Distinct Difference Configurations

Simon R. Blackburn
Joint work with:
Tuvi Etzion, Keith M. Martin, Maura B. Paterson

Royal Holloway, University of London

16th July 2009

Distinct Difference Configurations

Definition

A distinct difference configuration with m dots is a set $\{v_1, v_2, \ldots, v_m\} \subseteq \mathbb{Z}^2$ such that the differences $v_i - v_j$ for $i \neq j$ are all distinct.

We abbreviate the above to $\mathrm{DD}(m)$.

Royal Holloway University of London

Distinct Difference Configurations

Definition

A distinct difference configuration with m dots is a set $\{v_1, v_2, \ldots, v_m\} \subseteq \mathbb{Z}^2$ such that the differences $v_i - v_j$ for $i \neq j$ are all distinct.

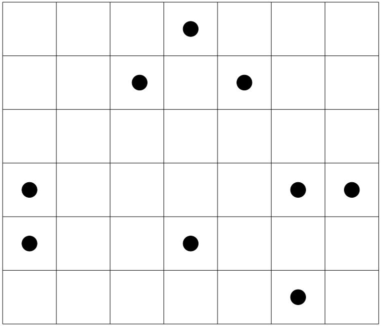
We abbreviate the above to $\mathrm{DD}(m)$.

So $\{(0,0),(1,0),(0,1)\}$ is a $\mathrm{DD}(3)$ with differences given by:

	$(0,0)$	$(1,0)$	$(0,1)$
$(0,0)$		$(1,0)$	$(0,1)$
$(1,0)$	$(-1,0)$		$(-1,1)$
$(0,1)$	$(0,-1)$	$(1,-1)$	

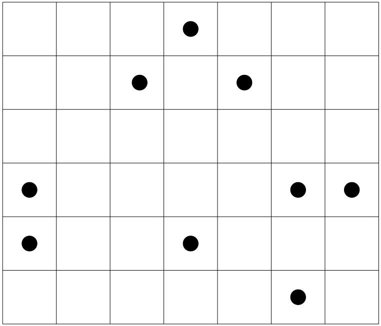
Distinct Difference Configurations

The following is a $\mathrm{DD}(9)$:



Distinct Difference Configurations

The following is a $\mathrm{DD}(9)$:



All pairs of dots are at distance at most 7. This is the largest such example.

Distinct Difference Configurations

Definition

A distinct difference configuration with m dots of diameter d is a $\mathrm{DD}(m)$ such that $|v_i - v_j| \leq d$ for all i, j.

So any pair of dots is at distance d or less.

- We abbreviate this to $\mathrm{DD}(m, d)$.
- The example above is a $\mathrm{DD}(9, 7)$.

Distinct Difference Configurations

Definition

A distinct difference configuration with m dots of diameter d is a $\mathrm{DD}(m)$ such that $|v_i - v_j| \leq d$ for all i, j.

So any pair of dots is at distance d or less.

- We abbreviate this to $\mathrm{DD}(m, d)$.
- The example above is a $\mathrm{DD}(9, 7)$.

Main combinatorial question

When d is fixed, how big can m be?

Royal Holloway
University of London

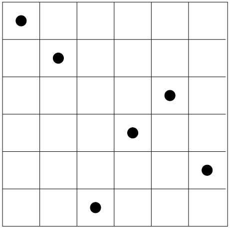
Motivation

- Key predistribution schemes in Wireless Sensor Networks.

Motivation

- Key predistribution schemes in Wireless Sensor Networks.
- A 2 dimensional generalisation of B_2-sequences.

Some constructions



Definition

An $n \times n$ Costas array is a $\mathrm{DD}(n)$ contained in $\{0, 1, \ldots, n-1\}^2$ with no pair of dots parallel with the x-axis, and no pair of points parallel with the y-axis.

Costas arrays

There exist several constructions of Costas arrays.

For example let p be a prime. Let α be a primitive root mod p.

Construction

Let $n = p - 2$. Put a dot in position (i, j) when $\alpha^{i+1} + \alpha^{j+1} = 1$. Then the dots form an $n \times n$ Costas array.

Royal Holloway University of London

A lower bound on m

Costas arrays give:

Theorem

There exists a $\mathrm{DD}(m,d)$ *with* $m = \frac{1}{\sqrt{2}}d - o(d) \approx 0.70711d$.

Proof: Place an $n \times n$ square in a circle of diameter d. $\square$

A corresponding upper bound

In fact we have an explicit construction such that:

Theorem

There exists a $\mathrm{DD}(m, d)$ *with* $m \approx 0.80795d$.

Royal Holloway University of London

A corresponding upper bound

In fact we have an explicit construction such that:

Theorem

There exists a $\mathrm{DD}(m,d)$ *with* $m \approx 0.80795d$.

Theorem

A $\mathrm{DD}(m,d)$ *must satisfy* $m \leq (\sqrt{\pi}/2)d + o(d) \approx 0.88623d$.

A new distance measure

A $\overline{\mathrm{DD}}(m, d)$ is a $\mathrm{DD}(m)$ in which every pair of dots are at Manhattan distance at most d.

A new distance measure

A $\overline{\mathrm{DD}}(m,d)$ is a $\mathrm{DD}(m)$ in which every pair of dots are at Manhattan distance at most d.

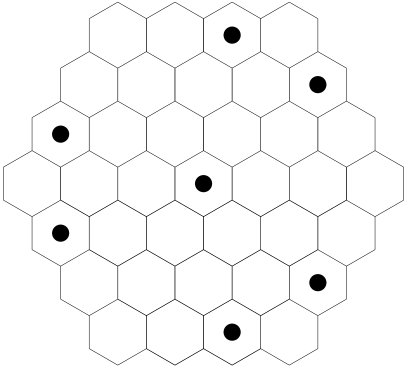
Theorem

There exists a $\overline{\mathrm{DD}}(m,d)$ *with* $m=(1/\sqrt{2})d-o(d)$. *Moreover, in any* $\overline{\mathrm{DD}}(m,d)$ *we have that* $\overline{\mathrm{DD}}(m,d)\leq(1/\sqrt{2})d+o(d)$.

Royal Holloway University of London

A new grid

A $\mathrm{DD}^*(m)$ is a set of vectors in the hexagonal grid whose differences are all distinct.



The hexagonal grid

If all pairs of dots are within Euclidean distance d, we have a $\mathrm{DD}^*(m, d)$.

Theorem

There exists a $\mathrm{DD}^*(m, d)$ *with* $m = 0.86819d - o(d)$. *In any* $\mathrm{DD}^*(m, d)$ *we have that* $\overline{\mathrm{DD}}(m, d) \leq 0.95231d + o(d)$.

Royal Holloway University of London

The hexagonal grid

If all pairs of dots are within Euclidean distance d, we have a $\mathrm{DD}^*(m, d)$.

Theorem

There exists a $\mathrm{DD}^*(m, d)$ *with* $m = 0.86819d - o(d)$. *In any* $\mathrm{DD}^*(m, d)$ *we have that* $\overline{\mathrm{DD}}(m, d) \leq 0.95231d + o(d)$.

Open Problem

Close this gap.

Hexagonal distance

If we replace Euclidean distance by hexagonal distance we call the resulting object a $\overline{\mathrm{DD}}^*(m, d)$.

Theorem

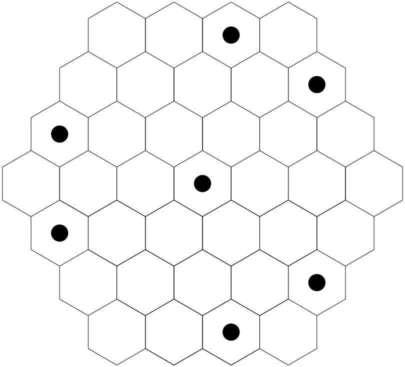
There exists a $\overline{\mathrm{DD}}^*(m, d)$ *with* $m = 0.79444d - o(d)$. *In any* $\mathrm{DD}^*(m, d)$ *we have that* $\overline{\mathrm{DD}}(m, d) \leq 0.86603d + o(d)$.

Royal Holloway University of London

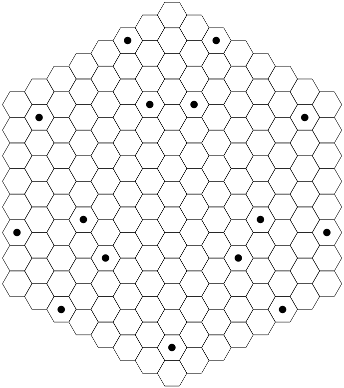
Honeycomb arrays

Definition (Golomb and Taylor 1984)

A honeycomb array of radius r is a $\mathrm{DD}^*(2r+1)$ contained in a hexagonal sphere of radius r, with the property that there is exactly one dot in every 'row', where 'rows' go in three directions.



A radius 7 honeycomb array



Honeycomb arrays

Honeycomb arrays are known to exist for $r = 0, 1, 3, 4, 7, 10, 13$ and 22.

Theorem (Anastasia Panoui, 2009)

This list is complete for $r \leq 13$.

Royal Holloway University of London

Honeycomb arrays

Honeycomb arrays are known to exist for $r = 0, 1, 3, 4, 7, 10, 13$ and 22.

Theorem (Anastasia Panoui, 2009)

This list is complete for $r \leq 13$.

A Honeycomb array is a $\overline{\mathrm{DD}}^*(m, d)$ where $m = 2r + 1$ and $d = 2r$.
But we know that $m \leq 0.86603d + o(d)$.
So there are only finitely many honeycomb arrays!

Royal Holloway University of London

Honeycomb arrays

Honeycomb arrays are known to exist for $r = 0, 1, 3, 4, 7, 10, 13$ and 22.

Theorem (Anastasia Panoui, 2009)

This list is complete for $r \leq 13$.

A Honeycomb array is a $\overline{\mathrm{DD}}^*(m, d)$ where $m = 2r + 1$ and $d = 2r$.
But we know that $m \leq 0.86603d + o(d)$.
So there are only finitely many honeycomb arrays!

Theorem

Honeycomb arrays of radius r do not exist when $r \geq 644$.

Royal Holloway
University of London

Some links

This talk will appear soon on my homepage:

http://www.ma.rhul.ac.uk/sblackburn

Our preprint 'Two-dimensional patterns with distinct differences – Constructions, Bounds and Maximal Anticodes' is available at:

http://arxiv.org/abs/0811.3832

The following preprint explores other combinatorial properties motivated by our WSN key predistribution scheme:

http://arxiv.org/abs/0811.3896

Royal Holloway University of London