Meeting on Real Algebraic Geometry With A View Toward Systems Control and Free Positivity

Mathematisches Forschungsinstitut Oberwolfach

April 7–11, 2014

Markus Schweighofer (Universität Konstanz)

Positive polynomials, sums of squares, degree bounds and semidefinite representations

All students of mathematics should know that every polynomial in one variable nonnegative on the real line is a sum of two squares of polynomials:

Theorem 1. *Suppose* $f \in \mathbb{R}[X]$ *and* $f \geq 0$ *on* $\mathbb{R}$. *Then there exist* $p, q \in \mathbb{R}[X]$ *such that* $f = p^2 + q^2$.

Proof. By the *fundamental theorem of algebra*, f is a product of linear polynomials in $\mathbb{C}[X]$ corresponding to the multiset of complex roots of f (i.e., the roots counted with multiplicity). Since f is nonnegative, the real factors appear with an even multiplicity. Since f is real, the non-real factors appear in complex-conjugated pairs. Any division of the multiset into two complex-conjugated parts, now leads to a complex polynomial $p + \mathring{\imath} q$ ($p, q \in \mathbb{R}[X]$) such that

$$f = (p - \mathring{\imath} q)(p + \mathring{\imath} q) = p^2 + q^2$$

where $\mathring{\imath} \in \mathbb{C}$ denotes the imaginary unit. □

Note that this theorem can be reformulated in the following more systematic style (since a complex polynomial taking real values on the line is automatically real):

For all $f \in \mathbb{C}[X]$ *with* $f \geq 0$ *on* $\mathbb{R}$, *there exists* $p \in \mathbb{C}[X]$ *such that* $f = p^* p$.

Here $\mathring{\imath}^* = -\mathring{\imath}$ and $X^* = X$: We denote by $*$ the complex conjugation and extend it on an involution on polynomial rings by considering the variables to be formally self-adjoint. We also have obvious *degree bounds* in the above: If $d \in \mathbb{N}$ such that $\deg f \leq 2d$, then $\deg p \leq d$ follows immediately.

The following non-trivial generalization of Theorem 1 to *matrix polynomials positive semidefinite on the real line* was folklore at least since the 1960s (see for example [1]). Here $*$ acts as before but in addition transposes the matrices.

Theorem 2. *Suppose* $F \in \mathbb{C}[X]^{s \times s}$ *and* $F \succeq 0$ *on* $\mathbb{R}$. *Then there exists* $P \in \mathbb{C}[X]$ *such that* $F = P^* P$.

Taking the trace on both sides of the equation $F = P^* P$ yields $\sum_{i=1}^{s} F_{ii} = \sum_{i,j=1}^{s} P_{ij}^* P_{ij}$. Using this, it is easy exercise to show that we get the same kind of automatic degree bounds as before. The most elementary proof of Theorem 1 has been given (for the case $F \in \mathbb{R}[X]^{s \times s}$) by Choi, Lam and Reznick [2, Section 7]. The rough idea of their proof is by completing the square successively with respect to the different variables one by each. To compensate for the impossibility of division in the polynomial ring, during this process multipliers have to be introduced which can be neutralized using the fundamental theorem of algebra. In [2], this neutralization involves very tricky computations. In the first part of the talk, we present a new and very "clean" way to do this neutralization using basic linear algebra instead of computations. This yields arguably the easiest known proof of Theorem 2.

With a little more work, this new argument also allows to show that the determinant of the factors in the factorization can be described with the maximal possible freedom (compare to the proof of Theorem 1):

Theorem 3 (Hanselka & S., Ball & Rodman). *Suppose $F \in \mathbb{C}[X]^{s\times s}$ and $g \in \mathbb{C}[X]$ such that $F \succeq 0$ on $\mathbb{R}$ and $\det F = g^*g$. Then there exists $P \in \mathbb{C}^{s\times s}$ such that $F = P^*P$ and $\det P = g$.*

Theorem 3 was already known in the case where g and g^* have no common zero [1, Theorem 3]. Our question whether it is already known in the above stated general form, reached Joe Ball and Leiba Rodman who negated it and at the same gave an alternative unpublished proof which is however based on a considerable amount of the theory of matrix polynomials [3]. Our investigations were initially motivated by the fact that the algorithm described in [4] to compute the decomposition in Theorem 2 seems to use (at least weaker versions of) Theorem 3 [5] even though no version of this theorem is stated let alone proved in [4] (note also that the authors of [4] claim to give a system-theoretic proof of Theorem 2 [4, page 5660, last paragraph] which does not seem to be the case since they use the equation $Q^*(\lambda_i^*)v_i = 0$ in [4, page 5665] without any proof but this equation is almost equivalent to the existence of the decomposition).

The second part of the talk was a survey on modern versions of Theorems 1 and 2 which we state in the following synthesized way:

Theorem 4 (Schmüdgen 1991, Putinar 1993, Hol & Scherer 2005). *Let $m, n \in \mathbb{N}$, $g_1, \dots, g_m \in A := \mathbb{R}[X_1, \dots, X_n]$ and set $g_0 := 1 \in A$. Consider the basic closed semialgebraic set*

$$S := \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \dots, g_m(x) \geq 0\},$$

and the matricial quadratic modules

$$T^{(s)} := \left\{ \sum_{i=0}^{m} g_i \sum_j P_{ij}^* P_{ij} \mid P_{ij} \in A^{s\times s} \right\} \qquad (s \in \mathbb{N}),$$

and the ordinary quadratic module $T := T^{(1)}$. The following are equivalent:

(a) *There exist $t \in \mathbb{N}$ and $h_1, \dots, h_t \in A$ such that $\prod_{i\in I} h_i \in T$ for all $I \subseteq \{1, \dots, t\}$ and $\{x \in \mathbb{R}^n \mid h_1(x) \geq 0, \dots, h_t(x) \geq 0\}$ (and therefore also its subset S) is compact.*
(b) *There exists $h \in T$ such that $\{x \in \mathbb{R}^n \mid h(x) \geq 0\}$ is compact.*
(c) *There exists $N \in \mathbb{N}$ such that $N - \sum_{i=1}^n X_i^2 \in T$.*
(d) *For all $p \in A$ there is an $N \in \mathbb{N}$ such that $N + p \in T$.*
(e) *S is compact and for every $f \in A$ with $f > 0$ on S, we have $f \in T$.*
(f) *S is compact and for all $s \in \mathbb{N}$ and all $F \in \mathbb{R}[X]^{s\times}$ with $F \succ 0$ on S, we have $f \in T^{(s)}$.*

The backward implications are obvious whereas the forward implications are not: We don't know if there is an easy direct proof of (a)⇒(b). The hardest implications are (a)⇒(c) (or even (b)⇒(c)): This is the essence of Schmüdgen's celebrated 1991 theorem [6] whose first algebraic proof was found by Wörmann [7]. All proofs of Schmüdgen's Theorem use Krivine's (classical) Positivstellensatz from real algebraic geometry [8] (reproved by Stengle [9] and Prestel [10]). The implication (c)⇒(d) is just a few lines of tricky identities. Implication (d)⇒(e) was just a by-product in the article [11] by Putinar but got famous due to its numerous applications. The easiest known proof today stems from Marshall [14]. Finally, (d)⇒(f) is a theorem due to Hol & Scherer [12]. See [16, 14, 15].

The advantage of modern versions of Theorems 1 and 2 such as Theorem 4 is that they work in severable variables instead of only one and that they allow to consider positivity on arbitrary basic closed semialgebraic sets.

The big drawback of the modern versions is that there no obvious or "clean" degree bounds. The degree bounds instead depend on the geometry [16, 17, 18, 19, 20]. Indeed, the validity of these theorems even strongly relies on the possibility of huge degree cancellations. Related to this, strict positivity is in general needed although the certificate is only for nonnegativity.

An ingenious idea of Helton and Nie however surmounts partially these difficulties in cases where S is stricly convex and the polynomial to represent is of degree one [20, 21, 22, 23]. In Theorem 4, instead of applying (e) to the degree one polynomial, they apply (f) to the Hessians of certain polynomials defining the set S locally and write the degree one polynomial as a double integral over an expression involving this Hessian. This leads to strong theorems about semidefinite representability of large classes of convex semialgebraic sets. Indeed, it is an open question if all convex semialgebraic sets are projections of spectrahedra (i.e., solution sets of linear matrix inequalities). Even if one is interested in sums of squares representations of polynomials rather than matrix polynomials, it can be of great help to study the case of matrix polynomials.

References

[1] V.A. Jakubovič: Factorization of symmetric matrix polynomials, Dokl. Akad. Nauk SSSR 194, 1970, 532–535 ↑1, 2

[2] M.D. Choi, T.Y. Lam, B. Reznick: Real zeros of positive semidefinite forms I, Math. Z. 171 (1980), no. 1, 1–26 ↑1

[3] I. Gohberg, P. Lancaster, L. Rodman: Matrix polynomials, Computer Science and Applied Mathematics. Academic Press, Inc., New York-London, 1982 ↑2

[4] E. Aylward, S. Itani, P.A. Parrilo: Explicit SOS decompositions of univariate polynomial matrices and the Kalman-Yakubovich-Popov Lemma, Proceedings of the 46th IEEE Conference on Decision and Control, New Orleans, 2007 ↑2

[5] B. Mangold: Quadratsummen von Matrixpolynomen in einer Variablen, Bachelor's thesis, November 2013, Universitt Konstanz ↑2

[6] K. Schmüdgen: The K-moment problem for compact semi-algebraic sets, Math. Ann. 289 (1991), no. 2, 203–206 ↑3

[7] R. Berr, T. Wörmann: Positive polynomials on compact sets, Manuscripta Math. 104 (2001), no. 2, 135–143 ↑3

[8] J.-L. Krivine: Anneaux préordonnés, J. Analyse Math. 12 1964 307–326 ↑3

[9] G. Stengle: A Nullstellensatz and a Positivstellensatz in semialgebraic geometry, Math. Ann. 207 (1974), 87–97 ↑3

[10] A. Prestel: Lectures on formally real fields, Rio de Janeiro: IMPA (1975), reprinted in: Lecture Notes in Mathematics 1093, Springer-Verlag, Berlin, 1984 ↑3
[11] M. Putinar: Positive polynomials on compact semi-algebraic sets, Indiana Univ. Math. J. 42 (1993), no. 3, 969–984 ↑3
[12] C.W.J. Hol, C.W. Scherer: Matrix sum-of-squares relaxations for robust semi-definite programs, Math. Program. 107 (2006), no. 1-2, Ser. B, 189–211 ↑3
[13] A. Prestel, C.N. Delzell: Positive polynomials, From Hilbert's 17th problem to real algebra, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2001 ↑3
[14] M. Marshall: Positive polynomials and sums of squares, Mathematical Surveys and Monographs, 146, American Mathematical Society, Providence, RI, 2008 ↑3
[15] M. Laurent; Sums of squares, moment matrices and optimization over polynomials, Emerging applications of algebraic geometry, 157270, IMA Vol. Math. Appl., 149, Springer, New York, 2009, updated versions available at `http://homepages.cwi.nl/~monique/files/moment-ima-update-new.pdf` ↑3
[16] A. Prestel: Bounds for representations of polynomials positive on compact semi-algebraic sets, Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999), 253260, Fields Inst. Commun., 32, Amer. Math. Soc., Providence, RI, 2002 ↑3
[17] M. Schweighofer: On the complexity of Schmüdgen's Positivstellensatz, J. Complexity 20 (2004), no. 4, 529543 ↑3
[18] J. Nie, M. Schweighofer: On the complexity of Putinar's Positivstellensatz, J. Complexity 23 (2007), no. 1, 135150 ↑3
[19] R. Hess: Die Sätze von Putinar und Schmüdgen für Matrixpolynome mit Gradschranken, Diplomarbeit, January 2013, Universität Konstanz ↑3
[20] J.W. Helton, J. Nie: Semidefinite representation of convex sets, Math. Program. 122 (2010), no. 1, Ser. A, 21–64 ↑3
[21] J.W. Helton, J. Nie: Sufficient and necessary conditions for semidefinite representability of convex hulls and sets, SIAM J. Optim. 20 (2009), no. 2, 759–791 ↑3
[22] R. Sinn: Spectrahedra and a relaxation of convex semialgebraic sets, Diplomarbeit, April 2010, Universität Konstanz ↑3
[23] T.-L. Kriel: Semidefinite representability of closed semi-algebraic sets, Bachelor's thesis, September 2012, Universität Konstanz ↑3