Canad. J. Math. Vol. **61** (1), 2009 pp. 205–221

Representations of Non-Negative Polynomials, Degree Bounds and Applications to Optimization

M. Marshall

Abstract. Natural sufficient conditions for a polynomial to have a local minimum at a point are considered. These conditions tend to hold with probability 1. It is shown that polynomials satisfying these conditions at each minimum point have nice presentations in terms of sums of squares. Applications are given to optimization on a compact set and also to global optimization. In many cases, there are degree bounds for such presentations. These bounds are of theoretical interest, but they appear to be too large to be of much practical use at present. In the final section, other more concrete degree bounds are obtained which ensure at least that the feasible set of solutions is not empty.

Fix an algebraic set V in R^n, where R is a real closed field. Let A denote the coordinate ring of V, *i.e.*,

$$A = R[V] := \frac{R[\underline{x}]}{\mathcal{I}(V)},$$

where $\mathcal{I}(V)$ denotes the ideal of polynomials vanishing on V. The reader may assume, for simplicity, that $V = R^n$, so $A = R[\underline{x}]$. Fix a quadratic module M in A, *i.e.,* a subset M of A satisfying $M + M \subseteq M$, $1 \in M$, and $f^2M \subseteq M$ for all $f \in A$, and let

$$K = \{p \in V \mid \forall g \in M\, g(p) \geq 0\}.$$

We often assume, in addition, that $MM \subseteq M$, *i.e.,* that M is a quadratic preordering. One is especially interested in the case where M is finitely generated (as a quadratic module or as a quadratic preordering). In this case, K is the basic closed semialgebraic set $\{p \in V \mid g_i(p) \geq 0, i = 1, \dots, s\}$, where $g_1, \dots, g_s$ are generators for M.

One is especially interested in the case $R = \mathbb{R}$. The quadratic module M is said to be archimedean if for each $f \in A$ there exists an integer $k \geq 1$ such that $k - f \in M$. Results of Putinar [14] and Jacobi [2] show that if $R = \mathbb{R}$ and the quadratic module M is archimedean, then for all $f \in A$, $f > 0 \text{ on } K \Rightarrow f \in M$. When M is a quadratic preordering which is finitely generated, the arithmetic hypothesis "M is archimedean" is equivalent to the geometric hypothesis "K is compact" [21]. This result extends to quadratic modules in various ways [3]. Scheiderer [20] showed that if M is archimedean, then

$$f \in M + (f^2) \text{ and } f \geq 0 \text{ on } K \Longrightarrow f \in M.$$

Received by the editors January 4, 2006; revised July 6, 2006.
This research was supported in part by NSERC of Canada and in part by the Trimester on Real Geometry, Sept. 12 – Dec. 16, 2005, Institut Henri Poincaré, Université de Paris.
AMS subject classification: Primary 13J30; Secondary 12Y05, 13P99, 14P10, 90C22.

https://doi.org/10.4153/CJM-2009-010-4 Published online by Cambridge University Press

See [9] for another proof of this. Applications of this result are given in [17, 19, 20]. The proof of [9, Theorem 2.3] shows that if $R = \mathbb{R}$, V is irreducible, M is archimedean, the zeros of f in K are non-singular points of V, and certain "boundary hessian conditions" hold at each zero of f in K, then $f \in M+(f^2)$ (and consequently, if we also assume $f \geq 0$ on K, then $f \in M$).

We prove that the above stated version of [9, Theorem 2.3] continues to hold when the hypothesis "$R = \mathbb{R}$ and M is archimedean" is replaced by the hypothesis "M is a finitely generated preordering". The proof of this result is, in fact, simpler than the proof of [9, Theorem 2.3]. Using standard ideas from model theory, this yields degree bounds for the presentation of f as an element of $M + (f^2)$ in this case. The result has application to global optimization, yielding a new class of polynomials f such that $f - f_*$ is contained in $\sum R[\underline{x}]^2 + I$, where f_* is the minimum value of f on R^n and I is the gradient ideal of f, *cf.* [10], and again we obtain degree bounds for the presentation. Exploiting other degree bounds in [13,22], we show that if $R = \mathbb{R}$, M is a finitely generated preordering, K is compact, and $f \geq 0$ on K, then there are degree bounds for the presentation of f as an element of M in terms of the presentation of f as an element of $M + (f^2)$. This has application to the optimization algorithm in [5]. We also consider the likelihood of the boundary hessian conditions holding in case the algebraic set V and the boundary of K in V are sufficently well behaved. The conclusion is that, in a suitable sense, these conditions hold with probability 1. In the final section, we determine concrete degree bounds for the algorithms in [5, 10], which ensure that the feasible set of solutions obtained is not the empty set.

1 The Condition $f \in M + (f^2)$

The condition $f \in M + (f^2)$ does not by itself imply $f \geq 0$ on K.

Example 1.1 If the zero set of f is disjoint from K and either M is a finitely generated quadratic preordering, or $R = \mathbb{R}$ and M is a quadratic module which is archimedean, then $-1 \in M + (f^2)$ (so $M + (f^2) = A$).

Indeed, in the quadratic preordering case this follows from the Positivstellensatz. In the quadratic module case it follows using [7, Corollary 3.4.4], for example.

If we know also that the set K is semialgebraic (which is automatically true if M is finitely generated) and each semialgebraically connected component of K contains a point p satisfying $f(p) \geq 0$, then $f \geq 0$ on K. This is clear from the following observation, and is particularly striking if K is semialgebraically connected, *e.g.,* if $K = V = R^n$.

Proposition 1.2 *The condition $f \in M + (f^2)$ implies the following equivalent conditions:*

(i) *The closed set $\{p \in K \mid f(p) \geq 0\}$ is (relatively) open in K.*
(ii) *Every zero of f in K is a local minimum of f on K.*

Proof Suppose $f = \sigma + hf^2$, *i.e.,* $f(1 - hf) = \sigma$ with $\sigma \in M$, $h \in A$. Thus $f(p)(1 - h(p)f(p)) \geq 0$ on K. If $p \in K$ satisfies $f(p) < 0$, then $h(p)f(p) \geq 1$. Since the inequality $hf \geq 1$ defines a closed set disjoint from the zero set of f, the result follows. ■

One is interested in knowing when the converse of Proposition 1.2 holds. In view of Example 1.1, we are mainly interested in the case where the zero set of f has non-empty intersection with K.

We fix some terminology. Given $f, g_1, \dots, g_s \in A$, and setting

$$K = \{p \in V \mid g_i(p) \geq 0, i = 1, \dots, s\},$$

we say f satisfies BHC (boundary hessian conditions) at the point p in K if p is a non-singular point of V and there is some $0 \leq k \leq d$, where $d := \dim(V)$, and some $1 \leq \nu_1 < \cdots < \nu_k \leq s$ such that $g_{\nu_1}, \dots, g_{\nu_k}$ are part of a system of local parameters at p, and the standard sufficient conditions for a local minimum of $f|_L$ at p hold, where L is the subset of V defined by $g_{\nu_1}(x) \geq 0, \dots, g_{\nu_k}(x) \geq 0$. This means that if $t_1, \dots, t_d$ are local parameters at p chosen so that $t_i = g_{\nu_i}$ for $i \leq k$, then in the completion $R[[t_1, \dots, t_d]]$ of A at p, f decomposes as $f = f_0 + f_1 + f_2 + \cdots$ (where f_j is homogeneous of degree j in the variables $t_1, \dots, t_d$ with coefficients in R), $f_1 = a_1 t_1 + \cdots + a_k t_k$ with $a_i > 0$, $i = 1, \dots, k$, and the quadratic form $f_2(0, \dots, 0, t_{k+1}, \dots, t_d)$ is positive definite.

Theorem 1.3 *For any irreducible $V \subseteq \mathbb{R}^n$, and any $f, g_1, \dots, g_s \in A := \mathbb{R}[V]$, if f satisfies BHC at each zero of f in $K := \{p \in V \mid g_i(p) \geq 0, i = 1, \dots, s\}$ and the quadratic module M in A generated by $g_1, \dots, g_s$ is archimedean, then $f \in M + (f^2)$ (and consequently, if we also assume $f \geq 0$ on K, then $f \in M$).*

Proof This follows from the proof of [9, Theorem 2.3]. ■

We note also the following variant of Theorem 1.3.

Theorem 1.4 *For any real closed field R and any irreducible $V \subseteq R^n$, and any $f, g_1, \dots, g_s \in A := R[V]$, if f satisfies BHC at each zero of f in*

$$K := \{p \in V \mid g_i(p) \geq 0, i = 1, \dots, s\},$$

then $f \in M + (f^2)$, where M denotes the quadratic preordering in A generated by $g_1, \dots, g_s$.

Proof Consider the ideal $J = (M + (f^2)) \cap -(M + (f^2))$. As in the proof of [9, Theorem 2.3], it suffices to show that A/J has Krull dimension ≤ 0. For if this is the case, then there are just finitely many minimal prime ideals over J, each corresponding to a zero of f in K. Using the fact that f satisfies BHC at each zero of f in K, and [9, Lemma 2.2], we see that $f \in M + I^k$ holds for each such minimal prime I over J and each $k \geq 1$. By the Chinese Remainder Theorem, $A/J \cong \prod_I A/(I^k + J)$ holds for k sufficiently large. As in the proof of [9, Theorem 1.3], this implies $f \in M + (f^2)$. So we fix a prime ideal I of A minimal subject to the condition $I \supseteq J$, and we try to prove $A/I \cong R$. Let L denote the quotient field of A/I. By [9, Lemma 1.2], $(M + I) \cap -(M + I) = I$, so M extends naturally to a proper preordering of L.

Fix an ordering $\leq$ of L non-negative on this preordering, and let R' denote the real closure of L at $\leq$. We claim that $Z(I)$ (the set of real zeros of I) is the Zariski closure of $Z(I) \cap K$. Fix any $g \in A$, $g \neq 0$ on $Z(I)$. Then $g \notin I$, so $g \neq 0$ in R'. Also $g_i \geq 0$ in R', $i = 1, \dots, s$. By the transfer principle, there exists $p \in Z(I)$ such that $p \in K$ and $g(p) \neq 0$. This proves the claim.

See also [17, Remark 3.12]. On the other hand, the BHC assumption implies that $Z(f) \cap K$ is discrete, *i.e.,* finite. Since $Z(I) \subseteq Z(f)$, this forces $Z(I) \cap K$ to be finite. Thus the algebraic set $Z(I) = Z(I) \cap K$ is zero-dimensional. Since the prime ideal I is real (because $I = (M + I) \cap -(M + I)$), it follows that A/I is real and has Krull dimension zero. By Hilbert's Nullstellensatz, this implies $A/I \cong R$. ■

Note. 1. There is no assumption in Theorem 1.4 that K is bounded or that $f \geq 0$ on K.

2. There is no claim that Theorem 1.4 holds when M is just the quadratic module generated by $g_1, \dots, g_s$. In fact, this is false in general (although it is true if $R = \mathbb{R}$ and M is archimedean, or if $\dim(V) \leq 2$).

Example 1.5 (i) Let M be the quadratic module in $R[x, y, z]$ generated by x, y and $(1 + xy)(z - x^2 - y^2)$. The associated basic closed set K is defined by $x \geq 0$, $y \geq 0$, $z \geq x^2 + y^2$. One checks that $z \geq 0$ on K, the unique zero of z in K occurs at $(0, 0, 0)$ and z satisfies BHC at $(0, 0, 0)$. We claim that $z \notin M + (z^2)$. For suppose $z = \sigma_0 + \sigma_1 x + \sigma_2 y + \sigma_3 (1 + xy)(z - x^2 - y^2) + hz^2$ with $h \in R[x, y, z]$ and σ_i a sum of squares in $R[x, y, z]$. Setting $z = 0$, this yields $0 = \overline{\sigma}_0 + \overline{\sigma}_1 x + \overline{\sigma}_2 y - \overline{\sigma}_3 (1 + xy)(x^2 + y^2)$, where $\overline{\sigma}_i := \sigma_i(x, y, 0)$. A standard valuation-theoretic argument shows that the quadratic module in the function field $R(x, y)$ generated by x, y and $-(1 + xy)$ is proper, so this forces $\overline{\sigma}_i = 0$, *i.e.,* z^2 divides σ_i, for each i. This, in turn, implies that z^2 divides z, a contradiction.

(ii) An even simpler example is obtained by looking at the quadratic module in $R[x, y, z]$ generated by x, y and $-(1 + xy)$. In this example, K is the empty set and $z \notin M + (z^2)$.

An advantage of Theorem 1.4 over Theorem 1.3 is that it yields degree bounds for presentations $f = \sigma + hf^2$, $\sigma \in M$, $h \in R[V]$.

Corollary 1.6 *Given positive integers n, d, δ, there exists a positive integer ℓ such that for each real closed field R and each irreducible algebraic set V of dimension d in R^n defined by polynomial equations $h_i = 0$, $i = 1, \dots, t$, where $h_i \in R[\underline{x}]$ has degree $\leq \delta$, and each basic closed set K in V defined by polynomial inequalities $g_j \geq 0$, $j = 1, \dots, s$, and each f, where $f, g_1, \dots, g_s \in R[V]$ are represented by polynomials of degree $\leq \delta$, if f satisfies BHC at each zero of f in K, then f has a presentation $f = \sigma + hf^2$, where σ is a sum of terms of the form $w^2 g_{i_1} \cdots g_{i_k}$, $k \geq 0$, $1 \leq i_1 < \cdots < i_k \leq s$, where $w \in R[V]$ is represented by a polynomial of degree $\leq \ell$.*

Proof This follows using the standard ultraproduct argument. We sketch the proof.

If the result is false, then there are positive integers n, d, δ such that for each positive integer ℓ there is a real closed field R_ℓ, an irreducible algebraic set V_ℓ in R_ℓ^n of dimension d defined by polynomial equations $h_{i\ell} = 0$, $i = 1, \dots, t$, $\deg(h_{i\ell}) \leq \delta$, a basic closed semialgebraic set K_ℓ in V_ℓ defined by polynomial inequalities $g_{j\ell} \geq 0$, $j = 1, \dots, s$, $\deg(g_{j\ell}) \leq \delta$, and a polynomial f_ℓ with $\deg(f_\ell) \leq \delta$, such that f_ℓ satisfies BHC at each zero of f_ℓ in K_ℓ. But f_ℓ has no presentation $f_\ell = \sigma_\ell + h_\ell f_\ell^2$ where σ_ℓ has a presentation as a sum of terms $w^2 g_{i_1\ell} \cdots g_{i_k\ell}$ with $\deg(w) \leq \ell$.

Consider an ultraproduct $R = \prod_\ell R_\ell/\mathcal{U}$ where $\mathcal{U}$ is a non-principal ultrafilter on $\mathbb{N}$. Define h_i, g_j, f in $R[\underline{x}]$ in the obvious way, by patching together the $h_{i\ell}$ (resp. $g_{j\ell}$, resp. f_ℓ) coefficientwise. Define $V \subseteq R^n$ to be the algebraic set defined by the polynomial equations $h_i = 0$ and $K \subseteq V$ to be the basic closed semialgebraic set in V defined by the inequalities $g_j \geq 0$. One checks that V is irreducible, $\dim(V) = d$, every zero of f in K is a non-singular point of V, and f satisfies BHC at each such zero. It follows from Theorem 1.4 that f has a presentation $f = \sigma + hf^2$ with $\sigma, h \in R[\underline{x}]$, σ a sum of terms $w^2 g_{i_1} \cdots g_{i_k}$. Take σ_ℓ, h_ℓ and the w_ℓ to be the associated elements of $R_\ell[\underline{x}]$ for each ℓ. Then the set of ℓ such that $f_\ell = \sigma_\ell + h_\ell f_\ell^2$ and σ_ℓ is the sum of the corresponding terms $w_\ell^2 g_{i_1\ell} \cdots g_{i_k\ell}$ belongs to the ultrafilter $\mathcal{U}$ (so, in particular, there are arbitrarily large ℓ in this set). Since the w_ℓ have bounded degree, (since $\deg(w_\ell) \leq \deg(w)$) this contradicts our assumptions. ∎

The bound implied by Corollary 1.6 is purely theoretical in nature. There is no claim that this bound is in any sense "good".

Before continuing on, we pause to consider briefly the overall relationship between the various conditions discussed so far:

(i) f satisfies BHC at each zero of f in K.
(ii) $f \in M + (f^2)$.
(iii) The closed set $\{p \in K \mid f(p) \geq 0\}$ is (relatively) open in K, (*i.e.,* it is a union of connected components of K).
(iv) Every zero of f in K is a local minimum of f on K.

Here, V is assumed to be irreducible, and M is the quadratic preordering generated by $g_1, \dots, g_s$. By Theorem 1.4 (i) $\Rightarrow$ (ii). By Remark 1.2 (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (iv). Of course, (iv) $\Rightarrow$ (i) is false in general but, at the same time, it seems clear intuitively that (iv) $\Rightarrow$ (i) is true "with high probability".

2 Application to Global Optimization

Fix $f \in R[\underline{x}]$ and denote by I the gradient ideal of f in $R[\underline{x}]$, *i.e.,* the ideal in $R[\underline{x}]$ generated by the partial derivatives $\frac{\partial f}{\partial x_i}$, $i = 1, \dots, n$. In [10, Theorem 3.1] it was shown that if f achieves a minimum value f_* on R^n and the ideal I is radical, then $f - f_* \in \sum R[\underline{x}]^2 + I$. (Actually, the result [10] is stated only in the case $R = \mathbb{R}$, but the proof given carries through for any real closed R.) Using Theorem 1.4 one can show that this same conclusion can be obtained with a somewhat different hypothesis.

Theorem 2.1 *Suppose $f \in R[\underline{x}]$ achieves a minimum value f_* on R^n and that the matrix $(\frac{\partial^2 f}{\partial x_i \partial x_j}(p))$ is positive definite for each minimum point p of f on R^n. Then $f - f_* \in \sum R[\underline{x}]^2 + I$, where I denotes the gradient ideal of f in $R[\underline{x}]$.*

Example 2.2 The polynomial $f(x) = 6x^2 + 8x^3 + 3x^4$ satisfies the hypothesis of Theorem 2.1 but its gradient ideal is not radical. The polynomial $f(x, y) = x^2$ does

https://doi.org/10.4153/CJM-2009-010-4 Published online by Cambridge University Press

not satisfy the hypothesis of Theorem 2.1, but its gradient ideal is radical.

Suppose $\deg(f) = m$, $f = f_0 + f_1 + \cdots + f_m$, f_i homogeneous of degree i. As in [8, §5], we say f is stably bounded below on R^n if f remains bounded from below on R^n for all sufficiently small perturbations of the coefficients of f (equivalently, if f_m is positive definite).

Later, we show that the set of polynomials stably bounded below on R^n and satisfying the hypotheses of Theorem 2.1 is open and dense in the set of all polynomials stably bounded below on R^n; see Theorem 4.4. In concrete terms, this means that one might expect the hypothesis of Theorem 2.1 to hold rather frequently.

Proof of Theorem 2.1 Replacing f by $f - f_*$, we reduce to the case $f_* = 0$. As explained [10, Theorem 3.3], there are (complex) algebraic sets W_i, $i = 0, \dots, t$ and corresponding ideals J_i, $i = 0, \dots, t$ in $R[\underline{x}]$ such that W_i is the set of complex zeros of J_i, $\bigcap_{i=0}^t J_i = I$, $J_i + J_j = (1)$ for $i \neq j$ (so the Chinese Remainder Theorem applies), W_0 has no real points, and W_i has a real point and f is constant on W_i for $i = 1, \dots, t$. We may assume $f(W_i) = \nu_i$ with $\nu_1 > \cdots > \nu_t = 0$. As explained [10], there exists $\sigma_i \in \sum R[\underline{x}]^2$ such that $f \equiv \sigma_i \mod J_i$ for $i = 0, \dots, t-1$. It remains to show the same holds for $i = t$. By Theorem 1.4, $f = \sigma + hf^2$, *i.e.*, $f(1 - hf) = \sigma$, for some $\sigma \in \sum R[\underline{x}]^2$ and some $h \in R[\underline{x}]$. Since $f = 0$ on W_t, $f^m \in J_t$ for some positive integer m. It follows from this that $1 - hf$ is a unit and a square modulo J_t. Multiplying the equation $f(1 - hf) = \sigma$ by the inverse of $1 - hf$ modulo J_t, this yields $\sigma_t \in \sum R[\underline{x}]^2$ satisfying $f \equiv \sigma_t \mod J_t$ as required. ■

Remark 2.3. The proof of Theorem 2.1 shows that if $f \geq 0$ on $Z(I)$, then $f \in \sum R[\underline{x}]^2 + I + (f^2)$ if and only if $f \in \sum R[\underline{x}]^2 + I$. This is similar in form to Scheiderer's main theorem [20] (if $f \geq 0$ on K, then $f \in M + (f^2)$ if and only if $f \in M$), taking $K =$ the set of real zeros of I and $M = \sum R[\underline{x}]^2 + I$. But there is no requirement here that the real closed field R be the field of real numbers or that the basic closed set K be compact.

As in the case of Theorem 1.4, there is a result on degree bounds to accompany Theorem 2.1.

Corollary 2.4 *Given positive integers n, δ, there exists a positive integer ℓ such that, for each real closed field R and for each polynomial $f \in R[\underline{x}]$ of degree $\leq \delta$, if f achieves a minimum value f_* on R^n, and the matrix $(\frac{\partial^2 f}{\partial x_i \partial x_j}(p))$ is positive definite for each minimum point p of f on R^n, then $f - f_* = \sigma + \sum_{i=1}^n h_i \frac{\partial f}{\partial x_i}$, where $\sigma \in \sum R[\underline{x}]^2$ and $h_1, \dots, h_n \in R[\underline{x}]$, have degree bounded by ℓ.*

Proof The proof here is even simpler than the proof of Corollary 1.6, and will be omitted. ■

We remark that since [10, Theorem 3.1] is valid for any real closed field, and since the hypothesis is expressible in terms of first order formulas, one also has degree bounds in this case. In either case, the degree bounds are purely theoretical in nature. If I is radical and the set of complex zeros of I is finite, then one has concrete degree bounds as described [11].

Example 3.4 of [10] shows that even if f is stably bounded from below on $\mathbb{R}^n$ and the set of complex zeros of the gradient ideal I is finite, the conclusion of Theorem 2.1 (or of [10, Theorem 3.3]) does not hold in general, without some extra hypothesis on f. At the same time, and in contrast to this, [10, Theorem 3.5] shows that for any f, if f is strictly positive on $Z(I)$, then f is a sum of squares modulo I. If f is strictly positive on the set of real zeros of I and the set of complex zeros of I is finite, then as explained in [6, Theorem 23], one can compute degree bounds for the presentation $f \equiv \sigma \bmod I$, σ a sum of squares, using Gröbner basis techniques.

We remark that the assumption that f achieves a minimum value on $\mathbb{R}^n$ is restrictive. The minimum value of f on $Z(I)$ need not equal the infimum of f on $\mathbb{R}^n$, *e.g.*, consider $f(x, y) = x^2 + (xy - 1)^2$. In [23] it was explained how the algorithm in [10] can be modified to handle the case where f is bounded from below on $\mathbb{R}^n$ but does not achieve a minimum value on $\mathbb{R}^n$.

3 Degree Bounds in the Compact Case

We assume in this section that M is the quadratic preordering generated by $g_1, \dots, g_s$. We assume that $R = \mathbb{R}$ and that $K = \{p \in V \mid g_i(p) \geq 0, i = 1, \dots, s\}$ is compact.

Scheiderer proved that if $\dim(K) \geq 2$, there is no degree bound for the degree of a presentation of an element $f \in M$ depending only on $n, V, g_1, \dots, g_s$ and the degree of f [18]. Prestel proved that if $f > 0$ on K, then there is a degree bound for the presentation of f as an element of M depending only on $n, V, g_1, \dots, g_s$, the degree of f and $\frac{\|f\|}{f_*}$, where $\|f\|$ is the norm of f and f_* is the minimum value of f on K [13, Theorem 1] [22, Theorem 3].

We assume $f \geq 0$ on K and that f has some fixed presentation $f = \sigma + hf^2$ with $\sigma \in M$, $h \in A$. By Scheiderer [20], this implies $f \in M$. We establish degree bounds for the presentation of f as an element of M in terms of the degree of the presentation of σ and and the degree and the norm of f and h. The key result is the following variant of [4, Basic Lemma].

Lemma 3.1 *For any real $N > 0$, there exist elements α, β in the preordering generated by $N - t$ and $\frac{1}{2} + t$ in the polynomial ring $\mathbb{R}[t]$ such that $1 = \alpha t + \beta(1 + t)$. Moreover, α and β can be chosen so each term in their presentations has degree $\leq k$, where k is the least integer $\geq \frac{\ln 2}{\ln(1+1/2N)}$.*

Note that for any reasonably large N, $\frac{\ln 2}{\ln(1+\frac{1}{2N})} \approx 2 \ln 2 \cdot N \approx 1.4N$.

Proof Clearly $1 = (1-rt)(1+t)+(-1+r(1+t))t$ for any r. Take $r = \frac{1}{N} \sum_{i=0}^{k-1} (\frac{N-t}{N})^i$, $\alpha = 1 - rt$, $\beta = -1 + r(1 + t)$, where k is the least integer $\geq \frac{\ln 2}{\ln(1+1/2N)}$. Note that

$$\alpha = 1 - rt = 1 - rN\Big(1 - \frac{N - t}{N}\Big) = 1 - \Big(1 - \Big(\frac{N - t}{N}\Big)^k\Big) = \Big(\frac{N - t}{N}\Big)^k,$$

so α has the required form. Also, if $t \neq 0$, then $r = \frac{1-\alpha}{t}$, so

$$\beta = -1 + r(1 + t) = -1 + \frac{(1 + t)(1 - \alpha)}{t} = \frac{1 - (1 + t)\alpha}{t} = \frac{1 - (1 + t)(\frac{N-t}{N})^k}{t}.$$

By [4, Theorem 4.1], it suffices to show that $\beta \geq 0$ on the closed interval $[-\frac{1}{2}, N]$. Let $\gamma = 1 - (1+t)(\frac{N-t}{N})^k$. Clearly $\gamma(0) = 0$. The definition of k implies $\gamma(-\frac{1}{2}) \leq 0$. Computing the derivative of γ, we see that γ is decreasing on $(-\infty, -\frac{k-N}{k+1}]$ and increasing on $[-\frac{k-N}{k+1}, N]$. The definition of k implies $k > N$. It follows that $\gamma \leq 0$ on $[-\frac{1}{2}, 0]$ and $\gamma \geq 0$ on $[0, N]$, so $\beta \geq 0$ on $[-\frac{1}{2}, N]$. ■

Combining Lemma 3.1 with [22, Theorem 3] yields the following.

Corollary 3.2 *Suppose V is an algebraic set in $\mathbb{R}^n$, K is a compact subset of V defined by inequalities $g_i \geq 0$, $i = 1, \dots, s$, $f \geq 0$ on K, and f has a presentation $f = \sigma + hf^2$, $\sigma \in M$, $h \in \mathbb{R}[V]$, where M denotes the quadratic preordering in $\mathbb{R}[V]$ generated by $g_1, \dots, g_s$. Then there exists an integer $\ell \geq 1$ depending only on n, V, $g_1, \dots, g_s$, the degree and the norm of f and h and the degree of the presentation of σ as an element of M, such that f has a presentation as a sum of terms of the form $w^2 g_{i_1} \dots g_{i_k}$, $k \geq 0$, $1 \leq i_1 < \cdots < i_k \leq s$, where $w \in \mathbb{R}[V]$ is represented by a polynomial of degree $\leq \frac{1}{2}(\ell - \sum_{j=1}^k \delta_{i_j})$.*

Proof Write f as $f = \sigma + hf^2 = \sigma + (m+h)f^2 - mf^2 = \sigma' - mf^2$ where $\sigma' := \sigma + (m+h)f^2$. We know that $m + h \in M$ for $m > 0$ sufficiently large. Then m and the degree of the presentation of $m + h$ depend on n, V, $g_1, \dots, g_s$ and the norm and the degree of h. Similarly, we have $N - mf \in M$ for $N > 0$ sufficiently large. Choose α, β in the preordering in $\mathbb{R}[mf]$ generated by $N - mf$ and $\frac{1}{2} + mf$, as in Lemma 3.1, so that $1 = \alpha mf + \beta(1 + mf)$. Then

$$f = \alpha mf^2 + \beta f(1 + mf) = \alpha mf^2 + \beta\sigma'.$$

Since $\frac{1}{2} + mf$ is $\geq \frac{1}{2}$ on K, $\frac{1}{2} + mf$ belongs to M, so this yields a presentation of f as an element of M. The degrees of the presentations of α and β in terms of $N - mf$ and $\frac{1}{2} + mf$ depend on N as in Lemma 3.1. The degree of the presentation of $\frac{1}{2} + mf$ is bounded using [22, Theorem 3]. ■

Note that one might expect to have bounds on the degree of the presentation of σ and on the degree of h using Corollary 1.6. Unfortunately, one does not expect to have much control over the norm of h in general.

4 Likelihood of BHC

We assume here that V is an irreducible algebraic set in R^n, $d := \dim(V)$, and K is the basic closed semialgebraic set in V defined by $g_1 \geq 0, \dots, g_s \geq 0$, $g_1, \dots, g_s \in R[V]$. We deal with the case where the following condition holds for each point p of K:

($*$) p is a non-singular point of V and there exist $0 \leq k \leq d$ and $1 \leq v_1 < \cdots < v_k \leq s$ such that $g_{v_1}, \dots, g_{v_k}$ is part of a system of local parameters at p and, in a neighbourhood of p in V, K is defined by the k inequalities $g_{v_1} \geq 0, \dots, g_{v_k} \geq 0$.

Note: ($*$) is not a condition on K. rather, it is a condition on the particular presentation $g_1 \geq 0, \dots, g_s \geq 0$ of K.

https://doi.org/10.4153/CJM-2009-010-4 Published online by Cambridge University Press

Lemma 4.1 *Suppose $p \in K$ is a non-singular point of V, $u_1, \dots, u_d$ is a system of local parameters at p with $u_i \geq 0$ on K, $i = 1, \dots, \ell$, and $f \in R[V]$ decomposes as $f = a_0 + a_1 u_1 + \cdots + a_\ell u_\ell + \sum_{i,j=1}^d a_{ij} u_i u_j + \cdots$ with $a_i > 0$, $i = 1, \dots, \ell$ and $\sum_{i,j>\ell} a_{ij} u_i u_j$ positive definite. Suppose $t_1, \dots, t_d$ is another system of local parameters at p such that K is defined locally at p by $t_i \geq 0$, $i = 1, \dots, k$. Then $\ell \leq k$ and, after reindexing $t_1, \dots, t_k$ suitably, $f = b_0 + b_1 t_1 + \cdots + b_{\ell'} t_{\ell'} + \sum_{i,j=1}^d b_{ij} t_i t_j + \cdots$ with $b_i > 0$, $i = 1, \dots, \ell'$ and $\sum_{i,j>\ell'} b_{ij} t_i t_j$ positive definite, for some $\ell \leq \ell' \leq k$.*

Proof Say $u_\nu = r_{\nu 1} t_1 + \cdots + r_{\nu d} t_d + \sum_{i,j=1}^d r_{\nu ij} t_i t_j + \cdots$, $\nu = 1, \dots, \ell$. Since u_ν has a local minimum on K at p, $r_{\nu i} = 0$ for $i > k$ and $r_{\nu i} \geq 0$ for $i \leq k$. Reindexing $t_1, \dots, t_k$ suitably, we can assume that for $i > \ell'$, $r_{\nu i} = 0$ for each ν and, for $i \leq \ell'$, $r_{\nu i} > 0$ for some ν and that $u_1, \dots, u_\ell, t_{\ell+1}, \dots, t_d$ is a system of local parameters at p. Since the hypothesis does not depend on how $u_1, \dots, u_\ell$ is completed to a system of parameters at p, we can assume $u_i = t_i$ for $i > \ell$. The linear part of f (as a power series in $t_1, \dots, t_d$) is $b_1 t_1 + \cdots + b_{\ell'} t_{\ell'}$ where $b_i = \sum_{\nu=1}^{\ell} a_\nu r_{\nu i} > 0$, $i = 1, \dots, \ell'$. $\sum_{i,j>\ell'} b_{ij} t_i t_j$ is the quadratic part of the power series in $t_{\ell'+1}, \dots, t_d$ obtained from the power series of f by setting $t_1 = \cdots = t_{\ell'} = 0$. It is easy to see that this is just $\sum_{\nu=1}^{\ell} a_\nu \sum_{i,j>\ell'} r_{\nu ij} t_i t_j + \sum_{i,j>\ell'} a_{ij} t_i t_j$. Since $\ell' \geq \ell$, the second term is positive definite. Also $\sum_{i,j>\ell'} r_{\nu ij} t_i t_j$ is positive semidefinite for each ν (since u_ν has a local minimum on K at p) and $a_\nu > 0$, so the first term is positive semidefinite. This proves $\sum_{i,j>\ell'} b_{ij} t_i t_j$ is positive definite. ∎

Denote by $\mathcal{P}_{m,n}$ the set of all polynomials of degree $\leq m$ in n variables $x_1, \dots, x_n$ with coefficients in the real closed field R. This is a finite dimensional vector space over R and, as such, has natural Euclidean topology. The same holds true for the image of $\mathcal{P}_{m,n}$ in $R[V]$ under the natural map $R[\underline{x}] \to R[V]$. For what we do here, we could work either with $\mathcal{P}_{m,n}$ or with the image of $\mathcal{P}_{m,n}$ in $R[V]$.

Lemma 4.2 *If $f \in \mathcal{P}_{m,n}$ satisfies BHC at some point p in K satisfying $(*)$, then for any $\overline{f} \in \mathcal{P}_{m,n}$ sufficiently close to f and any $q \in K$ sufficiently close to p, if $\overline{f}$ has a local minimum at q, then $\overline{f}$ satisfies BHC at q.*

Proof By $(*)$ we have local parameters $t_1, \dots, t_d$ at p such that K is defined locally at p by $t_1 \geq 0, \dots, t_k \geq 0$, where $\{t_1, \dots, t_k\}$ is some subset of $\{g_1, \dots, g_s\}$, $k \geq 0$. By Lemma 4.1, $f = a_0 + a_1 t_1 + \cdots + a_\ell t_\ell + \sum_{i,j=1}^d a_{ij} t_i t_j + \cdots$ with $a_i > 0$, $1 \leq i \leq \ell$, $\sum_{i,j>\ell} a_{ij} t_i t_j$ positive definite, $0 \leq \ell \leq k$. Since q is close to p, q is a non-singular point of V, $\delta_i := t_i(q)$ is close to 0, and $t'_1, \dots, t'_d$ is a system of local parameters at q, where $t'_i := t_i - \delta_i$. Say $\overline{f} = b_0 + b_1 t'_1 + \cdots + b_d t'_d + \sum_{i,j=1}^d b_{ij} t'_i t'_j + \cdots$. Since $\overline{f}$ is close to f and q is close to p, b_i is close to a_i and b_{ij} is close to a_{ij}. In particular, $b_i > 0$ for $1 \leq i \leq \ell$ and $\sum_{i,j>\ell} b_{ij} t'_i t'_j$ is positive definite. Since $q \in K$, $\delta_i \geq 0$, $i = 1, \dots, k$. Since $\overline{f}$ has a local minimum on K at q, $b_i = 0$ if $i > k$, $b_i = 0$ for all $1 \leq i \leq k$ with $\delta_i > 0$ and $b_i \geq 0$ for all $1 \leq i \leq k$ with $\delta_i = 0$. Reindexing $t_{\ell+1}, \dots, t_k$ we can assume $b_i > 0$ and $\delta_i = 0$ for $i = 1, \dots, \ell'$ and $b_i = 0$ for $i > \ell'$, $\ell \leq \ell' \leq k$. Since $t'_i = t_i \in \{g_1, \dots, g_s\}$, $i = 1, \dots, \ell'$ and $\sum_{i,j>\ell'} b_{ij} t'_i t'_j$ is positive definite (since $\ell' \geq \ell$) the result is now clear. ∎

https://doi.org/10.4153/CJM-2009-010-4 Published online by Cambridge University Press

Lemma 4.3 *Suppose $f \in \mathcal{P}_{m,n}$ achieves its minimum on K at a point $p \in K$ and that* $(*)$ holds at p. Then there exists $g \in \mathcal{P}_{2,n}$ such that $g(p) = 0$, $g(q) > 0$ for $q \in K$, $q \neq p$, and $f + \delta g$ satisfies BHC at p for each $\delta > 0$.

Proof Choose a system of local parameters $t_1, \dots, t_d$ at p so that K is defined locally at p by $t_1 \geq 0, \dots, t_k \geq 0, t_1, \dots, t_k \in \{g_1, \dots, g_s\}$. Since f has a minimum at p, $f = a_0 + a_1 t_1 + \cdots + a_k t_k + \sum_{i,j=1}^{d} a_{ij} t_i t_j + \cdots$ with $a_i \geq 0$, $\sum_{i,j>k} a_{ij} t_i t_j$ positive semidefinite. Choose local generators $t_{d+1}, \dots, t_n$ for the ideal $\mathcal{I}(V)$ at p so that $t_1, \dots, t_n$ is a system of local parameters at p in R^n. Making a suitable affine change in coordinates, we can assume $p = 0$, $t_i = x_i +$ terms of degree ≥ 2 for $i = 1, \dots, n$. It is easy to see that for $\epsilon > 0$ sufficiently close to zero, the open sphere with center

$$(\underbrace{-\epsilon, \dots, -\epsilon}_{k \text{ times}}, \underbrace{0, \dots, 0}_{d-k \text{ times}}, \underbrace{-\epsilon, \dots, -\epsilon}_{n-d \text{ times}})$$

and radius $\epsilon\sqrt{n-d+k}$ has empty intersection with the set K. Take $g = 2\epsilon \sum_{j \leq k} x_j + 2\epsilon \sum_{j>d} x_j + \|x\|^2$. Viewed as a power series in $t_1, \dots, t_d$ in the natural way, g has the form $g = 2\epsilon \sum_{i=1}^{k} t_i + \sum_{i=1}^{d} t_i^2 + \epsilon \sum_{i,j=1}^{d} t_i t_j$ for some $b_{ij} \in R$ (coming from the degree 2 parts of the various $x_i - t_i$). Since the quadratic form $\sum_{i>k} t_i^2 + \epsilon \sum_{i,j>k} b_{ij} t_i t_j$ is positive definite for ϵ sufficiently close to 0, the result is clear. ■

If K is bounded, every $f \in \mathcal{P}_{m,n}$ achieves a minimum value on K. Since we would also like to say something in the case when K is unbounded, we must restrict a bit the sort of elements of $\mathcal{P}_{m,n}$ that we consider, in general. We consider the following two sets:

$$\mathcal{B}_{m,K} := \{f \in \mathcal{P}_{m,n} \mid \exists N, \epsilon > 0 \text{ such that } \forall x \in K, \|x\| \geq N \Rightarrow f(x) \geq \epsilon\|x\|^m\}$$
$$\mathcal{C}_{m,K} := \{f \in \mathcal{B}_{m,K} \mid f \text{ satisfies BHC at each minimum of } f \text{ on } K\}.$$

The set $\mathcal{B}_{m,K}$ consists of all $f \in \mathcal{P}_{m,n}$ which remain bounded below on K for small perturbations of the coefficients of f. This is straightforward to check. If K is bounded, then $\mathcal{B}_{m,K} = \mathcal{P}_{m,n}$. If $K = V = R^n$, then $\mathcal{B}_{m,K}$ consists of all polynomials of degree m in $\mathcal{P}_{m,n}$ which are stably bounded below on R^n in the sense of [8, §5] (so $\mathcal{B}_{m,K} = \varnothing$ if m is odd).

Theorem 4.4 *The set $\mathcal{B}_{m,K}$ is open in $\mathcal{P}_{m,n}$. If V is irreducible and* $(*)$ *holds at each point p of K, then the set $\mathcal{C}_{m,K}$ is open in $\mathcal{P}_{m,n}$. If, in addition, $m \geq 2$, then $\mathcal{C}_{m,K}$ is dense in $\mathcal{B}_{m,K}$.*

Proof Suppose $f \in \mathcal{B}_{m,K}$. Thus we have $N, \epsilon > 0$ such that $x \in K$, $\|x\| \geq N \Rightarrow f(x) \geq \epsilon\|x\|^m$. Write f as $f(x) = \sum_{|\alpha| \leq m} a_\alpha x^\alpha$ where $x^\alpha := x_1^{\alpha_1} \dots x_n^{\alpha_n}$, $|\alpha| := \alpha_1 + \cdots + \alpha_n$. Suppose $g = \sum_\alpha b_\alpha x^\alpha$ with $|b_\alpha - a_\alpha| \leq \delta$ for each α where

$$\delta := \frac{\epsilon}{2\sum_{i=0}^{m} n^i}.$$

Then for $x \in K$, $\|x\| \geq \max\{1, N\}$,

$$\begin{aligned} g(x) = f(x) + \sum_{\alpha}(b_\alpha - a_\alpha)x^\alpha &\geq f(x) - \sum_{\alpha}|b_\alpha - a_\alpha| \cdot |x^\alpha| \\ &\geq f(x) - \delta\sum_{\alpha}|x^\alpha| \geq f(x) - \delta\sum_{i=0}^{m}(|x_1| + \cdots + |x_n|)^i \\ &\geq f(x) - \delta\sum_{i=0}^{m} n^i\|x\|^i \geq f(x) - \delta\sum_{i=0}^{m} n^i\|x\|^m \\ &\geq \Big(\epsilon - \delta\sum_{i=0}^{m} n^i\Big)\|x\|^m = \frac{\epsilon}{2}\|x\|^m. \end{aligned}$$

This proves that $\mathcal{B}_{m,K}$ is open. Each $f \in \mathcal{B}_{m,K}$ achieves a minimum on K at some point $p \in K$ (assuming $K \neq \varnothing$). The last assertion is clear from this, using Lemma 4.3. It remains to check that $\mathcal{C}_{m,K}$ is open. Fix $f \in \mathcal{C}_{m,K}$. Replacing f by $f - f_*$ where $f_* :=$ the minimum value of f on K, we may assume $f_* = 0$. Since f satisfies BHC at each minimum point, f has only finitely many minimum points in K, say $p_1, \dots, p_k$ are the minimum points. By Lemma 4.2 we have an open ball B_i about p_i such that, for $g \in \mathcal{P}_{m,n}$ sufficiently close to f, g satisfies BHC at each minimum point of g in $K \cap B_i$. We also have $N, \epsilon > 0$ such that $\forall x \in K$, $\|x\| \geq N \Rightarrow f(x) \geq \epsilon\|x\|^m$. We may assume $N \geq 1$. Let B denote the closed ball centered at the origin with radius N. Let $\delta > 0$ be the minimum value of f on $K \cap (B \setminus \bigcup_{i=1}^k B_i)$. Choose $g \in \mathcal{P}_{m,n}$ so close to f that $g(p_1) < \min\{\epsilon/2, \delta/2\}, g(x) \geq \delta/2$ on $K \cap (B \setminus \bigcup_{i=1}^k B_i)$, $g(x) \geq (\epsilon/2)\|x\|^m$ on $K \setminus B$, and g satisfies BHC at each minimum point of g in $K \cap (\bigcup_{i=1}^k B_i)$. Then each minimum of g on K occurs in some B_i, so g satisfies BHC at each minimum point. ■

Corollary 4.5 *Suppose V is irreducible, K is bounded, and* $(*)$ holds at each point p of K. Then the set

$$\mathcal{C}_{m,K} := \{f \in \mathcal{P}_{m,n} \mid f \text{ satisfies BHC at each minimum of } f \text{ on } K\}$$

is open and dense in $\mathcal{P}_{m,n}$ (assuming $m \geq 2$).

Corollary 4.6 *Let*

$$\mathcal{B}_{m,n} := \{f \in \mathcal{P}_{m,n} \mid \deg(f) = m, f \textit{ is stably bounded below on } R^n\},$$
$$\mathcal{C}_{m,n} := \{f \in \mathcal{B}_{m,n} \mid \textit{BHC holds at each minimum point of } f \textit{ on } R^n\}.$$

Then $\mathcal{C}_{m,n}$ is open and dense in $\mathcal{B}_{m,n}$.

In view of Theorem 1.3, Corollary 4.5 says something about the likelihood of $f - f_* \in M$ holding, where f_* denotes the minimum value of f on K and M denotes the quadratic module in $R[V]$ generated by $g_1, \dots, g_s$. Of course, the hypothesis $(*)$

of Corollary 4.5 applies in a wide variety of cases. For example, it holds if $V = R^n$ and K is the closed ball defined by $\|x\| \leq 1$ or the hypercube $[-1, 1]^n$ (with the obvious presentation).

Similarly, Corollary 4.6 says something about the likelihood of $f - f_* \in \sum R[\underline{x}]^2 + I$ holding, where I is the gradient ideal of f and f_* is the minimum value of f on R^n, given that f is stably bounded below on R^n.

5 Bounds Which Ensure a Non-Empty Feasible Set

Fix $f \in \mathbb{R}[\underline{x}]$. Set

$$f_* = \inf\{f(p) \mid p \in \mathbb{R}^n\}, \ f_{\rm sos} = \sup\left\{\lambda \mid \lambda \in \mathbb{R}, f - \lambda \in \sum \mathbb{R}[\underline{x}]^2\right\}.$$

Decompose f as $f = f_0 + \cdots + f_m$ where f_i is homogeneous of degree i, $f_m \neq 0$. Assume $m > 0$. A necessary condition for $f_* \neq -\infty$ is that (m is even and) f_m is positive semidefinite. A sufficient condition for $f_* \neq -\infty$ is that f is stably bounded from below on $\mathbb{R}^n$, *i.e.,* that f_m is positive definite. Moreover, in this situation, f achieves a minimum value on $\mathbb{R}^n$.

Clearly $f_{sos} \leq f_*$. If $n = 1$, $m = 2$, or $n = 2$ and $m = 4$, then $f_{sos} = f_*$. For all other choices of n and m there exists f such that $f_{sos} < f_*$. This was known already to Hilbert in 1888. One would like to know how closely f_{sos} approximates f_* in general. As a first step, one would at least like to know when $f_{sos} \neq -\infty$, *i.e.,* when there exists $\lambda \in \mathbb{R}$ such that $f - \lambda$ is a sum of squares.

Denote by $\Pi_{m,n}$ the set of all positive semidefinite forms of degree m in $x_1, \ldots, x_n$ and by $\Sigma_{m,n}$ the subset of $\Pi_{m,n}$ consisting of all elements of $\Pi_{m,n}$ which are sums of squares. Then $\Pi_{m,n}$ and $\Sigma_{m,n}$ are closed cones in the $\mathbb{R}$-vector space consisting of all forms of degree m in the variables $x_1, \ldots, x_n$.

Proposition 5.1 *A necessary condition for $f_{sos} \neq -\infty$ is that f_m is a sum of squares. A sufficient condition for $f_{sos} \neq -\infty$ is that f_m is an interior point of the cone $\Sigma_{m,n}$.*

Example 5.2 (i) The Motzkin polynomial $f = 1 - 3x^2y^2 + x^4y^2 + x^2y^4$ satisfies $f_* = 0$, $f_{sos} = -\infty$ and $f_6 = x^4y^2 + x^2y^4 \in \Sigma_{6,2}$. This shows that the necessary condition on Proposition 5.1 is not sufficient.

(ii) If $f = (x - y)^2$, then $f_* = f_{sos} = 0$ and $f_2 = (x - y)^2$ is a boundary point of $\Sigma_{2,2}$. This shows that the sufficient condition in Proposition 5.1 is not necessary.

(iii) Let $f = 1 - 3x^2y^2 + x^4y^2 + x^2y^4 + \epsilon(x^6 + y^6)$, $\epsilon > 0$. Here, $f_* = \frac{\epsilon}{1+\epsilon}$. Since $f_6 = x^4y^2 + x^2y^4 + \epsilon(x^6 + y^6)$ is an interior point of the cone $\Sigma_{6,2}$, $f_{sos} \neq -\infty$. Observe however that $f_{sos} \to -\infty$ as $\epsilon \to 0$. For, if this were not the case, then there would be some real number N such that for any choice of $\epsilon > 0$, $f + N$ is a sum of squares. Letting $\epsilon \to 0$, this would contradict the conclusion in (i).

Regarding interior points of $\Sigma_{m,n}$, we make use of the following.

Proposition 5.3 (i) *Suppose f is an interior point of $\Sigma_{m,n}$ and $g \in \Sigma_{m,n}$. Then g is an interior point of $\Sigma_{m,n}$ if and only if $g - \epsilon f \in \Sigma_{m,n}$ for some real $\epsilon > 0$.*

(ii) *$(x_1^2 + \cdots + x_n^2)^{m/2}$ and $x_1^m + \cdots + x_n^m$ are interior points of $\Sigma_{m,n}$.*

https://doi.org/10.4153/CJM-2009-010-4 Published online by Cambridge University Press

Remark 5.4. In [12], f_* is approximated by computing f_{sos} in a large number of random instances with $f_m = x_1^m + \cdots + x_n^m$. Since $x_1^m + \cdots + x_n^m$ is an interior point of $\Sigma_{m,n}$, Proposition 5.1 explains why $-\infty$ was never obtained as an output in these computations. (But it does not explain the high degree of accuracy that was observed, which is still a bit of a mystery.)

We sketch proofs of Proposition 5.1 and Proposition 5.3.

Proof of Proposition 5.3 Let $m = 2k$. The proof of (i) is trivial. To show $p := (x_1^2+\cdots+x_n^2)^k$ is an interior point of $\Sigma_{m,n}$ we must show that if we modify p by terms of degree m the form bx^α, with $|b|$ sufficiently small, we remain in $\Sigma_{m,n}$. Now p is a sum of terms ax^α, where a is positive and x^α is a square (of a monomial of degree k) and, furthermore, all such terms appear in the expansion of p. Thus the result is clear for terms of the form bx^α where x^α is a square. If x^α is not a square, write $x^\alpha = x^\beta x^\gamma$ where x^β, x^γ have degree k, and use the identity $\pm 2x^\alpha = (x^\beta \pm x^\gamma)^2 - (x^{2\beta} + x^{2\gamma})$.

Lemma 5.5 $x_0^{2k} - \frac{1}{2^{k-1}}(\sum_{i=0}^n x_i^2)^k + (\sum_{i=1}^n x_i^2)^k$ *is a sum of squares.*

Proof Dehomogenizing, we can assume $x_0 = 1$. Let

$$H(t) = 1 - \frac{1}{2^{k-1}}(1+t)^k - t^k.$$

Then $H(t)$ has minimum value 0 on the interval $[0,\infty)$, which occurs at $t = 1$. Thus $H(t) \in \sum \mathbb{R}[t]^2 + \sum \mathbb{R}[t]^2 t$. Substituting $t = x_1^2 + \cdots + x_n^2$ yields the result we want. ■

Using Lemma 5.5 and induction on n, one checks easily that $x_1^m + \cdots + x_n^m - \epsilon(\sum_{i=1}^n x_i^2)^k$ is a sum of squares, where

$$\epsilon := \frac{1}{2^{(k-1)(n-1)}}.$$

According to Proposition 5.3(1), this implies that $x_1^m + \cdots + x_n^m$ is also an interior point of $\Sigma_{m,n}$. ■

Proof of Proposition 5.1 The first assertion is trivial. Suppose f has degree $m = 2k$ and f_m is an interior point of $\Sigma_{m,n}$. For each term cx^α of degree $< m$ appearing in f where x^α is not a square, write $x^\alpha = x^\beta x^\gamma$ where x^β has degree $< k$ and x^γ has degree $\le k$. If x^β, x^γ both have degree $< k$, write cx^α as $\frac{|c|}{2}(x^\beta \pm x^\gamma)^2 - \frac{|c|}{2}(x^{2\beta} + x^{2\gamma})$. If x^γ has degree k, write cx^α as $\frac{|c|}{2}(\frac{1}{\delta}x^\beta \pm \delta x^\gamma)^2 - \frac{|c|}{2}(\frac{1}{\delta^2}x^{2\beta} + \delta^2 x^{2\gamma})$, where $\delta > 0$ is close to zero. In this way, one is reduced to the case where x^α is a square for each term cx^α of degree $< m$ appearing in f. Write f_m as $f_m = g + \epsilon(\sum_{i=1}^n x_i^2)^k$, $g \in \Sigma_{m,n}$, $\epsilon > 0$. Scaling suitably, we can assume $\epsilon = 1$. Lemma 5.5 implies that the polynomial

$$x_0^{2k} - \frac{1}{2^{k-1}-1}\sum_{i=1}^{k-1}\binom{k}{i}x_0^{2i}(x_1^2+\cdots+x_n^2)^{k-i} + (x_1^2+\cdots+x_n^2)^k \tag{5.1}$$

is a sum of squares. Taking x_0 to be a real number which is so large that the coefficients of the monomials in $x_1,\ldots,x_n$ coming from the middle term of (5.1) (these are

https://doi.org/10.4153/CJM-2009-010-4 Published online by Cambridge University Press

negative numbers) are $\leq$ the coefficients of the corresponding monomials appearing in f, and using the fact that (5.1) is a sum of squares, we see that $f - f_0 + x_0^m$ is a sum of squares. ■

We now explain how Proposition 5.1 combines with [15, Theorem 3.12] to yield degree bounds which ensure the existence of feasible solutions for the optimization method described in [10]. We use notation from [15]. If p is a form of (even) degree m in n variables, with coefficients in $\mathbb{R}$,

$$\epsilon(p) := \frac{\inf\{p(u) \mid u \in S^{n-1}\}}{\sup\{p(u) \mid u \in S^{n-1}\}}.$$

Corollary 5.6 *Suppose $f \in \mathbb{R}[\underline{x}]$ is stably bounded from below on $\mathbb{R}^n$, $\deg(f) = m > 0$, and $r > \frac{nm(m-1)}{(4\log 2)\epsilon(f_m)} - \frac{n+m}{2}$. Then there exist $h_1, \dots, h_n \in \mathbb{R}[\underline{x}]$ of degree $\leq 2r+1$ and $\lambda \in \mathbb{R}$ such that $f + \sum_{i=1}^n h_i \frac{\partial f}{\partial x_i} - \lambda \in \sum \mathbb{R}[\underline{x}]^2$.*

Proof Decompose $p := f_m$ as $p = \overline{p} + \delta(\sum_{i=1}^n x_i^2)^{m/2}$, $\delta > 0$. For δ close to zero, the form $\overline{p}$ is positive definite. By [15, Theorem 3.12], $(\sum_{i=1}^n x_i^2)^r \overline{p}$ is a sum of squares for $r \geq \frac{nm(m-1)}{(4\log 2)\epsilon(\overline{p})} - \frac{n+m}{2}$. Since $\epsilon(\overline{p}) \to \epsilon(p)$ as $\delta \to 0$, this proves that $(\sum_{i=1}^n x_i^2)^r p$ is an interior point of $\Sigma_{m+2r,n}$, for r as in the statement of Corollary 5.6. Combining this with the fact that the highest degree term of $\frac{1}{m}\sum_{i=1}^n x_i \frac{\partial f}{\partial x_i}$ is precisely p, we see that the highest degree term of

$$\overline{f} = f + \Big(\Big(\sum_{j=1}^n x_j^2\Big)^r - 1\Big)\frac{1}{m}\sum_{i=1}^n x_i \frac{\partial f}{\partial x_i}$$

is an interior point of $\Sigma_{m+2r,n}$. The result follows now by applying Proposition 5.1 to the polynomial $\overline{f}$, and taking $h_i = \frac{1}{m}x_i((\sum_{j=1}^n x_j^2)^r - 1)$. ■

One might suspect that the bound given by Corollary 5.6 is not the best possible. At the same time, it is not clear, to the author at least, how one can improve on it in general. Of course, if p is an interior point of $\Sigma_{m,n}$, we can take $r = 0$.

If the set of complex zeros of the gradient ideal of f is finite, there is a simpler bound.

Corollary 5.7 *Assume the set of complex zeros of the gradient ideal I of f is finite, and let e be the least even integer $\geq m$ such that, for each $i = 1, \dots, n$, x_i^e is a linear combination of monomials of degree $< e$ modulo I. Then there exists $h \in I$ of degree e and $\lambda \in \mathbb{R}$ such that $f + h - \lambda \in \sum \mathbb{R}[\underline{x}]^2$.*

Proof By assumption, there exists $g \in \mathbb{R}[\underline{x}]$ of degree $< e$ such that $\sum_{i=1}^n x_i^e + g \in I$. The highest degree term of $\overline{f} = f + \sum_{i=1}^n x_i^e + g - \frac{1}{m}\sum_{i=1}^n x_i \frac{\partial f}{\partial x_i}$ is $\sum_{i=1}^n x_i^e$, which is an interior point of $\Sigma_{e,n}$, by Proposition 5.3. The result follows by applying Proposition 5.1 to the polynomial $\overline{f}$, taking $h = \sum_{i=1}^n x_i^e + g - \frac{1}{m}\sum_{i=1}^n x_i \frac{\partial f}{\partial x_i}$. ■

In particular cases, one can compute the integer e using Gröbner basis techniques. The bound in Corollary 5.7 may be better than the bound in [6, Theorem 23] in certain cases (*e.g.*, if $f_m = \sum_{i=1}^n x_i^m$, then $e = m$) but, at the same time, of course, the conclusion of Corollary 5.7 is considerably weaker than the conclusion in [6, Theorem 23].

We now turn our attention to the optimization method in the compact case described in [5]. Again, we look for degree bounds which ensure the existence of feasible solutions. We begin with the special case where the compact set in question is the closed ball defined by the single inequality $\sum_{i=1}^n x_i^2 \le N$.

Proposition 5.8 *Suppose $f \in \mathbb{R}[\underline{x}]$, $\deg(f) = m$, and $N > 0$. Then there exists $\lambda \in \mathbb{R}$ and $\sigma, \tau \in \sum \mathbb{R}[\underline{x}]^2$ such that $f - \lambda = \sigma + \tau(N - \sum_{i=1}^n x_i^2)$, where σ and $\tau(N - \sum_{i=1}^n x_i^2)$ each have degree $\le m$ (resp. $m+1$) if m is even (resp. if m is odd).*

Proof Let $f = \sum a_\alpha x^\alpha$, where $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. The construction of λ, σ, and τ is completely algorithmic. Let $\lambda = -P$ where

$$P := \sum_\alpha |a_\alpha| (\sqrt{N})^{\alpha_1 + \cdots + \alpha_n},$$

and α runs through all indices such that x^α is not a perfect square and $a_\alpha \neq 0$, or x^α is a perfect square and $a_\alpha < 0$. Replacing the variables $x_1, \dots, x_n$ by $y_1, \dots, y_n$, where $y_i = \frac{x_i}{\sqrt{N}}$, we are reduced to proving the result when $N = 1$. Clearly it suffices to consider the case where f is itself a monomial, say $f = a x^\alpha$. We can assume further that either x^α is a non-square and $a = \pm 1$ or x^α is a square and $a = -1$. One makes use of the identity

$$1 - x_j^2 = \sum_{i \neq j} x_i^2 + \Big(1 - \sum_{i=1}^n x_i^2\Big).$$

To handle the case where x^α is a square, use the identity

$$1 - u^2 v^2 = \frac{1}{2}(1+u^2)(1-v^2) + \frac{1}{2}(1-u^2)(1+v^2),$$

and induction on m. To reduce from the case where x^α is not a square to the case where x^α is a square, use the identity

$$1 \pm uv = \frac{1}{2}(u \pm v)^2 + \frac{1}{2}(1-u^2) + \frac{1}{2}(1-v^2),$$

where u and v have the same degree if m is even, and $\deg(u) = \deg(v) + 1$ if m is odd. The details are left to the reader. ∎

Finally we consider the case where the compact set K in question is defined by finitely many polynomial inequalities $g_i \ge 0$, $i = 1, \dots, s$. If we assume the associated quadratic module is archimedean, then we have a relation $N - \sum_{i=1}^n x_i^2 =$

https://doi.org/10.4153/CJM-2009-010-4 Published online by Cambridge University Press

$\sigma_0 + \sigma_1 g_1 + \cdots + \sigma_s g_s$, for some $N > 0$, where the σ_i are sums of squares. Applying Proposition 5.8, this yields

$$f - \lambda = \sigma + \tau\Big(N - \sum_{i=1}^{n} x_i^2\Big) = (\sigma + \tau\sigma_0) + (\tau\sigma_1)g_1 + \cdots + (\tau\sigma_i)g_i.$$

We have good degree bounds on σ and τ, given by Proposition 5.8, but since the degrees of the σ_i may be large, the overall degree bound obtained in this way may not be good. Of course, one way to get around this (and at the same time to ensure that the quadratic module is archimedean) is to simply add the inequality $N - \sum_{i=1}^{n} x_i^2 \geq 0$ to our description of K.

References

[1] J. Bochnak, M. Coste, and M.-F. Roy, *Real Algebraic Geometry.* Ergebnisse der Mathematik und ihrer Grenzgebiete 36, Springer-Verlag, Berlin, 1998.

[2] T. Jacobi, *A representation theorem for certain partially ordered commutative rings.* Math. Zeit. **237**(2001), no. 2, 259–273.

[3] T. Jacobi and A. Prestel, *Distinguished presentations of strictly positive polynomials.* J. Reine Angew. Math. **532**(2001), 223–235.

[4] S. Kuhlmann, M. Marshall, and N. Schwartz, *Positivity, sums of squares and the multi-dimensional moment problem. II.* Adv. Geom. **5**(2005), no. 4, 583–606.

[5] J. B. Lasserre, *Optimisation globale et théorie des moments.* C. R. Acad. Sci. Paris Sér. I Math. **331**(2000), no. 11, 929–934.

[6] M. Laurent, *Semidefinite representations for finite varieties.* Math. Program. **109**(2007), no. 1, 1–26.

[7] M. Marshall, *Positive polynomials and sums of squares.* Dottorato de Ricerca in Matematica, Universita Pisa, 2000.

[8] ———, *Optimization of polynomial functions.* Canad. Math. Bull. **46**(2003), no. 4, 575–587.

[9] ———, *Representation of non-negative polynomials with finitely many zeros.* Ann. Fac. Sci., Toulouse, **15**(2006), 599–609.

[10] J. Nie, J. Demmel, and B. Sturmfels, *Minimizing polynomials via sum of squares over the gradient ideal.* Math. Program. **106**(2006), no. 3, 587–606.

[11] P. Parrilo, *An explicit construction of distinguished representations of polynomials nonnegative over finite sets.* http://www.control.ee.ethz.ch/~parrilo/pubs/files/aut02-02.pdf.

[12] P. Parrilo, and B. Sturmfels, *Minimizing polynomial functions.* In: Algorithmic and Quantitative Real Algebraic Geometry. DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 60, American Mathematical Society, Providence, RI, 2003, pp. 83–100.

[13] A. Prestel, *Bounds for polynomials positive on compact semialgebraic sets.* In: Valuation Theory and Its Applications. Fields Inst. Commun. 32, American Mathematical Society, Providence, RI, 2002, pp. 253–260.

[14] M. Putinar, *Positive polynomials on compact semi-algebraic sets.* Indiana Univ. Math. J. **42**(1993), no. 3, 969–984.

[15] B. Reznick, *Uniform denominators in Hilbert's seventeenth problem.* Math. Zeit. **220**(1995), no. 1, 75–98.

[16] C. Scheiderer, *Sums of squares of regular functions on real algebraic varieties.* Trans. Amer. Math. Soc. **352**(2000), no. 3, 1039–1069.

[17] ———, *Sums of squares on real algebraic curves.* Math. Zeit. **245**(2003), no. 4, 725–760.

[18] ———, *Non-existence of degree bounds for weighted sums of squares representations.* J. Complexity **21**(2005), no. 6, 823–844.

[19] ———, *Sums of squares on real algebraic surfaces.* Manuscripta Math. **119**(2006), no. 4, 395–410.

[20] ———, *Distinguished representations of non-negative polynomials.* J. Algebra **289**(2005), no. 2, 558–573.

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

[22] M. Schweighofer, *On the complexity of Schmüdgen's positivstellensatz.* J. Complexity **20**(2004), no. 4, 529–543.

[23] ———, *Global optimization of polynomials using gradient tentacles and sums of squares.* SIAM J. Optim. **17**(2006), no. 3, 920–942. (electronic)

Department of Mathematics and Statistics, University of Saskatchewan, Saskatoon, SK, S7N 5E6
e-mail: marshall@snoopy.usask.ca