HAL
archives-ouvertes.fr

Towards fast one-block quantifier elimination through generalised critical values

Jérémy Berthomieu, Andrew Ferguson, Mohab Safey El Din

▶ **To cite this version:**

Jérémy Berthomieu, Andrew Ferguson, Mohab Safey El Din. Towards fast one-block quantifier elimination through generalised critical values. ACM Communications in Computer Algebra, Association for Computing Machinery (ACM), 2020. hal-02929626

HAL Id: hal-02929626
https://hal.archives-ouvertes.fr/hal-02929626

Submitted on 9 Sep 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Towards fast one-block quantifier elimination through generalised critical values

Jérémy Berthomieu, Andrew Ferguson and Mohab Safey El Din

Sorbonne Université, CNRS, LIP6, F-75005, Paris, France

jeremy.berthomieu@lip6.fr; andrew.ferguson@lip6.fr; mohab.safey@lip6.fr

1 Introduction and Preliminaries

One-block quantifier elimination is comprised of computing a semi-algebraic description of the projection of a semi-algebraic set or of deciding the truth of a semi-algebraic formula with a single quantifier.

Until now, it has been tackled in practice by using variants and improvements of the Cylindrical Algebraic Decomposition (CAD) algorithm. For example, see the software packages QEPCAD [3], RegularChains [10] or the system Mathematica [11]. This algorithmic framework suffers from a complexity that is doubly exponential in the dimension of the ambient space. However, in [6] it is shown that one-block quantifier elimination can be performed within a complexity that is singly exponential in that dimension.

This abstract reports on preliminary works which would allow one to avoid CAD and obtain faster one-block quantifier elimination algorithms in practice. Given a semi-algebraic set $S \subset \mathbb{R}^n$ and a projection map $\pi : S \to \mathbb{R}^p$, the core idea is to identify a real algebraic set $\mathscr{K} \subset \mathbb{R}^p$ with codimension at least one that contains the boundary of the projection $\pi(S)$. Then, the connected components of $\mathbb{R}^p - \mathscr{K}$ would provide a finite collection of open semi-algebraic sets of $\mathbb{R}^p$ whose union is dense in $\pi(S)$.

Polynomial optimisation provides additional geometric ingredients which aid the development of the above approach and as such serves as an illustrative context for these techniques. To optimise a function f over a compact smooth real algebraic set S one may compute the critical values of f, noting that by Sard's Theorem these are in finite number, and identify the one corresponding to the minimum. This approach has been extended to one-block quantifier elimination in [8]. Furthermore, by Thom's isotopy lemma [4], critical values capture the topological changes in the fibres of f.

Our goal is now to further develop these techniques by dropping the compactness assumption. In this context, computing the set of critical values is no longer sufficient. For instance, the map $f : \mathbb{R}^2 \to \mathbb{R}$ defined by $f(z_1, z_2) = z_1^4 + (z_1 z_2 - 1)^2$ is clearly non-negative as it is a sum of squares. However, along the path $\theta(t) = (1/t, t)$ we see that $f(\theta(t))$ converges to 0 as $t \to \infty$. We deduce that the infimum of f, f^*, is 0 and is not reached. Furthermore, a short computation, solving the system $\frac{\partial f}{\partial z_1} = \frac{\partial f}{\partial z_2} = 0$, confirms that 0 is not a critical value of f. This illustrates that one needs a notion of *asymptotic critical values* which captures topological changes in the fibres of polynomial maps "at infinity".

For the remainder of this article, let $\mathbb{K}$ be a field (either $\mathbb{R}$ or $\mathbb{C}$). The foundations for defining a notion of asymptotic critical values of polynomial mappings, $f = (f_1, \ldots, f_p) \in \mathbb{K}[z_1, \ldots, z_n]^p$, were introduced by Rabier in [1]. It has been shown that with a slightly modified definition, one that we will use, this set has dimension at most $p - 1$. Therefore, Sard's theorem extends beyond critical values [2]. Define the Kuo distance

$$\kappa(\mathrm{d}f(z)) = \min_{1 \leq j \leq p} \|w_j(z)\|,$$

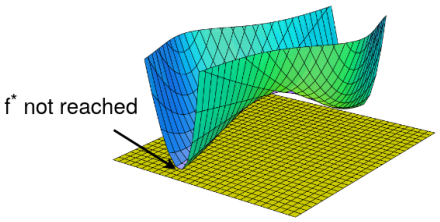
where $w_j(z)$ is the restriction of $\mathrm{d}f_j$ to the kernel of the Jacobian matrix of f with the jth row removed. The set of asymptotic critical values is defined as follows in [2]:

$$K_\infty(f) = \{c \in \mathbb{C}^p | \exists z(t) \in \mathbb{K}^n \text{ such that } \|z(t)\| \to \infty, f(z(t)) \to c, \|z(t)\|\kappa(\mathrm{d}f(z(t))) \to 0\}.$$

Furthermore, we denote by $K_0(f)$ the set of critical values of the map f. Using the above notations we can define it as

$$K_0(f) = \{c \in \mathbb{C}^p | \exists z \in \mathbb{K}^p \text{ such that } \mathrm{d}_z f \text{ is not surjective}\}.$$

Theorem 1 ([2, Theorems 2.1, 3.1, and 4.1])**.** Let $f : \mathbb{K}^n \to \mathbb{K}^p$ be a polynomial mapping. Then, the set of asymptotic critical values of f, $K_\infty(f)$, is a complex algebraic set of dimension less than p. Furthermore, let $V \subset \mathbb{C}^n$ be a connected component of $\mathbb{C}^n \setminus (K_0(f) \cup K_\infty(f))$. Then, $f^{-1}(V) = \emptyset$ or $f : f^{-1}(V) \to V$ is a locally trivial fibration.



Consider once more the example $f = z_1^4 + (z_1 z_2 - 1)^2$ and the path $\theta(t) = (1/t, t)$. For $i, j \in \{1, 2\}$, we see that as $t \to \infty$, $\theta(t)_i \frac{\partial f}{\partial z_j}(\theta(t)) \to 0$. Thus, 0 is an asymptotic critical value of f.

Moreover, degree bounds for the set of asymptotic critical values of such a map f have previously been given. Without delving too deep into the details, it is shown in [5] that $K_0(f) \cup K_\infty(f)$ is contained in an algebraic set whose degree lies in $O(D^n)$ where D dominates the degrees of the components of f. Note that one cannot hope to do much better since similar Bézout-like bounds already apply to $K_0(f)$ and in the worst-case these bounds are reached.

Hence, a topical issue now is to obtain an efficient algorithm for computing asymptotic critical values. Our contributions are the design and implementation of such an algorithm and new degree bounds on the asymptotic critical values. Additionally, when $p = 1$ the practical behaviour of this algorithm demonstrates the complexity results given in Proposition 6; that is the complexity is polynomial in the degree of the input polynomial. For polynomials in $\mathbb{K}[z_1, \ldots, z_n]$, we shall make use of the following change of coordinates to handle the asymptotic behaviour, sending $z_s = 0$ to ∞:

$$\tau_s(z) = \left(\frac{z_1}{z_s}, \ldots, \frac{z_{s-1}}{z_s}, \frac{1}{z_s}, \frac{z_{s+1}}{z_s}, \ldots, \frac{z_n}{z_s} \right).$$

2 Our contribution

The first algorithm in this paper is designed based on the proof of Theorem 1 ([2, Theorems 3.1 and 4.1]), with one major difference. The geometric interpretation of the algorithm as designed in [2] is to split the set of asymptotic critical values of a polynomial mapping f into np sets which can be computed separately and then combined. That is, for $1 \leq s \leq n$, $1 \leq j \leq p$, it is proven that $K_\infty(f) = \bigcup_{(s,j)=(1,1)}^{(n,p)} K_s^j(f)$.

For a given (s, j), consider the mapping

$$M_s^j : z \in \mathbb{K}^n \setminus \{z_s = 0\} \mapsto \left(f(\tau_s(z)), \frac{1}{z_s} w_j(\tau_s(z)) \right) \in \mathbb{K}^p \times \mathbb{K}^{n-p+1}.$$

We assume that f is a dominant mapping and so, the image of w_j has dimension $n - p + 1$ outside of a non-empty Zariski closed set. We consider the Zariski closure of the graph of $M_s^j(z)$ and its intersection with the set $\{z \in \mathbb{K}^n | z_s = 0\} \times \mathbb{K}^p \times \{0\}$ and project onto the value space $\mathbb{K}^p$. The resulting set is called K_s^j. The first change we make is to remove the necessity of taking all $1 \leq s \leq n$, using a generic linear change of coordinates.

Proposition 2. Let $f : \mathbb{K}^n \to \mathbb{K}^p$ be a dominant polynomial mapping. Let $A \in \mathrm{GL}(n)$ be a generic invertible matrix and define f^A by $f^A(z) = f(Az)$. Let π be the canonical projection map from $\mathbb{K}^n \times \mathbb{K}^p \times \mathbb{K}^{n-p+1}$ to $\mathbb{K}^p$. Then, with the set K_1^j defined as above, $K_\infty(f) = \bigcup_{j=1}^p K_1^j(f^A)$.

Note that one can derive from the above result an algorithm computing $K_\infty(f)$ using algebraic elimination routines. Denote this method Algorithm 1.

We give a sketch of the proof. Firstly, the sets of asymptotic critical values of f^A and f are equal, $K_\infty(f) = K_\infty(f^A)$, see [7, Lemma 2.4]. Now, note that for a given s, the sets K_s^j consist of the asymptotic critical values reached when the sth variable tends to ∞. Therefore, a generic choice of A implies that for $1 \leq s \leq n$, whenever z_s goes to ∞ in a path towards an asymptotic critical value, then so does $(Az)_1$. Thus, $\bigcup_{j=1}^p K_1^j(f^A) = \bigcup_{(s,j)=(1,1)}^{(n,p)} K_s^j(f^A) = K_\infty(f^A) = K_\infty(f)$ and so we need only compute p sets as opposed to np. We assume now that the matrix A is generic enough.

Proposition 3. For $1 \leq j \leq p$, assume that $w_j(z)$ is a dominant mapping. Let π be the projection onto the value space of f. Let V be the Zariski closure of the graph of the mapping $M_1^j(f^A)$ and let u_i be the value in this graph of the $(p+i)$th component so that $\pi\left(\overline{(V \setminus V(z_1))} \cap V(z_1, u_1, \ldots, u_{n-p+1})\right) = K_1^j(f^A)$. Let $\mathcal{E}$ be the set of affine linear spaces of dimension $n+p+1$ that contain the $(z_1, \ldots, z_n, c_1, \ldots, c_p)$-space. There exists a non-empty Zariski open set $\mathcal{O}$ such that for all $E \in \mathcal{O}$, $\pi\left(\overline{((V \cap E) \setminus V(z_1))} \cap V(z_1, e)\right) = K_1^j(f^A)$, where e is the variable corresponding to the generic line in the $(u_1, \ldots, u_{n-p+1})$-space. We denote this method Algorithm 2.

From this proposition, one can derive a probabilistic algorithm which avoids considering the extra variables introduced in Algorithm 1. In the case where the gradient mapping corresponding to the $(u_1, \ldots, u_{n-p+1})$-space is dominant, we can intersect this space with a generic line. Alternatively, we could force the gradient mapping $w_j(\tau_s(z))$ to be parallel to a generic line.

Proposition 4. For $1 \leq j \leq p$, assume that $w_j(z)$ is a dominant mapping. Let π be the canonical projection onto the value space of f, $\mathbb{K}^p$. Let V be the Zariski closure of the graph of the mapping $M_1^j(f^A)$ and let $\pi_c : \mathbb{K}^n \times \mathbb{K}^p \times \mathbb{K}^{n-p+1} \to \mathbb{K}^n \times \mathbb{K}^p$ be the canonical projection map onto the graph of the first p components of the mapping $M_1^j(f^A)$. Let $(r_1, \ldots, r_{n-p+1}) \in \mathbb{K}^{n-p+1}$ be a generic vector. Then let D_j be the hyperspace defined by set of minors of the matrix

$$\begin{bmatrix} w_{j_1}(z) & \cdots & w_{j_{n-p+1}}(z) \\ r_1 & \cdots & r_{n-p+1} \end{bmatrix}.$$

Then, $K_1^j(f^A) \subseteq \pi\left(\overline{\pi_c(V \cap D_j) \setminus V(z_1)} \cap V(z_1)\right)$.

Again, the above result can be translated into an algorithm which we denote Algorithm 3. We show that the algebraic set returned by Algorithm 3 has codimension at least 1 and that it contains the set of asymptotic critical values of the input polynomial mapping. In many practical cases, we will indeed find additional values but this method still has its merits. For example, we can use it to quickly determine that a polynomial mapping does not have asymptotic critical values if the output is empty. Algorithm 3 also allows us to give a tighter bound on the degree of the asymptotic critical values.

Proposition 5. Let $f = (f_1, \ldots, f_p) \in \mathbb{K}[z_1, \ldots, z_n]^p$ be a polynomial mapping. Let $d = \max_{1 \leq i \leq p} \deg f_i$. Then the asymptotic critical values of f are contained in a hypersurface of degree at most $p(d+1)^p((2p-1)(d-1))^{n-p}$.

Proposition 6. Let $f \in \mathbb{Q}[z_1, \ldots, z_n]$ be a polynomial with degree d. Then, up to logarithmic factors,

- Algorithm 1 computes $K_\infty(f)$ in $O(d^{2n^2+O(n)})$ arithmetic operations in $\mathbb{Q}$;
- Algorithm 2 computes $K_\infty(f)$ in $O(n^7 d^{4n+O(1)})$ arithmetic operations in $\mathbb{Q}$;
- Algorithm 3 computes a set containing $K_\infty(f)$ in $O(n^7 d^{4n+O(1)})$ arithmetic operations in $\mathbb{Q}$.

3 Experimental results

f_n	Algo. 1	Algo. 2	Algo. 3
n	time (s)	time (s)	time (s)
2	0.130	0.065	0.044
5	1.700	0.070	0.074
10	1511.148	0.330	0.275
15	∞	1.410	1.206
20	∞	5.124	4.170
25	∞	17.630	13.547

m_n	Algo. 1	Algo. 2	Algo. 3
n	time (s)	time (s)	time (s)
3	1.443	0.579	0.059
4	∞	4.192	0.560
5	∞	271.094	100.696

Poly.	Algo. 1	Algo. 2	Algo. 3
n	time (s)	time (s)	time (s)
d_2n_{20}	45.458	0.306	0.245
d_2n_{50}	∞	7.037	5.243
d_2n_{100}	∞	269.335	123.789
d_3n_3	143.473	0.143	0.051
d_3n_5	∞	8.409	0.142
d_3n_7	∞	15812.523	1.054
d_4n_2	1.079	0.112	0.046
d_4n_4	∞	1.812	0.247
d_4n_6	∞	442.459	16.747

We implemented the above algorithms using the Gröbner basis algorithm F_4. We use the computer algebra system Maple and FGb [9], implemented in C by J.-Ch. Faugère, to perform the Gröbner basis computations. The computations were performed on one thread of a computing server equipped with an Intel Xeon CPU E7-4820 v4 running at 2 GHz and with 1511 GiB of memory. The entry ∞ has been given in the cases when the algorithm has not terminated within 2 days.

Here, $f_n = z_1^4 + \sum_{i=2}^n (z_1 z_i - 1)^2$ is a family of polynomials that share an asymptotic critical value 0 and for $n \geq 3$ they have an additional asymptotic critical value at $n-1$. The degree of the polynomials in this family is fixed at 4 and so we show how the algorithms perform with a large number of variables. We see that Algorithm 1 struggles for $n \geq 10$ while much larger values of n are handled well by Algorithms 2 and 3.

Additionally, $m_n = \sum_{i=1}^n \prod_{j=1}^i z_j^{2^{i-j}}$ is a family of polynomials whose degree grows exponentially with the number of variables; for $n \geq 2$, m_n has a single asymptotic critical value at 0. Algorithm 1 cannot reach even $n = 4$ while Algorithm 3 shows some improvement over Algorithm 2.

On the other hand, one shows that sufficiently generic dense polynomials do not have asymptotic critical values. Then, they serve as a good illustrator of how Algorithm 3 can efficiently certify that the set of asymptotic critical values of a polynomial mapping is empty. We use the notation $d_i n_j$ to denote a generic dense polynomial of degree i in a polynomial ring of j variables. Experimentally, it is clear that Algorithm 3 severely outperforms Algorithm 1 and even Algorithm 2 when no asymptotic critical values are present. All three algorithms perform far better in the simple case where $d = 2$. In this special case, the degree bound we provide in Proposition 5 for the asymptotic critical values drops from $O(d^n p^{n-p+1})$ to $O(d^p p^{n-p+1})$.

Acknowledgements. The authors are supported by the ANR grants ANR-18-CE33-0011 Sesame, ANR-19-CE40-0018 De Rerum Natura and ANR-19-CE48-0015 ECARP, the PGMO grant CAMiSAdo and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement N. 813211 (POEMA).

References

[1] P. J. Rabier. "Ehresmann Fibrations and Palais-Smale Conditions for Morphisms of Finsler Manifolds". In: *Annals of Mathematics* 146.3 (1997), pp. 647–691. ISSN: 0003486X. URL: http://www.jstor.org/stable/2952457.

[2] K. Kurdyka, P. Orro, and S. Simon. "Semialgebraic Sard Theorem for Generalized Critical Values". In: *J. Differential Geom.* 56.1 (Sept. 2000), pp. 67–92. DOI: 10.4310/jdg/1090347525. URL: https://doi.org/10.4310/jdg/1090347525.

[3] C. W. Brown. "QEPCAD B: A System for Computing with Semi-Algebraic Sets via Cylindrical Algebraic Decomposition". In: *SIGSAM Bull.* 38.1 (Mar. 2004), pp. 23–24. ISSN: 0163-5824. DOI: 10.1145/980175.980185. URL: https://doi.org/10.1145/980175.980185.

[4] K. Kaveh. "Morse theory and Euler characteristic of sections of spherical varieties". In: *Transformation groups* 9.1 (2004), pp. 47–63.

[5] Z. Jelonek and K. Kurdyka. "Quantitative Generalized Bertini-Sard Theorem for Smooth Affine Varieties". In: *Discrete and Computational Geometry, v.34, 659-678 (2005)* 34 (Nov. 2005). DOI: 10.1007/s00454-005-1203-1.

[6] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Berlin, Heidelberg: Springer-Verlag, 2006. ISBN: 3540330984.

[7] M. Safey El Din. "Generalized critical values and testing sign conditions on a polynomial". In: *International Conference on Mathematical Aspects of Computer and Information Sciences*. Beijing, China, July 2006, pp. 61–84. URL: https://hal.archives-ouvertes.fr/hal-01351457.

[8] H. Hong and M. Safey El Din. "Variant real quantifier elimination: algorithm and application". In: *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*. 2009, pp. 183–190.

[9] J.-Ch. Faugère. "FGb: A Library for Computing Gröbner Bases". In: *Mathematical Software – ICMS 2010*. Ed. by Komei Fukuda et al. Berlin, Heidelberg: Springer, 2010, pp. 84–87. ISBN: 978-3-642-15582-6. DOI: 10.1007/978-3-642-15582-6_17. URL: http://dx.doi.org/10.1007/978-3-642-15582-6_17.

[10] The RegularChains Library. 2015. URL: http://www.regularchains.org/.

[11] Wolfram Research, Inc. *Mathematica, Version 12.1*. Champaign, IL, 2020. 2020. URL: https://www.wolfram.com/mathematica.