# Monodromy method for polynomial systems

Guillem Fernández Rodríguez

July, 2023

## Homotopy continuation to solve polynomial systems

Given some system of polynomials

$$F(x) = F(x_1, \ldots, x_n) = \begin{pmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_N(x_1, \ldots, x_n) \end{pmatrix}$$

for $f_i \in \mathbb{C}[x_1, \ldots, x_n]$. We want to find all of the solutions, that is, the points in the solution variety

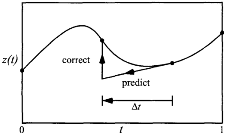
$$V(F) = \{x \in \mathbb{C}^n | F(x) = 0\}.$$

Suppose we also have a system $G$ of $m$ polynomials in $\mathbb{C}[x_1, \ldots, x_n]$, with at least as many solutions than $F$. Then under certain assumptions, we can construct a homotopy

$$H(x,t), \quad H(x,0) = F(x) \quad H(x,1) = G(x)$$

such that the all systems $H(x,t)$ for $t \in (0,1]$ have the same number of isolated solutions.

We can then track the solution paths $H(x^*(t),t) = 0$, $x^*(1) = y$ for $y$ a solution of $G$, by solving the differential equation obtained by differentiating with respect to $t$. This can be done using predictor-corrector numerical methods.




Figure

To construct the system $G$ and homotopy $H(x, t)$ we embed them in a parametrized family of polynomials. To be able to find all solutions in $F$ then, we need to consider a start polynomial in this system with at least as many roots as $F$, so obtaining a bound on the solution count gives us enough information to choose them.

The tighter the bound we have on the number of solutions the less paths we need to track. The most simple case are **total degree homotopies**, using Bezout's bound.

### Theorem (Bezout)

*If $f_1, \ldots, f_N$ have degrees $d_1, \ldots, d_N$, then the system has at most $d_1, \cdots, d_N$ solutions.*

# BKK bound

A better bound for the solutions with non-zero entries is the BKK bound.

### Theorem (Bernstein, 1975)

*The root count on* $(\mathbb{C}^*)^n$ *of a Laurent polynomial family specified by supports* $S_i, \ldots, S_n$ *and parameterized by the coefficients of the corresponding monomials is the mixed volume*

$$M(S_1, \ldots, S_n)$$

Because in the monodromy method applied to sparse polynomial systems we will be searching for solutions in $(\mathbb{C}^*)^n$, this is the bound we will mostly use.

# Monodromy method

We can now outline how the monodromy method [Bli+18] differs from homotopy continuation methods. Instead of tracking a solution from a different system, we will start from a known solution in the original system, and try to find a different solution. The basic idea, that we will refine later, will be the following:

1. Start from a solution $x_0$ of the system $F$.
2. Create a solution path that will end in some solution of $F$
3. Track $x_0$ through this solution path, to potentially find a new solution $x_i$.

# Setting

We will solve a generic polynomial system in a family of complex polynomial systems

$$F_p = \left(f_p^{(1)}, \ldots, f_p^{(N)}\right) = 0, \quad f_p^{(i)} \in \mathbb{C}[p][x], i = 1, \ldots, N.$$

with parameters $p \in \mathbb{C}^m$ and variables $x \in \mathbb{C}^n$ for some $m, n \in \mathbb{N}$. We constrain the problem to **linear parametric families of systems**

$$f_p^{(i)} = \sum_j A_j(p) x^j$$

for $A_j$ affine functions, $j = (j_1, \ldots, j_n)$ and $x^j = x_1^{j_1} \cdots x_n^{j_n}$.

We will also consider a subfamily of these called **sparse polynomial systems**, which consist of square ($N = n$) polynomial systems

$$f_p^{(i)} = \sum_j p_{i,j} x^j.$$

We can see that for a generic $p$ we have a nonempty finite set of solutions of $F_p(x) = 0$ with the same cardinality $d$, by the sharpness of Bezout's theorem.

Consider the example

$$f(x) = x^2 - 1 = 0.$$

that is in the parametrized linear system

$$f_{(v,w)} = vx^2 - w = 0$$

If $v = 0$ then there are no solutions except for $w = 0$, where there are infinite. If $w = 0$ then the solutions are the square roots of $\frac{w}{v}$, that are distinct if $w \neq 0$ and they are 0 with multiplicity two when $w = 0$.

For $(v, w) \in \mathbb{C}^2 \setminus (V(w) \cup V(v))$ there are 2 distinct solutions of multiplicity one.

Now we define a **parametrized linear variety of systems** as the image of an affine linear map

$$\begin{aligned} \varphi : \quad C^m &\to \varphi(C^m) \\ p &\mapsto F_p \end{aligned}$$

and we call the image **base space** $B := \varphi(C^m)$. Then $B$ is an irreducible variety because $C^m$ is irreducible.

With this notation we define the **solution variety** as

$$V = \{(F_p, x) \in B \times C^m | F_p(x) = 0\}.$$

We call **discriminant variety** $D$ the subset of the systems in the base space with nongeneric fibers. We have that its complement $B \setminus D$ is path-connected by the following theorem:

### Theorem (4.1.3 in [SW05])

*The complement of a proper quasiprojective algebraic subset $Y$ in an irreducible quasiprojective set $X$ is connected. If a quasiprojective set $X$ is connected, then $X$ is path connected.*

Then we have that the projection

$$\pi : V \to B$$

gives us a branched covering:

1. The fiber $\pi^{-1}(F_p)$ is finite of the same cardinality for a generic $p$.
2. $\pi$ is a covering of the generic points.

# Monodromy group

Now consider the fundamental group over $\pi_1(B \setminus D, p)$.

If we consider a system $F_p \in B \setminus D$ we can take a loop without branch points $\tau$, that is, a continuous function

$$\tau : [0,1] \to B \setminus D.$$

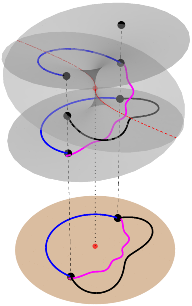
such that $\tau(0) = \tau(1) = F_p$.

Because $\pi$ is a branched covering with branch locus $D$, the restriction of $\pi$ to $V' = \pi^{-1}(B \setminus D)$ is a covering map over $B \setminus D$ (so for this matter we use $V := V'$). Then given an element in the fiber $x_i \in \pi^{-1}(F_p) = \{x_1, \ldots, x_d\}$, we can consider the unique corresponding lifting $\tilde{\pi}_i$, that is a continuous function

$$\tilde{\tau}_i : [0,1] \to V.$$

such that $\tilde{\tau}_i(0) = x_i$ and $\tilde{\tau}_i(1) = x_j$ for some $x_j \in \pi^{-1}(F_p)$ and $\pi \circ \tau_i = \tilde{\tau}_i$.

$$\begin{tikzcd}
V \arrow[drr, "\pi"'] & & {[0,1]} \arrow[ll, dashed, "\tilde{\tau}_i"'] \arrow[d, "\tau_i"] \\
& & B \setminus D
\end{tikzcd}$$



Now consider $F_p \in B \setminus D$ and $x_i \in \pi^{-1}(F_p)$.

Then given $[\tau] \in \pi_1(B \setminus D, F_p)$ we can define the lifting correspondence

$$\phi : \pi_1(B \setminus D, F_p) \to p^{-1}(F_p)$$

such that $\phi([\tau]) = \tilde{\tau}(1)$ for $\tilde{\tau}$ the lifting of a representant of $[\tau]$. This is a well-defined map and in fact we have the following result:

**Theorem (54.4. [Mun14])**

*Let $p : E \to B$ be a covering map; let $p(e_0) = b_0$. If $E$ is path connected, then the lifting correspondence $\phi$ is surjective.*

So if we could suppose that $V$ is path connected, we would have that all roots of the fiber $\pi^{-1}(F_p)$ are the endpoints of the lifting path of some loop in $x_i$. We make this assumption by replacing $V$ with its unique dominant irreducible component, and using that an affine variety in $C^N$ is path connected if it irreducible.

Now if consider the map

$$\varphi : \pi_1(B \setminus D, b_0) \to S_d$$

such that $\varphi([\tau]) = (ij)$ the permutation of the roots $x_i$ and $\tilde{\tau}(1) = x_j$, we have that $\varphi$ is a homomorphism of groups that acts transitively over the fiber $\pi^{-1}(F_p)$.

We call the image of $\varphi$ the **monodromy group** associated to $\pi^{-1}(F_p)$ and also represent it by $M(\pi_1(B \setminus D))$.

# Monodromy method

Now we have refined the idea to

1. Find one pair $(F_{p_0}, x_0)$ for a generic $F_{p_0}$.
2. Use the monodromy action on the fiber $\pi^{-1}(F_{p_0})$

but we still need a way to generate the monodromy group elements. As we have seen it is enough to generate different elements of $\pi_1(B \setminus D, F_{p_0})$. To do this we need to use homotopy continuation.

# Homotopy continuation

Given $F_{p_1}$ and $F_{p_2}$ in the base space $B$ we consider the **linear segment homotopy**

$$H(t) = (1-t)F_{p_1} + tF_{p_2}, \quad t \in [0,1]$$

If we take sufficiently generic $p_1, p_2$ we have that $H(t) \in B \setminus D$ for all $t \in [0,1]$, so $H(t)$ has $d$ solutions.

The lifting of this path on the solution variety is called **homotopy path** and establishes a one-to-one correspondence between the fibers, so we can obtain well defined solution paths.

We can also use the "Gamma trick" method to obtain different correspondences between the fibers.

Consider $\gamma F_p$ for $\gamma \in \mathbb{C} \setminus \{0\}$, it has the same solutions as $F_p$.

Consider generic $\gamma_1, \gamma_2 \in \mathbb{C}$ and a new linear segment homotopy $H'(t)$ between $\gamma_1 F_{p_1}$ and $\gamma_2 F_{p_2}$

$$H'(t) = (1-t)\gamma_1 F_{p_1} + t\gamma_2 F_{p_2}, \quad t \in [0,1] \tag{1}$$

we can see this is equivalent to using the gamma trick. The gamma trick proves that for a generic $\gamma$, the reparametrization $t = \frac{\gamma\tau}{1+(\gamma-1)\tau}$ of $H(t)$ is contained in $B \setminus D$.

$$H''(t) = \frac{1-\tau}{1+(\gamma-1)\tau} F_{p_1} + \frac{\gamma\tau}{1+(\gamma-1)\tau} F_{p_2}.$$

Because $1+(\gamma-1)\tau \neq 0$ we can consider

$$H''(t) = (1-\tau) F_{p_1} + \gamma\tau F_{p_2}, \quad \tau \in [0,1].$$

that generates the same homotopy path. Then we can see that $H'(t)$ can also be created in this way.

We have to note that $H'(t) \in B$ in the case that we have a linear or affine family of systems. In the first case it is obvious by linearity, in the second case if we express it as $F_p = F'_p + C$ for $C$ a constant system, then

$$\begin{aligned} H'(t) &= (1-t)\gamma_1 F_{p_1} + t\gamma_2 F_{p_2} = \\ &= (1-t)\gamma_1 (F'_{p_1} + C) + t\gamma_2 (F'_{p_2} + C) = \\ &= F'_{(1-t)\gamma_1 p_1 + t\gamma_2 p_2} + ((1-t)\gamma_1 + t\gamma_2)\, C. \end{aligned}$$

To see that $H'(t) \in B$ for $t \in (0,1)$, we consider its rescaling

$$H''(t) = \frac{1}{(1-t)\gamma_1 + t\gamma_2} H'(t) = F'_{\frac{(1-t)\gamma_1 p_1 + t\gamma_2 p_2}{(1-t)\gamma_1 + t\gamma_2}} + C = F_{\frac{(1-t)\gamma_1 p_1 + t\gamma_2 p_2}{(1-t)\gamma_1, \qquad t \in [0,1]}}$$

and note that it does not leave $B$ and clearly has the same homotopy paths.

# Monodromy method

Now we have

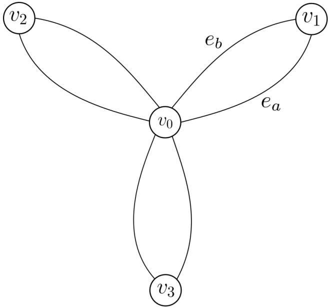
- A way of creating different homotopies between different generic systems.
- The guarantee that for generic systems and parameters $\gamma_1, \gamma_2$ are well behaved, except if they are close to the branch locus.

so we can create different loops for a generic system, we introduce some notation to represent the homotopies.

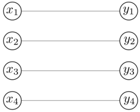
# Homotopy graph representation

We consider a finite undirected graph $G$ with vertex set $V(G)$ and edge set $E(G)$ so that

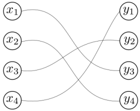
- $v_i \in V(G)$ represents a system $F_{p_i}$ and a set $Q_i \subset \pi^{-1}(F_{p_i})$.
- $e \in E(G)$ represents the homotopy between $F_{p_i}$ and $F_{p_j}$ with values $(\gamma_1, \gamma_2) \in \mathbb{C}^2$ and a set $C_e \subset Q_i \times Q_j$




$$e_a = v_0 \xleftrightarrow{(\gamma_1,\gamma_2)} v_1$$



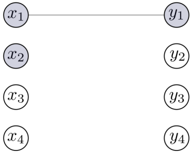

$$e_b = v_0 \xleftrightarrow{(\gamma_3,\gamma_4)} v_1$$



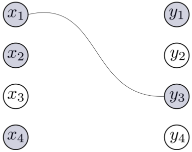
# Homotopy graph: example

We can see the following example to see that tracking some solutions is more useful than tracking others.

$$e_a = v_0 \xleftrightarrow{(\gamma_1,\gamma_2)} v_1$$




$$e_b = v_0 \xleftrightarrow{(\gamma_3,\gamma_4)} v_1$$



# Graph homotopy: operations

We can also define the operations we will perform over the graphs

1. Given an edge $e = v_i \xleftrightarrow{(\gamma_1,\gamma_2)} v_j$, we consider the homotopy $H^{(e)}$

$$H^{(e)}(t) = (1-t)\gamma_1 F_{p_i} + t\gamma_2 F_{p_2}, \quad t \in [0, j]$$

   and track a subset of points of the known solutions $S_i \subset Q_i$ through $H^{(e)}$ to get a subset of the solutions $S_j \subset \pi^{-1}(F_{p_j})$. Then we can extend the known points in $v_j$, by setting $Q_j := Q_j \cup S_j$.

2. Add a new vertex corresponding to $F_p$ for a generic $B \setminus D$.

3. Add a new edge $e = v_i \xleftrightarrow{(\gamma_1,\gamma_2)} v_j$ between two existing vertices $v_i, v_j$ choosing generic $(\gamma_1, \gamma_2) \in \mathbb{C}^2$.

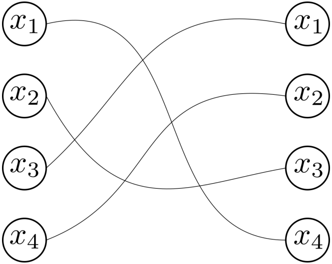
# Monodromy method

We finally have all the ingredients to implement the main monodromy idea:

1. We have a solution $x_0$ of $F_{p_0}(x_0) = 0$, that is, a known solution $x_0 \in Q_0$ of the vertex $v_0$.
2. Add a new vertex $v_1$ by choosing a random $p_1 \in \mathbb{C}^m$.
3. Create two different edges $e_a, e_b$ from $v_0$ to $v_1$, by choosing random gamma values.
4. Track the solution $x_0$ through the lifting of the loop $\tau = [e_a e_b^{-1}] \in \pi_1(B \setminus D, F_{p_0})$ to obtain $\varphi(\tau)(x_0)$, which can be a new solution.

# Example

We can revisit a previous example of a graph and see how the monodromy group acts over a fiber fiber $\pi^{-1}(F_{p_0}) = \{x_1, x_2, x_3, x_4\}$. If we consider the loop $e_a e_b^{-1}$ and track all solutions in $v_0$ we obtain the following permutation $\varphi([e_a e_b^{-1}])$.




In this case the permutation acts transitively over the fiber.

# Algorithms

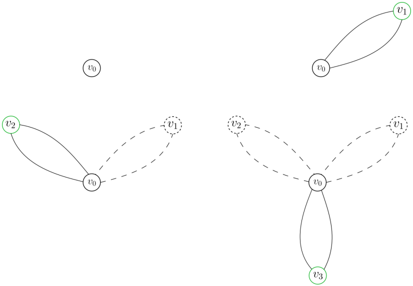
Now that some intuition has been given to the strategy of discovery of new solutions, we establish the two types of algorithms used with this end goal.

1. Static algorithms, in which the graph remains unchanged during the discovery process, using only operation (1).
2. Dynamic algorithms, in which the graph is augmented with vertices or edges during the discovery process, using operations (2) and (3).

# Naive dynamic strategy
## Algorithm

*We start from the seed solution at the vertex $v_0$, that is $Q_0 = \{x_0\}$.*
*Repeat until some stop condition:*

1. *Perfom steps (2) to (4) for all known solutions $Q_0$, to obtain potentially new solutions $S_0$.*
2. *Add them to the known solution set $Q_0 := Q_0 \cup S_0$.*




The average number of steps to find all solutions is of $O(d \log d)$, as it is analogous to the coupon's collector problem, under uniform distribution assumption.

# Static strategy

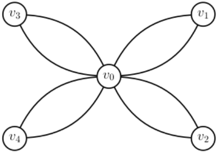
## Algorithm

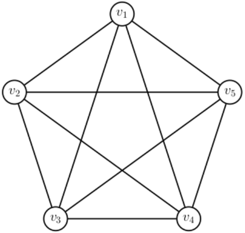
*Given a graph $G$ with subsets $Q_i \subset \pi^{-1}(F_{p_i})$ not all empty and a stoping criterion:*
*While there exists an edge $(j, k)$ from vertex $v_j$ to vertex $v_k$ such that $Q_j$ has untracked solutions:*

1. *Select such an edge $(j, k)$.*
2. *Track all untracked solutions $S \subset Q_j$ using $H^{(e)}$ to obtain $T \subset \pi^{-1}(F_{p_k})$.*
3. *Add the new solutions to the vertex by redefining $Q_k := Q_k \cup T$.*
4. *If the stoping criterion is satisfied, then stop.*

This strategy can be specialized by choosing different graph structures, specifying efficient stopping criterion and choose a strategy to select the edge at each step.

# Graph layouts



# Stopping and edge selection criterions

Stopping criterions

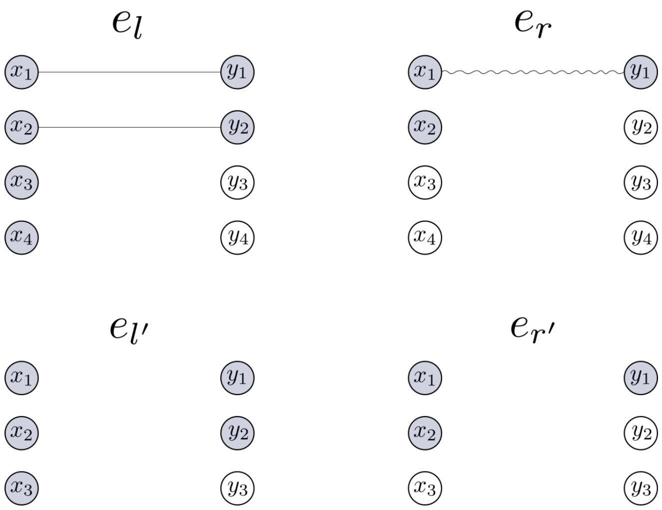
1. When solution count is reached.
2. When no more untracked solutions are left, or no new solutions are discovered in a number of iterations.

Edge selection criterions

1. $$\text{PotentialE}\ (e) = \begin{cases} \frac{d-|Q_j|}{d-|C_e|} & \text{if } |Q_i| - |C_e| > 0 \\ 0 & \text{otherwise} \end{cases}$$

2. $$\text{PotentialLowerBound}\ (e) = max\left((|Q_i| - |C_e|) - (|Q_j| - |C_e|), 0\right) =$$

# Edge selection: example



# Incremental dynamic strategy

We can combine the two previous strategies into the following one:

## Algorithm

*Given a graph $G$ with subsets $Q_i \subset \pi^{-1}(F_{p_i})$ not all empty, an augmentation method and a stopping criterion: Repeat:*

1. *Apply (2) to $G$ (with any of the modifications described above) and store all new solutions obtained.*
2. *If the stopping criterion is satisfied, then stop.*
3. *If not, augment $G$ using the augmentation method.*

# Statistical analysis

To perform statistical analysis we need to make some assumptions of uniformity over the permutations generated by a graph.

Let us consider an induced element in the monodromy group from a cycle in the graph:

$$\begin{array}{ccccc} C(G) & \to \pi_1(B \setminus D) & \to & M(\pi_1(B \setminus D)) \subset S_d \\ c & \mapsto \quad \tau & \mapsto & \varphi(\tau) & , \end{array}$$

Because the considered cycles of $G$ form a group $C(G)$ ($C(G) = Z_1(G)$ is the kernel of the boundary map), then they induce a subgroup $M(G)$ of $M(\pi_1(B \setminus D)) \subset S_d$.

We can see that the minimal number of cycles needed to generate $M(G)$ is $\beta_1(G)$, the rank of $\pi_1(G)$.

As an example if $G =$ flowerGraph(t,2), we have that $\pi_1(G) \cong \mathbb{Z}^t$ and by choosing the cycles given by the $t$ petals we obtain the generators of $\pi_1(G)$, for $G =$ completeGraph(2,j+1), then $\pi_1(G) \cong \mathbb{Z}^{(}j)$, and the cycles $e_1$ to $e_2$, $e_2$ to $e_3$ until $e_j$ to $e_{j+1}$ generate it.

Then if we have a graph with $\beta_1(G) = j$, there exist $j$ cycles that induce $j$ generators of $M(G)$. We make the assumption that a random decorated graph $G$ with $j = \beta_1(G)$ induces the generators $\sigma_1, \ldots, \sigma_j$ of $M(G)$ uniformly and independently from $S_d$.

We want to get the probability of the static algorithm finding all solutions or more generally the dynamic algorithm (3) finding all solutions after $j$ iterations (then the probability for the static algorithm corresponds to $j = 1$).

Now if we suppose that $d = |\pi^{-1}(F_p)|$ is known, and that after $j$ iterations $\beta_1(G) = j$ (that is, each augmentation step adds one more generator of $\pi_1(G)$), we want the probability of the induced subgroup $M(G) = \langle \sigma_1, \dots, \sigma_j \rangle$ being transitive. This is equivalent to obtaining $P(X_d \leq j)$ for

$$X_d = \inf\{i \in \mathbb{N} : \langle \sigma_1, \dots, \sigma_i \rangle \text{ is transitive}\}.$$

If $d > 1$, a generic fiber has at least two solutions, so given one solution, at least one permutation is needed to find more, that means $X_d \geq 1$ in this case, so

$$P(X_d = 0) = 0.$$

The probability to finish after one step however is the probability of the $\sigma_1$ being transitive, which means $\sigma_1$ must be a $d - cycle$, so it is

$$P(X_d = 1) = \frac{K}{|M(\pi_1(B \setminus D))|}.$$

for $K$ the number of $d$-cycles in the monodromy group.

For $j \geq 2$, the following theorem is proven in the paper, which is a generalization of a result for $j = 2$ in [EV16]:

**Theorem**

*For $j \geq 2$, $P(X_d \leq j) = 1 - d^{1-j} + R_j(d)$, where the error term $R_j$ satisfies $|R_j(d)| = O(d^{-j})$.*

# Bibliography I


[SW05] Andrew J Sommese and Charles W Wampler. *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science*. WORLD SCIENTIFIC, Mar. 2005. ISBN: 978-981-256-184-8 978-981-256-772-7. DOI: 10.1142/5763. URL: https://www.worldscientific.com/worldscibooks/10.1142/5763 (visited on 07/03/2023).

[Mun14] James Raymond Munkres. *Topology*. 2. ed., Pearson new internat. ed. Harlow: Pearson, 2014. 503 pp. ISBN: 978-1-292-02362-5.

# Bibliography II


[EV16] Sean Eberhard and Stefan-Christoph Virchow. “The Probability of Generating the Symmetric Group”. In: (2016). Publisher: arXiv Version Number: 2. DOI: 10.48550/ARXIV.1611.02501. URL: https://arxiv.org/abs/1611.02501 (visited on 07/14/2023).

[Bli+18] Nathan Bliss et al. “Monodromy Solver: Sequential and Parallel”. In: (2018). Publisher: arXiv Version Number: 1. DOI: 10.48550/ARXIV.1805.12212. URL: https://arxiv.org/abs/1805.12212 (visited on 07/03/2023).