Problem Set 1 – Solutions

Samuel B. Hopkins

November 11, 2024

Problem 1 (On $\models$, borrowed from Aaron Potechin)**.** Consider the following polynomial equation in 3 variables, x, y, z.

$$(x^2+1)y = z^2.$$

Because it implies $y = \frac{z^2}{x^2+1}$, any solution (x, y, z) to the above must have $y \geq 0$. We will see if sum-of-squares can capture this reasoning.

1. Construct a degree 4 pseudoexpectation $\widetilde{\mathbb{E}}$ in variables x, y, z such that $\widetilde{\mathbb{E}} \models (x^2+1)y = z^2$ but $\widetilde{\mathbb{E}}\, y < 0$. (Computer-aided proofs are allowed.)

   By $\widetilde{\mathbb{E}} \models (x^2+1)y = z^2$, we mean that for any polynomial p of degree at most 1 in x, y, z, $\widetilde{\mathbb{E}}\, p(x,y,z)(x^2+1)y = \widetilde{\mathbb{E}}\, p(x,y,z)z^2$.

2. Despite the above, show that there exists a sum-of-squares refutation to the following system of polynomial inequalities, for any $c > 0$: $\{(x^2+1)y = z^2, y \leq -c\}$.

Solution, Part 1 (courtesy of Mahbod Majid)

Recall that $\widetilde{\mathbb{E}}$ is a degree 4 pseudoexpectation in variables x, y, z if and only if

$$\widetilde{\mathbb{E}}\left[(1,x,y,z,xy,yz,xz,x^2,y^2,z^2)(1,x,y,z,xy,yz,xz,x^2,y^2,z^2)^T\right] \succcurlyeq 0.$$

Therefore, we wish to find a pseudoexpectation $\widetilde{\mathbb{E}}$ satisfying the following constraints.

$$\begin{aligned}
&\widetilde{\mathbb{E}}\left[(1,x,y,z,xy,yz,xz,x^2,y^2,z^2)(1,x,y,z,xy,yz,xz,x^2,y^2,z^2)^T\right] \succcurlyeq 0\\
&\widetilde{\mathbb{E}}\left[x^2y - z^2\right] = -\widetilde{\mathbb{E}}\left[y\right]\\
&\widetilde{\mathbb{E}}\left[x^3y - xz^2\right] = -\widetilde{\mathbb{E}}\left[xy\right]\\
&\widetilde{\mathbb{E}}\left[x^2y^2 - z^2y\right] = -\widetilde{\mathbb{E}}\left[y^2\right]\\
&\widetilde{\mathbb{E}}\left[x^2yz - z^3\right] = -\widetilde{\mathbb{E}}\left[yz\right]\\
&\widetilde{\mathbb{E}}\left[y\right] < 0
\end{aligned}$$

Such a pseudoexpectation may be constructed as follows.

	1	x	y	z	xy	yz	zx	x^2	y^2	z^2
1	1	0	−0.5	0	0	0	0	1.5	1	0.5
x	0	1.5	0	0	1	0	0	0	0	0
y	−0.5	0	1	0	0	0	0	1	0.25	1.75
z	0	0	0	0.5	0	1.75	0	0	0	0
xy	0	1	0	0	0.75	0	0	0	0	0
yz	0	0	0	1.75	0	8.25	0	0	0	0
zx	0	0	0	0	0	0	4.75	0	0	0
x^2	1.5	0	1	0	0	0	0	10	0.75	4.75
y^2	1	0	0.25	0	0	0	0	0.75	10	8.25
z^2	0.5	0	1.75	0	0	0	0	4.75	8.25	10

Solution, Part 2 (courtesy of Mahbod Majid)

Indeed, for the given family of polynomials $\mathcal{A}$, we have that

$$\begin{aligned}
&\mathcal{A} \vdash_4 (x^2+1)y \le -c(x^2+1)\\
&\mathcal{A} \vdash_4 z^2 \le -c(x^2+1)\\
&\mathcal{A} \vdash_4 0 \le -c(x^2+1)\\
&\mathcal{A} \vdash_4 cx^2 \le -c\\
&\mathcal{A} \vdash_4 0 \le -c\\
&\mathcal{A} \vdash_4 0 \le -1
\end{aligned}$$

as desired.

Problem 2. Suppose $\widetilde{\mathbb{E}}$ is a pseudoexpectation of degree d, with d even, and $\widetilde{\mathbb{E}} \models p \leq 0, p \geq 0$ for some polynomial p. (Informally, we have been writing $\widetilde{\mathbb{E}} \models p = 0$.) Show that if p has even degree, for every q such that the degree of pq is at most d, we have $\widetilde{\mathbb{E}}\, pq = 0$. Similarly, show that if p has odd degree, for every q such that the degree of pq is at most $d-1$, we have $\widetilde{\mathbb{E}}\, pq = 0$.

Solution By definition, we have that $\widetilde{\mathbb{E}}\, pq = 0$ for every sum-of-squares polynomial q such that the degree of pq is at most d. Given an arbitrary polynomial q, we may write it in terms of its Fourier expansion as a sum of monomials $q = \sum \widehat{q}_\alpha x^\alpha$, in which case it suffices to show that $\widetilde{\mathbb{E}}\, px^\alpha = 0$ for every bounded-degree monomial x^α.

Thus, let $q = x^\alpha$ and $\deg(q) = k \leq d$. Then, q may be written as the difference of two sum-of-squares polynomials, each of degree at most $\lfloor \frac{k+1}{2} \rfloor$. Indeed, we may write $x^\alpha = x^\beta x^\gamma$ for β, γ each being the indicators on an arbitrary partition of the nonzero indices of α (of which there are at most k) into two sets of size at most $\lfloor \frac{k+1}{2} \rfloor$. Then,

$$x^\alpha = \left(\frac{x^\beta + x^\gamma}{2}\right)^2 - \left(\frac{x^\beta - x^\gamma}{2}\right)^2.$$

Note that each of the polynomials inside the squares is of degree $\lfloor \frac{k+1}{2} \rfloor$. If p has even degree, the degree of $p \cdot \left(\frac{x^\beta + x^\gamma}{2}\right)^2$ is at most d if $\deg(pq) \leq d$. If $\deg(p)$ is odd on the other hand, the degree of $p \cdot \left(\frac{x^\beta + x^\gamma}{2}\right)^2$ is equal to $\deg(pq) + 1$, which is at most d if $\deg(pq) \leq d - 1$.

The desideratum follows since for such monomials, $\widetilde{\mathbb{E}}\left[p \cdot \left(\frac{x^\beta + x^\gamma}{2}\right)^2\right] = \widetilde{\mathbb{E}}\left[p \cdot \left(\frac{x^\beta - x^\gamma}{2}\right)^2\right] = 0$ by the discussion in the first paragraph.