Journal of Pure and Applied Algebra 225 (2021) 106608

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

# A note on mediated simplices

Victoria Powers [a,*], Bruce Reznick [b]

[a] Department of Mathematics, Emory University, Atlanta, GA 30322, United States of America
[b] Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801, United States of America

ARTICLE INFO

*Article history:*
Available online 19 October 2020

*MSC:*
11E76; 52B20

ABSTRACT

Many homogeneous polynomials that arise in the study of sums of squares and Hilbert's 17th problem are those formed by monomial substitutions into the arithmetic-geometric inequality. In 1989, Reznick [14] gave a necessary and sufficient condition for such a form to have a representation as a sum of squares of forms, involving the arrangement of lattice points in the simplex whose vertices were the $n$-tuples of the exponents used in the substitution. Further, a claim was made, and not proven, that sufficiently large dilations of any such simplex will also satisfy this condition. The aim of this short note is to prove the claim, and provide further context for the result, both in the study of Hilbert's 17th Problem and the study of lattice point simplices.



## 1. Introduction

In 1989, the second author considered [14] a class of homogeneous polynomials (forms) which had arisen in the study of Hilbert's 17th Problem as monomial substitutions into the arithmetic-geometric inequality. The goal was to determine when such a form, which must be positive semidefinite, had a representation as a sum of squares of forms. The answer was a necessary and sufficient condition involving the arrangement of lattice points in the simplex whose vertices were the $n$-tuples of the exponents used in the substitution. Further, a claim was made in [14], and not proven, that sufficiently large dilations of any such simplex will also satisfy this condition. The aim of this short note is to prove the claim, and provide further context for the result, both in the study of Hilbert's 17th Problem and the study of lattice point simplices. The second author is happy to acknowledge that the return to this claim was triggered by two nearly simultaneous events: an invitation to speak at the 2019 SIAM Conference on Applied Algebraic Geometry, and a request

* Corresponding author.
*E-mail addresses:* vpowers@emory.edu (V. Powers), reznick@illinois.edu (B. Reznick).

https://doi.org/10.1016/j.jpaa.2020.106608
0022-4049/

from Jie Wang for a copy of [15], which was announced in [14] but never written. The second author was supported in part by Simons Collaboration Grant 280987.

## 2. Preliminaries

We work with homogeneous polynomials (forms) in $\mathbb{R}[x] = \mathbb{R}[x_1, \dots, x_n]$, the ring of real polynomials in $n$ variables. Write the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ as $x^\alpha$, for $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n$. For $S \subset \mathbb{Z}^n$, $cvx(S)$ denotes the convex hull of $S$. For $p(x) = \sum_\alpha c(\alpha) x^\alpha \in \mathbb{R}[x]$, let $\mathrm{supp}(p) = \{\alpha \mid c(\alpha) \neq 0\}$, write $\mathrm{New}(p)$ for the *Newton polytope* of $p$, that is, $\mathrm{New}(p) = cvx(\mathrm{supp}(p))$, and let $C(p) = \mathrm{New}(p) \cap \mathbb{Z}^n$.

A form $p \in \mathbb{R}[x]$ is *positive semidefinite* or *psd* if $p(x) \geq 0$ for all $x \in \mathbb{R}^n$. It is a *sum of squares* or *sos* if $p = \sum_j h_j^2$ for forms $h_j \in \mathbb{R}[x]$. Clearly, every sos form is psd. In 1888, D. Hilbert [8] proved that there exist psd forms which are not sos.

The *arithmetic-geometric inequality* (or *AGI*) states that if $t_i \geq 0$, $\lambda_i \geq 0$ and $\sum_{i=1}^n \lambda_i = 1$, then

$$\lambda_1 t_1 + \cdots + \lambda_n t_n \geq t_1^{\lambda_1} \cdots t_n^{\lambda_n},$$

with equality only if the $t_i$'s are equal. In 1891, A. Hurwitz [9] gave a proof of the AGI, in which the key step was setting $\lambda_i = a_i/N$ where $a_i \in \mathbb{Z}^n$ with $\sum a_i = N$ for even $N$, and $t_i = x_i^N$. Under this substitution and a scaling, one obtains the form

$$a_1 x_1^N + \cdots + a_n x_n^N - N x_1^{a_1} \cdots x_n^{a_n}.$$

Hurwitz then proves that each such form is sos (in fact, a sum of squares of binomials), and hence psd. (He cites [8] to observe that this is not automatic.) For example, after a scaling and relabeling of the $x_i$'s as $x, y, z$, we have

$$\begin{aligned} H(x,y,z) &:= x^6 + y^6 + z^6 - 3x^2y^2z^2 \\ &= \tfrac{3}{2}(x^2y - yz^2)^2 + (x^3 - xy^2)^2 + \tfrac{1}{2}(x^2y - y^3)^2 + (z^3 - y^2z)^2 + \tfrac{1}{2}(yz^2 - y^3)^2. \end{aligned}$$

For more on Hurwitz' proof, see [13], where Eq. (3.5) gives a representation of $H$ as a sum of four squares, one of which is the square of a trinomial.

The first explicit example of a psd form which is not sos was presented in 1967 by T. Motzkin [11]. It, too, arises as a substitution into the AGI: let $t_1 = x^4y^2, t_2 = x^2y^4, t_3 = z^6$, $\lambda_i = \frac{1}{3}$ and scale:

$$M(x,y,z) := x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2.$$

The proof that $M$ is not sos was based on a preliminary argument that if $M = \sum h_j^2$, then $h_j(x,y,z) = c_{1j}x^2y + c_{2j}xy^2 + c_{3j}z^3 + c_{4j}xyz$: the coefficient of $x^2y^2z^2$ in $\sum h_j^2$ is then $\sum c_{4j}^2 \neq -3$. The argument of Motzkin's proof was formalized in [12], where it is shown that, in general, $p = \sum h_j^2$ implies that $C(h_j) \subseteq \frac{1}{2}C(p)$.

The following machinery was developed in [12,14] to analyze such forms. Consider a set $\mathcal{U} = \{u_1, \dots, u_m\}$ with $u_i \in (2\mathbb{Z}_{\geq 0})^n$ and $\sum_{j=1}^m u_{ij} = 2d$. We further assume that $cvx(\mathcal{U})$ is a simplex, and $w \in cvx(\mathcal{U}) \cap \mathbb{Z}^n$ has the barycentric representation $w = \sum \lambda_i u_i$, $\lambda_i \geq 0$ and $\sum_{i=1}^m \lambda_i = 1$. In this way, the substitution $\{t_i = x^{u_i}\}$ into the AGI yields a psd form of degree 2d,

$$p(x) = \lambda_1 x^{u_1} + \cdots + \lambda_m x^{u_m} - x^w.$$

This was called an *agiform* in [14] and the set $\mathcal{U}$ was called a *trellis*. Observe that $C(p) = cvx(\mathcal{U}) \cap \mathbb{Z}^n$. More generally, a polynomial $p(x) = \sum_{i=1}^m a_i x^{u_i} - bx^w$ with $a_i > 0$ for $i = 1, \dots, m$ is called a *circuit polynomial*.

Circuit polynomials have recently been studied by M. Dressler, J. Forsgård, S. Iliman, T. de Wolff, and J. Wang; see for example [10], [2], [3], [16]. Interest in circuit polynomials is in part due to their use in finding efficiently-computable certificates of positivity based on the AGI, which are then independent of sos representations.

There is a geometric criterion which determines whether an agiform is sos.

**Definition.** Suppose $\mathcal{U}$ is given as above, and let $S \subset cvx(\mathcal{U}) \cap \mathbb{Z}^n$ be a set of lattice points containing the $u_i$'s. Then $S$ is *$\mathcal{U}$-mediated* if for every $y \in S$, either $y = u_i$ for some $i$, or there exist $z_1 \neq z_2 \in S \cap (2\mathbb{Z})^n$ so that $y = \frac{1}{2}(z_1 + z_2)$. In other words, $S$ is $\mathcal{U}$-mediated if every point in $S$ is either a vertex of $\mathcal{U}$ or an average of two different even points in $S$.

**Theorem 2.1.** *[14, Cor. 4.9] With $\mathcal{U}, \lambda_i$ as above, the agiform $\lambda_1 x^{u_1} + \cdots + \lambda_m x^{u_m} - x^w$ is sos if and only if there is a $\mathcal{U}$-mediated set containing $w$.*

Let $\mathcal{U}_1 = \{(4,2,0), (2,4,0), (0,0,6)\}$ and $\mathcal{U}_2 = (\{(6,0,0), (0,6,0), (0,0,6)\}$. Up to scaling, both $H$ and $M$ are agiforms, since $w = (2,2,2)$ is the centroid to both $cvx(\mathcal{U}_1)$ and $cvx(\mathcal{U}_2)$. By Theorem 2.1, $M$ is not sos because $cvx(\mathcal{U}_1) \cap (2\mathbb{Z})^3 = \{u_1, u_2, u_3, w\}$ and it is impossible to write $w$ as an average of two different members of this set. However, it is easy to check that the set

$$S = \{(6,0,0), (0,6,0), (0,0,6), (2,2,2), (4,2,0), (2,4,0), (0,2,4), (0,4,2)\}$$

is $\mathcal{U}_2$-mediated, providing an independent proof that $H$ is sos.

We refer the reader to [14] for the separate proofs of the necessity and sufficiency in Theorem 2.1.

## 3. Main theorem

The following theorem was asserted in [14, Prop. 2.7].

**Theorem 3.1.** *For every integer $k \geq \max\{2, m-2\}$, $cvx(k\mathcal{U}) \cap \mathbb{Z}^n$ is $(k\mathcal{U})$-mediated.*

**Corollary 3.2.** *Any agiform $p \in \mathbb{R}[x_1, \ldots, x_n]$ can be written as a sum of squares of forms in the variables $x_i^{1/k}$ for $k \geq \max\{2, m-2\}$.*

To prove Theorem 3.1, we show that any non-vertex $w \in cvx(k\mathcal{U}) \cap \mathbb{Z}^n$ is the average of two different points in $cvx(k\mathcal{U}) \cap (2\mathbb{Z})^n$. The proof for $k \geq m-1$ is easy, while the proof for the remaining case ($m \geq 4$ and $k = m-2$) is more delicate. We defer the discussion of Corollary 3.2 to the next section.

We start with some notation and lemmas. First, recall that $t \in \mathbb{R}$ may be written as $t = \lfloor t \rfloor + \{t\}$, where $\lfloor t \rfloor \in \mathbb{Z}$ and $\{t\} \in [0,1)$. If $v = \sum a_i u_i \in cvx(k\mathcal{U})$ with $a_i \in \mathbb{Z}_{\geq 0}, \sum a_i = k$, then we say that $v$ is a *bead*. Observe that beads are always even.

**Lemma 3.3.** *Suppose $k > 1$ and $v \in cvx(k\mathcal{U})$ is a non-vertex bead. Then $v$ is an average of two different beads in $cvx(k\mathcal{U})$.*

**Proof.** Suppose that $v = \sum a_i u_i$ is a non-vertex bead. At least two of the $a_i$'s must be positive; without loss of generality, suppose $a_1, a_2 \geq 1$. Then $v$ is the average of the beads $v \pm (u_1 - u_2)$ in $cvx(k\mathcal{U})$. □

**Lemma 3.4.** *Suppose non-negative integers $b_i$ and $S$ are given and $\sum_{i=1}^m b_i = R$. If $S \leq R$, then there exist non-negative integers $a_i$ so that $a_i \leq b_i$ and $\sum_{i=1}^m a_i = S$.*

**Proof.** Define the partial sums $s_k := \sum_{i=1}^{k} b_i$ and choose the largest $k$ so that $s_k \leq S$. Then set $a_i = b_i$ for $i = 1, \ldots, k$; $a_{k+1} = S - s_k$; and $a_j = 0$ for $j = k+2, \ldots, m$. $\square$

**Lemma 3.5.** *Suppose $k$ is a positive integer and $w \in cvx(k\mathcal{U}) \cap (\mathbb{Z})^n$, say $w = \sum_{i=1}^{m} \lambda_i (ku_i)$ with $\sum \lambda_i = 1$. If $w$ is not a bead and $k \leq \sum_{i=1}^{m} \lfloor 2k\lambda_i \rfloor$, then $w$ is the average of two different points in $cvx(k\mathcal{U}) \cap (2\mathbb{Z})^n$.*

**Proof.** By Lemma 3.4, there exist $a_i \in \mathbb{Z}_{\geq 0}$ with $\sum a_i = k$ and $a_i \leq \lfloor 2k\lambda_i \rfloor$. Let $v = \sum a_i u_i$, then $v$ is a bead, hence even. Since $w$ is not a bead, $w \neq v$ and hence $v \neq 2w - v$. Thus $w = \frac{1}{2}(v + (2w - v)) = \sum_i (2k\lambda_i - a_i)u_i$ is the average of two different even points in $cvx(k\mathcal{U}) \cap \mathbb{Z}^n$. $\square$

**Proof of Theorem 3.1.** Suppose $w \in cvx(k\mathcal{U}) \cap \mathbb{Z}^n$ is not a vertex, then we must show that $w$ is an average of two different points in $cvx(k\mathcal{U}) \cap (2\mathbb{Z})^n$. If $w$ is a bead, we are done by Lemma 3.3, so assume that $w$ is not a bead.

Since $w \in cvx(k\mathcal{U})$, $w = \sum_{i=1}^{m} \lambda_i (ku_i)$ with $\lambda_i \geq 0$, $\sum \lambda_i = 1$. Let $\beta_i = k\lambda_i$, then $w = \sum_{i=1}^{m} \beta_i u_i$; since $w$ is not a bead, at least one $\beta_i \notin \mathbb{Z}$. We have $\sum \beta_i = k$, hence $\sum_{i=1}^{m} \lfloor 2\beta_i \rfloor > \sum_{i=1}^{m} (2\beta_i - 1) = 2k - m$ and since the $\lfloor 2\beta_i \rfloor$'s and $2k - n$ are integers, a strict inequality implies a gap of at least 1. Then

$$\sum_{i=1}^{m} \lfloor 2\beta_i \rfloor \geq 2k - m + 1.$$

If $k \geq m - 1$, then $2k - m + 1 = k + (k - (m-1)) \geq k$ and hence, by Lemma 3.5, $w$ is the average of two different points in $cvx(k\mathcal{U}) \cap (2\mathbb{Z})^n$.

We are left with the case $k < m - 1$. In this case, the hypothesis $k \geq \max\{2, m-2\}$ implies $m \geq 4$ and thus $k = m - 2$. If $\sum_{i=1}^{m} \lfloor 2\beta_i \rfloor \geq m - 2$, then we can apply Lemma 3.5 and we are done. Suppose $\sum_{i=1}^{m} \lfloor 2\beta_i \rfloor < m - 2$, then $2k - m + 1 = m - 3$ implies $\sum_{i=1}^{m} \lfloor 2\beta_i \rfloor = m - 3$. This implies

$$\sum_{i=1}^{m} \{2\beta_i\} = \sum_{i=1}^{m} (2\beta_i - \lfloor 2\beta_i \rfloor) = 2(m-2) - (m-3) = m - 1.$$

Since each $\{2\beta_i\} < 1$, it follows that none of the summands is zero; that is, $2\beta_i \notin \mathbb{Z}$. Further, $\sum_{i=1}^{m} (1 - \{2\beta_i\}) = m - (m-1) = 1$, and each $1 - \{2\beta_i\}$ is positive. Define

$$\tilde{u} := \sum_{i=1}^{m} (1 - \{2\beta_i\})u_i = \sum_{i=1}^{m} (1 - (2\beta_i - \lfloor 2\beta_i \rfloor))u_i = \sum_{i=1}^{m} (1 + \lfloor 2\beta_i \rfloor)u_i - 2w.$$

Then $\tilde{u}$ is strictly interior to $cvx(\mathcal{U})$ (since $1 - \{2\beta_i\} > 0$) and is also an even point.

If $w = (m-2)\tilde{u}$,

$$w = (m-2)\tilde{u} = (m-2)\left( \sum_{i=1}^{m} (1 + \lfloor 2\beta_i \rfloor)u_i - 2w \right) \implies$$

$$(2m-3)w = (m-2)\left( \sum_{i=1}^{m} (1 + \lfloor 2\beta_i \rfloor)u_i \right) = (m-2)y,$$

for some bead $y \in cvx((2m-3)\mathcal{U})$. Let $d_i := 1 + \lfloor 2\beta_i \rfloor \geq 0$, so that $\tilde{u} = \sum_{i=1}^{m} \frac{d_i}{2m-3} u_i$, where $1 \leq d_i \in \mathbb{Z}$ and $\sum_i d_i = 2m - 3$. Since $m \geq 4$, $2m - 3 > m$, thus at least one of the $d_i$'s is $> 1$. Without loss of generality assume that $d_1 \geq 2$.

We now note that $w = (m-2)\tilde{u}$ is the average of $(m-3)\tilde{u} + u_1$ and $(m-1)\tilde{u} - u_1$, both of which are evidently even points. The first is obviously in $cvx((m-2)\mathcal{U})$. The second, $(m-1)\tilde{u} - u_1$, can be written as

$$(m-1)\left(\sum_{i=1}^{m}\frac{d_i}{2m-3}u_i\right)-u_1=\left(\frac{(m-1)d_1}{2m-3}-1\right)u_1+\sum_{i=2}^{m}\frac{(m-1)d_i}{2m-3}u_i.$$

Since $d_1\geq 2$, the coefficient of $u_1$ is $\geq \frac{2m-2}{2m-3}-1>0$. Thus, $(m-1)\tilde{u}-u_1$ is in $cvx((m-2)\mathcal{U})$, so $w$ is an average of two different even points in $cvx((m-2)\mathcal{U})$.

If $w\neq(m-2)\tilde{u}$, then since $\tilde{u}$ is an interior point of $cvx(\mathcal{U})$, we can form the trellises

$$\mathcal{U}_1=\{\tilde{u},u_2,\ldots,u_m\},\mathcal{U}_2=\{u_1,\tilde{u},u_3,\ldots,u_m\},\ldots,\mathcal{U}_m=\{u_1,\ldots,u_{m-1},\tilde{u}\}.$$

Then $w$ must be in the interior of one of $cvx((m-2)\mathcal{U}_i)$, without loss of generality assume it is $cvx((m-2)\mathcal{U}_1)$. Repeating the process above, we have either that $w$ is the average of two different even points in $cvx((m-2)\mathcal{U}_1)$ and we are done, or $w=\beta_1\tilde{u}+\sum_{i=2}^{m}\beta_i u_i$ with $\beta_i=(m-2)\lambda_i$ and $\sum\lambda_i=1$. If $\sum_{i=1}^{m}\lfloor 2\beta_i\rfloor\geq m-2$, we are done as above. If not, we can construct a strictly interior point of $\mathcal{U}_1$ and subdivide $\mathcal{U}_1$ using this point. The process of subdivision must stop after finitely many steps and thus eventually we will be able to write $w$ as an average of two different even points in $cvx((m-2)\mathcal{U})$, completing the proof. □

## 4. Implication for Hilbert's 17th problem

**Proof of Corollary 3.2.** Suppose $p(x)=\lambda_1x^{u_1}+\cdots+\lambda_nx^{u_n}-x^w$. Let

$$q(x_1,\ldots,x_n):=p(x_1^k,\cdots,x_n^k)=\lambda_1x^{ku_1}+\cdots+\lambda_nx^{ku_n}-x^{kw},$$

which is also an agiform. By Theorems 2.1 and 3.1, $q$ is sos, and so

$$q=\sum_{j=1}^{r}h_j^2\implies p(x_1,\ldots,x_n)=\sum_{j=1}^{r}h_j^2(x_1^{1/k},\ldots,x_n^{1/k}),$$

which shows that $p$ has the desired representation. □

At the time that [14] was written, and the proof given here was relegated to the proposed preprint [15], the second author entertained the possibility that such a result might be true for any psd form. Unfortunately, he discovered that the so-called "Horn form" was a counterexample, and then abandoned writing [15]. The Horn form was communicated to M. Hall by A. Horn in the early 1960s, as a counterexample to a conjecture of P. H. Diananda (see [1, p. 25] and [4, p. 334-5]).

Our example comes from squaring the variables in the Horn form, but the essence of this proof is found in the original. Let

$$F(x_1,\ldots,x_5)=\left(\sum_{j=1}^{5}x_j^2\right)^2-4\sum_{j=1}^{5}x_j^2x_{j+1}^2.$$

We view the subscripts cyclically mod 5, so that the coefficient of $x_j^2x_k^2$ is $-2$ (resp. 2) if $|k-j|=1$ (resp. $|k-j|=2$); $F$ is cyclically symmetric:

$$F(x_1,x_2,x_3,x_4,x_5)=F(x_2,x_3,x_4,x_5,x_1)=\cdots$$

We first show that $F$ is psd. Consider $a\in\mathbb{R}^5$; by the cyclic symmetry, we may assume that $a_1^2\leq a_2^2$. We have the alternate representation

$$F(x_1,\dots,x_5) = (x_1^2 - x_2^2 + x_3^2 - x_4^2 + x_5^2)^2 + 4(x_2^2 - x_1^2)x_5^2 + 4x_1^2x_4^2,$$

hence $F(a) \geq 0$, and so $F$ is psd.

Suppose $F = \sum h_j^2$ and let the coefficient of $x_\ell^2$ in $h_j$ be $b_{j\ell}$. Then

$$(x_1^2 - x_2^2 + x_3^2)^2 = F(x_1, x_2, x_3, 0, 0) = \sum_{j=1}^{r} h_j^2(x_1, x_2, x_3, 0, 0).$$

Since the quadratic form $h_j(x_1, x_2, x_3, 0, 0)$ vanishes on the (irreducible) real cone $g(x_1, x_2, x_3) = x_1^2 - x_2^2 + x_3^2 = 0$, it must be a multiple of $g$; thus, $b_{j1} = -b_{j2} = b_{j3}$. By cycling the variables, we see that $b_{j2} = -b_{j3} = b_{j4}$, $b_{j3} = -b_{j4} = b_{j5}$ and $b_{j4} = -b_{j5} = b_{j1}$, so that $b_{j1} = -b_{j1} = 0$ for all $j$. This implies that the coefficient of $x_1^4$ in $h_j$ is $\sum_j b_{j1}^2 = 0$, so each $h_j(x_1, x_2, x_3, 0, 0) = 0 \cdot g$, a contradiction.

Suppose $F(x_1^k, \cdots, x_5^k)$ is sos. The proof proceeds as before, leading to the equation

$$(x_1^{2k} - x_2^{2k} + x_3^{2k})^2 = F(x_1^k, x_2^k, x_3^k, 0, 0) = \sum_{j=1}^{r} h_j^2(x_1, x_2, x_3, 0, 0).$$

Each form $h_j(x_1, x_2, x_3, 0, 0)$, which has degree $2k$, vanishes on the irreducible real variety $x_1^{2k} - x_2^{2k} + x_3^{2k} = 0$, and hence must be a multiple of it. We obtain the same fatal alternation of the coefficients of $x_\ell^{2k}$ which leads to the contradiction. Therefore, $F(x_1^k, x_2^k, x_3^k, x_4^k, x_5^k)$ is never sos.

We thank the referee for noting that the irreducibility of $x_1^{2k} - x_2^{2k} + x_3^{2k}$ requires some explanation. More generally, we give an elementary proof of the following fact.

**Theorem 4.1.** *Suppose $f(x, y)$ is a square-free binary form of degree $n$ in $\mathbb{C}[x, y]$. Then $F(x, y, z) = f(x, y) + z^n$ is irreducible over $\mathbb{C}$.*

**Proof.** Suppose otherwise that $F = GH$, where $\deg G = k$, $\deg H = n - k$ and $1 \leq k \leq n - 1$. Since $F(0, 0, 1) = 1$, both $G$ and $H$ must have terms involving $z$. Write $G$ and $H$ as polynomials in increasing powers of $z$:

$$\begin{aligned} G(x, y, z) &= G_0(x, y) + G_a(x, y)z^a + \cdots, \\ H(x, y, z) &= H_0(x, y) + H_b(x, y)z^b + \cdots. \end{aligned} \tag{4.1}$$

Here, $G_a$ and $H_b$ are non-zero forms of degree $k - a$ and $n - k - b$ respectively. We see that $F(x, y, 0) = f(x, y) = G_0(x, y)H_0(x, y)$, and since $f$ is square-free, $\gcd(G_0, H_0) = 1$. If $a < b$, then $F = GH$ will contain the un-cancelled term $H_0(x, y)G_a(x, y)z^a$, so $H_0G_a = 0$, which is impossible. A similar contradiction will arise from $b < a$, hence $a = b$ and the coefficient of $x^a$ in $GH$ is $G_0H_a + H_0G_a$. Since $a \leq k < n$, we must have $G_0H_a + H_0G_a = 0$. Since $\gcd(G_0, H_0) = 1$, it follows that $G_0 \mid G_a$. Since $\deg G_0 = k > k - a = \deg G_a$, this contradiction completes the proof. □

In particular, $x_1^n - x_2^n$ is square-free, and the irreducibility of $x_1^n - x_2^n + x_3^n$ over $\mathbb{C}$ implies irreducibility over $\mathbb{R}$.

## 5. Implication for polytopes

From the point of view of polytopes, one would more naturally write $\mathcal{U} = 2\mathcal{P}$, where $P$ is a lattice-point simplex in $\mathbb{R}^n$; without loss of generality, we also assume $m = n$. Further, the conditions that the vertices lie on a hyperplane and have non-negative coefficients seem artificial. In this way, we can drop $n$-th component, so that $\mathcal{P}$ is the usual $n$-point lattice simplex in $\mathbb{R}^{n-1}$.

Let $d = n - 1$. Then Theorem 3.1 says that if $k \geq \max\{2, d-1\}$, then a non-vertex $w \in 2k\mathcal{P} \cap Z^d$ can be written as a sum of two different points in $w \in k\mathcal{P} \cap Z^d$.

Requiring different points comes from the application to agiforms. There is some literature on this subject without that requirement, which means that one needn't treat vertices as a special case. The question then becomes: when can $w \in 2k\mathcal{P} \cap Z^d$ be written as a sum of two points in $k\mathcal{P} \cap Z^d$? This has been studied by D. Handelman [5–7]. In particular, [7] contains a proof using the Shapley-Folkman Lemma that if $k \geq d-1$ (even for $n - 1 = d = 2$), then every point in $2k\mathcal{P} \cap Z^d$ is a sum of two (not necessarily distinct) points in $k\mathcal{P} \cap Z^d$.

## References


[1] P.H. Diananda, On non-negative forms in real variables some or all of which are non-negative, Proc. Camb. Philos. Soc. 58 (1962) 17–25.
[2] M. Dressler, S. Iliman, T. de Wolff, A Positivstellensatz for sums of nonnegative circuit polynomials, SIAM J. Appl. Algebra Geom. 1 (2017) 536–555.
[3] J. Forsgård, T. de Wolff, The algebraic boundary of the sonc cone, arXiv:1905.04776v1.
[4] M. Hall Jr, M. Newman, Copositive and completely positive quadratic forms, Proc. Camb. Philos. Soc. 59 (1963) 329–339.
[5] D. Handelman, Integral body-building in $\mathbb{R}^3$, J. Geom. 27 (1986) 140–152.
[6] D. Handelman, Positive Polynomials, Convex Integral Polytopes and a Random Walk Problem, Springer Lecture Notes in Mathematics, vol. 1282, 1987.
[7] D. Handelman, A Shapley-Folkman lemma for lattice polytopes, manuscript viewed March 19, 2019.
[8] D. Hilbert, Über die Darstellung definiter Formen als Summe von Formenquadraten, Math. Ann. 32 (1888) 342–350; Ges. Abh., vol. 2, Springer, Berlin, 1981, pp. 154–161, reprinted by Chelsea, New York.
[9] A. Hurwitz, Über den Vergleich des arithmetischen und des geometrischen Mittels, J. Reine Angew. Math. 108 (1891) 266–268; see Math. Werke II, Birkhaüser, Basel, 1933, pp. 505–507.
[10] S. Iliman, T. de Wolff, Amoebas, nonnegative polynomials and sums of squares supported on circuits, Res. Math. Sci. 3 (2016) 9.
[11] T.S. Motzkin, The arithmetic-geometric inequality, in: O. Shisha (Ed.), Inequalities, Proc. of Sympos. at Wright-Patterson AFB, August 19–27, 1965, Academic Press, New York, 1967, pp. 205–224;
Also in: D. Cantor, B. Gordon, B. Rothschild (Eds.), S. Motzkin: Selected Papers, Birkhäuser, Boston, 1983, MR36 #6569.
[12] B. Reznick, Extremal psd forms with few terms, Duke Math. J. 45 (1978) 363–374.
[13] B. Reznick, A quantitative version of Hurwitz' theorem on the arithmetic-geometric inequality, J. Reine Angew. Math. 377 (1987) 108–112.
[14] B. Reznick, Forms derived from the arithmetic-geometric inequality, Math. Ann. 283 (1989) 431–464.
[15] B. Reznick, Midpoint polytopes and the map $x_i \mapsto x_i^k$, in preparation circa 1987.
[16] J. Wang, On supports of sums of nonnegative circuit polynomials, arXiv:1809.10608.