Notes towards a constructive proof of Hilbert's Theorem on ternary quartics

Victoria Powers and Bruce Reznick

1. Introduction

In 1888, Hilbert [**5**] proved that a real ternary quartic which is positive semidefinite (psd) must have a representation as a sum of three squares of quadratic forms. Hilbert's proof is short, but difficult; a high point of 19th century algebraic geometry. There have been two modern expositions of the proof – one by Cassels in the 1993 book [**6**] by Rajwade, and one by Swan [**8**] in these Proceedings – but there are apparently no other proofs of this theorem in the literature. In 1977, Choi and Lam [**2**] gave a short elementary proof that a psd ternary quartic must be a sum of (five) squares of quadratic forms, but as we shall see, the number "three" is critical.

Hilbert's approach does not address two interesting computational issues:

1. Given a psd ternary quartic, how can one find three such quadratics?
2. How many "fundamentally different" ways can this be done?

In this paper, we describe some methods for finding and counting representations of a psd ternary quartic as a sum of three squares. In certain special cases, we can answer these questions completely, describing all representations in detail. For example, if $p(x, y, z) = x^4 + F(y, z)$, where F is a psd quartic, then we give an algorithm for constructing all representations of p as a sum of three squares. We show that if F is not the fourth power of a linear form, then there are at most 8 such representations. The key idea to our work is the simple observation that if $p = f^2 + g^2 + h^2$, then $p - f^2$ is a sum of two squares. We also give an equivalent form of Hilbert's Theorem which involves only binary forms.

2. Preliminaries

Suppose

$$p(x, y, z) = \sum_{i+j+k=4} \alpha_{i,j,k} x^i y^j z^k \tag{1}$$

is a ternary quartic. How can we tell whether p is psd? The general answer, by the theory of quantifier elimination (see, e.g., [**1**]) tells us that this is the case if and only if the coefficients of p belong to a particular semi-algebraic set. This general

1991 *Mathematics Subject Classification.* 11E20, 11E76, 14N15, 12Y05.

set is likely to be rather unedifying to look at in detail, so it will be convenient to make a few harmless assumptions about p.

Suppose that $p(x_1, \dots, x_n)$ is a homogeneous polynomial. By an *invertible change* taking p to p', we will mean a formal identity:

$$p(x_1'\dots, x_n') = p'(x_1, \dots, x_n), \qquad \begin{bmatrix} x_1' \\ \vdots \\ x_n' \end{bmatrix} = \begin{bmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix},$$

where the matrix $M = [m_{ij}]$ above is in $GL(n, \mathbf{R})$. Note that p is psd if and only if p' is psd, and representations of p as a sum of m squares are immediately transformed into similar representations of p' and vice versa.

For example, if $p(x_1, \dots, x_n)$ is a psd quadratic form of rank r, then after an invertible change, $p = x_1^2 + \cdots + x_r^2$. If $deg\ p = d$ and $M = cI$, then $p' = c^d p$. Thus, multiplying p by a positive constant is an invertible change. A non-trivial application of invertible changes is given in Theorem 6 below. When making invertible changes, we will customarily drop the primes as soon as no confusion would result.

Suppose now that p is a non-zero psd ternary quartic. Then there exists a point (a, b, c) for which $p(a, b, c) > 0$. By an (invertible) rotation, we may assume that $p(t, 0, 0) = t^4 p(1, 0, 0) = u > 0$, and so we may assume that $p(1, 0, 0) = 1$; hence $\alpha_{4,0,0} = 1$. Writing p in decreasing powers of x, we have

$$p(x, y, z) = x^4 + \alpha_{3,1,0}x^3y + \alpha_{3,0,1}x^3z + \dots.$$

If we now let $x' = x + \frac{1}{4}(\alpha_{3,1,0}y + \alpha_{3,0,1}z)$, $y' = y$, $z' = z$, then $x = x' - \frac{1}{4}(\alpha_{3,1,0}y' + \alpha_{3,0,1}z')$, $y = y'$, $z = z'$, and it's easy to see that $p'(x, y, z) = x^4 + 0\cdot x^3y + 0\cdot x^3z + \cdots$.

We may thus assume without loss of generality that

$$p(x, y, z) = x^4 + 2F_2(y, z)x^2 + 2F_3(y, z)x + F_4(y, z), \tag{2}$$

where F_j is a binary form of degree j in (y, z). Henceforth, we shall restrict our attention to ternary quartics of this shape.

We present a condition for p to be psd. No novelty is claimed for this result, which has surely been known in various guises for centuries. Note that p is psd if and only if, for all $(y, z) \in \mathbf{R}^2$ and all real t,

$$\Phi_{(y,z)}(t) := t^4 + 2F_2(y, z)t^2 + 2F_3(y, z)t + F_4(y, z) \geq 0.$$

THEOREM 1. *The quartic* $\Phi(t) = t^4 + 2at^2 + 2bt + c$ *satisfies* $\Phi(t) \geq 0$ *for all* t *if and only if* $c \geq 0$ *and*

$$|b| \leq \frac{2}{3\sqrt{3}} \left(-a + \sqrt{a^2 + 3c}\right)^{1/2} \left(2a + \sqrt{a^2 + 3c}\right) := K(a, c). \tag{3}$$

PROOF. A necessary condition for $\Phi(t) \geq 0$ for all t is that $\Phi(0) = c \geq 0$. If $\Phi(0) = 0$, then $\Phi'(0) = 2b = 0$ as well, and clearly $t^4 + 2at^2 \geq 0$ if and only if $a \geq 0$. Thus, one possibility is that $c = 0$, $b = 0$, and $a \geq 0$.

We may henceforth assume that $\Phi(0) = c > 0$, and so, dividing by $|t|$, $\Phi(t) \geq 0$ for all $|t|$ if and only if $|t|^3 + 2a|t| + 2b \cdot \mathrm{Sign}(t) + c|t|^{-1} \geq 0$, which holds if and only if

$$\min_{u>0} \left(u^3 + 2au + \frac{c}{u}\right) \geq 2|b|.$$

The minimum occurs when $3u_0^4 + 2au_0^2 - c = 0$. The only positive solution to this equation is

$$u_0 = \left(\frac{-a + \sqrt{a^2 + 3c}}{3} \right)^{1/2}.$$

Thus, using $c = 3u_0^4 + 2au_0^2$ to simplify the computation, we see that $\Phi(t) \geq 0$ if and only if

$$2|b| \leq u_0^3 + 2au_0 + cu_0^{-1} = 4u_0^3 + 4au_0 = 4u_0(u_0^2 + a) \tag{4}$$

$$= 4\left(\frac{1}{3}\left(-a + \sqrt{a^2+3c}\right)\right)^{1/2}\left(\frac{1}{3}\left(-a + \sqrt{a^2+3c}\right) + a\right) = 2K(a,c). \tag{5}$$

We are nearly done, because this case assumes that $c > 0$. But note that if $c = 0$, we have $K(a, 0) = 0$ if $a \geq 0$ and $K(a, 0) < 0$ if $a < 0$, so $|b| \leq K(a, 0)$ implies $b = 0$ and $a \geq 0$ when $c = 0$, subsuming the first case. □

Note that if (a, b, c) satisfies (3), then $K(a, c) \geq 0$, and it's easy to check that this implies that $a \geq -\sqrt{c}$. However, it is not necessary to write this as a separate condition.

COROLLARY 2. *Suppose p is given by* (2). *Then p is psd if and only if F_4 is psd, and for all $(r, s) \in \mathbf{R}^2$,*

$$|F_3(r, s)| \leq K(F_2(r, s), F_4(r, s)). \tag{6}$$

We remark, that, even after squaring, (6) is not a "true" illustration of quantifier elimination, because there will still be square roots on the right-hand side.

3. The Gram matrix method

Observe that for polynomials in $f, g \in \mathbf{R}[X] := \mathbf{R}[x_1, \ldots, x_n]$ and for all θ,

$$f^2 + g^2 = (\cos\theta f + \sin\theta g)^2 + (\pm\sin\theta f \mp \cos\theta g)^2. \tag{7}$$

More generally, if $M = [m_{ij}]$ is a real $t \times t$ orthogonal matrix, then

$$\sum_{i=1}^{t}\left(\sum_{j=1}^{t} m_{ij} f_j\right)^2 = \sum_{j=1}^{t}\sum_{k=1}^{t}\left(\sum_{i=1}^{t} m_{ij}m_{ik}\right) f_j f_k = \sum_{j=1}^{t} f_j^2. \tag{8}$$

(Note that (7) includes all real 2×2 orthogonal matrices.) Thus, any attempt to count the number of representations of a form as a sum of squares must mod out the action of the orthogonal group.

Choi, Lam and Reznick [**4**] have developed a method for studying representations of a form $p \in \mathbf{R}[X]$ as a sum of squares, called the *Gram matrix method.* For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$, we write $|\alpha|$ to denote $\sum \alpha_i$ and X^α to denote $x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$. Suppose p is a form in $\mathbf{R}[X]$ which is a sum of squares of forms. Then p must have even degree $2d$ and thus can be written

$$p = \sum_{|\alpha|=2d} a_\alpha X^\alpha.$$

Suppose now that p has a representation

$$p = h_1^2 + \cdots + h_t^2 \tag{9}$$

where $h_i = \sum_{|\beta|=d} b_\beta^{(i)} X^\beta$. For each $\beta \in \mathbf{N}^n$ of degree d, set $U_\beta = (b_\beta^{(1)}, \dots, b_\beta^{(t)})$. Then (9) becomes $p = \sum_{\beta,\beta'} U_\beta \cdot U_{\beta'} X^{\beta+\beta'}$. Hence, for each α,

$$a_\alpha = \sum_{\beta+\beta'=\alpha} U_\beta \cdot U_{\beta'}. \tag{10}$$

The matrix $V := [U_\beta \cdot U_{\beta'}]$ (indexed by $\beta \in \mathbf{N}^n$ with $|\beta| = d$) is the *Gram matrix* of p associated to (9). Note that $V = (v_{\beta,\beta'})$ is symmetric, positive semidefinite, and the entries satisfy the equations

$$a_\alpha = \sum_{\beta+\beta'=\alpha} v_{\beta,\beta'}. \tag{11}$$

The following result is proven in [**4**, Thm. 2.4, Prop. 2.10]:

THEOREM 3. *Suppose $p = \sum_{|\alpha|=2d} a_\alpha X^\alpha$ and $V = [v_{\beta,\beta'}]$ is a real symmetric matrix indexed by all $\beta \in \mathbf{N}^n$ such that $|\beta| = d$.*

1. *The following are equivalent: (a) p is a sum of squares of forms and V is the Gram matrix associated to a representation $p = \sum h_i^2$, (b) V is positive semidefinite and the entries of V satisfy the equations* (11).
2. *If V is the Gram matrix of a representation of p as a sum of squares, then the minimum number of squares needed in a representation corresponding to V is the rank of V.*
3. *Two representations of p as a sum of t squares are orthogonally equivalent, as in* (8)*, if and only if they have the same Gram matrix.*

We now form the (general) Gram matrix of p by solving the linear system corresponding to the equations (11), where the $v_{\beta,\beta'}$ are variables, with $v_{\beta,\beta'} = v_{\beta',\beta}$. This gives the $v_{\beta,\beta'}$'s as linear polynomials in some parameters. Then $V = [v_{\beta,\beta'}]$ is the Gram matrix of p. By Theorem 3, values of the parameters for which V is psd correspond to representations of p as a sum of squares, with the minimum number of squares needed equal to the rank of V.

If we consider the two sets of vectors of coefficients from the two representations given in (8), we see that one set is the image of the other upon by the action of M, and since M is orthogonal, the dot products of the vectors are unaltered. If p happens to be a quadratic form, then upon arranging the monomials in the usual order, it's easy to see that the (unique) Gram matrix for p is simply the usual matrix representation for p. It follows that a psd quadratic form has, in effect, only one representation as a sum of squares.

Henceforth, when we say that $p \in \mathbf{R}[X]$ is *a sum of t real squares in m ways*, we shall mean that the sums of t squares comprise m distinct orbits under the action of the orthogonal group, or, equivalently, that there are exactly m different psd matrices of rank t which satisfy (11).

Finally, we remark that a real Gram matrix for p of rank t which is *not* psd corresponds to a representation of p as a sum or difference of t squares over $\mathbf{R}$ and that a complex Gram matrix of rank t corresponds to a sum of t squares over $\mathbf{C}$. These facts require relatively simple proofs, but we defer these to a future publication.

4. Hilbert's Theorem and Gram matrices – an introduction

We describe how the Gram matrix method works for ternary quartics. There are 6 monomials in a quadratic form in three variables, and 15 coefficients in the ternary quartic. This means that there are 21 distinct entries in the Gram matrix and 15 equations in (11), and hence the solution to the linear system will have $6 = 21-15$ parameters. Thus the Gram matrix of a ternary quartic is 6×6 with entries linear in 6 parameters. If we recall (1), denote the parameters by $\{a,b,c,d,e,f\}$, and write the monomials of degree 2 in the order $x^2, y^2, z^2, xy, xz, yz$, then we find the general form of a Gram matrix of a ternary quartic p:

$$\begin{bmatrix} \alpha_{4,0,0} & a & b & \frac{1}{2}\alpha_{3,1,0} & \frac{1}{2}\alpha_{3,0,1} & d \\ a & \alpha_{0,4,0} & c & \frac{1}{2}\alpha_{1,3,0} & e & \frac{1}{2}\alpha_{0,3,1} \\ b & c & \alpha_{0,0,4} & f & \frac{1}{2}\alpha_{1,0,3} & \frac{1}{2}\alpha_{0,1,3} \\ \frac{1}{2}\alpha_{3,1,0} & \frac{1}{2}\alpha_{1,3,0} & f & \alpha_{2,2,0}-2a & \frac{1}{2}\alpha_{2,1,1}-d & \frac{1}{2}\alpha_{1,2,1}-e \\ \frac{1}{2}\alpha_{3,0,1} & e & \frac{1}{2}\alpha_{1,0,3} & \frac{1}{2}\alpha_{2,1,1}-d & \alpha_{2,0,2}-2b & \frac{1}{2}\alpha_{1,1,2}-f \\ d & \frac{1}{2}\alpha_{0,3,1} & \frac{1}{2}\alpha_{0,1,3} & \frac{1}{2}\alpha_{1,2,1}-e & \frac{1}{2}\alpha_{1,1,2}-f & \alpha_{0,2,2}-2c \end{bmatrix}$$

Hilbert's Theorem together with Theorem 3 says that if p is psd, then for some choice of the parameters $\{a,b,c,d,e,f\}$, this matrix will be psd and have rank 3.

We ignore the psd requirement for the moment and consider the problem of finding choices of parameter for which this Gram matrix has rank 3. For any such matrix, all 4×4 minors will equal zero. There are 225 such minors, although by symmetry there are at most 120 different minors. Each minor is the determinant of a 4×4 matrix with entries linear in the parameters, and hence its vanishing is an equation of degree at most 4 in the 6 parameters.

Thus for a specific ternary quartic p we can form a system of 120 equations of degree at most 4 in 6 variables so that the solutions correspond to rank 3 Gram matrices for p. We can attempt to solve this system, however in almost all cases, the system is much too complicated to solve "by hand". We have made use of a computational tool called RealSolving, which can count the number of solutions, both complex and real, in the case where there are only finitely many complex solutions. For details on RealSolving, see [**7**] and the RealSolving webpage

`www.loria.fr/~rouillie`

Example. We consider $p(x,y,z) = x^4+y^4+z^4$. The Gram matrix of p is

$$V = V(a,b,c,d,e,f) := \begin{bmatrix} 1 & a & b & 0 & 0 & d \\ a & 1 & c & 0 & e & 0 \\ b & c & 1 & f & 0 & 0 \\ 0 & 0 & f & -2a & -d & -e \\ 0 & e & 0 & -d & -2b & -f \\ d & 0 & 0 & -e & -f & -2c \end{bmatrix}.$$

Since p is psd, Hilbert's Theorem states that it is a sum of three squares; indeed, one such representation is evident. In terms of the Gram matrix, this means that there is a choice of values for the parameters so that $V(a,b,c,d,e,f)$ is psd with rank 3. The obvious representation

$$x^4 + y^4 + z^4 = (x^2)^2 + (y^2)^2 + (z^2)^2$$

corresponds to $V(0,0,0,0,0,0)$. But p has other representations. In fact, it's easy to see that $V(-1,0,0,0,0,0)$ is also psd with rank 3. If we seek vectors whose dot products are given by this matrix, we are easily led to the following representation:

$$x^4 + y^4 + z^4 = (x^2 - y^2)^2 + 2(xy)^2 + (z^2)^2.$$

Clearly two other such representations can be found by cycling the variables: $V(0,-1,0,0,0,0)$ and $V(0,0,-1,0,0,0)$. It turns out that there are four others. One of them is $V(r,r,r,s,s,s)$, with $r = 1-\sqrt{2}$ and $s = \sqrt{2}-2$; the three others correspond to the symmetry of p under the sign changes $y \to -y$ and $z \to -z$. (See (15), (16) below.) We will later show how these representations can be derived without using a Gram matrix.

Using RealSolving, for $p = x^4 + y^4 + z^4$ we have found that there are 15 choices of parameter in which V is a real matrix of rank 3, and 63 choices of parameter in which V is a complex matrix of rank 3. As noted above, the non-psd cases correspond to the representations of p as a sum or *difference* of three real squares or as a sum of three *complex* squares. Thus we know that there are exactly 63 (orthogonally inequivalent) ways to write p as a sum of three squares of forms over $\mathbf{C}$, of which 15 are a sum or difference of three squares over $\mathbf{R}$.

In this case, after "by hand" manipulation of the 120 equations, we can find the following 15 representations of p as a sum or difference of three squares of real quadratic forms:

$$(x^2)^2 + (y^2)^2 + (z^2)^2 \tag{12}$$

$$(x^2 - y^2)^2 + 2(xy)^2 + (z^2)^2 \tag{13}$$

$$(x^2 + y^2)^2 - 2(xy)^2 + (z^2)^2 \tag{14}$$

$$\begin{aligned}(x^2 + (1-\sqrt{2})(y^2 + \sqrt{2}yz + z^2))^2 + (\sqrt{2}-1)(x(\sqrt{2}y + z) + yz - z^2)^2 \\ +(\sqrt{2}-1)(xz - (y-z)(\sqrt{2}y + z))^2\end{aligned} \tag{15}$$

$$\begin{aligned}(x^2 + (1+\sqrt{2})(y^2 - \sqrt{2}yz + z^2))^2 - (\sqrt{2}+1)(x(-\sqrt{2}y + z) + yz - z^2)^2 \\ -(\sqrt{2}+1)(xz - (y-z)(-\sqrt{2}y + z))^2.\end{aligned} \tag{16}$$

These five equations correspond to 15 different representations, because p is both symmetric under permutation of the variables and even in each of the variables. Thus, $p = \sum f_i(x,y,z)^2$ implies that $p = \sum f_i(x, \pm y, \pm z)^2 = \sum f_i(x, \pm z, \pm y)^2 =$ etc. The "obvious" representation (12) is unaffected by these symmetries. The equations (13) and (14) correspond to three psd and three non-psd representations each, after the cyclic permutation of the variables. It is not obvious, but (15) and (16) are already symmetric in the variables (this shows up in their Gram matrices); however, the substitutions $(y,z) \to (\pm_1 y, \pm_2 z)$ make them correspond to four psd and four non-psd representations respectively.

If we consider p as a sum of three complex quadratic forms, we need to allow the entries of the Gram matrix to be complex. There are 48 non-real Gram matrices of rank 3. We find, for example, that $V(1,i,i,0,0,2i)$ has rank 3, and this gives us a representation of p as a sum of three squares:

$$(x^2+y^2+iz^2)^2+2(ixy+z^2)^2-2i(xz+yz)^2. \tag{17}$$

Since $p(x,y,z)=p(x,i^m y,i^n z)$, a cyclic permutation of the variables gives potentially $3\times 4^2=48$ different sums of squares. However, (17) is symmetric under $z\to -z$, so that it corresponds to only 24 non-real representations. We turn to the real representations of the previous paragraph, and note that (13) and (14) are now equivalent under $y\to iy$. There are also $4^2-2^2=12$ ways to take $(y,z)\to(i^m y,i^n z)$, with $0\le m,n\le 3$, where at least one of (m,n) is odd, and 12 non-real representations which correspond to such a substitution into each of (15) and (16), completing the inventory.

Finally, we note that by [**4**, Cor. 2.12], given a psd Gram matrix for p with rank 3, we may assume that x^2 appears only in the first square and xy appears only in the first two squares. Thus, we can view the totality of sums of three squares as inducing a polynomial map from $\mathbf{R}^{15}\to\mathbf{R}^{15}$:

$$\begin{gathered}(b_1x^2+b_2xy+b_3xz+b_4y^2+b_5yz+b_6z^2)^2+\\ (b_7xy+b_8xz+b_9y^2+b_{10}yz+b_{11}z^2)^2+(b_{12}xz+b_{13}y^2+b_{14}yz+b_{15}z^2)^2\\ =\textstyle\sum_{i+j+k=4}\alpha_{i,j,k}(b_1,\dots,b_{15})x^iy^jz^k.\end{gathered}$$

Hilbert's Theorem, in these terms, is that $\{\alpha_{i,j,k}(\mathbf{R}^{15})\}$ is precisely the set of coefficients of psd ternary quartics. It is not unreasonable to expect that the degree of this mapping would (usually) be finite, but we have not seen this issue discussed in detail in the other proofs of Hilbert's Theorem. We know of no studies of Hilbert's Theorem over $\mathbf{C}$.

We have applied the method of the example to a number of different real ternary quartics. In all cases, we have obtained the values $(63,15)$ for the number of complex and real solutions, apart from a couple of "degenerate" cases where the numbers are less. Our experiments suggest that the values $(63,15)$ are generic. We hope to have much more to say about this in a future publication.

5. Some preparatory results on binary forms

We now show how the representations of certain psd ternary quartics as a sum of three squares can be analyzed without using Gram matrices explicitly. This is done by reducing the analysis to certain questions about binary forms.

Suppose $p(t,u)$ is a psd binary form of degree $2d$. An invertible change is now defined by

$$p'(t,u)=p(at+bu,ct+du),\qquad ad\ne bc.$$

By the same reasoning applied to ternary quartics, we may assume that, after an invertible change, $p(1,0)=1$, so $p(t,u)=t^{2d}+\cdots$. In any given representation $p=f_1^2+f_2^2$, we have $f_1(t,u)=at^d+\dots$ and $f_2(t,u)=bt^d+\dots$. Then $a^2+b^2=1$, hence there exists α such that $a=\cos\alpha$ and $b=\sin\alpha$, and we have from (7),

$$\begin{aligned}p(t,u)&=(\cos\theta f_1+\sin\theta f_2)^2+(\pm\sin\theta f_1\mp\cos\theta f_2)^2\\ &=(\cos(\theta-\alpha)t^d+\dots)^2+(\pm(\sin(\theta-\alpha)t^d+\dots))^2\\ &:=f_{1,\theta,\pm}^2(t,u)+f_{2,\theta,\pm}^2(t,u).\end{aligned}$$

We see that, for exactly one value of θ (namely α) and one choice of sign in $\pm$, the coefficients of t^d in $f_{1,\theta,\pm}$ and $f_{2,\theta,\pm}$ are 1 and 0 respectively, and the highest power of t in $f_{2,\theta,\pm}$ has a non-negative coefficient. We will call this a *standard form* for writing p as a sum of two squares; in our terminology, p is a sum of two squares in m ways means that there are exactly m standard forms for p.

Sums of two squares always factor over $\mathbf{C}$: $p = f_1^2 + f_2^2 \implies p = (f_1 + if_2)(f_1 - if_2)$, so the expression of p in standard form as a sum of squares is equivalent to a factorization $p = G_+G_-$ over $\mathbf{C}[t,u]$ as a product of conjugate factors so that $G_\pm(1,0) = f_1(1,0) \pm if_2(1,0) = 1$. Note also that if $p = G_+G_-$, where $G_\pm = f_1 \pm if_2$, then for all θ, $p = (e^{-i\theta}G_+)(e^{i\theta}G_-)$, where

$$e^{\mp i\theta}G_\pm = (\cos\theta f_1 + \sin\theta f_2) \mp i(\sin\theta f_1 - \cos\theta f_2).$$

The linear factors of $p(t,u)$ over $\mathbf{C}[t,u]$ are either real or appear as conjugate pairs, and since the coefficient of t^{2d} in p is 1, we may arrange that the coefficient of t is 1 in each of these factors:

$$p(t,u) = \prod_{j=1}^{q}(t+\lambda_j u)^{m_j}\prod_{k=1}^{r}(t+(\mu_k+i\nu_k)u)^{n_k}\prod_{k=1}^{r}(t+(\mu_k-i\nu_k)u)^{n_k}. \tag{18}$$

Furthermore, since $p \ge 0$, the exponents of the real factors, m_j, must be even.

THEOREM 4. *Suppose $p(t,u)$ is a psd binary form of degree $2d$ with $p(1,0) = 1$, and suppose that p factors over $\mathbf{C}$ as in* (18). *Then p is a sum of two squares in $\lceil \frac{1}{2}\prod_{k=1}^{r}(n_k+1)\rceil$ ways.*

PROOF. Suppose $p = f_1^2 + f_2^2$ is given in standard form, with $f_1(1,0) = 1$, $f_2(1,0) = 0$. Suppose first that p has the real linear factor $\ell(t,u) = t + \lambda u$. Then $p(\lambda,-1) = 0$ for $j = 1,2$, hence $f_j(\lambda,-1) = 0$ as well, and so ℓ divides both f_1 and f_2. In this way, we can "peel off" all the real linear factors of p, and we may assume without loss of generality that p has only the complex conjugate factors.

As noted above, we consider the possible factorizations of $p = G_+G_-$. Since $G_+ \mid p$, there exist $0 \le a_k, b_k \le n_k$ such that

$$G_+(t,u) = \prod_{k=1}^{r}(t+(\mu_k+i\nu_k)u)^{a_k}\prod_{k=1}^{r}(t+(\mu_k-i\nu_k)u)^{b_k}.$$

Taking conjugates, we see that

$$G_-(t,u) = \prod_{k=1}^{r}(t+(\mu_k+i\nu_k)u)^{b_k}\prod_{k=1}^{r}(t+(\mu_k-i\nu_k)u)^{a_k}.$$

Comparison with the factorization of p shows that $a_k + b_k = n_k$, hence $b_k = n_k - a_k$ for all k. There are $N = \prod_{k=1}^{r}(n_k+1)$ ways to choose the a_k's, giving N pairs (G_+, G_-) of complex conjugate factors of p, which in turn define N pairs $(f_1, f_2) = (\frac{1}{2}(G_+ + G_-), \frac{1}{2i}(G_+ - G_-))$. If $G_+ \ne G_-$, then exactly one of the pairs $\{(G_+, G_-), (G_-, G_+)\}$ will leave f_2 in standard form. There is one exceptional case: if all n_k's are even, then taking $a_k = \frac{1}{2}n_k$ gives $G_+ = G_-$, and $f_2 = 0$. This occurs in the case that p is already a square. □

We shall need the following result, though not in its full generality for n variables.

THEOREM 5. *Suppose $p \in \mathbf{R}[X]$ is quartic and can be written as a sum of two squares. If p has no linear factors over $\mathbf{R}[X]$, but factors as a product of linear* *forms over* $\mathbf{C}[X]$*, then* p *is a sum of two squares in 2 ways. Otherwise,* p *is a sum of two squares in 1 way.*

PROOF. Since p is psd, if ℓ is a real linear factor and $\ell \mid p$, then $\ell^2 \mid p$, and if $p = f_1^2 + f_2^2$, then $\ell \mid f_j$. Writing $p = \ell^2\bar{p}$, $f_j = \ell\bar{f}_j$, we'd have $\bar{p} = \bar{f}_1^2 + \bar{f}_2^2$. Since $\bar{p}$ is quadratic, this means it has rank two, and there is only one way to write it as a sum of two squares (up to (8), as always.)

We now assume that p has no linear factors, $p(x_1, \dots, x_n) = x_1^4 + \dots$ and that a representation $p = f_1^2 + f_2^2$ has $f_1(1, 0, \dots, 0) = 1$ and $f_2(1, 0, \dots, 0) = 0$. Then $p = (f_1 + if_2)(f_1 - if_2)$ factors over $\mathbf{C}[X]$ as a product of conjugate quadratics, and conversely, any such factorization gives p as a sum of two squares. If p has a different standard form representation $p = g_1^2 + g_2^2$, then p has a different factorization $p = (g_1 + ig_2)(g_1 - ig_2)$, with $g_1 \pm ig_2 \neq c(f_1 \pm if_2)$. Let $\ell_1 = \gcd(f_1 + if_2, g_1 + ig_2)$. Then ℓ_1 has to be linear, and we can normalize so that $\ell_1(1, 0, \dots, 0) = 1$. It is now easy to show by unique factorization in $\mathbf{C}[X]$ that there are linear factors ℓ_j so that $\ell_j(1, 0, \dots, 0) = 1$ and

$$f_1 + if_2 = \ell_1\ell_2, \quad f_1 - if_2 = \ell_3\ell_4; \qquad g_1 + ig_2 = \ell_1\ell_3, \quad g_1 - ig_2 = \ell_2\ell_4$$

It follows that $\ell_4 = \bar{\ell}_1$ and $\ell_3 = \bar{\ell}_2$, so that $p = \ell_1\bar{\ell}_1\ell_2\bar{\ell}_2$, and this implies that the two representations are all that are possible. (It does not matter whether ℓ_1 and ℓ_2 are distinct in this case; in the notation of the last theorem, $2 = \lceil \frac{2+1}{2} \rceil = \lceil \frac{(1+1)(1+1)}{2} \rceil$.) □

Finally, we shall need the following result. It is similar to the classical canonical form for the binary quartic, which is in the literature. However, the classical theorem allows invertible changes in $GL(2, \mathbf{C})$; it is unclear whether our analysis of the real case is in the literature.

THEOREM 6. *If* $p(t, u)$ *is a psd quartic form, then using an invertible change,* $p(t, u)$ *can be put into one of the following shapes:* t^4, t^2u^2, $t^2(t^2 + u^2)$, $(t^2 + u^2)^2$, *or* $t^4 + \lambda t^2u^2 + u^4$ *with* $|\lambda| < 2$*. The particular shape of* p *depends only on the factorization of* p *over* $\mathbf{C}[t, u]$.

PROOF. Factor p as in (18). If $\sum m_j = 4$, then since the m_j's are even, either $p = \ell_1^4$ or $p = \ell_1^2\ell_2^2$, where ℓ_1 and ℓ_2 are non-proportional linear forms. Make the invertible change $t' = \ell_1(t, u)$ and $u' = \ell_2(t, u)$ to get the first two cases.

If $\sum m_j = 2$, then $p(t, u) = \ell^2 q(t, u)$, where ℓ is linear and q is a positive definite quadratic. Make a preliminary invertible change so that $\ell = t'$, drop the prime and note that $q(t, u) = at^2 + 2btu + cu^2$, where $c > 0, ac > b^2$. Thus,

$$q(t, u) = (a - \tfrac{b^2}{c})t^2 + c(\tfrac{b}{c}t + u)^2.$$

Writing $d = a - \frac{b^2}{c} > 0$ and $\ell'(t, u) = \frac{b}{c}t + u$, we can make another invertible change so that $\ell' = u'$. This shows that p can be turned into $t^2(dt^2 + u^2)$. By taking $u = \sqrt{d}u'$ and dividing by d, we obtain the third case.

In the last two cases, p has only complex conjugate roots. If they are repeated, then p is the square of a positive definite binary quadratic form, which after an invertible change is $t^2 + u^2$.

Otherwise, we may assume that $p(t, u) = (t^2 + u^2)(at^2 + 2btu + cu^2)$, where the second factor is positive definite. Under an orthogonal change of variables $t = ct' + su', u = -st' + cu'$, where $s = \sin\alpha$, $c = \cos\alpha$, the first factor becomes $(t')^2 + (u')^2$ and the coefficient of $t'u'$ in the second becomes $(a - c)\sin 2\alpha + 2b\cos 2\alpha$.

Thus, we may choose α so that the second factor is also even in t' and u'. (In fact, any two positive definite quadratic forms can be simultaneously diagonalized.) In other words, after an invertible change, we may assume that p is a product of two even positive definite quadratic forms, and after rescaling t and u if necessary, we have $p(t,u) = (t^2 + ru^2)(t^2 + \frac{1}{r}u^2) = t^4 + Rt^2u^2 + u^4$, with $R = r + \frac{1}{r} > 2$. A final invertible change gives

$$p(t+u, t-u) = (2+R)\left(t^4 + \left(\frac{12-2R}{2+R}\right)t^2u^2 + u^4\right),$$

and since $\lambda = \frac{12-2R}{2+R} = -2 + \frac{16}{2+R} = 2 - \frac{4R-8}{2+R}$, we have $|\lambda| < 2$.

$\square$

6. The direct approach to Hilbert's Theorem

Let us now assume Hilbert's Theorem, and write

$$p(x,y,z) = x^4 + 2x^2F_2(y,z) + 2xF_3(y,z) + F_4(y,z) = \sum_{j=1}^{3} f_j^2(x,y,z). \tag{19}$$

As noted earlier, we may assume that the term x^2 appears only in f_1, and up to sign, we may assume that its coefficient is 1. Thus,

$$p(x,y,z) = \Big(x^2 + g_{1,1}(y,z)x + g_{2,1}(y,z)\Big)^2 + \sum_{j=2}^{3}\Big(g_{1,j}(y,z)x + g_{2,j}(y,z)\Big)^2. \tag{20}$$

Comparing the coefficients of x^3 in (19) and (20), we see that $0 = 2g_{1,1}(y,z)$, hence we may assume that $f_1(x,y,z) = x^2 + Q(y,z)$ for a binary quadratic Q and

$$p(x,y,z) = \Big(x^2 + Q(y,z)\Big)^2 + \sum_{j=2}^{3}\Big(g_{1,j}(y,z)x + g_{2,j}(y,z)\Big)^2. \tag{21}$$

We now exploit the algebraic properties of sums of two squares, in a lemma which will be applied to $p - (x^2+Q)^2$. The basic idea is similar to [**3**, Lemma 7.5].

Lemma 7. *Suppose*

$$\phi(x,y,z) = h_2(y,z)x^2 + 2h_3(y,z)x + h_4(y,z)$$

is a quartic form (so that h_k is a form of degree k). Then there exist forms $\psi_{(j)}$ so that $\phi = \psi_{(1)}^2 + \psi_{(2)}^2$ if and only if ϕ is psd and the discriminant of ϕ as a quadratic in x,

$$\Delta(y,z) := h_2(y,z)h_4(y,z) - h_3^2(y,z),$$

is the square of a real cubic form.

Proof. First, if $\phi = \psi_{(1)}^2 + \psi_{(2)}^2$, then it is psd and we have

$$\psi_{(j)}(x,y,z) = \lambda_{(j)}(y,z)x + \mu_{(j)}(y,z),$$

hence $h_2 = \lambda_{(1)}^2 + \lambda_{(2)}^2$, $h_3 = \lambda_{(1)}\mu_{(1)} + \lambda_{(2)}\mu_{(2)}$, $h_4 = \mu_{(1)}^2 + \mu_{(2)}^2$. It follows that

$$\Delta = h_2h_4 - h_3^2 = (\lambda_{(1)}\mu_{(2)} - \lambda_{(2)}\mu_{(1)})^2.$$

Conversely, suppose ϕ is psd and Δ is a square. Then $h_2(y,z)$ is a psd quadratic form, so after an invertible change in (y,z), which will affect neither the hypothesis nor the conclusion, we may consider one of three cases: $h_2(y,z) = 0$, $h_2(y,z) = y^2$, $h_2(y,z) = y^2 + z^2$.

In the first case, $\Delta = -h_3^2$, so $h_3 = 0$ as well and $\phi(x,y,z) = h_4(y,z)$ is a psd binary quartic. By Theorem 4, $\phi = h_4$ is a sum of two squares.

In the second case, $\Delta(y,z) = y^2 h_4(y,z) - h_3^2(y,z) \geq 0$, hence $\Delta(0,z) = -h_3^2(0,z) \geq 0$, so $h_3(0,z) = 0$. Thus $h_3(y,z) = yk_2(y,z)$ for some quadratic k_2. Further, there exists a cubic form $c_3(y,z)$ so that

$$\Delta(y,z) = y^2(h_4(y,z) - k_2^2(y,z)) = c_3^2(y,z).$$

Thus, $c_3(y,z) = ys_2(y,z)$ for some quadratic s_2. But this means that $h_4 - k_2^2 = s_2^2$, hence

$$\phi(y,z) = x^2y^2 + 2xyk_2(y,z) + k_2^2(y,z) + s_2^2(y,z) = (xy + k_2(y,z))^2 + s_2^2(y,z)$$

is a sum of two squares.

Finally, in the third case, since Δ is a square, there exists real c_3 so that

$$\Delta(y,z) = (y^2+z^2)h_4(y,z) - h_3^2(y,z) = c_3^2(y,z).$$

It follows that, over $\mathbf{C}[y,z]$,

$$\begin{aligned}(y+iz)(y-iz)h_4(y,z) &= (y^2+z^2)h_4(y,z) = h_3^2(y,z) + c_3^2(y,z)\\ &= (h_3(y,z) + ic_3(y,z))(h_3(y,z) - ic_3(y,z)).\end{aligned} \tag{22}$$

Thus, up to choice of sign of c_3, $y + iz$ is a factor of $h_3(y,z) + ic_3(y,z)$. Write

$$h_3(y,z) + ic_3(y,z) = (y+iz)(k_2(y,z) + is_2(y,z)). \tag{23}$$

so that

$$h_3(y,z) = yk_2(y,z) - zs_2(y,z), \qquad c_3(y,z) = ys_2(y,z) + zk_2(y,z).$$

Taking conjugates in (23) and substituting into (22), we get

$$h_4(y,z) = (k_2(y,z) + is_2(y,z))(k_2(y,z) - is_2(y,z)) = k_2^2(y,z) + s_2^2(y,z).$$

Thus,

$$\begin{aligned}\phi(y,z) &= x^2(y^2+z^2) + 2x(yk_2(y,z) - zs_2(y,z)) + k_2^2(y,z) + s_2^2(y,z)\\ &= (xy + k_2(y,z))^2 + (xz - s_2(y,z))^2.\end{aligned}$$

□

This lemma leads to the fundamental constructive theorem of this paper.

THEOREM 8. *If p is a quartic satisfying* (19), *then p can be written as in* (21) *if and only if*

$$p(x,y,z) - (x^2 + Q(y,z))^2 = 2(F_2(y,z) - Q(y,z))x^2 + 2F_3(y,z)x + F_4(y,z) - Q^2(y,z)$$

is psd and

$$\Delta(y,z) = 2(F_2(y,z) - Q(y,z))(F_4(y,z) - Q^2(y,z)) - F_3^2(y,z)$$

is the square of a real cubic form.

Note that for every Q which satisfies the above conditions, $p(x,y,z) - (x^2 + Q(y,z))^2$ is quadratic in x and is a sum of two squares, and hence by Theorem 5 can be written as a sum of two squares in at most two ways. That is, the number of representations of p as a sum of three squares is bounded by twice the number of suitable Q.

Whereas the Gram matrix approach involves a system of polynomial equations in the six parameters $\{a,b,c,d,e,f\}$, the method of Theorem 8 involves three parameters, the coefficients of Q. It is not difficult to set up necessary conditions for a binary sextic to be the square of a cubic form, and when applied to $\Delta = 2(F_2 - Q)(F_4 - Q^2) - F_3^2$, these give a non-trivial system of three equations, although the degree is much higher than that which arises in the Gram matrix approach.

Finally, by comparing Corollary 2 and Theorem 8, we see that Hilbert's Theorem can be reduced entirely to a theorem in binary forms.

COROLLARY 9. *Suppose F_2, F_3, F_4 are binary forms of degree $2, 3, 4$ respectively, such that F_4 is psd and*

$$27F_3^2 \le 4\left(-F_2 + \sqrt{F_2^2 + 3F_4}\right)\left(2F_2 + \sqrt{F_2^2 + 3F_4}\right)^2.$$

Then there exists a binary quadratic Q such that $2(F_2 - Q)(F_4 - Q^2) - F_3^2$ is a perfect square and $F_2 - Q$ and $F_4 - Q^2$ are psd.

We believe that it should be possible to prove Corollary 9 directly. This would provide a purely constructive proof of Hilbert's Theorem. We hope to validate this belief in a future publication.

7. Some constructions

The simplest applications of Theorem 8 occur when $F_3(y,z) = 0$; that is, when p is an even polynomial in x. (Unfortunately, a constant-counting argument which we omit shows that not every real ternary quartic can be put in this form after an invertible change.) We revisit Theorem 8 in this special case:

COROLLARY 10. *There is a representation*

$$x^4 + 2F_2(y,z)x^2 + F_4(y,z) = (x^2 + Q(y,z))^2 + \sum_{j=2}^{3} f_j^2(x,y,z) \tag{24}$$

if and only if one of the following four cases holds:

- **(a):** *$F_4 - F_2^2$ is psd and $Q = F_2$.*
- **(b):** *$F_4 = k_2^2$ is a square, $Q = \pm k_2$ and $F_2 \mp k_2$ is psd.*
- **(c):** *There is a linear form ℓ so that $Q = F_2 - \ell^2$, and $F_4 - (F_2 - \ell^2)^2$ is a square.*
- **(d):** *There is a linear form ℓ so that $F_4 - Q^2 = \ell^2(F_2 - Q)$ and $F_2 - Q$ is psd. (In this case, $F_2 - Q$ is a factor of $F_4 - F_2^2$.)*

PROOF. By Theorem 8, the necessary and sufficient conditions are that

$$2(F_2(y,z) - Q(y,z))x^2 + F_4(y,z) - Q^2(y,z)$$

be psd, and that

$$\Delta(y,z) = (F_2(y,z) - Q(y,z))(F_4(y,z) - Q^2(y,z)) \tag{25}$$

is the square of a real cubic form. The first condition is equivalent to $F_2 - Q$ and $F_4 - Q^2$ both being psd. We now turn to the second condition.

If the first factor in (25) is 0, then $\Delta = 0$ is trivially a square, and $Q = F_2$. Thus, the remaining condition is that $F_4 - F_2^2$ be psd. This is (a).

If the second factor in (25) is 0, then again Δ is trivially a square and $Q^2 = F_4$. Suppose $F_4 = k_2^2$, then $Q = \pm k_2$, and the remaining condition is that $F_2 - Q = F_2 \mp k_2$ be psd and we obtain case (b).

In the remaining two cases, we have a quadratic $q_2 = F_2 - Q$ and a quartic $q_4 = F_4 - Q^2$ whose product is a square. If q_2 and q_4 are relatively prime, then each must be a square. Thus, $F_2 - Q = \ell^2$ for some linear form ℓ, and $F_4 - Q^2 = s_2^2$ is a square. This is (c).

Finally, if $\gcd(q_2, q_4) = g$, then $q_2 = gu$ and $q_4 = gv$, with u and u relatively prime, so that $q_2 q_4 = g^2 uv$ is a square. This implies that u and v are squares, so that g has even degree. This last case is that g is quadratic, so we may take $g = q_2$ and write $v = \ell^2$ for a linear form ℓ; that is, $F_4 - Q^2 = (F_2 - Q)\ell^2$. Note that this implies that $(F_2 - Q)(\ell^2 - F_2 - Q) = F_4 - F_2^2$. Thus any Q which satisfies this condition will have the additional property that $F_2 - Q$ is a psd factor of $F_4 - F_2^2$. $\square$

REMARK. We can use Corollary 10 to count the number of possible representations as a sum of three squares of $x^4 + 2F_2(y,z)x^2 + F_4(y,z)$. If (a) holds, then

$$p(x,y,z) = (x^2 + F_2(y,z))^2 + (F_4(y,z) - F_2^2(y,z)),$$

and the second summand above is a sum of two squares by Theorem 4, in one or two ways, depending on whether $F_4 - F_2^2$ has linear factors. (It may also happen to be a square: $q^2 + 0^2$ can be viewed as a sum of two squares.)

In case (b), the condition that $F_2 - Q = F_2 \mp k_2$ is psd may be true for zero, one or two choices of sign. If it is true, we have

$$p(x,y,z) = (x^2 + Q(y,z))^2 + 2x^2(F_2(y,z) - Q(y,z)),$$

If $F_2 - Q$ is psd, it is a sum of two squares (in exactly one way) by Theorem 4.

If (c) holds, then

$$p(x,y,z) = (x^2 + F_2(y,z) - \ell^2(y,z))^2 + 2\ell^2(y,z)x^2 + s_2(y,z)^2$$

is, as written, a sum of three squares. Furthermore, although $2\ell^2(y,z)x^2 + s_2(y,z)^2$ factors into quadratic forms over $\mathbf{C}[y,z]$, it does not factor into linear forms unless $\ell \mid s_2$, and so the sum of three squares is unique except in this case. It is not *a priori* clear how many different linear forms ℓ satisfy these conditions for a given pair (F_2, F_4).

Finally, in case (d),

$$p(x,y,z) = (x^2 + Q(y,z))^2 + 2(F_2(y,z) - Q(y,z))(x^2 + \ell^2(y,z)).$$

Since $F_2 - Q$ is a psd binary form, it splits into linear factors over $\mathbf{C}[y,z]$, and so any suitable Q leads to two representations of p as a sum of three squares. Again, it is not *a priori* clear how many such forms Q exist for given (F_2, F_4).

We conclude this section with some simple examples.

EXAMPLE. The psd quartic

$$p(x,y,z) = (x^2 + y^2)(x^2 + z^2) = x^4 + x^2(y^2 + z^2) + y^2 z^2$$

is a product of two sums of two squares and hence is a sum of two squares in two different ways. Are there other ways to write p as a sum of three squares? Using Theorem 8, if one of the squares is $x^2 + Q(y,z)$, then $F_2 - Q$ and $F_4 - Q^2$ must be psd. If $y^2 z^2 - Q^2(y,z)$ is psd, then $Q(y,z) = \alpha yz$ with $|\alpha| \le 1$ and $F_2 - Q = \frac{1}{2}(y^2 - 2\alpha yz + z^2)$ is psd. But

$$\Delta(y,z) = \tfrac{1-\alpha^2}{2}(y^2 - 2\alpha yz + z^2)y^2 z^2$$

will be a perfect square only when $\alpha = \pm 1$. This re-derives the familiar representations from the two-square identity:

$$p(x,y,z) = (x^2 - yz)^2 + x^2(y+z)^2 = (x^2 + yz)^2 + x^2(y-z)^2$$

EXAMPLE. The similar-looking psd quartic

$$p(x,y,z) = x^4 + x^2y^2 + y^2z^2 + z^4$$

is irreducible, and so is not a sum of two squares. It is not trivial to write p as a sum of three squares, so we apply the algorithm.

Here, $F_2(y,z) = \frac{1}{2}y^2$ and $F_4(y,z) = z^2(y^2+z^2)$. If $F_4 - Q^2$ is psd then $z \mid Q$, so $Q(y,z) = ayz + bz^2$ for some (a,b). It is easily checked that $F_4 - Q^2$ is psd if and only if $a^2 + b^2 \le 1$ and it's a square, $z^2(by - az)^2$, if and only if $a^2 + b^2 = 1$. And $F_2 - Q$ is psd if and only if $a^2 + 2b \le 0$, and it's a square, $(y - \frac{1}{2}az)^2$, if and only if $b = -\frac{1}{2}a^2$.

Running through the cases, we see that (a) and (b) are not possible, because Q cannot equal F_2 and F_4 is not a square. For (c), $F_2 - Q$ and $F_4 - Q^2$ are both squares when $b = -\frac{1}{2}a^2$ and $a^2 + b^2 = 1$, which implies that

$$a = \pm\tau := \pm\sqrt{2\sqrt{2} - 2}, \qquad b = 1 - \sqrt{2}.$$

This gives the representation

$$p(x,y,z) = (x^2 \pm \tau yz + (1-\sqrt{2})z^2)^2 + x^2(y \mp \tau z)^2 + z^2((\sqrt{2}-1)y \pm \tau z)^2.$$

The sum of the last two squares does not split over $\mathbf{C}[y,z]$, so there are no additional representations in this case. In (d), $\frac{1}{2}y^2 - Q(y,z) = \frac{1}{2}(y^2 - 2ayz - 2bz^2)$ must be a psd factor of

$$F_4 - F_2^2 = z^4 + z^2y^2 - \tfrac{1}{4}y^4 = \left(z^2 + \tfrac{1-\sqrt{2}}{2}y^2\right)\left(z^2 + \tfrac{1+\sqrt{2}}{2}y^2\right).$$

Thus, it is a multiple of $z^2 + \frac{1+\sqrt{2}}{2}y^2$, and $a = 0$, $b = 1 - \sqrt{2}$. This leads to

$$p(x,y,z) = (x^2 + (1-\sqrt{2})z^2)^2 + (x^2 + z^2)(y^2 + (2\sqrt{2}-2)z^2);$$

since the last sum of two squares splits into linear factors over $\mathbf{C}$, there are two more representations of p as a sum of two squares, making four in all.

EXAMPLE. We consider the class of quartics: $p(x,y,z) = (x^2 + G(y,z))^2$, so that $F_2(y,z) = 2G(y,z)$ and $F_4(y,z) = G^2(y,z)$. By Corollary 10, p is a sum of three squares as in (24) if and only if $2(G - Q)$ and $G^2 - Q^2$ are both psd and $(G-Q)(G^2-Q^2) = (G-Q)^2(G+Q)$ is a square. If $G = Q$, then these conditions are satisfied immediately, and of course, we recover the representation of p as a single square. If $G = -Q$, then we get another representation, provided G is psd:

$$(x^2 + G(y,z))^2 = (x^2 - G(y,z))^2 + 4x^2G(y,z).$$

Since G is a quadratic form, this gives p as a sum of two squares if $G = \ell^2$ and a sum of three squares if G is positive definite. Otherwise, we must have that $G - Q$ is psd and $G + Q$ is a square. This means that $G(y,z) \ge |Q(y,z)|$ for all (y,z), and hence G is psd. Thus $Q(y,z)$ can be $-(G(y,z) - (ay+bz)^2)$ for any (a,b) for which $2G(y,z) - (ay+bz)^2$ is psd.

If G has rank 1, then after an invertible change, $G(y,z) = y^2$, and $Q(y,z) = (1-a^2)y^2$, so that $(G+Q)(y,z) = (2-a^2)y^2 \ge 0$; that is, $Q(y,z) = -\lambda y^2$, with $-1 \le \lambda \le 1$. This gives an infinite family of representations:

$$(x^2+y^2)^2 = (x^2 - \lambda y^2)^2 + (2+2\lambda)x^2y^2 + (1-\lambda^2)y^4.$$

If G has rank 2, then after an invertible change, $G(y,z) = y^2+z^2$, and $G \ge |Q|$ if and only if $a^2+b^2 \le 2$. This gives a doubly infinite family of representations:

$$(x^2+y^2+z^2)^2 = (x^2-(y^2+z^2-(ay+bz)^2))^2+(2(y^2+z^2)-(ay+bz)^2)(2x^2+(ay+bz)^2).$$

If G is not psd, then p has only the trivial representation. This also can be seen directly: since $x^2+G(y,z)$ is indefinite, in any representation $p = \sum f_j^2$, f_j must be a multiple of $x^2+G(y,z)$; by degrees, it must be a scalar multiple. Thus any representation of p as a sum of squares is orthogonally equivalent to the trivial one.

8. A complete answer in a special case

We now simplify further still, by supposing that $F_2(y,z) = 0$ as well, so that

$$p(x,y,z) = x^4 + F_4(y,z),$$

where F_4 is a psd quartic form. Hilbert's Theorem is no mystery in this special case, because we already know that F_4 can be written as a sum of two squares, and this gives one way to write p as a sum of three squares. Are there any other representations? Note that necessary conditions on Q include that $-Q$ and $F_4 - Q^2$ are both psd.

There are five cases, based on the factorization of F_4; we shall need two lemmas about real binary forms.

LEMMA 11. *Suppose $F(y,z)$ is a positive definite quartic form, and consider the equation*

$$F(y,z) - (ay+bz)^4 = q^2(y,z) \tag{26}$$

for linear forms $ay+bz$ and quadratic forms q. If F is a square, then (26) has only the trivial solution $(a,b) = (0,0)$. If F is not a square, then there are two different q's for which (26) holds.

PROOF. By Theorem 6, we may assume that $F(y,z) = y^4 + \lambda y^2z^2 + z^4$ and that $-2 < \lambda \le 2$. There are two trivial solutions to (26):

$$\begin{aligned} &y^4 + \lambda y^2z^2 + z^4 - (1 - \tfrac{\lambda^2}{4})z^4 = (y^2 + \tfrac{\lambda}{2}z^2)^2, \\ &y^4 + \lambda y^2z^2 + z^4 - (1 - \tfrac{\lambda^2}{4})y^4 = (\tfrac{\lambda}{2}y^2 + z^2)^2. \end{aligned} \tag{27}$$

If $\lambda = 2$, these are truly trivial! It is easy to see that these are the only possible expressions in which $a = 0$ or $b = 0$. For other solutions, assume $ab \ne 0$, and set up the five equations for the coefficients of $F(y,z) - (ay+bz)^4 = (ry^2+syz+tz^2)^2$:

$$1-a^4 = r^2, \quad -4a^3b = 2rs, \quad \lambda - 6a^2b^2 = 2rt + s^2, \quad -4ab^3 = 2st, \quad 1 - b^4 = t^2.$$

Since $4r^2s^2t^2 = r^2(2st)^2 = t^2(2rs)^2$, we have

$$(1-a^4)(-4ab^3)^2 = (1-b^4)(-4a^3b)^2 \implies a^2b^6 - a^6b^6 = a^6b^2 - a^6b^6.$$

Since $ab \ne 0$ it follows that $a^4 = b^4$, so $a^2 = b^2$ and so $rs = st$. If $s = 0$, then $ab = 0$, which is impossible, so we conclude that $r = t$. But then

$$s^2 = s^2 + 2rt - 2r^2 = (\lambda - 6a^2b^2) - 2(1-a^4) = \lambda - 2 - 4a^4 < 0,$$

which is a contradiction. Thus, (27) gives the only solutions to (26). □

LEMMA 12. *If $F(y,z)$ and $G(y,z)$ are non-proportional positive definite quadratic forms, then there is a unique positive number μ_0 such that $F - \mu_0 G$ is the non-zero square of a linear form.*

PROOF. Since F and G are both positive definite, the following minimum is well-defined; it is positive, and achieved for $\theta = \theta_0$:

$$\mu_0 = \min_{0 \le \theta \le 2\pi} \frac{F(\cos\theta, \sin\theta)}{G(\cos\theta, \sin\theta)}.$$

Let $H_\mu(y,z) = F(y,z) - \mu G(y,z)$. Then H_{μ_0} is psd and $H_{\mu_0}(\cos\theta_0, \sin\theta_0) = 0$, and as F and G are not proportional, H_{μ_0} is not identically zero. Thus H_{μ_0} is the non-zero square of a linear form. If $\mu < \mu_0$, then H_μ is positive definite, and so is not a square; if $\mu > \mu_0$, then $H_\mu(\cos\theta_0, \sin\theta_0) < 0$, so H_μ is not even psd. □

If $|\lambda| < 2$, then $\lambda = 2 - \nu^2$ with $0 < \nu < 2$, so

$$y^4 + \lambda y^2 z^2 + z^4 = (y^2 + \nu yz + z^2)(y^2 - \nu yz + z^2)$$

is a product of two positive definite quadratics. In this case, the computation of μ_0 is extremely easy: the minimum occurs at the extreme value of $\cos\theta\sin\theta$, namely, $\pm\frac{1}{2}$ and

$$\mu_0 = \min_{0 \le \theta \le 2\pi} \frac{1 + \nu\cos\theta\sin\theta}{1 - \nu\cos\theta\sin\theta} = \frac{1 - \frac{\nu}{2}}{1 + \frac{\nu}{2}}.$$

In this case, note that

$$(y^2 \pm \nu yz + z^2) - \left(\frac{2-\nu}{2+\nu}\right)(y^2 \mp \nu yz + z^2) = \left(\frac{2\nu}{2+\nu}\right)(y \pm z)^2.$$

COROLLARY 13. *Suppose $p(x,y,z) = x^4 + F_4(y,z)$ is psd. The one of the following holds:*

1. *$F_4 = \ell^4$ for some linear form ℓ, and p is a sum of three squares in infinitely many ways.*
2. *$F_4 = \ell_1^2 \ell_2^2$ for non-proportional linear forms ℓ_1 and ℓ_2, and p is a sum of three squares in exactly one way.*
3. *$F_4 = \ell^2 k_2$, where k_2 is positive definite, and p is a sum of three squares in exactly two ways.*
4. *$F_4 = k_2^2$, where k_2 is positive definite, and p is a sum of three squares in exactly three ways.*
5. *$F_4 = k_2 q_2$, where k_2 and q_2 are positive definite and not proportional, and p is a sum of three squares in exactly eight ways.*

PROOF. Throughout, we shall use the classification of Theorem 6 as the first step in the proof.
1. We assume that $\ell(y,z) = y$. We must have that $-Q(y,z)$ and $y^4 - Q^2(y,z)$ are psd. The second condition implies that $Q(y,z) = \alpha y^4$ with $1 \ge \alpha^2$, and the first implies that $\alpha < 0$. In this case $\Delta = -\alpha(1-\alpha^2)y^6$ is always a square and, writing $\alpha = -\beta^2$, $0 \le \beta \le 1$ we have

$$x^4 + y^4 = (x^2 - \beta^2 y^2)^2 + 2\beta^2 x^2 y^2 + (1 - \beta^4) y^4.$$

The distinct values of β give orthogonally distinct different representations of p as a sum of three squares. This can't be too surprising, because p is obviously a sum of two squares. However, the next case gives another sum of two squares which has no additional representations as a sum of three squares.

2. In this case, $\ell_1(y,z) = y$ and $\ell_2(y,z) = z$. We must have that $-Q(y,z)$ and $y^2z^2 - Q^2(y,z)$ are psd. The second condition implies that $yz \mid Q$, hence $Q(y,z) = \alpha yz$. But the first condition then implies that $\alpha = 0$, so $Q = 0$ and we have

$$x^4 + y^2z^2 = (x^2)^2 + \sum_{j=2}^{3} f_j^2(x,y,z).$$

But this implies that $f_j(y,z) = \alpha_j yz$ and $1 = \alpha_2^2 + \alpha_3^2$; these are all orthogonally equivalent to $(yz)^2 + 0^2$. So the only representations of p as a sum of three squares are orthogonally equivalent to those as a sum of two squares. In fact, the psd Gram matrices for p have no parameters, and p has, up to orthogonal equivalence, a unique representation as a sum of squares.

3. In this case, we assume that $F_4(y,z) = y^2(y^2+z^2)$. The condition that $F_4 - Q^2$ is psd implies that $y \mid Q$, and the condition that $-Q$ is psd implies that $Q(y,z) = -\alpha y^2$, with $\alpha \ge 0$, so now $F_4(y,z) - Q^2(y,z) = y^2((1-\alpha^2)y^2 + z^2)$, hence $0 \le \alpha \le 1$. Finally, the condition that $\Delta = \alpha y^4((1-\alpha^2)y^2+z^2)$ be a square implies that $\alpha = 0$ or $\alpha = 1$. In the first case, we have

$$x^4 + y^2(y^2+z^2) = (x^2)^2 + \sum_{j=2}^{3} f_j^2(x,y,z).$$

There is by Theorem 4 exactly one way to write $y^2(y^2+z^2)$ as a sum of two squares, $(y^2)^2 + (yz)^2$. In the second case, we have

$$x^4 + y^2(y^2+z^2) = (x^2-y^2)^2 + \sum_{j=2}^{3} f_j^2(x,y,z) \implies 2x^2y^2 + y^2z^2 = \sum_{j=2}^{3} f_j^2(x,y,z).$$

By Theorem 5, there is also just one way to write $y^2(2x^2+z^2)$ as a sum of two squares, $2(xy)^2 + (yz)^2$, so altogether there are two ways to write p as a sum of three squares.

4. We assume that $k_2(y,z) = y^2 + z^2$. We now run through the four cases in Corollary 10. In case (a), we have $Q = 0$, and

$$x^4 + (y^2+z^2)^2 = (x^2)^2 + \sum_{j=2}^{3} f_j^2(x,y,z).$$

We know from Theorem 4 that there are two inequivalent choices for (f_2, f_3). These are easy to compute by hand and give

$$x^4 + (y^2+z^2)^2 = (x^2)^2 + (y^2+z^2)^2 + 0^2 = (x^2)^2 + (y^2-z^2)^2 + (2yz)^2.$$

In case (b), $Q(y,z) = \pm(y^2+z^2)$ and $-Q$ is psd, so $Q(y,z) = -(y^2+z^2)$ and

$$x^4 + (y^2+z^2)^2 = (x^2-(y^2+z^2))^2 + \sum_{j=2}^{3} f_j^2(x,y,z).$$

This implies that $2x^2(y^2+z^2) = \sum_{j=2}^{3} f_j^2(x,y)$, and, as before, Theorem 5 implies that there is a unique representation:

$$x^4 + (y^2+z^2)^2 = (x^2-(y^2+z^2))^2 + 2(xy)^2 + 2(xz)^2.$$

In case (c), we have that $Q(y,z) = -(ay+bz)^2$ and $(y^2+z^2)^2 - (ay+bz)^4$ is a square. We have seen in Lemma 11 that this is impossible. Finally, in case (d), $-Q$ is a psd factor of $F_4 - F_2^2 = (y^2+z^2)^2$, hence $Q(y,z) = -\alpha(y^2+z^2)$ for some $\alpha > 0$. This implies that $\Delta(y,z) = \alpha(1-\alpha^2)(y^2+z^2)^3$, which is only a square for $\alpha = 0,1$, which have been already discussed. Altogether, there are only three representations.

5. We write $F_4(y,z) = y^4 + \lambda y^2z^2 + z^4$, with $|\lambda| < 2$ and, as before, write $\lambda = 2-\nu^2$, with $0 < \nu < 2$. In case (a), $Q = 0$, and as in the last case, F_4 is a sum of two squares in two ways:

$$y^4 + \lambda y^2z^2 + z^4 = (y^2 + \tfrac{\lambda}{2}z^2)^2 + (1-\tfrac{\lambda^2}{4})z^4 = (y^2-z^2)^2 + (2+\lambda)(yz)^2.$$

This gives two ways to write $x^4 + F_4(y,z)$ as a sum of three squares.

Case (b) does not apply, since F_4 is not a square. In case (c), $Q = -\ell^2$, and $F_4 - \ell^4 = s_2^2$ is a square. By Lemma 11, there are two different choices of (ℓ^2, s^2) for which this is the case. For simplicity, let $\rho = \sqrt{1-\frac{\lambda^2}{4}}$. These give the representations

$$x^4 + y^4 + \lambda y^2z^2 + z^4 = (x^2 - \rho y^2)^2 + 2\rho x^2y^2 + (\tfrac{\lambda}{2}y^2 + z^2)^2,$$

and a similar one, with y and z permuted. Note that the factors of the two summands are $\sqrt{2\rho}xy \pm i(\frac{\lambda}{2}y^2 + z^2)$ which are irreducible over $\mathbf{C}$. Thus there is only one representation of p as a sum of three squares for each $Q = -\ell^2$, and so two in all.

Finally, in case (d), we have that $-Q$ is a psd factor of

$$F_4(y,z) = (y^2 + \nu yz + z^2)(y^2 - \nu yz + z^2)$$

Thus $Q = \kappa(y^2 \pm \nu yz + z^2)$ for some choice of sign. In this case

$$F_4(y,z) - Q^2(y,z) = \tfrac{1}{\kappa}Q(y,z)\big((y^2 - \mp\nu yz + z^2) - \kappa^2((y^2 \pm \nu yz + z^2)\big).$$

By Lemma 12, the last factor is a square if and only if $\kappa^2 = \frac{2-\nu}{2+\nu}$. In this case, we have

$$x^4+y^4+\lambda y^2z^2+z^4 = (x^2-\kappa(y^2\pm\nu yz+z^2))^2+(y^2\pm\nu yz+z^2)(2\kappa x^2+(1-\kappa^2)(y\mp z)^2)$$

Since the sum of these last two squares splits over $\mathbf{C}$, we get four different representations of p as a sum of three squares altogether, so there are four from case (d) and eight in all. □

Example. We illustrate the eight representations of $p(x,y,z) = x^4+y^4+z^4$ as a sum of three squares of real quadratic forms. In this case, $\lambda = 0$, $\rho = 1$, $\nu = \sqrt{2}$ and $\kappa = \sqrt{\frac{2-\sqrt{2}}{2+\sqrt{2}}} = \sqrt{2}-1$, so that $1-\kappa^2 = 2\kappa$. The two from case (a) are

$$p(x,y,z) = (x^2)^2 + (y^2)^2 + (z^2)^2 = (x^2)^2 + (y^2-z^2)^2 + 2(yz)^2.$$

That is, (12) and one of (13). The two cases from (c) become the other two from (13).

$$p(x,y,z) = (x^2-y^2)^2 + 2(xy)^2 + (z^2)^2 = (x^2-z^2)^2 + 2(xz)^2 + (y^2)^2.$$

Finally, from case (d), we get four representations from

$$(x^2 - (\sqrt{2}-1)(y^2 \pm \sqrt{2}yz + z^2))^2 + 2(\sqrt{2}-1)(y^2 \pm \sqrt{2}yz + z^2)(x^2 + (y \mp z)^2).$$

The two-square identity then gives (15).

References

[1] J. Bochnak, M. Coste, and M.-F. Roy, *Real Algebraic Geometry*, Springer-Verlag, Berlin, 1998.
[2] M.D. Choi and T.Y. Lam, *Extremal positive semidefinite forms*, Math. Ann. **231** (1977), 1-26.
[3] M. D. Choi, T.Y. Lam, and B. Reznick, *Real zeros of positive semidefinite forms I*, Math. Z. **171** (1980), 1-25.
[4] M.D. Choi, T.Y. Lam, and B. Reznick, *Sums of squares of real polynomials*, Symp. in Pure Math. **58** (1995), 103–126, Amer. Math. Soc., Providence, R.I.
[5] D. Hilbert, *Über die Darstellung definiter Formen als Summe von Formenquadraten*, Math. Ann. **32** (1888), 342-350.
[6] A. R. Rajwade, *Squares*, London Mathematical Society Lecture Notes **171**, Cambridge University Press, Cambridge, 1993.
[7] F. Rouillier, *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*, PhD. thesis, Université Rennes, France, 1997.
[8] R. G. Swan, *Hilbert's Theorem on positive ternary quartics*, these proceedings.

Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322
E-mail address: `vicki@mathcs.emory.edu`

Department of Mathematics, University of Illinois, Urbana, IL 61801
E-mail address: `reznick@math.uiuc.edu`