PFISTER'S THEOREM ON SUMS OF SQUARES

KEITH CONRAD

A classical identity in algebra is the 2-square identity:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2. \tag{1}$$

This expresses a sum of two squares times a sum of two squares as another sum of two squares. It was known by Brahmagupta in the 600s and rediscovered 1000 years later by Fermat. For example, since $5 = 1^2 + 2^2$ and $13 = 2^2 + 3^2$, we get

$$65 = 5 \cdot 13 = (1 \cdot 2 - 2 \cdot 3)^2 + (1 \cdot 3 + 2 \cdot 2)^2 = 4^2 + 7^2.$$

A similar 4-square identity was found by Euler in 1748:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \\ &\quad (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ &\quad (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + \\ &\quad (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned}$$

This was rediscovered by Hamilton (1843) in his work on quaternions. Soon thereafter, Graves (1843) and Cayley (1845) independently found an 8-square identity: the product $(x_1^2+\cdots+x_8^2)(y_1^2+\cdots+y_8^2)$ equals

$$\begin{aligned}&(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2 \quad + \\ &(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7)^2 \quad + \\ &(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6)^2 \quad + \\ &(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5)^2 \quad + \\ &(x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4)^2 \quad + \\ &(x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3)^2 \quad + \\ &(x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2)^2 \quad + \\ &(x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1)^2.\end{aligned}$$

This formula had been discovered about 25 earlier, by Degen, but that was unknown to Hamilton, Cayley, and Graves. Mathematicians began searching next for a 16-square identity, but results were inconclusive for a long time.

The general question we ask is: for which n is there an identity

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \tag{2}$$

where the z's are algebraically determined by the x's and y's? The 2-square and 4-square identities (as well as the 8-square identity of Cayley and Graves) describe the z's as simple polynomial functions of the x's and y's. In 1898, Hurwitz proved a theorem that killed this subject: if an identity of the form (2) holds in a field of characteristic 0, where each z_i is a bilinear function of the x's and the y's, then $n = 1, 2, 4$ or 8. In fact, as was shown later, for these values of n the identity must be the known one up to a linear change of variables.

Hurwitz's theorem should not have ended the seach for a 16-square identity. Hurwitz proved you can't hope for an identity like (2) for $n = 16$ where the z's are bilinear functions of the x's and the y's. But perhaps there is an identity of a different form.

In the 1960s, a 16-square identity was finally discovered [4]. The identity did not violate Hurwitz's theorem (with bilinear z_i's), since it involved variables in the denominators. Even more generally, and without knowing about [4], Pfister [1, 2] proved that an identity like (2) holds whenever n is a power of 2, with the z's being rational functions in the x's and y's. His method was so simple that everyone was taken by surprise. A few years later, Pfister found an even easier approach to his result, and this is what we describe here (based on [3, pp. 22-24]).

The heart of the argument is the following lemma. We write $M^\top$ for the transpose of M.

Lemma 1. *Let F be a field. Suppose $c = c_1^2 + \cdots + c_n^2$, where n is a power of 2 and $c_i \in F$. Then there is an $n \times n$ matrix C with first row*

$$(c_1, \ldots, c_n)$$

and $CC^\top = C^\top C = cI_n$.

Note: The $(1,1)$ entry of $CC^\top$ is c. This is how we will use the lemma.

Proof. Writing $n = 2^m$, we induct on m. The case $m = 0$ is easy. For the case $m = 1$, we want a matrix

$$C = \begin{pmatrix} c_1 & c_2 \\ u & v \end{pmatrix}$$

such that

$$CC^\top = C^\top C = \begin{pmatrix} c_1^2 + c_2^2 & 0 \\ 0 & c_1^2 + c_2^2 \end{pmatrix}.$$

Well,

$$\begin{aligned} CC^\top &= \begin{pmatrix} c_1 & c_2 \\ u & v \end{pmatrix}\begin{pmatrix} c_1 & u \\ c_2 & v \end{pmatrix} \\ &= \begin{pmatrix} c_1^2 + c_2^2 & c_1u + c_2v \\ c_1u + c_2v & u^2 + v^2 \end{pmatrix}. \end{aligned}$$

Setting $u = c_2, v = -c_1$ (or $u = -c_2, v = c_1$) works. The reader can check $C^\top C$ also equals cI_2.

Now we suppose the result is true for $2^{m-1} \times 2^{m-1}$ matrices, with $m \geq 2$, and we want to prove it for $2^m \times 2^m$ matrices. Let $c = a + b$, where a and b are each sums of half the squares involved in c, say

$$a = c_1^2 + \cdots + c_{n/2}^2,\ b = c_{n/2+1}^2 + \cdots + c_n^2.$$

By induction, there are $2^{m-1} \times 2^{m-1}$ matrices A and B, with respective first rows $(c_1, \ldots, c_{n/2})$ and $(c_{n/2+1}, \ldots, c_n)$, such that

$$AA^\top = A^\top A = aI_{n/2},\ BB^\top = B^\top B = bI_{n/2}.$$

Based on what we want C to look like, let's try to get it in the form

$$C = \begin{pmatrix} A & B \\ U & V \end{pmatrix}. \tag{3}$$

What should U and V be?

When matrices are decomposed into square blocks of the same size, as in (3), addition and multiplication of such matrices can be carried out by working with the blocks as the "entries",

taking care to remember that matrices may not multiplicatively commute. Therefore

$$\begin{aligned} CC^\top &= \begin{pmatrix} A & B \\ U & V \end{pmatrix} \begin{pmatrix} A^\top & U^\top \\ B^\top & V^\top \end{pmatrix} \\ &= \begin{pmatrix} AA^\top + BB^\top & AU^\top + BV^\top \\ UA^\top + VB^\top & UU^\top + VV^\top \end{pmatrix} \\ &= \begin{pmatrix} (a+b)I_{n/2} & AU^\top + BV^\top \\ UA^\top + VB^\top & UU^\top + VV^\top \end{pmatrix}. \end{aligned}$$

The off-diagonal blocks are transposes of each other, so we will have $CC^\top = cI_n$ provided

$$AU^\top + BV^\top = O,\ UU^\top + VV^\top = cI_{n/2}. \tag{4}$$

Inspired by the discussion in the 2×2 case, let's take $V = A$. Then the first equation implies

$$U = -AB^\top (A^{-1})^\top,$$

provided A is invertible. Is A invertible? Since $AA^\top = aI_{n/2}$, $\det(A)^2 = a^{n/2}$. So if a is nonzero then A is invertible. Is $a \neq 0$? When $c \neq 0$, the equation $c = a + b$ shows one of a or b is nonzero, and we can suppose $a \neq 0$ by relabelling. The case $c = 0$ is tricky, and we will treat it later.

First, let's check that, when $c \neq 0$ (so we can choose $a \neq 0$ and thus A is invertible), the above choices of U and V work:

$$\begin{aligned} UU^\top + VV^\top &= (-AB^\top (A^{-1})^\top)(-A^{-1}BA^\top) + AA^\top \\ &= AB^\top (A^\top)^{-1} A^{-1} BA^\top + AA^\top \\ &= AB^\top (AA^\top)^{-1} BA^\top + aI_{n/2} \\ &= AB^\top (aI_{n/2})^{-1} BA^\top + aI_{n/2} \\ &= (1/a) AB^\top BA^\top + aI_{n/2} \\ &= (1/a) A(bI_{n/2}) A^\top + aI_{n/2} \\ &= (b/a) AA^\top + aI_{n/2} \\ &= bI_{n/2} + aI_{n/2} \\ &= cI_{n/2}. \end{aligned}$$

This shows $CC^\top = cI_n$. Since $c \neq 0$, C is invertible, so the equation $C^\top C = cI_n$ follows automatically.

We return to the case $c = 0$, which is almost wholly a technicality. It is possible here that both a and b vanish. Consider $0 = (1^2 + i^2) + (1^2 + i^2)$. However, in this example there is a rearranged half-sum decomposition with nonzero a (and b), namely $0 = (1^2 + 1^2) + (i^2 + i^2)$. This is true in general: if

$$0 = c_1^2 + c_2^2 + \cdots + c_n^2,$$

where n is a power of 2 (or any positive even integer), then either some half-sum of terms is nonzero or the c_j^2 are all equal. Indeed, if every half-sum of terms vanishes, then the sum of the first $n/2$ squares is 0 and the sum of the first $n/2 - 1$ squares added to $c_{n/2+1}^2$ is 0, so $c_{n/2}^2 = c_{n/2+1}^2$. By symmetry, all c_j^2 are equal.

When $c = 0$ and one of the $\binom{n}{2}$ possible half-sums is nonzero, choose that for a and run through the above argument. (Now, since C is not invertible, one really has to check directly that $C^\top C = cI_n$ rather than deduce it from $CC^\top = cI_n$. This is left to the reader.)

When $c = 0$ and all c_j^2 are equal, then $0 = nc_1^2$. Recall $n = 2^m$ is a power of 2. Therefore when F has odd characteristic, $c_1 = 0$ (so each c_j is zero) and we can take for C the zero matrix. When

F has characteristic 2, let C be the matrix whose rows all equal $(c_1, \ldots, c_n)$. Then each entry of $CC^\top$ is $\sum c_j^2 = 0$, so $CC^\top = O$. Multiplying in the other order, the (i,j) entry of $C^\top C$ is nc_ic_j, which vanishes since $n = 0$ in F. Thus, $C^\top C = O$. □

Theorem 1 (Pfister)**.** *In any field F, the set of sums of n squares is closed under multiplication when n is a power of 2.*

Proof. Let

$$x = x_1^2 + \cdots + x_n^2,\ y = y_1^2 + \cdots + y_n^2,$$

with $x_i, y_i \in F$. In the lemma, choose $n \times n$ matrices X and Y such that

$$XX^\top = X^\top X = xI_n,\ \ YY^\top = Y^\top Y = yI_n,$$

with the first row of X being $(x_1, \ldots, x_n)$ and the first row of Y being $(y_1, \ldots, y_n)$. Then

$$(XY)(XY)^\top = XYY^\top X^\top = yXX^\top = xyI_n.$$

Let the first row of XY be denoted $(z_1, \ldots, z_n)$. Then $(XY)(XY)^\top$ has (1,1) entry

$$z_1^2 + \cdots + z_n^2 = xy = (x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2).$$

□

In the proof of this theorem, the main point was to get the $(1,1)$ entry, but we needed the full matrix machinery to produce it. Using $XY^\top$ in place of XY, we can arrange that

$$z_1 = x_1y_1 + \cdots + x_ny_n,$$

but we are not assured that the other z_i will be bilinear functions of the two sets of variables. However, we are always assured that z_i is a linear function in one of the set of variables (say the x's for concreteness). It will not be linear in the other set of variables, however.

Corollary 1. *If n is a power of 2 and $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ are independent variables over a field K, there is an algebraic identity of the form*

$$(X_1^2 + \cdots + X_n^2)(Y_1^2 + \cdots + Y_n^2) = Z_1^2 + \cdots + Z_n^2,$$

where $Z_i \in K(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$.

Proof. Apply Pfister's theorem to the field $F = K(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$, with $x_i = X_i$ and $y_i = Y_i$. □

Corollary 2. *Let n be a power of 2. In any field F, the set of nonzero sums of n squares in F is a group under multiplication.*

Proof. Pfister's theorem tells us this set is closed under multiplication. Closure under inversion follows by a simple trick: for nonzero s,

$$s = a_1^2 + \cdots + a_n^2 \Rightarrow \frac{1}{s} = \frac{s}{s^2} = \left(\frac{a_1}{s}\right)^2 + \cdots + \left(\frac{a_n}{s}\right)^2.$$

□

If we make the proof of Pfister's theorem explicit, then we see denominators are introduced from the term $-AB^\top(A^{-1})^\top$ in the lemma. (Specifically, there will be a denominator $\det A$.) Let's describe this recursively and see what sum of squares formulas Pfister's theorem gives us for small n.

Suppose $n > 1$ is a power of 2 and we have a formula for products of sums of $n/2$ squares. Then, when $x = \sum_{i=1}^n x_i^2$ and $y = \sum_{i=1}^n y_i^2$, Pfister says xy is a sum of squares of the first row of XY (or $XY^\top$), where X and Y are $n \times n$ matrices of the form

$$X = \begin{pmatrix} A & B \\ -AB^\top(A^{-1})^\top & A \end{pmatrix},\quad Y = \begin{pmatrix} C & D \\ -CD^\top(C^{-1})^\top & C \end{pmatrix},$$

with A being the $n/2 \times n/2$ matrix from the lemma which corresponds to $\sum_{i=1}^{n/2} x_i^2$, B being the $n/2 \times n/2$ matrix corresponding to $\sum_{i=n/2+1}^{n} x_i^2$, and likewise for C and D. (Here, for simplicity, we are assuming the half-sums in their initial order are nonzero, which is certainly the case if the x_i's and y_i's are indeterminates.)

Let's start with $n = 2$. Say $x = x_1^2 + x_2^2$ and $y = y_1^2 + y_2^2$. Matrices of size $n/2 \times n/2$ are numbers, so they commute and equal their transpose. We take

$$X = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 & y_2 \\ -y_2 & y_1 \end{pmatrix},$$

and the sum of squares formula for xy (using either XY or $XY^\top$) is the classical identity (1). Notice that the 2×2 matrices we obtain are the usual matrix representations of the complex numbers $x_1 + x_2 i$ and $y_1 + y_2 i$.

Now let $n = 4$, $x = \sum_{i=1}^4 x_i^2$, and $y = \sum_{i=1}^4 y_i^2$. By the previous step, the 2×2 matrices corresponding to the half-sums $x_1^2 + x_2^2$, $x_3^2 + x_4^2$, $y_1^2 + y_2^2$, and $y_3^2 + y_4^2$ are the usual matrix representations of the complex numbers $x_1 + x_2 i$, $x_3 + x_4 i$, $y_1 + y_2 i$, and $y_3 + y_4 i$. In particular, transposition of these 2×2 matrices corresponds to complex conjugation of the complex numbers. A 2×2 matrix product $-AB^\top (A^{-1})^\top$ here corresponds to a complex number of the form $-z\overline{w}/\overline{z} = -z^2\overline{w}/|z|^2$, which introduces a genuine denominator. Using the lemma, a 4×4 matrix X which has first row (x_1, x_2, x_3, x_4) and satisfies $XX^\top = X^\top X = xI_4$, is

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ w_1/d & w_2/d & x_1 & x_2 \\ -w_2/d & w_1/d & -x_2 & x_1 \end{pmatrix},$$

where $w_1 = -(x_1^2 - x_2^2)x_3 - 2x_1x_2x_4$, $w_2 = (x_1^2 - x_2^2)x_4 - 2x_1x_2x_3$, and $d = x_1^2 + x_2^2$. Unlike Euler's 4-square identity, Pfister's 4-square identity has denominators: $(\sum_{i=1}^4 x_i^2)(\sum_{i=1}^4 y_i^2) = \sum_{i=1}^4 z_i^2$, where (z_1, z_2, z_3, z_4) is the first row of the matrix product XY:

$$z_1 = x_1y_1 - x_2y_2 + x_3\frac{-y_1^2y_3 - 2y_1y_2y_4 + y_2^2y_3}{y_1^2 + y_2^2} + x_4\frac{-y_4y_1^2 + 2y_1y_2y_3 + y_2^2y_4}{y_1^2 + y_2^2},$$

$$z_2 = x_1y_2 + x_2y_1 + x_3\frac{y_1^2y_4 - 2y_1y_2y_3 - y_2^2y_4}{y_1^2 + y_2^2} + x_4\frac{-y_1^2y_3 - 2y_1y_2y_4 + y_2^2y_3}{y_1^2 + y_2^2},$$

$$z_3 = x_1y_3 - x_2y_4 + x_3y_1 - x_4y_2, \qquad z_4 = x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1.$$

(The change of variables $y_1 \to y_2, y_2 \to -y_1, y_3 \to y_4, y_4 \to -y_3$ interchanges z_1 with z_2 and z_3 with z_4.)

If instead we let (z_1, z_2, z_3, z_4) be the first row of $XY^\top$, then

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \qquad z_2 = -x_1y_2 + x_2y_1 - x_3y_4 + x_4y_3,$$

$$z_3 = x_1\frac{-y_1^2y_3 - 2y_1y_2y_4 + y_2^2y_3}{y_1^2 + y_2^2} + x_2\frac{y_4y_1^2 - 2y_1y_2y_3 - y_2^2y_4}{y_1^2 + y_2^2} + x_3y_1 + x_4y_2,$$

$$z_4 = x_1\frac{-y_1^2y_4 + 2y_1y_2y_3 + y_2^2y_4}{y_1^2 + y_2^2} + x_2\frac{-y_1^2y_3 - 2y_1y_2y_4 + y_2^2y_3}{y_1^2 + y_2^2} - x_3y_2 + x_4y_1.$$

What can be said about products of sums of n squares if n is not a power of 2? Depending on the choice of n, one can write down an explicit field K such that an identity of the form

$$(X_1^2 + \cdots + X_n^2)(Y_1^2 + \cdots + Y_n^2) = Z_1^2 + \cdots + Z_n^2$$

does not exist with $Z_i \in K(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$. This is stronger than the nonexistence of a bilinear sum of n squares formula, and shows no formula like Pfister's exists for sums of n squares when n is not a power of 2. The fields K can be found in [3, p. 20–21].

References

[1] A. Pfister, "Zur Darstellung von -1 als Summe von Quadraten in einem Körper," *J. London Math. Soc.* **40** (1965), 159–165.
[2] A. Pfister, "Multiplikative quadratische Formen," *Arch. Math.* **16** (1965), 363–370.
[3] A. R. Rajwade, *Squares*, Cambridge Univ. Press, Cambridge, 1993.
[4] H. Zassenhaus and W. Eichhorn, "Herleitung von Acht- und Sechzehn-Quadrate-Identitäten mit Hilfe von Eigenschaften der verallgemeinerten Quaternionen und der Cayley-Dicksonchen Zahlen," *Arch. Math.* **17** (1966), 492–496.