Sequence Folding, Lattice Tiling, and Multidimensional Coding

Tuvi Etzion, *Fellow, IEEE*

***Abstract*—Folding a sequence $\mathcal{B}$ into a multidimensional box is a well-known method which is used as a multidimensional coding technique. The operation of folding is generalized in a way that the sequence $\mathcal{B}$ can be folded into various shapes and not just a box. The novel definition of folding is based on a lattice tiling for the given shape $\mathcal{S}$ and a direction in the D-dimensional integer grid. Necessary and sufficient conditions that a lattice tiling for $\mathcal{S}$ combined with a direction define a folding of a sequence into $\mathcal{S}$ are derived. The immediate and most impressive applications are some new lower bounds on the number of dots in two-dimensional synchronization patterns. Asymptotically optimal such patterns were known only for rectangular shapes. We show asymptotically optimal such patterns for a large family of hexagons. This is also generalized for multidimensional synchronization patterns. The best known patterns, in terms of dots, for circles and other polygons are also given. The technique and its application for two-dimensional synchronization patterns, raises some interesting problems in discrete geometry. We will also discuss these problems. It is also shown how folding can be used to construct multidimensional error-correcting codes. Finally, by using the new definition of folding, new types of multidimensional pseudo-random arrays with various shapes are generated.**

***Index Terms*—Distinct difference configuration, folding, lattice tiling, pseudo-random array, two-burst-correcting code.**

I. Introduction

MULTIDIMENSIONAL coding in general and two-dimensional coding in particular are subjects which attract lot of attention in the last three decades. One of the main reasons is their modern applications which have developed during these years. Such applications for synchronization patterns include radar, sonar, physical alignment, and time-position synchronization. For error-correcting codes they include two-dimensional magnetic and optical recording as well as three-dimensional holographic recording. These are the storage devices of the future. Applications for pseudo-random arrays include scrambling of two-dimensional data, two-dimensional digital watermarking, and structured light patterns for imaging systems. Each one of these structures (multidimensional synchronization patterns, error-correcting array codes, and pseudo-random arrays), and its related coding problem, is a generalization of an one-dimensional structure. But, although the related theory of the one-dimensional case is well developed, the theory for the multidimensional case is developed rather slowly. This is due that the fact the most of the one-dimensional techniques are not generalized easily to higher dimensions. Hence, specific techniques have to be developed for multidimensional coding. One approach in multidimensional coding is to take an one-dimensional code and to transform it into a multidimensional code. One technique in this approach is called folding and it is the subject of the current paper. This technique was applied previously for two-dimensional synchronization patterns, for pseudo-random arrays, and lately for multidimensional error-correcting codes. We start with a short introduction to these three multidimensional coding problems which motivated our interest in the generalization of folding.

Synchronization patterns

One-dimensional synchronization patterns were first introduced by Babcock in connection with radio interference [1]. Other applications are discussed in details in [2] and some more are given in [3] and [4]. The two-dimensional applications and related structures were first introduced in [5] and discussed in many papers, e.g., [6]–[10]. The two-dimensional problems has also interest from discrete geometry point of view and it was discussed for example in [11] and [12]. Recent new application in key predistribution for wireless sensor networks [13] led to new related two-dimensional problems concerning these patterns which are discussed in [14] and [15]. It has raised the following discrete geometry problem: given a regular polygon with area s on the square (or hexagonal) grid, what is the maximum number of grid points that can be taken, such that any two lines connecting these grid points are different either in their length or in their slope. Upper bound technique based on an idea of Erdös and Turán [11], [16] is given in [14]. Some preliminary lower bounds on the number of dots are also given in [14], where the use of folding is applied. Folding for such patterns was first used by [10]. An one-dimensional ruler was presented as a binary sequence and written into a two-dimensional array row by row, one binary symbol to each entry of the array. This was generalized for higher dimensions, say $n_1 \times n_2 \times n_3$ array, by first partitioning the array into n_1 two-dimensional arrays of size $n_2 \times n_3$. The one-dimensional sequence is written into the these $n_2 \times n_3$ arrays one by one in the order defined by the three-dimensional array. To each of these $n_2 \times n_3$ arrays the sequence is written row by row. Folding into higher dimensions is done similarly and can be defined recursively. This technique was used in [10] to generate asymptotically optimal high dimensional synchronization patterns.

Error-correcting codes

There is no need for introduction to one-dimensional error-correcting codes. Two-dimensional and multidimensional error-correcting codes were discussed by many authors, e.g., [17]–[27]. Multidimensional error-correcting codes are of interest when the errors are not random errors. For correction of

Manuscript received November 09, 2009; revised July 18, 2010; accepted January 11, 2011. Date of current version June 22, 2011 This work was supported in part by the United States-Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant 2006097.

The author is with the Department of Computer Science, Technion—Israel Institute of Technology, Haifa 32000, Israel. (email: etzion@cs.technion.ac.il).

Communicated by M. G. Parker, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2146010

0018-9448/$26.00 © 2011 IEEE

up to t random errors in a multidimensional array, we can consider the elements in the array as an one-dimensional sequence and use a t-error-correcting code to correct these errors. Hence, when we talk about multidimensional error-correcting codes we refer to the errors as special ones such as the rank of the error array [28], [29], or crisscross patterns [29]–[31], etc. An important family of multidimensional error-correcting codes are the burst-error-correcting codes. In these codes, we assume that the errors are contained in a cluster whose size is at most b. The one-dimensional case was considered for more than forty years. Fire [32] was the first to present a general construction. Optimal burst-correcting codes were considered in [33]–[35]. Generalizations, especially for two-dimensional codes, but also for multidimensional codes were considered in various research papers, e.g., [18], [19], [22], [23], [25], [27]. Folding of one-dimensional codes were considered for two-dimensional error-correcting codes in [20], [24] and optimal codes were constructed by a combination of folding and interleaving in [26]. In other papers, one-dimensional burst-correcting codes and error-correcting codes, were transferred into two-dimensional codes, e.g., [21]–[23], [25]–[27]. Colorings for two-dimensional coding, which transfer one-dimensional codes into multidimensional arrays were considered for interleaving schemes [22] and other techniques [27]. These colorings can be compared to the coloring which will be used in the sequel for folding. There is another related problem of generating an array in which burst-errors can be corrected on an unfolded sequence generated from the array [36]–[40].

Pseudo-random arrays

The one-dimensional pseudo-random sequences are the maximal length linear shift register sequences known as M-sequences and also pseudo-noise (PN) sequences [41]. These are sequences of length $2^n - 1$ generated by a linear feedback shift-register of order n. They have many desired properties such as follows.

- Recurrences Property—the entries satisfy a recurrence relation of order n.
- Balanced Property—2^{n-1} entries in the sequence are *ones* and $2^{n-1} - 1$ entries in the sequence are *zeros*.
- Shift-and-Add Property—when a sequence is added bitwise to its cyclic shift another cyclic shift of the sequence is obtained.
- Autocorrelation Property—the out-of-phase value of the autocorrelation function is always -1.
- Window Property—each nonzero n-tuple appears exactly once in one period of the sequence.

There are other properties which we will not mention [42]. For a comprehensive work on these sequences the reader is referred to [41]. Related sequences are the de Bruijn sequences of length 2^n which are generated by nonlinear feedback shift-register of order n. These sequences have the window property, i.e., each n-tuple appears exactly once in one period of the sequence.

The two-dimensional generalizations of pseudo-noise and de Bruijn sequences are the pseudo-random arrays and perfect maps [42]–[47]. Pseudo-random arrays were also called *linear recurring arrays having maximum-area matrices* by Nomura, Miyakawa, Imai, and Fukuda [43] who were the first to construct them. Perfect maps and pseudo-random arrays have been used in two-dimensional range-finding, in data scrambling, and in various kinds of mask configurations. More recently, pseudo-random arrays have found other applications in new and emerging technological areas. One such application is robust, undetectable, digital watermarking of two-dimensional test images [48], [49]. Another interesting example is the use of pseudo-random arrays in creating *structured light*, which is a new reliable technique for recovering the surface of an object. The structured-light technique is based on projecting a light pattern and observing the illuminated scene from one or more points of view [50]–[53]. As mentioned in these papers, this technique can be generalized to three dimensions; hence, constructions of three-dimensional perfect maps and pseudo-random arrays are also of interest.

The main goal of this paper is to generalize the well-known technique, folding, for generating multidimensional codes of these types, synchronization patterns, burst-correcting codes, and pseudo-random arrays. The generalization will enable to obtain the following results:

1) form new two-dimensional codes for these applications;
2) generalize all the multidimensional codes for any number of dimensions in a simple way;
3) form some optimal codes not known before;
4) make these codes feasible not just for multidimensional boxes, but also for many other different shapes;
5) solve the synchronization pattern problem as a discrete geometry problem for various two-dimensional shapes, and in particular regular polygons.

It is important to note that folding which was used in other places in the literature aim only at one goal. Our folding aim is at several goals. Even so, our description of folding is simple and very intuitive for all these goals.

The rest of this paper is organized as follows. In Section II we define the basic concepts of folding and lattice tiling. Tiling and lattices are basic combinatorial and algebraic structures. We will consider only integer lattice tiling. We will summarize the important properties of lattices and lattice tiling. In Section III we will present the generalization of folding into multidimensional shapes. All previous known folding definitions are special cases of the new definition. This novel definition involves a lattice tiling and a direction. We will prove necessary and sufficient conditions that a lattice with a direction define a folding. We first present a proof for the two-dimensional case since it is the most applicable case. We continue to show the generalization for the multidimensional case. For the two-dimensional case the proof is slightly simpler than the slightly different proof for the multidimensional case. In Section IV we give a short summary on synchronization patterns and present basic theorems concerning the bounds on the number of elements in such patterns. In Section V we apply the results of the previous sections to obtain new type of synchronization patterns which are asymptotically either optimal or almost optimal. In particular we show how to construct asymptotically optimal patterns for a large family hexagonal shapes, something which was previously known only for rectangular shapes. In Section VI we discuss folding in the hexagonal grid and present a construction for synchronization patterns in this grid with shapes of hexagons or circles. In Section VII we show how folding can

be applied to construct multidimensional error-correcting codes. In Section VIII we generalize the constructions in [42], [43] to form pseudo-random arrays on different multidimensional shapes. Conclusion and problems for further research are given in Section IX.

II. Folding and Lattice Tiling

A. Folding

Folding a rope, a ruler, or any other feasible object is a common action in every day life. Folding an one-dimensional sequence into a D-dimensional array is very similar, but there are a few variants. First, we will summarize three variants for folding of an one-dimensional sequence into a two-dimensional array $\mathcal{A}$. The generalization for a D-dimensional array is straightforward while the description becomes more clumsy.

F1. $\mathcal{A}$ is considered as a cyclic array horizontally and vertically in such a way that a walk diagonally visits all the entries of the array. The elements of the sequence are written along the diagonal of the $r \times t$ array $\mathcal{A}$. This folding works (i.e., all elements of the sequence are written into the array) if and only if r and t are relatively primes.

F2. The elements of the sequence are written row by row (or column by column) in $\mathcal{A}$.

F3. The elements of the sequence are written diagonal by diagonal in $\mathcal{A}$.

Example 1:

Example for **F1**: Given the M-sequence 000111101011001 of length 15, we fold it into a 3×5 array with a 2×2 window property (the extra row and extra column are given for better understanding of the folding).

0	6	12	3	9	0
5	11	2	8	14	5
10	1	7	13	4	10
0	6	12	3	9	0

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

Example for **F2**: The following sequence (ruler) of length 13 with five dots is folded into a 3×5 array.

0	1	2	3	4	5	6	7	8	9	10	11	12
•	•			•						•		•

10	11	12	13	14
5	6	7	8	9
0	1	2	3	4

•		•		
•	•			•

Example for **F3**: The following B_2-sequence in $\mathbb{Z}_{31}$: $\{0, 1, 4, 10, 12, 17\}$ (can be viewed as a cyclic ruler) is folded into an infinite array (we demonstrate part of the array with folding into a small rectangle is given in bold). Note, that while the folding is done we should consider all the integers modulo 31 (see Fig. 1).

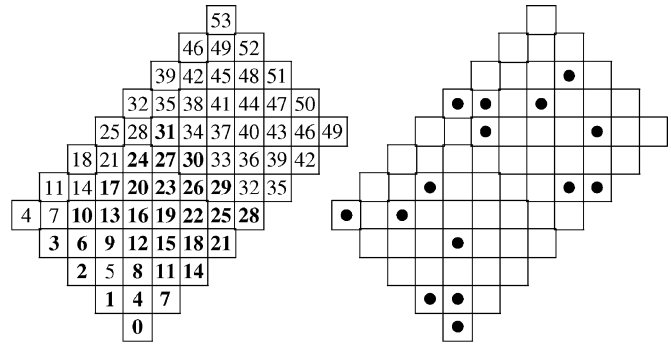


Fig. 1. Folding by diagonals.

F1 and **F2** were used by MacWilliams and Sloane [42] to form pseudo-random arrays. **F2** was also used by Robinson [10] to fold a one-dimensional ruler into a two-dimensional Golomb rectangle. The generalization to higher dimensions is straight forward. **F3** was used in [14] to obtain some synchronization patterns in $\mathbb{Z}^D$.

B. Tiling

Tiling is one of the most basic concepts in combinatorics. We say that a D-dimensional shape $\mathcal{S}$ tiles the D-dimensional space $\mathbb{Z}^D$ if disjoint copies of $\mathcal{S}$ cover $\mathbb{Z}^D$.

Remark 1: We assume that our shape $\mathcal{S}$ is a discrete shape, i.e., it consists of discrete points of $\mathbb{Z}^D$ such that there is a path between any two points of $\mathcal{S}$ which consists only from points of $\mathcal{S}$. The shape $\mathcal{S}$ in $\mathbb{Z}^D$ is usually not represented as a union of points in $\mathbb{Z}^D$, but rather as a union of units cubes in $\mathbb{R}^D$ with 2^D vertices in $\mathbb{Z}^D$. Let A be the set of points in the first representation. The set of unit cubes by the second representation is

$$\{\mathcal{U}_{(i_1,i_2,\ldots,i_D)} : (i_1, i_2, \ldots, i_D) \in A\}$$

where

$$\mathcal{U}_{(i_1,i_2,\ldots,i_D)} = \{(i_1, i_2, \ldots, i_D) + \xi_1\epsilon_1 + \xi_2\epsilon_2 + \cdots + \xi_D\epsilon_D : 0 \le \xi_i < 1, 1 \le i \le D\}$$

and ϵ_i is a vector of length D and weight one with a *one* in the ith position. We omit the case of shapes in $\mathbb{R}^D$ which are not of interest to our discussion.

A cover for $\mathbb{Z}^D$ with disjoint copies of $\mathcal{S}$ is called a *tiling* of $\mathbb{Z}^D$ with $\mathcal{S}$. For each shape $\mathcal{S}$ we distinguish one of the points of $\mathcal{S}$ to be the *center* of $\mathcal{S}$. Each copy of $\mathcal{S}$ in a tiling has the center in the same related point. The set $\mathcal{T}$ of centers in a tiling defines the tiling, and hence the tiling is denoted by the pair $(\mathcal{T}, \mathcal{S})$. Given a tiling $(\mathcal{T}, \mathcal{S})$ and a grid point $(i_1, i_2, \ldots, i_D)$ we denote by $c(i_1, i_2, \ldots, i_D)$ the center of the copy of $\mathcal{S}$ for which $(i_1, i_2, \ldots, i_D) \in \mathcal{S}$. We will also assume that the origin is a center of some copy of $\mathcal{S}$.

Remark 2: It is easy to verify that any point of $\mathcal{S}$ can serve as the center of $\mathcal{S}$. If $(\mathcal{T}, \mathcal{S})$ is a tiling then we can choose any point

of $\mathcal{S}$ to serve as a center without affecting the fact that $(\mathcal{T},\mathcal{S})$ is a tiling.

Lemma 1: If $(\mathcal{T},\mathcal{S})$ is a tiling then for any given point $(i_1,i_2,\ldots,i_D) \in \mathbb{Z}^D$ the point $(i_1,i_2,\ldots,i_D) - c(i_1,i_2,\ldots,i_D)$ belongs to the shape $\mathcal{S}$ whose center is in the origin.

Proof: Let $\mathcal{S}_1$ be the copy of $\mathcal{S}$ whose center is in the origin and $\mathcal{S}_2$ be the copy of $\mathcal{S}$ with the point $(i_1,i_2,\ldots,i_D)$. Let $(x_1,x_2,\ldots,x_D)$ be the point in $\mathcal{S}_1$ related to the point $(i_1,i_2,\ldots,i_D)$ in $\mathcal{S}_2$. By definition, $(i_1,i_2,\ldots,i_D) = c(i_1,i_2,\ldots,i_D) + (x_1,x_2,\ldots,x_D)$ and the lemma follows. ■

One of the most common types of tiling is a *lattice tiling*. A *lattice* Λ is a discrete, additive subgroup of the real D-space $\mathbb{R}^D$. W.l.o.g., we can assume that

$$\Lambda = \{u_1v_1 + u_2v_2 + \cdots + u_Dv_D : u_1,\ldots,u_D \in \mathbb{Z}\}, \quad (1)$$

where $\{v_1,v_2,\ldots,v_D\}$ is a set of linearly independent vectors in $\mathbb{R}^D$. A lattice Λ defined by (1) is a sublattice of $\mathbb{Z}^D$ if and only if $\{v_1,v_2,\ldots,v_D\} \subset \mathbb{Z}^D$. We will be interested solely in sublattices of $\mathbb{Z}^D$ since our shapes are defined in $\mathbb{Z}^D$. The vectors $v_1,v_2,\ldots,v_D$ are called a *base* for $\Lambda \subseteq \mathbb{Z}^D$, and the $D \times D$ matrix

$$\mathbf{G} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1D} \\ v_{21} & v_{22} & \cdots & v_{2D} \\ \vdots & \vdots & \ddots & \vdots \\ v_{D1} & v_{D2} & \cdots & v_{DD} \end{bmatrix}$$

having these vectors as its rows is said to be a *generator matrix* for Λ.

The *volume* of a lattice Λ, denoted by $V(\Lambda)$, is inversely proportional to the number of lattice points per unit volume. More precisely, $V(\Lambda)$ may be defined as the volume of the *fundamental parallelogram* $\Pi(\Lambda)$ in $\mathbb{R}^D$, which is given by

$$\Pi(\Lambda) \stackrel{\text{def}}{=} \{\xi_1v_1+\xi_2v_2+\cdots+\xi_Dv_D : 0 \le \xi_i < 1, 1 \le i \le D\}.$$

There is a simple expression for the volume of Λ, namely, $V(\Lambda) = |\det \mathbf{G}|$.

We say that Λ is a *lattice tiling* for $\mathcal{S}$ if the lattice points can be taken as the set $\mathcal{T}$ to form a tiling $(\mathcal{T},\mathcal{S})$. In this case we have that $|\mathcal{S}| = V(\Lambda) = |\det \mathbf{G}|$.

There is a large variety of literature about tiling and lattices. We will refer the reader to two of the most interesting and comprehensive books [54], [55].

Remark 3: Note, that different generator matrices for the same lattice will result in different fundamental parallelograms. This is related to the fact that the same lattice can induce a tiling for different shapes with the same volume. A fundamental parallelogram is always a shape in $\mathbb{R}^D$ which is tiled by Λ (usually this is not a shape in $\mathbb{Z}^D$ and as a consequence, most and usually all, of the shapes in $\mathbb{Z}^D$ are not fundamental parallelograms).

Lattice is a very fundamental structure in various coding problems, e.g., [56]–[58] is a small sample which does not mean to be representative. Lattices are also applied in multidimensional coding, e.g., [22]. This paper exhibits a new application of lattices for multidimensional coding and for discrete geometry problems. To conclude this section we give the following lemma whose proof is left as an exercise to the reader.

Lemma 2: Let Λ be a D-dimensional lattice, with a generator matrix $\mathbf{G}$, and $\mathcal{S}$ be a D-dimensional shape. Λ is a lattice tiling for $\mathcal{S}$ if and only if $|\det \mathbf{G}| = |\mathcal{S}|$ and there are no two points $(i_1,i_2,\ldots,i_D)$ and $(j_1,j_2,\ldots,j_D)$ in any copy of $\mathcal{S}$ such that $(i_1-j_1,i_2-j_2,\ldots,i_D-j_D)$ is a lattice point.

III. The Generalized Folding Method

In this section, we will generalize the definition of folding. All the previous three definitions (**F1**, **F2**, and **F3**) are special cases of the new definition. The new definition involves a lattice tiling Λ, for a shape $\mathcal{S}$ on which the folding is performed.

A *direction* of length $D, (d_1,d_2,\ldots,d_D)$, is a nonzero integer word of length D, where $d_i \in \mathbb{Z}$.

Let $\mathcal{S}$ be a D-dimensional shape and let $\delta = (d_1,d_2,\ldots,d_D)$ be a direction of length D. Let Λ be a lattice tiling for a shape $\mathcal{S}$, and let $\mathcal{S}_1$ be the copy of $\mathcal{S}$, in the related tiling, which includes the origin. We define recursively a *folded-row* starting in the origin. If the point $(i_1,i_2,\ldots,i_D)$ is the current point of $\mathcal{S}_1$ in the folded-row, then the next point on its folded-row is defined as follows:

- If the point $(i_1+d_1,i_2+d_2,\ldots,i_D+d_D)$ is in $\mathcal{S}_1$ then it is the next point on the folded-row.
- If the point $(i_1+d_1,i_2+d_2,\ldots,i_D+d_D)$ is in $\mathcal{S}_2 \neq \mathcal{S}_1$ whose center is in the point $(c_1,c_2,\ldots,c_D)$ then $(i_1+d_1-c_1,i_2+d_2-c_2,\ldots,i_D+d_D-c_D)$ is the next point on the folded-row (by Lemma 1 this point is in $\mathcal{S}_1$).

The new definition of folding is based on a lattice Λ, a shape $\mathcal{S}$, and a *direction* δ. The triple $(\Lambda,\mathcal{S},\delta)$ defines a *folding* if the definition yields a folded-row which includes all the elements of $\mathcal{S}$. It will be proved that only Λ and δ determine whether the triple $(\Lambda,\mathcal{S},\delta)$ defines a folding. The role of $\mathcal{S}$ is only in the order of the elements in the folded-row; and of course Λ must define a lattice tiling for $\mathcal{S}$. Different lattice tilings for the same shape $\mathcal{S}$ can function completely different in this respect. Also, not all directions for the same lattice tiling of the shape $\mathcal{S}$ should define (or not define) a folding.

Remark 4: It is not difficult to see that the three folding defined earlier (**F1**, **F2**, and **F3**) are special cases of the new definition. The definition of the generator matrices for the three corresponding lattices are left as an exercise to the interested reader.

How many different folded-rows do we have? In other words, how many different folding operations are defined in this way? It can readily verified that there are at most $|\mathcal{S}|-1$ different folded-rows. If Λ with the direction $(d_1,d_2,\ldots,d_D)$ defines a folding then also Λ with the direction vector $(-d_1,-d_2,\ldots,-d_D)$ defines a folding. The two folded-rows are in reverse order, and hence they will be considered to be *equivalent*. If two folded-rows are not equal and not a reverse pair then they will considered to be *nonequivalent*. The question whether for each D, there exists a D-dimensional shape $\mathcal{S}$ with $\lfloor \frac{|\mathcal{S}|-1}{2} \rfloor$ nonequivalent folded-rows will be partially answered in the sequel.

How do we fold a sequence into a shape $\mathcal{S}$? Let Λ be a lattice tiling for the shape $\mathcal{S}$ for which $n = |\mathcal{S}|$. Let δ be a direction for which $(\Lambda, \mathcal{S}, \delta)$ defines a folding and let $\mathcal{B} = b_0 b_1 \ldots b_{n-1}$ be a sequence of length n. The folding of $\mathcal{B}$ induced by $(\Lambda, \mathcal{S}, \delta)$ is denoted by $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$ and is defined as the shape $\mathcal{S}$ with the elements of $\mathcal{B}$, where b_i is in the ith entry of the folded-row of $\mathcal{S}$ defined by $(\Lambda, \mathcal{S}, \delta)$.

Next, we aim to find sufficient and necessary conditions that a triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding. We start with a simple characterization for the order of the elements in a folded-row.

Lemma 3: Let Λ be a lattice tiling for the shape $\mathcal{S}$ and let $\delta = (d_1, d_2, \ldots, d_D)$ be a direction. Let $g(i) = (i \cdot d_1, \ldots, i \cdot d_D) - c(i \cdot d_1, \ldots, i \cdot d_D)$ and let i_1, i_2 be two integers. Then $g(i_1) = g(i_2)$ if and only if $g(i_1 + 1) = g(i_2 + 1)$.

Proof: The lemma follows immediately from the observation that $g(i_1) = g(i_2)$ if and only if $(i_1 \cdot d_1, \ldots, i_1 \cdot d_D)$ and $(i_2 \cdot d_1, \ldots, i_2 \cdot d_D)$ are the same related positions in $\mathcal{S}$, i.e., correspond to the same position of the folded-row. ■

The next two lemmas are an immediate consequence of the definitions and provide a concise condition whether the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding.

Lemma 4: Let Λ be a lattice tiling for the shape $\mathcal{S}$ and let $\delta = (d_1, d_2, \ldots, d_D)$ be a direction. $(\Lambda, \mathcal{S}, \delta)$ defines a folding if and only if the set $\{(i \cdot d_1, i \cdot d_2, \ldots, i \cdot d_D) - c(i \cdot d_1, i \cdot d_2, \ldots, i \cdot d_D) : 0 \le i < |\mathcal{S}|\}$ contains $|\mathcal{S}|$ distinct elements.

Proof: The lemma is an immediate consequence of Lemmas 1, 3, and the definition of folding. ■

Lemma 5: Let Λ be a lattice tiling for the shape $\mathcal{S}$ and let $\delta = (d_1, d_2, \ldots, d_D)$ be a direction. $(\Lambda, \mathcal{S}, \delta)$ defines a folding if and only if $(|\mathcal{S}| \cdot d_1, \ldots, |\mathcal{S}| \cdot d_D) - c(|\mathcal{S}| \cdot d_1, \ldots, |\mathcal{S}| \cdot d_D) = (0, \ldots, 0)$ and for each $i, 0 < i < |\mathcal{S}|$ we have $(i \cdot d_1, \ldots, i \cdot d_D) - c(i \cdot d_1, \ldots, i \cdot d_D) \neq (0, \ldots, 0)$.

Proof: Assume first that $(\Lambda, \mathcal{S}, \delta)$ defines a folding. If for some $0 < j < |\mathcal{S}|$ we have $(j \cdot d_1, \ldots, j \cdot d_D) - c(j \cdot d_1, \ldots, j \cdot d_D) = (0, \ldots, 0)$ then $g(j) = g(0)$ and hence by Lemma 3 the folded-row will have at most j elements of $\mathcal{S}$. Since $j < |\mathcal{S}|$ we will have that $(\Lambda, \mathcal{S}, \delta)$ does not define a folding. On the other hand, Lemma 3 also implies that if $(\Lambda, \mathcal{S}, \delta)$ defines a folding then $g(|\mathcal{S}|) = (0, \ldots, 0)$.

Now assume that $(|\mathcal{S}| \cdot d_1, \ldots, |\mathcal{S}| \cdot d_D) - c(|\mathcal{S}| \cdot d_1, \ldots, |\mathcal{S}| \cdot d_D) = (0, \ldots, 0)$ and for each i, $0 < i < |\mathcal{S}|$ we have $(i \cdot d_1, \ldots, i \cdot d_D) - c(i \cdot d_1, \ldots, i \cdot d_D) \neq (0, \ldots, 0)$. Let $0 < i_1 < i_2 < |\mathcal{S}|$; if $g(i_1) = g(i_2)$ then by Lemma 3 we have $g(i_2 - i_1) = g(0) = (0, \ldots, 0)$, a contradiction. Therefore, the folded-row contains all the elements of $\mathcal{S}$ and hence by definition $(\Lambda, \mathcal{S}, \delta)$ defines a folding. ■

Corollary 1: If $(\Lambda, \mathcal{S}, \delta), \delta = (d_1, d_2, \ldots, d_D)$, defines a folding then the point $(|\mathcal{S}| \cdot d_1, \ldots, |\mathcal{S}| \cdot d_D)$ is a lattice point.

Before considering the general D-dimensional case we want to give a simple condition to check whether the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding in the two-dimensional case.

Lemma 6: Let G be the generator matrix of a lattice Λ and let $s = |\det G|$. Then the points $(0, s)$, $(s, 0)$, (s, s), and $(s, -s)$ are lattice points.

Proof: It is sufficient to prove that the points $(0, s), (s, 0)$ are lattice points. Let Λ be a lattice whose generator matrix is given by

$$G = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}.$$

i.e., $s = v_{11}v_{22} - v_{12}v_{21}$. Since $v_{22}(v_{11}, v_{12}) - v_{12}(v_{21}, v_{22}) = (s, 0)$ and $v_{11}(v_{21}, v_{22}) - v_{21}(v_{11}, v_{12}) = (0, s)$, it follows that $(0, s), (s, 0)$ are lattice points. ■

Theorem 1: Let Λ be a lattice whose generator matrix is given by

$$G = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}.$$

Let d_1 and d_2 be two positive integers and $\tau = \text{g.c.d.}(d_1, d_2)$. If Λ defines a lattice tiling for the shape $\mathcal{S}$ then the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding as follows:

- with the direction $\delta = (+d_1, +d_2)$ if and only if $\text{g.c.d.}(\frac{d_1 v_{22} - d_2 v_{21}}{\tau}, \frac{d_2 v_{11} - d_1 v_{12}}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$;
- with the direction $\delta = (+d_1, -d_2)$ if and only if $\text{g.c.d.}(\frac{d_1 v_{22} + d_2 v_{21}}{\tau}, \frac{d_2 v_{11} + d_1 v_{12}}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$;
- with the direction $\delta = (+d_1, 0)$ if and only if $\text{g.c.d.}(v_{12}, v_{22}) = 1$ and $\text{g.c.d.}(d_1, |\mathcal{S}|) = 1$;
- with the direction $\delta = (0, +d_2)$ if and only if $\text{g.c.d.}(v_{11}, v_{21}) = 1$ and $\text{g.c.d.}(d_2, |\mathcal{S}|) = 1$.

G is taken in a way that the parameters in the term "g.c.d.$(\cdot, \cdot)$" are nonzero for the related direction.

Proof: We will prove the case where $\delta = (+d_1, +d_2)$; the other three cases are proved similarly.

Let Λ be a lattice tiling for the shape $\mathcal{S}$. By Lemma 6 we have that $(|\mathcal{S}| \cdot d_1, |\mathcal{S}| \cdot d_2)$ is a lattice point. Therefore, there exist two integers α_1 and α_2 such that $\alpha_1(v_{11}, v_{12}) + \alpha_2(v_{21}, v_{22}) = (|\mathcal{S}| \cdot d_1, |\mathcal{S}| \cdot d_2)$, i.e., $\alpha_1 v_{11} + \alpha_2 v_{21} = d_1|\mathcal{S}|, \alpha_1 v_{12} + \alpha_2 v_{22} = d_2|\mathcal{S}|$, and $|\mathcal{S}| = v_{11}v_{22} - v_{12}v_{21}$. These equations have exactly one solution, $\alpha_1 = d_1 v_{22} - d_2 v_{21}$ and $\alpha_2 = d_2 v_{11} - d_1 v_{12}$. By Lemma 5, $(\Lambda, \mathcal{S}, \delta)$ defines a folding if and only if $(|\mathcal{S}| \cdot d_1, |\mathcal{S}| \cdot d_2) = c(|\mathcal{S}| \cdot d_1, |\mathcal{S}| \cdot d_2)$ and for each $i, 0 < i < |\mathcal{S}|$ we have $(i \cdot d_1, i \cdot d_2) \neq c(i \cdot d_1, i \cdot d_2)$.

Assume first that $\text{g.c.d.}(\frac{d_1 v_{22} - d_2 v_{21}}{\tau}, \frac{d_2 v_{11} - d_1 v_{12}}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$. Assume for the contrary, that there exist three integers i, β_1, and β_2, such that $\beta_1(v_{11}, v_{12}) + \beta_2(v_{21}, v_{22}) = (i \cdot d_1, i \cdot d_2), 0 < i < |\mathcal{S}|$. Hence we have, $\frac{\beta_2}{\beta_1} = \frac{d_2 v_{11} - d_1 v_{12}}{d_1 v_{22} - d_2 v_{21}} = \frac{\alpha_2}{\alpha_1}$. Since $\text{g.c.d.}(\frac{d_1 v_{22} - d_2 v_{21}}{\tau}, \frac{d_2 v_{11} - d_1 v_{12}}{\tau}) = 1$ it follows that $\beta_1 = \gamma \frac{d_1 v_{22} - d_2 v_{21}}{\tau}$ and $\beta_2 = \gamma \frac{d_2 v_{11} - d_1 v_{12}}{\tau}$, for some $0 < \gamma < \tau$. Therefore, we have $i \cdot d_1 = \beta_1 v_{11} + \beta_2 v_{21} = \frac{\gamma d_1 |\mathcal{S}|}{\tau}$, i.e., $i = \frac{\gamma |\mathcal{S}|}{\tau}$. But, since $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$ it follows that $\gamma = \rho\tau$, for some integer $\rho > 0$, a contradiction to the fact that $0 < \gamma < \tau$. Hence, our assumption on the existence of three integers i, β_1, and β_2 is false. Thus, by Lemma 5 we have that if $\text{g.c.d.}(\frac{d_1 v_{22} - d_2 v_{21}}{\tau}, \frac{d_2 v_{11} - d_1 v_{12}}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$ then $(\Lambda, \mathcal{S}, \delta)$ defines a folding with the direction $\delta = (+d_1, +d_2)$.

Assume now that $(\Lambda, \mathcal{S}, \delta)$ defines a folding with the direction $\delta = (+d_1, +d_2)$. Assume for the contrary that $\text{g.c.d.}(\frac{d_1 v_{22} - d_2 v_{21}}{\tau}, \frac{d_2 v_{11} - d_1 v_{12}}{\tau}) = \nu_1 > 1$ or $\text{g.c.d.}(\tau, |\mathcal{S}|) = \nu_2 > 1$. We distinguish now between two cases.

Case 1: If $\text{g.c.d.}(\frac{d_1v_{22}-d_2v_{21}}{\tau}, \frac{d_2v_{11}-d_1v_{12}}{\tau}) = \nu_1 > 1$ then $\beta_1 = \frac{d_1v_{22}-d_2v_{21}}{\tau\nu_1}$ and $\beta_2 = \frac{d_2v_{11}-d_1v_{12}}{\tau\nu_1}$ are integers. Therefore, $\beta_1(v_{11}, v_{12}) + \beta_2(v_{21}, v_{22}) = (\frac{|\mathcal{S}|\cdot d_1}{\tau\nu_1}, \frac{|\mathcal{S}|\cdot d_2}{\tau\nu_1})$. Hence, $\frac{|\mathcal{S}|}{\nu_1}$ is an integer and for the integers $\beta_1' = \frac{d_1v_{22}-d_2v_{21}}{\nu_1}$ and $\beta_2' = \frac{d_2v_{11}-d_1v_{12}}{\nu_1}$ we have $\beta_1'(v_{11}, v_{12}) + \beta_2'(v_{21}, v_{22}) = (\frac{|\mathcal{S}|}{\nu_1}d_1, \frac{|\mathcal{S}|}{\nu_1}d_2)$, i.e., $(\frac{|\mathcal{S}|}{\nu_1}d_1, \frac{|\mathcal{S}|}{\nu_1}d_2)$ is a lattice point, and as a consequence by Lemma 5 we have that $(\Lambda, \mathcal{S}, \delta)$ does not define a folding, a contradiction.

Case 2: If $\text{g.c.d.}(\tau, |\mathcal{S}|) = \nu_2 > 1$ then let $\beta_1 = \frac{d_1v_{22}-d_2v_{21}}{\nu_2}$ and $\beta_2 = \frac{d_2v_{11}-d_1v_{12}}{\nu_2}$. Hence, $\beta_1(v_{11}, v_{12}) + \beta_2(v_{21}, v_{22}) = (\frac{|\mathcal{S}|}{\nu_2}d_1, \frac{|\mathcal{S}|}{\nu_2}d_2)$. Clearly, β_1, β_2, and $\frac{|\mathcal{S}|}{\nu_2}$ are integers, and as a consequence by Lemma 5 we have that $(\Lambda, \mathcal{S}, \delta)$ does not define a folding, a contradiction.

Therefore, if $(\Lambda, \mathcal{S}, \delta)$ defines a folding with the direction $\delta = (+d_1, +d_2)$ then $\text{g.c.d.}(\frac{d_1v_{22}-d_2v_{21}}{\tau}, \frac{d_2v_{11}-d_1v_{12}}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$. ■

The generalization of Theorem 1 for the D-dimensional case is Theorem 16 given in Appendix A. The most important types of directions (used for **F1**, **F2**, and **F3**), are those in which the points P and $\delta + P$, where δ is the direction, are adjacent for any given point P, i.e., if $\delta = (d_1, d_2, \ldots, d_D)$ then $|d_i| \leq 1$ for each $i, 1 \leq i \leq D$. For these types of directions we have the following result.

Corollary 2: Let Λ be a lattice whose generator matrix is given by

$$G = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}.$$

If Λ defines a lattice tiling for the shape $\mathcal{S}$ then the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding

- with the direction $\delta = (+1, +1)$ if and only if $\text{g.c.d.}(v_{22} - v_{21}, v_{11} - v_{12}) = 1$;
- with the direction $\delta = (+1, -1)$ if and only if $\text{g.c.d.}(v_{22} + v_{21}, v_{11} + v_{12}) = 1$;
- with the direction $\delta = (+1, 0)$ if and only if $\text{g.c.d.}(v_{12}, v_{22}) = 1$;
- with the direction $\delta = (0, +1)$ if and only if $\text{g.c.d.}(v_{11}, v_{21}) = 1$.

G is taken in a way that the parameters in the term "$\text{g.c.d.}(\cdot, \cdot)$" are nonzero for the related direction.

There are cases when we can determine immediately without going into all the computations, whether $(\Lambda, \mathcal{S}, \delta)$ defines a folding. It will be a consequence of the following lemmas.

Lemma 7:

- The number of elements in a folded-row does not depend on the point chosen to be the center of $\mathcal{S}$.
- The number of elements in a folded-row is a divisor of $|\mathcal{S}| = V(\Lambda)$.

Proof: By Lemmas 3 and 5 and the definition of the folded-row, if we start the folded-row in the origin then the number of elements in the folded-row is the smallest t such that $t \cdot \delta$ is a lattice point (since the folded-row starts at a lattice point and ends one step before it reaches again a lattice point). This implies that the number of elements in a folded-row does not depend on the point of $\mathcal{S}$ chosen to be the center of $\mathcal{S}$. We can make any point of $\mathcal{S}$ to be the center of $\mathcal{S}$ and hence any point can be at the origin. Therefore, all folded-rows with the direction δ have t elements. For a given lattice Λ and a direction δ, any two folded-rows are either equal or disjoint. Hence t must be a divisor $|\mathcal{S}|$ and t does not depend on which point of $\mathcal{S}$ is the center. ■

The next lemma is an immediate consequence from the definition of a folded-row.

Lemma 8: The number of elements in a folded-row is one if and only if δ is a lattice point.

Corollary 3: Let Λ be a lattice tiling for a shape $\mathcal{S}$. If the volume of Λ is a prime number then $(\Lambda, \mathcal{S}, \delta)$ defines a folding with any direction δ, unless δ is a lattice point.

Lemma 9: Let Λ be a lattice tiling for the shape $\mathcal{S}$. Let $(d_1, d_2, \ldots, d_D)$ be a direction, $(i_1, i_2, \ldots, i_D)$ be a lattice point, and the point $(d_1, d_2, \ldots, d_D)$ is in the shape $\mathcal{S}$ whose center is in the origin. Then the folded-rows defined by the directions $(d_1, d_2, \ldots, d_D)$ and $(i_1 + d_1, i_2 + d_2, \ldots, i_d + d_D)$ are equivalent.

Proof: Follows immediately from the observation that $c(i_1 + d_1, i_2 + d_2, \ldots, i_d + d_D) = (i_1, i_2, \ldots, i_D)$. ■

In view of Lemma 9 we should examine only the $|\mathcal{S}| - 1$ directions related to the points of $\mathcal{S}$ whose center is in the origin. Hence, in the sequel each direction $\delta = (d_1, d_2, \ldots, d_D)$ will have the property that the point $(d_1, d_2, \ldots, d_D)$ will be contained in the copy of $\mathcal{S}$ whose center is in the origin. One might puzzle how this relates to the observation that the necessary and sufficient conditions that a direction defines a folding depend only on the generator matrix of Λ and not on $\mathcal{S}$? The answer is that the folded-row itself is defined on the elements of $\mathcal{S}$. Therefore, Λ will have different directions and folded-rows depending on the shape $\mathcal{S}$.

Lemma 10: Let Λ be a lattice tiling for the shape $\mathcal{S}, n = |\mathcal{S}|$. Let $\delta = (d_1, d_2, \ldots, d_D)$ be a direction and let $f_0 f_1 \ldots f_{n-1}$ be its folded-row, where $f_0 = (0, 0, \ldots, 0)$ and $f_1 = (d_1, d_2, \ldots, d_D)$. Then the direction $\delta' = f_i$ defines a folding if and only if $\text{g.c.d.}(i, n) = 1$. If the direction $\delta' = f_i$ defines a folding then its folded-row is $f_0 f_i f_{2i} \ldots f_{n-i}$, where indices are taken modulo n.

Proof: By definition and by Lemma 3 we have that $\delta' = f_i = (i \cdot d_1, i \cdot d_2, \ldots, i \cdot d_D) - c(i \cdot d_1, i \cdot d_2, \ldots, i \cdot d_D)$ and $f_{\ell \cdot i} = (\ell \cdot i \cdot d_1, \ell \cdot i \cdot d_2, \ldots, \ell \cdot i \cdot d_D) - c(\ell \cdot i \cdot d_1, \ell \cdot i \cdot d_2, \ldots, \ell \cdot i \cdot d_D)$. Since the sequence $f_0 f_1 \ldots f_{n-1}$ consists of n distinct points of $\mathbb{Z}^D$, it follows that the sequence $f_0 f_i f_{2i} \ldots f_{n-i}$ consists of n distinct points of $\mathbb{Z}^D$ if and only if $\text{g.c.d.}(i, n) = 1$. Thus, the lemma follows. ■

Corollary 4: Let Λ be a lattice tiling for the shape $\mathcal{S}$. There exists at least one folding with respect to Λ if and only if the number of nonequivalent folding operations with respect to Λ is $\frac{\phi(|\mathcal{S}|)}{2}$, where $\phi(\cdot)$ is the Euler function.

By considering Corollary 3, we obtain the following corollary.

Corollary 5: Let Λ be a lattice tiling for the shape $\mathcal{S}$. If $|\mathcal{S}|$ is a prime number then there exists $\frac{|\mathcal{S}|-1}{2}$ different directions which form $\frac{|\mathcal{S}|-1}{2}$ nonequivalent folded-rows.

Corollary 4 implies that once we have one folding operation with its folded-row, then we can easily find and compute all the other folding operations with their folded-rows. It also implies that once the necessary and sufficient conditions for the existence of one folding in the related theorems are satisfied, then the necessary and sufficient conditions for the existence of other foldings are also satisfied. Nevertheless, there are cases in which no direction defines a folding.

Lemma 11: Let γ a positive integer greater than one, $a_1, a_2, \ldots, a_D$, be nonzero integers, and $b_1, b_2, \ldots, b_D$ be nonzero integers such that either $b_i = a_i$ or $b_i = a_i\gamma$, for each $1 \le i \le D$, and $|\{i : b_i = a_i\gamma, 1 \le i \le D\}| \ge 2$. Let $\mathcal{S}$ be a D-dimensional shape and Λ be a lattice tiling for $\mathcal{S}$ whose generator matrix is given by

$$\begin{bmatrix} b_1 & 0 & \ldots & 0 \\ 0 & b_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b_D \end{bmatrix}.$$

Then there is no direction δ for which the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding.

Proof: Let $\delta = (d_1, d_2, \ldots, d_D)$ be any direction and let $\sigma = \gamma \prod_{i=1}^{D} a_i$. Then, $\sigma < |\mathcal{S}|$ and for any given shape $\mathcal{S}$ for which Λ is a lattice tiling we have $(\sigma \cdot d_1, \sigma \cdot d_2, \ldots, \sigma \cdot d_D) - c(\sigma \cdot d_1, \sigma \cdot d_2, \ldots, \sigma \cdot d_D) = (0, 0, \ldots, 0)$. Hence, by Lemma 5, the triple $(\Lambda, \mathcal{S}, \delta)$ does not define a folding. ■

IV. Bounds on Synchronization Patterns

Our original motivation for the generalization of the folding operation came from the design of two-dimensional synchronization patterns. Given a grid (square or hexagonal) and a shape $\mathcal{S}$ on the grid, we would like to find what is the largest set Δ of dots on grid points, $|\Delta| = m$, located in $\mathcal{S}$, such that the following property hold. All the $\binom{m}{2}$ lines between dots in Δ are distinct either in their length or in their slope. Such a shape $\mathcal{S}$ with dots is called a *distinct difference configuration* (DDC). If $\mathcal{S}$ is an $m \times m$ array with exactly one dot in each row and each column then $\mathcal{S}$ is called a Costas array [5]. If $\mathcal{S}$ is a $k \times m$ array with exactly one dot in each column then $\mathcal{S}$ is called a sonar sequence [5]. If $\mathcal{S}$ is a $k \times n$ DDC array then $\mathcal{S}$ is called a Golomb rectangle [7]. These patterns have various applications as described in [5]. A new application of these patterns to the design of key predistribution scheme for wireless sensor networks was described lately in [13]. In this application the shape $\mathcal{S}$ might be a Lee sphere, an hexagon, or a circle, and sometimes another regular polygon. This application requires in some cases to consider these shapes in the hexagonal grid. **F3** was used for this application in [14] to form a DDC whose shape is a rectangle rotated in 45 degrees on the square grid (see Fig. 1). Henceforth, we assume that our grid is $\mathbb{Z}^D$, i.e., the square grid for $D = 2$. Since all the results of the previous sections hold for D-dimensional shapes we will continue to state the results in a D-dimensional language, even so the applied part for synchronization patterns is two-dimensional.

We will generalize some of the definitions given for DDCs in two-dimensional arrays [14] for multidimensional arrays. The reason is not just the generalization, but we also need these definitions in the sequel. Let $\mathcal{A}$ be a (generally infinite) D-dimensional array of dots in $\mathbb{Z}^D$, and let $\eta_1, \eta_2, \ldots, \eta_D$ be positive integers. We say that $\mathcal{A}$ is a *multiperiodic* (or *doubly periodic* if $D = 2$) with period $(\eta_1, \eta_2, \ldots, \eta_D)$ if $\mathcal{A}(i_1, i_2, \ldots, i_D) = \mathcal{A}(i_1 + \eta_1, i_2, \ldots, i_D) = \mathcal{A}(i_1, i_2 + \eta_2, \ldots, i_D) = \cdots = \mathcal{A}(i_1, i_2, \ldots, i_D + \eta_D)$. We define the *density* of $\mathcal{A}$ to be $d/(\Pi_{j=1}^{D} \eta_j)$, where d is the number of dots in any $\eta_1 \times \eta_2 \times \cdots \times \eta_D$ subarray of $\mathcal{A}$. Note that the period $(\eta_1, \eta_2, \ldots, \eta_D)$ might not be unique, but that the density of $\mathcal{A}$ does not depend on the period we choose. We say that a multiperiodic array $\mathcal{A}$ of dots is a *multiperiodic* $n_1 \times n_2 \times \cdots n_D$ *DDC* if every $n_1 \times n_2 \times \cdots n_D$ subarray of $\mathcal{A}$ is a DDC.

We write $(i_1, i_2, \ldots, i_D) + \mathcal{S}$ for the shifted copy $\{(i_1 + i'_1, i_2 + i'_2, \ldots, i_D + i'_D) : (i'_1, i'_2, \ldots, i'_D) \in \mathcal{S}\}$ of $\mathcal{S}$. We say that a multiperiodic array $\mathcal{A}$ is a *multiperiodic $\mathcal{S}$-DDC* if the dots contained in every shift $(i_1, i_2, \ldots, i_D) + \mathcal{S}$ of $\mathcal{S}$ form a DDC.

The definition of the density is given based on periodicity of a D-dimensional box. If μ is the density, of the multiperiodic array $\mathcal{A}$, it implies that given a shape $\mathcal{S}$, the average number of dots in any shape $\mathcal{A}$ shifted all over $\mathcal{S}$ is $\mu|\mathcal{S}|$. This leads to the following theorem given in [14] for the two-dimensional case and which has a similar proof for the multidimensional case.

Theorem 2: Let $\mathcal{S}$ be a shape, and let $\mathcal{A}$ be a multiperiodic $\mathcal{S}$-DDC of density μ. Then there exists a set of at least $\lceil \mu|\mathcal{S}| \rceil$ dots contained in $\mathcal{S}$ that form a DDC.

Another important observation from the definition of multiperiodic $\mathcal{S}$-DDC is the following lemma from [14].

Lemma 12: Let $\mathcal{A}$ be a multiperiodic $\mathcal{S}$-DDC, and let $\mathcal{S}' \subseteq \mathcal{S}$. Then $\mathcal{A}$ is a multiperiodic $\mathcal{S}'$-DDC.

Let $\mathcal{S}_1, \mathcal{S}_2, \ldots$ be an infinite sequence of similar shapes such that $|\mathcal{S}_{i+1}| > |\mathcal{S}_i|$. Using the technique of Erdös and Turán [11], [16], for which a detailed proof is given in [14], one can prove that

Theorem 3: An upper bound on the number of dots in $\mathcal{S}_i, i \to \infty$, is $\lim_{i\to\infty}(\sqrt{|\mathcal{S}_i|} + o(\sqrt{|\mathcal{S}_i|}))$.

Let $\mathcal{S}$ and $\mathcal{S}'$ be two-dimensional shapes in the grid. We will denote by $\Delta(\mathcal{S}, \mathcal{S}')$ the largest intersection between $\mathcal{S}$ and $\mathcal{S}'$ in any orientation. Our bounds on the number of dots in a DDC with a given shape are based on the following result.

Theorem 4: Assume we are given a multiperiodic $\mathcal{S}$-DDC array $\mathcal{A}$ with density μ. Let $\mathcal{Q}$ be another shape on $\mathbb{Z}^D$. Then there exists a copy of $\mathcal{Q}$ on $\mathbb{Z}^D$ with at least $\lceil \mu \cdot \Delta(\mathcal{S}, \mathcal{Q}) \rceil$ dots.

Proof: Let $\mathcal{Q}'$ be the shape such that $\mathcal{Q}' = \mathcal{S} \cap \mathcal{Q}$ and $|\mathcal{Q}'| = \Delta(\mathcal{S}, \mathcal{Q})$. By Lemma 12, we have that $\mathcal{A}$ is a multiperiodic $\mathcal{Q}'$-DDC. By Theorem 2, there exists a set of at least $\lceil \mu|\mathcal{Q}'| \rceil$ dots contained in $\mathcal{S}$ that form a DDC. Thus, there exists a copy of $\mathcal{Q}$ on $\mathbb{Z}^D$ with at least $\lceil \mu \cdot \Delta(\mathcal{S}, \mathcal{Q}) \rceil$ dots. ■

In order to apply Theorem 4, we will use folding of the sequences defined as follows. Let A be an Abelian group, and let $\mathcal{B} = \{b_1, b_2, \ldots, b_m\} \subseteq A$ be a sequence of m distinct elements of A. We say that $\mathcal{B}$ is a *B_2-sequence over A* if all the sums $a_{i_1} + a_{i_2}$ with $1 \le i_1 \le i_2 \le m$ are distinct. For a survey on B_2-sequences and their generalizations the reader is referred to [59]. The following lemma is well known and can be readily verified.

Lemma 13: A subset $\mathcal{B} = \{a_1, a_2, \ldots, a_m\} \subseteq A$ is a B_2-sequence over A if and only if all the differences $a_{i_1} - a_{i_2}$ with $1 \le i_1 \ne i_2 \le m$ are distinct in A.

Note that if $\mathcal{B}$ is a B_2-sequence over $\mathbb{Z}_n$ and $a \in \mathbb{Z}_n$, then so is the shift $a + B = \{a + e : e \in B\}$. The following theorem, due to Bose [60], shows that large B_2-sequences over $\mathbb{Z}_n$ exist for many values of n.

Theorem 5: Let q be a prime power. Then there exists a B_2-sequence $a_1, a_2, \ldots, a_m$ over $\mathbb{Z}_n$ where $n = q^2 - 1$ and $m = q$.

A. A Lattice Coloring for a Given Shape

In this section, we will describe how we apply folding to obtain a DDC with a shape $\mathcal{S}$ and a multiperiodic $\mathcal{S}$-DDC. Let Λ be a lattice tiling for $\mathcal{S}$ and let $\delta = (d_1, d_2, \ldots, d_D)$ be a direction such that $(\Lambda, \mathcal{S}, \delta)$ defines a folding. We assign an integer from $\mathbb{Z}_n, n = |\mathcal{S}|$, to each point of $\mathbb{Z}^D$. The *lattice coloring* $\mathcal{C}(\Lambda, \delta)$ is defined as follows. We assign 0 to the point $(0, 0, \ldots, 0)$ and 1 to the next element of the folded-row and so on until $|\mathcal{S}| - 1$ is assigned to the last element of the folded-row. This complete the coloring of the points in the shape $\mathcal{S}$ whose center is the origin. To position $(i_1, i_2, \ldots, i_D)$ we assign the color of position $(i_1, i_2, \ldots, i_D) - c(i_1, i_2, \ldots, i_D)$. The color of position $(i_1, i_2, \ldots, i_D)$ will be denoted by $\mathcal{C}(i_1, i_2, \ldots, i_D)$.

We will generalize the definition of folding a sequence into a shape $\mathcal{S}$ by the direction δ, given the lattice tiling Λ for $\mathcal{S}$. The folding of a sequence $\mathcal{B} = b_0 b_1 \ldots b_{n-1}$ into an array colored by the elements of $\mathbb{Z}_n$ is defined by assigning the value b_i to all the points of the array colored with the color i. If the coloring was defined by the use of the folding as described in this subsection, we say that the array is defined by $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$. Note, that we use the same notation for folding the sequence $\mathcal{B}$ into the shape $\mathcal{S}$. The one to which we refer should be understood from the context.

Given a point $(i_1, i_2, \ldots, i_D) \in \mathbb{Z}^D$, we say that the set of points $\{(i_1 + \ell \cdot d_1, i_2 + \ell \cdot d_2, \ldots, i_D + \ell \cdot d_D) : \ell \in \mathbb{Z}\}$ is a *row of $\mathbb{Z}^D$ defined by $\delta = (d_1, d_2, \ldots, d_D)$*. This is also the row of $(i_1, i_2, \ldots, i_D)$ defined by δ.

Lemma 14: If the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding then in any row of $\mathbb{Z}^D$ defined by δ there are lattice points.

Proof: Given a point $(i_1, i_2, \ldots, i_D)$ and its color $\mathcal{C}(i_1, i_2, \ldots, i_D)$, then by the definitions of the folding and the coloring we have that $\mathcal{C}(i_1 + d_1, i_2 + d_2, \ldots, i_D + d_D) \equiv \mathcal{C}(i_1, i_2, \ldots, i_D) + 1 (\mathrm{mod} |\mathcal{S}|)$. Hence, the row defined by δ has all the values between 0 and $|\mathcal{S}| - 1$ in their natural order modulo $|\mathcal{S}|$. Therefore, any row defined by δ has lattice points (which are exactly the points of this row which are colored with *zeros*). ■

Corollary 6: If $(i_1, i_2, \ldots, i_D)$, $(i_1 + e_1, i_2 + e_2, \ldots, i_D + e_D)$, $(j_1, j_2, \ldots, j_D)$, and $(j_1 + e_1, j_2 + e_2, \ldots, j_D + e_D)$ are four points of $\mathbb{Z}^D$ then $\mathcal{C}(i_1 + e_1, i_2 + e_2, \ldots, i_D + e_D) - \mathcal{C}(i_1, i_2, \ldots, i_D) \equiv \mathcal{C}(j_1 + e_1, j_2 + e_2, \ldots, j_D + e_D) - \mathcal{C}(j_1, j_2, \ldots, j_D) (\mathrm{mod} |\mathcal{S}|)$.

Proof: By Lemma 14 to each one of these four points there exists a lattice point in its row defined by δ. Let

- $P_1 = (i_1 + \alpha_1 \cdot d_1, i_2 + \alpha_1 \cdot d_2, \ldots, i_D + \alpha_1 \cdot d_D)$ be the lattice point in the row of $(i_1, i_2, \ldots, i_D)$;
- $P_2 = (j_1 + \alpha_2 \cdot d_1, j_2 + \alpha_2 \cdot d_2, \ldots, j_D + \alpha_2 \cdot d_D)$ the lattice point in the row of $(j_1, j_2, \ldots, j_D)$;
- $P_3 = ((i_1 + e_1) + \alpha_3 \cdot d_1, (i_2 + e_2) + \alpha_3 \cdot d_2, \ldots, (i_D + e_D) + \alpha_3 \cdot d_D)$ the lattice point in the row of $(i_1 + e_1, i_2 + e_2, \ldots, i_D + e_D)$.

Therefore, $P_4 = P_2 + P_3 - P_1 = ((j_1 + e_1) + (\alpha_2 + \alpha_3 - \alpha_1) \cdot d_1, (j_2 + e_2) + (\alpha_2 + \alpha_3 - \alpha_1) \cdot d_2, \ldots, (j_D + e_D) + (\alpha_2 + \alpha_3 - \alpha_1) \cdot d_D)$ is also a lattice point. P_4 is a lattice point in the row, defined by δ, of $(j_1 + e_1, j_2 + e_2, \ldots, j_D + e_D)$. All these four points are colored with *zeros*. Hence, $\mathcal{C}(i_1, i_2, \ldots, i_D) \equiv -\alpha_1 (\mathrm{mod} |\mathcal{S}|), \mathcal{C}(i_1 + e_1, i_2 + e_2, \ldots, i_D + e_D) \equiv -\alpha_3 (\mathrm{mod} |\mathcal{S}|), \mathcal{C}(j_1, j_2, \ldots, j_D) \equiv -\alpha_2 (\mathrm{mod} |\mathcal{S}|)$, and $\mathcal{C}(j_1 + e_1, j_2 + e_2, \ldots, j_D + e_D) \equiv -(\alpha_2 + \alpha_3 - \alpha_1) (\mathrm{mod} |\mathcal{S}|)$. Now, the claim of the corollary is readily verified. ■

Corollary 7: If δ' is an integer vector of length D then there exists an integer $e(\delta')$ such that for any given point $P = (i_1, i_2, \ldots, i_D)$ we have $\mathcal{C}(P + \delta') = \mathcal{C}(P) + e(\delta') (\mathrm{mod} |\mathcal{S}|)$.

Corollary 8: If the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding and $\mathcal{B}$ is a B_2-sequence over $\mathbb{Z}_n$, where $n = |\mathcal{S}|$, then the array $\mathcal{A}$ defined by $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$ is multiperiodic.

Proof: Clearly, the array has period $(|\mathcal{S}|, |\mathcal{S}|, \ldots, |\mathcal{S}|)$ and the result follows. ■

Theorem 6: If the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding and $\mathcal{B}$ is a B_2-sequence over $\mathbb{Z}_n$, where $n = |\mathcal{S}|$, then the pattern of dots defined by $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$ is a multiperiodic $\mathcal{S}$-DDC.

Proof: By Corollary 8 the constructed array is multiperiodic.

Since $(\Lambda, \mathcal{S}, \delta)$ defines a folding it follows that the $|\mathcal{S}|$ colors inside the shape $\mathcal{S}$ centered at the origin are all distinct. By Corollary 6, for the four positions $(i_1, i_2, \ldots, i_D), (i_1 + e_1, i_2 + e_2, \ldots, i_D + e_D), (j_1, j_2, \ldots, j_D)$, and $(j_1 + e_1, j_2 + e_2, \ldots, j_D + e_D)$ we have that $\mathcal{C}(i_1 + e_1, i_2 + e_2, \ldots, i_D + e_D) - \mathcal{C}(i_1, i_2, \ldots, i_D) \equiv \mathcal{C}(j_1 + e_1, j_2 + e_2, \ldots, j_D + e_D) - \mathcal{C}(j_1, j_2, \ldots, j_D) (\mathrm{mod} |\mathcal{S}|)$. Hence, at most three of these integers (colors) are contained in $\mathcal{B}$. It implies that if these four points belong to the same copy of $\mathcal{S}$ on the grid then at most three of these points have dots, since the dots are distributed by the B_2-sequence $\mathcal{B}$. Thus, any shape $\mathcal{S}$ on $\mathbb{Z}^D$ will define a DDC and the theorem follows. ■

Corollary 9: If the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding and $\mathcal{B}$ is a B_2-sequence over $\mathbb{Z}_n$, where $n = |\mathcal{S}|$, then the pattern of dots defined by $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$ is a DDC.

Note, that the difference between Theorem 6 and Corollary 9 is related to the folding of $\mathcal{B}$ into $\mathbb{Z}^D$ and the folding of $\mathcal{B}$ into $\mathcal{S}$, respectively. The last lemma is given for completeness.

Lemma 15: If $(\Lambda, \mathcal{S}, \delta)$ defines a folding then the $|\mathcal{S}|$ colors inside any copy of $\mathcal{S}$ on $\mathbb{Z}^D$ are all distinct.

Proof: Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two distinct copies of $\mathcal{S}$ on $\mathbb{Z}^D$. Clearly, $\mathcal{S}_2 = (e_1, \ldots, e_D) + \mathcal{S}_1$. By Corollary 6, for each $(i_1, \ldots, i_D), (j_1, \ldots, j_D), \in \mathcal{S}_1$ we have $\mathcal{C}(i_1+e_1, \ldots, i_D+e_D) - \mathcal{C}(i_1, \ldots, i_D) \equiv \mathcal{C}(j_1+e_1, \ldots, j_D+e_D) - \mathcal{S}(j_1, \ldots, j_D) (\mathrm{mod}\ |\mathcal{S}|)$. Therefore, if $\mathcal{S}_1$ contains $|\mathcal{S}|$ distinct colors then also $\mathcal{S}_2$ contains $|\mathcal{S}|$ distinct colors. The lemma follows now from the fact that $(\Lambda, \mathcal{S}, \delta)$ defines a folding and therefore all the colors in the shape $\mathcal{S}$ whose center is in the origin are distinct. ■

V. Bounds for Specific Shapes

In this section, we will present some lower bounds on the number of dots in some two-dimensional DDCs with specific shapes. In the sequel we will use Theorem 4, Theorem 6, and Corollary 9 to form DDCs with various given shapes and a large number of dots. To examine how good are our lower bounds on the number of dots, in a DDC whose shape is $\mathcal{Q}$, we should know what is the upper bound on the number of dots in a DDC whose shape is $\mathcal{Q}$. By Theorem 3 we have that for a DDC whose shape is a regular polygon or a circle, an upper bound on the number of dots is at most $\sqrt{s} + o(\sqrt{s})$, where the shape contains s points of the square grid and $s \to \infty$. One of the main keys of our constructions, and the usage of the given theory, is the ability to produce a multiperiodic $\mathcal{S}$-DDC, where $\mathcal{S}$ is a rectangle, the ratio between its sides is close as much as we want to any given number γ, and if its area is s then the number of dots in it is $\sqrt{s+1}$. For the construction we will need the well known Dirichlet's Theorem [61, p. 27] and the well known Euclidian Theorem [61, p. 11].

Theorem 7: If a and b are two positive relatively primes integers then the arithmetic progression of terms $ai + b$, for $i = 1, 2, \ldots$, contains an infinite number of primes.

Theorem 8: If α and β are two integers such that $\mathrm{g.c.d.}(\alpha, \beta) = 1$ then there exist two integers c_α and c_β such that $c_\alpha \alpha + c_\beta \beta = 1$.

These well known old foundations are used in the following theorem.

Theorem 9: For each positive number γ and any $\epsilon > 0$, there exist two integers n_1 and n_2 such that $\gamma \le \frac{n_1}{n_2} < \gamma + \epsilon$; and there exists a multiperiodic $\mathcal{S}$-DDC $\mathcal{A}$ with, where $\mathcal{S}$ is an $n_1 \times n_2 = (aR + o(R)) \times (bR + o(R))$ rectangle, $n_1 n_2 = p^2 - 1$ for some prime p, and n_1 is an even integer. Each $n_1 \times n_2$ rectangle in $\mathcal{A}$ has $p = \sqrt{a \cdot b} R + o(R)$ dots.

Proof: Given a positive number γ and an $\epsilon > 0$, it is easy to verify that there exist two integers α and β such that $\sqrt{\gamma} \le \frac{\beta}{\alpha} < \sqrt{\gamma + \epsilon}$ and $\mathrm{g.c.d.}(\alpha, \beta) = 2$. By Theorem 8 there exist two integers c_α, c_β such that either $c_\alpha \alpha + 2 = c_\beta \beta > 0$ or $c_\beta \beta + 2 = c_\alpha \alpha > 0$.

Assume $c_\alpha \alpha + 2 = c_\beta \beta > 0$ (the case where $c_\beta \beta + 2 = c_\alpha \alpha > 0$ is handled similarly). Clearly, any factor of α cannot divide $c_\alpha \alpha + 1$. Since β divides $c_\alpha \alpha + 2$, it follows that a factor of β cannot divide $c_\alpha \alpha + 1$. Hence, $\mathrm{g.c.d.}(\alpha\beta, c_\alpha \alpha + 1) = 1$. Therefore, by Theorem 7 there exist infinitely many primes in the sequence $\alpha\beta R + c_\alpha \alpha + 1$, $R = 1, 2, \ldots$.

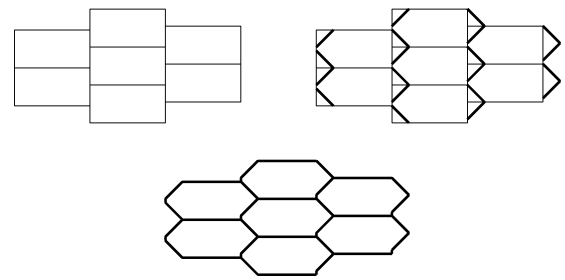


Fig. 2. From rectangle to "almost" quasi-regular hexagon with the same lattice tiling.

Let p be a prime number of the form $\alpha\beta R + c_\alpha \alpha + 1$. Now, $p^2 - 1 = (p+1)(p-1) = (\alpha\beta R + c_\alpha \alpha + 2)(\alpha\beta R + c_\alpha \alpha) = (\alpha\beta R + c_\beta \beta)(\alpha\beta R + c_\alpha \alpha) = (\alpha^2 R + \alpha c_\beta)(\beta^2 R + \beta c_\alpha)$. Thus, a $(\beta^2 R + \beta c_\alpha) \times (\alpha^2 R + \alpha c_\beta)$ rectangle satisfies the size requirements for the $n_1 \times n_2$ rectangle of the Theorem.

Let $a = \beta^2$, $b = \alpha^2$, $n_1 = \beta^2 R + \beta c_\alpha$, $n_2 = \alpha^2 R + \alpha c_\beta$, and let $\mathcal{S}$ be an $n_1 \times n_2$ rectangle. Let Λ be the a lattice tiling for $\mathcal{S}$ with the generator matrix

$$G = \begin{bmatrix} n_2 & \frac{n_1}{2} + \theta \\ 0 & n_1 \end{bmatrix}$$

where $\theta = 1$ if $n_1 \equiv 0 (\mathrm{mod}\ 4)$ and $\theta = 2$ if $n_1 \equiv 2 (\mathrm{mod}\ 4)$. By Corollary 2, $(\Lambda, \mathcal{S}, \delta), \delta = (+1, 0)$, defines a folding.

The existence of a multiperiodic $\mathcal{S}$-DDC with $\sqrt{a \cdot b} R + o(R)$ dots follows now from Theorems 5 and 6. ■

The next key structure in our constructions is a certain family of hexagons defined next. A *centroid hexagon* is an hexagon with three disjoint pairs of parallel sides. If the four angles of two parallel sides (called the *bases* of the hexagon) are equal and the four other sides are equal, the hexagon will be called a *quasi-regular hexagon* and will be denoted by $\mathrm{QRH}(w, b, h)$, where b is the length of a base, h is the distance between the two bases, and $b + 2w$ is the length between the two vertices not on the bases. We will call the line which connects these two vertices, the *diameter* of the hexagon (even if it might not be the longest line between two points of the hexagon). Quasi-regular hexagon will usually be the shape $\mathcal{S}$ that will have the role of $\mathcal{S}$ when we will apply Theorem 4 to obtain a lower bound on the number of dots in a shape $\mathcal{Q}$ which usually will be a regular polygon. In the sequel we will say that $\frac{\beta}{\alpha} \approx \gamma$, when we means that $\gamma \le \frac{\beta}{\alpha} < \gamma + \epsilon$.

We want to show that there exists a quasi-regular hexagon $\mathrm{QRH}(w, b, h)$ with approximately $\sqrt{(b+w)h} + o(\sqrt{(b+w)h})$ dots. By Theorem 9, there exists a doubly periodic $\mathcal{S}$-DCC, where $\mathcal{S}$ is an $n_1 \times n_2 = (\alpha R + o(R)) \times (\beta R + o(R))$ rectangle, such that $\frac{n_2}{n_1} \approx \frac{b+w}{h}, n_1 n_2 = p^2 - 1$ for some prime p, where n_1 is an even integer. The lattice Λ of Theorem 9 is also a lattice tiling for a a shape $\mathcal{S}'$, where $\mathcal{S}'$ is "almost" a quasi-regular hexagon $\mathrm{QRH}(w, b, h)$ (part of this lattice tiling is depicted in Fig. 2). By Corollary 2, $(\Lambda, \mathcal{S}, \delta), \delta = (+1, 0)$, defines a folding for this shape too. Hence, we obtain a doubly periodic $\mathcal{S}'$-DCC, where $\mathcal{S}'$ is "almost" a a quasi-regular hexagon $\mathrm{QRH}(w, b, h)$ with approximately $\sqrt{(b+w)h} + o(\sqrt{(b+w)h})$ dots. This construction implies the following theorem.

Theorem 10: If $R \to \infty$ then there exists a regular hexagon with sides of length R and approximately $\frac{\sqrt{3\sqrt{3}}}{\sqrt{2}}R + o(R)$ dots.

Now, we can give a few examples for other specific shapes, mostly, regular polygons. To have some comparison between the bounds for various shapes we will assume that the radius of the circle or the regular polygons is R (the *radius* is the distance from the center of the regular polygon to any one its vertices). We also define the *packing ratio* as the ratio between the lower and the upper bounds on the number of dots. The shape $\mathcal{S}$ that we use will always be a multiperiodic $\mathcal{S}$-DDC on a multiperiodic array $\mathcal{A}$.

A. Circle

We apply Theorem 4 with a multiperiodic $\mathcal{S}$-DDC $\mathcal{A}$, where $\mathcal{S}$ is a regular hexagon with radius ρ and $\mathcal{Q}$ is a circle with radius R, sharing the same center. The upper bound on the number of dots in $\mathcal{Q}$ is $\sqrt{\pi}R + o(R)$. A lower bound on the number of dots in $\mathcal{S}$ is approximately $\frac{\sqrt{3\sqrt{3}}}{\sqrt{2}}\rho + o(\rho)$ and hence the density of $\mathcal{A}$ is approximately $\frac{\sqrt{2}}{\sqrt{3\sqrt{3}}\rho}$. Let θ be the angle between two radius lines to the two intersection points of the hexagon and the circle on one edge of the hexagon. We have that $\Delta(\mathcal{S}, \mathcal{Q}) = (\pi - 3\theta + 3\sin\theta)R^2$ and $\rho = \frac{\cos\frac{\theta}{2}}{\cos\frac{\pi}{6}}R$. Thus, a lower bound on the number of dots in $\mathcal{Q}$ is $\frac{\sqrt{3\sqrt{3}}\rho + o(\rho)}{\sqrt{2}|\mathcal{S}|}\Delta(\mathcal{S}, \mathcal{Q})$. The maximum is obtained when $\theta = 0.536267$ yielding a lower bound of $1.70813R + o(R)$ on the number of dots in $\mathcal{Q}$ and a packing ratio of 0.9637. The previous best packing ratio was 0.91167 and it was given in [14].

We must note again, that even so this construction works for infinitely many values of R, the density of these values is quite low. This is a consequence of Theorem 9 which can be applied for an arbitrary ratio γ only when the corresponding integers obtained by Dirichlet's Theorem are primes. Of course, there are many possible ratios between the sides of the rectangle that can be obtained for infinitely many values. A simple example is for any factorization of $p^2 - 1 = n_1 n_2$ we can form an $n_1 \times n_2$ DDC and from its related quasi-regular hexagons. We won't go into details to obtain bounds which hold asymptotically for any given R as we conjecture that the construction for quasi-regular hexagon can be strengthen asymptotically for almost all parameters.

B. Regular Polygon

For regular polygons with small number of sides we will use specific constructions some of which are given in Appendix C. For some constructions we need DDCs with other shapes like a Corner and a Flipped T which are defined in Appendix B, where also constructions of multiperiodic $\mathcal{S}$-DDCs for these shapes are given. If the number of sides is large we will use Theorem 4, where $\mathcal{Q}$ will be the regular polygon and $\mathcal{S}$ is a regular hexagon (for small number of sizes quasi-regular hexagons will be used). A computer program was developed to compute the packing ratios, some of which can be obtained by mathematical methods. Table I presents the results. Finally, we note that the problem is of interest also from discrete geometry point of view. Some similar questions can be found in [12].

TABLE I
BOUNDS ON THE NUMBER OF DOTS IN AN n-GON DDC

n	upper bound	lower bound	packing ratio
3	$1.13975R$	$1.02462R$	0.899
4	$1.41421R$	$1.41421R$	1
5	$1.54196R$	$1.45992R$	0.946795
6	$1.61185R$	$\approx 1.61185R$	≈ 1
7	$1.65421R$	$1.58844R$	0.960241
8	$1.68179R$	$1.62625R$	0.966977
9	$1.70075R$	$1.63672R$	0.96235
10	$1.71433R$	$1.65141R$	0.963297
60	$1.77083R$	$1.70658R$	0.963718
96	$1.77182R$	$1.70752R$	0.96371
circle	$1.77245R$	$1.70813R$	0.963708

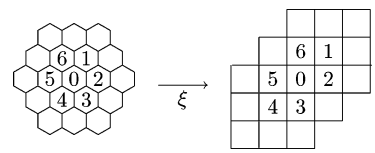


Fig. 3. The hexagonal model translation.

VI. FOLDING IN THE HEXAGONAL GRID

The questions concerning DDCs can be asked in the hexagonal grid in the same way that they are asked in the square grid. Similarly, they can be asked in dense D-dimensional lattices. In this section we will consider some part of our discussion related to the hexagonal grid. The hexagonal grid is a two-dimensional grid and hence we will compare it to $\mathbb{Z}^2$. We can define a folded-row and folding in the hexagonal grid in the same way as they are defined in $\mathbb{Z}^2$. To prove that the results remain unchanged we will describe the well known transformation between the hexagonal grid and $\mathbb{Z}^2$.

The *hexagonal grid* is defined as follows. We start by tiling the plane $\mathbb{R}^2$ with regular hexagons whose sides have length $1/\sqrt{3}$ (so that the centers of hexagons that share an edge are at distance 1). The center points of the hexagons are the points of the grid. The hexagons tile $\mathbb{R}^2$ in a way that each point $(i, 0), i \in \mathbb{Z}$, is a center of some hexagon.

The transformation uses an isomorphic representation of the hexagonal grid. Each point $(x, y) \in \mathbb{Z}^2$ has the following neighboring vertices,

$$\{(x + a, y + b) | a, b \in \{-1, 0, 1\}, a + b \neq 0\}.$$

It may be shown that the two representations are isomorphic by using the mapping $\xi : \mathbb{R}^2 \to \mathbb{R}^2$, which is defined by $\xi(x, y) = (x + \frac{y}{\sqrt{3}}, \frac{2y}{\sqrt{3}})$. The effect of the mapping on the neighbor set is shown in Fig. 3. From now on, slightly changing notation, we will also refer to this representation as the hexagonal grid. Using this new representation the neighbors of point (i, j) are

$$\{(i-1, j-1), (i-1, j), (i, j-1), (i, j+1) \\ (i+1, j), (i+1, j+1)\}.$$

Lemma 16: Two lines differ in length or slope in one representation if and only if they differ in length or slope in the other representation.

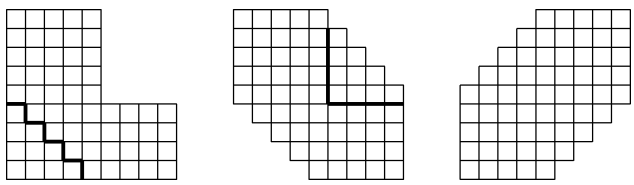


Fig. 4. From a corner CR$(9, 9; 5, 4)$ to hexagonal sphere with radius 4

Proof: This claim can be verified easily by observing that two lines are equal in length and slope in one representation if and only if they are equal in length and slope in the other representation. ■

Corollary 10: A shape $\mathcal{S}$ is a DDC in the hexagonal grid if and only if $\xi(\mathcal{S}) = \{\xi(p) : p \in \mathcal{S}\}$ is a DDC in $\mathbb{Z}^2$.

Clearly, the representation of the hexagonal grid in terms of $\mathbb{Z}^2$ implies that all the results on folding in the square grid hold also in the hexagonal grid. We will consider now the most important families of DDCs in the hexagonal grid, regular hexagons and circles. A regular hexagon in the hexagonal grid is also called an *hexagonal sphere* with radius R. It is a shape with a center hexagon which includes all the points in the hexagonal grid which are within Manhattan distance R from the center point. Applying the transformation ξ on this sphere we obtain a new shape in the square grid. This shape is a $(2R+1) \times (2R+1)$ square from which isosceles right triangle with sides of length R are removed from the left upper corner and the right lower corner. For the construction we use as our shape $\mathcal{S}$, in Theorem 4, a corner CR$(2R, w_1 + w_2; R, w_2)$, where $\frac{R}{w_2} \approx 1, |w_1 - w_2| \leq 3$ and g.c.d.$(w_1, w_2) = 1$. In Appendix B, a construction for doubly periodic $\mathcal{S}$-DDC, where $\mathcal{S}$ is such corner, is given where the number of dots in $\mathcal{S}$ is approximately $\sqrt{|\mathcal{S}|} + o(\sqrt{|\mathcal{S}|})$. The lattice tiling for $\mathcal{S}$ is also a lattice tiling for the shape $\mathcal{S}'$ obtained from $\mathcal{S}$ by removing an isosceles right triangle with sides of length R from the lower left corner and adding it to the upper right corner of the $\mathcal{S}$ (see Fig. 4). The constructed doubly periodic $\mathcal{S}'$-DDC can be rotated by 90 degrees or flipped either horizontally or vertically to obtain a doubly periodic $\mathcal{Q}$-DDC, where $\mathcal{Q}$ is approximately an hexagonal sphere with radius R. This yields a packing ratio approximately 1 between the lower bound and the upper bound on the number of dots. Now, it is easy to verify that the same construction, for a DDC with a circle shape, given in Subsection V-A for the square grid will work in the hexagonal grid. For this construction we will use regular hexagon and a circle in the hexagonal grid to obtain a packing ratio between the lower bound and the upper bound on the number of dots in the circle which is the same as in the square grid.

VII. Application for Error-Correction

In this section, we will discuss the usage of folding to design optimal (or "almost" optimal) codes which can correct adjacent errors in a multidimensional array, i.e., a multidimensional 2-burst-correcting code. The construction is a generalization of the construction of optimal one-dimensional 2-burst-correcting codes given by Abramson [33]. His construction was generalized for larger bursts by [34] and [35] who gave a comprehensive treatment for this topic. Multidimensional generalization for the 2-burst-correcting codes were given in [25], [62]. We will give a multidimensional generalization only for the 2-burst-correcting codes. The parity-check matrix of a code of length $2^m - 1$ and redundancy $m+1$, consists of the $2^m - 1$ consecutive nonzero elements (powers of a primitive element α) of GF(2^m) followed by a row of *ones*. The received word has one or two errors depending if the last entry of its syndrome is *one* or *zero*, respectively. The position of the error is determined by the first m entries of the syndrome.

The generalization of this idea is done by folding the nonzero elements of GF(2^m) into the parity-check matrix of a multidimensional code row by row, dimension by dimension. Assume that we have a D-dimensional array of size $n_1 \times n_2 \times \cdots \times n_D$ and we wish to correct any D-dimensional burst of length 2 (at most two adjacent positions are in error). The following construction given in [62] is based on folding the nonzero elements of a Galois field with characteristic 2 into a parity check matrix, where the order of the elements of the field is determined by a primitive element of the field.

Construction A: Let α be a primitive element in GF(2^m) for the smallest integer m such that $2^m - 1 \geq \prod_{\ell=1}^{D} n_\ell$. Let $d = \lceil \log_2 D \rceil$ and $\mathbf{i} = (i_1, i_2, \ldots, i_D)$, where $0 \leq i_\ell \leq n_\ell - 1$. Let A be a $d \times D$ matrix containing distinct binary d-tuples as columns. We construct the following $n_1 \times n_2 \times \cdots \times n_D \times (m+d+1)$ parity check matrix H.

$$h_{\mathbf{i}} = \begin{bmatrix} 1 \\ A\mathbf{i}^T \bmod 2 \\ \alpha^{\sum_{j=1}^{D} i_j (\prod_{\ell=j+1}^{D} n_\ell)} \end{bmatrix}.$$

for all $\mathbf{i} = (i_1, i_2, \ldots, i_D)$, where $0 \leq i_\ell \leq n_\ell - 1$.

For completeness we present the decoding algorithm given in [62]. We assume that the error occurred is a 2-burst. The syndrome received v in the decoding algorithm consists of three parts.

- The first bit determines the number of errors occurred. Obviously if the syndrome is the all-zeros vector than no errors occurred. If the first bit of the syndrome is an *one* then exactly one error occurred and its position is the position of v in H. If the first bit of a non-zero vector v is a *zero* then two errors occurred. Their position is determined by the other $m+d$ entries of v.
- The next d bits determine the dimension in which the burst occurred. There are D dimensions and each column of the matrix A corresponds to a different dimension for two consecutive errors. If the errors occurred in positions $\mathbf{i}_1 = (i_1, \ldots, i_D)$ and $\mathbf{i}_2 = (i_1, \ldots, i_{j-1}, i_j + 1, i_{j+1}, \ldots, i_D)$ then the value of the d bits, $(A\mathbf{i}_1^T + A\mathbf{i}_2^T) \bmod 2$, is the j-th column of the matrix A.
- The entries of the last m rows of the matrix H form the folding of the first $\Pi_{i=1}^{D} n_i$ consecutive elements of GF(2^m). Given a dimension ℓ there exists an integer $i(\ell)$ such that each two consecutive elements in dimension ℓ have the form $\alpha^j, \alpha^{j+i(\ell)}$. It is easy to verify that for $j_1 \neq j_2$ we have $\alpha^{j_1} + \alpha^{j_1+i(\ell)} \neq \alpha^{j_2} + \alpha^{j_2+i(\ell)}$. Thus, given the dimension of the burst of size two the last m bits of v can determine the two consecutive positions of the burst.

It leads to the following theorems [62].

Theorem 11: The code constructed in Construction A can correct any 2-burst in an $n_1 \times n_2 \times \cdots \times n_D$ array codeword.

Theorem 12: The code constructed by Construction A has redundancy which is greater by at most one from the trivial lower bound on the redundancy.

The same construction will work if instead of a D-dimensional array our codewords will have have a shape $\mathcal{S}$ of size $2^m - 1$, there is a lattice tiling Λ for $\mathcal{S}$, and there is a direction vector δ such that $(\Lambda, \mathcal{S}, \delta)$ defines a folding. The nonzero elements of GF(2^m) will be ordered along the folded-row of $\mathcal{S}$. Since usually the number of elements in $\mathcal{S}$ is not $2^m - 1$ we should find a shape $\mathcal{S}'$ which contains $\mathcal{S}$ and $|\mathcal{S}'| = 2^m - 1$. We design a code with the shape of $\mathcal{S}'$ and since $\mathcal{S} \subset \mathcal{S}'$ the code will be able to correct the same type of errors in $\mathcal{S}$.

Finally, the construction can be generalized in a way that the multidimensional code will be able to correct other types of two errors in a multidimensional array [62].

VIII. Application for Pseudo-Random Arrays

MacWilliams and Sloane [42] gave the name *pseudo-random sequence* to a maximal length sequence obtained from a linear feedback shift register. These sequences called also PN (Pseudo Noise) sequences or M-sequences have many desired properties as described in [41], [42]. The term pseudo-random array was given by MacWilliams and Sloane [42] to a rectangular array obtained by folding a pseudo-random sequence $\mathcal{B}$ into its entries. The constructed arrays can be obtained also as what is called maximum-area matrices [43]. In [42] it was proved that if a pseudo-random sequence of length $n = 2^{k_1 k_2} - 1$ is folded into an $n_1 \times n_2$ array such that $n_1 = 2^{k_1} - 1 > 1, n_2 = \frac{n}{n_1} > 1$, and g.c.d$(n_1, n_2) > 1$ then the constructed array has many desired properties and hence they called this array $\mathcal{A}$ a *pseudo-random array*. Some of the properties they mentioned are as follows.

1) *Recurrences*—the entries satisfy a recurrence relation along the folding.
2) *Balanced*—$2^{k_1 k_2 - 1}$ entries in the array are *ones* and $2^{k_1 k_2 - 1} - 1$ entries in the array are *zeros*.
3) Shift-and-Add—the sum of $\mathcal{A}$ with any of its cyclic shifts is another cyclic shift of $\mathcal{A}$.
4) *Autocorrelation Function*—has two values: n in-phase and -1 out-of-phase.
5) *Window property*—each of the $2^{k_1 k_2} - 1$ nonzero matrices of size $k_1 \times k_2$ is seen exactly once as a window in the array.

All these properties except for the window property are a consequence of the fact that the elements in the folded-row are consecutive elements of an M-sequence $\mathcal{B}$. Before we examine whether an array of any shape, obtained by folding $\mathcal{B}$ into it, has these properties we have to define what is a cyclic shift of any given shape $\mathcal{S}$ (even so we used the term without definition before). Our definition will assume again that there exists a lattice tiling Λ for $\mathcal{S}$ and a direction δ such that $(\Lambda, \mathcal{S}, \delta)$ defines a folding. A *cyclic shift* of the shape $\mathcal{S}$ (placed on the grid) is obtained by taking the set of elements $\{x + \delta : x \in \mathcal{S}\}$. Clearly, we have the following lemma.

Lemma 17: The shape of a cyclic shift of $\mathcal{S}$ is $\mathcal{S}$.

Theorem 13: Let Λ be a lattice tiling for a shape $\mathcal{S}$ and let δ be a direction such that $(\Lambda, \mathcal{S}, \delta)$ defines a folding. If an M-sequence $\mathcal{B}$ is folded into $\mathcal{S}$ in the direction δ then the Recurrences, Balanced, Shift-and-Add, and the Autocorrelation Function properties hold for the constructed array.

Proof: These properties follows immediately from the fact that the entries of $\mathcal{S}$ by the order of the folded-row are consecutive elements of the M-sequence $\mathcal{B}$. The two cyclic shifts of $\mathcal{S}$ have the same folded-row up to a cyclic shift. Therefore, these four properties are a direct consequence from the related properties of the M-sequence $\mathcal{B}$. ■

Lemma 18: Let Λ be a lattice tiling for the shape $\mathcal{S}$ and δ be a direction for which the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding. Let $\mathcal{B}$ be a binary sequence of length $|\mathcal{S}|$. Let P_1 and P_2 be two points for which $P_1 - c(P_1) = P_2 - c(P_2)$. Then, for any two positive integers k_1 and k_2 the two $k_1 \times k_2$ windows of $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$ whose leftmost bottom points are P_1 and P_2 are equal.

Proof: The lemma is an immediate consequence from the definition of the lattice coloring induced by $(\Lambda, \mathcal{S}, \delta)$ and the definition of $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$. ■

Theorem 14: Assume Λ define a lattice tiling for an $n_1 \times n_2$ array $\mathcal{A}$, such that $n_1 n_2 = 2^{k_1 k_2} - 1$. Assume further that Λ defines a lattice tiling for the shape $\mathcal{S}$ and $(\Lambda, \mathcal{S}, \delta)$ defines a folding for the direction δ. Then, if we fold an M-sequence $\mathcal{B}$ into $\mathcal{S}$ in the direction δ, the resulting shape $\mathcal{S}$ has the $k_1 \times k_2$ window property if and only if the $n_1 \times n_2$ array $\mathcal{A}$ has the $k_1 \times k_2$ window property by folding $\mathcal{B}$ into $\mathcal{A}$ in the direction δ.

Proof: Since Λ is a lattice tiling for both $\mathcal{A}$ and $\mathcal{S}$ there is a sequence of arrays $\mathcal{A}_0 = \mathcal{A}, \mathcal{A}_1, \ldots, \mathcal{A}_r = \mathcal{S}$, such that $|\mathcal{A}_{i+1} \setminus \mathcal{A}_i| = |\mathcal{A}_i \setminus \mathcal{A}_{i+1}| = 1, 0 \le i \le r - 1, \Lambda$ is a lattice tiling for $\mathcal{A}_i, 0 \le i \le r$, and the origin is contained in $\mathcal{A}_i, 0 \le i \le r$. Moreover, it is easy to verify that given the shape $\mathcal{A}_i, P_1 = \mathcal{A}_{i+1} \setminus \mathcal{A}_i, P_2 = \mathcal{A}_i \setminus \mathcal{A}_{i+1}$, we have that $P_2 = P_1 - c(P_1)$ with respect to $\mathcal{A}_i$. The theorem follows now by induction and using Lemma 18. ■

Theorem 14 does not give any new information about window sizes which are not covered in [42], [43]. The following lemma provides such information. We say that a shape $\mathcal{S}$ of size $2^n - 1$ has the $\mathcal{Q}$ window property if $|\mathcal{Q}| = n$ and each nonzero value for $\mathcal{Q}$ appears exactly once in a copy of $\mathcal{S}$, where $\mathcal{S}$ is considered to be a cyclic shape.

Lemma 19: Let Λ be a lattice tiling for a shape $\mathcal{S}$, $|\mathcal{S}| = 2^n - 1$, and let δ be a direction, such that $(\Lambda, \mathcal{S}, \delta)$ defines a folding. Let $\mathcal{B}$ be an M-sequence of length $2^n - 1$ and let $\mathcal{Q}$ be a shape with volume n. If in the array $\mathcal{S}'$ defined by $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$ there is no copy of $\mathcal{Q}$ which contains only *zeros* then $\mathcal{S}$ has the $\mathcal{Q}$ window property.

Proof: By the Shift-and-Add property (Theorem 13), $\mathcal{S}'$ has two identical copies of $\mathcal{Q}$ if and only if $\mathcal{S}'$ has a copy of $\mathcal{Q}$ which contains only *zeros*. Thus, $\mathcal{S}'$ has the $\mathcal{Q}$ window property if and only if there is no copy of $\mathcal{Q}$ in $\mathcal{S}'$ which contains only *zeros*. ■

We can use now the properties we have found for folding to obtain various results. An example is given in the following corollary.

Corollary 11: Let Λ be a lattice tiling for a shape $\mathcal{S}$, $|\mathcal{S}| = 2^n - 1$, and let δ be a direction, such that $(\Lambda, \mathcal{S}, \delta)$ defines a folding. Let $\mathcal{B}$ be an M-sequence of length $2^n - 1$. If $2^n - 1$ is a Mersenne prime then $(\Lambda, \mathcal{S}, \delta, \mathcal{B})$ has the $1 \times n$ and the $n \times 1$ window property for any given direction vector δ.

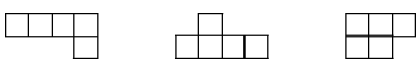
Example 2: Consider the following M-sequence $\mathcal{B} = 0000100101100111110001101110101$ of length 31. Let Λ be a lattice tiling for a corner CR(5,7;1,4) with the generator matrix

$$G_2 = \begin{bmatrix} 3 & 4 \\ 10 & 3 \end{bmatrix}.$$

By folding of $\mathbf{S}$ in the direction $(+1, 0)$ we obtain the following pseudo-random array:

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

This array has the 5×1 and 1×5 window properties. Out of the 19 shapes of size 5 with exactly two rows it does not have the window property only for the following three shapes:



The pseudo-random array obtained by folding $\mathcal{B}$ with the direction $(0, +1)$ is

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

It has the 5×1 and 1×5 window properties. But, out of the 19 shapes of size 5 with exactly two rows it does not have the window property for eight shapes.

Both pseudo-random arrays have a window property for the star shape given by

IX. Conclusion and Open Problems

The well-known definition of folding was generalized. The generalization and its applications led to several new results summarized as follows:

1) The generalization is based on a lattice tiling for a shape $\mathcal{S}$ and a direction δ. The number of possible nonequivalent directions is $\frac{\phi(|\mathcal{S}|)}{2}$. Necessary and sufficient conditions that a direction defines a folding are derived.
2) Folding a B_2-sequence into a shape $\mathcal{S}$ result in a distinct difference configuration with the shape $\mathcal{S}$.
3) Lower bounds on the number of dots in a distinct difference configuration with shape of regular polygon, circle, and other interesting geometrical shapes are derived. In particular asymptotically optimal such patterns were constructed for a large family of hexagonal shapes.
4) Low redundancy multidimensional codes for correcting a burst of length two are obtained.
5) New pseudo-random arrays with window and correlation properties are derived. These arrays differ from known arrays either in their shape or the shape of their window property.

The discussion on these results leads to many new interesting open problems. We conclude with a list of six open problems related to our discussion.

1) We have discussed several applications for the folding operation in general and for the new generalization of folding in particular. We believe that there are more interesting applications for this operation and we would like to see them explored.
2) The construction for DDCs whose shape is a quasi-regular hexagon works for infinite number of parameters. But, the set of parameters is very sparse. Its density depends on the number of primes obtained by Dirichlet's Theorem. This immediately implies the same for the parameters of DDCs whose shape is a regular polygon. We would like to see a construction of such DDCs with a dense set of parameters.
3) What is the lower bound on the number of dots in a DDC whose shape is a circle with radius R? We conjecture that the lower bound is $\sqrt{\pi}R + o(R)$.
4) We would like to see an asymptotic improvement on the lower bounds on the number of dots in a DDC whose shape is a regular n-gon with radius R.
5) Are there cases where we can improve the upper bound on the number of dots in these DDCs asymptotically?
6) We would like to see a more general theorem which connects folding of M-sequences and general window property.

Appendix A

In this Appendix A, we prove the necessary and sufficient condition for a triple $(\Lambda, \mathcal{S}, \delta)$ to define a folding. For the proof of the theorem we use the well-known Cramer's rule [63] which is given first.

Theorem 15: Given the following system with the n linear equations and the variables $x_1, x_2, \ldots, x_n$

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

If

$$A = \det \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix},$$

then $x_k = \frac{A_k}{A}$ for $1 \le k \le n$, where

$$A_k = \det \begin{vmatrix} a_{11} & \dots & a_{1(k-1)} & b_1 & a_{1(k+1)} & \dots & a_{1n} \\ a_{21} & \dots & a_{2(k-1)} & b_2 & a_{2(k+1)} & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{n(k-1)} & b_n & a_{n(k+1)} & \dots & a_{nn} \end{vmatrix}.$$

Let Λ be a D-dimensional lattice tiling for the shape $\mathcal{S}$. Let G be the following generator matrix of Λ:

$$G = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1D} \\ v_{21} & v_{22} & \dots & v_{2D} \\ \vdots & \vdots & \ddots & \vdots \\ v_{D1} & v_{D2} & \dots & v_{DD} \end{bmatrix}.$$

Given the direction $\delta = (d_1, d_2, \dots, d_D)$, w.l.o.g. we assume that the first ℓ values of δ are nonzeros and the last and the last $D - \ell$ values are zeros. By Lemma 5 and Corollary 1, if $(\Lambda, \mathcal{S}, \delta)$ defines a folding then there exist D integer coefficients $\alpha_1, \alpha_2, \dots, \alpha_D$ such that

$$\sum_{j=1}^{D} \alpha_j (v_{j1}, v_{j2}, \dots, v_{jD}) = (|\mathcal{S}| d_1, \dots, |\mathcal{S}| d_\ell, 0, \dots, 0)$$

and there is no integer $i, 0 < i < |\mathcal{S}|$, and D integer coefficients $\beta_1, \beta_2, \dots, \beta_D$ such that

$$\sum_{j=1}^{D} \beta_j (v_{j1}, v_{j2}, \dots, v_{jD}) = (i \cdot d_1, \dots, i \cdot d_\ell, 0, \dots, 0).$$

Hence we have the following D equations:

$$\sum_{j=1}^{D} \alpha_j v_{jr} = |\mathcal{S}| \cdot d_r, \quad 1 \le r \le \ell \tag{2}$$

$$\sum_{j=1}^{D} \alpha_j v_{jr} = 0, \quad \ell + 1 \le r \le D. \tag{3}$$

Let $\tau = d_1$ if $\ell = 1$ and $\tau = \text{g.c.d.}(d_1, d_2, \dots, d_\ell)$ if $\ell > 1$. The D equations in (2), (3) are equivalent to the following D equations:

$$\sum_{j=1}^{D} \alpha_j v_{j1} = |\mathcal{S}| \cdot d_1,$$
$$\sum_{j=1}^{D} \alpha_j \frac{d_1 v_{jr} - d_r v_{j1}}{\tau} = 0, \quad 2 \le r \le \ell$$
$$\sum_{j=1}^{D} \alpha_j v_{jr} = 0, \quad \ell + 1 \le r \le D.$$

We define now a set of $D(D-1)$ new coefficients $u_{rj}, 2 \le r \le D, 1 \le j \le D$, as follows:

$$u_{rj} = \frac{d_1 v_{jr} - d_r v_{j1}}{\tau} \quad \text{for } 2 \le r \le \ell,$$
$$u_{rj} = v_{jr} \quad \text{for } \ell + 1 \le r \le D.$$

Consider the $(D-1) \times D$ matrix

$$H = \begin{bmatrix} u_{21} & u_{22} & \dots & u_{2D} \\ u_{31} & u_{32} & \dots & u_{3D} \\ \vdots & \vdots & \ddots & \vdots \\ u_{D1} & u_{D2} & \dots & u_{DD} \end{bmatrix}.$$

Using Theorem 15 it is easy to verify that the unique solution for the α_k's is

$$\alpha_k = (-1)^{k-1} \frac{d_1 \tau^{\ell-1} \det H_k}{d_1^{\ell-1}} \tag{4}$$

where H_k is the $(D-1) \times (D-1)$ matrix obtained from H by deleting column k of H.

Lemma 20: For each $k, 1 \le k \le D, \tau$ divides α_k defined in (4).

Proof: Consider the following $D \times D$ matrix

$$\tilde{G} = \begin{bmatrix} v_{11} & v_{21} & \dots & v_{D1} \\ u_{21} & u_{22} & \dots & u_{2D} \\ u_{31} & u_{32} & \dots & u_{3D} \\ \vdots & \vdots & \ddots & \vdots \\ u_{D1} & u_{D2} & \dots & u_{DD} \end{bmatrix}.$$

By the definition of the entries in the matrix H and since $\det G = |\mathcal{S}|$ it follows that $\det \tilde{G} = |\mathcal{S}|(\frac{d_1}{\tau})^{\ell-1}$. $\det \tilde{G}$ in Theorem 15 is equal A, while A_k is equal $|\mathcal{S}| \cdot d_1 (\frac{d_1}{\tau})^{\ell-2} Y$, for some integer Y. Therefore, $\alpha_k = \tau Y$ and the lemma follows. ■

This analysis leads to the following theorem.

Theorem 16: If Λ is a lattice tiling for the shape $\mathcal{S}$ then the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding if and only if $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \dots, \frac{\alpha_D}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$.

Proof: Assume first that $(\Lambda, \mathcal{S}, \delta)$ defines a folding.

Now, assume for the contrary that $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \dots, \frac{\alpha_D}{\tau}) = \nu_1 > 1$ or $\text{g.c.d.}(\tau, |\mathcal{S}|) = \nu_2 > 1$. We distinguish between two cases.

Case 1:

Assume that $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \dots, \frac{\alpha_D}{\tau}) = \nu_1 > 1$.

Equations (2), and (3) have exactly one solution for the α_i's given in (4). Since $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \dots, \frac{\alpha_D}{\tau}) = \nu_1$, it follows that $\beta_i = \frac{\alpha_i}{\tau \nu_1}, 1 \le i \le D$, are integers. Therefore, we have

$$\sum_{j=1}^{D} \beta_j v_{jr} = \frac{|\mathcal{S}|}{\tau \nu_1} d_r, \quad 1 \le r \le \ell, \quad \sum_{j=1}^{D} \beta_j v_{jr} = 0, \quad \ell + 1 \le r \le D,$$

i.e.,

$$\sum_{j=1}^{D} \beta_j (v_{j1}, v_{j2}, \dots, v_{jD}) = \left(\frac{|\mathcal{S}|}{\tau \nu_1} d_1, \dots, \frac{|\mathcal{S}|}{\tau \nu_1} d_\ell, 0, \dots, 0 \right),$$

and as a consequence by Lemma 5 we have that $(\Lambda, \mathcal{S}, \delta)$ does not define a folding, a contradiction.

Case 2:

Assume that $\text{g.c.d.}(\tau, |\mathcal{S}|) = \nu_2 > 1$.

Let $\beta_i = \frac{\alpha_i}{\nu_2}, 1 \le i \le \ell$. Therefore

$$\sum_{j=1}^{D} \beta_j(v_{j1}, v_{j2}, \ldots, v_{jD}) = \left(\frac{|\mathcal{S}|}{\nu_2} d_1, \ldots, \frac{|\mathcal{S}|}{\nu_2} d_\ell, 0, \ldots, 0\right),$$

and as a consequence by Lemma 5 we have that $(\Lambda, \mathcal{S}, \delta)$ does not define a folding, a contradiction.

As a consequence of Case 1 and Case 2 we have that if $(\Lambda, \mathcal{S}, \delta)$ defines a folding with the vector δ then $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \ldots, \frac{\alpha_D}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$.

Now assume that $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \ldots, \frac{\alpha_D}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$. Consider the set of D equations defined by

$$\sum_{j=1}^{D} \alpha_j(v_{j1}, \ldots, v_{jD}) = (|\mathcal{S}|d_1, \ldots, |\mathcal{S}|d_\ell, 0, \ldots, 0). \quad (5)$$

Since the rows of G are linearly independent, it follows that this set of equations has a unique solution for the α_i's (but, these coefficients are not necessary integers). Using the same analysis proceeding the theorem, we have by the Cramer's rule that this solution is given by (4) and hence the α_i's are integers. Assume for the contrary that $(\Lambda, \mathcal{S}, \delta)$ does not define a folding. Then, by Lemma 5 we have that there exist D integers $\beta_i, 1 \le i \le D$, such that

$$\sum_{j=1}^{D} \beta_j(v_{j1}, v_{j2}, \ldots, v_{jD}) = (\mu \cdot d_1, \ldots, \mu \cdot d_\ell, 0, \ldots, 0), \quad (6)$$

for some integer $0 < \mu < |\mathcal{S}|$.

Since the rows of G are linearly independent then there exists exactly one set of β_i's (integers or non-integers) which satisfies (6). Let $\nu = \text{g.c.d.}(\mu, |\mathcal{S}|)$, where clearly $1 \le \nu \le \mu < |\mathcal{S}|$. From (5) and (6) we obtain

$$\begin{aligned}\sum_{j=1}^{D} (\mu\alpha_j)(v_{j1}, v_{j2}, \ldots, v_{jD}) &= (\mu|\mathcal{S}|d_1, \ldots, \mu|\mathcal{S}|d_\ell, 0, \ldots, 0) \\ &= \sum_{j=1}^{D} (|\mathcal{S}|\beta_j)(v_{j1}, v_{j2}, \ldots, v_{jD}),\end{aligned}$$

Since the rows of G are linearly independent it implies that $\mu\alpha_i = |\mathcal{S}|\beta_i$ for each $1 \le i \le D$, i.e., $\beta_i = \frac{\mu\alpha_i}{|\mathcal{S}|}$. $\beta_i = \frac{\mu\alpha_i}{|\mathcal{S}|}$ is an integer and $\nu = \text{g.c.d.}(\mu, |\mathcal{S}|)$ implies that $\beta_i = \frac{\mu/\nu}{|\mathcal{S}|/\nu}\alpha_i, 1 \le i \le D$. $\text{g.c.d.}(\mu/\nu, |\mathcal{S}|/\nu) = 1$ and hence $\frac{|\mathcal{S}|}{\nu}$ divides α_i for each $i, 1 \le i \le D$. $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1, \tau$ divides α_i, and hence $\frac{|\mathcal{S}|}{\nu}$ divides $\frac{\alpha_i}{\tau}$ for each i, $1 \le i \le D$. Hence, $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \ldots, \frac{\alpha_D}{\tau}) \ge \frac{|\mathcal{S}|}{\nu}$. But, $\text{g.c.d.}(\frac{\alpha_1}{\tau}, \frac{\alpha_2}{\tau}, \ldots, \frac{\alpha_D}{\tau}) = 1$ and hence $\nu = |\mathcal{S}|$, i.e., $\mu \ge |\mathcal{S}|$, a contradiction. Thus, $(\Lambda, \mathcal{S}, \delta)$ defines a folding. ■

APPENDIX B

In this Appendix B, we consider DDCs with two special shapes, called corner and flipped T. The DDCs with these shapes and special parameters are important in applying Theorem 4 to obtain other DDCs such as triangles in the square grid and hexagonal spheres in the hexagonal grid.

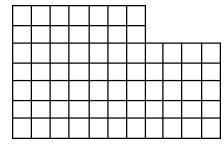


Fig. 5. A corner CR (7,11;2,4).

A. Corner

A *corner*, $\text{CR}(h_1 + h_2, w_1 + w_2; h_2, w_2)$, is an $(h_1 + h_2) \times (w_1 + w_2)$ rectangle from which an $h_2 \times w_2$ rectangle was removed from its right upper corner. An example is given in Fig. 5. Let $\mathcal{S}$ be a $\text{CR}(h_1 + h_2, w_1 + w_2; h_2, w_2)$ and let Λ the lattice with the following generator matrix:

$$G = \begin{bmatrix} w_1 & h_1 \\ -w_2 & h_1 + h_2 \end{bmatrix}.$$

Clearly, Λ is a lattice tiling for $\mathcal{S}$. A general result concerning DDCs whose shape is a corner seems to be quite difficult. We will consider the case which seems to be the most useful for our purpose. First note, that by Corollary 2, $\delta = (0, +1)$ defines a folding for Λ if and only if $\text{g.c.d.}(w_1, w_2) = 1$. Assume first that $h_1 = h_2$ and $|w_1 - w_2| \le 3$. By Theorem 9, we have an $n_1 \times n_2$ rectangle $\mathcal{Q}$ such that $n_1 n_2 = p^2 - 1$ for some prime p, $\frac{2n_1}{n_2} \approx \frac{h_1 + h_2}{2w_1 + w_2}$, and n_1 is even. Now, we will make new choices for h_1, h_2, w_1, and w_2, which are close to the old ones. Let $h_1 = h_2 = n_1$; we distinguish between three cases of n_2:

(W.1) If $n_2 = 3\omega + 1$ then $w_1 = \omega$ and $w_2 = \omega + 1$.

(W.2) If $n_2 = 3\omega + 2$ then $w_1 = \omega + 1$ and $w_2 = \omega$.

(W.3) If $n_2 = 3\omega$ then we distinguish between two cases:

- if $\omega - 1 \equiv 0 (\text{mod} 3)$ then $w_1 = \omega + 1$ and $w_2 = \omega - 2$.
- if $\omega - 1 \not\equiv 0 (\text{mod} 3)$ then $w_1 = \omega - 1$ and $w_2 = \omega + 2$.

It is easy to verify that the size of the new corner $\text{CR}(h_1 + h_2, w_1 + w_2; h_2, w_2), \mathcal{S}'$, is $n_1 n_2 = p^2 - 1$, Λ is a lattice tiling for $\mathcal{S}', (\Lambda, \mathcal{S}', \delta)$, $\delta = (0, +1)$, defines a folding, and we can form a doubly periodic $\mathcal{S}'$-DDC with it. Hence, we have the following theorem.

Theorem 17: Let n_1 and n_2 be two integers such that $n_1 n_2 = p^2 - 1$ for some prime number $p, n_2 = 2w_1 + w_2$, where n_1 is an even integer, w_1, w_2, are defined by (W.1), (W.2), (W.3). Then there exists a doubly periodic $\mathcal{S}$-DDC, whose shape is a corner, $\text{CR}(2n_1, w_1 + w_2; n_1, w_2)$, with p dots.

B. Flipped T

A *flipped T*, $\text{FT}(h, w_1 + w_2 + w_3; w_1, w_3)$, is an $(2h) \times (w_1 + w_2 + w_3)$ rectangle from which an $h \times w_1$ rectangle was removed from its left upper corner and an $h \times w_3$ rectangle was removed from its right upper corner. An example is given in Fig. 6. Let $\mathcal{S}$ be a $\text{FT}(h, w_1 + w_2 + w_3; w_1, w_3)$ and let Λ the lattice with the following generator matrix

$$G = \begin{bmatrix} w_1 + w_2 & h \\ w_1 + 2w_2 + w_3 & 0 \end{bmatrix}.$$

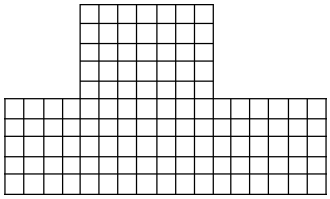


Fig. 6. A flipped T FT(5,17;4,6).

Clearly, Λ is a lattice tiling for $\mathcal{S}$. A general result concerning DDCs whose shape is a flipped T seems to be quite difficult. We will consider the case which seems to be the most useful for our purpose. First note, that by Corollary 2, $\delta = (0, +1)$ defines a folding for Λ if and only if $\mathrm{g.c.d.}(w_1+w_2, w_1+2w_2+w_3) = 1$ which is equivalent to $\mathrm{g.c.d.}(w_1 + w_2, w_2 + w_3) = 1$. Assume that $|w_1-w_3| \leq 4$. By Theorem 9, we have an $n_1 \times n_2$ rectangle $\mathcal{Q}$ such that $n_1 n_2 = p^2-1$ for some prime p, $\frac{n_1}{n_2} \approx \frac{h}{w_1+2w_2+w_3}$, and n_2 is even. Now, we will make new choices for h, w_1, and w_3, which are close to the old ones. Let $h = n_1$; we distinguish between two cases of n_2:

(Y.1) If $n_2 = 4\omega$ then $w_1 = 2\omega+1-w_2$ and $w_3 = 2\omega-1-w_2$.

(Y.2) If $n_2 = 4\omega + 2$ then $w_1 = 2\omega + 3 - w_2$ and $w_3 = 2\omega - 1 - w_2$.

It is easy to verify that the size of the new flipped T, $\mathrm{FT}(h, w_1 + w_2 + w_3; w_1, w_3), \mathcal{S}'$, is $n_1 n_2 = p^2 - 1$, Λ is a lattice tiling for $\mathcal{S}', (\Lambda, \mathcal{S}', \delta)$, $\delta = (0, +1)$, defines a folding, and we can form a doubly periodic $\mathcal{S}'$-DDC with it. Hence, we have the following theorem.

Theorem 18: Let n_1 and w_2 be two integers such that $n_2 = w_1+2w_2+w_3, w_1, w_3$, are defined by (Y.1), (Y.2), and $n_1 n_2 = p^2 - 1$ for some prime number p. Then there exists a doubly periodic $\mathcal{S}$-DDC, whose shape is a flipped T, $\mathrm{FT}(n_1, w_1+w_2+w_3; w_1, w_3)$, with p dots.

Appendix C

In this Appendix C, we demonstrate how Theorem 4 is applied for several geometric shapes (having the role of $\mathcal{Q}$ in the theorem), where our shape $\mathcal{S}$ in the doubly periodic $\mathcal{S}$-DDC is an appropriate corner, a flipped T, or a quasi-regular hexagon.

A. Equilateral Triangle

Let $\mathcal{Q}$ be an equilateral triangle with sides of length B. The area of $\mathcal{Q}$ is $\frac{\sqrt{3}}{4}B^2$ and hence an upper bound on the number of dots in $\mathcal{Q}$ is $\frac{3^{\frac{1}{4}}}{2}B+o(B) = 0.658B+o(B)$. For our shape $\mathcal{S}$ we take a flipped T, $\mathrm{FT}(\frac{B}{2\sqrt{2}}, \sqrt{\frac{2}{3}}B; \frac{B}{2\sqrt{6}}, \frac{B}{2\sqrt{6}})$ which overlaps in its shorter base with the base of $\mathcal{Q}$. These bases of $\mathcal{S}$ and $\mathcal{Q}$ share the same center. The area of $\mathcal{S}$ is $\frac{\sqrt{3}}{4}B^2$ and hence the density of the array is $\frac{2}{3^{\frac{1}{4}}B}$. The intersection of $\mathcal{S}$ and $\mathcal{Q}, \Delta(\mathcal{Q}, \mathcal{S})$, equal to $\frac{3\sqrt{2}-2\sqrt{3}}{2}B^2$. Therefore, a lower bound on the number of dots in $\mathcal{Q}$ is $\frac{3\sqrt{2}-2\sqrt{3}}{3^{\frac{1}{4}}}B+o(B) = 0.5916B+o(B)$ and the resulting packing ratio is 0.899. The same result can be obtained by using other structures instead of a flipped T.

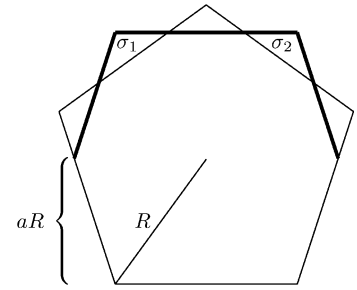


Fig. 7. Quasi-regular hexagon intersecting a regular pentagon.

B. Isosceles Right Triangle

Let $\mathcal{Q}$ be an equilateral triangle with base and height of length B. The area of $\mathcal{Q}$ is $\frac{1}{2}B^2$ and hence an upper bound on the number of dots in $\mathcal{Q}$ is $\frac{1}{\sqrt{2}}B + o(B) = 0.707B + o(B)$. For our shape $\mathcal{S}$ we take a corner $CR(\sqrt{\frac{2}{3}}B, \sqrt{\frac{2}{3}}B; \frac{B}{\sqrt{6}}, \frac{B}{\sqrt{6}})$ which overlaps in its two longer sides with the base and height of $\mathcal{Q}$. $\mathcal{S}$ and $\mathcal{Q}$ shares the intersection vertex of these sides. The area of $\mathcal{S}$ is $\frac{1}{2}B^2$ and hence the density of the array is $\frac{\sqrt{2}}{B}$. The intersection of $\mathcal{S}$ and $\mathcal{Q}, \Delta(\mathcal{Q}, \mathcal{S})$, equal to $(\sqrt{6}-2)B^2$. Therefore, a lower bound on the number of dots in $\mathcal{Q}$ is $(\sqrt{12}-2\sqrt{2})B+o(B) = 0.63567B + o(B)$ and the resulting packing ratio is 0.899 (exactly as in the case of an equilateral triangle).

C. Regular Pentagon

Let $\mathcal{Q}$ be a pentagon with radius R. The area of $\mathcal{Q}$ is $\frac{5}{2}\sin\frac{2\pi}{5}$ and hence an upper bound on the number of dots in $\mathcal{Q}$ is $1.54196R + o(R)$. Let $\mathcal{S}$ be a quasi-regular hexagon having a joint base with $\mathcal{Q}$ and two short overlapping sides with $\mathcal{Q}$, where these sides are connected to this base (see Fig. 7). The distance between the base and the diameter of $\mathcal{S}$ is $aR, 2\sin\frac{\pi}{10}\cos\frac{3\pi}{10} < a \leq (1 + \sin\frac{3\pi}{10})/2$. The length of the base is $2R\sin\frac{\pi}{5}$ and the length of the diameter of $\mathcal{S}$ is $2R\sin\frac{\pi}{5} + 2aR\tan\frac{\pi}{10}$. Hence, the area of $\mathcal{S}$ is $(4\sin\frac{\pi}{5} + 2a\tan\frac{\pi}{10})aR^2$ and the density of the array is $\frac{1}{\sqrt{4a\sin\frac{\pi}{5}+2a^2\tan\frac{\pi}{10}}R}$. The area of the intersection between $\mathcal{Q}$ and $\mathcal{S}, \Delta(\mathcal{S}, \mathcal{Q})$, is computed by subtracting from the area of $\mathcal{S}$ the area of the two isosceles triangles σ_1 and σ_2. The lower bound on the number of dots is $\frac{1}{\sqrt{4a\sin\frac{\pi}{5}+2a^2\tan\frac{\pi}{10}}R}\Delta(\mathcal{S}, \mathcal{Q})$. The maximum on this lower bound is obtained for $a = 0.814853$, i.e., the lower bound on the number of dots in a pentagon with radius R is $1.45992R+o(R)$ yielding a packing ratio of 0.946795.

Acknowledgment

The author's new interest in DDCs is a consequence of discussions with Simon Blackburn, Keith Martin, and Maura Paterson during spring 2007 on key predistribution for wireless sensor networks. The author would like to thank them all and also for the continuous hospitality which he receives yearly from the Mathematics Department at the Royal Holloway College. Without these discussions, the current work would not have been born. Discussions on related problems with Eitan Yaakobi were also inspirational.

REFERENCES

[1] W. C. Babcock, "Intermodulation interference in radio systems," *Bull. Syst. Tech. J.*, pp. 63–73, Jun. 1953.

[2] G. S. Bloom and S. W. Golomb, "Applications of numbered undirected graphs," *Proc. IEEE*, vol. 65, pp. 562–570, Apr. 1977.

[3] M. D. Atkinson, N. Santoro, and J. Urrutia, "Integer sets with distinct sums and differences and carrier frequency assignments for nonlinear repeaters," *IEEE Trans. Commun.*, vol. COM-34, pp. 614–617, 1986.

[4] A. W. Lam and D. V. Sarwate, "On optimum time-hopping patterns," *IEEE Trans. Commun.*, vol. COM-36, pp. 380–382, 1988.

[5] S. W. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," *IEEE Trans. Inf. Theory*, vol. IT-28, pp. 600–604, 1982.

[6] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proc. IEEE*, vol. 72, pp. 1143–1163, 1984.

[7] J. P. Robinson, "Golomb rectangles," *IEEE Trans. Inf. Theory*, vol. IT-31, pp. 781–787, 1985.

[8] R. A. Games, "An algebraic construction of sonar sequences using M-sequences," *SIAM J. Algebr. Discr. Meth.*, vol. 8, pp. 753–761, Oct. 1987.

[9] A. Blokhuis and H. J. Tiersma, "Bounds for the size of radar arrays," *IEEE Trans. Inf. Theory*, vol. IT-34, pp. 164–167, Jan. 1988.

[10] J. P. Robinson, "Golomb rectangles as folded ruler," *IEEE Trans. Inf. Theory*, vol. IT-43, pp. 290–293, 1997.

[11] P. Erdos, R. Graham, I. Z. Ruzsa, and H. Taylor, "Bounds for arrays of dots with distinct slope or lengths," *Combinatorica*, vol. 12, pp. 39–44, 1992.

[12] H. Lefmann and T. Thiele, "Point sets with distinct distances," *Combinatorica*, vol. 15, pp. 379–408, 1995.

[13] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, "Efficient key predistribution for grid-based wireless sensor networks," *Lecture Notes in Computer Science*, vol. 5155, pp. 54–69, Aug. 2008.

[14] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, "Two-dimensional patterns with distinct differences—Constructions, bounds, and maximal anticodes," *IEEE Trans. Inf. Theory*, vol. IT-56, pp. 1216–1229, Mar. 2010.

[15] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, "Distinct difference configurations: Multihop paths and key predistribution in sensor networks," *IEEE Trans. Inf. Theory*, vol. IT-56, pp. 3961–3972, Aug. 2010.

[16] P. Erdös and P. Turán, "On a problem of Sidon in additive number theory and some related problems," *J. London Math. Soc.*, vol. 16, pp. 212–215, 1941.

[17] H. Imai, "Two-dimensional fire codes," *IEEE Trans. Inf. Theory*, vol. IT-19, pp. 796–806, 1973.

[18] K. A. S. Abdel-Ghaffar, "An Information- and Coding-Theoretic Study of Bursty Channels with Applications to Computer Memories," Ph.D. Dissertation, California Inst. Technol., Pasadena, CA, Jun. 1986.

[19] K. A. S. Abdel-Ghaffar, R. J. McEliece, and H. C. A. van Tilborg, "Two-dimensional burst identification codes and their use in burst correction," *IEEE Trans. Inf. Theory*, vol. IT-34, pp. 494–504, May 1988.

[20] E. M. Gabidulin and V. V. Zanin, "Codes correcting two-dimensional burst errors," in *Proc. 3rd Int. Symp. on Communication Theory and Applications*, Ambleside, U.K., 1995, pp. 66–78.

[21] M. Breitbach, M. Bossert, V. Zyablov, and V. Sidorenko, "Array codes correcting a two-dimensional cluster of errors," *IEEE Trans. Inf. Theory*, vol. IT-44, pp. 2025–2031, Sep. 1998.

[22] M. Blaum, J. Bruck, and A. Vardy, "Interleaving schemes for multidimensional cluster errors," *IEEE Trans. Inf. Theory*, vol. IT-44, pp. 730–743, Mar. 1998.

[23] T. Etzion and A. Vardy, "Two-dimensional interleaving schemes with repetitions: Constructions and bounds," *IEEE Trans. Inf. Theory*, vol. IT-48, pp. 428–457, Feb. 2002.

[24] I. M. Boyarinov, "Two-dimensional array codes correcting 2×2 clusters of errors," in *Proc. Int. Wokshop on Coding Cryptogr. (WCC2003)*, Versailles, France, 2003.

[25] M. Schwartz and T. Etzion, "Two-dimensional cluster-correcting codes," *IEEE Trans. Inf. Theory*, vol. IT-51, pp. 2121–2132, Jun. 2005.

[26] I. M. Boyarinov, "Two-dimensional array codes correcting rectangular burst errors," *Prob. Inf. Transm.*, vol. 42, pp. 26–43, June 2006.

[27] T. Etzion and E. Yaakobi, "Error-correction of multidimensional bursts," *IEEE Trans. Inf. Theory*, vol. IT-55, pp. 961–976, Mar. 2009.

[28] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, pp. 3–16, 1985.

[29] R. M. Roth, "Maximum-rank arrays codes and their application to crisscross error correction," *IEEE Trans. Inf. Theory*, vol. IT-37, pp. 328–336, Mar. 1991.

[30] R. M. Roth, "Probabilistic crisscross error correction," *IEEE Trans. Inf. Theory*, vol. IT-43, pp. 1425–1438, Sep. 1997.

[31] M. Blaum and J. Bruck, "MDS array codes for correcting criss-cross errors," *IEEE Trans. Inf. Theory*, vol. IT-46, pp. 1068–1077, May 2000.

[32] P. Fire, A Class of Multiple Error Correcting Binary Codes for Nonindependent Errors Sylvania Reconnaisance Lab., Mountain View, CA, Sylvania Rep. RSL-e-2, 1959.

[33] N. M. Abramson, "A class of systematic codes for non-independent errors," *IRE Trans. Inf. Theory*, vol. IT-5, pp. 150–157, 1959.

[34] B. Elspas and R. A. Short, "A note on optimum burst-error-correcting codes," *IRE Trans. Inf. Theory*, vol. IT-8, pp. 39–42, 1962.

[35] K. A. S. Abdel-Ghaffar, R. J. Mceliece, A. M. Odlyzko, and H. C. A. van Tilborg, "On the existence of optimum cyclic burst correcting codes," *IEEE Trans. Inf. Theory*, vol. IT-32, pp. 768–775, 1986.

[36] P. G. Farrell and S. J. Hopkins, "Burst-error-correcting array codes," *Radio Elec. Eng.*, vol. 52, pp. 188–192, Apr. 1982.

[37] M. Blaum, P. G. Farrell, and H. C. A. van Tilborg, "A class of error-correcting array codes," *IEEE Trans. Inf. Theory*, vol. IT-32, pp. 836–839, Nov. 1986.

[38] M. Blaum, "A family of efficient burst-correcting array codes," *IEEE Trans. Inf. Theory*, vol. IT-36, pp. 671–674, May 1990.

[39] W. Zhang and J. K. Wolf, "A class of binary burst error-correcting quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. IT-34, pp. 463–479, May 1988.

[40] Z. Zhang, "Limitimng efficiencies of burst-correcting array codes," *IEEE Trans. Inf. Theory*, vol. IT-37, pp. 976–982, July 1991.

[41] S. W. Golomb, *Shift Register Sequences*. Walnut Creek, CA: Aegean Park Press, 1982.

[42] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, vol. 64, pp. 1715–1729, Dec. 1976.

[43] T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "The theory of two-dimensional linear recurring arrays," *IEEE Trans. Inf. Theory*, vol. IT-18, pp. 773–785, Nov. 1972.

[44] I. S. Reed and R. M. Stewart, "Note on the existence of perfect maps," *IRE Trans. Inf. Theory*, vol. IT-8, pp. 10–12, Jan. 1962.

[45] C. T. Fan, S. M. Fan, S. L. Ma, and M. K. Siu, "On de Bruijn arrays," *Ars Combinatoria*, vol. 19A, pp. 205–213, May 1985.

[46] T. Etzion, "Construction for perfect maps and pseudo-random arrays," *IEEE Trans. Inf. Theory*, vol. IT-34, pp. 1308–1316, 1988.

[47] K. G. Paterson, "Perfect maps," *IEEE Trans. Inf. Theory*, vol. IT-40, pp. 743–753, 1994.

[48] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," *Image Processing Proc.*, vol. 2, pp. 86–90, 1994.

[49] A. Z. Tirkel, R. G. van Schyndel, and C. F. Osborne, "A two-dimensional digital watermark," in *Proc. DICTA95*, 1998, pp. 210–216.

[50] Y. C. Hsieh, "Decoding structured light patterns for three-dimensional imaging systems," *Pattern Recogn.*, vol. 34, pp. 343–349, 2001.

[51] R. A. Morano, C. Ozturk, R. Conn, S. Dubin, S. Zietz, and J. Nissanov, "Structured light using pseudorandom codes," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, pp. 322–327, 1988.

[52] J. Salvi, J. Pages, and J. Battle, "Pattern codification strategies in structured light systems," *Pattern Recogn.*, vol. 37, pp. 827–849, 2004.

[53] J. Pages, J. Salvi, C. Collewet, and J. Forest, "Optimised de Bruijn patterns for one-shot shape acquisition," *Image Vision Comput.*, vol. 23, pp. 707–720, 2005.

[54] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*. New York: Springer-Verlag, 1993.

[55] S. K. Stein and S. Szabó, *Algebra and Tiling*. Washington, DC: Mathematical Association of America, 1994.

[56] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on AWGN channel," *IEEE Trans. Inf. Theory*, vol. IT-44, pp. 273–278, Jan. 1998.

[57] E. Viterbo and J. Boutros, "A universal lattice decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. IT-45, pp. 1639–1642, Jul. 1999.

[58] T. Tarokh, A. Vardy, and K. Zeger, "Universal bounds on the performance of lattice codes," *IEEE Trans. Inf. Theory*, vol. IT-45, pp. 670–681, Mar. 1999.

[59] K. O'Bryant, "A complete annotated bibliography of work related to Sidon sequences," *The Elec. J. Combin.*, vol. DS11, pp. 1–39, July 2004.

[60] R. C. Bose, "An affine analogue of Singer's theorem," *J. Indian Math. Soc. (N.S.)*, vol. 6, pp. 1–15, 1942.

[61] I. Nivan and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, 4th ed. New York: Wiley, 1979.

[62] E. Yaakobi and T. Etzion, "High dimensional error-correcting codes," in *Proc. 2010 Int. Symp. Inf. Theory*, Austin, TX, June 2010, pp. 1178–1182.

[63] S. MacLane and G. Birkhoff, *Algebra*, 3rd ed. New York: Chelsea, 1988.

Tuvi Etzion (M'89–SM'94–F'04) was born in Tel Aviv, Israel, in 1956. He received the B.A., M.Sc., and D.Sc. degrees from the Technion—Israel Institute of Technology, Haifa, Israel, in 1980, 1982, and 1984, respectively.

In 1984, he held a position in the Department of Computer Science at the Technion, where he is currently a Professor. During 1986–1987, he was Visiting Research Professor with the Department of Electrical Engineering—Systems at the University of Southern California, Los Angeles. During summers 1990 and 1991, he was Visiting at Bellcore, Morristown, NJ. During 1994–1996, he was a Visiting Research Fellow in the Computer Science Department at Royal Holloway College, Egham, England. He also had several visits to the Coordinated Science Laboratory at the University of Illinois in Urbana-Champaign during 1995–1998, two visits to HP Bristol during summers 1996 and 2000, a few visits to the Department of Electrical Engineering, University of California at San Diego during 2000–2010, and several visits to the Mathematics Department at Royal Holloway College, during 2007–2009. His research interests include applications of discrete mathematics to problems in computer science and information theory, coding theory, and combinatorial designs.

Dr. Etzion was an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2006 to 2009.