Distinct difference configurations: multihop paths and key predistribution in sensor networks

Journal Article

Blackburn, S.R.; Etzion, T.; Martin, K.M.; Paterson, M. (2010) Distinct difference configurations: multihop paths and key predistribution in sensor networks – *IEEE Transactions on Information Theory* 56(8), pp. 3961-3972

Distinct Difference Configurations: Multihop Paths and Key Predistribution in Sensor Networks

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

***Abstract*—A distinct difference configuration is a set of points in $\mathbb{Z}^2$ with the property that the vectors (*difference vectors*) connecting any two of the points are all distinct. Many specific examples of these configurations have been previously studied: the class of distinct difference configurations includes both Costas arrays and sonar sequences, for example.**

Motivated by an application of these structures in key predistribution for wireless sensor networks, we define the k-hop coverage of a distinct difference configuration to be the number of distinct vectors that can be expressed as the sum of k or fewer difference vectors. This is an important parameter when distinct difference configurations are used in the wireless sensor application, as this parameter describes the density of nodes that can be reached by a short secure path in the network. We provide upper and lower bounds for the k-hop coverage of a distinct difference configuration with m points, and exploit a connection with B_h sequences to construct configurations with maximal k-hop coverage. We also construct distinct difference configurations that enable all small vectors to be expressed as the sum of two of the difference vectors of the configuration, an important task for local secure connectivity in the application.

***Index Terms*—Data Security, Key Predistribution, Wireless Sensor Networks**

I. Introduction

A *distinct difference configuration* $\mathrm{DD}(m)$ is a set of m dots in a square grid, with the property that the lines joining distinct pairs of dots are all different in length or slope. For instance, the dots depicted in the following array form a $\mathrm{DD}(3)$:

If we pick a position on the square grid to be the origin, we may think of the dots in a $\mathrm{DD}(m)$ as a set $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ of vectors in $\mathbb{Z}^2$. The condition that the dots form a $\mathrm{DD}(m)$ is then the same as the condition that the *difference vectors* $\mathbf{v}_i - \mathbf{v}_j$ with $i \neq j$ are all distinct. So we may think of the dots in the example above as the set $\{(0,0),(1,2),(2,1)\}$ of vectors; it is easy to verify that the six difference vectors are all different in this case.

Many special classes of distinct difference configurations have been studied previously: these include B_2 sequences over $\mathbb{Z}$ and Golomb rulers in the one-dimensional case, and Costas arrays, Golomb rectangles and sonar sequences in the two-dimensional case. See [1] for a summary of these configurations.

This work was supported in part by EPSRC grants EP/D053285/1 and EP/F056486/1, and Israel Science Foundation grant 230/08.

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. T. Etzion is with the Computer Science Department, Technion–Israel Institute of Technology, Haifa 32000, Israel.

This paper is concerned with the *k-hop properties* of distinct difference configurations. Before we explain this, we first need to discuss an application to key predistribution in grid-based wireless sensor networks due to Blackburn, Etzion, Martin and Paterson [2] that motivates our work.

A. Wireless Sensor Networks

A *wireless sensor network* is a large collection of small sensor nodes that are equipped with wireless communication capability. Sensor nodes have limited communication range and thus data transmitted over the network is typically passed from node to node in a series of *hops* in order to reach its end destination. Such networks can be employed for a wide range of applications [3], whether scientific, commercial, humanitarian or military. The data being transmitted over the wireless medium is frequently valuable or sensitive; hence, there is a need for cryptographic techniques to provide data integrity, confidentiality and authentication.

On deployment, the sensor nodes aim to form a secure and connected network. In other words, we desire a significant proportion of nodes within communication range to share cryptographic keys. The nodes' size limits their computational power and battery capacity, so it is assumed that the sensor nodes are unable to use public key cryptography to establish shared keys. So symmetric cryptographic keys are preloaded onto each node before deployment: methods for deciding which keys are assigned to a node are known as key predistribution schemes (see [4]–[6] for surveys of this subject). The sensor nodes are assumed to be highly vulnerable to compromise, so a single key should not be given to too many nodes. A balancing constraint is that each node can only store a limited number of keys. The aim is to design an efficient and secure key predistribution scheme so that a sensor node can establish secure wireless links with many of its neighbours: it is important to establish as many short secure links in the network as possible, since the nodes' capacity to relay information is very limited.

Key predistribution schemes for wireless sensor networks generally assume that the precise location of nodes is not known before deployment, hence schemes such as [7] aim to provide reasonable levels of "average" connectivity across the entire network. However in many applications the location of sensor nodes can be determined prior to deployment. In such cases this knowledge can be used to improve the efficiency of the underlying key predistribution scheme. One such scenario is that of networks consisting of a large number of sensor nodes arranged in a square grid. Grid-based networks can arise in many applications, including soil moisture sensing [8],

monitoring conditions in an orchard [9], and measuring the efficiency of water use during irrigation [10].

B. Key Predistribution for a Grid-based Network

In [2] a key predistribution scheme for a grid-based network was proposed and analysed. This scheme was shown to be significantly more efficient than using general approaches such as that of [7]. We now discuss this scheme in more detail.

Although the number of sensor nodes is evidently finite in practice, it is convenient to model the physical location of the nodes by the set of points of $\mathbb{Z}^2$. The scheme in [2] employs a distinct difference configuration to create a key predistribution scheme in the following way.

Scheme 1 *Let $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ be a distinct difference configuration. Allocate keys to nodes as follows:*

- *Label each node with its position in $\mathbb{Z}^2$.*
- *For every 'shift' $\mathbf{u} \in \mathbb{Z}^2$, generate a key $k_{\mathbf{u}}$ and assign $k_{\mathbf{u}}$ to the nodes labelled by $\mathbf{u} + \mathbf{v}_i$, for $i = 1, 2, \ldots, m$.*

More informally, we can think of the scheme as covering $\mathbb{Z}^2$ with all possible translations of the dots in D. We generate one key per translation, and assign that key to all dots in the corresponding translation of D. Distributing keys in this manner ensures that each node stores m keys and each key is shared by m nodes. In addition, the distinct difference property of the configuration implies that any pair of nodes shares at most one key, since the vector representing the difference in two nodes' positions can occur at most once as a difference vector of D. This leads to an efficient distribution of keys, since for a fixed number of stored keys the number of distinct pairs of nodes that share a key is maximised.

As an example, consider the distinct difference configuration given at the start of this introduction. If we use this configuration for key distribution in Scheme 1, each node stores three keys. Figure 1 illustrates this key distribution: each square in the grid represents a node, and each symbol contained in a square represents a key possessed by that node. The central square stores keys marked by the letters A, B and C; two further nodes share each of these keys, which are marked in bold. Letters in standard type represent keys used to connect the central node to one of its neighbours via a two-hop path, other keys are marked in grey. Note that we have only illustrated some of the keys; the pattern of key sharing extends in a similar manner throughout the entire network. See [2] for a comparison of how Scheme 1 outperforms related key predistribution schemes in the literature.

Note that the sensors' strictly limited battery power limits the range over which they can feasibly communicate. In support of Scheme 1, distinct difference configurations with bounds on the distance between any two dots in the configuration were considered in [2]. Supposing that each sensor has a fixed communication range r, a $\mathrm{DD}(m, r)$ is defined to be a $\mathrm{DD}(m)$ in which the Euclidean distance between any two points of the configuration is at most r. From an application point of view, it is only necessary for a pair of nodes to share a key if they are located within communication range of each other; the use of a $\mathrm{DD}(m, r)$ in Scheme 1 ensures that this is the case.

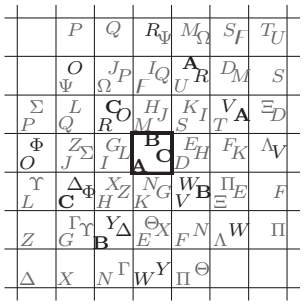

Fig. 1. Key distribution using a distinct difference configuration.

While Scheme 1 was designed to suit wireless sensor networks in which the sensors are arranged in a square grid, for certain applications a hexagonal arrangement of sensor nodes may be preferred, as it yields the most efficient packing of sensors (see [11] for details of circle packings in the plane). Section II defines the hexagonal model more precisely and discusses the relationship between the two models. Scheme 1 is easily adapted to suit sensors arranged in a hexagonal grid by replacing the $\mathrm{DD}(m)$ by a $\mathrm{DD}^*(m)$, which we informally define to be a set of m dots on a hexagonal grid such that the vector differences between pairs of dots are distinct. We define a $\mathrm{DD}^*(m, r)$ to be a $\mathrm{DD}^*(m)$ in which the Euclidean distance between any pair of dots is at most r. Another model that is natural when working with either the square or hexagonal grids is to replace the Euclidean metric by its discrete equivalent: the Manhattan metric (in the case of square grids), or an analogous metric on the hexagonal grid; in this case, we use the notation $\overline{\mathrm{DD}}(m, r)$ and $\overline{\mathrm{DD}}^*(m, r)$, respectively. Constructions and bounds on the parameters for such configurations were studied in [1]. Section II contains a summary of the relationships between configurations based on different grids when using different metrics.

C. Contributions

Recall that wireless sensor networks rely on data being relayed via intermediate nodes using a series of hops. From an efficiency perspective it is thus of interest to consider properties relating to the nodes that can be reached from a specific node by means of a restricted number of hops.

If two nodes A and B are within communication range and share a key we say there is a *one-hop path* between A and B. If they do not share a key, however, they may still be able to establish a secure connection if there is a node C that is within range of A and B and shares a key with each of them. This is referred to as a *two-hop path*; more generally we consider *k-hop paths* of the form $A - C_1 - C_2 \ldots - C_{k-1} - B$, where there is a one-hop path between any two adjacent users in the chain. A significant, and widely studied, measure of the performance of a key predistribution scheme for a wireless sensor network is the expected number of nodes with which a given node can communicate via a one hop or two-hop path (we do not count the given node in this total). As in [2], we refer to this parameter as the *two-hop coverage* of the scheme. More

generally, we can define the k-*hop coverage* to be the expected number of nodes with which a given node can communicate via some ℓ-hop path with $1 \leq \ell \leq k$ (where we do not count the given node itself).

This measure is important from the point of view of our application, since it captures the ability of the network to transmit information in the context of the nodes' limited capacity to relay messages. The case when $k = 2$ is the most studied situation in the literature, since results are often easier to establish than in the general k-hop case. Lee and Stinson use the notation $\mathbf{Pr}_1 + \mathbf{Pr}_2$ to describe this quantity, referring to it as the *local connectivity* [12]; similar metrics are used in [13], [14], and various related measures of the expected number of hops required for secure communication between two nodes are prevalent in the sensor network literature [7], [15], [16].

We define the k-hop coverage of a distinct difference configuration to be the k-hop coverage of the resulting instance of Scheme 1. In [2] a number of distinct difference configurations with good two-hop coverage were found by computer search. However no concrete construction techniques were provided. In this paper we provide an exposition of the two-hop coverage case, as well as consider the generalisation to k-hop coverage.

Section III is devoted to a study of the k-hop coverage $C_k(D)$ obtained by the use of the distinct difference configuration $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ in Scheme 1. Subsection III-A shows how to calculate the k-hop coverage from the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$. In Subsection III-B we study configurations where $C_k(D)$ is as large as possible, and show a connection between such configurations and B_h sequences (a well studied concept in combinatorial number theory). We determine the maximum value of the k-hop coverage $C_k(D)$ where D is a $\mathrm{DD}(m)$ (or a $\mathrm{DD}^*(m)$), and show that D achieves this level of k-hop coverage if and only if D is a B_{2k} sequence. If we restrict D to be a $\mathrm{DD}(m, r)$ for some small integer r, we might no longer be able to achieve this maximum value of $C_k(D)$: we provide bounds on the smallest value of r for which there exists a configuration D which is a $\mathrm{DD}(m, r)$ with $C_k(D)$ maximal. We also provide similar bounds on this smallest value of r when we consider configurations $\mathrm{DD}^*(m, r)$ in the hexagonal grid. Finally, in Subsection III-C, we provide a lower bound on $C_k(D)$ and characterise those configurations that meet this lower bound.

Using a distinct difference configuration with maximal k-hop coverage ensures that as many users as possible are connected by k-hop paths. However, in many applications these paths are used to establish keys which are later used for direct communication between the two end nodes: thus we are only interested in k-hop paths whose start and end nodes are within communication range. For these applications, rather than optimising the total number of pairs of users connected by k-hop paths we wish to optimise coverage in a locally defined region: We say that a $\mathrm{DD}(m)$ or $\mathrm{DD}^*(m)$ achieves *complete k-hop coverage with respect to a region R and point $\mathbf{p} \in R$* if every point in R can be reached by a two-hop path from $\mathbf{p}$. This means that every node $\mathbf{u}$ can communicate via a k-hop path with the nodes in the region corresponding to a shift of R that moves $\mathbf{p}$ to $\mathbf{u}$, giving Scheme 1 good local connectivity. In Section IV we give a construction for a $\mathrm{DD}(m)$ that achieves complete two-hop coverage with respect to the centre of a $(2p-3) \times (2p-1)$ rectangle when p is prime.

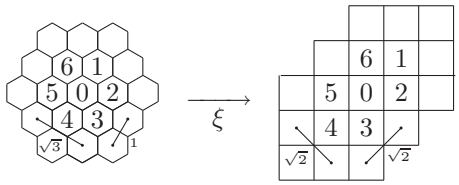

Fig. 2. A transformation from a hexagonal grid to a square grid (grid points are represented by the centres of the cells).

II. Different Grids and Different Metrics

A. Square and Hexagonal Grids

Suppose that the sensor nodes are arranged in a square grid, and the shortest distance between a pair of nodes is 1. So we tile the plane by unit squares, and think of the nodes as lying at the centres of these squares. By supposing one of the nodes is at the origin, the location of a node can be identified with a vector in $\mathbb{Z}^2$. Because of this, we call $\mathbb{Z}^2$ the *square grid*.

A hexagonal arrangement of sensor nodes is obtained by tiling the plane with regular hexagons and placing a node at the centre of each hexagon. We suppose that one of the nodes is located at the origin and the shortest distance between two nodes is 1. In a similar way to the square grid, the locations of the nodes can be represented by vectors in the set $\Lambda_H = \{\lambda(1,0) + \mu(-1/2, \sqrt{3}/2) | \lambda, \mu \in \mathbb{Z}\}$, which we call the *hexagonal grid*.

We have already defined a (square) distinct difference configuration $\mathrm{DD}(m)$ to be a set $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\} \subseteq \mathbb{Z}^2$ of m dots with the property that the difference vectors $\mathbf{v}_i - \mathbf{v}_j$ for $i \neq j$ between any pair of dots are distinct. In the same way, we define a (hexagonal) distinct difference configuration $\mathrm{DD}^*(m)$ to be a set $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\} \subseteq \Lambda_H$ of m dots in the hexagonal grid with the property that the difference vectors $\mathbf{v}_i - \mathbf{v}_j$ for $i \neq j$ are distinct. A hexagonal distinct difference configuration can be used in Scheme 1 for sensors arranged in a hexagonal grid, provided that shifts $\mathbf{u} \in \Lambda_H$ are used: as in the square grid, every node is assigned m keys and the distinct difference property implies that any pair of nodes has at most one key in common. We define a $\mathrm{DD}^*(m, r)$ to be a $\mathrm{DD}^*(m)$ in which the Euclidean distance between any pair of dots in the configuration is at most r: these configurations must be used when the wireless communication range of a sensor node is r.

The map $\xi \colon \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$\xi \colon (x, y) \mapsto (x + \frac{y}{\sqrt{3}}, \frac{2y}{\sqrt{3}})$$

induces a bijection from Λ_H to $\mathbb{Z}$. This is illustrated in Fig. 2, in which the cells whose centres form the points of the grid are depicted. We can use ξ and ξ^{-1} to convert a $\mathrm{DD}^*(m)$ into a $\mathrm{DD}(m)$ and *vice versa*:

(a) Lee sphere of radius 2 (b) Hexagonal ball of radius 1

Theorem 1. *If $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ is a $\mathrm{DD}^*(m)$, then $\xi(D) = \{\xi(\mathbf{v}_1), \xi(\mathbf{v}_2), \ldots, \xi(\mathbf{v}_m)\}$ is a $\mathrm{DD}(m)$. Similarly, if D' is a $\mathrm{DD}(m)$, then $\xi^{-1}(D')$ is a $\mathrm{DD}^*(m)$.*

Proof: Since ξ is a linear bijection, we have that $\mathbf{v}_i - \mathbf{v}_j = \mathbf{v}_k - \mathbf{v}_\ell$ if and only if $\xi(\mathbf{v}_i) - \xi(\mathbf{v}_j) = \xi(\mathbf{v}_k) - \xi(\mathbf{v}_\ell)$; the first statement of the theorem follows directly. The second statement follows as ξ^{-1} is also a linear bijection. ∎

Despite Theorem 1, the square and hexagonal models differ once we are interested in distances between dots, since ξ does not preserve Euclidean distances. Fig. 2 shows a line segment of length $\sqrt{3}$ that transforms into one of length $\sqrt{2}$, and one of length 1 that also transforms into one of length $\sqrt{2}$. It is straightforward to show that these line segments represent the maximum extent to which ξ can extend or contract the length of a vector; we formalise this in the following theorem:

Theorem 2. *If D is a $\mathrm{DD}^*(m, r)$ then $\xi(D)$ is a $\mathrm{DD}(m, r\sqrt{2})$. If D' is a $\mathrm{DD}(m, r)$, then $\xi^{-1}(D')$ is a $\mathrm{DD}^*(m, r\sqrt{3/2})$.*

Thus we can convert between results about $\mathrm{DD}(m, r)$ and results about $\mathrm{DD}^*(m, r)$ (although the bounds on the converted lengths are not tight in general).

B. Alternative Metrics on Grids

In [2], the need to take sensor nodes' communication range into account when using distinct difference configurations to distribute keys to sensors arranged in a square grid motivated the definition of a $\mathrm{DD}(m, r)$ based on a Euclidean measure of distance. However, when working with a square grid it is natural to consider the Manhattan metric (also known as the Lee metric), in which the distance between dots with coordinates (i_1, j_1) and (i_2, j_2) is given by $|i_1 - i_2| + |j_1 - j_2|$. Distinct difference configurations $\overline{\mathrm{DD}}(m, r)$ in which the distance between dots in the configuration is at most r in the Manhattan metric were studied in [1]. A ball of radius r in this metric is referred to as a *Lee sphere* (Fig. 3a), and for small r gives a reasonable approximation of a Euclidean circle. The well-known relation between these two metrics is expressed in the following theorem, which permits conversion between results about $\overline{\mathrm{DD}}(m, r)$ and results about $\mathrm{DD}(m, r)$.

Theorem 3. *For $r \in \mathbb{Z}$, a $\overline{\mathrm{DD}}(m, r)$ is a $\mathrm{DD}(m, r)$ and a $\mathrm{DD}(m, r)$ is a $\overline{\mathrm{DD}}(m, \lceil\sqrt{2}r\rceil)$.*

For the hexagonal grid, we say that a given point is *adjacent* to the six grid points that lie at Euclidean distance 1 from that point (for example, in Fig. 2 the points at the centres of cells $1, 2, \ldots, 6$ are adjacent to the point at the centre of cell 0). We can then define a graph in which the grid points correspond to vertices, with edges connecting vertices whose grid points are adjacent. This gives rise to a *hexagonal metric* in which the distance between two points is the length of the shortest path between the corresponding vertices in the graph. A distinct difference configuration in which the hexagonal distance between any two points is at most r is denoted $\overline{\mathrm{DD}}^*(m, r)$. The relation between the hexagonal and Euclidean metrics can be used to prove the following theorem:

Theorem 4. *For $r \in \mathbb{Z}$, a $\overline{\mathrm{DD}}^*(m, r)$ is a $\mathrm{DD}^*(m, r)$ and a $\mathrm{DD}^*(m, r)$ is a $\overline{\mathrm{DD}}^*(m, \lceil\frac{2}{\sqrt{3}}r\rceil)$.*

We note that the hexagonal metric gives a closer approximation to the Euclidean distance than the Manhattan metric.

III. k-Hop Coverage

In this section we investigate the properties of distinct difference configurations with respect to their k-hop coverage. While the motivation for this work comes from the application, the results are of independent combinatorial interest.

A. Characterising k-hop coverage

Let D be a (square or hexagonal) distinct difference configuration given by $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$. Define $C_k(D)$ to be the number of non-zero vectors that can be written as the sum of k or fewer difference vectors. So $C_k(D)$ is the number of non-zero vectors of the form

$$\sum_{i=1}^{\ell} (\mathbf{v}_{\alpha_i} - \mathbf{v}_{\beta_i}) \tag{1}$$

where $\alpha_i, \beta_i \in \{1, 2, \ldots, m\}$ with $\alpha_i \neq \beta_i$ and where $0 \leq \ell \leq k$.

Theorem 5. *Suppose that D is used in Scheme 1. Then the k-hop coverage of the scheme is equal to $C_k(D)$.*

Proof: Let $\mathbf{x}$ be any fixed node. Two nodes that share a key are located at points of the form $\mathbf{v}_i + \mathbf{u}$ and $\mathbf{v}_j + \mathbf{u}$ for some $i, j \in \{1, 2, \ldots, m\}$ and some shift $\mathbf{u}$. This implies that the vector difference between their positions is $\mathbf{v}_i - \mathbf{v}_j$, which is a difference vector of D. Hence a one-hop path between nodes with keys distributed according to Scheme 1 corresponds to a difference vector of the underlying distinct difference configuration. So there is an ℓ-hop path from $\mathbf{x}$ to another node $\mathbf{y}$ if and only if the vector difference between their positions is the sum of ℓ difference vectors. Note also that $\mathbf{x} = \mathbf{y}$ if and only if this sum is the zero vector: since we do not count $\mathbf{x}$ in the k-hop coverage, we are only interested in sums of the form (1) which are non-zero. So $C_k(D)$ is equal to the k-hop coverage of Scheme 1 implemented using D, as required. ∎

Theorem 6. *Let $\xi : \mathbb{R}^2 \to \mathbb{R}^2$ be the map defined in Section II. Let D be a $\mathrm{DD}^*(m)$ and let D' be a $\mathrm{DD}(m)$ such that $D' = \xi(D)$. Then the k-hop coverage of D is equal to the k-hop coverage of D'.*

Proof: Theorem 5 shows that we must show that $C_k(D) = C_k(D')$. But $C_k(D)$ and $C_k(D')$ both count the number of non-zero vectors that can be expressed as the sum of k or fewer difference vectors (of D or D' respectively). The theorem now follows, since ξ is a linear bijection. ∎

B. Maximal k-hop coverage

In this subsection we determine the maximal k-hop coverage of a $\mathrm{DD}(m)$. By Theorem 6, these results apply equally to a $\mathrm{DD}^*(m)$. We begin with some preliminary notation and lemmas.

For a non-negative integer k we define a set H_k of m-tuples of integers as follows:

$$H_k = \left\{ (a_1, a_2, \ldots, a_m) \in \mathbb{Z}^m \;\middle|\; \sum_{i=1}^{m} a_i = 0, \sum_{\{i:a_i>0\}} a_i = k \right\}.$$

For example, when $m = 3$ the triple $(0, 0, 0)$ is the unique element of H_0, the triple $(1, -1, 0)$ is a typical element of H_1, and the triples $(2, -2, 0)$, $(2, -1, -1)$ and $(1, 1, -2)$ are typical elements of H_2. The following results about the sets H_k are easily proved.

Lemma 7. *Define the sets H_k as above.*

(i) Let $\mathbf{a} \in H_{k_1}$ and $\mathbf{b} \in H_{k_2}$. Then $\mathbf{a} + \mathbf{b} \in H_{k_3}$ where k_3 is an integer satisfying $0 \le k_3 \le k_1 + k_2$. In particular, if a non-zero m-tuple $\mathbf{v}$ is a sum of k m-tuples from H_1, then $\mathbf{v} \in H_{k_3}$ for some k_3 satisfying $1 \le k_3 \le k$.

(ii) Let $\mathbf{a} \in H_{k_1}$ and $\mathbf{b} \in H_{k_2}$ with $\mathbf{a} \neq \mathbf{b}$. Then $\mathbf{a} - \mathbf{b} \in H_{k_3}$ where k_3 is an integer satisfying $1 \le k_3 \le k_1 + k_2$.

(iii) Any element of H_{k_1} may be written as the sum of k_1 elements from H_1.

The connection between H_k and the k-hop coverage of $\mathrm{DD}(m)$ is given by the following theorem:

Theorem 8. *The k-hop coverage of a $\mathrm{DD}(m)$ is at most $\sum_{i=1}^{k} |H_i|$, with equality if and only if all the vectors $\sum_{i=1}^{m} a_i \mathbf{v}_i$ with $(a_1, a_2, \ldots, a_m) \in \bigcup_{j=0}^{k} H_j$ are distinct.*

Proof: The difference vectors of D are precisely the vectors of the form $\sum_{i=1}^{m} a_i \mathbf{v}_i$ where $\mathbf{a} \in H_1$. By Lemma 7 (i) and (iii), a vector is a sum of k or fewer difference vectors if and only if it can be written in the form $\sum_{i=1}^{m} a_i \mathbf{v}_i$ with $(a_1, a_2, \ldots, a_m) \in \bigcup_{j=0}^{k} H_j$. The zero vector can always be written in this form, since the sum is zero when $(a_1, a_2, \ldots, a_m) \in H_0$. Since and we are only interested in non-zero vectors, we find that

$$\begin{aligned} C_k(D) + 1 &= \left| \left\{ \sum_{i=1}^{m} a_i \mathbf{v}_i \text{ where } \mathbf{a} \in \bigcup_{j=0}^{k} H_j \right\} \right| \\ &\le \left(\sum_{i=0}^{k} |H_i| \right) \\ &= 1 + \left(\sum_{i=1}^{k} |H_i| \right), \end{aligned}$$

and it is clear that equality is satisfied if and only if the vectors $\sum_{i=1}^{m} a_i \mathbf{v}_i$ where $\mathbf{a} \in \bigcup_{j=0}^{k} H_j$ are distinct. Thus the theorem follows. ∎

TABLE I
COUNTING ELEMENTS IN H_2

Type	Non-zero coeffs	Symm	Number
(a)	$1, 1, -1, -1$	4	$\frac{1}{4}m(m-1)(m-2)(m-3)$
(b)	$2, -1, -1$	2	$\frac{1}{2}m(m-1)(m-2)$
(c)	$1, 1, -2$	2	$\frac{1}{2}m(m-1)(m-2)$
(d)	$2, -2$	1	$m(m-1)$

Corollary 9. *The two-hop coverage of a $\mathrm{DD}(m)$ is at most*

$$\begin{aligned} &\frac{1}{4}m(m-1)(m-2)(m-3) + m(m-1)(m-2) \\ &\qquad + 2m(m-1) = \frac{1}{4}m(m-1)(m^2 - m + 6). \end{aligned}$$

Proof: By Theorem 8 the two-hop coverage is at most $|H_1| + |H_2|$. It is clear that $|H_1| = m(m-1)$, since the m-tuples in H_1 have exactly two non-zero components, one equal to 1 and one equal to -1. To determine $|H_2|$, note that there are four types of element in H_2, corresponding to the four possibilities for the multiset of non-zero coefficients in an m-tuple $\mathbf{a} \in H_2$ (see Table I). The number of elements in H_2 of each type is equal to $(1/s)m!/(m-t)!$, where t is the number of non-zero components in an m-tuple of this type, and s is the number of symmetries that preserve such m-tuples. Thus $|H_2| = \frac{1}{4}m(m-1)(m-2)(m-3) + m(m-1)(m-2) + m(m-1)$, and so the bound of the corollary follows. ∎

In order to show that the bound of Theorem 8 and Corollary 9 is tight, we must show that there exists a $\mathrm{DD}(m)$ given by $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ such that the vectors $\sum_{i=1}^{m} a_i \mathbf{v}_i$, where $\mathbf{a} \in H_0 \cup H_1 \cup \cdots \cup H_k$, are all distinct. This is not difficult to do: for example we may choose $\mathbf{v}_i = ((2k+1)^i, 0)$ for $i = 1, 2, \ldots, m$. We say that a configuration meeting the bound of Theorem 8 has *maximal k-hop coverage*. Note that the example we have just given of a configuration with maximal k-hop coverage is not useful for our application, as the dots in the configuration are exponentially far apart: we would like to construct a $\mathrm{DD}(m, r)$ with r small having maximal k-hop coverage. In order to do this, we now aim to characterise those configurations with maximal k-hop coverage in terms of the much studied concept of B_h sequences (see below). First, we make the following observation.

Lemma 10. *The k-hop coverage of a $\mathrm{DD}(m)$ given by $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ meets the bound of Theorem 8 if and only if $\sum_{i=1}^{m} c_i \mathbf{v}_i \neq 0$ for all $\mathbf{c} \in \bigcup_{i=1}^{2k} H_i$.*

Proof: Suppose that D does not meet the bound of Theorem 8. Then Theorem 8 implies that $\sum_{i=1}^{m} a_i \mathbf{v}_i = \sum_{i=1}^{m} b_i \mathbf{v}_i$, where $\mathbf{a}, \mathbf{b} \in \bigcup_{i=0}^{k} H_i$ and $\mathbf{a} \neq \mathbf{b}$. Writing $\mathbf{c} = \mathbf{a} - \mathbf{b}$ we have that $\sum_{i=1}^{m} c_i \mathbf{v}_i = 0$, and $\mathbf{c} \in \bigcup_{i=1}^{2k} H_i$ by Lemma 7 (ii) above.

Conversely, suppose that there exists $\ell \in \{1, 2, \ldots, 2k\}$ and $\mathbf{c} \in H_\ell$ such that $\sum_{i=1}^{m} c_i \mathbf{v}_i = 0$. By Lemma 7 (iii), we may

write $\mathbf{c}$ as the sum of ℓ difference vectors. Since multiplying a difference vector by the scalar -1 produces another difference vector, we may write $\mathbf{c} = \mathbf{a} - \mathbf{b}$, where $\mathbf{a}, \mathbf{b}$ are the sum of $\lfloor \ell/2 \rfloor$ and $\lceil \ell/2 \rceil$ difference vectors respectively. Note that $\mathbf{a} \neq \mathbf{b}$ since $\mathbf{c} \neq 0$. But $\mathbf{a} \in H_{\lfloor \ell/2 \rfloor}$ and $\mathbf{b} \in H_{\lceil \ell/2 \rceil}$, where $0 \leq \lfloor \ell/2 \rfloor \leq \lceil \ell/2 \rceil \leq \lceil 2k/2 \rceil = k$, and so Theorem 8 implies that D does not meet the bound, as required. ■

Definition 1. *Let A be an abelian group. Let $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\} \subseteq A$ be a sequence of elements of A. We say that D is a* B_h sequence over A *if all the sums*

$$\mathbf{v}_{i_1} + \mathbf{v}_{i_2} + \cdots + \mathbf{v}_{i_h} \text{ with } 1 \leq i_1 \leq \cdots \leq i_h \leq m \qquad (2)$$

are distinct.

B_h sequences (sometimes known as B_h-sets) have been studied for many years, mainly in the case where $A = \mathbb{Z}$. See Graham [17], Halberstam and Roth [18], Lindström [19], O'Bryant [20], for example.

Example 1. *Let q be a prime power, let h be an integer such that $h \geq 2$ and let α be a primitive element of $\mathrm{GF}(q^h)$. Bose and Chowla [21] have shown that the set $\{a \in \mathbb{Z}_{q^h-1} | \alpha^a - \alpha \in \mathrm{GF}(q)\}$ is a B_h set in $\mathbb{Z}_{q^h-1}$ containing q elements.*

The following theorem demonstrates the relation between B_h sequences and distinct difference configurations.

Theorem 11. *Let k be a fixed integer, where $k \geq 2$. Let $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\} \subseteq \mathbb{Z}^2$. Then D is a $\mathrm{DD}(m)$ with maximal k-hop coverage if and only if D is a B_{2k} sequence over $\mathbb{Z}^2$.*

Proof: Suppose D is a B_{2k} sequence over $\mathbb{Z}^2$. We aim to show that D is a $\mathrm{DD}(m)$ with maximal k-hop coverage.

If $\mathbf{v}_i = \mathbf{v}_j$ for $i \neq j$ then $(2k-1)\mathbf{v}_1 + \mathbf{v}_i = (2k-1)\mathbf{v}_1 + \mathbf{v}_j$ and so D cannot be a B_{2k} sequence. This contradiction implies that the vectors are all distinct.

Suppose that $\mathbf{v}_i - \mathbf{v}_j = \mathbf{v}_{i'} - \mathbf{v}_{j'}$, where $i \neq j$, $i' \neq j'$. Then $(2k-2)\mathbf{v}_1 + \mathbf{v}_i + \mathbf{v}_{j'} = (2k-2)\mathbf{v}_1 + \mathbf{v}_{i'} + \mathbf{v}_j$. This contradicts the fact that D is a B_{2k} sequence, unless $i = i'$ and $j' = j$. Thus D has the distinct differences property. Hence D is a $\mathrm{DD}(m)$.

Suppose, for a contradiction, that D does not have maximal k-hop coverage. By Lemma 10 there exists $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in H_1 \cup \cdots \cup H_{2k}$ such that $\sum_{i=1}^m a_i \mathbf{v}_i = 0$. Define $\mathbf{b}$ by

$$b_i = \begin{cases} a_i & \text{when } a_i \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Define $\mathbf{c}$ by the equation $\mathbf{a} = \mathbf{b} - \mathbf{c}$. Then the components of $\mathbf{b}$ and $\mathbf{c}$ are all non-negative. Writing $t = \sum_{i=1}^m b_i = \sum_{i=1}^m c_i = \sum_{a_i > 0} a_i$, the definition of $H_1, H_2, \ldots, H_{2k}$ implies that $1 \leq t \leq 2k$. Since $\mathbf{a}$ is non-zero, $\mathbf{b} \neq \mathbf{c}$. But then our choice of $\mathbf{a}$ implies that

$$(2k-t)\mathbf{v}_1 + \sum_{i=1}^m b_i \mathbf{v}_i = (2k-t)\mathbf{v}_1 + \sum_{i=1}^m c_i \mathbf{v}_i.$$

There are exactly $2k$ summands on both sides of this equality, so D cannot be a B_{2k} sequence. This contradiction shows that D has maximal k-hop coverage, as required.

Now suppose that D is a $DD(m)$ with maximal k-hop coverage. Assume that D is not a B_{2k} sequence, so there exist two distinct sums of the form (2) that are equal. By cancelling terms that occur in both sums, we find that $\sum_{i=1}^m b_i \mathbf{v}_i = \sum_{i=1}^m c_i \mathbf{v}_i$, where the coefficients b_i, c_i are all non-negative and where $\sum_{i=1}^m b_i = \sum_{i=1}^m c_i = t$ for some integer t such that $1 \leq t \leq 2k$. But defining $a_i = b_i - c_i$ we find that $(a_1, a_2, \ldots, a_m) \in H_t$ and $\sum_{i=1}^m a_i \mathbf{v}_i = 0$. Hence D does not have maximal k-hop coverage, by Lemma 10, as required. ■

The following construction converts a known construction for a B_{2k} sequence in $\mathbb{Z}_{q^{2k}-1}$ into a B_{2k} sequence in $\mathbb{Z}^2$, which is a $\mathrm{DD}(m)$ with maximal k-hop coverage by Theorem 11.

Construction 1 *Let k be a fixed integer such that $k \geq 2$. Let q be a prime power, and let $q^{2k} - 1 = ab$ where a and b are coprime. Then there exists a set $X \subseteq \mathbb{Z}^2$ of dots that is doubly periodic with periods a and b, and such that the intersection of X with any $b \times a$ rectangle is a $\mathrm{DD}(q)$ with maximal k-hop coverage.*

Proof: The construction of Bose and Chowla [21] described in Example 1 shows there is a B_{2k} sequence over $\mathbb{Z}_{q^{2k}-1}$ consisting of q elements. Note that by the Chinese Remainder Theorem there is a group isomorphism $\mathbb{Z}_{q^{2k}-1} \to \mathbb{Z}_a \times \mathbb{Z}_b$ given by $x \mapsto (x \bmod a, x \bmod b)$. Thus there are elements $\overline{\mathbf{v}}_1, \overline{\mathbf{v}}_2, \ldots, \overline{\mathbf{v}}_q \in \mathbb{Z}_a \times \mathbb{Z}_b$ that form a B_{2k} sequence over $\mathbb{Z}_a \times \mathbb{Z}_b$. Let $\rho : \mathbb{Z}^2 \to \mathbb{Z}_a \times \mathbb{Z}_b$ be the map defined by $\rho((x, y)) = (x \bmod a, y \bmod b)$. We define $X \subseteq \mathbb{Z}^2$ to be the set of vectors $\mathbf{v} \in \mathbb{Z}^2$ such that $\rho(\mathbf{v}) \in \{\overline{\mathbf{v}}_1, \overline{\mathbf{v}}_2, \ldots, \overline{\mathbf{v}}_q\}$.

Since $\rho((x, y)) = \rho((x+ia, y+jb))$ for any $i, j \in \mathbb{Z}$, we see that X is doubly periodic with periods a and b respectively. Let R be an $b \times a$ rectangle in $\mathbb{Z}^2$. For all $i \in \{1, 2, \ldots, m\}$, there is a unique $\mathbf{v}_i \in R$ such that $\rho(\mathbf{v}_i) = \overline{\mathbf{v}}_i$. Hence $X \cap R = \{\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_q\}$. Moreover, $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_q$ form a B_{2k} sequence over $\mathbb{Z}^2$, since if there are two sums of the form (2) that are equal, then the images of these sums under ρ are also equal, which contradicts the fact that $\overline{\mathbf{v}}_1, \overline{\mathbf{v}}_2, \ldots, \overline{\mathbf{v}}_q$ form a B_{2k} sequence over $\mathbb{Z}_a \times \mathbb{Z}_b$. Thus $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_q$ form a $\mathrm{DD}(q)$ with maximal k-hop coverage by Theorem 11, as required. ■

This construction can be used to prove the existence of a $\mathrm{DD}(m, r)$ with maximal k-hop coverage where r is small:

Theorem 12. *Let k be a fixed integer such that $k \geq 2$. Define $c = (\pi/16)2^{1/k}$. Then there exists a $\mathrm{DD}(m, r)$ with maximal k-hop coverage such that $m \sim cr^{1/k}$.*

Proof: Let $\mathcal{S} \subseteq \mathbb{Z}^2$ be the set of points in $\mathbb{Z}^2$ contained in a circle of radius $\lfloor r/2 \rfloor$ about the origin. Note that $|\mathcal{S}| = (\pi/4)r^2 + O(r)$ (by the Gauss Circle Problem).

Let q be the smallest prime power such that $q^k > 2r$. We have that $q \leq (2r)^{1/k} + ((2r)^{1/k})^{5/8}$ whenever r is sufficiently large by a classical result of Ingham [22] on the gaps between primes. In particular, $q \sim (2r)^{1/k}$.

Define the integer a by

$$a = \begin{cases} q^k - 1 & \text{when } q \text{ is even,} \\ (q^k - 1)/2 & \text{when } q^k \equiv 3 \bmod 4, \\ (q^k + 1)/2 & \text{when } q^k \equiv 1 \bmod 4. \end{cases}$$

Define $b = (q^{2k}-1)/a$. Since $\gcd(q^k-1, q^k+1) = 1$ when q is even and $\gcd(q^k-1, q^k+1) = 2$ when q is odd, we find that a and b are coprime. Moreover, our choice of q shows that $r \le a \le b$. Let X be the set of dots in $\mathbb{Z}^2$ given in Construction 1.

The average number of dots in a shift of S by an element of $\mathbb{Z}^2$ is $|S|q/(ab)$, and so we can find a shift T of S such that $|T \cap X| \ge |\mathcal{S}|q/(ab)$. Define $D \subseteq T \cap X$ to be a subset of size m, where $m = \lceil |\mathcal{S}|q/(ab) \rceil$. Note that $m \sim (\pi/4)r^2 q/(2r)^2 \sim (\pi/16)2^{1/k} r^{1/k}$. Since T is a sphere of radius $\lfloor r/2 \rfloor$, any pair of dots in D are at distance at most r. Moreover, the fact that $r \le a \le b$ implies that T is contained in a $b \times a$ rectangle R. By Construction 1, $R \cap X$ is a $\mathrm{DD}(q)$ with maximal k-hop coverage. Since $D \subseteq T \cap X \subseteq R \cap S$, we see that D is a $\mathrm{DD}(m, r)$ with maximal k-hop coverage. So the theorem follows, as required. ∎

Combining Theorems 2, 6 and 12, we have the analogous result for the hexagonal grid:

Corollary 13. *Let k be a fixed integer such that $k \ge 2$. Define $c' = (\pi/16)2^{1/k}\left(\frac{2}{3}\right)^{1/2k}$. Then there exists a $\mathrm{DD}^*(m, r)$ with maximal k-hop coverage such that $m \sim c' r^{1/k}$.*

For any fixed values of m and k, we define $r(k, m)$ to be the smallest value of r such that there exists a $\mathrm{DD}(m, r)$ with maximal k-hop coverage. It is an important problem to determine $r(k, m)$. The construction in Theorem 12 provides an upper bound on $r(k, m)$, showing that when k is fixed and $m \to \infty$ we have $r(k, m) = O(m^k)$. We now provide a corresponding lower bound on $r(k, m)$, which shows that the construction in Theorem 12 is reasonable:

Theorem 14. *Let k be an integer such that $k \ge 2$. Then $\frac{m^k}{\sqrt{\pi} k! \cdot k} + o(m^k) \le r(k, m) \le \frac{1}{2}\left(\frac{16}{\pi}\right)^k m^k + o(m^k)$.*

Proof: The upper bound is proved in Theorem 12.

To prove the lower bound, let D be a $\mathrm{DD}(m, r)$ with maximal k-hop coverage, where $r = r(k, m)$. The definition of maximal k-hop coverage and Theorem 5 show that $C_k(D) = \sum_{i=1}^{k} |H_i|$. Let $B = \{(a_1, a_2, \ldots, a_m) \in H_k \ : \ |\{i : a_i \ne 0\}| = 2k\}$. Clearly $|B| = \frac{m!}{(m-2k)!k!^2}$ and

$$\sum_{i=1}^{k} |H_i| = \frac{m!}{(m-2k)!k!^2} + o(m^{2k}) = \frac{m^{2k}}{k!^2} + o(m^{2k}).$$

So $C_k(D) = \frac{m^{2k}}{k!^2} + o(m^{2k})$.

Every vector counted by $C_k(D)$ is the sum of at most k difference vectors of D. Each difference vector has length at most r, and so every vector counted by $C_k(D)$ is contained in a circle of radius kr centred at the origin. Such a circle contains at most $\pi(kr)^2 + O(r)$ vectors in $\mathbb{Z}^2$ (by Gauss's solution to the Gauss circle problem). Thus

$$\frac{m^{2k}}{k!^2} + o(m^{2k}) = C_k(D) \le \pi(kr)^2 + O(r),$$

which implies the lower bound of the theorem, as required. ∎

For the hexagonal grid, we denote the smallest r for which there exists a $\mathrm{DD}^*(m, r)$ with complete k-hop coverage by $r^*(m, k)$. Combining Theorems 14 and 2, we have the following.

Theorem 15. *If $k \ge 2$ then $\sqrt{\frac{3}{2}}\frac{m^k}{\sqrt{\pi} k! \cdot k} + o(m^k) \le r^*(k, m) \le \sqrt{\frac{3}{2}}\,\frac{1}{2}\left(\frac{16}{\pi}\right)^k m^k + o(m^k)$.*

In the case $k = 1$, we can use the results of [1] to give tighter bounds, as every distinct difference configuration has a one-hop coverage of $m(m-1)$, which is thus maximal.

Theorem 16. *We have that*

$$\frac{2}{\sqrt{\pi}} m + o(m) \le r(1, m) \le \frac{2}{\mu} m + o(m),$$

where $\mu \approx 0.914769$ is the maximum value of $((\pi/2) - 2\theta + \sin 2\theta)/\cos\theta$ on the interval $0 \le \theta \le \pi/4$.

Proof: It is proved in [1] that if a $\mathrm{DD}(m, r)$ exists, then $m \le \frac{\sqrt{\pi}}{2} r + O(r^{2/3})$, which gives rise to the lower bound on $r(1, m)$. Furthermore, [1] contains a construction of a $\mathrm{DD}(m, r)$ with $m = (\mu/2)r + o(r)$ dots, from which we derive the upper bound. ∎

The paper [1] also contains analogous results in the hexagonal grid. From these, we can deduce the following bounds on $r^*(1, m)$:

Theorem 17. *We have that*

$$\frac{\sqrt{2}\,3^{1/4}}{\sqrt{\pi}} m + o(m) \le r^*(1, m) \le \frac{2^{1/2} 3^{1/4}}{\mu} m + o(m),$$

where μ is defined as in Theorem 16.

Recall that we introduced the Manhattan and hexagonal metrics on the square and hexagonal grids respectively in Section II. We conclude this subsection with a brief discussion about the situation when we use these metrics rather than Euclidean distance. For integers k and m, define $\overline{r}(k, m)$ to be the smallest integer r such that there exists a $\overline{\mathrm{DD}}(m, r)$ with maximal k-hop coverage, and define $\overline{r}^*(k, m)$ to be the smallest integer r such that there exists a $\overline{\mathrm{DD}}^*(m, r)$ with maximal k-hop coverage.

Theorem 18. *Let k be a fixed integer, $k \ge 2$. There exist constants c_1, c_2, c_3 and c_4 such that for all sufficiently large integers m*

$$c_1 m^k \le \overline{r}(k, m) \le c_2 m^k \text{ and}$$
$$c_3 m^k \le \overline{r}^*(k, m) \le c_4 m^k.$$

Proof: By Theorem 3, a $\overline{\mathrm{DD}}(m, r)$ with maximal k-hop coverage is also a $\mathrm{DD}(m, r)$ with maximal k-hop coverage. So $r(k, m) \le \overline{r}(k, m)$. Moreover, a $\mathrm{DD}(m, r)$ with maximal k-hop coverage is a $\overline{\mathrm{DD}}(m, \lceil \sqrt{2} r \rceil)$ with maximal k-hop coverage, so $\overline{r}(k, m) \le \lceil \sqrt{2}\, r(k, m) \rceil$. The first statement of the theorem now follows by Theorem 14.

The proof of the second statement of the theorem is similar, using Theorems 4 and 15 in place of Theorems 3 and 14 respectively. ∎

The results in [1] can be used to establish the following:

Theorem 19. *We have that*

$$\overline{r}(1,m) = \sqrt{2}\,m + o(m).$$

Moreover,

$$(2/\sqrt{3})m + o(m) \le \overline{r}^*(1,m) \le (2/\mu)m + o(m),$$

where $\mu = (2/3)^{3/2}(1+2\sqrt{7})/(\sqrt{2+\sqrt{7}}) \approx 1.58887$.

C. Minimum k-hop coverage

Having established an upper bound for the k-hop coverage of a $\mathrm{DD}(m)$ (and hence of a $\mathrm{DD}^*(m)$), we now consider the smallest values it can take.

Theorem 20. *The k-hop coverage of a $\mathrm{DD}(m)$ is at least $km(m-1)$.*

Proof: The one-hop coverage of a $\mathrm{DD}(m)$ is $m(m-1)$. For $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ a $\mathrm{DD}(m)$, let $\mathbf{u} = (d,e)$ be the difference vector with $|d|$ as large as possible. If there is more than one choice for $\mathbf{u}$, choose $\mathbf{u}$ with $|e|$ as large as possible subject to $|d|$ being maximal. Without loss of generality, we can assume that $d > 0$ and $e \ge 0$ (if not we can flip and rotate the array to obtain an equivalent array with such vector).

Let S_1 be the set of $m(m-1)$ vectors that can be reached by one-hop paths from the origin. Then S_1 can be written as the disjoint union of the two sets

$$S_1^+ = \{(x,y) | (x,y) \in S_1,\ x > 0 \text{ or } (x = 0 \text{ and } y > 0)\}$$

and $S_1^- = \{-(x,y) | (x,y) \in S_1^+\}$.

For $i > 1$, we define

$$S_i = \{\mathbf{w} + (i-1)\mathbf{u} | \mathbf{w} \in S_1^+\} \cup \{(-\mathbf{w} - (i-1)\mathbf{u} | \mathbf{w} \in S_1^+\}.$$

As $\mathbf{u}$ is a difference vector of D, the vectors of S_i can all be reached by i-hop paths from the origin. Furthermore, $S_i \cap S_j = \emptyset$ for $i \ne j$ and $|S_i| = m(m-1)$. Hence, the theorem is proved. ∎

For certain values of m there exist $\mathrm{DD}(m)$ for which the above bound is tight. For example, consider the following $\mathrm{DD}(3)$:

The difference vectors in this example are $\{\pm(1,0), \pm(2,0), \pm(3,0)\}$, and hence any of the $6k$ vectors of the form $\pm(t,0)$ for $0 < t \le 3k$ can be reached by a k-hop path.

We can construct more examples where the bound is tight as follows. A *Golomb ruler* is a set M of m integers such that the differences $x - y$ where $x, y \in M$ and $x \ne y$ are all distinct. A Golomb ruler is *perfect* if

$$\{u - v : u, v \in S\} = \{i \in \mathbb{Z} : |i| \le m(m-1)/2\}.$$

For example, the sequence $\{0,1,3\}$ is a perfect Golomb ruler. The $\mathrm{DD}(3)$ above was constructed from this sequence by taking appropriate multiples of the vector $(1,0)$. More generally, if M is a perfect Golomb ruler then a configuration D consisting of the vectors $\mathbf{r} + i\mathbf{s}$ where $i \in M$ is a $\mathrm{DD}(m)$ with a k-hop coverage of $km(m-1)$, and so meets the bound of Theorem 20. We say that D is *equivalent to a perfect Golomb ruler* if we can construct it in this way. In fact, we will now show that a $\mathrm{DD}(m)$ meets the bound of Theorem 20 if and only if it is equivalent to a perfect Golomb ruler.

Lemma 21. *Let k be an integer, $k \ge 2$. Suppose D is a $\mathrm{DD}(m)$ in which there are differences $\mathbf{d}$ and $\mathbf{d}'$ that are not parallel. Then the k-hop coverage of D is strictly greater than $km(m-1)$.*

Proof: Define the difference vector $\mathbf{u}$ and the sets S_i as in the proof of Theorem 20. The set of difference vectors not parallel to $\mathbf{u}$ is non-empty by assumption. Let $\mathbf{v}$ be a difference vector whose projection in the direction perpendicular to $\mathbf{u}$ has length $p(\mathbf{v})$ as large as possible. Since $k \ge 2$, the k-hop coverage of D is at least

$$|S_1 \cup S_2 \cup \cdots \cup S_k \cup \{2\mathbf{v}\}|.$$

The argument in Theorem 20 shows the sets S_i are disjoint and have order $m(m-1)$. So the theorem follows if we can show that $2\mathbf{v} \notin S_1 \cup S_2 \cup \cdots \cup S_k$. But any vector in S_i can be written in the form $\mathbf{w} \pm (i-1)\mathbf{u}$ where $\mathbf{w}$ is a difference vector, and therefore

$$p(\mathbf{w} \pm (i-1)\mathbf{u}) = p(\mathbf{w}) \le p(\mathbf{v}) < 2p(\mathbf{v}) = p(2\mathbf{v}).$$

Hence $2\mathbf{v}$ does not lie in any of the sets S_i, as required. ∎

Theorem 22. *Let k be an integer such that $k \ge 2$, and let D be a $\mathrm{DD}(m)$. Then D meets the bound of Theorem 20 if and only if it is equivalent to a perfect Golomb ruler.*

Proof: It is easy to see that if D is equivalent to a perfect Golomb ruler, then D meets the bound of Theorem 20.

Let D be a $\mathrm{DD}(m)$ that meets the bound of Theorem 20. The set S_ℓ defined in the proof of Theorem 20 is a set of $m(m-1)$ vectors that can be reached by an ℓ-hop path from the origin, but cannot be reached by a path of length $\ell - 1$. Thus $C_k(D) \ge C_2(D) + (k-2)m(m-1)$, so D meets the bound of Theorem 20 in the case $k = 2$. So to prove the theorem, we need only consider the case $k = 2$.

Let $\mathbf{r}$ be a vector in D. Lemma 21 implies that all the difference vectors in D are parallel to a fixed vector $\mathbf{u}$. Let $\mathbf{s}$ be the shortest vector in $\mathbb{Z}^2$ that is parallel to $\mathbf{u}$. Then (since $\mathbb{Z}^2$ is a lattice) $D \subseteq \{\mathbf{r} + i\mathbf{s} \mid i \in \mathbb{Z}\}$. Thus D is equivalent to a Golomb ruler $M \subseteq \mathbb{Z}$. Without loss of generality, we may assume that the greatest common divisor of the elements of M is 1, for if the greatest common divisor is a then we can replace $\mathbf{s}$ by $a\mathbf{s}$ and M by $(1/a)M$.

It remains to show that M is perfect. The set $S = \{x - y | x, y \in M\}$ contains $m(m-1)+1$ elements, since M is a Golomb ruler. A square reachable from the origin by a one-hop or two-hop path corresponds to an element of $S + S = \{a + b | a, b \in S\}$. It is a well-known result of additive combinatorics that for a set A of integers with $|A| = n$ it holds that $|A+A| = 2n-1$ if and only if the elements of A are in arithmetic progression. The bound of Theorem 20 requires $S+S$ to have size $2m(m-1)+1$ (due to the inclusion of 0); as this is equal to $2|S|-1$ it follows that the elements of S are in arithmetic

progression. Since $S = -S$ and the greatest common divisor of the elements of M is 1 we find that $S = \{x \in \mathbb{Z} \mid |x| \leq m(m-1)/2\}$. So M is a perfect Golomb ruler, as required. ∎

IV. A DD(m) with Complete Two-Hop Coverage in a Rectangle

In Section III we explored the range of values that the k-hop coverage of a distinct difference configuration can take. When choosing a distinct difference configuration for use in Scheme 1 it may seem desirable to select a configuration with maximal two-hop coverage. However, from Theorem 14 we see that a DD(m, r) with maximal two-hop coverage has "approximately" $m^2 = r$, which places too great a restriction on the maximum number of keys that each node can store in the resulting scheme. From a practical perspective it thus may be desirable to focus on connectivity within a localised region.

In this section we give a construction of a DD(m) that ensures a two-hop path between a given point $\mathbf{x}$ and any other grid point within a $(2p-3) \times (2p-1)$ rectangle centred at $\mathbf{x}$, where p is any prime greater than or equal to five. This allows the region to be tailored to the requirements of a specific application environment.

Our construction can be thought of as being based on the periodicity properties of a B_2 sequence in $\mathbb{Z}_{(p^2-p)}$ proposed by Ruzsa in [23], or as a consequence of a periodic generalisation of the Welch construction of a Costas array [24]. In Subsection IV-A we discuss some properties of a related doubly periodic array that we will exploit later. In Subsection IV-B we present the construction and demonstrate that it achieves complete two-hop coverage.

A. The Welch Periodic Array

Definition 2. (Welch Periodic Array) *Let α be a primitive root modulo a prime p. We define the* Welch periodic array *to be the set*

$$\mathcal{R}_p = \{(i, j) \in \mathbb{Z}^2 | \alpha^j \equiv i \bmod p\}.$$

This array is doubly periodic in the sense that if $\mathcal{R}_p$ contains a dot at position (i, j) then it also contains dots at all positions of the form $(i + \lambda p, j + \mu(p-1))$ where $\lambda, \mu \in \mathbb{Z}$. It has a distinct difference property "up to periodicity": see the lemma below. We say that dots A and A' at positions (i, j) and (i', j') are *equivalent*, and we write $A \equiv A'$, if $i' = i + \lambda p$ and $j' = j + \mu(p-1)$ for some $\lambda, \mu \in \mathbb{Z}$.

Lemma 23. *Let d and e be integers such that $d \not\equiv 0 \bmod p$ and $e \not\equiv 0 \bmod (p-1)$. Suppose that $\mathcal{R}_p$ contains dots A and B at positions (i_1, j_1) and $(i_1 + d, j_1 + e)$ respectively, and dots A' and B' at positions (i_2, j_2) and $(i_2 + d, j_2 + e)$ respectively. Then $A \equiv A'$ and $B \equiv B'$.*

Proof: By the definition of $\mathcal{R}_p$ we have

$$\begin{aligned} i_1 &\equiv \alpha^{j_1} \bmod p \\ i_2 &\equiv \alpha^{j_2} \bmod p \\ i_1 + d &\equiv \alpha^{j_1+e} \bmod p \\ i_2 + d &\equiv \alpha^{j_2+e} \bmod p. \end{aligned}$$

Eliminating i_1, i_2 and d from these equations we get

$$(\alpha^e - 1)(\alpha^{j_1} - \alpha^{j_2}) \equiv 0 \bmod p.$$

Since $e \not\equiv 0 \bmod (p-1)$, this implies that $j_1 \equiv j_2 \bmod (p-1)$. The first two equations above then imply that $i_1 \equiv i_2 \bmod p$. ∎

We note that in addition, if $\mathcal{R}_p$ contains dots at (i, j) and $(i + d, j)$ then $d \equiv 0 \bmod p$ and if it contains dots at (i, j) and $(i, j + e)$ then $e \equiv 0 \bmod (p-1)$. Thus we see that a vector (d, e) can occur at most once as a difference between two of the dots of $\mathcal{R}_p$ that lie within any particular $(p-1) \times p$ rectangle.

B. Construction of the DD(m)

We now define a DD(m) by choosing a finite subset of the dots in $\mathcal{R}_p$, as follows.

Construction 2 *Let p be an odd prime. Let $(i, j) \in \mathbb{Z}^2$ be such that $\mathcal{R}_p$ has dots at (i, j) and $(i+1, j+1)$. Note that such a position (i, j) exists. To see this, let i and j be integers such that*

$$\alpha^j \equiv i \equiv \frac{1}{\alpha - 1} \bmod p.$$

The right-hand side of this equality is well-defined and non-zero modulo p, and so there is a suitable choice for i and j. Clearly $\mathcal{R}_p$ has a dot at the position (i, j). But there is also a dot at $(i+1, j+1)$ since

$$\alpha^{j+1} \equiv \frac{\alpha}{\alpha - 1} \equiv \frac{1}{\alpha - 1} + 1 \equiv i + 1 \bmod p.$$

Consider the $(p-1) \times p$ rectangle S bounded by the positions (i, j), $(i + p - 1, j)$, $(i, j + p - 2)$ and $(i + p - 1, j + p - 2)$. By construction, $\mathcal{R}_p$ has $p - 1$ dots in S. Due to its periodic nature, $\mathcal{R}_p$ also has dots at positions $(i, j + (p-1))$, $(i + p, j)$ and $(i+p+1, j+p)$. We construct a configuration $\mathcal{B}$ by adding these three dots to the set of dots in $\mathcal{R}_p \cap S$.

Our configuration $\mathcal{B}$ is shown in Fig. 3. The configuration is contained in a $(p+1) \times (p+2)$ rectangle. The *border region* of width 2 contains exactly 5 dots: A, A', A'', B and B'. The *central region* is a $(p-3) \times (p-2)$ rectangle. This region contains $p - 3$ dots: one column is empty, but every other column and every row contains exactly one dot. Note that $A \equiv A' \equiv A''$ and $B \equiv B'$, but there are no other equivalent pairs of dots in $\mathcal{B}$.

Lemma 24. *The configuration $\mathcal{B}$ is a DD$(p+2)$, all of whose points lie in a $(p+1) \times (p+2)$ rectangle.*

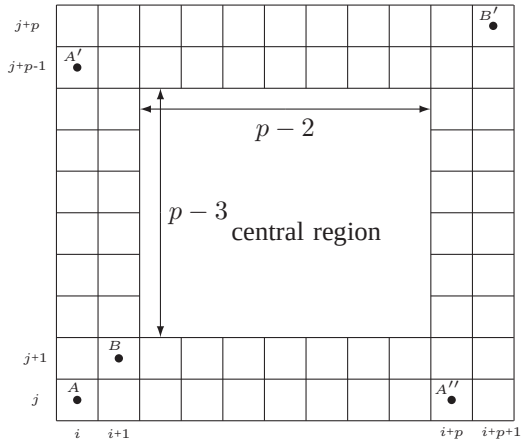

Fig. 3. The configuration $\mathcal{B}$. The five dots shown are the dots that lie the border of width 2 of the $(p+1) \times (p+2)$ rectangle containing the configuration.

Proof: We have already remarked that $\mathcal{B}$ contains $p+2$ dots, all lying in a $(p+1) \times (p+2)$ rectangle. So it remains to show that $\mathcal{B}$ satisfies the distinct differences property.

Suppose, for a contradiction, that X and Y, and X' and Y', are distinct pairs of dots in $\mathcal{B}$ with the same difference vector (d, e).

Suppose that $d \in \{0, -p, p\}$ or $e \in \{0, -(p-1), (p-1)\}$. A difference vector between a dot in the central region of our configuration and any other dot has $x-$ and $y-$coordinates of absolute value at most $p-1$ or $p-2$ respectively. Moreover, a central dot is the only dot in its row and column. So our assumption implies that none of X, X', Y, Y' can lie in the central region of our configuration. But the 5×4 ordered pairs of dots in the border region all have distinct difference vectors, and so we have a contradiction in this case.

So we may assume that $d \notin \{0, -p, p\}$ and $e \notin \{0, -(p-1), (p-1)\}$. In particular, since all dots lie in a $(p+1) \times (p+2)$ rectangle, we see that $d \not\equiv 0 \bmod p$ and $e \not\equiv 0 \bmod (p-1)$. Lemma 23 now implies that $X \equiv X'$ and $Y \equiv Y$. If $X = X'$ then $Y = Y'$ which contradicts the fact that our pairs of dots are distinct. Hence $X \neq X'$. The fact that $X \equiv X'$ now implies that X and X' must lie in the border of our configuration. A similar argument implies the same is true for Y and Y'. As in the paragraph above, we now have a contradiction. Thus the lemma follows. ∎

Our aim is to show (Theorem 27) that $\mathcal{B}$ achieves complete two-hop coverage on a $(2p-3) \times (2p-1)$ rectangle relative to the central point of the rectangle. In order to demonstrate this, it is necessary to show that every vector (d, e) with $|d| \leq p-1$ and $|e| \leq p-2$ can be expressed as a two-hop path of difference vectors from $\mathcal{B}$. The following lemma proves this for the majority of such vectors (d, e).

Lemma 25. *Any vector of the form (d, e), where d and e are non-zero integers satisfying $|d| \leq p-1$ and $|e| \leq p-2$, can be expressed as the sum of two difference vectors from $\mathcal{B}$.*

Proof: Consider the $(p-1) \times p$ rectangle S defined in Construction 2, and let $\mathcal{A}$ be the restriction of $\mathcal{R}_p$ to the $(2p-2) \times 2p$ subarray whose lower leftmost corner coincides with that of S.

We partition $\mathcal{A}$ into four $(p-1) \times p$ subarrays as follows:

$$\left(\begin{array}{c|c} \mathcal{D}_3 & \mathcal{D}_4 \\ \hline \mathcal{D}_1 & \mathcal{D}_2 \end{array}\right)$$

The periodicity of $\mathcal{R}_p$ means that the set of dots of $\mathcal{R}_p$ contained in each subarray is a translation of the set of dots of $\mathcal{R}_p$ contained in $\mathcal{D}_1$. Moreover, since $\mathcal{D}_1 = S$, all the dots in $\mathcal{D}_1$ are contained in $\mathcal{B}$.

We claim that each of the vectors (d, e) appears as the difference of two points in $\mathcal{A}$. Since the negative of a difference vector is always a difference vector, we may assume without loss of generality that $d > 0$. Suppose that $e > 0$. There is a unique position $(i', j') \in \mathcal{D}_1$ such that

$$\alpha^{j'} \equiv i' \equiv \frac{d}{\alpha^e - 1} \bmod p.$$

It is easy to check, just as in Construction 2, that $\mathcal{R}_p$ has dots at (i', j') and $(i'+d, j'+e)$. Since d and e are both positive, $(i'+d, j'+e)$ lies in $\mathcal{A}$, and so our claim follows in this case. The argument for the case when $e < 0$ is exactly the same, except now we choose $(i', j') \in \mathcal{D}_3$. So the claim follows.

To prove the lemma, we need to show that each difference vector (d, e) can be written as the sum of two difference vectors of $\mathcal{B}$. This follows from the paragraph above and the following observations:

- Any vector connecting two dots of $\mathcal{D}_1$ is a difference vector of $\mathcal{B}$ by construction.
- Due to the periodicity of $\mathcal{R}_p$, a vector connecting a dot in $\mathcal{D}_1$ with a dot in $\mathcal{D}_3$ (or, similarly, a dot in $\mathcal{D}_2$ with a dot in $\mathcal{D}_4$) can be expressed as the sum of the vector $(0, p-1)$ (which occurs as a difference between the dots A and A' in $\mathcal{B}$) and some other difference vector of $\mathcal{B}$.
- A vector connecting a dot in $\mathcal{D}_1$ with a dot in $\mathcal{D}_2$ (or, similarly, a dot in $\mathcal{D}_3$ with a dot in $\mathcal{D}_4$) can be expressed as the sum of the difference vector $(p, 0)$ (which occurs between A and A'') and some other difference vector of $\mathcal{B}$.
- A vector connecting a dot in $\mathcal{D}_1$ with a dot in $\mathcal{D}_4$ is the sum of the difference vector $(p, p-1)$ (which occurs between B and B') and some other difference vector of $\mathcal{B}$.
- A vector connecting a dot in $\mathcal{D}_3$ with a dot in $\mathcal{D}_2$ is the sum of the difference vector $(p, -(p-1))$ (which occurs between A' and A'') and some other difference vector of $\mathcal{B}$.

∎

It remains to consider vectors that have a zero co-ordinate. We will use the following lemma in our proof that such vectors all occur as the sum of two difference vectors from $\mathcal{B}$.

Lemma 26. *Let t be a positive integer with $t \geq 3$. Let $\mathcal{F}$ be a set of integers satisfying the following properties:*

(a) $|\mathcal{F}| = t+1$,

(b) $\mathcal{F} \subset \{-(t-1), -(t-2), \ldots, -1\} \cup \{1, 2, \ldots, t-1\} \cup \{t+1\}$,

(c) $\{1, -(t-1), t+1\} \subset \mathcal{F}$,

(d) $\exists i \in \mathcal{F} \setminus \{1, -(t-1), t+1\}$ *with* $i < 0$,
(e) if $i > 0$ *and* $i \in \mathcal{F} \setminus \{1, -(t-1), t+1\}$ *then* $i - t \notin \mathcal{F}$.
Then each positive integer γ *with* $1 \leq \gamma \leq t-1$ *has a representation of the form* $\gamma = j - i$ *where* $i, j \in \mathcal{F}$.

Proof: Since $\mathcal{F} \setminus \{1, -(t-1), t+1\}$ contains $t-2$ elements, (e) implies that $\mathcal{F}$ must contain precisely one element of each pair $\{i, i-t\}$ for $i = 2, 3, \ldots, t-1$. Suppose, for a contradiction, that there exists a positive integer $\gamma \leq t-1$ that cannot be expressed as the difference between two elements of $\mathcal{F}$.

Suppose that $\gamma > 1$. Since $1, t+1 \in \mathcal{F}$, our assumption implies that $1 - \gamma \notin \mathcal{F}$ and $t + 1 - \gamma \notin \mathcal{F}$. But $1 - \gamma = (t+1-\gamma) - t$, hence one of these numbers must be contained in $\mathcal{F}$, which gives a contradiction in this case.

Suppose that $\gamma = 1$. The assumption implies that $\mathcal{F}$ does not contain a pair of integers that differ by 1. If t is odd this implies that $\mathcal{F} \setminus \{t+1\}$ contains at most $(t-1)/2$ positive integers, and at most $(t-1)/2$ negative integers, hence $\mathcal{F}$ contains at most $(t-1)+1 = t$ integers, which contradicts (a). If t is even, then in order for the size of $\mathcal{F}$ to be $t+1$, $\mathcal{F} \setminus \{t+1\}$ must contain $t/2$ positive integers, all of which are odd, and $t/2$ negative integers that are also all odd. This implies that for each positive odd integer $1 < i < t$ we have that $i \in \mathcal{F}$ and $i - t \in \mathcal{F}$, which contradicts (e). So the lemma follows. ∎

We can now combine these two lemmas to obtain our desired result:

Theorem 27. *Let* p *be a prime,* $p \geq 5$. *The distinct difference configuration* $\mathcal{B}$ *achieves complete two-hop coverage on a* $(2p-3) \times (2p-1)$ *rectangle relative to the central point of the rectangle.*

Proof: By Lemma 25, any vector (d, e) from the centre of a $(2p-3) \times (2p-1)$ rectangle to another point of the rectangle can be expressed as the sum of two difference vectors of $\mathcal{B}$ if d and e are non-zero.

We now consider vectors of the form $(0, e)$ with $0 < e \leq p-2$. Such a vector can be expressed as the sum of two difference vectors of $\mathcal{B}$ if $\mathcal{B}$ has difference vectors of the form $(1, y')$ and $(1, y)$ with $y' - y = e$. The second coordinates of the set of difference vectors of $\mathcal{B}$ of the form $(1, y)$ with $y \neq 0$ satisfy the conditions of Lemma 26 for $t = p-1$, since:

(a) The left-most column of the array contains two dots; all other columns contain a single dot apart from a single central column which is empty. So $\mathcal{B}$ has p difference vectors of the form $(1, y)$ with $y \neq 0$.
(b) Except for the vector $(1, p)$, all difference vectors of $\mathcal{B}$ of the form $(1, y)$ with $y \neq 0$ satisfy $|y| \leq p-2$.
(c) The vectors $(1, 1)$, $(1, -(p-2))$ and $(1, p+1)$ are all difference vectors of $\mathcal{B}$ (as they occur as differences between dots in the border region of $\mathcal{B}$, see Fig. 3).
(d) The difference vectors of $\mathcal{B}$ of the form $(1, y)$ cannot all satisfy $y > 0$. This is obvious if the right-most central column contains a dot. If this column is empty and y is always positive, then the remaining $(p-3) \times (p-3)$ central region must contain dots along a lower-left to top-right diagonal. Since $p \geq 5$, two central dots have the difference vector $(1, 1)$. Since dots A and B also have this difference vector, the distinct difference property is violated and so we have a contradiction, as required.
(e) If $(1, y)$ with $y \neq 1, p$ is a difference vector of $\mathcal{B}$ then $(1, y-(p-1))$ is not. For Lemma 23 implies that the dots involved must be equivalent, and so must be in the border region of our construction.

Lemma 26 now implies that any vector $(0, e)$ with $0 < e \leq p-2$ has an expression in the form $(0, e) = (1, y') + (-1, -y)$ where $(1, y')$ and $(1, y)$ are difference vectors of $\mathcal{B}$. Vectors of the form $(0, e)$ with $-(p-2) < e < 0$ can be written as $(1, y) + (-1, -y')$.

In a similar manner, we can show that the first coordinates of the difference vectors of $\mathcal{B}$ of the form $(x, 1)$ satisfy the conditions of Lemma 26 with $t = p$, and hence any vector of the form $(d, 0)$ with $0 < |d| \leq p-1$ can be written as the sum of two difference vectors of $\mathcal{B}$. Thus the result is proved. ∎

We can thus apply the $DD(m)$ specified in Construction 2 to Scheme 1 in order to establish a key predistribution scheme which guarantees two-hop paths between a node and all of its neighbours within a surrounding rectangular region. This provides a powerful notion of local connectivity in order to facilitate connectivity across the wider network. The resulting scheme is also highly configurable, since the value of p can be adjusted in order to tradeoff storage against the size of the fully connected local region.

V. Conclusion and Open Problems

In this paper we have studied properties of distinct difference configurations, which can be used to design efficient key predistribution schemes for wireless sensor networks based on grids.

In Section III we explored the k-hop coverage of a $\mathrm{DD}(m, r)$. We characterised maximal k-hop coverage in terms of B_{2k} sequences over $\mathbb{Z}^2$, and we used a known construction of B_{2k} sequences over $\mathbb{Z}$ to produce a $\mathrm{DD}(m, r)$ with maximal k-hop coverage and of the order of $r^{1/k}$ dots. We provided an argument that shows that the order of magnitude of the number of dots is correct (by bounding the functions $r(k, m)$). These results indicate the range of achievable parameters, which in turn determine the connectivity properties of the resulting key predistribution schemes. It would be interesting to find better bounds on the leading coefficient of $r(k, m)$, and it would be worthwhile determining $r(k, m)$ precisely for small values of k and m. Similar comments hold for the function $r^*(k, m)$, and for the analogous situations using the Manhattan or hexagonal metric.

In Section IV we constructed a $\mathrm{DD}(m, r)$ with complete 2-hop coverage within a large rectangular region centred on the origin. This $\mathrm{DD}(m, r)$ can be used to design key predistribution schemes with excellent local connectivity properties. The area of the fully connected region is of the order of m^2. It would be interesting to investigate whether there are any constructions that achieve complete two-hop coverage in significantly larger rectangles. Constructions that are optimised with respect to two-hop coverage for other natural regions, for

example a circle of large radius, would also be of practical interest. A further open problem is whether there exist any good constructions, for any natural region, achieving complete k-hop coverage for $k \geq 3$.

REFERENCES

[1] S.R. Blackburn, T. Etzion, K.M. Martin, and M.B. Paterson, "Two-dimensional patterns with distinct differences: Constructions, bounds and maximal anticodes," *preprint*, 2008.

[2] S.R. Blackburn, T. Etzion, K.M. Martin, and M.B. Paterson, "Efficient key predistribution for grid-based wireless sensor networks," in (R. Safavi-Naini, Ed) *Proc. ICITS 2008*, Lecture Notes in Computer Science 5155, Springer-Verlag, Berlin, pp. 54–69, 2008.

[3] K. Römer and F. Mattern. The design space of wireless sensor networks. *IEEE Wireless Communications Magazine*, 11(6):54–61, 2004.

[4] S.A. Çamtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", *Rensselaer Polytechnic Institute Tech. Report* TR-05-07 March 2005.

[5] K.M. Martin and M.B. Paterson, "An Application-Oriented Framework for Wireless Sensor Network Key Establishment", *Electron. Notes Theor. Comput. Sci.*, vol. 192, pp. 31–41, 2008.

[6] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu and M. Galloway, "A survey of key management schemes in wireless sensor networks", *Comput. Commun.*, vol. 30, pp. 2314–2341, 2007.

[7] L. Eschenauer and V.D. Gligor "A key-management scheme for distributed sensor networks", *CCS '02: Proc. of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, 2002.

[8] Institut für Chemie und Dynamik der Geosphäre (ICG), Forschungszentrum Jülich: SoilNet – a Zigbee based soil moisture sensor network. http://www.fz-juelich.de/icg/icg-4/index.php?index=739, 2008.

[9] Integrated smart sensing systems. http://dpi.projectforum.com/isss/11, 2007.

[10] J. McCulloch, P. McCarthy, S. M. Guru, W. Peng, D. Hugo, and A. Terhorst. Wireless sensor network deployment for water use efficiency in irrigation. In *REALWSN '08: Proceedings of the Workshop on Real-world Wireless Sensor Networks*, pages 46–50, New York, NY, USA, 2008. ACM.

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

[12] J. Lee and D.R. Stinson "On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs", *ACM Trans. Inf. Syst. Secur.*, vol. 11(2), pp. 1–35, 2008.

[13] W. Du, J. Ding, Y.S. Han, P.K. Varshney, J.Katz and A.Khalili "A pairwise key pre-distribution scheme for wireless sensor networks", *ACM Trans. Inf. Syst. Secur.*, vol. 8, pp. 228–258, 2005.

[14] H. Chan, A. Perrig and D. Song "Random key predistirbution schemes for sensor networks" *IEEE Sumposium on Security and Privacy*, pp. 197–213, 2003.

[15] S.A. Çamtepe, B. Yener and M. Yung "Expander graph based key distribution mechanisms in wireless sensor networks", *ICC '06, IEEE International Conference on Communications*, pp. 2262–2267, 2006.

[16] D. Liu, P. Ning and R. Li "Establishing pairwise keys in distributed sensor networks", *ACM Trans. Inf. Syst. Secur.*, vol. 8(1), pp. 41–77, 2005.

[17] S.W. Graham, "B_h sequences", *Analytic Number Theory, Vol. 1 (Allerton Park, IL, 1995)*, Birkhauser, Boston, pp. 431–449, 1996.

[18] H. Halberstam and K.F. Roth, *Sequences, Volume I*, London: OUP, 1966.

[19] B. Lindström, "On B_2 sequences of vectors", *J Combinatorial Theory*, vol. 4, pp. 261–265, 1972.

[20] K. O'Bryant, "A complete annotated bibliography of work related to Sidon sequences", *Electron. J. Combin* Dynamic Survey 11, 2004.

[21] R.C. Bose and S. Chowla, "Theorems in the additive theory of numbers", *Comment. Math. Helvet.* vol. 37, pp. 141–147, 1962–63.

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

[23] I.Z. Ruzsa "Solving a linear equation in a set of integers", *Acta Arith.*, vol. 65, pp. 259–282, 1993.

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

Simon R. Blackburn received his BSc in Mathematics from the University of Bristol in 1989, and his DPhil in Mathematics from the University of Oxford in 1992. Since then he has worked at Royal Holloway, University of London as a Research Assistant (1992-95), an Advanced Fellow (1995-2000), a Reader in Mathematics (2000-2003) and a Professor in Pure Mathematics (2004-). 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, Israel, in 1980, 1982, and 1984, respectively.

From 1984 he held a position in the department of Computer Science at the Technion, where he has a Professor position. During the years 1986-1987 he was 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, New Jersey. During the years 1994-1996 he was a Visiting Research Fellow in the Computer Science Department at Royal Holloway, University of London. He also had several visits to the Coordinated Science Laboratory at University of Illinois in Urbana-Champaign during the years 1995-1998, two visits to HP Bristol during the summers of 1996, 2000, several visits to the department of Electrical Engineering, University of California at San Diego during the years 2000-2009, and to the Mathematics department at Royal Holloway, University of London during the years 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 till 2009.

Keith M. Martin joined the Information Security Group at Royal Holloway, University of London as a lecturer in January 2000. He received his BSc (Hons) in Mathematics from the University of Glasgow in 1988 and a PhD from Royal Holloway in 1991. Between 1992 and 1996 he held a Research Fellowship in the Department of Pure Mathematics at the University of Adelaide, investigating mathematical modeling of cryptographic key distribution problems. In 1996 he joined the COSIC research group of the Katholieke Universiteit Leuven in 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. Keith's current research interests include cryptography, key management and wireless sensor network security.

Prof. Martin is an Associate Editor for Complexity and Cryptography for IEEE Transactions on Information Theory.

Maura B. Paterson received a BSc from the University of Adelaide in 2002 and a PhD from Royal Holloway, University of London in 2005. She has worked as a research assistant in the Information Security Group at Royal Holloway, and is currently at the Department of Economics, Mathematics and Statistics at Birkbeck, University of London. Her research interests include applications of combinatorics in information security.