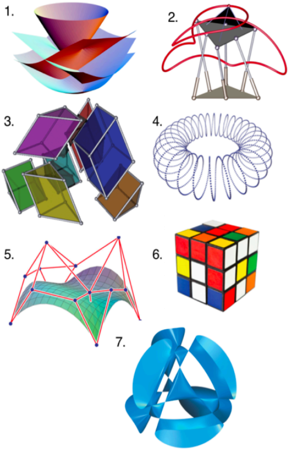
计算机代数

牟晨琪

北航沙河校区E403-7
chenqi.mou@buaa.edu.cn

2020年春



第六章

应用: 几何定理的机器证明

几何定理证明的四种风格

1. Euclid 风格：基于公理系统，使用定义和公理，依据逻辑推理规则，定理的证明是从假设到结论的推演过程.
   - 对于这种风格的证明，其方法没有统一、确定的步骤，因而难以用来系统地证明一大类定理.
2. Descartes 风格：通过建立坐标系将几何对象与代数关系联系起来，进而可以使用代数计算代替逻辑推理.
   - 尽管这种风格未为几何定理的证明提供系统的方法，但其代数化思想为实现几何定理证明的机械化铺平了道路.
3. Hilbert 风格：在 Euclid 公理系统的基础上引入数系，对只涉及点和直线关联性质的一类几何命题给出其证明的算法化方法.
   - 这种风格的证明是针对一类定理，因而是可以机械化的.
4. 计算机风格：针对各类几何定理，设计算法并将其在计算机上实施，从而实现定理证明的机械化和自动化.

线性等式型几何定理的机器证明

等式型几何定理

通过选取坐标系, 并用变元 $\boldsymbol{x}$ 表示定理中的点的坐标和其他几何量 (如三角形的面积、距离的平方、直线的斜率等), 大多数 (平面) 几何定理的假设和结论都可以用关于这些变元的多项式等式来表示. 这类几何定理称为等式型的.

设所考虑几何的附属数域为 $\mathcal{K}$, 那么等式型定理的假设可以表示为 $\mathcal{H}=0$, 而结论为 $G=0$,

$$\mathcal{H}=\{H_1,\ldots,H_s\}\subseteq\mathcal{K}[\boldsymbol{x}],\quad G\in\mathcal{K}[\boldsymbol{x}].$$

线性等式型几何定理

现考虑一类特殊的等式型定理, 其中每个定理的假设都可以通过有限多步来构造性地叙述. 设定理的第 k 步构造引进的变元为 $x_{i_k},\ldots,x_{i_{k+1}-1}$ $(k\geqslant 1)$. 如果对所有 k, 表示第 k 步构造中的几何关系的 l_k 个多项式等式关于 $x_{i_k},\ldots,x_{i_{k+1}-1}$ 中的某 l_k 或更多个变元都是线性的, 则称该定理为线性等式型的.

线性等式型几何定理的机器证明

1. 过已构点 (x_1, x_2) 构造任意一条直线.
2. 过已构点 (x_1, x_2) 构造由已构点 (x_3, x_4) 和 (x_5, x_6) 确定的直线的平行线. 只需构造欲构平行线上一点 (u_1, y_1) 或 (y_1, u_1), 该点满足等式

$$(x_5 - x_3)(y_1 - x_2) - (x_6 - x_4)(u_1 - x_1) = 0, \quad 或$$

$$(x_5 - x_3)(u_1 - x_2) - (x_6 - x_4)(y_1 - x_1) = 0.$$

3. 过已构点 (x_1, x_2) 构造由已构点 (x_3, x_4) 和 (x_5, x_6) 确定的直线的垂线. 只需构造欲构垂线上一点 (u_1, y_1) 或 (y_1, u_1), 则该点满足等式

$$(x_6 - x_4)(y_1 - x_2) + (x_5 - x_3)(u_1 - x_1) = 0, \quad 或$$

$$(x_6 - x_4)(u_1 - x_2) + (x_5 - x_3)(y_1 - x_1) = 0.$$

4. 构造分别由已构两点 (x_1, x_2) 和 (x_3, x_4) 与 (x_5, x_6) 和 (x_7, x_8) 确定的两条直线的交点. 设交点的坐标为 (y_1, y_2), 则:

$$(x_3 - x_1)(y_2 - x_2) - (x_4 - x_2)(y_1 - x_1) = 0,$$

$$(x_7 - x_5)(y_2 - x_6) - (x_8 - x_6)(y_1 - x_5) = 0.$$

线性等式型几何定理的机器证明

外心定理

任意三角形的三条中垂线交于一点.

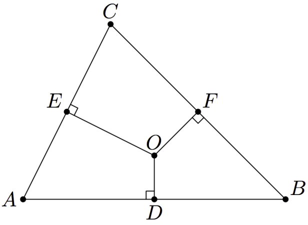


图 6.1　外心定理

$A(0,0), B(u_1,0), C(u_2,u_3) \Longrightarrow D(u_1/2,0)$ 和 $E(u_2/2,u_3/2)$. 令 BC 的中点为 F, 其坐标为 $(y_1,y_2) \Longrightarrow y_1=(u_1+u_2)/2,\ y_2=u_3/2$.

线性等式型几何定理的机器证明

分别过 D 和 E 作 AB 和 AC 的中垂线, 其交点可设为 $O(u_1/2, y_3)$, 则

$$u_3\left(y_3 - \frac{u_3}{2}\right) + u_2\left(\frac{u_1}{2} - \frac{u_2}{2}\right) = 0.$$

$\Longrightarrow$ $y_3 = u_3/2 - u_2(u_1 - u_2)/(2\,u_3)$.

要证明三条中垂线交于一点, 只需证明 $OF \perp BC$, 即

$$\left(y_1 - \frac{u_1}{2}\right)(u_2 - u_1) + u_3(y_2 - y_3) = 0.$$

将上面求出的 y_1, y_2, y_3 的表达式代入上式, 容易验证等式恒成立.

- y_3 的表达式中的分母 u_3 不能为零. 因此定理在 $u_3 \neq 0$ 的条件下成立. $\Longrightarrow$ 如果 $u_3 = 0$??

定理 (几何定理机械化证明原理 I)

任意线性等式型几何定理都可以机械化证明.

等式型定理的机器证明——一般原理

- 上述方法不适用于证明非线性等式型定理: 圆

定理 (几何定理机械化证明原理 II)

设等式型定理的假设和结论分别为 $\mathcal{H}=0$ 和 $G=0$, 其中 $\mathcal{H}, G$ 如前所示. 又设 $\mathcal{C}$ 为 $\mathcal{H}$ 关于变元序 $x_1<\cdots<x_n$ 的特征列, 而 $I=\prod_{C\in\mathcal{C}}\operatorname{ini}(C)$. 若 $\operatorname{prem}(G,\mathcal{C})\equiv 0$, 则 $\mathsf{Z}(\mathcal{H}/I)\subseteq \mathsf{Z}(G)$, 因此定理在条件 $I\neq 0$ 之下成立.

定理 (几何定理机械化证明原理 II′)

设等式型定理的假设和结论分别为 $\mathcal{H}=0$ 和 $G=0$, 其中 $\mathcal{H}, G$ 如前所示. 又设 $\boldsymbol{u}$ 为 $\boldsymbol{x}$ 中的所有自由变元, 并令 $\mathcal{G}$ 为 $\mathcal{H}$ 在 $\mathcal{K}(\boldsymbol{u})$ 上的任意 Gröbner 基. 如果 $\operatorname{nform}(G,\mathcal{G})\equiv 0$, 那么在某个 $J(\boldsymbol{u})\neq 0$ 的条件之下该定理成立.

等式型定理的机器证明：特征列方法

Simson 定理

从任意一点 P 向任意 $\triangle ABC$ 的三边作垂线, 那么垂足 D, E, F 共线当且仅当 P 在 $\triangle ABC$ 的外接圆上.

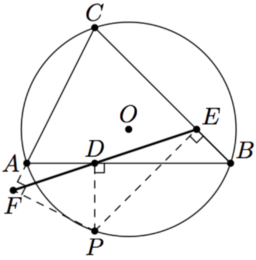


图 6.2 Simson 定理

(只证必要性)

等式型定理的机器证明：特征列方法

坐标化：选取直线 AB 为 x 轴，A, B 的中点为原点，并设各点坐标如下:

$$A(-u_1, 0),\quad B(u_1, 0),\quad C(u_2, u_3),\quad P(y_1, y_2),$$
$$D(y_1, 0),\quad E(y_3, y_4),\quad F(y_5, y_6).$$

假设条件：

$$(\mathcal{H}=0)\begin{cases} H_1 = u_3 y_2^2 - (u_3^2 + u_2^2 - u_1^2) y_2 + u_3(y_1^2 - u_1^2) = 0, \\ H_2 = (u_2 + u_1)(y_3 - y_1) + u_3(y_4 - y_2) = 0, \\ H_3 = (u_2 + u_1) y_4 - u_3(y_3 + u_1) = 0, \\ H_4 = (u_2 - u_1)(y_5 - y_1) + u_3(y_6 - y_2) = 0, \\ H_5 = (u_2 - u_1) y_6 - u_3(y_5 - u_1) = 0. \end{cases}$$

定理结论: $G = (y_3 - y_1) y_6 - y_4(y_5 - y_1) = 0$

等式型定理的机器证明：特征列方法

计算得到特征列如下

$$\mathcal{C} = \left[\begin{array}{l} u_3 y_2^2 + (u_1^2 - u_2^2 - u_3^2) y_2 + u_3 y_1^2 - u_3 u_1^2, \\ I_2 y_3 - I_3^2 y_1 - I_3 u_3 y_2 + u_3^2 u_1, \\ I_3 y_4 - u_3 y_3 - u_3 u_1, \\ I_4 y_5 + I_5^2 y_1 + I_5 u_3 y_2 + u_3^2 u_1, \\ I_5 y_6 - u_3 y_5 + u_3 u_1 \end{array} \right],$$

其中

$$I_2 = u_2^2 + 2\,u_1 u_2 + u_1^2 + u_3^2, \quad I_3 = u_2 + u_1,$$
$$I_4 = u_2^2 - 2\,u_2 u_1 + u_1^2 + u_3^2, \quad I_5 = u_2 - u_1.$$

可以验证，上述零点关系在 $u_1 u_3 I_2 \cdots I_5 \neq 0$ 的条件下成立：定理的必要性得证.

等式型定理的机器证明：特征列方法

退化条件

我们观察下定理成立的条件：$u_1 u_3 I_2 \cdots I_5 \neq 0$

- I_2: AC 是迷向的 (即 AC 的斜率为 $\pm\mathrm{i}$);
- I_3: $AB \perp AC$;
- I_4: BC 是迷向的;
- I_5: $AB \perp BC$.

等式型定理的机器证明：Gröbner 基方法

计算 $\mathcal{H}$ 在 $\mathcal{K}(u_1, u_2, u_3)$ 上由 $y_1 < \cdots < y_6$ 确定的字典序 Gröbner 基

$$\mathcal{G} = \left[\begin{array}{l} u_3 y_2^2 + (u_1^2 - u_3^2 - u_2^2) y_2 + u_3 y_1^2 - u_3 u_1^2, \\ I_2 y_3 - I_3 u_3 y_2 - I_3^2 y_1 + u_3^2 u_1, \\ I_2 y_4 - y_2 u_3^2 - I_3 u_3 y_1 - I_3 u_1 u_3, \\ I_4 y_5 - I_5 u_3 y_2 - I_5^2 y_1 - u_3^2 u_1, \\ I_4 y_6 - y_2 u_3^2 - I_5 u_3 y_1 + I_5 u_1 u_3 \end{array} \right],$$

其中 $I_2, \ldots, I_5$ 如前所示. 计算表明, $\mathrm{nform}(G, \mathcal{G}) \equiv 0$.

- 根据原理 II′, 定理在某个条件 $J(u_1, u_2, u_3) \neq 0$ 之下成立. 条件 $J \neq 0$ 是不可缺少的, 因为该定理并不普遍成立.

等式型定理的机器证明: 完备方法

定理 (几何定理机械化证明原理 III)

设等式型定理的假设和结论分别为 $\mathcal{H}=0$ 和 $G=0$, 其中 $\mathcal{H}, G$ 如 (4) 式所示. 又设三角系统 $[\mathcal{T}_1, \mathcal{U}_1], \ldots, [\mathcal{T}_t, \mathcal{U}_t]$ 使得

$$\mathsf{Z}(\mathcal{H})=\bigcup_{i=1}^{t} \mathsf{Z}(\mathcal{T}_i/\mathcal{U}_i).$$

若对某个 i, $\operatorname{prem}(G, \mathcal{T}_i) \equiv 0$, 则 $\mathsf{Z}(\mathcal{T}_i/\mathcal{U}_i) \subseteq \mathsf{Z}(G)$, 因此定理在 $\mathsf{Z}(\mathcal{H})$ 的分支 $\mathsf{Z}(\mathcal{T}_i/\mathcal{U}_i)$ 上成立.

计算 $\mathcal{H}$ 关于变元序 $u_1<u_2<u_3<y_1<\cdots<y_6$ 的正则序列可得 14 个正则系统 $[\mathcal{T}_i, \mathcal{U}_i]$. 不难验证, $\operatorname{prem}(G, \mathcal{T}_i) \equiv 0$ 对 $i=1, \ldots, 7$ 都成立. 结合前例, 可知 Simson 定理在退化情形 $I_3=0$ 和 $I_5=0$ 也成立. 因此前例给出的非退化条件中只有 $u_1 u_3 I_2 I_4 \neq 0$ 是必要的.

等式型定理的机器证明: 完备方法

定理 (几何定理机械化证明原理 IV)

设等式型定理的假设和结论分别为 $\mathcal{H}=0$ 和 $G=0$, 其中 $\mathcal{H}, G$ 如 (4) 式所示. 又设 $\mathcal{T}_1, \ldots, \mathcal{T}_t$ 为 $\mathcal{H}$ 的不可约三角序列或简单序列, 则定理在分支 $\mathrm{Z}(\mathcal{T}_i/\operatorname{ini}(\mathcal{T}_i))$ 上成立当且仅当 $\operatorname{prem}(G, \mathcal{T}_i) \equiv 0$.

- 原理 I–IV 只能证明在复数域上普遍成立的几何定理, 因为这类定理属于无序几何的范畴, 不涉及有序不等式. 如果定理的代数表达式含有 $<$ 和 $>$, 那么前面介绍的原理将会失效. 此时定理的证明需要用到第四章中介绍的、实代数几何中的方法, 如柱形代数分解方法等.

含不等式定理的机器证明：柱形代数分解方法

Pompeiu 定理

设 $\triangle ABC$ 为等边三角形，而 P 为不在其外接圆上的任意一点，则以线段 AP, BP 和 CP 为边可以作一非退化的三角形，即 $|AP|$, $|BP|$, $|CP|$ 中任意两者之和大于第三者.

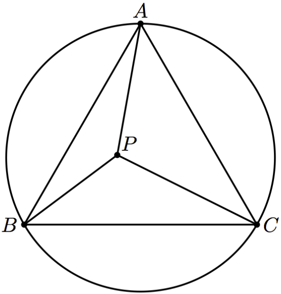


图 6.4　Pompeiu 定理

含不等式定理的机器证明：柱形代数分解方法

设外心坐标为 $(0,0)$, 点 A, B, C, P 的坐标分别为 $(0,1)$, $(-x_0,x_1)$, (x_0,x_1), (x_2,x_3), 而 AP, BP, CP 的长度分别为 x_4, x_5, x_6.

假设:

- $\triangle ABC$ 为等边三角形 $\Longleftrightarrow 4\,x_0^2-3=0\wedge 2\,x_1-1=0$;
- P 不在 $\triangle ABC$ 的外接圆上 $\Longleftrightarrow x_2^2+x_3^2-1\neq 0$;
- $|AP|=x_4 \Longleftrightarrow x_2^2+(x_3-1)^2-x_4^2=0\wedge x_4>0$;
- $|BP|=x_5 \Longleftrightarrow (x_2+x_0)^2+(x_3-x_1)^2-x_5^2=0\wedge x_5>0$;
- $|CP|=x_6 \Longleftrightarrow (x_2-x_0)^2+(x_3-x_1)^2-x_6^2=0\wedge x_6>0$.

结论:

$|AP|+|BP|>|CP| \Longleftrightarrow x_4+x_5-x_6>0$.

含不等式定理的机器证明：柱形代数分解方法

因此 Pompeiu 定理可以用下面含量词的公式来表示:

$$
\begin{aligned}
&(\forall x_0)(\forall x_1)(\forall x_2)(\forall x_3)(\forall x_4)(\forall x_5)(\forall x_6)[4\,x_0^2 - 3 = 0 \wedge 2\,x_1 - 1 = 0\\
&\qquad \wedge x_2^2 + x_3^2 - 1 \neq 0 \wedge x_2^2 + (x_3 - 1)^2 - x_4^2 = 0 \wedge x_4 > 0\\
&\qquad \wedge (x_2 + x_0)^2 + (x_3 - x_1)^2 - x_5^2 = 0 \wedge x_5 > 0\\
&\qquad \wedge (x_2 - x_0)^2 + (x_3 - x_1)^2 - x_6^2 = 0 \wedge x_6 > 0\\
&\qquad \Longrightarrow x_4 + x_5 - x_6 > 0].
\end{aligned}
$$

利用柱形代数分解将上述含量词公式进行量词消去后得到 true,
所以定理的结论在假设的条件下总是成立.

第六章

应用: 多元公钥密码学

公钥密码学简介

单向函数

密码体制的设计建立在单向函数的基础上. 映射 $f: X \longrightarrow Y$ 称为单向函数 (one-way function), 如果对任意 $x \in X$, $f(x)$ "容易" 计算; 而对于 "绝大多数" $y \in f(X)$, 寻找 x 使得 $f(x) = y$ 是 "计算不可行" 的.

Example

令 $X = \{i \in \mathbb{N} : 1 \leqslant i \leqslant 16\}$. 对任意 $x \in X$, 定义 $f(x) = 3^x \bmod 17$. 下表显示了 X 与 $f(X)$ 之间的对应关系.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

- 由 $x \in X$ 计算对应的 $f(x)$ 十分简单;
- 而对于大部分 $y \in f(X)$ 而言, 计算其原像并不简单.

陷门单向函数

陷门单向函数

单向函数 $f: X \longrightarrow Y$ 称作陷门单向函数 (trapdoor one-way function), 如果存在特定信息, 使得在获得该信息后, 对任意 $y \in f(X)$, 可以计算出 $x \in X$ 满足 $f(x) = y$.

- 这些特定信息称作陷门信息 (trapdoor information).
- 通常密码学家选择数学中的困难问题进行密码设计: RSA

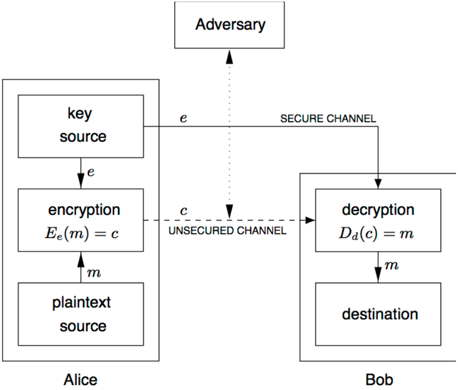
基本术语

- 明文 (plaintext): 希望加密的文档
- 密文 (ciphertext): 加密后的文档
- 消息空间: 全体明文构成的有限集合, 记作 $\mathcal{M}$
- 密文空间: 全体密文构成的有限集合, 记作 $\mathcal{C}$
- 密钥空间, 记作 $\mathcal{K}$, 其中的元素称作密钥 (key)
- 每个 $e \in \mathcal{K}$ 唯一确定了一个由 $\mathcal{M}$ 至 $\mathcal{C}$ 的映射 E_e, 该映射称作加密变换.
  - 利用加密变换将明文转换为密文的过程即为加密 (encryption)
- 任意 $d \in \mathcal{K}$ 唯一确定的 $\mathcal{C}$ 至 $\mathcal{M}$ 的映射 D_d 称作解密变换
  - 利用解密变换将密文转换为明文的过程即为解密 (decryption)

加密体制

包括加密变换集合 $\{E_e : e \in \mathcal{K}\}$ 及解密变换集合 $\{D_d : d \in \mathcal{K}\}$, 且对于任意 $e \in \mathcal{K}$, 存在唯一 $d \in \mathcal{K}$ 使得 $D_d = E_e^{-1}$, 即对任意 $m \in \mathcal{M}$, 有 $D_d(E_e(m)) = m$. 满足上述条件的 e 与 d 称作密钥对 (key pair), 记作 (e, d).

对称加密体制

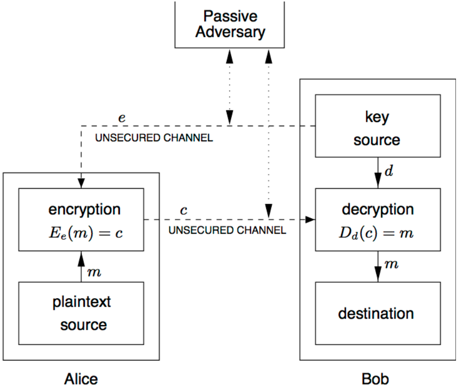


对称加密体制

即对于其中的任意密钥对 (e, d), 可以十分容易地从加密密钥 e 计算出与其对应的解密密钥 d.

- 将解密密钥传递给解密方时必须通过安全的渠道: 战时

公钥加密体制



- 对于公钥加密体制中的任意密钥对 (e, d)，在已知加密密钥 e 的情况下，敌方仍然无法计算出其对应的解密密钥 d.

公钥加密体制

RSA

- 基于大整数因子分解的困难性
- 安全的 RSA 体制，需要一个可因子分解为两个素数的大整数 N，它至少需要 1024 位比特数. $\Longrightarrow$ 涉及如此庞大整数的相关计算是十分费时的，因此 RSA 加密体制的效率并不高.
- RSA 加密体制也无法抵御量子计算机的攻击 $\Longrightarrow$ 后量子密码学

多元公钥密码体制 (multivariate public-key scheme)

建立在求解有限域上多元多项式方程组的困难性上. 已经证明，一般而言，求解有限域上多元多项式方程组是 NP 难的.

多元公钥密码体制

设 $\mathcal{F}$ 为有限域. 多元公钥密码体制的加密函数 $\bar{\psi}:\mathcal{F}^n \longrightarrow \mathcal{F}^m$ 定义如下:

$$\bar{\psi}(x_1,\ldots,x_n) := (\bar{F}_1,\ldots,\bar{F}_m),$$

其中 $\bar{F}_1,\ldots,\bar{F}_m \in \mathcal{F}[\boldsymbol{x}]$.

加密函数 $\bar{\psi}$ 的构造

1. 寻找 $\mathcal{F}[\boldsymbol{x}]$ 中 m 个特殊多项式 $F_1,\ldots,F_m$, 使得 $\psi(x_1,\ldots,x_n) := (F_1,\ldots,F_m)$ 满足如下性质:
   - 对任意 $(y'_1,\ldots,y'_m) \in \mathcal{F}^m$, 容易计算 $(x'_1,\ldots,x'_n) \in \mathcal{F}^n$ 使得 $\psi(x'_1,\ldots,x'_n) = (y'_1,\ldots,y'_m)$. 记上求解过程为 $\psi^{-1}(y'_1,\ldots,y'_m) = (x'_1,\ldots,x'_n)$.
2. 然后, 分别随机选取可逆仿射变换 $L_1:\mathcal{F}^m \longrightarrow \mathcal{F}^m$ 与 $L_2:\mathcal{F}^n \longrightarrow \mathcal{F}^n$. 定义 $\bar{\psi}$ 为如下映射的复合:

$$\bar{\psi} = L_1 \circ \psi \circ L_2.$$

多项式映射 ψ 称为该多元公钥密码体制的中心函数.

多元公钥密码体制

$$
\begin{tikzcd}
\mathcal{F}^n \arrow[r, "L_2"] \arrow[dr, "\mathrm{id}"'] & \mathcal{F}^n \arrow[r, "\psi"] & \mathcal{F}^m \arrow[r, "L_1"] & \mathcal{F}^m \\
 & \mathcal{F}^n \arrow[r, "\overline{\psi}"] & \mathcal{F}^m \arrow[ur, "\mathrm{id}"'] &
\end{tikzcd}
$$

图 6.7　多元公钥密码体制

多元公钥密码体制

- 公钥：加密函数 $\bar{\psi}$
- 私钥: 仿射变换 L_1 与 L_2
- 加密明文 $X' = (x'_1, \ldots, x'_n) \in \mathcal{F}^n$: 通过公钥计算密文 $\bar{\psi}(X')$
- 解密密文 $Y' = (y'_1, \ldots, y'_m)$: 只需求解

$$\bar{\psi}(x_1, \ldots, x_n) = (y'_1, \ldots, y'_m).$$

由 $\bar{\psi}$ 的构造知，求解上述多项式方程组只需依次计算 $Y_1 = L_1^{-1}(Y')$, $Y_2 = \psi^{-1}(Y_1)$ 及 $L_2^{-1}(Y_2)$.

- 在映射 ψ 两侧复合仿射变换 L_1 与 L_2 的目的在于隐藏 ψ 容易求逆的结构.

MI 加密体制

由 T. Matsumoto 和 H. Imai 于 1988 年提出的 MI 加密体制

一一映射

设 $\mathcal{F}$ 为 q 元有限域，$P \in \mathcal{F}[x]$ 为 m 次不可约多项式. 令 $\mathcal{K} = \mathcal{F}[x]/\langle P \rangle$，则 $\mathcal{K}$ 为 $\mathcal{F}$ 的 m 次扩域. 令 ϕ 为由 $\mathcal{K}$ 映至 $\mathcal{F}^m$ 的标准同构，即 $\phi(a_0 + \cdots + a_{m-1}x^{m-1}) = (a_0, \ldots, a_{m-1})$.

中心映射

选取 θ 满足 $0 < \theta < m$ 且 $\gcd(q^\theta + 1, q^m - 1) = 1$.
定义 $\mathcal{K}$ 上的映射 $\tilde{\psi}$ 为 $\tilde{\psi}(G) = G^{1+q^\theta}$. 定义 $\mathcal{F}^m$ 上的中心函数 ψ 为

$$\psi = \phi \circ \tilde{\psi} \circ \phi^{-1} = (F_1, \ldots, F_m),$$

其中 $F_1, \ldots, F_m \in \mathcal{F}[\boldsymbol{x}]$.

MI 加密体制

中心函数的逆

关于 θ 的条件使得映射 $\tilde{\psi}$ 容易求逆: 若整数 t 满足

$$t(1+q^{\theta}) \equiv 1 \mod (q^m - 1),$$

则 $\tilde{\psi}^{-1}(G) = G^t$.

进而可定义加密函数

$$\bar{\psi} = L_1 \circ \psi \circ L_2,$$

其中 $L_1, L_2 : \mathcal{F}^m \longrightarrow \mathcal{F}^m$ 为随机选取的可逆仿射变换.

MI 加密体制

- 公钥：域 $\mathcal{F}$ 和其中的元素运算，以及加密变换 $\bar{\psi}$ 中的 m 个多项式 $\bar{F}_1, \ldots, \bar{F}_m$;
- 私钥：仿射变换 L_1 与 L_2
- 加密明文 $X' = (x'_1, \ldots, x'_m) \in \mathcal{F}^m$：对任意 $i\ (1 \leqslant i \leqslant m)$ 计算 $y'_i = \bar{F}_i(X')$，密文即为 $Y' = (y'_1, \ldots, y'_m)$;
- 解密密文 $Y' = (y'_1, \ldots, y'_m)$：计算

$$
\begin{aligned}
\bar{F}^{-1}(y'_1, \ldots, y'_n) &= L_2^{-1} \circ \psi^{-1} \circ L_1^{-1}(y'_1, \ldots, y'_n) \\
&= L_2^{-1} \circ \phi \circ \tilde{\psi}^{-1} \circ \phi^{-1} \circ L_1^{-1}(y'_1, \ldots, y'_n).
\end{aligned}
$$

MI 加密体制

Example

设 $\mathcal{F}=\mathbb{F}_2$, 令 $m=3$ 并选取 $\mathcal{F}[x]$ 中的不可约多项式 $P=x^3+x+1$, 令 $\mathcal{K}=\mathcal{F}[x]/\langle P\rangle$. 选取 $\theta=2$ 满足条件, 此时计算可得

$$\tilde{\psi}(G)=G^{1+2^2}, \qquad \tilde{\psi}^{-1}(G)=G^3.$$

选取 L_1 和 L_2 为如下仿射变换:

$$L_1(x_1,x_2,x_3)=\begin{pmatrix}1&0&1\\0&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}+\begin{pmatrix}0\\1\\0\end{pmatrix},$$

$$L_2(x_1,x_2,x_3)=\begin{pmatrix}1&1&1\\0&0&1\\0&1&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}+\begin{pmatrix}1\\0\\1\end{pmatrix}.$$

MI 加密体制

Example

为了计算公钥 $\bar{\psi}$, 我们首先计算

$$\phi^{-1} \circ L_2(x_1, \ldots, x_2) = (x_1 + x_3) + (x_3 + 1)x + x_2 x^2.$$

令上式右侧多项式为 G, 则

$$\begin{aligned}\tilde{\psi}(G) = \; & (x_2x_3 + x_1 + 1) + (x_1x_2 + x_2x_3 + x_2 + x_3 + 1)x \\ & + (x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_3 + 1)x^2.\end{aligned}$$

再在左端复合映射 $L_1 \circ \phi$, 可得公钥多项式如下:

$$\begin{aligned}\bar{F}_1(x_1, x_2, x_3) &= x_1x_3 + x_2x_3 + x_2, \\ \bar{F}_2(x_1, x_2, x_3) &= x_1x_2 + x_1x_3 + x_1 + x_2x_3 + x_3 + 1, \\ \bar{F}_3(x_1, x_2, x_3) &= x_1x_3 + x_1 + x_2 + 1.\end{aligned}$$

选取明文 $(0, 1, 1)$, 则加密结果为:

$$\bar{F}_1(0, 1, 1) = 0, \quad \bar{F}_2(0, 1, 1) = 1, \quad \bar{F}_3(0, 1, 1) = 0.$$

HFE 加密体制

- 注意：在 MI 加密体制中有两个域 (有限域 $\mathbb{F}_2$ 和 $\mathcal{K} = \mathbb{F}_2[x]/\langle P\rangle$, 而中心函数是 $\mathcal{K}$ 上的一元多项式)
- MI 加密体制于 1995 年被 J. Patarin 利用 "线性化等式" 的技巧攻破 $\Longrightarrow$ HFE 加密体制由 Patarin 于 1996 年提出，是对 MI 加密体制的改进与优化.

中心函数

$$\tilde{\psi}(y) = \sum_{i=0}^{r_2-1}\sum_{j=0}^{i} a_{ij} y^{q^i+q^j} + \sum_{i=0}^{r_1-1} b_i y^{q^i} + c \in \mathcal{K}[y],$$

其中 $a_{ij}, b_i, c \in \mathcal{K}$ 随机选取，而 r_1, r_2 保证 $\tilde{\psi}$ 的次数小于参数 d.

- 上述中心函数（一元函数）可以用 Berlekamp 算法求解
- 多项式 $\tilde{\psi}$ 的次数 d 对求解复杂度有较大影响，一般选取 d 较小 (不超过 512)

HFE 加密体制

设 $\mathcal{F} = \mathbb{F}_{2^2}$, 即 $\mathcal{F}$ 为特征为 2 的 4 元域. 易知 $\mathcal{F} = \mathbb{F}_2(\alpha)$, 其中 α 满足 $\alpha^2 + \alpha + 1 = 0$. 从而 $\mathcal{F}$ 中元素可表示为 $0, 1, \alpha$ 和 α^2, 且元素间的加法及乘法运算如下表所示.

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$*$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

选取不可约多项式 $P = x^4 + x^3 + \alpha^2 x^2 + \alpha^2 x + \alpha^2 \in \mathcal{F}[x]$, 令 $\mathcal{K} = \mathcal{F}[x]/\langle P \rangle$, 而

$$\tilde{\psi}(y) = y^{4+4} + \alpha\, y^{4+1} + y + 1 \in \mathcal{K}[y].$$

此时 $\deg(\tilde{\psi}) = 8$.

HFE 加密体制

再选取随机可逆仿射变换 L_1 与 L_2 如下:

$$L_1(x_1,x_2,x_3,x_4)=\begin{pmatrix}\alpha & \alpha & 0 & \alpha\\ 0 & \alpha & 1 & 0\\ 1 & \alpha & \alpha & 1\\ 1 & \alpha & 0 & \alpha^2\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\\ x_4\end{pmatrix}+\begin{pmatrix}0\\ 0\\ \alpha\\ 0\end{pmatrix},$$

$$L_2(x_1,x_2,x_3,x_4)=\begin{pmatrix}1 & 0 & \alpha^2 & 1\\ \alpha^2 & 1 & 1 & \alpha\\ 1 & \alpha^2 & 1 & \alpha^2\\ 1 & \alpha & \alpha^2 & 1\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\\ x_4\end{pmatrix}+\begin{pmatrix}\alpha^2\\ \alpha^2\\ 0\\ 0\end{pmatrix}.$$

HFE 加密体制

于是加密映射 $\bar{\psi} = L_1 \circ \tilde{\psi} \circ L_2$ 即为

$$
\begin{aligned}
\bar{F}_1 &= \alpha^2\, x_1x_2 + \alpha\, x_1x_3 + \alpha^2\, x_1x_4 + \alpha\, x_1 + x_2x_3 + \alpha^2\, x_2x_4 + \alpha\, x_3^2 \\
&\quad + \alpha\, x_3x_4 + x_4^2 + \alpha, \\
\bar{F}_2 &= x_1^2 + \alpha\, x_1x_2 + \alpha^2\, x_1x_4 + \alpha^2\, x_1 + x_2x_3 + \alpha\, x_2x_4 + \alpha^2\, x_3^2 + x_3 \\
&\quad + \alpha^2\, x_4^2 + \alpha^2\, x_4, \\
\bar{F}_3 &= \alpha^2\, x_1^2 + x_1x_2 + \alpha^2\, x_1x_4 + \alpha^2\, x_1 + x_2^2 + \alpha\, x_2 + \alpha\, x_3^2 + x_3 + \alpha^2\, x_4^2, \\
\bar{F}_4 &= \alpha^2\, x_1^2 + x_1x_2 + \alpha^2\, x_1x_3 + \alpha\, x_1 + x_2x_3 + \alpha\, x_2x_4 + \alpha\, x_2 + x_3^2 \\
&\quad + \alpha\, x_3x_4 + x_3.
\end{aligned}
$$

- 加密明文 $(0, \alpha^2, 1, \alpha)$: 代入映射, 密文 $c = (0, 0, \alpha, \alpha^2)$.
- 解密 c: $L_1^{-1}(c) = (1, 1, \alpha, 0)$, $\phi^{-1}(1, 1, \alpha, 0) = 1 + x + \alpha\, x^2 \in \mathcal{K}$. 求解 $\mathcal{K}$ 上的方程

$$y^8 + \alpha\, y^5 + y + 1 = 1 + x + \alpha\, x^2$$

得唯一解 $\alpha + \alpha\, x + \alpha\, x^2$, 再经过 ϕ 及 L_2^{-1} 可得明文 m.

油醋签名体制

设 $\mathcal{F}$ 为 q 元有限域. 变元 $x_1, \ldots, x_o$ 称为油变量 (oil variable), 变元 $\tilde{x}_1, \ldots, \tilde{x}_v$ 称为醋变量 (vinegar variable). 令 $n = o + v$.

定义：油醋多项式

$\mathcal{F}[x_1, \ldots, x_o, \tilde{x}_1, \ldots, \tilde{x}_v]$ 中形如

$$\sum_{i=1}^{o}\sum_{j=1}^{v} a_{ij}\, x_i\tilde{x}_j + \sum_{i=1}^{v}\sum_{j=1}^{v} b_{ij}\, \tilde{x}_i\tilde{x}_j + \sum_{i=1}^{o} c_i\, x_i + \sum_{j=1}^{v} d_j\, \tilde{x}_j + e$$

的全次数为 2 的多项式称作油醋多项式 (oil-vinegar polynomial), 其中 $a_{ij}, b_{ij}, c_i, d_j, e \in \mathcal{F}$.

- 容易发现, 油醋多项式中没有 $x_i x_j$ 的项, 因此油醋多项式中的油变量与醋变量并没有充分混合. 取定醋变量为 $(\tilde{x}'_1, \ldots, \tilde{x}'_v)$, 则上述多项式变为关于油变量的线性函数. 该性质保证了此类多项式容易求逆.

油醋签名体制

定义：油醋映射

设 $F_1, \ldots, F_o$ 为 $\mathcal{F}[x_1, \ldots, x_o, \tilde{x}_1, \ldots, \tilde{x}_v]$ 中的油醋多项式, 则多项式映射 $\psi : \mathcal{F}^n \to \mathcal{F}^o$

$$\psi(x_1, \ldots, x_o, \tilde{x}_1, \ldots, \tilde{x}_v) := (F_1, \ldots, F_o)$$

称为油醋映射 (oil-vinegar map).

- 油醋映射也具有容易求逆的性质: 给定油醋映射 ψ 及 $(y_1', \ldots, y_o') \in \mathcal{F}^o$, 随机取定醋变量为 $(\tilde{x}_1', \ldots, \tilde{x}_v')$, 然后求解关于油变量 $x_1, \ldots, x_o$ 的线性方程组

$$F_i(x_1, \ldots, x_o) = y_i' \ (1 \leqslant i \leqslant o).$$

油醋签名体制

由于油醋映射由 $\mathcal{F}^n$ 映至 $\mathcal{F}^o$ $(o < n)$, 因此它只能用于设计签名体制

具体方法

1. 随机选取 $\mathcal{F}[x_1, \ldots, x_o, \tilde{x}_1, \ldots, \tilde{x}_v]$ 中的 o 个油醋多项式 $F_1, \ldots, F_o$ 构造油醋映射 $\psi = (F_1, \ldots, F_o)$.
2. 随机选取可逆仿射变换 $L : \mathcal{F}^n \to \mathcal{F}^n$, 形如
$$(x_1, \ldots, x_o, \tilde{x}_1, \ldots, \tilde{x}_v) = L(z_1, \ldots, z_n).$$
3. 则公钥变换 $\bar{\psi} : \mathcal{F}^n \to \mathcal{F}^o$ 定义为
$$\bar{\psi} = \psi \circ L = (\bar{F}_1, \ldots, \bar{F}_o).$$

- 注意到油醋多项式 $F_1, \ldots, F_o$ 已经为随机取定的了, 因此没有必要在 $\psi \circ L$ 左侧再复合随机的可逆仿射函数.

油醋签名体制

公私钥

- 公钥: 有限域 $\mathcal{F}$ 和其中元素运算, 以及映射 $\bar{\psi} = (\bar{F}_1, \ldots, \bar{F}_o)$;
- 私钥: 可逆仿射变换 L 及油醋映射 $\psi = (F_1, \ldots, F_o)$.

签名 (计算 $\bar{\psi}^{-1} = (\psi \circ L)^{-1}$)

1. 对文件 $(y'_1, \ldots, y'_o) \in \mathcal{F}^o$ 签名, 应随机选取醋变量为 $\tilde{x}'_1, \ldots, \tilde{x}'_v$ 并求解线性方程 $(x'_1, \ldots, x'_o, \tilde{x}'_1, \ldots, \tilde{x}'_v) = \psi(y'_1, \ldots, y'_o)$.
2. 计算 $(z'_1, \ldots, z'_n) = L^{-1}(x'_1, \ldots, x'_o, \tilde{x}'_1, \ldots, \tilde{x}'_v)$ 即可获得签名.

验证签名

$(y'_1, \ldots, y'_o)$ 的签名是否为 $(z'_1, \ldots, z'_n)$? 利用公钥映射 $\bar{\psi}$ 验证

$$\bar{\psi}(z'_1, \ldots, z'_n) = (y'_1, \ldots, y'_o).$$

油醋签名体制

- 当 $o = v$, 即油变量与醋变量数目相等时, 油醋签名体制称为平衡的 (balanced), 否则称为非平衡的 (unbalanced).

Example

设 $\mathcal{F} = \mathbb{F}_{2^2}$, 现考虑 $o = v = 3$ 的平衡油醋签名体制. 选择 3 个油醋多项式如下 (注意观察油变量)

$$
\begin{aligned}
F_1 = \; & x_1\tilde{x}_1 + \alpha^2\, x_1\tilde{x}_2 + \alpha^2\, x_1\tilde{x}_3 + x_2\tilde{x}_1 + \alpha\, x_2\tilde{x}_2 + x_2\tilde{x}_3 + \alpha^2\, x_2\tilde{x}_1 \\
& + \alpha^2\, x_3\tilde{x}_2 + \alpha^2\, x_3\tilde{x}_3 + \alpha^2\, x_3\tilde{x}_3 + \alpha\, \tilde{x}_1\tilde{x}_3 + \alpha^2\, \tilde{x}^2 + \tilde{x}_2\tilde{x}_3 + \tilde{x}_3^2, \\
F_2 = \; & \alpha\, x_1\tilde{x}_2 + \alpha\, x_1\tilde{x}_3 + x_2\tilde{x}_3 + x_2\tilde{x}_2 + \alpha\, x_2\tilde{x}_3 + \alpha\, x_3\tilde{x}_1 + x_3\tilde{x}_2 \\
& + \alpha^2\, x_3\tilde{x}_3 + x_1^2 + \alpha\, \tilde{x}_1\tilde{x}_2 + \tilde{x}_1\tilde{x}_3 + \tilde{x}_3^2, \\
F_3 = \; & \alpha\, x_1\tilde{x}_1 + \alpha\, x_1\tilde{x}_2 + x_2\tilde{x}_1 + x_2\tilde{x}_3 + \alpha^2\, x_3\tilde{x}_1 + x_3\tilde{x}_2 + x_3\tilde{x}_2 \\
& + \alpha^2\, x_3\tilde{x}_3 + \alpha^2\, \tilde{x}_1\tilde{x}_2 + \tilde{x}_1\tilde{x}_3 + \tilde{x}_2\tilde{x}_3 + \alpha\, \tilde{x}_3^2.
\end{aligned}
$$

油醋签名体制

取 L 为如下线性变换

$$L=\begin{pmatrix} 1 & \alpha^2 & \alpha & \alpha & 0 & \alpha^2 \\ \alpha^2 & \alpha^2 & 1 & 1 & 1 & \alpha \\ 1 & 0 & 1 & \alpha^2 & 1 & \alpha^2 \\ \alpha & \alpha & 1 & \alpha & 0 & 1 \\ \alpha & 1 & \alpha & \alpha^2 & 0 & \alpha^2 \\ 1 & 1 & 1 & \alpha & \alpha & 0 \end{pmatrix},$$

则经过复合后的公钥多项式为

$$\begin{aligned}
\bar{F}_1 = {}& z_1^2+\alpha^2 z_1z_2+\alpha z_1z_3+z_1z_6+\alpha^2 z_2^2+z_2z_3+\alpha z_2z_4+z_2z_5 \\
& +\alpha^2 z_2z_6+\alpha^2 z_3z_5+z_3z_6, \\
\bar{F}_2 = {}& z_1^2+z_1z_2+\alpha^2 z_1z_3+z_1z_4+\alpha z_1z_6+z_2^2+\alpha^2 z_2z_4+z_2z_5 \\
& +\alpha z_2z_6+z_3^2+\alpha^2 z_3z_4+z_3z_6+\alpha z_4^2+z_5^2+z_6^2, \\
\bar{F}_3 = {}& \alpha z_1^2+\alpha z_1z_2+\alpha z_1z_4+\alpha^2 z_1z_5+z_1z_6+z_2^2+\alpha^2 z_2z_6 \\
& +\alpha^2 z_3z_4+\alpha^2 z_3z_6+z_4^2+z_4z_6+\alpha z_5^2+\alpha z_5z_6+\alpha z_6^2.
\end{aligned}$$

- 经过复合后油变量与醋变量已经完全混合

油醋签名体制

若希望对文件 $M=(m_1,m_2,m_3)=(\alpha,1,\alpha^2)$ 进行签名:
首先随机选取醋变量的值, 例如选取 $(\tilde{x}_1,\tilde{x}_2,\tilde{x}_3)=(\alpha^2,\alpha^2,1)$, 然后带入油醋多项式得到关于油变量的线性函数如下

$$
\begin{aligned}
F_1(x_1,x_2,x_3,\alpha^2,\alpha^2,1) &= \alpha\, x_1+\alpha^2\, x_2+\alpha^2\, x_3+\alpha,\\
F_2(x_1,x_2,x_3,\alpha^2,\alpha^2,1) &= \alpha^2\, x_1+\alpha^2\, x_2+x_3+\alpha^2,\\
F_3(x_1,x_2,x_3,\alpha^2,\alpha^2,1) &= \alpha\, x_2+\alpha\, x_3+\alpha^2.
\end{aligned}
$$

令 $F_i(x_1,x_2,x_3,\alpha^2,\alpha^2,1)=m_i$ $(i=1,2,3)$, 求解该方程组可得 $(x_1,x_2,x_3)=(0,1,1)$. 因此, 文件 $(\alpha,1,\alpha^2)$ 的签名为

$$L^{-1}(0,1,1,\alpha^2,\alpha^2,1)=(\alpha^2,1,\alpha,\alpha^2,0,\alpha^2).$$

代数攻击

密码分析学与代数攻击

- 密码分析学：主要研究如何利用各种数学技巧对密码体制进行攻击，以检验密码体制的安全性.
- 代数攻击：利用密码体制的代数结构进行密码分析的方法.
  $\Longrightarrow$ 多项式代数在密码分析中的应用

它通常包含如下三个步骤:

(1) 将密码系统转化为多项式方程组;

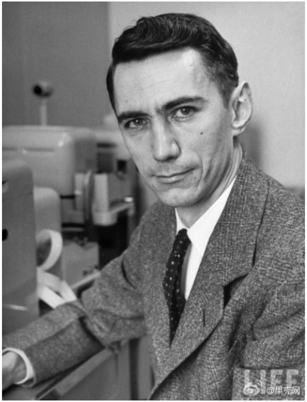
(2) 简化多项式方程组;

(3) 求解多项式方程组.

由于大部分密码体系均建立在二元域 $\mathbb{F}_2$ 之上，因此代数攻击通常关心密码体制对应的多项式方程组在 $\mathbb{F}_2^n$ 中的解. 为此，我们需要向方程组中添加域方程 $x_i^2 - x_i = 0$ $(i = 1, \ldots, n)$.

代数攻击

Breaking a cipher should require “as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type” — C. Shannon, 1949



第六章

应用: 微分系统的定性分析

奇点及其个数

考虑如下形式的 n 维自治微分系统:

$$\begin{cases} \dfrac{\mathrm{d}x_1}{\mathrm{d}t} = \dfrac{P_1(u_1,\ldots,u_m,x_1,\ldots,x_n)}{Q_1(u_1,\ldots,u_m,x_1,\ldots,x_n)}, \\ \qquad\qquad \cdots\cdots \\ \dfrac{\mathrm{d}x_n}{\mathrm{d}t} = \dfrac{P_n(u_1,\ldots,u_m,x_1,\ldots,x_n)}{Q_n(u_1,\ldots,u_m,x_1,\ldots,x_n)}, \\ \Omega(u_1,\ldots,u_m,x_1,\ldots,x_n), \end{cases}$$

- $P_1,\ldots,P_n,\ Q_1 \neq 0,\ldots,Q_n \neq 0$ 是以 $u_1,\ldots,u_m,x_1,\ldots,x_n$ 为变元的整系数多项式
- Ω 是关于 $u_1,\ldots,u_m,x_1,\ldots,x_n$ 的整系数多项式等式和不等式构成的集合,
- $u_1,\ldots,u_m$ 为不依赖于求导变元 t 的实参数.
- 每个 x_i 都是 t 的函数: 有时将 $\mathrm{d}x_i/\mathrm{d}t$ 简写为 $\dot{x}_i$.

奇点及其个数

命 $\boldsymbol{u}=(u_1,\ldots,u_m)$, $\boldsymbol{x}=(x_1,\ldots,x_n)$, 而

$$\begin{aligned}\Psi := \Omega\ &\cup\{P_1(\boldsymbol{u},\boldsymbol{x})=0,\ldots,P_n(\boldsymbol{u},\boldsymbol{x})=0\}\\ &\cup\{Q_1(\boldsymbol{u},\boldsymbol{x})\neq 0,\ldots,Q_n(\boldsymbol{u},\boldsymbol{x})\neq 0\}.\end{aligned}$$

Ψ 是一个以 $\boldsymbol{u}$ 为参数、$\boldsymbol{x}$ 为变元的半代数系统.

定义：奇点

对参数 $\boldsymbol{u}$ 的任给实值 $\bar{\boldsymbol{u}}$, 称 n 维实空间 $\mathbb{R}^n$ 中的点 $\bar{\boldsymbol{x}}$ 为自治微分系统的 奇点 (singular point) 或平衡点 (equilibrium), 如果 $\boldsymbol{x}=\bar{\boldsymbol{x}}$ 是 $\Psi|_{\boldsymbol{u}=\bar{\boldsymbol{u}}}$ 中所有方程和不等式的一个公共实解, 即 $\bar{\boldsymbol{x}}\in\mathbb{R}^n$ 满足 $\Omega|_{\boldsymbol{u}=\bar{\boldsymbol{u}}}$ 中的所有等式和不等式, 且

$$P_1(\bar{\boldsymbol{u}},\bar{\boldsymbol{x}})=\cdots=P_n(\bar{\boldsymbol{u}},\bar{\boldsymbol{x}})=0,\quad Q_1(\bar{\boldsymbol{u}},\bar{\boldsymbol{x}})\cdots Q_n(\bar{\boldsymbol{u}},\bar{\boldsymbol{x}})\neq 0.$$

奇点及其个数

于是求微分系统的奇点及其个数问题可以归结为下列代数问题

问题 1 假定参数 $\boldsymbol{u}$ 不出现. 判定半代数系统 Ψ 关于变元 $\boldsymbol{x}$ 的实解个数, 并用有理区间隔离 Ψ 的所有孤立实解.

问题 2 对任意整数 $k \geqslant 0$, 确定使半代数系统 Ψ 关于变元 $\boldsymbol{x}$ 有且仅有 k 个互异实解的参数 $\boldsymbol{u}$ 所满足的条件.

- 上述两个问题可以用实解隔离和实解分类算法完全解决.

奇点及其个数

考虑平面微分系统

$$\dot{x} = \frac{P_1}{30 + v^4 y^4}, \quad \dot{y} = \frac{P_2}{1 + x^4}, \quad x \geqslant 0, \quad y \geqslant 0, \quad v \geqslant 0, \qquad (1)$$

其中

$$P_1 = 30 - 30\,x + v^4(1 - 201\,x)\,y^4,$$
$$P_2 = 1 + x^4 - (1 + 11\,x^4)\,y,$$

而 v 为实参数.

- 上述系统是一个著名的生物网络模型 $\Longrightarrow$ v 满足什么条件时该系统有 1 个、2 个或更多的奇点.

对于上述系统，$\Omega = \{x \geqslant 0, y \geqslant 0, v \geqslant 0\}$，而 $Q_1 = 30 + v^4 y^4$ 与 $Q_2 = 1 + x^4$ 对任意实的 v 和 x 都恒正，因而不会为 0. 所以上述系统的奇点就是系统 $\Psi = \{P_1 = 0, P_2 = 0, x \geqslant 0, y \geqslant 0, v \geqslant 0\}$ 关于 x, y 的实解.

奇点及其个数

由 $P_2 = 0$ 解出 y, 再将所得的解代入 $P_1 \Longrightarrow$ 以 v 为参数、关于 x 次数为 17 的不可约多项式

$$\begin{aligned} H = \ & (439230 + 201\, v^4)\, x^{17} - (439230 + v^4)\, x^{16} + (159720 + 804\, v^4)\, x^{13} \\ & - (159720 + 4\, v^4)\, x^{12} + (21780 + 1206\, v^4)\, x^9 - (21780 + 6\, v^4)\, x^8 \\ & + (1320 + 804\, v^4)\, x^5 - (1320 + 4\, v^4)\, x^4 + (30 + 201\, v^4)\, x - 30 - v^4. \end{aligned}$$

- 给出关于 x 有 $0, 1, 2, \ldots$ 个实根时参数 v 所要满足的条件.

使用软件包 DISCOVERER, 我们可以求得 H 关于 x 的判别式 R. 用 $0 = v_0 < v_1 < v_2$ 表示 R 的 3 个非负实根 (这里 $v_1 \approx 0.8315735076$, $v_2 \approx 1.796868764$).

1. 当 $0 < v < v_1$ 或 $v_2 < v < +\infty$ 时, 系统仅有一个奇点;
2. 当 $v_1 < v < v_2$ 时, 系统有三个奇点;
3. 当 $v = 0$ 时, 系统有唯一奇点;
4. 当 $v = v_1$ 或 $v = v_2$ 时, 系统有两个奇点.

稳定性分析

定义：奇点的稳定性

对给定参数值 $\bar{\boldsymbol{u}}$, 称系统的孤立奇点 $\bar{\boldsymbol{x}}$ 为稳定的 (stable), 如果对每个 $\epsilon > 0$ 和任意 $t_0 > 0$ 都存在 $\delta(\epsilon) > 0$, 使得只要 $\|\boldsymbol{x}(t_0) - \bar{\boldsymbol{x}}\| < \delta(\epsilon)$ 就有 $\|\boldsymbol{x}(t) - \bar{\boldsymbol{x}}\| < \epsilon$ 对所有 $t \geqslant t_0$ 成立.

- $\bar{\boldsymbol{x}}$ 是稳定的, 如果系统开始时与 $\bar{\boldsymbol{x}}$ “充分近” 的所有解都保持与 $\bar{\boldsymbol{x}}$ 很 “近”.
- 如果这些开始与 $\bar{\boldsymbol{x}}$ 充分近的解不仅保持与 $\bar{\boldsymbol{x}}$ 很近, 而且在 t 趋于无穷时都最终逼近 $\bar{\boldsymbol{x}}$, 那么称 $\bar{\boldsymbol{x}}$ 为渐近 (asymptotically) 稳定的.

稳定性分析

Liapunov (李雅普诺夫) 第一方法

考虑 $n \times n$ Jacobi 矩阵

$$\boldsymbol{J}(\boldsymbol{u}, \boldsymbol{x}) = \begin{pmatrix} \dfrac{\partial \frac{P_1}{Q_1}}{\partial x_1} & \cdots & \dfrac{\partial \frac{P_1}{Q_1}}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial \frac{P_n}{Q_n}}{\partial x_1} & \cdots & \dfrac{\partial \frac{P_n}{Q_n}}{\partial x_n} \end{pmatrix}.$$

对给定 $\bar{\boldsymbol{u}}$ 的每个孤立奇点 $\bar{\boldsymbol{x}}$, 系统可写作如下矩阵形式:

$$\dot{\boldsymbol{x}}^{\mathrm{T}} = \boldsymbol{J}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}})(\boldsymbol{x} - \bar{\boldsymbol{x}})^{\mathrm{T}} + \boldsymbol{G},$$

式中的上标 T 表示矩阵的转置, 而高阶项

$$\boldsymbol{G} = \left(\frac{P_1(\bar{\boldsymbol{u}}, \boldsymbol{x})}{Q_1(\bar{\boldsymbol{u}}, \boldsymbol{x})}, \ldots, \frac{P_n(\bar{\boldsymbol{u}}, \boldsymbol{x})}{Q_n(\bar{\boldsymbol{u}}, \boldsymbol{x})} \right)^{\mathrm{T}} - \boldsymbol{J}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}})(\boldsymbol{x} - \bar{\boldsymbol{x}})^{\mathrm{T}}$$

在 $\boldsymbol{x} \to \bar{\boldsymbol{x}}$ 时是 $||\boldsymbol{x} - \bar{\boldsymbol{x}}||$ 的高阶无穷小.

稳定性分析

$$\boldsymbol{J}(\boldsymbol{u},\boldsymbol{x}) = \begin{pmatrix} \dfrac{\partial \frac{P_1}{Q_1}}{\partial x_1} & \cdots & \dfrac{\partial \frac{P_1}{Q_1}}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial \frac{P_n}{Q_n}}{\partial x_1} & \cdots & \dfrac{\partial \frac{P_n}{Q_n}}{\partial x_n} \end{pmatrix}.$$

定理

(a) 如果矩阵 $\boldsymbol{J}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}})$ 的所有特征值都有负实部, 那么 $\bar{\boldsymbol{x}}$ 是渐近稳定的.

(b) 如果矩阵 $\boldsymbol{J}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}})$ 至少有一个实部为正的特征值, 那么 $\bar{\boldsymbol{x}}$ 是不稳定的.

稳定性分析：平面微分系统 ($n = 2$)

设 $n = 2$, 系统在 $(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}})$ 处的 Jacobi 矩阵为

$$\boldsymbol{J}_2(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

而 λ_1, λ_2 为 $\boldsymbol{J}_2(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}})$ 的两个特征值. 也就是说, λ_1, λ_2 是特征多项式

$$\begin{vmatrix} a - \lambda & b \\ c & d - \lambda \end{vmatrix} = \lambda^2 + p\lambda + q$$

的两个根, 上式中 $p = -(a + d)$, $q = ad - bc$. 令 $\Delta = p^2 - 4\,q$. 我们有下列判别准则:

稳定性分析：平面微分系统 $(n=2)$

1. 当 $q>0,\ p>0,\ \Delta\geqslant 0$ 时 (这时 λ_1,λ_2 为实的, 且 $\lambda_1<0,\lambda_2<0$), $\bar{\boldsymbol{x}}$ 为稳定结点 (stable node);
2. 当 $q>0,\ p<0,\ \Delta\geqslant 0$ 时 (这时 λ_1,λ_2 为实的, 且 $\lambda_1>0,\lambda_2>0$), $\bar{\boldsymbol{x}}$ 为不稳定结点 (unstable node);
3. 当 $q<0$ 时 (这时 λ_1,λ_2 为实的, 且 $\lambda_1\lambda_2<0$), $\bar{\boldsymbol{x}}$ 为 (不稳定) 鞍点 (saddle);
4. 当 $q>0,\ p>0,\ \Delta<0$ 时 (这时 λ_1,λ_2 是复共轭的, 且 $\operatorname{Re}\lambda_1=\operatorname{Re}\lambda_2<0$, 这里 Re 表示实部), $\bar{\boldsymbol{x}}$ 为稳定焦点 (stable focus);
5. 当 $q>0,\ p<0,\ \Delta<0$ 时 (这时 λ_1,λ_2 是复共轭的, 且 $\operatorname{Re}\lambda_1=\operatorname{Re}\lambda_2>0$), $\bar{\boldsymbol{x}}$ 为不稳定焦点 (unstable focus);
6. 当 $q>0,\ p=0$ 时 (这时 λ_1,λ_2 是复共轭的, 且 $\operatorname{Re}\lambda_1=\operatorname{Re}\lambda_2=0$), $\bar{\boldsymbol{x}}$ 为 $\dot{\boldsymbol{x}}^{\mathrm{T}}=\boldsymbol{J}_2(\bar{\boldsymbol{u}},\bar{\boldsymbol{x}})(\boldsymbol{x}-\bar{\boldsymbol{x}})^{\mathrm{T}}$ 的中心 (center) $\Longrightarrow$ 系统的奇点 $\bar{\boldsymbol{x}}$ 的稳定性依赖于 (高阶项) $\boldsymbol{G}$;
7. 当 $q=0$ 时, Jacobi 矩阵 $\boldsymbol{J}_2(\bar{\boldsymbol{u}},\bar{\boldsymbol{x}})$ 是奇异的, 因此 $\bar{\boldsymbol{x}}$ 是系统的高次奇点, 其稳定性依赖于 $\boldsymbol{G}$.

稳定性分析：平面微分系统 ($n = 2$)

$$\dot{x} = \frac{P_1}{30 + v^4 y^4}, \quad \dot{y} = \frac{P_2}{1 + x^4}, \quad x \geqslant 0, \quad y \geqslant 0, \quad v \geqslant 0,$$

其中

$$P_1 = 30 - 30\,x + v^4(1 - 201\,x)\,y^4,$$
$$P_2 = 1 + x^4 - (1 + 11\,x^4)\,y,$$

而 v 为实参数.

考虑该系统的 Jacobi 矩阵, 其元素为

$$F_1 = \frac{P_1}{30 + v^4 y^4}, \quad F_2 = \frac{P_2}{1 + x^4}$$

关于 x 和 y 的偏导数, 即

$$a = \frac{\partial F_1}{\partial x} = -\frac{3\,(10 + 67\,v^4 y^4)}{30 + v^4 y^4} < 0, \qquad b = \frac{\partial F_1}{\partial y} = -\frac{24000\,v^4 x y^3}{(30 + v^4 y^4)^2},$$

$$c = \frac{\partial F_2}{\partial x} = -\frac{40\,x^3 y}{(1 + x^4)^2}, \qquad d = \frac{\partial F_2}{\partial y} = -\frac{1 + 11 x^4}{1 + x^4} < 0.$$

稳定性分析：平面微分系统 ($n = 2$)

令

$$p = -(a+d) = \frac{2\,\bar{p}}{(30+v^4y^4)\,(1+x^4)},$$

$$q = ad - bc = \frac{3\,\bar{q}}{(30+v^4y^4)^2\,(1+x^4)^2},$$

$$\Delta = p^2 - 4\,q = \frac{100\,\bar{\Delta}}{(30+v^4y^4)^2\,(1+x^4)^2},$$

其中

$$\bar{p} = 30 + 180\,x^4 + 101\,v^4y^4 + 106\,v^4x^4y^4,$$

$$\bar{q} = 67\,y^8\,(1+x^4)\,(1+11\,x^4)\,v^8 + 20\,y^4\,(101 - 14788\,x^4 + 1111\,x^8)\,v^4 + 300\,(1+x^4)\,(1+11\,x^4),$$

$$\bar{\Delta} = x^8\,(30 - 19\,v^4y^4)^2 + 40\,v^4x^4\,(930 + 19\,v^4y^4)\,y^4 + 400\,v^8y^8.$$

容易看出, $a < 0,\ d < 0,\ p > 0,\ \Delta \geqslant 0$ 总是成立.

稳定性分析：平面微分系统 $(n=2)$

使用 DISCOVERER, 我们可以得到下列结果:

1. 当 $0 < v < v_1$ 或 $v_2 < v < +\infty$ 时, $q > 0$ 和 $\Delta > 0$ 在仅有的奇点处成立, 所以该奇点为稳定结点;
2. 当 $v_1 < v < v_2$ 时, 在三个奇点之一处有 $q < 0$, 所以该奇点为 (不稳定) 鞍点, 而在另外两个奇点处有 $q > 0$, $\Delta > 0$, 因此它们是稳定结点;
3. 当 $v = 0$ 时, $p > 0$, $q > 0$ 和 $\Delta > 0$ 在唯一的奇点处均成立, 所以该奇点是稳定结点;
4. 当 $v = v_1$ 或 $v = v_2$ 时, $q > 0$ 和 $\Delta > 0$ 在两个奇点之一处成立, 所以该奇点是稳定结点, 而 $q = 0$, $a < 0$, $d < 0$ 和 $bc > 0$ 在另一个奇点处成立: 需要进一步分析

稳定性分析：高维微分系统 $(n > 2)$

定义：稳定多项式

一个实系数一元多项式 A 称为是稳定的, 如果 A 的所有根的实部都是负的. 特别设

$$A = a_0\lambda^n + a_1\lambda^{n-1} + \cdots + a_n$$

为 $\bar{\boldsymbol{J}} = \boldsymbol{J}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{x}})$ 的特征多项式. $\bar{\boldsymbol{J}}$ 的特征值就是多项式 A 关于 λ 的根, 因此若 A 是稳定的, 则 $\bar{\boldsymbol{x}}$ 是稳定的.

设 A 如上所示, 并假定 $a_0 > 0$. 定义 $n \times n$ 方阵

$$\boldsymbol{H} = \begin{pmatrix} a_1 & a_3 & a_5 & \cdots & a_{2n-1} \\ a_0 & a_2 & a_4 & \cdots & a_{2n-2} \\ 0 & a_1 & a_3 & \cdots & a_{2n-3} \\ 0 & a_0 & a_2 & \cdots & a_{2n-4} \\ 0 & 0 & a_1 & \cdots & a_{2n-5} \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix},$$

称 $\boldsymbol{H}$ 为附属于 A 的Hurwitz 矩阵. 设 $\Delta_1, \Delta_2, \ldots, \Delta_n$ 为 $\boldsymbol{H}$ 的前主子式, 称为 A 的Hurwitz 行列式.

稳定性分析：高维微分系统 ($n > 2$)

定理：Routh–Hurwitz 准则

多项式 A 是稳定的当且仅当

$$\Delta_1 > 0,\ \Delta_2 > 0, \ldots, \Delta_n > 0.$$

定理：Liénard–Chipart 准则

多项式 A 是稳定的当且仅当下列条件之一成立:

(a) $a_n > 0,\ a_{n-2} > 0, \ldots, a_{n-2m} > 0,\ \Delta_1 > 0,\ \Delta_3 > 0, \ldots, \Delta_{2m'-1} > 0$;

(b) $a_n > 0,\ a_{n-2} > 0, \ldots, a_{n-2m} > 0,\ \Delta_2 > 0,\ \Delta_4 > 0, \ldots, \Delta_{2m} > 0$;

(c) $a_n > 0,\ a_{n-1} > 0,\ a_{n-3} > 0, \ldots, a_{n-2m'+1} > 0,\ \Delta_1 > 0,\ \Delta_3 > 0, \ldots, \Delta_{2m'-1} > 0$;

(d) $a_n > 0,\ a_{n-1} > 0,\ a_{n-3} > 0, \ldots, a_{n-2m'+1} > 0,\ \Delta_2 > 0,\ \Delta_4 > 0, \ldots, \Delta_{2m} > 0$,

这里 m 和 m' 分别是 $n/2$ 和 $(n+1)/2$ 的整数部分，而 $\Delta_1, \Delta_2, \ldots, \Delta_n$ 为 A 的 Hurwitz 行列式.

稳定性分析：高维微分系统 ($n > 2$)

现设 $H_1, \ldots, H_r$ 为 $\boldsymbol{u}$ 和 $\boldsymbol{x}$ 的有理系数多项式. 特别地, 每个 H_i 可以是上述的 a_i 或 Δ_j.

稳定性分析问题 $\Longrightarrow$ 给定参数值多项式 H_i 在各奇点处的符号 $\Longrightarrow$ 建立使得 H_i 在指定个数的奇点处为 0、为正或者为负的参数 $\boldsymbol{u}$ 所满足的条件.

化归的代数问题

问题 3 假定参数 $\boldsymbol{u}$ 不出现. 确定多项式 $H_1, \ldots, H_r$ 在半代数系统 Ψ 的每个孤立实解处的符号.

问题 4 确定使得 $H_1, \ldots, H_r$ 在系统定义的半代数系统 Ψ 的 (指定个数的) 孤立实解处为零、为正或者为负的参数 $\boldsymbol{u}$ 所满足的条件.

稳定性分析：高维微分系统 ($n > 2$)

代数分析方法

步骤 1 [构造半代数系统和 Hurwitz 行列式]. 利用需分析的自治微分系统构造半代数系统 Ψ, 并设 Ψ 中等式对应的多项式构成的集合为 $\mathcal{P}$, 而 Ψ 中不等式对应的多项式为 $G_1, \ldots, G_t$. 计算系统 Jacobi 矩阵 $\boldsymbol{J}(\boldsymbol{u}, \boldsymbol{x})$ 的特征多项式及其 Hurwitz 行列式, 并设按照 Routh–Hurwitz 准则或 Liénard–Chipart 准则需要判定其符号为正的多项式为 $H_1, \ldots, H_r$.

步骤 2 [计算三角列]. 用 2.2 节中介绍的三角分解或 2.3 节中介绍的 Gröbner 基方法将多项式组 $\mathcal{P}$ 三角化, 得到一个或多个 (正则) 三角列 $\mathcal{T}_k$. 如果参数 $\boldsymbol{u}$ 出现, 则转至步骤 4 (参数系统).

步骤 3 [求解问题 1 和问题 3 (无参数系统)]. 在不出现参数 $\boldsymbol{u}$ 时, 用 4.5.1 节中的算法隔离每个 $\mathcal{T}_k$ 的、满足 $G_1, \ldots, G_t$ 和 $H_1, \ldots, H_r$ 的不等式的实零点, 由此得到用有理区间隔离的 Ψ 的所有满足 H_j 的不等式的实解. 问题 1 和问题 3 获得解决.

稳定性分析：高维微分系统 ($n > 2$)

代数分析方法

步骤 4 [实解分类]. 对每个三角列 $\mathcal{T}_k$, 利用不等式多项式 $G_1, \ldots, G_t$ 和 $H_1, \ldots, H_r$ 计算一个以 $\boldsymbol{u}$ 为变元的代数簇 V, 该代数簇将实参数空间 $\mathbb{R}^m$ 分解为有限多个胞腔, 使得在每个胞腔中 $_k$ 的实零点的个数和 $G_1, \ldots, G_t$ 及 $H_1, \ldots, H_r$ 在这些实零点处的符号都保持不变.

- 使用 4.4 节中介绍的 (部分) 柱形代数分解和 4.5.2 节中介绍的实解分类方法

然后从每个胞腔中选取一个有理样本点, 并在该样本点处用有理区间隔离 $_k$ 的实零点, 计算 $\mathcal{T}_k$ 的实零点的个数以及 $G_1, \ldots, G_t$ 和 $H_1, \ldots, H_r$ 在实零点处的符号.

步骤 5 [求解问题 2 和问题 4 (含参系统)]. 确定 V 的定义多项式 (的因子) 在每个样本点处的符号. 根据这些多项式 (的因子) 在 Ψ 具有指定个数的实解的胞腔中样本点处的符号, 建立参数 $\boldsymbol{u}$ 所要满足的条件. 问题 2 和问题 4 获得完全解决.