Sequence Folding, Lattice Tiling, and Multidimensional Coding

Tuvi Etzion

Computer Science Department
Technion -Israel Institute of Technology
etzion@cs.technion.ac.il

Nanyang Technological University, Singapore, July, 2010

Distinct Difference Configuration

Definition

A set of dots in a grid is a distinct differences configuration (DDC) if the lines connecting pairs of dots are different either in length or in slope.

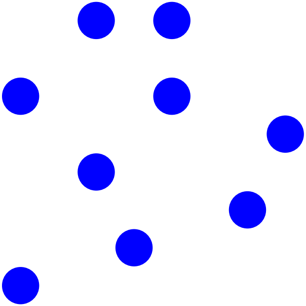
Motivation

These synchronization patterns have known applications in radar, sonar, physical alignment, and time-position synchronization.

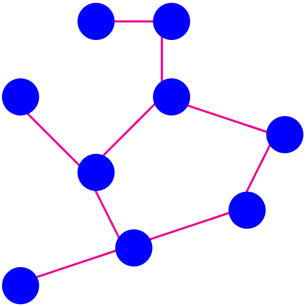
Outline

New Motivation – Wireless Sensor Networks

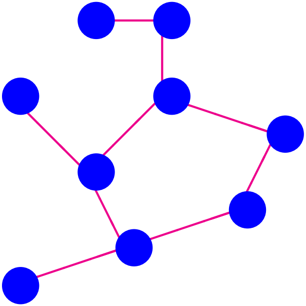
New Motivation – Wireless Sensor Networks



New Motivation – Wireless Sensor Networks

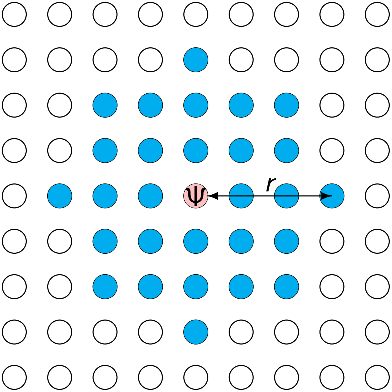


New Motivation – Wireless Sensor Networks

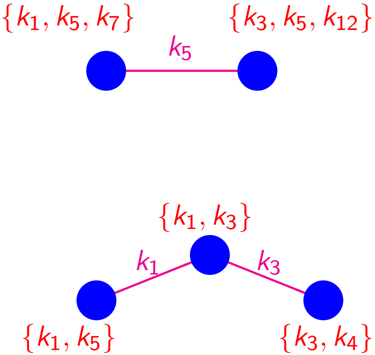


- restricted memory
- restricted battery power
- restricted computational ability

Grid-Based Wireless Sensor Networks



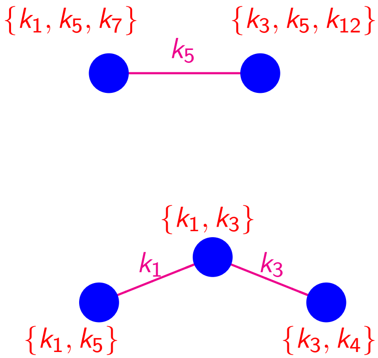
Key Predistribution



key predistribution scheme (KPS)

- nodes are assigned keys before deployment
- nodes that share keys can communicate securely
- two-hop path: nodes communicate via intermediate node

Key Predistribution

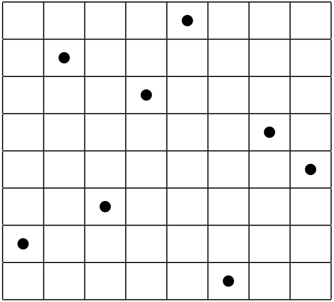


key predistribution scheme (KPS)

- nodes are assigned keys before deployment
- nodes that share keys can communicate securely
- two-hop path: nodes communicate via intermediate node

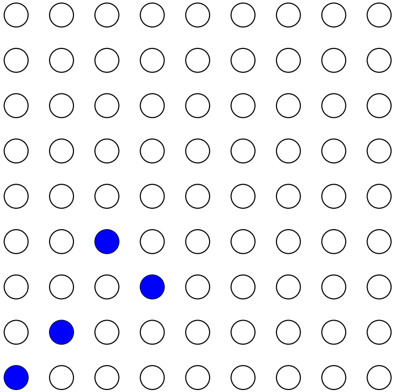
Observation: it is not necessary for two nodes to share more than one key

Costas Arrays

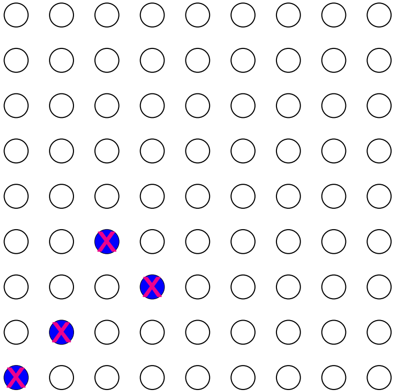


- one dot per row/column
- vector differences between dots are distinct

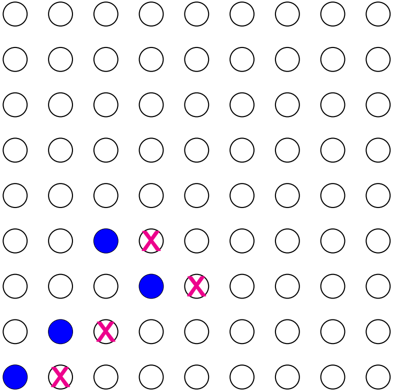
Translated Costas Arrays Overlap is at Most One



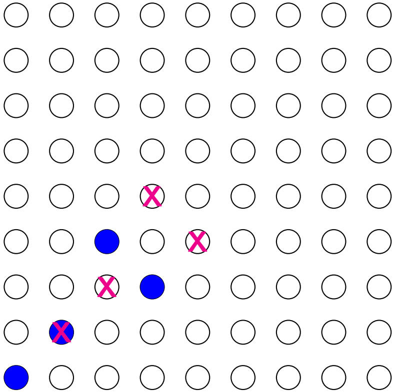
Translated Costas Arrays Overlap is at Most One



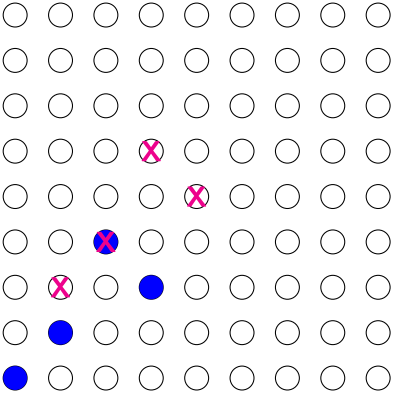
Translated Costas Arrays Overlap is at Most One



Translated Costas Arrays Overlap is at Most One

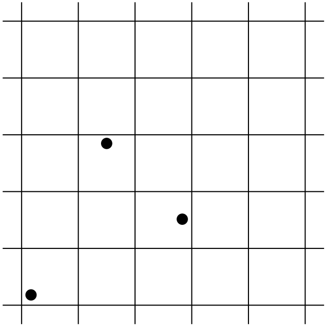


Translated Costas Arrays Overlap is at Most One



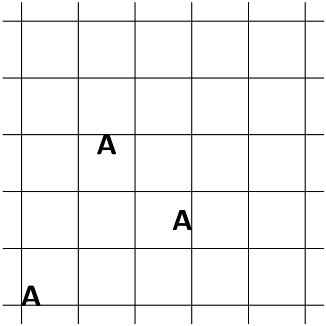
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



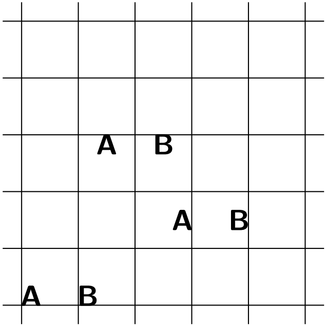
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



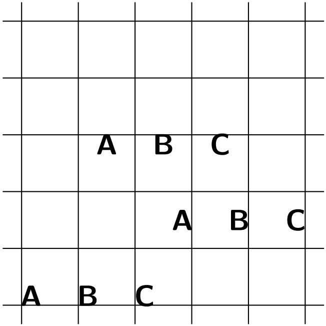
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



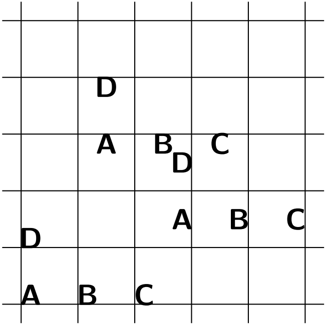
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



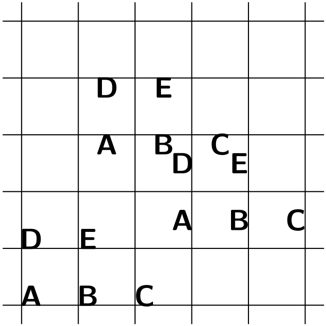
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



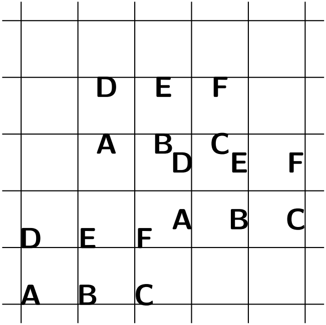
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



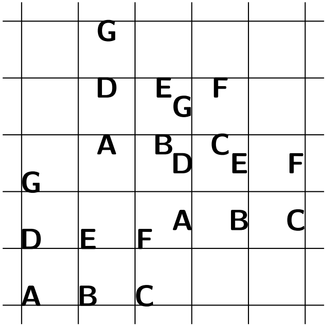
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



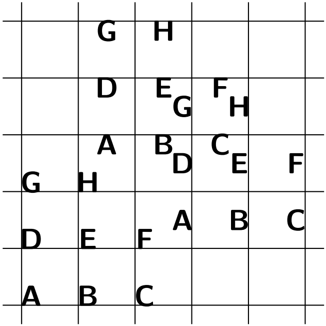
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



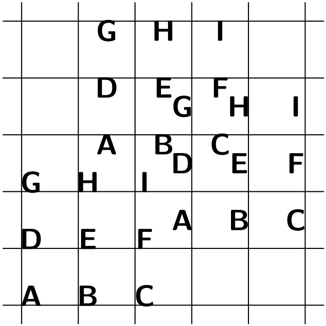
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$



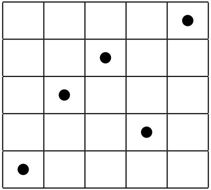
Key Predistribution Using Costas Arrays

- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

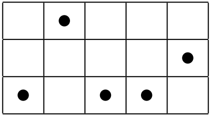


Classical Structures

A Costas array of order n is an $n \times n$ permutation array which is also a DDC.

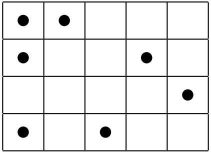


A sonar sequence in an $n \times k$ DDC with k dots, exactly one dot in each column.



Classical Structures

A Golomb rectangle in an $n \times k$ DDC with m dots.



New Definitions

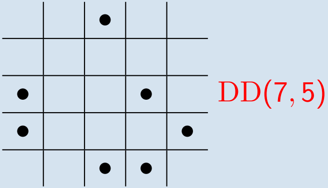
Definition (Distinct-Difference Configuration $\mathrm{DD}(m, r)$)

A 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:

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

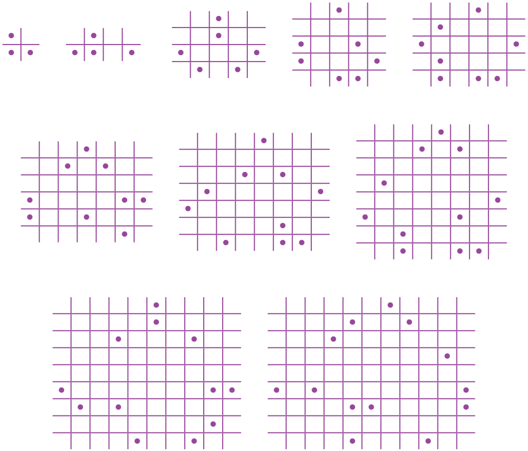
New Definitions – $\mathrm{DD}(m, r)$

Example (Distinct-Difference Configuration $\mathrm{DD}(7,5)$)



- can be used for key predistribution in the same way as a Costas array
- more general than a Costas array $\Rightarrow$ more flexible choice of parameters

$\mathrm{DD}(m,r)$ - **Optimal DDCs,** $r = 2, 3, \ldots, 11$



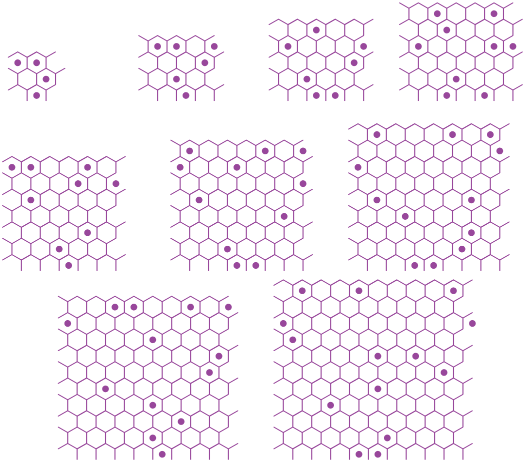
New Definitions

Definition (Distinct-Difference Configuration $\mathrm{DD}^*(m,r)$)

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

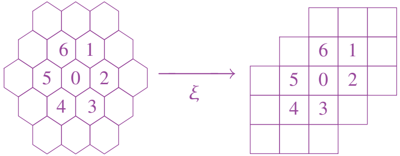
- Any two of the dots in the configuration are at hexagonal distance at most r apart.
- All the $\binom{m}{2}$ differences between pairs of dots are distinct either in length or in slope.

$\overline{\mathrm{DD}}^*(m, r)$ - Optimal DDCs, $r = 2, 3, \ldots, 10$



Translation from Square Grid to Hexagonal Grid

$$\xi(x,y) = \left(x + \frac{y}{\sqrt{3}}, \frac{2y}{\sqrt{3}}\right)$$



Anticodes

Definitions

An anticode of diameter r is a set $\mathcal{S}$ such that for each pair of elements $x, y \in \mathcal{S}$ we have $d(x, y) \leq r$.

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 $x \notin \mathcal{S}$.

Lemma

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

Size of Maximal Anticodes

Lemma

The size of a maximal anticode of diameter r in the square grid is at most $\frac{1}{2}r^2 + O(r)$.

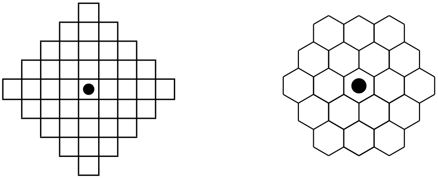
Lemma

The size of a maximal anticode of diameter r in the hexagonal grid is at most $\frac{3}{4}r^2 + O(r)$.

Lee spheres with radius R and hexagonal spheres with radius R corresponds to maximal anticodes with the largest size in the square grid and the hexagonal grid, respectively.

Maximal Anticodes with Maximum Size

- Lee sphere with radius 4.
- Hexagonal sphere with radius 2.



Upper Bounds on the Number of Dots

Theorem

In any given $\mathrm{DD}(m, r)$ *we have*

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

Theorem

For any given $\mathrm{DD}^*(m, r)$ *we have*

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

Upper Bounds – Sketch of Proof

Lemma

Let r be a non-negative 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 $\mathcal{A}$ non-trivially. Then $w \leq \frac{1}{2}(r + 2\ell)^2 + O(r)$.

Upper Bounds – Sketch of Proof

- Let $\ell = c \cdot \sqrt{r}$, c large.
- Number of small Lee spheres $w = \frac{1}{2}r^2 + O(r)$.
- Area of a small Lee sphere $a = 2\ell^2 + 2\ell + 1$.
- Average number of dots per small Lee sphere $\mu = \frac{am}{w}$.
- Let m_i be the number of dots in the ith small Lee sphere.
- Number of vectors in the small Lee spheres $\sum_{i=1}^{w} m_i(m_i - 1)$.
- Number of possible vectors $a(a-1)$, each one can be counted at most once.
- Lower bound on the number of counted vectors $w\mu(\mu - 1)$.

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

Consequence : $m \leq \frac{1}{\sqrt{2}}r + o(r)$.

Upper Bounds on the Number of Dots

Theorem

The number of dots in a DDC whose shape is a regular polygon (a circle, a rectangle, an hexagon with two parallel edges and four equal angles to these edges) with area s is at most $\sqrt{s} + o(\sqrt{s})$.

In the sequel, we assume that the radius of the circle or the regular polygons is R (the *radius* is the distance from the center of the regular polygon to any one its vertices).

Periodic Configurations

Definition

Let $\mathcal{A}$ be an 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 $\kappa \times \eta$ sub-array 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 $n \times k$ sub-array of $\mathcal{A}$ is a DDC.

Periodic Configurations

Construction (Periodic Welch)

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 $\alpha^i \equiv j \pmod{p}$.

Theorem

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 $1/p$.

Periodic Configurations

Construction (Periodic Golomb)

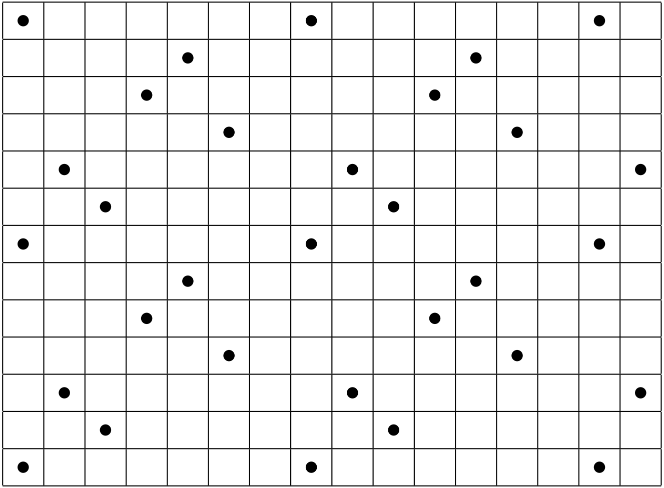
Let α and β be two primitive elements in GF(q), where q is a prime power. For any integers i and j, there is a dot in $\mathcal{A}(i,j)$ if and only if $\alpha^i + \beta^j = 1$.

Theorem

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 $(q-2)/(q-1)^2$.

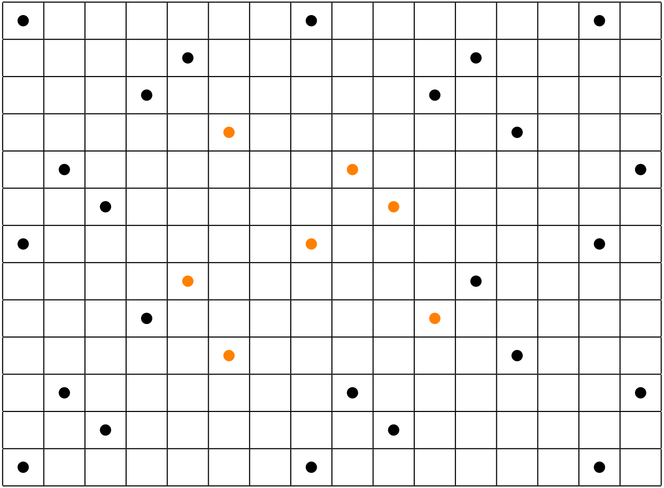
Periodic Configuration – an Example

Each 7×7 array is a DDC



Periodic Configuration – an Example

Each 7×7 array is a DDC



Lower Bounds – General technique

Definition ($\mathcal{S}$-DDC)

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.

Lemma

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.

Theorem

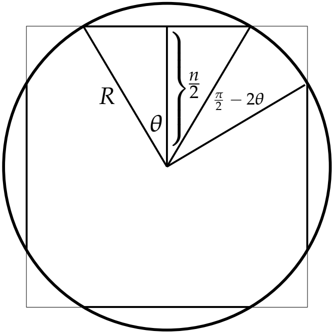
Let $\mathcal{S}$ be a shape, and let $\mathcal{A}$ be a doubly periodic $\mathcal{S}$-DDC of density δ. Then there exists a set of at least $\lceil \delta|\mathcal{S}| \rceil$ dots contained in $\mathcal{S}$ that form a DDC.

Lower Bounds – Circle

Theorem (Blackburn, Etzion, Martin, Paterson 2008)

There exists a circle with diameter r which is a DDC with at least $0.80795r - o(r)$ dots.

- $r = 2R$
- area of circle inside square $2R^2((\pi/2) - 2\theta + \sin 2\theta)$

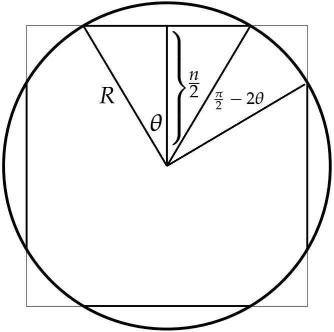


Lower Bounds – Circle

Theorem (Blackburn, Etzion, Martin, Paterson 2008)

There exists a circle with diameter r which is a DDC with at least $0.80795r - o(r)$ dots.

- $r = 2R$
- area of circle inside square $2R^2((\pi/2) - 2\theta + \sin 2\theta)$
- density $1/n = 1/(2R\cos\theta)$

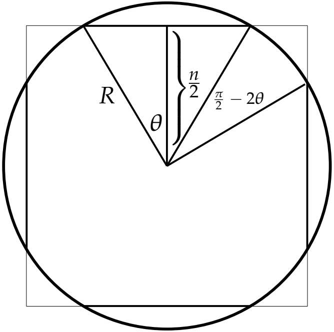


Lower Bounds – Circle

Theorem (Blackburn, Etzion, Martin, Paterson 2008)

There exists a circle with diameter r which is a DDC with at least $0.80795r - o(r)$ dots.

- $r = 2R$
- area of circle inside square $2R^2((\pi/2) - 2\theta + \sin 2\theta)$
- density $1/n = 1/(2R\cos\theta)$
- lower bound is the maximum of $R((\pi/2) - 2\theta + \sin 2\theta)/\cos\theta$

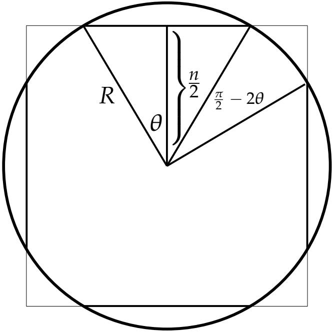


Lower Bounds – Circle

Theorem (Blackburn, Etzion, Martin, Paterson 2008)

There exists a circle with diameter r which is a DDC with at least $0.80795r - o(r)$ dots.

- $r = 2R$
- area of circle inside square $2R^2((\pi/2) - 2\theta + \sin 2\theta)$
- density $1/n = 1/(2R\cos\theta)$
- lower bound is the maximum of $R((\pi/2) - 2\theta + \sin 2\theta)/\cos\theta$
- maximum is attained for $\theta \approx 0.41586$.



Folding Along Rows

A Golomb ruler of length 17 and order 6 : $\{0, 1, 4, 10, 12, 17\}$.

•	•			•						•		•					•

15	16	17	18	19
10	11	12	13	14
5	6	7	8	9
0	1	2	3	4

		•		
•		•		
•	•			•

Folding Along Diagonals

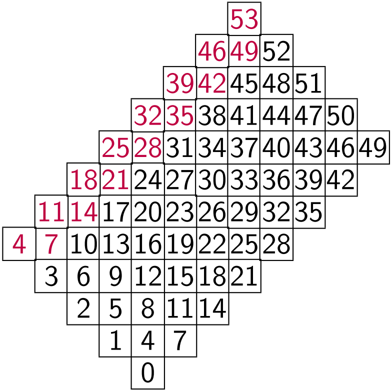
m-sequence : 000111101011001.

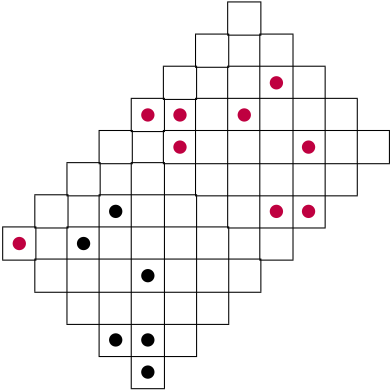
0	6	12	3	9	0
5	11	2	8	14	5
10	1	7	13	4	10
0	6	12	3	9	0

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

Periodic Configurations – Folding Along Diagonals

B_2-sequence in $\mathbb{Z}_{31}$: $\{0, 1, 4, 10, 12, 17\}$.





Tiling and Lattices

Definition (Tiling)

A D-dimensional shape $\mathcal{S}$ tiles the D-dimensional space $\mathbb{Z}^D$ if disjoint copies of $\mathcal{S}$ cover $\mathbb{Z}^D$. This cover of $\mathbb{Z}^D$ with disjoint copies of $\mathcal{S}$ is called *tiling* of $\mathbb{Z}^D$ with $\mathcal{S}$.

Tiling

Definition (Center)

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

Lemma

For a given tiling $(\mathcal{T}, \mathcal{S})$ *and a point* $(i_1, i_2, \ldots, i_D)$ *the point* $(i_1, i_2, \ldots, i_D) - c(i_1, i_2, \ldots, i_D)$ *belongs to the shape* $\mathcal{S}$ *whose center is in the origin.*

Lattices

Definition (Lattice)

A *lattice* Λ is a discrete, additive subgroup of the real D-space $\mathbb{R}^D$.

$$\Lambda = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_D v_D \ : \ \alpha_1, \ldots, \alpha_D \in \mathbb{Z}\} \ ,$$

where $\{v_1, \ldots, v_D\}$ is a set of linearly independent vectors in $\mathbb{R}^D$. A lattice Λ is a sublattice of $\mathbb{Z}^D$ if and only if $\{v_1, \ldots, v_D\} \subset \mathbb{Z}^D$. The vectors $v_1, \ldots, v_D$ are the *basis* for Λ. The $D \times D$ matrix

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

where $v_i = (v_{i1}, \ldots, v_{iD})$ is the *generator matrix* for Λ.

Lattices

Definition (Volume of a Lattice)

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

$$\Pi(\Lambda) \stackrel{\text{def}}{=} \{\xi_1 v_1 + \xi_2 v_2 + \cdots + \xi_D v_D : 0 \leq \xi_i < 1, \ , 1 \leq i \leq D\} \ .$$

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

Tiling and Lattices

Definition (Lattice Tiling)

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

Generalization of Folding

Definition (Ternary Vector)

A *ternary vector* of length D, $(d_1, d_2, \ldots, d_D)$, is a word of length D, where $d_i \in \{-1, 0, +1\}$.

Generalization of Folding

Definition (Ternary Vector)

A *ternary vector* of length D, $(d_1, d_2, \ldots, d_D)$, is a word of length D, where $d_i \in \{-1, 0, +1\}$.

Definition (Folded-Row)

Let $\mathcal{S}$ be a D-dimensional shape and let $\delta = (d_1, d_2, \ldots, d_D)$ be a nonzero ternary vector of length D (or any nonzero integer vector). Let $(\mathcal{T}, \mathcal{S})$ be a lattice tiling induced by a D-dimensional lattice Λ, and let $\tilde{\mathcal{S}}$ be the copy of $\mathcal{S}$ in $(\mathcal{T}, \mathcal{S})$ which includes the origin.

Generalization of Folding

Definition (Ternary Vector)

A *ternary vector* of length D, $(d_1, d_2, \ldots, d_D)$, is a word of length D, where $d_i \in \{-1, 0, +1\}$.

Definition (Folded-Row)

Let $\mathcal{S}$ be a D-dimensional shape and let $\delta = (d_1, d_2, \ldots, d_D)$ be a nonzero ternary vector of length D (or any nonzero integer vector). Let $(\mathcal{T}, \mathcal{S})$ be a lattice tiling induced by a D-dimensional lattice Λ, and let $\tilde{\mathcal{S}}$ be the copy of $\mathcal{S}$ in $(\mathcal{T}, \mathcal{S})$ which includes the origin. We define recursively a *folded-row* starting in the origin. If the point $(i_1, i_2, \ldots, i_D)$ is in $\tilde{\mathcal{S}}$ then the next point on its folded-row is:

Generalization of Folding

Definition (Ternary Vector)

A *ternary vector* of length D, $(d_1, d_2, \ldots, d_D)$, is a word of length D, where $d_i \in \{-1, 0, +1\}$.

Definition (Folded-Row)

Let $\mathcal{S}$ be a D-dimensional shape and let $\delta = (d_1, d_2, \ldots, d_D)$ be a nonzero ternary vector of length D (or any nonzero integer vector). Let $(\mathcal{T}, \mathcal{S})$ be a lattice tiling induced by a D-dimensional lattice Λ, and let $\tilde{\mathcal{S}}$ be the copy of $\mathcal{S}$ in $(\mathcal{T}, \mathcal{S})$ which includes the origin. We define recursively a *folded-row* starting in the origin. If the point $(i_1, i_2, \ldots, i_D)$ is in $\tilde{\mathcal{S}}$ then the next point on its folded-row is:

- If the point $(i_1 + d_1, i_2 + d_2, \ldots, i_D + d_D)$ is in $\tilde{\mathcal{S}}$ then it is the next point on the folded-row.

Generalization of Folding

Definition (Ternary Vector)

A *ternary vector* of length D, $(d_1, d_2, \ldots, d_D)$, is a word of length D, where $d_i \in \{-1, 0, +1\}$.

Definition (Folded-Row)

Let $\mathcal{S}$ be a D-dimensional shape and let $\delta = (d_1, d_2, \ldots, d_D)$ be a nonzero ternary vector of length D (or any nonzero integer vector). Let $(\mathcal{T}, \mathcal{S})$ be a lattice tiling induced by a D-dimensional lattice Λ, and let $\tilde{\mathcal{S}}$ be the copy of $\mathcal{S}$ in $(\mathcal{T}, \mathcal{S})$ which includes the origin. We define recursively a *folded-row* starting in the origin. If the point $(i_1, i_2, \ldots, i_D)$ is in $\tilde{\mathcal{S}}$ then the next point on its folded-row is:

- If the point $(i_1 + d_1, i_2 + d_2, \ldots, i_D + d_D)$ is in $\tilde{\mathcal{S}}$ then it is the next point on the folded-row.
- If the point $(i_1 + d_1, i_2 + d_2, \ldots, i_D + d_D)$ is in $\tilde{\mathcal{S}}' \neq \tilde{\mathcal{S}}$ whose center is $(c_1, \ldots, c_D)$ then $(i_1 + d_1 - c_1, \ldots, i_D + d_D - c_D)$ is the next point on the folded-row.

Generalization of Folding

Definition (Folding)

The triple $(\Lambda, \mathcal{S}, \delta)$ defines a *folding* if the definition yields a folded-row which includes all the elements of $\mathcal{S}$.

Generalization of Folding

Theorem

Let d_1, d_2 be two positive integers, $\tau = g.c.d.(d_1, d_2)$. Let Λ be a lattice tiling, for the shape $\mathcal{S}$, whose generator matrix is given by

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

Then the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding

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

Application to Pseudo-Random Arrays

m-sequence : 000111101011001.

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

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

Rulers and B_2-Sequences

Definition (ruler)

Let $D = \{a_1, a_2, \dots, a_m\}$ be a sequence of m distinct integers, $a_1 = 0,\ a_i < a_{i+1}$. We say that D is a ruler if the differences $a_{i_2} - a_{i_1}$ with $1 \leq i_1 < i_2 \leq m$ are distinct.

Definition (B_2-sequence)

Let A be an abelian group, and let $D = \{a_1, a_2, \dots, a_m\} \subseteq A$ 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.

Lemma

A subset $D = \{a_1, a_2, \dots, a_m\} \subseteq A$ 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.

B_2-sequences and DDCs

Theorem (Bose 1942)

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 $m = q$.

Theorem

Let Λ be a lattice, $\mathcal{S}$, $n = |\mathcal{S}|$, a D-dimensional shape, and δ a direction. Let E be a B_2-sequence over $\mathbb{Z}_n$. If $(\Lambda, \mathcal{S}, \delta)$ defines a folding then the folded-row, with E in it, is a D-dimensional DDC. Moreover, this DDC can be extended to doubly periodic $\mathcal{S}$-DDC.

Euclid and Dirichlet's Thorems

Theorem (Euclid's Theorem)

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

Theorem (Dirichlet's Theorem)

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

Bounds for Specific Shapes

Theorem

For each positive number γ there exist two integers a and b such that $\frac{b}{a} \approx \gamma$ and an infinite $\mathcal{S}$-DDC with $\sqrt{a \cdot b}R + o(R)$ dots whose shape is an $n_1 \times n_2 = (bR + o(R)) \times (aR + o(R))$ rectangle, $n_1 n_2 = p^2 - 1$ for some prime p, and n_1 is even.

Proof.

Let α, β be two integers such that $\frac{\beta}{\alpha} \approx \sqrt{\gamma}$ and $\text{g.c.d.}(\alpha, \beta) = 2$. By Euclid's Theorem there exist two integers c_α, c_β such that either $c_\alpha \alpha + 2 = c_\beta \beta > 0$ or $c_\beta \beta + 2 = c_\alpha \alpha > 0$. W.l.o.g. assume $c_\alpha \alpha + 2 = c_\beta \beta > 0$. Let p be a prime of the form $\alpha\beta R + c_\alpha \alpha + 1$ (implied by Dirichlet's Theorem since $(\alpha\beta, c_\alpha \alpha + 1) = 1$). Now, $p^2 - 1 = (p+1)(p-1) = (\alpha\beta R + c_\alpha \alpha + 2)(\alpha\beta R + c_\alpha \alpha) = (\alpha\beta R + c_\beta \beta)(\alpha\beta R + c_\alpha \alpha) = (\alpha^2 R + \alpha c_\beta)(\beta^2 R + \beta c_\alpha)$. Thus, a $(\beta^2 R + \beta c_\alpha) \times (\alpha^2 R + \alpha c_\beta)$ rectangle fulfill our requirements. □

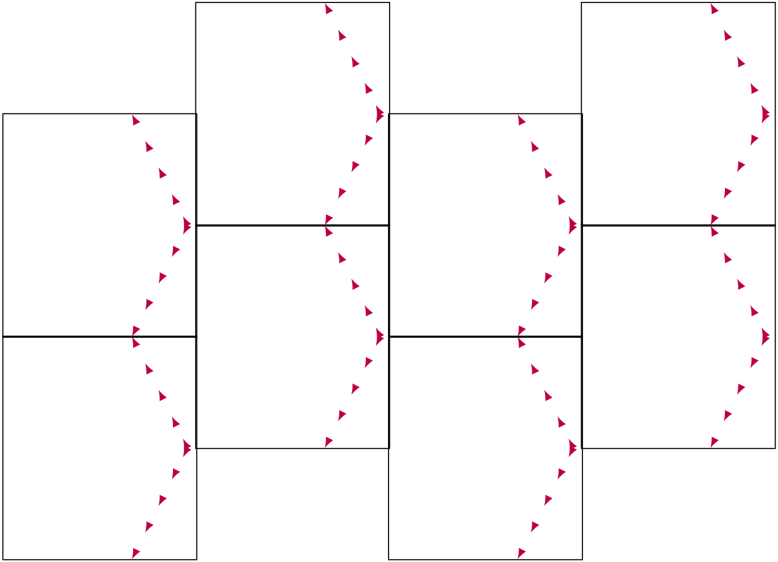
Bound for Regular Hexagon

There exists an infinite $\mathcal{S}$-DCC, where $\mathcal{S}$ is an $\alpha \times \beta = (\sqrt{3}R + o(R)) \times (\frac{3}{2}R + o(R))$ rectangle, such that $\alpha\beta = p^2 - 1$ for some prime p, and $\text{g.c.d.}(\alpha, \beta) = 2$. Let Λ be the a lattice tiling for $\mathcal{S}$ with the generator matrix

$$G = \begin{bmatrix} \beta & \frac{\alpha}{2} + \theta \\ 0 & \alpha \end{bmatrix},$$

where $\theta = 1$ if $\alpha \equiv 0 \ (mod\ 4)$ and $\theta = 2$ if $\alpha \equiv 2 \ (mod\ 4)$. There is a folded-row for Λ and $\mathcal{S}$ with $\delta = (+1, 0)$. We now can form an infinite $\mathcal{S}'$-DCC, where $\mathcal{S}'$ is a regular hexagon with radius $\frac{2}{3}\beta = R + o(R)$ and $\sqrt{a \cdot b}R + o(R)$ dots. Hence, a lower bound on the number of dots in $\mathcal{S}'$ is approximately $\frac{\sqrt{3\sqrt{3}}}{\sqrt{2}}R + o(R)$. The area of $\mathcal{S}'$ is $\frac{3\sqrt{3}}{2}R^2 + o(R^2)$.

Bound for Hexagon



Bounds for Specific Shapes

Theorem

Assume we are given an doubly periodic $\mathcal{S}$-DDC with m dots on the grid. Let $\mathcal{Q}$ be another shape on the grid. Then there exists a copy of $\mathcal{Q}$ on the grid with at least $\frac{m}{|\mathcal{S}|}|\mathcal{S} \cap \mathcal{Q}|$ dots.

Bounds – Summarize

Table: Bounds on the number of dots in an n-gon DDC

n	upper bound	lower bound	ratio between bounds
3	$1.13975R$	$1.02462R$	0.899
4	$1.41421R$	$1.41421R$	1
5	$1.54196R$	$1.45992R$	0.9468
6	$1.61185R$	$\approx 1.61185R$	≈ 1
7	$1.65421R$	$1.58844R$	0.960241
8	$1.68179R$	$1.62625R$	0.966977
9	$1.70075R$	$1.63672R$	0.96235
10	$1.71433R$	$1.65141R$	0.963297
60	$1.77083R$	$1.70658R$	0.963718
96	$1.77182R$	$1.70752R$	0.96371
circle	$1.77245R$	$1.70813R$	0.963708

THANK YOU