Quadratic form

From Wikipedia, the free encyclopedia

In mathematics, a **quadratic form** is a homogeneous polynomial of degree two in a number of variables. For example,

$$4x^2 + 2xy - 3y^2$$

is a quadratic form in the variables *x* and *y*.

Quadratic forms occupy a central place in various branches of mathematics, including number theory, linear algebra, group theory (orthogonal group), differential geometry (Riemannian metric), differential topology (intersection forms of four-manifolds), and Lie theory (the Killing form).

Contents

Introduction

Quadratic forms are homogeneous quadratic polynomials in *n* variables. In the cases of one, two, and three variables they are called **unary**, **binary**, and **ternary** and have the following explicit form:

$$q(x) = ax^2 \quad \text{(unary)}$$
$$q(x,y) = ax^2 + bxy + cy^2 \quad \text{(binary)}$$
$$q(x,y,z) = ax^2 + by^2 + cz^2 + dxy + exz + fyz \quad \text{(ternary)}$$

where *a*,…,*f* are the **coefficients**.[1] Note that quadratic functions, such as $ax^2 + bx + c$ in the one variable case, are not quadratic forms, as they are typically not homogeneous (unless *b* and *c* are both 0).

The theory of quadratic forms and methods used in their study depend in a large measure on the nature of the coefficients, which may be real or complex numbers, rational numbers, or integers. In linear algebra, analytic geometry, and in the majority of applications of quadratic forms, the coefficients are real or complex numbers. In the algebraic theory of quadratic forms, the coefficients are elements of a certain field. In the arithmetic theory of quadratic forms, the coefficients belong to a fixed commutative ring, frequently the integers $\mathbf{Z}$ or the p-adic integers $\mathbf{Z}_p$.[2] Binary quadratic forms have been extensively studied in number theory, in particular, in the theory of quadratic fields, continued fractions, and modular forms. The theory of integral quadratic forms in n variables has important applications to algebraic topology.

Using homogeneous coordinates, a non-zero quadratic form in n variables defines an $(n-2)$-dimensional quadric in the $(n-1)$-dimensional projective space. This is a basic construction in projective geometry. In this way one may visualize 3-dimensional real quadratic forms as conic sections.

A closely related notion with geometric overtones is a **quadratic space**, which is a pair (V,q), with V a vector space over a field K, and $q: V \to K$ a quadratic form on V. An example is given by the three-dimensional Euclidean space and the square of the Euclidean norm expressing the distance between a point with coordinates (x,y,z) and the origin:

$$q(x,y,z) = d((x,y,z),(0,0,0))^2 = \|(x,y,z)\|^2 = x^2 + y^2 + z^2.$$

History

The study of particular quadratic forms, in particular the question of whether a given integer can be the value of a quadratic form over the integers, dates back many centuries. One such case is Fermat's theorem on sums of two squares, which determines when an integer may be expressed in the form $x^2 + y^2$, where x, y are integers. This problem is related to the problem of finding Pythagorean triples, which appeared in the second millennium B.C.[3]

In 628, the Indian mathematician Brahmagupta wrote *Brahmasphutasiddhanta* which includes, among many other things, a study of equations of the form $x^2 - ny^2 = c$. In particular he considered what is now called Pell's equation, $x^2 - ny^2 = 1$, and found a method for its solution.[4] In Europe this problem was studied by Brouncker, Euler and Lagrange.

In 1801 Gauss published *Disquisitiones Arithmeticae,* a major portion of which was devoted to a complete theory of binary quadratic forms over the integers. Since then, the concept has been generalized, and the connections with quadratic number fields, the modular group, and other areas of mathematics have been further elucidated.

Real quadratic forms

See also: Sylvester's law of inertia and Definite form

Any $n \times n$ real symmetric matrix A determines a quadratic form q_A in n variables by the formula

$$q_A(x_1,\ldots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_i x_j.$$

Conversely, given a quadratic form in n variables, its coefficients can be arranged into an $n \times n$ symmetric matrix. One of the most important questions in the theory of quadratic forms is how much can one simplify a quadratic form q by a homogeneous linear change of variables. A fundamental theorem due to Jacobi asserts that q can be brought to a **diagonal form**

$$\lambda_1\tilde{x}_1^2+\lambda_2\tilde{x}_2^2+\cdots+\lambda_n\tilde{x}_n^2,$$

so that the corresponding symmetric matrix is diagonal, and this is even possible to accomplish with a change of variables given by an orthogonal matrix – in this case the coefficients $\lambda_1, \lambda_2, \ldots, \lambda_n$ are in fact determined uniquely up to a permutation. If the change of variables is given by an invertible matrix, not necessarily orthogonal, then the coefficients λ_i can be made to be 0,1, and −1. Sylvester's law of inertia states that the numbers of 1 and −1 are invariants of the quadratic form, in the sense that any other diagonalization will contain the same number of each. The **signature** of the quadratic form is the triple (n_0, n_+, n_-) where n_0 is the number 0s and $n_\pm$ is the number of ±1s. Sylvester's law of inertia shows that this is a well-defined quantity attached to the quadratic form. The case when all λ_i have the same sign is especially important: in this case the quadratic form is called **positive definite** (all 1) or **negative definite** (all −1); if none of the terms are 0 then the form is called **nondegenerate**; this includes positive definite, negative definite, and indefinite (a mix of 1 and −1); equivalently, a nondegenerate quadratic form is one whose associated symmetric form is a nondegenerate *bilinear* form. A real vector space with an indefinite nondegenerate quadratic form of index (p,q) (p 1s, q −1s) is often denoted as $\mathbf{R}^{p,q}$ particularly in the physical theory of space-time.

The discriminant of a quadratic form, concretely the class of the determinant of a representing matrix in $K/(K^*)^2$ (up to non-zero squares) can also be defined, and for a real quadratic form is a cruder invariant than signature, taking values of only "positive, zero, or negative". Zero corresponds to degenerate, while for a non-degenerate form it is the parity of the number of negative coefficients, $(-1)^{n_-}$.

These results are reformulated in a different way below.

Let q be a quadratic form defined on an n-dimensional real vector space. Let A be the matrix of the quadratic form q in a given basis. This means that A is a symmetric $n\times n$ matrix such that

$$q(v)=x^{\mathrm{T}}Ax,$$

where x is the column vector of coordinates of v in the chosen basis. Under a change of basis, the column x is multiplied on the left by an $n\times n$ invertible matrix S, and the symmetric square matrix A is transformed into another symmetric square matrix B of the same size according to the formula

$$A\to B=SAS^{\mathrm{T}}.$$

Any symmetric matrix A can be transformed into a diagonal matrix

$$B=\begin{pmatrix}\lambda_1 & 0 & \cdots & 0\\ 0 & \lambda_2 & \cdots & 0\\ \vdots & \vdots & \ddots & 0\\ 0 & 0 & \cdots & \lambda_n\end{pmatrix}$$

by a suitable choice of an orthogonal matrix S, and the diagonal entries of B are uniquely determined — this is Jacobi's theorem. If S is allowed to be any invertible matrix then B can be made to have only 0,1, and −1 on the diagonal, and the number of the entries of each type (n_0 for 0, n_+ for 1, and n_- for −1) depends only on A. This is one of the formulations of Sylvester's law of inertia and the numbers n_+ and n_- are called the **positive** and **negative indices of inertia**. Although their definition involved a choice of basis and consideration of the corresponding real symmetric matrix *A*, Sylvester's law of inertia means that they are invariants of the quadratic form *q*.

The quadratic form *q* is positive definite (resp., negative definite) if $q(v) > 0$ (resp., $q(v) < 0$) for every nonzero vector *v*.[5] When $q(v)$ assumes both positive and negative values, *q* is an **indefinite** quadratic form. The theorems of Jacobi and Sylvester show that any positive definite quadratic form in *n* variables can be brought to the sum of *n* squares by a suitable invertible linear transformation: geometrically, there is only *one* positive definite real quadratic form of every dimension. Its isometry group is a *compact* orthogonal group O(*n*). This stands in contrast with the case of indefinite forms, when the corresponding group, the indefinite orthogonal group O(*p*, *q*), is non-compact. Further, the isometry groups of *Q* and −*Q* are the same ($O(p, q) \approx O(q, p)$), but the associated Clifford algebras (and hence Pin groups) are different.

Definitions

An *n*-ary **quadratic form** over a field *K* is a homogeneous polynomial of degree 2 in *n* variables with coefficients in *K*:

$$q(x_1,\ldots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j, \quad a_{ij} \in K.$$

This formula may be rewritten using matrices: let *x* be the column vector with components $x_1, \ldots, x_n$ and $A = (a_{ij})$ be the $n\times n$ matrix over *K* whose entries are the coefficients of *q*. Then

$$q(x) = x^{\mathrm{T}}Ax.$$

Two *n*-ary quadratic forms φ and ψ over *K* are **equivalent** if there exists a nonsingular linear transformation $T \in GL(n, K)$ such that

$$\psi(x) = \varphi(Tx).$$

Let us assume that the characteristic of K *is different from 2.* (The theory of quadratic forms over a field of characteristic 2 has important differences and many definitions and theorems have to be modified.) The coefficient matrix *A* of *q* may be replaced by the symmetric matrix $(A + A^{\mathrm{T}})/2$ with the same quadratic form, so it may be assumed from the outset that *A* is symmetric. Moreover, a symmetric matrix *A* is uniquely determined by the corresponding quadratic form. Under an equivalence *T*, the symmetric matrix *A* of φ and the symmetric matrix *B* of ψ are related as follows:

$$B = T^{\mathrm{T}}AT.$$

The **associated bilinear form** of a quadratic form *q* is defined by

$$b_q(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = x^{\mathrm{T}}Ay = y^{\mathrm{T}}Ax.$$

Thus, b_q is a symmetric bilinear form over *K* with matrix *A*. Conversely, any symmetric bilinear form *b* defines a quadratic form

$$q(x) = b(x,x)$$

and these two processes are the inverses of one another. As a consequence, over a field of characteristic not equal to 2, the theories of symmetric bilinear forms and of quadratic forms in *n* variables are essentially the same.

Quadratic spaces

A quadratic form *q* in *n* variables over *K* induces a map from the *n*-dimensional coordinate space K^n into *K*:

$$Q(v) = q(v), \quad v = [v_1, \ldots, v_n]^{\mathrm{T}} \in K^n.$$

The map *Q* is a **quadratic map**, which means that it has the properties:

- $Q(av) = a^2 Q(v) \quad \text{for all } a \in K, v \in V.$
- When the characteristic of *K* is not two, the map B_Q: $V \times V \to K$ defined below is bilinear over *K*:

$$B_Q(v, w) = (Q(v + w) - Q(v) - Q(w))/2.$$

This bilinear form B_Q has the special property that $B(x, x) = Q(x)$ for all *x* in *V*. When the characteristic of *K* is two so that 2 is not a unit, it is still possible to use a quadratic form to define a bilinear form $B(x,y) = Q(x+y) - Q(x) - Q(y)$. However, $Q(x)$ can no longer be recovered from this *B* in the same way, since $B(x, x) = 0$ for all *x*.

The pair (*V*, *Q*) consisting of a finite-dimensional vector space *V* over *K* and a quadratic map from *V* to *K* is called a **quadratic space** and B_Q is the associated bilinear form of *Q*. The notion of a quadratic space is a coordinate-free version of the notion of quadratic form. Sometimes, *Q* is also called a quadratic form.

Two *n*-dimensional quadratic spaces (*V*,*Q*) and (V', Q') are **isometric** if there exists an invertible linear transformation T: $V \to V'$ (**isometry**) such that

$$Q(v) = Q'(Tv) \text{ for all } v \in V.$$

The isometry classes of *n*-dimensional quadratic spaces over *K* correspond to the equivalence classes of *n*-ary quadratic forms over *K*.

Further definitions

See also: Isotropic quadratic form

Two elements *v* and *w* of *V* are called **orthogonal** if $B(v,w) = 0$. The **kernel** of a bilinear form *B* consists of the elements that are orthogonal to all elements of *V*. *Q* is **non-singular** if the kernel of its associated bilinear form is 0. If there exists a non-zero *v* in *V* such that $Q(v) = 0$, the quadratic form *Q* is **isotropic**, otherwise it is **anisotropic**. This terminology also applies to vectors and subspaces of a quadratic space. If the restriction of *Q* to a subspace *U* of *V* is identically zero, *U* is **totally singular**.

The orthogonal group of a non-singular quadratic form *Q* is the group of the linear automorphisms of *V* that preserve *Q*, i.e. the group of isometries of (*V*,*Q*) into itself.

Equivalence of forms

Every quadratic form *q* in *n* variables over a field of characteristic not equal to 2 is equivalent to a **diagonal**

form

$$q(x) = a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2.$$

Such a diagonal form is often denoted by $\langle a_1, \ldots, a_n \rangle$.

Classification of all quadratic forms up to equivalence can thus be reduced to the case of diagonal forms.

Geometric meaning

If we let the equation be $x^{\mathrm{T}} Ax + b^{\mathrm{T}} x = 1$ with symmetric matrix *A*, then the geometric meaning is as follows.

If all eigenvalues of *A* are non-zero, then it is an ellipsoid or a hyperboloid. If all the eigenvalues are positive, then it is an ellipsoid; if all the eigenvalues are negative, it is an image ellipsoid; if some eigenvalues are positive and some are negative, then it is a hyperboloid.

If there exist one or more eigenvalues $\lambda_i = 0$, then if the corresponding $b_i \neq 0$, it is a paraboloid (either elliptic or hyperbolic); if the corresponding $b_i = 0$, the dimension *i* degenerates and does not get into play, and the geometric meaning will be determined by other eigenvalues and other components of *b*. When it is a paraboloid, whether it is elliptic or hyperbolic is determined by whether all other non-zero eigenvalues are of the same sign: if they are, then it is elliptic; otherwise, it is hyperbolic.

Integral quadratic forms

Quadratic forms over the ring of integers are called **integral quadratic forms**, whereas the corresponding modules are **quadratic lattices** (sometimes, simply lattices). They play an important role in number theory and topology.

An integral quadratic form has integer coefficients, such as $x^2 + xy + y^2$; equivalently, given a lattice Λ in a vector space *V* (over a field with characteristic 0, such as **Q** or **R**), a quadratic form *Q* is integral *with respect to* Λ if and only if it is integer-valued on Λ, meaning $Q(x,y) \in \mathbf{Z}$ if $x,y \in \Lambda$.

This is the current use of the term; in the past it was sometimes used differently, as detailed below.

Historical use

Historically there was some confusion and controversy over whether the notion of **integral quadratic form** should mean:

twos in
: the quadratic form associated to a symmetric matrix with integer coefficients

twos out
: a polynomial with integer coefficients (so the associated symmetric matrix may have half-integer coefficients off the diagonal)

This debate was due to the confusion of quadratic forms (represented by polynomials) and symmetric bilinear forms (represented by matrices), and "twos out" is now the accepted convention; "twos in" is instead the theory of integral symmetric bilinear forms (integral symmetric matrices).

In "twos in", binary quadratic forms are of the form $ax^2 + 2bxy + cy^2$, represented by the symmetric matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$; this is the convention Gauss uses in Disquisitiones Arithmeticae.

In "twos out", binary quadratic forms are of the form $ax^2 + bxy + cy^2$, represented by the symmetric matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$.

Several points of view mean that *twos out* has been adopted as the standard convention. Those include:

- better understanding of the 2-adic theory of quadratic forms, the 'local' source of the difficulty;
- the lattice point of view, which was generally adopted by the experts in the arithmetic of quadratic forms during the 1950s;
- the actual needs for integral quadratic form theory in topology for intersection theory;
- the Lie group and algebraic group aspects.

Universal quadratic forms

An integral quadratic form whose image consists of all the positive integers is sometimes called *universal*. Lagrange's four-square theorem shows that $w^2 + x^2 + y^2 + z^2$ is universal. Ramanujan generalized this to $aw^2 + bx^2 + cy^2 + dz^2$ and found 54 $\{a,b,c,d\}$ such that it can generate all positive integers, namely,

$\{1,1,1,d\}$, $1 \le d \le 7$
$\{1,1,2,d\}$, $2 \le d \le 14$
$\{1,1,3,d\}$, $3 \le d \le 6$
$\{1,2,2,d\}$, $2 \le d \le 7$
$\{1,2,3,d\}$, $3 \le d \le 10$
$\{1,2,4,d\}$, $4 \le d \le 14$
$\{1,2,5,d\}$, $6 \le d \le 10$

There are also forms whose image consists of all but one of the positive integers. For example, {1,2,5,5} has 15 as the exception. Recently, the 15 and 290 theorems have completely characterized universal integral quadratic forms: if all coefficients are integers, then it represents all positive integers if and only if it represents all integers up through 290; if it has an integral matrix, it represents all positive integers if and only if it represents all integers up through 15.

See also

- ε-quadratic form
- Quadratic form (statistics)
- Discriminant of a quadratic form
- Cubic form
- Witt group
- Witt's theorem
- Hasse–Minkowski theorem
- Orthogonal group
- Square class
- Ramanujan's ternary quadratic form

Notes

1. ^ A tradition going back to Gauss dictates the use of manifestly even coefficients for the products of distinct variables, i.e. $2b$ in place of b in binary forms and $2d$, $2e$, $2f$ in place of d, e, f in ternary forms. Both conventions occur in the literature
2. ^ away from 2, i. e. if 2 is invertible in the ring, quadratic forms are equivalent to symmetric bilinear forms (by the polarization identities), but at 2 they are different concepts; this distinction is particularly important for quadratic forms over the integers.
3. ^ Babylonian Pythagoras (http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Babylonian_Pythagoras.html)
4. ^ Brahmagupta biography (http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Brahmagupta.html)
5. ^ If a non-strict inequality (with ≥ or ≤) holds then the quadratic form q is called semidefinite.

References

- O'Meara, O.T. (2000), *Introduction to Quadratic Forms*, Berlin, New York: Springer-Verlag, ISBN 978-3-540-66564-9
- Conway, John Horton; Fung, Francis Y. C. (1997), *The Sensual (Quadratic) Form*, Carus Mathematical Monographs, The Mathematical Association of America, ISBN 978-0-88385-030-5
- Shafarevich, I. R.; A. O. Remizov (2012). *Linear Algebra and Geometry* (http://www.springer.com/mathematics/algebra/book/978-3-642-30993-9) . Springer. ISBN 978-3-642-30993-9.

External links

- A.V.Malyshev (2001), "Quadratic form" (http://www.encyclopediaofmath.org/index.php?title=q/q076080) , in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4, http://www.encyclopediaofmath.org/index.php?title=q/q076080
- A.V.Malyshev (2001), "Binary quadratic form" (http://www.encyclopediaofmath.org/index.php?title=b/b016370) , in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4, http://www.encyclopediaofmath.org/index.php?title=b/b016370