TWO REMARKS ON SUMS OF SQUARES WITH RATIONAL COEFFICIENTS

JOSE CAPCO

University of Innsbruck, Unit Geometry and Surveying
Technikerstrasse 13, 6020 Innsbruck, Austria
ORCID: 0000-0001-5938-5687   E-mail: jose.capco@uibk.ac.at

CLAUS SCHEIDERER

Fachbereich Mathematik und Statistik, Universität Konstanz
78457 Konstanz, Germany
ORCID: 0000-0002-5452-1114   E-mail: claus.scheiderer@uni-konstanz.de

Abstract. There exist homogeneous polynomials f with $\mathbb{Q}$-coefficients that are sums of squares over $\mathbb{R}$ but not over $\mathbb{Q}$. The only systematic construction of such polynomials that is known so far uses as its key ingredient totally imaginary number fields $K/\mathbb{Q}$ with specific Galois-theoretic properties. We first show that one may relax these properties considerably without losing the conclusion, and that this relaxation is sharp at least in a weak sense. In the second part we discuss the open question whether any f as above necessarily has a (non-trivial) real zero. In the minimal open cases $(3, 6)$ and $(4, 4)$, we prove that all examples without a real zero are contained in a thin subset of the boundary of the sum of squares cone.

1. Introduction. Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be a polynomial with rational coefficients. Given a field extension $E/\mathbb{Q}$ we say that f is a sum of squares over E, or briefly that f is *E-sos*, if there is a polynomial identity $f = \sum_{i=1}^r p_i^2$ with $p_1, \ldots, p_r \in E[x_1, \ldots, x_n]$. Suppose that f is $\mathbb{R}$-sos. Then does it follow that f is $\mathbb{Q}$-sos? This question is certainly

of theoretical interest, but is also relevant from a practical perspective. Indeed, it is one particular instance of the general problem of finding exact (rather than floating-point) positivity certificates.

In general, the answer is negative, as was shown in [13]. In fact, an explicit construction was presented there of $\mathbb{Q}$-polynomials f that are $\mathbb{R}$-sos but not $\mathbb{Q}$-sos. From this negative answer, a series of natural follow-up questions arises, see Section 5 in [13]. In this article we discuss two of them. Throughout we assume that our polynomials are forms, i.e. they are homogeneous.

Recall that the basic construction in [13] starts out with a totally imaginary number field $K/\mathbb{Q}$ of even degree $2d$ and a linear form $l \in K[x_1, \ldots, x_n]$ with sufficiently general coefficients. The norm form $f = N_{K/\mathbb{Q}}(l)$ is a degree $2d$ form over $\mathbb{Q}$ and is $\mathbb{R}$-sos. Let $K^{\mathrm{gal}}/\mathbb{Q}$ be the Galois hull of $K/\mathbb{Q}$, and let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q})$ act on the set $X = \mathrm{Hom}(K, \mathbb{C})$ of (complex) places of K (note $|X| = 2d$). According to [13], if G is sufficiently "big" as a subgroup of the symmetric group S_{2d}, then f cannot be $\mathbb{Q}$-sos. For example, it is enough that G is doubly transitive on X. In Section 2 we show that a condition much weaker than 2-transitivity suffices to make the construction work (condition $(**)$), and that this relaxation is sharp at least in a weak sense. Moreover we present empirical data showing that up to degree $2d = 16$, all transitive group actions satisfying this condition do actually arise from a number field $K/\mathbb{Q}$ as before.

All known examples of $\mathbb{R}$-sos forms $f \in \mathbb{Q}[x_1, \ldots, x_n]$ that are not $\mathbb{Q}$-sos have real zeros. In fact, the proofs for the impossibility of writing f as a sum of squares over $\mathbb{Q}$ make crucial use of the existence of these real zeros. Therefore it is natural to ask if there can be any examples of such forms without any (non-trivial) real zero. See also Question 5.1 in [13]. Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be a form with $\deg(f) = 2d$ that is $\mathbb{R}$-sos and has strictly positive values. In Section 3 we discuss the first open case, namely $(n, 2d) = (3, 6)$. We conjecture that f is $\mathbb{Q}$-sos in this case, and we prove this conjecture for all f outside of a Zariski-thin subset of the boundary of the sum of squares cone Σ_6. An analogous result holds in the other "Hilbert case" $(n, 2d) = (4, 4)$.

In Section 3 we use some simple facts on Gram spectrahedra of forms. For the reader's convenience we have included a brief introduction to Gram spectrahedra in Section 4, together with proofs or references for the facts that we use.

We remark that Question 5.3 from [13] has recently been given a negative answer by Laplagne [11]. This question was asking whether f is $\mathbb{Q}$-sos if it becomes K-sos in an odd degree extension $K/\mathbb{Q}$. Laplagne shows that the answer is negative. In fact, he constructs examples of degree 4 polynomials $f \in \mathbb{Q}[x_1, \ldots, x_4]$ that are sums of squares over $\mathbb{Q}(\sqrt[3]{2})$ but not over $\mathbb{Q}$.

2. Conditions on the Galois group

2.1. Let $K/\mathbb{Q}$ be a totally imaginary number field of degree $[K : \mathbb{Q}] = 2d \geq 4$, let $K^{\mathrm{gal}}/\mathbb{Q}$ be its Galois hull and $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q})$ the Galois group. The group G acts transitively on the set $X = \mathrm{Hom}(K, \mathbb{C})$ of cardinality $|X| = 2d$. (This action can be identified with the G-action on the roots of the minimal polynomial of a primitive element of $K/\mathbb{Q}$.) We fix once and for all an embedding $K \subseteq \mathbb{C}$ and denote complex conjugation (restricted to K^{gal}) by $\tau \in G$. Since K has no real place, τ acts on X without fixed point, i.e. as a product of d pairwise disjoint transpositions.

Let $l \in K[x_1, x_2, x_3]$ be a linear form, and let $f = N_{K/\mathbb{Q}}(l)$ be the $K/\mathbb{Q}$-norm of l. So $f \in \mathbb{Q}[x_1, x_2, x_3]$, and f is the product of the $2d$ Galois conjugates of l. The form f is a sum of two squares of forms over the field $\mathbb{R}$ of real numbers. The following was proved in [13, Section 2]:

2.2. THEOREM. *Suppose that the G-action on X is 2-transitive or, more generally, satisfies condition $(*)$ below. Then, for l a linear form with sufficiently general coefficients, the form $f = N_{K/\mathbb{Q}}(l)$ fails to be $\mathbb{Q}$-sos.*

"Sufficiently general coefficients" means that no three of the $2d$ Galois conjugates of l have a common nontrivial (complex) zero. For example, when α is a primitive element for $K/\mathbb{Q}$, the form $l = x_1 + \alpha x_2 + \alpha^2 x_3$ has sufficiently general coefficients in this sense. Condition $(*)$ is the following condition on the Galois action on X:

$(*)$ *For any x, $y \in X$ with $x \neq y$ there exists $z \in X$ and $\sigma \in G$ such that $x = \sigma z$ and $y = \sigma \tau z$.*

Condition $(*)$ requires, in other words, that every 2-element subset $\{x, y\} \subseteq X$ is G-conjugate to a subset of the form $\{z, \tau z\}$ with $z \in X$. This is a weaker condition than 2-transitivity, and is in fact strictly weaker (see [13, Remark 2.9] or Section 2.8 below).

2.3. We are going to show that Theorem 2.2 remains true under a condition that is still much more general than condition $(*)$. To this end let G be a finite group, and let X be a transitive and faithful G-set (i.e. only $1 \in G$ acts as the identity). Let $t \in G$ be a fixed-point-free involution, i.e. t acts on X without fixed point and satisfies $t^2 = 1$. This forces $|X|$ to be even. For $x \in X$ let

$$M_t(x) = \{y \in X : \exists\, z \in X, \ \exists\, g \in G \text{ such that } x = gz, \ y = gtz\}$$
$$= \{gtg^{-1}x : g \in G\},$$

be the "orbit" of x under the conjugacy class of t in G. It is easy to see that $M_t(hx) = hM_t(x)$ for any $h \in G$, $x \in X$, and that $x \notin M_t(x)$. Therefore the cardinality $|M_t(x)|$ is independent of $x \in M$ and depends only on the conjugacy class of t in G. We write $c(G, X, t) := |M_t(x)|$ and call this the *characteristic number* of the triple (G, X, t).

Property $(*)$ above says $M_t(x) = X \setminus \{x\}$ for $x \in X$, or in other words, $(*)$ says $c(G, X, t) = |X| - 1$.

2.4. DEFINITION. Let the finite group G act transitively and faithfully on the set X, and let $t \in G$ be an involution without fixed points in X. We say that the triple (G, X, t) *has property $(**)$*, if $c(G, X, t) > \frac{1}{2}|X|$.

Clearly, property $(*)$ implies property $(**)$.

We return to the setting in Section 2.1. So let again $K \subseteq \mathbb{C}$ be a totally imaginary field extension of $\mathbb{Q}$, of degree $[K : \mathbb{Q}] = 2d \geq 4$ and with Galois hull $K^{\mathrm{gal}}/\mathbb{Q}$. We consider the action of $G = \mathrm{Gal}(E/\mathbb{Q})$ on $X = \mathrm{Hom}(K, \mathbb{C})$. Let $\tau \in G$ be complex conjugation. Theorem 2.2 holds when condition $(*)$ gets replaced by the weaker condition $(**)$:

2.5. THEOREM. *Suppose that the triple (G, X, τ) satisfies condition $(**)$. Then, for l a linear form with sufficiently general coefficients, the form $f = N_{K/\mathbb{Q}}(l)$ fails to be $\mathbb{Q}$-sos.*

Proof. Let $l \in K[x_1, x_2, x_3]$ be a linear form, let $l_1, \ldots, l_{2d}$ be its G-conjugates, and assume that no three of them have a common nontrivial complex zero. For $i = 1, \ldots, 2d$ let $L_i \subseteq \mathbb{P}^2(\mathbb{C})$ be the projective zero set of l_i. For $i \neq j$ in $\{1, \ldots, 2d\}$ let $M_{ij} = L_i \cap L_j$, the intersection point of L_i and L_j. Let $Q := \{M_{ij} \colon 1 \leq i < j \leq 2d\}$, and let $Q_0 \subseteq Q$ be the subset of all real points in Q. By the general position assumption, Q_0 consists just of the d intersection points $L_i \cap \overline{L}_i$ $(1 \leq i \leq 2d)$.

As in [13], we can identify the 2-element subsets of X with the points in Q, by letting $\{i, j\} \subseteq X$ correspond to $M_{ij} \in Q$. This identifies the subsets $\{x, \tau x\}$ $(x \in X)$ with the points in Q_0. Condition $(**)$ therefore says that one (in fact, any) of the lines $L_1, \ldots, L_{2d}$ contains at least $d + 1$ points that are G-conjugate to a point in Q_0. Assume that f is $\mathbb{Q}$-sos, i.e. $f = \sum_\nu p_\nu^2$ with forms $p_\nu \in \mathbb{Q}[x_1, x_2, x_3]$. Since $f(\xi) = 0$ for every $\xi \in Q_0$, we have $p_\nu(\xi) = 0$ for every ν and every $\xi \in Q_0$. Therefore every p_ν vanishes in at least $d + 1$ different points of every line L_j. Since $\deg(p_\nu) = d$, this implies that the p_ν vanish identically on each line L_j, implying $p_\nu = 0$, contradiction. ∎

2.6. REMARK. In a weak sense at least, condition $(**)$ is sharp for Theorem 2.5. Indeed, $(**)$ requires $c(G, X, t) \geq d + 1$. If we allow $c(G, X, t) = d$, then Theorem 2.5 fails in general. An example showing this is provided by the dihedral group G of order 8, acting on the vertices X of a square by symmetries of the square (so $2d = 4$ here). If $t \in G$ is one of the two fixed-point-free reflections then $M_t(x)$ consists of the two vertices adjacent to the vertex $x \in X$, and so $c(G, X, t) = 2 = d$. But when $K/\mathbb{Q}$ is an extension with $[K : \mathbb{Q}] = 4$ and $\mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q}) \cong G$, the construction in Section 2.1 always produces forms that are $\mathbb{Q}$-sos. Indeed, this is a consequence of [13, Theorem 4.1].

2.7. To complete this discussion, we add some empirical observations. We consider finite transitive (faithful) group actions (G, X) up to isomorphism, i.e. G is a finite group that acts transitively and faithfully on the set X. The notion of isomorphism $(G_1, X_1) \to (G_2, X_2)$ is obvious. For small degrees, the isomorphism classes of such transitive group actions are well known, and corresponding data is both available on the web and implemented in computer algebra systems. For example, the transitive permutation groups of degree ≤ 30 are contained in a Magma database [3].

Given a finite extension $K \subseteq \mathbb{C}$ of $\mathbb{Q}$ with Galois closure $K^{\mathrm{gal}} \subseteq \mathbb{C}$, we shall say that K realizes the transitive group (G, X) if there is an isomorphism $(G, X) \xrightarrow{\sim} (\mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q}), \mathrm{Hom}(K, \mathbb{C}))$. Given moreover an involution $t \in G$, we say that K realizes the triple (G, X, t) if such an isomorphism can be found that sends t to (the restriction of) complex conjugation. Of course, the realization question for (G, X) is a strong version of the inverse Galois problem, that becomes even stronger when an involution $t \in G$ is fixed.

Since we are interested in the group actions of totally imaginary number fields, we only consider transitive groups (G, X) that contain a fixed-point-free (*fpf*) involution.

2.8. The following information was obtained with the help of the Magma computer algebra system [3]. For $2d = 4$ there are 5 transitive groups (G, X) (up to isomorphism). Only the 2-transitive groups S_4 and A_4 satisfy condition $(**)$.

For $2d = 6$ there are 16 transitive groups (G, X), 11 of which contain a fpf involution. Two of these 11 are 2-transitive. Two other groups contain a fpf involution which satisfies $(*)$, namely the transitive groups 6T8 and 6T11. (The first of them was already discussed in [13, 2.9]). No further group satisfies $(**)$.

For $2d = 8$ we have the first examples of transitive groups which satisfy $(**)$, but not $(*)$, with respect to some involution. Note that in general, a transitive group (G, X) contains several conjugacy classes of fpf involutions t, whose characteristic numbers $c(G, X, t)$ will usually be different.

For $2d = 10$ or 14, condition $(**)$ is not more general than $(*)$. But in degrees 12, 16, 18 and 20 there are many transitive groups that have at least one involution satisfying $(**)$, but no involution satisfying $(*)$. Combined with the remarks in Section 2.9, this shows that we gain quite a bit of new examples with Theorem 2.5. A precise statistics up to degree 20 is provided in the following table:

n	(1)	(2)	(3)	(4)
4	5	2	–	–
6	11	2	2	–
8	50	7	2	3
10	27	3	6	–
12	282	5	21	50
14	44	2	9	–
16	1954	13	35	120
18	678	2	83	132
20	1020	4	126	197

Here row n contains the numbers of (isomorphism classes of) transitive groups (G, X) with $|X| = n$ that

(1) contain a fpf involution,
(2) contain a fpf involution and are 2-transitive,
(3) satisfy $(*)$ for some fpf involution but are not 2-transitive,
(4) satisfy $(**)$ for some fpf involution, but do not satisfy $(*)$ for any fpf involution.

2.9. By consulting the Klüners–Malle data base for number fields ([9], see also [10]), one can verify that for every transitive group (G, X) of degree $|X| \leq 16$ and every fpf involution $t \in G$, the triple (G, X, t) is realized by some number field $K/\mathbb{Q}$. We are grateful to Jürgen Klüners for confirming to us this last assertion. A list of Galois realizations of all triples (G, X, t) with $|X| \leq 16$ that satisfy $(**)$, extracted from [9], is available under [4].

3. Strictly positive forms in Hilbert's sos cones

3.1. We consider Open Problem 5.1 from [13]. Let $f \in \mathbb{Q}[x] = \mathbb{Q}[x_1, \ldots, x_n]$ be a form of degree $\deg(f) = 2d$ which is $\mathbb{R}$-sos, and assume that f is strictly positive (i.e. $f(a) > 0$ for $0 \neq a \in \mathbb{R}^n$). Then, does it follow that f is $\mathbb{Q}$-sos?

Although we expect a negative answer in general, no argument or example is known so far to decide this question in general. Here we are looking at the first open cases. When $n \leq 2$ or $2d = 2$, f is clearly $\mathbb{Q}$-sos, and the same is true for $(n, 2d) = (3, 4)$ according to [13, Theorem 4.1]. We therefore consider the cases $(n, 2d) = (3, 6)$ or $(4, 4)$. They may be called the Hilbert cases, alluding to Hilbert's celebrated 1888 theorem [7], by which $(3, 6)$ and $(4, 4)$ are the minimal cases for which there exist nonnegative forms (over $\mathbb{R}$) that are not sums of squares.

In all that follows, the two cases $(3, 6)$ and $(4, 4)$ are completely parallel. For simplicity we will focus on the $(3, 6)$ case, and will point out at the end how to adapt the results to the $(4, 4)$ case. Our main result in the $(3, 6)$ case is Theorem 3.11. Roughly it says that if there exists strictly positive f over $\mathbb{Q}$ which is $\mathbb{R}$-sos but not $\mathbb{Q}$-sos, then f lies in a thin subset of the boundary of the sos cone.

3.2. Let $x = (x_1, x_2, x_3)$, and consider the polynomial ring $A = \mathbb{R}[x] = \mathbb{R}[x_1, x_2, x_3]$ with the natural grading $A = \bigoplus_{d \geq 0} A_d$. We say that a form $f \in A$ is *strictly positive*, denoted by $f > 0$, if $f(a) > 0$ for any $0 \neq a \in \mathbb{R}^3$. Recall that A_d is a finite-dimensional real vector space and thus carries a unique topology. For even $d \geq 0$ let $\Sigma_d \subseteq A_d$ be the set of all sums of squares, a closed convex cone of full dimension (i.e. with non-empty interior relative to A_d).

Let $f \in \mathbb{Q}[x] = \mathbb{Q}[x_1, x_2, x_3]$ be a strictly positive form of degree 6 which is $\mathbb{R}$-sos, i.e. $f \in \mathbb{Q}[x]_6 \cap \Sigma_6$. If f lies in the interior of Σ_6 then f is a sum of squares over $\mathbb{Q}$ ([8, Theorem 1.2] or [13, Lemma 4.6]). So we assume that f lies on the boundary $\partial \Sigma_6$. The Zariski closure $\partial^a \Sigma_6$ of $\partial \Sigma_6$ is called the *algebraic boundary* of Σ_6, and is known to be a union of two irreducible hypersurfaces inside the space A_6. Namely

$$\partial^a \Sigma_6 = \Delta \cup V$$

where Δ is the discriminant hypersurface, consisting of all forms with at least one (complex) singularity, and V is the Zariski closure of the sets of all sums of three squares of forms. The degree of Δ resp. V is 75 resp. 83200. See [2] for proofs of these facts (we will not make use of the precise degrees).

3.3. For basic notions from convexity we refer to standard texts like [15] or [12]. Let $A_6^\vee = \operatorname{Hom}(A_6, \mathbb{R})$ be the dual space of the linear space A_6, and let $\Sigma_6^* = \{\alpha \in A_6^\vee \colon \alpha(\Sigma_6) \geq 0\}$, the dual cone of Σ_6. Given $f \in \Sigma_6$, the *normal cone* of Σ_6 at f is

$$N_f = N_f(\Sigma_6) = \{\alpha \in \Sigma_6^* \colon \alpha(f) = 0\},$$

a closed convex cone contained in Σ_6^*. For $f \in \partial \Sigma_6$ we have $N_f \neq \{0\}$. Moreover, then, N_f is the (closed) convex cone generated by the extreme rays $\mathbb{R}_+ \alpha$ of Σ_6^* satisfying $\alpha(f) = 0$, according to the Krein–Milman theorem for closed pointed convex cones.

3.4. Let $f \in \partial\Sigma_6$ be strictly positive. Let us recall how Blekherman [1] proves that f is a sum of three squares of forms. Let $\alpha \in N_f$ span an extreme ray. Since f is strictly positive, α cannot be evaluation in a point $u \in \mathbb{R}^3$. The symmetric bilinear form

$$b_\alpha \colon A_3 \times A_3 \to \mathbb{R}, \quad (p, q) \mapsto \alpha(pq),$$

is positive semidefinite. Let $U_\alpha \subseteq A_3$ be its kernel, so

$$U_\alpha = \{p \in A_3 \colon pA_3 \subseteq \ker(\alpha)\} = \{p \in A_3 \colon \alpha(p^2) = 0\}.$$

By [1], Corollary 2.3 and Lemma 2.4, the forms in U_α have no common (real or complex) projective zero in $\mathbb{P}^2$, so the projective zero set $V(U_\alpha)$ is empty.

By assumption, f has at least one sums of squares representation $f = \sum_{i=1}^r p_i^2$ (with $p_i \in A_3$). For any such identity we have $\alpha(p_i^2) = 0$ for all i, so the p_i lie in U_α. According to [1, Theorem 2.7], the linear space U_α has dimension 3. Therefore f can be written as a sum of 3 squares. In particular, any strictly positive $f \in \partial\Sigma_6$ lies in the hypersurface V.

Moreover, Blekherman proves that f is not a sum of two squares [1, Corollary 1.3]. Hence for every sum of squares representation $f = \sum_{i=1}^r p_i^2$ (with $p_i \in A_3$), the linear span of the forms $p_1, \ldots, p_r$ is equal to U_α. By Lemma 4.3, this implies that f has essentially only one such representation:

3.5. COROLLARY. *Let $f \in \partial\Sigma_6$ be strictly positive. Then f is a sum of three squares, and up to orthogonal equivalence, there is only one sum of squares representation of f.*

In particular, the Gram spectrahedron of f is reduced to a single point.

3.6. We keep assuming that $f \in \partial\Sigma_6$ is strictly positive, and that $\alpha \in N_f$ spans an extreme ray. Let U_α be the kernel of b_α, as in Section 3.4, and let $I \subseteq A$ be the (homogeneous) ideal generated by U_α. Since $V(I) = \varnothing$ and $\dim(U_\alpha) = 3$, the ideal I is a complete intersection. Therefore, according to [6, Theorem CB8], the graded ring A/I is a 0-dimensional Gorenstein ring with socle degree 6, see also [1, Theorem 2.5]. In particular, $\ker(\alpha) \subseteq A_6$ is the degree 6 part of I, i.e. $\ker(\alpha) = I_6 = U_\alpha A_3$.

3.7. COROLLARY. *For every strictly positive form f in $\partial\Sigma_6$, the normal cone $N_f(\Sigma_6)$ has dimension one, i.e. it is a single ray.*

Proof. Let $\mathbb{R}_+\alpha$, $\mathbb{R}_+\beta$ be two extreme rays contained in N_f. It suffices to show that both are equal. By the discussion in Section 3.4 we have $U_\alpha = U_\beta$. But this implies $\ker(\alpha) = \ker(\beta)$, so α and β are positive scalar multiples of each other. ∎

3.8. COROLLARY. *Let $f \in \partial\Sigma_6$ be strictly positive, and assume that f is a nonsingular point of the hypersurface V. Let $\alpha \in A_6^\vee$ span the normal cone $N_f(\Sigma_6)$. Then the kernel of α coincides with the tangent space to V at f.*

Proof. Let $f = p_1^2 + p_2^2 + p_3^2$ be the unique sos representation of f. Then $U_\alpha = \mathrm{span}(p_1, p_2, p_3)$ and $\ker(\alpha) = U_\alpha A_3$ (Section 3.4, Corollary 3.5). Consider the morphism of algebraic varieties (affine spaces) $\phi \colon A_3 \times A_3 \times A_3 \to V \subseteq A_6$, $(q_1, q_2, q_3) \mapsto q_1^2 + q_2^2 + q_3^2$, and its tangent map at the triple (p_1, p_2, p_3). The image of this tangent map is $p_1 A_3 + p_2 A_3 + p_3 A_3 = U_\alpha A_3 \subseteq A_6$, and this subspace is contained in $T_f(V)$. We conclude $\ker(\alpha) \subseteq T_f(V)$, and equality must hold since both are codimension one subspaces of A_6. ∎

The following result summarizes most of what we discussed so far:

3.9. COROLLARY. *Let $f \in \partial\Sigma_6$ be strictly positive. Then the following hold*:

(a) *There are $p_1, p_2, p_3 \in A_3$, linearly independent, with $f = p_1^2 + p_2^2 + p_3^2$, and up to orthogonal equivalence, this is the only sum of squares representation of f.*

Let $U = \mathrm{span}(p_1, p_2, p_3) \subseteq A_3$, let $I \subseteq A$ be the ideal generated by U.

(b) *The normal cone $N_f(\Sigma_6)$ is a ray*: $N_f(\Sigma_6) = \mathbb{R}_+ \alpha$ *for some α.*
(c) *A/I is a Gorenstein graded algebra with socle degree 6.*
(d) *$I_6 = \ker(\alpha) = U A_3$.*

If in addition, f is a nonsingular point of the hypersurface V, then

(e) *$I_6 = \ker(\alpha)$ is the tangent space of V at f.*

Much of Corollary 3.9 was already known from [1]. New are (b), (e) and the uniqueness part of (a).

3.10.   The hypersurface $V \subseteq A_6$ is defined by a homogeneous polynomial F (of degree 83200) in the $\binom{8}{2} = 28$ coefficients of a ternary sextic. Since (the complexification of) V is the Zariski closure of all sums of three squares of cubic forms, this hypersurface is defined over $\mathbb{Q}$. So the polynomial F can be taken to have coefficients in $\mathbb{Q}$.

Let $f \in \partial\Sigma_6$ be strictly positive, so $f \in V$, and assume that f has $\mathbb{Q}$-coefficients. By Corollary 3.5, f has a unique sos representation over $\mathbb{R}$. We are going to show that this representation is defined over $\mathbb{Q}$, provided that f is a smooth point of the hypersurface V.

Indeed, since f has $\mathbb{Q}$-coefficients, the tangent space $T_f(V) \subseteq A_6$ of V at f is the kernel of a linear form with $\mathbb{Q}$-coefficients. By Corollary 3.9(e), we conclude that the normal cone $N_f(\Sigma_6)$ is generated by a linear form α with $\mathbb{Q}$-coefficients. Hence the 3-dimensional subspace $U_\alpha = \{p \in A_3 \colon A_3 p \subseteq \ker(\alpha)\}$ of A_3 has a basis consisting of $\mathbb{Q}$-polynomials. According to Lemma 4.4, this implies that the unique matrix (or tensor) in $\mathrm{Gram}(f)$ has $\mathbb{Q}$-coefficients. Thus, f is a sum of squares over $\mathbb{Q}$. Altogether this proves:

3.11. THEOREM. *Let $f \in \Sigma_6$ be a strictly positive form with coefficients in $\mathbb{Q}$. If f fails to be a sum of squares over $\mathbb{Q}$, then f lies in the boundary of Σ_6, and f is a singular point of the hypersurface V.*

In view of this theorem, it would be very interesting to see a characterization of the forms in V that are singular as points of V. Unfortunately we do not know how to approach this question. A direct computation of the singularities of V seems hopeless due to the complexity of the equation of V (a homogeneous polynomial in 28 variables of degree 83200).

3.12. REMARKS.
    1. Beware that a strictly positive form $f \in \Sigma_6$ which is a sum of three squares will not in general lie on the boundary of Σ_6. For example, the symmetric form $f = x_1^6 + x_2^6 + x_3^6$ is strictly positive, and it is easily seen that $f \in \mathrm{int}(\Sigma_6)$.

2. There is another aspect that makes the form $f = x_1^6 + x_2^6 + x_3^6$ interesting. Indeed, f can be written as a sum of 3 squares in more than one way, for example

$$f = (x_1^3 - 2x_1x_2^2)^2 + (2x_1^2x_2 - x_2^3)^2 + x_3^6.$$

By Corollary 3.5, this directly implies that f lies in the interior of Σ_6. Using the arguments from the proof of Corollary 3.8, we can also conclude that f is a singular point of V.

3. According to Blekherman [1], examples of strictly positive forms in $\partial\Sigma_6$ can be constructed as follows. Let $p_1, p_2 \in A_3$ be two cubics which intersect transversely in nine projective $\mathbb{R}$-points. For example, we may take $p_1 = x_1(x_1^2 - x_3^2)$ and $p_2 = x_2(x_2^2 - x_3^2)$, intersecting in nine points with affine representatives

$$\xi_1 = (1, 1, 1), \quad \xi_2 = (-1, 1, 1), \quad \xi_3 = (1, -1, 1), \quad \xi_4 = (1, 1, -1),$$
$$\xi_5 = (0, 1, 1), \quad \xi_6 = (0, 1, -1), \quad \xi_7 = (1, 0, 1), \quad \xi_8 = (1, 0, -1), \quad \xi_9 = (0, 0, 1).$$

The Cayley–Bacharach relation is the unique (up to scaling) linear relation between the nine values $p(\xi_i)$ $(1 \leq i \leq 9)$ of a general cubic p. In our example it is $\sum_{i=1}^9 u_i p(\xi_i) = 0$ where

$$(u_1, \ldots, u_9) = (1, 1, 1, 1, -2, -2, -2, -2, 4).$$

Following [1, Theorem 6.1] we consider 9-tuples $a = (a_1, \ldots, a_9)$ of nonzero real numbers with $a_i < 0$ for precisely one index i, that satisfy the relation $\sum_{i=1}^9 \frac{u_i^2}{a_i} = 0$. For any such tuple a the linear form

$$\alpha\colon A_6 \to \mathbb{R}, \quad \alpha(f) = \sum_{i=1}^9 a_i f(\xi_i),$$

is an extreme form in Σ_6^* and is not evaluation in a point.

In our example, $a = (1, 1, 1, 1, 4, 4, 4, 4, -2)$ is an example of such a tuple, giving rise to $\alpha \in \Sigma_6^*$ as above. The kernel U_α of the psd bilinear form b_α has $\dim(U_\alpha) = 3$ and is spanned by p_1, p_2 and $p_3 = (3x_1^2 + 3x_2^2 - 4x_3^2)x_3$. For any three linearly independent forms q_1, q_2, q_3 in $U_\alpha = \mathrm{span}(p_1, p_2, p_3)$, the sextic $f = q_1^2 + q_2^2 + q_3^2$ is strictly positive and lies in $\partial\Sigma_6$. For example,

$$f = x_1^6 + x_2^6 + 7(x_1^4 + x_2^4)x_3^2 + 18x_1^2x_2^2x_3^2 - 23(x_1^2 + x_2^2)x_3^4 + 16x_3^6$$

is such a sextic, obtained by taking $q_i = p_i$ $(i = 1, 2, 3)$. According to Corollary 3.5, $f = p_1^2 + p_2^2 + p_3^2$ is, up to orthogonal equivalence, the only sum of squares representation of f over $\mathbb{R}$.

Instead of 9 real points of intersection, the two conics p_1 and p_2 may also intersect in seven real and one complex conjugate pair of points. Then the a_i have to satisfy a slightly different condition, see [1, Theorem 7.1].

3.13. The results and remarks in this section all carry over to the $(4, 4)$ case, i.e. forms $f(x_1, x_2, x_3, x_4)$ of degree 4, as follows. Put $A = \mathbb{R}[x_1, x_2, x_3, x_4]$, let now Σ_4 denote the sos cone in A_4. The Zariski closure of $\partial\Sigma_4$ is a union $\Delta \cup V$ of two irreducible hypersurfaces, with Δ the discriminant (of degree 108), and V (of degree 38475) the Zariski closure of the sums of 4 squares of quadratic forms [2]. For $f \in \partial\Sigma_4$ a strictly positive form, the normal cone $N_f(\Sigma_4)$ is a ray, and f has a unique sos representation, which is of length 4. Defining the ideal $I \subseteq A$ similarly to Corollary 3.9, A/I is Gorenstein of socle degree 4.

The argument in Section 3.10 carries over (using four instead of three squares), and so the analogue of Theorem 3.11 holds for $\mathbb{Q}$-forms in Σ_4. The proofs resp. references are the same as in the $(3, 6)$ case.

4. Background on Gram spectrahedra.

We give a brief introduction to Gram spectrahedra of forms here, including proofs or references for a few basic facts that we are using in Section 3. See [14] for a more detailed account of Gram spectrahedra in general.

4.1. Let $n \in \mathbb{N}$ and $A = \mathbb{R}[x_1, \ldots, x_n] = \mathbb{R}[x]$, considered with the usual grading $A = \bigoplus_{d \geq 0} A_d$. Let $d \geq 0$ and $f \in A_{2d}$, let $X = (x_1^d, x_1^{d-1}x_2, \ldots, x_n^d)$ be the list of monomials of degree d in some fixed order, let $N = \binom{n-1+d}{d}$ be the number of these monomials. The *Gram spectrahedron* of f is defined to be

$$\mathrm{Gram}(f) = \{G \in \mathbb{S}^N : G \succeq 0, \ X^t G X = f\},$$

where $\mathbb{S}^N$ is the space of real symmetric $N \times N$ matrices and $G \succeq 0$ means that G is positive semidefinite (has non-negative eigenvalues). So $\mathrm{Gram}(f)$ is an affine-linear section of the cone $\mathbb{S}^N_+$ of psd symmetric matrices, and one easily checks that $\mathrm{Gram}(f)$ is compact.

If $f = p_1^2 + \ldots + p_r^2$ with $p_i \in A_d$, and if $u_i \in \mathbb{R}^N$ is the coefficients (column) vector of p_i, then the matrix $G = \sum_{i=1}^r u_i u_i^t$ lies in $\mathrm{Gram}(f)$. Conversely, every point of $\mathrm{Gram}(f)$ arises in this way. More precisely, two sum of squares representations $f = \sum_{i=1}^r p_i^2 = \sum_{i=1}^r q_i^2$ (which we can assume to have the same length by possibly adding zero summands to one of them) give the same element of $\mathrm{Gram}(f)$ if and only if they are *orthogonally equivalent*, which means that there is an orthogonal $r \times r$ matrix (a_{ij}) such that $q_i = \sum_{j=1}^r a_{ij} p_j$ $(i = 1, \ldots, r)$. See [5] for this fact, where Gram spectrahedra were first introduced. In other words, the points of $\mathrm{Gram}(f)$ are in natural bijection with the orthogonal equivalence classes of sum of squares representations of f.

For our purposes it is more convenient to represent elements of $\mathrm{Gram}(f)$ as symmetric tensors $\sum_{i=1}^r p_i \otimes q_i = \sum_{i=1}^r q_i \otimes p_i$ with $p_i, q_i \in A_d$, i.e. as elements of $\mathsf{S}_2 A_d$, the subspace of $A_d \otimes A_d$ of symmetric tensors. By using the multiplication (linear) map $\mu \colon \mathsf{S}_2 A_d \to A_{2d}$, $\mathrm{Gram}(f)$ consists of all $\theta \in \mathsf{S}_2 A_d$ with $\mu(\theta) = f$ and $\theta \succeq 0$. Here $\theta \succeq 0$ means that θ can be written $\theta = \sum_{i=1}^r p_i \otimes p_i$ with $p_i \in A_d$. See [14] for this point of view.

4.2. Let $\theta \in \mathrm{Gram}(f)$, say $\theta = \sum_{i=1}^r p_i \otimes p_i$. With θ we associate the linear subspace $U_\theta := \mathrm{span}(p_1, \ldots, p_r)$ of A_d. The supporting face F of f in $\mathrm{Gram}(f)$ (i.e. the unique face that contains f in its relative interior) consists of all $\eta \in \mathrm{Gram}(f)$ with $U_\eta \subseteq U_\theta$. It therefore corresponds to the sos representations of f that use only polynomials from U_θ. For describing the dimension of F we can assume that $p_1, \ldots, p_r$ are linearly independent. Then $\dim(F)$ is the number of linear relations between the forms $p_i p_j$ $(1 \leq i \leq j \leq r)$, i.e.

$$\dim(F) + \dim(U_\theta U_\theta) = \binom{r+1}{2}$$

where $U_\theta U_\theta := \mathrm{span}(p_i p_j : 1 \leq i \leq j \leq r)$ [14, Proposition 3.6]. In particular, θ is an extreme point of $\mathrm{Gram}(f)$ if and only if the $\binom{r+1}{2}$ forms $p_i p_j$ are linearly independent. In this case we say that $p_1, \ldots, p_r$ are *quadratically independent*.

4.3. LEMMA. *Assume that $f \in A_{2d}$ has two non-equivalent sos representations $f = \sum_{i=1}^{r} p_i^2 = \sum_{i=1}^{r} q_i^2$ with $\text{span}(p_1, \ldots, p_r) = \text{span}(q_1, \ldots, q_r) =: U$. Then f has another sos representation $f = \sum_{j=1}^{s} u_j^2$ for which $\text{span}(u_1, \ldots, u_s)$ is a proper subspace of U.*

Proof. The two given representations represent two different points in the Gram spectrahedron $\text{Gram}(f)$, that both lie in the relative interior of the same face F of $\text{Gram}(f)$. Since $\text{Gram}(f)$ is compact, F has some extreme point θ. If $f = \sum_{j=1}^{s} u_j^2$ is an sos representation that corresponds to θ, then $\text{span}(u_1, \ldots, u_s)$ is a proper subspace of U. ∎

The following lemma is used in the proof of our main result in Section 3:

4.4. LEMMA. *Let $f \in \Sigma_{2d}$ be a form with $\mathbb{Q}$-coefficients, and let θ be an extreme point of $\text{Gram}(f)$. If the space U_θ is defined over $\mathbb{Q}$, then the sos representation of f corresponding to θ is (can be) defined over $\mathbb{Q}$.*

That U_θ is defined over $\mathbb{Q}$ means that U_θ has a linear $\mathbb{R}$-basis consisting of polynomials with $\mathbb{Q}$-coefficients.

Proof. Let $p_1, \ldots, p_r$ be a basis of U_θ consisting of $\mathbb{Q}$-polynomials. Since θ is an extreme point of $\text{Gram}(f)$, the forms p_i are quadratically independent, see Section 4.2. Hence there is a unique $\mathbb{R}$-linear combination $f = \sum_{i,j=1}^{r} a_{ij} p_i p_j$ with $a_{ij} = a_{ji} \in \mathbb{R}$. The matrix (a_{ij}) is positive definite, and $a_{ij} \in \mathbb{Q}$ by uniqueness of the linear combination. So f is $\mathbb{Q}$-sos. ∎

References

[1] G. Blekherman, *Nonnegative polynomials and sums of squares*, J. Amer. Math. Soc. 25 (2012), 617–635.

[2] G. Blekherman, J. Hauenstein, J. C. Ottem, K. Ranestad, B. Sturmfels, *Algebraic boundaries of Hilbert's SOS cones*, Compos. Math. 148 (2012), 1717–1735.

[3] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), *Handbook of Magma functions*, Edition 2.24 (2018)

[4] J. Capco, C. Scheiderer, *Galois realizable permutation groups satisfying condition* (∗∗), Data set, Zenodo (2019), http://doi.org/10.5281/zenodo.2875785.

[5] M. D. Choi, T. Y. Lam, B. Reznick, *Sums of squares of real polynomials*, in: *K*-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras, Proc. Sympos. Pure Math. 58.2, Amer. Math. Soc., Providence, RI, 1995, 103–126.

[6] D. Eisenbud, M. Green, J. Harris, *Cayley–Bacharach theorems and conjectures*, Bull. Amer. Math. Soc. (N.S.) 33 (1996), 295–324.

[7] D. Hilbert, *Über die Darstellung definiter Formen als Summe von Formenquadraten*, Math. Ann. 32 (1888), 342–350.

[8] Ch. J. Hillar, *Sums of squares over totally real fields are rational sums of squares*, Proc. Amer. Math. Soc. 137 (2009), 921–930.

[9] J. Klüners, G. Malle, *Database of Number Fields*, online: galoisdb.math.upb.de, accessed 06.2018.

[10] J. Klüners, G. Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. 4 (2001), 182–196.

[11] S. Laplagne, *Facial reduction for exact polynomial sum of squares decompositions*, Math. Comp. 89 (2020), 859–877.

[12] R. T. Rockafellar, *Convex Analysis*, Princeton Math. Ser. 28, Princeton Univ. Press, Princeton, NJ, 1970.

[13] C. Scheiderer, *Sums of squares of polynomials with rational coefficients*, J. Eur. Math. Soc. (JEMS) 18 (2016), 1495–1513.

[14] C. Scheiderer, *Extreme points of Gram spectrahedra of binary forms*, arxiv.org/1802.05513.

[15] R. Webster, *Convexity*, Oxford Sci. Publ., Oxford Univ. Press, New York, 1994.