Complexity and Accuracy in Numeric Computations
(Fields, Tuesdays 10-12 pm, Fall'09)

Instructors: Lenore Blum and Felipe Cucker

Will approach computation in 2 phases

1. **Algebraic phase: Computing over a Ring or Field**
2. **Numerical analysis phase: Introduce condition, round-off error, etc., into analysis**

Algebraic

1) Computing over a ring or field (especially over the reals or complex numbers): a machine model.
2) Measuring Complexity and the classes P and NP over a ring or field
3) NP-Complete Problems (universal and specific)
4) Algebraic setting for the problem "P=NP?"
5) Lower bounds and other complexity classes

Numerical Analysis

6) Measuring accuracy
7) Error analysis and Condition numbers
8) Poor conditioning and Ill-posedness
9) Condition and the distance to ill-posedness
10) Condition of random data

Some References:

L. Blum, M. Shub, and S. Smale, "On a Theory of Computation and Complexity over the Real Numbers: NP Completeness, Recursive Functions and Universal machines," Bull. Am. Math. Soc., 21, 1 (1989).
L. Blum, F. Cucker, M. Shub, and S. Smale, "Complexity and Real Computation," Springer-Verlag, 1998.

Expository:

F. Cucker, Real Computations with Fake Numbers. *Journal of Complexity* 18, pp. 104-134, March 2002.
L. Blum, Computing over the Reals, Where Turing Meets Newton, *Notices* of the AMS, pp. 1024- 1034 October, 2004. http://www.ams.org/notices/200409/fea-blum.pdf

Many other papers,authors, …

Computing over a ring or field (especially over the reals or complex numbers): a machine model

Algebraic approach:
Let R be a commutative ring or field with unit. Assume without zero divisors. May be ordered (eg $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$) or unordered (eg $\mathbb{Z}_2$ or $\mathbb{C}$).

First Main Goal. Explain and prove**:**

Theorem (lb, Shub, Smale, BAMS '89): For any field (R,=)
HN_R is NP-complete over R.

So, **P = NP $\Leftrightarrow$ $HN_R \in$ P over R.**

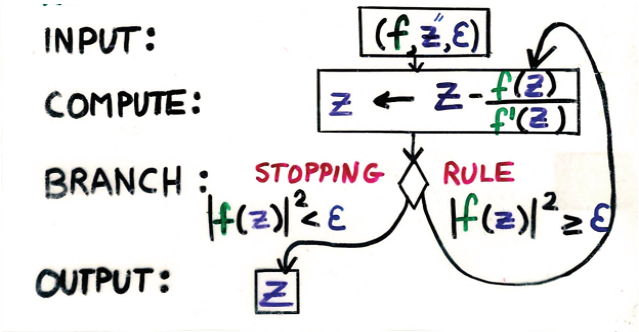
HN_R (Hilbert Nullstellensatz over R) is the problem of deciding, given any finite polynomial system over R, whether or not it is solvable over R.

If R = $\mathbb{Z}_2$, then this is the classical NP-completeness result.

Will define the model of computation over R. Main tool will be the **computing endomorphism**. Most salient concepts are defined via the computing endomorphism. Analyzing it will show how these concepts are naturally described algebraically. The NP-completeness of HN_R then follows.

An early Motivation: The Newton "machine"

Input, poly f, starting point z, threshold ε



$N_f(z)=z-f(z)/f'(z)=(zf'(z)-f(z))/f'(z)$ is a rational function.

Finite dimensional machines M over R

3 ***spaces***: **Input space** $I_M = R^n$, **State space** $S_M = R^m$, **Output space**, $O_M = R^l$

In the following, subscripts M and R will be understood.

M is a finite directed graph with 4 types of ***nodes N*** and *associated maps:*

- **Input node**: linear map I: $I \to S$; unique next node β_1
- **Computation nodes**, η: g_η: $S \to S$, poly map (rat map if R is a field); unique next node β_η

(A polynomial map g: $R^m \to R^m$ is given by m polynomials in m variables, $g_1, \ldots, g_m$, such that $g(x_1, \ldots, x_m) = (g_1(x_1, \ldots, x_m), \ldots, g_m(x_1, \ldots, x_m))$. In case of rational maps, the g_i's are rational functions, p_i/q_i where the p_i's,q_i's are polynomials in m variables.[1])

- **Branch nodes**, η: h_η: $S \to R$; β^+_η is the unique next node associated with $h_\eta(y) \geq 0$ and β^-_η the unique next node associated with $h_\eta(y) < 0$
  In the unordered case, β^+_η is node associated with $h_\eta(y) = 0$ and β^-_η with $h_\eta(y) \neq 0$
- **Output node** η: linear map O_η: $S \to O$

Convenient to assume β_η and g_η are always defined.
So for the output node, let $\beta_\eta = \eta$. So now we can define $\beta_\eta(y)$ for $y \in S$.
And for input, branch and output nodes, $g_\eta(y) = y$.

The **degree of M**, $\mathbf{D_M}$ is the maximum degree of the g_η's.(deg p/q = max (deg p, deg q)).
The **dimension of M** is **m**. **C** = set of constants from R.

Will assume, ***Normal form***:

1. $N = \{1, \ldots, N\}$,with 1, unique input node; N, unique output node.
2. All branch nodes are *standard*: $h_\eta(y) = y_1$, $\eta \in B$, $y \in S$.
3. Can assume never divides by 0 at computation node (by checking before hand).

We will soon extend to uniform machines to deal with inputs of arbitrary finite dimension

Alternate definition in terms of algebraic circuits (non-uniform) with constants and Turing machines (uniform).

---

[1] We assume a standard representation of polynomials as a sum of monomials $a_\alpha x^\alpha$ where $a_\alpha \in R$, $x^\alpha = x_1^{\alpha_1} \ldots x_m^{\alpha_m}$, $\sum_{i=1}^{m} \alpha_i \leq d$. Usually we assume the dense representation, ie every monomial is specified.

Definitions: Given machine M over R:

- **A MAIN TOOL: The Computing Endomorphism**: **$H = (\beta, g): NxS \to NxS$**
  (node, state) $\to$ (next node, next state)

Here $\beta: NxS \to N$ where $\beta(\eta, y) = \beta_\eta(y)$ and $g: NxS \to S$ where $g(\eta, y) = g_\eta(y)$

(NB. $g_\eta(y)$ may not be defined if we allow division, but will not run into this if we start at input node.)

All key concepts are defined using the computing endomorphism. Analyzing the computing endomorphism will enable us to give natural and transparent proofs eg of universal NP-complete problems.

Given $x \in I$. Let $z^0 = (\eta^0, x^0)$ where $\eta^0 = 1$ and $x^0 = I(x)$.

- The **computation** with input x is the **orbit** of z^0 under iterates of H.
  $z^0 = (1, x^0), \ldots, z^{k+1} = H(z^k) = H(\eta^k, x^k) = (\eta^{k+1}, x^{k+1}), \ldots$
- The computation **halts** in time T (or less) on input x if $\eta^T = N$.
- The least such T is the **halting time, $T_M(x)$** (let $_{TM}(x) = \infty$, if no such T)

We can already see how using the computing endomorphism, many assertions can be made succinctly. For example: Let **$F_M(x, y, T)$** be the assertion:
"Machine M with input x halts with output y in time $\leq$ T." This can be expressed:

$$\exists\, z^0, z^1, \ldots, z^T \in (NxS)^{T+1}\ \exists\, w \in S$$

$$[(z^0 = (1, I(x))) \,\&\, (z^T = (N, w)) \,\&\, (O(w) = y) \,\&_{k=1}^{T} (z^k = H(z^{k-1}))]$$

This essentially asserts that a certain "algebraic" system has a solution, as we shall see.

- The **halting set** of M, **Ω_M** , is the set of all inputs on which M halts.

  Over $\mathbb{Z}$, halting sets are called **recursively enumerable** since they are identical to "output sets." This is true also over real closed and algebraically closed fields (for deeper reasons) but not in general. (It is clear that hating sets are output sets. Conversely, given M construct M' as follows: For each input y and each time T, use elimination of quantifiers to check if $\exists x\, F_M(x, y, T)$. Output 1 if yes, and if not, increment T by 1 and check again. But we are getting ahead of ourselves.)

  Over $\mathbb{Z}$ a number of concepts become identical. Not true in general. Looking generally sometimes helps identify the most natural definition.

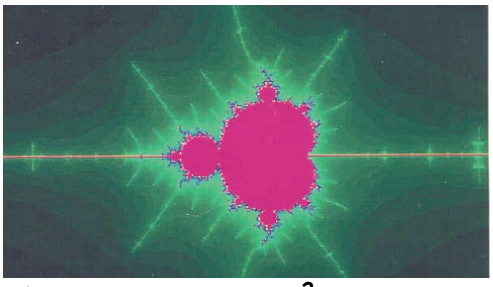
- The **input-output map** is given by $\Phi_M(x) = O(x^T)$ where $T = T_M(x)$. ($\Phi_M(x)$is undefined if $T_M(x) = \infty$)
- A (partial) function over R is (partial) **computable** over R if it is in the input-output map of a machine over R.

- A set $S \subset R^n$ is **decidable over R** if its characteristic function is computable over R.
- A set $S \subset R^n$ is **semi-decidable over R** if there is a computable partial function which has value 1 only on elements of S.

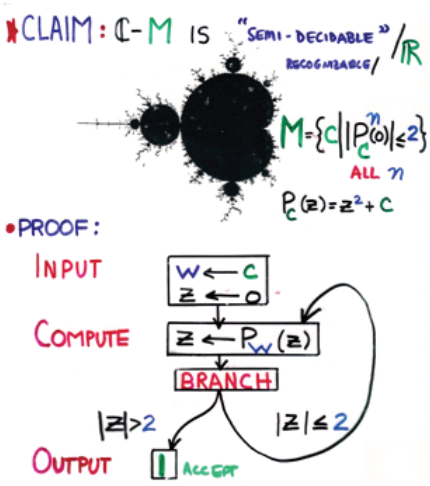
Halting sets are exactly the semi-decidable sets.

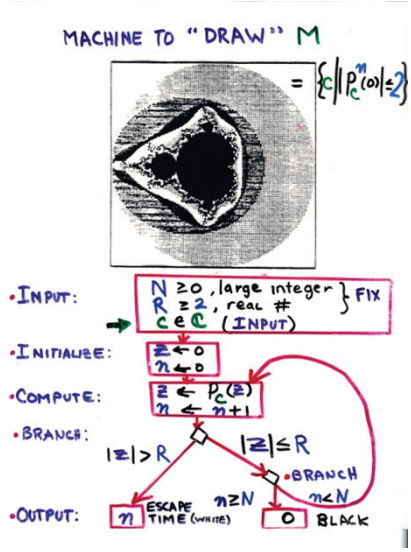
Examples of semi-decidable sets: The complement of the Mandelbrot set, Newton "good" points, the complement of Cantor Middle Third.

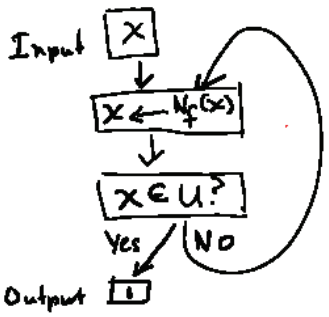
The Mandelbrot set



$M=\{c \mid p_c^n(0) \not\to \infty\}$, $p_c(z) = z^2+c$, $c \in \mathbb{C}$, $M \subset \mathbb{C}=\mathbb{R}^2$







Let $f(x) \in \mathbb{R}[x]$ or $\mathbb{C}[x]$. The zeros of f are the fixed points of N_f, and the fixed point of N_f are attracting. Therefore, for each zero ζ of f, there is a ball U_ξ, contracting under N_f and given by polynomial inequalities. Let $\zeta_1,\ldots,\zeta_n$ be the zeros of f with corresponding contracting neighborhoods U_{ζ_i} and let $U = \bigcup U_{\zeta_i}$.

$\Omega_M = \bigcup_{k=0}^{\infty} N_f^{-k}(U)$ = good starting points = basin of attraction of the fixed points of N_f.

Proposition. A set is decidable ⇔ both it and its complement are semi-decidable.

Proof. ⇒) clear
⇐) Suppose S= Ω_M and S'= $\Omega_{M'}$.

We construct a decision machine M* for S: With input x in R^n,
M* parallel processes M and M' on input x. One and only one machine will halt.
If M halts, then M* outputs 1. If M' halts, M* outputs 0.

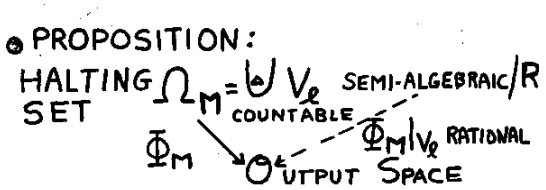
- Let $I_{M^*} = I_M = I_{M'}$; $S_{M^*} = S_M \times S_{M'}$; $O_{M^*} = R$.
- For $x \in I_{M^*}$, let $I_{M^*}(x) = (I_M(x), (I_{M'}(x))$
- For $y^* \in S_{M^*}$, let $O_{M^*}(y^*)$ be the first coordinate of y^*.
- $N_{M^*} \subset \{0,1\} \times N_M \times N_{M'} \cup \{1^*, N^*\}$ (the latter are the distinguished input and output nodes)
- Let $\beta_{1^*} = (1,1,1)$

Suppose $\eta^* = (s, \eta, \eta')$ and $y^* = (y, y')$ and suppose s=1. Then

a) If η is an input or computation node of M, then η* is a computation node of M*. Let $g_{\eta^*}(y^*) = (g_\eta(y), y')$ and $\beta_{\eta^*} = (0, \beta_\eta, \eta')$.
b) If η is a branch node, then η* is a branch node with $\beta^+_{\eta^*} = (0, \beta^+_\eta, \eta')$ and $\beta^-_{\eta^*} = (0, \beta^-_\eta, \eta')$.
c) If η is an output node of M, then η* is a computation node of M*. Let $g_{\eta^*}(y^*) = (1,\ldots,1)$ and $\beta_{\eta^*} = N^*$.

Modify appropriately for s = 0.

So, want to know what semi-decidable sets, ie halting sets, look like.
Fix M over R.



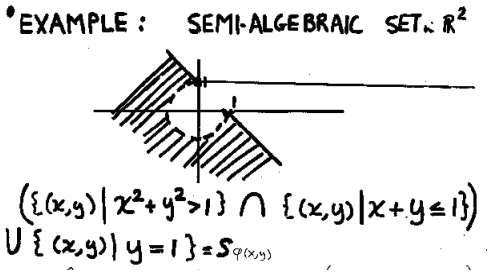
Computable maps are piecewise polynomial (or rational).

Let $T_M(x) = T$. The finite sequence, $z^0, \ldots, z^T$ is the **halting computation** for x and $\gamma_x = \eta^0, \ldots, \eta^T$ is the **halting computation path** traversed by x.

Let $\Gamma_M = \{\gamma_x \mid x \in \Omega_M\}$ be the set of halting computation paths.
For $\gamma \in \Gamma_M$, let $V\gamma = \{x \in \Omega_M \mid \gamma_x = \gamma\}$. So, $\Omega_M = \bigcup_{\gamma \in \Gamma_M} V_\gamma$, a disjoint union.

Proposition. V_γ is a basic semi-algebraic (quasi-algebraic) set.

- A **basic semi-algebraic** (**quasi-algebraic**) set in R^n is given by a finite system of polynomial equalities and inequalities (equations and inequations) over R.
- A **semi-algebraic** (**quasi-algebraic**) set is a given by a Boolean combination of basic semi-algebraic (quasi-algebraic).



Proof.
Let γ be a halting computation path. At each *step* η^k in γ, **M *evaluates* a polynomial (rational) map,** $G_{\gamma(k)} : V_\gamma \longrightarrow R^m$ where $G_{\gamma(k)} = g_{\eta^k} \ldots g_{\eta^0} I$ (Clearly, $\Phi_M | V_\gamma = O \cdot G_{\gamma(T)}$).

For each branch node η^k in γ, **M *evaluates* a branching function** $f_{\gamma(k)} : V_\gamma \longrightarrow R$ where $f_{\gamma(k)} = \pi_1(G_{\gamma(k)})$.

Let $L_\gamma = \{ f_{\gamma(k)} | \ k < T, \ \eta^k$ a branch node and $\eta^{k+1} = \beta^-(\eta^k) \}$
and $R_\gamma = \{ f_{\gamma(k)} | \ k < T, \ \eta^k$ a branch node and $\eta^{k+1} = \beta^+(\eta^k) \}$.

Thus, $V\gamma = \{x \in R^n | \ f(x) < 0$ and $g(x) \geq 0$ for all $f \in L_\gamma$ and $g \in R_\gamma\}$.
And similarly, for the ordered case

Now let $\Omega_T = \{ \mathbf{x} \in R^n | \ T_M(x) \leq T \}$ be the **time-T halting set** of M.
Let $\Gamma_T = \{ \gamma_x | \ x \in \Omega^T_M \}$.

Path Decomposition Theorem

1. Ω_T is a finite disjoint union of basic semi-algebraic sets (quasi-algebraic sets). In particular, $\Omega_T = \bigcup_{\gamma \in \Gamma_T} V_\gamma$

Thus the time-T halting set Ω_T is described by a semi-algebraic (quasi-algebraic) formula whose length may be exponential in T. (**Will want a more succinct description.)**

2. The halting set Ω_M is a countable disjoint union of basic semi-algebraic sets (quasi-algebraic sets) . In particular, $\Omega_M = \bigcup_{\gamma \in \Gamma_M} V_\gamma$
3. $\Phi_M |_{V_\gamma}$, the input-output map restricted to V_γ , is a polynomial (rational) map.

Consequence. The above examples are not decidable over $\mathbb{R}$ since:

- $\dim_H \partial$ Mandelbrot =2.
- The Cantor set is totally disconnected (contains no intervals) and uncountable.
- Bad Newton pts can be a Cantor set.

We now show how to get succinct descriptions of time-T Halting sets. This construction will also be the basis of the proof that HN is a universal NP-complete problem over any field.

The Register Equations and Succinct Descriptions of Time-T Computations and Time-T Halting Sets

Given M. Let $I = R^n$, $S = R^m$, $O_M = R^1$ Let $x \in I = R^n$.
$x \in \Omega_T \Leftrightarrow \exists$ a sequence $z = (z^0, z^1, \ldots, z^T) \in (NxS)^{T+1}$ satisfying the

(Time-T) Register equations, $R_T(x,z)$, 1st form:

1. $z^0 = (1, I(x))$ and $\pi_N(z^T) = N$ (*initial and terminal conditions*)
2. $z^k = H(z^{k-1})$, k = 1, …, T (*next state conditions*)

Thus,
$x \in \Omega_T \Leftrightarrow \exists z R_T(x,z)$ where $R_T(x,z)$ is $\left(z^0 = (1, I(x))\right) \& (\pi_N(z^T) = N) \&_{k=1}^{T} (z^k = H(z^{k-1}))$.

We now transform $R_T(x,z)$ naturally into an equivalent "small" semi-algebraic (quasi-algebraic) system over R. Thus, Ω_T is the projection of a succinctly defined semi-algebraic (quasi-algebraic) set.

If R is a field, we further get a "small" system of quadratic equations.
Over $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, we get a "small" single degree-4 polynomial equation.
So in each of these cases, Ω_T is the projection of a succinctly defined variety.

To do so, it is useful to make explicit the coordinate maps:

$x \in \Omega_T \Leftrightarrow \exists$ a sequence $((\eta^0, x^0), \ldots, (\eta^T, x^T)) \in (NxS)^{T+1}$ satisfying the

(Time-T) Register equations, 2nd form:

1. $(\eta^0, x^0) = (1, I(x))$ and $\eta^T = N$
2. $\eta^k = \beta(\eta^{k-1}, x^{k-1})$, $x^k = g(\eta^{k-1}, x^{k-1})$, k = 1, …, T (mT poly (rat) equations)

We now extend these equations to R by injecting $N \hookrightarrow R^N$ given by $j \longrightarrow e_j$, the jth coordinate vector, j =1,…,N. (ie $e_j = (0,\ldots 0,1$ (jth coordinate), $0,\ldots,0)$ Let,

$$\beta'(\alpha, y) = \sum_{j=1}^{N} \alpha_j e_{\beta(j,y)}, \quad g'(\alpha, y) = \sum_{j=1}^{N} \alpha_j g(j,y)$$

So for $\alpha = e_j$, $\beta'(\alpha, y) = e_{\beta(j,y)}$ and $g'(\alpha, y) = g(j,y)$.

So we have extended H to H: $R^N \times R^m \longrightarrow R^N \times R^m$.

NB. g': $R^N \times R^m \to R^m$ is a polynomial (rat) map of degree $D_M + 1$ in N + m variables with at most N times the $\max_\eta$(# of terms in g_η). Soon will deal with β': $R^N \times R^m \to R^N$ (not a polynomial map, not even continuous!)

Now, $x \in \Omega^T \Leftrightarrow$ there is a sequence $((\alpha^0, x^0), \ldots, (\alpha^T, x^T)) \in (R^N x S)^{T+1}$ satisfying the

(Time-T) Register equations, 3rd form (over R):

1. $(\alpha^0, x^0) - (e_1, I(x)) = 0$ and $\alpha^T - e_N = 0$ (2N +m) linear equations
2. $\alpha^k - \beta'(\alpha^{k-1}, x^{k-1}) = 0$ (soon), $x^k - g'(\alpha^{k-1}, x^{-1}) = 0$, $k = 1, \ldots, T$ (mT polynomial equations with max degree $D_M + 1$ in case of polynomial (and $N D_M + 1$ if rational[2]).

Let $\mathbf{w} = (w_1, w_2, \ldots, w_t) = (\alpha^0, x^0, \ldots, \alpha^T, x^T)$ where $t = (N+m)(T+1)$ variables.

Let $\mathbf{R'_T(x, w)}$ denote the time-T register equations in 3rd form.

Theorem A. $\mathbf{R'_T(x, w)}$ is equivalent to a semi-algebraic (quasi-algebraic) system $\Phi_T(x, w)$ in $n + t$ variables with $t = (N+m)(T+1)$, with at most $4(N+m)T$ polynomial equations (of degree at most $N D_M + 1$ in) plus $2T$ inequalities.

Corollary. So, $x \in \Omega_T \Leftrightarrow \exists w\, \Phi_T$ true over R. That is, the time-T halting set Ω_T is the projection of a semi-algebraic (quasi-algebraic) set $S \subset R^{n+t}$ defined by a "small" system $\Phi_T(x, w')$.

Corollary. Same for $\Omega_T(v) = \{x \in \Omega_T \mid \Phi_M(x) = v\}$
Just add l linear equations for the output map.

Proof of Theorem A.

The only subtle part is analyzing: $\alpha^k - \beta'(\alpha^{k-1}, x^{k-1}) = 0$

---

[2] **Rational map case:** Suppose $x' = g'(\alpha, x)$ where $g(j,x)|_i = p_i(j,x)/q_i(j,s)$.

Then $x'_i = g'(\alpha, x)_i = \sum_{j=1}^{N} \alpha_j g(j,x)|_i = \sum_{j=1}^{N} \alpha_j p_i(j,x)/q_i(j,x) = P_i(\alpha, x)/Q_i(x)$ where

$Q_i(x) = \prod_{j=1}^{N} q_i(j,x)$, $P_i(\alpha, x) = \sum_{j=1}^{N} \alpha_j \prod_{k \neq j}^{N} q_i(k,x) p_i(j,x)$.

The degree $Q_i \leq N D_M$ and degree $P_i \leq N D_M + 1$.

So replace the rational equation, $x'_i - g'(\alpha, x)_i = 0$ [ie, $x'_i - P_i(\alpha, x)/Q_i(x) = 0$] with $x'_i Q_i(x) - P_i(\alpha, x) = 0$.

Define linear maps: $\beta'^{-}, \beta'^{+} : R^N \to R^N$ where
$\beta'^{-}(\alpha) = \sum \alpha_j e_{\beta_j^-}$ and $\beta'^{+}(\alpha) = \sum \alpha_j e_{\beta_j^+}$, where for j not a branching node, $\beta_j^- = \beta_j^+ = \beta_j$
NB. If α is the j-th coordinate vector e_j, then $\beta'^{-}(\alpha) = \beta_j^-$ and $\beta'^{+}(\alpha) = \beta_j^+$ and both of these are equal to β_j for non-branching nodes.

So, if $\alpha = e_j$:
$\alpha' - \beta'(\alpha, x) = 0 \Leftrightarrow B(\alpha', \alpha, x)$: $(x_1 < 0 \to \alpha' - \beta'^{-}(\alpha) = 0) \wedge (x_1 \geq 0 \to \alpha' - \beta'^{+}(\alpha) = 0)$

Recall: "$A \longrightarrow B$" is equivalent to "$\neg A \vee B$."
So, if $\alpha = e_j$:
$\alpha' - \beta'(\alpha, x) = 0 \Leftrightarrow B^*(\alpha', \alpha, x)$: $(x_1 \geq 0 \vee \alpha' - \beta'^{-}(\alpha) = 0) \wedge (x_1 < 0 \vee \alpha' - \beta'^{+}(\alpha) = 0)$

If R is unordered, use $B^*_{=}(\alpha', \alpha, x)$: $(x_1 = 0 \vee \alpha' - \beta'^{-}(\alpha) = 0) \wedge (x_1 \neq 0 \vee \alpha' - \beta'^{+}(\alpha) = 0)$

So, replace $\alpha^k - \beta'(\alpha^{k-1}, x^{k-1}) = 0$ k=1,…,T in the Register equations, 3rd form, by $B^*(\alpha^k, \alpha^{k-1}, x^{k-1})$ (or in the unordered case, by $B^*_{=}(\alpha^k, \alpha^{k-1}, x^{k-1})$).
These consist of 2NT linear equations and 2T inequalities.
■

Get More Succinct Descriptions

Suppose M is a machine over (R, =) where R a field, or over (R,<) where R is $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$.

Theorem B. The register equations can be replaced by k quadratic equations, $q_1(x,u) = 0, \ldots, q_k(x,u) = 0$, in n + s variables, $x_1, \ldots, x_n, u_1, \ldots u_s$, where $s, k \leq (n + mT)^c$ and c is a constant depending on N and D_M and not on n, m, or T.

In case R is $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, can replace the quadratic system, $q_1(x,u) = 0, \ldots, q_k(x,u) = 0$, by a single degree 4 polynomial equation, $q(x, u) = 0$ where $q(x,u) = \sum_{i=1}^{k} q_i(x,u)^2$.

Corollary. Ω_T **is the projection of an algebraic set** in R^{n+s} defined by the k quadratic equations as above. That is, $\Omega_T = \{ x \in R^n \mid \exists u \in R^s \ (q_1(x,u) = 0, \ldots, q_k(x,u) = 0)\}$.

Again, in case R is $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, we can replace the quadratic system by a single degree 4 polynomial equation.

Proof of Theorem B.

Suppose first that M is a machine over (R, =) where R is a field.
Then $x \neq 0 \Leftrightarrow \exists u(xu = 1)$
Consider:
$B^*_{=}(\alpha^k, \alpha^{k-1}, x^{k-1})$:
$(x_1^{k-1} = 0 \vee \alpha^k - \beta'^{-}(\alpha^{k-1}) = 0) \wedge (x_1^{k-1} \neq 0 \vee \alpha^k - \beta'^{+}(\alpha^{k-1}) = 0),\ k = 1,\ldots,T$
Replace by
$x_1^{k-1}(\alpha^k - \beta'^{-}(\alpha^{k-1})) = 0;\ \exists u^{k-1}[(x_1^{k-1}u^{k-1} - 1)(\alpha^k - \beta'^{+}(\alpha^{k-1})) = 0],\ k = 1,\ldots,T$
T new variables, small degrees.

Suppose now M is a machine of an ordered field where positive elements have square roots. For example, $(\mathbb{R}, <)$ or any real closed field.

Then $x > 0 \Leftrightarrow \exists u(xu^2 = 1)$
Consider:
$B^*(\alpha^k, \alpha^{k-1}, x^{k-1})$:
$(x_1^{k-1} \geq 0 \vee \alpha^k - \beta'^{-}(\alpha^{k-1}) = 0) \wedge (x_1^{k-1} < 0 \vee \alpha^k - \beta'^{+}(\alpha^{k-1}) = 0),\ k = 1,\ldots,T$
Replace by
$\exists u^{k-1}[x_1^{k-1}(x_1^{k-1}(u^{k-1})^2 - 1)(\alpha^k - \beta'^{-}(\alpha^{k-1})) = 0]; \exists v^{k-1}(-x_1^{k-1}(v^{k-1})^2 - 1)(\alpha^k - \beta'^{+}(\alpha^{k-1})),\ k = 1,\ldots,T$
2T new variables.

Now for $(\mathbb{Z}, <)$:

$x > 0 \Leftrightarrow \exists u \geq 0\ (x = 1 + u)$ and

Recall: Lagrange's theorem for $\mathbb{Z}$: $u \geq 0 \Leftrightarrow \exists u_1\, u_2\, u_3\, u_4\ (u = u_1^2 + u_2^2 + u_3^2 + u_4^2)$

So replace $B^*(\alpha^k, \alpha^{k-1}, x^{k-1})$

by
$\exists u_1^{k-1} u_2^{k-1} u_3^{k-1} u_4^{k-1}[(x_1^{k-1} - (u_1^2 + u_2^2 + u_3^2 + u_4^2))(\alpha^k - \beta'^{-}(\alpha^{k-1})) = 0];$
$\exists v_1^{k-1} v_2^{k-1} v_3^{k-1} v_4^{k-1}[(-x_1^{k-1} - (v_1^2 + v_2^2 + v_3^2 + v_4^2) - 1)(\alpha^k - \beta'^{+}(\alpha^{k-1})) = 0],\quad k = 1,\ldots,T$
8T new variables

Modify for $(\mathbb{Q}, <)$: Consider p/q.

The following Lemma finishes the proof of Theorem B.

Lemma. Suppose R is a ring or field. Then any system of polynomial equations $p_1(x)=0,\ldots, p_t(x)=0$ in n variables of degree at most D and with at most K monomials per equation (so $K = O(n^D)$) is n-equivalent to a quadratic polynomial system $q_1(x,u) = 0, \ldots, q_{t+t'}(x,u) = 0$ in n+n' variables with $n',t' \leq KD$. Here, $x = (x_1, ..., x_n)$ and $u = (u_1,...,u_{n'})$. (NB. In our case, D is dependent only on the machine M.)

Proof:
Let $I = (i_1,...,i_d)$ (where $i_j \in \{1,...,n\}$, $i_j \leq i_{j+1}$ and $2 \leq d \leq D$)
For each monomial of type $a_I x_I$ with $a_I \in R$, $x_I = x_{i_1} \ldots x_{i_d}$, add d-2 new variables, $u_{I_1} \ldots u_{I_{d-2}}$. Then replace $a_I x_I$ by $a_I x_{i_1} u_{I_1}$ and add the d-2 equations

$$u_{I_1} - x_{i_2} u_{I_2} = 0,\ u_{I_2} - x_{i_3} u_{I_3} = 0\ ,\ldots,\ u_{I_{d-2}} - x_{i_{d-1}} x_{i_d} = 0.$$

■■

All arguments are uniform in everything in sight.

General Machines over R

Input and Output spaces : $R^\infty = \bigcup_{n\geq 0} R^n$ disjoint union.

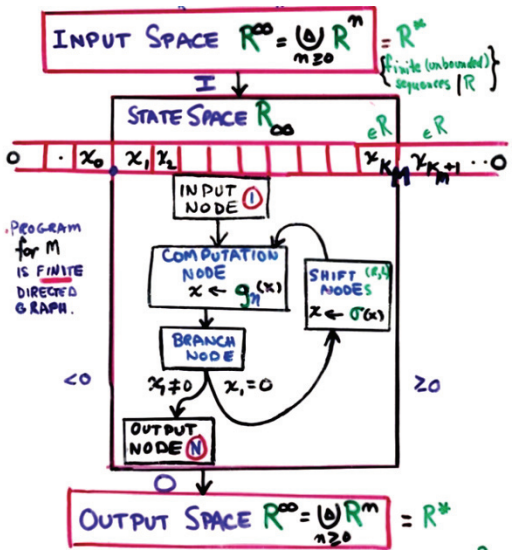
State space: $\mathbf{R}_\infty$ = bi-infinite direct sum space over R
Elements: x = (…, x_{-2}, x_{-1}, x_0 . x_1, x_2, …) such that for |k| sufficiently large, $x_k = 0$.

Can define **polynomial and rational maps** as finite objects as follows:
If h: $R^m \longrightarrow R$ is a polynomial map then
$\hat{h}$: $R_\infty \to R$ is a polynomial map defined by $\hat{h}(x) = h(x_1,...,x_m)$
If g_i: $R^m \longrightarrow R$, i=1,..., m are polynomial maps then
$\hat{g}$: $R_\infty \to R_\infty$ is a polynomial map of dimension m defined by $\hat{g}(x)_i = \hat{g}_i(x)$ for $i = 1,...,m$
and $\hat{g}(x)_i = x_i$ for i <1 or i > m.

Define **Input and Output maps**: I_∞: $R^\infty \longrightarrow R_\infty$ and O_∞ : $R_\infty \longrightarrow R^\infty$ by
$I_\infty(x) = (...,0,0,\hat{n}\ .\ x_1,..x_n,0,0,0,...)$ for x ∈ R^n where $\hat{n}$ denotes the sequence of n 1's, $\hat{0}$=0.
$O_\infty(...,x_0\ .\ x_1,..x_l,0,0,0,...) = (x_1,..x_l)$ where $l = \min_{i\geq 0}(x_{-i} = 0)$. (Output ∈ R^0 if $l = 0$.)

Machine has 4 node types as before with associated maps. In addition, to access inputs of arbitrary dimension, we add **shift nodes**, η, with associated maps: $g_\eta \in \{\sigma_l, \sigma_r\}$ where $\sigma_l(x)_i = x_{i+1}$, $\sigma_r(x)_i = x_{i-1}$, and unique next nodes β_η. Let $\sum_M$ be the set of shift nodes of M.

Associated to M is the **dimension K_M, degree D_M**, and set of **constants C_M**.



Time –T Register Equations
NB. Reduces to the finite dimensional case since in time T, need only consider the **basic active state space** $S_m = R^{2m} = \{(x_{-(m-1),...}, x_0, x_1,..., x_m)\}$ where **m = K_M + T**.
On S_m, shift nodes become polynomials: $g_\eta = \sigma_l$ on S_m becomes
$g_{\eta,m}(x_{-(m-1)},..., x_0,..., x_m) = (x_{-(m-2)},..., x_0,..., x_m, 0)$. Similarly for $g_\eta = \sigma_r$, shift right.

Theorem C.

1. The register equations $\mathbf{R'_T(x, w)}$ of machine M over R are equivalent to a semi-algebraic (quasi-algebraic) system $\Phi_T(x,u)$ where
   - The number of variables is at most $n + cT^2$
   - The number of polynomial equations is at most cT^2
   - The number of inequalities (all linear) is at most $2T$

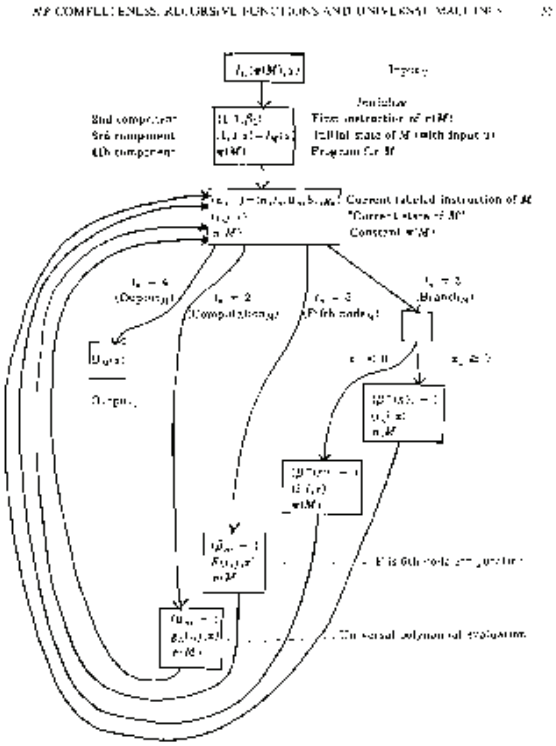
Here c is a constant depending on N, D_M and K_M and is independent of n and T.

2. Over $(\mathbb{C}, =)$, $(\mathbb{Z}_2, =)$ or any field (F,=) as well as over $(\mathbb{Z},<)$, $(\mathbb{Q},<)$ or $(\mathbb{R},<)$ we have
   - $\mathbf{R'_T(x, w)}$ is n-equivalent to a **polynomial system** $\Phi'_T(x,u)$ with the same qualitative bounds as above.
   - $\Phi'_T(x,u)$ is equivalent to a **quadratic system** $Q_M(x, u')$ where both the length of u' and the number of equations are bounded above by $(n+T)^C$, c, a constant depending only on M.

3. Over $(\mathbb{Z},<)$, $(\mathbb{Q},<)$ or $(\mathbb{R},<)$, the register equations, $\mathbf{R'_T(x, w)}$ are n-equivalent to a single **degree-4 polynomial equation** $p_T(x, u) = 0$ where $u = (u_1,\ldots,u_s)$ and $s \le (n+T)^C$, c, a constant depending only on M.

Corollary. For case 2, the validity of $F_M(x, 1, T)$,"Machine M with input x halts with output 1 in time $\le T$," is equivalent to the solvability over R of a quadratic system $Q_M(x, u')$ where both the length of u'and the number of equations are bounded above by $(n+T)^C$, c, a constant depending only on M. For case 3, can replace the quadratic system by a single polynomial equation.

The Universal Polynomial System Evaluator (UPSE) and Universal Machines



Decision Problems, Complexity, Classs P, NP and NP Completeness over R

A **problem** (language) over R is a set $S \subseteq R^\infty$.
A **structured problem** *over R* is a pair, (X, X_{yes}), where $X_{yes} \subseteq X \subseteq R^\infty$. X consists of the ***problem instances***, X_{yes}, the ***yes-instances***.

For HN_R,
$X = \{f = (f_1,\ldots,f_m) |\ f_i \in R[x_1,\ldots,x_n],\ m, n > 0.$
$X_{yes} = \{f \in X |\ \exists\ \zeta \in R^n,\ f_i(\zeta_1,\ldots,\zeta_n) = 0,\ i=1,\ldots,m\}.$

Finite polynomial systems over R can be coded as elements of R^∞ (by systematically listing coefficients); thus X can be viewed as a subspace of R^∞. (We assume dense representation, unless otherwise stated.)

A problem is **decidable** over R if its characteristic function of is computable over R.
A structured problem over R, (X, X_{yes}), is **decidable** if the characteristic function of X_{yes} in X is computable over R.***

Suppose a **height function**, $ht_R(x)$, defined over R with values in the positive integers.
Then for $x \in R^n \subset R^\infty$, define **length (x)** = n and **size (x)** = $\text{length}(x) \cdot ht_R(x)$.

Now, suppose M is a machine over R.
For $x \in R^n \subset R^\infty$, define **$cost_M(x)$** = $T_M(x) \cdot ht_{max}(x)$ where $ht_{max}(x)$ is the maximum height of any element occurring in the computation of M on input x.

For the moment we assume, $ht_R(x) = 1$. Then size(x) = length(x) and **$cost_M(x)$** = $T_M(x)$.
For $R = \mathbb{Z}_2$, these are just the classical measures of size and cost. Moreover, for $R = \mathbb{Z}_2$, all our complexity definitions and results reduce to the classical.
[For $\mathbb{Z}$ and $\mathbb{Q}$, to recapture the classical measures of size and cost, just code elements as binary and work over $\mathbb{Z}_2$. Alternatively, for bit complexity, let $ht_{\mathbb{Z}}(x) = \lceil \log(|x|+1) \rceil$ and $ht_{\mathbb{Q}}(p/q) = \max(ht_{\mathbb{Z}}(p), ht_{\mathbb{Z}}(q))$.]

M is **poly-time** over R on $X \subseteq R^\infty$ if there are positive integers c and q such that $cost_M(x) \le c(size(x))^q$ for all $x \in X$.

A map $\varphi: X \to Y \subseteq R^\infty$ is **poly-time computable** over R, if it is computable by a poly-time machine on X.

A (structured) problem (X, X_{yes}) is in **class P** over R (write: $(X, X_{yes}) \in \mathbf{P_R}$) if it is decidable by a poly-time machine over R.

***If (X, X_{yes}) is a structured problem over R, we usually assume that $(R^\infty, X) \in P_R$. ***

A problem (X, X_{yes}) is **p-reducible** to a problem (X', X'_{yes}) (write: $(X, X_{yes}) \xrightarrow[p]{} (X', X'_{yes})$) if there is a poly-time computable map $\phi : X \to X'$ such that $x \in X_{yes} \Leftrightarrow \phi(x) \in X'_{yes}$.

A problem (X, X_{yes}) is in **class NP** over R (write: $(X, X_{yes}) \in \mathbf{NP_R}$), if there exists a "non-deterministic" machine M over R, with $I_M = R^\infty \times R^\infty$ and positive integers c and q such that $x \in X_{yes} \Leftrightarrow \exists\, w \in R^\infty$ such that $\Phi_M(x, w) = 1$ and $\text{cost}_M(x, w) \le c(\text{size}(x))^q$.
w is called a **witness**.

A problem is **NP-hard** over R if every problem in class NP is p-reducible to it.
A problem is **NP-complete** over R if it is in NP over R and is NP-hard over R.

NP Complete Problems over R

Theorem D.

1. **For any field (R, =), Hilbert Nullstellensatz (HN) is NP-complete over R.**
2. **For any field (R, =), "quadratic systems" is NP-complete over R.**
3. **4-FEAS (the problem of deciding solvability over R of degree 4 polynomials) is NP-complete over** $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Corollary.

1. **For any field (R, =), P = NP $\Leftrightarrow$ $HN_R \in P$.**
2. **NP $\subset$ EXP for** $\mathbb{Z}_2$, $\mathbb{R}$ and $\mathbb{C}$. (Easy for $\mathbb{Z}_2$, as a consequence of Renegar et. al. for $\mathbb{R}$ and $\mathbb{C}$).
3. **P≠NP over** $\mathbb{Z}$ (Matiyaseivich). **P≠NP over** $\mathbb{Q}$. **(If F is an infinite field and P=NP over F, then F admits elimination of quantifiers and so is algebraically closed in the unordered case and real closed in the ordered case.)**

Proof of Theorem D.
Use USPE to show all the problems in 1, 2, and 3 are in class NP over R.

Now suppose (X, X_{yes}) is in class NP over R.
Then there is a machine M and polynomial p such that for each $x \in X_{yes}$,
$\exists\, w = (w_1, \ldots, w_{p(n)}) \in R^{p(n)}$ such that $F_M((x, w), 1, p(n))$.

By the Corollary to Theorem C, the validity of $F_M((x,w), 1, p(n))$ is equivalent to the solvability over R of a quadratic system $Q_M((x,w), u')$ where both the length of u' and the number of equations are bounded above by $((n + p(n)) + p(n))^C$, where c is a constant depending only on M.

So, for 1 and 2, map problem instance x to the quadratic system, $Q_M((x,w), u')$.
Then $x \in X_{yes} \Leftrightarrow Q_M((x, w), u') \in HN_{yes}$ is solvable over R $\Leftrightarrow Q_M((x, w), u') \in HN_{yes}$.

For 3, map x to the single degree 4 polynomial equation gotten from the taking the sum of squares of polynomials in $Q_M((x,w),u')$.■