Simplification of Real Polynomial Systems

- A root α of a polynomial p is said to be *isolated* if two rational numbers a and b are given such that $a \leq \alpha \leq b$ and p has only one root in the interval $[a, b]$. This interval is called the *isolating interval* of α.

- **Proposition 1.** Given an isolated root of a polynomial, we can reduced the size of the isolating interval, so that it is as small as desired.

- **Algorithm for Solving** $p(x) = 0; q_1 > 0; \cdots; q_k(x) > 0$

  1. Isolate all the roots of p and of the q_i.
  2. Reject those roots of p which are also roots of the q_i.
  3. Reduce the intervals so that each interval defining a root of p do not contain a root of one of the q_i.
  4. For each root α of p, isolate between a and b, check that all the q_i are positive.

- The *Sturm sequence* associated with the polynomial p is a sequence of polynomials with rational coefficients $p_0(x), p_1(x), \ldots, p_k(x)$ where $k \leq n$ and p_k is constant, defined by the following equations:

$$\begin{aligned} p_0(x) &= p(x), \\ p_1(x) &= p'(x), \\ p_i(x) &= -\text{remainder } (p_{i-2}(x), p_{i-1}(x)) \end{aligned}$$

  where "remainder" means the remainder from the division of one polynomial by another.

- Let y be a real number which is not a root of p. The *variation* at the point y of the Sturm sequence associated with p, written $V(y)$ is the number of variations of sign in the sequence $p_0(y), p_1(y), \ldots, p_k(y)$.

- **Sturm's Theorem.** If a and b are two points, which are not real roots of p, such that $a < b$, then the number of real roots of p in the interval (a, b) is $V(a) - V(b)$.

- **Cauchy's Bound 1.** Let a be a root of p. Then

$$|a! \leq 1 + \max\left(\left|\frac{a_{n-1}}{a_n}\right|, \left|\frac{a_{n-2}}{a_n}\right|, \cdots, \left|\frac{a_0}{a_n}\right|\right).$$

- **Cauchy's Bound 2.** Let a be a root of p. Then

$$|a| \leq 1 + \max\left(\left|\frac{na_{n-1}}{a_n}\right|, \left|\frac{na_{n-2}}{a_n}\right|^{1/2}, \cdots, \left|\frac{na_0}{a_n}\right|^{1/n}\right).$$

- **Knuth's Bound.** Let a be a root of p. Then

$$|a| \leq 2\max\left(\left|\frac{a_{n-1}}{a_n}\right|, \left|\frac{a_{n-2}}{a_n}\right|^{1/2}, \cdots, \left|\frac{a_0}{a_n}\right|^{1/n}\right).$$

- **Isolating Algorithm for Real Roots**
  1. Set $L := ((-b, b))$, where $b \geq \max|\alpha_i|$ for all zeros α_i of p.
  2. Compute Sturm sequence of p as $(p, p', \ldots, p_r)$.
  3. For every interval $(a, b]$ in L do
     (a) Bisect $(a, b]$ into $(a, m]$ and $(m, b]$.
     (b) For each subinterval compute the number t of real zeros using Sturm theorem.
     (c) If $r = 0$, drop the interval.
     If $r = 1$, output the interval.
     If $r > 1$, keep the interval in L.

- A *representation* of a real algebraic number consists of: a square-free polynomial p with integral coefficients; and an isolating interval $[a, b]$ of one of its roots.

- A *semi-algebraic* component of R^n is a set of points satisfying a family of polynomial equalities and inequalities:

$$\begin{aligned}\{(x_1, \ldots, x_n) \ : \ & p_1(x_1, \ldots, x_n) = \cdots = p_k(x_1, \ldots, x_n) = 0; \\ & q_1(x_1, \ldots, x_n) > 0; \ldots; q_k(x_1, \ldots, x_n) > 0\}.\end{aligned}$$

- A *semi-algebraic variety* is either a semi-algebraic component, or one of the sets $A \cap B$, $A \cup B$ and $A \backslash B$, where A and B are two semi-algebraic varieties.

- A *decomposition* of R^n is the representation of R^n as the union of a finite number of disjoint and connected semi-algebraic components.

- A decomposition is *pointed*, if for every component, a point with rational or algebraic coefficients belonging to this component is associated with it.

- A decomposition of R^n is *invariant* for the signs of a family of polynomials $r_i(x_1, \ldots, x_n)$ if , over each component of the decomposition, each polynomial is
  - always positive or
  - always negative or
  - always zero

- Let V be a semi-algebraic variety, and D a decomposition of R^n invariant for the signs of any polynomials occurring in the definition of V. For every component C of D, $C \cap V = \phi$ or $C \subset V$.

- A decomposition D of R^n, that is $R^n = E_1 \cup \ldots \cup E_N$, is *cylindrical* if $n = 0$ or if:
  1. R^{n-1} has a cylindrical decomposition D', which we can write $R^{n-1} = F_1 \cup \ldots \cup F_m$ and
  2. For each component E_i of D, there is a component F_j of D' such that E_i is written in one of the following forms:

$$\begin{array}{lll}
\{(x_1, \ldots, x_n) : (x_1, \ldots, x_{n-1}) \in F_j & \text{and} & x_n < f_k(x_1, \ldots, x_{n-1})\} \\
\{(x_1, \ldots, x_n) : (x_1, \ldots, x_{n-1}) \in F_j & \text{and} & x_n = f_k(x_1, \ldots, x_{n-1})\} \\
\{(x_1, \ldots, x_n) : (x_1, \ldots, x_{n-1}) \in F_j & \text{and} & f_k(x_1, \ldots, x_{n-1}) < x_n \\
 & \text{and} & x_n < f'_k(x_1, \ldots, x_{n-1})\} \\
\{(x_1, \ldots, x_n) : (x_1, \ldots, x_{n-1}) \in F_j & \text{and} & x_n > f_k(x_1, \ldots, x_{n-1})\}
\end{array}$$

     where the f_k are the solutions of polynomial equations with rational coefficients.

- **Collins's Algorithm for Cylindrical Decomposition of** R^n:

    1. Calculate a family Q of polynomials in the variables $x_1, \ldots, x_{n-1}$ such that a decomposition of R^{n-1} invariant for their signs can serve as a basis for the decomposition of R^n invariant for the signs of P.
    2. Calculate, by recursion, a decomposition D' of R^{n-1} invariant for the signs of Q.
    3. For each component F of D', calculate the decomposition of the cylinder above F induced by the polynomials of P

- For the case of R^2, if $P = \{p_1, \ldots, p_n\}$ is a family of square-free polynomials relatively prime in pairs, it suffices to take for Q the following family:

  $$\{\mathrm{lc}_y(p_i); 1 \le i \le n\} \cup \{\mathrm{Disc}_y(p_i); 1 \le i \le n\} \cup \{\mathrm{Res}_y(p_i, p_j); 1 \le i < j \le n\}.$$

- The problem of *quantifier elimination* is that of finding an algorithm, which, given a logical expression containing quantifiers, finds an equivalent expression which does not contain any.