Equivalence of Quadratic Forms

PADRAIG Ó CATHÁIN, RONAN EGAN & PATRICK BROWNE

DCU & TUS

July 8, 2023

The Jordan Canonical Form theorem classifies linear transformations up to change of basis. That is, for any two square matrices A and B, the theory of the JCF gives necessary and sufficient conditions for the existence of an invertible matrix X such that

$$X^{-1}AX = B\,.$$

The rank, determinant and eigenvalues are invariants for equivalence classes of matrices under this conjugacy. These are not sufficient to decide conjugacy however: an understanding of generalised eigenvectors is required (we will not enter into this here).

Recall that the *general linear group* of a vector space V is the set of all invertible linear transforms (forming a group under composition). A matrix is invertible (belongs to the general linear group) if and only if its columns form a basis for V. Given any two bases of V, there exists a linear transformation mapping one to the other: write M_i for the matrix with the vectors of B_i as columns. Then $M_1^{-1}M_2$ maps M_1 to M_2. We conclude that *all bases are equivalent under the action of the general linear group*.

We often motivate linear algebra by describing our own ambient space as $\mathbb{R}^3$. But this is inaccurate: we can perceive a difference between the bases $\{(1,0,0),(0,1,0),(0,0,1)\}$ (called the standard basis) and $\{(20,0,0),(20,1,0),(20,-1,1)\}$ in which all vectors point 'somewhat in the same direction'. In fact, our reality is described by a vector space with additional structure allowing us to measure lengths and angles. We begin by developing some of this language. For historical reasons, this subject has been investigated as part of geometry, algebra, number theory and further abroad in physics and engineering. While indicating the central importance of these topics, it has the unfortunate consequence that every concept has been developed in at least two equivalent ways, and has at least three names.

In these notes we work quadratic forms over a field of characteristic 0 (normally just $\mathbb{Q}$). Informally, a quadratic form assigns lengths to vectors. The equivalent concept of a bilinear form measures the angle between vectors (we make this precise below). Elementary geometry involving trigonometry allows us to translate from one to the other. Just as the JCF gives necessary and sufficient conditions for a pair of linear transformations to be 'the same up to change of basis' the methods described in these notes will allow use to decide when quadratic forms are equivalent in the appropriate sense. These ideas can then be applied to get non-trivial existence conditions for certain types of combinatorial design.

Our motivation will be the study of finite projective planes - by the end of these notes the reader will know the state of the art regarding existence and non-existence of these objects.

1 Quadratic forms: Background and motivation

This material is, of course, well known. But it is often presented in rather greater generality (as the theory of bilinear forms over an arbitrary field) within a more advanced graduate course, or in lesser generality (as the theory of inner product spaces) in a slightly less advanced course. We aim for a middle ground: where it does not lead to additional complication we state the theory in more general terms, but our applications will always require that $\mathbb{F} = \mathbb{Q}$.

Let V be a finite dimensional vector space of dimension n over a field $\mathbb{F}$, of characteristic different from 2. It will be convenient to fix a basis, B, of V. This gives an explicit isomorphism between elements of $\mathrm{End}(V)$ (the set of all linear operators on V) and the matrix algebra $\mathrm{M}_n(\mathbb{F})$. To be entirely clear: if a linear transformation T is defined by $Tb_j = \sum_{i=1}^{n} t_{ij} b_j$ then the matrix of T is $[t_{ij}]_{i,j}$ where $i, j \in [1, \ldots, n]$. While their exist co-ordinate-free axiomatic definitions of quadratic forms, they are not simpler than the following.

Definition 1. A *quadratic form* $Q : V \to \mathbb{F}$ is a function of the form $Q : v \mapsto v^\top A v$ for a matrix $A \in M_n(\mathbb{F})$. We say that the matrix A *represents* the quadratic form, and that the pair (V, Q) is a *quadratic space*. The form is *non-degenerate* if A has full rank.

Provided again that the field is not of characteristic 2, the matrix A may be taken to be a symmetric matrix, for $Q(v) = v^\top A v = v^\top A^\top v$ implies that $Q(v) = v^\top \left(\frac{1}{2}A + \frac{1}{2}A^\top\right) v$. We will always assume that A is symmetric. Associated to Q there is a *bilinear form* defined by

$$\langle x, y \rangle = \frac{1}{2} \left(Q(x + y) - Q(x) - Q(y) \right) .$$

Working in terms of matrices, $\langle x, y \rangle = x^\top A y$. From a symmetric bilinear form, we recover a quadratic form as $Q(v) = \langle v, v \rangle$. As an example of constructing the matrix of a bilinear form: let P_2 denote the space of real polynomials in one variable of degree at most 2, this is spanned by $\{1, x, x^2\}$. Define a bilinear form on P_2 by

$$\langle f, g \rangle := \int_0^1 f(x) g(x) \, dx \text{ for all } f, g \in P_2.$$

The matrix associated to this form is constructed by the bilinear form applied to the spanning set indexed appropriately

$$\langle x^{i-1}, x^{j-1} \rangle = \int_0^1 x^{i+j-2} \, dx = \frac{1}{i + j - 1}.$$

So that the matrix associated to the bilinear form is

$$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{pmatrix}.$$

The reader will have encountered many bilinear forms. For example:

1. The standard dot product is a bilinear form, with $v \cdot w = v^\top I_n w$.

2. In special relativity, spacetime is a 4-dimensional real vector space S, endowed with a quadratic form with diagonal entries $(1, 1, 1, -1)$. The space-like co-ordinates have positive entries while the time-like co-ordinate has a negative entry. The vectors which satisfy $Q(v) = 0$ are the *light-cone* at the origin. The Lorentzian transformations are those $L : S \to S$ for which $Q(Lv) = Q(v)$ for all $v \in S$. Much of the strange behaviour of special relativity comes from the assumption that the speed of light is finite and systematic application of linear algebra.

3. In Hamiltonian mechanics, each body is specified by an n dimensional position vector and an n dimensional momentum vector. Considering the $2n$ dimensional vector space spanned by $\{p_1, \ldots, p_n\}$ (giving the position) and $\{m_1, \ldots, m_n\}$ (giving the momentum) there is a natural bilinear form defined by $\langle p_i, m_j \rangle = 1$ if $i = j$ and 0 otherwise, and $\langle m_i, p_i \rangle = -1$. Such bilinear forms are called *symplectic*.

We will deal almost exclusively with the quadratic forms in this text, though we note that our results translate easily to the context of bilinear forms.

1.1 Inner products and positive definiteness

Provided that the field satisfies $\mathbb{Q} \leq \mathbb{F} \leq \mathbb{R}$, we have the following definition.

Definition 2. A bilinear form $\langle , \rangle$ is *positive definite* if $\langle v, v \rangle > 0$ for all non-zero $v \in V$. An *inner product* on a real vector space V is a bilinear form that is both positive definite and symmetric.

Similarly, a matrix is positive definite if $v^t A v > 0$ for all non zero $v \in V$. A bilinear form on V is positive definite if and only if the matrix of the form with respect to some basis is positive definite. Clearly a form is positive definite if and only if all eigenvalues of an associated matrix A are positive. The dot product is a simple example of a positive definite form since

$$\langle x, x \rangle = \sum_{i=1}^{n} x_i x_i = \sum_{i=1}^{n} x_i^2 > 0.$$

This allows us to define the length of a vector as $\| v \| = \sqrt{\langle v, v \rangle}$. Once lengths are assigned to vectors, the standard trigonometric functions allow the definition of angles, by

$$\cos\theta := \frac{\langle v, w \rangle}{\| v \| \| w \|},$$

where θ is the angle between v and w. We now quote a result that underpins a lot of our established geometric intuition.

Theorem 3 (Cauchy-Schwarz)**.** *When v is a real vector space with an inner product then*

$$|\langle v, w \rangle| \leq \| v \| \| w \|$$

The well known triangle inequality, $\| u + v \| \leq \| u \| + \| v \|$, is a simple consequence of Cauchy-Schwarz.

We will occasionally need to decide whether a given bilinear form or symmetric matrix is positive definite. A necessary and sufficient condition is that all eigenvalues of the matrix are positive. Another useful result is the following.

Theorem 4 (Sylvester's Criterion)**.** *An $n \times n$ symmetric matrix A is positive definite if and only if $det(A_k) > 0$ for all $1 \leq k \leq n$, where A_k is the $k \times k$ upper left submatrix (leading minor) of A.*

We illustrate this with a 3×3 matrix. Let

$$A = \begin{pmatrix} a & 1 & 1 \\ 1 & 1 & a \\ 1 & a & 5 \end{pmatrix}$$

By Sylvester's criterion, A is positive definite if and only if,

$$a > 0,\ det \begin{pmatrix} a & 1 \\ 1 & 1 \end{pmatrix} > 0,\ det(A) > 0$$

. It is left as an exercise to show that this implies that A is positive definite if and only if $1 < a < 2$.

Example 5. An application of the above that the reader would be familiar with is the standard second derivative test from undergraduate calculus.
Let $f(x, y)$ be a function of two variables, and u a vector. We can ask for the directional derivative of f along u. This is just $D_u(f) = u_1 f_x + u_2 f_y$ (with D being the differential and subscripts for partials). Taking a second derivative while messy is straightforward and yields

$$u_1(u_1 f_x + u_2 f_y)_x + u_2(u_1 f_x + u_2 f_y)_y = u_1^2 f_{xx} + u_1 u_2 f_{yx} + u_2 u_1 f_{xy} + u_2^2 f_{yy}.$$

This is more neatly expressed as $u^t Au$, with

$$A = \begin{pmatrix} f_{xx} & f_{yx} \\ f_{xy} & f_{yy} \end{pmatrix}.$$

This is a symmetric matrix with real eigenvalues, and their signs determine the usual three cases.

1.2 Symmetric and self-adjoint operators

In this section V is a vector space over a subfield k of the complex numbers $\mathbb{C}$. If k is not contained in $\mathbb{R}$ then complex conjugation acts nontrivially on k. To ensure positivity of a bilinear form, it is necessary to define

$$\langle x, y\rangle = \overline{\langle y, x\rangle},$$

and by convention we take the form to be conjugate-linear in the first argument, that is $\langle \lambda x, y\rangle = \lambda^* \langle x, y\rangle$ but $\langle x, \lambda y\rangle = \lambda \langle x, y\rangle$. For the sake of clarity, the conjugate transpose of a matrix is obtained by transposing a matrix, and then taking the complex conjugate of all entries. We write z^* for the complex conjugate of a number and M^* for the conjugate transpose of a matrix. We **never** apply the conjugate operation to a matrix without also taking the transpose, so the notation should not cause confusion.

Definition 6. Let V be a quadratic space and $T : V \to V$ an operator. The *adjoint* of T is the conjugate transpose of T, which satisfies $\langle Tv, w\rangle = \langle v, T^* w\rangle$ for all $v, w \in V$. We say that T is *self-adjoint* if it equals its own adjoint, that is $\langle Tv, w\rangle = \langle v, Tw\rangle$ for all $v, w \in V$.

If V carries the standard dot product over $\mathbb{R}$ then $T = T^\top$ and T is *symmetric*. If V carries the standard inner product over $\mathbb{C}$ then $T^* = T$, the conjugate transpose of T. Confusingly for those thinking of the formulae for determinants and matrix inverses, this *adjoint* has nothing to do with cofactors and minors.

Definition 7. A matrix equal to its own conjugate transpose is said to be *Hermitian*, or self adjoint.

Physicists often write $A^\dagger$ for the conjugate transpose over $\mathbb{C}$. The next result shows that symmetric and hermitian matrices have real eigenvalues.

Proposition 8. *The eigenvalues of a self-adjoint operator are real.*

Proof. Let $v \in V$ be an eigenvector of T with eigenvalue λ. Then

$$\lambda\langle v, v\rangle = \langle Tv, v\rangle = \langle v, Tv\rangle = \langle v, \lambda v\rangle = \lambda^* \langle v, v\rangle.$$

Since $\langle v, v\rangle \neq 0$, it follows that $\lambda = \lambda^*$. Hence λ is real. □

Next we will show that a generalised eigenvector of a self-adjoint operator is already an eigenvector. It will follow that all self-adjoint operators are diagonalisable.

Theorem 9. *A self-adjoint operator over $\mathbb{R}$ or $\mathbb{C}$ is diagonalisable.*

Proof. Suppose that v is a generalised eigenvector of the self-adjoint operator T. By Proposition 8 we may assume that the corresponding eigenvalue is real. Then $T - \lambda I$ is also self-adjoint, because

$$(T - \lambda I)^* = T^* - \lambda^* I = T - \lambda I.$$

Let k be the least integer for which $(T - \lambda I)^k v = 0$. Then $w = (T - \lambda I)^{k-1} v$ is an eigenvector of T with eigenvalue λ. Now consider the inner product

$$\langle w, w\rangle = \langle (T - \lambda I)^{k-1} v, (T - \lambda I)^{k-1} v\rangle = \langle v, (T - \lambda I)^{2k-2} v\rangle.$$

If $2k + 2 \geq k$ then $(T - \lambda I)^{2k+2} v = \mathbf{0}$, which would contradict the positive-definiteness of the inner product. Hence $2k - 2 < k$, which forces $k = 1$. So $(T - \lambda I)v = 0$ and $w = v$. We conclude that every generalised eigenvector of T is already an eigenvector. □

Corollary 10. *Suppose that T is self-adjoint and $\langle Tv, v\rangle = 0$ for all $v \in V$. Then $T = \mathbf{0}$.*

Proof. Let v be an eigenvector of T. Then $\langle Tv, v\rangle = \lambda\langle v, v\rangle = 0$. By positive definiteness, $\lambda = 0$. Hence all eigenvalues of T are zero. But T is diagonalisable by Theorem 9. So V admits a basis of eigenvectors, all of which have eigenvalue 0. So $N(T) = V$ and T is the zero matrix. □

Definition 11. Quadratic forms Q_1 and Q_2 are *equivalent* if there exists an invertible linear transformation M such that

$$Q_1(Mv) = Q_2(v)\,.$$

If Q_1 and Q_2 are represented by the matrices A_1 and A_2 respectively, then

$$Q_1(Mv) = v^\top M^\top A_1 M v = v^\top A_2 v\,,$$

for all vectors $v \in V$. We say that symmetric matrices A_1 and A_2 are *congruent* if there exists an invertible M such that $M^\top A_1 M = A_2$.

There are a few normal forms to which symmetric matrices can be reduced. For our purposes, the following reduction will suffice.

Proposition 12. *Suppose that S is a symmetric matrix defined over $\mathbb{Q}$. There exists a matrix M with entries in $\mathbb{F}$ such that $S' = M^\top S M$ is a diagonal matrix. Furthermore, the entries of S' can be taken to be square-free integers arranged in increasing order.*

Proof. Left multiplication by a matrix $M^\top$ corresponds to a sequence of row operations on S, while right multiplication by M corresponds to precisely the same operations on columns. Since $(M^\top S)M = M^\top(SM)$ by associativity of matrix multiplication, these row and column operations commute. In particular, the matrix $M^\top$ may be chosen so that $M^\top S$ is in lower triangular form. Since S is assumed to be symmetric, right multiplication by M diagonalises the matrix. (The usual caution about reordering rows if a diagonal element is zero applies, and the matrix M can be chosen integral by multiplying through by all denominators.)

It is clear that conjugation by a permutation matrix places the diagonal elements in arbitrary order, and multiplying the i^{th} row and column by d^{-1} eliminates any term d^2 on the diagonal. □

Remark 13. While row operations are familiar to every student of linear algebra, we illustrate the process in the interests of absolute clarity. Consider the matrix

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & -1 \end{pmatrix}.$$

We begin by eliminating the off-diagonal entries in the first row, and then the first column.

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

Since we have a zero pivot in position $(2,2)$, we swap the second and third rows. And since we work only to similarity, we can multiply the third row and column by -10, to achieve the matrix

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

Finally, subtracting the second row from the third and likewise for columns leaves a matrix with diagonal elements $\langle 1, -10, 10\rangle$. The matrix M can be computed explicitly by multiplying out the row operation matrices if desired.

Our convention is that the quadratic form represented by the diagonal matrix with entries $a_1, a_2, \ldots, a_n$ is denote $\langle a_1, a_2, \ldots, a_n \rangle$. Just as with row operations, the process above is not canonical: it involves choice. Unlike the reduced row echelon form, the result does depend on the choices made. For example,

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & -3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & -3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -10 & 0 \\ 0 & 0 & 10 \end{bmatrix},$$

so the matrix S of the example above also represents the quadratic form $\langle 1, -1, 1 \rangle$. Note that neither $\langle 1, -10, 10 \rangle$ nor $\langle 1, -1, 1 \rangle$ are the eigenvalues of S, which has characteristic polynomial $\lambda^4 - 4\lambda^2 - 39\lambda + 1$, which is an irreducible cubic with eigenvalues of approximately $8.5, -4.5, 0.02$. The quadratic form representatives detect the number of positive and negative eigenvalues of the matrix, but not their values. The theory of quadratic forms is to a large extent the resolution of quadratic forms into equivalence classes. We complete this classification now for the real and complex fields. We write $\mathbf{1}_d$ for the vector of length d with all entries equal to 1.

Theorem 14 (Sylvester's Law of Inertia)**.** *Let V be an n-dimensional vector space over $\mathbb{R}$. For a quadratic form Q on V there exist integers d, e, f such that Q is equivalent to a form $\langle \mathbf{1}_d, \text{-}\mathbf{1}_e, \mathbf{0}_f \rangle$. The pair (d, e) is the inertia of the form.*

Proof. By the general theory we have established, a quadratic form Q is represented by a symmetric matrix S which may be assumed diagonal, since it admits an orthonormal basis of eigenvectors. Suppose that the diagonal entries are $s_1, \ldots, s_n$, without loss of generality assume that s_i are ordered by decreasing absolute value. Since every positive real number has a square root in $\mathbb{R}$ we can multiply on both sides by an invertible real matrix X having diagonal entries $|s_i|^{-1/2}$ if $s_i \neq 0$ and 1 otherwise. Then $X^\top S X$ has all non-zero entries equal to 1 or -1. □

In the theory of quadratic forms, elements which differ by a square are typically regarded as equivalent. Theorem 14, takes the form it does because every non-zero real number may be written as $\pm x^2$, that is $\{\pm 1\}$ are coset representatives of the square group in the multiplicative group of the reals. In the complex numbers, every non-zero element is a square, and it is left as an exercise to the reader to show that the only invariants of a quadratic form over $\mathbb{C}$ are the rank of an associated matrix and the dimension of the underlying space. In contrast, over $\mathbb{Q}$ the quotient of the multiplicative group by the group of squares is infinite (generated by the prime numbers). So the theory of quadratic forms is rather richer there. We address this next.

2 Classification of quadratic forms over $\mathbb{Q}$ in dimension 2

Recall that a quadratic form $\mathcal{Q}$ over $\mathbb{Q}$ may be represented by a diagonal matrix S with integer entries. Any other matrix representing the same form is equal to $M^\top S M$ for some invertible integer matrix M. Conversely, forms represented by S_1 and S_2 are equivalent if and only if there exists an M such that $M^\top S_1 M = S_2$.

Clearly, one-dimensional forms $\langle a \rangle$ and $\langle b \rangle$ are similar if and only if ab is a square. In particular, the forms equivalent to $\langle 1 \rangle$ are precisely those given by rational squares. The first interesting case is the classification of quadratic forms in dimension 2. We will describe all forms equivalent to $\langle 1, 1 \rangle$. The following classical result of Fermat is the crucial insight required.

Theorem 15 (cf. Ireland and Rosen)**.** *A prime is a sum of two (integer) squares if and only if $p = 2$ or $p \equiv 1 \mod 4$.*

Proposition 16. *For prime p, the quadratic forms $\langle p, p \rangle$ and $\langle 1, 1 \rangle$ are similar if and only if $p = 2$ or $p \equiv 1 \mod 4$.*

Proof. Suppose that $p = a^2 + b^2$. Then

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} .$$

By Theorem 15 the form $\langle p, p \rangle$ is similar to $\langle 1, 1 \rangle$ for $p = 2$ or for $p \equiv 1 \mod 4$.

Conversely, suppose that $\langle p, p \rangle$ is a quadratic form equivalent to $\langle 1, 1 \rangle$. Then $pI_2 = M^\top M$ for some rational matrix M. Vanishing of the top-right entry in pI_2 essentially forces the matrix M to be as in the displayed equation, then the top left entry of $M^\top M$ is a sum of two squares. If $p \equiv 3 \mod 4$, then p is not a sum of two squares and hence $\langle p, p \rangle$ is not equivalent to $\langle 1, 1 \rangle$. □

From Proposition 16, it is not too difficult to describe all quadratic forms in dimension two which are similar to I_2.

Corollary 17. *In dimension 2 a quadratic form is congruent to $\langle 1, 1 \rangle$ if and only if it may be written as $\langle a, x^2 a \rangle$ where a is a sum of two squares and x is a non-zero integer.*

Proof. By the argument of Proposition 16, the forms $\langle a, x^2 a \rangle$ and $\langle 1, 1 \rangle$ are similar if and only if a may be written as a sum of two squares. □

The integers which are a sum of two squares may be characterised precisely. The Brahmagupta-Fibonacci identity,

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 ,$$

shows that the product of sums of two squares is again a sum of two squares. Write $n = mr^2$, where m is square-free. Clearly $r^2 + 0$ is a sum of two squares, while by Theorem 15 and the Brahmagupta-Fibonacci identity, m is a sum of two squares if and only if all of its prime factors are 2 or equivalent to $1 \mod 4$.

What then may be said of the other equivalence classes of quadratic forms? Suppose that p, q are distinct primes congruent to $3 \mod 4$. By the argument of Proposition 16, the forms $\langle p, p \rangle$ and $\langle q, q \rangle$ are congruent if and only if there exists an integer solution to

$$p(\frac{a^2 + b^2}{d^2}) = q ,$$

for integers a, b, d. Suppose first that d is coprime to p, then $p(a^2 + b^2) = qd^2$ is an integer equation, and p divides q. But this is absurd as p and q are distinct primes. Otherwise, p^2 divides d^2, say that $d = pt$. Then one obtains an integer equation $a^2 + b^2 = pqt^2$, but the square-free part of the right-hand side is divisible by a prime which is 3 mod 4, leading to a contradiction. Hence the forms $\langle p, p \rangle$ for primes $p \equiv 3 \mod 4$ are all inequivalent. Similarly the form $\langle pq, pq \rangle$ is inequivalent to $\langle p, p \rangle$ and $\langle q, q \rangle$. Observe that a quadratic form of discriminant 1 (i.e. square determinant) in dimension 2 is necessarily of the form $\langle a, x^2 a \rangle$ where a and x are integers. We may now classify forms in dimension 2 of discriminant 1 over $\mathbb{Q}$.

Theorem 18. *Denote by $r_3(n)$ the product of all primes congruent to 3 modulo 4 which divide the square-free part of n. The quadratic forms $\langle n, x^2 n \rangle$ and $\langle m, y^2 m \rangle$ are similar if and only if $r_3(n) = r_3(m)$.*

Proof. Observe that

$$\begin{bmatrix} 1 & 0 \\ 0 & x^{-1} \end{bmatrix} \begin{bmatrix} n & 0 \\ 0 & x^2 n \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & x^{-1} \end{bmatrix} = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} ,$$

so nothing is lost by considering only the forms $\langle n, n \rangle$ and $\langle m, m \rangle$.

Next, write $n = r_3(n)n'$ where n' can be written as a sum of two integer squares, say $n' = a^2 + b^2$. Then

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} r_3(n) & 0 \\ 0 & r_3(n) \end{bmatrix} \begin{bmatrix} a & b \\ b & -a \end{bmatrix} = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} ,$$

so $\langle n, n\rangle$ is similar to $\langle r_3(n), r_3(n)\rangle$. Since similarity in an equivalence relation, it follows that when $r_3(n) = r_3(m)$ the forms $\langle n, n\rangle$ and $\langle m, m\rangle$ are similar.

Finally, suppose that $r_3(n) \neq r_3(m)$. Then without loss of generality there exists a prime $p \equiv 3 \mod 4$ such that $p \mid n$ and $p \nmid m$. If the forms were similar we would obtain a rational equation

$$(a^2 + b^2x^2)n = m$$

Multiplying through by the square of the common denominator of a and b leaves an integer equation where by hypothesis the highest power of p dividing the left hand side is odd, while the highest power dividing the right hand side is even. This is absurd, and hence $\langle n, n\rangle$ and $\langle m, m\rangle$ cannot be similar. □

2.1 Legendre and Hilbert symbols

The standard treatments of quadratic forms adopt the language of Hilbert symbols for the discussion of quadratic forms in higher dimensions. Such symbols have the advantage of being easily manipulated algebraically, while capturing the classification of Proposition 18 precisely.

Definition 19. For prime number p and a coprime to p, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 1 if $x^2 \equiv a \mod p$ has a solution, and -1 otherwise.

It is often convenient to set $\left(\frac{0}{p}\right) = 0$, though we will not require this convention. Many authors say that a is a *quadratic residue modulo* p if $\left(\frac{a}{p}\right) = 1$, and a *quadratic non-residue* otherwise. It follows directly from the definition of the Legendre symbol that $\left(\frac{a^2}{p}\right) = 1$ and that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ where $a \equiv b \mod p$. It is easily established that the Legendre symbol is multiplicative in the sense that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ which reduces the evaluation to prime arguments. Gauss' celebrated law of quadratic reciprocity gives an efficient reduction for evaluation of such symbols.

Theorem 20 (Gauss, cf. Chapter 5, Ireland and Rosen)**.** *Let p and q be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

The symbol $\left(\frac{-1}{q}\right)$ evaluates to 1 if $q \equiv 1 \mod 4$ and -1 if $q \equiv 3 \mod 4$. The symbol $\left(\frac{2}{q}\right)$ evaluates to 1 if $q \equiv \pm 1 \mod 8$ and -1 if $q \equiv \pm 3 \mod 8$.

For the reader unfamiliar with Legendre symbols, we provide multiple computations below.

Example 21. The symbol $\left(\frac{4}{p}\right)$ evaluates to 1 for every prime since 4 is a square in the integers. The symbol $\left(\frac{2}{7}\right)$ evaluates to 1 because $3^2 \equiv 2 \mod 7$. The symbol $\left(\frac{2}{11}\right) = -1$ because 2 is not a quadratic residue. (This may be verified exhaustively, or by observing that $2 \equiv -9 \mod 11$, then use that the negative of a residue is a non-residue when $p \equiv 3 \mod 4$.)

Larger examples are evaluated by repeatedly flipping the terms in the symbol, factoring and evaluating 'easy' terms.

$$\left(\frac{31}{103}\right) = (-1)\left(\frac{103}{31}\right) = (-1)\left(\frac{10}{31}\right) =$$
$$(-1)\left(\frac{2}{31}\right)\left(\frac{5}{31}\right) = (-1)\left(\frac{2}{31}\right)\left(\frac{31}{5}\right) = (-1)\left(\frac{2}{31}\right)\left(\frac{1}{5}\right) = -1$$

In the last step, we used that the remaining Legendre symbols evaluate to 1.

$$\left(\frac{29}{151}\right) = \left(\frac{151}{29}\right) = \left(\frac{6}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{29}{3}\right) = \left(\frac{2}{29}\right)\left(\frac{2}{3}\right) = 1$$

We can verify with a computer that $28^2 \equiv 29 \mod 151$ so that the Legendre symbol is indeed correct.

Next, we introduce the Hilbert symbol, which was developed precisely to characterise equivalence of quadratic forms.

Definition 22. Define the *Hilbert symbol* $(a,b)_p$ for non-zero integers a, b and prime p to be 1 if the equation

$$ax^2 + by^2 = 1$$

has a solution in the p-adic numbers $\mathbb{Q}_p$ and -1 otherwise.

The definition mentions the p-adic numbers, which properly form the *local* part of the *local-global* theory of quadratic forms. They will not be necessary for our purposes: the value of the Hilbert symbol can always be determined in terms of Legendre symbols. Note that the integers form a subring of $\mathbb{Q}_p$ for all primes p and so an integer solution of Hilbert's equation means that the corresponding Hilbert symbols evaluate to 1 for any prime p. The following identities for the Hilbert symbol are immediate from the definition:

$$(a,b)_p = (b,a)_p, \;\; (a^2,b)_p = 1$$

the first identity by swapping variables x and y, the second by setting $x = a^{-1}$ and $y = 0$.

For an odd prime p the following properties hold, proofs may be found in Theorem 2 of Chapter 3 of Serre's *Arithmetic*.

1. $(a_1a_2, b)_p = (a_1, b)_p(a_2, b)_p$, the Hilbert symbol is *bilinear*.
2. If a and b are both coprime to p then $(a,b)_p = 1$.
3. $(a,p)_p = \left(\frac{a}{p}\right)$, this case of the Hilbert symbol reduces to the Legendre symbol.
4. $(p,p)_p = \left(\frac{-1}{p}\right)$ so $(p,p)_p = 1$ if $p \equiv 1 \mod 4$ and $(p,p)_p = -1$ if $p \equiv 3 \mod 4$.

Example 23. To illustrate the evaluation of the Hilbert symbol, we compute $(21, 33)_3$. By bilinearity, this the symbol splits into prime factors. By the remaining properties of the Hilbert symbol, each term is either trivial or evaluated in terms of a Legendre symbol as follows:

$$(3,3)_3(3,11)_3(7,3)_3(7,11)_3 = \left(\frac{-1}{3}\right)\left(\frac{11}{3}\right)\left(\frac{7}{3}\right) = 1\,.$$

Remark 24. In this paper, we restrict attention almost entirely to odd primes. The rules for manipulating $(a,b)_2$ are slightly more complicated than for odd primes, but are given in any specialist text on quadratic forms. We also overlook the so-called infinite prime (called the prime -1 by Conway) which relates to solvability of the equation $ax^2 + by^2 = 1$ in the real numbers, so $(a,b)_\infty = 1$ provided at least one of a and b is positive. Since we deal only with positive definite matrices in this paper, the Hilbert symbol at infinity is always 1.

Artin's *Global Product Formula* for Hilbert Symbols states that all-but-one of the Hilbert symbols determines the last one, where we quantify over primes. Hence if a (positive definite) quadratic form differs from I_n at $p = 2$ it also differs at an odd prime, and this fact can be detected there. So computing Hilbert symbols at odd primes suffices for our purposes.

Let us conclude this section with an explicit demonstration that Hilbert symbols characterise equivalence of quadratic forms in two dimensions.

Theorem 25 (cf. Proposition 18)**.** *Let m, n, x, y be positive integers. Quadratic forms $\langle n, nx^2\rangle$ and $\langle m, my^2\rangle$ are similar if and only if $(n, nx^2)_p = (m, mx^2)_p$ for every odd prime.*

Proof. First, by elementary properties of the Hilbert symbol

$$(n, nx^2)_p = (n,n)_p(n,x^2)_p = (n,n)_p\,.$$

Write $n = a^2n'p^t$ where n' is square-free and coprime to p, and $t \in \{0,1\}$ (note that p may divide a). Then $(n,n)_p = (p^t, p^t)_p$. This symbol evaluates to -1 if and only if $t = 1$ and $p \equiv 3 \mod 4$. So the Hilbert symbol detects the primes which are congruent to 3 modulo 4 which divide the square-free part of n. □

Observe that Theorem 25 is precisely equivalent to Theorem 18, but the rules for manipulating the Hilbert symbol will be required to compute invariants in higher dimensions.

Let us conclude this section with a summary of the discussion up to this point:

1. In dimension 2 a quadratic form of discriminant 1 is necessarily of the form $\langle a, x^2 a\rangle$. Every such form is equivalent to $\langle m, m\rangle$, for square-free integer m.

2. Two such forms are equivalent if and only if the set of primes congruent to $3 \mod 4$ dividing the square-free part of a are equal. We established this via elementary arguments.

3. The Hilbert symbols associated with $\langle a, a\rangle$ are $(a, a)_p$ where we allow p to range over the odd primes. Bilinearity of the Hilbert symbol reduces its evaluation to the Legendre symbol, and Gauss' Reciprocity Law allows practical evaluation of the Legendre symbol. The Hilbert symbol $(a, a)_p$ evaluates to -1 if and only if p is a prime congruent to $3 \mod 4$ dividing the square free part of n.

4. Two quadratic forms are equivalent only if their Hilbert symbols agree at all odd primes. This may be expressed in terms of the Hilbert symbols, which will be more convenient in dimensions larger than 2. (In fact, form agreeing at all Hilbert symbols are equivalent, this is the harder direction of the Hasse-Minkowski theorem. We do not require this for our applications.)

In the next section, we will extend the Hilbert symbol to an invariant of quadratic forms in dimension n.

3 Exercises for the morning session

1. Let J_n be the all ones matrix. For each of the following matrices S_i, find an integer matrix M such that $M^\top S_i M$ is a diagonal integer matrix.

   (a) J_4

   (b) $4I_5 + J_5$

   (c) $2I_7 + J_7$

2. Decide whether 61 is a quadratic residue modulo the primes $101, 103, 107$.

3. Compute the Hilbert symbol of $px^2 + 61y^2 = 1$ for $p = 101, 103, 107$. Decide whether each of these equations has a rational solution.

4. In the next set of lecture notes, we extend the Hilbert symbol to higher dimensional forms as

$$H_p\langle a_1, \ldots, a_n\rangle = \prod_{i<j} (a_i, a_j)_p \,.$$

   Taking this as given, compute the invariants for $\langle 2, 3, 6, 10, 20\rangle$ at the primes $p = 2, 3, 5$ and decide whether it is equivalent to the identity matrix I_5.

4 Invariants for Quadratic forms in dimension n

Recall that a rational quadratic form in n dimensions is represented by a symmetric $n \times n$ matrix A with integer entries, and any other matrix representing the same form is $M^\top AM$ for some invertible matrix M.

Definition 26. The *discriminant* of a square integer matrix A is the square-free part of the determinant of A. The *signature* of A is the number of positive, zero and negative eigenvalues of A.

Proposition 27. *Let A be a matrix representing the quadratic form Q. Then the discriminant and signature of A are invariants of Q.*

It is trivial to see that the discriminant is an invariant of quadratic forms. That the signature is an invariant does require proof: in the special case of the real field, this is Sylvester's *Law of Inertia*. The proof is contained in any text discussion quadratic forms. In this section, we develop more subtle arithmetic invariants of quadratic forms. This theory was developed by Hilbert, Hasse and Minkowski in the early twentieth century. We follow the exposition of Pall quite closely.

Recall that a *minor* of a matrix is the determinant of a square submatrix. The *principal minor* $M_{i,j}$ of an $n \times n$ matrix M is obtained by deleting row i and column j, and taking the determinant of the $(n-1)\times(n-1)$ submatrix remaining. The k^{th} *leading minor* of M is the determinant of the $k \times k$ submatrix in the upper left of M, which we denote m_k. In particular, $m_n = \det(M)$.

Definition 28. Let A be an $n \times n$ symmetric matrix with rational entries. The *Pall invariant* of A at the prime p is

$$c(A,p) = (-1, -m_n)_p \prod_{i=1}^{n-1} (m_i, -m_{i+1})_p \,,$$

where m_i is the i^{th} leading minor of A.

We will prove that $c(A,p)$ is in fact an invariant of quadratic forms: that it depends only on the congruence class of A. To do this we will require the following lemma on determinants, which was already well-known in the nineteenth century.

Lemma 29. *Let M be an $n \times n$ symmetric positive definite matrix. Denote by $M_{i,j}$ the minor of M obtained by removing the i^{th} row and j^{th} column, and for $i \neq j$, let $M_{[i,j]}$ be the $(n-2)\times(n-2)$ submatrix obtained from M by removing the i-th and j-th rows and the i-th and j-th columns. Then*

$$\det(M)\det(M_{[i,j]}) = M_{i,i}M_{j,j} - (M_{i,j})^2,$$

Proof. Since M is positive definite, it is invertible. Write N for the inverse of M. Decompose both matrices into block matrices,

$$M = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}, \quad N = \begin{bmatrix} N_1 & N_2 \\ N_3 & N_4 \end{bmatrix},$$

where M_1 and N_1 are $k \times k$ and M_4 and N_4 are $(n-k)\times(n-k)$. Consider the matrix identity

$$\begin{bmatrix} N_1 & N_2 \\ N_3 & N_4 \end{bmatrix} \begin{bmatrix} M_1 & 0 \\ M_3 & I \end{bmatrix} = \begin{bmatrix} I & N_2 \\ 0 & N_4 \end{bmatrix}.$$

Taking determinants, $\det(N)\det(M_1) = \det(N_4)$. Since the determinant of M is unchanged after a *symmetric* row/column permutation, we may assume without loss of generality that $M_1 = M_{[i,j]}$ and that

$$M_4 = \begin{bmatrix} m_{ii} & m_{ij} \\ m_{ij} & m_{jj} \end{bmatrix}.$$

Since N is the inverse of M, the entries of N are principal minors of M, multiplied by $\det(M)^{-1}$. So, up to a -1 factor which cancels out in the final formula, we find that

$$N_4 = \frac{1}{\det(M)} \begin{bmatrix} M_{i,i} & -M_{i,j} \\ -M_{i,j} & M_{j,j} \end{bmatrix}.$$

Therefore

$$\det(N)\det(M_1) = \det(M)^{-1}\det(M_{[i,j]}) = \det(N_4) = \det(M)^{-2}(M_{i,i}M_{j,j} - (M_{i,j})^2).$$

Multiplying by $\det(M)^2$ concludes the proof. □

By the theory of the Row Echelon Form, any invertible matrix may be reduced to the identity by a sequence of elementary row operations: permuting rows, adding one row to another and multiplying a row by a scalar. As a consequence, $\mathrm{GL}_n(\mathbb{Q})$ is generated by the matrices associated with these row operations.

Theorem 30. *Let A be a positive definite rational matrix. Then for each $N \in \mathrm{GL}_n(\mathbb{Q})$,*

$$c(A,p) = M(N^\intercal AN, p)\,.$$

Proof. It suffices to show that the Pall invariants are preserved by such matrices. To show that the Pall invariants are preserved by arbitrary (simultaneous) permutation of rows and columns, it will suffice to show that they are preserved by transpositions $(i, i+1)$ of adjacent rows or columns, since these permutations generate the symmetric group.

The leading minors of the matrix $M' = P^\intercal MP$ coincide with those of M except possibly for m_i and m_i', since all other leading minors are either unchanged, or have a pair of rows and columns swapped, leaving the determinant unchanged. It will suffice to show that

$$(m_{i-1}, -m_i')_p(m_i', -m_{i+1})_p = (m_{i-1}, -m_i)_p(m_i, -m_{i+1})_p.$$

Using bilinearity of the Hilbert symbol we find that the above equation is equivalent to

$$(m_i', -m_{i-1}m_{i+1})_p = (m_i, -m_{i-1}m_{i+1})_p.$$

Now, applying Lemma 29 to the leading $(i+1)\times(i+1)$ submatrix underlying the minor m_{i+1} with indices i and $j = i+1$,

$$m_{i+1}m_{i-1} = m_i'm_i - d^2,$$

for some $d \in \mathbb{Q}$. Thus we must check that

$$(m_i', d^2 - m_i'm_i)_p = (m_i, d^2 - m_i'm_i)_p.$$

Since M is positive definite, all leading minors are positive, so $m_{i+1}m_{i-1} = m_i'm_i - d^2 \neq 0$, and the displayed equation is equivalent to $(m_i'm_i, d^2 - m_i'm_i)_p = 1$. But

$$m_i'm_iX^2 + (d^2 - m_i'm_i)Y^2 = 1$$

has a solution by taking $X = Y = d^{-1}$ and so the Hilbert symbol evaluates to 1 as required. Unravelling this chain of equivalences to its start, we conclude that the Pall invariants are preserved by simultaneous permutation of rows and columns.

Next, consider the elementary row operation which adds row i to row j, and adds column i to column j. Since rows may be permuted arbitrarily, we assume without loss of generality that the only row altered is row n (and similarly, that all columns are preserved except column n). Thus all minors but the last are unchanged, while the last (the determinant) is unchanged since the matrices of the row and column operations have determinant 1. All the terms in the Pall invariant are unchanged when the last row and column of M are altered by a scalar multiple of another row, which concludes the argument for this row operation.

Finally, in the case of scalar multiplication, again we may assume that only the last row and column are altered. Then the determinant is updated by the square of a rational number λ and all other minors are unchanged. Again working with the definition of the Hilbert symbol, it is clear that $(\lambda^2 m_n, b)_p = (m_n, b)_p$ for any $b \in \mathbb{Q}^*$. Hence the Pall invariants are preserved by scalar multiplication of rows.

This concludes the proof: any invertible matrix N may be expressed as a product of elementary row operation matrices, and the elementary row operations preserve the Pall invariants. So the Pall invariants of $N^\top MN$ and M agree. □

Since the Hilbert symbol is defined only at non-zero arguments, we used implicitly in the argument above that the minors of M are non-vanishing. This follows from the assumption that M is positive definite via Sylvester's criterion (but can be evaded by slightly lengthier *ad hoc* arguments in the general case).

Remark 31. In fact, the invariants of Theorem 30 are a complete set, in the sense that two quadratic forms having the same rank, discriminant and inertia, and taking the same value at all primes (including now $p = 2, \infty$) are necessarily rationally equivalent. This is essentially the statement of the Hasse-Minkowski theorem. This is sometimes called the local-global principal. This is because the (difficult) question of rational equivalence is reduced to (easy) questions about Hilbert symbols, which are local in the sense that they depend only on a single prime. For a complete proof, the reader is referred to Serre's *Arithmetic*.

The astute reader will notice that we justified the reduction of quadratic forms to diagonal matrices by applying a change of basis operation in Section 1, while in Theorem 30 we applied a 'quadratic' transformation to the quadratic space by replacing the matrix A of the quadratic form by the matrix $N^\top AN$. This is precisely the distinction between computing the image of a linear transformation under a change of basis and considering a pair of distinct but conjugate linear transformations.

In any case, Theorem 30 allows us for reduction to diagonal matrices, at which point the invariants may be expressed a little more concisely.

Definition 32. The *Hasse-Minkowski invariant* of a (polarised) quadratic form $Q = \langle a_1, \ldots, a_n \rangle$ at the prime p is

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

Proposition 33. *At any odd prime, the Hasse-Minkowski and Pall invariants are equal for a polarised (diagonal) form of discriminant* 1.

Proof. Let Q be a quadratic form. By Theorem 30, the Pall invariants do not depend on the choice of symmetric matrix used to represent the form. By Proposition 12, we may take $Q = \langle a_1, \ldots, a_n \rangle$. We will reduce the Pall invariant to the Hasse-Minkowski invariant.

Recall that the Hilbert symbol satisfies the following identities: $(a, -a)_p = 1$ and $(a, bc)_p = (a, b)_p (a, c)_p$, and that the k^{th} minor is defined as $m_i = \prod_{i=1}^{k} a_i$. Then

$$(m_k, -m_{k+1})_p = (m_k, -m_k)_p (m_k, a_{k+1})_p = \prod_{i=1}^{k} (a_i, a_{k+1})_p \,.$$

By hypothesis, the discriminant is 1 and $(-1, -1)_p = 1$ since -1 is coprime to p. So the Pall symbol evaluates to the Hasse-Minkowski symbol as required.

$$c(Q, p) = (-1, -1)_p \prod_{k=1}^{n} \prod_{i=1}^{k-1} (a_i, a_k)_p = \prod_{i<k} (a_i, a_k)_p = H(Q, p) \,. \qquad \square$$

Remark 34. We caution the reader that, as defined, the Pall Invariant of I_n is -1 at $p = 2, \infty$, while the Hasse-Minkowski invariants of the identity matrix are all 1. Various authors have adopted different conventions for classifying quadratic forms: arguably the most natural quadratic form is the one composed of a direct sum of hyperbolic planes (over $\mathbb{Q}$ a hyperbolic plane has matrix $\langle 1, -1 \rangle$), and these have all Pall invariants equal to 1.

Example 35. To illustrate the computation of Hasse-Minkowski invariants (and Hilbert symbols), let us decide whether the form $\langle 1, 2, 7, 14\rangle$ is rationally equivalent to $\langle 1, 1, 1, 1\rangle$. Both forms are positive definite (and so have the same signature) and have discriminant 1. For this it suffices to consider the local invariant at 7, which is

$$H(Q, 7) = (1, 2)_7(1, 7)_7(1, 14)_7(2, 7)_7(2, 14)_7(7, 14)_7$$

Using bilinearity, we expand the composite terms:

$$H(Q, 7) = (1, 2)_7^2(1, 7)_7^2(2, 2)_7(2, 7)_7^3(7, 7)_7$$

Now, we cancel square terms:

$$H(Q, 7) = (2, 2)_7(2, 7)_7(7, 7)_7$$

Of these, the first is 1 because both arguments are coprime to 7, the second is likewise 1 because 2 is a square mod 7. But $7 \equiv 3 \mod 4$ so the last term is -1 and the local invariant differs from that of the standard form. Hence the forms are inequivalent over $\mathbb{Q}$. The local invariants typically do not provide any clue about the rational matrix relating one form to the other.

At last, we give the long-promised characterisation of positive definite matrices which are not rational Gram matrices.

Theorem 36. *Let G be a positive definite rational matrix. Suppose that at least one of the following holds:*

1. *G has discriminant different to 1.*
2. *For some odd prime, the Hasse-Minkowski symbol of G evaluates to -1.*

Then G is not a Gram matrix, there is no rational matrix M such that $M^\top M = G$.

5 Combinatorial designs

One of the most important theorems on the (non-)existence of combinatorial designs is the Bruck-Ryser-Chowla Theorem. It depends ultimately on the theory of quadratic forms that we build here. We give a quick sketch here of the definitions needed to appreciate the result.

Definition 37. A finite projective plane is an incidence structure with **points** and **lines** which satisfies the following axioms.

1. Given any two points P and Q there is a unique line incident with both.
2. Given any two lines ℓ, m there is a unique point incident with both.
3. There exist 4 points, no three incident with any line.

Example 38. The *Fano plane* consists of seven points $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\}$ and seven lines

$$\mathcal{L} = \{124, 235, 346, 457, 561, 672, 713\}.$$

Labelling the points and lines of the plane in this fashion makes clear one symmetry of the plane: both $\mathcal{P}$ and $\mathcal{L}$ are invariant under the permutation $\sigma = (1234567)$. An alternative labelling of the points is with the non-zero elements of a three dimensional vector space over $\mathbb{F}_2$ (simply express each integer in binary!). Then three points are *collinear* if and only if they lie in a two dimensional subspace of $\mathbb{F}_2^3$. In this representation, it is clear that any element of $\mathrm{GL}_2(3)$ preserves the set of lines. But it is perhaps unclear how to represent σ in this group.

While the axioms of a projective plane seem simple, they have surprisingly deep implications.

Proposition 39. *Let Π be a finite projective plane. There exists an integer n such that every line contains $n+1$ points and every point is contained in $n+1$ lines. The total number of points is n^2+n+1, as is the total number of lines.*

Proof. By Axiom 3, there exist a point P and a line ℓ not incident with P. By Axiom 2, every line through P meets ℓ, and by Axiom 1, the intersection is a single point. So we have a bijection between the lines through P and the points on ℓ.

By Axiom 3 there are at least 3 distinct lines through P, say ℓ_1, ℓ_2, ℓ_3. Let Q be a point on ℓ_1. By the argument in the previous paragraph we have that $|\ell_2| = |\ell_3|$. A similar argument using a point on ℓ_2 shows that all lines through P have the same size, which we denote $n+1$.

Now, for any other point Q in Π, there is a line through P not meeting Q: the number of lines through Q is $n+1$. And any line through Q not meeting P has $n+1$ points, through a bijection with the lines through P. So every line has $n+1$ points.

Finally, by Axiom 1, there is a unique line between P and any other point Q. There are $n(n+1)$ such points, so the total number of points in the projective plane is n^2+n+1. Each line has size $n+1$ and every pair of points is contained in a unique line, so the number of lines if $\binom{n^2+n+1}{2}/\binom{n+1}{2} = n^2+n+1$. □

The projective planes given in the next proposition are called *Desarguesian*, because Desargues Theorem holds in them.

Proposition 40. *Let V be a three dimensional vector space over a field $\mathbb{F}$. Define projective points to be one-dimensional subspaces of V and projective lines to be two-dimensional subspaces. These points and lines form a projective plane, with incidence given by containment.*

Proof.
1. Let P and Q be projective points. These are distinct one dimensional subspaces. There is a unique projective line $\langle P, Q\rangle$.
2. A projective line (two dimensional subspace) is defined by one linear equation in V. The intersection of two projective lines is the set of common solutions of two linear equations. This is a projective point.
3. The projective points spanned by a basis of V are not contained in any projective line.

□

Proposition 41. *Suppose that there exists a projective plane of order n. Then there exists a $(0,1)$-matrix M of order n^2+n+1 such that*

$$MM^\top = nI + J$$

where J is the all-ones matrix.

Proof. Construct M from the projective plane by labelling rows by points in the plane and columns by the lines in the plane, with 1 if $p_i \in \ell_j$ and 0 otherwise. Then the (i,j) entry of $MM^\top$ is the inner product of rows i and j, which counts the number of lines containing p_i and p_j, which is 1 is $i \neq j$ and $n+1$ if $i = j$. □

More generally, a (v,k,λ)-design has v points, subsets of points of size k, usually called *blocks*, and every pair of points is contained in λ blocks. Similarly to above, the incidence matrix satisfies $MM^\top = (k-\lambda)I + \lambda J$. A computation shows that the determinant of $(k-\lambda)I + \lambda J = k^2(k-\lambda)^{v-1}$. But the determinant of the left hand side is a square, so in the case that v is **even** we find that $k-\lambda$ must be the square of an integer. This is a strong condition which forces non-existence of many designs. The full Bruck-Ryser-Chowla theorem uses the theory of quadratic forms to say a little more.

6 Applications in Design theory

We are now in a position to give proofs of a number of results in design theory, which depend essentially on computing the Hasse-Minkowski invariants of certain potential Gram matrices. Recall that these are only necessary (and not sufficient) conditions for existence of designs. Tracing the historical development of these results, we begin with the Bruck-Ryser theorem on projective planes.

6.1 The Bruck-Ryser Theorem

Recall that a projective plane of order n is a finite geometry in which each line contains $n+1$ points and every pair of lines meet at a unique point. This is equivalent to a $0,1$-matrix of order n^2+n+1 which satisfies the equation

$$MM^\top = nI + J$$

where J is the all-ones matrix. Interpreted as a statement about quadratic forms, this states that the standard form in this dimension is equivalent to the form represented by the matrix on the right. To prove the non-existence of certain projective planes, it would be sufficient to show that the quadratic forms of I_n and $nI_n + J$ differ. This is what we will do, with the aid of the Hasse-Minkowski theorem.

We begin by *polarising* the matrix $nI+J$. While every symmetric matrix is diagonalisable over the reals by an orthogonal matrix (as a consequence of the spectral theorem), such a matrix does typically not have entries over the rationals. As such, we need to be a little more careful - while we labour the point a little here, it indicates some of the techniques used in working with quadratic forms.

Proposition 42. *The $d \times d$ matrices $nI + J$ and $\langle (n+d), (2\cdot 1)n, (3\cdot 2)n \ldots, (d\cdot d-1)n\rangle$ are congruent.*

Proof. Since every vector is an eigenvector of nI, it suffices to choose an eigenbasis for J in which each basis vector has rational entries. This may be accomplished as follows:

$$f_1^\top = (1,1,1,\ldots,1), \;\; f_i^\top = (1,1,\ldots,1,-i,0,\ldots,0), \;\; 2 \le i \le d$$

where $f_i^\top$ contains $-i+1$ in co-ordinate i, with 1's to the left and 0's to the right. By linearity, $(nI+J)f_1 = (n+d)f_1$ and $(nI+J)f_i = nf_i$ for $2 \le i \le d$. Let F be the matrix with f_i in the i^{th} column. Then $D = F^\top(nI+J)F$ is diagonal, with $D_1 = (n+d)d$ and $D_i = i(i-1)n$ for $2 \le i \le d$. $\square$

When $d = n^2+n+1$, the eigenvalues of $nI+J$ are $(n+1)^2$ with multiplicity 1 and n with multiplicity n^2+n. Proposition 42 rewrites $nI+J$ as a product of the usual (real) diagonalisation of $nI+J$ with a matrix $\langle n, 1\cdot 2, 2\cdot 3, \ldots, (n^2+n)\cdot(n^2+n+1)\rangle$. It will be convenient for us to eliminate this second diagonal matrix from later computations. Let us compare the local invariants of a matrix product to those of its terms.

Proposition 43. *Let $A = \langle a_1,\ldots,a_n\rangle$ and $B = \langle b_1,\ldots,b_n\rangle$ be quadratic forms. Then for any prime p, the local invariant of AB at p is equal to*

$$H(AB,p) = H(A,p)H(B,p)(\Delta A, \Delta B)_p \prod_{i=1}^{n} (a_i,b_i)_p\,,$$

where ΔA is the discriminant of A.

Proof. By bilinearity of the Hilbert symbol,

$$H(AB,p) = \prod_{i\le j} (a_i,a_j)_p (a_i,b_j)_p (a_j,b_i)_p (b_i,b_j)_p$$

and since the terms commute,

$$H(AB,p) = \prod_{i\le j} (a_i,a_j)_p (b_i,b_j)_p \prod_{i\ne j} (a_i,b_j)_p\,.$$

Now, add the diagonal terms, $\prod_i (a_i, b_i)_p^2 = 1$, gather one copy of each term into the rightmost product of above,

$$H(AB, p) = \prod_{i \le j} (a_i, a_j)_p (b_i, b_j)_p \prod_j (\prod_i a_i, b_j)_p \prod_i (a_i, b_i)_p \,.$$

Finally, by bilinearity in the second argument,

$$H(AB, p) = H(A, p) H(B, p) (\Delta A, \Delta B) \prod_i (a_i, b_i)_p \,. \qquad \square$$

Theorem 44. *Let $m = n^2 + n + 1$, for some positive integer n. Then the quadratic forms $nI_m + J_m$ and the polarised form $\langle (n+1)^2, n, n, \ldots, n \rangle$ are congruent.*

Proof. Set $a_1 = (n+1)^2$ and $a_i = n$ for $2 \le i \le m$, so that the a_i are the eigenvalues of $nI + J$; and set $b_1 = n$ and $b_i = i(i-1)$. We will apply Proposition 43 to show that the local invariant (AB, p) is equal to $(A, p)(B, p)$. First, $\det(A) = (n+1)^2 n^{n^2+n}$ is a square, so that $\Delta A = 1$. Hence $(\Delta A, \Delta B) = 1$. Similarly, $(a_1, b_1)_p = ((k+1)^2, b_1)_p = 1$ since the Hilbert symbol is 1 when either argument is the square of an integer. Finally, the following product telescopes:

$$\prod_{i=2}^{m} (n, i(i-1))_p = \prod_{i=1}^{m} (n, i-1)_p (n, i)_p = (n, 1)_p (n, m)_p \,.$$

The first term evaluates to 1. For the second, observe that it is trivially 1 for any prime not dividing n or m. If p divides n, then $m = n^2 + n + 1 \equiv 1 \mod p$ and the term is 1. If p divides m then $(n+1)^2 = n^2 + 2n + 1 \equiv n \mod m$ because $m = n^2 + n + 1$. Hence the product of diagonal terms vanishes always.

Finally, we evaluate the local invariants at the form $B = \langle n, 2 \cdot 1, 3 \cdot 2, \ldots, (m-1)m \rangle$. The local invariant at p is

$$\prod_{i}^{n-1} (n, i(i+1)) \prod_{i<j} (i(i+1), j(j+1)) = \prod_i (n, i)(n, i+1) \prod_{i<j} (i, j)(i, j+1)(i+1, j)(i+1, j+1)$$

The first product telescopes, leaving only a term (n, n). For a fixed value of i, the terms in the second product telescope leaving a remainder $(i, j)(i+1, j)(i, n)(i+1, n)$. These last terms telescope also in j, leaving an expression

$$(2, 2)(2, 3)(3, 3) \cdots (n, n) \,.$$

A prime occurs in 3 consecutive terms of the form $(p-1, p)_p (p, p)_p (p, p+1)_p$ or in two terms $(p-1, p)_p (p, p)_p$. In either case, these products evaluate to 1. In fact, this is not surprising, since this matrix is given by $FF^\top$. Hence the local invariants of $F^\top (nI + J) F$ agree with those of the diagonal form $\langle (n+1)^2, n, \ldots, n \rangle$ as required. $\square$

Finally, we prove the Bruck-Ryser theorem.

Theorem 45 (Bruck-Ryser)**.** *Suppose that Π is a projective plane of order n where $n \equiv 1, 2 \mod 4$. Then $n = a^2 + b^2$, for integers a and b.*

Proof. By Theorem 44, it suffices to compute the invariants of the quadratic form $A = \langle (n+1)^2, n, \ldots, n \rangle$ where there are $n^2 + n$ terms equal to n, and compare these to the invariants of the identity matrix. A single local invariant equal to -1 proves non-existence of the corresponding projective plane, while having all local invariants equal to 1 is inconclusive. The Hasse-Minkowski Invariant at a prime p is

$$(A, p) = (n^2 + 2n + 1, n)_p^{n^2+n} (n, n)_p^{\binom{n^2+n}{2}} \,.$$

Clearly the first term vanishes, while the exponent of the second term is odd precisely when $n \equiv 1, 2 \mod 4$.

Suppose now that p is an odd prime divisor of the square-free part of n. The local invariant at p reduces to the condition $(n,n)_p = 1$. By the definition of the Hilbert symbol, this is equal to $(n,-1)_p$, which is 1 if and only if $nx^2 - y^2 = z^2$ has a solution. But this is precisely equivalent to $nx^2 = z^2 + y^2$, which requires that n is a sum of two squares. □

Recall that Fermat's Theorem on sums of two squares gives a characterisation of the permissable values of n in Theorem 45: they are precisely those for which the square free part of n is not divisible by a prime congruent to 3 modulo 4. Thus, Theorem 45 rules out projective planes of order $6, 14, 21, 22, 30, \ldots$

7 Further applications

The full Bruck-Ryser-Chowla theorem requires a little more effort to prove, but the techniques illustrated above are more-or-less sufficient.

Theorem 46 (Bruck-Ryser-Chowla)**.** *If a symmetric 2-(v,k,λ) design exists, then*

(i) If v is even, then $n = k - \lambda$ is a perfect square.

(ii) If v is odd, then for all odd primes p

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

The Bose-Connor theorem gives non-existence conditions for *group developed designs*.

Definition 47. Let V be a set of size mn, divided into m *groups* of size n. Let B be a set of blocks, each of size k. Then (V,B) is a group-developed design with parameters $(mn,n,k,\lambda_1,\lambda_2)$ if any pair of points from the same group occurs in λ_1 blocks and any pair of points from distinct blocks occurs together in λ_2 blocks.

Standard counting arguments show that each point appears in $r = \frac{(n-1)\lambda_1 + n(m-1)\lambda_2}{k-1}$ blocks (and integrality of this quantity is a necessary condition for the existence of a GDD). A GDD is *symmetric* if the incidence matrix is square, in which case $r = k$ as in the usual theory of symmetric designs.

Recall that the Kronecker product of matrices A and B is given (as a block-matrix) by $[A \otimes B]_{ij} = a_{ij}B$. In particular, $I_m \otimes J_n$ is an $mn \times mn$ matrix with $n \times n$ blocks of ones on the diagonal and zeros elsewhere. It follows from the definition that the incidence matrix of a symmetric group developed design is $G = (r - \lambda_1 - \lambda_2)I + (\lambda_1 - \lambda_2)I_m \otimes J_n + \lambda_2 J_{mn}$. Non-existence conditions can be derived from the theory of quadratic forms by finding conditions under which G is not a Gram matrix. We refer the interested reader to the original paper for a proof.

Theorem 48 (Bose-Connor)**.** *Suppose that D is a symmetric group divisible design with parameters (mn,n,k,λ), and denote $Q = k - \lambda_1$ and $P = k^2 - v\lambda_2$. Then the following conditions hold:*

1. $(n-1)\lambda_1 + n(m-1)\lambda_2 = k(k-1)$.
2. $P > 0$ *and* $Q > 0$.
3. $P^{m-1}Q^{m(n-1)}$ *is a perfect square.*
4. *If m is even then P is a perfect square. If $m \equiv 2 \mod 4$ and Q is even then $(Q,-1)_p = 1$ for all odd primes p.*
5. *If m is odd and n is even then Q is a perfect square. Furthermore, $((-1)^{\binom{m}{2}}n\lambda_2, P)_p = 1$ for all odd primes p.*
6. *If m and n are odd then $((-1)^{\binom{m}{2}}n\lambda_2, P)_p = ((-1)^{\binom{n}{2}}n, Q)_p$ for all odd primes p.*

The *Hadamard maximal determinant problem* asks for the maximal determinant of a $\{\pm 1\}$ matrix in dimension n. If 4 divides n, then optimal solution is a Hadamard matrix, provided that one exists. (This is the original motivation for the Hadamard conjecture.) No obstructions arise from the theory of quadratic forms. The following result is compiled from the work of a number of mathematicians, principally Ehlich, Wojtas and Cohn. While the first two parts can be obtained without the use of quadratic forms, that theory allows for a uniform proof technique (essentially by computing the obvious invariants).

Theorem 49. *Let D_n be the absolute value of the maximal determinant of an $n \times n$ matrix with entries in $\{\pm 1\}$.*

1. *If $n \equiv 1 \mod 4$ then $D_n \leq \sqrt{2n-1}(n-1)^{\frac{n-1}{2}}$. If the bound is met with equality, then $(n-1)I_n + J_n$ is a Gram matrix and $2n-1$ is a perfect square.*
2. *If $n \equiv 2 \mod 4$ then $D_n \leq (2n-2)(n-2)^{\frac{n-2}{2}}$. If the bound is met with equality then $I_2 \otimes \big((n-2)I_{n/2} + 2J_{n/2}\big)$ is a Gram matrix and $2n-2$ is the sum of two squares.*
3. *If $n \equiv 3 \mod 4$ then $D_n \leq \frac{2 \cdot 11^3}{7^7} n(n-1)^3(n-3)^{\frac{n-7}{2}}$. If the bound is met with equality then $I_7 \otimes \big((n-3)I_{n/7} + 4J_{n/7}\big) - J_n$ is a Gram matrix. Letting $n = 7m$, this implies that $4m-3$ is a perfect square and that $(11m-3, -(7m-3))_p = 1$ for all odd primes p.*

In the first two cases above, the bound is known to be attained infinitely often, while the third is not known to be attained for any integer. The smallest integer for which the stated conditions hold is $n = 511$, but the existence of a $\{\pm 1\}$ valued solution to the Gram matrix condition is open.