Decidable fragments of FOL
~ solving polynomial constraints by QE-CAD ~

Mizuhito Ogawa@JAIST

Logic for software verification

- As description language
  - ✓Most of model checkers accepts temporal logic specification (e.g., LTL, CTL)
- As formal reasoning
  - ✓Inductive reasoning in higher order logic
- As automated reasoning
  - ✓Approximate system behavior (e.g., SAT/SMT)
  - ✓Limited class

Logic is useful in practice!

- **Note**. Theoretical complexity does not match practice.

FOL proving in software verification

- FOL formula for loop invariants
  - ✓Craig interpolation is a strong strategy
  - ✓Lots of FOL provers: Vampire, E, SPASS, …
    - –Based on resolution (refined as superposition)

- FOL for quantitative properties
  - ✓Solving linear (in)equality
    - –Presburger arithmetic widely used as backend of SMT.
  - ✓Solving nonlinear (in)equality
    - –PID control design, though still limited to 7-8 variables only.

Solving (in)equality with integer coefficients)

- Linear (in)equations : addition and subtraction only
  - ✓Both on integers and real numbers
  - ✓Algorithms:
    - (Existential) Quantifier elimination,
      e.g., $\exists y. (x < y \land y < z+3)$ is equivalent to
      $x < (z+3) - 1 = z+2$ (on integers)
      $x < z+3$ (on real numbers)
    - Linear programming (LP), e.g., simplex method

- What happen if we add multiplication?
  - ✓*Undecidable* for integers (Hilbert's 10^{th} problem)
  - ✓*Decidable* for real numbers (Tarski, 1930)

Entrance exam of Japanese University

- Tohoku U. (2010) : Let $f(x) = x^3 + 3x^2 - 9x$. Find the condition for a such that, for each x,y with $y < x < a$,

$$f(x) > \frac{(x-y)\,f(a) + (a-x)\,f(y)}{a-y}$$

0.14+0.67 secs reduce

File Edit Font Break Load Package Switch Help

```
1: load_package redlog;

2: rlset OFSF;
Grow hash from 1 chunks
... to 1 chunks
Rehashing done
```

$$\emptyset$$

```
3: psi := (y < x < a) impl (a-y)*(x**3 + 3*x**2 - 9*x) > (x-y)*(a**3 + 3*a**2 -
9*a) + (a-x)*(y**3 + 3*y**2 - 9*y);
```

$$\psi := (-x+y<0 \wedge -a+x<0) \longrightarrow -a^3x + a^3y - 3a^2x + 3a^2y + ax^3 + 3ax^2 - ay^3 - 3ay^2 - x^3y - 3x^2y + xy^3 + 3xy^2 > 0$$

```
4: rlcad all(x,all(y,psi));
```

$$a + 1 \leq 0$$

Approaches

- For polynomial inequalities
  - ✓Sandwich by testing (under-approximation) and intervals arithmetic (over-approximation)
    - There are no guarantee for termination.
    - Roundoff error of floating point is worry.

- QE-CAD (Cylindrical Algebraic Decomposition)
  - ✓Exact solution.
  - ✓Algebraic numbers are treated as an ideals (of defining polynomials).

Remark on roundoff errors: Rump's function

$$(333.75 - a^2)b^6 + a^2(11a^2b^2 - 121b^4 - 2) + 5.5b^8 + \frac{a}{2b}$$

- Tricky behavior when a=77617, b=33096 with IEEE 754 floating operations
  - ✓Single precision : 1.172604
  - ✓Double precision : 1.1726039400531786
  - ✓Fourfold precision : 1.1726039400531786318588349045201838
  - ✓Symbolic computation with rational number expressions (or, 140-150 bits) results

    - 54767 / 66192 (approx. - 0.8273960599).

Can remedy by validiated numerics

QE-CAD (Quantifier Elimination by Cylindrical Algebraic Decomposition)

Solving Tarski sentences

- Tarski sentences
  - ✓Boolean combination of polynomial constraints (in prenex normal forms)

- Tarski set
  - ✓If a closed formula, decide its truth-false over real numbers.
  - ✓If it has free variables, decide their conditions such that constraints hold, e.g.,

$$\forall x\ y\ .\ (y < x < a) \Rightarrow f(x) > \frac{(x-y)\,f(a) + (a-x)\,f(y)}{a-y}$$

Answer. $a+1 \leqq 0$

Brief histroy

- Tarski sentenses on real algebraic numbers is decidable (Tarsky 30)
  - ✓Complexity is non-elementary.
- QE-CAD (Collins 75)
  - ✓QE on polynomial constraints is double-exponential.
- Optimizations have been investigated
  - ✓Partial CAD (Collins-Hong 85)
  - ✓Single-exponential
    - –Virtual substitution (for small degrees)
    - –Sign-definite constraints on the single argument $\forall x>0.\ f(x)>0$ (typically for mechanical control).

QE-CAD implementations

- Open source tools
  - ✓REDLOG (Weispfenning,et.al. 88) built on REDUCE
    - latest 3.06 (2006, though REDUCE updated Oct 2010, also on windows)
    - rlcad (QE-CAD) not maintained, rlqe (virtual substitution) has been developed.
  - ✓QEPCAD (Hong, et.al. 90) built on SACLIB
    - latest 1.65 (May 2010, on UNIX only)

- Commercial tools
  - ✓Mathematica (latest 8.0)
  - ✓SynRac (Anai@Fujitsu, et.al. 03) built on Maple

Reference

- B.Mishra, Algorithmic Algebra, Springer, 1993
- S.Basu, R.Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometory, 2nd edition, Springer, 2006.

CAD idea

- A cell C is a connected (genus 0) component such that signs of constraints in $\mathbb{Q}[x_1,\ldots,x_n]$ are preserved.
  - ✓As a computable finite refinement, *cylindrical cells*.
  - ✓Each cylindrical cell is a *(semi-)algebraic set*.

- Cylindrical algebraic decomposition is computed by classifying the number of (real) roots.
  - ✓*Projection*: "*Discriminant*", and projection to lower dimensions. ⇒ *Counting roots + matrix operations*
  - ✓*Base*: Find sampling points
  - ✓*Lifting*: Algebraic extensions (as ideals).]

    ⇒ *Groebner basis*

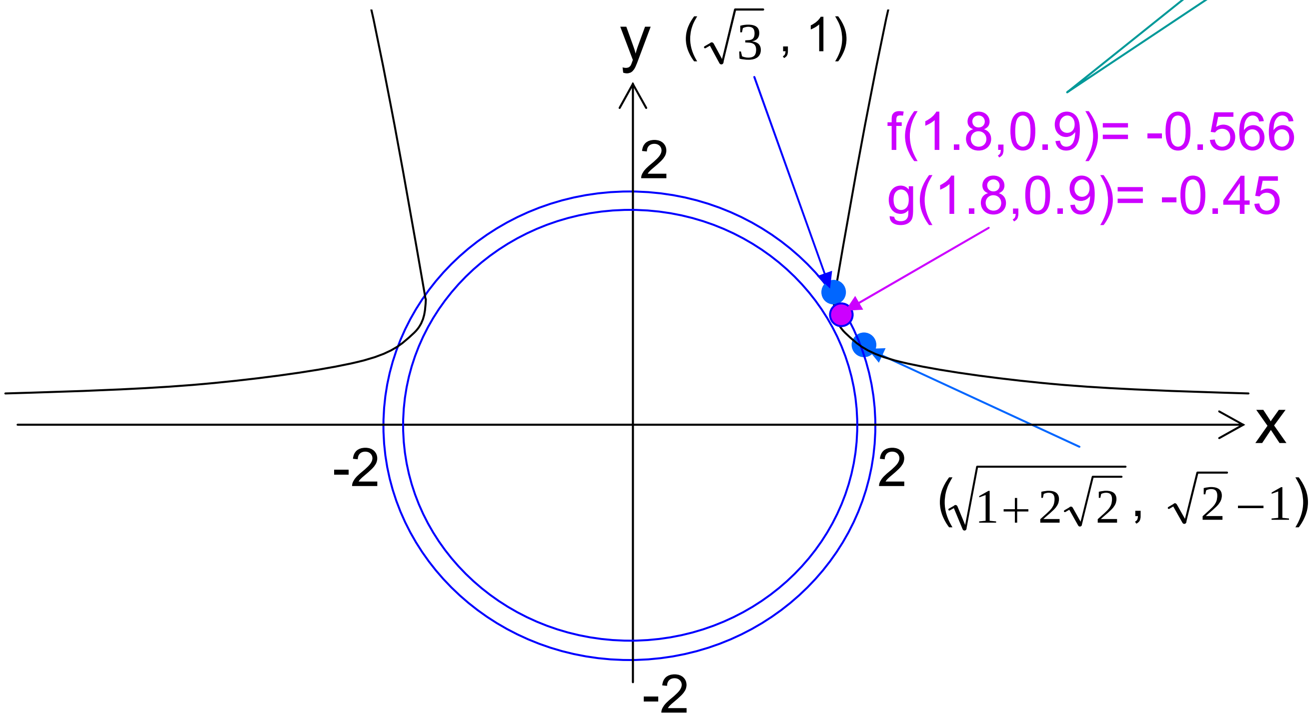
Projection phase

QE-CAD example

$\exists x \exists y . f(x,y) < 0 \wedge g(x,y) < 0?$

where $\begin{cases} f(x,y) = y^2 - (x^2 - 1)y + 1 \\ g(x,y) = x^2 + y^2 - 4 \end{cases}$

Yes



By REDLOG

0.07+0.81 secs reduce

File Edit Font Break Load Package Switch Help

```
1: load_package redlog;

2: rlset OFSF;
Grow hash from 1 chunks
... to 1 chunks
Rehashing done
```

$$\emptyset$$

```
3: psi := ex(x,ex(y,y**2 - (x**2 - 1)*y + 1 < 0 and x**2 + y**2 < 4));
```

$$\psi := \exists x \exists y(- x^2 y + y^2 + y + 1 < 0 \wedge x^2 + y^2 - 4 < 0)$$

```
4: rlqea psi;
```

Positive fraction ($\varepsilon_1 > \varepsilon_2 > 0$)

$$\left\{\left\{\mathrm{true}\,,\ \left\{x = \sqrt{-2\sqrt{2}\,\varepsilon_1 + 2\sqrt{2} - \varepsilon_1^2 + 2\,\varepsilon_1 - \varepsilon_2 + 1}\,,\ y = \sqrt{2} + \varepsilon_1 - 1\right\}\right\}\right\}$$

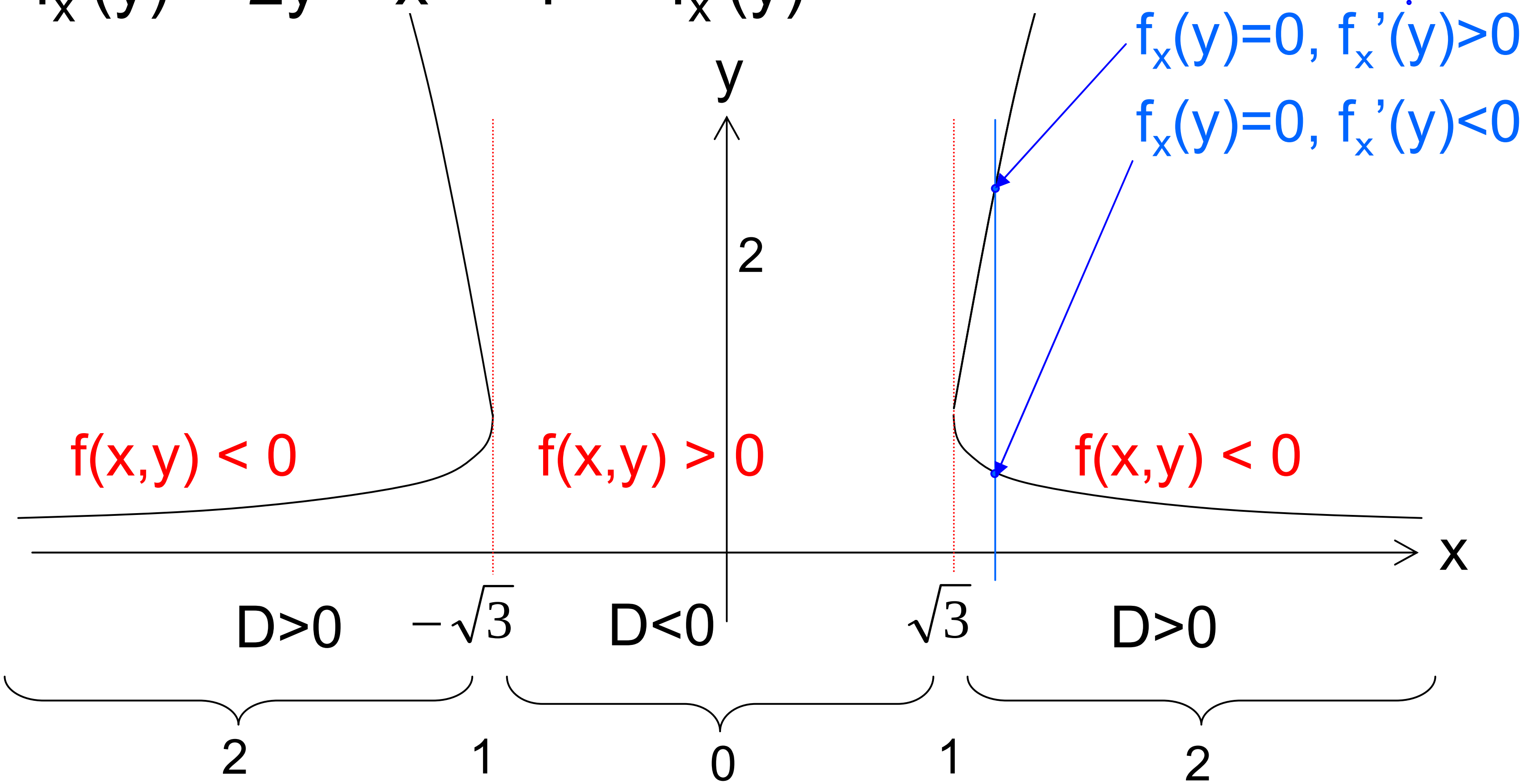
Example of counting real roots

- $f(x,y) = y^2 - (x^2 - 1)y + 1 \Rightarrow f_x(y) = y^2 - (x^2 - 1)y + 1$

  ✓D $= (x^2 - 1)^2 - 4 = x^4 - 2x^2 - 3 = (x^2 - 3)(x^2 + 1)$

  $\Leftrightarrow D \geqq 0$ is equivalent to existence of solutions.

  ✓$f_x{}'(y) = 2y - x^2 + 1 \Rightarrow f_x{}'(y)$



Counting the number of roots

- For a quadratic case, the discriminant D works. Then?

- Enumeration of complex roots of *f*(x), *f'*(x)
  ✓Number of complex roots (with duplication) of *f*(x) is
  $$\deg(f)$$
  ✓Number of different complex roots of *f*(x) is
  $$\deg(f) - \deg(\gcd(f, \frac{df}{dx}))$$

$$f(x) = a\prod_{i=1}^{k}(x-\beta_i)^{ei} \Rightarrow \gcd(f, \frac{df}{dx}) = \prod_{i=1}^{k}(x-\beta_i)^{ei-1}$$

- **Remark**. If they do not change, the number of real roots will not change (though do not know how many).

Example: preservation of the number of real roots

- $f(x,y) = y^2 – (x^2 – 1)y + 1$
  - ✓ $\deg (f_x(y)) = 2$
  - ✓ $f_x'(y) = 2y – x^2 +1$
  - ✓ $\gcd(f_x(y),f_x'(y)) = (x^2 –1)^2– 4 = (x^2 – 3) (x^2 + 1)$

    → $\deg(\gcd(f_x(y),f_x'(y))) = \begin{cases} 0 \text{ if } x^2 \neq 3, \\ 1 \text{ if } x^2 = 3 \end{cases}$

    → For $x^2 < 3$, $x^2=3$, $x^2 > 3$, the number of (real) roots are preserved.

    → Cells are decomposed to $x^2 < 3$, $x^2=3$, $x^2 > 3$, when the projection to x is applied.

Euclidian Algorithm to compute GCD

- **Euclid**: For $F_0(x) = f(x)$, $F_1(x) = g(x)$, repeat
  - ✓ $F_{i+1}(x) = F_{i-1}(x) - Q_i(x)\, F_i(x)$

  until $F_k(x) = 0$. Then, $F_{k-1}(x) = \gcd(f(x), g(x))$

- Note that this works also on $\mathbb{Q}(x_2,..,x_n)$,
  - ✓ i.e, By regarding $f(x_1,..,x_n) \in \mathbb{Q}[x_1,..,x_n]$ as $F(x_1) \in \mathbb{Q}(x_2,..,x_n)[x_1]$,

Extended Euclidian Algorithm

- **Extended Euclid**: For $F_0(x) = f(x)$, $F_1(x) = g(x)$, $(f \neq g)$
  $U_0(x) = 1$, $U_1(x) = 0$, $V_0(x) = 0$, $V_1(x) = 1$, repeat
  - ✓ $F_{i+1}(x) = F_{i-1}(x) - Q_i(x)\, F_i(x)$
  - ✓ $U_{i+1}(x) = U_{i-1}(x) - Q_i(x)\, U_i(x)$
  - ✓ $V_{i+1}(x) = V_{i-1}(x) - Q_i(x)\, V_i(x)$

  until $F_k(x) = 0$. Then, $F_{k-1}(x) = \gcd(f(x),g(x))$ and
  $$F_{k-1}(x) = U_{k-1}(x)\, f(x) + V_{k-1}(x)\, g(x)$$
  with $deg(U_{k-1}(x)) < deg(g(x)) - deg(F_{k-1}(x))$
  $deg(V_{k-1}(x)) < deg(f(x)) - deg(F_{k-1}(x))$

- **Remark**. Under degree constraints, $u(x)$, $v(x)$ with $\gcd(f(x),g(x)) = u(x)f(x) + v(x)g(x)$ are unique.

(Sub)Resultant

- For $f(x) = a_m x^m + \ldots + a_1 x + a_0$, $g(x) = b_n x^n + \ldots + b_1 x + b_0$, $u(x)f(x) + v(x)g(x) = h(x)$ are described by a matrix M_j, where $deg(u(x)) \leqq n - j$, $deg(v(x)) \leqq m - j$.
  - ✓We know GCD $h(x)$ is unique $\Leftrightarrow$ $\det(M_j) \neq 0$.

Starting from $j = 0$, try until $\det(M_j) \neq 0$

This j is $\deg(h(x))+1$

$$M_j = \begin{pmatrix}
a_m & \cdots & \cdots & a_l & \cdots & a_0 & & \\
 & a_m & \cdots & \cdots & a_l & \cdots & a_0 & \\
 & & \ddots & & & \ddots & & \ddots \\
 & & & a_m & \cdots & \cdots & a_l & a_{l-1} \\
 & & & & a_m & \cdots & a_{l+1} & a_l \\
b_n & \cdots & \cdots & b_l & \cdots & b_0 & & \\
 & b_n & \cdots & \cdots & b_l & \cdots & b_0 & \\
 & & \ddots & & & \ddots & & \ddots \\
 & & & b_n & \cdots & \cdots & b_l & b_{l-1} \\
 & & & & b_n & \cdots & b_{l+1} & b_l
\end{pmatrix}
\begin{matrix}
\left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} n - j \\
\left.\vphantom{\begin{matrix}b\\b\\b\\b\\b\end{matrix}}\right\} m - j
\end{matrix}$$

The number of common roots

- Number of common roots (with duplication) of $f(x)$ and $g(x)$ is $\deg(\gcd(f(x),g(x)))$
- With higher differentials, the number of duplicated roots with higher multiplicity is computed by gcd.
- They are obtained by degree of gcd only.

  ⇒ Reduced to computation of resultants.
- During projections, boundary of decompositions is set at each point where the number of roots changes.

Example: enumerating common roots

- $f(x,y) = y^2 - (x^2 - 1)y + 1$, $g(x,y) = x^2 + y^2 - 4$
  - ✓ $\gcd(f_x(y), g_x(y)) = x^6 - 5x^4 - x^2 + 21$

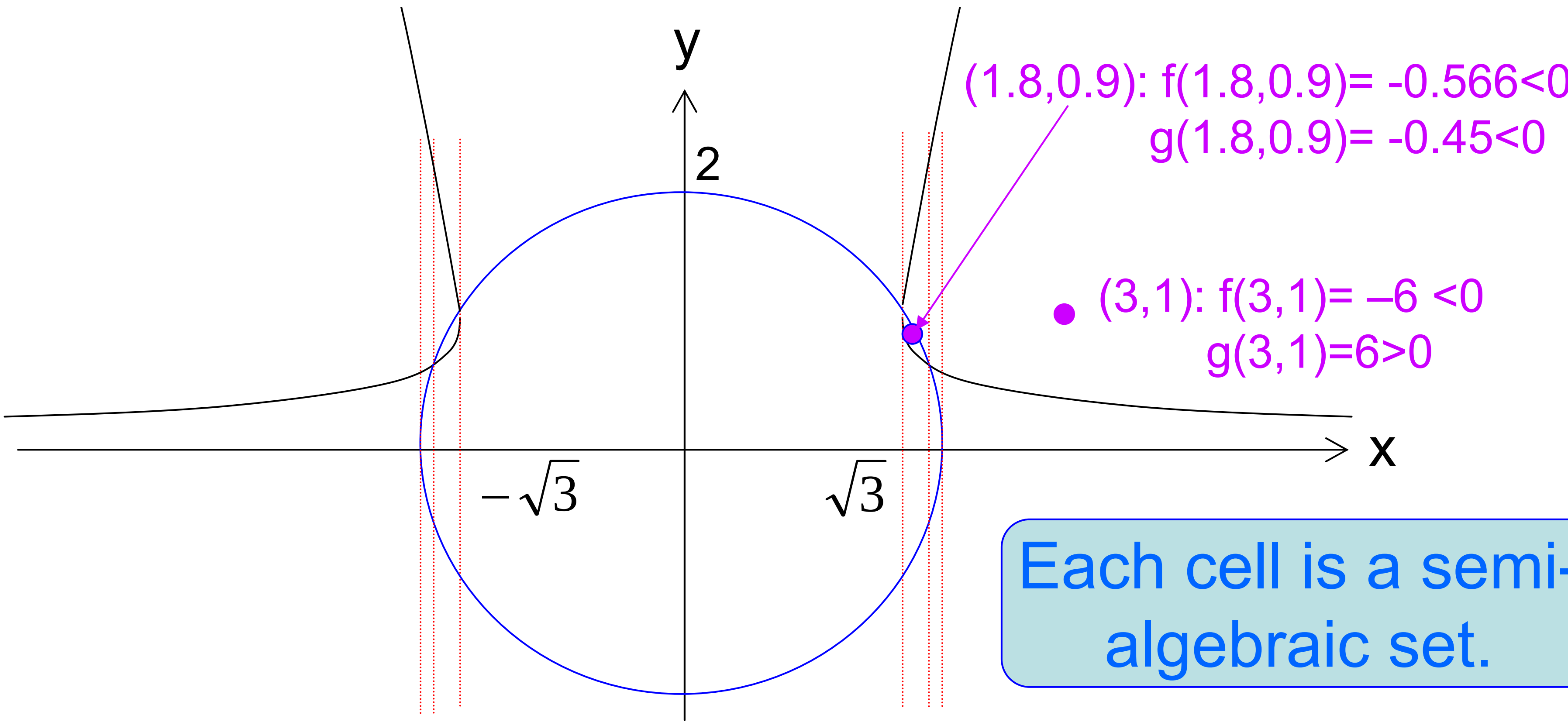
    $\rightarrow \deg(\gcd(f_x(y), g_x(y))) = \begin{cases} 0 \text{ if } x^6 - 5x^4 - x^2 + 21 \neq 0 \\ 1 \text{ if } x^6 - 5x^4 - x^2 + 21 = 0 \end{cases}$

    $\rightarrow$For $h(x) = x^6 - 5x^4 - x^2 + 21 = (x^2 - 3)(x^4 - 2x^2 - 7)$, $h(\pm\sqrt{3}) = h(\pm\sqrt{1+2\sqrt{2}}) = 0$. There is a common real root at $x = \pm\sqrt{3}$, $\pm\sqrt{1+2\sqrt{2}}$

    $\rightarrow$Cells are decomposed at $x = \pm\sqrt{3}$, $\pm\sqrt{1+2\sqrt{2}}$ when the projection to x is applied.

Example : Cylindrical decomposition

- For $f(x,y) = y^2 - (x^2 - 1)y + 1$, $g(x,y) = x^2 + y^2 - 4$,
  $\exists x \exists y.\ f(x,y)<0 \wedge g(x,y) < 0$?
  - ✓Each cylindrical cell has stable signs (of f and g), we will decide them by sampling.



Each cell is a semi-algebraic set.

Base phase

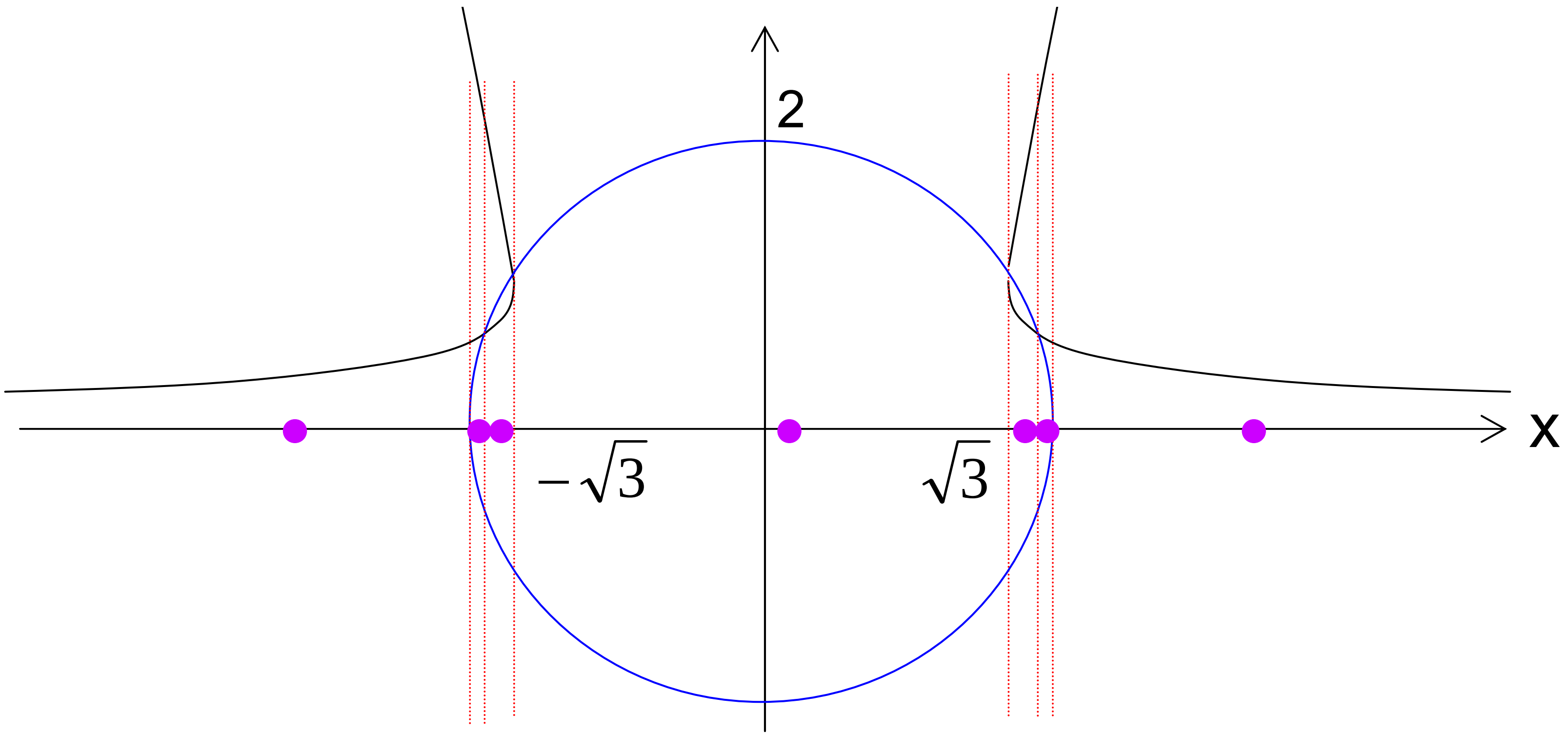
Compute sampling points

- Each cylindrical cell is guaranteed to keep sings of constraints and their differentials.
  - ✓Representatives by computing sample points.
  - ✓Better to have small denominators and numerators, especially 2 power denominators for shift operation.

- For inequalities, we can choose suitable rationals as sample points. For equalities, we need algebraic numbers.
  - ✓Representation: (Defining polynomial, [l, h])
  - ✓E.g., $\sqrt{3}$ is represented by ($x^2 - 3$, [1.7,1.8]))

Example: sampling

- For $f(x,y) = y^2 - (x^2 - 1)y + 1$, $g(x,y) = x^2 + y^2 - 4$, $\exists x \exists y.\ f(x,y)<0 \wedge g(x,y) < 0$?



Finding sample points

- How to find sampling points
  - ✓Estimation of upper / lower bounds of real roots.

    → For $f(x) = x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$ and a real root α, $|\alpha| \leqq \max(|a_0|, \ldots, |a_{m-1}|)$
  - ✓Decide the number of real roots.

    → Strum sequence (or, Fourier series)

- Then, by binary search, we can find sampling points, i.e., defining polynomial of (k real-)roots and

$$c_0 < \alpha_1 < c_1 < \ldots . < c_{k-1} < \alpha_k < c_k$$

Extended Euclidian Algorithm (again)

- **Extended Euclid**: For $F_0(x) = f(x)$, $F_1(x) = f'(x)$
  $U_0(x) = 1$, $U_1(x) = 0$, $V_0(x) = 0$, $V_1(x) = 1$, repeat
  ✓ $F_{i+1}(x) = F_{i-1}(x) - Q_i(x)\, F_i(x)$
  ✓ $U_{i+1}(x) = U_{i-1}(x) - Q_i(x)\, U_i(x)$
  ✓ $V_{i+1}(x) = V_{i-1}(x) - Q_i(x)\, V_i(x)$
  until $F_k(x) = 0$. Then, $F_{k-1}(x) = \gcd(f(x),g(x))$ and
  $$F_{k-1}(x) = U_{k-1}(x)\, f(x) + V_{k-1}(x)\, g(x)$$
  with $deg(U_{k-1}(x)) < deg(g(x)) - deg(F_{k-1}(x))$
  $deg(V_{k-1}(x)) < deg(f(x)) - deg(F_{k-1}(x))$

- Let $S_i(x) = -F_i(x)$ and $\mathcal{S}_i(x) = S_i(x)/S_{k-1}(x)$ for $2 \leqq i \leqq k-1$.

Strum's theorem

- **Notation**. $V_c(\mathcal{S})$ = var($\mathcal{S}_0$(c), $\mathcal{S}_1$(c), …, $\mathcal{S}_{k-1}$(c)), where var(a_0, a_1, …, a_{k-1}) is the number of the change of signs between neighborhoods (after removal of 0's).

  e.g., var(2,1,0,-1,3,5,0,4,,0,-2) = 3

- **Th**. (Strum 1835) For a < b with f(a),f(b) $\neq$ 0, the number of different real roots in (a,b] is $V_a(\mathcal{S}) - V_b(\mathcal{S})$.

- **Remark**. With a modified resultant, $V_a(\mathcal{S}) - V_b(\mathcal{S})$ can be computed.

Lifting phase

Lifting

- Lifting is finding sampling points over algebraic extensions.

- Lifting is the most heavy
  - ✓80-90% execution time devoted.
  - ✓Numeric method: approximation by intervals with validated numerics (Adam W.Strzebonski, CAD using validated numerics, JSC 41, pp.1021-1038, 2006)

Algebraic extensions

- Computing an algebraic number is computing a quotient of an ideal.
  - ✓E.g., $\mathbb{Q}(\sqrt{3})$ is equivalent to $\mathbb{Q}[z]/(z^2 - 3)$
- For higher degree formulae, we may need to repeat algebraic extensions.
  - ✓E.g., $f(x,y) = y^2 - (x^2 - 1)y + 1$, $g(x,y) = x^2 + y^2 - 4$, adding to $x^2 - 3$, we have $x^6 - 5x^4 - x^2 + 21$ (from $f(x,y) = 0$ and $g(x,y) = 0$, erasing y with $y^2 = 4 - x^2$)
  - ✓Thus, $\mathbb{Q}[z,w]/(z^2 - 3, w^6 - 5w^4 - w^2 + 21)$.

Groebner basis (Buchberger 65)

- Groebner basis is for computing quotient of ideals.
  - ✓ Starting from given basis of ideals (with WFO on monomials).
  - ✓ Completion for polynomial rewriting systems (PRS) until a confluent PRS (in which variables are not substituted and completion always succeed).

- Difference from Knuth-Bendix completion algorithm
  - ✓ Polynomial rewriting is not closed wrt context, e.g., $\{ x^2 \rightarrow y \}$, $s = x^2 + xy$, $t = xy + y$, $u = x^2 - xy$. Then, $s \rightarrow t$, but not $s + u \rightarrow t + u$.

A.Middeldorp, M.Starcevic, A rewrite approach to polynomial ideal theory, 1991

Groebner basis (Buchberger 65)

- Groebner basis is for computing quotient of ideals.
  - ✓Starting from given basis of ideals (with WFO on monomials).
  - ✓Completion for polynomials (in which variables are not substituted and completion always succeed).

- E.g., $\mathbb{Q}[z,w]/(z^2 - 3,\ zw^2 + 2w - 3z)$ with $w > z$.
  - →Regard them $z^2 \to 3$, $zw^2 \to -2w + 3z$
  - →Critical pair $(3w^2, -2zw + 3z^2)$
  - →New rule $3w^2 \to -2zw + 9$, …
  - →Finally, we obtain $z^2 \to 3$, $3w^2 \to -2zw + 9$ and $\mathbb{Q}[z,w]/(z^2 - 3,\ 3w^2 + 2zw - 9)$.

Middeldorp, Starcevic, A rewrite approach to polynomial ideal theory, 1991

Future of QE-CAD

- Hard to scale
  - ✓Double exponential to the number of variables. The current limit is 7-8 variables (say, degree 10).
  - ✓Groebner basis is not seriously used (rather by primitive elements).
  - ✓Combination with (under/over) approximation by validated numerics.

- Applications
  - ✓Quite successful PID control design of HDD head.
  - ✓Floating point roundoff errors