Testing systems of real quadratic equations for (approximate) solutions

Alexander Barvinok

February 4, 2021

Solving systems of polynomial equations

Given a system of real polynomial equations

$$p_i(x_1, \ldots, x_n) = 0 \quad \text{for} \quad i = 1, \ldots, m,$$

how hard is it to

a) decide if there is a solution

b) if there is a solution, to find one

c) describe the set of all solutions?

Answer: Generally speaking, pretty hard.
A good reference: S. Basu, R. Pollack, and M.-F. Roy, Algorithms in Real Algebraic Geometry. Second edition, Algorithms and Computation in Mathematics, **10** Springer-Verlag, Berlin, 2006. x+662.

Solving systems of polynomial equations

Two main parameters: the number n of variables and the largest degree d of the equation. Any number of equations can be reduced to one by doubling the degree:

$$p_i\left(x_1, \ldots, x_n\right) = 0 \quad \text{for} \quad i = 1, \ldots, m$$

$$\Updownarrow$$

$$\sum_{i=1}^{m} p_i^2\left(x_1, \ldots, x_n\right) = 0.$$

The complexity of
a) deciding whether there is a solution is roughly $d^{O(n)}$.

b) What does it even mean, to find a solution? One possibility is to use the *Thom encoding* of a real algebraic number: the minimal polynomial and signs of all its derivatives at the desired root. With that, the complexity is roughly $d^{O(n)}$.

c) The complexity of describing the set of solutions can be doubly exponential in n (computing Betti numbers). The problem can also be undecidable (homotopy type).

Systems of quadratic equations

If $d = 1$, we have a system of linear equations which can be solved in $O(n^3)$ time by Gaussian elimination.

What if $d = 2$? Quadratic equations are special.
First, any system of polynomial equations can be reduced to a system quadratic via substitutions of the type

$$y_{ij} := x_i x_j.$$

Second, some systems of quadratic equations naturally arise in applied problems.

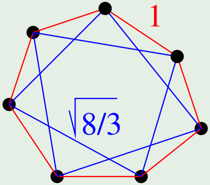
Example (Distance Geometry, Computational Chemistry)

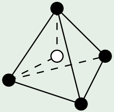
Question: Are there seven points $v_1, v_2, v_3, v_4, v_5, v_7$ in $\mathbb{R}^3$ such that

$$\|v_{(i+1) \mod 7} - v_i\| = 1 \quad \text{and} \quad \|v_{(i+2) \mod 7} - v_i\| = \sqrt{\frac{8}{3}}$$

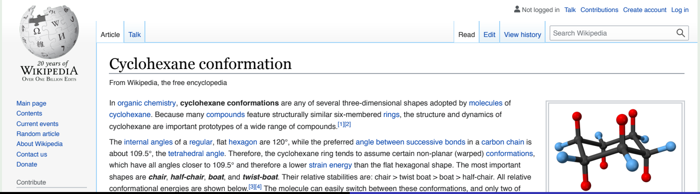
for $i = 1, \ldots, 7$?

Example (Distance Geometry, Computational Chemistry)





The same question for six points.
Check


20 years of WIKIPEDIA
Over One Billion Edits

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute

Cyclohexane conformation

From Wikipedia, the free encyclopedia

In organic chemistry, **cyclohexane conformations** are any of several three-dimensional shapes adopted by molecules of cyclohexane. Because many compounds feature structurally similar six-membered rings, the structure and dynamics of cyclohexane are important prototypes of a wide range of compounds.[1][2]

The internal angles of a regular, flat hexagon are 120°, while the preferred angle between successive bonds in a carbon chain is about 109.5°, the tetrahedral angle. Therefore, the cyclohexane ring tends to assume certain non-planar (warped) conformations, which have all angles closer to 109.5° and therefore a lower strain energy than the flat hexagonal shape. The most important shapes are ***chair***, ***half-chair***, ***boat***, and ***twist-boat***. Their relative stabilities are: chair > twist boat > boat > half-chair. All relative conformational energies are shown below.[3][4] The molecule can easily switch between these conformations, and only two of

Systems of quadratic equations

Another example includes "trust region subproblems", see D. Bienstock, A note on polynomial solvability of the CDT problem, *SIAM J. Optim.* **26** (2016), no. 1, 488–498.

Results: A system of k quadratic equations in n real variables can be solved (questions a) and b) answered) in $n^{O(k)}$ time. In particular, if k is fixed in advance, in polynomial time.

Testing whether a system of homogeneous quadratic equations has a non-trivial solution: A. Barvinok, Feasibility testing for systems of real quadratic equations, *Discrete Comput. Geom.* **10** (1993), no. 1, 1–13.
In the whole generality: D. Grigoriev and D.V. Pasechnik, Polynomial-time computing over quadratic maps. I. Sampling in real algebraic sets. *Comput. Complexity* **14** (2005), no. 1, 20–52.

Systems of quadratic equations

For the description of the set of solutions (question c)), see S. Basu, D.V. Pasechnik, and M.-F. Roy, Bounding the Betti numbers and computing the Euler-Poincaré characteristic of semi-algebraic sets defined by partly quadratic systems of polynomials, *J. Eur. Math. Soc. (JEMS)* **12** (2010), no. 2, 529–553.

Here is an idea for systems of homogeneous quadratic equations. This is *not* how it has been done, but it shows a useful underlying algebraic structure.

Let

$$q_i(x) = \langle x, Q_i x \rangle \quad \text{for} \quad i = 1, \ldots, k,$$

where Q_i are $n \times n$ symmetric matrices and $\langle \cdot, \cdot \rangle$ is the standard inner product in $\mathbb{R}^n$.

Let

$$\mathbb{S}^{n-1} = \{x \in \mathbb{R}^n : \quad \|x\| = 1\}$$

be the unit sphere endowed with the rotation invariant Borel probability measure μ.

The generating function

Theorem

In a neighborhood of $z_1 = \ldots = z_k = 0$, *we have*

$$\det^{-\frac{1}{2}}\left(I - \sum_{i=1}^{k} z_i Q_i\right) = \sum_{m_1,\ldots,m_k \geq 0} a_{m_1,\ldots,m_k} z_1^{m_1} \cdots z_k^{m_k},$$

where

$$a_{m_1,\ldots,m_k} = \frac{\Gamma\left(m_1 + \ldots + m_k + \frac{n}{2}\right)}{m_1! \cdots m_k! \Gamma\left(\frac{n}{2}\right)} \times \int_{\mathbb{S}^{n-1}} q_1^{m_1}(x) \cdots q_k^{m_k}(x) \; d\mu(x).$$

The generating function

Proof: We note that for

$$q(x) = \langle x, Q_x \rangle,$$

in a neighborhood of $z = 0$, we have

$$\frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} e^{zq(x)/2} e^{-\|x\|^2/2} \ dx = \det^{-\frac{1}{2}} (I - zQ) \, .$$

Consequently,

$$\frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} e^{(z_1 q_1(x) + \ldots + z_k q_k(x))/2} e^{-\|x\|^2/2} \ dx = \det^{-\frac{1}{2}} \left(I - \sum_{i=1}^{k} z_i Q_i \right) .$$

Expanding into the Taylor series in a neighborhood of $z_1 = \ldots = z_k = 0$, we get

$$\det^{-\frac{1}{2}} \left(I - \sum_{i=1}^{k} z_i Q_i \right) = \sum_{m_1, \ldots, m_k \geq 0} b_{m_1, \ldots, m_k} z_1^{m_1} \cdots z_k^{m_k},$$

The generating function

where

$$b_{m_1,\ldots,m_k} = \frac{1}{2^{m_1+\ldots+m_k} m_1! \cdots m_k!} \times \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} q_1^{m_1}(x) \cdots q_k^{m_k}(x) e^{-\|x\|^2/2} \, dx.$$

For a homogeneous polynomial $F(x)$ of degree $2m = 2m_1 + \ldots + 2m_k$, we have

$$\frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} F(x) e^{-\|x\|^2/2} \, dx = \frac{2^m \Gamma\left(m + \frac{n}{2}\right)}{\Gamma\left(\frac{n}{2}\right)} \int_{\mathbb{S}^{n-1}} F(x) e^{-\|x\|^2/2} \, d\mu(x).$$

$\square$

The generating function

Corollary: The integral

$$\int_{\mathbb{S}^{n-1}} q_1^{m_1}(x) \cdots q_k^{m_k}(x) \ d\mu(x)$$

can be computed in $n^{O(1)} \left(m_1 + \ldots + m_k\right)^{O(k)}$ time.

If $q_1, \ldots, q_k : \mathbb{R} \longrightarrow \mathbb{R}$ are positive semidefinite, then for large m,

$$\left(\int_{\mathbb{S}^{n-1}} \left(q_1(x) \ldots q_k(x)\right)^m \ d\mu(x) \right)^{1/m} \approx \max_{x \in \mathbb{S}^{n-1}} q_1(x) \cdots q_k(x).$$

In fact, to approximate the maximum within relative error ϵ, we can choose $m = O\left(\frac{n+km}{\epsilon}\right)$.
Remark: If k is fixed in advance, we can do it in polynomial time *exactly*.

The generating function

Connection to feasibility: Given quadratic forms $q_1, \ldots, q_k : \mathbb{R}^n \longrightarrow \mathbb{R}$, let us define

$$q_i^+ = \|x\|^2 + \epsilon q_i(x) \quad \text{and} \quad q_i^- = \|x\|^2 - \epsilon q_i(x) \quad \text{for} \quad i = 1, \ldots, k$$

and some small $\epsilon > 0$.
Then

$$\begin{aligned} &\max_{x \in \mathbb{S}^{n-1}} q_1^+(x) \cdots q_k^+(x) q_1^-(x) \cdots q_k^-(x) \\ = &\max_{x \in \mathbb{S}^{n-1}} \left(1 - \epsilon^2 q_1^2(x)\right) \cdots \left(1 - \epsilon^2 q_k^2(x)\right) \\ = &\begin{cases} 1 & \text{if} \quad q_i(x) = 0 \quad \text{for some } x \in \mathbb{S}^{n-1} \quad \text{and all } i \\ < 1 & \text{otherwise.} \end{cases} \end{aligned}$$

Computing the integral may allow us to estimate the volume of the set of solutions.

Partition function

What can we do if the number k of equations grows? Here is the idea: Choose a δ-shaped function $F \longrightarrow [0,1]$, such that

$$F(y) = \begin{cases} 1 & \text{if} \quad y = 0 \\ < 1 & \text{if} \quad y \neq 0 \end{cases}$$

and try to compute

$$\frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} F\left(q_1(x)\right) \cdots F\left(q_k(x)\right) e^{-\|x\|^2/2} \, dx.$$

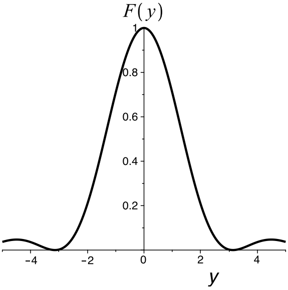
Note that the standard Gaussian probability measure with density $(2\pi)^{-n/2} e^{-\|x\|^2/2}$ is concentrated around $\|x\| = \sqrt{n}$, that is,

$$\mathbf{Prob}\left\{x: \ (1-\epsilon)n \leq \|x\|^2 \leq \frac{n}{1-\epsilon}\right\} \geq 1 - 2e^{-\epsilon^2 n/4} \quad \text{for} \quad 0 < \epsilon < 1.$$

Partition function

Hence if the integral is large, then there are many x with most $q_i(x) \approx 0$ and if the integral is small, then there are few such x's. The sharper F is peaked at 0, the better we can do. We choose

$$F(y) = \frac{\sin^2 y}{y^2}.$$



Partition function

Main result: There is an absolute constant $\gamma > 0$ (one can choose $\gamma = 0.09$) such that the following holds. Let $q_i : \mathbb{R}^n \longrightarrow \mathbb{R}$, $i = 1, \ldots, k$, be quadratic forms in n real variables $x_1, \ldots, x_n$, such that each q_i depends on at most r variables among $x_1, \ldots, x_n$, has common variables with at most $r - 1$ other forms q_j and satisfies

$$|q_i(x)| \leq \frac{\gamma \|x\|^2}{r} \quad \text{for} \quad i = 1, \ldots, k.$$

Then, for any $0 < \epsilon < 1$, one can compute the value of

$$\frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} e^{-\|x\|^2/2} \prod_{i=1}^{k} \frac{\sin^2 q_i(x)}{q_i^2(x)} \, dx$$

within relative error ϵ in quasi-polynomial $(m+n)^{O(\ln(m+n) - \ln \epsilon)}$ time.

Partition function

Suppose that $r = n$ (no restriction on sparseness) and consider the following asymptotic regime:

$$n \longrightarrow \infty, \quad n = km \quad \text{where} \quad m \gg \ln n.$$

Let

$$X = \left\{ x \in \mathbb{R}^n : \quad q_i(x) = 0 \quad \text{for} \quad i = 1, \ldots, k \right\}.$$

We say that "there are many solution" if

$$\textbf{Prob}\left\{ \operatorname{dist}(x, X) \ \leq \ n^{-\gamma} \right\} \ \geq \ n^{-O(k)}$$

for some constant $\gamma > 2$.

We say that the system is "far from having a solution", if for all $x \in \mathbb{R}^n$ such that $\|x\| = \sqrt{n}$, for at least δk of the forms q_i we have $|q_i(x)| > \beta$ for some constants $\delta > 0$ and $\beta > 0$.

Let us copy each form q_i exactly m times in the integral. Then, for systems having "many solutions" the value of the integral is $n^{-O(k)}$, while for systems that are "far from having a solution", the value is $2^{-\Omega(n)}$, so we can tell them apart.

Partition function

Theorem

There is an absolute constant $0 < \gamma_0 < 0.25$ *(one can choose* $\gamma_0 = 0.1$*) such that the following holds. Let* $q_i : \mathbb{R}^n \longrightarrow \mathbb{R}$, $i = 1, \ldots, k$, *be quadratic forms in* n *real variables* $x_1, \ldots, x_n$, *such that each* q_i *depends on at most* r *variables among* $x_1, \ldots, x_n$, *has common variables with at most* $r - 1$ *other forms* q_j *and satisfies*

$$|q_i(x)| \leq \frac{\gamma_0 \|x\|^2}{r} \quad \text{for} \quad i = 1, \ldots, k.$$

Let

$$\phi(z) = \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{R}^n} e^{-\|x\|^2/2} \prod_{i=1}^{k} \frac{\sin^2 z q_i(x)}{z^2 q_i^2(x)} \, dx.$$

Then for every $z \in \mathbb{C}$ *such that* $|z| \leq 1$, *we have*

$$(1 - 4\gamma_0)^{-n/2} \geq |\phi(z)| \geq 2^{-k/2} (1 + 4\gamma_0)^{-n/2}.$$

Interpolation Lemma

Lemma

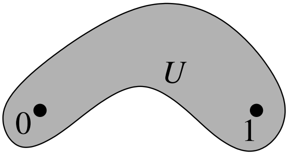
Let $U \subset \mathbb{C}$ be a connected open set containing 0 and 1. Then there is a constant $\gamma = \gamma(U) > 0$ such that the following holds: If

$$g(z) = \sum_{k=0}^{n} c_k z^k, \quad n \geq 2$$

is a polynomial such that $g(z) \neq 0$ for all $z \in U$ then, for any $0 < \epsilon < 1$, the value of $g(1)$, up to relative error ϵ, is determined by the coefficients c_k with $k \leq \gamma (\ln n - \ln \epsilon)$ and can be computed in $n^{O(1)}$ time from those coefficients.

Remark: We say that $w_1 \neq 0$ approximates $w_2 \neq 0$ within relative error ϵ if we can write $w_1 = e^{z_1}$ and $w_2 = e^{z_2}$ with $|z_1 - z_2| \leq \epsilon$.

Interpolation Lemma



If

$$g(z)=\sum_{k=0}^{n} c_k z^k$$

and $g(z) \neq 0$ in an open connected set containing 0 and 1, then, up to relative error $0<\epsilon<1$, the value of $g(1)$ is determined by only $O(\ln n - \ln \epsilon)$ lowest coefficients of g.

Interpolation Lemma: sketch of proof

So we have $g(z) = c_0 + c_1 z + \ldots + c_n z^n$ and $g(z) \neq 0$ for $z \in U$.
Special Case:

$$U = \{z : \ |z| < \beta\} \quad \text{for some} \quad \beta > 1.$$

Consider $f(z) = \ln g(z)$ and its Taylor polynomial at $z = 0$:

$$T_m(z) = f(0) + \sum_{k=1}^{m} \frac{f^{(k)}(0)}{k!} z^k.$$

Claim 1:

$$|f(1) - T_m(1)| \ \leq \ \frac{n}{\beta^m(\beta - 1)(m + 1)}.$$

Claim 2: $f^{(k)}(0)$ is a function of $c_0, \ldots, c_k$.

Interpolation Lemma: sketch of proof

Proof of Claim 1: We have

$$g(z) = g(0) \prod_{i=1}^{n} \left(1 - \frac{z}{\alpha_i}\right) \quad \text{where} \quad |\alpha_i| \geq \beta \quad \text{for} \quad i = 1, \ldots, n.$$

Hence

$$f(z) = f(0) + \sum_{i=1}^{n} \ln\left(1 - \frac{z}{\alpha_i}\right).$$

Now, if $|z| \leq 1$, we have

$$\ln\left(1 - \frac{z}{\alpha_i}\right) = -\sum_{k=1}^{m} \frac{z^k}{k\alpha_i^k} + \eta_i \quad \text{where}$$

$$|\eta_i| = \left| -\sum_{k=m+1}^{\infty} \frac{1}{k\alpha_i^k} \right| \leq \frac{1}{\beta^m(\beta - 1)(m+1)}.$$

Interpolation Lemma: sketch of proof

Proof of Claim 2: We have $f(z) = \ln g(z)$, so

$$f'(z) = \frac{g'(z)}{g(z)} \Longrightarrow g'(z) = f'(z)g(z)$$

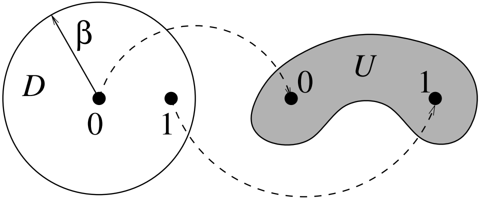
$$\Longrightarrow g^{(k)}(0) = \sum_{j=0}^{k-1} \binom{k-1}{j} f^{(k-j)}(0) g^{(j)}(0),$$

which is a triangular system of linear equations in $f^{(k)}(0)$ with $g(0) \neq 0$ on the diagonal.

General case: Construct an auxiliary disc

$$D = \{z : \ |z| < \beta\} \quad \text{for some} \quad \beta > 1$$

and a polynomial $\phi(z)$ such that $\phi(0) = 0$, $\phi(1) = 1$ and $\phi(D) \subset U$.



Interpolation Lemma: sketch of proof

Consider the composition

$$p(z) = g(\phi(z)).$$

Then $p(z) \neq 0$ for $z \in D$ and, by the special case, to compute $p(1) = g(1)$ within relative error ϵ, we need to access $O(\ln \deg p - \ln \epsilon)$ lowest coefficients of $p(z)$.

Since $\phi(0) = 0$, we need to access $O(\ln \deg g - \ln \epsilon)$ lowest coefficients of $g(z)$.