A bound on the minimum of a real positive polynomial over the standard simplex

Saugata Basu
(joint work with Richard Leroy and Marie-Francoise Roy)

MEGA 2009, June 17, 2009, Barcelona

Outline

Outline

Outline

Outline

Bounds in real algebraic geometry

- Let $Q \in \mathbb{R}[X_1, \ldots, X_k]$, with $\deg(Q) \leq d$.
- Then various topological invariants of $Z(Q, \mathbb{R}^k)$, such as the number of connected components, Betti numbers etc. can be bounded in terms of d and k (so called *uniform bounds*).
- However, if $Q \in \mathbb{Z}[X_1, \ldots, X_k]$, $\deg(Q) \leq d$ and additionally the bit-sizes of the coefficients of Q are bounded by τ, it is possible to obtain (*non-uniform*) bounds depending on d, k *and* τ on certain metric quantities such as:
- the minimum value attained by a polynomial $Q \in \mathbb{Z}[X_1, \ldots, X_k]$ on a standard simplex given that $Q > 0$ on the same;
- the radius of a ball guaranteed to contain all bounded connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$, or meeting all connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$ etc.

Bounds in real algebraic geometry

- Let $Q \in \mathbb{R}[X_1, \ldots, X_k]$, with $\deg(Q) \leq d$.
- Then various topological invariants of $Z(Q, \mathbb{R}^k)$, such as the number of connected components, Betti numbers etc. can be bounded in terms of d and k (so called *uniform bounds*).
- However, if $Q \in \mathbb{Z}[X_1, \ldots, X_k]$, $\deg(Q) \leq d$ and additionally the bit-sizes of the coefficients of Q are bounded by τ, it is possible to obtain (*non-uniform*) bounds depending on d, k *and* τ on certain metric quantities such as:
- the minimum value attained by a polynomial $Q \in \mathbb{Z}[X_1, \ldots, X_k]$ on a standard simplex given that $Q > 0$ on the same;
- the radius of a ball guaranteed to contain all bounded connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$, or meeting all connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$ etc.

Bounds in real algebraic geometry

- Let $Q \in \mathbb{R}[X_1, \ldots, X_k]$, with $\deg(Q) \leq d$.
- Then various topological invariants of $Z(Q, \mathbb{R}^k)$, such as the number of connected components, Betti numbers etc. can be bounded in terms of d and k (so called *uniform bounds*).
- However, if $Q \in \mathbb{Z}[X_1, \ldots, X_k]$, $\deg(Q) \leq d$ and additionally the bit-sizes of the coefficients of Q are bounded by τ, it is possible to obtain (*non-uniform*) bounds depending on d, k *and* τ on certain metric quantities such as:
- the minimum value attained by a polynomial $Q \in \mathbb{Z}[X_1, \ldots, X_k]$ on a standard simplex given that $Q > 0$ on the same;
- the radius of a ball guaranteed to contain all bounded connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$, or meeting all connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$ etc.

Bounds in real algebraic geometry

- Let $Q \in \mathbb{R}[X_1, \ldots, X_k]$, with $\deg(Q) \leq d$.
- Then various topological invariants of $Z(Q, \mathbb{R}^k)$, such as the number of connected components, Betti numbers etc. can be bounded in terms of d and k (so called *uniform bounds*).
- However, if $Q \in \mathbb{Z}[X_1, \ldots, X_k]$, $\deg(Q) \leq d$ and additionally the bit-sizes of the coefficients of Q are bounded by τ, it is possible to obtain (*non-uniform*) bounds depending on d, k *and* τ on certain metric quantities such as:
- the minimum value attained by a polynomial $Q \in \mathbb{Z}[X_1, \ldots, X_k]$ on a standard simplex given that $Q > 0$ on the same;
- the radius of a ball guaranteed to contain all bounded connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$, or meeting all connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$ etc.

Bounds in real algebraic geometry

- Let $Q \in \mathbb{R}[X_1, \ldots, X_k]$, with $\deg(Q) \leq d$.
- Then various topological invariants of $Z(Q, \mathbb{R}^k)$, such as the number of connected components, Betti numbers etc. can be bounded in terms of d and k (so called *uniform bounds*).
- However, if $Q \in \mathbb{Z}[X_1, \ldots, X_k]$, $\deg(Q) \leq d$ and additionally the bit-sizes of the coefficients of Q are bounded by τ, it is possible to obtain (*non-uniform*) bounds depending on d, k *and* τ on certain metric quantities such as:
- the minimum value attained by a polynomial $Q \in \mathbb{Z}[X_1, \ldots, X_k]$ on a standard simplex given that $Q > 0$ on the same;
- the radius of a ball guaranteed to contain all bounded connected components of $\mathbb{Z}(Q, \mathbb{R}^k)$, or meeting all connected components of $Z(Q, \mathbb{R}^k)$ etc.

Examples of applications of non-uniform bounds

- It is important to know very precise bounds on the minimum of Q over a simplex in order to have a good stopping criteria for sub-division algorithms for obtaining positivity certificates (explained by Richard Leroy in his talk).
- Recent work by Yakovenko et al. on obtaining (doubly exponential) *uniform* upper bounds on the infinitesimal version of Hilbert's sixteenth problem depends in an essential way on *non-uniform* bounds of the types mentioned.

Examples of applications of non-uniform bounds

- It is important to know very precise bounds on the minimum of Q over a simplex in order to have a good stopping criteria for sub-division algorithms for obtaining positivity certificates (explained by Richard Leroy in his talk).
- Recent work by Yakovenko et al. on obtaining (doubly exponential) *uniform* upper bounds on the infinitesimal version of Hilbert's sixteenth problem depends in an essential way on *non-uniform* bounds of the types mentioned.

Statement of the problem

- Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ with $\deg(P) = d$ taking only positive values on the k-dimensional simplex

$$\Delta = \left\{ x \in \mathbb{R}^k_{\geq 0} \,\middle|\, \sum_{i=1}^{k} x_i \leq 1 \right\}.$$

- Let τ be an upper bound on the bit-size of the coefficients of P.
- Writing

$$m = \min_{\Delta} P > 0,$$

we consider the problem of finding an explicit bound $m_{k,d,\tau}$ depending only on k, d and τ such that $0 < m_{k,d,\tau} \leq m$.

- *It is important in applications (such as obtaining certificates of positivity) that no extra assumptions (such as genericity*

Statement of the problem

- Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ with $\deg(P) = d$ taking only positive values on the k-dimensional simplex

$$\Delta = \left\{ x \in \mathbb{R}^k_{\geq 0} \,\middle|\, \sum_{i=1}^{k} x_i \leq 1 \right\}.$$

- Let τ be an upper bound on the bit-size of the coefficients of P.
- Writing

$$m = \min_{\Delta} P > 0,$$

we consider the problem of finding an explicit bound $m_{k,d,\tau}$ depending only on k, d and τ such that $0 < m_{k,d,\tau} \leq m$.

- *It is important in applications (such as obtaining certificates of positivity) that no extra assumptions (such as genericity*

Statement of the problem

- Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ with $\deg(P) = d$ taking only positive values on the k-dimensional simplex

$$\Delta = \left\{ x \in \mathbb{R}^k_{\geq 0} \,\middle|\, \sum_{i=1}^{k} x_i \leq 1 \right\}.$$

- Let τ be an upper bound on the bit-size of the coefficients of P.
- Writing

$$m = \min_{\Delta} P > 0,$$

we consider the problem of finding an explicit bound $m_{k,d,\tau}$ depending only on k, d and τ such that $0 < m_{k,d,\tau} \leq m$.

- *It is important in applications (such as obtaining certificates of positivity) that no extra assumptions (such as genericity*

Statement of the problem

- Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ with $\deg(P) = d$ taking only positive values on the k-dimensional simplex

$$\Delta = \left\{ x \in \mathbb{R}^k_{\geq 0} \,\middle|\, \sum_{i=1}^{k} x_i \leq 1 \right\}.$$

- Let τ be an upper bound on the bit-size of the coefficients of P.
- Writing

$$m = \min_{\Delta} P > 0,$$

we consider the problem of finding an explicit bound $m_{k,d,\tau}$ depending only on k, d and τ such that $0 < m_{k,d,\tau} \leq m$.

- *It is important in applications (such as obtaining certificates of positivity) that no extra assumptions (such as genericity*

Previous work

There are two main approaches:

- Canny's gap theorem can be used, under non-degeneracy conditions;
- de Loera and Santos prove a bound using Lojasiewicz inequality, leading to a bound in the general case, but involving a universal constant.
- We want an explicit bound, with no extra assumption on P.

Previous work

There are two main approaches:

- Canny's gap theorem can be used, under non-degeneracy conditions;
- de Loera and Santos prove a bound using Lojasiewicz inequality, leading to a bound in the general case, but involving a universal constant.
- We want an explicit bound, with no extra assumption on P.

Previous work

There are two main approaches:

- Canny's gap theorem can be used, under non-degeneracy conditions;
- de Loera and Santos prove a bound using Lojasiewicz inequality, leading to a bound in the general case, but involving a universal constant.
- We want an explicit bound, with no extra assumption on P.

The univariate case

- Let

$$P = \sum_{i=0}^{d} a_i T^i \in \mathbb{Z}[T],$$

taking only positive values on the interval $[0, 1]$. Let τ be a bound on the bitsize of its coefficients.

- The minimum m of P on $[0, 1]$ occurs either at 0 or 1, or at a point x^* lying in the interior $]0, 1[$ (and in this case the minimum occurs at a root of P').
- The first case is trivial, as $P(0), P(1) \in \mathbb{Z}$, so that m is clearly at least 1.
- In the second case, $P(x^*) = 0$, so that m is a root of the resultant $R(Z) = \mathrm{Res}_T(P(T) - Z, P'(T)) \in \mathbb{Z}[Z]$. The resultant $R(Z)$ is the determinant of the matrix $\mathrm{Syl}(Z)$, where $\mathrm{Syl}(Z)$ is the following Sylvester matrix:

The univariate case

- Let
$$P = \sum_{i=0}^{d} a_i T^i \in \mathbb{Z}[T],$$
taking only positive values on the interval $[0, 1]$. Let τ be a bound on the bitsize of its coefficients.
- The minimum m of P on $[0, 1]$ occurs either at 0 or 1, or at a point x^* lying in the interior $]0, 1[$ (and in this case the minimum occurs at a root of P').
- The first case is trivial, as $P(0), P(1) \in \mathbb{Z}$, so that m is clearly at least 1.
- In the second case, $P(x^*) = 0$, so that m is a root of the resultant $R(Z) = \mathrm{Res}_T(P(T) - Z, P'(T)) \in \mathbb{Z}[Z]$. The resultant $R(Z)$ is the determinant of the matrix $\mathrm{Syl}(Z)$, where $\mathrm{Syl}(Z)$ is the following Sylvester matrix:

The univariate case

- Let
$$P = \sum_{i=0}^{d} a_i T^i \in \mathbb{Z}[T],$$
taking only positive values on the interval $[0, 1]$. Let τ be a bound on the bitsize of its coefficients.
- The minimum m of P on $[0, 1]$ occurs either at 0 or 1, or at a point x^* lying in the interior $]0, 1[$ (and in this case the minimum occurs at a root of P').
- The first case is trivial, as $P(0), P(1) \in \mathbb{Z}$, so that m is clearly at least 1.
- In the second case, $P(x^*) = 0$, so that m is a root of the resultant $R(Z) = \mathrm{Res}_T(P(T) - Z, P'(T)) \in \mathbb{Z}[Z]$. The resultant $R(Z)$ is the determinant of the matrix $\mathrm{Syl}(Z)$, where $\mathrm{Syl}(Z)$ is the following Sylvester matrix:

The univariate case

- Let
$$P = \sum_{i=0}^{d} a_i T^i \in \mathbb{Z}[T],$$
taking only positive values on the interval $[0, 1]$. Let τ be a bound on the bitsize of its coefficients.
- The minimum m of P on $[0, 1]$ occurs either at 0 or 1, or at a point x^* lying in the interior $]0, 1[$ (and in this case the minimum occurs at a root of P').
- The first case is trivial, as $P(0), P(1) \in \mathbb{Z}$, so that m is clearly at least 1.
- In the second case, $P(x^*) = 0$, so that m is a root of the resultant $R(Z) = \mathrm{Res}_T(P(T) - Z, P'(T)) \in \mathbb{Z}[Z]$. The resultant $R(Z)$ is the determinant of the matrix $\mathrm{Syl}(Z)$, where $\mathrm{Syl}(Z)$ is the following Sylvester matrix:

Univariate case (cont).

$$\begin{pmatrix}
a_d & \cdots & \cdots & \cdots & a_1 & a_0 - Z & 0 & \cdots & 0 \\
0 & \ddots & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & & 0 \\
0 & \cdots & 0 & a_d & \cdots & \cdots & \cdots & a_1 & a_0 - Z \\
(d-1)a_{d-1} & \cdots & \cdots & \cdots & a_1 & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & (d-1)a_{d-1} & \cdots & \cdots & \cdots & a_1
\end{pmatrix}
\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} d-1 \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} d \end{matrix}$$

$R(Z) = \sum_{i=0}^{d-1} r_i Z^i$ is thus a polynomial of degree $d-1$ in Z, whose coefficients are controlled in the following fashion:

Univariate case (cont).

Lemma

For all $i \in \{0, \ldots, d-1\}$, *we have*

$$|r_i| < 3^{-d/2} \left[2^\tau \sqrt{(d+1)^3}\right]^d \binom{d-1}{i} \left[2^\tau \sqrt{d+1} - 1\right]^{d-1-i}.$$

Proof.

Use Hadamard's bound on bounding determinants. □

Univariate case (cont).

Lemma

For all $i \in \{0, \ldots, d-1\}$, *we have*

$$|r_i| < 3^{-d/2} \left[2^\tau \sqrt{(d+1)^3}\right]^d \binom{d-1}{i} \left[2^\tau \sqrt{d+1} - 1\right]^{d-1-i}.$$

Proof.

Use Hadamard's bound on bounding determinants. □

Univariate case (cont).

Since the minimum m is a root of $R(Z)$, Cauchy's bound finally implies the following theorem

Theorem

Let $P \in \mathbb{Z}[T]$ be a univariate polynomial of degree d taking only positive values on the interval $[0,1]$. Let τ be an upper bound on the bitsize of the coefficients of P. Let m denote the minimum of P over $[0,1]$. Then

$$m > \frac{3^{d/2}}{2^{(2d-1)\tau}(d+1)^{2d-1/2}}.$$

Multivariate Case

- We first show that, at the cost of slightly increasing the bitsize of the coefficients, we can assume that the minimum is attained in the interior of the simplex (and not on the boundary).
- Obviously, there exists a face (say) σ of Δ, of dimension $0 \leq s \leq k$, such that the minimum m is attained at a point of the interior of σ.
- Denote by

$$\begin{cases} V_0 = 0 \\ V_i = e_i \quad (1 \leq i \leq k) \end{cases}$$

the vertices of Δ, and

$$\begin{cases} \lambda_0 = 1 - \sum X_i \\ \lambda_i = X_i \quad (1 \leq i \leq k) \end{cases}$$

the associated barycentric coordinates.

Multivariate Case

- We first show that, at the cost of slightly increasing the bitsize of the coefficients, we can assume that the minimum is attained in the interior of the simplex (and not on the boundary).
- Obviously, there exists a face (say) σ of Δ, of dimension $0 \leq s \leq k$, such that the minimum m is attained at a point of the interior of σ.
- Denote by

$$\begin{cases} V_0 = 0 \\ V_i = e_i \quad (1 \leq i \leq k) \end{cases}$$

the vertices of Δ, and

$$\begin{cases} \lambda_0 = 1 - \sum X_i \\ \lambda_i = X_i \quad (1 \leq i \leq k) \end{cases}$$

the associated barycentric coordinates.

Multivariate Case

- We first show that, at the cost of slightly increasing the bitsize of the coefficients, we can assume that the minimum is attained in the interior of the simplex (and not on the boundary).
- Obviously, there exists a face (say) σ of Δ, of dimension $0 \leq s \leq k$, such that the minimum m is attained at a point of the interior of σ.
- Denote by

$$\begin{cases} V_0 = 0 \\ V_i = e_i \quad (1 \leq i \leq k) \end{cases}$$

the vertices of Δ, and

$$\begin{cases} \lambda_0 = 1 - \sum X_i \\ \lambda_i = X_i \quad (1 \leq i \leq k) \end{cases}$$

the associated barycentric coordinates.

Replacing P by P_σ

- There exists a subset $I = \{i_0, \ldots, i_s\}$ of $\{0, \ldots, k\}$ such that the vertices of σ are the vertices $(V_i)_{i \in I}$. Let $J = \{0, \ldots, k\} \setminus I$.
- Make the following substitutions in P:
  - If $j \in J$ and $j > 0$, replace the variable X_j by 0
  - If $j \in J$ and $j = 0$, replace the variable X_{i_0} by $1 - \sum_{\ell=1}^{s} X_{i_\ell}$

  to obtain $P_\sigma \in \mathbb{Z}\left[X_{i_1}, \ldots, X_{i_s}\right]$ satisfying :

$$\min_{\Delta} P = \min_{\mathring{\sigma}} P_\sigma.$$

- Renaming the variables X_{i_ℓ} by Y_ℓ, we obtain that $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ verifies:
- $\deg(P_\sigma) \leq d$ and the bitsize of its coefficients is bounded by $\tau = \tau + 1 + d\,\mathrm{bit}(k)$

Replacing P by P_σ

- There exists a subset $I = \{i_0, \ldots, i_s\}$ of $\{0, \ldots, k\}$ such that the vertices of σ are the vertices $(V_i)_{i \in I}$. Let $J = \{0, \ldots, k\} \setminus I$.
- Make the following substitutions in P:
  - If $j \in J$ and $j > 0$, replace the variable X_j by 0
  - If $j \in J$ and $j = 0$, replace the variable X_{i_0} by $1 - \sum_{\ell=1}^{s} X_{i_\ell}$

  to obtain $P_\sigma \in \mathbb{Z}\left[X_{i_1}, \ldots, X_{i_s}\right]$ satisfying :

$$\min_{\Delta} P = \min_{\overset{\circ}{\sigma}} P_\sigma.$$

- Renaming the variables X_{i_ℓ} by Y_ℓ, we obtain that $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ verifies:
- $\deg(P_\sigma) \leq d$ and the bitsize of its coefficients is bounded by $\tau = \tau + 1 + d\,\mathrm{bit}(k)$

Replacing P by P_σ

- There exists a subset $I = \{i_0, \ldots, i_s\}$ of $\{0, \ldots, k\}$ such that the vertices of σ are the vertices $(V_i)_{i \in I}$. Let $J = \{0, \ldots, k\} \setminus I$.
- Make the following substitutions in P:
  - If $j \in J$ and $j > 0$, replace the variable X_j by 0
  - If $j \in J$ and $j = 0$, replace the variable X_{i_0} by $1 - \sum_{\ell=1}^{s} X_{i_\ell}$

  to obtain $P_\sigma \in \mathbb{Z}\left[X_{i_1}, \ldots, X_{i_s}\right]$ satisfying :

$$\min_{\Delta} P = \min_{\mathring{\sigma}} P_\sigma.$$

- Renaming the variables X_{i_ℓ} by Y_ℓ, we obtain that $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ verifies:
- $\deg(P_\sigma) \leq d$ and the bitsize of its coefficients is bounded by $\tau = \tau + 1 + d\,\mathrm{bit}(k)$

Replacing P by P_σ

- There exists a subset $I = \{i_0, \ldots, i_s\}$ of $\{0, \ldots, k\}$ such that the vertices of σ are the vertices $(V_i)_{i \in I}$. Let $J = \{0, \ldots, k\} \setminus I$.
- Make the following substitutions in P:
  - If $j \in J$ and $j > 0$, replace the variable X_j by 0
  - If $j \in J$ and $j = 0$, replace the variable X_{i_0} by $1 - \sum_{\ell=1}^{s} X_{i_\ell}$

  to obtain $P_\sigma \in \mathbb{Z}\left[X_{i_1}, \ldots, X_{i_s}\right]$ satisfying :

$$\min_{\Delta} P = \min_{\mathring{\sigma}} P_\sigma.$$

- Renaming the variables X_{i_ℓ} by Y_ℓ, we obtain that $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ verifies:
- $\deg(P_\sigma) \leq d$ and the bitsize of its coefficients is bounded by $\tau_\sigma = \tau + 1 + d\,\mathrm{bit}(k)$

Zeros of the gradient ideal

- Since $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ achieves its minimum in the interior of σ (and not on the boundary of σ);
- Consequently, m is attained at a critical point of P_σ, *i.e.* a point $x \in \mathbb{R}^s$ such that the gradient of P_σ is zero at x.
- Thus, P achieves its minimum on some connected component C of the real zeros of the gradient ideal contained in the interior of σ (on which the P is constant).
- However, note that the real variety defined by the gradient ideal can have positive dimension and be singular.

Zeros of the gradient ideal

- Since $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ achieves its minimum in the interior of σ (and not on the boundary of σ);
- Consequently, m is attained at a critical point of P_σ, *i.e.* a point $x \in \mathbb{R}^s$ such that the gradient of P_σ is zero at x.
- Thus, P achieves its minimum on some connected component C of the real zeros of the gradient ideal contained in the interior of σ (on which the P is constant).
- However, note that the real variety defined by the gradient ideal can have positive dimension and be singular.

Zeros of the gradient ideal

- Since $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ achieves its minimum in the interior of σ (and not on the boundary of σ);
- Consequently, m is attained at a critical point of P_σ, *i.e.* a point $x \in \mathbb{R}^s$ such that the gradient of P_σ is zero at x.
- Thus, P achieves its minimum on some connected component C of the real zeros of the gradient ideal contained in the interior of σ (on which the P is constant).
- However, note that the real variety defined by the gradient ideal can have positive dimension and be singular.

Zeros of the gradient ideal

- Since $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ achieves its minimum in the interior of σ (and not on the boundary of σ);
- Consequently, m is attained at a critical point of P_σ, *i.e.* a point $x \in \mathbb{R}^s$ such that the gradient of P_σ is zero at x.
- Thus, P achieves its minimum on some connected component C of the real zeros of the gradient ideal contained in the interior of σ (on which the P is constant).
- However, note that the real variety defined by the gradient ideal can have positive dimension and be singular.

Technique for finding a critical point of P_σ

- Let
$$Q = \sum_1^s (\frac{\partial P_\sigma}{\partial Y_i})^2.$$
- We are interested in finding a point in each bounded connected component of $Z(Q, \mathbb{R}^k)$.

Technique for finding a critical point of P_σ

- Let
$$Q = \sum_1^s (\frac{\partial P_\sigma}{\partial Y_i})^2.$$
- We are interested in finding a point in each bounded connected component of $Z(Q, \mathbb{R}^k)$.

Rational Univariate Representation

An $s-$rational univariate representation u is an $(s+3)-$tuple of the form

$$u = (F(T), g_0(T), \ldots, g_s(T), \pi)$$

such that:

1. $F, g_0, \ldots, g_s \in \mathbb{R}[T]$,
2. F and g_0 are coprime,
3. π is a Thom encoding of a root $t_\pi \in \mathbb{R}$ of F.

The point associated to u is defined by

$$x_u = \left(\frac{g_1(t_\pi)}{g_0(t_\pi)}, \ldots, \frac{g_s(t_\pi)}{g_0(t_\pi)} \right).$$

Rational Univariate Representation

An $s-$rational univariate representation u is an $(s+3)-$tuple of the form

$$u = (F(T), g_0(T), \ldots, g_s(T), \pi)$$

such that:

1. $F, g_0, \ldots, g_s \in \mathbb{R}[T]$,
2. F and g_0 are coprime,
3. π is a Thom encoding of a root $t_\pi \in \mathbb{R}$ of F.

The point associated to u is defined by

$$x_u = \left(\frac{g_1(t_\pi)}{g_0(t_\pi)}, \ldots, \frac{g_s(t_\pi)}{g_0(t_\pi)} \right).$$

Rational Univariate Representation

An $s-$rational univariate representation u is an $(s+3)-$tuple of the form

$$u = (F(T), g_0(T), \ldots, g_s(T), \pi)$$

such that:

1. $F, g_0, \ldots, g_s \in \mathbb{R}[T]$,
2. F and g_0 are coprime,
3. π is a Thom encoding of a root $t_\pi \in \mathbb{R}$ of F.

The point associated to u is defined by

$$x_u = \left(\frac{g_1(t_\pi)}{g_0(t_\pi)}, \ldots, \frac{g_s(t_\pi)}{g_0(t_\pi)} \right).$$

Bounded Algebraic Sampling

- Input: A polynomial $Q \in \mathbb{Z}[X_1, \ldots X_s]$, of degree bounded by d_Q, nonnegative over $\mathbb{R}^s$.
- Output: A set $\mathcal{U}$ of rational univariate representations of the form

$$(F(T), g_0(T), \ldots, g_s(T), \pi)$$

where the polynomials $F, g_0, \ldots, g_s$ have integer coefficients, and such that the associated points meet every bounded connected component of $\mathrm{Z}(Q, \mathbb{R}^k)$.
- replace Q by a deformation $\mathrm{Def}(Q, d_Q, \zeta)$ of degree bounded by $d_Q + 2$, where ζ is an infinitesimal,
- consider the critical points $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ of $\mathrm{Def}(Q, d_Q, \zeta)$ in the X_1-direction,

Bounded Algebraic Sampling

- Input: A polynomial $Q \in \mathbb{Z}[X_1, \ldots X_s]$, of degree bounded by d_Q, nonnegative over $\mathbb{R}^s$.
- Output: A set $\mathcal{U}$ of rational univariate representations of the form

$$(F(T), g_0(T), \ldots, g_s(T), \pi)$$

where the polynomials $F, g_0, \ldots, g_s$ have integer coefficients, and such that the associated points meet every bounded connected component of $Z(Q, \mathbb{R}^k)$.

- replace Q by a deformation $\mathrm{Def}(Q, d_Q, \zeta)$ of degree bounded by $d_Q + 2$, where ζ is an infinitesimal,
- consider the critical points $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ of $\mathrm{Def}(Q, d_Q, \zeta)$ in the X_1-direction,

Bounded Algebraic Sampling

- Input: A polynomial $Q \in \mathbb{Z}[X_1, \ldots X_s]$, of degree bounded by d_Q, nonnegative over $\mathbb{R}^s$.
- Output: A set $\mathcal{U}$ of rational univariate representations of the form

$$(F(T), g_0(T), \ldots, g_s(T), \pi)$$

where the polynomials $F, g_0, \ldots, g_s$ have integer coefficients, and such that the associated points meet every bounded connected component of $Z(Q, \mathbb{R}^k)$.

- replace Q by a deformation $\mathrm{Def}(Q, d_Q, \zeta)$ of degree bounded by $d_Q + 2$, where ζ is an infinitesimal,
- consider the critical points $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ of $\mathrm{Def}(Q, d_Q, \zeta)$ in the X_1-direction,

Bounded Algebraic Sampling

- Input: A polynomial $Q \in \mathbb{Z}[X_1, \ldots X_s]$, of degree bounded by d_Q, nonnegative over $\mathbb{R}^s$.
- Output: A set $\mathcal{U}$ of rational univariate representations of the form

$$(F(T), g_0(T), \ldots, g_s(T), \pi)$$

where the polynomials $F, g_0, \ldots, g_s$ have integer coefficients, and such that the associated points meet every bounded connected component of $Z(Q, \mathbb{R}^k)$.

- replace Q by a deformation $\mathrm{Def}(Q, d_Q, \zeta)$ of degree bounded by $d_Q + 2$, where ζ is an infinitesimal,
- consider the critical points $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ of $\mathrm{Def}(Q, d_Q, \zeta)$ in the X_1-direction,

Bounded Algebraic Sampling (cont.)

- due to the properties of $\mathrm{Def}(Q, d_Q, \zeta)$,
  - $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ has a finite number of points,
  - the quotient ring defined by the equations of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ is a vector space of dimension at most

$$(d_Q + 2)(d_Q + 1)^{k-1},$$

  - its multiplication table can be easily computed,
- find rational univariate representations of the points of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$,
- take their limits with respect to ζ, which define a finite set of points intersecting all the bounded connected components of $\mathcal{Z}(Q)$.

Bounded Algebraic Sampling (cont.)

- due to the properties of $\mathrm{Def}(Q, d_Q, \zeta)$,
  - $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ has a finite number of points,
  - the quotient ring defined by the equations of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ is a vector space of dimension at most

$$(d_Q + 2)(d_Q + 1)^{k-1},$$

  - its multiplication table can be easily computed,
- find rational univariate representations of the points of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$,
- take their limits with respect to ζ, which define a finite set of points intersecting all the bounded connected components of $\mathcal{Z}(Q)$.

Bounded Algebraic Sampling (cont.)

- due to the properties of $\mathrm{Def}(Q, d_Q, \zeta)$,
  - $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ has a finite number of points,
  - the quotient ring defined by the equations of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ is a vector space of dimension at most

$$(d_Q + 2)(d_Q + 1)^{k-1},$$

  - its multiplication table can be easily computed,
- find rational univariate representations of the points of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$,
- take their limits with respect to ζ, which define a finite set of points intersecting all the bounded connected components of $\mathcal{Z}(Q)$.

Bounded Algebraic Sampling (cont.)

- due to the properties of $\mathrm{Def}(Q, d_Q, \zeta)$,
  - $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ has a finite number of points,
  - the quotient ring defined by the equations of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ is a vector space of dimension at most

$$(d_Q + 2)(d_Q + 1)^{k-1},$$

  - its multiplication table can be easily computed,
- find rational univariate representations of the points of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$,
- take their limits with respect to ζ, which define a finite set of points intersecting all the bounded connected components of $\mathcal{Z}(Q)$.

Bounded Algebraic Sampling (cont.)

- due to the properties of $\mathrm{Def}(Q, d_Q, \zeta)$,
  - $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ has a finite number of points,
  - the quotient ring defined by the equations of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ is a vector space of dimension at most

$$(d_Q + 2)(d_Q + 1)^{k-1},$$

  - its multiplication table can be easily computed,
- find rational univariate representations of the points of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$,
- take their limits with respect to ζ, which define a finite set of points intersecting all the bounded connected components of $\mathcal{Z}(Q)$.

Bounded Algebraic Sampling (cont.)

- due to the properties of $\mathrm{Def}(Q, d_Q, \zeta)$,
  - $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ has a finite number of points,
  - the quotient ring defined by the equations of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ is a vector space of dimension at most

$$(d_Q + 2)(d_Q + 1)^{k-1},$$

  - its multiplication table can be easily computed,
- find rational univariate representations of the points of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$,
- take their limits with respect to ζ, which define a finite set of points intersecting all the bounded connected components of $\mathcal{Z}(Q)$.

Complexity of Bounded Algebraic Sampling

The complexity analysis in *BPR* shows that, if d_Q is a bound on the degree of Q and τ_Q a bound on the bitsize of its coefficients, then:

1. The degrees of the polynomials $F, g_0, \ldots, g_k$ are bounded by
$$(d_Q + 2)(d_Q + 1)^{k-1}$$
2. The bitsize of their coefficients is bounded by
$$(d_Q+2)(d_Q+1)^{k-1}(kd_Q+2)\left(\tau' + 2\,\mathrm{bit}(kd_Q + 3) + 3\mu + \mathrm{bit}(k)\right),$$
where
$$\begin{aligned} \tau' &= \sup\left[\tau_Q, \mathrm{bit}(2k)\right] + 2\,\mathrm{bit}\left[k(d_Q + 2)\right] + 1 \\ \mu &= \mathrm{bit}\left[(d_Q + 2)(d_Q + 1)^{k-1}\right]. \end{aligned}$$

Complexity of Bounded Algebraic Sampling

The complexity analysis in *BPR* shows that, if d_Q is a bound on the degree of Q and τ_Q a bound on the bitsize of its coefficients, then:

1. The degrees of the polynomials $F, g_0, \ldots, g_k$ are bounded by
$$(d_Q + 2)(d_Q + 1)^{k-1}$$

2. The bitsize of their coefficients is bounded by
$$(d_Q+2)(d_Q+1)^{k-1}(kd_Q+2)\left(\tau' + 2\,\mathrm{bit}(kd_Q + 3) + 3\mu + \mathrm{bit}(k)\right),$$
where
$$\begin{aligned} \tau' &= \sup\left[\tau_Q, \mathrm{bit}(2k)\right] + 2\,\mathrm{bit}\left[k(d_Q + 2)\right] + 1 \\ \mu &= \mathrm{bit}\left[(d_Q + 2)(d_Q + 1)^{k-1}\right]. \end{aligned}$$

Bit size bounds in our case

Specializing to our system we get:

- The degree of the polynomials $F, g_0, \ldots, g_s$ is bounded by d_u, where
$$d_u = 2d(2d-1)^{k-1}.$$

- Moreover, the bitsize of their coefficients is bounded by
$$\tau_u = d_u(2kd-2k+2)\left[\tau' + 2\,\mathrm{bit}(2kd-2k+3) + 3\,\mathrm{bit}(d_u) + \mathrm{bit}(k)\right]$$
where
$$\tau' = 2\tau + (2d+2)\,\mathrm{bit}(k) + (k+3)\,\mathrm{bit}(d) + 5.$$

Bit size bounds in our case

Specializing to our system we get:

- The degree of the polynomials $F, g_0, \ldots, g_s$ is bounded by d_u, where
$$d_u = 2d(2d-1)^{k-1}.$$

- Moreover, the bitsize of their coefficients is bounded by
$$\tau_u = d_u(2kd-2k+2)\left[\tau' + 2\,\mathrm{bit}(2kd-2k+3) + 3\,\mathrm{bit}(d_u) + \mathrm{bit}(k)\right.$$
where
$$\tau' = 2\tau + (2d+2)\,\mathrm{bit}(k) + (k+3)\,\mathrm{bit}(d) + 5.$$

Main Result

Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ be a polynomial of degree d, τ a bound on the bitsize of its coefficients and $m = \min_{\Delta} P$ the minimum of P over the simplex Δ. Assume that $m > 0$.
Let

$$D = 2d(2d-1)^{k-1},$$
$$\rho = D(2kd - 2k + 2)\left[\tau' + 2\,\mathrm{bit}(2kd - 2k + 3) + 3\,\mathrm{bit}(D) + \mathrm{bit}(k)\right],$$
$$\rho' = d\left[\rho + \mathrm{bit}(D+1)\right] + \tau + d\,\mathrm{bit}(k) + d + k + 1,$$

where

$$\tau' = 2\tau + (2d+2)\,\mathrm{bit}(k) + (k+3)\,\mathrm{bit}(d) + 5.$$

Then,

$$m > m_{k,d,\tau} = \frac{1}{\left\lceil 2^{\rho'+1}\sqrt{dD+1}\right\rceil^{D}\left\lceil 2^{\rho}\sqrt{D+1}\right\rceil^{dD}}.$$

A more compact form

$$\frac{1}{m_{k,d,\tau}} \leq (2^{\tau})^{2^{k+3}d^{k+1}k} \, 2^{2^{k+6}d^{k+2}k^2} \, k^{2^{k+5}d^{k+2}k} \, d^{2^{k+5}d^{k+1}k^2}.$$

Improvements

- Jeronimo and Perrucci[2009] has obtained a better bound. They obtain

$$m > m_{k,d,\tau} = 2^{-(\tau+1)d^{k+1}} d^{-(k+1)d^k} \binom{d+k}{k+1}^{(d^k-1)(d-1)}.$$

Using the fact that $\binom{d+k}{k+1} < d^{k+1}$ the bound can be simplified to

$$m > m_{k,d,\tau} = 2^{-(\tau+1)d^{k+1}} d^{-(k+1)d^{k+1}}.$$

Idea behind the improvements

- Idea behind the improvement is to deform directly the polynomial P so that the gradient ideal becomes algebraically nice (zero-dimensional etc.), instead of dealing with a possibly singular gradient ideal of P as we do by taking a sum of squares and deforming it.
- In ongoing work we have obtained explicit non-uniform bounds on other quantities such as the radius of balls needed to contain all bounded components etc. using similar ideas.

Idea behind the improvements

- Idea behind the improvement is to deform directly the polynomial P so that the gradient ideal becomes algebraically nice (zero-dimensional etc.), instead of dealing with a possibly singular gradient ideal of P as we do by taking a sum of squares and deforming it.
- In ongoing work we have obtained explicit non-uniform bounds on other quantities such as the radius of balls needed to contain all bounded components etc. using similar ideas.