

# 小学期数学建模能力 提升课程

乔琛

数学与统计学院

qiaochen@xjtu.edu.cn

# 代数模型

利用线性代数等知识去解决一些实际问题,使大家体会向量空间等抽象概念怎样运用到解决实际问题的过程中去。

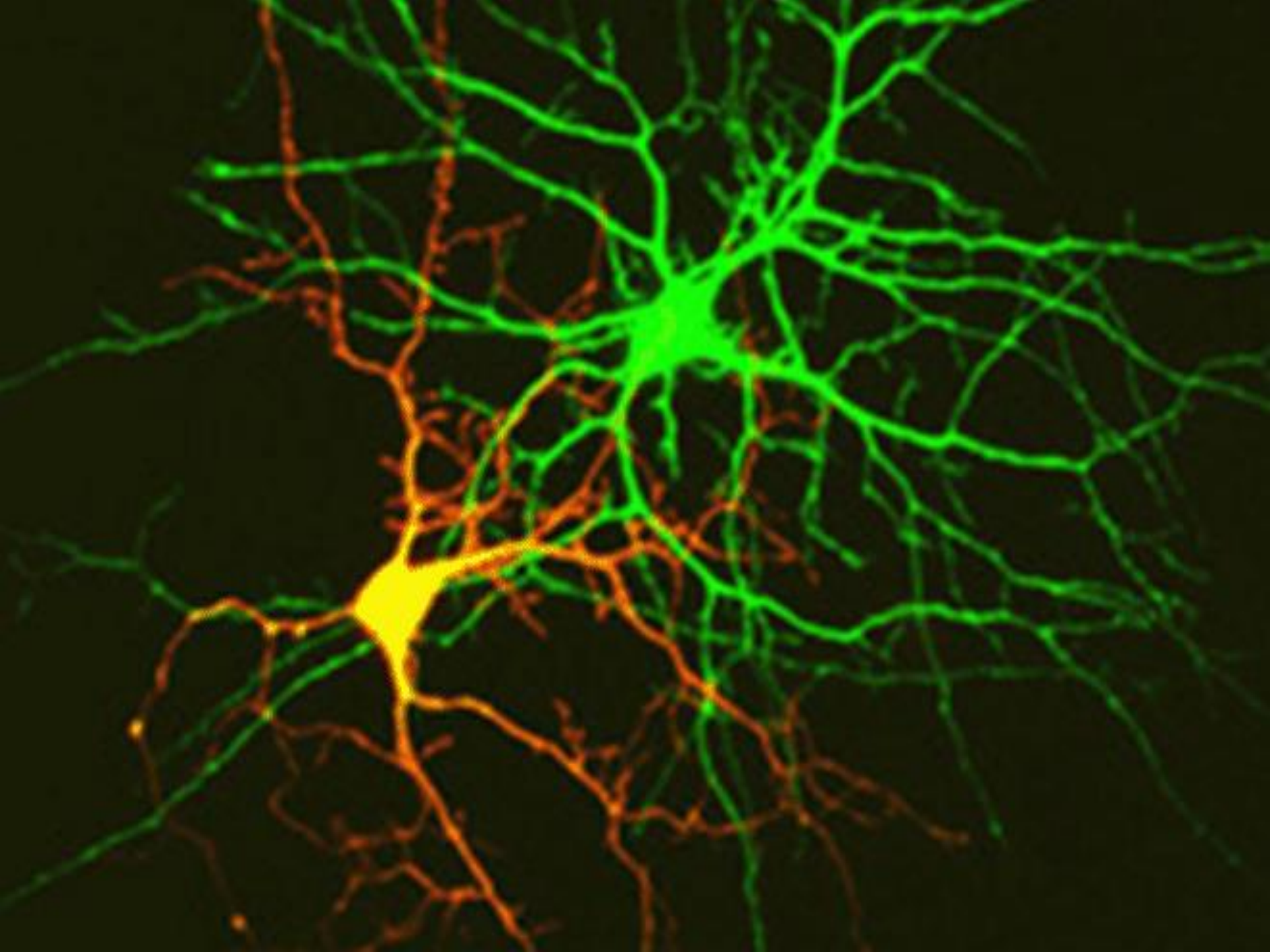
# 神经网络的数学模型

## 人脑

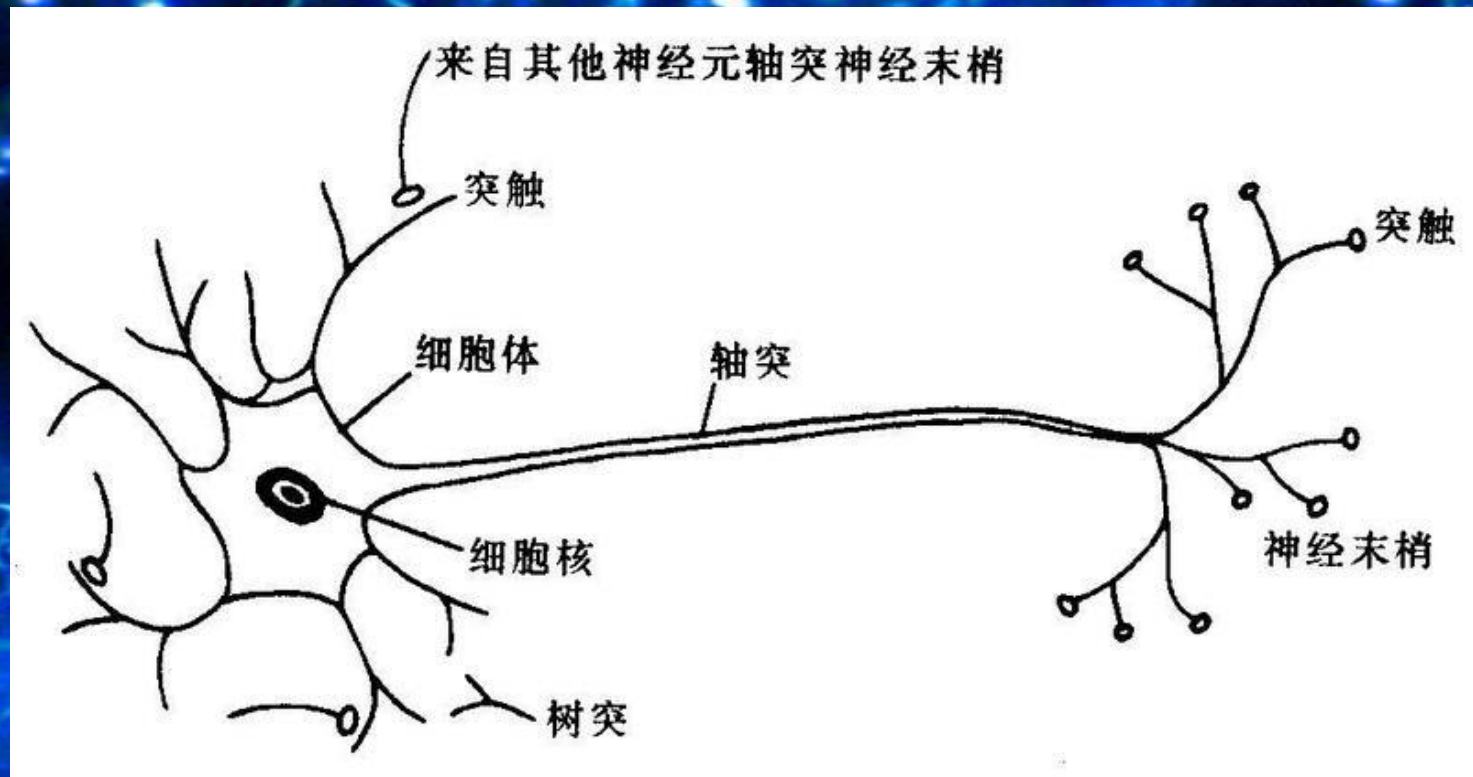
- ◆ 复杂的生物神经网络

由约 $10^{11}$  ~  $10^{13}$  个高度互连的神经细胞(神经元)构成

- ◆ 能灵活处理各种复杂、不精确的信息
- ◆ 善于理解语言、图象，具有直觉感知等功能

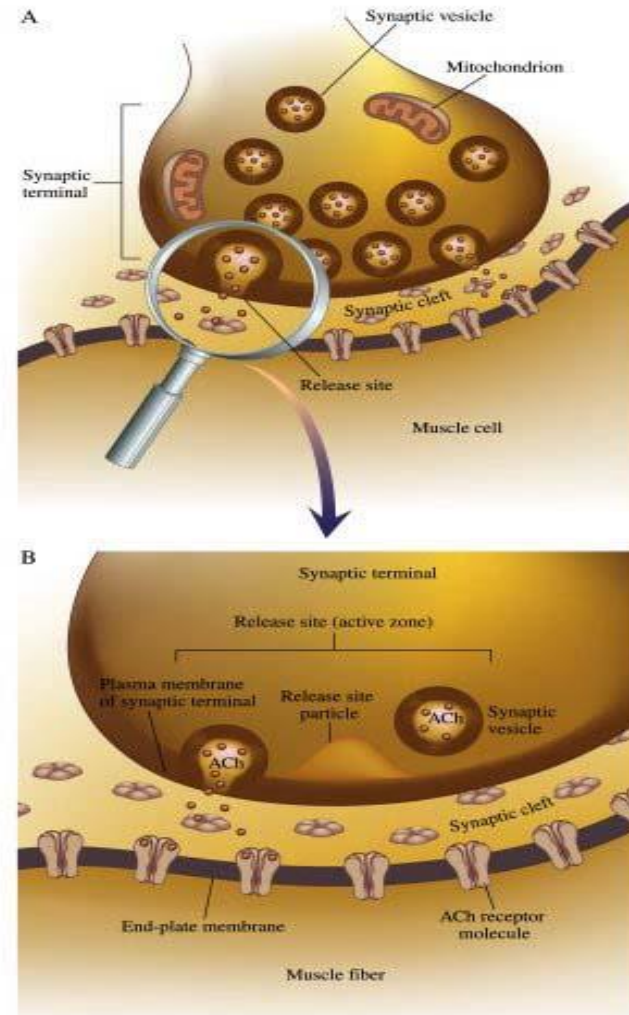
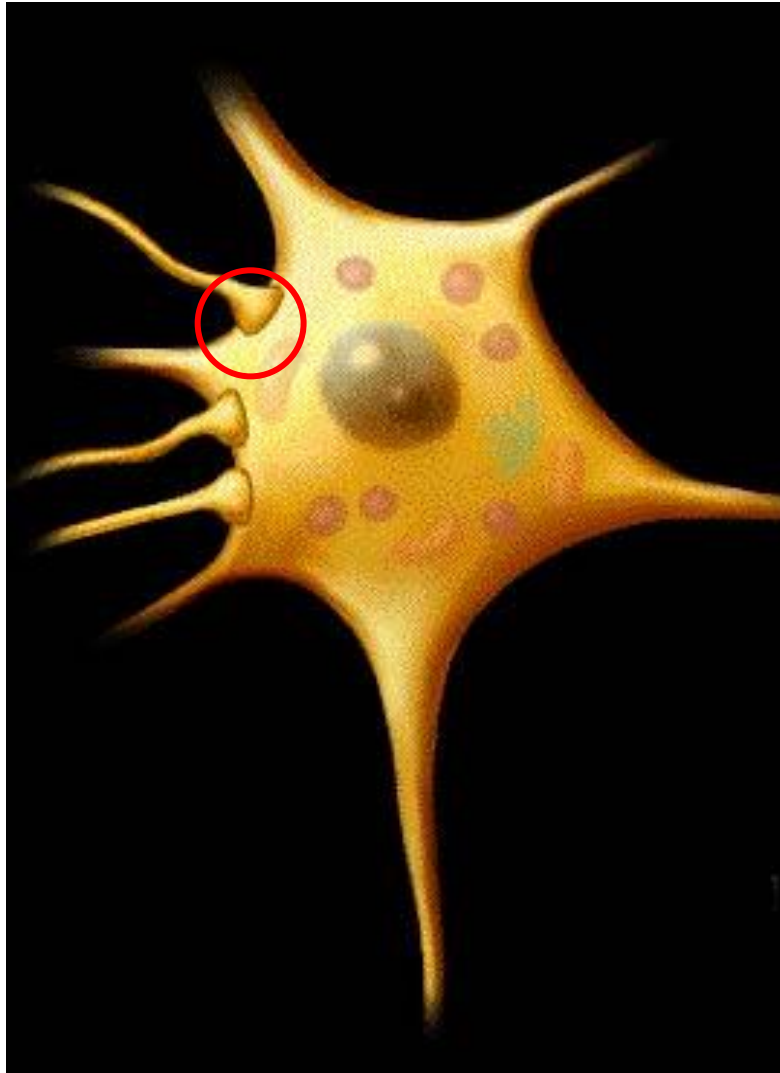




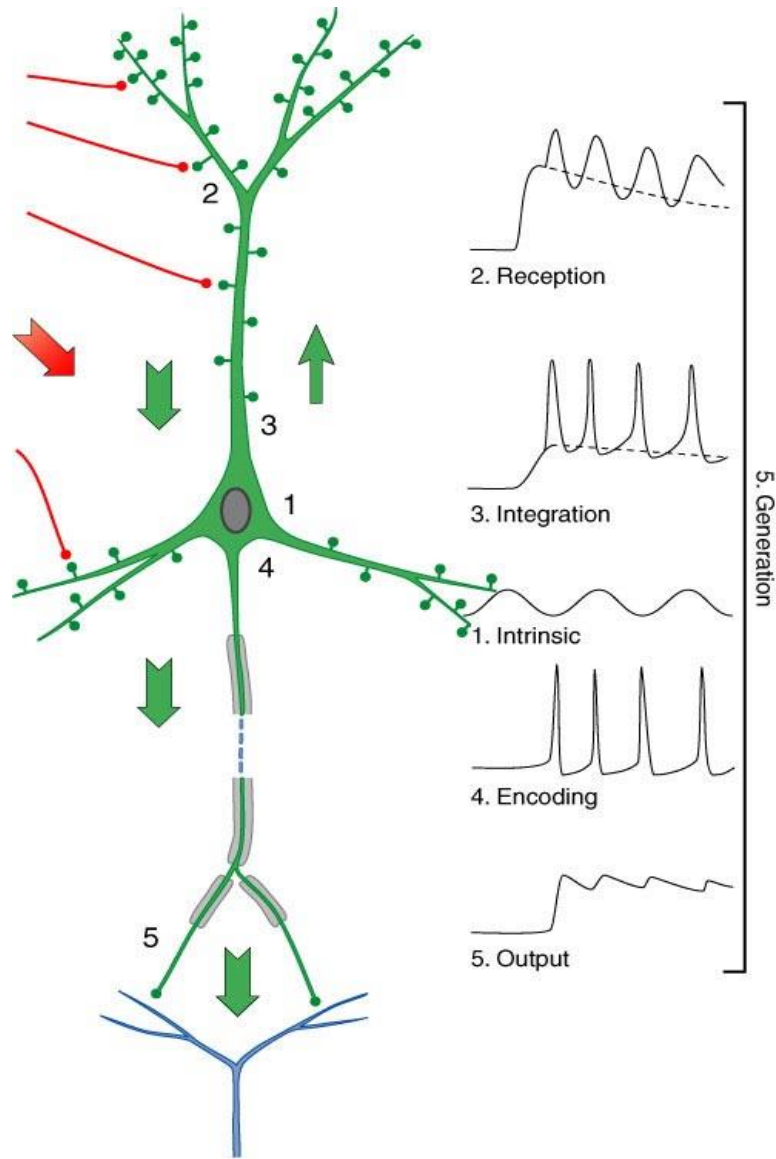


大脑以神经元为结构功能单位

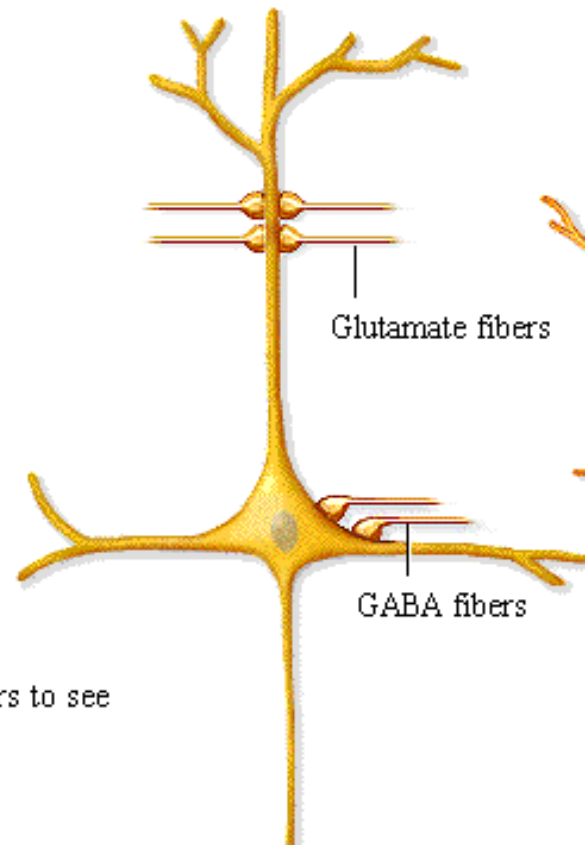
# 神经元间的联接 - - 突触



# 神经元信息整合模式图

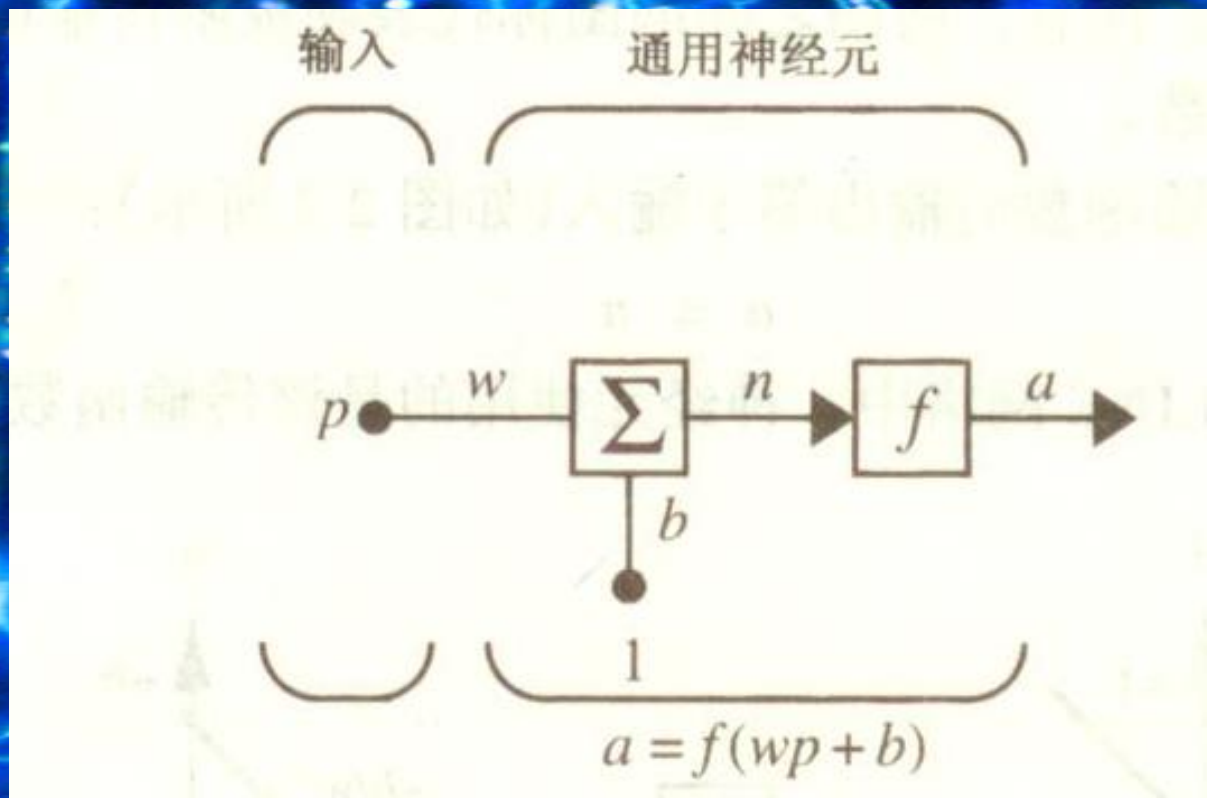


Copyright © 2002, Elsevier Science (USA). All rights reserved.



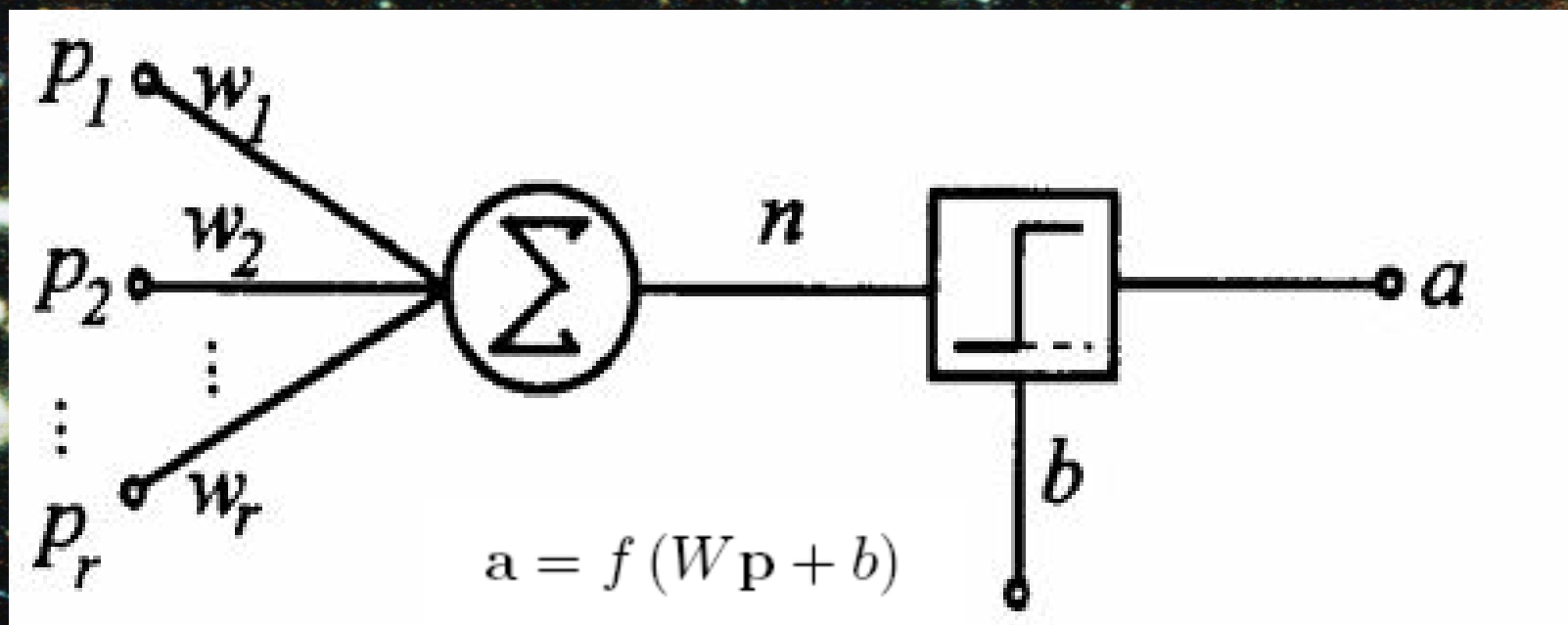
fibers to see  
gain.



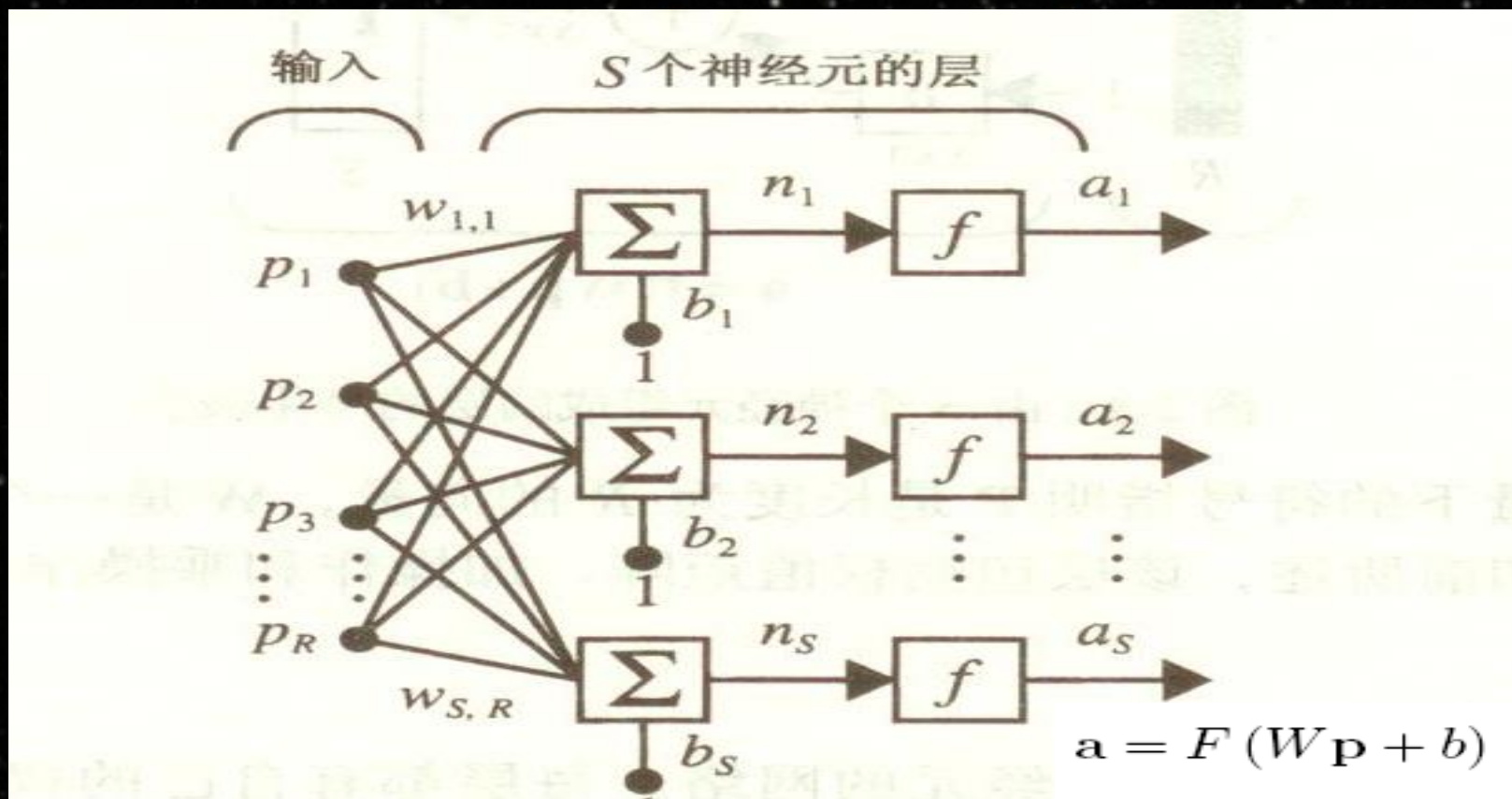


**神经元模型：单输入神经元**

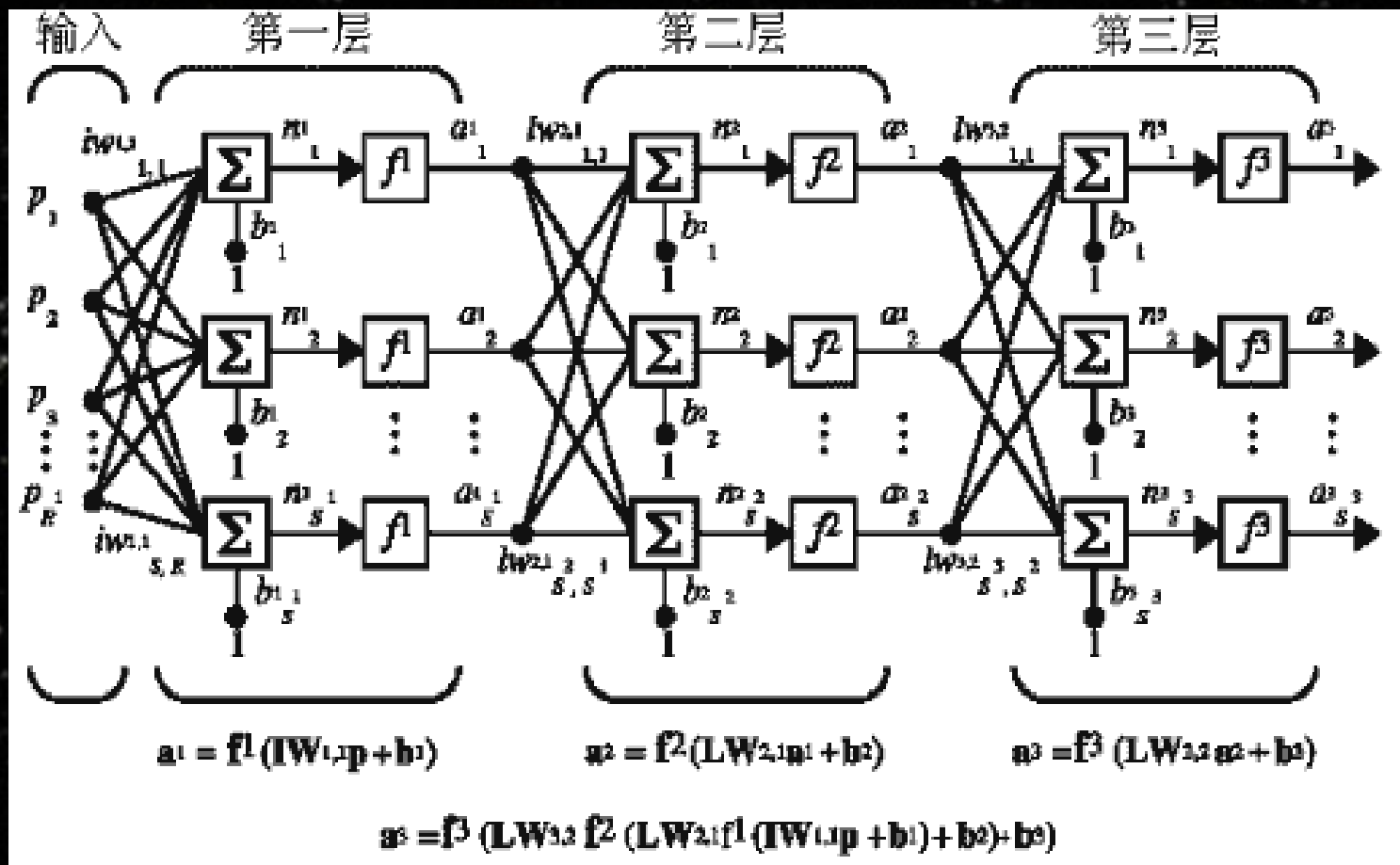




神经元模型：多输入神经元



**S个神经元组成的层**



### 3层神经网络

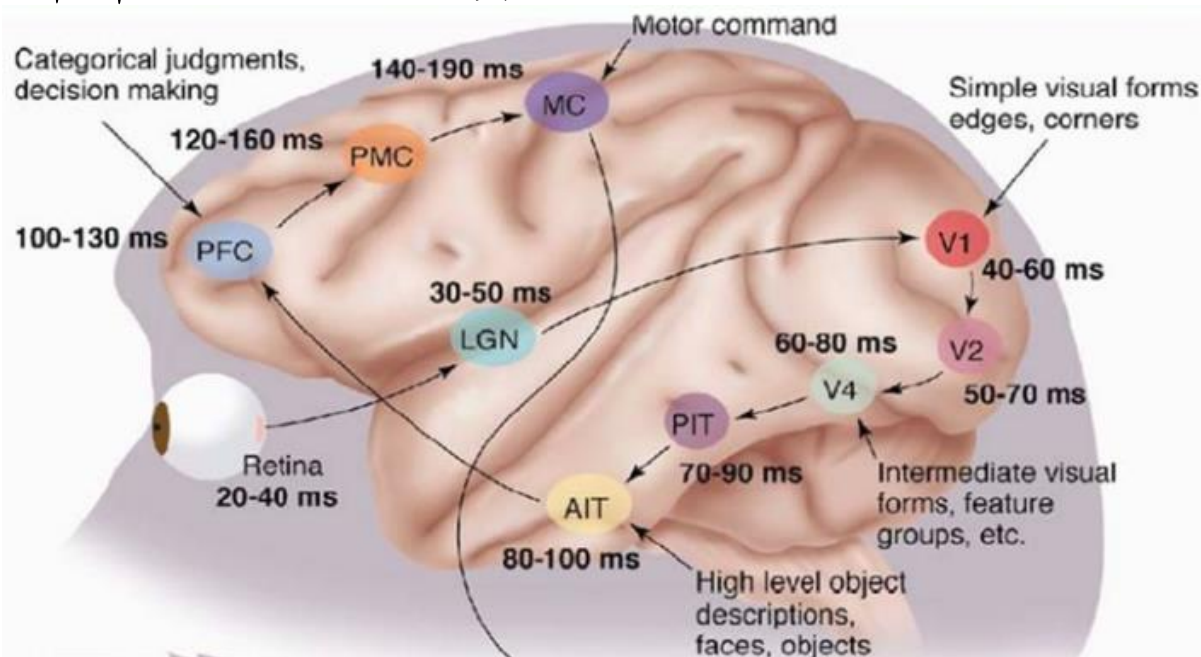


差分方程：

$$a(t + 1) = F(Wa(t) + b)$$

# 采用层次网络结构的动机

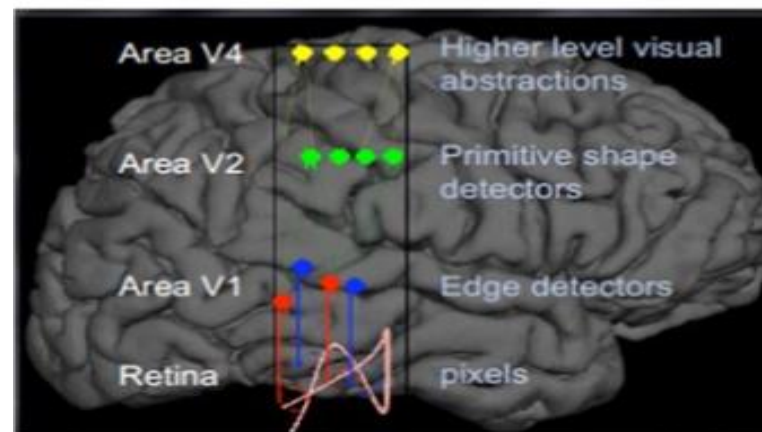
- 人脑视觉机理
  - ✓ 1981年的诺贝尔医学奖获得者 David Hubel和TorstenWiesel发现了视觉系统的信息处理机制
  - ✓ 发现了一种被称为“方向选择性细胞的神经元细胞，当瞳孔发现了眼前的物体的边缘，而且这个边缘指向某个方向时，这种神经元细胞就会活跃



# 采用层次网络结构的动机

## ● 人脑视觉机理

- ✓ 人的视觉系统的信息处理是分级的
- ✓ 高层特征是低层特征的组合，从低层到高层的特征表示越来越抽象，越来越能表现语义或者意图
- ✓ 抽象层面越高，存在的可能猜测就越少，越利于分类



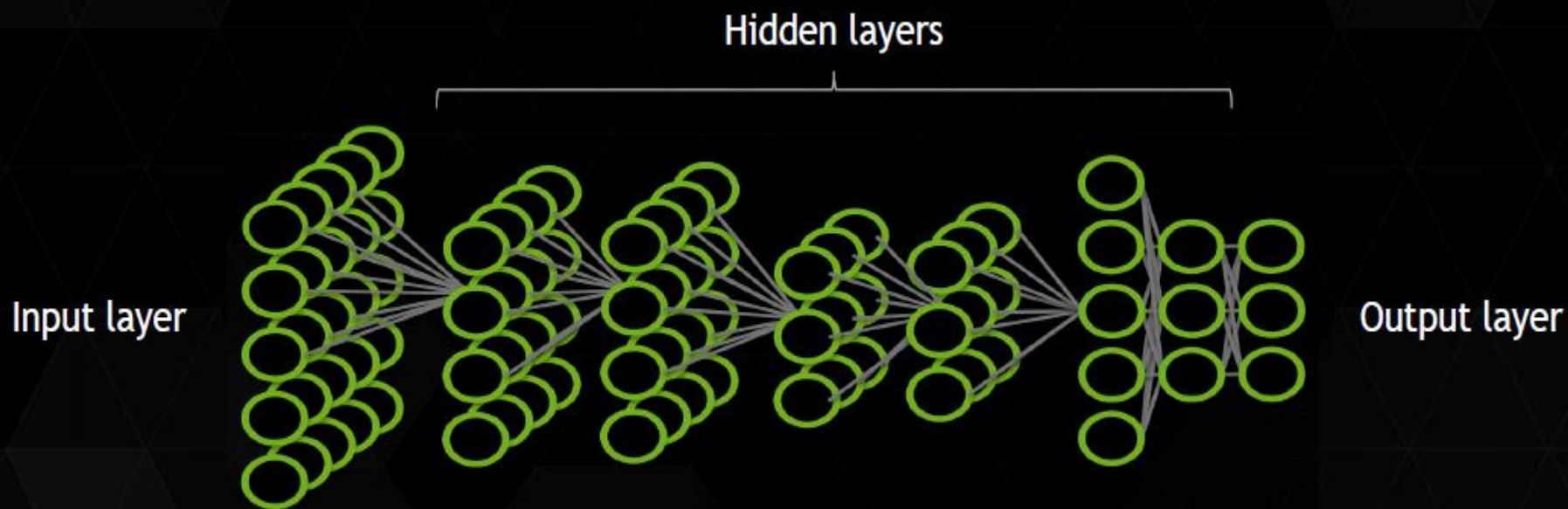


# 深度学习:多隐层的人工神经网络

- 2006年，加拿大多伦多大学教授、机器学习领域的泰斗Geoffrey Hinton在《科学》上发表论文提出深度学习主要观点：多隐层的人工神经网络具有优异的特征学习能力，学习得到的特征对数据有更本质的刻画，从而有利于可视化或分类

**本质：**通过构建多隐层的模型和海量训练数据（可为无标签数据），来学习更有用的特征，从而最终提升分类或预测的准确性。“深度模型”是手段，“特征学习”是目的

# 含有多个隐层的深度学习模型

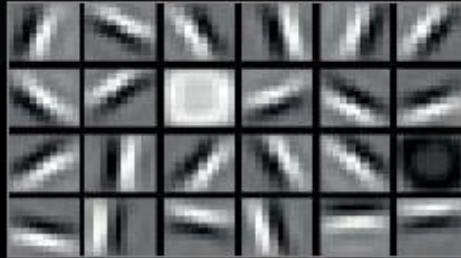


# DEEP NEURAL NETWORK (DNN)

Raw data



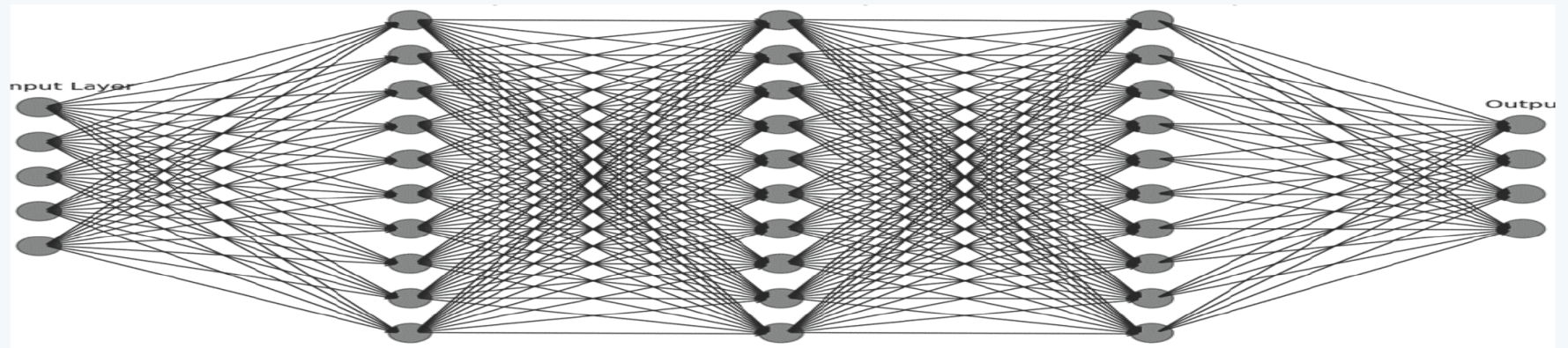
Low-level features



Mid-level features

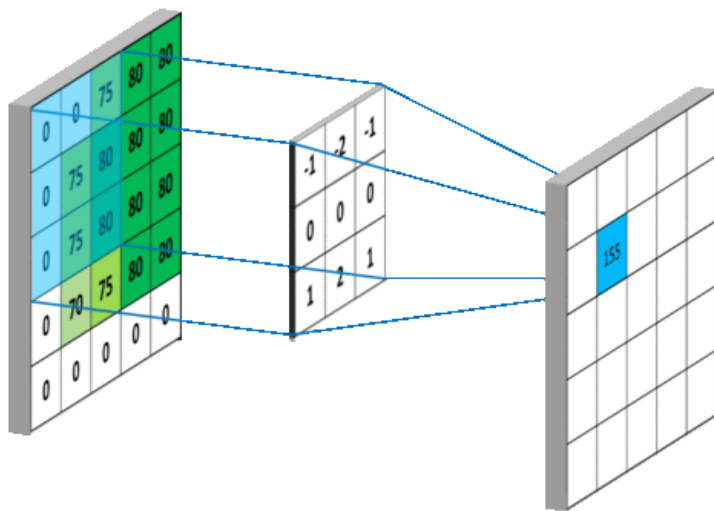


High-level features

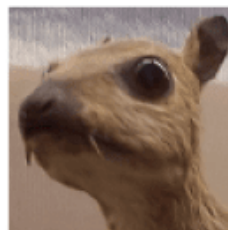




# CNN模型



Input image



Convolution  
Kernel

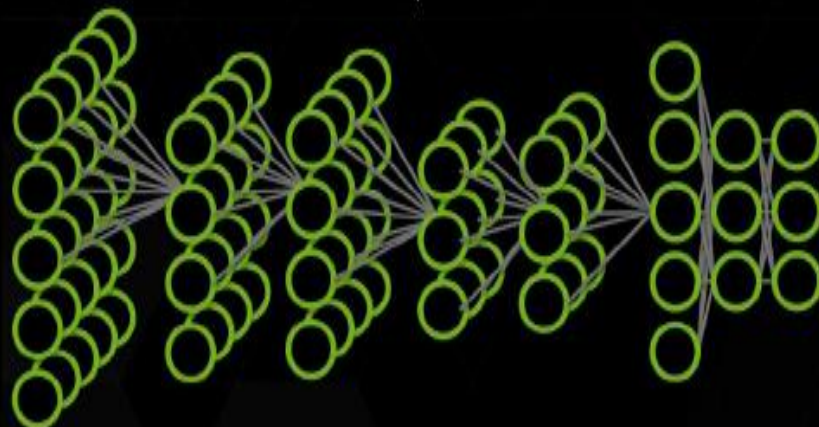
$$\begin{bmatrix} -1 & -1 & -1 \\ -1 & 8 & -1 \\ -1 & -1 & -1 \end{bmatrix}$$

Feature map



通过卷积核对于图像的作用，可实现对于图像某些特征的提取

Train:



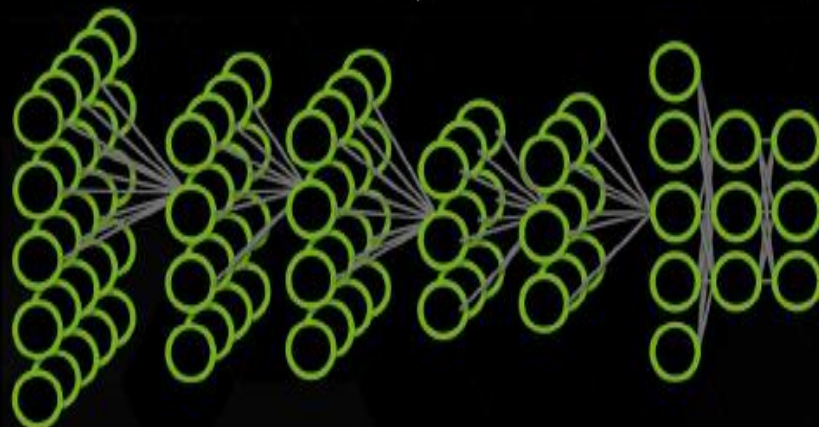
Errors



Dog  
Cat  
Raccoon



Deploy:

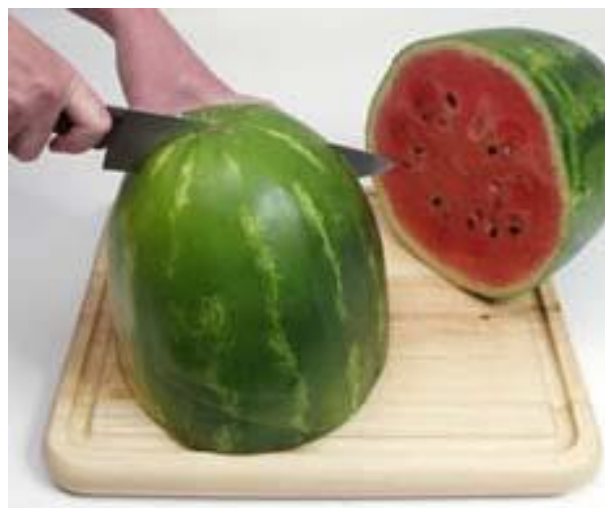


Dog



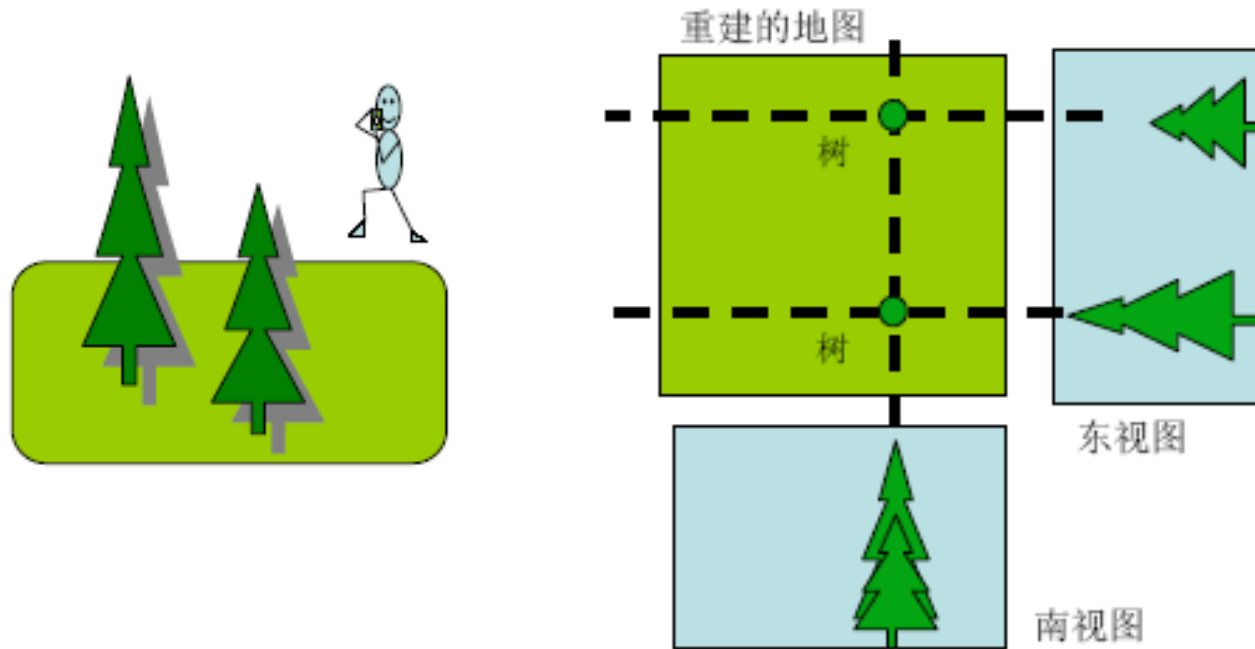
# 断层成像中的基础应用

断层成像：获取一个物体内部的截面图像



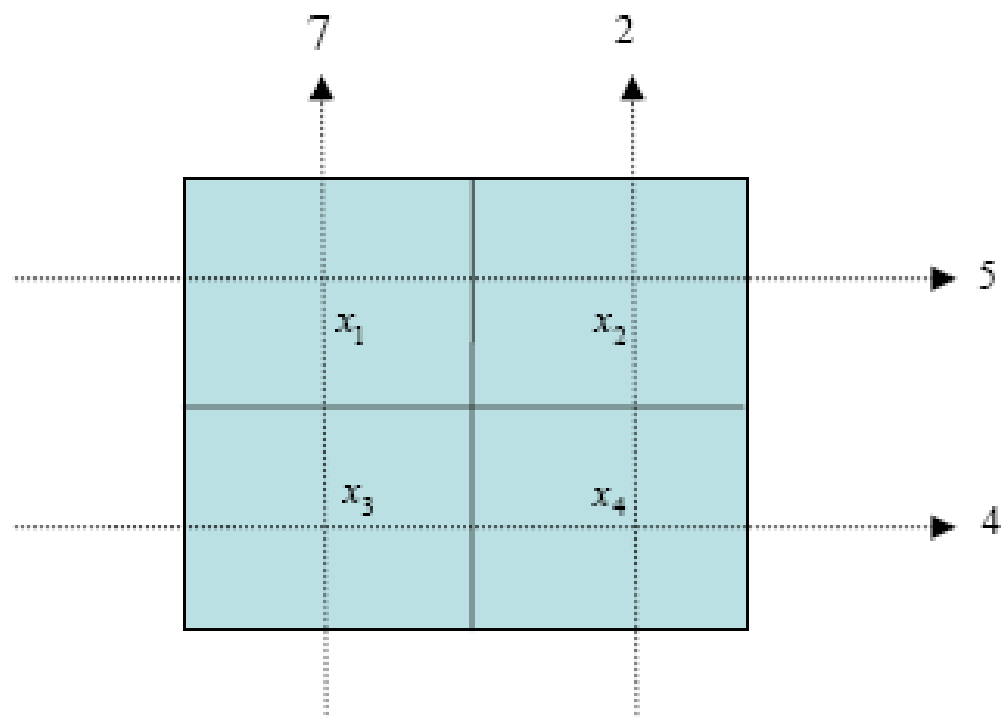
**为了获取西瓜的内部情况，我们只需切开它。  
但对一个病人呢？**





从不同方向拍到照片：投影（Projection）

用所获取的照片得到整个公园的地图：重建/反投影  
（ Backprojection ）



断层成像：数学计算的手段解决

CT (Computed Tomography 计算机断层成像，直译为计算出的断层成像)

矩阵每一行(列)的求和过程：

图像的射线和(线积分)及投影数据

从物体投影数据得到物体内部断层成像的过程：

图像重建

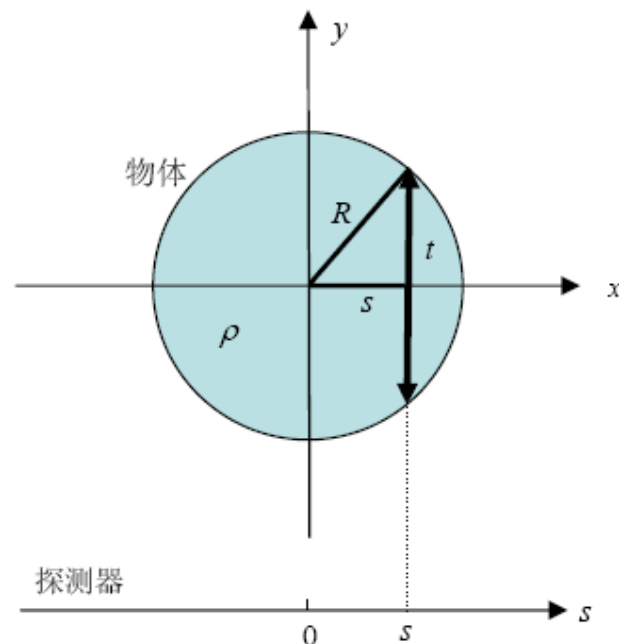
# 投影 (射线和, 线积分)

物体:  $x$ - $y$ 平面中一个均匀圆盘

圆心: 坐标原点

线密度函数: 常数 $\rho$

物体的投影值(线积分值): 弦长  $t$  乘以线密度  $\rho$



$$p(s) = \begin{cases} \rho t = 2\rho\sqrt{R^2 - s^2} & |s| < R \\ 0 & |s| \geq R \end{cases}$$



断层成像问题再复杂一些？

需要更多数据！

如何获取数据？

从多角度采集数据+矩阵求和+数学处理手段

**探测器**：由四个离散的探测元组成

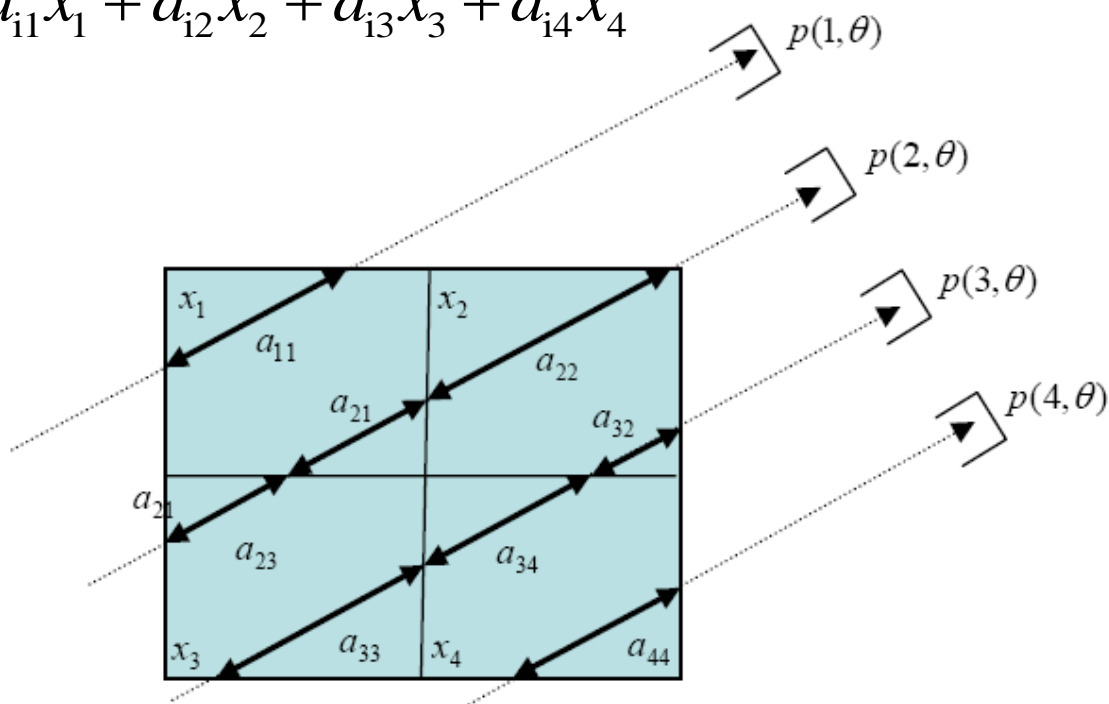
**矩阵**：连续图像。每个矩阵元素代表一个均匀的像素

$x_i$  ( $i = 1, 2, 3, 4$ )：第 $i$ 个像素的线密度数值

矩阵图像的**投影数据**：图像线积分数值  $p(s, \theta)$

线积分的“线”在每个像素内的**线段长度** $a_{ij}$  ( $i$  是探测元的编号;  $j$  是像素的编号)

$$p(i, \theta) = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 + a_{i4}x_4$$



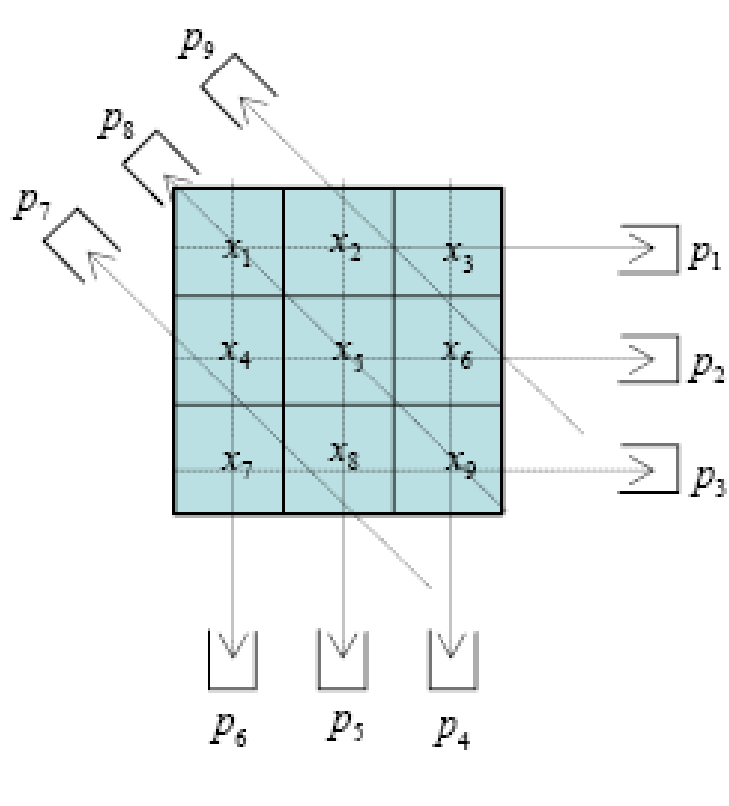


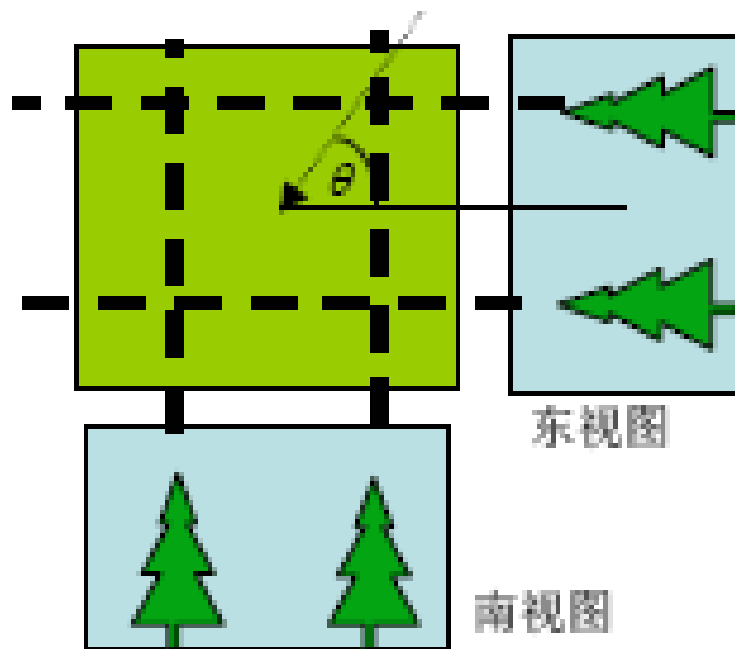
Diagram illustrating a 3x3 grid of variables  $x_1$  through  $x_9$ . The grid is shown with arrows pointing to summation boxes on the right, labeled  $p_1$ ,  $p_2$ , and  $p_3$ . Below the grid, three boxes are labeled  $p_6$ ,  $p_5$ , and  $p_4$ . Diagonal arrows from the top-left corner of the grid point to boxes labeled  $p_7$ ,  $p_8$ , and  $p_9$ .

$$\left\{ \begin{array}{l} x_1 + x_2 + x_3 = p_1 \\ x_4 + x_5 + x_6 = p_2 \\ x_7 + x_8 + x_9 = p_3 \\ x_3 + x_6 + x_9 = p_4 \\ x_2 + x_5 + x_8 = p_5 \\ x_1 + x_4 + x_7 = p_6 \\ 2(\sqrt{2}-1)x_4 + 2(\sqrt{2}-1)x_7 + 2(\sqrt{2}-1)x_8 = p_7 \\ \sqrt{2}x_1 + \sqrt{2}x_5 + \sqrt{2}x_9 = p_8 \\ 2(\sqrt{2}-1)x_2 + (2-\sqrt{2})x_3 + 2(\sqrt{2}-1)x_6 = p_9 \end{array} \right.$$

图像重建问题：解线性方程组，求解 $x$



思考：如图所示，在那两张照片中都可以看到两棵不重叠的大树。你可以唯一地画出那两棵树的地图吗？若不行的话，你也许需要多照些照片。如果你只允许再多照一张照片，选个什么角度照呢？



# 植物基因的分布分析

设一农业研究所植物园中某种植物的基因型为AA、Aa和aa。研究所计划采用AA型的植物与每一种基因型植物相结合的方案培育植物后代。问经过若干年后，这种植物的任意一代的三种基因型分布如何？

目的：研究能指导植物性状（如抗病抗虫、抗逆等）的基因培育方式，最终达到改变以及培育植物新品种的目的。



- 基因对确定了植物的特征
- 在常染色体的遗传中,后代是从每个亲本的基因对中各继承一个基因,形成自己的基因对(基因型)
- 在我们所研究的问题中,植物的基因对为AA、 Aa、 aa这3种

记:

$x_1(n)$ —第n代中基因型AA的植物占植物总数的百分比

$x_2(n)$ —第n代中基因型Aa的植物占植物总数的百分比

$x_3(n)$ —第n代中基因型aa的植物占植物总数的百分比

显然

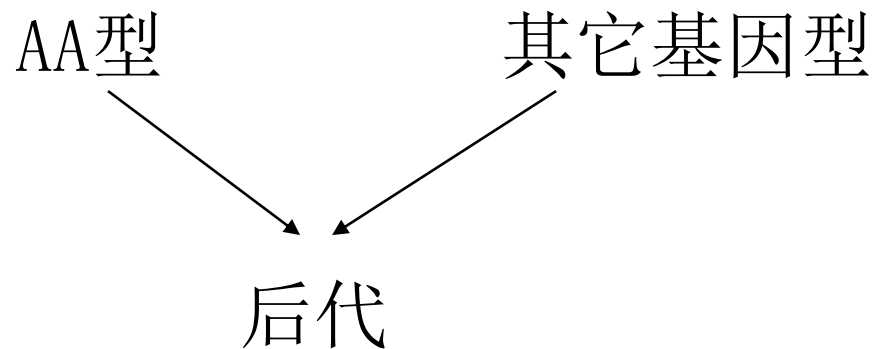
$$x_1(n) + x_2(n) + x_3(n) = 1$$

# 相邻两代间基因转移关系：

	概率	父体-母体的基因对		
		AA-AA	AA-Aa	AA-aa
后代基因对	AA	1	1/2	0
	Aa	0	1/2	1
	aa	0	0	0



育种方式:



故第n代与n-1代植物的基因型分布的关系为:

$$x_1(n) = x_1(n-1) + \frac{1}{2}x_2(n-1)$$

$$x_2(n) = \frac{1}{2}x_2(n-1) + x_3(n-1)$$

$$x_3(n) = 0,$$

引入

$$L = \begin{pmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \vec{x}(n) = \begin{pmatrix} x_1(n) \\ x_2(n) \\ x_3(n) \end{pmatrix}$$

则第n代与n-1代植物的基因型分布的关系的向量形式为：

$$\vec{x}(n) = L\vec{x}(n-1), \quad n = 1, 2, \dots \quad (1)$$

由 (1) 解得：

$$\vec{x}(n) = L^n \vec{x}(0), \quad n = 1, 2, \dots \quad (2)$$

## $L^n$ 的计算:

利用线性代数中**对角化的方法**将 $L$ 对角化, 即求出可逆矩阵 $P$  和对角矩阵 $D$ , 使得

$$L = PDP^{-1}$$

从而有

$$L^n = PD^n P^{-1}$$

利用特征值和特征向量的方法求得

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad P = P^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

从而得

$$L^n = \begin{pmatrix} 1 & 1 - \left(\frac{1}{2}\right)^n & 1 - \left(\frac{1}{2}\right)^{n-1} \\ 0 & \left(\frac{1}{2}\right)^n & \left(\frac{1}{2}\right)^{n-1} \\ 0 & 0 & 0 \end{pmatrix}$$

将 $L^n$ 代入(2)得



$$x_1(n) = x_1(0) + \left(1 - \left(\frac{1}{2}\right)^n\right)x_2(0) + \left(1 - \left(\frac{1}{2}\right)^{n-1}\right)x_3(0)$$

$$x_2(n) = \left(\frac{1}{2}\right)^n x_2(0) + \left(\frac{1}{2}\right)^{n-1} x_3(0)$$

$$x_3(n) = 0$$

显然可以看出当

$$n \rightarrow \infty \text{ 时, } x_1(n) \rightarrow 1, x_2(n) \rightarrow 0, x_3(n) \rightarrow 0$$

**结论：** 培育得植物AA型基因所占的比例在不断增加，**在极限状态下所有植物的基因型都会是AA型。**

# 森林管理问题

森林中的树木每年都要有一批被砍伐出售.为了使这片森林不被耗尽且每年都有所收获,每当砍伐一棵树时,应该就地补种一棵幼苗,使森林树木的总数保持不变.被出售的树木,其价值取决于树木的高度.开始时森林中的树木有着不同的高度.我们希望能找到一个方案,在维持收获的前提下,如何砍伐树木,才能使被砍伐的树木获得最大的经济价值?

把森林中的树木按照高度分为 $n$ 类:

第 $k$ 类: ( $1 \leq k < n$ ) 高度为  $[h_{k-1}, h_k]$  ,  
每棵的经济价值为  $p_k$

其中

第1类: 幼苗, 高度为  $[0, h_1]$  ,

$$p_1=0,$$

第 $n$ 类: 高度为  $[h_{n-1}, \infty)$

## 假设

1. 每年对森林中树木砍伐一次，留下的树木和补种的幼苗，经过一年的生长期后，与上一次砍伐前的高度状态相同（根据保持持续收获的要求）
2. 在一年的生长期内树木最多只能生长一个高度级，即第 $k$ 类的树木可能进入 $k+1$ 类，也可能停留在 $k$ 类中
3. 树木没有死亡

记  $x_k(t)$ ,  $k=1, 2, \dots, n$  是第 $t$ 年第 $k$ 类树木的数量.

$y_k$ ,  $k=1, 2, \dots, n$  是第 $k$ 类树木被砍伐的数量.



设 $g_k$ 是经过一年从第 $k$ 类中长高到第 $k+1$ 类中的树木比例, $0 < g_k < 1$

则  $1-g_k$ 是经过一年仍然留在第 $k$ 类中的树木比例.

设森林中树木的总数是 $s$ ,即

$$x_1(t) + x_2(t) + \dots + x_n(t) = s \quad (3)$$

其中 $s$ 是根据土地数量预先确定的数.

由前面的分析,引入

$\vec{x}(t)$  —— 数量向量

$\vec{y}$  —— 收获向量

$R$  —— 种植矩阵

$G$  —— 生长矩阵

$$\vec{x}(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ \vdots \\ x_{n-1}(t) \\ x_n(t) \end{pmatrix}, \quad \vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

$$G = \begin{pmatrix} 1 - g_1 & 0 & 0 & \cdots & 0 & 0 \\ g_1 & 1 - g_2 & 0 & \cdots & 0 & 0 \\ 0 & g_2 & 1 - g_3 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 - g_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & g_{n-1} & 1 \end{pmatrix}.$$

树木生长方程:

$$\vec{x}(t+1) = G\vec{x}(t), \quad t = 1, 2, \dots$$

根据问题的要求,我们要维持持续收获,所以树木的生长必须维持**平衡关系**: 生长期末的状态减去收获采伐的量后再加上补种的幼苗数应等于生长期开始的量,即

$$G\vec{x}(n) - \vec{y} + R\vec{y} = \vec{x}(n)$$

对于任意非负向量  $\vec{x}, \vec{y}$ , 满足上式的解就是维持森林持续稳定收获的**可行解**.

由于幼苗无经济价值,故对其不采伐,所以取  $y_1 = 0$ . 上式变为

$$y_2 + \cdots + y_n = g_1 x_1$$

$$y_2 = g_1 x_1 - g_2 x_2$$

$$\vdots$$

$$y_{n-1} = g_{n-2} x_{n-2} - g_{n-1} x_{n-1}$$

$$y_n = g_{n-1} x_{n-1}$$

$$\because y_k \geq 0, k = 2, 3, \dots, n$$

$$\therefore g_1 X_1 \geq g_2 X_2 \geq \dots \geq g_{n-1} X_{n-1} \geq 0$$



利用收获向量和价值向量得所收获树木的价值为

$$f(y_1, y_2, \dots, y_n)$$

$$= p_2 y_2 + p_3 y_3 + \dots + p_n y_n$$

$$= p_2 g_1 x_1 + (p_3 - p_2) g_2 x_2 + \dots + (p_n - p_{n-1}) g_{n-1} x_{n-1}$$

问题的模型为

$$\max p_2 g_1 x_1 + (p_3 - p_2) g_2 x_2 + \dots + (p_n - p_{n-1}) g_{n-1} x_{n-1}$$

$$s.t. \quad g_1 x_1 - g_2 x_2 \geq 0$$

$$g_2 x_2 - g_3 x_3 \geq 0$$

$$\vdots$$

$$g_{n-2} x_{n-2} - g_{n-1} x_{n-1} \geq 0$$

$$x_1 + x_2 + \dots + x_n = s$$

$$x_1 \geq 0, x_2 \geq 0, \dots, x_{n-1} \geq 0$$

## 模型求解

**利用线性规划基本理论，可得如下结论：**

**砍伐某一类树木而不砍伐其他类的树木时，可获得最大收益。**

利用这一结论，设被砍伐的树木为第  $k$  类，则

$$y_k > 0, y_j = 0, (j \neq k, j = 1, 2, \dots, n)$$

进一步根据收获向量与高度状态向量之间的关系，得

$$x_k = 0, x_{k+1} = 0, \dots, x_{n-1} = 0$$

$$g_2 x_2 = g_1 x_1$$

$\dots$

$$g_{k-1} x_{k-1} = g_{k-2} x_{k-2}$$

$$y_k = g_{k-1} x_{k-1}$$

$$y_k = g_1 x_1$$

所以

$$x_2 = \frac{g_1}{g_2} x_1, x_3 = \frac{g_1}{g_3} x_1, \dots x_{k-1} = \frac{g_1}{g_{k-1}} x_1,$$

$$x_k = 0, x_{k+1} = 0, \dots x_n = 0$$

将上式代入(3)得

$$x_1 = \frac{s}{1 + \frac{g_1}{g_2} + \frac{g_1}{g_3} + \dots + \frac{g_1}{g_{k-1}}}$$

故最大收益为

$$y_k p_k = g_1 x_1 p_k = \frac{p_k s}{\frac{1}{g_1} + \frac{1}{g_2} + \dots + \frac{1}{g_{k-1}}}$$



**例** 已知森林具有 6 年的生长期,  $g_1 = 0.28, g_2 = 0.32, g_3 = 0.25, g_4 = 0.23, g_5 = 0.37, p_2 = 50$  元,  $p_3 = 100$  元,  $p_4 = 150$  元,  $p_5 = 200$  元,  $p_6 = 250$  元. 求出对其进行最优采伐的策略.

**解** 问题的模型为

$$\max \quad 14x_1 + 16x_2 + 12.5x_3 + 11.5x_4 + 18.5x_5$$

$$s.t. \quad 0.28x_1 - 0.32x_2 \geq 0,$$

$$0.32x_2 - 0.25x_3 \geq 0,$$

$$0.25x_3 - 0.23x_4 \geq 0,$$

$$0.23x_4 - 0.37x_5 \geq 0,$$

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 10000,$$

$$x_j \geq 0, \quad j = 1, 2, 3, 4, 5, 6.$$

求出对其进行最优采伐的策略：

$$f_2=14.0s, \quad f_3=14.7s, \quad f_4=13.9s$$

$$f_5=13.2s, \quad f_6=14.0s$$

比较这5个值得 $f_3$ 最大, 故全部收获第三类的树木收获最大, 收益值为 $14.7s$ , 其中 $s$ 为森林中所能生长的树木的总数。

# 信息的加密与解密

信息安全本身包括的范围很大，大到国家军事政治等机密安全，小范围的当然还包括如防范商业企业机密泄露，个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名，信息认证，数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。

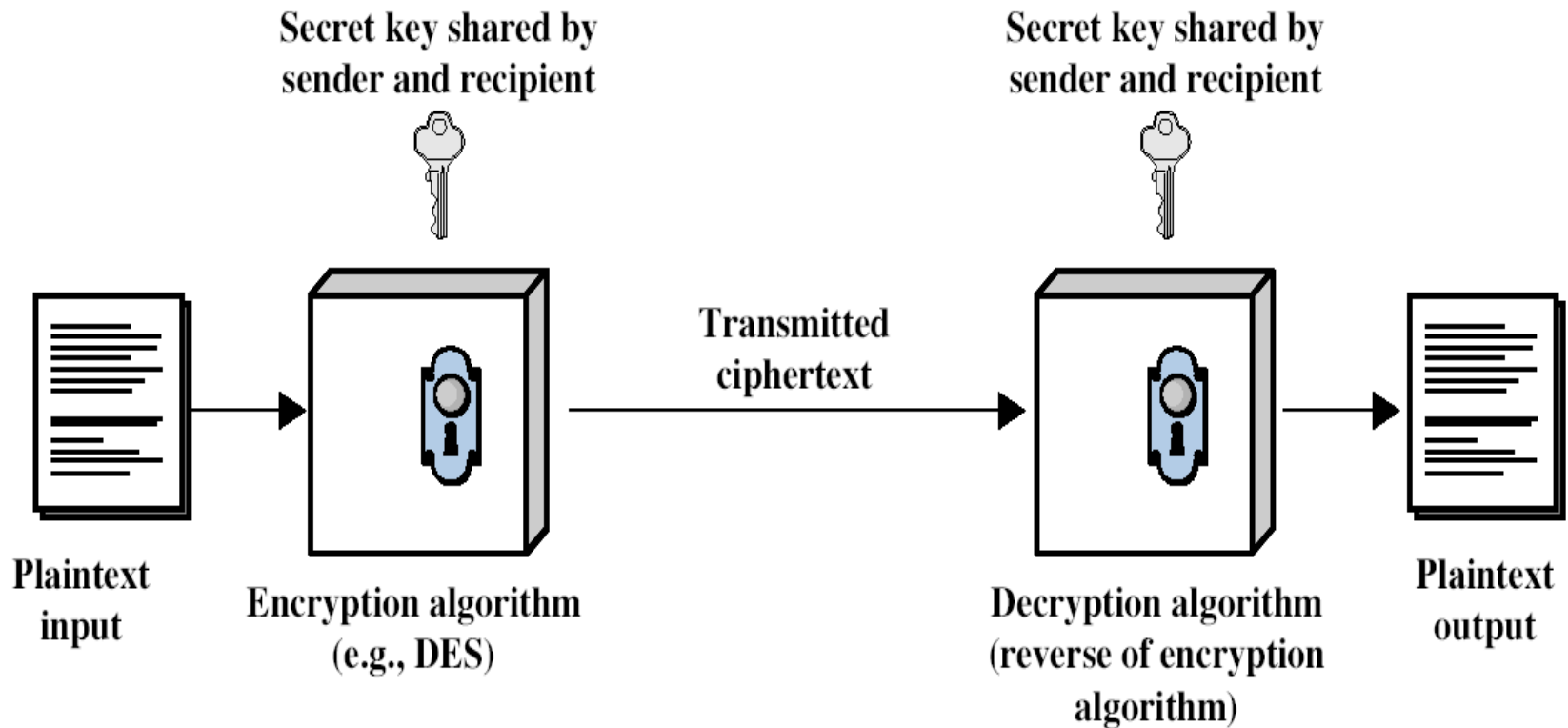
信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

- **密码的设计和使用至少可从追溯到四千多年前的埃及、巴比伦、罗马和希腊，历史极为久远**
- **古代隐藏信息的方法主要有两大类：其一为隐藏信息载体，采用隐写术等；其二为变换信息载体，使之无法为一般人所理解**

# 简单定义

在密码学中，信息代码被称为**密码**，加密前的信息被称为**明文**，经加密后不为常人理解的用密码表示的信息被称为**密文** (**ciphertext**)，将明文转变成密文的过程被称为**加密** (**enciphering**)，其逆过程则被称为**解密** (**deciphering**)，而用以加密、解密的方法或算法则被称为**密码体制** (**cryptosystem**)。

# 常规加密简化模型





记全体明文组成的集合为 $U$ ，全体密文组成的集合为 $V$ ，称 $U$ 为明文空间， $V$ 为密文空间。加密常利用某一被称为密钥的东西来实现，它通常取自于一个被称为密钥空间的含有若干参数的集合 $K$ 。按数学的观点来看，加密与解密均可被看成是一种变换：取一 $k \in K$ ， $\forall u \in U$ ，令  $u \xrightarrow{k} v \in V$ ， $v$ 为明文 $u$ 在密钥 $k$ 下的密文，而解码则要用到 $K$ 的逆变换 $K^{-1}$ 。由此可见，密码体系虽然可以千姿百态，但其关键还在于密钥的选取。

早在4000多年前，古希腊人就用一种名叫“天书”的器械来加密消息。该密码器械是用一条窄长的纸带缠绕在一个直径确定的圆筒上，明文逐行横写在纸带上，当取下纸带时，字母的次序就被打乱了，消息得以隐蔽。收方阅读消息时，要将纸带重新绕在直径与原来相同的圆筒上，才能看到正确的消息。在这里圆筒的直径起到了密钥的作用。

# 希尔密码



移位密码的一个致命弱点是明文字符和密文字符有相同的使用频率,破译者可从统计出来的字符频率中找到规律,进而找出破译的突破口。要克服这一缺陷,提高保密程度就必须改变字符间的一一对应。

1929年,希尔利用线性代数中的矩阵运算,打破了字符间的对应关系,设计了一种被称为希尔密码的代数密码。为了便于计算,希尔首先将字符变换成数,例如,对英文字母,我们可以作如下变换:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

将密文分成  $n$  个一组,用对应的数字代替,就变成了一个  $n$  维向量。如果取定一个  $n$  阶的非奇异矩阵  $A$  (此矩阵为主要密钥),用  $A$  去乘每一向量,即可起到加密的效果,解密也不麻烦,将密文也分成  $n$  个一组,同样变换成  $n$  维向量,只需用  $A$  逆去乘这些向量,即可将他们变回原先的明文。

但在具体实施时，我们很快会发现一些困难：

首先，我们的英文字母是与0~25这26个整数1-1对应的，所以变换或逆变换后需要产生0~25之间的整数。

只要密钥矩阵A或其逆矩阵 $A^{-1}$ 是非负整数矩阵，以A或 $A^{-1}$ 乘以任一向量后所得结果仍为整向量，对该整向量的每个元素以26为模求同余运算即可使密文或解密后的密文为0~25之间的整数。

**第一个困难引入同余运算即可解决**

其次， $A^{-1}$ 也应该是0~25之间的整数。这就要对密钥矩阵的行列式 $\det(A)$ 增加了一些限制。

由线性代数可知  $A^{-1} = \frac{A^*}{\det(A)}$ ，其中 $A^*$ 是 $A$ 的伴随矩阵，从而 $A^{-1}$ 的元素中就有可能出现分数。克服这一困难的途径仍然是引入同余运算，**即在同余意义上引入除法：**

若 $a \geq 0, b \geq 0$ ，满足  $ab \pmod{26} = 1$ ，则称 $b$ 为 $a$ 在同余意义上的逆元，记作 $a^{-1} = b \pmod{26}$

与逆矩阵的定义类似

故若有 $\det(A)^{-1} = b_0 \pmod{26}$ ，则  $A^{-1} = b_0 A^*$ 。

**一个矩阵要成为密钥矩阵，它的行列式必须有逆元**

关于0~25之间的整数有无同余意义上的逆元有下面的定理：

**定理1**  $a \in \{0, \dots, 25\}$ , 若  $\exists a^{-1} \in \{0, 25\}$  使得  $a a^{-1} = a^{-1} a \equiv 1 \pmod{26}$ , 则必有  $\gcd\{a, 26\} = 1$ , 其中  $\gcd\{a, 26\}$  为 **a** 与 **26** 的最大公因子。

还可以证明，如果 **a**<sup>-1</sup> 存在，那么它是唯一的。由定理1，0~25中除13以外的奇数均可取作这里的**a**，它们的逆元如下表。

<b>a</b>	1	3	5	7	9	11	15	17	19	21	23	25
<b>a</b> <sup>-1</sup>	1	9	21	15	3	19	7	23	11	5	17	25

# Hill密码的加密过程

- 选择一个 $n$ 阶可逆矩阵 $A$ 作为加密矩阵；
- 将明文字符按顺序排列分组；
- 将明文字符对应一个整数，组成一组列向量；
- 用加密矩阵左乘每一列向量；
- 将新向量的每个分量关于模 $m$ 取余运算；
- 将新向量的每个整数对应于一个字符。

**解密过程相反。**

例 取  $A = 3$  用希尔密码体系加密语句

**THANK YOU**

步1 将 **THANK YOU** 转换成 (20, 8, 1, 14, 11, 25, 15, 21)

步2 每一分量乘以  $A$  并关于 26 取余得 (8, 24, 3, 16, 7, 23, 19, 11)

密文为 **HXC PG WSK**

现在我们已经不难将方法推广到  $n$  为一般整数的情况了, 只需在乘法运算中结合应用取余, 求逆矩阵时用逆元素相乘来代替除法即可。





例 取  $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$  则  $A^{-1} = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}$  (具体求法见

后), 用  $A$  加密 **THANK YOU**, 再用  $A^{-1}$  对密文解密

解:(希尔密码加密)用相应数字代替字符, 划分为两个元素一组并表示为向量:

$$\begin{bmatrix} 20 \\ 8 \end{bmatrix} \begin{bmatrix} 1 \\ 14 \end{bmatrix} \begin{bmatrix} 11 \\ 25 \end{bmatrix} \begin{bmatrix} 15 \\ 21 \end{bmatrix}$$

用矩阵  $A$  左乘各向量加密 (关于 26 取余) 得

$$\begin{bmatrix} 10 \\ 24 \end{bmatrix} \begin{bmatrix} 3 \\ 16 \end{bmatrix} \begin{bmatrix} 9 \\ 23 \end{bmatrix} \begin{bmatrix} 5 \\ 11 \end{bmatrix}$$

得到密文 **JXCPI WEK**

## (希尔密码解密)

用 $A^{-1}$ 左乘求得的向量，即可还原为原来的向量。希尔密码是以矩阵法为基础的，明文与密文的对应由 $n$ 阶矩阵 $A$ 确定。矩阵 $A$ 的阶数是事先约定的，与明文分组时每组字母的字母数量相同，如果明文所含字数与 $n$ 不匹配，则最后几个分量可任意补足。

### $A^{-1}$ 的求法

方法1 利用公式  $A^{-1} = \frac{A^*}{\det(A)}$ ，例如，若取  $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$ ，

则  $\det(A) = 3$ ， $\frac{1}{\det(A)} = 9$ ， $A^{-1} \equiv 9 \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} \pmod{26}$ ，即

$$A^{-1} = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}$$

方法2 利用高斯消去法。将矩阵 $(A, E)$ 中的矩阵 $A$ 消为 $E$ ，则原先的 $E$ 即被消成了 $A^{-1}$ ，

如

$$\left( \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \rightarrow (\text{用 } 9 \text{ 乘第二行并取同余}) \rightarrow \left( \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 9 \end{bmatrix} \right)$$

第一行减去第二行的2倍并取同余，得

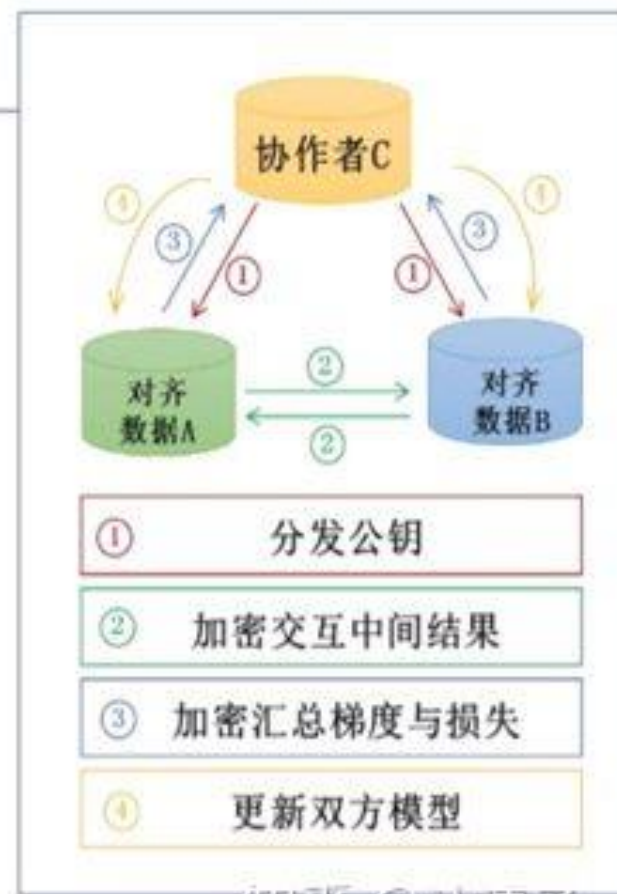
$$\left( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \right)$$

左端矩阵已化为单位阵，故右端矩阵即为  $A^{-1}$

随着计算机与网络技术的迅猛发展，大量各具特色的密码体系不断涌现。离散数学、数论、计算复杂性、混沌、……，许多相当高深的数学知识都被用上，逐步形成了（并仍在迅速发展的）具有广泛应用面的**现代密码学**。

**应用：**区块链技术：依靠密码学和数学巧妙的分布式算法，在无法建立信任关系的互联网上，无需借助任何第三方中心的介入就可以使参与者达成共识，以极低的成本解决了信任与价值的可靠传递难题。

联邦学习：在保证数据隐私安全及合法合规的基础上，实现共同建模，提升AI模型的效果。



# 联邦学习