Two-Dimensional Patterns With Distinct Differences—Constructions, Bounds, and Maximal Anticodes

Simon R. Blackburn, Tuvi Etzion, *Fellow, IEEE*, Keith M. Martin, and Maura B. Paterson

***Abstract*—A two-dimensional (2–D) grid with dots is called a *configuration with distinct differences* if any two lines which connect two dots are distinct either in their length or in their slope. These configurations are known to have many applications such as radar, sonar, physical alignment, and time-position synchronization. Rather than restricting dots to lie in a square or rectangle, as previously studied, we restrict the maximum distance between dots of the configuration; the motivation for this is a new application of such configurations to key distribution in wireless sensor networks. We consider configurations in the hexagonal grid as well as in the traditional square grid, with distances measured both in the Euclidean metric, and in the Manhattan or hexagonal metrics. We note that these configurations are confined inside maximal anticodes in the corresponding grid. We classify maximal anticodes for each diameter in each grid. We present upper bounds on the number of dots in a pattern with distinct differences contained in these maximal anticodes. Our bounds settle (in the negative) a question of Golomb and Taylor on the existence of honeycomb arrays of arbitrarily large size. We present constructions and lower bounds on the number of dots in configurations with distinct differences contained in various 2-D shapes (such as anticodes) by considering periodic configurations with distinct differences in the square grid.**

***Index Terms*—Anticodes, Costas arrays, distinct-difference configurations, Golomb rectangles, honeycomb arrays.**

I. Introduction

A GOLOMB ruler (or *ruler* for short) of order m (also known as a *Sidon set*) is a set S of integers with $|S| = m$ having the property that all differences $a - b$ (for $a, b \in S$, with $a \neq b$) are distinct. They were first used by Babcock, in connection with radio interference [1]. The *length* of a Golomb ruler S is the largest difference between any two elements of S. It is easy to show that a ruler of order m has length at least $\binom{m}{2}$; a ruler meeting this bound is called *perfect*. Golomb has shown that no perfect ruler exists with order greater than four [2]. The problem of finding the shortest possible length of a Golomb ruler of a given order has been widely studied; no general solution is known, but optimal rulers have been determined for orders less than 24 (see [3] for details). The elements of a Golomb ruler can be taken to represent marks ("dots") on a physical ruler occurring at integer differences from each other. The fact that the differences are all distinct implies that if a Golomb ruler is placed on top of a second, identical, ruler then at most one mark from the upper ruler will coincide with a mark from the lower ruler, unless they are exactly superimposed. Golomb rulers arise in the literature from both theoretical and practical aspects (see [1], [4]–[6]). It is well known that the largest order of a ruler of length n is $\sqrt{n} + o(\sqrt{n})$, see [4], [5], and [7].

There are various generalizations of 1-D rulers into 2-D arrays. One of the most general was given by Robinson [8]. A 2-D ruler is an $n \times k$ array with m dots such that all $\binom{m}{2}$ lines connecting two dots in the array are distinct as vectors, i.e., any two have either different length or slope. These arrays were also considered in [9] and [10]. The case where $n = k$ was first considered suggested by Costas and investigated by Golomb and Taylor [6]. Costas considered the case when $n = k$ and each row and each column in the array has exactly one dot [6]. These arrays have application to a sonar problem [6], [11] and also to radar, synchronization, and alignment; they are known as Costas arrays. Sonar sequences are another class of arrays mentioned in [6], where $m = k$ and each column has exactly one dot; see [12]–[14].

Other 2-D generalizations of a Golomb ruler have been considered in the literature, but do not have direct connection to our current work. For the sake of completeness we will mention them. A *radar array* is an $n \times k$ array with exactly one dot per column such that there are no two lines connecting two disjoint pairs of dots, occupying the same rows, which have the same length and slope. Radar arrays were defined in [6] and considered in [8], [16]–[18]. Arrays in which all lines have distinct slopes were considered in [18]–[20]. Arrays in which the Euclidean distances of any pair of lines are distinct were considered in [21].

The examples above are concerned with dots in an (infinite) square grid that are restricted to lie in a given line segment, square or rectangle. More generally, we can define a set of dots in a grid to be a distinct difference configuration (DDC) if the lines connecting pairs of dots are different either in length or in slope. Having surveyed the known structures of 2-D patterns with distinct differences, it seems that the following natural question has not been investigated: what is the maximum number of dots that can be placed on a 2-D square grid such

Manuscript received November 25, 2008; revised October 09, 2009. Current version published March 10, 2010. This work was supported in part by the Israel Science Foundation (ISF) by Grant no. 230/08 and by EPSRC grants EP/D053285/1 and EP/F056486/1.

S. R. Blackburn, K. M. Martin, and M. B. Paterson are with the Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, England(e-mail: s.blackburn@rhul.ac.uk; keithmartin@rhul.ac.uk; m.paterson@bbk.ac.uk).

T. Etzion is with the Computer Science Department, Technion-Israel Institute of Technology, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il).

Communicated by T. Fujiwara, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2009.2039046

that all lines connecting two dots are different either in their length or their slope and the distance between any two dots is at most r? In words, rather than considering the traditional rectangular regions of the square grid, we consider dots which lie in maximal anticodes of diameter r. (An anticode of diameter r is a set of positions in the grid such that any pair of positions are at distance at most r. See Section III for details.) We will consider two notions of distance in the square grid: Manhattan and Euclidean. We also consider distinct difference configurations in the hexagonal grid, using hexagonal distance (also known as Manhattan distance) and Euclidean distance.

Our motivation for considering these configurations comes from a new application to key predistribution for wireless sensor networks. We considered in [22] a key predistribution scheme based on DDCs in general, and Costas arrays in particular. A DDC $\mathcal{A}$ with m dots was shifted over the 2-D square grid. For each shift we assigned the same key to the m entries of the 2-D grid which coincide with the m dots of $\mathcal{A}$. In [22], we noted that a Costas array is a DDC, and gave examples of DDCs with small numbers of dots. However, the questions of finding more general constructions, and providing bounds on the number of dots in such configurations, were left open; it is these issues that are addressed by the results of this paper. Other properties of DDCs motivated by this application are considered in [23].

The rest of this paper is organized as follows. In Section II we describe the models on which we will consider our 2-D patterns with distinct differences. We consider two 2-D grids: the square grid and the hexagonal grid. In the square grid we consider the Manhattan distance and the Euclidean distance, while in the hexagonal grid we consider the hexagonal distance and the Euclidean distance. We define the classes of DDCs we will study, and list optimal examples for small parameter sizes. In Section III we explain the relation between DDCs and maximal anticodes. We classify the maximal anticodes when we use Manhattan distance and hexagonal distance. We also briefly review some properties of anticodes in $\mathbb{R}^2$ using Euclidean distance: these properties will allow us to bound the size of an anticode in either grid when we use Euclidean distance. In Section IV we present upper bounds on the number of dots in a DDC when we restrict the dots to lie in some simple regions (‘shapes’) in the grid. The most important shapes we consider are the anticodes, in particular the Lee sphere and the hexagonal sphere. As a consequence of our upper bound, we settle an old question of Golomb and Taylor [24] (on the existence of honeycomb arrays of arbitrarily large size) in the negative. In Sections V and VI, we turn our attention to constructions and lower bounds for the number of dots in the classes of DDC defined in Section II. We generalize a folding technique that was used by Robinson [9] to construct Golomb rectangles, and provide more good examples by constructing periodic infinite arrays that are locally DDCs. Our constructions are asymptotically optimal in the case of the square grid and Manhattan distance.

II. Grids, Distances, and DDCs

We first define some new classes of 2-D distinct difference configurations. We believe that the definitions are very natural and are of theoretical interest, independently of the application we have in mind. We will consider the square grid and the hexagonal grid as our surface. We start with a short definition of the two models. Before the formal definition we emphasize that we define a point (i,j) to be the point in column i and row j of either a coordinate system or a DDC. Hence, rows are indexed from bottom to top in increasing order; columns are indexed from left to right in increasing order. (So this is the usual convention for a Cartesian coordinate system, but is not the standard way of indexing the entries of a finite array.)

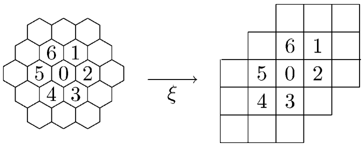

Fig. 1. The hexagonal model translation.

A. The Two Models

The first model is called the *square model*. In this model, a point $(i,j) \in \mathbb{Z}^2$ has the following four neighbors when we consider the model as a connected graph:

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

We can think of the points in $\mathbb{Z}^2$ as being the centers of a tiling of the plane by unit squares, with two centers being adjacent exactly when their squares share an edge. The distance $d((i_1,j_1),(i_2,j_2))$ between two points (i_1,j_1) and (i_2,j_2) in this model is the Manhattan distance defined by

$$d((i_1,j_1),(i_2,j_2)) = |i_2-i_1|+|j_2-j_1|.$$

The second model is called the *hexagonal model*. Instead of the square grid, we define the following graph. 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 vertices of the graph are the center points of the hexagons. We connect two vertices if and only if their respective hexagons share an edge. This way, each vertex has exactly six neighboring vertices.

We will often use an isomorphic representation of the hexagonal model which will be of importance in the sequel. This representation has $\mathbb{Z}^2$ as the set of vertices. 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 models 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. 1. From now on, slightly changing notation, we will also refer to this representation as the hexagonal model. Using this new notation the neighbors of point (i,j) are

$$\begin{aligned}\{(i-1,j-1),(i-1,j),(i,j-1),(i,j+1)&\\ (i+1,j),(i+1,j+1)\}.&\end{aligned}$$

The *hexagonal distance* $d(x,y)$ between two points x and y in the hexagonal grid is the smallest r such that there exists a path with $r+1$ points $x=p_1,p_2,\ldots,p_{r+1}=y$, where p_i and p_{i+1} are adjacent points in the hexagonal grid.

B. Distinct Difference Configurations

We will now define our basic notation for the DDCs we will focus on.

Definition 1: A *Euclidean square distinct difference configuration* $\mathrm{DD}(m,r)$ is a set of m dots placed in a square grid such that the following two properties are satisfied:

1) Any two of the dots in the configuration are at Euclidean distance at most r apart.
2) All the $\binom{m}{2}$ differences between pairs of dots are distinct either in length or in slope.

We will also study three more classes of DDCs: A *square distinct difference configuration* $\overline{\mathrm{DD}}(m,r)$ is defined by replacing 'Euclidean distance' by 'Manhattan distance' in Definition 1; a *Euclidean hexagonal distinct difference configuration* $\mathrm{DD}^*(m,r)$ is defined by replacing "square grid" by 'hexagonal grid' in Definition 1; a *hexagonal distinct difference configuration* $\overline{\mathrm{DD}}^*(m,r)$ is defined by replacing "square grid" by "hexagonal grid," and "Euclidean distance" by "hexagonal distance" in Definition 1.

In the application in [22], dots in the DDC are associated with sensor nodes, and their position in the square or hexagonal grid corresponds to a sensor's position. The parameter r corresponds to a sensor's wireless communication rage. So the most relevant distance measure for the application we have in mind is the Euclidean distance. Moreover, as the best packing of circles on a surface is by arranging the circles in a hexagonal grid (see [25]), the hexagonal model may be often be better from a practical point of view. But the Manhattan and hexagonal distances are combinatorially natural measures to consider, and our results for these distance measures are sharper. Note that Manhattan and hexagonal distance are both reasonable approximations to Euclidean distance (hexagonal distance being the better approximation). Indeed, since the distinct differences property does not depend on the distance measure used, it is not difficult to show that a $\overline{\mathrm{DD}}(m,r)$ is a $\mathrm{DD}(m,r)$, and a $\mathrm{DD}(m,r)$ is a $\overline{\mathrm{DD}}(m,\lceil\sqrt{2}r\rceil)$. Similarly a $\overline{\mathrm{DD}}^*(m,r)$ is a $\mathrm{DD}^*(m,r)$, and a $\mathrm{DD}^*(m,r)$ is an $\overline{\mathrm{DD}}^*(m,\lceil(2/\sqrt{3})r\rceil)$.

C. Small Parameters

For small values of r, we used a backtrack search to exhaustively find a $\overline{\mathrm{DD}}(m,r)$ with m as large as possible. The search shows that for $r=2,3$, the largest such m are 3 and 4, respectively, and for $4\le r\le 11$ the largest possible m is $r+2$. Fig. 2 contains examples of configurations meeting those bounds.

Similarly, we found the best configurations $\overline{\mathrm{DD}}^*(m,r)$ in the hexagonal grid (see Fig. 3) for $2\le r\le 10$.

III. Anticodes and DDCs

In this section, we will show a trivial connection between DDCs and maximal anticodes. This leads to a short investigation of maximal anticodes in the square and the hexagonal grids. We find all maximal anticodes in these two models under the Manhattan and hexagonal distance measures, respectively.

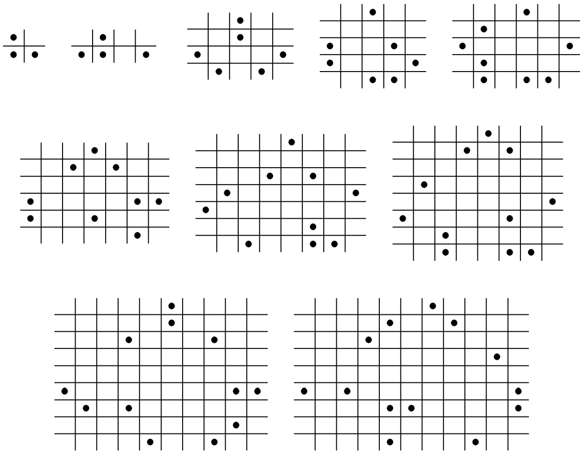

Fig. 2. Square distinct difference configurations with the largest number of dots possible for $r=2,3,\ldots,11$.

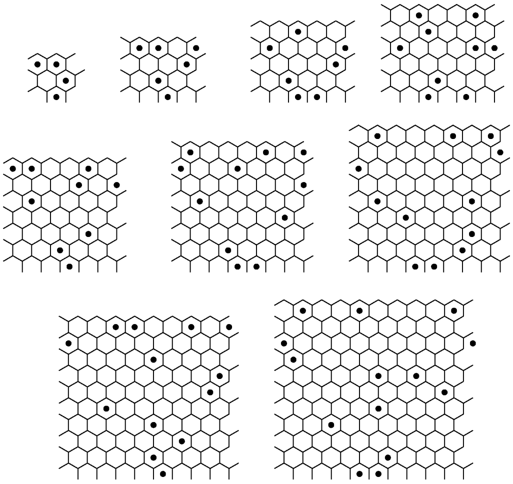

Fig. 3. Hexagonal distinct difference configurations with the largest number of dots possible for $r=2,3,\ldots,10$.

An *anticode* of diameter r in the 2-D grid (square or hexagonal) is a set $\mathcal{S}$ of points such that for each pair of points $x,y\in\mathcal{S}$ we have $d(x,y)\le r$, where the distance can be Manhattan, hexagonal, or Euclidean. An anticode $\mathcal{S}$ of diameter r is said to be *optimal* if there is no anticode $\mathcal{S}'$ of diameter r such that $|\mathcal{S}'|>|\mathcal{S}|$. An anticode $\mathcal{S}$ of diameter r is said to be *maximal* if $\{x\}\cup\mathcal{S}$ has diameter greater than r for any $x\notin\mathcal{S}$. Anticodes are important structures in various aspects of coding theory and extremal combinatorics [26]–[32].

The following two results provide an obvious connection between DDCs and anticodes.

Lemma 1: Any anticode $\mathcal{S}$ of diameter r is contained in a maximal anticode $\mathcal{S}'$ of diameter r.

Corollary 2: A $\mathrm{DD}(m,r)$ is contained in a maximal anticode of (Euclidean) diameter r. The same statement holds for a $\overline{\mathrm{DD}}(m,r)$, $\mathrm{DD}^*(m,r)$ or $\overline{\mathrm{DD}}^*(m,r)$ when the appropriate distance measure is used.

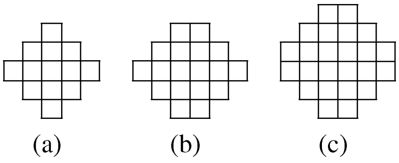

Fig. 4. Maximal anticodes in the square grid.

A. Maximal Anticodes in the Square Grid

We start by defining three shapes in the square grid. We will prove that these shapes are the only maximal anticodes in the square grid when we use Manhattan distance.

A *Lee sphere* of radius R is the shape in the square model which consists of one point as center and all positions of Manhattan distance at most R from this center. The area of this Lee sphere is $2R^2+2R+1$. For the seminal paper on Lee spheres see [33]. Fig. 4(a) illustrates a Lee sphere of radius 2.

A *bicentered Lee sphere* of radius R is the shape in the square model which consists of two center points (a 2×1 or a 1×2 rectangle) and all positions of Manhattan distance at most R from at least one point of this center. The area of this bicentered Lee sphere is $2R^2+4R+2$. These shapes were used for 2-D burst-correction in [34]. Fig. 4(b) illustrates a bicentered Lee sphere of radius 2.

A *quadricentered Lee sphere* of radius R is the shape in the square model which consists of four center points (a 2×2 square) and all positions of Manhattan distance at most $R-1$ from at least one point of this center. The area of this quadricentered Lee sphere is $2R^2+2R$. These shapes were defined using the name "generalized Lee sphere" in [35]. Fig. 4(c) illustrates a quadricentered Lee sphere of radius 3.

Theorem 3:

- For even r there are two different types of maximal anticodes of diameter r in square grid: the Lee sphere of radius $\frac{r}{2}$ and the quadricentered Lee sphere of radius $\frac{r}{2}$.
- For odd r there is exactly one type of maximal anticode of diameter r in the square grid: the bicentered Lee sphere of radius $\frac{r-1}{2}$.

Proof: Let $\mathcal{A}$ be a maximal anticode of diameter r in the square grid.

Assume first that r is even, so $r=2\rho$. We will embed $\mathcal{A}$ in the 2-D square grid in such a way that there is position in $\mathcal{A}$ on the line $y=x$, but no position below it. The Manhattan distance between a point on the line $y=x+2\rho$ and a point on the line $y=x$ is at least 2ρ and hence $\mathcal{A}$ is bounded by the lines $y=x$ and $y=x+2\rho$. Similarly, without loss of generality we can assume that there is a position in $\mathcal{A}$ on the line $y=-x$ or $y=-x+1$ and no position below this line, so $\mathcal{A}$ is bounded by the lines $y=-x$ and $y=-x+2\rho$, or by the lines $y=-x+1$ and $y=-x+2\rho+1$. These four lines define a Lee sphere of radius ρ or a quadricentered Lee sphere of radius ρ.

Now, assume that r is odd, so $r=2\rho+1$. We will embed $\mathcal{A}$ in the 2-D square grid in a way that a position of $\mathcal{A}$ lies on the line $y=x$, but no position lies below it. The Manhattan distance between a point on the line $y=x+2\rho+1$ and a point on the line $y=x$ is at least $2\rho+1$ and hence $\mathcal{A}$ is bounded by the lines $y=x$ and $y=x+2\rho+1$. Similarly, without loss of generality we can assume that there is a position of $\mathcal{A}$ on the line $y=-x$ or $y=-x+1$ and no position below this line, and so $\mathcal{A}$ is bounded by the lines $y=-x$ and $y=-x+2\rho+1$ or by the lines $y=-x+1$ and $y=-x+2\rho+2$. In either case, these four lines define a bicentered Lee sphere of radius ρ. □

Finally, the following theorem is interesting from a theoretical point of view.

Theorem 4: There exists a $\overline{\mathrm{DD}}(m,r)$ for which the only maximal anticode of diameter r containing it is a Lee sphere (bicentered Lee sphere, quadricentered Lee sphere) of diameter r.

Proof: We provide the configurations that are needed. All the claims in the proof below are readily verified and left to the reader.

When r is odd, we may take two points on the same horizontal line such that $d(x,y)=r$: this pair of points is in a bicentered Lee sphere of radius $\frac{r-1}{2}$. When r is even, the same example is contained in a Lee sphere of radius $r/2$, but is not contained in a quadricentered Lee sphere of radius $r/2$.

Let r be even, and set $R=r/2$. The points $(0,R-1),(0,R)$, $(2R-2,0),(2R-2,2R-1)$, and $(2R-1,R)$ form $\overline{\mathrm{DD}}(5,2R)$. This set of points is not contained in a Lee sphere of radius R, but is contained in a quadricentered Lee sphere of radius R. □

B. Maximal Anticodes in the Hexagonal Grid

Theorem 5: There are exactly $\lceil\frac{r+1}{2}\rceil$ different types of maximal anticodes of diameter r in the hexagonal grid, namely the anticodes $\mathcal{A}_0,\mathcal{A}_1,\ldots,\mathcal{A}_{\lceil\frac{r-1}{2}\rceil}$ defined in the proof later.

Proof: We consider the translation of the hexagonal grid into the square grid. By shifting it appropriately, any maximal anticode $\mathcal{A}$ of diameter r can be located inside an $(r+1)\times(r+1)$ square $\mathcal{B}$ with corners at $(0,0),(0,r),(r,0)$, and (r,r). Let i be defined by the property that the lines $y=x-i$ contains a point of $\mathcal{A}$, but no point of $\mathcal{A}$ lies below this line.

We claim that $i\geq 0$. To see this, assume for a contradiction that $i<0$. Then $\mathcal{A}$ is contained in the region of $\mathcal{B}$ bounded by the lines $y=x-i, y=r$, and $x=0$. But the point $(0,r+1)$ outside $\mathcal{B}$ is within distance r from all the points of this region, contradicting the fact that $\mathcal{A}$ is a maximal anticode. Thus, $i\geq 0$ and our claim follows.

All the points on the line $y=x-i$ that are inside $\mathcal{B}$ are within hexagonal distance r from all points on the lines $y=x-i+j, 0\leq j\leq r$, that lie inside $\mathcal{B}$. All the points on the line $y=x-i$ inside $\mathcal{B}$ have hexagonal distance greater than r from all the points on the line $y=x-i+r+1$. Hence, as $\mathcal{A}$ is maximal, $\mathcal{A}$ consists of all the points bounded by the lines $y=x-i$ and $y=x-i+r$ inside $\mathcal{B}$. It is easy to verify that each one of the $r+1$ anticodes $\mathcal{A}_i$ defined in this way is a maximal anticode. One can readily verify that $\mathcal{A}_i$ and $\mathcal{A}_{r-i}$ are equivalent anticodes, since $\mathcal{A}_{r-i}$ is obtained by rotating $\mathcal{A}_i$ by 180 degrees. So the theorem follows. □

Theorem 6: Let i be fixed, where $0\leq i\leq\lceil\frac{r-1}{2}\rceil$. There exists a $\overline{\mathrm{DD}}^*(m,r)$ for which the only maximal anticode of diameter r containing it is of the form $\mathcal{A}_i$.

Proof: Again, we provide the configurations, and leave the verification of the details to the reader.

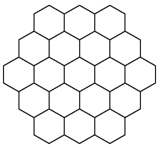

Fig. 5. Hexagonal sphere of radius 2.

For each $i, 1 \leq i \leq \frac{r-1}{2}, \mathcal{A}_i$ has six corner points. If we assign a dot to each corner point, then we will obtain a DDC which cannot be inscribed in another maximal anticode. When $r = 2R$ these six points do not define a DDC in $\mathcal{A}_R$. In this case, we assign seven dots to $\mathcal{A}_R$ as follows. In four consecutive corner points we assign a dot; in the next corner point we assign two dots in the adjacent points on the boundary of $\mathcal{A}_R$; in the last corner point we assign a dot in the adjacent point on the boundary of $\mathcal{A}_R$ towards the first corner point. When $i = 0, \mathcal{A}_i$ is a triangle and has three corner points. If we assign a dot to each of these corner points we will obtain a DDC which cannot be inscribed in another maximal anticode. □

We now consider some basic properties of these $\lceil \frac{r+1}{2} \rceil$ anticodes. First, the number of grid points in $\mathcal{A}_i$ is $(r+1)^2 - \frac{i(i+1)}{2} - \frac{(r-i)(r+1-i)}{2} = \frac{(r+1)(r+2)}{2} + i(r-i)$. The smallest anticode is $\mathcal{A}_0$, an isosceles right triangle with base and height of length $r+1$ containing $\frac{(r+1)(r+2)}{2}$ points. The largest anticode is the *hexagonal sphere* $\mathcal{A}_{\lceil \frac{r-1}{2} \rfloor}$ of radius $r/2$. The hexagonal sphere contains $\frac{3(r+1)^2}{4}$ points when r is odd, and contains $\frac{3r^2+6r+4}{4} = 3(\frac{r}{2})^2 + 3(\frac{r}{2}) + 1$ points when r is even. The hexagonal sphere of radius R is the shape in the hexagonal model which consists of a center point and all positions in hexagonal distance at most R from this center (Fig. 5).

C. Maximal Anticodes With Euclidean Distance

It seems much more difficult to classify the maximal anticodes in the square and hexagonal grids when we use Euclidean distance. Note that the representation of the hexagonal grid in the square grid does not preserve Euclidean distances, and so we cannot use the map ξ. We expect that the overall shape of a maximal anticode in both models should be similar, since a maximal anticode in both models is just the intersection of a maximal anticode in $\mathbb{R}^2$ with the centers of our squares or hexagons, respectively. But the "local" structure of an anticode will be different: for example, in the hexagonal grid we can have three dots that are pairwise at distance r, but this is not possible in the square grid.

Because maximal anticodes in $\mathbb{R}^2$ determine the shape of maximal anticodes in the square or hexagonal models, we conclude this section with a brief description of such anticodes.

An anticode is confined to the area as depicted in Fig. 6(a), where dots are two elements in the anticode at distance r. The most obvious maximal anticode is a circle of diameter r depicted in Fig. 6(b). Another maximal anticode is depicted in Fig. 6(c), and is constructed by taking three dots at the vertices of an equilateral triangle of side r, and intersecting the circles of radius r about these dots. Between the "triangular" anticode and the circle there are infinitely many other maximal anticodes. We will need the following "isoperimetrical" theorem; see Littlewood [36, p. 32] for a proof.

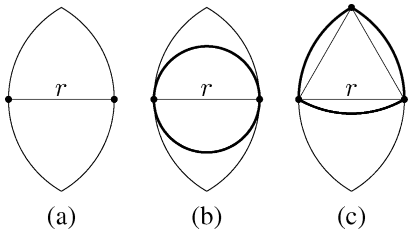

Fig. 6. Anticodes in the Euclidean distance.

Theorem 7: Let $\mathcal{A}$ be a region of $\mathbb{R}^2$ of diameter r and area a. Then $a \leq (\pi/4)r^2$.

We remark that the example of a circle of diameter r shows that the bound of this theorem is tight.

IV. Upper Bounds on the Number of Dots

In this section we will provide asymptotic upper bounds on the number of dots that can be contained in a DDC, using a technique due to Erdős and Turán [18], [37]. We start by considering upper bounds on the number m of dots in a $\overline{\mathrm{DD}}(m,r)$ and a $\overline{\mathrm{DD}}^*(m,r)$, and then consider upper bounds in a $\mathrm{DD}(m,r)$ and $\mathrm{DD}^*(m,r)$. The results for small parameters in Section II might suggest that a $\overline{\mathrm{DD}}(m,r)$ can always contain $r+2$ dots: our result (Theorem 9) that $m \leq \frac{1}{\sqrt{2}}r + o(r)$ surprised us. Our techniques easily generalise to DDCs where we restrict the dots to lie in various shapes in the grid not necessarily related to distance measures: we end the section with a brief discussion of this general situation.

A. Manhattan and Hexagonal Distances

Lemma 8: Let r be a nonnegative integer. Let $\mathcal{A}$ be an anticode of Manhattan diameter r in the square grid. Let ℓ be a positive integer such that $\ell \leq r$, and let w be the number of Lee spheres of radius ℓ that intersect $\mathcal{A}$ nontrivially. Then $w \leq \frac{1}{2}(r+2\ell)^2 + O(r)$.

Proof: Let $\mathcal{A}'$ be the set of centers of the Lee spheres we are considering, so $w = |\mathcal{A}'|$. We claim that $\mathcal{A}'$ is an anticode of diameter at most $r+2\ell$. To see this, let $c, c' \in \mathcal{A}'$. Since the spheres of radius ℓ about c and c' intersect $\mathcal{A}$ nontrivially, there exist elements $a, a' \in \mathcal{A}$ such that $d(c,a) \leq \ell$ and $d(c',a') \leq \ell$. But then

$$d(c,c') \leq d(c,a) + d(a,a') + d(a',c') \leq \ell + r + \ell = r + 2\ell,$$

and so our claim follows.

Let $\mathcal{A}''$ be a maximal anticode of diameter $r+2\ell$ containing $\mathcal{A}'$. Theorem 3 implies that $\mathcal{A}$" is a Lee sphere, bicentered Lee sphere, or quadricentered Lee sphere of radius R, where $R = \lfloor (r+2\ell)/2 \rfloor$. In all three cases, $|\mathcal{A}''| = 2R^2 + O(R) = \frac{1}{2}(r+2\ell)^2 + O(r)$. Since

$$w = |\mathcal{A}'| \leq |\mathcal{A}''|$$

the lemma follows. □

Theorem 9: If a $\overline{\mathrm{DD}}(m,r)$ exists, then

$$m \leq \frac{1}{\sqrt{2}}r + (3/2^{4/3})r^{2/3} + O(r^{1/3}).$$

Proof: We begin by giving a simple argument that leads to a linear bound on m in terms of r, with an inferior leading term to the bound in the statement of the theorem. There are $2r^2+2r$ nonzero vectors of Manhattan length r or less, where a vector is a line with direction which connects two points. The distinct difference property implies that each such vector arises at most once as the vector difference of a pair of dots. Since a configuration of m dots gives rise to $m(m-1)$ vector differences, we find that

$$m(m-1) \leq 2r^2 + 2r.$$

In particular, we see that $m \leq \sqrt{2}r + o(r) = O(r)$.

We now establish the bound of the theorem. Since all the dots are at distance at most r, we see that all dots are contained in a fixed anticode $\mathcal{A}$ of the square grid of diameter r. Set $\ell = \lfloor \alpha r^{2/3} \rfloor$, where we will choose the constant α later so as to optimize our bound. We cover $\mathcal{A}$ with all the 'small' Lee spheres of radius ℓ that intersect $\mathcal{A}$ nontrivially. Every point of $\mathcal{A}$ is contained in exactly a small Lee spheres, where $a = 2\ell^2+2\ell+1$. Moreover, by Lemma 8, we have used w small Lee spheres, where $w \leq \frac{1}{2}(r+2\ell)^2 + O(r)$.

Let m_i be the number of dots in the ith small Lee sphere. Let μ be the mean of the integers m_i. Since every dot is contained in exactly a small Lee spheres, $\mu = am/w$. We aim to show that

$$w(\mu^2-\mu) \leq \sum_{i=1}^{w} m_i(m_i-1) \leq a(a-1). \qquad (1)$$

The first inequality in (1) follows from expanding the nonnegative sum $\sum_{i=1}^{w}(\mu-m_i)^2$, so it remains to show the second inequality.

The sum $\sum_{i=1}^{w} m_i(m_i-1)$ counts the number of pairs $(\mathcal{L},d)$ where $\mathcal{L}$ is a small Lee sphere and d is a vector difference between two dots in ℓ. Every difference d arises from a unique ordered pair of dots in $\mathcal{A}$, since the dots form a distinct difference configuration. Thus

$$\sum_{i=1}^{w} m_i(m_i-1) \leq \sum_{d} k(d),$$

where we sum over all nonzero vector differences d and where $k(d)$ is the number of Lee spheres of radius ℓ that contain any fixed pair of dots with vector difference d. If we assume that the first element of the pair of dots with vector difference d lies at the origin, we see that

$$\sum_{d} k(d) = a(a-1)$$

since there are exactly a Lee spheres of radius ℓ containing the origin, and each such sphere contributes 1 to $k(d)$ for exactly $a-1$ values of d. Thus we have established (1).

Now, the inequality (1) together with the fact that $\mu = am/w$ imply that

$$(\mu-1)m \leq a-1 \leq a,$$

and so

$$m^2 \leq w\left(1+\frac{m}{a}\right). \qquad (2)$$

By Lemma 8,

$$\sqrt{w} \leq \frac{1}{\sqrt{2}}r\left(1+\frac{2\ell}{r}+O(r^{-1})\right),$$

and we have that

$$\sqrt{(1+(m/a))} = 1 + m/(2a) + O((m/a)^2).$$

Since $m = O(r)$ and $a \geq 2\alpha^2 r^{4/3}$, these two inequalities combine with (2) to show that

$$m \leq \frac{1}{\sqrt{2}}r\left(1+2\alpha r^{-1/3}+\frac{m}{4\alpha^2 r^{4/3}}+O(r^{-2/3})\right). \qquad (3)$$

Since $m = O(r)$, this inequality implies that $m \leq \frac{1}{\sqrt{2}}r + O(r^{2/3})$. Combining this tighter bound with (3) we find that

$$m \leq \frac{1}{\sqrt{2}}r\left(1+\left(2\alpha+\frac{1}{4\sqrt{2}\alpha^2}\right)r^{-1/3}+O(r^{-2/3})\right).$$

The expression $2\alpha + 1/(4\sqrt{2}\alpha^2)$ is minimized when $\alpha = 2^{-5/6}$ at the value $3/2^{5/6}$, so choosing this value for α we deduce that

$$\begin{aligned} m &\leq \frac{1}{\sqrt{2}}r\left(1+\frac{3}{2^{5/6}}r^{-1/3}+O(r^{-2/3})\right) \\ &= \frac{1}{\sqrt{2}}r + \frac{3}{2^{4/3}}r^{2/3} + O(r^{1/3}) \end{aligned}$$

as required. □

We now look at the hexagonal grid.

Lemma 10: Let r be a nonnegative integer. Let $\mathcal{A}$ be an anticode of hexagonal diameter r in the hexagonal grid. Let ℓ be a positive integer such that $\ell \leq r$, and let w be the number of hexagonal spheres of radius ℓ that intersect $\mathcal{A}$ nontrivially. Then $w \leq \frac{3}{4}(r+2\ell)^2 + O(r)$.

Proof: The set of centers of the hexagonal spheres of radius ℓ that have nontrivial intersection with $\mathcal{A}$ clearly form an anticode of diameter at most $r+2\ell$. Therefore the number w of such spheres is bounded by the maximal size of such an anticode. The results on the maximal anticodes in the hexagonal metric in Section III imply that

$$\begin{aligned} w &\leq \frac{1}{4}(3(r+2\ell)^2+6(r+2\ell)+4) \\ &= \frac{3}{4}(r+2\ell)^2 + O(r) \end{aligned}$$

as required. □

Theorem 11: If a $\overline{\mathrm{DD}}^{*}(m,r)$ exists, then

$$m \leq \frac{\sqrt{3}}{2}r + (3^{4/3}2^{-5/3})r^{2/3} + O(r^{1/3}).$$

Proof: The dots in a $\overline{\mathrm{DD}}^*(m,r)$ form an anticode of diameter r. Let $\ell = \lfloor 2^{-2/3}3^{-1/6}r^{2/3} \rfloor$. We may cover these dots with the w hexagonal spheres of radius ℓ that contain one or more of these dots. By Lemma 10, we have that $w \leq \frac{3}{4}(r+2\ell)^2+O(r)$.

Using the fact that a hexagonal sphere of radius ℓ contains a points in the hexagonal grid, where $a = 3\ell^2 + 3\ell + 1$, we may argue exactly as in Theorem 9 to produce the bound (2). There are $O(r^2)$ vectors in the hexagonal grid of hexagonal length r or less, so the argument in the first paragraph of Theorem 9 shows that $m = O(r)$. Since $m/a = O(r^{-1/3})$, the bound (2) implies that

$$m \leq \sqrt{w} + O(r^{2/3}) = \frac{\sqrt{3}}{2}r + O(r^{2/3}).$$

This bound on m implies that $m/a = 2^{1/3}3^{-1/6}r^{-1/3} + O(r^{-2/3})$, and so applying (2) once more we obtain the bound of the theorem, as required. □

One consequence of Theorem 11 is an answer to the ninth question asked by Golomb and Taylor [24]: a *honeycomb array* is a DDC in the hexagonal grid whose dots, when represented in the square grid, form an $m \times m$ Costas array whose dots lie in m consecutive 'North-East' diagonals. Honeycomb arrays are the natural hexagonal analogue of Costas arrays. Do honeycomb arrays exist for infinitely many m? The conjecture in [24] is that the answer is YES. However, the answer is in fact NO, as the following corollary to Theorem 11 shows.

Corollary 12: Honeycomb arrays exist for only a finite number of values of m.

Proof: The dots in a honeycomb array are contained in an anticode of diameter at most $m-1$ (using hexagonal distance). Hence a honeycomb array is a $\overline{\mathrm{DD}}^*(m, m-1)$. But Theorem 11 shows that $m \leq \frac{\sqrt{3}}{2}m + O(m^{2/3})$. Since $\frac{\sqrt{3}}{2} < 1$, no honeycomb array exists when m is sufficiently large. □

In fact, numerical computations indicate that no honeycomb arrays exist for $m \geq 1289$: for m in this range, there is a suitable choice of ℓ such that a honeycomb array violates (2).

B. Euclidean Distance

We now turn our attention to Euclidean distance. Our first lemma is closely related to Gauss's circle problem.

Lemma 13: Let ℓ be a positive integer, and let $\mathcal{S}$ be a (Euclidean) circle of radius ℓ in the plane. Then the number of points of the square grid contained in $\mathcal{S}$ is $\pi\ell^2 + O(\ell)$.

Proof: Let c be the center of $\mathcal{S}$. Let X be the set of points of the square grid contained in $\mathcal{S}$. Define $\mathcal{X}$ to be the union of all unit squares whose centers lie in X. Clearly $\mathcal{X}$ has area $|X|$. The maximum distance from the center of a unit square to any point in the unit square is at most $1/\sqrt{2}$, and so $\mathcal{X}$ is contained in the circle of radius $\ell + (1/\sqrt{2})$ with center c. Similarly, every point in a circle of radius $\ell - (1/\sqrt{2})$ with center c is contained in $\mathcal{X}$. Hence

$$\pi(\ell - (1/\sqrt{2}))^2 \leq |X| \leq \pi(\ell + (1/\sqrt{2}))^2$$

and so the lemma follows. □

Lemma 14: Let r be a nonnegative integer. Let $\mathcal{A}$ be an anticode in the square grid of Euclidean diameter r. Let ℓ be a positive integer such that $\ell \leq r$, and let w be the number of circles of radius ℓ whose centers lie in the square grid and that intersect $\mathcal{A}$ nontrivially. Then $w \leq (\pi/4)(r+2\ell)^2 + O(r)$.

Proof: As in Lemma 8, it is not difficult to see that the set $\mathcal{A}'$ of centers of circles we are considering form an anticode in the square grid of diameter at most $r + 2\ell$. Note that $w = |\mathcal{A}'|$. Let $\mathcal{X}$ be the union of the unit squares whose centers lie in $\mathcal{A}'$, so $\mathcal{X}$ has area w. The maximum distance between the center of a unit square and any other point in this square is $1/\sqrt{2}$, and so $\mathcal{X}$ is an anticode in $\mathbb{R}^2$ of diameter at most $r + 2\ell + (1/\sqrt{2})$. Hence, by Theorem 7, $w \leq (\pi/4)(r + 2\ell + (1/\sqrt{2}))^2$ and the lemma follows. □

Theorem 15: If a $\mathrm{DD}(m,r)$ exists, then

$$m \leq \frac{\sqrt{\pi}}{2}r + \frac{3\,\pi^{1/3}}{2^{5/3}}r^{2/3} + O(r^{1/3}).$$

Proof: The proof is essentially the same as the proof of Theorem 11, using Lemma 13 to bound the number a of points in a sphere of radius ℓ, and using Lemma 14 instead of Lemma 10. The bound of the theorem is obtained if we set $\ell = \lfloor 1/(2^{2/3}\pi^{1/6})r^{2/3} \rfloor$. □

Lemma 16: Let ℓ be a positive integer, and let $\mathcal{S}$ be a (Euclidean) circle of radius ℓ in the plane. Then the number of points of the hexagonal grid contained in $\mathcal{S}$ is $(2\pi/\sqrt{3})\ell^2 + O(\ell)$.

Proof: The proof of the lemma is essentially the same as the proof of Lemma 13. The hexagons whose centers form the hexagonal grid have area $\sqrt{3}/2$, and the maximum distance of the center of a hexagon to any point in the hexagon is $1/\sqrt{3}$. Define X to be the set of points of the hexagonal grid contained in $\mathcal{S}$, and let $\mathcal{X}$ be the union of all hexagons in our grid whose centers lie in X. Clearly, $\mathcal{X}$ has area $(\sqrt{3}/2)|X|$. The argument of Lemma 13 shows that

$$\pi(\ell - (1/\sqrt{3}))^2 \leq (\sqrt{3}/2)|X| \leq \pi(\ell + (1/\sqrt{3}))^2$$

and so the lemma follows. □

Lemma 17: Let r be a nonnegative integer. Let $\mathcal{A}$ be an anticode in the square grid of Euclidean diameter r. Let ℓ be a positive integer such that $\ell \leq r$, and let w be the number of circles of radius ℓ whose centers lie in the hexagonal grid and that intersect $\mathcal{A}$ nontrivially. Then $w \leq (\pi/(2\sqrt{3}))(r+2\ell)^2+O(r)$.

Proof: The proof of this lemma is essentially the same as the proof of Lemma 14. The argument there with appropriate modifications shows that $(\sqrt{3}/2)w \leq (\pi/4)(r+2\ell+(1/\sqrt{3}))^2$ (where the factor of $\sqrt{3}/2$ comes from the fact that the hexagons associated with our grid have area $\sqrt{3}/2$). □

Theorem 18: If a $\mathrm{DD}^*(m,r)$ exists, then

$$m \leq \frac{\sqrt{\pi}}{\sqrt{2}\,3^{1/4}}r + \frac{3^{5/6}\pi^{1/3}}{2^{4/3}}r^{2/3} + O(r^{1/3}).$$

Proof: The proof is the same as the proof of Theorem 15, using Lemmas 16 and 17 in place of Lemmas 13 and 14, and defining $\ell = \lfloor 3^{1/12}2^{-5/6}\pi^{-1/6}r^{2/3} \rfloor$. □

C. More General Shapes

All the theorems above consider a maximal anticode in some metric, and cover this region with small circles of radius ℓ. We comment (for use later) that the same techniques work for any "sensible" shape that is not necessarily an anticode. (We just need that the number of small circles that intersect our shape is approximately equal to the number of grid points contained in the shape.) So we can prove similar theorems for DDCs that are restricted to lie inside regular polygons, for example. The maximal number of dots in such a DDC is at most $\sqrt{s}+o(\sqrt{s})$ when the shape contains s points of the grid.

V. Periodic 2-D Configurations

The previously known constructions for DDCs restrict dots to lie in a line or a rectangular region (often a square region) of the plane. The application described in [22] instead demands that the dots lie in some anticode. The most straightforward approach to constructing DDCs for our application is to find a large square or rectangular subregion of our anticode, and use one of these known constructions to place dots in this subregion. This approach provides a lower bound for m that is linear in r, but, in fact, we are able to do much better than this by modifying known constructions (in the case of Robinson's folding technique later) and by making use of certain periodicity properties of infinite arrays related to rectangular constructions. We will explain how this can be done in the next section. In this section, we will survey some of the known constructions for rectangular DDCs, extend these constructions to infinite periodic arrays, and prove the properties we need for Section VI.

Let $\mathcal{A}$ be a (generally infinite) array of dots in the square grid, and let η and κ be positive integers. We say that $\mathcal{A}$ is *doubly periodic* with period (η,κ) if $\mathcal{A}(i,j)=\mathcal{A}(i+\eta,j)$ and $\mathcal{A}(i,j)=\mathcal{A}(i,j+\kappa)$ for all integers i and j. We define the *density* of $\mathcal{A}$ to be $d/(\eta\kappa)$, where d is the number of dots in any $\kappa\times\eta$ subarray of $\mathcal{A}$. Note that the period (η,κ) will not be unique, but that the density of $\mathcal{A}$ does not depend on the period we choose. We say that a doubly periodic array $\mathcal{A}$ of dots is *a doubly periodic* $n\times k$ *DDC* if every $n\times k$ subarray of $\mathcal{A}$ is a DDC. See [14], [38], and [39] for some information on doubly periodic arrays in this context. We aim to present several constructions of doubly periodic DDCs of high density.

A. Constructions From Costas Arrays

A Costas array of order n is an $n\times n$ permutation array which is also a DDC. Essentially two constructions for Costas arrays are known, and both give rise to doubly periodic DDCs.

The Periodic Welch Construction: Let α be a primitive root modulo a prime p and let $\mathcal{A}$ be the square grid. For any integers i and j, there is a dot in $\mathcal{A}(i,j)$ if and only if $\alpha^i\equiv j \bmod p$.

The following theorem is easy to prove. A proof which also mentions some other properties of the construction is given in [23].

Theorem 19: Let $\mathcal{A}$ be the array of dots from the Periodic Welch Construction. Then $\mathcal{A}$ is a doubly periodic $p\times(p-1)$ DDC with period $(p-1,p)$ and density $1/p$.

Indeed, it is not difficult to show that each $p\times(p-1)$ subarray is a DDC with $p-1$ dots: a dot in each column and exactly one empty row. The $(p-1)\times(p-1)$ subarray with lower left corner at $\mathcal{A}(1,1)$ is a Costas array.

The Periodic Golomb Construction: Let α and β be two primitive elements in GF(q), where q is a prime power. For any integers i and j, there is a dot in $\mathcal{A}(i,j)$ if and only if $\alpha^i+\beta^j=1$.

The following theorem is proved similarly to the proof in [23] and [40].

Theorem 20: Let $\mathcal{A}$ be the array of dots from the Periodic Golomb Construction. Then $\mathcal{A}$ is a doubly periodic $(q-1)\times(q-1)$ DDC with period $(q-1,q-1)$ and density $(q-2)/(q-1)^2$.

Indeed, each $(q-1)\times(q-1)$ subarray of $\mathcal{A}$ is a DDC with $q-2$ dots; exactly one row and one column are empty. The $(q-2)\times(q-2)$ subarray with lower left corner at $\mathcal{A}(1,1)$ is a Costas array.

If we take $\alpha=\beta$ in the Golomb construction, then the construction is known as the Lempel Construction. There are various variants for these two constructions resulting in Costas arrays with orders slightly smaller (by 1, 2, 3, or 4) or larger by one than the orders of these two constructions (see [41] and [24]). These are of less interest in our discussion, as they do not extend to doubly periodic arrays in an obvious way.

B. Constructions From Golomb Rectangles

A *Golomb rectangle* is an $n\times k$ DDC with m dots; Costas arrays are a special case. Apart from constructions of special cases, there is essentially one other general construction known, the *folded rulers* construction due to Robinson [9].

Folded Ruler Construction: Let $S=\{a_1,a_2,\cdots,a_m\}\subseteq\{0,1,\ldots,n\}$ be a Golomb ruler of length n. Let ℓ and k be integers such that $\ell\cdot k\leq n+1$. Define $\mathcal{A}$ to be the $\ell\times k$ array where $\mathcal{A}(i,j), 0\leq i\leq k-1, 0\leq j\leq \ell-1$, has a dot if and only if $i\cdot\ell+j=a_t$ for some t.

Theorem 21: The array $\mathcal{A}$ of the Folded Ruler Construction is an $\ell\times k$ Golomb rectangle.

We now show how to adapt the Folded Ruler Construction to obtain a doubly periodic $\ell\times k$ DDC. We require a stronger object than a Golomb ruler as the basis for our folding construction, defined as follows.

Definition 2: Let A be an abelian group, and let $D=\{a_1,a_2,\ldots,a_m\}\subseteq A$ be a sequence of m distinct elements of A. We say that D is a B_2*-sequence over* A if all the sums $a_{i_1}+a_{i_2}$ with $1\leq i_1\leq i_2\leq m$ are distinct.

For a survey on B_2-sequences and their generalizations the reader is referred to [42]. The following lemma is well known and can be readily verified.

Lemma 22: A subset $D=\{a_1,a_2,\ldots,a_m\}\subseteq A$ is a B_2-sequence over A if and only if all the differences $a_{i_1}-a_{i_2}$ with $1\leq i_1\neq i_2\leq m$ are distinct in A.

So, in particular, a Golomb ruler is exactly a B_2-sequence over $\mathbb{Z}$. Note that a B_2-sequence $\{a_1,a_2,\ldots,a_m\}$ over $\mathbb{Z}_n$ produces a Golomb ruler $\{b_1,b_2,\ldots,b_m\}$ whenever the b_i are integers such that $a_i\equiv b_i \bmod n$. Also note that if D is a B_2-sequence over $\mathbb{Z}_n$ and $a\in\mathbb{Z}_n$, then so is the shift $a+D=\{a+d: d\in D\}$. The following theorem, due to Bose [43], shows that large B_2-sequences over $\mathbb{Z}_n$ exist for many values of n.

Theorem 23: 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 $m = q$.

The Doubly Periodic Folding Construction: Let n be a positive integer and $D = \{a_1, a_2, \ldots, a_m\}$ be a B_2-sequence in $\mathbb{Z}_n$. Let ℓ and k be integers such that $\ell \cdot k \leq n$. Let $\mathcal{A}$ be the square grid. For any integers i and j, there is a dot in $\mathcal{A}(i,j)$ if and only if $a_t \equiv i \cdot \ell + j \bmod n$ for some t.

Theorem 24: Let $\mathcal{A}$ be the array of the Doubly Periodic Folding Construction. Then $\mathcal{A}$ is a doubly periodic $\ell \times k$ DDC of period $(\frac{n}{\gcd(n,\ell)}, n)$ and density m/n.

Proof: Let $f(x,y) = x \cdot \ell + y$. The period of $\mathcal{A}$ follows from the observation that for each two integers α and β we have $f(i,j) = f(i + \alpha\frac{n}{\gcd(n,\ell)}, j + \beta n) \equiv i \cdot \ell + j \bmod n$. The density of $\mathcal{A}$ is m/n follows since there are exactly m dots in any n consecutive positions in any column.

Let $\mathcal{S}$ be an $\ell \times k$ subarray, whose lower left-hand corner is at $\mathcal{A}(i,j)$. An alternative construction of the dots in $\mathcal{S}$ is as follows. Take the shift $(i \cdot \ell + j) + D$ of D, which is also a B_2-sequence in $\mathbb{Z}_n$. Let D' be the corresponding Golomb ruler in $\{0, 1, \ldots, n-1\}$, so $a \in D$ if and only if $a \equiv b \bmod n$, where $b \in (i \cdot \ell + j) + D$. Then form dots in $\mathcal{S}$ by using the Folded Ruler Construction. Hence, by Theorem 21, the dots in $\mathcal{S}$ form a DDC and so the theorem follows. □

The following slightly different construction also produces doubly periodic Golomb rectangles.

The Chinese Remainder Theorem Construction: Let n be a positive integer and let $D = \{a_1, a_2, \ldots, a_m\}$ be a B_2-sequence in $\mathbb{Z}_n$. Let $n = \ell \cdot k$ be any factorization of n such that $\gcd(\ell, k) = 1$. For any two integers i and j we place a dot in $\mathcal{A}(i,j)$, if and only if $a_t = (i \cdot \ell + j \cdot k) \bmod n$ for some t.

Theorem 25: Let $\mathcal{A}$ be the array constructed by the Chinese Remainder Theorem construction. Then $\mathcal{A}$ is a doubly periodic $\ell \times k$ DDC of period (k, ℓ) and density m/n. Moreover, every $\ell \times k$ subarray of $\mathcal{A}$ contains exactly m dots.

Proof: Let $f(x,y) = x \cdot \ell + y \cdot k$. For any two integers α and β we have $f(i,j) \equiv f(i + \alpha k, j + \beta\ell) \equiv i \cdot \ell + j \cdot k \bmod n$. So the definition of $\mathcal{A}$ implies that $\mathcal{A}$ is doubly periodic with period (k, ℓ).

Since ℓ and k are relatively primes, it follows (from the Chinese Remainder Theorem) that each integer s in the range $0 \leq s \leq \ell \cdot k - 1$, has a unique representation as $s = d \cdot \ell + e \cdot k$, where $0 \leq d \leq k-1, 0 \leq e \leq \ell-1$. Hence every $\ell \times k$ subarray of $\mathcal{A}$ has m dots corresponding to the m elements of the B_2-sequence D. In particular, this implies that $\mathcal{A}$ has density m/n.

Assume for a contradiction that there exists an $\ell \times k$ subarray $\mathcal{S}$ of $\mathcal{A}$ that is not a DDC. Suppose that the lower left-hand corner of $\mathcal{S}$ is at $\mathcal{A}(i,j)$. The distribution of dots in $\mathcal{S}$ is the same as the distribution in the subarray with lower left-hand corner the origin once we replace D by the shift $(i\ell + j\ell) + D$. So, without loss of generality, we may assume that the lower left-hand corner of $\mathcal{S}$ lies at the origin. As the distinct difference property fails to be satisfied, there are four positions with dots in $\mathcal{A}$ of the form:

$$\begin{array}{ll} \mathcal{A}(i_1, j_1) & \mathcal{A}(i_1 + d, j_1 + e) \\ \mathcal{A}(i_2, j_2) & \mathcal{A}(i_2 + d, j_2 + e) \end{array}$$

where $i_1, i_1 + d, i_2, i_2 + d \in \{0, 1, \ldots, k-1\}$ and $j_1, j_1 + e, j_2, j_2 + e \in \{0, 1, \ldots, \ell - 1\}$. By the definition of $\mathcal{A}$ we have

$$(i_1 + d)\ell + (j_1 + e)k - (i_1\ell + j_1 k) = d \cdot \ell + e \cdot k$$
$$(i_2 + d)\ell + (j_2 + e)k - (i_2\ell + j_2 k) = d \cdot \ell + e \cdot k$$

Since by Lemma 22 each nonzero residue s modulo n has at most one representation as a difference from two elements of D, it follows that the pairs

$$\{\mathcal{A}(i_1, j_1), \mathcal{A}(i_1 + d, j_1 + e)\}$$
$$\{\mathcal{A}(i_2, j_2), \mathcal{A}(i_2 + d, j_2 + e)\}$$

are identical, and the theorem follows. □

VI. Lower Bounds

A. Manhattan Distance

In this section we will prove that there exists a $\overline{\mathrm{DD}}(m, r)$ with $\frac{r}{\sqrt{2}} - o(r)$ dots: this attains asymptotically the upper bound of Theorem 9. We will see that this construction is actually using folding in a slightly different way. We further show that we can construct a doubly periodic array in which each Lee sphere of diameter r is a DDC with $\frac{r}{\sqrt{2}} + o(r)$ dots.

The LeeDD Construction: Let r be an integer, and define $R = \lfloor \frac{r}{2} \rfloor$. Let $D = \{a_1, a_2, \ldots, a_\mu\}$ be a ruler of length n. Define $f(i,j) = iR + j(R+1) + R^2 + R$. Let $\mathcal{A}$ be the Lee sphere of radius R centered at $(0,0)$, so $\mathcal{A}$ has the entry $\mathcal{A}(i,j)$ if $|i| + |j| \leq R$. We place a dot in $\mathcal{A}(i,j)$ if and only if $f(i,j) \in D$.

Theorem 26: The Lee sphere $\mathcal{A}$ of the LeeDD Construction is a $\overline{\mathrm{DD}}(m, r)$, where $m = |D \cap \{0, 1, \ldots, 2R^2 + 2R\}|$.

Proof: We first note that if $|i| + |j| \leq R$ then the smallest value that the function f takes is 0 and the largest value is $2R^2 + 2R$. Next, we claim that if (i_1, j_1) and (i_2, j_2) are two distinct points such that $|i_1| + |j_1| \leq |i_2| + |j_2| \leq R$ then $f(i_1, j_1) \neq f(i_2, j_2)$. Assume the contrary, that $f(i_1, j_1) = f(i_2, j_2)$. So $i_1 R + j_1(R+1) + R^2 + R = i_2 R + j_2(R+1) + R^2 + R$ and, therefore, $(i_2 - i_1)R = (j_1 - j_2)(R+1)$. If $i_1 = i_2$, then $j_1 = j_2$ which contradicts our assumption that (i_1, j_1) and (i_2, j_2) are distinct. So we may assume that $i_1 \neq i_2$. Similarly, we may assume that $j_1 \neq j_2$. The equality $(i_2 - i_1)R = (j_1 - j_2)(R+1)$ now implies that $R+1$ divides $|i_2 - i_1|$ and R divides $|j_2 - j_1|$. This implies that $|i_2 - i_1| + |j_2 - j_1| > 2R$, but

$$|i_2 - i_1| + |j_2 - j_1| \leq |i_1| + |j_1| + |i_2| + |j_2| \leq 2R$$

and so we have a contradiction. Thus, $f(i_1, j_1) \neq f(i_2, j_2)$. This implies that each one of the integers between 0 and $2R^2 + 2R$ is the image of exactly one pair (i,j). In particular, the number m of dots in the configuration is exactly $|D \cap \{0, 1, \ldots, 2R^2 + 2R\}|$.

Since $\mathcal{A}$ is a Lee sphere of radius R, it follows that the Manhattan distance between any two points is at most $2R \leq r$. Now, assume for a contradiction that $\mathcal{A}$ is not a $\overline{\mathrm{DD}}(m, r)$, so there exist four positions with dots in $\mathcal{A}$ as follows:

$$\begin{array}{ll} \mathcal{A}(i_1, j_1) & \mathcal{A}(i_1 + d, j_1 + e) \\ \mathcal{A}(i_2, j_2) & \mathcal{A}(i_2 + d, j_2 + e) \end{array}$$

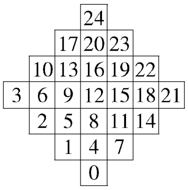

Fig. 7. Folding along diagonals.

By definition, we have that

$$f(i_1, j_1), f(i_1 + d, j_1 + e), f(i_2, j_2), f(i_2 + d, j_2 + e) \in D.$$

But then $f(i_1 + d, j_1 + e) - f(i_1, j_1) = f(i_1 + d, j_1 + e) - f(i_1, j_1) = dR + e(R + 1)$, contradicting the fact that D is a ruler.

Thus, the Lee sphere $\mathcal{A}$ of the LeeDD Construction is a $\overline{\mathrm{DD}}(m, r)$. □

Corollary 27: There exists a $\overline{\mathrm{DD}}(m, r)$ in which $m = \frac{r}{\sqrt{2}} - o(r)$.

Proof: Define $R = \lfloor r/2 \rfloor$ and let $n = 2R^2 + 2R + 1$. There exists a ruler of length at most n containing m dots, where $m \geq \sqrt{n} + o(\sqrt{n})$: see [4], [5], and [7]. Let $D \subseteq \{0, 1, \ldots, n-1\}$ be such a ruler. The corollary now follows, by Theorem 26. □

It is worth mentioning that the LeeDD Construction is actually a folding of the ruler by the diagonals of the Lee sphere. Fig. 7 illustrates why this is the case, by labelling the positions in a Lee sphere of radius 3 by the values of $f(i, j)$ at these positions. So if we use a B_2-sequence over $\mathbb{Z}_n$ instead of a ruler in the LeeDD Construction we obtain a doubly periodic array with nice properties:

The Doubly Periodic LeeDD Construction: Let r be an integer, $R = \lfloor \frac{r}{2} \rfloor$, and let $D = \{a_1, a_2, \ldots, a_\mu\}$ be a B_2-sequence over $\mathbb{Z}_n$, where $n \geq 2R^2 + 2R + 1$. Let $f(i, j) \equiv iR + j(R+1) \bmod n$. Let $\mathcal{A}$ be the square grid. For each two integers i and j, there is a dot in $\mathcal{A}(i, j)$ if and only if $f(i, j) \in D$.

Similarly to Theorem 26 we can prove the following result.

Theorem 28: The array $\mathcal{A}$ constructed in the LeeDD Construction is doubly periodic with period (n, n) and density μ/n. The dots contained in any Lee sphere of radius R form a DDC.

Proof: The first statement of the theorem is obvious. The second statement follows as in the proof of Theorem 26, once we observe that f is an injection when restricted to any Lee sphere of radius R. □

In Sections VI-D and VI-E we will make use of an extension of this construction. For positive integers R and t, an (R, t)-*diagonally extended Lee sphere* is a set of positions in the square grid defined as follows. Let $(i_0, j_0) \in \mathbb{Z}^2$, and define $C = \{(i_0 + k, j_0 + k) : 0 \leq k \leq t - 1\}$. Then an (R, t)-diagonally extended Lee sphere is the union of the Lee spheres of radius R with centers lying in C. (See Fig. 8, for an example.) An (R, t)-diagonally extended Lee sphere contains exactly $2R^2 + t(2R + 1)$ positions; the Lee sphere of radius R is the special case when $t = 1$.

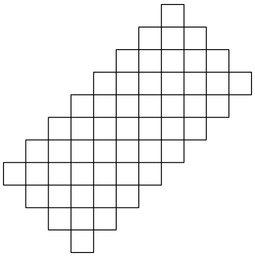

Fig. 8. A (3,5)-diagonally extended Lee sphere.

We observe that by choosing $n \geq 2R^2 + t(2R + 1)$, we can generalize the doubly periodic LeeDD construction by continuing folding along the diagonals of the rectangle. This yields the following corollary, which will prove useful in the construction of configurations for the hexagonal grid.

Corollary 29: Let a be positive, and let n be an integer such that $n \geq (2 + 2a)R^2 + aR$. Consider the array $\mathcal{A}$ constructed using the doubly periodic LeeDD Construction. Then $\mathcal{A}$ is a doubly periodic array with density μ/n. The dots contained in any $(R, \lfloor aR \rfloor)$-diagonally extended Lee sphere form a DDC. There exists a family of B_2 sequences so that $\mathcal{A}$ has density at least $1/\sqrt{(2 + 2a)R^2 + o(R^2)}$.

Proof: To establish the final statement of the corollary, we choose a family of B_2 sequences as follows. Let p be the smallest prime such that $p^2 - 1 \geq (2 + 2a)R^2 + aR$, and define $n = p^2 - 1$. By Ingham's classical result [44] on the gaps between primes, we have that $n \leq (2 + 2a)R^2 + O(R^{13/8}) = (2 + 2a)R^2 + o(R^2)$. By Theorem 23, there exists a B_2 sequence over $\mathbb{Z}_n$ with $\mu = p$. Hence, the density of $\mathcal{A}$ is

$$\mu/n = p/(p^2 - 1) \geq 1/\sqrt{(2 + 2a)R^2 + o(R^2)}$$

as required. □

B. A General Technique

Let $\mathcal{S}$ be a shape (a set of positions) in the square grid. We are interested in finding large DDCs contained in $\mathcal{S}$, where (for example) $\mathcal{S}$ is an anticode. This subsection presents a general technique for showing the existence of such DDCs, using the doubly periodic constructions from Section V.

We write $(i, j) + \mathcal{S}$ for the shifted copy $\{(i + i', j + j') : (i', j') \in \mathcal{S}\}$ of $\mathcal{S}$. Let $\mathcal{A}$ be a doubly periodic array. We say that $\mathcal{A}$ is a *doubly periodic* $\mathcal{S}$-DDC if the dots contained in every shift $(i, j) + \mathcal{S}$ of $\mathcal{S}$ form a DDC. So the doubly periodic arrays constructed in Section V are all doubly periodic $\mathcal{S}$-DDCs where $\mathcal{S}$ is a square or a rectangle; the arrays in Theorem 28 and Corollary 29 are doubly periodic $\mathcal{S}$-DDCs with $\mathcal{S}$ a Lee sphere and diagonally extended Lee sphere, respectively. The following lemma follows in a straightforward way from our definitions:

Lemma 30: Let $\mathcal{A}$ be a doubly periodic $\mathcal{S}$-DDC, and let $\mathcal{S}' \subseteq \mathcal{S}$. Then $\mathcal{A}$ is a doubly periodic $\mathcal{S}'$-DDC.

We will use doubly periodic DDCs to prove the existence of the configurations we are most interested in, using the following theorem.

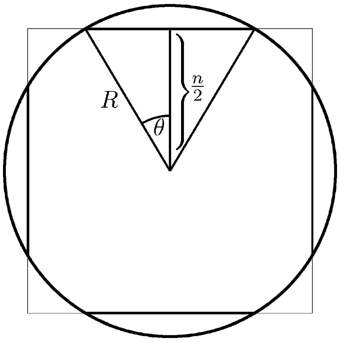

Fig. 9. Square intersecting a circle.

Theorem 31: Let $\mathcal{S}$ be a shape, and let $\mathcal{A}$ be a doubly periodic $\mathcal{S}$-DDC of density δ. Then there exists a set of at least $\lceil\delta|\mathcal{S}|\rceil$ dots contained in $\mathcal{S}$ that form a DDC.

Proof: Let the period of $\mathcal{A}$ be (η,κ). Write $m_{i,j}$ for the number of dots of $\mathcal{A}$ contained in the shift $(i,j)+\mathcal{S}$ of $\mathcal{S}$. Now $\mathcal{A}$ is periodic, so the definition of the density of $\mathcal{A}$ shows that

$$\sum_{i=1}^{\eta}\sum_{j=1}^{\kappa} m_{i,j} = (\eta\kappa)\delta|\mathcal{S}|.$$

Hence, the average size of the integer $m_{i,j}$ is $\delta|\mathcal{S}|$, so there exists an integer $m_{i',j'}$ such that $m_{i',j'} \geq \lceil\delta|\mathcal{S}|\rceil$. The $m_{i',j'}$ dots in $(i',j')+\mathcal{S}$ form a DDC, by our assumption on $\mathcal{A}$, and so the appropriate shift of these dots provides a DDC in $\mathcal{S}$ with at least $\lceil\delta|\mathcal{S}|\rceil$ dots, as required. □

C. Euclidean Distance in the Square Model

This subsection illustrates our general technique in the square grid using Euclidean distance. So we wish to construct a $\mathrm{DD}(m,r)$ with m as large as possible.

Let $R=\lfloor r/2\rceil$, and let $\mathcal{S}$ be the set of points in the square grid that are contained in the Euclidean circle of radius R about the origin. We construct a DDC contained in $\mathcal{S}$ with many dots: any such configuration is clearly a $\mathrm{DD}(m,r)$ for some value of m. The most straightforward approach is to find a large square contained in $\mathcal{S}$ (which will have sides of length approximately $\sqrt{2}R$), and then add dots within this square using a Costas array. This will produce a $\mathrm{DD}(m,r)$ where

$$m=\sqrt{2}R-o(R)=\frac{1}{\sqrt{2}}r-o(r)\approx 0.707r.$$

To motivate our better construction, we proceed as follows. We find a square of side n where $n>\sqrt{2}R$ that partially overlaps our circle: see Fig. 9. The constructions of Section V show that there exist doubly periodic $n\times n$ DDCs that have density approximately $1/n$. So Theorem 31 shows that for any shape $\mathcal{S}'$ within the square, there exist DDCs in $\mathcal{S}'$ that have at least $|\mathcal{S}'|/n$ dots. Let $\mathcal{S}'$ be the intersection of our square with $\mathcal{S}$. Defining θ as in the diagram, some basic geometry shows that the area of $\mathcal{S}'$ is

$$|\mathcal{S}'|=\frac{(\pi/2)-2\theta+\sin 2\theta}{2\cos^2\theta}|\mathcal{S}|=2R^2((\pi/2)-2\theta+\sin 2\theta).$$

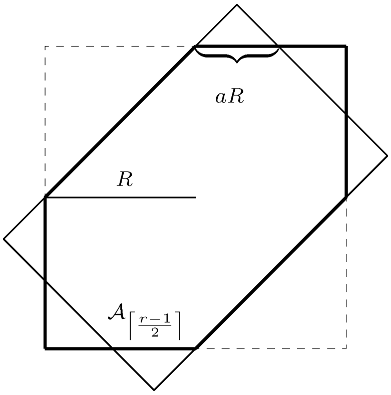

Fig. 10. A diagonal rectangle intersecting the image of a hexagonal sphere.

Since $n=2R\cos\theta$, Theorem 31 shows that the density of dots within $\mathcal{S}'$ can be about $1/n=1/(2R\cos\theta)$ when n is large. So we can hope for at least μR dots, where μ is the maximum value of

$$((\pi/2)-2\theta+\sin 2\theta)/\cos\theta$$

on the interval $0\leq\theta\leq\pi/4$. In fact $\mu\approx 1.61589$, achieved when $\theta\approx 0.41586$ (and so when $n=r\cos\theta=cr$, where $c\approx 0.914769$).

Theorem 32: Let μ be defined as above. There exists a $\mathrm{DD}(m,r)$ in which $m=(\mu/2)r-o(r)\approx 0.80795r$. Note that Theorem 15 gives an upper bound on m of the form $m\leq(\sqrt{\pi}/2)r+o(r)\approx 0.88623r$.

Proof: Define $c\approx 0.91477$ as above. Let q be the smallest prime power such that $q>cr$. We have that $cr<q<cr+(cr)^{5/8}$, by a classical result of Ingham [44] on the gaps between primes; so in particular $q\sim cr$. By Theorem 20, there exists a doubly periodic $(q-1)\times(q-1)$ DDC $\mathcal{A}$ of density $(q-2)/(q-1)^2$. Let $\mathcal{S}'$ be the intersection between $\mathcal{S}$ and a Euclidean circle of radius $\lfloor r/2\rfloor$ about the origin. Then $\mathcal{A}$ is a doubly periodic $\mathcal{S}'$-DDC. By Theorem 31, there exists a DDC in $\mathcal{S}'$ with at least m dots, where $|\mathcal{S}'|(q-2)/(q-1)^2$. But the geometric argument above shows that $|\mathcal{S}'|(q-2)/(q-1)^2\sim(\mu/2)r$, and so the theorem follows. □

D. Hexagonal Distance

By representing the hexagonal anticodes in the square grid, we may use Theorem 31 to show the existence of a $\overline{\mathrm{DD}}^*(m,r)$ where m is large. The method of producing lower bounds is essentially the same as above, but the geometrical problem we are solving is different, with the images under ξ of the maximal anticodes $\mathcal{A}_i$ replacing the circle, and the DDC contained a diagonally extended Lee sphere of Corollary 29 replacing the Costas array contained in a square. Here we consider the case of configurations contained in the hexagonal sphere $\mathcal{A}_{\lceil(r-1)/2\rceil}$; the cases of the other anticodes may be handled in a similar fashion. The problem we are solving is pictured in Fig. 10. The figure shows the image under ξ of the hexagonal sphere of radius $R=\lfloor r/2\rfloor$ in bold; the square of side $2R+1$ containing this image is also shown. The hexagonal sphere contains a Lee

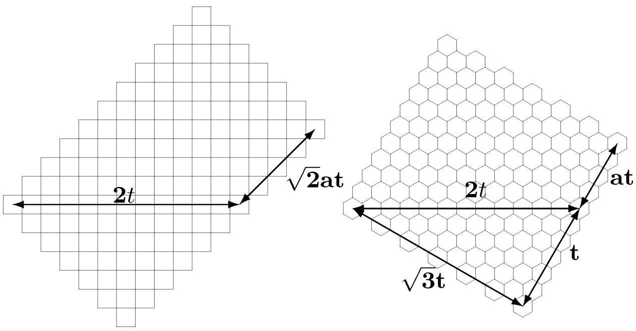

Fig. 11. A $(t, \lfloor at \rfloor)$-diagonally extended Lee sphere is transformed into a rotated square (when $at = (\sqrt{3} - 1)t + 1$).

sphere of radius R with the same center; the region $\mathcal{S}$ we consider is the $(R, \lfloor aR \rfloor)$-diagonally extended Lee sphere whose midpoint is at the center of the hexagonal sphere: see Fig. 10. Let $\mathcal{S}'$ be the intersection of $\mathcal{S}$ with the image of the hexagonal sphere. We have that $|\mathcal{S}'| = R^2(2 + 2a - a^2) + o(R^2)$. By Corollary 29, there is a doubly periodic $\mathcal{S}$-DDC of density at least $1/\sqrt{n}$ where $n = 2R^2(1 + a) + o(R^2)$. Thus Theorem 31 shows that there is a DDC contained in $\mathcal{S}'$ containing $\mu R - o(R)$ dots, where μ is the maximum of

$$\frac{2 + 2a - a^2}{\sqrt{2}\sqrt{1 + a}}.$$

It can be seen that $\mu = (\frac{2}{3})^{\frac{3}{2}} \frac{1+2\sqrt{7}}{\sqrt{2+\sqrt{7}}} \approx 1.58887$, achieved when $a = \frac{-1+\sqrt{7}}{3}$. Since $\mathcal{S}'$ is contained in a hexagonal sphere of radius R, all pairs of dots in our DDC are at hexagonal distance at most r. Thus we have the following theorem:

Theorem 33: Let μ be defined as above. There exists a $\overline{\mathrm{DD}}^*(m, r)$ in which $m = (\mu/2)r - o(r) \approx 0.79444r$.

E. Euclidean Distance in the Hexagonal Model

In this subsection we will obtain a construction for a $\mathrm{DD}^*(m, r)$ contained within a circle of radius $R = \lfloor r/2 \rfloor$, again based on the doubly periodic LeeDD construction. We first observe that a diagonally extended Lee sphere in the square grid is transformed by ξ^{-1} into a (rotated) rectangle in the hexagonal grid. In particular, a $(t, \lfloor (\sqrt{3} - 1)t + 1 \rfloor)$-diagonally extended Lee sphere is transformed by ξ^{-1} into a set of hexagons whose centers all lie within a (rotated) square $\mathcal{S}$ of side $\sqrt{3}\,t$ (see Fig. 11). Corollary 29 shows that there is a doubly periodic $\mathcal{S}$-DDC with density $1/\sqrt{n}$, where $n = 2\sqrt{3}t^2 + o(t^2)$.

Consider (see Fig. 12) a circle of radius R and a square $\mathcal{S}$ of side s where $s = 2R\cos\theta$. Since a hexagon has area $\sqrt{3}/2$, the square $\mathcal{S}$ contains $(8/\sqrt{3})R^2\cos^2\theta + O(R)$ hexagons. Let $\mathcal{S}'$ be the intersection of $\mathcal{S}$ with the circle of radius R. The calculations in Section VI-C show that

$$|\mathcal{S}'| = \frac{(\pi/2 - 2\theta + \sin 2\theta)}{2\cos^2\theta}|\mathcal{S}| + O(R).$$

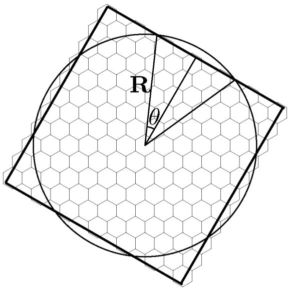

Fig. 12. Rotated square intersecting a circle.

TABLE I
UPPER AND LOWER BOUNDS ON THE NUMBER OF DOTS IN A DISTINCT DIFFERENCE CONFIGURATION

	lower bound	upper bound
$\overline{\mathrm{DD}}(m, r)$	$(1/\sqrt{2})r - o(r)$	$(1/\sqrt{2})r + O(r^{2/3})$
$\mathrm{DD(m, r)}$	$0.80795r - o(r)$	$0.88623r + O(r^{2/3})$
$\overline{\mathrm{DD}}^*(m, r)$	$0.79444r - o(r)$	$0.86603r + O(r^{2/3})$
$\mathrm{DD}^*\mathrm{(m, r)}$	$0.86819r - o(r)$	$0.95231r + O(r^{2/3})$

The previous paragraph shows that there is an periodic $\mathcal{S}'$-DCC of density $\delta = 1/\sqrt{n}$, where $n = (2/\sqrt{3})s^2 + o(s^2)$. So Theorem 31 now implies that there exists a distinct difference configuration in $\mathcal{S}'$ containing at least m dots, where

$$m = \frac{\sqrt{\frac{2}{\sqrt{3}}}(\pi/2 - 2\theta + \sin 2\theta)}{\cos\theta} R - o(R).$$

As in Section VI-C, we may take $\theta \approx 0.41586$ to maximize this expression. Hence, we have proved the following theorem:

Theorem 34: Let $\mu \approx 1.61589$ be the constant defined above Theorem 32. There exists a $\mathrm{DD}^*(m, r)$ in which the number of dots is at least $\sqrt{\frac{2}{\sqrt{3}}}\mu R - o(R) \approx 0.86819r$.

VII. CONCLUSION

We introduced the concept of a distinct difference configuration and gave specific examples for both the square and hexagonal grids for small parameters. We went on to provide general constructions for such configurations, as well as upper and lower bounds on the maximum number of dots such configurations may contain. In the case of distinct difference configurations using Manhattan distance these bounds are tight asymptotically, as we have provided a construction for configurations which meets the leading term in our upper bound. For the remaining classes of configurations, there is a gap between the upper and lower bounds we have provided (see Table I). We believe the upper bounds to be realistic, and it is an interesting challenge to provide constructions that meet these bounds.

REFERENCES

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

[2] S. W. Golomb, "How to number a graph," in *Graph Theory and Computing*. New York: Academic, 1972, pp. 23–37.

[3] J. B. Shearer, Golomb Rulers [Online]. Available: http://www.research.ibm.com/people/s/shearer/grule.html

[4] 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.

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

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

[7] J. P. Robinson and A. J. Bernstein, "A class of binary recurrent codes with limited error propagation," *IEEE Trans. Inf. Theory*, vol. IT-13, pp. 106–113, 1967.

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

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

[10] J. P. Robinson, "Genetic search for Golomb arrays," *IEEE Trans. Inf. Theory*, vol. IT-46, pp. 1170–1173, 2000.

[11] J. P. Costas, "Medium constraints on sonar design and performance," *EASCON Conv. Rec.*, pp. 68A–68I, 1975.

[12] R. Gagliardi, J. Robbins, and H. Taylor, "Acquisition sequences in PPM communications," *IEEE Trans. Inf. Theory*, vol. IT-33, pp. 738–744, Sep. 1987.

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

[14] O. Moreno, R. A. Games, and H. Taylor, "Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols," *IEEE Trans. Inf. Theory*, vol. IT-39, pp. 1985–1987, Sep. 1993.

[15] 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.

[16] J. Hamkins and K. Zeger, "Improved bounds on maximum size binary radar arrays," *IEEE Trans. Inf. Theory*, vol. IT-43, pp. 997–1000, May 1997.

[17] Z. Zhang and C. Tu, "New bounds for the sizes of radar arrays," *IEEE Trans. Inf. Theory*, vol. IT-40, pp. 1672–1678, Sep. 1994.

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

[19] R. E. Peile and H. Taylor, "Sets of points with pairwise distinct slopes," *Comput. Math.*, vol. 39, pp. 109–115, 2000.

[20] Z. Zhang, "A note on arrays of dots with distinct slopes," *Combinatorica*, vol. 13, pp. 127–128, 1993.

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

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

[23] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, Distinct Difference Configurations: Multihop Paths and Key Predistribution in Sensor Networks preprint.

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

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

[26] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Designs, Codes Crypto.*, vol. 22, pp. 221–237, 2001.

[27] R. Ahlswede and L. H. Khachatrian, "The complete nontrivial-intersection theorem for systems of finite sets," *J. Combin. Theory, Series A*, vol. 76, pp. 121–138, 1996.

[28] R. Ahlswede and L. H. Khachatrian, "The diametric theorem in Hamming spaces-optimal anticodes," *Adv. Appl. Math.*, vol. 20, pp. 429–449, 1998.

[29] P. Delsarte, "An algebraic approach to association schemes of coding theory," *Philips J. Res.*, vol. 10, pp. 1–97, 1973.

[30] T. Etzion, M. Schwartz, and A. Vardy, "Optimal tristance anticodes in certain graphs," *J. Combin. Theory, Series A*, vol. 113, pp. 189–224, 2006.

[31] W. J. Martin and X. J. Zhu, "Anticodes for the Grassman and bilinear forms graphs," *Designs, Codes, Crypt.*, vol. 6, pp. 73–79, 1995.

[32] M. Schwartz and T. Etzion, "Codes and anticodes in the Grassman graph," *J. Combin. Theory, Series A*, vol. 97, pp. 27–42, 2002.

[33] S. W. Golomb and L. R. Welch, "Perfect codes in the Lee metric and the packing of polyominos," *SIAM J. Appl. Math.*, vol. 18, pp. 302–317, 1970.

[34] 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.

[35] T. Etzion, "Tilings with generalized Lee spheres," in *Mathematical Properties of Sequences and Other Combinatorial Structures*, J. S. No, H. Y. Song, T. Helleseth, and P. V. Kumar, Eds. Boston, MA: Kluwer Academic, 2003, pp. 181–198.

[36] J. E. Littlewood*, Littlewood's Miscellany*, B. Bollobás, Ed. Cambridge, U.K.: Cambridge Univ. Press, 1986.

[37] P. Erdős 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.

[38] T. Etzion, "Combinatorial designs derived from Costas arrays," in *Sequences*, R. M. Capocelli, Ed. New York: Springer Verlag, 1989, pp. 208–227.

[39] H. Taylor, Non-Attacking Rooks With Distinct Differences Commun. Sci. Inst., Univ. Southern Calif., Tech. Rep. CSI-84-03-02, Mar. 1984.

[40] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Combin. Theory, Series A*, vol. 37, pp. 13–21, 1984.

[41] S. W. Golomb, "The T_4 and G_4 constructions for Costas arrays," *IEEE Trans. Inf. Theory*, vol. IT-38, pp. 1404–1406, 1992.

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

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

[44] A. E. Ingham, "On the difference between consecutive primes," *Quart. J. Math. Oxford (O.S.)*, vol. 8, pp. 255–266, 1937.

Simon R. Blackburn received the B.Sc. degree in mathematics from the University of Bristol, U.K., in 1989, and the D.Phil. degree in mathematics from the University of Oxford, U.K., in 1992.

Since then, he has been with Royal Holloway, University of London, U.K., as a Research Assistant (1992–1995), an Advanced Fellow (1995–2000), a Reader in Mathematics (2000–2003), and a Professor in Pure Mathematics (2004-present). He was Head of the Mathematics Department from 2004 to 2007. His research interests include cryptography, group theory, and combinatorics with applications to computer science.

Tuvi Etzion (M'89-SM'99-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, in 1980, 1982, and 1984, respectively.

Since 1984, he held a position with the Department of Computer Science, Technion, where he is a Professor. During 1986–1987, he was a Visiting Research Professor with the Department of Electrical Engineering—Systems at the University of Southern California, Los Angeles. During the summers of 1990 and 1991, he was visiting Bellcore in Morristown, NJ. During 1994–1996, he was a Visiting Research Fellow with the Computer Science Department, Royal Holloway, University of London. He also had several visits to the Coordinated Science Laboratory, University of Illinois in Urbana-Champaign, during 1995–1998, two visits to HP Bristol during the summers of 1996 and 2000, several visits to the Department of Electrical Engineering, University of California at San Diego, during 2000–2009, and with the Mathematics Department, Royal Holloway, University of London, 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 until 2009.

Keith M. Martin received the B.Sc. (Hons.) degree in mathematics from the University of Glasgow, Scotland, in 1988 and the Ph.D. degree from Royal Holloway in 1991.

He joined the Information Security Group of Royal Holloway, University of London, U.K., as a lecturer in January 2000. Between 1992 and 1996, he held a Research Fellowship with the Department of Pure Mathematics, University of Adelaide, investigating mathematical modeling of cryptographic key distribution problems. In 1996, he joined the COSIC Research Group, Katholieke Universiteit Leuven, Belgium, where he was primarily involved in an EU ACTS project concerning security for third-generation mobile communications. He has also held visiting positions at the University of Wollongong, University of Adelaide, and Macquarie University. His current research interests include cryptography, key management, and wireless sensor network security.

Prof. Martin is an Associate Editor for Complexity and Cryptography for the IEEE TRANSACTIONS ON INFORMATION THEORY.

Maura B. Paterson received the B.Sc. degree from the University of Adelaide in 2002 and the Ph.D. degree from Royal Holloway, University of London, U.K., in 2005.

She has worked as a Research Assistant in the Information Security Group, Royal Holloway. She is currently with the Department of Economics, Mathematics and Statistics at Birkbeck, University of London. Her research interests include applications of combinatorics in information security.