EXACT POLYNOMIAL SUM OF SQUARES DECOMPOSITIONS

JOSE CAPCO, SANTIAGO LAPLAGNE, AND CLAUS SCHEIDERER

ABSTRACT. We construct two examples of non-negative polynomials over $\mathbb{Q}$ that can be decomposed as sum of squares over $\mathbb{Q}(\alpha)$, for α the real root of $X^3 - 2$, but not over $\mathbb{Q}$. The first example is a polynomial in 3 variables of degree 6 and the second example is a polynomial of degree 4 in 4 variables. Furthermore, we show how to modify the construction to construct families of examples over more general algebraic extensions of degree 3.

1. INTRODUCTION

Determining if a given polynomial can be expressed as sums of squares of polynomials (SOS), and compute such decompositions, is a fundamental problem in real algebraic geometry. We address the problem of determining when a rational polynomial that can be decomposed as a sum of squares of real polynomials ($\mathbb{R}$-SOS) can also be decomposed as a sum of squares over the rational numbers ($\mathbb{Q}$-SOS).

In [6] the first families of negative examples were found (that is, rational polynomials that are $\mathbb{R}$-SOS but not $\mathbb{Q}$-SOS). Moreover, for the case of polynomials of degree 4 in 3 variables (shortly, the (3,4) case), the author gives a complete characterization of the negative examples. In particular, all such examples are sum of two squares with coefficients in algebraic extensions of $\mathbb{Q}$ of even degree.

In [4] a new negative example was found, given by a polynomial of degree 6 in 4 variables, with coefficients over an algebraic extension of $\mathbb{Q}$ of odd degree 3. The verification uses computational techniques difficult to extend to families of polynomials. It remained as an interesting question to study the smaller cases of polynomials of degree 6 in 3 variables and degree 4 in 4 variables (that is, the (3,6) and (4,4) cases). The general study of the SOS cone in these two cases has attracted a lot of interest recently (see [1], [2], [3]).

In our work, following the construction in [4], we provide new examples of non-negative polynomials that are $\mathbb{R}$-SOS but not $\mathbb{Q}$-SOS for both of those cases. Most interestingly, we are able to provide more general theoretical proofs that these polynomials cannot be decomposed as $\mathbb{Q}$-SOS, and that the given decomposition is unique, which allows us to extend the results to new families of counterexamples, perturbing the coefficients and using more general degree 3 algebraic extensions.

1.1. **Basic construction.**

Let $H_{n,d}$ be the vector space of homogeneous polynomials in n variables of degree d with coefficients in $\mathbb{R}$.

We recall from [4] the basic construction for polynomials over $\mathbb{Q}$ that are sum of squares of polynomials in an algebraic extension of $\mathbb{Q}$. We restrict first to the case of sum of 3 polynomials over $\mathbb{Q}(\alpha)$, where α is the real cubic root of 2.

SOS Construction 1.1. Let $\boldsymbol{x} = x_0, \dots, x_n$. Let α be the real cubic root of 2 and let

$$\begin{aligned}
p_1 &= b_1b_2^2 + b_1^3 + b_1b_3^2 - 2a_3b_3c_1 - 2c_1c_2^2 - 2c_1^3 + 2a_3b_1c_3 - 2c_1c_3^2 - 2b_1b_2c_2\alpha, \\
&\quad + 2b_2^2c_1\alpha - 2b_1c_2^2\alpha^2 + 2b_2c_1c_2\alpha^2 \\
p_2 &= b_1^2b_2 + b_2^3 + b_2b_3^2 - 2a_3b_3c_2 - 2c_1^2c_2 - 2c_2^3 + 2a_3b_2c_3 - 2c_2c_3^2 - 2b_1b_2c_1\alpha, \\
&\quad + 2b_1^2c_2\alpha - 2b_2c_1^2\alpha^2 + 2b_1c_1c_2\alpha^2 \\
p_3 &= 2(b_2c_1 - c_2b_1)(a_3 + b_3\alpha + \alpha^2c_3),
\end{aligned}$$

where $a_3, b_1, b_2, b_3, c_1, c_2, c_3$ are any choice of polynomials in $\mathbb{Q}[\boldsymbol{x}]$ such that p_1, p_2, p_3 are not identically 0. Then

$$p_1^2 + p_2^2 + p_3^2 \in \mathbb{Q}[\boldsymbol{x}].$$

One can verify the above by checking that the coefficients of α and α^2 vanish after computing the sum of squares. Notice also that p_2 is just p_1 where c_1 is swapped with c_2 and b_1 is swapped with b_2.

Remark 1.2. In the above construction, for simplicity, we only consider b_1, b_2, b_3, c_1, c_2, c_3, a_3 chosen as linear forms (or 0) in $\mathbb{Q}[\boldsymbol{x}]$. The sum of squares in this case is a sextic form. However, we will see in the example with quaternary forms that we can choose them so that they have a common factor which can be mod out to obtain examples of smaller degree.

2. Polynomials in 3 variables of degree 6

We construct an example of a polynomial of degree 6 in 3 variables that can be decomposed as a sum of squares over $\mathbb{R}$ but not over $\mathbb{Q}$. In [6], C. Scheiderer studies the case of polynomials of degree 4 in 3 variables and gives a complete characterization of the negative examples. In particular, all such examples are sum of two squares with coefficients in an algebraic extensions of $\mathbb{Q}$ of even degree. In his proof, he uses strongly the fact that non-negative polynomials of degree 4 in 3 variables are always sum of squares. The next example shows that the characterization provided in that paper cannot be extended to polynomials of degree 6. The example is constructed applying the following substitutions in Construction 1.1:

$$a_3 = z - x, \quad b_1 = x, \quad b_2 = y, \quad b_3 = y + z, \quad c_1 = z, \quad c_2 = z, \quad c_3 = x.$$

Proposition 2.1. For α the real root of $X^3 - 2$, define

$$\begin{aligned}
p_1 &= -2\alpha^2xz^2 + 2\alpha^2yz^2 - 2\alpha x^2z + 2\alpha xyz + x^2y + 2x^2z - 4xyz - 2xz^2 - 2y^3 \\
&\quad - 2y^2z + yz^2 + 6z^3, \\
p_2 &= -2\alpha^2xz^2 + 2\alpha^2yz^2 - 2\alpha xyz + 2\alpha y^2z - x^3 + 2xy^2 + 4xyz + 3xz^2 - 2yz^2 - 6z^3, \\
p_3 &= 2z(x - y)((z - x) + \alpha(y + z) + \alpha^2x),
\end{aligned}$$

polynomials in $\mathbb{Q}(\alpha)_3[x,y,z]$ and let $f = p_1^2 + p_2^2 + p_3^2 \in \mathbb{Q}_6[x,y,z]$,

$$\begin{aligned} f = {} & x^6 - 3x^4y^2 - 4x^4yz + 2x^4z^2 - 8x^3y^2z - 8x^3yz^2 + 28x^3z^3 + 4x^2y^3z \\ & + 10x^2y^2z^2 + 24x^2yz^3 + 41x^2z^4 + 16xy^4z + 32xy^3z^2 - 48xy^2z^3 \\ & - 120xyz^4 - 60xz^5 + 4y^6 + 8y^5z - 12y^3z^3 - 15y^2z^4 + 36yz^5 + 72z^6. \end{aligned}$$

Then f is a sum of squares over $\mathbb{Q}(\alpha)$ but not over $\mathbb{Q}$.

Proof. See [**?**] for the computations in `Maple` **jc:** the link is dead or perhaps wrong. Let K be the Galois closure of $\mathbb{Q}(\alpha)$. Then the common (projective) zeros of these four polynomials are all real points in $\mathbb{P}^3(K)$ and are given by:

$$\begin{array}{ll} P_1 = (1:1:1), & P_4 = (1:\sqrt{2}/2:0), \\ P_2 = (-2:-2:1), & P_5 = (1:-\sqrt{2}/2:0). \\ P_3 = (-3:-3:1), & \end{array}$$

To show that the polynomial f does not allow a $\mathbb{Q}$-SOS decomposition we can proceed as in [4]. We let v be the set of all 10 monomials of degree 3 in 3 variables and consider the set of symmetric matrices

$$\mathcal{L} := \{Q \in \mathbb{R}^{10\times 10} | f(\boldsymbol{x}) = v(\boldsymbol{x})^t Q v(\boldsymbol{x})\}.$$

Using the 5 real roots of f for facial reduction, we reduce to a 5×5 matrix in 2 variables:

$$A = \frac{1}{2}\begin{pmatrix} 2 & -4+x & 0 & -x & -2+y \\ -4+x & 20+2y & 0 & -12-2y & 16 \\ 0 & 0 & 4 & x & 8+y \\ -x & -12-2y & 2x & -14-y+4x & 12+x/2 \\ -2+y & 16 & 16+2y & 24+x & 130-12x \end{pmatrix}.$$

We need to find x, y such that A is positive semidefinite. This problem is harder to solve than what it might look like at first sight. We were able to solve it using `RegularChains` [5] package in `Maple` or `Cylindrical Algebraic Decomposition` [7] package in `Mathematica`. In both cases the system is solved completely and we get that there is a unique solution which coincides with the one given by the original decomposition. So we conclude that the Gram spectrahedron consists of only one point with non-rational entries and hence there is no $\mathbb{Q}$-SOS decomposition for f. □

We now give an alternate proof that this polynomial cannot be expressed as the sum of polynomials over $\mathbb{Q}$. This proof is less computational, it only requires some basic linear algebra computations, and it can be more easily generalized to further examples.

Alternative proof of Proposition 2.1. **jc:** are the computations for this alternative proof also in some Maple worksheet? Let $Z = \{P_1 = (1:1:1), P_2 = (-2:-2:1), P_3 = (-3:-3:1), P_4 = (1:\sqrt{2}/2:0), P_5 = (1:-\sqrt{2}/2:0)\}$ be the five common real zeros of p_1, p_2 and p_3. Let $W \subset H_{3,3}$ be the linear subspace consisting of all the cubic forms vanishing in Z. By an easy linear algebra computation we obtain a basis for W,

$$\begin{aligned}\mathcal{B} =&\{w_1 = p_1, w_2 = p_2, w_3 = p_3, w_4 = x^2y - 2y^3 - 4y^2z - yz^2 + 6z^3,\\ &w_5 = x^3 - 2xy^2 - 4y^2z - yz^2 + 6z^3\}\end{aligned}$$

(note that since $H_{3,3}$ has dimension 10 and we have 5 conditions, the expected dimension for W is indeed 5).

Let $W^2 \subset H_{3,6}$ be the set of all products $\{pq : p, q \in W\}$. It is generated by the 15 products $\{w_iw_j,\ 1 \leq i \leq j \leq 5\}$, and computing syzygies among these polynomials, we find two linear relations. Hence $\dim(W^2) = 13$. We now wish to construct a linear form $\varphi : W^2 \to \mathbb{R}$ such that the associated bilinear form $\mathfrak{b} : W \times W \to \mathbb{R}$, $\mathfrak{b}(p, q) := \varphi(pq)$, has the following two properties:

(1) $\mathfrak{b}$ is positive semidefinite,
(2) the kernel of $\mathfrak{b}$ is equal to $U = \langle p_1, p_2, p_3\rangle$.

In the base $\mathcal{B}$ the matrix for $\mathfrak{b}$ must have the form

$$A = \left(\begin{array}{ccc|cc} 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0\\ \hline 0 & 0 & 0 & a & b\\ 0 & 0 & 0 & b & c\end{array}\right)$$

where the values of a, b, c have to be chosen to satisfy the linear relations between the products w_iw_j, $1 \leq i \leq j \leq 5$ in W^2. Plugging in those relations, we get a unique solution in up to linear scaling.

Setting $a = 1$ we get the matrix

$$\begin{pmatrix} a & b\\ b & c\end{pmatrix} \approx \begin{pmatrix} 1 & -1.1417\\ -1.1417 & 2.9078\end{pmatrix},$$

which is a positive definite matrix, and hence the resulting matrix A is positive semidefinite.

To conclude the proof, assume now that we have a SOS representation $f = q_1^2 + \cdots + q_r^2$. Clearly $q_i \in W$, $1 \leq i \leq r$, but then $0 = \mathfrak{b}(p_1^2) + \mathfrak{b}(p_2^2) + \mathfrak{b}(p_3^2) = \mathfrak{b}(f) = \mathfrak{b}(q_1^2) + \cdots + \mathfrak{b}(q_r^2)$. So $q_i \in \ker(\mathfrak{b}) = U$. That is, every polynomial in a SOS decomposition of f is a linear combination of p_1, p_2, p_3.

It remains to show that there is no non-trivial linear combination of p_1, p_2 and p_3 with coefficients in $\mathbb{Q}$. Indeed, we consider a generic linear combination of p_1, p_2 and p_3, $g(c_1, c_2, c_3) = w_1p_1 + w_2p_2 + w_3p_3$ and assume $g(c_1, c_2, c_3) \in \mathbb{Q}[x, y, z]$. The coefficient of x_0^3 is w_2, hence $w_2 \in \mathbb{Q}$ and the coefficient of x_1^3 is w_1, hence $w_1 \in \mathbb{Q}$. The coefficient of y^2z is $-2\alpha w_2 - 2\alpha w_3 + 2w_1$, hence $w_3 = -w_2$. Now the coefficient of x^2z is $(2\alpha - 2)w_1 - 2(\alpha^2 - 1)w_2$ and this implies $w_1 = 0$ and $w_2 = 0$. **jc:** here you are using w_i are rational numbers, while you already reserved w_i as elements in the basis $\mathfrak{B}$ □

jc: I did not verify the paragraph below. We should share a script/worksheet that shows all this. As we mentioned before, we can easily get other examples in the neighborhood of f by small perturbations of the coefficients of the construction. We analyze an example perturbing the coefficient of z

in the expression of b_3. Let $b_3 = x + tz$ and all other variables as before. The construction 1.1 yields a polynomial f with 5 real roots:

$$P_1, P_2 = (\alpha : \alpha : 1), P_3 = (-(t+2) : -(t+2) : 1), P_4, P_5 = (1 : \beta : 0),$$

where α is a root of X^2+tX-2 (note that this give two real roots for any $t \in \mathbb{R}$) and β is a root of $2X^2-1$. Repeating the above construction we obtain a positive definite matrix for any t in the interval $t \in T = (0.364425, 4.97349)$. That is, for any $t \in \mathbb{Q} \cap T$, we get a polynomial $f \in \mathbb{Q}[x, y, z]$ that can be decomposed as a sum of squares over $\mathbb{R}$ but not over $\mathbb{Q}$.

3. Quaternary Forms

We now consider the case of polynomials of degree 4 in 4 variables. We construct an example of a rational polynomial that is a sum of squares over $\mathbb{R}$ but not over $\mathbb{Q}$. In this case, the Gram spectrahedron does not consist of a single point.

Proposition 3.1. For α the real root of X^3-2, define

$$\begin{aligned} p_1 &= -4\alpha^2x^2 + 4\alpha x^2 - 2x^2 + y^2 - 2yz + 2zw - 2w^2, \\ p_2 &= -4\alpha^2x^2 - 4\alpha x^2 + 6x^2 + y^2 + 2yz + 2zw + 2w^2, \\ p_3 &= 4x(\alpha^2 w + \alpha y + z), \end{aligned}$$

polynomials in $\mathbb{Q}(\alpha)_2[x, y, z, w]$ and let $f = p_1^2 + p_2^2 + p_3^2 \in \mathbb{Q}_4[x, y, z, w]$,

$$\begin{aligned} f = {} & 40x^4 + 8x^2y^2 + 32x^2yz + 64x^2yw + 16x^2z^2 + 16x^2zw + \\ & + 32x^2w^2 + 2y^4 + 8y^2z^2 + 8y^2zw + 16yzw^2 + 8z^2w^2 + 8w^4. \end{aligned}$$

Then f cannot be decomposed as a sum of squares of polynomials in $\mathbb{Q}$.

Proof. See [**?**] for the computations in `Maple`. We have the following real vanishing points of f in $\mathbb{P}^3$ **jc:** this is written in $(x : y : z : w)$ order. Should we change it to $(w : x : y : z)$?:

$$\begin{aligned} P_1 &= (0 : 0 : 1 : 0), & P_3 &= (\gamma : \beta : -\alpha - \alpha^2\beta : 1), \\ P_2 &= (0 : 2\alpha : -\alpha^2 : 2), & P_4 &= (-\gamma : \beta : -\alpha - \alpha^2\beta : 1), \end{aligned}$$

where β is the positive real root of $X^2 + (\alpha^2 - 2\alpha)X - 1$ and $\gamma, -\gamma$ are the two (real) roots of $2X^2 + 2\alpha\beta + 1$.

If we perform facial reduction using these four points, we reduce to a 10×10 matrix Q of rank 6 in two unknowns a, b. In this case the Gram matrix is not unique, but it is still easy to see that there is no rational matrix by inspecting the entries. We observe **jc:** I did not compute the remaining observations. Do you have this in the worksheet?

$$\begin{aligned} Q_{1,9} &= 8 - (1/2)\alpha^2 a, \\ Q_{1,8} &= -(1/2)a, \end{aligned}$$

hence if Q is rational it must be $a = 0$. Substituting $a = 0$ in Q, we now observe that

$$Q_{1,5} = (27/4)\delta^{10} + 27\delta^8 + 9\delta^6 - 88\delta^4 - 24\delta^2 + 48,$$

where δ is a root of $27X^{12}+108X^{10}+36X^8-352X^6-48X^4+192X^2-64$. This polynomial is irreducible over $\mathbb{Q}$, hence $\mathbb{Q}(\delta)$ is an extension of degree 12 and therefore $Q_{1,5}$ is non–rational. □

Remark 3.2. The example was built using the following substitutions on Construction 1.1:

$$b_1 = x \quad b_2 = -x \quad b_3 = y \quad c_1 = -x \quad c_2 = -x \quad c_3 = w \quad a_3 = z.$$

The resulting polynomials p_1, p_2, p_3 have $\alpha^2 w + \alpha y + z$ as common factor, and we divided out this factor to obtain polynomials of degree 2.

As for the case of ternary sextics, we provide an alternate more geometrical proof that this polynomial cannot be decomposed as a sum of squares in $\mathbb{Q}$.

Alternative proof of Proposition 3.1. Let p_1, p_2, p_3 be as above. The polynomial p_3 splits as a product $p_3 = x \cdot l$ of two linear forms, where $l = z + \alpha y + \alpha^2 w$.

The set Z of common real zeros of p_1, p_2, p_3 therefore consists of

(1) the common real zeros Z_1 of p_1, p_2 in the plane $x = 0$;
(2) the common real zeros Z_2 of p_1, p_2 in the plane $l = 0$.

In either case, we intersect two plane conics, so we expect 4 complex zeros each. In either case, precisely two of the four are real, namely

- in case (1), Z_1 consists of the two points $P_1 = (0 : 0 : 1 : 0)$ and $P_2 = (0 : 2\alpha : -\alpha^2 : 2)$ (P_2 two non–real conjugates);
- in case (2), the four complex points are Galois conjugate to each other over $\mathbb{Q}(\alpha)$, and exactly two of them are real, i.e. in Z_2. They have coordinates

$$P_3 = (\gamma : \beta : -\alpha - \alpha^2\beta : 1), \quad P_4 = (-\gamma : \beta : -\alpha - \alpha^2\beta : 1)$$

where β is the positive real root of $X^2 + (\alpha^2 - 2\alpha)X - 1$ and $\gamma, -\gamma$ are the two (real) roots of $2X^2 + 2\alpha\beta + 1$.

To show that there is no quadratic form p over $\mathbb{Q}$ vanishing in $Z_1 \cup Z_2$, we start with Z_1. The linear space of such forms has dimension 10. Vanishing on Z_1 already gives 4 independent linear conditions on p, so there is a 6-dimensional linear space L_1 of quadratic forms over $\mathbb{Q}$ that vanish on Z_1. A linear basis for L_1 is easy to read off, namely

$$\{x^2, xy, xz, xw, yz + w^2, 2zw + y^2\}.$$

We now consider a generic form $p = a_1x^2 + a_2xy + a_3xz + a_4xw + a_5(yz + w^2) + a_6(2zw + y^2)$ and we have to find rational a_i, $1 \le i \le 6$, such that p vanishes in P_3 and P_4. Moreover, since p is rational, it must also vanish in all the 12 conjugates of these points in $\mathbb{Q}(\alpha, \beta, \gamma)$. This gives us 12 equations and we can verify in `Maple` that the only solution is the trivial solution $p \equiv 0$. We conclude that no rational quadratic form vanishes in Z and hence f admits no $\mathbb{Q}$-SOS decomposition. **jc:** could you provide the link to the Maple verification. □

3.1. **Examples over more general algebraic extensions.** We want to generalize the above construction to any radical real field extension of $\mathbb{Q}$ of degree 3, i.e. we want to achieve the same results by assuming α is the real root of $X^3 - s$ for a positive non-cube $s \in \mathbb{Q}$. Using the same substitution of linear forms as in Remark 3.2 we obtain a positive polynomial (parameterized by s)

$$\begin{aligned} f = {} & 8s^2x^4 + 8s^2x^2w^2 + 2s^2w^4 + 16sx^2yz + 32sx^2yw + 8syzw^2 \\ & + 8x^4 + 8x^2y^2 + 16x^2z^2 + 16x^2zw + 2y^4 + 8y^2z^2 + 8y^2zw + 8z^2w^2 \end{aligned}$$

which is the sum of squares of the following three polynomials:

$$\begin{aligned} p_1 &= -2sx^2 - sw^2 - 4\alpha^2x^2 + 4\alpha x^2 + 2x^2 + y^2 - 2yz + 2zw, \\ p_2 &= 2sx^2 + sw^2 - 4\alpha^2x^2 - 4\alpha x^2 + 2x^2 + y^2 + 2yz + 2zw, \\ p_3 &= 4x(\alpha^2w + \alpha y + z). \end{aligned}$$

One can check that the the conjugates of the following points define $Z(p_1, p_2, p_3)$:

$$\begin{aligned} P_1 &= (0 : 0 : 1 : 0) \\ P_2 &= (0 : 2\alpha : -\alpha^2 : 2) \\ P_3 &= (\gamma : \beta : -\alpha^2 - \alpha\beta : 1) \end{aligned}$$

where we take

- $\alpha = \alpha(s)$ to be the positive real root of $X^3 - s$ (recall that s is a positive non-cube rational number),
- $\beta = \beta(\alpha, s)$ to be a real root of $\alpha X^2 + (2\alpha^2 - 2)X - \alpha$,
- $\gamma = \gamma(\alpha, \beta, s)$ to be a real root of $2sX^2 + s + 2\beta\alpha^2$.

For any $\alpha \in \mathbb{R}$, we have the following choices for β:

$$\begin{aligned} -(\alpha - \alpha^{-1}) + \sqrt{(\alpha - \alpha^{-1})^2 + 1} > 0, \\ -(\alpha - \alpha^{-1}) - \sqrt{(\alpha - \alpha^{-1})^2 + 1} < 0, \end{aligned}$$

but only the negative choice of β will give us a real root of $2sX^2 + s + 2\beta\alpha^2$. For this choice of β and α there are exactly two real roots $\gamma, -\gamma$ of $2sX^2 + s + 2\beta\alpha^2$ or equivalently of $2\alpha X^2 + \alpha + 2\beta$. Thus, in total there are four real points in $Z(p_1, p_2, p_3)$.

We claim that no quadratic form in $\mathbb{Q}[x, y, z, w]$ will have P_1, P_2, P_3 and P_4 in its set of zeros. If we look at the evaluation of the vector of monomials of degree 2 at these points in $\mathbb{P}^9$ (i.e. the image of these points under the Veronese map $v := v_{2,3}$) we obtain

$$\begin{aligned} v(P_1) &= (0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1) \\ v(P_2) &= (4 : 0 : 4\alpha : -2\alpha^2 : 0 : 0 : 0 : 4\alpha^2 : -2s : s\alpha) \\ v(P_3) &= (s : s\gamma : s\beta : -(\alpha + \beta)s\alpha : -\alpha^2\beta - s/2 : s\beta\gamma : -(\alpha + \beta)s\alpha\gamma \\ &\quad : -2s\alpha\beta + 2\alpha^2\beta + s : (\alpha^2\beta - \alpha - 2\beta)s : (s + \alpha + 2\beta)s\alpha) \end{aligned}$$

Let Q be a hyperplane in $\mathbb{P}^9(K)$, $Q = \{\boldsymbol{x} \in \mathbb{P}^9(K) : \boldsymbol{c} \cdot \boldsymbol{x} = 0\}$, where $\boldsymbol{c} := (c_0 : \ldots : c_9)$. We claim that there is no $\mathbb{Q}$-rational hyperplane Q that contain the points $v(P_1), \ldots, v(P_4)$.

We assume, by contradiction, that Q is $\mathbb{Q}$-rational containing all these points. We take advantage of the fact that $\mathbb{Q}(\alpha, \beta, \gamma)$ is a 12-dimensional $\mathbb{Q}$-algebra generated by α, β, γ. and as a $\mathbb{Q}$-vector-space it is spanned by a basis

$$1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta, \gamma, \alpha\gamma, \alpha^2\gamma, \beta\gamma, \beta\alpha\gamma, \alpha^2\beta\gamma.$$

We iteratively show that all the coefficients c_i must be 0 leading to a contradiction. From $\boldsymbol{c} \cdot v(P_1) = 0$ we know that $c_9 = 0$. We look now at $\boldsymbol{c} \cdot v(P_3) = 0$. Since γ appears only in the second coordinate, we conclude that $c_1 = 0$. A similar argument for $\alpha^2, \beta\gamma$ and $\alpha^2\gamma$ yields $c_3 = 0, c_5 = 0$ and $c_6 = 0$ respectively. All these zero coordinates lead us to conclude that $c_2 = 2c_8$ (for β), $-c_4 + 2c_7 + sc_8 = 0$ (for $\alpha^2\beta$) and $c_0 - sc_4/2 + sc_7 = 0$ (for 1). We can continue this argument with $\boldsymbol{c} \cdot v(P_2)$ knowing many coordinates that are already 0 and get $c_2 = 0$ (for α) and show that the remaining coordinates are also 0. Thus we conclude that Q cannot be $\mathbb{Q}$-rational.

4. General Construction and Geometric Proof

To study the higher degree number fields we generalize Construction 1.1. Let $d \geq 3$ and consider α to be a d-th real root of a prime number. We want to find $q_i \in \mathbb{Q}(x, y, z)[\alpha]$ of degree $d - 1$ over α, i.e.

$$q_i := \sum_{j=1}^{d} a_{i,j}\alpha^{j-1} \quad i = 1, \ldots, d \quad a_{i,j} \in \mathbb{Q}(x, y, z),$$

by solving solving for the coefficients $a_{i,j}$ upon imposing the condition that $\sum_{i=1}^{d} q_i^2 \in \mathbb{Q}(x, y, z)$. We have an underdetermined system of $d - 1$ polynomial equations (coefficients of $\alpha, \alpha^2, \ldots, \alpha^{d-1}$) that are quadratic in the $a_{i,j}$'s with $j \neq 1$ and linear in the $a_{i,1}$'s. We choose generic linear forms for the $a_{i,j}$'s with $j \neq 1$ and choose also a generic linear form for $a_{1,1}$. We will call these chosen linear forms the *initial forms*. We can then solve for the $a_{i,1}$'s with $i \neq 1$. This yields $a_{i,1}$'s that are rational functions in $\mathbb{Q}(x, y, z)$ with a common denominator $q(x, y, z)$ with $\deg q = d - 1$. It is almost clear from the construction that q is the determinant of $B := (a_{i,j})_{2 \leq i,j \leq d}$. Thus, because the choice of initial forms were generic, q cannot be identical to 0.

Let now $b_{i,j} = qa_{i,j}$, then

$$p_i := \sum_{j=1}^{d} b_{i,j}\alpha^{j-1} \quad i = 1, \ldots, d$$

satisfy $\sum_{i=1}^{d} p_i^2 \in \mathbb{Q}[x, y, z]$. These p_i are degree d forms. Moreover, the polynomial p_1 is the product of a linear form and a degree $d - 1$ form. We do not elaborate on this procedure as it is just Construction 1.1 when $d = 3$. Notice that when $d = 3$, p_3 can be obtained from p_2 by swapping $(a_{3,2}, a_{3,3})$ with $-(a_{2,2}, a_{2,3})$ (compare with Construction 1.1 and Example 4.2).

One remarkable fact about the above construction is that $Z(p_i)$, as curves on the projective plane over $\overline{\mathbb{Q}}$, will have common points.

Theorem 4.1. For the above general construction $Z(p_1, \ldots, p_d)$ in $\mathbb{P}^2(\overline{\mathbb{Q}})$ will have

$$m(d) := \binom{d+1}{2} - 1$$

points

Example 4.2. Here is an example with a general construction for $d = 3$. The initial forms are

$$\begin{aligned} a_{1,1} = x \quad a_{1,2} = y \quad a_{1,3} = z \\ a_{2,2} = 3y + z \quad a_{2,3} = -x - 3y - 3z \\ a_{3,2} = x - y + 3z \quad a_{3,3} = x + 2y - 3z \end{aligned}$$

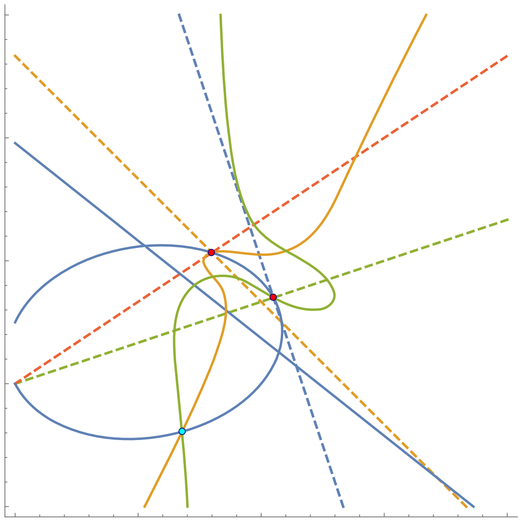
Thus

$$B = \begin{pmatrix} 3y + z & -x - 3y - 3z \\ x - y + 3z & x + 2y - 3z \end{pmatrix}$$

The resulting polynomials are

$$\begin{aligned} p_1 &= (x + y\alpha + z\alpha^2)(2x^2 + 10xy + 14xz + 6y^2 - 2yz + 12z^2) \\ p_2 &= -5x^3 - 23x^2y + x^2z - 59xy^2 - 12xyz - 72xz^2 - 77y^3 - 27y^2z - 286yz^2 + 84z^3 \\ &\quad + (6x^2y + 2x^2z + 30xy^2 + 52xyz + 14xz^2 + 18y^3 + 34yz^2 + 12z^3)\alpha \\ &\quad + (2x^3 + 8x^2y + 20x^2z - 4xy^2 + 14xyz + 54xz^2 - 6y^3 + 20y^2z - 18yz^2 + 36z^3)\alpha^2 \\ p_3 &= 4x^3 - x^2y + 11x^2z - 14xy^2 - 48xyz + 30xz^2 - 67y^3 - 25y^2z - 200yz^2 + 104z^3 \\ &\quad + (-2x^3 - 16x^2y - 20x^2z - 36xy^2 - 70xyz - 54xz^2 - 18y^3 - 12y^2z - 30yz^2 - 36z^3)\alpha \\ &\quad + (2x^3 + 14x^2y + 8x^2z + 26xy^2 - 4xyz - 30xz^2 + 12y^3 - 22y^2z + 30yz^2 - 36z^3)\alpha^2 \end{aligned}$$

Observe that $Z(p_1)$ is the union of a line and the non-degenerate conic section $Z(q)$, while $Z(p_i)$ for $i = 2, 3$ are smooth cubics on the plane. We plot the real points of each of these curves, including the zeros of $a_{i,j}$ for $2 \leq i, j \leq 3$ (i.e. the zeros of the entries of B, which are illustrated as dashed lines).



Investigating further shows us that $Z_{\bar{\mathbb{Q}}}(p_1, p_2, p_3) = Z_{\bar{\mathbb{Q}}}(q, p_2, p_3)$ and indeed, as stated in Theorem 4.1, it consists of $m(3) = 5$ points! Only one of these 5 points in $\mathbb{P}^2(\overline{\mathbb{Q}})$ is real and this is indicated by the blue dot in the figure. There are two red dots lying on $Z(q)$, one of them is $Z(a_{2,2}, a_{2,3})$ and the other is $Z(a_{3,2}, a_{3,3})$

The above observation gives us an intuition for proving Theorem 4.1 especially when $d = 3$

4.3. Let us look more explicitly on how $b_{i,1}$ $(i > 1)$ is computed. In the beginning we have a system of linear equations in the $a_{i,1}$ for $i \geq 2$ i.e.

$$B^\top \begin{pmatrix} a_{2,1} \\ \vdots \\ a_{d,1} \end{pmatrix} = \begin{pmatrix} c_2 \\ \vdots \\ c_d \end{pmatrix}$$

where c_j $(j \geq 2)$ are polynomials in the initial forms i.e. $a_{i,j}$ with either $j \neq 1$ or $(i,j) = (1,1)$. We obtain $b_{i,1}$ via

$$\begin{pmatrix} b_{2,1} \\ \vdots \\ b_{d,1} \end{pmatrix} = \operatorname{adj}(B^\top) \begin{pmatrix} c_2 \\ \vdots \\ c_d \end{pmatrix}$$

Note that each entry of the adjugate matrix $\operatorname{adj}(B^\top)$ is of degree $d-2$. We then get

$$p_i = \tilde{b}_{i,2}c_2 + \tilde{b}_{i,3}c_3 + \dots \tilde{b}_{i,d}c_d + q \sum_{j=2}^{d} a_{i,j}\alpha^{j-1} \qquad i \geq 2 \tag{1}$$

where $(\tilde{b}_{i,2}, \dots, \tilde{b}_{i,d})$ is the $(i-1)$-th row of $\operatorname{adj}(B^\top)$.

4.4. Let us now prove Theorem 4.1 for $d = 3$. Since the terms with q in Equation (1) are independent of $a_{1,1}$, we can easily conclude that $Z(a_{1,1}, p_2, p_3) = \emptyset$. Thus $Z(p_1, p_2, p_3) = Z(q, p_2, p_3)$. By Bézout, $Z(q, p_i)$ for $i = 2, 3$ will have 6 points. It suffices to explain how 5 out of these 6 points are the common points of the three curves $Z(q)$, $Z(p_2)$ and $Z(p_3)$.

We can explicity write

$$\operatorname{adj}(B^\top) = \begin{pmatrix} a_{3,3} & -a_{3,2} \\ -a_{2,3} & a_{2,2} \end{pmatrix}$$

and we are interested in the rows of this matrix. Consider the intersection point P of the two lines $a_{3,3} = 0$ and $a_{3,2} = 0$. This point is also in $Z(p_2, q)$. Symbolically c_2 and c_3 has terms in the initial forms that does not consist of $a_{3,3}$ and $a_{3,2}$. Therefore, by the general choice of the initial forms, the vector $(c_2, c_3)(P)$ is not orthogonal to $(a_{3,3}, -a_{3,2})(P)$. This rules out one of the 6 points in $Z(q, p_2)$. We claim that any point in $Q \in Z(p_2, q)$ with $Q \neq P$ is also a point of the cubic curve $Z(p_3)$. The entries of B are generic linear forms and so $q = 0$ must be a smooth conic section so that the specialization $B(Q)$ is a singular matrix with corank 1 and the kernel of $B^\top(Q)$ is spanned by a non-trivial row of the $\operatorname{adj}(B^\top)(Q)$ (e.g. see Lemma 4.5b.)). In other words, $(a_{3,3}, -a_{3,2})(Q)$ and $(-a_{2,3}, a_{2,2})(Q)$ (by the general construction, this second vector is non-zero as well) differ by a non-zero scalar factor. We have therfore proven that $(c_2, c_3)(Q)$ is orthognal to both of these vectors and this implies that $p_2(Q) = p_3(Q)$.

The above proof for $d = 3$ could be made easier by some cross-ratio argument. But we want to emphasize the fact that a non-trivial row of $\operatorname{adj}(B^\top)$ evaluated at Q spans the kernel of the corank 1 matrix $B^\top(Q)$. This becomes more relevant in the proof for arbitrary d. To prove the general case we make use of the following lemma

Lemma 4.5. Let A be a $n \times n$ matrix ($n \geq 2$) with entries being generic linear forms in $\mathbb{C}[x, y, z]$. We then have

a.) The zero set of $\det A$ is a smooth planar projective curve.

b.) Let $P \in Z(\det A)$, the specialization $A(P)$ is a corank 1 matrix and its kernel is spanned by a non-trivial row of $\operatorname{adj}(A)$.

c.) Let $\boldsymbol{v}$ be a row of $\operatorname{adj}(A)$, then

$$\#\{P \in \mathbb{P}^2(\mathbb{C}) \,:\, \boldsymbol{v}(P) = \boldsymbol{0}\} = \frac{n(n-1)}{2}$$

Proof. Smoothness is an immediate result of the fact that a determinantal variety is non-singular in codimension 1 (see [**?**] §II) and Bertini's theorem ($Z(\det A)$ is the section of a determinantal variety with a plane in general position). Hence, the second statement follows from [**?**] Lemma 2.1 and its proof.

Consider now a point $P \in \mathbb{P}^2(\mathbb{C})$ that satsfies $\boldsymbol{v}(P) = \boldsymbol{0}$, where $\boldsymbol{v}$ is the i-th row of $\operatorname{adj}(A)$. This means that the $(n-1) \times n$ submatrix of $A(P)$ without the i-th row are linearly dependent i.e. have rank $\leq (n-2)$. Because the entries of the matrix are generic linear forms, the number of points at which the row $\boldsymbol{v}$ is zero, is the number of the points of the determinantal variety $M_{n-2}(n-1, n)$ (the points of this variety corresponds to $(n-1) \times n$ matrices whose corank is ≥ 2) intersected with a general plane on the space of matrices. It is known that $M_{n-2}(n-1, n)$ has codimension 2, therefore the intersection with a general plane is finite. This number is exactly the degree of $M_{n-2}(n-1, n)$. By the Porteous formula the degree is $\binom{n}{2}$ (see [**?**] Prop. 12 or [**?**] §II.5). □

Proof of Theorem 4.1. Similar to the proof for $d = 3$ in 4.4, we will rule out the points in $Z(q, p_2)$ for which the first row of $\operatorname{adj}(B^\top)$ vanishes at these points. By Lemma 4.5c.) there are $\binom{d-1}{2}$ such points. The rest of the proof uses exactly the same argument as the proof for $d = 3$ following Lemma 4.5b.). We thus have

$$m(d) = \#Z(q, p_2) - \binom{d-1}{2} = d(d-1) - \binom{d-1}{2} = \binom{d+1}{2} - 1$$

□

References

1. Grigoriy Blekherman, *Nonnegative polynomials and sums of squares*, Semidefinite optimization and convex algebraic geometry, MOS-SIAM Ser. Optim., vol. 13, SIAM, Philadelphia, PA, 2013, pp. 159–202. MR 3050243
2. Grigoriy Blekherman, Jonathan Hauenstein, John Christian Ottem, Kristian Ranestad, and Bernd Sturmfels, *Algebraic boundaries of Hilbert's SOS cones*, Compos. Math. **148** (2012), no. 6, 1717–1735. MR 2999301
3. Jose Capco and Claus Scheiderer, *Two remarks on sums of squares with rational coefficients*, arXiv e-prints (2019), arXiv:1905.13282.

4. Santiago Laplagne, *Facial reduction for exact polynomial sum of squares decompositions*, Mathematics of Computation (2018), to appear.
5. F. Lemaire, Moreno Maza, and Y. Xie, *`RegularChains`, a Maple package for solving systems of algebraic equations and inequations*, 2005.
6. Claus Scheiderer, *Sums of squares of polynomials with rational coefficients*, J. Eur. Math. Soc. (JEMS) **18** (2016), no. 7, 1495–1513. MR 3506605
7. Inc. Wolfram Research, *`Cylindrical Algebraic Decomposition`, a Mathematica package for solving systems of algebraic equations and inequations*, 2005.

Universität Innsbruck - Austria
Email address: `jose.capco@uibk.ac.at`

Departamento de Matemática, FCEN, Universidad de Buenos Aires - Ciudad Universitaria, Pabellón I - (C1428EGA) - Buenos Aires, Argentina
Email address: `slaplagn@dm.uba.ar`

Universität Konstanz - Germany
Email address: `claus.scheiderer@uni-konstanz.de`