# Finding sampling points on real hypersurfaces is easier in singular situations 

M. Safey El Din*

January 22, 2005

Let $f$ be a polynomial in $\mathbb{Q}\left[X_{1}, \ldots, X_{n}\right]$ of degree $D$ and, for $t \in \mathbb{Q}$, let $\mathcal{H}_{t} \subset \mathbb{C}^{n}$ be the hypersurface defined by $f-t=0$. The main result of this paper is an algorithm computing at least one point in each connected component of $\mathcal{H}_{0} \cap \mathbb{R}^{n}$, without smoothness assumptions on $\mathcal{H}_{0}$, whose complexity is polynomial in $n$, the evaluation complexity $\mathcal{L}$ of $f, D$ and an intrinsic geometric degree $\delta$ which is always less than $D^{n}$ when $\mathcal{H}_{0}$ has a positive dimensional singular locus. As a by-product, we prove that given $H_{1}, \ldots, H_{n-2}$ generic hyperplanes of $\mathbb{Q}^{n}$, the 0-th Betti number of $\mathcal{H}_{0} \cap \mathbb{R}^{n}$ is bounded by $D\left(1+(D-1)+\cdots+(D-1)^{n-1}-\left(\mathfrak{d}_{0}+\cdots+\mathfrak{d}_{n-2}\right)\right)$ where for $i=1, \ldots, n-2, \mathfrak{D}_{i}\left(\right.$ resp. $\left.\mathfrak{d}_{0}\right)$ denotes the sum of the degree of the positive equidimensional components of the singular locus of $\mathcal{H}_{0} \cap\left(\cap_{j=1}^{i} H_{i}\right)$ (resp. $\left.\mathcal{H}_{0}\right)$. In singular situations, this is always less than the Thom-Milnor bound, which is here equal to $D^{n}$.

Motivation and description of the problem. Computing at least one point in each connected component of a real algebraic set $\mathcal{H}_{0} \cap \mathbb{R}^{n}$ defined by a single equation $f=0$ is a question of first importance since it is a basic subroutine used in several algorithms dealing with semialgebraic sets (see [4]). To tackle this problem, we focus on the critical point method. This is based on reducing the problem to compute the critical points of a polynomial mapping reaching its extrema on each connected component of the studied hypersurface $\mathcal{H}_{0} \cap \mathbb{R}^{n}$.
Critical points are algebraically characterized by the vanishing of some minors of a jacobian matrix. Supposing $\mathcal{H}_{0}$ to be smooth forbids rank defects on $\operatorname{Jac}(f)$ and makes easier the problem of computing sampling points in $\mathcal{H}_{0} \cap \mathbb{R}^{n}$. The algorithms provided in $[9,3]$ have a worst-case complexity within $\mathcal{O}\left(n^{3} D^{3 n}\right)$ arithmetic operations in $\mathbb{Q}$ which improves the one of [4] whose complexity is within $\mathcal{O}\left(n^{2}(2 D)^{5 n}\right)$ arithmetic operations in $\mathbb{Q}$. A more accurate analysis shows the one of [9] is better and an implementation of this algorithm shows its practical efficiency. Dealing efficiently with singular situations is the main objective of the algorithms provided in $[4,7,1]$. The contributions in $[4,7]$ deform infinitesimally $\mathcal{H}_{0}$ to retrieve a smooth situation, compute sampling points on the deformed hypersurface, and compute the limits of these points when the introduced infinitesimals tend to 0 . This leads to asymptotically optimal algorithms. Nevertheless, the computational cost induced by the use of infinitesimals, which is generically exponential in the number of variables, has forbidden to obtain efficient implementations. The strategy developed in [1] consists in studying recursively imbricated singular loci on the one hand and computing critical points of mappings restricted to the regular locus of the considered varieties on the other hand. The complexity of this latter approach is not well-controlled.
Thus, the algorithms dealing with singular situations have a worst-case complexity which is greater than the ones developed for smooth cases. The aim of this work is to remedy to this situation, providing an algorithm whose complexity is the one of [9], even when $\mathcal{H}_{0}$ is not smooth.

[^0]An apparently surprising result is that the algorithm we provide never reaches its worst-case complexity when $\mathcal{H}_{0}$ has a positive-dimensional singular locus. In the next paragraph, we detail our results. The last paragraph is devoted to comparisons with related works.

Main contributions. Our approach goes back to [7], by trying to compute limits of critical points of a mapping restricted to $\mathcal{H}_{t}$ (when $t \rightarrow 0$ ). Our contribution is to avoid the computation of a rational parametrization with coefficients in a Puiseux series field for this task. Given $\phi \in \mathbb{Q}\left[X_{1}, \ldots, X_{n}\right]$, consider, for $t \in \mathbb{Q}$, the critical locus $K\left(\phi, \mathcal{H}_{t}\right)$ of $\phi$ restricted to the regular locus of $\mathcal{H}_{t}$. Let $L$ be a new variable and denote by $\mathcal{C} \subset \mathbb{C}^{n+1}$ be the zero-set of the polynomial system

$$
L \frac{\partial f}{\partial X_{1}}-\frac{\partial \phi}{\partial X_{1}}=\cdots=L \frac{\partial f}{\partial X_{n}}-\frac{\partial \phi}{\partial X_{n}}=0 .
$$

Consider the projection $\Pi: \mathbb{C}^{n} \times \mathbb{C} \rightarrow \mathbb{C}$ sending $(x, \ell) \in \mathbb{C}^{n} \times \mathbb{C}$ to $x$ and $\mathfrak{C}$ the Zariski-closure of $\Pi(\mathcal{C})$.

Theorem 1 Suppose that $K\left(\phi, \mathcal{H}_{0}\right)$ is zero-dimensional and that $\mathcal{C}$ has dimension 1. Then, the bounded limits of $K\left(\phi, \mathcal{H}_{t}\right)$ when $t$ tends to 0 are contained in $\mathcal{H}_{0} \cap \mathfrak{C}$. Moreover, $\mathcal{H}_{0} \cap \mathfrak{C}$ is zero-dimensional.

Outline of proof: Consider a sequence of points $\left(y_{k}\right)_{k \in \mathbb{N}}$ such that $y_{k} \in K\left(\phi, \mathcal{H}_{1 / k}\right)$ which converges to a point $y \in \mathbb{C}^{n}$. Remark that $f\left(y_{k}\right) \rightarrow 0$ when $k \rightarrow \infty$ and that, for any $k$, $y_{k} \in \Pi(\mathcal{C})$. This implies $f$ vanishes at $y$ and $y \in \mathfrak{C}$ which implies $y \in \mathcal{H}_{0} \cap \mathfrak{C}$.
It remains to prove $\mathcal{H}_{0} \cap \mathfrak{C}$ is zero-dimensional. Since by assumption $K\left(\phi, \mathcal{H}_{0}\right)$ is zero-dimensional, it is sufficient to prove $\mathcal{H}_{0} \cap \mathfrak{C} \backslash K\left(\phi, \mathcal{H}_{0}\right)$ is zero-dimensional. This is a consequence of $\left(\mathcal{H}_{0} \cap \mathfrak{C} \backslash K\left(\phi, \mathcal{H}_{0}\right)\right) \subset \mathfrak{C} \backslash \Pi(\mathcal{C})$ which is zero-dimensional since $\mathcal{C}$ has dimension 1 .

Classical results allow us to design a procedure computing the limits of $K\left(\phi, \mathcal{H}_{t}\right)$ (when $t \rightarrow 0$ ) based on Gröbner bases using monomial block-orderings. Designing a similar procedure using geometric resolution (see [5] and references therein) is possible by computing a parametric geometric resolution encoding the Zariski-closure $C$ of the zero-set of the vanishing of all (2,2) minors of $\operatorname{Jac}(f, \phi)$ and $\frac{\partial f}{\partial X_{1}}+\cdots+\frac{\partial f}{\partial X_{n}}{ }^{2} \neq 0$ and then use the intersection step provided in [5] to compute a geometric resolution of $C \cap \mathcal{H}_{0}$.
Theorem 1 is used below to compute sampling points in $\mathcal{H}_{0} \cap \mathbb{R}^{n}$ by computing the limits of the critical locus of some mapping restricted to $\mathcal{H}_{t}$, when $t \rightarrow 0$. We study the use of quadratic mappings (see also [7, 1, 3]) and projection functions (see [9] for a similar approach in the smooth case).
The following result extends the ones of $[7,1,3]$ to compute efficiently sampling points on a singular hypersurface, by computing critical points of a quadratic mapping. Given a point $A=\left(a_{1}, \ldots, a_{n}\right) \in \mathbb{Q}^{n}$, denote by $W_{A}$ the variety defined by

$$
\langle f\rangle+\left(\left\langle L \frac{\partial f}{\partial X_{1}}-\left(X_{1}-a_{1}\right), \ldots, L \frac{\partial f}{\partial X_{n}}-\left(X_{n}-a_{n}\right)\right\rangle \cap \mathbb{Q}\left[X_{1}, \ldots, X_{n}\right]\right) .
$$

Theorem 2 There exists a Zariski-closed subset $\mathcal{A} \subsetneq \mathbb{C}^{n}$ such that for any $A=\left(a_{1}, \ldots, a_{n}\right) \in$ $\mathbb{Q}^{n} \backslash \mathcal{A}, W_{A} \subset \mathcal{H}_{0}$ is zero-dimensional. Moreover, it has a non-empty intersection with each connected component of the real algebraic set $\mathcal{H}_{0} \cap \mathbb{R}^{n}$.

Outline of proof: Given $A=\left(a_{1}, \ldots, a_{n}\right) \in \mathbb{Q}^{n}$, let $\phi_{A}: \mathbb{C}^{n} \rightarrow \mathbb{C}$ denote the mapping sending $\left(x_{1}, \ldots, x_{n}\right) \in \mathbb{C}^{n}$ to $\left(x_{1}-a_{1}\right)^{2}+\cdots+\left(x_{n}-a_{n}\right)^{2}$. From [7, Lemma 3.7], each connected component of $\mathcal{H}_{0}$ contains a bounded limit of $K\left(\phi_{A}, \mathcal{H}_{t}\right)$. It remains to prove there exists a

Zariski-closed subset $\mathcal{A} \subsetneq \mathbb{C}^{n}$ such that for $A \in \mathbb{Q}^{n} \backslash \mathcal{A}$, Theorem 1 applies (with $\phi=\phi_{A}$ ). This is a consequence of Sard's theorem (see [7, Lemma 3.2] or [3]) which shows that $K\left(\phi_{A}, \mathcal{H}_{0}\right)$ is zero-dimensional and $\operatorname{Jac}\left(L \frac{\partial f}{\partial X_{1}}-2\left(X_{1}-a_{1}\right), \ldots, L \frac{\partial f}{\partial X_{n}}-2\left(X_{n}-a_{n}\right)\right)$ has rank $n$ at any point $(x, \ell) \in \mathbb{C}^{n} \times \mathbb{C}$.

The following result extends the algorithm of [9] to non-smooth situations in the case of hypersurfaces. It allows us to use generic projections (instead of quadratic mappings). Given $\mathbf{A} \in G L_{n}(\mathbb{Q}), f^{\mathbf{A}}$ denotes the polynomial $f(\mathbf{A} \cdot X)$ (where $X=\left(X_{1}, \ldots, X_{n}\right)$ ). Given an algebraic variety $\mathcal{V} \subset \mathbb{C}^{n}$ defined as the zero-set of $\left(f_{1}, \ldots, f_{s}\right), \mathcal{V}^{\mathbf{A}}$ denotes the variety defined by $\left(f_{1}^{\mathbf{A}}, \ldots, f_{s}^{\mathbf{A}}\right)$.
Additionally consider an arbitrary point $\left(p_{1}, \ldots, p_{n-1}\right) \in \mathbb{Q}^{n-1}$ and denote by $\mathcal{W}_{p}^{\mathbf{A}}$ the union of the zero-sets of

$$
\begin{aligned}
& \left\langle f^{\mathbf{A}}\right\rangle+\left\langle X_{1}-p_{1}, \ldots, X_{i}-p_{i}, L \cdot \frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}}-1, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}} \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_{n}}\right\rangle \cap \mathbb{Q}\left[X_{1}, \ldots, X_{n}\right](\text { for } i=1, \ldots, n-2), \\
& \left\langle f^{\mathbf{A}}\right\rangle+\left(\left\langle L \cdot \frac{\partial f^{\mathbf{A}}}{\partial X_{1}}-1, \frac{\partial f^{\mathbf{A}}}{\partial X_{2}} \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_{n}}\right\rangle \cap \mathbb{Q}\left[X_{1}, \ldots, X_{n}\right]\right)
\end{aligned}
$$

and $\left\langle f, X_{1}-p_{1}, \ldots, X_{n-1}-p_{n-1}\right\rangle$.
Theorem 3 Given an arbitrary point $\left(p_{1}, \ldots, p_{n-1}\right) \in \mathbb{Q}^{n-1}$, there exists a Zariski-closed subset $\mathcal{A} \subsetneq G L_{n}(\mathbb{C})$ such that for $\mathbf{A} \in G L_{n}(\mathbb{Q}) \backslash \mathcal{A}, \mathcal{W}_{p}^{\mathbf{A}} \subset \mathcal{H}_{0}^{\mathbf{A}}$ is zero-dimensional and has a nonempty intersection with each connected component of $\mathcal{H}_{0} \cap \mathbb{R}^{n}$.

Outline of proof: Denote by $\Pi_{i}: \mathbb{C}^{n} \rightarrow \mathbb{C}^{i}$ the canonical projection sending $\left(x_{1}, \ldots, x_{n}\right)$ to $\left(x_{1}, \ldots, x_{i}\right)$ and by $\pi_{i}: \mathbb{C}^{n} \rightarrow \mathbb{C}$ the canonical projection sending $\left(x_{1}, \ldots, x_{n}\right)$ to $x_{i}$.
A first part of the proof is dedicated to show that, given an algebraic variety, there exists a Zariski-closed subset $\mathcal{A} \subsetneq G L_{n}(\mathbb{C})$ such that for any $\mathbf{A} \in G L_{n}(\mathbb{Q}) \backslash \mathcal{A}$ and for any connected component $C^{\mathbf{A}}$ of $\mathcal{V}^{\mathbf{A}} \cap \mathbb{R}^{n}, \Pi_{i}\left(C^{\mathbf{A}}\right)$ is closed for all $i=1, \ldots, n-1$.
Now, given an arbitrary point $\left(p_{1}, \ldots, p_{n-1}\right) \in \mathbb{Q}^{n-1}$, denote by $H_{0}=\mathbb{C}^{n}$ and by $H_{i}$ is the zero-set of $X_{1}-p_{1}=\cdots=X_{i}-p_{i}$ (for $i=1, \ldots, n-1$ ). Under the above statement, one shows that either $C^{\mathbf{A}} \cap H_{n-1} \neq \emptyset$ or, for some $i=0, \ldots, n-1, C^{\mathbf{A}}$ contains a limit of $K\left(\pi_{i+1}, \mathcal{H}_{t}^{\mathbf{A}} \cap H_{i}\right)$ when $t \rightarrow 0$. It remains to verify that for $\mathbf{A}$ chosen outside a Zariski-closed subset of $G L_{n}(\mathbb{C})$ the assumptions of Theorem 1 are satisfied. This is done classically by using Sard's Theorem (see e.g. [2]) to prove that for A chosen outside a Zariski-closed subset and for $i=1, \ldots, n-2$ the matrices $\operatorname{Jac}\left(L \frac{\partial f^{\mathrm{A}}}{\partial X_{i+1}}-1, \frac{\partial f^{\mathrm{A}}}{\partial X_{i+2}}, \ldots, \frac{\partial f^{\mathrm{A}}}{\partial X_{n}}, X_{1}-p_{1}, \ldots, X_{i}-p_{i}\right)$ and the

The above remark on the rank of the jacobian matrices is important since it allows us to use the algorithm provided in [5] and computes a geometric resolution of the Zariski-closure of a system of equations and inequations $f_{1}=\ldots=f_{s}=0, g \neq 0$.
In this algorithm, the intermediate data are parametric geometric resolutions encoding lifted curves and geometric resolutions of Zariski-closure of the zero-set of the intermediate polynomial systems $f_{1}=\ldots=f_{i}=0, g \neq 0$. At each step a Hensel-lifting is performed to recover a lifting curve of the Zariski-closure of the zero-set of $f_{1}=\ldots=f_{i}=0, g \neq 0$ and an intersection step computes a geometric resolution for the intersection of this curve and the hypersurface defined by $f_{i+1}=0$. Then, a cleaning step produces a geometric resolution of a generic fiber of the Zariski-closure of the zero-set of $f_{1}=\cdots=f_{i+1}=0, g \neq 0$.
Our algorithm which relies on Theorem 3 runs as follows:

- choose randomly $\mathbf{A} \in G L_{n}(\mathbb{Q})$ and $\left(p_{1}, \ldots, p_{n-1}\right) \in \mathbb{Q}^{n-1}$;
- for $i=1$ to $n-2$ compute a parametric geometric resolution encoding the Zariski-closure $C_{i}$ of the zero-set of

$$
\frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}}=\cdots=\frac{\partial f^{\mathbf{A}}}{\partial X_{n}}=X_{1}-p_{1}=\cdots=X_{i}-p_{i}=0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} \neq 0
$$

and compute a geometric resolution of $C_{i} \cap \mathcal{H}_{0}$.

- Compute a parametric geometric resolution encoding the Zariski-closure $C$ of the zero-set of

$$
\frac{\partial f^{\mathbf{A}}}{\partial X_{2}}=\cdots=\frac{\partial f^{\mathbf{A}}}{\partial X_{n}}=0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_{1}} \neq 0
$$

and compute a geometric resolution of $C_{i} \cap \mathcal{H}_{0}$.

- Return all the computed geometric resolutions and $f=X_{1}-p_{1}=\cdots=X_{n-1}-p_{n-1}=0$.

Compared to the algorithm of [9], the algorithm we provide here only performs additional gcd computations to take into account the non-vanishing of the aforementioned inequations. Thus, its complexity is the same than the one of [9].

Theorem 4 Let $f$ be a polynomial in $\mathbb{Q}\left[X_{1}, \ldots, X_{n}\right]$ of degree $D$, encoded by a straight-line program of length $\mathcal{L}$ and $\mathcal{H} \subset \mathbb{C}^{n}$ be the hypersurface defined by $f=0$. There exists a probabilistic algorithm which computes at least one point in each connected component of $\mathcal{H}_{0} \cap \mathbb{R}^{n}$ within $\mathcal{O}\left(n^{2}\left(n \mathcal{L}+n^{4}\right) \mathcal{U}(D . \delta)^{2}\right)$ arithmetic operations in $\mathbb{Q}$ where $\delta$ is the maximal degree of the intermediate algebraic varieties studied during the incremental process and is bounded by D. $(D-1)^{n-1}$.

The procedure relying on Theorem 2 which computes sampling points in $\mathcal{H}_{0} \cap \mathbb{R}^{n}$ has a similar complexity but the degree $\delta$ can at best be bounded by $D^{n}$.

At last, we mention that, following the complexity result of [6], using Gröbner bases to perform algebraic elimination inside our algorithms leads also to a complexity within $D^{\mathcal{O}(n)}$ arithmetic operations in $\mathbb{Q}$.

Remark. Let $\mathfrak{d}$ be the sum of the degrees of the equidimensional components of the singular locus of $\mathcal{H}_{0}$ having positive dimension. One can refine the above degree bound $D(D-1)^{n-1}$ dominating $\delta$ by remarking that the degree of the curve defined as the Zariski-closure of the solution set of:

$$
\frac{\partial f^{\mathbf{A}}}{\partial X_{2}}=\cdots=\frac{\partial f^{\mathbf{A}}}{\partial X_{n}}=0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_{1}} \neq 0
$$

is bounded by $(D-1)^{n-1}-\mathfrak{d}$. Thus, while in the smooth case the degree bound $D \cdot(D-1)^{n-1}$ can be reached, it cannot in the case where $\mathcal{H}_{0}$ has a positive dimensional singular locus.
Taking into account the above discussion and performing a careful analysis of degree bounds for the algorithm relying on Theorem 3, this leads to the following result.

Theorem 5 Let $H_{1}, \ldots, H_{n-2}$ be generic hyperplanes of $\mathbb{Q}^{n}$. The number of connected components of the real counterpart of $\mathcal{H}_{0}$ is bounded by

$$
D\left(1+(D-1)+\cdots+(D-1)^{n-1}-\left(\mathfrak{d}_{0}+\cdots+\mathfrak{d}_{n-2}\right)\right),
$$

where $\mathfrak{d}_{i}$ (resp. $\mathfrak{d}_{0}$ ) denotes the sum of the degree of the positive-dimensional components of the singular locus of $\mathcal{H}_{0} \cap\left(\cap_{j=1}^{i} H_{i}\right)$ (resp. $\left.\mathcal{H}_{0}\right)$.

Comparison with previous complexity results. Previous contributions [4, 7] dealing with singular hypersurfaces with an asymptotically optimal complexity. We compare here our complexity result with previous ones and show it is exponentially better than the others.
We first focus on Basu, Pollack and Roy's algorithm (see [4]) which was known to have the best complexity to compute sampling points on hypersurfaces without any assumption. This algorithm reduces the question to solving a zero-dimensional system with coefficients in a Puiseux series field $\mathbb{Q}\langle\varepsilon, \zeta\rangle$ (where $\varepsilon$ and $\zeta$ are infinitesimals), which has always a degree $\mathfrak{D}=\prod_{i=1}^{n} \max \left(4,2 \operatorname{deg}_{i}(f)\right) \leq(\max (4,2 D))^{n}$, where $\operatorname{deg}_{i}(f)$ is the partial degree of $f$ in $X_{i}$. This resolution is done by means of linear algebra operations in a quotient algebra, so that the complexity is $\mathcal{O}\left(\mathfrak{D}^{3}+n \mathfrak{D}^{2}\right)$ arithmetic operations in $\mathbb{Q}(\varepsilon, \zeta)$. In worst cases, the maximal degree, in $\varepsilon$ and $\zeta$, of the coefficients appearing during the computations equals the degree $\mathfrak{D}$. Thus, the cost of each arithmetic operation in $\mathbb{Q}(\varepsilon, \zeta)$ can at best be bounded by $\mathbb{M}(\mathfrak{D})^{2}$ (where $\left.\mathrm{M}(p)=p \log ^{2}(p) \log \log (p)\right)$. Then, the complexity of this algorithm written in expanded form is $\mathcal{O}\left(\left(\mathfrak{D}^{3}+n \mathfrak{D}^{2}\right) \mathrm{M}(\mathfrak{D})^{2}\right)$ arithmetic operations in $\mathbb{Q}$. Here, we bring an algorithm computing sampling points in $\mathcal{H}_{0} \cap \mathbb{R}^{n}$, without smoothness assumptions on $\mathcal{H}_{0}$, whose worst-case complexity (which is reached on generic inputs) is within $\mathcal{O}\left(n^{2}\left(D^{n}+n^{3}\right) \mathrm{M}\left(D^{2}(D-1)^{n-1}\right)^{2}\right)$ arithmetic operations in $\mathbb{Q}$. On generic inputs, the complexity gain is, up to $\log$ factors, equivalent to $\left(2^{5 n} D^{2 n}\right) / n^{2}$ in terms of arithmetic operations in $\mathbb{Q}$. Taking into account the bit-size of the coefficients which grow linearly in the degree of the studied zero-dimensional ideal on generic inputs, this leads to a complexity gain equivalent to $\left(2^{6 n} D^{2 n}\right) / n^{2}$.
We now focus on contributions introducing a single infinitesimal (see for example [7]). The algorithm described in [7] makes use of an infinitesimal arithmetic and can be decomposed in two steps:

- first, it computes sampling points in the perturbed hypersurface $\mathcal{H}_{\varepsilon} \cap \mathbb{R}\langle\varepsilon\rangle^{n}$ (where $\varepsilon$ is an infinitesimal) which are here encoded by a parametric rational parametrization of degree denoted by $\delta$,
- then it computes the bounded limits of these sampling points when $\varepsilon \rightarrow 0$.

Up to the author's knowledge, the most efficient algorithm to compute parametric geometric resolutions is the one of [10]. This algorithm starts from a geometric resolution computed for a generic value of $\varepsilon$ having rationals as coefficients of bit-size $\tau . D^{n}$ (where $\tau$ is the size of the rationals appearing in the initial polynomial system to solve). Its worst-case bit complexity is (up to log factors) $\mathcal{O}\left(n D^{4 n} \tau\right)$. Like for our algorithm, this worst-case complexity is reached for generic inputs. Thus, the complexity gain is equivalent to $D^{n}$. Remark that the bit-size of a parametric geometric resolution computed for a generic input is $\mathcal{O}\left(n D^{4 n} \tau\right)$ which implies this complexity gain is independent of any algorithmic procedure.

Thus, our algorithm is exponentially better (in the number of variables) than any contribution involving an explicit deformation of the studied hypersurface.

Full proofs of these results can be found in [8]. An implementation is available in the RAGLib Maple package using Gb and RS softwares respectively implemented by J.-C. Faugère and F. Rouillier. It can be downloaded from the author's web page. An other one based on the Kronecker Magma package implemented by G. Lecerf is planned. Generalizing this approach to polynomial systems is an on-going work.

## References

[1] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. Journal of Symbolic Computation, 34(6):543-560, 2002.
[2] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. Journal of Complexity, 13(1):5-27, 1997.
[3] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties and efficient real elimination procedure. Kybernetika, 40(5):519-550, 2004.
[4] S. Basu, R. Pollack, and M.-F. Roy. Algorithms in real algebraic geometry. Springer-Verlag, 2003.
[5] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. Journal of Complexity, 17(1):154-211, 2001.
[6] Y. N. Lakshmann. A single exponential bound of the complexity of computing Gröbner bases of zero-dimensional ideals. In C. Traverso T. Mora, editor, Proc. Effective Methods in Algebraic Geometry, MEGA'90, volume 94 of Progress in Mathematics, pages 227-234. Birkhaüser, 1991.
[7] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a real algebraic set defined by a single equation. Journal of Complexity, 16:716-750, 2000.
[8] M. Safey El Din. Finding sampling points on real hypersurfaces is easier in singular situations. Technical report, INRIA, www-calfor.lip6.fr/~safey, 2005.
[9] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In Proceedings of the 2003 international symposium on Symbolic and algebraic computation, pages 224-231. ACM Press, 2003.
[10] É. Schost. Computing parametric geometric resolutions. Journal of Applicable Algebra in Engineering, Communication and Computing 13(5): 349-393, 2003, 13(5):349-393, 2003.


[^0]:    *Mohab.Safey@lip6.fr, Computer Algebra Team (CalFor) of LIP6, Université Pierre et Marie Curie, INRIA/LIP6 SALSA Project

