

1 概述

1.1 人工智能的基本概念

弱人工智能**ANI** 完成特定任务,不具有自主意识

强人工智能**AGI** 通用人工智能, 能执行所有任务

超人工智能**ASI** 具有自我意识包括独立自主的价值观

- 大模型的涌现能力

1.2 人工智能的典型应用

- Google Brain
- Deep Face (人脸识别)
- Microsoft speech recognition,translation and synthesis (微软语音识别、翻译和合成)

1.3 计算机发展

图灵机 冯·诺依曼结构 ENIAC 奠定了现代计算机的基础。

1.4 计算思维的基本概念

运用计算机科学的基础概念进行问题求解、系统设计、以及人类行为理解等涵盖计算机科学之广度的一系列思维活动。

计算思维的特征:

- 人的思维方式
- 可由人类执行
- 一种思想概念

1.5 图灵贡献

图灵机	计算所有直觉上可计算的函数	计算机科学之父	可计算问题
图灵测试	测试机器是否具有智能	人工智能之父	人工智能测试问题

2 计算机信息数字化基础

2.1 二进制、十六进制

二进制Binary

$$(1001)_2 = 1001B$$

十六进制Hexademical

$$(1001)_{16} = 1001H$$

2.2 数制间转换

将R进制转换为十进制 按权展开法

将十进制转换为R进制 整数除R倒取余数，小数乘R正取整数

2.3 原码、补码计算

十进制	14	-22
二进制	1110	-10110
原码	0000 1110	1001 0110
反码	0000 1110	1110 1001
补码	0000 1110	1110 1010

2.4 浮点数表示

浮点数表示形式： $X = \pm \text{尾数} \times 2^{\text{阶}}$

	浮点数表示				
精度	阶符	阶码	数符	尾数	总位数
单精度	1位	7位	1位	23位	32位4字节
双精度	1位	11位	1位	51位	64位8字节

2.5 逻辑运算

非	与	或	异或	(按运算顺序从左到右排列)
NOT	AND	OR	XOR	

2.6 西文字符编码

ASCII码 7位编码，128个字符

2.7 汉字字符编码

- 汉字输入码 键盘输入
- 汉字国标码 信息交换
- 汉字机内码 计算机内部存储
- 汉字字形码 记录字形点阵

2.8 模数转换器ADC

音频信息处理时，将模拟信号转换为数字信号的装置。

2.9 音频编码

- 1. 采样
- 2. 量化
- 3. 编码

存储量（字节数）= 采样频率 × 采样精度 × 声道数

2.10 图像编码

- 按颜色分类：
 - 二值图像
 - 灰度图像
 - 彩色图像

- 主要参数：

尺寸	图像大小	图像像素点个数
分辨率	图像清晰度	注意屏幕分辨率与图像分辨率的区别
色深	图像RGB颜色值存储大小	超过24bit的颜色为真彩色

- 图像文件大小计算公式：

图像文件大小（字节数） = 图像宽度 × 图像高度 × 色深/8

2.11 图形编码

图形	图元	矢量图
图像	像素点	位图

2.12 信息编码

用数字、字母等按规定的方法和位数来代表特定的信息。

2.13 特征编码

将原始数据转化为数值形式的数据，用以分类

类别特征 离散、非连续

小型分类特征	类别较少	
二进制编码	用0-1表示类别	
序列编码	用整数表示类别	类别具有顺序关系
独热编码	用向量表示类别	类别不具有大小关系
大型分类特征	类别较多	
哈希编码	用较小的数值表示大量数据	唯一性、固定长度

2.14 熵

随机变量不确定性的平均值

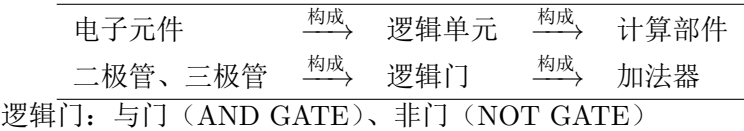
2.15 数据压缩

信源编码时减少数据量的编码方案			
压缩	信息	压缩率	应用
无损压缩	保留全部信息	低	文本文件
有损压缩	牺牲部分冗余	高	多媒体文件

3 人工智能的计算基础

3.1 人工智能的硬件基础

3.1.1 基本逻辑运算单元



3.1.2 冯·诺依曼型计算机结构

主要部件	功能	说明
运算器ALU	算术运算、逻辑运算	算术逻辑部件ALU、累加器、通用寄存器、状态寄存器
控制器CU	指令解释、执行控制	指令寄存器IR、程序计数器PC、指令译码器ID
存储器	存储数据与指令	内存储器、外存储器
输入设备	输入数据与指令	键盘、鼠标等
输出设备	输出结果	显示器、打印机等

3.1.3 计算机存储体系

- 内存储器（内存）

随机存取存储器RAM 断电数据消失

只读存储器ROM 写入后无法更改
- 外存储器（外存）

位bit 信息的最小单位

字节Byte 8 bit组成一个字节

字word 计算机处理数据的基本单位，通常为2字节或4字节

地址address 存储单元的编号

3.1.4 指令系统

指令

- 由操作码和地址码组成
- 对应计算机直接实现的基本操作

指令系统 确定数量指令的总和

指令应包括的功能

- 数据传送类
- 算术运算和逻辑运算类
- 程序控制类
- 输入输出类
- 控制和管理机器类

指令周期（程序自动控制）

1. 取指令
2. 分析指令
3. 执行指令

指令流水线技术

3.1.5 总线

计算机系统中各个功能部件（如CPU、内存、I/O设备）之间共享的公共通信干线

3.2 计算机的软件基础

3.2.1 操作系统

- 直接与硬件交流
- 最底层软件
- 管理和控制计算机硬件与软件资源
- 用户通过操作系统来使用计算机系统

3.2.2 多级存储体系

外存——内存——多级Cache——CPU寄存器			
存取速度	低	—————→	高
存储容量	小	—————→	大
存储成本	高	—————→	低

3.2.3 磁盘管理

- 磁盘数据存取：
 - 以簇为单位
 - 1个扇区（Sector）=512字节
 - 调用磁盘驱动程序
- 磁盘主要区域：
 - 保留扇区 计算机开机自检和启动操作系统
 - 文件分配表区 文件在数据区存储的位置
 - 根目录区 文件在数据区存储的起始单元
 - 数据区 文件化整为零后存放的区域

3.2.4 文件系统

多级目录结构
完整的文件描述（盘符、路径、文件名.扩展名）

3.2.5 进程

- 概念：
 - 程序 指令序列
 - 作业 面向用户的程序的执行实例
 - 进程 面向计算机的程序的执行实例
 - 线程 进程中的一个执行单元
- 进程状态：

就绪态 等待CPU分配时间片

运行态 正在使用CPU

阻塞态 等待某事件发生（I/O请求、申请缓冲空间……）

- **动态调度：**

进程在三种状态间转换

3.3 程序与算法基础

3.3.1 计算机语言发展

机器语言	二进制指令	机器直接运行
汇编语言	助记符表示指令	汇编程序翻译
高级语言	英语和数学语言	编译器或解释器翻译

3.3.2 图灵机

组成：

- 无限长纸带
- 读写头
- 状态寄存器
- 控制器

图灵论题：

一个**可计算**问题是“当且仅当它在图灵机上经过有限步骤之后可以得到正确的结果”

3.3.3 计算复杂度

库克论题：

一个问题是**实际可计算**的当且仅当它能够在图灵机上经过多项式步骤得到正确结果

时间复杂度 计算所需的步数或指令条数

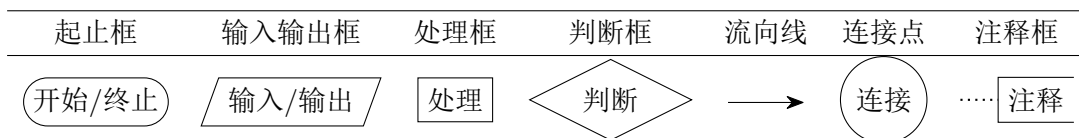
空间复杂度 计算所需的存储单元数

3.3.4 算法

- 算法：
解决问题的有限步骤
- 算法特性：
 - 有穷性 算法步骤有限
 - 确定性 算法步骤含义确定
 - 有效性 每一步都能被执行
 - 有零个或多个输入
 - 有一个或多个输出

3.3.5 流程图

- 算法的图形化表示



- 基本结构：

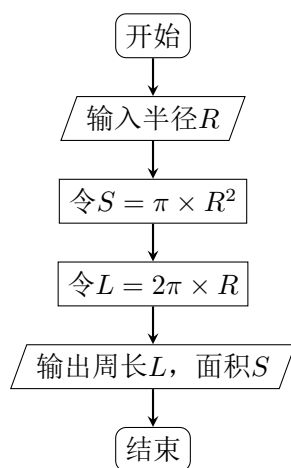
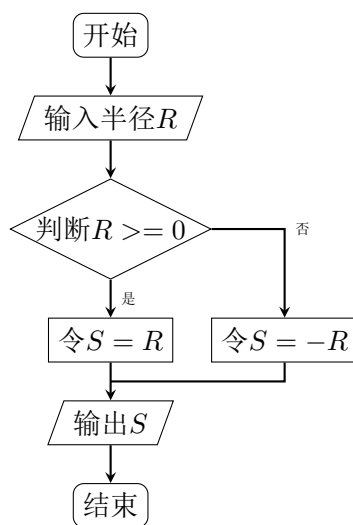


图 1: 顺序结构：输入圆的半径R，输出圆的周长和面积

图 2: 选择结构:输入任意常数 R , 输出 R 的绝对值 S

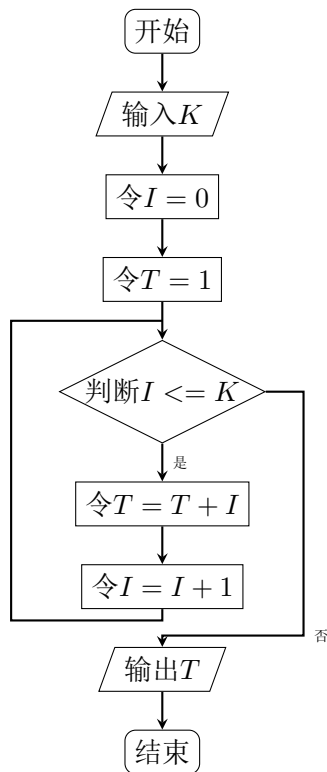


图 3: 循环结构:输入任意自然数K, 输出自然数1到K的和

- 常见算法:

求和算法 绘图算法 排序算法 穷举算法

3.4 并行计算机体系结构

3.4.1 并行计算

- 并行计算:

同时使用多台计算机或多处理器同时工作以提高计算速度和处理能力的计算方式。

- 特点:

软件算法复杂、硬件结构复杂（多核微处理器）

3.4.2 摩尔定律

微处理器的处理能力每**18个月到24个月**将增加一倍

4 符号智能

4.1 搜索与问题求解

搜索 人工智能技术中进行问题求解的基本技术

状态空间 对智能体和环境当前情形的描述

动作 智能体在某一状态下可执行的操作

问题的解 初始状态到目标状态的一组行动序列

路径/代价 一个完整的状态序列

最优解 代价最小的解

4.2 状态空间表示法

状态 一组数据: $S_k = \{S_{k0}, S_{k1}, \dots\}$

操作 (算符)

状态空间 四元组: (S, O, S_0, G)

其中,

- S 为状态集合
- O 为操作集合
- S_0 为初始状态
- G 为若干具体状态或满足某些性质的路径信息

4.3 盲目图搜索策略

广度优先搜索 (BFS)	深度优先搜索 (DFS)
优先选择最浅节点扩展	优先选择最深节点扩展
逐层扩展	盲目搜索
高价搜索	低价搜索
有解问题能求最优解	有解问题不一定能求解

4.4 启发式搜索

运用条件：

- 问题没有明确的解
- 状态空间特别大

估价函数 $f(n)$ ：

$$f(n) = g(n) + h(n)$$

其中， $g(n)$ 为从初始状态 S_0 到节点 n 的实际代价，启发函数 $h(n)$ 为从节点 n 到目标状态 S_g 的最优路径的估计代价。

- $h(n)$ 占比大时，趋向深度优先搜索
- $h(n)$ 占比小时，趋向广度优先搜索

在A算法中，若启发函数 $h(n) < h^*(n)$ ，则称 $h(n)$ 为一致启发函数，此时A算法能得到最优解，称为**A*算法**。

如果启发函数 $h(n)$ 满足以下条件：

$$h(n_i) - h(n_j) \leq C(n_i, n_j) \text{ 且 } h(t) = 0$$

其中 n_j 是 n_i 的子节点， t 目标节点， $C(n_i, n_j)$ 是 n_j 与 n_i 间的耗散值，则称启发函数 $h(n)$ 满足**单调限制条件**。

4.5 知识表示

人类知识符号化或模型化，转换为机器内部的一种数据结构

- 一阶谓词逻辑表示法
- 产生式表示法
- 语义网络表示法
- 框架表示法

4.6 一阶谓词逻辑表示法

$$P(x_1, x_2, \dots, x_n)$$

其中, P 为谓词, x_1, x_2, \dots, x_n 为个体

- 谓词连接词:

否定	合取	析取	蕴涵
\neg	\wedge	\vee	\rightarrow

- 知识类别:

事实性知识 合取、析取

规则性知识 蕴涵

- 特点

— 优点:

自然性 与自然语言相近

精确性 只有真假两种取值

易实现 便于计算机处理

严密性 有严格的语法和语义规则

— 缺点:

表达能力有限 无法表示不确定性知识

推理能力有限 无法进行复杂推理

知识表示有限 难以表示启发性知识或元知识

4.7 知识推理

确定性推理 推理时所用的知识与证据都是确定的, 推出的结论也是确定的, 其真值或者为真或者为假。

不确定性推理 推理时所用的知识与证据是不确定的, 推出的结论也是不确定的。

- 似然推理
- 近似推理 (模糊推理)

5 机器学习基础

5.1 机器学习的基本概念

机器学习：

通过算法解析数据、提取模式，并将这些模式转化为可用于预测或决策的模型

机器学习类型：

监督学习 需要带标签的训练数据完成学习

- 分类
 - K最近邻 (KNN)
 - 决策树
- 回归
 - 线性回归
 - LASSO回归

无监督学习 没有标签或正确答案的情况下，自己探索数据内在结构或关系

- 聚类
 - K-means
 - 均值漂移
- 降维
 - PCA
 - SVD
 - t-SNE
 - LLE

强化学习 基于行为结果的奖励反馈调整策略

5.2 回归

- 回归：
预测数值

- 多元线性回归的模型函数如下：

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n + \epsilon$$

其中： y 是因变量， x_1, x_2, \dots, x_n 是自变量， β_0 是截距项， $\beta_1, \beta_2, \dots, \beta_n$ 是各自变量的系数， ϵ 是误差项。

- 梯度下降法：

迭代优化残差平方和（RSS）不断趋于最小

$$\text{RSS}(\beta_0, \beta_1) = \sum_{i=1}^n (y_i - \hat{y}_i)^2 = \sum_{i=1}^n (y_i - \beta_0 - \beta_1 x_i)^2$$

5.3 分类

- 分类：

将数据划分为不同类别

- K最近邻（KNN）算法：

数据准备 数据清洗，数据处理，将每条数据整理成向量

计算距离 计算待分类数据与训练集中每条数据的距离

选择K值 选择距离最近的K个数据点

决策分类 从K个数据点中选择出现频率最高的类别作为待分类数据的类别

不同K值分类准确率不同

- 决策树：

做决策时层层递进的思考过程的监督学习模型

5.4 降维

降维：简化模型、避免维度灾难

主成分分析（PCA）：

通过线性变换将数据从高维空间映射到数据方差最大的低维空间

$$X_c = X - \bar{X}$$

X 为数据矩阵, \bar{x} 为平均数据, X_c 为中心化后的数据矩阵

$$\lambda_i = \frac{1}{n-1}(X_c v_i)^T (X_c v_i)$$

$$\sum v_i = \lambda_i v_i$$

λ_i 为 X 最大的特征值, 则 v_i 为最大特征值对应的特征向量

5.5 聚类

聚类:

将事物根据其特征分成多个簇

K均值算法 (K-means) 步骤:

选择K值 确定要分成的簇的数量

初始化质心 随机选择位置或数据点作为初始质心

分配数据点 将每个数据点分配给距离最近的质心所属的簇

更新质心 计算每个簇的质心, 通常为所有数据点的均值

重复迭代 重复步骤3和4, 直到质心变化极小或达到预设的迭代次数

5.6 强化学习

五个要素:

环境 智能体所处的外部世界

智能体 强化学习中的核心部分, 嵌入到环境中的决策实体

状态 环境在某一时刻的具体情形

动作 智能体在某一状态下可执行的操作

奖励 智能体执行某一动作后从环境中获得的反馈信号

- 基于价值函数的间接优化
- 基于策略梯度的直接优化

Q-learning算法:

5.7 过拟合

模型过于复杂，以至于很好地拟合了训练数据中的噪声和异常值，导致在新数据上的表现较差。

6 神经网络与深度学习

6.1 人工神经网络

人工神经网络 (ANNs):

模拟生物神经网络结构和功能的计算模型

人工神经元:

大量人工神经元相互连接构成人工神经网络

$$y_i = f\left(\sum_{j=1}^n w_{ij}x_j - \theta_i\right)$$

其中,

· x_i 输入

· w_i 权重

· θ_i 偏置, 微调神经元激活阈值

· $f(\cdot)$ 激活函数, 引入非线性

逻辑函数 $\sigma \quad \sigma(z) = \frac{1}{1+e^{-z}}$

线性整流函数 **ReLU** $R(z) = \max(0, z)$

· y_i 输出

损失函数 (Loss Function): 对输出结果评分

二分类交叉熵损失函数 (Cross-Entropy) :

$$CE = -(y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i))$$

其中,

· y_i 真实标签, 取值为0或1, 代表两个类别

· \hat{y}_i 模型预测的概率

6.2 前馈神经网络

信息单向流动：输入层→隐藏层→输出层

感知器(Perceptron)：用于模式分类

感知器	非线性分类	“异或”问题
单层感知器	不能	不能
多层感知器	能	能

卷积神经网络：一种前馈神经网络

卷积层 提取特征，生成特征图将卷积核在输入数据上滑动，并计算卷积核与输入数据的局部区域之间的点积

RGB三个通道输出结果相加得到最终结果

通过多通道多卷积核卷积层提取多种特征

参数：

填充 防止图像信息在卷积过程中缩小

步幅 步幅增大，卷积层输出尺寸变小

池化层 简化提取的特征平均池化、最大池化

全连接层 整合和转换特征，分类或回归预测

6.3 反馈神经网络

信息循环传递

循环神经网络(RNN)：

构成 输入层、隐藏层、输出层

原理 隐藏层状态由此刻的输入和上一刻的隐藏层状态同时决定

长短期记忆神经网络(LSTM)：

引入记忆参数 更好地保存长距离的序列依赖关系

引入遗忘门、输入门、输出门结构 控制信息结构

6.4 深度学习

- 基于人工神经网络的智能计算方法
- 机器学习的重要分支
- 核心基础算法：卷积神经网络、反向传播算法、梯度下降优化等关键技术

计算机视觉领域的典型应用

- 图像分类
 - AlexNet:
 - 神经网络层数更多
 - ReLU作为激活函数 运算简单
 - 随机失活层(Dropout) 增强模型泛化能力
 - ResNet: 引入残差结构解决退化问题
 - 退化问题: 更深的网络会伴随梯度消失、梯度爆炸等问题无法收敛, 测试数据误差增大, 训练数据误差增大
- 图像分割
 - FCN
 - Unet

7 生成式人工智能

7.1 生成式人工智能

应用场景 生成文本、生成视频……

技术升级 基于模板与规则→基于深度神经网络、融合专业场景

大模型	视觉	语言	多模态
	感知	认知	内容创作

AI Agent 感知环境及需求、进行决策和执行动作的智能体

7.2 对抗网络

使用两个网络互相竞争，称之为**对抗式**(adversarial)结构

- 生成式对抗网络(GAN):
 - 能在非监督学习中生成新样本
- 深度卷积对抗式生成网络(DCGAN):
 - 有监督学习的CNN与无监督学习的GAN的整合
 - 通过编码运算控制人脸图像

7.3 Transformer模型

基于自注意力机制 (Self-attention) 的神经网络

自注意力机制:

- 优势:
 - 更好建模长距离依赖关系
 - 更好实现并行计算
- 缺点:
 - 不采用循环结构或卷积结构

位置向量:

明确单词位置关系, 从而明确句子语义

多头注意力机制、缩放点积注意力机制

解码器

$N \text{ 层} * 3 \text{ 个子层} = 3N$

- 掩码多头自注意力子层
- 编码-解码注意力子层
- 前馈网络子层

每个子层间采用残差连接(residual connection)和层归一化(layer normalization)。

编码-解码注意力子层:

- 只对**隐层状态**做注意力计算
- 在解码过程中利用源语言信息
- 查询向量 (q) 来自**目标端**隐层状态
- B. 键向量 (k) 和值向量 (v) 来自**源端**隐层状态

Transformer应用:

自然语言处理、计算机视觉和语音识别以及**预训练语言模型**

7.4 视觉处理系统

- 图像采集
 - 纠正几何失真 (图像坐标变换)
 - 提高视觉质量 (灰度映射、直方图修正)
 - 降低噪声干扰 (空域滤波)
- 特征工程: 提取各种复杂度的特征 (特征点检测)
- 模型训练
- 评价

7.5 扩散模型

- 训练阶段
 1. 向真实动作序列添加噪声
 2. 模型学习“如何还原原始动作”
- 生成阶段
 1. 从纯噪声开始逐步迭代去噪
 2. 生成逼真的动作

7.6 自然语言处理（NLP）

研究能实现人与计算机之间用自然语言进行通信的各种理论和方法。
阶段：

1. 形式
2. 语义
3. 推理
4. 语用

7.7 大模型开发

预训练	通识教育	自监督学习	海量无标注数据
精调	专业教育		任务相关少量数据

7.8 AI Agent

- AI Agent：

具有自适应性和智能性的软件实体，能代表用户或其它程序，以主动服务的方式完成一项工作。

Agent = LLM + 记忆 + 规划技能+ 工具使用
- 多智能体：

一个松散耦合的Agent网络，通过交互、协作进行问题求解

- 特点：
自主性、反应性、主动性、社会性
- Agent技术架构：
感知记忆模块、规划决策模块、工具和行动模块

8 行为智能与群智能

8.1 行为智能

通过观察环境，或通过身体与环境的直接相互作用产生的智能

8.2 群智能

群居昆虫的集体行为

特点：

个体的行为很简单，协同工作时表现出非常复杂（智能）的行为特征

蚁群算法：寻找最优路径

- 要素：
 - 信息素 蚂蚁沿路径释放，随时间推移挥发
 - 移动规则 倾向于走信息素浓度高，路径短的路径
 - 启发式信息 距离、方向、障碍物等，有利于指导蚂蚁移动方向，提高搜索效率
- 收敛性：蚁群算法具有较好的收敛性，能够在较短的时间内找到近似最优解
- 参数：信息素挥发速度、蚂蚁数量、移动概率
- 优化方法：遗传算法、粒子群算法等
- 步骤：
 1. 初始化蚁群
 - (a) 每只蚂蚁的方向和位置
 - (b) 信息素浓度

2. 迭代搜索过程

- (a) 蚂蚁根据移动规则运动
- (b) 更新路径信息素浓度
- (c) 重复迭代过程

3. 最优解输出

8.3 具身智能

基于物理身体进行感知和行动的智能系统
虚拟环境

优势 安全、可扩展

要素 模拟器、资产、任务

模拟器

物理仿真 动力学的数学模型

感知信号渲染 对机器人和周围环境的观测

要素 渲染、物理特性、速度、对象类型和属性、动作建模、人机交互界面

资产 (静态/可交互): 物体、场景、指令等数据结构

任务

- 定位 Localization
- 视觉导航 Visual Navigation
- 对话驱动视觉导航 Visual Navigation
- 具身问答 Embodied Question Answering

Sim2Real迁移:

1. 环境
2. 仿真
3. 任务

8.4 进化计算

概念:

进化计算 模仿生物遗传并运用于复杂的优化问题

遗传算法 基于进化过程中信息遗传机制和优胜劣汰自然选择原则的算法

基本遗传算法 Simple Genetic Algorithm(SGA)

要素:

染色体编码 将问题的解空间编码为染色体, 用于遗传算法操作

适应度函数 评估染色体好坏

遗传算子

选择算子/复制算子 挑选一部分父代个体进入子代

交叉算子/杂交算子 挑选两个个体交换部分染色体形成新的个体

变异算子 改变染色体基因的值

参数

N 群体大小

T 进化代数

Pc 交叉概率 (0.4-0.99)

Pm 变异概率 (0.0001-0.1)

步骤

1. 初始化群体: 字符串编码、随机生成个体
2. 迭代: 计算个体适应值、通过三种算子(选择、杂交、变异)产生子代
3. 计算最高适应值, 输出最优值

9 人工智能系统与应用

9.1 自动驾驶系统

- 分级
 - 环境感知系统
 - 中央决策系统
 - 底层执行系统