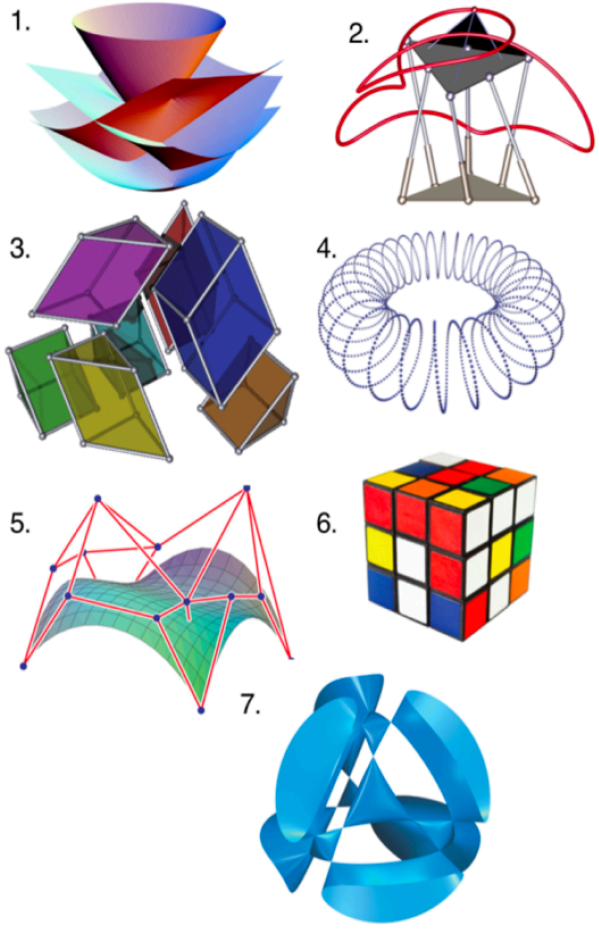
计算机代数

牟晨琪

北航沙河校区E403-7
chenqi.mou@buaa.edu.cn

2020年春



第四章

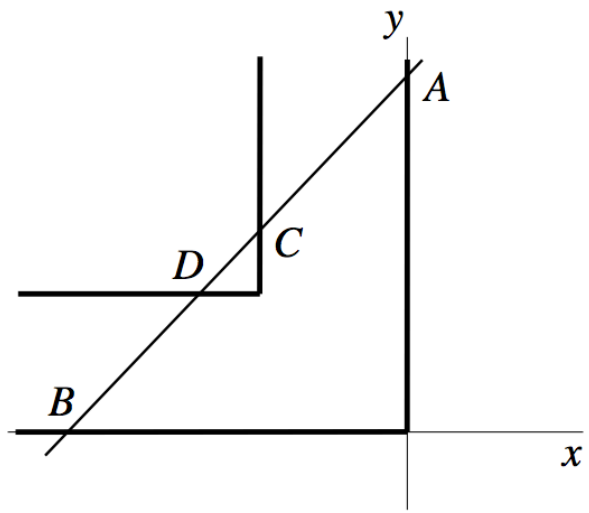
计算实代数几何

第四章

计算实代数几何

搬钢琴问题

问题：确定一把长度为 3、充分细的梯子能否穿过宽度为 1 的直角走廊的拐角



- **机器人运动规划**

走廊可以用下述集合表示

$$\left\{(x,y)\in\mathbf{R}^2 \mid \ x\leqslant 0,\, 0\leqslant y\leqslant 1\right\}\cup\left\{(x,y)\in\mathbf{R}^2 \mid \ y\geqslant 0,\, -1\leqslant x\leqslant 0\right\}$$

搬钢琴问题

容易发现，梯子不能穿过走廊的拐角当且仅当梯子与四面墙 $\{x=0, y\geqslant 0\}, \{y=0, x<0\}, \{x=-1, y\geqslant 1\}, \{y=1, x<-1\}$ 均相交.

- 设梯子与四面墙的交点为 $A(0,a), B(b,0), C(-1,c), D(d,1)$，则相应的约束条件为：

$$\begin{cases} a\geqslant 0,\ b<0,\ c\geqslant 1,\ d<-1, & (A,B,C,D \text{ 分别位于四面墙上}) \\ a^2+b^2\leqslant 9, & (|AB|\leqslant 3 = \text{梯子的长度}) \\ d-(1-a)(d-b)=0, & (A,D,B \text{ 三点共线}) \\ c-(1+b)(c-a)=0. & (A,C,B \text{ 三点共线}) \end{cases}$$

- 梯子无法通过等价于 (取实数值)

$$(\exists\, a,b,c,d)\,[a\geqslant 0\wedge b<0\wedge c\geqslant 1\wedge d<-1\wedge a^2+b^2\leqslant 9\wedge d-(1-a)(d-b)=0\wedge c-(1+b)(c-a)=0].$$

摄像机定位问题

问题：以平面截正四面体，问怎样的三角形截面可以将正四面体的一个顶点和其他三个顶点分居两侧？→ **摄像机定位问题**特例

- 设三角形截面的三边长为 $1, a, b$ (不妨设 $b \geqslant a \geqslant 1$)，而四面体的顶点距三角形的三个顶点的距离为 x, y, z，则问题变为计算下述系统关于变元 x, y, z 是否有实解

$$\begin{cases} H_1 = x^2 + y^2 - xy - 1 = 0, \\ H_2 = y^2 + z^2 - yz - a^2 = 0, \\ H_3 = z^2 + x^2 - zx - b^2 = 0, \\ x > 0, y > 0, z > 0, a - 1 \geqslant 0, b - a \geqslant 0, a - b + 1 > 0 \end{cases}$$

- 这等价于

$$(\exists x)\,(\exists y)\,(\exists z)\,[H_1 = 0 \wedge H_2 = 0 \wedge H_3 = 0 \wedge x > 0 \wedge y > 0 \wedge z > 0 \wedge a - 1 \geqslant 0 \wedge b - a \geqslant 0 \wedge a - b + 1 > 0]$$

量词消去的基本概念

如何将带量词的公式转化为等价的无量词公式：量词消去

高中！$\exists x\ ax^2 + bx + c = 0 \Leftrightarrow b^2 - 4ac \geqslant 0$

基本定义

- 变量：形如 x, y, z 的符号；代数常量：整数；代数运算符：指 $+, -$ 和 $\cdot$
- 代数项：由变量和代数常量通过代数运算符号连接得到的有意义的表达式
- 二元关系运算符：$=, \neq, >, <, \leqslant$ 和 $\geqslant$
- 原子公式：形如 $P \sim 0$ 的表达式，其中 P 为代数项，$\sim$ 表示某个二元关系运算符
- 逻辑联结词：包含 $\vee$ (或)，$\wedge$ (且) 和 $\neg$ (非)；
- Tarski 公式：通过逻辑联结词和量词 ($\exists$, $\forall$) 将原子公式连接而成的表达式.
- $\rightarrow, \leftrightarrow$：$A \rightarrow B := A \wedge \neg B$，$A \leftrightarrow B := A \rightarrow B \wedge B \rightarrow A$

量词消去的基本概念

示例

- x, $x+y$, $(x+y)\cdot z$ 都是代数项
- $x+$, $x+\sqrt{3}$ 不是代数项, 因为 $x+$ 是无意义的表达式, $x+\sqrt{3}$ 含有非法符号 $\sqrt{3}$.
- 原子公式:
  - $0=0$
  - $1+1\neq 0$
  - $x^2+y-x>0$
  - $x^3+x<0$
  - $x+xy+y^2\leqslant 0$
- Tarski 公式:
  - $0=0$
  - $(\exists\, x)[x^2-1=0]$
  - $(x=0)\vee(\exists\, y)[x-y=0]$
  - $(\exists\, x)\neg(\exists\, y)\neg\big[(x-y=0)\wedge(x-(1+y)>0)\big]$
  - $\neg(x-1>0)\wedge(\exists\, y)[x-y^2=0]$

量词消去的定义

无量词公式

称不含量词的 Tarski 公式为无量词公式 (quantifier-free formula).

- 例如 $(x > 0) \wedge (x^2 - 2 = 0)$ 为无量词公式, 它定义了 $\mathbb{R}$ 中的无理数 $\sqrt{2}$.

量词消去

给定一含量词 $(\forall, \exists)$ 的 Tarski 公式, 求一个与之等价的无量词公式.

- 例如, 对 $(\forall x)[ax^2 + bx + c > 0]$ 约化可得到等价的无量词公式

量词消去的定义

无量词公式

称不含量词的 Tarski 公式为无量词公式 (quantifier-free formula).

- 例如 $(x > 0) \wedge (x^2 - 2 = 0)$ 为无量词公式, 它定义了 $\mathbb{R}$ 中的无理数 $\sqrt{2}$.

量词消去

给定一含量词 $(\forall, \exists)$ 的 Tarski 公式, 求一个与之等价的无量词公式.

- 例如, 对 $(\forall x)[ax^2 + bx + c > 0]$ 约化可得到等价的无量词公式 $(a > 0) \wedge (b^2 - 4ac < 0)$.

问题: 是否量词消去总能进行?

Taski 定理

定理

设 $\Phi = (\exists_k x)[\Phi_1 \wedge \cdots \wedge \Phi_r]$, 其中 Φ_i 形如 $F = 0$ 或 $F > 0$, 则存在有效算法来计算与 Φ 等价的无量词公式.

不含自由变量的 Tarski 公式称为 Tarski 命题或初等代数命题.

- 例: $(\forall a)[a^2 - 2a < 0]$ 或 $a \neq 0 \to ax + b = 0$ 有一根
- 初等代数命题均可判断真假

Tarski 定理

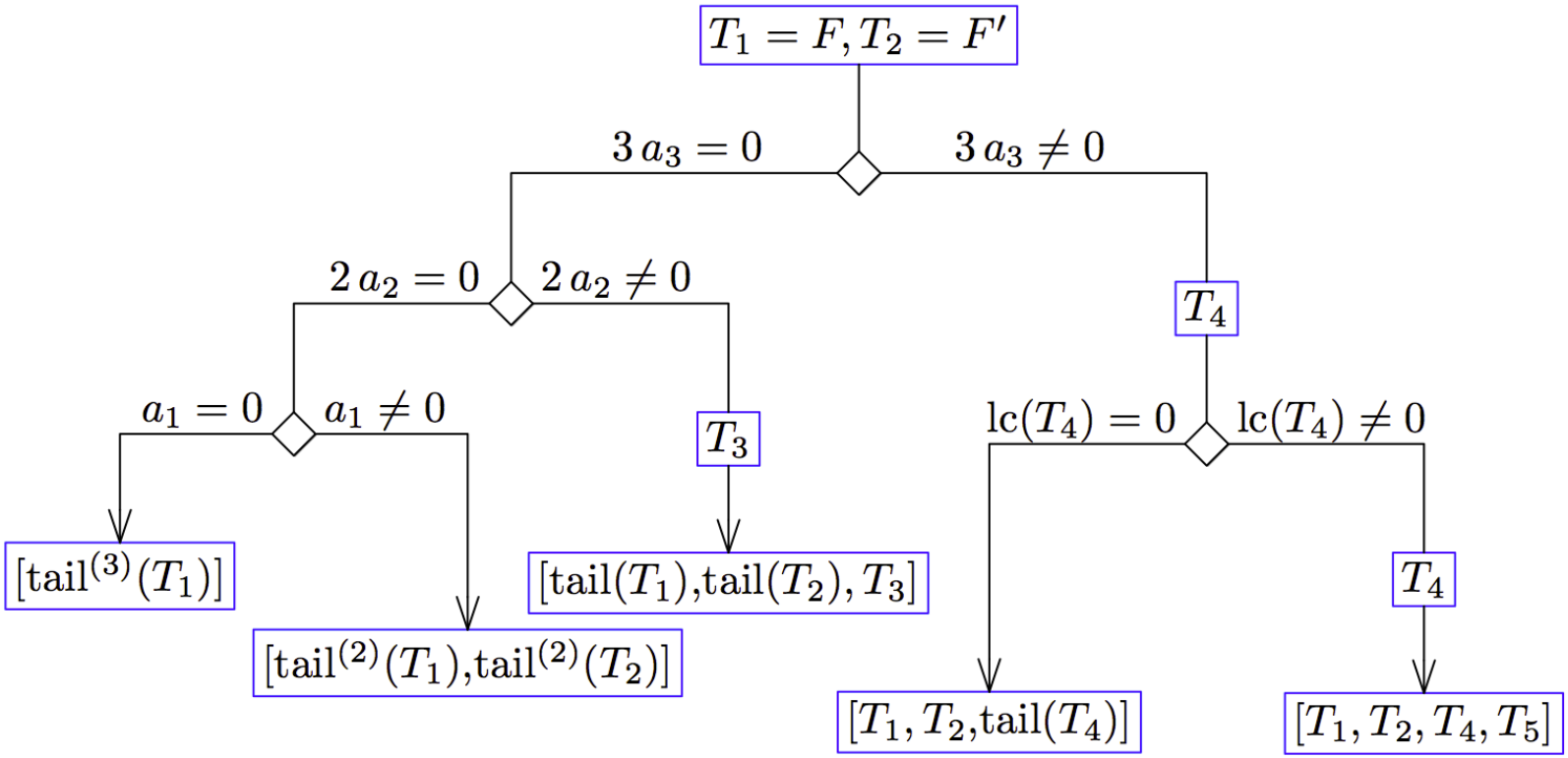
设 Φ 为初等代数命题, 则存在有效的判定算法来判定 Φ 的真假.

- 量词使得命题真假难以确定 $\Rightarrow$ 量词消去 $\Rightarrow$ 可以判定
- 实几何中初等问题的可判定性：Hilbert, Gödel, Tarski
- 构造性方法，但复杂度太高

Tarski 方法示例

示例

设 $F = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$, 下求与公式 $\Phi = (\exists\, x)[F = 0]$ 等价的无量词公式.



Tarski 方法示例

示例

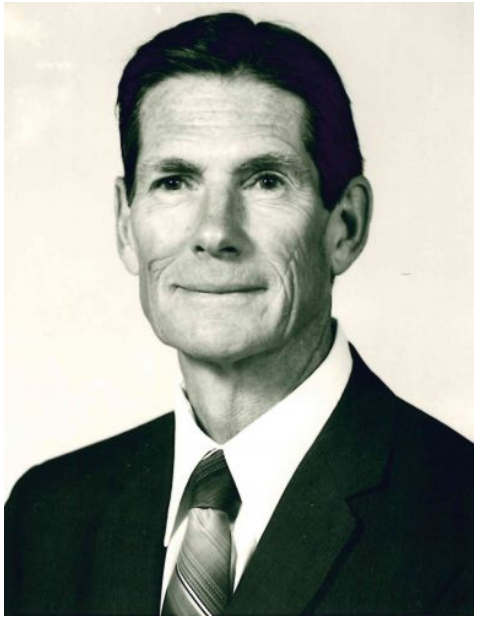
设 $F = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$, 下求与公式 $\Phi = (\exists\, x)[F = 0]$ 等价的无量词公式.

- 结果

$$\begin{aligned}\phi =&[(a_3 = 0) \wedge (a_2 = 0) \wedge (a_1 \neq 0)] \vee \\ &[(a_3 = 0) \wedge (a_2 \neq 0) \wedge (a_1^2 - 4\, a_0\, a_2 \geqslant 0)] \vee \\ &[(a_3 \neq 0) \wedge (3\, a_1\, a_3 - a_2^2 = 0)] \vee \\ &[(a_3 \neq 0) \wedge (3\, a_1\, a_3 - a_2^2 \neq 0) \wedge (T_5'/a_3 \leqslant 0)].\end{aligned}$$

- 其中 T_5' 为 Tarski 构造过程所计算出的某个多项式

柱形代数分解



George E. Collins (1928–2017)

He is the inventor of garbage collection by reference counting and of the method of quantifier elimination by cylindrical algebraic decomposition.

半代数集

半代数集

设 $S \subseteq \mathbb{R}^n$. 若 S 可由

$$\bigcup_{i=1}^{s} \bigcap_{j=1}^{t_i} \{\boldsymbol{a} \in \mathbb{R}^n : F_{ij}(\boldsymbol{a}) \sim 0\}$$

表示, 其中 $F_{ij} \in \mathbb{R}[\boldsymbol{x}]$, $\sim \in \{=, >, <, \geqslant, \leqslant, \neq\}$, 则称 S 为 $\mathbb{R}^n$ 中的半代数集 (semi-algebraic set), 并将 $\{F_{ij} : 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t_i\}$ 称为 S 的定义多项式组.

半代数集的基本性质

半代数集的基本性质

1. 设 $P \in \mathbb{R}[\boldsymbol{x}]$, 则 $\{\boldsymbol{a} \in \mathbb{R}^n : P(\boldsymbol{a}) = 0\}$ 和 $\{\boldsymbol{a} \in \mathbb{R}^n : P(\boldsymbol{a}) > 0\}$ 是半代数集.
2. 设 S_1, S_2 为半代数集, 则 $S_1 \cap S_2$, $S_1 \cup S_2$ 及 $\mathbb{R}^n \setminus S_1$ 也是半代数集. (交、并、补)
3. 设 S_1 和 S_2 分别为 $\mathbb{R}^n$ 和 $\mathbb{R}^m$ 中的半代数集, 则 $S_1 \times S_2$ 是 $\mathbb{R}^n \times \mathbb{R}^m$ 中的半代数集.(笛卡尔积)

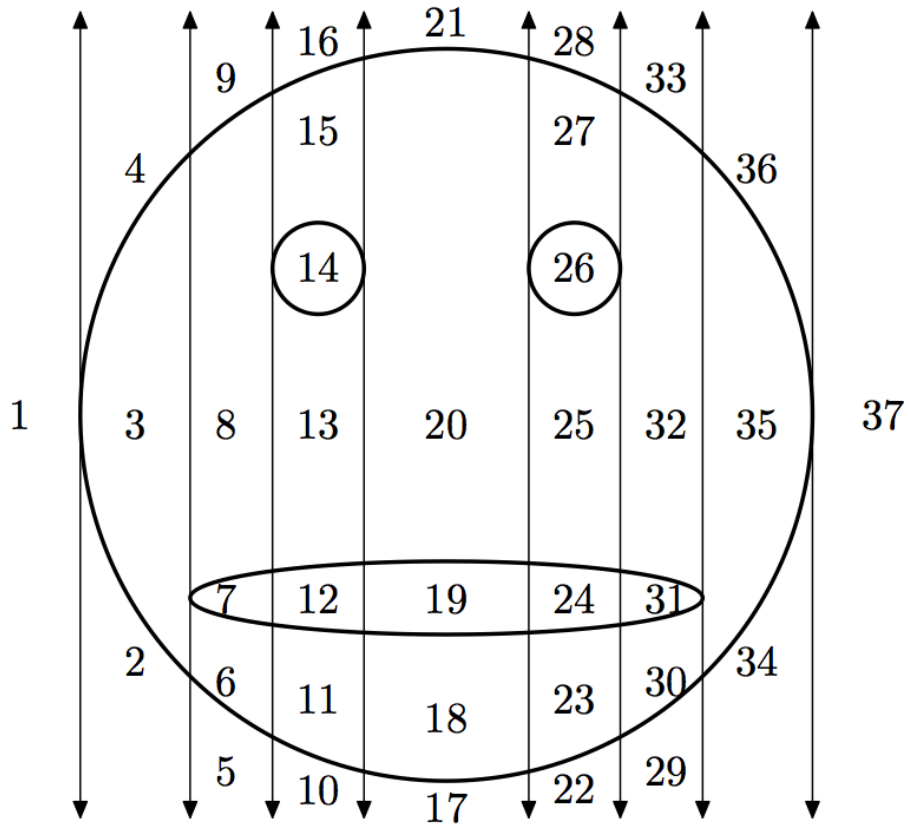
示例

1. $\mathbb{R}$ 中的半代数集是有限个点和开区间的并.
2. 设 S 为 $\mathbb{R}^n$ 中的半代数集, σ 为 $\mathbb{R}^n$ 到 $\mathbb{R}^s$ 的映射, 并且 $\sigma(\boldsymbol{x}) = (F_1, \ldots, F_s)$, $F_i \in \mathbb{R}[\boldsymbol{x}]$ $(1 \leqslant i \leqslant s)$, 则 $\sigma(S)$ 也为半代数集.

柱形代数分解: 大意

设 $\mathcal{F} = \{F_1, \ldots, F_s\} \subseteq \mathbb{R}[\boldsymbol{x}]$, 利用 $\mathcal{F}$ 对 $\mathbb{R}^n$ 进行柱形代数分解就是要从 $\mathcal{F}$ 构造出一个 $\mathbb{R}^n$ 的有限胞腔分解, 并且在每个胞腔上 $\mathcal{F}$ 中所有多项式的符号恒定。

- 验证符号只需在每个胞腔中取样本点



柱形代数分解：步骤

Tarski–Seidenberg 定理

将 $\mathbb{R}^n$ 中的半代数集投影到 $\mathbb{R}^{n-1}$ 上仍得到半代数集.

计算 $\mathbb{R}^n$ 的一个 $\mathcal{F}$ 的柱形代数分解及其样本的步骤.

1. 投影：将一个半代数集通过连续的投影得到新的半代数集，在投影的过程中半代数集的维数依次递减. 设初始半代数集是在 $\mathbb{R}^n$ 中定义的，则依次投影直至得到 $\mathbb{R}$ 上的一元多项式.
2. 一元情形：投影完成后，利用对投影得到的一元多项式的根来分解 $\mathbb{R}$，从而得到包含一维胞腔 (区间) 和零维胞腔 (孤立点) 的 $\mathbb{R}$ 的分解.
3. 提升：此后，可以逐次将 $\mathbb{R}^r$ 的胞腔分解提升为 $\mathbb{R}^{r+1}$ 的胞腔分解，直到提升至 $\mathbb{R}^n$ 为止.
4. 测试点：在每个胞腔上选取一个样本点检验命题成立与否.

柱形代数分解：胞腔

定义：胞腔

称 $\mathbb{R}$ 中的一个开区间或某一点为一维胞腔 (1-dimensional cell). 设 $S \subseteq \mathbb{R}^{n-1}$ 为 $n-1$ 维胞腔, 则称形如

$$\{(\bar{\boldsymbol{x}}, y) : \bar{\boldsymbol{x}} \in S,\ y = f(\bar{\boldsymbol{x}})\} \quad 或 \quad \{(\bar{\boldsymbol{x}}, y) : \bar{\boldsymbol{x}} \in S, f(\bar{\boldsymbol{x}}) < y < g(\bar{\boldsymbol{x}})\}$$

的集合为 n 维胞腔 (n-dimensional cell), 其中 f, g 为 $\pm\infty$ 或使得 $f(\bar{\boldsymbol{x}}) < g(\bar{\boldsymbol{x}})$ $(\forall \bar{\boldsymbol{x}} \in S)$ 成立的连续实值函数.

- 若存在 $F, G \in \mathbb{R}[\boldsymbol{x}, y]$ 使得 $F(\boldsymbol{x}, f(\boldsymbol{x})) = 0$, $G(\boldsymbol{x}, g(\boldsymbol{x})) = 0$, 则称如上定义的胞腔为代数胞腔 (algebraic cell).

代数叠加

设 $n-1$ 维区域 S 上有连续实值函数 $-\infty = f_0 < f_1 < \cdots < f_l < f_{l+1} = +\infty$, 并且对任意 i $(1 \leqslant i \leqslant l)$ 都存在 $F_i \in \mathbb{R}[\boldsymbol{x}, y]$ 使得 $F(\boldsymbol{x}, f_i(\boldsymbol{x})) = 0$, 则由 f_i 和 (f_i, f_{i+1}) $(0 \leqslant i \leqslant l)$ 可以确定柱形 $Z(S)$ 的一个代数分解, 称该分解为 S 上的一个由 $f_1, \ldots, f_l$ 定义的代数叠加.

柱形代数分解：定义

$\mathbb{R}^n$ 的柱形代数分解 (cylindrical algebraic decomposition) 可以递归定义如下:

1. 当 $n = 1$ 时, $\mathbb{R}$ 可分解为有限个实代数数, 设为 $a_1 < \cdots < a_t$ 以及由这些实代数数界定的有界和无界的开区间, 则所得到的柱形代数分解为

$$((-\infty, a_1), [a_1, a_1], \cdots, (a_{i-1}, a_i), [a_i, a_i], (a_i, a_{i+1}), \ldots, [a_t, a_t], (a_t, +\infty)).$$

2. 当 $n > 1$ 时, 存在 $\mathbb{R}^{n-1}$ 的一个柱形代数分解 $\mathcal{C}_{n-1} = (S_1, \ldots, S_l)$ 使得

$$\mathcal{C}_n = (S_{1,1}, \ldots, S_{1,2\,m_1+1}, \ldots, S_{l,1}, \ldots, S_{l,2\,m_l+1}),$$

这里, 对任意 i $(1 \leqslant i \leqslant l)$, $(S_{i,1}, \ldots, S_{i,2\,m_i+1})$ 都是 S_i 上的一个代数叠加. 此时, $\mathcal{C}_{n-1}$ 称为 $\mathcal{C}_n$ 诱导的 $\mathbb{R}^{n-1}$ 上的柱形代数分解.

柱形代数分解：$n = 1$

设 $\mathbb{R}$ 中的半代数集 S 由 $\mathcal{F} = \{F_i \in \mathbb{R}[x] : 1 \leqslant i \leqslant s\}$ 定义. 令 $F = \prod_{i=1}^{s} F_i$, 又设 F 的互异实根为 $a_1, \ldots, a_t$, 并且

$$a_1 < \cdots < a_{i-1} < a_i < a_{i+1} < \cdots < a_t.$$

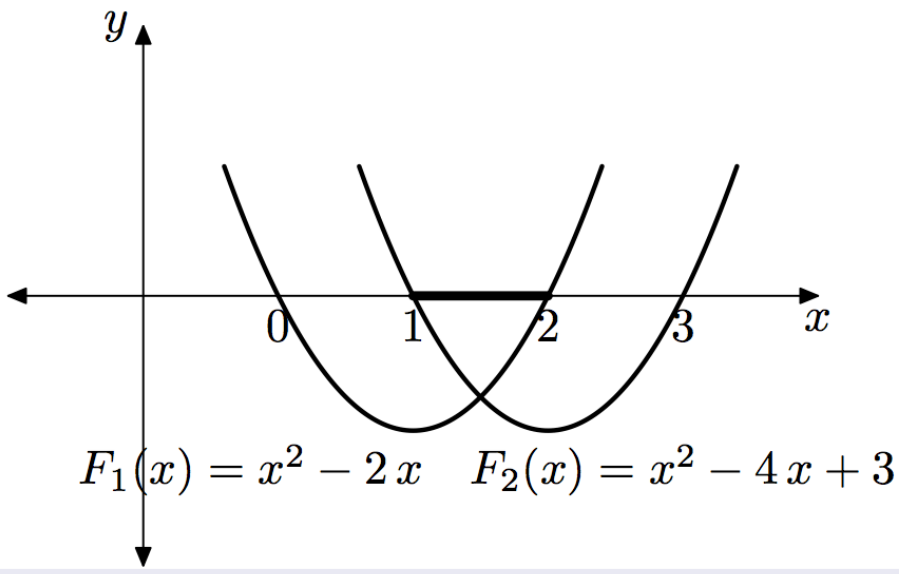
于是, $\mathbb{R}$ 的柱形代数分解为

$$((-\infty, a_1), [a_1, a_1], \ldots, (a_{i-1}, a_i), [a_i, a_i], (a_i, a_{i+1}), \ldots, [a_t, a_t], (a_t, +\infty)).$$

对应样本点的选取方法为:

1. $(-\infty, a_1)$ 和 $(a_t, +\infty)$ 的样本点分别取为 $a_1 - 1$ 和 $a_t + 1$
2. 对于有限长度的一维胞腔 (a_i, a_{i+1}), 样本点取为区间中点
3. 零维胞腔 $[a_i, a_i]$, 样本点即为 a_i.

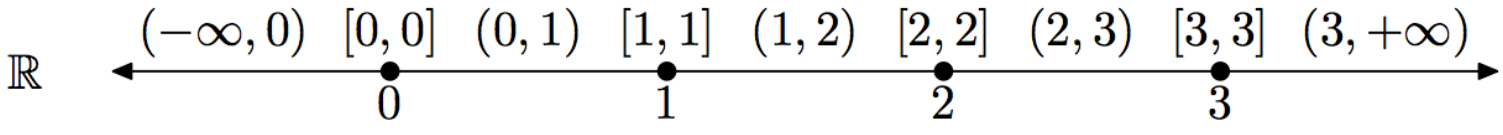
柱形代数分解：$n = 1$



对于 $F_1 = x^2 - 2x$, $F_2 = x^2 - 4x + 3$, 一维数轴 $\mathbb{R}$ 实施柱形代数分解可得到 5 个一维胞腔和 4 个零维胞腔, 分别为

$$(-\infty, 0), [0, 0], (0, 1), [1, 1], (1, 2), [2, 2], (2, 3), [3, 3], (3, +\infty),$$

对应的样本点可选为 $-1, 0, 1/2, 1, 3/2, 2, 5/2, 3, 4$.



柱形代数分解：投影

以 $\mathbb{R}^2$ 向 $\mathbb{R}$ 的投影为例：

投影算子

设 $\mathcal{F} = \{F_1, \ldots, F_s\} \subseteq \mathbb{R}[x, y]$, F_i $(1 \leqslant i \leqslant s)$ 无平方且两两互素. 定义 $\mathcal{F}$ 的投影算子 (projection operator) 为

$$\begin{aligned} \mathrm{proj}(\mathcal{F}) := \ & \{\mathrm{lc}(F_i, y) : 1 \leqslant i \leqslant s\} \cup \\ & \{\mathrm{disc}(F_i, y) : 1 \leqslant i \leqslant s\} \cup \\ & \{\mathrm{res}(F_i, F_j, y) : 1 \leqslant i < j \leqslant s\}. \end{aligned}$$

- $\mathrm{lc}(F_i, y)$: F_i 关于 y 的首项系数
- $\mathrm{disc}(F_i, y)$: F_i 关于 y 的判别式 (一元二次方程判别式的推广)
- $\mathrm{res}(F_i, F_j, y)$: F_i 和 F_j 关于 y 的结式

投影算子可以保证由 $\mathbb{R}^n$ 到 $\mathbb{R}^{n-1}$ 的合理映射: 可提升!

柱形代数分解：提升

已有 $\mathbb{R}^{r-1}$ 的柱形代数分解为 $\mathcal{C}_{r-1} = (S_1, \ldots, S_m)$. 对 $\mathcal{C}_{r-1}$ 中的任意 k 维胞腔 S_i, 都可构造 $k+1$ 维集合 $\{(\boldsymbol{p}, x_r) \in \mathbb{R}^r : \boldsymbol{p} \in S_i\}$, 其中 $\boldsymbol{p} = (\bar{x}_1, \ldots, \bar{x}_{r-1}) \in \mathbb{R}^{r-1}$.

$\mathbb{R}^r$ 的柱形代数分解 $\mathcal{C}_r$ 的构造过程

对任意 $F \in \mathcal{F}_r$, 令 f_j 为使得 $F(\boldsymbol{p}, f_j(\boldsymbol{p})) = 0$ $(1 \leqslant j \leqslant m_i,\ m_i = \#\mathcal{F}_r)$ 成立的连续实值函数, 并且对任意 $\boldsymbol{p} \in S_i$ 都有 $f_j(\boldsymbol{p}) < f_{j+1}(\boldsymbol{p})$ 成立, 则 $\mathbb{R}^r$ 上的柱形代数分解 $\mathcal{C}_r$ 可定义为 $(S_{1,1}, \ldots, S_{1,2\,r_1+1}, \ldots, S_{m,1}, \ldots, S_{m,2\,r_m+1})$, 其中

$$
\begin{aligned}
S_{i,1} &= \{(\boldsymbol{p}, x_r) \in \mathbb{R}^r : \boldsymbol{p} \in S_i, x_r < f_1(\boldsymbol{p})\},\\
S_{i,2\,j} &= \{(\boldsymbol{p}, x_r) \in \mathbb{R}^r : \boldsymbol{p} \in S_i, x_r = f_j(\boldsymbol{p})\}\ (1 \leqslant j \leqslant r_i),\\
S_{i,2\,j+1} &= \{(\boldsymbol{p}, x_r) \in \mathbb{R}^r : \boldsymbol{p} \in S_i, f_j(\boldsymbol{p}) < x_r < f_{j+1}(\boldsymbol{p})\}\ (1 \leqslant j < r_i),\\
S_{i,2\,r_i+1} &= \{(\boldsymbol{p}, x_r) \in \mathbb{R}^r : \boldsymbol{p} \in S_i, f_{r_i}(\boldsymbol{p}) < x_r\}.
\end{aligned}
$$

柱形代数分解：样本点

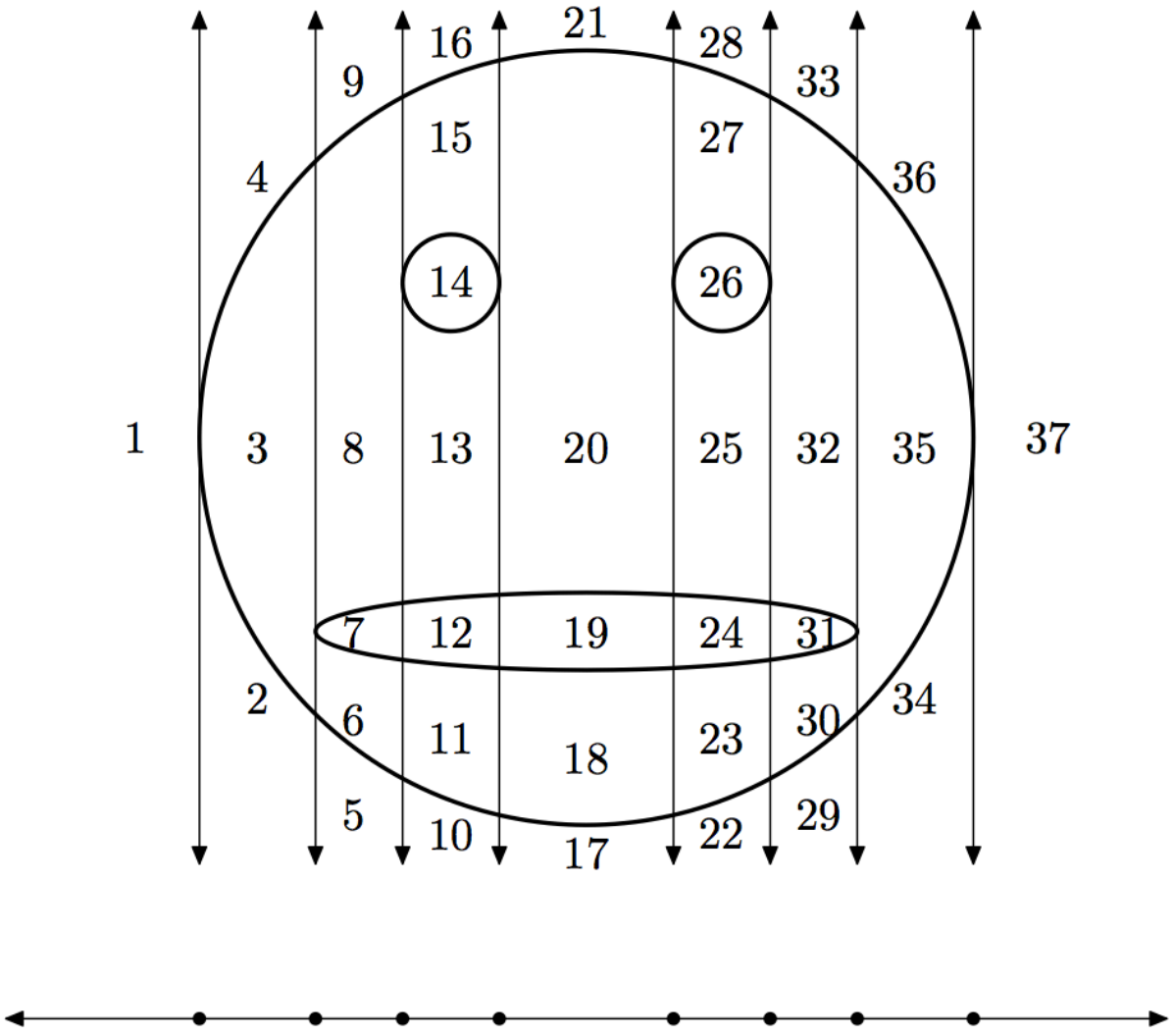
设 $\mathbb{R}^{r-1}$ 的柱形分解的样本为 $S'_{\mathrm{sp}} = (\boldsymbol{s}_1, \ldots, \boldsymbol{s}_m)$, 则 $\mathbb{R}^r$ 的柱形分解样本

$$S_{\mathrm{sp}} = (\boldsymbol{s}_{1,1}, \ldots, \boldsymbol{s}_{1,2\,r_1+1}, \ldots, \boldsymbol{s}_{m,1}, \ldots, \boldsymbol{s}_{m,2\,r_m+1})$$

可以通过下列步骤构造:

1. $\boldsymbol{s}_{i,j}$ 的前 $r-1$ 个坐标取 $\boldsymbol{s}_i$ 的相应坐标;
2. $\boldsymbol{s}_{i,1}$ 的第 r 个坐标可取为 $f_1(\boldsymbol{s}_i) - 1$;
3. $\boldsymbol{s}_{i,2\,j}$ 的第 r 个坐标可取为 $f_j(\boldsymbol{s}_i)$ $(1 \leqslant j \leqslant r_i)$;
4. $\boldsymbol{s}_{i,2\,j+1}$ 的第 r 个坐标可取为 $\frac{1}{2}(f_j(\boldsymbol{s}_i) + f_{j+1}(\boldsymbol{s}_i))$ $(1 \leqslant j < r_i)$;
5. $\boldsymbol{s}_{i,2r_i+1}$ 的第 r 个坐标可取为 $f_{r_i}(\boldsymbol{s}_i) + 1$.

柱形代数分解：示例



- 37 个 2 维胞腔, 64 个一维胞腔和 28 个零维胞腔

柱形代数分解：示例

令 $\mathcal{F} = \{x^2 + y^2 - 1\}$. 对 $\mathcal{F}$ 进行连续投影可以得到 $\mathcal{F}_2 = \{F_2\}, \mathcal{F}_1 = \{F_1\}$, 其中 $F_2 = x^2 + y^2 - 1, F_1 = x^2 - 1$. 通过计算可得 F_1 的实根为 $-1, 1$, 所以 $\mathbb{R}$ 的 $\mathcal{F}$ 不变号的分解为 $\mathcal{C}_1 = (S_1, \ldots, S_5)$, 这里

$$S_1 = [-2, F_1 > 0], \quad S_2 = [-1, F_1 = 0], \quad S_3 = [0, F_1 < 0],$$
$$S_4 = [1, F_1 = 0], \quad S_5 = [2, F_1 > 0].$$

下面以 S_1, S_2 和 S_3 为例来说明如何将 $\mathcal{C}_1$ 提升为 $\mathbb{R}^2$ 上的柱形分解. 将 $x = -2$ 代入 F_2 可知 F_2 无实根, 因此将 S_1 提升后对应的柱形分解为 $[(-2, 0), F_1 > 0 \wedge F_2 > 0]$. 将 $x = -1$ 代入 F_2 得到 S_2 提升后对应的柱形分解为

$$([(-1, -1), F_1 = 0 \wedge F_2 > 0], \ [(-1, 0), F_1 = 0 \wedge F_2 = 0],$$
$$[(-1, 1), F_1 = 0 \wedge F_2 > 0]).$$

柱形代数分解：示例

将 $x=0$ 代入 F_2 并求得其实根为 $-1,1$. 于是可得 S_3 提升后的柱形分解为

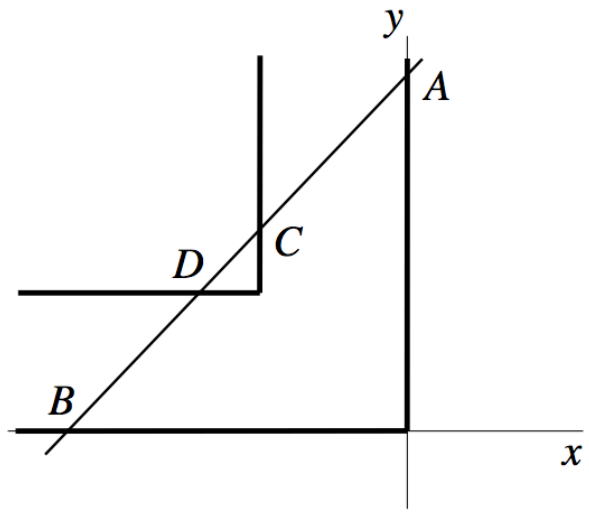
$$([(0,-2),F_1<0\wedge F_2>0],\ [(0,-1),F_1<0\wedge F_2=0],$$
$$[(0,0),F_1<0\wedge F_2<0],\ [(0,1),F_1<0\wedge F_2=0],$$
$$[(0,2),F_1<0\wedge F_2>0]).$$

类似地得到 S_4 和 S_5 的提升, 于是可得 $\mathbb{R}^2$ 的一个柱形代数分解为

$$S_{1,1}=[(-2,0),F_1>0\wedge F_2>0],\ S_{2,1}=[(-1,-1),F_1=0\wedge F_2>0],$$
$$S_{2,2}=[(-1,0),F_1=0\wedge F_2=0],\ S_{2,3}=[(-1,1),F_1=0\wedge F_2>0],$$
$$S_{3,1}=[(0,-2),F_1<0\wedge F_2>0],\ S_{3,2}=[(0,-1),F_1<0\wedge F_2=0],$$
$$S_{3,3}=[(0,0),F_1<0\wedge F_2<0],\ S_{3,4}=[(0,1),F_1<0\wedge F_2=0],$$
$$S_{3,5}=[(0,2),F_1<0\wedge F_2>0],\ S_{4,1}=[(1,-1),F_1=0\wedge F_2>0],$$
$$S_{4,2}=[(1,0),F_1=0\wedge F_2=0],\ S_{4,3}=[(1,1),F_1=0\wedge F_2>0],$$
$$S_{5,1}=[(2,0),F_1>0\wedge F_2>0]).$$

搬梯子问题

问题：长度为 3 的梯子能否穿过宽度为 1 的直角走廊的拐角



$$(\exists\, a, b, c, d)\,[a \geqslant 0 \wedge b < 0 \wedge c \geqslant 1 \wedge d < -1 \wedge a^2 + b^2 \leqslant 9 \wedge$$
$$d - (1 - a)\,(d - b) = 0 \wedge c - (1 + b)\,(c - a) = 0].$$

- 柱形代数分解方法: 不能通过拐角
- 进一步假设梯子的长度 r 未知，则可以得到类似的梯子无法通过的公式，利用柱形代数分解可以得到：

$$r^2 > 8 \wedge r > 2.$$

即梯子能通过当且仅当$r \leqslant 2\sqrt{2}$.

几何对象的包含

椭圆和圆的包含

考虑中心在 $(c,0)$、两个轴平行于坐标轴而半轴长分别为a, b的椭圆和圆心在原点的单位圆. 试给出椭圆完全包含在单位圆内（含相切）的充要条件.

椭圆上的点满足 $F(x,y)=0$, 其中$F(x,y)=(x-c)^2/a^2+y^2/b^2-1$, 而包含在单位圆指 $G(x,y)\leqslant 0$, 其中$G(x,y)=x^2+y^2-1$. 因此问题变为公式

$$(\forall x)(\forall y)[F(x,y)=0\Rightarrow G(x,y)\leqslant 0].$$

几何对象的包含：CAD 求解

该公式可以进一步化简为

$$(\forall x)\,(\forall y)\,[0 < a \leqslant 1 \wedge 0 < b \leqslant 1 \wedge 0 \leqslant c \leqslant 1 - a \wedge \\ c - a < x < c + a \wedge F(x, y) = 0 \Longrightarrow G(x, y) \leqslant 0]$$

利用柱形代数分解计算上式的等价无量词公式

$$[b^2 - a \leqslant 0 \vee a^2 - a^2b^2 - b^2 + b^2c^2 + b^4 \leqslant 0] \wedge \\ c + a - 1 \leqslant 0 \wedge c \geqslant 0 \wedge a - 1 \leqslant 0 \wedge a > 0 \wedge b - 1 \leqslant 0 \wedge b > 0.$$

不等式的机器证明

判断多项式的正定性

$$(\forall x)(\forall y)\,[x^6 - x^4y^2 - x^2y^4 + y^6 - x^4 + 3\,x^2y^2 - y^4 - x^2 - y^2 + 1 \geqslant 0].$$

令 F 为上述公式中出现的多项式，则经过投影步骤得到如下一元多项式

$$G = 64x^6(x-1)^6(x+1)^6(5 - 25x^2 + 32x^4)^2.$$

因此 G 的实根为 $-1, 0, 1$. 因此可令样本点为

$$-2, -1, -1/2, 0, 1/2, 1, 2.$$

经过提升步骤后最终共得到23 个样本点：一一验证 F 在这 23 个样本点处的符号，发现F 是半正定的。

柱形代数分解：一元方程的解？

柱形代数分解：$n = 1$

设 $\mathbb{R}$ 中的半代数集 S 由 $\mathcal{F} = \{F_i \in \mathbb{R}[x] : 1 \leqslant i \leqslant s\}$ 定义. 令 $F = \prod_{i=1}^{s} F_i$, 又设 F 的互异实根为 $a_1, \ldots, a_t$, 并且

$$a_1 < \cdots < a_{i-1} < a_i < a_{i+1} < \cdots < a_t.$$

于是, $\mathbb{R}$ 的柱形代数分解为

$$((-\infty, a_1), [a_1, a_1], \ldots, (a_{i-1}, a_i), [a_i, a_i], (a_i, a_{i+1}), \ldots, [a_t, a_t], (a_t, +\infty)).$$

- 如何无误差地计算一元多项式的互异实根?

数值算法的一些问题

- $F(x) = (x+1)(x+2)\cdots(x+20)$: 20个实根，$F(x) - 10^{-9}x^{19}$ 却只有14个实根
- The zero problem: 例如 $\sqrt{2} + \sqrt{3} - \sqrt{5 + 2\sqrt{6}} = 0$?
- $F(x) = 0$?

实根隔离

求 $\mathbb{R}$ 上一列互不相交的有理区间使其包含给定多项式的所有实根, 并且每个区间恰含一个根 (重根看作一个).

算法 31 实根隔离 $L :=$RealIsol(F)

输入: 无平方多项式 $F \in \mathbb{R}[x], \deg(F) = m$.
输出: F 的实根隔离区间列 L.

$\mathcal{S} :=$ F 的 Sturm 序列;
$b :=$ F 根的界; $a := -b$;
$N := \mathrm{var}(\mathcal{S}, a) - \mathrm{var}(\mathcal{S}, b)$;
if $N = 0$ **then return** $\emptyset$;
$i := 1$; $L := \emptyset$;
$a_i := a$; $b_i := b$;
while $i \leqslant N$ **do**
  while $\mathrm{var}(\mathcal{S}, a_i) - \mathrm{var}(\mathcal{S}, b_i) > 1$ **do**
    $c := (a_i + b_i)/2$;
    if $\mathrm{var}(\mathcal{S}, a_i) - \mathrm{var}(\mathcal{S}, c) \geqslant 1$ **then**
      $b_i := c$;
    else
      $a_i := c$;
    end
  end
  $L := L \cup \{[a_i, b_i]\}$;
  $i := i + 1$;
  $a_i := b_{i-1}$; $b_i := b$;
end
return L;

实根隔离算法

一元实系数多项式根的界

给定 $F \in \mathbb{R}[x]$, 首先需要找到包含 F 所有实根的区间, 即找到 $M > 0$, 使得F 的所有实根都在区间 $(-M, M)$ 上.

一元实系数多项式根的界

设 $F = \sum_{i=0}^{m} c_i x^i \in \mathbb{R}[x]$, 并令

$$M = \max\left\{1, \sum_{i=0}^{m-1} \left|\frac{c_i}{c_m}\right|\right\}, \qquad N = 1 + \max\left\{\left|\frac{c_0}{c_m}\right|, \ldots, \left|\frac{c_{m-1}}{c_m}\right|\right\},$$

则对任意 $|x| \geqslant M$ 或 $|x| \geqslant N$, $|F| > 0$.

- 即 $|x| < \min(M, N)$.
- 证明：主要利用三角不等式

变号数

序列的变号数

设 $\boldsymbol{a}$ 为 $\mathbb{R}$ 中的序列, 而 $\boldsymbol{a}' = [a_1, \ldots, a_t]$ 为删除 $\boldsymbol{a}$ 中所有 0 后得到的新序列, 则 $\boldsymbol{a}$ 的变号数 $\mathrm{var}(\boldsymbol{a})$ 定义为集合 $\{a_i a_{i+1} | 1 \leqslant i \leqslant t-1\}$ 中的负数个数, 即

$$\mathrm{var}(\boldsymbol{a}) = \sum_{i=1}^{l-1} \frac{1 - \mathrm{sgn}(a_i a_{i+1})}{2}, \text{ 其中 } \mathrm{sgn}(a) \text{ 为 } a \text{ 的符号}$$

- 序列 $\boldsymbol{a}$ 的符号序列 $\mathrm{sgn}(\boldsymbol{a}) := [\mathrm{sgn}(a_1), \ldots, \mathrm{sgn}(a_t)]$, 显然 $\mathrm{var}(\boldsymbol{a}) = \mathrm{var}(\mathrm{sgn}(\boldsymbol{a}))$

Example

序列 $[1, -1, 0, 3, 2, -2, 0, 1, -1]$ 的符号序列

$$\boldsymbol{s} = \mathrm{sgn}(\boldsymbol{a}) = [1, -1, 0, 1, 1, -1, 0, 1, -1],$$

从而变号数 $\mathrm{var}(\boldsymbol{a}) = \mathrm{var}(\boldsymbol{s}) = 5$.

变号数

多项式组的变号数

设 $\mathcal{F} = [F_1, \ldots, F_t]$ 为 $\mathbb{R}[x]$ 中的多项式序列, 则 $\mathcal{F}$ 在 $x = a$ 处的变号数为 $\operatorname{var}(\mathcal{F}, a) := \operatorname{var}([F_1(a), \ldots, F_t(a)])$

- 推广定义至 ∞ 和 $-\infty$.

多项式组在区间的变号数

记 $\overline{\mathbb{R}} := \mathbb{R} \cup \{-\infty, +\infty\}$, 并设 $I = (c, d)$, 其中 $c, d \in \overline{\mathbb{R}}$, 则 $\mathcal{F}$ 在 I 上的变号数为

$$\operatorname{var}(\mathcal{F}, I) := \operatorname{var}(\mathcal{F}, c) - \operatorname{var}(\mathcal{F}, d).$$

变号数

Example

考虑 $\mathbb{R}[x]$ 中的多项式序列 $\mathcal{F} = [F_1, \ldots, F_5]$, 其中

$$F_1 = x^4 - 5\,x^2 + 4, \quad F_2 = 4\,x^3 - 10\,x,$$
$$F_3 = \frac{5}{2}\,x^2 - 4, \quad F_4 = \frac{18}{5}\,x, \quad F_5 = 4,$$

则 $\mathcal{F}$ 在 $x = \pm\infty, \pm 1, \pm 2$ 处的符号序列及区间 $(-\infty, +\infty)$ 上的变号数为

$$\operatorname{sgn}(\mathcal{F}, -\infty) = [1, -1, 1, -1, 1], \quad \operatorname{sgn}(\mathcal{F}, +\infty) = [1, 1, 1, 1, 1],$$
$$\operatorname{sgn}(\mathcal{F}, -2) = [0, -1, 1, -1, 1], \quad \operatorname{sgn}(\mathcal{F}, 2) = [0, 1, 1, 1, 1],$$
$$\operatorname{sgn}(\mathcal{F}, -1) = [0, 1, -1, -1, 1], \quad \operatorname{sgn}(\mathcal{F}, 1) = [0, -1, -1, 1, 1],$$

$$\operatorname{var}(\mathcal{F}, (-\infty, +\infty)) = \operatorname{var}(\mathcal{F}, -\infty) - \operatorname{var}(\mathcal{F}, +\infty) = 4.$$

Sylvester 序列与变号数

Sylvester 与 Sturm 序列

设 $F, G \in \mathbb{R}[x]$, $P_1 = F$, $P_2 = F'G$, $P_{i+1} = -\operatorname{rem}(P_{i-1}, P_i)$. 令 t 为最后一个使得 $P_t \neq 0$ 的下标,

- 称 $\mathcal{P} = [P_1, \ldots, P_t]$ 为 F 和 G 的 Sylvester 序列
- 当 $G = 1$ 时, 称 $\mathcal{P}$ 为 F 的 Sturm 序列

- 最后一项 P_t 即为 F 和 $F'G$ 的最大公因子.

引理

设 $F, G \in \mathbb{R}[x]$, 而 $\mathcal{P} = [P_1, \ldots, P_t]$ 为 F 和 G 的 Sylvester 序列. 令 $U_i = P_i/P_t$ $(1 \leqslant i \leqslant t)$, $\mathcal{U} = [U_1, \ldots, U_t]$, 则

1. 对任意 $a \in \overline{\mathbb{R}}$, 若 a 使得 F 和 $F'G$ 不同时为零, 则 $\operatorname{var}(\mathcal{P}, a) = \operatorname{var}(\mathcal{U}, a)$;
2. 对任意 i, 不存在 $x \in \mathbb{R}$ 使得 $U_i(x) = U_{i+1}(x) = 0$;
3. 若 $U_i(a) = 0$, 则存在 $\varepsilon > 0$ 使得 $U_{i-1}(x)U_{i+1}(x) < 0$ 对所有 $x \in (a - \varepsilon, a + \varepsilon)$ 成立.

Sylvester 定理

设 $F, G \in \mathbb{R}[x]$, $I = (c, d) \subseteq \overline{\mathbb{R}}$. num_+ 使得给定多项式为正的某一元多项式的根的数目 num_- 使得给定多项式为负的某一元多项式的根的数目记

$$\begin{aligned}
\mathrm{num}_+(F, G, I) &= \#\{x : F = 0, G > 0, x \in I\}, \\
\mathrm{num}_-(F, G, I) &= \#\{x : F = 0, G < 0, x \in I\}, \\
\mathrm{num}(F, I) &= \#\{x : F = 0, x \in I\}.
\end{aligned}$$

Sylvester 定理

设 $F, G \in \mathbb{R}[x]$, 而 $\mathcal{P}$ 为 F 和 G 的 Sylvester 序列. 在任意区间 $I = (c, d) \subseteq \overline{\mathbb{R}}$ 上, 若 $F(c)F(d) \neq 0$, 则 $\mathrm{var}(\mathcal{P}, I) = \mathrm{num}_+(F, G, I) - \mathrm{num}_-(F, G, I)$.

Sturm 定理

Sturm 定理

设 $F \in \mathbb{R}[x]$, $\mathcal{P}$ 为 F 的 Sturm 序列, $I = (c, d) \subseteq \overline{\mathbb{R}}$. 若 $F(c)F(d) \neq 0$, 则 $\operatorname{var}(\mathcal{P}, I) = \operatorname{num}(F, I)$.

- Sylvester 定理的直接推论
- 任意多项式在任意区间上的实根个数可以判定!

Example

$F = x^4 - 3\,x^2 + 2$，其 Sturm 序列为 $[P_1, \ldots, P_5]$, 其中

$$P_1 = F = x^4 - 3\,x^2 + 2, \qquad P_2 = F' = 4\,x^3 - 6\,x,$$

$$P_3 = -\operatorname{rem}(P_1, P_2, x) = \frac{3}{2}\,x^2 - 2, \quad P_4 = -\operatorname{rem}(P_2, P_3, x) = \frac{2}{3}\,x,$$

$$P_5 = -\operatorname{rem}(P_3, P_4, x) = 2.$$

现在计算 F 在 $(0, 2)$ 上的实根数: (1) P_5 为非零常数 $\Longrightarrow$ F 无重根; (2) 又由 $F(0)F(2) \neq 0$ 和 Sturm 定理 $\Longrightarrow$ F 在 $(0, 2)$ 上的实根数为 $V(0) - V(2) = 2 - 0 = 2$.

实根隔离算法

算法 Isolate: $L := \mathrm{Isolate}(F)$. 任给无平方因子的整系数多项式 $F = F(x) \in \mathbf{Z}[x]$, 本算法计算 F 的实根隔离区间 L.

I1. 计算 F 根的界 B.

I2. 计算 F 的 Sturm 序列 Θ.

I3. 命 $L := \varnothing$, $W := \{(-B, B)\}$.

I4. 若 W 为空集，则输出 L, 且算法终止. 否则执行下列步骤：

I4.1. 任取 $(a, b) \in W$, 且命 $W := W \setminus \{(a, b)\}$. 由 Θ 计算在 $x = a$ 和 b 时 $F(x)$ 的 Sturm 序列变号数 $V(a)$ 和 $V(b)$, 并记

$$v := V(a) - V(b).$$

I4.2. 若 $v = 0$, 则返回 I4; 若 $v = 1$, 则命 $L := L \cup \{(a, b)\}$, 且返回 I4. 否则：

I4.2.1. 命 $W := W \cup \left\{\left(a, \frac{a+b}{2}\right), \left(\frac{a+b}{2}, b\right)\right\}$.

I4.2.2. 若 $F\left(\frac{a+b}{2}\right) = 0$, 则命

$$L := L \cup \left\{\left[\frac{a+b}{2}, \frac{a+b}{2}\right]\right\}, \quad F := \frac{F}{x - (a+b)/2}.$$

返回 I4.

第三次大作业

1. 给定一元多项式 $F \in \mathbb{Q}[x]$ 和一个有理数 $a \in \mathbb{Q}$, 编写程序计算 F 的 Sturm 序列 $\boldsymbol{s}$, 然后计算 $\boldsymbol{s}$ 在 a 处的变号数 $\mathrm{var}(\boldsymbol{s}, a)$.
2. 给定一元多项式 $F \in \mathbb{Q}[x]$ 和任意有理数 $\epsilon \in \mathbb{Q}$, 编写程序计算 F 所有实根的隔离区间，使得区间长度小于 ϵ.
3. 计算 $x^4 - 3x^2 + 1$ 的实根隔离区间，使得区间长度小于 10^{-5}.

格式与时间要求

- 上交作业为电子版，需包含源程序和简单的解决方式描述（例如主要步骤及其计算结果等），后者鼓励用 Latex 写.
- 等待进一步通知.

几点提示

1. 建议用 Maple 软件写，因为已经有常见的有关实根隔离的函数 (例如 realroot)
2. 利用 Maple 软件完成作业时的提示
   - 计算 Sturm 序列时带余除法的余式可用 rem(F, G) 计算 (算法结果可与 Maple 内置函数 sturmseq 比较)
   - 多项式 $F(x)$ 的 Sturm 序列在区间 $[a, b]$ 上的变号数计算结果可与 Maple 内置函数 sturm(F, x, a, b) 比较
   - 计算变号数时需要用多项式 F 在某点 a 处的取值：eval(F, x=a)
   - 计算序列变号数时要排除其中的零元素
   - 要求隔离区间长度 $< \epsilon$，这意味着即时算法中找到一个区间仅含一个解，若区间不够小则仍需继续二分.
   - 计算实根的界时需要用到展开形式多项式的系数:expand(F) 会将多项式展开, coeffs(expand(F)) 返回展开形式多项式的系数
3. 源程序需包含适量的注释

半代数系统

设 $F_i, G_j, H_k \in \mathbb{R}[\boldsymbol{x}]$, 称形如

$$\begin{cases} F_1 = 0, \ldots, F_s = 0, H_1 \neq 0, \ldots, H_r \neq 0, \\ G_1 \geqslant 0, \ldots, G_m \geqslant 0, G_{m+1} > 0, \ldots, G_t > 0 \end{cases}$$

的系统为半代数系统 (semi-algebraic system): $s \geqslant 1$, $r, m, t \geqslant 0$.

令

$$\mathcal{P} = \{F_1(\boldsymbol{u}, x_1, \ldots, x_s), \ldots, F_s(\boldsymbol{u}, x_1, \ldots, x_s)\},$$

其中 $\boldsymbol{u} = (u_1, \ldots, u_d)$ 为除 $x_1, \ldots, x_s$ 外的变元集, 则 $n = s + d$.

- 常系数半代数系统: 当 $n = s$ 并且 $\mathcal{P}$ 的实零点为有限集合 $\Longrightarrow$ 实解隔离
- 参系数半代数系统: 当 $s < n$ 时, 如果对其中参数的任意取值系统都有有限解 $\Longrightarrow$ 实解分类

实解隔离

一元多项式的实根隔离到半代数系统的实根隔离：高维推广

- 《多项式代数》第 4.5 节

Example

考虑

$$\begin{cases} F_1 = 6\,x^2 - 1 = 0, \\ F_2 = -3\,y^2 + 3\,xy + 1 = 0, \\ F_3 = 18\,z^2 - 12\,xz + 6\,xy - 5 = 0, \\ x > 0, y > 0, z > 0. \end{cases}$$

计算其实解隔离区间如下, 其中 $\varepsilon = 1/10$:

$$\left\{\left[\frac{13}{32}, \frac{53}{128}\right] \times \left[\frac{3309}{4096}, \frac{6789}{8192}\right] \times \left[\frac{9}{16}, \frac{5}{8}\right]\right\}.$$

实解分类

参系数半代数系统：可能具有无穷多组实解从而使得我们无法将这些实解一一隔离出来. 因此主要考虑：

1. 参数取何值时 $\mathbb{S}$ 有实解?
2. 参数取何值时 $\mathbb{S}$ 有正维数的实解? 实解的维数?
3. 参数取何值时 $\mathbb{S}$ 有指定数目的互异实解?

(1) 和 (2) 都可以化为 (3) 的情形进行讨论.

$\Longrightarrow$ 微分系统的定性分析: 《多项式代数》第 6.5 节