Using Galois Rings to construct DRADs

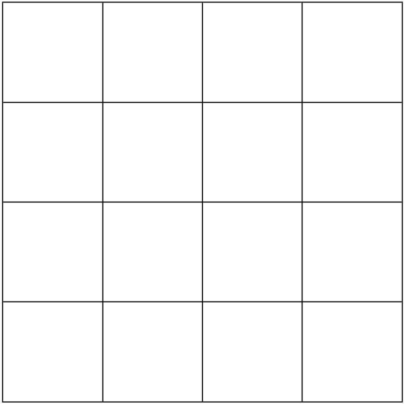
James Davis[1] John Polhill[2]

[1]Department of Mathematics and Computer Science
University of Richmond

[2]Department of Mathematical Sciences
Bloomsburg University

Finite Fields and their Applications, July 13, 2009

McFarland/Dillon difference sets



McFarland/Dillon difference sets

	♭		♭

McFarland/Dillon difference sets

	$\flat$		$\flat$
$\sharp$			
$\sharp$			

McFarland/Dillon difference sets

	♭	√	♭
♯			
√			
♯			

McFarland/Dillon difference sets

	$\flat$	$\surd$	$\flat$
$\sharp$			
$\surd$			
$\sharp$			

$$D = (1,0) + \langle (2,0) \rangle$$

McFarland/Dillon difference sets

	$\flat$	$\surd$	$\flat$
$\sharp$			
$\surd$			
$\sharp$			

$$D = (1,0) + \langle (2,0) \rangle \cup (0,1) + \langle (0,2) \rangle$$

McFarland/Dillon difference sets

	♭	√	♭
♯			
√			
♯			

$$D = (1,0) + \langle(2,0)\rangle \cup (0,1) + \langle(0,2)\rangle \cup (2,0) + \langle(2,2)\rangle$$

Other choices of coset representatives

	$\surd$	$\sharp$	
	$\flat$		$\flat$
		$\sharp$	$\surd$

$$D = (1,2) + \langle (2,0) \rangle \cup (2,1) + \langle (0,2) \rangle \cup (1,1) + \langle (2,2) \rangle$$

Special session on Association Schemes

Find a difference set with the following properties:

- $D \cap D^{(-1)} = \emptyset$

Special session on Association Schemes

Find a difference set with the following properties:

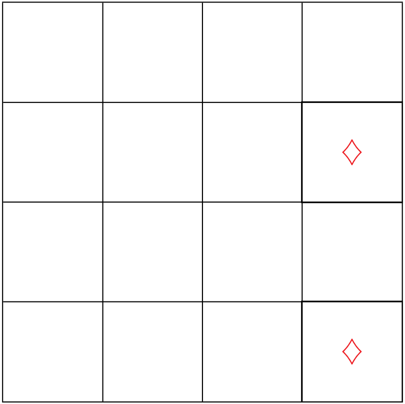
- $D \cap D^{(-1)} = \emptyset$
- $G - (D \cup D^{(-1)}) = H$

Special session on Association Schemes

Find a difference set with the following properties:

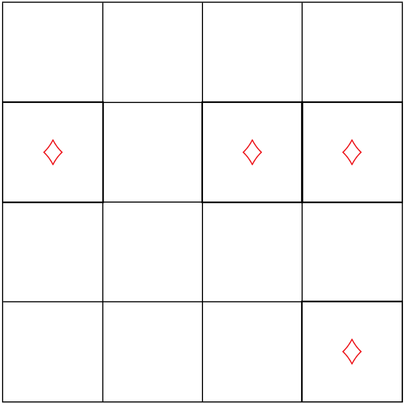
- $D \cap D^{(-1)} = \emptyset$
- $G - (D \cup D^{(-1)}) = H$
- D should be a $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$ Hadamard difference set

Napkin work



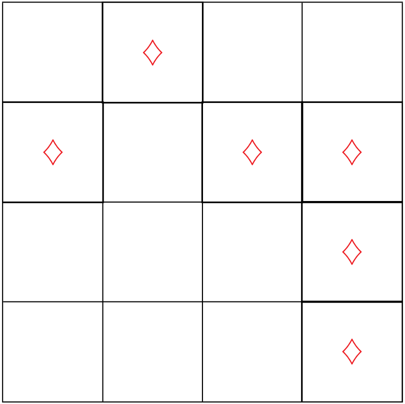
$$D = (3,3) + \langle(2,0)\rangle$$

Napkin work



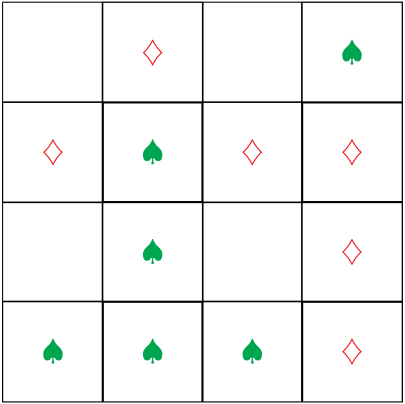
$$D = (3,3) + \langle (2,0) \rangle \cup \mathbf{(1,0)} + \langle \mathbf{(0,2)} \rangle$$

Napkin work



$$D = (3,3) + \langle (2,0) \rangle \cup (1,0) + \langle (0,2) \rangle \cup \mathbf{(0,1)} + \langle \mathbf{(2,2)} \rangle$$

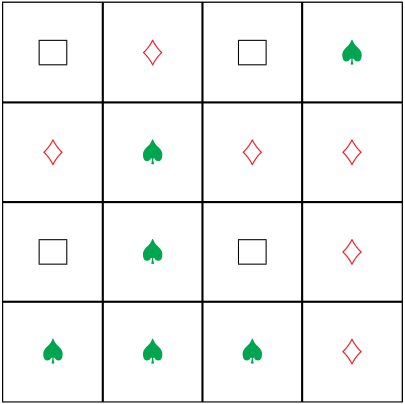
Napkin work



$$D = (3,3) + \langle (2,0) \rangle \cup$$
$$(1,0) + \langle (0,2) \rangle \cup \mathbf{(0,1)} + \langle \mathbf{(2,2)} \rangle$$

$$D^{(-1)} = (1,1) + \langle (2,0) \rangle \cup$$
$$(3,0)\langle (0,2) \rangle \cup (0,3) + \langle (2,2) \rangle$$

Napkin work

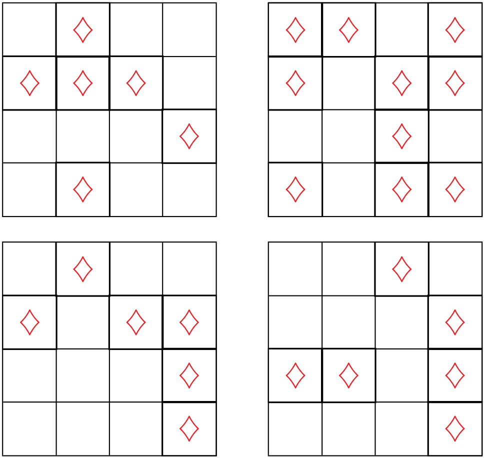


$$D = (3,3) + \langle (2,0) \rangle \cup$$
$$(1,0) + \langle (0,2) \rangle \cup \mathbf{(0,1)} + \langle \mathbf{(2,2)} \rangle$$

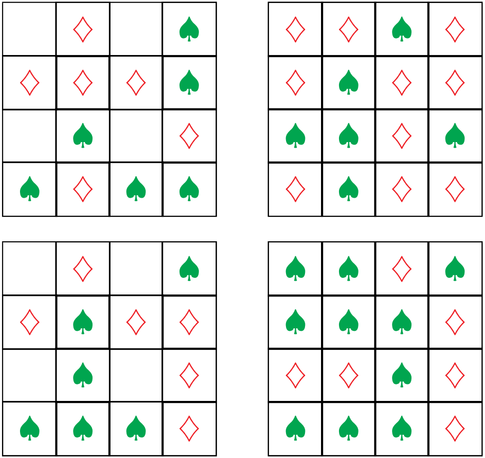
$$D^{(-1)} = (1,1) + \langle (2,0) \rangle \cup$$
$$(3,0)\langle (0,2) \rangle \cup (0,3) + \langle (2,2) \rangle$$

$$G - D - D^{(-1)} = \langle (2,0), (0,2) \rangle$$

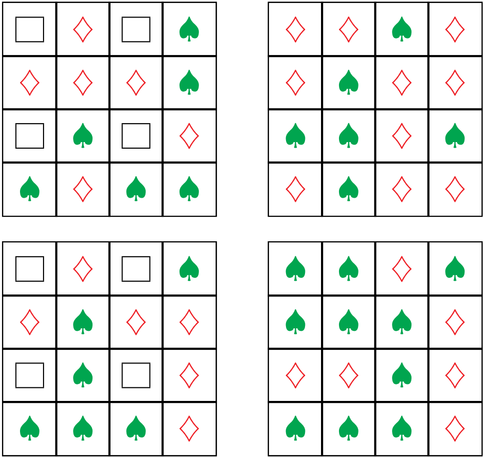
Harder work



Harder work



Harder work



Notation and examples

$GR(4,2) = \mathbb{Z}_4[\xi]$ where $\xi^2 + \xi + 1 = 0$ (could say $GR(4,2) = \mathbb{Z}_4[x]/\langle x^2 + x + 1 \rangle$).

Notation and examples

$GR(4,2) = \mathbb{Z}_4[\xi]$ where $\xi^2 + \xi + 1 = 0$ (could say $GR(4,2) = \mathbb{Z}_4[x]/\langle x^2 + x + 1\rangle$).

g_i	ξ^2	1	ξ
H_i	$\langle 2 \rangle$	$\langle 2\xi \rangle$	$\langle 2\xi^2 \rangle$

Notation and examples

$GR(4,2) = \mathbb{Z}_4[\xi]$ where $\xi^2 + \xi + 1 = 0$ (could say $GR(4,2) = \mathbb{Z}_4[x]/\langle x^2 + x + 1 \rangle$).

g_i	ξ^2	1	ξ
H_i	$\langle 2 \rangle$	$\langle 2\xi \rangle$	$\langle 2\xi^2 \rangle$

Correspondance: $(2,0) \longleftrightarrow 2; (0,2) \longleftrightarrow 2\xi; (2,2) \longleftrightarrow 2\xi^2$

Notation and examples

$GR(4,2) = \mathbb{Z}_4[\xi]$ where $\xi^2 + \xi + 1 = 0$ (could say $GR(4,2) = \mathbb{Z}_4[x]/\langle x^2 + x + 1\rangle$).

g_i	ξ^2	1	ξ
H_i	$\langle 2\rangle$	$\langle 2\xi\rangle$	$\langle 2\xi^2\rangle$

Correspondance: $(2,0) \longleftrightarrow 2; (0,2) \longleftrightarrow 2\xi; (2,2) \longleftrightarrow 2\xi^2$

$$D = (\xi^2 + \langle 2\rangle) \cup (1 + \langle 2\xi\rangle) \cup (\xi + \langle 2\xi^2\rangle)$$

Next size up

$GR(4,3) = \mathbb{Z}_4[\zeta]$ where $\zeta^3 + 2\zeta^2 + \zeta + 3 = 0$.

Next size up

$GR(4,3) = \mathbb{Z}_4[\zeta]$ where $\zeta^3 + 2\zeta^2 + \zeta + 3 = 0$.

g_i	ζ^6	1	ζ	$\cdots$	ζ^5
H_i	$\langle 2, 2\zeta \rangle$	$\langle 2\zeta, 2\zeta^2 \rangle$	$\langle 2\zeta^2, 2\zeta^3 \rangle$	$\cdots$	$\langle 2\zeta^6, 2 \rangle$

Next size up

$GR(4,3) = \mathbb{Z}_4[\zeta]$ where $\zeta^3 + 2\zeta^2 + \zeta + 3 = 0$.

g_i	ζ^6	1	ζ	$\cdots$	ζ^5
H_i	$\langle 2, 2\zeta \rangle$	$\langle 2\zeta, 2\zeta^2 \rangle$	$\langle 2\zeta^2, 2\zeta^3 \rangle$	$\cdots$	$\langle 2\zeta^6, 2 \rangle$

Correspondance:
$(2,0,0) \longleftrightarrow 2; (0,2,0) \longleftrightarrow 2\zeta; (0,0,2) \longleftrightarrow 2\zeta^2; \ldots$

Next size up

$GR(4,3) = \mathbb{Z}_4[\zeta]$ where $\zeta^3 + 2\zeta^2 + \zeta + 3 = 0$.

g_i	ζ^6	1	ζ	$\cdots$	ζ^5
H_i	$\langle 2, 2\zeta \rangle$	$\langle 2\zeta, 2\zeta^2 \rangle$	$\langle 2\zeta^2, 2\zeta^3 \rangle$	$\cdots$	$\langle 2\zeta^6, 2 \rangle$

Correspondance:
$(2,0,0) \longleftrightarrow 2; (0,2,0) \longleftrightarrow 2\zeta; (0,0,2) \longleftrightarrow 2\zeta^2; \ldots$

$$D = (\zeta^6 + \langle 2, 2\zeta \rangle) \cup (1 + \langle 2\zeta, 2\zeta^2 \rangle) \cup \cdots \cup (\zeta^5 + \langle 2\zeta^6, 2 \rangle)$$

General construction

Theorem

Let $GR(4,t) = \mathbb{Z}_4[\varsigma]$ *where* $\Phi(\varsigma) = 0$ *for* Φ *a basic primitive polynomial of degree* t. *Define:*

g_i	ς^{2^t-2}	1	$\cdots$	ς^{2^t-3}
H_i	$\langle 2, 2\varsigma, \ldots, 2\varsigma^{t-1}\rangle$	$\langle 2\varsigma, \ldots, 2\varsigma^{t}\rangle$	$\cdots$	$\langle 2\varsigma^{2^t-2}, \ldots, 2\varsigma^{t-2}\rangle$

Then $D = \cup_{i=0}^{2^t-2} \varsigma^{i-1} + \langle 2\varsigma^{i}, 2\varsigma^{i+1}, \ldots, 2\varsigma^{i+t-1}\rangle$ *is a DS with correct properties.*

Key observation

Key observation: If $g_i \notin H$

Key observation

Key observation: If $g_i \notin H$ and $2g_i \notin H_i$

Key observation

Key observation: If $g_i \notin H$ and $2g_i \notin H_i$ for all i, then D satisfies $D \cap D^{(-1)} = \emptyset$, $G - (D \cup D^{(-1)}) = H$.

Key observation

Key observation: If $g_i \notin H$ and $2g_i \notin H_i$ for all i, then D satisfies $D \cap D^{(-1)} = \emptyset$, $G - (D \cup D^{(-1)}) = H$.

Secondary observation: Any t consecutive powers of ς in the Galois Ring will be a basis for the maximal ideal.

Key observation

Key observation: If $g_i \notin H$ and $2g_i \notin H_i$ for all i, then D satisfies $D \cap D^{(-1)} = \emptyset$, $G - (D \cup D^{(-1)}) = H$.

Secondary observation: Any t consecutive powers of ς in the Galois Ring will be a basis for the maximal ideal.

Question: In what groups can we make this work?

Interesting observation

Example

$D = \{\xi^2, \xi^2 + 2, 1, 1 + 2\xi, \xi, \xi + 2\xi^2\}$ is a multiplicative subgroup of $GR(4, 2)$.

More generally, $D = \cup_{i=0}^{2^t-2} \varsigma^{i-1} + \langle 2\varsigma^i, 2\varsigma^{i+1}, \ldots, 2\varsigma^{i+t-1} \rangle$ is a multiplicative subgroup of $GR(4, t)$.

All Rings?????

Example

$\mathcal{D}_m = \{\xi^i(1 + p^{s-1}\Sigma_{j=1}^m a_j \xi^j)\}$ is a multiplicative subgroup of $GR(p^s, t)$.

All Rings?????

Example

$\mathcal{D}_m = \{\xi^i(1 + p^{s-1}\Sigma_{j=1}^m a_j \xi^j)\}$ is a multiplicative subgroup of $GR(p^s, t)$.

$(x, y) \in R_i$ if $x - y \in a_i \mathcal{D}_m$ defines an association scheme.

All Rings?????

Example

$\mathcal{D}_m = \{\xi^i(1 + p^{s-1}\Sigma_{j=1}^m a_j \xi^j)\}$ is a multiplicative subgroup of $GR(p^s, t)$.

$(x, y) \in R_i$ if $x - y \in a_i \mathcal{D}_m$ defines an association scheme.

Theorem

Let R be a ring with unity and let D be a multiplicative subgroup. Then there is an association scheme associated defined as in the Galois Ring example.

Ito's Theorem

If $\mathcal{X}$ is the set of points of the DRAD and if G is an automorphism group of the DRAD, then the rank of G is the number of orbits of $\mathcal{X} \times \mathcal{X}$.

Theorem

The DRAD coming from the (16,6,2) example is the only (up to equivalence) DRAD which has an automorphism group of rank 4.

Counterexamples

Example

Jorgensen did a computer search for nonsymmetric 3-class association schemes, and found a (64,28,12) example that can be used to construct a DRAD with a rank 4 automorphism group.

Counterexamples

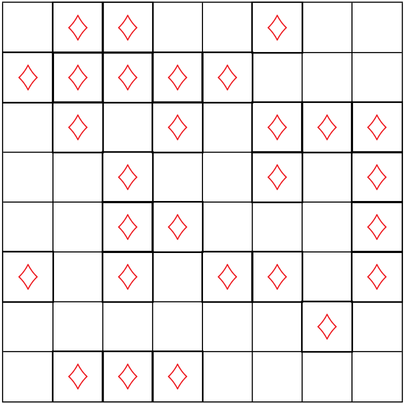
Example

Jorgensen did a computer search for nonsymmetric 3-class association schemes, and found a (64,28,12) example that can be used to construct a DRAD with a rank 4 automorphism group.

Theorem

There are DRADs with rank 4 automorphism groups with valency 4^t *for all* $t \geq 2$.

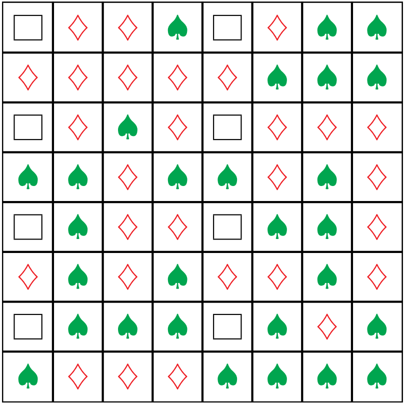
$Z_{2^t}^2$ examples



$Z_{2^t}^2$ examples

	♢	♢	♠		♢	♠	♠
♢	♢	♢	♢	♢	♠	♠	♠
	♢	♠	♢		♢	♢	♢
♠	♠	♢	♠	♠	♢	♠	♢
	♠	♢	♢		♠	♠	♢
♢	♠	♢	♠	♢	♢	♠	♢
	♠	♠	♠		♠	♢	♠
♠	♢	♢	♢	♠	♠	♠	♠

$Z_{2^t}^2$ examples



5-class examples

Example

McFarland (96,20,4) difference sets, find four disjoint in the same group so that $D_i^{(-1)} = D_j$, $G - D_1 - D_2 - D_3 - D_4 = H$ for H a subgroup of order 16. There are such examples!

5-class examples

Example

McFarland (96,20,4) difference sets, find four disjoint in the same group so that $D_i^{(-1)} = D_j$, $G - D_1 - D_2 - D_3 - D_4 = H$ for H a subgroup of order 16. There are such examples!

How to generalize?