When Can You Factor a Quadratic Form?

BRIAN G. KRONENTHAL
Kutztown University of Pennsylvania
Kutztown, PA 19530
kronenthal@kutztown.edu

FELIX LAZEBNIK
University of Delaware
Newark, DE 19716
lazebnik@math.udel.edu

Can you factor either of the polynomials

$$Q_1 = 2X_3^2 + 2X_1X_2 - X_1X_3 - 4X_2X_3 - 6X_3X_4 + 3X_1X_4$$

or

$$Q_2 = 2X_3^2 + 2X_1X_2 - X_1X_3 - 4X_2X_3 - 6X_3X_4$$

into a product of polynomials of smaller degree? Feel free to use complex coefficients, but no computers or calculators are allowed.

It turns out that one of Q_1 and Q_2 factors, while the other does not. If you want to check your answer, or do not feel like trying, see the related examples ahead. Of course, we ultimately wish to consider the following general problem:

Given any quadratic form, determine whether it is a product of two linear forms.

If you are uncertain about the meaning of the terms "quadratic form" or "linear form," definitions will appear in the next section. Interestingly enough, this problem has a simple solution, and was answered several centuries ago. However, many people we talked to found it intriguing and were surprised that they had not thought about or seen this problem before. A solution will be a part of what we present in this article. However, our story begins elsewhere.

Problems with terminology?

Undoubtedly, every reader has tried to clarify a notion in one source by consulting another, only to be frustrated that the presentations are inconsistent in vocabulary or notation. Recently, this happened to us in a study of conics. While reading Peter Cameron's *Combinatorics: Topics, Techniques, and Algorithms* [**8**], we encountered a definition of a nonsingular quadratic form $Q = Q(x, y, z)$ as one that

. . . cannot be transformed into a form in less than three variables by any nonsingular linear substitution of the variables x, y, z.

For example, this definition implies that the quadratic form $Q = X_1^2 + 2X_1X_2 + X_2^2$ is singular because $Q = (X_1 + X_2)^2$, and applying the nonsingular linear transformation of variables that maps X_1 to $X_1 - X_2$ and X_2 to itself, Q can be rewritten as X_1^2 (a form in only one variable). In contrast, the quadratic form $X_1^2 + 4X_1X_2 + X_2^2$ is

Math. Mag. **87** (2014) 25–36. doi:10.4169/math.mag.87.1.25. © Mathematical Association of America

nonsingular because it cannot be rewritten in only one variable via a nonsingular linear transformation of variables. All this will be made more precise and explained later in this paper.

Though the definition Cameron presents was clear, it did not appear to translate into simple criteria for determining whether a given quadratic form was nonsingular. In searching for such a test, we found that various sources used the word "singular" to describe quadratic forms in (what seemed to be) completely different ways. Complicating matters further was that terms such as "degenerate" and "reducible" started to appear, and these three words were often used interchangeably. For more details regarding this usage, look ahead to the section titled "Related terminology in the literature," and in particular TABLE 1.

In all, we found five criteria related to degeneracy (or nondegeneracy) of quadratic forms $Q = Q(x, y, z)$ in the literature. While we believed them to be equivalent, few sources proved the equivalence of even two of them, and we found only two sources that proved the equivalence of three. Three of the five criteria have immediate generalizations to n dimensions.

Our main motivation for writing this paper was to show once and for all, for ourselves and for the record, that the several conditions that are widely used as definitions are actually equivalent. We found the writing process instructive, and we hope the reader will find what we present to be useful. In particular, many of the proofs we used draw ideas from the basic principles of analysis, algebra, linear algebra, and geometry. We think that some of these equivalences can serve as useful exercises in related undergraduate courses, as they help to stress the unity of mathematics.

Notation and an example

The main object of our study will be a quadratic form and its associated quadric. We will now define these terms. Additional definitions and related results can be found in Hoffman and Kunze [**17**] or in Shilov [**31**], for example. Let $\mathbb{F}$ be a field whose characteristic, denoted char($\mathbb{F}$), is not 2. Examples include the fields of rational numbers, real numbers, and complex numbers, as well as finite fields containing an odd (prime power) number of elements. We view $\mathbb{F}^n$ as the n-dimensional vector space over $\mathbb{F}$. Any $(n-1)$-dimensional subspace of $\mathbb{F}^n$ is called a *hyperplane*. By $\mathbb{F}[X_1, \ldots, X_n]$, we denote the ring of polynomials with (commuting) indeterminants $X_1, \ldots, X_n$ and coefficients in $\mathbb{F}$. It will often be convenient to view a polynomial of k indeterminants as a polynomial of one of them, with coefficients being polynomials of the other $k-1$ indeterminants. For instance, a polynomial in $\mathbb{F}[X_1, X_2, X_3]$ may be viewed as an element of $\mathbb{F}[X_2, X_3][X_1]$, i.e., a polynomial of X_1 whose coefficients are polynomials of X_2 and X_3.

For $f \in \mathbb{F}[X_1, \ldots, X_n]$, let $\mathcal{Z}(f) = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n : f(\alpha_1, \ldots, \alpha_n) = 0\}$. The "$\mathcal{Z}$" in $\mathcal{Z}(f)$ stands for the zeros of f. To illustrate, if we consider the polynomial $X_1^2 - X_2$ (with $n = 2$) over the field $\mathbb{R}$ of real numbers, then the graph of $\mathcal{Z}(X_1^2 - X_2)$ in the Cartesian coordinate system with axes X_1 and X_2 is the parabola $X_2 = X_1^2$. For $\boldsymbol{f} = (f_1, \ldots, f_m)$, where all $f_i \in \mathbb{F}[X_1, \ldots, X_n]$, we define $\mathcal{Z}(\boldsymbol{f})$ to be the intersection of all $\mathcal{Z}(f_i)$.

A polynomial $Q \in \mathbb{F}[X_1, \ldots, X_n]$ of the form

$$Q = Q(X_1, \ldots, X_n) = \sum_{1 \le i, j \le n} a_{ij} X_i X_j,$$

where $a_{ij} \in \mathbb{F}$ for all i, j, is called a *quadratic form*. For example, $X_1^2 + X_1 X_2$ is a quadratic form, and so are each of Q_1 and Q_2 from the introduction. We may view a quadratic form either as an abstract algebraic object, or as a function $Q : \mathbb{F}^n \to \mathbb{F}$ defined by $(\alpha_1, \ldots, \alpha_n) \mapsto Q(\alpha_1, \ldots, \alpha_n)$. We use the same notation for the algebraic object and the corresponding function. The set $\mathcal{Z}(Q)$ is often referred to as the *quadric* corresponding to Q, and it is the zero-set of Q when Q is viewed as a function.

Since $X_i X_j = X_j X_i$, we have some flexibility in choosing the coefficients; the coefficients a_{ij} and a_{ji} are interchangeable. We will always choose the coefficients to satisfy $a_{ij} = a_{ji}$. For every Q, we define the $n \times n$ matrix of coefficients $M_Q = (a_{ij})$. So for the quadratic form $Q = X_1^2 + X_1 X_2$ in $n = 2$ variables mentioned just above, the associated matrix is

$$M_Q = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 0 \end{pmatrix}.$$

Let V denote the set of all degree-one polynomials in $\mathbb{F}[X_1, \ldots, X_n]$ having zero constant term, called *linear forms*, together with the zero polynomial. A few examples of linear forms are X_1, X_2, and $X_1 + X_2$ (if $n \geq 2$), and $7X_1 + 2X_5 + X_6$ (if $n \geq 6$). The set V can be viewed as a vector space over $\mathbb{F}$ with basis $\{X_1, \ldots, X_n\}$.

For any linear transformation $\varphi : V \to V$ and any quadratic form Q, we can substitute $\varphi(X_i)$ for X_i in Q for all $i = 1, \ldots, n$. After simplifying the result by combining like terms, we again obtain a quadratic form, which we denote by

$$\widetilde{Q}(X_1, \ldots, X_n) = Q(\varphi(X_1), \ldots, \varphi(X_n)).$$

For $T = (t_1, \ldots, t_n) \in \mathbb{F}^n$, $\widetilde{Q}(T) = Q(\varphi(X_1)(T), \ldots, \varphi(X_n)(T))$.

Next, a comment on derivatives. We treat partial derivatives formally, as is done in algebra. For example, to differentiate Q with respect to X_1, we view Q as an element of $\mathbb{F}[X_2, \ldots, X_n][X_1]$:

$$Q = a_{11} X_1^2 + (2a_{12} X_2 + \cdots + 2a_{1n} X_n) X_1 + \sum_{2 \leq i, j \leq n} a_{ij} X_i X_j$$

and thus

$$\frac{\partial Q}{\partial X_1} = 2a_{11} X_1 + (2a_{12} X_2 + \cdots + 2a_{1n} X_n).$$

In other words, we treat Q as a polynomial in X_1, and differentiate it with respect to X_1. Partial derivatives with respect to the other indeterminants are defined similarly. The gradient $\nabla \boldsymbol{Q}$ of Q is then defined as $\nabla \boldsymbol{Q} = \left(\frac{\partial Q}{\partial X_1}, \ldots, \frac{\partial Q}{\partial X_n}\right)$.

Before stating our main result in the next section, we illustrate it with some examples.

EXAMPLES. Let $n = 4$ and let $\mathbb{F}$ be $\mathbb{R}$, the field of real numbers. The following examples are also valid over all fields of characteristic different from 2 (that is, fields in which $2 \neq 0$ as field elements). Consider the quadratic forms mentioned at the beginning of this article, namely

$$Q_1 = 2X_3^2 + 2X_1 X_2 - X_1 X_3 - 4X_2 X_3 - 6X_3 X_4 + 3X_1 X_4$$

and

$$Q_2 = 2X_3^2 + 2X_1 X_2 - X_1 X_3 - 4X_2 X_3 - 6X_3 X_4.$$

We now examine several properties of Q_1 and Q_2.

1. The matrix associated with Q_1 is

$$M_{Q_1} = \begin{pmatrix} 0 & 1 & -1/2 & 3/2 \\ 1 & 0 & -2 & 0 \\ -1/2 & -2 & 2 & -3 \\ 3/2 & 0 & -3 & 0 \end{pmatrix}.$$

It has row reduced echelon form

$$\begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & -1/2 & -3/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and thus M_{Q_1} has rank 2. In contrast,

$$M_{Q_2} = \begin{pmatrix} 0 & 1 & -1/2 & 0 \\ 1 & 0 & -2 & 0 \\ -1/2 & -2 & 2 & -3 \\ 0 & 0 & -3 & 0 \end{pmatrix}$$

has rank 4. That is, M_{Q_1} is a singular matrix and M_{Q_2} is nonsingular.

2. Define a linear transformation $\varphi_1 : V \to V$ by

$$\begin{aligned} \varphi_1(X_1) &= X_1 + 2X_3 \\ \varphi_1(X_2) &= \frac{1}{2}X_2 + \frac{1}{2}X_3 - \frac{3}{2}X_4 \\ \varphi_1(X_3) &= X_3 \\ \varphi_1(X_4) &= X_4. \end{aligned}$$

It is a straightforward verification that φ is nonsingular, and that

$$\widetilde{Q}_1 = Q_1(\varphi_1(X_1), \varphi_1(X_2), \varphi_1(X_3), \varphi_1(X_4)) = X_1X_2,$$

which contains only $r = 2$ indeterminants. Furthermore, we comment (without proof) that for any nonsingular linear transformation $\varphi : V \to V$, the simplified polynomial $Q_1(\varphi(X_1), \varphi(X_2), \varphi(X_3), \varphi(X_4))$ contains *at least* two indeterminants: The argument is the same as in the proof of Theorem 1.

In contrast, for any nonsingular linear transformation $\varphi : V \to V$,

$$\widetilde{Q}_2 = Q_2(\varphi(X_1), \varphi(X_2), \varphi(X_3), \varphi(X_4))$$

contains all four indeterminants. This also follows from the proof of Theorem 1.

3. We now consider the zeros of the gradient fields of Q_1 and Q_2. We have

$$\nabla \boldsymbol{Q_1} = \begin{pmatrix} \partial Q_1/\partial X_1 \\ \partial Q_1/\partial X_2 \\ \partial Q_1/\partial X_3 \\ \partial Q_1/\partial X_4 \end{pmatrix} = \begin{pmatrix} 2X_2 - X_3 + 3X_4 \\ 2X_1 - 4X_3 \\ -X_1 - 4X_2 + 4X_3 - 6X_4 \\ 3X_1 - 6X_3 \end{pmatrix} = 2M_{Q_1}\boldsymbol{X},$$

where $\boldsymbol{X} = (X_1, X_2, X_3, X_4)^t$ is the transpose of (X_1, X_2, X_3, X_4). Therefore, $\mathcal{Z}(\nabla \boldsymbol{Q_1})$ is the null space of the matrix $2M_{Q_1}$. In much the same way,

$$\nabla \boldsymbol{Q_2} = \begin{pmatrix} 2X_2 - X_3 \\ 2X_1 - 4X_3 \\ -X_1 - 4X_2 + 4X_3 - 6X_4 \\ -6X_3 \end{pmatrix} = 2M_{Q_2}\boldsymbol{X}$$

implies that $\mathcal{Z}(\nabla \boldsymbol{Q_2})$ is the null space of the matrix $2M_{Q_2}$. However, while $\mathcal{Z}(\nabla \boldsymbol{Q_1})$ has dimension $2 = 4 - 2 = n - r$, $\mathcal{Z}(\nabla \boldsymbol{Q_2})$ has dimension 0 (i.e., $\mathcal{Z}(\nabla \boldsymbol{Q_2})$ contains only the zero vector).

4. $Q_1 = (X_1 - 2X_3)(2X_2 - X_3 + 3X_4)$, a product of two polynomials that are not scalar multiples of each other. In contrast, Q_2 does not factor into a product of linear polynomials (even over the complex numbers). These results offer a solution to the problem posed at the beginning of this article.
5. It is clear from the above factorization of Q_1 that $\mathcal{Z}(Q_1)$ is the union of two hyperplanes whose equations are $X_1 - 2X_3 = 0$ and $2X_2 - X_3 + 3X_4 = 0$. As $X_1 - 2X_3$ and $2X_2 - X_3 + 3X_4$ are not scalar multiples of one another, these hyperplanes are distinct. This contrasts with $\mathcal{Z}(Q_2)$, which contains only the zero vector.

The main result

The main result of this paper is the following pair of theorems. They establish the equivalence of several definitions of degeneracy (or nondegeneracy) of quadratic forms.

THEOREM 1. *Let $n \geq 2$, $\mathbb{F}$ be a field, and* $\operatorname{char}(\mathbb{F}) \neq 2$. *Let $Q = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j$ be a nonzero quadratic form in $\mathbb{F}[X_1, \ldots, X_n]$. Then the following statements are equivalent.*

1. *The matrix $M_Q = (a_{ij})$ has rank r.*
2. *There exists a nonsingular linear transformation $\varphi : V \to V$ such that the transformed polynomial $\widetilde{Q} = Q(\varphi(X_1), \ldots, \varphi(X_n))$ contains precisely r of the indeterminants $X_1, \ldots, X_n$; furthermore, for any other nonsingular linear transformation, this number is at least r.*
3. *$\mathcal{Z}(\nabla \boldsymbol{Q})$ is a vector space of dimension $n - r$.*

Define r, the *rank* of a quadratic form Q, as in any of the three equivalent statements listed above. Then r is an integer such that $1 \leq r \leq n$. If $r = 1$ or 2, then we can supplement the above three statements with two more, which appear frequently in the context of conics or quadratic surfaces. In the following, let $\mathbb{K}$ denote a field that is either equal to $\mathbb{F}$, or is a quadratic extension $\mathbb{F}(m)$ of $\mathbb{F}$ for some $m \in \mathbb{K} \setminus \mathbb{F}$ such that $m^2 \in \mathbb{F}$.

THEOREM 2. *Let n, $\mathbb{F}$, and Q be as in Theorem 1, and let $r = 1$ or 2. Then the following statements are equivalent.*

1. *The matrix $M_Q = (a_{ij})$ has rank r.*
2. *There exists a nonsingular linear transformation $\varphi : V \to V$ such that the transformed polynomial $\widetilde{Q} = Q(\varphi(X_1), \ldots, \varphi(X_n))$ contains precisely r of the indeterminants $X_1, \ldots, X_n$; furthermore, for any other nonsingular linear transformation, this number is at least r.*
3. *$\mathcal{Z}(\nabla \boldsymbol{Q})$ is a vector space of dimension $n - r$.*
4. *Q is a product of two linear forms with coefficients in $\mathbb{K}$. These forms are scalar multiples of one another if $r = 1$, and are not if $r = 2$.*
5. *$\mathcal{Z}(Q)$ is a hyperplane in $\mathbb{K}^n$ for $r = 1$. $\mathcal{Z}(Q)$ is the union of two distinct hyperplanes in $\mathbb{K}^n$ for $r = 2$.*

Statements 1, 2, 3, and 5 primarily use terms of linear algebra, with statement 3 having an analysis flavor and statement 5 a geometric one. Statement 4 is algebraic. The statements in Theorems 1 and 2 correspond to the properties of Q_1 and Q_2 discussed in the above examples.

We are now ready for our main definition.

DEFINITION. Let Q be as in Theorem 1, and suppose that Q has rank r. If $1 \leq r < n$, we call Q *degenerate* and *singular*. If instead $r = n$, we call Q *nondegenerate* and *nonsingular*.

If $r = 1$ or 2, we call Q *reducible*. If instead $r \geq 3$, we call Q *irreducible*.

We make several comments about this definition.

- As a nonzero quadratic form can be factored only into the product of two linear forms, our definition of irreducibility corresponds to the one in algebra for polynomials. Indeed, a quadratic form factors into linear forms (over some extension $\mathbb{K}$ of $\mathbb{F}$) for $n \geq 2$ if and only if $1 \leq r \leq 2$.
- Similar definitions can be applied to the case $n = 1$, where every nonzero form $Q = aX_1^2 = (aX_1)X_1$, $a \neq 0$, is called *reducible*, *nondegenerate*, and *nonsingular*.
- We wish to emphasize that $n = 3$ is the only case in which the notions of degeneracy, singularity, and reducibility are equivalent.
- Consider the example from the previous section. Note that since $n = 4$ and $r = 2$, our definition implies that Q_1 is degenerate, singular, and reducible. By contrast, Q_2 is nondegenerate, nonsingular, and irreducible.

Proof of Theorems 1 and 2

First we mention a few well-known results that we will need.

Let R^t denote the transpose of a matrix R, and let $\boldsymbol{X} = (X_1, \ldots, X_n)^t$ be the column vector of indeterminants. Then, in terms of matrix multiplication, we have $(Q) = \boldsymbol{X}^t M_Q \boldsymbol{X}$, a 1×1 matrix. From now on, we will view (Q) as the polynomial Q, and simply write $Q = \boldsymbol{X}^t M_Q \boldsymbol{X}$.

Let $\varphi : V \to V$ be a linear transformation, $Y_i = \varphi(X_i)$ for all i, and let $\boldsymbol{Y} = (Y_1, \ldots, Y_n)^t$. Then we define

$$\varphi(\boldsymbol{X}) = (\varphi(X_1), \ldots, \varphi(X_n))^t,$$

and therefore

$$\varphi(\boldsymbol{X}) = (Y_1, \ldots, Y_n)^t = \boldsymbol{Y}.$$

Letting B_φ be the matrix of φ with respect to a basis $\{X_1, \ldots, X_n\}$ of V, we have

$$\boldsymbol{Y} = B_\varphi \boldsymbol{X}.$$

This allows us to use matrix multiplication in order to determine $M_{\widetilde{Q}}$. Indeed, we have

$$\widetilde{Q} = \widetilde{Q}(X_1, \ldots, X_n) = \boldsymbol{X}^t M_{\widetilde{Q}} \boldsymbol{X}$$

and

$$\begin{aligned} \widetilde{Q} = Q(\varphi(X_1), \ldots, \varphi(X_n)) &= Q(Y_1, \ldots, Y_n) \\ &= \boldsymbol{Y}^t M_Q \boldsymbol{Y} \\ &= \left(B_\varphi \boldsymbol{X}\right)^t M_Q \left(B_\varphi \boldsymbol{X}\right) \\ &= \boldsymbol{X}^t \left(B_\varphi^t M_Q B_\varphi\right) \boldsymbol{X}. \end{aligned}$$

The equality $X^t M_{\widetilde{Q}} X = X^t \left(B_\varphi^t M_Q B_\varphi\right) X$, viewed as an equality of 1×1 matrices with polynomial entries, implies that

$$M_{\widetilde{Q}} = B_\varphi^t M_Q B_\varphi.$$

Recall that for any square matrix M and any nonsingular matrix N of the same dimensions, $\operatorname{rank}(MN) = \operatorname{rank}(M) = \operatorname{rank}(NM)$. Therefore, φ nonsingular implies that so is B_φ. Thus,

$$\operatorname{rank}(M_Q) = \operatorname{rank}(M_{\widetilde{Q}}).$$

Finally, we will need the fundamental fact (see, for example, [**31**, Section 7.33(b)]) that given any quadratic form Q with $\operatorname{rank}(M_Q) = r$, there exists a nonsingular linear transformation ψ of V such that if $Q' = Q(\psi(X_1), \ldots, \psi(X_n))$, then $M_{Q'}$ is diagonal. In other words,

$$Q' = d_1 X_1^2 + \cdots + d_r X_r^2,$$

where all d_i are nonzero elements of $\mathbb{F}$. This implies that for any nonsingular linear transformation φ of V, $\widetilde{Q} = Q(\varphi(X_1), \ldots, \varphi(X_n))$ contains at least r variables X_i. Indeed, if $\widetilde{Q}$ contained $r' < r$ variables, then $r = \operatorname{rank}(M_Q) = \operatorname{rank}(M_{\widetilde{Q}}) \leq r'$, a contradiction.

We are now ready to prove Theorems 1 and 2. Let (k) stand for statement k of Theorem 1 or Theorem 2, $k = 1, \ldots, 5$. We need to prove that (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3), and, when $r = 1$ or 2, that (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5).

(1) $\Leftrightarrow$ (2). The statement follows immediately from our remarks above on the diagonal form of Q, as the rank of a diagonal matrix is the number of its nonzero entries.

(1) $\Leftrightarrow$ (3). It is straightforward to verify that $(2M_Q)X = \nabla Q$. Since $\operatorname{char}(\mathbb{F}) \neq 2$, $\mathcal{Z}(\nabla Q)$ coincides with the null space of M_Q. Hence,

$$\dim(\mathcal{Z}(\nabla Q)) = n - \operatorname{rank}(M_Q) = n - r.$$

This proves the equivalence of statements (1), (2), and (3), and thus concludes the proof of Theorem 1. This equivalence leads to the notion of the rank of a quadratic form Q, which was defined to be r as it occurs in any of these equivalent statements.

We now suppose that the rank of Q is $r = 1$ or 2.

(2) $\Leftrightarrow$ (4). We have $\operatorname{rank}(M_Q) = r = 1$ or 2. As explained above, there exists a nonsingular transformation ψ of V such that $Q' = Q(\psi(X_1), \ldots, \psi(X_n)) = d_1 X_1^2 + \cdots + d_r X_r^2$, with all d_i being nonzero elements of $\mathbb{F}$, and $\operatorname{rank}(M_{Q'}) = \operatorname{rank}(M_Q) = r$. If $r = 1$, then $Q' = d_1 X_1^2$, where $d_1 \neq 0$. Then $Q = d_1(\psi^{-1}(X_1))^2$ factors as claimed. If instead $r = 2$, then $Q' = d_1 X_1^2 + d_2 X_2^2$, where both $d_i \neq 0$. Let $m \in \mathbb{K}$ such that $m^2 = -d_2/d_1$. Then

$$\begin{aligned} Q' &= d_1 X_1^2 + d_2 X_2^2 \\ &= d_1 \left(X_1^2 - \frac{-d_2}{d_1} X_2^2 \right) \\ &= d_1 \left(X_1^2 - m^2 X_2^2 \right) \\ &= (d_1 X_1 - d_1 m X_2)(X_1 + m X_2). \end{aligned}$$

The two factors of Q' are independent in the vector space of linear forms; otherwise, $m = -m$, which is equivalent to $m = 0$ because $\operatorname{char}(\mathbb{F}) \neq 2$. This implies that $d_2 = 0$, a contradiction. Hence,

$$Q = \left(d_1\psi^{-1}(X_1) - d_1 m\psi^{-1}(X_2)\right) \cdot \left(\psi^{-1}(X_1) + m\psi^{-1}(X_2)\right).$$

Since ψ^{-1} is nonsingular, $\psi^{-1}(X_1)$ and $\psi^{-1}(X_2)$ are linearly independent over $\mathbb{F}$. Hence, the factors of Q are linearly independent over $\mathbb{K}$. This proves that (2) $\Rightarrow$ (4).

Suppose Q factors over $\mathbb{K}$ such that $Q = a(a_1X_1 + \cdots + a_nX_n)^2$ with $a, a_i \in \mathbb{K}$ and $a \neq 0$. Permuting indices as necessary, suppose $a_1 \neq 0$; then apply the linear substitution φ defined by

$$\varphi(X_1) = \frac{1}{a_1}X_1 - \sum_{i=2}^{n} \frac{a_i}{a_1}X_i \quad \text{and} \quad \varphi(X_i) = X_i \text{ for all } 2 \leq i \leq n.$$

This transformation is nonsingular, and the resulting quadratic form $\widetilde{Q} = aX_1^2$ has $r = 1$ indeterminant, implying (2).

Suppose instead that Q factors over $\mathbb{K}$ with $Q = (a_1X_1 + \cdots + a_nX_n)(b_1X_1 + \cdots + b_nX_n)$, where $a_i, b_i \in \mathbb{K}$ such that the factors do not differ by a scalar multiple. This is equivalent to the vectors $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ being linearly independent. Therefore, permuting indices as necessary, the vectors $(a_1, a_2), (b_1, b_2) \in \mathbb{F}^2$ are linearly independent with $a_1 \neq 0$ and $b_2 \neq 0$. Apply the linear substitution φ defined by

$$\begin{aligned}
\varphi(X_1) &= \alpha_{11}X_1 + \alpha_{12}X_2 + \cdots + \alpha_{1n}X_n \\
\varphi(X_2) &= \alpha_{21}X_1 + \alpha_{22}X_2 + \cdots + \alpha_{2n}X_n \\
\varphi(X_i) &= X_i \text{ for all } i = 3, \ldots, n,
\end{aligned}$$

where (α_{ij}) is the inverse of the matrix

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix},$$

and I_{n-2} is the $(n-2) \times (n-2)$ identity matrix. This nonsingular transformation produces the quadratic form $\widetilde{Q} = X_1X_2$, which contains $r = 2$ indeterminants. Note that if there existed a linear transformation $\phi : V \to V$ such that $\hat{Q} = Q(\phi(X_1), \ldots, \phi(X_n))$ had only one indeterminant, then

$$1 = \operatorname{rank}(M_{\hat{Q}}) = \operatorname{rank}(M_Q) = \operatorname{rank}(M_{\widetilde{Q}}) = 2,$$

a contradiction. This proves that (4) $\Rightarrow$ (2).

(4) $\Leftrightarrow$ (5). The implication (4) $\Rightarrow$ (5) is obvious, and we concentrate on the converse.

Let $a_1X_1 + \cdots + a_nX_n = 0$ be an equation of a hyperplane W of $\mathbb{K}^n$ such that $W \subseteq \mathcal{Z}(Q)$. Then for every solution $(\alpha_1, \ldots, \alpha_n)$ of $a_1X_1 + \cdots + a_nX_n = 0$, $Q(\alpha_1, \ldots, \alpha_n) = 0$. As not all a_i are zero, we may assume by permuting the indices as necessary that $a_1 \neq 0$. Dividing by a_1, we rewrite the equation $a_1X_1 + \cdots + a_nX_n = 0$ as $X_1 + a_2'X_2 + \cdots + a_n'X_n = 0$. Viewing Q as an element of $\mathbb{K}[X_2, \ldots, X_n][X_1]$ and dividing it by $X_1 + (a_2'X_2 + \cdots + a_n'X_n)$ with remainder, we obtain

$$Q = q \cdot \left(X_1 + \left(a_2'X_2 + \cdots + a_n'X_n\right)\right) + t,$$

with quotient $q \in \mathbb{K}[X_2, \ldots, X_n][X_1]$ and remainder $t \in \mathbb{K}[X_2, \ldots, X_n]$. Now, we have $Q(w_1, \ldots, w_n) = 0 = w_1 + (a_2'w_2 + \cdots + a_n'w_n)$ for every $(w_1, \ldots, w_n) \in$

W. Furthermore, for every $(w_2, \ldots, w_n) \in \mathbb{K}^{n-1}$, there exists $w_1 \in \mathbb{K}$ such that $(w_1, \ldots, w_n) \in W$. This implies that $t(w_2, \ldots, w_n) = 0$ for every $(w_2, \ldots, w_n) \in \mathbb{K}^{n-1}$. The following lemma will allow us to conclude that $t = 0$.

LEMMA. *Let $n \geq 1$, $\mathbb{K}$ be a field such that* $\operatorname{char}(\mathbb{K}) \neq 2$, *and $f \in \mathbb{K}[X_1, ..., X_n]$ be a quadratic form that vanishes on $\mathbb{K}^n$. Then $f = 0$.*

Proof. We proceed by induction. For $n = 1$, $f = f(X_1) = aX_1^2$ for some $a \in \mathbb{K}$. Then $0 = f(1) = a$, and so $f = 0$.

Suppose the statement holds for all quadratic forms containing fewer than n indeterminants. We write f as

$$f(X_1, \ldots, X_n) = aX_1^2 + f_2(X_2, \ldots, X_n)X_1 + f_3(X_2, \ldots, X_n),$$

where $a \in \mathbb{K}$, $f_2 \in \mathbb{K}[X_2, \ldots, X_n]$ is a linear form, and $f_3 \in \mathbb{K}[X_2, \ldots, X_n]$ is a quadratic form. As $\operatorname{char}(\mathbb{K}) \neq 2$, we know that 0, 1, and -1 are distinct elements of $\mathbb{K}$. As f vanishes on $\mathbb{K}^n$, f vanishes at every point of the form $(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathbb{K}^n$ with $\alpha \in \{0, 1, -1\}$. Therefore, we obtain the three equations

$$\begin{aligned} 0 &= f(0, \alpha_2, \ldots, \alpha_n) = f_3(\alpha_2, \ldots, \alpha_n) \\ 0 &= f(1, \alpha_2, \ldots, \alpha_n) = a + f_2(\alpha_2, \ldots, \alpha_n) + f_3(\alpha_2, \ldots, \alpha_n) \\ 0 &= f(-1, \alpha_2, \ldots, \alpha_n) = a - f_2(\alpha_2, \ldots, \alpha_n) + f_3(\alpha_2, \ldots, \alpha_n) \end{aligned}$$

for all $(\alpha_2, \ldots, \alpha_n) \in \mathbb{K}^{n-1}$. By induction hypothesis, the first equation implies that $f_3 = 0$. Then the second and third equations together imply that $a = 0$ and that $f_2(\alpha_2, \ldots, \alpha_n) = 0$ for all $(\alpha_2, \ldots, \alpha_n) \in \mathbb{F}^{n-1}$. Let $f_2 = a_2X_2 + \cdots + a_nX_n$. If $f_2 \neq 0$, then there exists $a_i \neq 0$. Setting $\alpha_i = 1$ and $\alpha_j = 0$ for all $j \neq i$, we obtain

$$0 = f_2(0, \ldots, 0, 1, 0, \ldots, 0) = a_i \neq 0,$$

a contradiction. Thus, $f_2 = 0$, and so $f = 0$. The lemma is proved. ■

Indeed, this lemma implies that $t = 0$. Therefore, Q factors into a product of two linear forms, each defining a hyperplane in $\mathbb{K}^n$. We now proceed based on whether $r = 1$ or 2. If $r = 1$, then $\mathcal{Z}(Q)$ is a hyperplane of $\mathbb{K}^n$. Thus, both factors of Q must define $\mathcal{Z}(Q)$, and so they are nonzero scalar multiples of one another. If instead $r = 2$, then $\mathcal{Z}(Q)$ is the union of two hyperplanes of $\mathbb{K}^n$, corresponding to the two factors of Q. As the hyperplanes are distinct, the factors are not scalar multiples of one another. Therefore, (5) $\Rightarrow$ (4).

This concludes the proof of the theorem. ■

We end this section with the following comment. Let $Q = Q(X_1, \ldots, X_n)$ be a quadratic form of rank $r = 2$ over a field $\mathbb{F}$, $\operatorname{char}(\mathbb{F}) \neq 2$. It easily follows from our arguments that Q is a product of two linear forms over $\mathbb{F}$ if and only if there exists a nonsingular linear transformation $\varphi : V \to V$ such that

$$Q(\varphi(X_1), \ldots, \varphi(X_n)) = X_1^2 - X_2^2.$$

Related terminology in the literature

We now present a table of sources that utilize the statements from Theorems 1 and 2. The letters used in the table are as follows: D for *degenerate*, S for *singular*, and R for *reducible*. The columns labeled (1) to (5) refer to the corresponding statements from the theorems. Entries with a $*$ indicate that the source mentions the statement, but does not use a particular term to describe it. In addition to providing the reader with additional materials, we use this table to illustrate the variety of ways in which the words *degenerate*, *reducible*, and *singular* are used to refer to these statements. In particular, we see that each word is used to describe multiple statements, and that statements (1), (2), (4), and (5) are each referred to by multiple words!

A few additional notes will prove useful before studying the table. While some sources consider forms (often in the $n = 3$ case), others focus on conics in the classical projective plane $PG(2, q)$. As conics are simply quadrics in projective space, it is not surprising that the characterizations of degenerate quadrics and degenerate conics are nearly identical. Thus, we will not make any further attempt to distinguish them. In addition, we found many sources that discuss equivalent notions, but not in the context of quadratic forms or conics; they have therefore been excluded from this table.

The table illustrates the vocabulary in some of the sources that are available to us. The decision to exclude (or include) a source should not be interpreted as a criticism (or endorsement).

TABLE 1: This table shows how the words degenerate (D), reducible (R), and singular (S) are used in the literature to refer to the statements in Theorems 1 and 2. A $*$ indicates that a source refers to the statement, but does not use a particular term to describe it.

	(1)	(2)	(3)	(4)	(5)
[1]		D or S			
[2]				R	$*$
[3]				D	D
[4]	S				
[6]					R
[8]		S			
[9]	$*$			D	
[10]	$*$		S	R	R
[11]	S	$*$			
[15]	$*$	$*$	S		
[16]	S				
[19]	$*$		$*$		$*$
[20]	D				
[23]	$*$			D	D
[24]	$*$		S		
[25]	$*$			D	D
[26]				$*$	R
[28]	D				
[29]	$*$		$*$	D or R	$*$
[30]	D	$*$			
[31]	S				
[33]	$*$				D
[35]	$*$		S	R	

Concluding remarks

The discussion in previous sections leads to many interesting questions. We will briefly describe some of them.

What about similar studies of higher-order forms? Let $1 \le d \le n$, and let f be a polynomial from $\mathbb{F}[X_1, \dots, X_n]$ such that $f = \sum_{(i_1,\dots,i_d)} a_{i_1\dots i_d} X_{i_1} \cdots X_{i_d}$, where all $a_{i_1\dots i_d} \in \mathbb{F}$, and summation is taken over all integer sequences $(i_1, \dots, i_d)$, $1 \le i_1 \le i_2 \le \cdots \le i_d$. Then f is called a d-form of n indeterminants. 1-forms and 2-forms were discussed in the previous sections as linear and quadratic forms, respectively. When $d \ge 3$, the coefficients $a_{i_1\dots i_d}$ can be considered as entries of a d-dimensional matrix, which has n^d entries total. Such matrices and their determinants have been studied for more than three hundred years, and by many mathematicians, including Cayley, Silvester, Weierstrass, Garbieri, Gegenbauer, Dedekind, Lecat, Oldenburger, and Sokolov. The time and space necessary to define related notions and results is much more that this article allows, and we refer the reader to a monograph by Sokolov [**32**]. It contains a complete classification of forms over the fields of real and complex numbers for $d = 3$ and $n = 2$ or 3, but discussion of even these cases is far from short. (The classification is with respect to the nonsingular linear transformation of variables). While the monograph is in Russian, it contains 231 references in a variety of languages.

The question of factorization of a general d-form with n indeterminants, over a field for $d \ge 3$, seems to be highly nontrivial, and we could not find any useful criteria for this.

The question of classification of quadratic forms over the integers with respect to the unimodular linear transformation of variables is classical, and significant progress was made in this direction in the 18th and 19th centuries, culminating with the work of Gauss. Its source is the problem of representing integers by a given quadratic form with integer coefficients. For example:

Let $Q(X_1, X_2) = X_1^2 - X_1X_2 + 5X_2^2$. Describe all ordered triples of integers (n, a, b) such that $n = Q(a, b)$.

For related results and their extensions for forms over other rings, see O'Meara [**27**], Buell [**7**], and Conway [**12**]. For new directions and results related to multidimensional determinants, d-forms, see Gelfand, Kapranov, and Zelevinsky [**13**]. For cubic forms in algebra, geometry and number theory, see Manin [**22**].

Acknowledgment We thank attendees of the University of Delaware Discrete Mathematics/Algebra Seminar for their ruthless criticism.

REFERENCES

1. S. Barwick and G. Ebert, *Unitals in Projective Planes,* Springer, New York, 2008. http://dx.doi.org/10.1007/978-0-387-76366-8
2. L. M. Batten, *Combinatorics of Finite Geometries,* Cambridge University Press, Cambridge, 1997.
3. M. K. Bennett, *Affine and Projective Geometry,* John Wiley, New York, 1995.
4. G. Birkhoff and S. MacLane, *A Survey of Modern Algebra,* Macmillan, New York, 1941.
5. R. Bix, *Conics and Cubics, A Concrete Introduction to Algebraic Curves,* Springer, New York, 2006. http://dx.doi.org/10.1007/0-387-39273-4
6. E. Brieskorn and H. Knörrer, *Plane Algebraic Curves,* Birkhäuser, Basel, 1986. http://dx.doi.org/10.1007/978-3-0348-5097-1
7. D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations,* Springer, New York, 1989. http://dx.doi.org/10.1007/978-1-4612-4542-1
8. P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms,* Cambridge University Press, Cambridge, 1994.

9. A. D. Campbell, *Advanced Analytic Geometry,* John Wiley, New York, 1938.
10. R. Casse, *Projective Geometry: An Introduction,* Oxford University Press, Oxford, 2006.
11. J. W. S. Cassels, *Rational Quadratic Forms,* London Mathematical Society Monographs **13**, Academic Press, London, 1978.
12. J. H. Conway with the assistance of F. Y. C. Fung, *The Sensual (Quadratic) Form,* Mathematical Association of America, Washington, DC, 2005.
13. I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, Resultants, and Multidimensional Determinants,* Birkhäuser, Boston, MA, 1994. http://dx.doi.org/10.1007/978-0-8176-4771-1
14. K. W. Gruenberg and A. J. Weir, *Linear Geometry,* Van Nostrand, Princeton, N.J., 1967.
15. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* The Clarendon Press/Oxford University Press, New York, 1998.
16. W. V. D. Hodge and D. Pedoe, *Methods of Algebraic Geometry,* Vol. II, Cambridge Mathematical Library, Book III: General theory of algebraic varieties in projective space, Book IV: Quadrics and Grassmann varieties, Reprint of the 1952 original, Cambridge University Press, Cambridge, 1994.
17. K. Hoffman and R. Kunze, *Linear Algebra,* Prentice-Hall Inc., Englewood Cliffs, N.J., 1971.
18. D. R. Hughes and F. C. Piper, *Projective Planes,* Springer, New York, 1973.
19. W. E. Jenner, *Rudiments of Algebraic Geometry,* Oxford University Press, New York, 1963.
20. A. Kurosh, *Higher Algebra,* Mir, Moscow, 1988.
21. R. Lidl and H. Niederreiter, *Finite Fields,* Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997.
22. Yu. I. Manin, *Cubic Forms,* North-Holland, Amsterdam, 1986.
23. E. A. Maxwell, *The Methods of Plane Projective Geometry, Based on the Use of General Homogeneous Coordinates,* Cambridge University Press, Cambridge, 1946.
24. R. Miranda, *Algebraic Curves and Riemann Surfaces,* American Mathematical Society, Providence, RI, 1995.
25. P. S. Modenov and A. S. Parkhomenko, *Geometric Transformations. Vol. 2: Projective Transformations,* Academic Press, New York, 1965.
26. M. Namba, *Geometry of Projective Algebraic Curves,* Marcel Dekker, New York, 1984.
27. O. T. O'Meara, *Introduction to Quadratic Forms,* Springer, Berlin, 2000. http://dx.doi.org/10.1007/978-3-642-62031-7
28. M. Reid, *Undergraduate Algebraic Geometry,* Cambridge University Press, Cambridge, 1988.
29. P. Samuel, *Projective Geometry,* Springer, New York, 1988.
30. I. R. Shafarevich, *Basic Algebric Geometry: Varieties in Projective Space,* Springer, New York, 1995.
31. G. E. Shilov, *Linear Algebra,* Dover, New York, 1977.
32. N. P. Sokolov, *Space Matrices and Their Application* (in Russian), Moscow, 1961.
33. D. M. Y. Sommerville, *Analytic Geometry of Three Dimensions,* Cambridge University Press, New York, 1951.
34. J. Stolfi, *Oriented Projective Geometry, A Framework for Geometric Computations,* Academic Press, Boston, MA, 1991.
35. R. J. Walker, *Algebraic Curves,* Princeton University Press, Princeton, NJ, 1950.

Summary Consider the problem of determining, without using a computer or calculator, whether a given quadratic form factors into the product of two linear forms. A solution derived by inspection is often highly nontrivial; however, we can take advantage of equivalent conditions. In this article, we prove the equivalence of five such conditions. Furthermore, we discuss vocabulary such as "reducible," "degenerate," and "singular" that are used in the literature to describe these conditions, highlighting the inconsistency with which this vocabulary is applied.

BRIAN G. KRONENTHAL is an assistant professor of mathematics at Kutztown University of Pennsylvania. He earned a B.S. from Lafayette College (Easton, Pennsylvania) and a Ph.D. from the University of Delaware, where his advisor was F. Lazebnik. His research problems are currently motivated by extremal combinatorics; however, he uses tools from a variety of mathematical areas. In addition to teaching and research, he enjoys playing tennis and rooting for the Philadelphia Phillies.

FELIX LAZEBNIK is a professor of mathematics at the University of Delaware. His research interests are in graph theory and combinatorics, and as tools, he likes to use number theory, algebra, geometry, and simple analysis. After receiving his M.S. from Kiev State University under L. A. Kalužnin and M. H. Klin, for four and a half years he worked as a mathematics teacher in a high school. He received his Ph.D. from the University of Pennsylvania, where his advisor was H. S. Wilf. He likes both teaching and doing research. He enjoys literature, history of mathematics and sciences, art of Leonard Cohen, movies, nature, travels and food, especially when these can be discussed or shared with friends and family.