

SUM OF SQUARES LENGTH OF REAL FORMS

CLAUS SCHEIDERER

ABSTRACT. For $n, d \geq 1$ let $p(n, 2d)$ denote the smallest number p such that every sum of squares of forms of degree d in $\mathbb{R}[x_1, \dots, x_n]$ is a sum of p squares. We establish lower bounds for these numbers that are considerably stronger than the bounds known so far. Combined with known upper bounds they give $p(3, 2d) \in \{d + 1, d + 2\}$ in the ternary case. Assuming a conjecture of Iarrobino-Kanev on dimensions of tangent spaces to catalecticant varieties, we show that $p(n, 2d) \sim \text{const} \cdot d^{(n-1)/2}$ for $d \rightarrow \infty$ and all $n \geq 3$. For ternary sextics and quaternary quartics we determine the exact value of the invariant, showing $p(3, 6) = 4$ and $p(4, 4) = 5$.

INTRODUCTION

Given a polynomial $f(x_1, \dots, x_n)$ with real coefficients that has nonnegative values, Artin proved that f can be written as a sum of squares of rational functions over \mathbb{R} . By a famous theorem of Pfister [13], 2^n squares are always sufficient to represent f . For $n \leq 2$ this bound is known to be best possible, whereas for $n \geq 3$ it is only known that the best general bound lies between $n + 2$ and 2^n (see [14], for instance).

In general it is not possible to represent f as a sum of squares of polynomials, as Hilbert [9] proved in 1888. However if we restrict attention to sums of squares of polynomials, it is natural to ask for an upper bound on the number of squares needed. Switching to homogeneous polynomials (forms), we therefore fix $n, d \geq 1$ and ask for the smallest number $p = p(n, 2d)$ such that every form of degree $2d$ in $\mathbb{R}[x_1, \dots, x_n]$ that is a sum of squares of forms is a sum of p such squares. For $n \leq 2$ or $d = 1$ this is an elementary question, but otherwise the only case where $p(n, 2d)$ is known exactly is $(n, 2d) = (3, 4)$, where $p(3, 4) = 3$ according to Hilbert [9].

Still quite a bit is known for other combinations $(n, 2d)$. Choi, Lam and Reznick [5] established both upper and lower bounds for $p(n, 2d)$. Fixing the number n of variables, they proved in particular that $p(n, 2d) = O(d^{(n-1)/2})$ for $d \rightarrow \infty$. While the upper bounds from [5] are still largely the best ones known when $n \geq 4$, there exists a substantial improvement for $n = 3$, due to Leep [11]. Using Cassels-Pfister theory over a univariate polynomial ring, he improved the upper bound for $p(3, 2d)$ from $2d + 1$ to $d + 2$. On the other hand, there is a huge gap between known upper and lower bounds. Fixing n and letting d grow, the asymptotically best lower bounds known for $p(n, 2d)$ are only logarithmic in d [4]. See Section 1 below for precise details.

The first main result of this paper establishes new lower bounds that are much closer to the existing upper bounds. In fact they have the same growth rate for $d \rightarrow \infty$, showing $p(n, 2d) \sim d^{(n-1)/2}$ for $d \rightarrow \infty$. For ternary forms, they combine with Leep's theorem to show that $p(3, 2d)$ is either $d + 1$ or $d + 2$. The idea is to consider forms f that are sums of squares and vanish in a generic finite set $Z \subseteq \mathbb{P}^{n-1}(\mathbb{R})$ of appropriate size. For such f we show that the sum of squares representation of f is essentially unique. The explicit form of the resulting bound depends on the assumption that the Hilbert series of the squared vanishing ideal

$I(Z)^2$ is the expected one. For $n = 3$ this has been proved, but for $n \geq 4$ it is merely a conjecture due to Iarrobino-Kanev. Although the conjecture has been verified for small values of n and d , our bounds for $n \geq 4$ depend therefore in general on this conjecture.

The second main result computes the invariants $p(3, 6)$ and $p(4, 4)$ exactly, showing $p(3, 6) = 4$ and $p(4, 4) = 5$. Note that $(3, 6)$ and $(4, 4)$ are precisely the two minimal cases where the sums of squares cone is strictly smaller than the cone of nonnegative forms.

The paper is organized as follows. Section 1 recalls the upper and lower bounds for $p(n, 2d)$ that can be found in the literature. Section 2 studies the collection of typical sums of squares lengths of forms in $\Sigma_{n, 2d}$, i.e., lengths that occur for an open nonempty set of forms. We show that every integer between the typical complex length (essentially known) and the maximum length $p(n, 2d)$ is a typical length in this sense. Section 3 establishes the new lower bound for $p(n, 2d)$ (depending on the Iarrobino-Kanev conjecture for $n \geq 4$) and discusses the asymptotics of $p(n, 2d)$. In Section 4 we show that in the cases $(3, 6)$ and $(4, 4)$ the existing lower bound for $p(n, 2d)$ is sharp.

We remark that the results of this paper remain true over any real closed field, instead of \mathbb{R} .

1. REVIEW OF KNOWN UPPER AND LOWER BOUNDS

1.1. We start with setting up basic notation. Let $n \geq 1$, $e \geq 0$, and write $\mathbf{x} = (x_1, \dots, x_n)$. By $\mathbb{R}[\mathbf{x}]_e$ we denote the space of degree e forms (homogeneous polynomials) in $\mathbb{R}[\mathbf{x}]$. We often abbreviate

$$N_{n,e} := \dim \mathbb{R}[\mathbf{x}]_e = \binom{n+e-1}{n-1}.$$

If $e = 2d$ is even then $\Sigma_{n, 2d}$ denotes the subset of $\mathbb{R}[\mathbf{x}]_{2d}$ of all forms that are sums of squares of forms of degree d . It is well known that $\Sigma_{n, 2d}$ is a closed convex cone in $\mathbb{R}[\mathbf{x}]_{2d}$ with nonempty interior. Given $f \in \Sigma_{n, 2d}$, we denote by

$$\ell(f) = \min\{r \geq 0: \exists p_1, \dots, p_r \in \mathbb{R}[\mathbf{x}]_d \text{ with } f = p_1^2 + \dots + p_r^2\}$$

the *sum of squares length* (or *sos length*) of f . We call

$$p(n, 2d) := \sup\{\ell(f): f \in \Sigma_{n, 2d}\}$$

the *Pythagoras number* of n -ary forms of degree $2d$.

1.2. It is elementary to see $p(1, 2d) = 1$, $p(2, 2d) = 2$ ($d \geq 1$) and $p(n, 2) = n$ ($n \geq 1$). Clearly, $n \leq m$ and $d \leq e$ imply $p(n, 2d) \leq p(m, 2e)$. Hilbert [9] proved $p(3, 4) = 3$. So far, these are the only cases where the precise value of $p(n, 2d)$ is known.

1.3. For $n \geq 2$, Choi, Dai, Lam and Reznick [4] proved in 1982 that the ring $\mathbb{R}[x_1, \dots, x_n]$ has Pythagoras number ∞ . This amounts to $p(n, 2d) \rightarrow \infty$ for $n \geq 3$ and $d \rightarrow \infty$. From the proof of [4] Theorem 4.10 one can extract explicit lower bounds for $p(n, 2d)$ when $n \geq 3$. In particular, it is shown there that $p(n, 4d+2) > p(n, 2d)$, resulting in lower bounds for $p(n, 2d)$ that are logarithmic in d .

A systematic study of the invariants $p(n, 2d)$ was initiated by Choi, Lam and Reznick [5] in 1995. Adopting notation from [5], the following is essentially the main result:

Theorem 1.4. *Let $n, d \geq 1$. The Pythagoras number $p := p(n, 2d)$ satisfies the inequalities*

$$(1) \quad \binom{p+1}{2} \leq N_{n,2d} \leq pN_{n,d} - \binom{p}{2}.$$

These translate into

$$(2) \quad \lambda(n, 2d) \leq p(n, 2d) \leq \Lambda(n, 2d)$$

where (writing $a = N_{n,2d}$ and $e = N_{n,d}$)

$$(3) \quad \lambda(n, 2d) := \frac{1}{2} \left(2e + 1 - \sqrt{(2e+1)^2 - 8a} \right), \quad \Lambda(n, 2d) := \frac{1}{2} \left(-1 + \sqrt{1 + 8a} \right).$$

Proof. (Sketch) The first inequality in (1) comes from the fact that when $f = \sum_{i=1}^r f_i^2$ is a sum of squares representation of f of minimal length, the products $f_i f_j$ are linearly independent. The second follows from the fact that the sum of squares map $(\mathbb{R}[x]_d)^p \rightarrow \mathbb{R}[x]_{2d}$ is submersive generically on the source, according to Sard's theorem. \square

1.5. The setup of [5] is in fact more general than in Theorem 1.4. The authors consider sums of squares f whose Newton polytope $\text{New}(f)$ is contained in a fixed convex set ("cage") C . Inequalities (2) are generalized (with essentially the same proof) to

$$\lambda(C) \leq p(C) \leq \Lambda(C)$$

for any cage C , where $p(C) = \max\{\ell(f) : f \in \Sigma, \text{New}(f) \subseteq C\}$, and $\lambda(C), \Lambda(C)$ are defined as in (3), with e resp. a (related to) the numbers of lattice points in $\frac{1}{2}C$ and C . See [5] for precise definitions.

1.6. Particular choices of C may lead to improved lower bounds for $p(n, 2d)$. Namely, let $\bar{\lambda}(n, 2d) = \max_C \lambda(C)$, maximum over the Newton polytopes C of forms in $\mathbb{R}[x_1, \dots, x_n]_{2d}$. Then $\bar{\lambda}(n, 2d) \leq p(n, 2d)$, and it may happen that $\lceil \lambda(n, 2d) \rceil < \lceil \bar{\lambda}(n, 2d) \rceil$. This phenomenon was already discussed in [5], and was later studied in detail by Leep and Starr [12].

Unfortunately there is a huge discrepancy between lower and upper bounds. The reason is that the lower bounds λ are quite weak in general, even in the improved version $\bar{\lambda}$. Indeed, it is easy to see that $d \mapsto \lambda(n, 2d)$ is growing with limit 2^{n-1} for $d \rightarrow \infty$, and it is expected ([12] Conjecture 4.3) that the same holds for $\bar{\lambda}$. For $n = 3$ it has been shown that $\bar{\lambda}(n, 2d) = \lceil \lambda(n, 2d) \rceil = 4$ for all $d \geq 3$ ([12] Theorem 4.3). Therefore, when d is large relative to n , then λ (and probably $\bar{\lambda}$ as well) only gives the lower bound 2^{n-1} for $p(n, 2d)$, which does not even depend on d . This strongly contrasts with the fact that $p(n, 2d) \rightarrow \infty$ for $d \rightarrow \infty$, when $n \geq 3$. See also the discussion at the end of [12]. Altogether, when one considers the general case (d large relative to $n \geq 3$), it seems that the strongest known lower bounds for $p(n, 2d)$ are still the logarithmic bounds derived from [4], see 1.3 above.

1.7. We now discuss a substantial improvement for the upper bound in the case of ternary forms, due to Leep [11]. To describe his result, let A be a ring containing $\frac{1}{2}$. For $r \geq 1$ let $g_r(A)$ denote the smallest number $g \geq 1$ such that, for any finite number l_1, \dots, l_N of linear forms in $A[x_1, \dots, x_r]$, there exist g other linear forms $l'_1, \dots, l'_g \in A[x_1, \dots, x_r]$ with $l_1^2 + \dots + l_N^2 = l_1'^2 + \dots + l_g'^2$. If there is no finite such bound we write $g_r(A) = \infty$.

For example, when R is a real closed field and t is a variable, $g_r(R[t]) = r + 1$ for every $r \geq 1$ ([2] Example iii).

1.8. Upper bounds on g_r can lead to upper bounds for sos lengths, by the following elementary observation (compare [4] Theorem 2.7). Let B be an A -algebra, and

let M be an A -submodule of B generated by $r < \infty$ elements. Let $g = g_r(A)$. If $b \in B$ is a sum of squares of elements of M , then there exist $b_1, \dots, b_g \in M$ with $b = b_1^2 + \dots + b_g^2$.

Leep proves ([11] Theorem 5.2):

Theorem 1.9. (Leep) *If k is any real field then $g_r(k[t]) = g_r(k(t))$ for all $r \geq 1$.*

Corollary 1.10. *When R is a real closed field then $g_r(R[t]) = r + 1$ for any $r \geq 1$. \square*

Corollary 1.10 remains true when the field R is merely hereditarily pythagorean, see [11] Theorem 6.3 and thereafter.

1.11. When we speak of zeros of a form $f(x_1, \dots, x_n)$ we mean zeros in complex projective space $\mathbb{P}^{n-1}(\mathbb{C})$. Recall that the multiplicity of a form $0 \neq f \in \mathbb{R}[x_1, \dots, x_n]$ at a point $\xi \in \mathbb{P}^{n-1}(\mathbb{C})$ is the minimal number $m \geq 0$ for which there exists an n -tuple $a = (a_1, \dots, a_n)$ of nonnegative integers with $\sum_{i=1}^n a_i = m$ and with $(\partial^a f)(\xi) = \partial_1^{a_1} \dots \partial_n^{a_n} f(\xi) \neq 0$. When f has nonnegative values, the multiplicity of f at any point in $\mathbb{P}^{n-1}(\mathbb{R})$ is even. The form f is singular if and only if it has multiplicity ≥ 2 at some $\xi \in \mathbb{P}^{n-1}(\mathbb{C})$.

Applying Corollary 1.10 we get:

Theorem 1.12. *Let $n \geq 2$ and $d \geq 1$, let $f \in \Sigma_{n,2d}$, and assume that f has a real zero of multiplicity $2m \geq 0$. Then*

$$\ell(f) \leq 1 + \binom{n+d-2}{n-2} - \binom{n+m-3}{n-2}.$$

In particular, $m = 0$ gives

$$(4) \quad p(n, 2d) \leq 1 + \binom{n-2+d}{n-2}$$

for all $d \geq 1$.

The most interesting case is when $n = 3$ (ternary forms):

Corollary 1.13. (Leep) *If $f \in \Sigma_{3,2d}$ has a real zero of multiplicity $2m \geq 0$ then $\ell(f) \leq d + 2 - m$. In particular, $p(3, 2d) \leq d + 2$ for all $d \geq 1$. \square*

Proof of Theorem 1.12. Let $\xi \in \mathbb{P}^{n-1}(\mathbb{R})$ be a real zero of f of multiplicity $2m \geq 0$. After a linear change of coordinates we can assume $\xi = (0 : \dots : 0 : 1)$. Then $\deg_{x_n}(f) = 2(d - m)$. If f is written as a sum of squares, say $f = \sum_{\nu} p_{\nu}^2$, the p_{ν} contain only monomials x^{β} with $|\beta| = d$ and $0 \leq \beta_n \leq d - m$. Let $\mathbb{R}[x_1, \dots, x_n] \rightarrow \mathbb{R}[x_2, \dots, x_n]$, $g \mapsto g' := g(1, x_2, \dots, x_n)$ be the dehomogenization operator. The p'_{ν} lie in the $\mathbb{R}[x_2]$ -submodule of $\mathbb{R}[x_2, \dots, x_n]$ spanned by the monomials $x_3^{\beta_3} \dots x_n^{\beta_n}$ with $\beta_3 + \dots + \beta_n \leq d$ and $\beta_n \leq d - m$. The number of these monomials is

$$\sum_{j=0}^{d-m} \binom{n-3+d-j}{n-3} = \binom{n-2+d}{n-2} - \binom{n-3+m}{n-2} =: N.$$

Using Remark 1.8 and Corollary 1.10 we conclude $\ell(f) \leq N + 1$. \square

Remarks 1.14.

1. Denote the bound from Theorem 1.12 by $L(n, 2d) := 1 + \binom{n+d-2}{n-2}$. Let us compare $L(n, 2d)$ with the general upper bound $\Lambda(n, 2d)$ (Theorem 1.4). When $n = 3$ we have $L(3, 2d) = d + 2$, which is significantly better than $\Lambda(3, 2d) = 2d + 1$. For $n \geq 4$, however $L(n, 2d)$ is usually weaker (bigger) than $\Lambda(n, 2d)$. This is clear since $L(n, 2d)$ is a polynomial of degree $n - 2$ in d , whereas $\Lambda(n, 2d) = O(d^{(n-1)/2})$.

In fact, there are only three pairs (n, d) with $n \geq 4$ and $d \geq 1$ where $L(n, 2d) < \lfloor \Lambda(n, 2d) \rfloor$. These are

$$(n, 2d) = (4, 6), (4, 8) \text{ and } (4, 10),$$

where $\lfloor \Lambda(n, 2d) \rfloor = 12, 17, 23$ respectively, while $L(n, 2d)$ is smaller by one.

2. As far as we know, the upper bounds $p(3, 2d) \leq d + 2$ for $d \geq 2$ (1.13), resp.

$$p(n, 2d) \leq \begin{cases} L(n, 2d) & n = 4 \text{ and } 3 \leq d \leq 5, \\ \Lambda(n, 2d) & \text{otherwise} \end{cases}$$

for $n \geq 4$ and $d \geq 2$, are the best ones known to date.

2. TYPICAL SUM OF SQUARES LENGTHS

Let $\mathbf{x} = (x_1, \dots, x_n)$. We show that the set of typical sos lengths for forms in $\mathbb{R}[\mathbf{x}]_d$ is determined by $p(n, 2d)$ and by the (unique) typical sos length over \mathbb{C} .

2.1. Fix $n, d \geq 1$, and work over \mathbb{C} first. Let $t = t(n, 2d) \geq 1$ be the minimal number for which the set $\{p_1^2 + \dots + p_t^2 : p_1, \dots, p_t \in \mathbb{C}[\mathbf{x}]_d\}$ is (Zariski) dense in $\mathbb{C}[\mathbf{x}]_{2d}$. By Sard's theorem, this is also the minimal number t of forms p_1, \dots, p_t of degree d with $\langle x_1, \dots, x_n \rangle^{2d} \subseteq \langle p_1, \dots, p_r \rangle$, where $\langle \dots \rangle$ denotes the ideal generated in $\mathbb{C}[\mathbf{x}]$.

2.2. It is clear that $t(2, 2d) = 2$ for all $d \geq 1$ and $t(n, 2) = n$ for all $n \geq 1$, and that $t = t(n, 2d)$ always satisfies $tN_{n,d} - \binom{t}{2} \geq N_{n,2d}$, i.e. $t \geq \lambda(n, 2d)$ (see 1.4). A general conjecture due to Fröberg [7] predicts the Hilbert series of an ideal generated by a generic collection of forms of prescribed degrees. As a very particular case, this conjecture predicts $t(n, 2d) = \lceil \lambda(n, 2d) \rceil$ for all (n, d) . For all (n, d) , the theorem of Fröberg, Ottaviani and Shapiro [8] implies $t(n, 2d) \leq 2^{n-1}$. In particular we have $t(n, 2d) = 2^{n-1}$ when $\lceil \lambda(n, 2d) \rceil = 2^{n-1}$, which is the case for d large enough. For smaller d the values of $t(n, 2d)$ may be determined with the help of a computer algebra system, as long as n is not too big. In this way one shows that $t(3, 2) = t(3, 4) = 3$ and $t(3, 2d) = 4$ for $2d \geq 6$. For $n = 4$ the values of t are

$$t(4, 2d) = \begin{cases} 5 & \text{if } 2 \leq d \leq 4, \\ 6 & \text{if } 5 \leq d \leq 8, \\ 7 & \text{if } 9 \leq d \leq 20, \\ 8 & \text{if } d \geq 21. \end{cases}$$

2.3. Now fix $n, d \geq 1$. For $r \geq 1$ let

$$\Sigma_{n,2d}(r) := \{f \in \Sigma_{n,2d} : \ell(f) \leq r\},$$

and let

$$T(n, 2d) := \left\{ r \geq 1 : \Sigma_{n,2d}(r) \setminus \Sigma_{n,2d}(r-1) \text{ has nonempty interior in } \mathbb{R}[\mathbf{x}]_{2d} \right\}.$$

$T(n, 2d)$ is the set of *typical sos lengths* for $\Sigma_{n,2d}$, i.e., the set of numbers r for which there exists a non-empty open set consisting of forms of sos length r . Clearly $t(n, 2d)$ is the smallest element of $T(n, 2d)$.

Proposition 2.4. *Let $n, d, r \geq 1$, and let $m_r = \dim(I_{2d})$ where I is an ideal generated by a generic sequence of r forms of degree d .*

- (a) $\Sigma_{n,2d}(r)$ is a closed semi-algebraic subset of $\mathbb{R}[\mathbf{x}]_{2d}$.
- (b) For every $f \in \Sigma_{n,2d}(r)$, the local dimension of $\Sigma_{n,2d}(r)$ at f is m_r .
- (c) If $r \geq t(n, 2d)$ then $\Sigma_{n,2d}(r)$ is the closure of its interior.

Proof. Consider the map $\phi: (\mathbb{R}[\mathbf{x}]_d)^r \rightarrow \mathbb{R}[\mathbf{x}]_{2d}$, $(p_1, \dots, p_r) \mapsto \sum_{i=1}^r p_i^2$. (a) is clear since ϕ is a proper polynomial map. In (b) it is clear that $\dim \Sigma_{n,2d}(r) \leq m_r$. For all r -tuples $p = (p_1, \dots, p_r) \in (\mathbb{R}[\mathbf{x}]_d)^r$ outside a proper real algebraic set we have $\dim \langle p_1, \dots, p_r \rangle_{2d} = m_r$. For these p , the local dimension of $\Sigma_{n,2d}(r)$ at $\phi(p)$ is equal to m_r . Since these p are dense in $\text{im}(\phi)$ we get (b). For $r \geq t(n, 2d)$ we have $m_r = N_{n,2d}$, so (b) implies (c). \square

Corollary 2.5. *The typical sos lengths for $\Sigma_{n,2d}$ are $T(n, 2d) = \{t, t+1, \dots, p\}$ where $t = t(n, 2d)$ and $p = p(n, 2d)$.*

Proof. Write $\Sigma := \Sigma_{n,2d}$, and let $t \leq r \leq p$. Then $\Sigma(r-1) \neq \Sigma(r)$, and hence $\text{int } \Sigma(r) \not\subseteq \Sigma(r-1)$ since $\Sigma(r) = \overline{\text{int } \Sigma(r)}$ (Proposition 2.4). So $\text{int}(\Sigma(r)) \setminus \Sigma(r-1)$ is a non-empty open set of forms of length equal to r . \square

3. LOWER BOUNDS

3.1. Let k be a field of characteristic zero, let V be a vector space over k . For $m \geq 0$ let $S^m V$ be the m -th symmetric power of V over k . We will identify $S^m V$ with the subspace of symmetric tensors in the m -fold tensor power $V^{\otimes m}$, which is possible since $\text{char}(k) = 0$.

Let A be a k -algebra. The *Gram tensor* of a given sum of squares representation $f = \sum_{i=1}^m a_i^2$ in A (with $a_1, \dots, a_m \in A$) is the symmetric tensor

$$\vartheta = \sum_{i=1}^m a_i \otimes a_i \in S^2 A.$$

Of course we may as well regard ϑ as an element of $S^2 U$, for any linear subspace $U \subseteq A$ containing a_1, \dots, a_m . Two sum of squares representations $f = \sum_{i=1}^m a_i^2 = \sum_{i=1}^m b_i^2$ (with $a_i, b_i \in A$) are (*orthogonally*) *equivalent* if there exists an orthogonal matrix $u = (u_{ij})_{1 \leq i, j \leq m}$ over k (satisfying $uu^t = I$) such that $b_j = \sum_{i=1}^m u_{ij} a_i$ for $1 \leq j \leq m$. Clearly, equivalent sum of squares representations have the same Gram tensor. An elementary but important fact is that the converse holds provided the field k is real (see [5]).

3.2. If $I \subseteq k[\mathbf{x}] = k[x_1, \dots, x_n]$ is a homogeneous ideal, we write $h_j(I) = \dim k[\mathbf{x}]_j / I_j$ for $j \geq 0$. For any set $Z \subseteq \mathbb{P}^{n-1}(k)$, the full (saturated) vanishing ideal of Z is denoted $I(Z)$.

We first discuss ternary forms (case $n = 3$, $\mathbf{x} = (x_1, x_2, x_3)$), and abbreviate $\Sigma_d := \Sigma_{3,d}$.

Proposition 3.3. *Let $d \geq 1$, and let $Z \subseteq \mathbb{P}^2(\mathbb{R})$ be a set of $|Z| = \binom{d+1}{2}$ real points in sufficiently general position. Then any $f \in \Sigma_{2d}$ vanishing on Z has a unique sum of squares representation, up to orthogonal equivalence.*

Proof. Let $I = I(Z)$. It is enough to show that the product map $\mu: S^2(I_d) \rightarrow \mathbb{R}[\mathbf{x}]_{2d}$ is injective. Indeed, if $f \in \Sigma_{2d}$ vanishes on Z and $f = \sum_{\nu} p_{\nu}^2$ is any sum of squares representation, then $p_{\nu} \in I_d$ for all ν . By the asserted injectivity of μ , the symmetric Gram tensor $\sum_{\nu} p_{\nu} \otimes p_{\nu}$ is uniquely determined by f , which is the claim (see 3.1).

Since the points in Z are general we have $I_{d-1} = \{0\}$ and $\dim(I_d) = \binom{d+2}{2} - \binom{d+1}{2} = d+1$. In particular, the subspace $\text{im}(\mu) = I_d I_d$ of $\mathbb{R}[\mathbf{x}]_{2d}$ satisfies $I_d I_d = (I^2)_{2d}$. Injectivity of μ means that this space has dimension equal to $\dim S^2(I_d) = \binom{d+2}{2}$, and hence is equivalent to

$$(5) \quad h_{2d}(I^2) = \binom{2d+2}{2} - \binom{d+2}{2} = 3 \binom{d+1}{2}.$$

Equality (5) is known to be true, see Iarrobino-Kanev [10] Prop. 4.8. In fact, the complete Hilbert series of I^2 is determined there. This proves Proposition 3.3. \square

Proposition 3.3 has the following consequences:

Corollary 3.4. *If $Z \subseteq \mathbb{P}^2(\mathbb{R})$ is a set of s general points where $\binom{d+1}{2} \leq s \leq \binom{d+2}{2}$, then any general sum of squares $f \in \Sigma_{2d}$ that vanishes on Z has sos length $\ell(f) = \binom{d+2}{2} - s$.*

Proof. Since $\dim I(Z)_d = \binom{d+2}{2} - s =: m$, the general $f \in \Sigma_{2d}$ vanishing on Z has the form $f = p_1^2 + \cdots + p_m^2$ where p_1, \dots, p_m form a basis of $I(Z)_d$. \square

In particular we get a lower bound for the Pythagoras number:

Corollary 3.5. *Let $d \geq 2$. Any general sum of squares of degree $2d$ in $\mathbb{R}[x_1, x_2, x_3]$ vanishing in $\binom{d+1}{2}$ general \mathbb{R} -points has sos length $d + 1$. Therefore $p(3, 2d) \geq d + 1$.* \square

Combined with Corollary 1.13 this gives:

Theorem 3.6. *For any $d \geq 2$, the Pythagoras number $p(3, 2d)$ is either $d + 1$ or $d + 2$.* \square

3.7. In principle the same argument extends to the case of $n \geq 4$ variables. In general however, when I is the vanishing ideal of a generic finite set of points in \mathbb{P}^{n-1} , the Hilbert function of I^2 is known only conjecturally. In [10] Sect. 3.2, Iarrobino-Kanev formulate conjectures about the dimensions of tangent spaces to catalecticant varieties corresponding to power sums. These conjectures can be formulated in terms of the Hilbert function of I^2 . In particular, if d is the lowest degree with $I_d \neq \{0\}$, and if $b = \dim(I_d)$, it is conjectured that $(I^2)_{2d} = I_d I_d$ has the maximum possible dimension $\binom{b+1}{2}$, unless a smaller value is forced by the Alexander-Hirschowitz theorem. Explicitly, this means (we write $N_d := N_{n,d} = \binom{n+d-1}{n-1}$ in the sequel):

Conjecture 3.8. *(Iarrobino-Kanev, [10] Conjecture 3.25) Let $n \geq 3$, $d \geq 2$ and $N_{d-1} \leq s < N_d$, and let $I = I(Z)$ be the vanishing ideal of a set Z of s general points in \mathbb{P}^{n-1} . Then*

$$h_{2d}(I^2) = \max\left\{ns, N_{2d} - \binom{N_d - s + 1}{2}\right\},$$

except for $(n, d, s) = (3, 2, 5), (4, 2, 9)$ and $(5, 2, 14)$, where \max has to be replaced by \min .

Of course, the exceptional cases correspond to exceptional cases of the Alexander-Hirschowitz theorem. Conjecture 3.8 is proved in [10] for $n = 3$, and also for $n \geq 4$ in the case $N_d - n \leq s < N_d$. Note that [10] Conjecture 3.25 contains misprints, but compare with loc. cit., Conjecture 3.20.

Assuming Conjecture 3.8 we can conclude:

Corollary 3.9. *Let $n \geq 4$ and $d \geq 2$, and let $s = s_{\min}(n, d)$ be the smallest integer satisfying $\binom{N_d - s + 1}{2} \leq N_{2d} - ns$. Then $N_{d-1} < s < N_d$. If Conjecture 3.8 is true for the given values of (n, d, s) , then*

$$p(n, 2d) \geq N_d - s.$$

In fact, then, any generic sum of squares in Σ_{2d} that vanishes in a generic set of s real points has sos length equal to $N_d - s$.

Proof. We only sketch the proof of $N_{d-1} < s < N_d$. Check the claim directly for $(n, d) = (4, 2)$ or $(5, 2)$ and discard these cases. Consider the polynomial

$$P(x) = x^2 - (2N_d - 2n + 1)x + N_d(N_d + 1) - 2N_{2d}.$$

By definition, $s = s_{\min}(n, d)$ is the smallest integer satisfying $P(s) \leq 0$. One shows that $P(N_d - 1) \leq 0$, thereby proving $s < N_d$. To prove the other inequality, fix n and consider $P(N_{d-1})$ as a polynomial in d . One shows that $P(N_{d-1}) = (d-1)Q(d)$ where Q is a polynomial with all coefficients nonnegative. This implies $P(N_{d-1}) > 0$, and thus $s > N_{d-1}$. The details are left to the reader.

By the argument in the proof of 3.3 we get $p(n, 2d) \geq N_d - t$ for any number t such that the map $\mathbb{S}^2 I_d \rightarrow \mathbb{R}[\mathbf{x}]_{2d}$ is injective, where I is the vanishing ideal of a generic set of t points in $\mathbb{P}^{n-1}(\mathbb{R})$. Since $s = s_{\min}(n, d) \geq N_{d-1}$, Conjecture 3.8 predicts that this property holds for $t = s$. \square

Remarks 3.10.

1. In Conjecture 3.8 it is clear that \geq holds, i.e. that $h_{2d}(I^2)$ is at least the right hand maximum (resp. minimum in the exceptional cases). For any concrete values of n, d and s , the conjecture can be verified by finding a single concrete set Z with $|Z| = s$ for which equality holds in 3.8. In this way the conjecture is easily verified for sufficiently small values of n, d, s , using a computer algebra system.

2. An unconditional formulation of Corollary 3.9, not depending on Conjecture 3.8, would be: *Let $n \geq 4$ and $d \geq 2$, let $N_{d-1} \leq s < N_d$, and let I be the vanishing ideal of a generic set $Z \subseteq \mathbb{P}^{n-1}(\mathbb{R})$ of s points. If $h_{2d}(I^2) = N_{2d} - \binom{N_d - s + 1}{2}$, then $p(n, 2d) \geq N_d - s$.* The drawback, of course, is that we have no good control of what numbers s satisfy the condition. Theorem 4.19 in [10] shows that $s = N_d - n$ is admitted, but this only gives the useless bound $p(n, 2d) \geq n$.

Remark 3.11. For small values of $n \geq 4$ and $d \geq 2$ we record the bounds on $p(n, 2d)$ that we have obtained. The following table lists the minimal number $s = s_{\min}(n, d)$ and the corresponding lower bound $N_d - s$ for $p(n, 2d)$ from Corollary 3.9. We compare these with the upper bounds from Section 1. (Those upper bounds are usually the numbers $\lfloor \Lambda(n, 2d) \rfloor$, with only three exceptions where $L(n, 2d)$ is better, see Remark 1.14.)

d	2	3	4	5	6	7	8
$s_{\min}(4, d)$	5	12	24	41	65	97	137
$p(4, 2d) \geq$	5	8	11	15	19	23	28
$p(4, 2d) \leq$	7	11	16	22	29	36	43
$s_{\min}(5, d)$	8	21	48	94	166	273	422
$p(5, 2d) \geq$	7	14	22	32	44	57	73
$p(5, 2d) \leq$	11	20	30	44	59	77	97
$s_{\min}(6, d)$	10	34	88	192	374	670	1123
$p(6, 2d) \geq$	11	22	38	60	88	122	164
$p(6, 2d) \leq$	15	29	50	77	110	152	201

Remark 3.12. The forms in $\Sigma_{n, 2d}$ of large sos length that were constructed in Corollaries 3.5 and 3.9 are of very special nature, in that they have many real zeros. Corollary 2.5 on typical lengths shows that there exists a nonempty open set of nonsingular forms with the same sos length.

Theorem 3.13. *Let $n \geq 4$. Assuming Conjecture 3.8, the Pythagoras number $p(n, 2d)$ grows asymptotically like $d^{(n-1)/2}$ for $d \rightarrow \infty$. More precisely, for any $\varepsilon > 0$ the inequalities*

$$(C_n - \varepsilon) d^{(n-1)/2} < p(n, 2d) < (C_n + \varepsilon) d^{(n-1)/2}$$

hold for all but finitely many d , where

$$c_n = \sqrt{\frac{2^n - 2n}{(n-1)!}}, \quad C_n = \sqrt{\frac{2^n}{(n-1)!}}.$$

Proof. Let $\vartheta(n, 2d) := N_d - s_{\min}(n, d)$, see 3.9. For all $d \geq 2$ we have $\vartheta(n, 2d) \leq p(n, 2d) \leq \Lambda(n, 2d)$. Since $N_{2d} = \frac{1}{(n-1)!}(2d+1) \cdots (2d+n-1)$, it is clear that

$$\Lambda(n, 2d) \sim \sqrt{2N_{2d}} \sim \sqrt{\frac{2}{(n-1)!}(2d)^{n-1}} = C_n d^{(n-1)/2}$$

for $d \rightarrow \infty$ (meaning that the quotient of both sides converges to 1). On the other hand, $\vartheta = \vartheta(n, 2d)$ is the largest integer $0 < \vartheta < N_d$ satisfying $\binom{\vartheta+1}{2} \leq N_{2d} - n(N_d - \vartheta)$. This means

$$\vartheta \approx n - \frac{1}{2} + \sqrt{2N_{2d} - 2nN_d + n^2 - n + \frac{1}{4}},$$

and since

$$N_{2d} - nN_d = \frac{1}{(n-1)!} \left((2d+1) \cdots (2d+n-1) - n(d+1) \cdots (d+n-1) \right)$$

we get $\vartheta(n, 2d) \sim c_n d^{(n-1)/2}$. \square

Remark 3.14. A different view on the asymptotic behaviour of $p(n, 2d)$ is taken in [5] Theorem 6.4. Fixing the degree, it is shown there that $\gamma_1 n^d \leq p(n, 2d) \leq \gamma_2 n^d$ for all $n \geq 1$ and suitable $\gamma_1, \gamma_2 > 0$ depending on d . This result only uses the weak lower bound $\lambda(n, 2d)$.

4. TERNARY SEXTICS AND QUATERNARY QUARTICS

We now prove that the lower bounds for the Pythagoras number from Section 3 are sharp, in the case of ternary sextics or quaternary quartics:

Theorem 4.1. $p(3, 6) = 4$: Every ternary sextic that is a sum of squares is a sum of four squares.

Theorem 4.2. $p(4, 4) = 5$: Every quaternary quartic that is a sum of squares is a sum of five squares.

Corollary 4.3. The elements of length 4 in $\Sigma_{3,6}$, or those of length 5 in $\Sigma_{4,4}$, form an open dense subset.

Proof. The set of three squares in $\Sigma_{3,6}$ (resp. of four squares in $\Sigma_{4,4}$) is nowhere dense since $\lambda(3, 6) = 4$ (resp. $\lambda(4, 4) = 5$). So the claims follow from 4.1 resp. 4.2. \square

The proofs of Theorems 4.1 and 4.2 are similar. We do the (3, 6) case first, and then explain how to modify the argument in the (4, 4) case. See Remark 4.8 below for comments on the proofs.

4.4. In the following let k be a field, $\text{char}(k) = 0$. Write $A = k[\mathbf{x}] = k[x_1, \dots, x_n] = \bigoplus_{e \geq 0} A_e$. Given $e \geq 1$ and $0 \neq \alpha \in A_e^\vee = \text{Hom}(A_e, k)$, let $I(\alpha) \subseteq A$ be the graded ideal defined by $I(\alpha)_i = \{p \in A_i : pA_{e-i} \subseteq \ker(\alpha)\}$ ($0 \leq i \leq e$) and $I(\alpha)_i = A_i$ for $i > e$. Then the graded artinian ring $R = A/I(\alpha)$ is Gorenstein with socle degree e . In particular, this means that α induces a linear duality between R_i and R_{e-i} for $0 \leq i \leq e$.

The following is the key observation in the (3, 6) case:

Proposition 4.5. *Let $p_1, \dots, p_r \in k[x_1, x_2, x_3]$ be linearly independent cubic forms such that $\langle x_1, x_2, x_3 \rangle^6 \not\subseteq \langle p_1, \dots, p_r \rangle$. If $r \neq 3$ then p_1, \dots, p_r have a common zero (in \bar{k}). In particular, then, the form $p_1^2 + \dots + p_r^2$ is singular.*

Proof. Write $\mathbf{x} = (x_1, x_2, x_3)$, let $U \subseteq k[\mathbf{x}]_3$ be the linear span of p_1, \dots, p_r . By assumption there exists a linear functional $0 \neq \alpha \in (k[\mathbf{x}]_6)^\vee$ with $Uk[\mathbf{x}]_3 \subseteq \ker(\alpha)$. Let $I = I(\alpha) \subseteq k[\mathbf{x}]$ be the Gorenstein ideal defined by α . Then $U \subseteq I_3$. It is enough to assume that p_1, \dots, p_r have no common zero and to show $r \leq 3$. By the assumption there exist three forms $q_1, q_2, q_3 \in U$ without common zero. Hence the ideal $J := \langle q_1, q_2, q_3 \rangle$ is a complete intersection, so J is an artinian Gorenstein ideal with socle degree 6 (see [6] Theorem CB8). By construction we have $J \subseteq I$. On the other hand, both I and J are Gorenstein ideals with same socle degree. Therefore $J = I$, and in particular, $I_3 = J_3$ has dimension 3, whence $r \leq 3$. \square

4.6. We now give the proof of Theorem 4.1. Let $\Sigma = \Sigma_{3,6}$, and let $\Sigma(4) \subseteq \Sigma$ be the set of sums of four squares. The map

$$\phi: (\mathbb{R}[\mathbf{x}]_3)^4 \rightarrow \mathbb{R}[\mathbf{x}]_6, \quad \phi(p_1, p_2, p_3, p_4) = \sum_{i=1}^4 p_i^2$$

is proper, and its image set $\Sigma(4)$ has nonempty interior in $\mathbb{R}[\mathbf{x}]_6$. Let $Z \subseteq \Sigma(4)$ be the set of critical values of ϕ . So Z consists of all forms $\phi(p)$ where $p = (p_1, p_2, p_3, p_4) \in (\mathbb{R}[\mathbf{x}]_3)^4$ is such that $\langle p_1, p_2, p_3, p_4 \rangle_6 \neq \mathbb{R}[\mathbf{x}]_6$. The set Z is closed and semi-algebraic in $\mathbb{R}[\mathbf{x}]_6$ and has empty interior, e.g. by Sard's theorem. Whenever $[0, 1] \rightarrow \mathbb{R}[\mathbf{x}]_6$, $t \mapsto f_t$ is a smooth path in $\mathbb{R}[\mathbf{x}]_6$ with $f_t \in \text{int}(\Sigma)$ and $f_t \notin Z$ for all $0 \leq t \leq 1$, then $f_0 \in \Sigma(4)$ implies $f_1 \in \Sigma(4)$, since one can lift the path $t \mapsto f_t$ to a path in $(\mathbb{R}[\mathbf{x}]_3)^4$.

Since $\lambda(3, 6) = 4$, it is clear that $p(3, 6) \geq 4$. We assume $p(3, 6) \geq 5$ and will arrive at a contradiction. By assumption the semi-algebraic set $Z' := \text{int}(\Sigma) \cap \Sigma(4) \cap (\Sigma \setminus \Sigma(4))$ is non-empty. It is contained in Z and has codimension one in $\mathbb{R}[\mathbf{x}]_6$, by the above path argument and since the complement of a codimension two set in $\text{int}(\Sigma)$ is connected. So there exists $f \in Z'$, together with an open neighborhood W of f contained in Σ , such that $Z' \cap W$ is a smooth codimension one submanifold of W . Since every singular form in $\text{int}(\Sigma)$ has at least two distinct singularities (complex conjugate), the set $\{f \in \text{int}(\Sigma): f \text{ is singular}\}$ has codimension two. Therefore we can choose f to be nonsingular. Then it follows from Proposition 4.5 that f is a sum of three squares.

Let $0 \neq \alpha \in (\mathbb{R}[\mathbf{x}]_6)^\vee$ such that $\{g \in \mathbb{R}[\mathbf{x}]_6: \alpha(g - f) = 0\}$ is the affine hyperplane in $\mathbb{R}[\mathbf{x}]_6$ tangent to Z' at f . If we shrink W appropriately, the hypersurface Z' divides W into two open halves, one contained in $\Sigma(4)$, the other contained in $\Sigma \setminus \Sigma(4)$. Replacing α with $-\alpha$ if necessary, we can thus assume: If $h \in \mathbb{R}[\mathbf{x}]_6$ satisfies $\alpha(h) > 0$, then $\ell(f + th) \leq 4$ and $\ell(f - th) \geq 5$, for all sufficiently small $t > 0$. It follows that $\alpha(f) = 0$. Since $f \in \text{int}(\Sigma)$, there exists $p \in \mathbb{R}[\mathbf{x}]_3$ with $\alpha(p^2) < 0$. By the choice of α we have $\ell(f + tp^2) \geq 5$ for small $t > 0$. But this is a contradiction since $\ell(f) \leq 3$. Theorem 4.1 is proved.

In the (4, 4) case, the analogue to Proposition 4.5 is

Proposition 4.7. *Let $p_1, \dots, p_r \in k[x_1, x_2, x_3, x_4]$ be linearly independent quadratic forms such that $\langle x_1, x_2, x_3, x_4 \rangle^4 \not\subseteq \langle p_1, \dots, p_r \rangle$. If $r \neq 4$ then p_1, \dots, p_r have a common zero. In particular, then, the form $p_1^2 + \dots + p_r^2$ is singular.*

The proof is completely parallel to the proof of 4.5. The essential point is that four quadratic forms in $k[\mathbf{x}] = k[x_1, \dots, x_4]$ without common zero define a complete intersection with socle degree 4. Having proved 4.7, one considers the sum of squares

map $\phi: (\mathbb{R}[x]_2)^5 \rightarrow \mathbb{R}[x]_4$ and proceeds similarly to 4.6, thereby proving Theorem 4.2.

Remark 4.8. The proofs of Theorems 4.1 and 4.2 have much in common with Hilbert's argument for showing that every nonnegative ternary quartic is a sum of three squares [9]. Hilbert considered the sum of squares map $\phi: (\mathbb{R}[x]_2)^3 \rightarrow \mathbb{R}[x]_4$ ($\mathbf{x} = (x_1, x_2, x_3)$) and showed that the critical values of ϕ are singular forms. Hence the strictly positive ones among them form a codimension two subset of $\mathbb{R}[x]_4$. This implies that the set of strictly positive forms that are not critical values of ϕ is connected, leading to the desired conclusion.

To prove 4.1, say, we have shown that the critical values of $(\mathbb{R}[x]_3)^4 \rightarrow \mathbb{R}[x]_6$ are singular or else sums of three squares. We then needed an extra argument to deal with the second case.

Remark 4.9. Blekherman proved that every positive definite form in the boundary $\partial(\Sigma_{3,6})$ (resp. in $\partial(\Sigma_{4,4})$) is a sum of three (resp. four) squares ([3], Corollaries 1.3 and 1.4). Propositions 4.5 and 4.7 give a quick way of reproving these results. We explain this for $(n, d) = (4, 4)$. Let B be the set of positive definite forms in $\partial(\Sigma_{4,4})$. Every singular form in B has at least two different singularities (complex conjugate), so these forms constitute a subset of codimension ≥ 2 in $\mathbb{R}[x]_4$. Since the semi-algebraic set B has codimension one in $\mathbb{R}[x]_4$ locally at each of its points, every form in B is a limit of nonsingular forms in B . Every nonsingular form in B is a sum of four squares by 4.7. Since the sums of four squares form a closed set, it follows that B consists of sums of four squares.

Remark 4.10. Unfortunately, Propositions 4.5 and 4.7 do not directly extend to higher degrees. Still we conjecture in the ternary case that the lower bound 3.5 is sharp, i.e. that $p(3, 2d) = d + 1$ holds for all $d \geq 2$.

REFERENCES

- [1] D. J. Anick: Thin algebras of embedding dimension three. *J. Algebra* **100**, 235–259 (1986).
- [2] R. Baeza, D. Leep, M. O’Ryan, J.P. Prieto: Sums of squares of linear forms. *Math. Z.* **193**, 297–306 (1986).
- [3] G. Blekherman: Nonnegative polynomials and sums of squares. *J. Am. Math. Soc.* **25**, 617–635 (2012).
- [4] M. D. Choi, Z. D. Dai, T. Y. Lam, B. Reznick: The Pythagoras number of some affine algebras and local algebras. *J. reine angew. Math.* **336**, 45–82 (1982).
- [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*, B. Jacob, A. Rosenberg (eds), *Proc. Symp. Pure Math.* **58.2**, Am. Math. Soc., 1995, pp. 103–126.
- [6] D. Eisenbud, M. Green, J. Harris: Cayley-Bacharach theorems and conjectures. *Bull. Am. Math. Soc.* **33**, 295–324 (1996).
- [7] R. Fröberg: An inequality for Hilbert series of graded algebras. *Math. Scand.* **56**, 117–144 (1985).
- [8] R. Fröberg, G. Ottaviani, B. Shapiro: On the Waring problem for polynomial rings. *Proc. Nat. Acad. Sci.* **109**, 5600–5602 (2012).
- [9] D. Hilbert: Über die Darstellung definiter Formen als Summe von Formenquadraten. *Math. Ann.* **32**, 342–350 (1888).
- [10] A. Iarrobino, V. Kanev: *Power Sums, Gorenstein Algebras, and Degeneration Loci*. *Lect. Notes Math.* **1721**, Springer, Berlin, 1999.
- [11] D. Leep: Sums of squares of polynomials and the invariant $g_n(R)$. Preprint, 2006.
- [12] D. Leep, C. Starr: Estimates of the Pythagoras number of $\mathbb{R}_m[x_1, \dots, x_n]$ through lattice points and polytopes. *Discrete Math.* **308**, 5771–5781 (2008).
- [13] A. Pfister: Zur Darstellung definiter Funktionen als Summe von Quadraten. *Invent. math.* **4**, 229–237 (1967).
- [14] W. Scharlau: *Quadratic and Hermitian Forms*. *Grundlehr. math. Wiss.* **270**, Springer, Berlin, 1985.

FACHBEREICH MATHEMATIK UND STATISTIK, UNIVERSITÄT KONSTANZ, 78457 KONSTANZ, GER-
MANY
E-mail address: `claus.scheiderer@uni-konstanz.de`