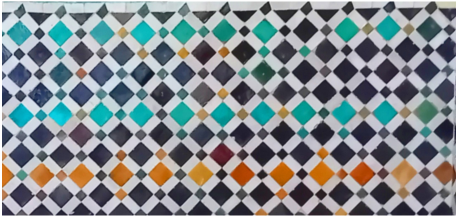
On mosaics of designs*



Vedran Krčadinac

University of Zagreb, Croatia

11.7.2024.

* This work was fully supported by the Croatian Science Foundation under the project 9752.

Mosaics of combinatorial designs

O. W. Gnilke, M. Greferath, M. O. Pavčević, *Mosaics of combinatorial designs*, Des. Codes Cryptogr. **86** (2018), no. 1, 85–95.

Definition.

Let t_i-(v, k_i, λ_i), $i = 1, \ldots, c$ be parameters of combinatorial designs, all with v points and b blocks and $\sum_{i=1}^{c} k_i = v$. A mosaic with parameters

$$t_1\text{-}(v, k_1, \lambda_1) \oplus \cdots \oplus t_c\text{-}(v, k_c, \lambda_c)$$

is a $v \times b$ matrix with entries from $\{1, \ldots, c\}$ such that the entries i represent incidences of a t_i-(v, k_i, λ_i) design, for $i = 1, \ldots, c$. Here, c is the number of colors and the matrix is also called a c-mosaic.

Mosaics of combinatorial designs

O. W. Gnilke, M. Greferath, M. O. Pavčević, *Mosaics of combinatorial designs*, Des. Codes Cryptogr. **86** (2018), no. 1, 85–95.

Definition.

Let t_i-(v, k_i, λ_i), $i = 1, \ldots, c$ be parameters of combinatorial designs, all with v points and b blocks and $\sum_{i=1}^{c} k_i = v$. A mosaic with parameters

$$t_1\text{-}(v, k_1, \lambda_1) \oplus \cdots \oplus t_c\text{-}(v, k_c, \lambda_c)$$

is a $v \times b$ matrix with entries from $\{1, \ldots, c\}$ such that the entries i represent incidences of a t_i-(v, k_i, λ_i) design, for $i = 1, \ldots, c$. Here, c is the number of colors and the matrix is also called a c-mosaic.

Related concept: (strong) colored t-design

A. Bonnecaze, E. Rains, P. Solé, 3-*colored* 5-*designs and* $\mathbb{Z}_4$-*codes*, J. Statist. Plann. Inference **86** (2000), no. 2, 349–368.

Mosaics of combinatorial designs

O. W. Gnilke, M. Greferath, M. O. Pavčević, *Mosaics of combinatorial designs*, Des. Codes Cryptogr. **86** (2018), no. 1, 85–95.

Definition.

Let t_i-(v, k_i, λ_i), $i = 1, \ldots, c$ be parameters of combinatorial designs, all with v points and b blocks and $\sum_{i=1}^{c} k_i = v$. A mosaic with parameters

$$t_1\text{-}(v, k_1, \lambda_1) \oplus \cdots \oplus t_c\text{-}(v, k_c, \lambda_c)$$

is a $v \times b$ matrix with entries from $\{1, \ldots, c\}$ such that the entries i represent incidences of a t_i-(v, k_i, λ_i) design, for $i = 1, \ldots, c$. Here, c is the number of colors and the matrix is also called a c-mosaic.

Theorem.

A resolvable t-(v, k, λ) design gives rise to a c-mosaic

$$t\text{-}(v, k, \lambda) \oplus \cdots \oplus t\text{-}(v, k, \lambda)$$

with $c = v/k$ colors.

Mosaics of combinatorial designs

O. W. Gnilke, M. Greferath, M. O. Pavčević, *Mosaics of combinatorial designs*, Des. Codes Cryptogr. **86** (2018), no. 1, 85–95.

Definition.

Let t_i-(v, k_i, λ_i), $i = 1, \ldots, c$ be parameters of combinatorial designs, all with v points and b blocks and $\sum_{i=1}^{c} k_i = v$. A mosaic with parameters

$$t_1\text{-}(v, k_1, \lambda_1) \oplus \cdots \oplus t_c\text{-}(v, k_c, \lambda_c)$$

is a $v \times b$ matrix with entries from $\{1, \ldots, c\}$ such that the entries i represent incidences of a t_i-(v, k_i, λ_i) design, for $i = 1, \ldots, c$. Here, c is the number of colors and the matrix is also called a c-mosaic.

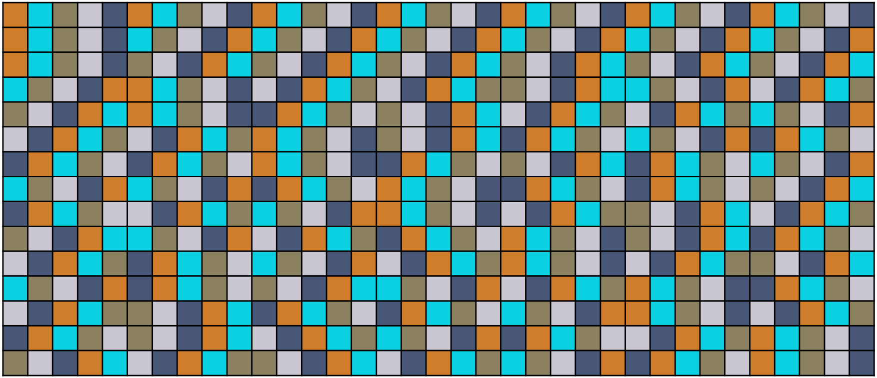
Theorem.

A resolvable t-(v, k, λ) design gives rise to a homogenous c-mosaic

$$t\text{-}(v, k, \lambda) \oplus \cdots \oplus t\text{-}(v, k, \lambda)$$

with $c = v/k$ colors.

Mosaics of combinatorial designs



$$2\text{-}(15,3,1) \oplus 2\text{-}(15,3,1) \oplus 2\text{-}(15,3,1) \oplus 2\text{-}(15,3,1) \oplus 2\text{-}(15,3,1)$$

Are there mosaics that are not homogenous?

Are there mosaics that are not homogenous?

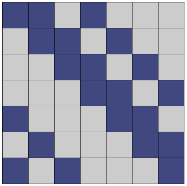
Trivial examples:

$$t\text{-}(v,k,\lambda) \oplus t\text{-}(v,v-k,\overline{\lambda}), \qquad \overline{\lambda} = \lambda\binom{v-t}{k}/\binom{v-t}{k-t}$$

Are there mosaics that are not homogenous?

Trivial examples:

$$t\text{-}(v,k,\lambda) \oplus t\text{-}(v,v-k,\overline{\lambda}), \qquad \overline{\lambda} = \lambda \binom{v-t}{k} / \binom{v-t}{k-t}$$

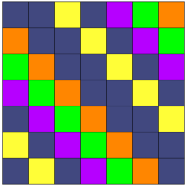


$2\text{-}(7,3,1) \oplus 2\text{-}(7,4,2)$

Are there mosaics that are not homogenous?

Trivial examples:

$$t\text{-}(v,k,\lambda) \oplus t\text{-}(v,v-k,\overline{\lambda}), \qquad \overline{\lambda} = \lambda\binom{v-t}{k}/\binom{v-t}{k-t}$$

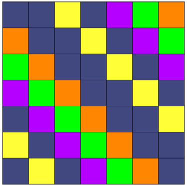


$$2\text{-}(7,3,1) \oplus 2\text{-}(7,1,0) \oplus 2\text{-}(7,1,0) \oplus 2\text{-}(7,1,0) \oplus 2\text{-}(7,1,0)$$

Are there mosaics that are not homogenous?

Trivial examples:

$$t\text{-}(v,k,\lambda) \oplus t\text{-}(v,v-k,\overline{\lambda}), \qquad \overline{\lambda} = \lambda\binom{v-t}{k}/\binom{v-t}{k-t}$$



$$2\text{-}(7,3,1) \oplus 2\text{-}(7,1,0) \oplus 2\text{-}(7,1,0) \oplus 2\text{-}(7,1,0) \oplus 2\text{-}(7,1,0)$$

Proposition.

Every partial mosaic of symmetric designs, with $v = b$ and $\sum_{i=1}^{c} k_i < v$

$$2\text{-}(v,k_1,\lambda_1) \oplus \cdots \oplus 2\text{-}(v,k_c,\lambda_c)$$

can be completed by adding $2\text{-}(v,1,0)$ designs.

Are there mosaics that are not homogenous?

Nontrivial: $c \geq 3$, $t_i \geq 2$ and $k_i \geq 3$ for $i = 1, \ldots, c$

Are there mosaics that are not homogenous?

Nontrivial: $c \geq 3$, $t_i \geq 2$ and $k_i \geq 3$ for $i = 1, \ldots, c$

O. W. Gnilke, M. Greferath, M. O. Pavčević, *Mosaics of combinatorial designs*, Des. Codes Cryptogr. **86** (2018), no. 1, 85–95.

Purely arithmetically, we may think of

$$2\text{-}(31,\ 15,\ 7)\ \oplus\ 2\text{-}(31,\ 10,\ 3)\ \oplus\ 2\text{-}(31,\ 6,\ 1),$$

however, so far, we have not been able to provide an example of a 3-valued incidence matrix giving rise to this decomposition.

Are there mosaics that are not homogenous?

Nontrivial: $c \geq 3$, $t_i \geq 2$ and $k_i \geq 3$ for $i = 1, \ldots, c$

O. W. Gnilke, M. Greferath, M. O. Pavčević, *Mosaics of combinatorial designs*, Des. Codes Cryptogr. **86** (2018), no. 1, 85–95.

Purely arithmetically, we may think of

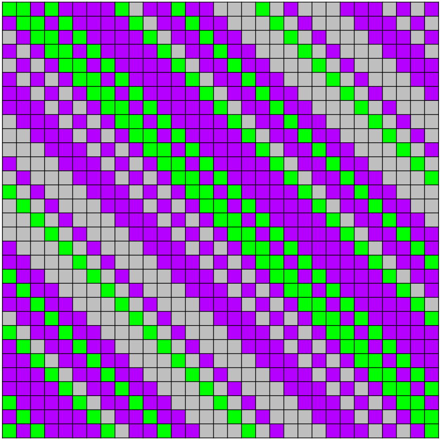
$$2\text{-}(31,\ 15,\ 7)\ \oplus\ 2\text{-}(31,\ 10,\ 3)\ \oplus\ 2\text{-}(31,\ 6,\ 1),$$

however, so far, we have not been able to provide an example of a 3-valued incidence matrix giving rise to this decomposition.

Number of non-isomorphic designs:

2-(31, 15, 7)	$\geq$ **22 478 260**	(Hadamard)
2-(31, 10, 3)	**151**	(E. Spence, 1992)
2-(31, 6, 1)	**1**	(PG(2, 5))

Are there mosaics that are not homogenous?



$2\text{-}(31, 15, 7) \oplus 2\text{-}(31, 6, 1)$

Are there mosaics that are not homogenous?

O. Gnilke, P. Ó Catháin, O. Olmez, G. Nuñez Ponasso, *Invariants of quadratic forms and applications in design theory*, Linear Algebra Appl. **682** (2024), 1–27.

$$2\text{-}(31, 6, 1) \oplus 2\text{-}(31, 15, 7) \oplus 2\text{-}(31, 10, 3)$$

Are there mosaics that are not homogenous?

O. Gnilke, P. Ó Catháin, O. Olmez, G. Nuñez Ponasso, *Invariants of quadratic forms and applications in design theory*, Linear Algebra Appl. **682** (2024), 1–27.

$$2\text{-}(31,6,1) \oplus 2\text{-}(31,15,7) \oplus 2\text{-}(31,10,3)$$

4.3. Decomposition of symmetric designs

We consider the following question: when can the incidence matrix of a symmetric design be written as the sum of two disjoint $\{0, 1\}$ matrices, each of which is the incidence matrix of a symmetric design? The obvious necessary condition is that designs with suitable parameters should exist individually. In this section, we develop a further necessary condition in terms of invariants of quadratic forms.

Are there mosaics that are not homogenous?

O. Gnilke, P. Ó Catháin, O. Olmez, G. Nuñez Ponasso, *Invariants of quadratic forms and applications in design theory*, Linear Algebra Appl. **682** (2024), 1–27.

$$\overline{2\text{-}(31,6,1)} = 2\text{-}(31,15,7) \oplus 2\text{-}(31,10,3)$$

4.3. Decomposition of symmetric designs

We consider the following question: when can the incidence matrix of a symmetric design be written as the sum of two disjoint $\{0,1\}$ matrices, each of which is the incidence matrix of a symmetric design? The obvious necessary condition is that designs with suitable parameters should exist individually. In this section, we develop a further necessary condition in terms of invariants of quadratic forms.

Are there mosaics that are not homogenous?

O. Gnilke, P. Ó Catháin, O. Olmez, G. Nuñez Ponasso, *Invariants of quadratic forms and applications in design theory*, Linear Algebra Appl. **682** (2024), 1–27.

$$2\text{-}(31,25,20) = 2\text{-}(31,15,7) \oplus 2\text{-}(31,10,3)$$

4.3. Decomposition of symmetric designs

We consider the following question: when can the incidence matrix of a symmetric design be written as the sum of two disjoint $\{0,1\}$ matrices, each of which is the incidence matrix of a symmetric design? The obvious necessary condition is that designs with suitable parameters should exist individually. In this section, we develop a further necessary condition in terms of invariants of quadratic forms.

Are there mosaics that are not homogenous?

O. Gnilke, P. Ó Catháin, O. Olmez, G. Nuñez Ponasso, *Invariants of quadratic forms and applications in design theory*, Linear Algebra Appl. **682** (2024), 1–27.

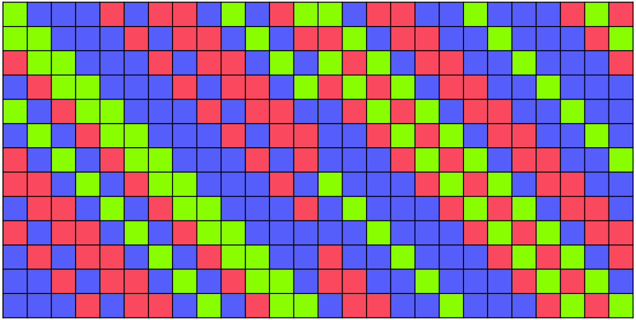
$$2\text{-}(31,25,20) = 2\text{-}(31,15,7) \oplus 2\text{-}(31,10,3)$$

4.3. Decomposition of symmetric designs

We consider the following question: when can the incidence matrix of a symmetric design be written as the sum of two disjoint $\{0,1\}$ matrices, each of which is the incidence matrix of a symmetric design? The obvious necessary condition is that designs with suitable parameters should exist individually. In this section, we develop a further necessary condition in terms of invariants of quadratic forms.

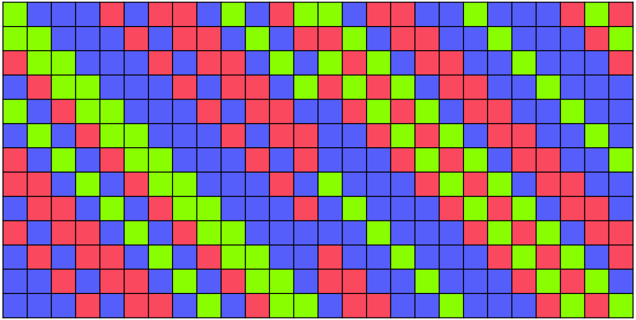
These methods **cannot** rule out the existence of a $(31,25,20)$-design (the complement of a projective plane of order 5) which decomposes into a $(31,15,7)$-design and a $(31,10,3)$-design. This is the smallest open case for a decomposition. Finally, we observe that solutions to this problem do exist, the sum of a skew-Hadamard design with parameters $(4t-1,2t-1,t-1)$ with a trivial $(4t-1,1,0)$-design gives a $(4t-1,2t,t)$-design, so the concept is not vacuous [10]. This topic will be considered more fully in forthcoming work of the authors.

Are there mosaics that are not homogenous?



$2\text{-}(13,3,1) \oplus 2\text{-}(13,4,2) \oplus 2\text{-}(13,6,5)$

Are there mosaics that are not homogenous?



$$2\text{-}(13,3,1) \oplus 2\text{-}(13,4,2) \oplus 2\text{-}(13,6,5)$$

$$\left.\begin{array}{l}\mathcal{F}_1 = (\{0,1,4\},\ \{0,2,7\}) \\ \mathcal{F}_2 = (\{2,6,7,9\},\ \{1,3,10,11\}) \\ \mathcal{F}_3 = (\{3,5,8,10,11,12\},\ \{4,5,6,8,9,12\})\end{array}\right\} \mathbb{Z}_{13}$$

Applications of mosaics

M. Wiese, H. Boche, *Mosaics of combinatorial designs for information-theoretic security*, Des. Codes Cryptogr. **90** (2022), no. 3, 593–632.

M. Wiese, H. Boche, *ε-Almost collision-flat universal hash functions and mosaics of designs*, Des. Codes Cryptogr. **92** (2024), no. 4, 975–998.

Applications of mosaics

M. Wiese, H. Boche, *Mosaics of combinatorial designs for information-theoretic security*, Des. Codes Cryptogr. **90** (2022), no. 3, 593–632.

M. Wiese, H. Boche, *ε-Almost collision-flat universal hash functions and mosaics of designs*, Des. Codes Cryptogr. **92** (2024), no. 4, 975–998.

6 Open questions

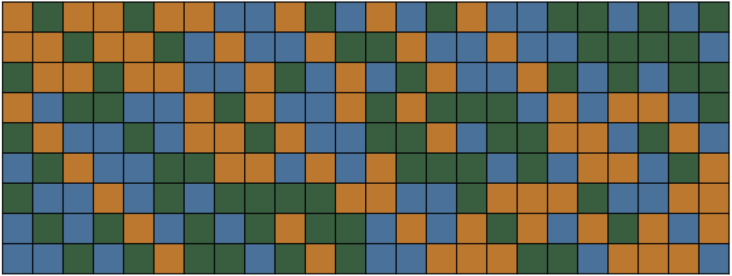
After our extension results (Theorems 3 and 4), we discussed how the original function g and the generated $\hat{g}$ or $\check{g}$ relate with respect to equalities in the lower bounds on the seed sizes. What remained open was whether every seed-optimal OCFU hash function can be derived from a seed-optimal OU hash function. Formulated in terms of mosaics and designs, the question is: *Are the members of every mosaic of BIBDs resolvable?* In other words, is the method of Gnilke, Geferath and Pavčević (Corollary 3) essentially the only way of constructing a mosaic of BIBDs? By Corollary 2, the members of a mosaics of BIBD(v, k, λ) certainly need to satisfy the necessary condition $b \geq v + r - 1$ for resolvable designs.

Homogenous mosaics of non-resolvable designs

Number of non-isomorphic 2-$(9, 3, 2)$ designs: **36** (resolvable: **9**)

Homogenous mosaics of non-resolvable designs

Number of non-isomorphic 2-$(9,3,2)$ designs: **36** (resolvable: **9**)

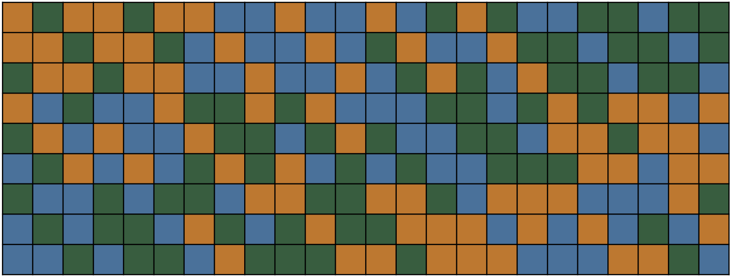


$$2\text{-}(9,3,2) \oplus 2\text{-}(9,3,2) \oplus 2\text{-}(9,3,2)$$

Contains 3 isomorphic copies of a non-resolvable design

Homogenous mosaics of non-resolvable designs

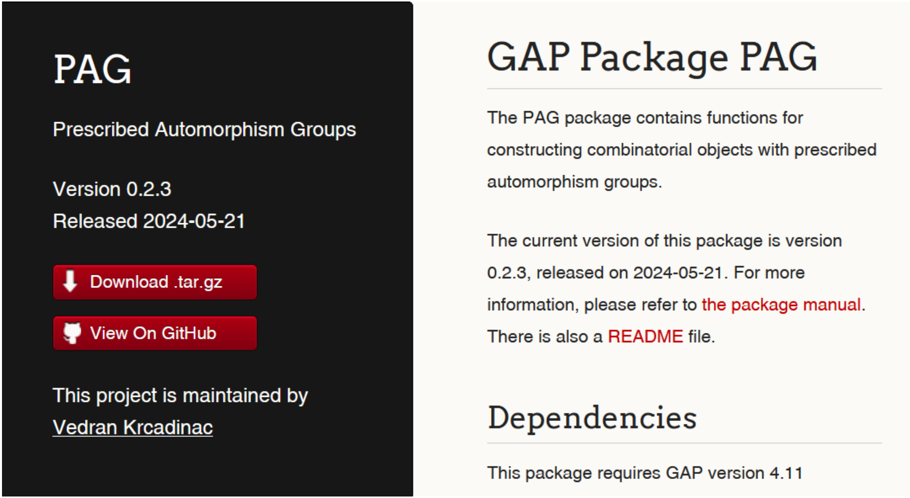
Number of non-isomorphic 2-$(9,3,2)$ designs: **36** (resolvable: **9**)



2-$(9,3,2)$ $\oplus$ 2-$(9,3,2)$ $\oplus$ 2-$(9,3,2)$

Contains 3 non-isomorphic designs (1 resolvable, 2 non-resolvable)

Prescribed Automorphism Groups



PAG

Prescribed Automorphism Groups

Version 0.2.3
Released 2024-05-21

Download .tar.gz

View On GitHub

This project is maintained by Vedran Krcadinac

GAP Package PAG

The PAG package contains functions for constructing combinatorial objects with prescribed automorphism groups.

The current version of this package is version 0.2.3, released on 2024-05-21. For more information, please refer to the package manual. There is also a README file.

Dependencies

This package requires GAP version 4.11

https://vkrcadinac.github.io/PAG/

Autotopies and automorphisms of mosaics

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be c-mosaics of type $v \times b$.

They are isotopic if there are permutations $(\alpha, \beta, \gamma) \in S_v \times S_b \times S_c$ such that $b_{ij} = \gamma(a_{\alpha(i)\,\beta(j)})$ for all $i = 1, \ldots, v$, $j = 1, \ldots, b$.

If $A = B$, the triple (α, β, γ) is an autotopy of the mosaic.

Autotopies and automorphisms of mosaics

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be c-mosaics of type $v \times b$.

They are isotopic if there are permutations $(\alpha, \beta, \gamma) \in S_v \times S_b \times S_c$ such that $b_{ij} = \gamma(a_{\alpha(i)\,\beta(j)})$ for all $i = 1, \ldots, v$, $j = 1, \ldots, b$.

If $A = B$, the triple (α, β, γ) is an autotopy of the mosaic.

If $\gamma = id$, the mosaics are isomorphic.

If $A = B$ and $\gamma = id$, the pair (α, β) is an automorphism.

Autotopies and automorphisms of mosaics

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be c-mosaics of type $v \times b$.

They are isotopic if there are permutations $(\alpha, \beta, \gamma) \in S_v \times S_b \times S_c$ such that $b_{ij} = \gamma(a_{\alpha(i)\,\beta(j)})$ for all $i = 1, \ldots, v$, $j = 1, \ldots, b$.

If $A = B$, the triple (α, β, γ) is an autotopy of the mosaic.

If $\gamma = id$, the mosaics are isomorphic.

If $A = B$ and $\gamma = id$, the pair (α, β) is an automorphism.

Similar as for Latin squares!

Tiling groups with difference sets

A. Ćustić, V. Krčadinac, Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.56, 13 pp.

Tiling groups with difference sets

A. Ćustić, V. Krčadinac, Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.56, 13 pp.

Definition.

A tiling of an additively written group G is a family of pairwise disjoint (v, k, λ) difference sets $\{D_1, \ldots, D_c\}$ such that $D_1 \cup \cdots \cup D_c = G \setminus \{0\}$.

Tiling groups with difference sets

A. Ćustić, V. Krčadinac, Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.56, 13 pp.

Definition.

A tiling of an additively written group G is a family of pairwise disjoint (v, k, λ) difference sets $\{D_1, \ldots, D_c\}$ such that $D_1 \cup \cdots \cup D_c = G \setminus \{0\}$.

Theorem.

The development of a tiling of G with (v, k, λ) difference sets is a mosaic

$$2\text{-}(v, k, \lambda) \oplus \cdots \oplus 2\text{-}(v, k, \lambda) \oplus 2\text{-}(v, 1, 0)$$

of symmetric designs. It has G as an automorphism group acting regularly on the rows and columns.

Tiling groups with difference sets

Example. A tiling of $\mathbb{Z}_{31} = \{0, \ldots, 30\}$ with $(31, 6, 1)$ difference sets:

$$D_1 = \{1, 5, 11, 24, 25, 27\}$$

$$D_2 = \{2, 10, 17, 19, 22, 23\}$$

$$D_3 = \{3, 4, 7, 13, 15, 20\}$$

$$D_4 = \{6, 8, 9, 14, 26, 30\}$$

$$D_5 = \{12, 16, 18, 21, 28, 29\}$$

Example. A tiling of $\mathbb{Z}_{31} = \{0, \ldots, 30\}$ with $(31, 6, 1)$ difference sets:

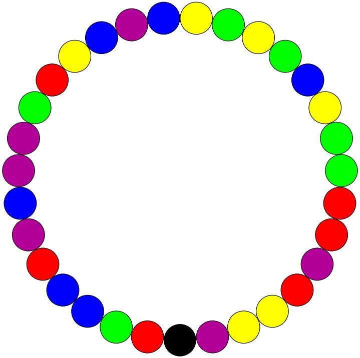
$D_1 = \{1, 5, 11, 24, 25, 27\}$

$D_2 = \{2, 10, 17, 19, 22, 23\}$

$D_3 = \{3, 4, 7, 13, 15, 20\}$

$D_4 = \{6, 8, 9, 14, 26, 30\}$

$D_5 = \{12, 16, 18, 21, 28, 29\}$



Tiling groups with difference sets

Example. A tiling of $\mathbb{Z}_{31} = \{0, \ldots, 30\}$ with $(31, 6, 1)$ difference sets:

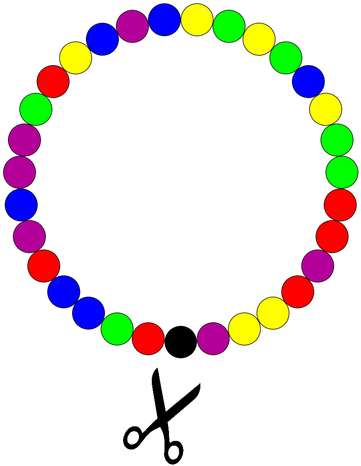
$D_1 = \{1, 5, 11, 24, 25, 27\}$

$D_2 = \{2, 10, 17, 19, 22, 23\}$

$D_3 = \{3, 4, 7, 13, 15, 20\}$

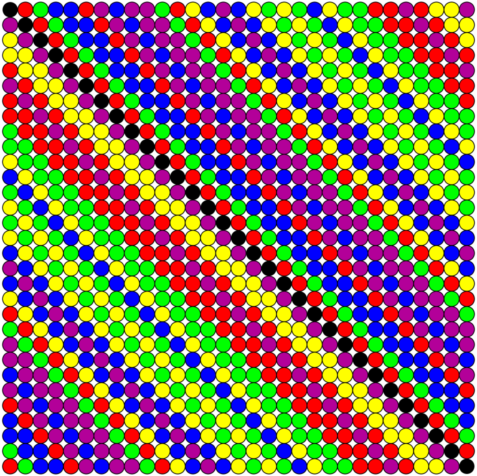
$D_4 = \{6, 8, 9, 14, 26, 30\}$

$D_5 = \{12, 16, 18, 21, 28, 29\}$

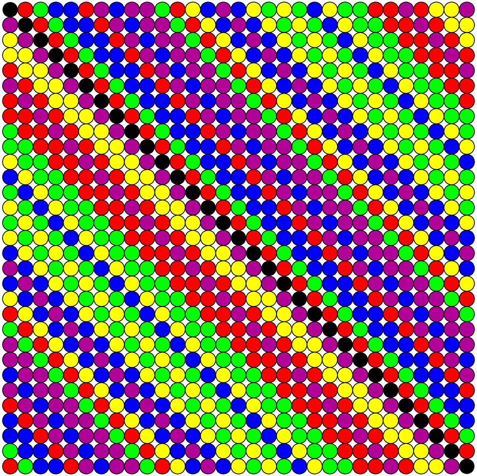


Tiling groups with difference sets

Tiling groups with difference sets



Tiling groups with difference sets



$2\text{-}(31,6,1) \oplus 2\text{-}(31,6,1) \oplus 2\text{-}(31,6,1) \oplus 2\text{-}(31,6,1) \oplus 2\text{-}(31,6,1) \oplus 2\text{-}(31,1,0)$

Tiling groups with difference sets

https://www.imaginary.org/gallery/difference-bracelets

A model of the (31,6,1) bracelet

Difference bracelets cannot be built without the black bead, representing the identity element of the group. A slightly larger faceted bead was used here.

More Galleries

Mosaics of projective planes

For what orders q are there q-mosaics of projective planes of order q?

$$(q^2+q+1, q+1, 1) \oplus \cdots \oplus (q^2+q+1, q+1, 1) \oplus (q^2+q+1, 1, 0)$$

Mosaics of projective planes

For what orders q are there q-mosaics of projective planes of order q?

$$(q^2+q+1, q+1, 1) \oplus \cdots \oplus (q^2+q+1, q+1, 1) \oplus (q^2+q+1, 1, 0)$$

A. Ćustić, V. Krčadinac, Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.56, 13 pp.

q	2	3	4	5	7	8	9	...
Tiling	✓	✗	✗	✓	✓	✓	?	...
Mosaic								...

Mosaics of projective planes

For what orders q are there q-mosaics of projective planes of order q?

$$(q^2+q+1, q+1, 1) \oplus \cdots \oplus (q^2+q+1, q+1, 1) \oplus (q^2+q+1, 1, 0)$$

A. Ćustić, V. Krčadinac, Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.56, 13 pp.

q	2	3	4	5	7	8	9	$\cdots$
Tiling	✓	✗	✗	✓	✓	✓	?	$\cdots$
Mosaic	✓			✓	✓	✓		$\cdots$

Mosaics of projective planes

For what orders q are there q-mosaics of projective planes of order q?

$$(q^2+q+1, q+1, 1) \oplus \cdots \oplus (q^2+q+1, q+1, 1) \oplus (q^2+q+1, 1, 0)$$

A. Ćustić, V. Krčadinac, Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.56, 13 pp.

q	2	3	4	5	7	8	9	...
Tiling	✓	✗	✗	✓	✓	✓	?	...
Mosaic	✓	✓		✓	✓	✓		...

V. Krčadinac, *Small examples of mosaics of combinatorial designs*, preprint, 2024. https://arxiv.org/abs/2405.12672

Mosaics of projective planes

For what orders q are there q-mosaics of projective planes of order q?

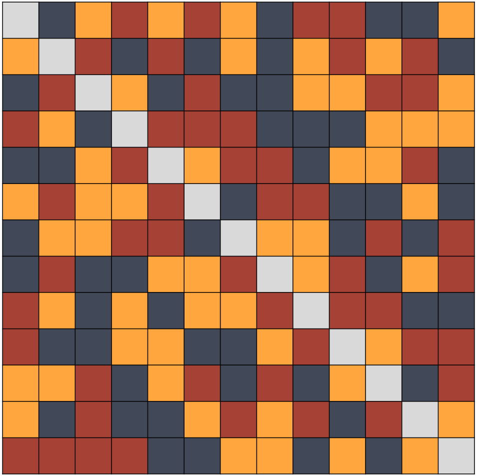
$$(q^2+q+1, q+1, 1) \oplus \cdots \oplus (q^2+q+1, q+1, 1) \oplus (q^2+q+1, 1, 0)$$

A. Ćustić, V. Krčadinac, Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.56, 13 pp.

q	2	3	4	5	7	8	9	...
Tiling	✓	✗	✗	✓	✓	✓	?	...
Mosaic	✓	✓	?	✓	✓	✓	?	...

V. Krčadinac, *Small examples of mosaics of combinatorial designs*, preprint, 2024. https://arxiv.org/abs/2405.12672

Mosaics of projective planes



$$2\text{-}(13,4,1) \oplus 2\text{-}(13,4,1) \oplus 2\text{-}(13,4,1) \oplus 2\text{-}(13,1,0)$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v, k, \lambda) \oplus 2\text{-}(v, k, \lambda) \oplus 2\text{-}(v, 1, 0)$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow \quad (v,k,\lambda) = (4n-1, 2n-1, n-1)$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow \quad (v,k,\lambda) = (4n-1, 2n-1, n-1)$

A Hadamard matrix H is skew if it is of the form $H = I + A, \;\; A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$).

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow \;\; (v,k,\lambda) = (4n-1, 2n-1, n-1)$

A Hadamard matrix H is skew if it is of the form $H = I + A$, $A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

$$\begin{bmatrix} 1 & - & - & 1 & 1 & 1 & 1 & - \\ 1 & 1 & - & 1 & - & 1 & - & 1 \\ 1 & 1 & 1 & 1 & 1 & - & 1 & 1 \\ - & - & - & 1 & - & - & 1 & 1 \\ - & 1 & - & 1 & 1 & - & - & - \\ - & - & 1 & 1 & 1 & 1 & - & 1 \\ - & 1 & - & - & 1 & 1 & 1 & 1 \\ 1 & - & - & - & 1 & - & - & 1 \end{bmatrix}$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow \quad (v,k,\lambda) = (4n-1, 2n-1, n-1)$

A Hadamard matrix H is skew if it is of the form $H = I + A,\ \ A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

$$\begin{bmatrix} 1 & 1 & - & 1 & 1 & 1 & 1 & - \\ - & 1 & 1 & - & 1 & - & 1 & - \\ 1 & - & 1 & 1 & 1 & - & 1 & 1 \\ - & 1 & - & 1 & - & - & 1 & 1 \\ - & - & - & 1 & 1 & - & - & - \\ - & 1 & 1 & 1 & 1 & 1 & - & 1 \\ - & - & - & - & 1 & 1 & 1 & 1 \\ 1 & 1 & - & - & 1 & - & - & 1 \end{bmatrix}$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$$\Rightarrow \quad (v,k,\lambda) = (4n-1, 2n-1, n-1)$$

A Hadamard matrix H is skew if it is of the form $H = I + A$, $A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & - \\ - & 1 & - & - & 1 & - & 1 & - \\ - & 1 & 1 & - & - & 1 & - & - \\ - & 1 & 1 & 1 & - & - & 1 & 1 \\ - & - & 1 & 1 & 1 & - & - & - \\ - & 1 & - & 1 & 1 & 1 & - & 1 \\ - & - & 1 & - & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & - & 1 & - & - & 1 \end{bmatrix}$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow \ (v,k,\lambda) = (4n-1, 2n-1, n-1)$

A Hadamard matrix H is skew if it is of the form $H = I + A, \ \ A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ - & 1 & - & - & 1 & - & 1 & 1 \\ - & 1 & 1 & - & - & 1 & - & 1 \\ - & 1 & 1 & 1 & - & - & 1 & - \\ - & - & 1 & 1 & 1 & - & - & 1 \\ - & 1 & - & 1 & 1 & 1 & - & - \\ - & - & 1 & - & 1 & 1 & 1 & - \\ - & - & - & 1 & - & 1 & 1 & 1 \end{bmatrix}$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$$\Rightarrow \quad (v,k,\lambda) = (4n-1, 2n-1, n-1)$$

A Hadamard matrix H is skew if it is of the form $H = I + A,\ \ A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
- & 1 & - & - & 1 & - & 1 & 1 \\
- & 1 & 1 & - & - & 1 & - & 1 \\
- & 1 & 1 & 1 & - & - & 1 & - \\
- & - & 1 & 1 & 1 & - & - & 1 \\
- & 1 & - & 1 & 1 & 1 & - & - \\
- & - & 1 & - & 1 & 1 & 1 & - \\
- & - & - & 1 & - & 1 & 1 & 1
\end{bmatrix}$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow\ (v,k,\lambda) = (4n-1, 2n-1, n-1)$

A Hadamard matrix H is skew if it is of the form $H = I + A$, $A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ - & 0 & - & - & 1 & - & 1 & 1 \\ - & 1 & 0 & - & - & 1 & - & 1 \\ - & 1 & 1 & 0 & - & - & 1 & - \\ - & - & 1 & 1 & 0 & - & - & 1 \\ - & 1 & - & 1 & 1 & 0 & - & - \\ - & - & 1 & - & 1 & 1 & 0 & - \\ - & - & - & 1 & - & 1 & 1 & 0 \end{bmatrix}$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow \quad (v,k,\lambda) = (4n-1, 2n-1, n-1)$

A Hadamard matrix H is skew if it is of the form $H = I + A, \;\; A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ - & 0 & 2 & 2 & 1 & 2 & 1 & 1 \\ - & 1 & 0 & 2 & 2 & 1 & 2 & 1 \\ - & 1 & 1 & 0 & 2 & 2 & 1 & 2 \\ - & 2 & 1 & 1 & 0 & 2 & 2 & 1 \\ - & 1 & 2 & 1 & 1 & 0 & 2 & 2 \\ - & 2 & 1 & 2 & 1 & 1 & 0 & 2 \\ - & 2 & 2 & 1 & 2 & 1 & 1 & 0 \end{bmatrix}$$

Hadamard mosaics

A Hadamard mosaic is a mosaic consisting of two symmetric designs:

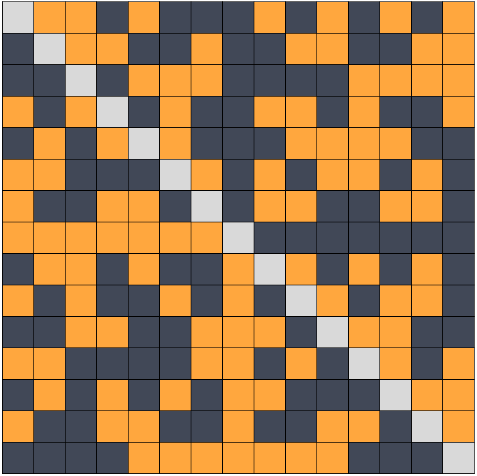
$$2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,k,\lambda) \oplus 2\text{-}(v,1,0)$$

$\Rightarrow \quad (v,k,\lambda) = (4n-1, 2n-1, n-1)$

A Hadamard matrix H is skew if it is of the form $H = I + A, \;\; A^t = -A$ (alternatively: if it satisfies $H + H^t = 2I$). **Skew** standard form:

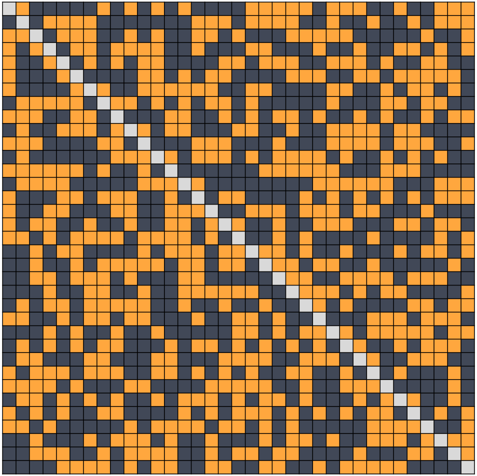
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ - & 0 & 2 & 2 & 1 & 2 & 1 & 1 \\ - & 1 & 0 & 2 & 2 & 1 & 2 & 1 \\ - & 1 & 1 & 0 & 2 & 2 & 1 & 2 \\ - & 2 & 1 & 1 & 0 & 2 & 2 & 1 \\ - & 1 & 2 & 1 & 1 & 0 & 2 & 2 \\ - & 2 & 1 & 2 & 1 & 1 & 0 & 2 \\ - & 2 & 2 & 1 & 2 & 1 & 1 & 0 \end{bmatrix} \quad \rightsquigarrow \quad \begin{matrix} 2\text{-}(7,3,1) \oplus 2\text{-}(7,3,1) \\ \oplus\, 2\text{-}(7,1,0) \end{matrix}$$

Hadamard mosaics



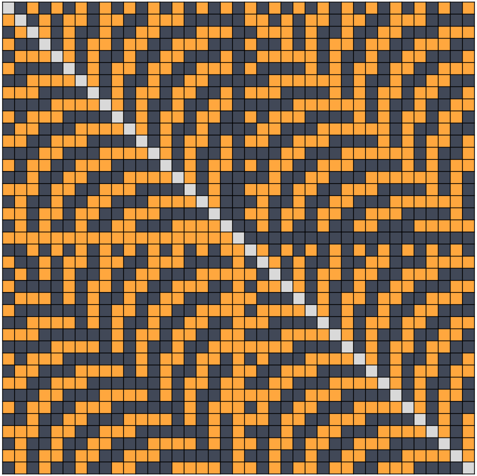
$$2\text{-}(15,7,3) \oplus 2\text{-}(15,7,3) \oplus 2\text{-}(15,1,0)$$

Hadamard mosaics



$$2\text{-}(35,17,8) \oplus 2\text{-}(35,17,8) \oplus 2\text{-}(35,1,0)$$

Hadamard mosaics



$$2\text{-}(39,19,9) \oplus 2\text{-}(39,19,9) \oplus 2\text{-}(39,1,0)$$

Hadamard mosaics

Conjecture: skew Hadamard matrices exist for all orders divisible by 4 (Jennifer Seberry)

Hadamard mosaics

Conjecture: skew Hadamard matrices exist for all orders divisible by 4 (Jennifer Seberry)

Theorem.

Hadamard mosaics are equivalent with skew Hadamard matrices.

Hadamard mosaics

Conjecture: skew Hadamard matrices exist for all orders divisible by 4 (Jennifer Seberry)

Theorem.

Hadamard mosaics are equivalent with skew Hadamard matrices.

Padraig Ó Catháin, *Nesting symmetric designs*, Irish Math. Soc. Bull. **72** (2013), 71–74.

Theorem.

A symmetric 2-(v, k, λ) design can be extended to a 2-$(v, k+1, \lambda')$ design if and only if it comes from a skew Hadamard matrix.

The End

Thanks for your attention!