

# The Work of Mike Shub in Complexity

Felipe Cucker

City University of Hong Kong

Shubfest, Toronto 2012

# Complexity Theory

**Goal:** Determine the amount of resources (most commonly, computer time) necessary to solve problems with a computer.

# Complexity Theory

**Goal:** Determine the amount of resources (most commonly, computer time) necessary to solve problems with a computer.

This broad goal alternates its focus between two extremes:

# Complexity Theory

**Goal:** Determine the amount of resources (most commonly, computer time) necessary to solve problems with a computer.

This broad goal alternates its focus between two extremes:

(G) To develop a general theory of computational cost (which includes formal models of computation, diverse cost notions, complexity classes built upon them, complete problems in these classes, and —the ultimate desideratum— separations between these complexity classes).

# Complexity Theory

**Goal:** Determine the amount of resources (most commonly, computer time) necessary to solve problems with a computer.

This broad goal alternates its focus between two extremes:

(G) To develop a general theory of computational cost (which includes formal models of computation, diverse cost notions, complexity classes built upon them, complete problems in these classes, and —the ultimate desideratum— separations between these complexity classes).

(P) To analyze (in terms of cost) the behavior of specific algorithms (meant to solve specific problems).

Mike has worked on both ends of this spectrum with contributions that can be grouped in 3 main themes:

Mike has worked on both ends of this spectrum with contributions that can be grouped in 3 main themes:

(1) Zeros of Polynomial Systems.

Mike has worked on both ends of this spectrum with contributions that can be grouped in 3 main themes:

- (1) Zeros of Polynomial Systems.
- (2) Structural Complexity for Numerical Problems.

Mike has worked on both ends of this spectrum with contributions that can be grouped in 3 main themes:

- (1) Zeros of Polynomial Systems.
- (2) Structural Complexity for Numerical Problems.
- (3) Conditioning of Numerical Problems.

# Zeros of Polynomial Systems

- **M.S.**, S. Smale. “Computational complexity. On the geometry of polynomials and a theory of cost.” I. *Ann. Sci. École Norm. Sup.*, 1985. II. *SIAM J. Comput.*, 1986.

One polynomial in one variable.

# Zeros of Polynomial Systems

- **M.S.**, S. Smale. “Computational complexity. On the geometry of polynomials and a theory of cost.” I. *Ann. Sci. École Norm. Sup.*, 1985. II. *SIAM J. Comput.*, 1986.

One polynomial in one variable.

- **M.S.**, S. Smale. “Complexity of Bézout’s Theorem.” I, II, III, IV, and V, 1993–1996.

$n$  polynomials in  $n + 1$  homogeneous variables.

**Smale's 17th problem:** Can one find an approximate zero of a system ( $n$  polynomials in  $n + 1$  homogeneous variables) in time polynomial on the average?

**Smale's 17th problem:** Can one find an approximate zero of a system ( $n$  polynomials in  $n + 1$  homogeneous variables) in time polynomial on the average?

**approximate zero:** a point from which Newton's method converges to a zero, immediately, quadratically fast.

**Smale's 17th problem:** Can one find an approximate zero of a system ( $n$  polynomials in  $n + 1$  homogeneous variables) in time polynomial on the average?

**approximate zero:** a point from which Newton's method converges to a zero, immediately, quadratically fast.

**polynomial time:** number of arithmetic operations bounded by  $N^{\mathcal{O}(1)}$  where  $N$  is the size of the input system  $f$ .

**Smale's 17th problem:** Can one find an approximate zero of a system ( $n$  polynomials in  $n + 1$  homogeneous variables) in time polynomial on the average?

**approximate zero:** a point from which Newton's method converges to a zero, immediately, quadratically fast.

**polynomial time:** number of arithmetic operations bounded by  $N^{\mathcal{O}(1)}$  where  $N$  is the size of the input system  $f$ .

**on the average:** w.r.t. a Gaussian distribution on the input  $f$ .

**Smale's 17th problem:** Can one find an approximate zero of a system ( $n$  polynomials in  $n + 1$  homogeneous variables) in time polynomial on the average?

**approximate zero:** a point from which Newton's method converges to a zero, immediately, quadratically fast.

**polynomial time:** number of arithmetic operations bounded by  $N^{\mathcal{O}(1)}$  where  $N$  is the size of the input system  $f$ .

**on the average:** w.r.t. a Gaussian distribution on the input  $f$ .

$$D := \max\{d_1, \dots, d_n\} \qquad N \approx n \binom{D+n}{n}$$

# Adaptive linear homotopy

- ▶ Given an **initial pair**  $(g, \zeta)$  with  $g(\zeta) = 0$  and an input  $f$ :

# Adaptive linear homotopy

- ▶ Given an **initial pair**  $(g, \zeta)$  with  $g(\zeta) = 0$  and an input  $f$ :
- ▶ Consider the line segment  $[g, f]$  connecting  $g$  and  $f$ . It consists of the systems

$$q_t := (1 - t)g + tf \quad \text{for } t \in [0, 1].$$

# Adaptive linear homotopy

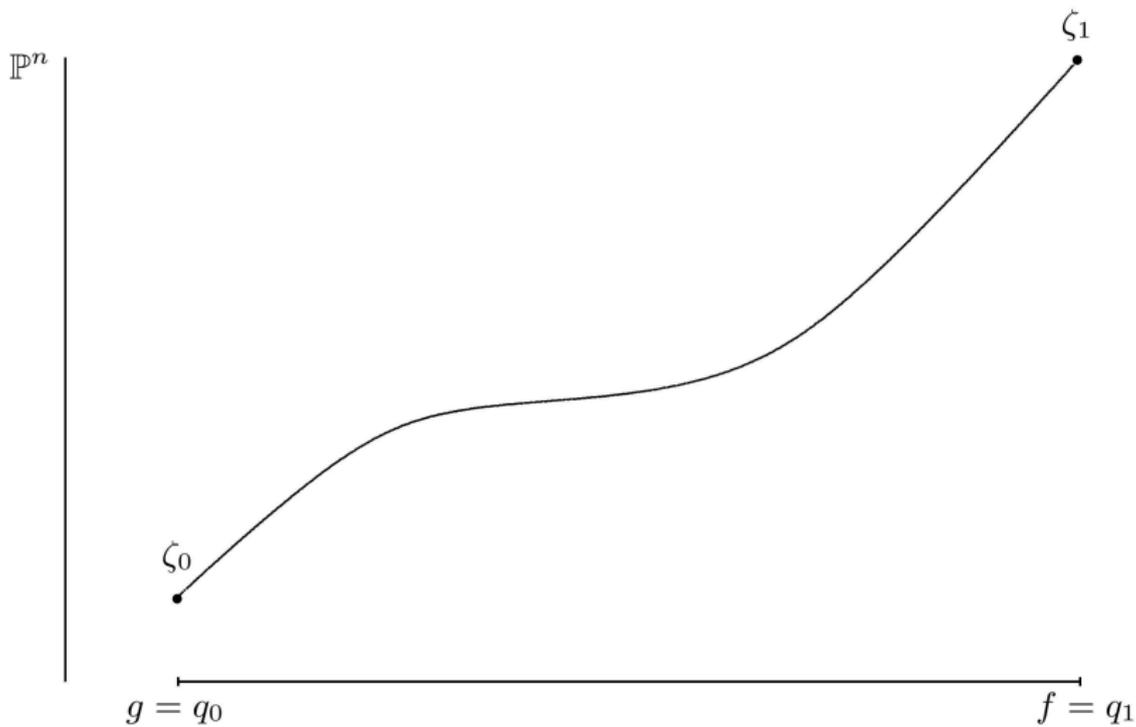
- ▶ Given an **initial pair**  $(g, \zeta)$  with  $g(\zeta) = 0$  and an input  $f$ :
- ▶ Consider the line segment  $[g, f]$  connecting  $g$  and  $f$ . It consists of the systems

$$q_t := (1 - t)g + tf \quad \text{for } t \in [0, 1].$$

- ▶ If no  $q_t$  has a multiple zero, then there exists a unique lifting of this segment to a curve

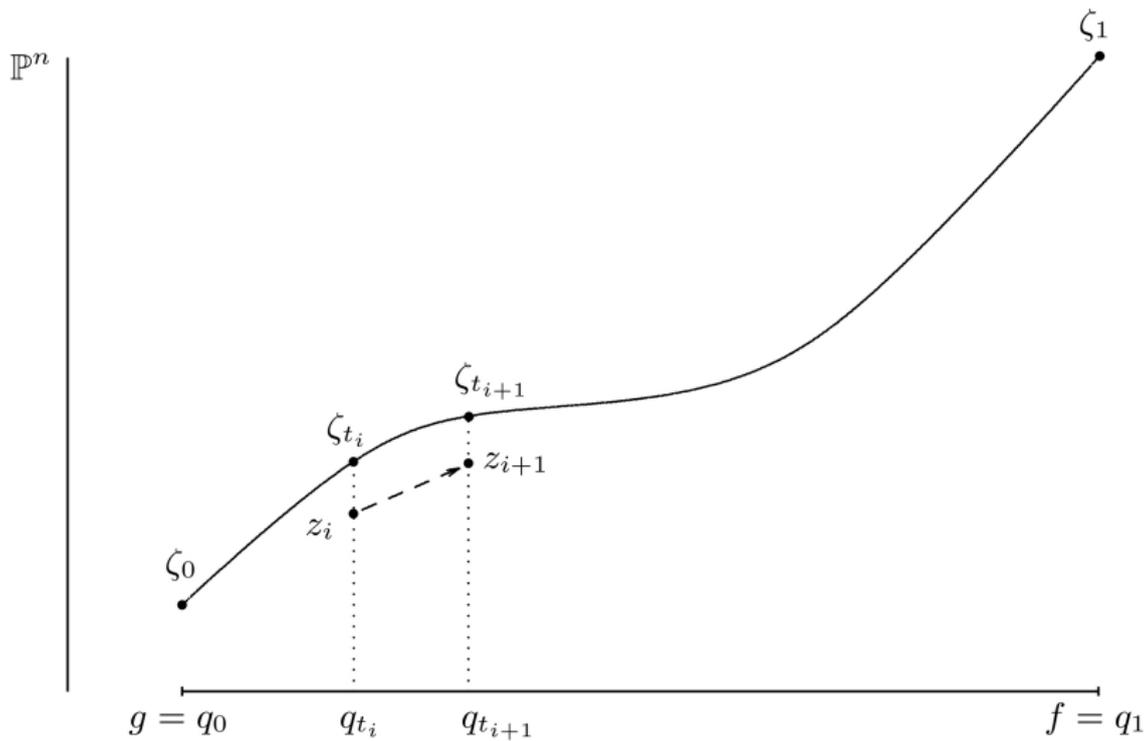
$$t \in [0, 1] \mapsto (q_t, \zeta_t)$$

such that  $\zeta_0 = \zeta$ . **Since  $q_1 = f$ ,  $\zeta_1$  is a zero of  $f$ .**



The idea is to **follow this curve numerically**: partition  $[0, 1]$  into  $t_0 = 0, \dots, t_k = 1$ . Writing  $q_i := q_{t_i}$ , successively compute approximations  $z_i$  of  $\zeta_{t_i}$  by Newton's method starting with  $z_0 := \zeta$ . More specifically, compute

$$z_{i+1} := N_{q_{i+1}}(z_i).$$



The Bézout series set up the main properties of this algorithmic scheme and put in place the theoretical tools used today in its study.

I won't give details of what these tools are or how they are used in recent work. I will instead limit my exposition to the description of the state-of-the-art in the subject.

The Bézout series set up the main properties of this algorithmic scheme and put in place the theoretical tools used today in its study.

I won't give details of what these tools are or how they are used in recent work. I will instead limit my exposition to the description of the state-of-the-art in the subject.

Two issues neglected in my exposition above:

(1) How to choose the initial pair  $(g, \zeta)$ ?

The Bézout series set up the main properties of this algorithmic scheme and put in place the theoretical tools used today in its study.

I won't give details of what these tools are or how they are used in recent work. I will instead limit my exposition to the description of the state-of-the-art in the subject.

Two issues neglected in my exposition above:

- (1) How to choose the initial pair  $(g, \zeta)$ ?
- (2) How large should  $d(q_{i+1}, q_i)$  be?

How large should  $d(q_{i+1}, q_i)$  be?

- ▶ We compute  $t_{i+1}$  **adaptively** from  $t_i$  such that

$$d(q_{i+1}, q_i) = \frac{0.0085}{D^{3/2} \mu_{\text{norm}}^2(q_i, z_i)}.$$

## How large should $d(q_{i+1}, q_i)$ be?

- ▶ We compute  $t_{i+1}$  **adaptively** from  $t_i$  such that

$$d(q_{i+1}, q_i) = \frac{0.0085}{D^{3/2} \mu_{\text{norm}}^2(q_i, z_i)}.$$

- ▶ Denote by  $K(f, g, \zeta)$  the **number  $K$  of iterations** performed to follow the curve.

## How large should $d(q_{i+1}, q_i)$ be?

- ▶ We compute  $t_{i+1}$  **adaptively** from  $t_i$  such that

$$d(q_{i+1}, q_i) = \frac{0.0085}{D^{3/2} \mu_{\text{norm}}^2(q_i, z_i)}.$$

- ▶ Denote by  $K(f, g, \zeta)$  the **number  $K$  of iterations** performed to follow the curve.

“Bézout VI” (M.S., *Found. Comput. Math.* 2009)

For all  $i$ ,  $z_i$  is an approximate zero of  $q_i$ . In particular  $z_K$  is an approximate zero of  $f$ . Moreover,

$$K(f, g, \zeta) \leq 217 D^{3/2} d(f, g) \int_0^1 \mu_{\text{norm}}^2(q_\tau, \zeta_\tau) d\tau.$$

Here  $\tau \in [0, 1]$  is a ratio of angles and not of Euclidean distances.

This result relates to cost in a clear manner. Each Newton step takes  $\mathcal{O}(N)$  arithmetic operations. Therefore, the total number of such operations performed along the homotopy is  $\mathcal{O}(N K(f, g, \zeta))$ .

This result relates to cost in a clear manner. Each Newton step takes  $\mathcal{O}(N)$  arithmetic operations. Therefore, the total number of such operations performed along the homotopy is  $\mathcal{O}(N K(f, g, \zeta))$ .

It has been used in the following:

This result relates to cost in a clear manner. Each Newton step takes  $\mathcal{O}(N)$  arithmetic operations. Therefore, the total number of such operations performed along the homotopy is  $\mathcal{O}(N K(f, g, \zeta))$ .

It has been used in the following:

(1) a randomized algorithm computing approximate zeros in average randomized polynomial time:  $\mathcal{O}(D^{3/2} n N^2)$   
[C. Beltán – L.M. Pardo].

This result relates to cost in a clear manner. Each Newton step takes  $\mathcal{O}(N)$  arithmetic operations. Therefore, the total number of such operations performed along the homotopy is  $\mathcal{O}(N K(f, g, \zeta))$ .

It has been used in the following:

(1) a randomized algorithm computing approximate zeros in average randomized polynomial time:  $\mathcal{O}(D^{3/2} n N^2)$   
[C. Beltán – L.M. Pardo].

(2) a deterministic algorithm working in near-polynomial time (average polynomial time for all but a few pairs  $(n, D)$  and average time  $N^{\mathcal{O}(\log \log N)}$  on those pairs). [P. Bürgisser – F.C.].

## Additional remarks:

- Projective Newton method introduced by Mike.

## Additional remarks:

- Projective Newton method introduced by Mike.
- Several extensions of Newton method to more general systems (overdetermined, underdetermined, multihomogeneous, ...) studied by Mike, mostly in joint work with Jean-Pierre Dedieu.

## Additional remarks:

- Projective Newton method introduced by Mike.
- Several extensions of Newton method to more general systems (overdetermined, underdetermined, multihomogeneous, ...) studied by Mike, mostly in joint work with Jean-Pierre Dedieu.
- Back to the roots? [D. Armentano, **M.S.**]

# Structural Complexity for Numerical Problems

An algorithm solving a problem provides —through its analysis— an upper bound on the resources necessary to solve this problem.

# Structural Complexity for Numerical Problems

An algorithm solving a problem provides —through its analysis— an upper bound on the resources necessary to solve this problem.

To obtain lower bounds one needs instead to consider **all** algorithms solving the problem. Thus, the study of lower bounds demands a formal notion of algorithm at hand.

# Structural Complexity for Numerical Problems

An algorithm solving a problem provides —through its analysis— an upper bound on the resources necessary to solve this problem.

To obtain lower bounds one needs instead to consider **all** algorithms solving the problem. Thus, the study of lower bounds demands a formal notion of algorithm at hand.

Classical complexity theory (as studied in Theoretical Computer Science) has the **Turing machine** for this notion. This is very useful for discrete computations but not so for numerical computations. A “continuous” complexity theory is needed in this context.

# Structural Complexity for Numerical Problems

An algorithm solving a problem provides —through its analysis— an upper bound on the resources necessary to solve this problem.

To obtain lower bounds one needs instead to consider **all** algorithms solving the problem. Thus, the study of lower bounds demands a formal notion of algorithm at hand.

Classical complexity theory (as studied in Theoretical Computer Science) has the **Turing machine** for this notion. This is very useful for discrete computations but not so for numerical computations. A “continuous” complexity theory is needed in this context.

- L. Blum, **M.S.**, S. Smale. “On a theory of computation over the real numbers: NP-completeness, recursive functions and universal machines”, *Bull. AMS*, 1989.

- Introduced the **BSS-machine**.

- Introduced the **BSS-machine**.
- Natural notions of **deterministic cost** and **nondeterministic cost**.

Cost is, essentially, number of arithmetic operations and comparisons performed.

Nondeterminism is a theoretical mode of computation that, instead of “finding” or “computing” the solution to a problem, simply “verifies” that a candidate solution is a solution indeed.

- Introduced the **BSS-machine**.
- Natural notions of **deterministic cost** and **nondeterministic cost**.

Cost is, essentially, number of arithmetic operations and comparisons performed.

Nondeterminism is a theoretical mode of computation that, instead of “finding” or “computing” the solution to a problem, simply “verifies” that a candidate solution is a solution indeed.

- Classes  $P_{\mathbb{R}}$  and  $NP_{\mathbb{R}}$  (and  $P_{\mathbb{C}}$  and  $NP_{\mathbb{C}}$ ).

- Introduced the **BSS-machine**.
- Natural notions of **deterministic cost** and **nondeterministic cost**.

Cost is, essentially, number of arithmetic operations and comparisons performed.

Nondeterminism is a theoretical mode of computation that, instead of “finding” or “computing” the solution to a problem, simply “verifies” that a candidate solution is a solution indeed.

- Classes  $P_{\mathbb{R}}$  and  $NP_{\mathbb{R}}$  (and  $P_{\mathbb{C}}$  and  $NP_{\mathbb{C}}$ ).

A problem in  $NP_{\mathbb{R}}$ .

**4FEAS** Given a polynomial  $f$  in  $\mathbb{R}[X_1, \dots, X_n]$  of degree 4, does there exist  $\xi \in \mathbb{R}^n$  such that  $f(\xi) = 0$ ?

- Introduced the **BSS-machine**.
- Natural notions of **deterministic cost** and **nondeterministic cost**.

Cost is, essentially, number of arithmetic operations and comparisons performed.

Nondeterminism is a theoretical mode of computation that, instead of “finding” or “computing” the solution to a problem, simply “verifies” that a candidate solution is a solution indeed.

- Classes  $P_{\mathbb{R}}$  and  $NP_{\mathbb{R}}$  (and  $P_{\mathbb{C}}$  and  $NP_{\mathbb{C}}$ ).

A problem in  $NP_{\mathbb{R}}$ .

**4FEAS** Given a polynomial  $f$  in  $\mathbb{R}[X_1, \dots, X_n]$  of degree 4, does there exist  $\xi \in \mathbb{R}^n$  such that  $f(\xi) = 0$ ?

A problem in  $NP_{\mathbb{C}}$ .

**QUAD** Given  $f_1, \dots, f_m$  in  $\mathbb{C}[X_1, \dots, X_n]$  of degree 2, is there a  $\xi \in \mathbb{C}^n$  such that  $f_1(\xi) = \dots = f_m(\xi) = 0$ ?

- Existence of natural  $\text{NP}_{\mathbb{R}}$ -complete problems.

- Existence of natural  $\text{NP}_{\mathbb{R}}$ -complete problems.

A complete problem  $\mathcal{P}$  in  $\text{NP}_{\mathbb{R}}$  is one such that, if  $\mathcal{P} \in \text{P}_{\mathbb{R}}$  then  $\text{P}_{\mathbb{R}} = \text{NP}_{\mathbb{R}}$ .

- Existence of natural  $\text{NP}_{\mathbb{R}}$ -complete problems.

A complete problem  $\mathcal{P}$  in  $\text{NP}_{\mathbb{R}}$  is one such that, if  $\mathcal{P} \in \text{P}_{\mathbb{R}}$  then  $\text{P}_{\mathbb{R}} = \text{NP}_{\mathbb{R}}$ .

**Explanation:** All problems in  $\text{NP}_{\mathbb{R}}$  “reduce” to  $\mathcal{P}$  (negligible overhead cost).

- Existence of natural  $\text{NP}_{\mathbb{R}}$ -complete problems.

A complete problem  $\mathcal{P}$  in  $\text{NP}_{\mathbb{R}}$  is one such that, if  $\mathcal{P} \in \text{P}_{\mathbb{R}}$  then  $\text{P}_{\mathbb{R}} = \text{NP}_{\mathbb{R}}$ .

**Explanation:** All problems in  $\text{NP}_{\mathbb{R}}$  “reduce” to  $\mathcal{P}$  (negligible overhead cost).

4FEAS is  $\text{NP}_{\mathbb{R}}$ -complete

QUAD is  $\text{NP}_{\mathbb{C}}$ -complete

- Existence of natural  $\text{NP}_{\mathbb{R}}$ -complete problems.

A complete problem  $\mathcal{P}$  in  $\text{NP}_{\mathbb{R}}$  is one such that, if  $\mathcal{P} \in \text{P}_{\mathbb{R}}$  then  $\text{P}_{\mathbb{R}} = \text{NP}_{\mathbb{R}}$ .

**Explanation:** All problems in  $\text{NP}_{\mathbb{R}}$  “reduce” to  $\mathcal{P}$  (negligible overhead cost).

4FEAS is  $\text{NP}_{\mathbb{R}}$ -complete

QUAD is  $\text{NP}_{\mathbb{C}}$ -complete

These results put focus on the problems 4FEAS and QUAD.

- Existence of natural  $\text{NP}_{\mathbb{R}}$ -complete problems.

A complete problem  $\mathcal{P}$  in  $\text{NP}_{\mathbb{R}}$  is one such that, if  $\mathcal{P} \in \text{P}_{\mathbb{R}}$  then  $\text{P}_{\mathbb{R}} = \text{NP}_{\mathbb{R}}$ .

**Explanation:** All problems in  $\text{NP}_{\mathbb{R}}$  “reduce” to  $\mathcal{P}$  (negligible overhead cost).

4FEAS is  $\text{NP}_{\mathbb{R}}$ -complete

QUAD is  $\text{NP}_{\mathbb{C}}$ -complete

These results put focus on the problems 4FEAS and QUAD.

**Relations of QUAD and Smale's 17th problem:**

decision vs function problem

- Existence of natural  $\text{NP}_{\mathbb{R}}$ -complete problems.

A complete problem  $\mathcal{P}$  in  $\text{NP}_{\mathbb{R}}$  is one such that, if  $\mathcal{P} \in \text{P}_{\mathbb{R}}$  then  $\text{P}_{\mathbb{R}} = \text{NP}_{\mathbb{R}}$ .

**Explanation:** All problems in  $\text{NP}_{\mathbb{R}}$  “reduce” to  $\mathcal{P}$  (negligible overhead cost).

4FEAS is  $\text{NP}_{\mathbb{R}}$ -complete

QUAD is  $\text{NP}_{\mathbb{C}}$ -complete

These results put focus on the problems 4FEAS and QUAD.

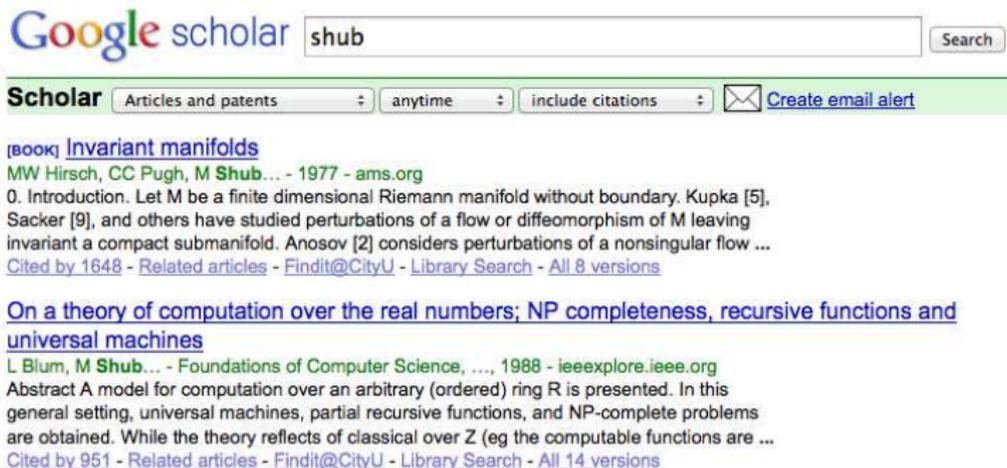
**Relations of QUAD and Smale's 17th problem:**

decision vs function problem

average-case vs worst-case

The BSS paper has had a tremendous impact in the work of a group of people who made its complexity theory the center of their research.

The BSS paper has had a tremendous impact in the work of a group of people who made its complexity theory the center of their research.



The screenshot shows a Google Scholar search interface. At the top, the Google Scholar logo is on the left, and a search box containing the text 'shub' is on the right, with a 'Search' button. Below the search box is a navigation bar with the word 'Scholar' on the left and several filters: 'Articles and patents', 'anytime', and 'include citations', each with a dropdown arrow. To the right of these filters is an envelope icon and the text 'Create email alert'. The search results are listed below. The first result is for the book 'Invariant manifolds' by MW Hirsch, CC Pugh, and M Shub, published in 1977 by AMS. The abstract begins with '0. Introduction. Let  $M$  be a finite dimensional Riemann manifold without boundary. Kupka [5], Sacker [9], and others have studied perturbations of a flow or diffeomorphism of  $M$  leaving invariant a compact submanifold. Anosov [2] considers perturbations of a nonsingular flow ...'. Below the abstract are links for 'Cited by 1648', 'Related articles', 'Findit@CityU', 'Library Search', and 'All 8 versions'. The second result is for the paper 'On a theory of computation over the real numbers; NP completeness, recursive functions and universal machines' by L Blum and M Shub, published in 1988 in the 'Foundations of Computer Science'. The abstract starts with 'Abstract A model for computation over an arbitrary (ordered) ring  $R$  is presented. In this general setting, universal machines, partial recursive functions, and NP-complete problems are obtained. While the theory reflects of classical over  $Z$  (eg the computable functions are ...'. Below this abstract are links for 'Cited by 951', 'Related articles', 'Findit@CityU', 'Library Search', and 'All 14 versions'. At the bottom right of the page, there are navigation icons for back, forward, and search.

Google scholar shub Search

Scholar Articles and patents anytime include citations Create email alert

[book](#) [Invariant manifolds](#)  
MW Hirsch, CC Pugh, M Shub... - 1977 - [ams.org](#)  
0. Introduction. Let  $M$  be a finite dimensional Riemann manifold without boundary. Kupka [5], Sacker [9], and others have studied perturbations of a flow or diffeomorphism of  $M$  leaving invariant a compact submanifold. Anosov [2] considers perturbations of a nonsingular flow ...  
[Cited by 1648](#) - [Related articles](#) - [Findit@CityU](#) - [Library Search](#) - [All 8 versions](#)

[On a theory of computation over the real numbers; NP completeness, recursive functions and universal machines](#)  
L Blum, M Shub... - [Foundations of Computer Science, ..., 1988](#) - [ieeexplore.ieee.org](#)  
Abstract A model for computation over an arbitrary (ordered) ring  $R$  is presented. In this general setting, universal machines, partial recursive functions, and NP-complete problems are obtained. While the theory reflects of classical over  $Z$  (eg the computable functions are ...  
[Cited by 951](#) - [Related articles](#) - [Findit@CityU](#) - [Library Search](#) - [All 14 versions](#)

- F.C., **M.S.** “Generalized knapsack problems and fixed degree separations”, *Theoret. Comput. Sci.*, 1996.

- F.C., **M.S.** “Generalized knapsack problems and fixed degree separations”, *Theoret. Comput. Sci.*, 1996.

For every  $d \geq 1$

$$\text{DTIME}(\mathcal{O}(n^d)) \neq \text{NTIME}(\mathcal{O}(n^d)).$$

# Conditioning of Numerical Problems

$$\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^m \quad a \in \mathbb{R}^n$$

The **condition number of  $a$**  is the worst-case magnification in  $\varphi(a)$  of small relative errors in  $a$ :

$$\text{cond}^\varphi(a) := \lim_{\delta \rightarrow 0} \sup_{\text{RelError}(a) \leq \delta} \frac{\text{RelError}(\varphi(a))}{\text{RelError}(a)}.$$

# Conditioning of Numerical Problems

$$\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^m \quad a \in \mathbb{R}^n$$

The **condition number of  $a$**  is the worst-case magnification in  $\varphi(a)$  of small relative errors in  $a$ :

$$\text{cond}^\varphi(a) := \lim_{\delta \rightarrow 0} \sup_{\text{RelError}(a) \leq \delta} \frac{\text{RelError}(\varphi(a))}{\text{RelError}(a)}.$$

- ▶ The condition number plays a key role in finite-precision analyses of algorithms.

# Conditioning of Numerical Problems

$$\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^m \quad a \in \mathbb{R}^n$$

The **condition number of  $a$**  is the worst-case magnification in  $\varphi(a)$  of small relative errors in  $a$ :

$$\text{cond}^\varphi(a) := \lim_{\delta \rightarrow 0} \sup_{\text{RelError}(a) \leq \delta} \frac{\text{RelError}(\varphi(a))}{\text{RelError}(a)}.$$

- ▶ The condition number plays a key role in finite-precision analyses of algorithms.
- ▶ For many problems  $\varphi$  the quantity  $\text{cond}^\varphi(a)$  can be characterized (or approximated) in a more friendly manner.

# Conditioning of Numerical Problems

$$\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^m \quad a \in \mathbb{R}^n$$

The **condition number of  $a$**  is the worst-case magnification in  $\varphi(a)$  of small relative errors in  $a$ :

$$\text{cond}^\varphi(a) := \lim_{\delta \rightarrow 0} \sup_{\text{RelError}(a) \leq \delta} \frac{\text{RelError}(\varphi(a))}{\text{RelError}(a)}.$$

- ▶ The condition number plays a key role in finite-precision analyses of algorithms.
- ▶ For many problems  $\varphi$  the quantity  $\text{cond}^\varphi(a)$  can be characterized (or approximated) in a more friendly manner.
- ▶ These characterizations have allowed, in many cases, to obtain estimates of the expectation  $\mathbb{E}(\text{cond}^\varphi)$  with respect to a measure on  $\mathbb{R}^n$ .

# Conditioning of Numerical Problems

$$\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^m \quad a \in \mathbb{R}^n$$

The **condition number of  $a$**  is the worst-case magnification in  $\varphi(a)$  of small relative errors in  $a$ :

$$\text{cond}^\varphi(a) := \lim_{\delta \rightarrow 0} \sup_{\text{RelError}(a) \leq \delta} \frac{\text{RelError}(\varphi(a))}{\text{RelError}(a)}.$$

- ▶ The condition number plays a key role in finite-precision analyses of algorithms.
- ▶ For many problems  $\varphi$  the quantity  $\text{cond}^\varphi(a)$  can be characterized (or approximated) in a more friendly manner.
- ▶ These characterizations have allowed, in many cases, to obtain estimates of the expectation  $\mathbb{E}(\text{cond}^\varphi)$  with respect to a measure on  $\mathbb{R}^n$ .
- ▶ Condition numbers have also been used in estimates for the speed of convergence of iterative algorithms (complexity!).

Mike's first work in conditioning studies a notion of condition number obtained by replacing "worst-case perturbation" by "average perturbation." This is relevant for finite-precision analyses.

- N. Weiss, G. Wasikowski, H. Wozniakowski, **M.S.** "Average condition number for solving linear equations." *Linear Algebra Appl.*, 1986.

Mike's first work in conditioning studies a notion of condition number obtained by replacing "worst-case perturbation" by "average perturbation." This is relevant for finite-precision analyses.

- N. Weiss, G. Wasikowski, H. Wozniakowski, **M.S.** "Average condition number for solving linear equations." *Linear Algebra Appl.*, 1986.

Then attention turned to the relationship between condition and complexity. This relationship pervades the Bézout series.

For each of the zeros  $\zeta_1, \dots, \zeta_{\mathcal{D}}$  of a system  $f$  we have that  $\mu_{\text{norm}}(f, \zeta_i)$  is a condition number in the sense above!

For each of the zeros  $\zeta_1, \dots, \zeta_{\mathcal{D}}$  of a system  $f$  we have that  $\mu_{\text{norm}}(f, \zeta_i)$  is a condition number in the sense above!

The problem is, the map **system**  $\rightarrow$  **zero** is multivalued.

What should we define as the condition of input  $f$ ?

For each of the zeros  $\zeta_1, \dots, \zeta_{\mathcal{D}}$  of a system  $f$  we have that  $\mu_{\text{norm}}(f, \zeta_i)$  is a condition number in the sense above!

The problem is, the map **system**  $\rightarrow$  **zero** is multivalued.  
What should we define as the condition of input  $f$ ?

In the Bézout series the answer to this problem is

$$\mu_{\max}(f) := \max_{i \leq \mathcal{D}} \mu_{\text{norm}}(f, \zeta_i).$$

For each of the zeros  $\zeta_1, \dots, \zeta_{\mathcal{D}}$  of a system  $f$  we have that  $\mu_{\text{norm}}(f, \zeta_i)$  is a condition number in the sense above!

The problem is, the map **system**  $\rightarrow$  **zero** is multivalued.  
What should we define as the condition of input  $f$ ?

In the Bézout series the answer to this problem is

$$\mu_{\text{max}}(f) := \max_{i \leq \mathcal{D}} \mu_{\text{norm}}(f, \zeta_i).$$

The main result in Bézout VI allows one to use instead

$$\mu_{\text{av}}(f) := \sqrt{\frac{1}{\mathcal{D}} \sum_{i \leq \mathcal{D}} \mu_{\text{norm}}^2(f, \zeta_i)}.$$

This fact is, as we already pointed out, at the core of the recent advances towards a final solution to Smale's 17th problem.

## A Unifying Theory?

c) For a decision problem  $\mathbb{R}^{\infty}$ ,  $\mathbb{R}_{yes}^{\infty}$   
we say a problem instance  $x \in \mathbb{R}^k$   
is  $\epsilon$ -fused if  $\forall \delta > 0 \exists y_1, y_2 \in \mathbb{R}^k$   
with  $\|x - y_i\| \leq \delta \|x\| + \delta \quad i=1,2$   
and  $y_1 \in \mathbb{R}_{yes}^k$  while  $y_2 \in \mathbb{R}_{no}^k$ . We  
denote the set of  $\epsilon$ -fused problems  
by  $I_{\epsilon}$  and  $I_{\epsilon,k}$  for inputs of  
size  $k$  if confusion is likely.