Modélisation et résolutions numérique et symbolique

via les logiciels MAPLE et MATLAB (MODEL)

Jérémy Berthomieu Mohab Safey El Din Stef Graillat

jeremy.berthomieu@lip6.fr

Roadmap

1. Chinese Remainder Theorem in $\mathbb{Z}$.
2. Lagrange Interpolation in $\mathbb{K}[X]$.
3. Comparison between CRT and Lagrange Interpolation.
4. Eigenvalues problem.

Chinese Remainder Theorem (I)

Theorem 1

If $n_0, \ldots, n_d$ are pairewise coprime integers and $a_0, \ldots, a_d$ are integers modulo $n_0, \ldots, n_d$, then system $(S) = \begin{cases} x = a_0 \bmod n_0 \\ \vdots \\ x = a_d \bmod n_d. \end{cases}$ has solutions in $\mathbb{Z}$.

Chinese Remainder Theorem (I)

Theorem 1

If $n_0, \ldots, n_d$ are pairewise coprime integers and $a_0, \ldots, a_d$ are integers modulo $n_0, \ldots, n_d$, then system $(S) = \begin{cases} x = a_0 \bmod n_0 \\ \vdots \\ x = a_d \bmod n_d. \end{cases}$ has solutions in $\mathbb{Z}$.

If x_0 is a solution, then the other ones are $x = x_0 + kn_0 \cdots n_d$ for any $k \in \mathbb{Z}$.

Chinese Remainder Theorem (II)

Solution

Let $v_0, \ldots, v_d$ be such that $v_i n_0 \cdots n_{i-1} n_{i+1} \cdots n_d = 1 \bmod n_i$, *i.e.*

$$v_i \prod_{\substack{0 \le j \le d \\ j \neq i}} n_j = 1 \bmod n_i,$$

then

$$x_0 = \sum_{0 \le i \le d} a_i v_i \prod_{\substack{0 \le j \le d \\ j \neq i}} n_j.$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 & 7v_1 = 1 \bmod 2 \\ x = -1 \bmod 7, & 2v_2 = 1 \bmod 7 \end{cases}$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{array}{l} 7v_1 = 1 \bmod 2 \\ 2v_2 = 1 \bmod 7 \end{array} \qquad \begin{array}{l} \Rightarrow \\ \Rightarrow \end{array} \qquad \begin{array}{l} v_1 = 1, \\ v_2 = 4. \end{array}$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{array}{ll} 7v_1 = 1 \bmod 2 & \Rightarrow \quad v_1 = 1, \\ 2v_2 = 1 \bmod 7 & \Rightarrow \quad v_2 = 4. \end{array}$$

$$x_0 = 1 \times 1 \times 7 - 1 \times 4 \times 2.$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{array}{ll} 7v_1 = 1 \bmod 2 & \Rightarrow \quad v_1 = 1, \\ 2v_2 = 1 \bmod 7 & \Rightarrow \quad v_2 = 4. \end{array}$$

$$x_0 = -1.$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{aligned} 7v_1 &= 1 \bmod 2 \\ 2v_2 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 4. \end{aligned}$$

$$x = -1 + 14k, k \in \mathbb{Z}.$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{aligned} 7v_1 &= 1 \bmod 2 \\ 2v_2 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 4. \end{aligned}$$

$$x = -1 + 14k, k \in \mathbb{Z}.$$

2. $$\begin{cases} x = 1 \bmod 2 \\ x = 1 \bmod 3 \\ x = 5 \bmod 7, \end{cases} \qquad \begin{aligned} 21v_1 &= 1 \bmod 2 \\ 14v_2 &= 1 \bmod 3 \\ 6v_3 &= 1 \bmod 7 \end{aligned}$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{aligned} 7v_1 &= 1 \bmod 2 \\ 2v_2 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 4. \end{aligned}$$

$$x = -1 + 14k, k \in \mathbb{Z}.$$

2. $$\begin{cases} x = 1 \bmod 2 \\ x = 1 \bmod 3 \\ x = 5 \bmod 7, \end{cases} \qquad \begin{aligned} 21v_1 &= 1 \bmod 2 \\ 14v_2 &= 1 \bmod 3 \\ 6v_3 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 2, \\ &\Rightarrow \quad v_3 = 6. \end{aligned}$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = \quad 1 \bmod 2 & 7v_1 = 1 \bmod 2 \Rightarrow v_1 = 1, \\ x = -1 \bmod 7, & 2v_2 = 1 \bmod 7 \Rightarrow v_2 = 4. \end{cases}$$

   $$x = -1 + 14k, k \in \mathbb{Z}.$$

2. $$\begin{cases} x = 1 \bmod 2 & 21v_1 = 1 \bmod 2 \Rightarrow v_1 = 1, \\ x = 1 \bmod 3 & 14v_2 = 1 \bmod 3 \Rightarrow v_2 = 2, \\ x = 5 \bmod 7, & 6v_3 = 1 \bmod 7 \Rightarrow v_3 = 6. \end{cases}$$

   $$x_0 = 1 \times 1 \times 21 + 1 \times 2 \times 14 + 5 \times 6 \times 6.$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{aligned} 7v_1 &= 1 \bmod 2 \\ 2v_2 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 4. \end{aligned}$$

$$x = -1 + 14k, k \in \mathbb{Z}.$$

2. $$\begin{cases} x = 1 \bmod 2 \\ x = 1 \bmod 3 \\ x = 5 \bmod 7, \end{cases} \qquad \begin{aligned} 21v_1 &= 1 \bmod 2 \\ 14v_2 &= 1 \bmod 3 \\ 6v_3 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 2, \\ &\Rightarrow \quad v_3 = 6. \end{aligned}$$

$$x_0 = 229.$$

Chinese Remainder Theorem (III)

Examples

1. $$\begin{cases} x = 1 \bmod 2 \\ x = -1 \bmod 7, \end{cases} \qquad \begin{aligned} 7v_1 &= 1 \bmod 2 \\ 2v_2 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 4. \end{aligned}$$

$$x = -1 + 14k, k \in \mathbb{Z}.$$

2. $$\begin{cases} x = 1 \bmod 2 \\ x = 1 \bmod 3 \\ x = 5 \bmod 7, \end{cases} \qquad \begin{aligned} 21v_1 &= 1 \bmod 2 \\ 14v_2 &= 1 \bmod 3 \\ 6v_3 &= 1 \bmod 7 \end{aligned} \qquad \begin{aligned} &\Rightarrow \quad v_1 = 1, \\ &\Rightarrow \quad v_2 = 2, \\ &\Rightarrow \quad v_3 = 6. \end{aligned}$$

$$x = 19 + 42k, k \in \mathbb{Z}.$$

Chinese Remainder Theorem (IV)

Applications

1. RSA : $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
2. Multimodular computation, parallelism.
3. Fast Fourier Transform.
4. Generalization to any ring, *e.g.* Lagrange interpolation for polynomial rings $\mathbb{K}[X]$.

Lagrange Interpolation (I)

Theorem 2

If $(x_0, \ldots, x_d)$ are different elements of $\mathbb{K}$ and $a_0, \ldots, a_d$ are in $\mathbb{K}$,

then system $(S) = \begin{cases} P(x_0) = a_0 \\ \vdots \\ P(x_d) = a_d. \end{cases}$ has solutions in $\mathbb{K}[X]$.

Lagrange Interpolation (I)

Theorem 2

If $(x_0, \ldots, x_d)$ are different elements of $\mathbb{K}$ and $a_0, \ldots, a_d$ are in $\mathbb{K}$,

then system $(S) = \begin{cases} P(x_0) = a_0 \\ \vdots \\ P(x_d) = a_d. \end{cases}$ has solutions in $\mathbb{K}[X]$.

If P_0 is a solution, then the other ones are

$P = P_0 + Q \cdot (X - x_0) \cdots (X - x_d)$ for any $Q \in \mathbb{K}[X]$.

Lagrange Interpolation (II)

Solution

Let $L_0, \ldots, L_d$ be such that $L_i = \prod_{\substack{0 \le j \le d \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$, *i.e.*

$$\prod_{\substack{0 \le j \le d \\ j \neq i}} \frac{X - x_j}{x_i - x_j} = 1 \bmod (X - x_i),$$

then

$$P_0 = \sum_{0 \le i \le d} a_i L_i = \sum_{0 \le i \le d} a_i \prod_{\substack{0 \le j \le d \\ j \neq i}} \frac{X - x_j}{x_i - x_j}.$$

$\rightarrow$ P_0 is the only polynomial of degree at most d, solution of (S).

Lagrange Interpolation (III)

Algorithm

1. $T \leftarrow \prod_{0 \leq i \leq d} X - x_i,$
2. $U \leftarrow \prod_{\substack{0 \leq j \leq d \\ j \neq i}} x_i - x_j,$
3. $P \leftarrow \sum_{0 \leq i \leq d} \frac{T}{X - x_i} \frac{1}{U} y_i.$

$\rightarrow$ Complexity is in $O(d^2)$.

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1) = 3 & L_1 = \frac{X-1}{-1-1} \cdot \frac{X-2}{-1-2} \\ P(1) = 1 & L_2 = \frac{X+1}{1+1} \cdot \frac{X-2}{1-2} \\ P(2) = 3, & L_3 = \frac{X+1}{2+1} \cdot \frac{X-1}{2-1} \end{cases}$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{x-1}{-1-1}\cdot\frac{x-2}{-1-2} \Rightarrow L_1=\frac{x^2-3x+2}{6}, \\ P(1)=1 & L_2=\frac{x+1}{1+1}\cdot\frac{x-2}{1-2} \Rightarrow L_2=\frac{x^2-x-2}{-2}, \\ P(2)=3, & L_3=\frac{x+1}{2+1}\cdot\frac{x-1}{2-1} \Rightarrow L_3=\frac{x^2-1}{3}. \end{cases}$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=1 & L_2=\frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & L_3=\frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P_0=3\frac{X^2-3X+2}{6}+\frac{X^2-X-2}{-2}+3\frac{X^2-1}{3}.$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=1 & L_2=\frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & L_3=\frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P_0=X^2-X+1.$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=1 & L_2=\frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & L_3=\frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P=X^2-X+1+Q\cdot(X+1)(X-1)(X-2), Q\in\mathbb{K}[X].$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 \\ P(1)=1 \\ P(2)=3, \end{cases} \quad \begin{aligned} L_1 &= \frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \\ L_2 &= \frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \\ L_3 &= \frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \end{aligned} \quad \begin{aligned} &\Rightarrow \\ &\Rightarrow \\ &\Rightarrow \end{aligned} \quad \begin{aligned} L_1 &= \frac{X^2-3X+2}{6}, \\ L_2 &= \frac{X^2-X-2}{-2}, \\ L_3 &= \frac{X^2-1}{3}. \end{aligned}$$

   $$P = X^2 - X + 1 + Q\cdot(X+1)(X-1)(X-2), Q \in \mathbb{K}[X].$$

2. $$\begin{cases} P(-1)=3 \\ P(1)=3 \\ P(2)=3, \end{cases}$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=1 & L_2=\frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & L_3=\frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P=X^2-X+1+Q\cdot(X+1)(X-1)(X-2), Q\in\mathbb{K}[X].$$

2. $$\begin{cases} P(-1)=3 \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=3 \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=1 & L_2=\frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & L_3=\frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P=X^2-X+1+Q\cdot(X+1)(X-1)(X-2), Q\in\mathbb{K}[X].$$

2. $$\begin{cases} P(-1)=3 \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=3 \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P_0=3\frac{X^2-3X+2}{6}+3\frac{X^2-X-2}{-2}+3\frac{X^2-1}{3}.$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=1 & L_2=\frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & L_3=\frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P=X^2-X+1+Q\cdot(X+1)(X-1)(X-2), Q\in\mathbb{K}[X].$$

2. $$\begin{cases} P(-1)=3 & \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=3 & \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P_0=3.$$

Lagrange Interpolation (IV)

Examples

1. $$\begin{cases} P(-1)=3 & L_1=\frac{X-1}{-1-1}\cdot\frac{X-2}{-1-2} \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=1 & L_2=\frac{X+1}{1+1}\cdot\frac{X-2}{1-2} \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, & L_3=\frac{X+1}{2+1}\cdot\frac{X-1}{2-1} \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P=X^2-X+1+Q\cdot(X+1)(X-1)(X-2), Q\in\mathbb{K}[X].$$

2. $$\begin{cases} P(-1)=3 \Rightarrow L_1=\frac{X^2-3X+2}{6}, \\ P(1)=3 \Rightarrow L_2=\frac{X^2-X-2}{-2}, \\ P(2)=3, \Rightarrow L_3=\frac{X^2-1}{3}. \end{cases}$$

$$P=3+Q\cdot(X+1)(X-1)(X-2), Q\in\mathbb{K}[X].$$

Lagrange Interpolation (V)

Applications

1. Computation of characteristic polynomials.
2. Shamir's Secret Sharing.
3. Computation of the inverse of a Vandermonde matrix.
4. Evaluation-interpolation algorithm.

Comparison between CRT and Lagrange interpolation (I)

$n_0, \ldots, n_d$ pairwise coprime.

$$(S) = \begin{cases} x = a_0 \bmod n_0 \\ \quad \vdots \\ x = a_d \bmod n_d. \end{cases}$$

$x_0, \ldots, x_d$ pairwise distinct.

$$(S) = \begin{cases} P(x_0) = a_0 \\ \quad \vdots \\ P(x_d) = a_d. \end{cases}$$

Comparison between CRT and Lagrange interpolation (I)

$n_0, \ldots, n_d$ pairwise coprime.

$$(S) = \begin{cases} x = a_0 \bmod n_0 \\ \quad \vdots \\ x = a_d \bmod n_d. \end{cases}$$

$x_0, \ldots, x_d$ pairwise distinct.

$$(S) = \begin{cases} P(x_0) = a_0 \\ \quad \vdots \\ P(x_d) = a_d, \end{cases}$$

$$= \begin{cases} P = a_0 \bmod (X - x_0) \\ \quad \vdots \\ P = a_d \bmod (X - x_d). \end{cases}$$

Comparison between CRT and Lagrange interpolation (II)

$$v_i \prod_{\substack{0 \le j \le d \\ j \neq i}} n_j = 1 \bmod n_i.$$

$$L_i = \prod_{\substack{0 \le j \le d \\ j \neq i}} \frac{X - x_j}{x_i - x_j}.$$

Comparison between CRT and Lagrange interpolation (II)

$$v_i \prod_{\substack{0 \le j \le d \\ j \neq i}} n_j = 1 \bmod n_i.$$

$$\begin{aligned} L_i &= \prod_{\substack{0 \le j \le d \\ j \neq i}} \frac{X - x_j}{x_i - x_j} \\ &= 1 \bmod (X - x_i) \\ &= 0 \bmod (X - x_j),\ j \neq i. \end{aligned}$$

Comparison between CRT and Lagrange interpolation (II)

$$v_i \prod_{\substack{0 \le j \le d \\ j \neq i}} n_j = 1 \bmod n_i$$

$$= 0 \bmod n_j, \ j \neq i.$$

$$L_i = \prod_{\substack{0 \le j \le d \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$$

$$= 1 \bmod (X - x_i)$$

$$= 0 \bmod (X - x_j), \ j \neq i.$$

Comparison between CRT and Lagrange Interpolation (III)

Reminder

There is an Euclidean division in $\mathbb{K}[X]$:

$$\forall\ A, B \in \mathbb{K}[X], \exists\ Q, R \in \mathbb{K}[X], \quad A = BQ + R,\ \deg R < \deg B.$$

Comparison between CRT and Lagrange Interpolation (III)

Reminder

There is an Euclidean division in $\mathbb{K}[X]$:

$$\forall\ A, B \in \mathbb{K}[X], \exists\ Q, R \in \mathbb{K}[X], \quad A = BQ + R,\ \deg R < \deg B.$$

Example

If $A = X^3 + X + 1$ and $B = X^2 - 1$, then $Q = X$, $R = 2X + 1$.

$$X^3 + X + 1 = X(X^2 - 1) + (2X + 1).$$

Comparison between CRT and Lagrange Interpolation (IV)

Consequence

1. One can perform the Euclidean algorithm to compute the GCD of two polynomials of $\mathbb{K}[X]$.
2. Chinese Remainder Theorem (CRT) is valid in $\mathbb{K}[X]$!

Chinese Remainder Theorem in $\mathbb{K}[X]$

Rewritten Theorem

If $R_1, \ldots, R_r$ are pairewise coprime polynomials and $A_1, \ldots, A_r$ are polynomials modulo $R_1, \ldots, R_r$, then system $(S) = \begin{cases} P = A_1 \bmod R_1 \\ \vdots \\ P = A_r \bmod R_r. \end{cases}$ has solutions in $\mathbb{K}[X]$.

Chinese Remainder Theorem in $\mathbb{K}[X]$

Rewritten Theorem

If $R_1, \ldots, R_r$ are pairewise coprime polynomials and $A_1, \ldots, A_r$ are polynomials modulo $R_1, \ldots, R_r$, then system $(S) = \begin{cases} P = A_1 \bmod R_1 \\ \vdots \\ P = A_r \bmod R_r. \end{cases}$ has solutions in $\mathbb{K}[X]$.
If P_0 is a solution, then the other ones are $P = P_0 + QR_1 \cdots R_r$ for any $Q \in \mathbb{K}[X]$.

Special case

If each R_i has degree 1, then $R_i = X - x_i$ and $A_i = a_i \in \mathbb{K}$.
Furthermore, R_i, R_j are coprime if, and only if, $x_i \neq x_j$.

$\rightarrow$ This is Lagrange interpolation problem!

Eigenvalues problem

Definition

Let A be a square matrix of size d with coefficients in $\mathbb{K}$. We say that λ is an eigenvalue of A if there is a vector $v \neq 0$ such that $Av = \lambda v$.

Problem

How can one determine the eigenvalues of A?
How long does it take?

Characteristic polynomial (I)

Definition

Let A be a square matrix of size d with coefficients in $\mathbb{K}$. We say that λ is an eigenvalue of A if there is a vector $v \neq 0$ such that $Av = \lambda v$.

Proposition

The eigenvalues are the roots of a specific polynomial called the characteristic polynomial of A defined by

$$P_A(\lambda) = \det(A - \lambda \mathrm{Id}) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} - \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{d-1,d} \\ a_{d1} & \cdots & a_{d,d-1} & a_{dd} - \lambda \end{vmatrix}.$$

Characteristic polynomial always has degree d.
Eigenvalues are not always in $\mathbb{K}$!

Characteristic polynomial (II)

Proposition

$P_A(\lambda) = \det(A - \lambda \mathrm{Id})$ and P_A has degree d.

Proof

Let λ be an eigenvalue of A and $v \neq 0$ be an eigenvector of A for λ, *i.e.* $Av = \lambda v$.

- One has $(A - \lambda \mathrm{Id})v = 0$ and $v \neq 0$ if, and only if, $\det(A - \lambda \mathrm{Id}) = 0$ if, and only if, λ is a root of P_A.
- When expanding the determinant, only one term has degree d, it is $(a_{11} - \lambda) \cdots (a_{dd} - \lambda)$.

Characteristic polynomial (III)

Examples

1. $$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},$$
$$P_A(\lambda) = \begin{vmatrix} 2-\lambda & 1 \\ 1 & 2-\lambda \end{vmatrix} = (2-\lambda)^2 - 1 = (\lambda - 1)(\lambda - 3),$$

2. $$B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$
$$P_B(\lambda) = \begin{vmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 = (\lambda - 1)^2.$$

Characteristic polynomial: complexity (I)

Naive method

$\rightarrow$ Gaussian elimination.

Characteristic polynomial: complexity (I)

Naive method

$\rightarrow$ Gaussian elimination.

- Matrix $A - \lambda \mathrm{Id}$ has coefficients in $\mathbb{K}[\lambda]$.

$\rightarrow$ If one inverts the pivot, one introduces rational fractions. They are very costly!

- Otherwise, one must take care that at each step, the computed determinant is a multiple of the target determinant.

Characteristic polynomial: complexity (II)

Example: Gaussian elimination, 1st attempt

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{pmatrix}$$

$$P_A(\lambda) = \begin{vmatrix} 1-\lambda & 1 & 1 \\ 1 & 2-\lambda & 2 \\ 1 & 2 & 3-\lambda \end{vmatrix} = \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \frac{\lambda^2-3\lambda+1}{1-\lambda} & \frac{-2\lambda+1}{1-\lambda} \\ 0 & \frac{-2\lambda+1}{1-\lambda} & \frac{\lambda^2-4\lambda+1}{1-\lambda} \end{vmatrix}$$

$$= \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \frac{\lambda^2-3\lambda+1}{1-\lambda} & \frac{-2\lambda+1}{1-\lambda} \\ 0 & 0 & \frac{\lambda^4-7\lambda^3+12\lambda^2-4\lambda}{(1-\lambda)(\lambda^2-3\lambda+1)} \end{vmatrix}.$$

Denominators introduce a memory overhead.

Characteristic polynomial: complexity (III)

Example: Gaussian elimination, 2nd attempt

$$
\begin{aligned}
P_A(\lambda) &= \begin{vmatrix} 1-\lambda & 1 & 1 \\ 1 & 2-\lambda & 2 \\ 1 & 2 & 3-\lambda \end{vmatrix} \\
&= \frac{1}{(1-\lambda)^2} \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \lambda^2-3\lambda+1 & -2\lambda+1 \\ 0 & -2\lambda+1 & \lambda^2-4\lambda+1 \end{vmatrix} \\
&= \frac{1}{(1-\lambda)^2(\lambda^2-3\lambda+1)} \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \lambda^2-3\lambda+1 & -2\lambda+1 \\ 0 & 0 & \lambda^4-7\lambda^3+12\lambda^2-4\lambda \end{vmatrix}.
\end{aligned}
$$

- Divisions of polynomials are still needed.
- The degrees of the polynomials are multiplied by two at each step of the Gaussian elimination.

Characteristic polynomial: complexity (III)

Example: Gaussian elimination, 2nd attempt

$$
\begin{aligned}
P_A(\lambda) &= \begin{vmatrix} 1-\lambda & 1 & 1 \\ 1 & 2-\lambda & 2 \\ 1 & 2 & 3-\lambda \end{vmatrix} \\
&= \frac{1}{(1-\lambda)^2} \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \lambda^2-3\lambda+1 & -2\lambda+1 \\ 0 & -2\lambda+1 & \lambda^2-4\lambda+1 \end{vmatrix} \\
&= \frac{1}{(1-\lambda)^2(\lambda^2-3\lambda+1)} \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \lambda^2-3\lambda+1 & -2\lambda+1 \\ 0 & 0 & \lambda^4-7\lambda^3+12\lambda^2-4\lambda \end{vmatrix}.
\end{aligned}
$$

- Divisions of polynomials are still needed.
- The degrees of the polynomials are multiplied by two at each step of the Gaussian elimination.

$\rightarrow$ We deal with polynomials of degree 2^{d-1} at the end!

Characteristic polynomial: complexity (III)

Example: Gaussian elimination, 2nd attempt

$$
\begin{aligned}
P_A(\lambda) &= \begin{vmatrix} 1-\lambda & 1 & 1 \\ 1 & 2-\lambda & 2 \\ 1 & 2 & 3-\lambda \end{vmatrix} \\
&= \frac{1}{(1-\lambda)^2} \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \lambda^2-3\lambda+1 & -2\lambda+1 \\ 0 & -2\lambda+1 & \lambda^2-4\lambda+1 \end{vmatrix} \\
&= \frac{1}{(1-\lambda)^2(\lambda^2-3\lambda+1)} \begin{vmatrix} 1-\lambda & 1 & 1 \\ 0 & \lambda^2-3\lambda+1 & -2\lambda+1 \\ 0 & 0 & \lambda^4-7\lambda^3+12\lambda^2-4\lambda \end{vmatrix}.
\end{aligned}
$$

- Divisions of polynomials are still needed.
- The degrees of the polynomials are multiplied by two at each step of the Gaussian elimination.

$\rightarrow$ We deal with polynomials of degree 2^{d-1} at the end!

$\rightarrow$ The complexity would be exponential in d. This cannot be right.

Characteristic polynomial: algorithm (I)

Interpolation method

- Characteristic polynomial has degree d.

Characteristic polynomial: algorithm (I)

Interpolation method

- Characteristic polynomial has degree d.

$\rightarrow$ The complexity should be polynomial in d.

Characteristic polynomial: algorithm (I)

Interpolation method

- Characteristic polynomial has degree d.

$\rightarrow$ The complexity should be polynomial in d.

$\rightarrow$ It suffices to know $d+1$ of its value to compute it.

- One computes $d+1$ determinants of $A-\lambda_0 \mathrm{Id}, \ldots, A-\lambda_d \mathrm{Id}$ for different $\lambda_0, \ldots, \lambda_d$.

Characteristic polynomial: algorithm (I)

Interpolation method

- Characteristic polynomial has degree d.

$\rightarrow$ The complexity should be polynomial in d.

$\rightarrow$ It suffices to know $d+1$ of its value to compute it.

- One computes $d+1$ determinants of $A-\lambda_0 \mathrm{Id}, \ldots, A-\lambda_d \mathrm{Id}$ for different $\lambda_0, \ldots, \lambda_d$.

$\rightarrow$ By Lagrange interpolation, one can recover the characteristic polynomial.

Characteristic polynomial: algorithm (II)

Algorithm

1. Pick $\lambda_0, \ldots, \lambda_d \in \mathbb{K}$ pairwise distinct.
2. **for** i **from** 0 **to** d

   $a_i \leftarrow \det(A - \lambda_i \mathrm{Id})$.
3. Call LagrangeInterpol with $\lambda_0, \ldots, \lambda_d$, $a_0, \ldots, a_d$.

Characteristic polynomial: algorithm (III)

Complexity

1. Computation of $d+1$ determinants of size d: $O(d^4)$.
2. Interpolation of a polynomial of degree at most d: $O(d^2)$.

$\rightarrow$ Complexity is in $O(d^4)$.

Characteristic polynomial: algorithm (IV)

Warning

- If there are less than $d+1$ elements in $\mathbb{K}$, this cannot be used.

$\rightarrow$ This is not an issue in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

$\rightarrow$ This is an issue in $\mathbb{F}_p$, $\mathbb{F}_q$: the finite fields.

- In that case, one needs to pick up $\lambda_0, \ldots, \lambda_d$ in a bigger field $\mathbb{L}$ containing $\mathbb{K}$.

Maple

1. Use of linalg package, not LinearAlgebra (too young in Maple 10).
2. Use `collect` and `simplify` when dealing with rational fractions and polynomials.
   - $\rightarrow$ Maple will sort the terms by degree,
   - $\rightarrow$ and will write the expression with only one denominator.
3. Use `?package` and `?function` to see the help page of the chosen package or function.

Sylvester Matrix

Definition

Let P and Q be two polynomials of $\mathbb{K}[X]$ of degree m and n.

$$P = p_m X^m + \cdots + p_0$$
$$Q = q_n X^n + \cdots + q_0.$$

The Sylvester matrix associated to P and Q is the $(m+n) \times (m+n)$ matrix

$$\begin{pmatrix}
p_m & 0 & \cdots & 0 & q_n & 0 & \cdots & 0 \\
p_{m-1} & p_m & & \vdots & q_{n-1} & q_n & & \vdots \\
\vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\
 & p_{m-1} & & & & q_{n-1} & & \\
p_1 & \vdots & & 0 & q_1 & \vdots & & 0 \\
p_0 & p_1 & & p_m & q_0 & q_1 & & q_m \\
0 & p_0 & & p_{m-1} & 0 & q_0 & & q_{m-1} \\
\vdots & 0 & & \vdots & \vdots & 0 & & \vdots \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\
0 & 0 & \cdots & p_1 & 0 & 0 & \cdots & q_1 \\
 & & & p_0 & & & & q_0
\end{pmatrix}$$

Sylvester Matrix

Example

If $P = X^4 + 2X^3 + 3X^2 + 4X + 5$ and $Q = 9X^3 + 8X^2 + 7X + 6$, then their Sylvester Matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 9 & 0 & 0 & 0 \\ 2 & 1 & 0 & 8 & 9 & 0 & 0 \\ 3 & 2 & 1 & 7 & 8 & 9 & 0 \\ 4 & 3 & 2 & 6 & 7 & 8 & 9 \\ 5 & 4 & 3 & 0 & 6 & 7 & 8 \\ 0 & 5 & 4 & 0 & 0 & 6 & 7 \\ 0 & 0 & 5 & 0 & 0 & 0 & 6 \end{pmatrix}$$