Quadratic Forms in Design Theory

Padraig Ó Catháin

Dublin City University

Australasian Combinatorics Conference
University of Western Australia
15 December 2023

- Joint work with Oliver Gnilke, Oktay Olmez & Guillermo Nunez Ponasso
- Inspired by a problem of Darryn Bryant
- Supported by the Faculty of Humanities Travel Grant (DCU) & Teaching and Learning grant from Technical University of the Shannon (TUS)

The symmetric mosaic problem

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Question: For which parameters does there exist a mosaic of symmetric designs?

- A symmetric balanced incomplete-block design (SBIBD, design) with parameters (v, k, λ) has v **points** and v **blocks**. Each block is **incident** with k points, and each pair of points are jointly incident with λ blocks.
- Finite projective planes are designs with parameters $(n^2 + n + 1, n + 1, 1)$.
- A (v, k, λ) design is described by its incidence matrix, which is a square $\{0, 1\}$-matrix satisfying

$$MM^\top = (k - \lambda)I_v + \lambda J_v$$

The symmetric mosaic problem

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Question: For which parameters does there exist a mosaic of symmetric designs?

Theorem

If M and $M + I$ are both symmetric designs, then M is the incidence matrix of a skew-Hadamard design.

Theorem

If M and $M + I$ are both symmetric designs, then M is the incidence matrix of a skew-Hadamard design.

- $\lambda_1 = \frac{k(k-1)}{v-1}$ and $\lambda_2 = \frac{(k+1)k}{v-1}$ are integers.

Theorem

If M and $M + I$ are both symmetric designs, then M is the incidence matrix of a skew-Hadamard design.

- $\lambda_1 = \frac{k(k-1)}{v-1}$ and $\lambda_2 = \frac{(k+1)k}{v-1}$ are integers.
- So is their difference, so $v - 1$ divides $2k$.

Theorem

If M and $M + I$ are both symmetric designs, then M is the incidence matrix of a skew-Hadamard design.

- $\lambda_1 = \frac{k(k-1)}{v-1}$ and $\lambda_2 = \frac{(k+1)k}{v-1}$ are integers.
- So is their difference, so $v - 1$ divides $2k$.
- But $k \leqslant \frac{v-1}{2}$ so the parameters are $(4t - 1, 2t - 1, t - 1)$.

Theorem

If M and $M + I$ are both symmetric designs, then M is the incidence matrix of a skew-Hadamard design.

- $\lambda_1 = \frac{k(k-1)}{v-1}$ and $\lambda_2 = \frac{(k+1)k}{v-1}$ are integers.
- So is their difference, so $v - 1$ divides $2k$.
- But $k \leqslant \frac{v-1}{2}$ so the parameters are $(4t - 1, 2t - 1, t - 1)$.
- $$(M + I)(M + I)^\top = MM^\top + M + M^\top + I = \alpha I + \beta J$$

  so $M + M^\top = J - I$ and M is *skew*.

Theorem

If M and $M+I$ are both symmetric designs, then M is the incidence matrix of a skew-Hadamard design.

- $\lambda_1 = \frac{k(k-1)}{v-1}$ and $\lambda_2 = \frac{(k+1)k}{v-1}$ are integers.
- So is their difference, so $v-1$ divides $2k$.
- But $k \leqslant \frac{v-1}{2}$ so the parameters are $(4t-1, 2t-1, t-1)$.
- $$(M+I)(M+I)^\top = MM^\top + M + M^\top + I = \alpha I + \beta J$$
  so $M + M^\top = J - I$ and M is *skew*.
- Such designs exist when $4t-1$ is a prime power. Conjectured to exist for all integers $4t-1$.

Non-trivial mosaics: v even

- One infinite family of mosaics, in any other mosaic all the designs are non-trivial ($0 < \lambda < v - 2$). Are there any other examples?

Non-trivial mosaics: v even

- One infinite family of mosaics, in any other mosaic all the designs are non-trivial ($0 < \lambda < v - 2$). Are there any other examples?
- Clear necessary condition: designs with parameters (v, k_1, λ_1) and (v, k_2, λ_2) should exist such that

$$\lambda_{1+2} = \frac{(k_1 + k_2)(k_1 + k_2 - 1)}{v - 1} = \lambda_1 + \lambda_2 + \frac{2k_1 k_2}{v - 1}\,.$$

Non-trivial mosaics: v even

- One infinite family of mosaics, in any other mosaic all the designs are non-trivial ($0 < \lambda < v - 2$). Are there any other examples?
- Clear necessary condition: designs with parameters (v, k_1, λ_1) and (v, k_2, λ_2) should exist such that

$$\lambda_{1+2} = \frac{(k_1 + k_2)(k_1 + k_2 - 1)}{v - 1} = \lambda_1 + \lambda_2 + \frac{2k_1 k_2}{v - 1} .$$

- **Bruck-Ryser-Chowla (easy part):** If v is even then $k_i - \lambda_i$ is a **square**.
  Proof: $\det(MM^\top) = \det((k - \lambda)I + \lambda J) = k^2(k - \lambda)^{v-1}$ is **square.**

Non-trivial mosaics: v even

- One infinite family of mosaics, in any other mosaic all the designs are non-trivial ($0 < \lambda < v - 2$). Are there any other examples?
- Clear necessary condition: designs with parameters (v, k_1, λ_1) and (v, k_2, λ_2) should exist such that

$$\lambda_{1+2} = \frac{(k_1 + k_2)(k_1 + k_2 - 1)}{v - 1} = \lambda_1 + \lambda_2 + \frac{2k_1 k_2}{v - 1} .$$

- **Bruck-Ryser-Chowla (easy part):** If v is even then $k_i - \lambda_i$ is a **square**.
  Proof: $\det(MM^\top) = \det((k - \lambda)I + \lambda J) = k^2(k - \lambda)^{v-1}$ is **square.**
- One potential parameter set with $v \leqslant 10,000$:

$$(2380, 183, 14) \oplus (2380, 793, 264) \oplus (2380, 1404, 828) .$$

Non-trivial mosaics: v even

- One infinite family of mosaics, in any other mosaic all the designs are non-trivial ($0 < \lambda < v - 2$). Are there any other examples?
- Clear necessary condition: designs with parameters (v, k_1, λ_1) and (v, k_2, λ_2) should exist such that

$$\lambda_{1+2} = \frac{(k_1 + k_2)(k_1 + k_2 - 1)}{v - 1} = \lambda_1 + \lambda_2 + \frac{2k_1 k_2}{v - 1}\,.$$

- **Bruck-Ryser-Chowla (easy part):** If v is even then $k_i - \lambda_i$ is a **square**.
  Proof: $\det(MM^\top) = \det((k - \lambda)I + \lambda J) = k^2(k - \lambda)^{v-1}$ is **square.**
- One potential parameter set with $v \leqslant 10,000$:

$$(2380, 183, 14) \oplus (2380, 793, 264) \oplus (2380, 1404, 828)\,.$$

- **Conjecture:** There are no even symmetric mosaics (on three colours).

Non-trivial mosaics: v even

- One infinite family of mosaics, in any other mosaic all the designs are non-trivial ($0 < \lambda < v - 2$). Are there any other examples?
- Clear necessary condition: designs with parameters (v, k_1, λ_1) and (v, k_2, λ_2) should exist such that

$$\lambda_{1+2} = \frac{(k_1 + k_2)(k_1 + k_2 - 1)}{v - 1} = \lambda_1 + \lambda_2 + \frac{2k_1 k_2}{v - 1} .$$

- **Bruck-Ryser-Chowla (easy part):** If v is even then $k_i - \lambda_i$ is a **square**.
  Proof: $\det(MM^\top) = \det((k - \lambda)I + \lambda J) = k^2(k - \lambda)^{v-1}$ is **square.**
- One potential parameter set with $v \leqslant 10,000$:

$$(2380, 183, 14) \oplus (2380, 793, 264) \oplus (2380, 1404, 828) .$$

- **Conjecture:** There are no even symmetric mosaics (on three colours).
- Before the end of the talk, we'll rule out the displayed example.

Non-trivial mosaics: v odd

- The skew-Hadamard family exists, so results are more delicate.

Non-trivial mosaics: v odd

- The skew-Hadamard family exists, so results are more delicate.
- An infinite-looking family exists:

$$(n^2+n+1, n+1, 1) \oplus (4t-1, 2t-1, t-1) \oplus (v, k, \lambda)$$

$$'' \oplus (n^2+n+1, \frac{n^2+n}{2}, \frac{n^2+n-2}{4}) \oplus (n^2+n+1, \frac{n^2-n}{2}, \frac{n^2-3n+2}{4})$$

Non-trivial mosaics: v odd

- The skew-Hadamard family exists, so results are more delicate.
- An infinite-looking family exists:

$$(n^2+n+1, n+1, 1) \oplus (4t-1, 2t-1, t-1) \oplus (v, k, \lambda)$$

$$'' \oplus (n^2+n+1, \frac{n^2+n}{2}, \frac{n^2+n-2}{4}) \oplus (n^2+n+1, \frac{n^2-n}{2}, \frac{n^2-3n+2}{4})$$

- Some other parameters up to 1,000. Smallest example we can't rule out is $n = 5$ above.

Non-trivial mosaics: v odd

- The skew-Hadamard family exists, so results are more delicate.
- An infinite-looking family exists:

$$(n^2+n+1, n+1, 1) \oplus (4t-1, 2t-1, t-1) \oplus (v, k, \lambda)$$

$$" \oplus (n^2+n+1, \frac{n^2+n}{2}, \frac{n^2+n-2}{4}) \oplus (n^2+n+1, \frac{n^2-n}{2}, \frac{n^2-3n+2}{4})$$

- Some other parameters up to 1,000. Smallest example we can't rule out is $n = 5$ above.
- **Question:** Can the complement of a projective plane of order 5 be partitioned into a $(31, 15, 7)$ and a $(31, 10, 3)$-design? (Both are known to exist individually.)

Bruck-Ryser-Chowla with v odd: traditional form

Theorem

Suppose that M is the incidence matrix of a symmetric (v, k, λ) design where v is odd. Then the Diophantine equation

$$X^2 - (k - \lambda)Y^2 - (-1)^{\frac{v-1}{2}} \lambda Z^2 = 0$$

has a non-trivial solution.

Bruck-Ryser-Chowla with v odd: traditional form

Theorem

Suppose that M is the incidence matrix of a symmetric (v, k, λ) design where v is odd. Then the Diophantine equation

$$X^2 - (k - \lambda)Y^2 - (-1)^{\frac{v-1}{2}}\lambda Z^2 = 0$$

has a non-trivial solution.

- **Question:** How do I solve such equations?

Bruck-Ryser-Chowla with v odd: traditional form

Theorem

Suppose that M is the incidence matrix of a symmetric (v, k, λ) design where v is odd. Then the Diophantine equation

$$X^2 - (k-\lambda)Y^2 - (-1)^{\frac{v-1}{2}}\lambda Z^2 = 0$$

has a non-trivial solution.

- **Question:** How do I solve such equations?
- **Marshall Hall**: the computations involved are **detailed and troublesome.**

Bruck-Ryser-Chowla with v odd: traditional form

Theorem

Suppose that M is the incidence matrix of a symmetric (v, k, λ) design where v is odd. Then the Diophantine equation

$$X^2 - (k-\lambda)Y^2 - (-1)^{\frac{v-1}{2}}\lambda Z^2 = 0$$

has a non-trivial solution.

- **Question:** How do I solve such equations?
- **Marshall Hall**: the computations involved are **detailed and troublesome.**
- **Question:** What does this have to do with design theory?

Bruck-Ryser-Chowla with v odd: traditional form

Theorem

Suppose that M is the incidence matrix of a symmetric (v, k, λ) design where v is odd. Then the Diophantine equation

$$X^2 - (k - \lambda) Y^2 - (-1)^{\frac{v-1}{2}} \lambda Z^2 = 0$$

has a non-trivial solution.

- **Question:** How do I solve such equations?
- **Marshall Hall**: the computations involved are **detailed and troublesome.**
- **Question:** What does this have to do with design theory?
- **Question:** Given a **symmetric positive definite matrix** G, when does there exist a **rational matrix** M such that $MM^\top = G$?

Quadratic forms

Definition

A *quadratic form* is a (multivariate) polynomial in which every term has degree 2.

$$5x^2 + 14xy + 10y^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Quadratic forms

Definition

A *quadratic form* is a (multivariate) polynomial in which every term has degree 2.

$$5x^2 + 14xy + 10y^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

- Linear substitution of variables yields an equivalence operation on forms: $x_0 = x + \frac{9}{5}y$ and $y_0 = 2x + \frac{13}{5}y$ gives

$$x_0^2 + y_0^2 = 5x^2 + 14xy + 10y^2$$

Quadratic forms

Definition

A *quadratic form* is a (multivariate) polynomial in which every term has degree 2.

$$5x^2 + 14xy + 10y^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

- Linear substitution of variables yields an equivalence operation on forms: $x_0 = x + \frac{9}{5}y$ and $y_0 = 2x + \frac{13}{5}y$ gives

$$x_0^2 + y_0^2 = 5x^2 + 14xy + 10y^2$$

- Yields a rational matrix factorisation:

$$MM^\top = \begin{pmatrix} 1 & 2 \\ \frac{9}{5} & \frac{13}{5} \end{pmatrix} \begin{pmatrix} 1 & \frac{9}{5} \\ 2 & \frac{13}{5} \end{pmatrix} = \begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix}$$

$$x^2 + 4xy + 6xz + 4y^2 + 10yz - z^2 \sim \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & -1 \end{bmatrix}.$$

$$x^2 + 4xy + 6xz + 4y^2 + 10yz - z^2 \sim \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & -1 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & -1 \end{bmatrix} \begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & -10 \end{bmatrix}.$$

$$x^2 + 4xy + 6xz + 4y^2 + 10yz - z^2 \sim \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & -1 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & -1 \end{bmatrix} \begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & -10 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 10 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & -10 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 10 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -10 & -10 \\ 0 & -10 & 0 \end{bmatrix}$$

$$x^2+4xy+6xz+4y^2+10yz-z^2 \sim \begin{bmatrix}1 & 2 & 3\\ 2 & 4 & 5\\ 3 & 5 & -1\end{bmatrix}.$$

$$\begin{bmatrix}1 & 0 & 0\\ -2 & 1 & 0\\ -3 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 2 & 3\\ 2 & 4 & 5\\ 3 & 5 & -1\end{bmatrix}\begin{bmatrix}1 & -2 & -3\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\ 0 & 0 & -1\\ 0 & -1 & -10\end{bmatrix}.$$

$$\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 10 & 0\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & -1\\ 0 & -1 & -10\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & 10\\ 0 & 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\ 0 & -10 & -10\\ 0 & -10 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & -1 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & -10 & -10\\ 0 & -10 & 0\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & -1\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\ 0 & -10 & 0\\ 0 & 0 & -10\end{bmatrix}$$

Polarisation is no harder than Gaussian elimination. Every quadratic form can be **polarised**. $S \sim x_0^2 - 10y_0^2 - 10z_0^2 \sim \langle 1, -10, -10\rangle$

Quadratic forms

Definition

Quadratic forms are **congruent** if there exists an invertible linear substitution of variables from one form to the other. If matrices S and T represent the forms, then there exists invertible M such that

$$M^\top SM = T\,.$$

Quadratic forms

Definition

Quadratic forms are **congruent** if there exists an invertible linear substitution of variables from one form to the other. If matrices S and T represent the forms, then there exists invertible M such that

$$M^\top SM = T\,.$$

- Every form can be polarised (over any characteristic 0 field).

Quadratic forms

Definition

Quadratic forms are **congruent** if there exists an invertible linear substitution of variables from one form to the other. If matrices S and T represent the forms, then there exists invertible M such that

$$M^\top SM = T\,.$$

- Every form can be polarised (over any characteristic 0 field).
- **Sylvester:** All invertible (Hermitian) $n \times n$ matrices over $\mathbb{C}$ are congruent.
- **Sylvester:** (Symmetric) Matrices over $\mathbb{R}$ are congruent if and only they have the same number of positive and negative eigenvalues.

Quadratic forms

Definition

Quadratic forms are **congruent** if there exists an invertible linear substitution of variables from one form to the other. If matrices S and T represent the forms, then there exists invertible M such that

$$M^{\top} S M = T \, .$$

- Every form can be polarised (over any characteristic 0 field).
- **Sylvester:** All invertible (Hermitian) $n \times n$ matrices over $\mathbb{C}$ are congruent.
- **Sylvester:** (Symmetric) Matrices over $\mathbb{R}$ are congruent if and only they have the same number of positive and negative eigenvalues.
- Over $\mathbb{Q}$ the question is harder (because $\mathbb{Q}^{*}/\mathbb{Q}^{*2}$ is infinite).

Definition

A symmetric matrix S represents the form $\langle 1, 1, \ldots, 1 \rangle$ if and only if $S = M^\top M$ for some invertible matrix M. Then S is a Gram matrix.

Definition

A symmetric matrix S represents the form $\langle 1, 1, \ldots, 1\rangle$ if and only if $S = M^{\top} M$ for some invertible matrix M. Then S is a Gram matrix.

- If we show $nI + J$ is not a Gram matrix, certain projective planes will not exist.
- If S is a Gram matrix, $\det(S)$ is a square. **Discriminant = 1**

Definition

A symmetric matrix S represents the form $\langle 1, 1, \dots, 1 \rangle$ if and only if $S = M^\top M$ for some invertible matrix M. Then S is a Gram matrix.

- If we show $nI + J$ is not a Gram matrix, certain projective planes will not exist.
- If S is a Gram matrix, $\det(S)$ is a square. **Discriminant = 1**
- If S is a Gram matrix its eigenvalues are positive. **Positive Definite**

Definition

A symmetric matrix S represents the form $\langle 1, 1, \ldots, 1 \rangle$ if and only if $S = M^\top M$ for some invertible matrix M. Then S is a Gram matrix.

- If we show $nI + J$ is not a Gram matrix, certain projective planes will not exist.
- If S is a Gram matrix, $\det(S)$ is a square. **Discriminant = 1**
- If S is a Gram matrix its eigenvalues are positive. **Positive Definite**
- These conditions are not sufficient.

The matrix

$$S = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

is a Gram matrix if and only if S is positive definite, of discriminant 1 and a_0 is a sum of two squares.

The matrix

$$S = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

is a Gram matrix if and only if S is positive definite, of discriminant 1 and a_0 is a sum of two squares.

- Polarise S, since it has discriminant 1, get $\langle a_0, n^2 a_0 \rangle$.

$$\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & n^2 a \end{pmatrix}$$

  so without loss of generality such a form is equivalent to $\langle a, a \rangle$.

The matrix

$$S = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

is a Gram matrix if and only if S is positive definite, of discriminant 1 and a_0 is a sum of two squares.

- Polarise S, since it has discriminant 1, get $\langle a_0, n^2 a_0 \rangle$.

$$\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & n^2 a \end{pmatrix}$$

  so without loss of generality such a form is equivalent to $\langle a, a \rangle$.
- If $a = x^2 + y^2$ then

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

  So $\langle a, a \rangle = \langle 1, 1 \rangle$ if and only if a is a sum of two squares.

The matrix

$$S = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

is a Gram matrix if and only if S is positive definite, of discriminant 1 and a_0 is a sum of two squares.

- Polarise S, since it has discriminant 1, get $\langle a_0, n^2 a_0 \rangle$.

$$\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & n^2 a \end{pmatrix}$$

  so without loss of generality such a form is equivalent to $\langle a, a \rangle$.
- If $a = x^2 + y^2$ then

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

  So $\langle a, a \rangle = \langle 1, 1 \rangle$ if and only if a is a sum of two squares.
- **Fermat:** An integer a is a sum of two squares if and only if no prime $p \equiv 3 \mod 4$ divides the square free part of a.

Definition

For prime p and integer a, a *Legendre symbol* is defined to be $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. It is 1 if a is a quadratic residue and -1 otherwise.

Definition

For prime p and integers a, b, a *Hilbert symbol* is defined to be $(a, b)_p = 1$ if $aX^2 + bY^2 = Z^2$ has a solution (in the p-adics). It is -1 otherwise.

- This is **not** the definition we need for this talk. It is equivalent to the following rules (for odd p).

Definition

For prime p and integer a, a *Legendre symbol* is defined to be $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. It is 1 if a is a quadratic residue and -1 otherwise.

Definition

For prime p and integers a, b, a *Hilbert symbol* is defined to be $(a, b)_p = 1$ if $aX^2 + bY^2 = Z^2$ has a solution (in the p-adics). It is -1 otherwise.

- This is **not** the definition we need for this talk. It is equivalent to the following rules (for odd p).
- $(a, b)_p = 1$ if ab is coprime to p.
- $(a, p)_p = \left(\frac{a}{p}\right)$.

Definition

For prime p and integer a, a *Legendre symbol* is defined to be $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. It is 1 if a is a quadratic residue and -1 otherwise.

Definition

For prime p and integers a, b, a *Hilbert symbol* is defined to be $(a, b)_p = 1$ if $aX^2 + bY^2 = Z^2$ has a solution (in the p-adics). It is -1 otherwise.

- This is **not** the definition we need for this talk. It is equivalent to the following rules (for odd p).
- $(a, b)_p = 1$ if ab is coprime to p.
- $(a, p)_p = \left(\frac{a}{p}\right)$.
- $(p, p)_p = \left(\frac{-1}{p}\right)$ this is 1 if $p \equiv 1 \mod 4$ and -1 if $p \equiv 3 \mod 4$.

Definition

For prime p and integer a, a *Legendre symbol* is defined to be $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. It is 1 if a is a quadratic residue and -1 otherwise.

Definition

For prime p and integers a, b, a *Hilbert symbol* is defined to be $(a, b)_p = 1$ if $aX^2 + bY^2 = Z^2$ has a solution (in the p-adics). It is -1 otherwise.

- This is **not** the definition we need for this talk. It is equivalent to the following rules (for odd p).
- $(a, b)_p = 1$ if ab is coprime to p.
- $(a, p)_p = \left(\frac{a}{p}\right)$.
- $(p, p)_p = \left(\frac{-1}{p}\right)$ this is 1 if $p \equiv 1 \mod 4$ and -1 if $p \equiv 3 \mod 4$.
- $(ab, c)_p = (a, c)_p(b, c)_p$ - the Hilbert symbol is bilinear.

Theorem

Suppose that Q is a quadratic form in two variables, which polarises to $\langle a, a \rangle$. Then Q is congruent to $x^2 + y^2$ if and only if $(a, a)_p = 1$ for every prime p.

Proof.

Suppose p divides the square-free part of a. Then

$$(a, a)_p = (-1, a)_p = \left(\frac{-1}{p}\right)$$

which is -1 if and only if $p \equiv 3 \mod 4$ by **Gauss.**
So $\langle a, a \rangle = \langle 1, 1 \rangle$ if and only if no prime $3 \mod 4$ divides the square-free part of a. This is if-and-only-if a is a sum of two squares by **Fermat**. □

Theorem (Two dimensional Hasse-Minkowski)

A symmetric matrix G is a Gram matrix if and only if

- *It is positive definite.*
- *It has discriminant* 1.
- *For some (in fact, any) polarisation $G = \langle a, a \rangle$, all the Hilbert symbols $(a, a)_p$ are* 1.

Theorem (Two dimensional Hasse-Minkowski)

A symmetric matrix G is a Gram matrix if and only if

- *It is positive definite.*
- *It has discriminant* 1.
- *For some (in fact, any) polarisation* $G = \langle a, a \rangle$, *all the Hilbert symbols* $(a, a)_p$ *are* 1.

- This is all computationally easy, and **very concrete.**
- The Hilbert symbol is bilinear, which simplifies the construction of invariants in higher dimensions.
- Gnilke, Ó C., Olmez, Ponasso: *Invariants of Quadratic Forms and applications in Design Theory*, LAA, 2024.

Definition

Let Q be a quadratic form, equivalent to the polarisation $\langle a_1, a_2, \ldots, a_n \rangle$. The *Hasse-Minkowski invariant* of Q at the prime p is

$$HM(Q, p) = \prod_{i<j} (a_i, a_j)_p \,.$$

Theorem (Hasse-Minkowski, easy part)

A symmetric matrix G is a Gram matrix (if and) only if

- *It is positive definite.*
- *It has discriminant 1.*
- *For some (in fact, any) polarisation $G = \langle a_1, a_2, \ldots, a_n \rangle$, the invariants $HM(Q, p)$ are 1 for all (odd) primes p.*

Hasse-Minkowski is neither detailed nor troublesome (mostly)

$$\begin{aligned}
\langle 5, 7, 21, 15\rangle &= \mathbf{(5,\ 7)}\mathit{(5,\ 21)}\underline{(5, 15)}(7, 21)(7, 15)(21, 15) \\
&= \mathbf{(5,\ 7)}\mathit{(5,7)\ (5,\ 3)}\underline{(5, 3)(5, 5)}(7, 3)(7, 7)\ldots \\
&= \ldots \\
&= (3, 3)(3, 5)(3, 7)(5, 5)(5, 7)
\end{aligned}$$

Hasse-Minkowski is neither detailed nor troublesome (mostly)

$$
\begin{aligned}
\langle 5,7,21,15\rangle &= \mathbf{(5,\,7)}\mathit{(5,\,21)}\underline{(5,15)}(7,21)(7,15)(21,15)\\
&= \mathbf{(5,\,7)}\mathit{(5,7)}\ \mathit{(5,\,3)}\underline{(5,3)(5,5)}(7,3)(7,7)\dots\\
&= \dots\\
&= (3,3)(3,5)(3,7)(5,5)(5,7)
\end{aligned}
$$

For $p = 5$, this evaluates to

$$(3,5)_5(5,5)_5 = \left(\frac{3}{5}\right)\left(\frac{-1}{5}\right) = -1 \cdot 1$$

So $\langle 5,7,21,15\rangle$ and $\langle 1,1,1,1\rangle$ are **not** congruent.

Hasse-Minkowski is neither detailed nor troublesome (mostly)

$$\begin{aligned}\langle 5,7,21,15\rangle &= \mathbf{(5,\,7)}\mathit{(5,\,21)}\underline{(5,15)}(7,21)(7,15)(21,15)\\ &= \mathbf{(5,\,7)}\mathit{(5,7)\ (5,\,3)}\underline{(5,3)(5,5)}(7,3)(7,7)\ldots\\ &= \ldots\\ &= (3,3)(3,5)(3,7)(5,5)(5,7)\end{aligned}$$

For $p = 5$, this evaluates to

$$(3,5)_5(5,5)_5 = \left(\frac{3}{5}\right)\left(\frac{-1}{5}\right) = -1 \cdot 1$$

So $\langle 5,7,21,15\rangle$ and $\langle 1,1,1,1\rangle$ are **not** congruent.
Legendre: $\langle n,n,n,n\rangle \sim \langle 1,1,1,1\rangle$ for any integer n.

Bruck-Ryser

Polarising $(k-\lambda)I + \lambda J$ means constructing a set of orthogonal eigenvectors over $\mathbb{Q}$ for J.

Bruck-Ryser

Polarising $(k-\lambda)I+\lambda J$ means constructing a set of orthogonal eigenvectors over $\mathbb{Q}$ for J.

$$\begin{pmatrix}1 & 1 & 1 & 1 & 1\\ 1 & -1 & 0 & 0 & 0\\ 1 & 1 & -2 & 0 & 0\\ 1 & 1 & 1 & 3 & 0\\ 1 & 1 & 1 & 1 & -4\end{pmatrix}\begin{pmatrix}5 & 1 & 1 & 1 & 1\\ 1 & 5 & 1 & 1 & 1\\ 1 & 1 & 5 & 1 & 1\\ 1 & 1 & 1 & 5 & 1\\ 1 & 1 & 1 & 1 & 5\end{pmatrix}\begin{pmatrix}1 & 1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1 & 1\\ 1 & 0 & -2 & 1 & 1\\ 1 & 0 & 0 & 3 & 1\\ 1 & 0 & 0 & 0 & -4\end{pmatrix}$$

$$= \begin{pmatrix}25 & 0 & 0 & 0 & 0\\ 0 & 2\cdot 4 & 0 & 0 & 0\\ 0 & 0 & 6\cdot 4 & 0 & 0\\ 0 & 0 & 0 & 12\cdot 4 & 0\\ 0 & 0 & 0 & 0 & 20\cdot 4\end{pmatrix} \sim \begin{pmatrix}25 & 0 & 0 & 0 & 0\\ 0 & 4 & 0 & 0 & 0\\ 0 & 0 & 4 & 0 & 0\\ 0 & 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 0 & 4\end{pmatrix}$$

Bruck-Ryser

Polarising $(k-\lambda)I+\lambda J$ means constructing a set of orthogonal eigenvectors over $\mathbb{Q}$ for J.

$$\begin{pmatrix}1&1&1&1&1\\1&-1&0&0&0\\1&1&-2&0&0\\1&1&1&3&0\\1&1&1&1&-4\end{pmatrix}\begin{pmatrix}5&1&1&1&1\\1&5&1&1&1\\1&1&5&1&1\\1&1&1&5&1\\1&1&1&1&5\end{pmatrix}\begin{pmatrix}1&1&1&1&1\\1&-1&1&1&1\\1&0&-2&1&1\\1&0&0&3&1\\1&0&0&0&-4\end{pmatrix}$$

$$=\begin{pmatrix}25&0&0&0&0\\0&2\cdot 4&0&0&0\\0&0&6\cdot 4&0&0\\0&0&0&12\cdot 4&0\\0&0&0&0&20\cdot 4\end{pmatrix}\sim\begin{pmatrix}25&0&0&0&0\\0&4&0&0&0\\0&0&4&0&0\\0&0&0&4&0\\0&0&0&0&4\end{pmatrix}$$

- The pattern generalises, simplifies to $\langle k^2, n, n, \ldots\rangle$ where $n=k-\lambda$.
- Properties of Hilbert symbols simplify this to $(n,n)^{\binom{v-1}{2}}$.

Bruck-Ryser

Polarising $(k-\lambda)I+\lambda J$ means constructing a set of orthogonal eigenvectors over $\mathbb{Q}$ for J.

$$\begin{pmatrix}1 & 1 & 1 & 1 & 1\\ 1 & -1 & 0 & 0 & 0\\ 1 & 1 & -2 & 0 & 0\\ 1 & 1 & 1 & 3 & 0\\ 1 & 1 & 1 & 1 & -4\end{pmatrix}\begin{pmatrix}5 & 1 & 1 & 1 & 1\\ 1 & 5 & 1 & 1 & 1\\ 1 & 1 & 5 & 1 & 1\\ 1 & 1 & 1 & 5 & 1\\ 1 & 1 & 1 & 1 & 5\end{pmatrix}\begin{pmatrix}1 & 1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1 & 1\\ 1 & 0 & -2 & 1 & 1\\ 1 & 0 & 0 & 3 & 1\\ 1 & 0 & 0 & 0 & -4\end{pmatrix}$$

$$= \begin{pmatrix}25 & 0 & 0 & 0 & 0\\ 0 & 2\cdot 4 & 0 & 0 & 0\\ 0 & 0 & 6\cdot 4 & 0 & 0\\ 0 & 0 & 0 & 12\cdot 4 & 0\\ 0 & 0 & 0 & 0 & 20\cdot 4\end{pmatrix} \sim \begin{pmatrix}25 & 0 & 0 & 0 & 0\\ 0 & 4 & 0 & 0 & 0\\ 0 & 0 & 4 & 0 & 0\\ 0 & 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 0 & 4\end{pmatrix}$$

- The pattern generalises, simplifies to $\langle k^2, n, n, \ldots \rangle$ where $n = k - \lambda$.
- Properties of Hilbert symbols simplify this to $(n, n)^{\binom{v-1}{2}}$.
- Non-trivial condition if $n \equiv 1, 2 \mod 4$, requires $n = x^2 + y^2$.
- **Fermat:** There is no projective plane of order 6 or 14 or …

Summary of quadratic forms

- The Hilbert symbols are **computationally easy** to compute (assuming that the matrix entries are factorised).
- Can decide effectively whether symmetric matrices are congruent.
- In contrast, Diophantine equations are typically hard to solve. BRC state their theorem in a way which avoids mention of congruence.

Summary of quadratic forms

- The Hilbert symbols are **computationally easy** to compute (assuming that the matrix entries are factorised).
- Can decide effectively whether symmetric matrices are congruent.
- In contrast, Diophantine equations are typically hard to solve. BRC state their theorem in a way which avoids mention of congruence.
- Hasse-Minkowski theory is non-constructive: typically to not find any congruence matrix (let alone $(0,1)$-congruence matrices).
- The hard (and non-constructive) part of the theorem shows that every global obstruction comes from a local obstruction.
- Deciding whether $(k-\lambda)I + \lambda J = MM^\top$ has a rational solution is, in practice, easy. The condition is that

$$(k-\lambda, (-1)^{v-1/2}\lambda)_p = 1$$

for all primes p.

Back to the symmetric mosaic problem

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Question: For which parameters does there exist a mosaic of symmetric designs?

Proposition

Suppose that M_1, M_2 and $M_1 + M_2$ are incidence matrices of symmetric designs. Define $Q = M_1 M_2^\top + I$. Then $QQ^\top = \sigma I + \tau J$ where $\sigma = (k_1 - \lambda_1)(k_2 - \lambda_2) - \alpha + 1$ and $\tau = v\lambda_1\lambda_2 + \lambda_2(k_1 - \lambda_1) + \lambda_1(k_2 - \lambda_2) + \alpha$.

Theorem

If v is even then

$$(k_1 - \lambda_1)(k_2 - \lambda_2) - \frac{2k_1k_2}{v-1} + 1$$

is the square of an integer. If v is odd, then

$$(\sigma, \sigma)_p^{\binom{v-1}{2}}(\sigma, v)_p = (\sigma, (-1)^{v-1/2}v)_p = 1$$

for all odd primes p.

- Our theorem rules out the only even mosaic on less than $10,000$ points

$$(2380, 183, 14) \oplus (2380, 793, 264) \oplus (2380, 1404, 828)\,.$$

because $13^2 \times 23^2 - 11^2$ is not a square.

- Our theorem rules out the only even mosaic on less than $10,000$ points

$$(2380, 183, 14) \oplus (2380, 793, 264) \oplus (2380, 1404, 828) .$$

because $13^2 \times 23^2 - 11^2$ is not a square.

- As in BRC, the result is weaker in the odd case, ruling out about half of possible parameter sets. It rules out decomposing the complement of a projective plane of order 9:

$$(91, 45, 22) \oplus (91, 36, 14) \oplus (91, 10, 1) .$$

The Hilbert symbol reduces to $(471, 471)_p(471, 91)_p$. At $p = 3$ this is $(3, 3)_p(3, 1)_p = -1$.

- Our theorem rules out the only even mosaic on less than $10,000$ points

$$(2380, 183, 14) \oplus (2380, 793, 264) \oplus (2380, 1404, 828)\,.$$

because $13^2 \times 23^2 - 11^2$ is not a square.

- As in BRC, the result is weaker in the odd case, ruling out about half of possible parameter sets. It rules out decomposing the complement of a projective plane of order 9:

$$(91, 45, 22) \oplus (91, 36, 14) \oplus (91, 10, 1)\,.$$

The Hilbert symbol reduces to $(471, 471)_p(471, 91)_p$. At $p = 3$ this is $(3, 3)_p(3, 1)_p = -1$.

- But the theorem does not rule out existence of a

$$(31, 15, 7) \oplus (31, 10, 3) \oplus (31, 6, 1)\,.$$

Go raibh maith agaibh!