Filling a much-needed gap in the literature: A re-creation of a blackboard talk

Bruce Reznick
University of Illinois at Urbana-Champaign

MS129: Sparsity in polynomial systems and applications
SIAM Applied Algebraic Geometry
Bern, Switzerland — July 13, 2019

0. History and jokes

I wrote a paper: "Forms derived from the arithmetic-geometric inequality", *Math. Ann.*, 283 (1989), 431-464 (MR 90i.11043), in which I defined a "mediated" set, deciding when certain psd polynomials called "agiforms" can be written as a sum of squares.

I liked the paper. So did the referee and, presumably, the editor. Like most papers, after a decent interval it settled on the bottom of the ocean. A couple of mistakes I made led to this outcome. One was the poor choice of the term "agiform", with a soft "g", which doesn't work well either in English or in German.

The second was visual: the manuscript was written on a Mac but before TeX was available, necessitating the use of some *ad hoc* "symbol fonts". I used what was intended to be Script. The typesetter thought it was Fraktur, and there were too many instances for me to correct reliably, so I left it in. You choose:

$\mathcal{U}$ or $\mathfrak{U}$?

0. History and jokes

So, my paper was lying on the bottom of the ocean for decades. A few years ago, it discovered its inner Godzilla and resurfaced as "circuit polynomials" in the work of Timo de Wolff and his colleagues.

In the same week last August, I received the kind invitation from Timo and Mareike Dressler to speak in this minisymposium, as well as a request from Jie Wang for a reference to an announced but unproved result in the paper. I took the invitation as a challenge to recreate the proof in time for this talk. I think I've done so, subject to the usual jet-lag uncertainty. I am grateful that this session wasn't yesterday; I didn't finish the proof until last night.

Now imagine that I'm giving this talk 30 years ago, so I have more and darker hair, but a boring shirt and much less ... charm.

1. From the old paper

Write the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ as x^α, for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$. Given a homogeneous polynomial (form)

$$p(x) = \sum_\alpha c(\alpha) x^\alpha,$$

write $C(p) = cvx\{\alpha : c(\alpha) \neq 0\}$ for the Newton polytope of p.

In 1978, I codified part of Motzkin's 1967 proof into a necessary condition for an sos representation:

$$p = \sum_{k=1}^r h_k^2 \implies C(h_k) \subseteq \tfrac{1}{2} C(p).$$

1. From the old paper

Suppose $u_i \in (2\mathbb{Z})^n$, $1 \le i \le n$, with $u_{ij} \ge 0$ and $\sum_{j=1}^n u_{ij} = 2d$. Suppose further that $\mathcal{U} = \{u_1, \ldots, u_n\}$ is a simplex and $w \in \mathcal{U}$, and $w = \sum_{i=1}^n \lambda_i u_i$, where $\lambda_i \ge 0$ and $\sum_{i=1}^n \lambda_i = 1$.

The arithmetic-geometric inequality states that if $t_i \ge 0$, $\lambda_i \ge 0$ and $\sum_{i=1}^n \lambda_i = 1$, then

$$\lambda_1 t_1 + \cdots + \lambda_n t_n \ge t_1^{\lambda_1} \cdots t_n^{\lambda_n}.$$

By making the substitution $t_i = x^{u_i}$ into the arithmetic-geometric inequality, we obtain a psd form (I called it an *agiform*, it's now a special case of a *circuit polynomial*):

$$\lambda_1 x^{u_1} + \cdots + \lambda_n x^{u_n} - x^w \ge 0.$$

1. From the old paper

The motivating examples for this paper came from Motzkin (1967) (not sos) and Hurwitz (1891) (sos)

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

These are both agiforms, up to a multiplicative factor of 3, since $(2,2,2)$ is the centroid to both $\{(4,2,0),(2,4,0),(0,0,6)\}$ and $\{(6,0,0),(0,6,0),(0,0,6)\}$.

The only monomials in a sos representation of M have exponents in $\frac{1}{2}cvx(\{4,2,0),(2,4,0),(0,0,6)\})$; that is, x^2y, xy^2, xyz, z^3, so

$$M = \sum_k h_k^2 \implies M = \sum_k (a_k x^2y + b_k xy^2 + c_k xyz + d_k z^3)^2.$$

The coefficient of $x^2y^2z^2$ above gives $-3 = \sum_k c_k^2$.

1. From the old paper

On the other hand, we have (with color-coded) versions of $c(x^\alpha - x^\beta)^2$ appearing on the right with c at 2α and 2β, and $-2c$ at $\alpha + \beta$.

$x^6 + y^6 + z^6 - 3x^2y^2z^2$

$= \frac{3}{2}(x^2y - yz^2)^2$

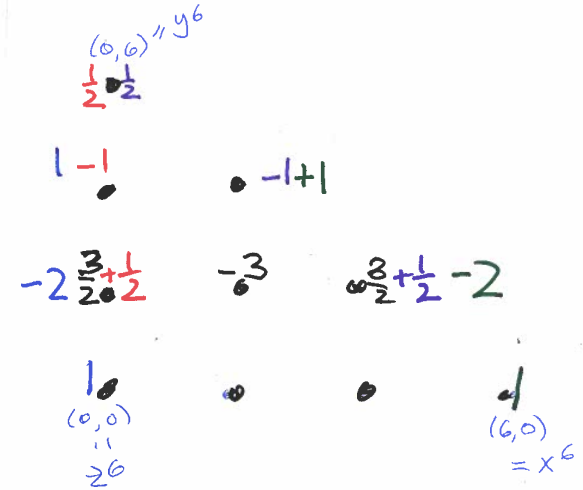
$+ \frac{1}{2}(x^2y - y^3)^2$

$+ (x^3 - xy^2)^2$

$+ \frac{1}{2}(yz^2 - y^3)^2$

$+ (z^3 - y^2z)^2$

The squares written out visually as a set of triples in a row, with cancellations as needed



1. From the old paper

It turns out that there is a geometric criterion which determines whether an agiform is sos. Suppose as before that $u_i \in (2\mathbb{Z})^n$, $1 \leq i \leq n$, with $u_{ij} \geq 0$ and $\sum_{j=1}^n u_{ij} = 2d$, $\mathcal{U} = \{u_1, \ldots, u_n\}$ is a simplex and $w = \sum \lambda_i u_i \in \mathcal{U}$. Theorem: $\lambda_1 x^{u_1} + \cdots + \lambda_n x^{u_n} - x^w$ is sos if and only if there is a $\mathcal{U}$-mediated set containing w.

I guess I better tell you what that means! Suppose $S \subset \mathcal{U} \cap \mathbb{Z}^n$ is 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 the Motzkin case, it is impossible to write $(2, 2, 2)$ as an average. In the Hurwitz case, it suffices to take $S = \{(6, 0, 0), (0, 6, 0), (0, 0, 6), (2, 2, 2), (4, 2, 0), (2, 4, 0), (0, 2, 4), (0, 4, 2).\}$

Notice that the relevant averages appeared in the pictorial representation of H as the binomial squares.

2. The announced result - background

In that 1989 paper, I claimed that if $k \geq \min\{2, n-2\}$, then $k\mathcal{U} \cap \mathbb{Z}^n$ is $(k\mathcal{U})$-mediated. This implies that for any agiform $p(x_1, \ldots, x_n) = \lambda_1 x^{u_1} + \cdots + \lambda_n x^{u_n} - x^w$, the related agiform $p(x_1^k, \ldots, x_n^k)$ is sos, or equivalently, that any agiform p can be written as a sum of squares in the variables $x_i^{1/k}$.

For more on this, see Jie Wang's recent paper.

I thought this might be a more generally true result: that every psd form is a sum of squares of forms in fractional variables. However, this conjecture is false.

2. The announced result - background

The simplest (and basically only) known counterexample is the Horn form

$$H(x_1, \ldots, x_5) = \sum_{i=1}^{5} x_i^4 - 2\sum_{i=1}^{5} x_i^2 x_{i+1}^2 + 2\sum_{i=1}^{5} x_i^2 x_{i+2}^2,$$

where the variables are taken cyclically mod 5. We give a quick proof that H is psd and not sos. First observe that

$$H = (x_1^2 - x_2^2 + x_3^2 - x_4^2 + x_5^2)^2 + 4x_1^2 x_4^2 + 4(x_2^2 - x_1^2)x_5^2,$$

So if $x = (a_1, a_2, a_3, a_4, a_5)$ and $a_2^2 \geq a_1^2$, then $H(a) \geq 0$. Since $H(x_1, x_2, x_3, x_4, x_5) = H(x_2, x_3, x_4, x_5, x_1)$, etc., the same holds if $a_3^2 \geq a_2^2$, etc., and one of these five inequalities must hold for all a.

2. The announced result - background

If $H = \sum h_j^2$, then by setting $x_4 = x_5 = 0$, we have

$$H(x_1, x_2, x_3, 0, 0) = (x_1^2 - x_2^2 + x_3^2)^2 = \sum_j h_j(x_1, x_2, x_3, 0, 0)^2.$$

Since $x_1^2 - x_2^2 + x_3^2$ is irreducible and indefinite, it essentially follows from the Nullstellensatz that each $h_j(x_1, x_2, x_3, 0, 0)$ is a multiple of $x_1^2 - x_2^2 + x_3^2$. In particular, the coefficients of x_1^2, x_2^2, x_3^2 in h_j are $c_j, -c_j, c_j$ for some c_j and $\sum c_j^2 = 1$.

By the cyclic symmetry, it follows that the coefficient of x_4^2 is $-c_j$, that of x_5^2 is c_j, but now that of x_1^2 is $-c_j = c_j$, so each $c_j = 0$, which gives a contradiction. Since $x_1^{2k} - x_2^{2k} + x_3^{2k}$ is also irreducible and indefinite for any integer $k \geq 1$, it follows that $H(x_1^k, \ldots, x_5^k)$ is never sos.

3. The announced result - proof

We begin with a simpler result: if $k \geq n-1$, then that $k\mathcal{U} \cap \mathbb{Z}^n$ is $k\mathcal{U}$-mediated. First a possibly unnecessary lemma.

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

Sketch of proof: do a greedy construction: let $a_i = b_i$ as long as the partial sum is $\leq S$, have one transitional term and set the rest of the a_i's equal to zero. For example, if $b = (1, 4, 5, 6, 2)$ with $R = 18$ and $S = 13$, choose $a = (1, 4, 5, 3, 0)$.

We also need one provisional notation. If $v = \sum_{i=1}^n a_i u_i$, where $0 \leq a_i \in \mathbb{Z}$ and $\sum_{i=1}^n a_i = k$, we will say that v is a *bead* in $k\mathcal{U}$.

3. The announced result - proof

Theorem: If $k \geq n-1$, then $k\mathcal{U} \cap \mathbb{Z}^n$ is $k\mathcal{U}$-mediated.

Proof: We need to show that every non-vertex $w \in k\mathcal{U} \cap \mathbb{Z}^n$ is an average of two different even points in $k\mathcal{U} \cap \mathbb{Z}^n$. First suppose that $w = \sum a_i u_i$ is a bead but not a vertex. Then at least two of the a_i's are positive; without loss of generality, suppose $a_1, a_2 \geq 1$. Then w is the average of $w \pm (u_1 - u_2)$, each of which is even and in $k\mathcal{U} \cap \mathbb{Z}^n$.
Otherwise, w is not a bead. If we find a bead v so that $2w - v$ is in $k\mathcal{U}$, then it will necessarily be an even lattice point and also $v \neq 2w - v$, because w is not a bead but v is! (And w is of course the average of v and $2w - v$.)

3. The announced result - proof

Write w as a barycentric combination of the ku_i's, so that $w = \sum \beta_i u_i$, where $\beta_i \geq 0$, $\sum \beta_i = k$ and at least one $\beta_i \notin \mathbb{Z}$. Let $v = \sum a_i u_i$ be any bead. Then $2w - v = \sum_{i=1}^{n} (2\beta_i - a_i) v_i$, and we are done if we can show that there exists a choice of $0 \leq a_i \in \mathbb{Z}$ so that $2\beta_i \geq a_i$ for all i.

For $t \in \mathbb{R}$, we write $t = \lfloor t \rfloor + \{t\}$, where $\lfloor t \rfloor \in \mathbb{Z}$ and $\{t\} \in [0, 1)$.

It suffices to show that we can find a_i so that $\lfloor 2\beta_i \rfloor \geq a_i$. But $\sum_{i=1}^{n} \lfloor 2\beta_i \rfloor > \sum_{i=1}^{n} (2\beta_i - 1) = 2k - n$, and since $\lfloor 2\beta_i \rfloor$ and $2k - n$ are integers, a strict inequality implies a gap of at least 1. Hence $\sum_{i=1}^{n} \lfloor 2\beta_i \rfloor \geq 2k - n + 1 = k + (k - (n-1)) \geq k$. By the Lemma, this means we can find such a_i's and construct the desired bead v. This completes the proof.

3. The announced result - proof

When $k = n-2$, the proof is much more delicate. (Note: the rest of this section was hand-waved at the talk and not presented in accurate detail.)

Theorem: If $n \geq 4$, then $(n-2)\mathcal{U} \cap \mathbb{Z}^n$ is $(n-2)\mathcal{U}$-mediated.

Proof: We start by repeating the last proof. The beads are all averages as before. Suppose $w = \sum \beta_i u_i$ is a non-bead. We conclude as before that $\sum_{i=1}^n \lfloor 2\beta_i \rfloor \geq 1 + \sum_{i=1}^n (2\beta_i - 1)$ $= 1 + 2(n-2) - n = n-3$. If this sum is $\geq n-2$, then we proceed as before and find a bead v so that $2w - v$ is in $(n-2)\mathcal{U}$.

What if the sum is $n-3$? Observe that $\sum_{i=1}^n \lfloor 2\beta_i \rfloor = n-3 \implies$ $\sum_{i=1}^n \{2\beta_i\} = 2(n-2) - (n-3) = n-1$. Since each $\{2\beta_i\} < 1$, it follows that none of the summands is zero; that is, $2\beta_i \notin \mathbb{Z}$.

3. The announced result - proof

Furthermore, $\sum_{i=1}^{n}(1-\{2\beta_i\}) = n-(n-1) = 1$, and since $\{x\} < 1$, each $1-\{2\beta_i\}$ is positive. Now the fun begins! Define

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

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

Then $\tilde{u}$ is evidently strictly interior to $\mathcal{U}$ and is also an even point. At this point in the talk, I reminisced of the ten minutes in my undergraduate days when I thought I had proved Fermat's Last Theorem, though was a bit suspicious, since my proof worked for $n = 2$ as well. The proof was wrong. I'm pretty sure that this is the point I reached in 1989 and then was careless in saying I was done. I missed one important case.

3. The announced result - proof

This is the case I missed. Suppose we are so lucky that our non-bead w is actually a multiple of the even point $\tilde{u}$. The multiple has to be $n-2$ and

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

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

Let $d_i := (1+\lfloor 2\beta_i \rfloor)$, so that $\tilde{u} = \sum_{i=1}^{n} \frac{d_i}{2n-3} u_i$, where $1 \leq d_i \in \mathbb{Z}$ and $\sum_i d_i = 2n-3$. Since $n \geq 4$, $2n-3 > n$ (!), so at least one of the d_i's is > 1; say, without loss of generality that $d_1 \geq 2$.

We now observe that $w = (n-2)\tilde{u}$ is the average of $(n-3)\tilde{u} + u_1$ and $(n-1)\tilde{u} - u_1$, both of which are evidently even points. The first is obviously in $(n-2)\mathcal{U}$.

3. The announced result - proof

The second point, $(n-1)\tilde{u} - u_1$, is

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

Since $d_1 \geq 2$, the coefficient of u_1 is at least $\frac{2n-2}{2n-3} - 1 > 0$. Thus, $(n-1)\tilde{u} - v_1$ is in $(n-2)\mathcal{U}$ and we are again done. Thus the only way we have not already written w as an average of two distinct even points is when w is not a multiple of the new even point $\tilde{u}$. What we do now is subdivide $\mathcal{U}$ by $\tilde{u}$ into n sub-simplices; w will be a non-vertex in the multiplication of one of them by $n-2$, say

$$w \in (n-2)cvx(\tilde{u}, u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n).$$

We repeat the process. Since $\mathcal{U} \cap \mathbb{Z}^n$ has only finitely many points, this process can only occur finitely many times and terminates in the construction of an average.

I believe I am allowed to say QED now.

4. Speculations

So the obvious question is this. Given $\mathcal{U}$ as above, what is the smallest k so that $k\mathcal{U} \cap \mathbb{Z}^n$ is always mediated? With a profound lack of imagination let $f(n)$ denote this smallest value.

It's easy to show that $f(2) = 1$, and examples of Motzkin and Choi and Lam (as well as the paper) show that $f(n) > 1$ for $n \geq 3$. This talk has shown you, I hope, that $f(3) = f(4) = 2$.

The first open question is whether $f(5) = 2$ or 3.

The next natural question is whether $f(n) = n - 2$ for larger n or whether it's more like $\lceil \frac{n}{2} \rceil$, or perhaps, it grows sublinearly.

The explorations of these questions might well require some actual theory.

5. The talk nobody could understand

I talked about this briefly at the end of the Monday thing, and I thought I'd record it here. I gave talks on this subject at Oberwolfach, Caltech and Urbana in the mid 80s and nobody could figure out what I was talking about. I will give this in $\mathbb{R}^2$, though there are obvious extensions to any number of variables. The name I gave to the topic was "deeper arithmetic-geometric inequalities", though my naming skills weren't so good back then.

Suppose k points are given in the plane: (a_i, b_i) and we consider a polynomial supported on these points: $p(x, y) = \sum c_i x^{a_i} y^{b_i}$. We do not assume that a_i, b_i are integers and so we restrict to $x, y > 0$. Suppose we require that p vanish to first order at $(1, 1)$, and that the points are such that there is a unique (projective) solution p and that all points are necessary, so no $c_i = 0$. The equations are $\sum c_i = \sum c_i a_i = \sum c_i b_i = 0$. We want to know the conditions on the points so that $\pm p \geq 0$ on $\mathbb{R}^2$.

5. The talk nobody could understand

It is neither hard nor interesting to show that these conditions are satisfied either if $k = 3$ and the points are on a line, or if $k = 4$ and no three points are on a line. In the first case, Descartes' Rule of Signs says that $p \geq 0$ and the resulting p is an agiform. In the second case, there are in fact two cases: either each point is a vertex of the convex hull, or there is a triangle with a single point inside. In the first case, p is not psd, because the c_j's take both signs. In the second case, p is an agiform and so is psd.

The same thing holds for general n: $p \geq 0$ is equivalent to the geometric shape of the given points being one point inside a simplex, and the form is an agiform.

So the question I asked, was, what happens in the "next" case: when you replace "vanish to first order" with "vanish to third order"? (Or of course, more generally to $(2m-1)$-st order.)

5. The talk nobody could understand

Again, in one variable, Descartes' Rule of Signs says that every form you get is psd. In the plane, there are 10 equations, and one very special example I wish I had 35 years ago. Let 10 of the 11 points be the integer points $(i,j) : 0 \le i,j, i+j \le 3$ plus one other point (a,b). Then there is exactly one choice of c_{ij} so that $x^a y^b - \sum_{i=0}^{3} \sum_{j=0}^{3-i} c_{ij} x^i y^j$ vanishes to third order at (1,1), and that is when the sum above is the Taylor approximation to $x^a y^b$ at $(1,1)$. Fortunately, the difference is the *error* to the Taylor approximation, and it can be expressed exactly as a fourth derivative in some direction at some point. In this way, I can show that if (a,b) lies in the open triangle with vertices $(0,0),(1,0),(0,1)$, then the resulting form is psd.

Big questions: What shapes correspond to $p \ge 0$? Must there be concentric layers of positive and negative coefficients?

6. Thanks

My thanks to the organizers for the chance to revisit and improve on some old ideas.

My thanks (and sympathy) also to the people who saw this talk in its original blackboard form.