n,n,n,n)-affine array obtained for two different pairs (M,Z) and (M',Z') are indeed different. Let $N_0,\dots,N_{2^{n^2}-1}$ be the enumeration of all $n\times n$ matrices over $\mathbb{F}_2$. Let M and M' be two matrices of the form $M_d^{m_0,\dots,m_{n-1}}$. Let Z and Z' be two $n\times n$ matrices $\mathbb{F}_2$. Let $U_i = N_i \oplus Z$ and $U'_i = N_i \oplus Z'$ for $i = 0,\dots,2^n-1$. Let W and W' be the two placements is defined as follows: for each integer i such that $0 \leqslant i \leqslant 2^{2^n}-1$, the matrix MU_k is placed in W in such a way that its upper left corner cell is at position $(\mathrm{odd}(i)n, \mathrm{even}(i)n)$. Similarly for W' using U'_i instead of U_i. We claim that if $W = W'$, then $M = M'$ and $Z = Z'$. We suppose that $W = W'$. Since both matrices M and M' are invertible by Lemma 2, MU_i (respectively $M'U'_i$) is the zero vector if and only if U_i (respectively U'_i) is the zero vector, that is, $Z = W_i$ (respectively $Z' = W_i$). This implies that $Z = Z'$ and thus $U_i = U'_i$ for $i = 0,..,2^n-1$. Note that the matrix U_i ranges over all possible $n\times n$ matrices. If $MU_i = M'U_i$ for all $i = 0,\dots,2^n-1$, then $M = M'$. □

For d a non negative integer and $n = 2^d$ Definition 10 gives a construction method of (n,n,n,n)-affine arrays. Proposition 3 counts how many can be constructed and proves that they are all different. This completes the proof of Theorem 2.

Acknowledgements.

Both authors are members of SINFIN Laboratory Université de Paris/CNRS-Universidad de Buenos Aires/CONICET. This research is supported by projects CONICET PIP 11220210100220CO and UBACyT 20020220100065BA.

References

[1] N. Alvarez, V. Becher, P. A. Ferrari, and S. Yuhjtman. Perfect necklaces. *Adv. in Appl. Math.*, 80:48–61, 2016.

[2] R. Bacher and R. Chapman. Symmetric pascal matrices modulo p. *European Journal of Combinatorics*, 25(4):459–473, 2004.

[3] V. Becher and O. Carton. Normal numbers and perfect necklaces. *Journal of Complexity*, 54, 2019.

[4] F.R.K Chung, P Diaconis, and R.L Graham. Universal cycles for combinatorial structures. *Discrete math.*, 110:43–59, 1992.

[5] T. Etzion. Constructions for perfect maps and pseudorandom arrays. *IEEE Trans. Inform. Theory*, 34(5, part 2):1308–1316, 1988.

[6] T. Etzion. *Sequences and the de Bruijn Graph, Properties, Constructions, and Applications*. Academic Press, 2024.

[7] C. T. Fan, S. M. Fan, S. L. Ma, and M. K. Siu. On de Bruijn arrays. *Ars Combin.*, 19(A):205–213, 1985.

[8] H. Faure. Discrépance de suites associées à un système de numération (en dimension s). *Acta Arithmetica*, 41, 1982.

[9] B. Gordon. On the existence of perfect maps (corresp.). *IEEE Transactions on Information Theory*, 12(4):486–487, 1966.

[10] M. Horváth and A. Iványi. Growing perfect cubes. *Discrete Math.*, 308(19):4378–4388, 2008.

[11] G. Hurlbert and G. Isaak. On the de Bruijn torus problem. *J. Comb. Theory, Ser. A*, 64(1):50–62, 1993.

[12] M. B. Levin. On the discrepancy estimate of normal numbers. *Acta Arithmetica*, 88(2):99–111, 1999.

[13] S. L. Ma. A note on binary arrays with a certain window property. *IEEE Trans. Inform. Theory*, 30(5):774–775, 1984.

[14] K. Paterson. Perfect maps. *IEEE Trans. Inform. Theory*, 40(3):743–753, 1994.

[15] I. S. Reed and R. M. Stewart. Note on the existence of perfect maps. *IRE Trans. on Information Theory*, IT-8:10–12, 1962.

[16] J. Salvi, J. Pagès, and J. Batlle. Pattern codification strategies in structured light systems. *Pattern Recognition*, 37(4):827–849, 2004.

Verónica Becher
Departamento de Computación, Facultad de Ciencias Exactas y Naturales & ICC
Universidad de Buenos Aires & CONICET, Argentina
vbecher@dc.uba.ar

Olivier Carton
Institut de Recherche en Informatique Fondamentale
Université Paris Cité, France
Olivier.Carton@irif.fr