线性代数

逆矩阵

节选自第2章 矩阵及其运算 第三节

授课对象 理工商科一、二年级本科生

军密游戏闯关

破译军密矩阵1

游戏介绍

已知加密矩阵$A=\begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix}$，信息矩阵$B=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$，通过矩阵的乘法，转换成密文矩阵$C$，即

$$AB=\begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix}\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}4 & 3\\ 2 & 1\end{pmatrix}=C$$

军密游戏闯关

方案1：

已知加密矩阵$C_1=\begin{pmatrix}1&2\\0&1\end{pmatrix}$，密文矩阵$E_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，如何求解信息矩阵X。

$$C_1\ X=E_2$$

方案1：$X=\dfrac{E_2}{C_1}=\dfrac{\begin{pmatrix}1&0\\0&1\end{pmatrix}}{\begin{pmatrix}1&2\\0&1\end{pmatrix}}$

任务失败

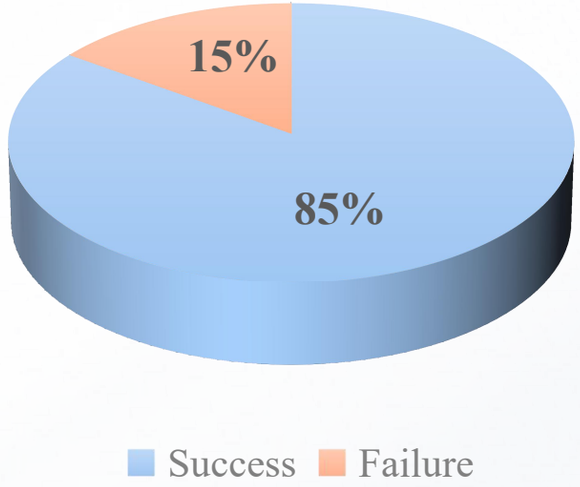
返回上一步

第二关：假设已知加密矩阵J，寻找信息矩阵X，使其JX=E

方案1：若J=$\begin{pmatrix}1&1\\1&1\end{pmatrix}$，能找到矩阵X ⇒ JX=E

方案2：若J=$\begin{pmatrix}1&1\\1&2\end{pmatrix}$，能找到矩阵X ⇒ JX=E

请选择你的方案



信息的加密与破译蕴含着什么数学原理？

目　录

CONTENTS

一、　逆矩阵定义

二、　逆矩阵判定

三、　逆矩阵应用

逆矩阵定义

$$ab = ba = 1 \Rightarrow b = a^{-1}$$

$$AB = BA = \underline{E} \Rightarrow B = A^{-1}$$

1

逆矩阵定义

定义 **对于n阶矩阵A，若存在n阶矩阵B，使得$AB=BA=E$，则称矩阵A是可逆的，并称B为A的逆矩阵，简称逆阵.**

- B矩阵是否可逆，B的逆矩阵是什么？
- A的逆矩阵是否唯一？
- 任意矩阵都可逆吗？

逆矩阵定义

定义 对于n阶矩阵A，若存在n阶矩阵B，使得$AB=BA=E$，则称矩阵A是可逆的，并称B为A的逆矩阵，简称逆阵.

- B矩阵是否可逆，B的逆矩阵是什么？

对称美

分析

$$AB=BA=E \Leftrightarrow \begin{cases} BA=E \\ AB=E \end{cases} \Rightarrow B\text{可逆}, B^{-1}=A.$$

逆矩阵定义

定义 对于n阶矩阵A，若存在n阶矩阵B，使得$AB=BA=E$，则称矩阵A是可逆的，并称B为A的逆矩阵，简称逆阵.

- A的逆矩阵是否唯一?

分析

若$AB=BA=E$，且 $AC=CA=E$，

则 $B=BE=B(AC)=(BA)C=EC=C$，

反证法

$\Rightarrow$ A 的逆矩阵是唯一的，记作A^{-1}.

单位矩阵是"雷锋"矩阵，看似可有可无，实则至关重要.

逆矩阵定义

定义 对于n阶矩阵A，若存在n阶矩阵B，使得$AB=BA=E$，

则称矩阵A是可逆的，并称B为A的逆矩阵，简称逆阵.

➢ 任意矩阵都可逆吗？

分析

一般情况下，$AB \neq BA$

$$A_{m\times n}B_{n\times m}=E_{m\times m}$$

$$B_{n\times m}A_{m\times n}=E_{n\times n}$$

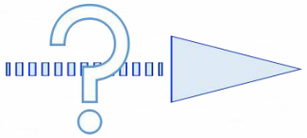
$$\Rightarrow m=s=n.$$

方阵

显然，n 阶 O 矩阵不可逆.

逆矩阵判定

问题 任意非零方阵都可逆吗？

$a \neq 0 \Leftrightarrow a$可逆  $A \neq O \Leftrightarrow A$ 可逆

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a+2c & b+2d \\ a+2c & b+2d \end{pmatrix}\overset{?}{=}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$1=0$ 矛盾 因此$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$不可逆.

结论 并非任意非零方阵都可逆.

问题探究

- 如何判定方阵 A 可逆？
- 如果 A 可逆, 怎样求 A^{-1}？

逆矩阵判定

定理1 若矩阵A可逆, 则$|A|\neq 0$.

分析 A可逆, 即有A^{-1}, 使 $AA^{-1}=E$

$$\Rightarrow |AA^{-1}|=|E|$$

$$\Rightarrow |A||A^{-1}|=1$$

$$\Rightarrow |A|\neq 0$$

结论 A可逆 $\Rightarrow |A|\neq 0$

反之成立吗?

定理2 若$|A|\neq 0$, 则矩阵A可逆, 且 $A^{-1}=\dfrac{A^*}{|A|}$.

分析 若$\exists B$,使得 $AB=BA=E$,则A可逆.

$$AA^*=A^*A=|A|E$$

若$|A|\neq 0$, 有

$$A\left(\frac{A^*}{|A|}\right)=\left(\frac{A^*}{|A|}\right)A=E$$

结论 A可逆, 且 $A^{-1}=\dfrac{1}{|A|}A^*$.

探究结果

如何判定方阵 A 可逆？

以“量”定“质”

方阵A 可逆的充分必要条件是$|A|\neq 0$.

如果A可逆,怎样求A^{-1}?

$$A^{-1}=\frac{1}{|A|}A^{*}$$

逆矩阵计算

例1 讨论矩阵$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$的可逆性，并求$A^{-1}$.

分析

第一步：判断 A 可逆

$$|A|=\begin{vmatrix} a & b \\ c & d \end{vmatrix}=ad-bc$$

当$ad-bc=0$ 时，A不可逆；

当$ad-bc\neq 0$ 时，A 可逆.

第二步：求 A^*

$$A^*=\begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix}=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$A_{11}=d$, $A_{12}=-c$

$A_{21}=-b$, $A_{22}=a$

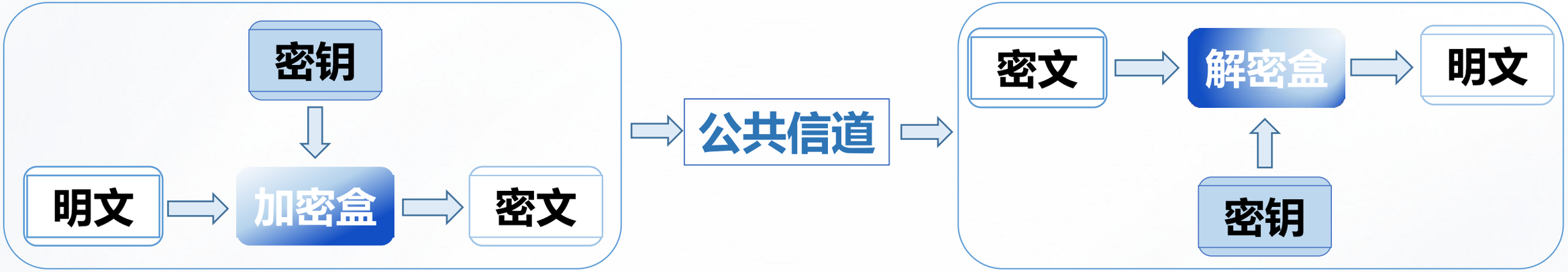
第三步：求 A^{-1}

$$A^{-1}=\frac{1}{|A|}A^*=\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

主对调

副变号

应用案例：保密通信



信息加密与破译——战场上的智慧较量

1943年，数学家华罗庚仅用一夜时间便发现了日军使用的缪比乌斯函数加密方法，他利用该函数的反函数(即**逆矩阵在函数领域的对应概念**)破解了密码，从而化解了一场轰炸危机.

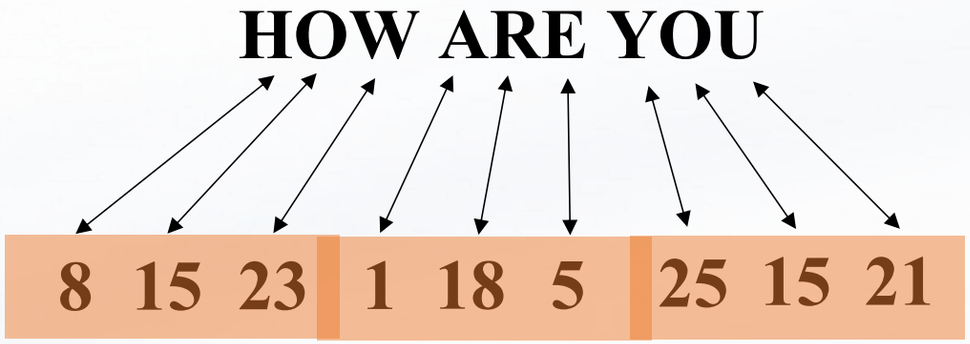
应用案例: 保密通信

执行任务1: 传递信息“ HOW ARE YOU”.

希尔密码是一种基于矩阵理论的加密技术.

将26个英文字母与数字一一对应:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26



明文 $X=\begin{pmatrix} 8 & 1 & 25 \\ 15 & 18 & 15 \\ 23 & 5 & 21 \end{pmatrix}$

应用案例: 保密通信

$$A=\begin{pmatrix}1&2&1\\2&5&3\\2&3&2\end{pmatrix}$$

密钥矩阵： 1. 元素都是正整数;

2. 密钥矩阵 $|A|=\pm 1$.

加密

$$AX=C$$

$$\begin{pmatrix}1&2&1\\2&5&3\\2&3&2\end{pmatrix}\begin{pmatrix}8&1&25\\15&18&15\\23&5&21\end{pmatrix}=\begin{pmatrix}61&42&76\\160&107&188\\107&66&137\end{pmatrix}$$

密钥　　明文　　密文

对应发出去的密文编码依次为: 61, 160, 107, 42, 107, 66, 76, 188, 137.

接收方收到发送方的密文后, 应该如何解码才可以得到原文信息?

应用案例: 保密通信

接收方收到发送方的密文后, 应该如何解码才可以得到原文信息?

$$AX=\begin{pmatrix}1&2&1\\2&5&3\\2&3&2\end{pmatrix}\begin{pmatrix}8&1&25\\15&18&15\\23&5&21\end{pmatrix}=\begin{pmatrix}61&42&76\\160&107&188\\107&66&137\end{pmatrix}=C$$

密钥　　明文　　密文

$|A|=1\neq 0$, 故A 可逆.

解密　$AX=C\Rightarrow A^{-1}AX=A^{-1}C\Rightarrow (A^{-1}A)X=A^{-1}C\Rightarrow EX=A^{-1}C$

$$X=A^{-1}C$$

应用案例: 保密通信

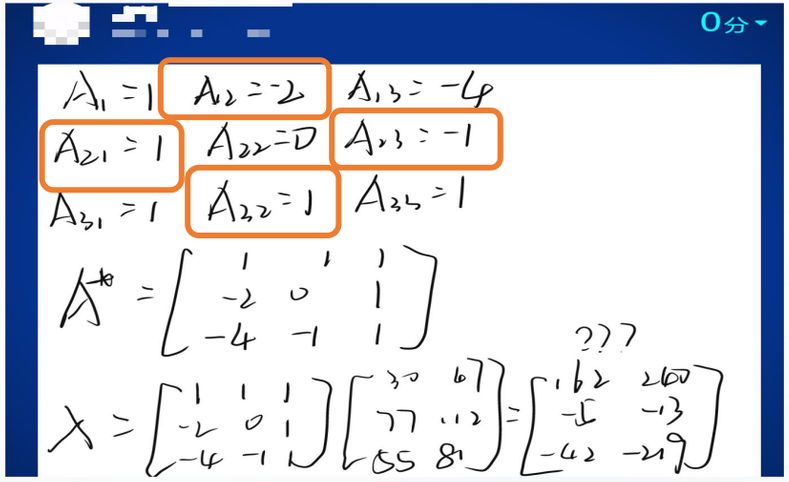
执行任务2：你接收到一组密文: 30, 77, 55, 47, 112, 81, 请立即破译密文.

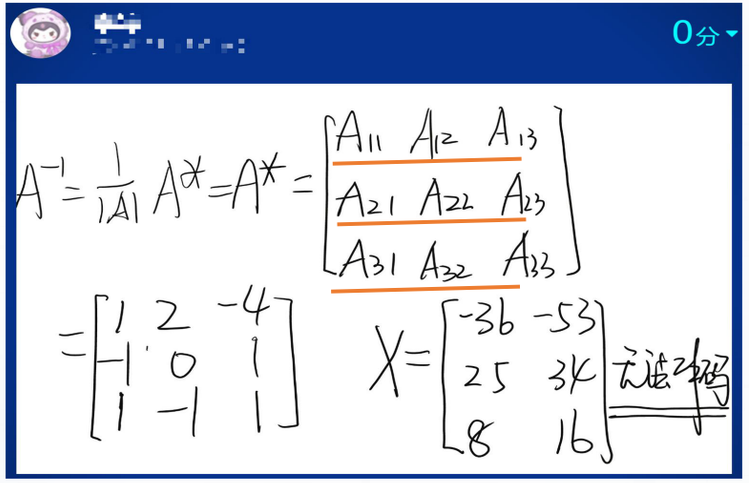
$$AX=C,\text{其中}A=\begin{pmatrix}1&2&1\\2&5&3\\2&3&2\end{pmatrix},C=\begin{pmatrix}30&47\\77&112\\55&81\end{pmatrix}$$

$|A|=1\neq 0$, A 可逆, 且$A^{-1}=A^{*}$

保密遮挡

HELP ME　　无法解码　　HEMP NE





是否存在更优化的方法求解逆矩阵?

⚠ 代数余子式符号

⚠ 代数余子式要转置

应用案例：保密通信

科学家始终要把国家的责任摆在第一位，任何条件都比不上祖国的需要.

广义逆矩阵应用

Moore-Penrose广义逆矩阵理论

定义 设$A \in C^{m\times n}$为任意复数矩阵，如果存在$G \in C^{m\times n}$，满足

- 1) $AGA = A$
- 2) $GAG = G$
- 3) $(AG)^H = AG$
- 4) $(GA)^H = GA$

4个方程的全部或一部分，则称G 为A 的一个广义逆矩阵，并把上述4个方程叫做$Moore-Penrose$ 方程.

Roger Penrose
诺贝尔物理学奖得主

广义逆矩阵在飞艇×型尾翼舵面解耦中的应用

杜 伟 罗战虎
（中国特种飞行器研究所，湖北荆门 448035）

尾翼作为稳定、操控飞艇的重要部件，其布局形式多种多样。常见的布局形式有＋型和×型。由于×型尾翼在安装空间、操纵安全等方面较传统的＋型尾翼具有明显的优势[3]，因而在现代飞艇中应用非常广泛。但是，×型尾翼舵面的纵、横向通道是耦合的，不利于飞行控制律的设计。因此，将×型尾翼舵面解耦是设计飞行控制律的基础。本文基于最小范数广义逆矩阵的方法，给出了×型尾翼舵偏和通道舵偏之间的转换关系，成功实现解耦。

第58卷 第7期 西安交通大学学报 Vol.58 No.7
2024年7月 JOURNAL OF XI'AN JIAOTONG UNIVERSITY Jul. 2024

采用曲波变换和电容层析成像的两相流含水率测量方法

张皓冬[1]，陆程程[1]，胡红利[1]，杨海潮[1]，董海健[2]
(1. 西安交通大学电力设备电气绝缘国家重点实验室，710049，西安；
2. 西安西电电力电容器有限责任公司，710082，西安)

摘要：针对电容层析成像（ECT）逆问题的欠定性，提出了一种基于曲波变换的图像稀疏重构算法。首先，采用曲波变换基作为稀疏基，从多尺度对模拟介质分布图像进行稀疏表示，提高了ECT灰度值向量的稀疏度；其次，应用迭代软阈值算法对曲波系数进行稀疏重构，同时使用奇异值分解算法计算最优步敏度广义逆矩阵；最后，搭建ECT测量平台，通过静态实验重构5种典型实际流型，验证所提算法的有效性。实验结果表明，所提算法可有效抑制伪影，重构图像边界清晰。同时在图像相关系数、相对图像误差上均优于传统重构算法，比Landweber迭代算法相关系数提高约37.9%，相对误差减小约17.6%。基于稀疏重构的后处理图像可用于截面含水率的测量，含水率平均误差低于10%，最低为4.32%。该方法有效提高了ECT重构图像质量，能够满足天然气精准开采的工业需求。

关键词：电容层析成像；曲波变换；两相流；压缩感知；
中图分类号： **文献标志码**：A
DOI: 文章编号：

Two-Phase Flow Water Fraction Measurement Using Curvelet Transform and Electrical Capacitance Tomography

基于现场可编程门阵列的矩阵求逆算法设计

安国臣[1]，刘若凡[1]，赵满[2]，袁玉鑫[1]，王晓君[1]

的重大研究方向。

采用阵列信号处理方法来进行卫星导航系统的抗干扰算法有很多，其中采样矩阵求逆（sample matrix invert，SMI）算法具有很好的抗干扰性能，得到了广泛的应用。然而SMI算法需要进行矩阵求逆运算导致运算量过大，尤其是采用空时联合抗干扰时，矩阵维数很大，导致运算量激增，很难满足动态性能要求[5-6]。文献[7-8]中均对SMI算法的性能进行分析，说明了该算法相比较于其他的自适应处理算法有较好抗干扰性能，但是由于运算量较大导致硬件难以实现。

为了解决上面所说的运算量大的问题，常采用矩阵分解的方法进行求逆，其中矩阵分解常用的方

Cholesky分解矩阵$\boldsymbol{L}$，计算下三角矩阵$\boldsymbol{L}$的逆矩阵$\boldsymbol{S}$和三角矩阵相乘。下面对每个步骤进行具体说明。

1.1 计算Cholesky分解矩阵

设协方差矩阵$\boldsymbol{R}$由一个下三角矩阵$\boldsymbol{L}$与其共轭转置$\boldsymbol{L}^{\mathrm{H}}$的乘积组成，即

$$\boldsymbol{R} = \boldsymbol{L}\boldsymbol{L}^{\mathrm{H}} \tag{1}$$

式(1)中：

$$\boldsymbol{R} = \begin{bmatrix} r_{11} & \cdots & r_{1k} & \cdots & r_{1M} \\ \vdots & & \vdots & & \vdots \\ r_{k1} & \cdots & r_{kk} & \cdots & r_{kM} \\ \vdots & & \vdots & & \vdots \\ r_{M1} & \cdots & r_{Mk} & \cdots & r_{MM} \end{bmatrix} \tag{2}$$

逆矩阵

1. **定义**：$AB=BA=E$，则B 为A 的逆矩阵.

2. **定理**：$|A|\neq 0 \Leftrightarrow A$ 可逆，且$A=\dfrac{1}{|A|}A^{*}$.

3. **计算**：定义法；伴随矩阵公式法.

4. **应用**：保密通信($AX=C$).

课后作业

必做题

1. 结合课中保密通信案例，设计一种新的加密方法.

2. 设方阵A满足$A^2-A-2E=O$，证明A及$A+2E$都可逆，并求逆矩阵.

思考题

(华罗庚等式)设n阶矩阵$A, B, AB-E$均可逆，证明$A-B^{-1}$以及$(A-B^{-1})-A^{-1}$均可逆，并求它们的逆矩阵.

阅读云平台相关文献，了解华罗庚等式在数学或其他学科中的应用，总结你们的发现，并上传小组报告.

华罗庚
(1910-1985)