- 计算机导论重要知识点
  - 无向图G存在欧拉通路的充要条件
  - 有向图D存在欧拉通路的充要条件
  - 简述欧拉回路与哈密尔顿回路的区别
  - 汉诺塔的搬动次数
  - 什么是顺序程序设计？什么是并行程序设计？
  - 什么是NP类问题？
  - 阿姆达尔定律
  - 寻找一个数的真因子
  - RSA公钥密码系统
    - 例1 在一个RSA公钥密码系统中，设公钥为（7，77），请找出其私钥
    - 例2 设p=11, q=13, n=11×13=143，请构建一个RSA公钥密码系统，并对报文9加密和解密。
  - 简述停机问题
  - 简述找零问题、背包问题与贪婪算法
  - 两军问题
  - 图灵测试和“中文屋子”是如何从哲学的角度反映人工智能本质特征的？
  - ER图
    - 例1：试给出3个实际的E-R图，要求实体之间的关系分别为一对一，一对多，多对多。
    - 例2： 一个公司有一个销售部门，一个销售部门有若干员工，每位员工都可以销售若干商品，每个商品都可以由若干员工销售，一个商品可以存放在若干不同的仓库中，一个仓库可以存放不同的商品，一个员工可以管理若干仓库，请画出该单位销售部的E-R图（提示：销售时有一个“销售明细”属性；存放时有一个“存放与出库时间”的属性）,请建立该公司销售部门的概念模型。
  - 图灵机
    - 工作原理：
    - 例题：
  - 冯·诺依曼型计算机
    - 体系结构及其特点
  - Vcomputer
    - 例1
    - 例2：
    - 例3(自修改）：
    - 例4(自修改）:
    - 什么是机器语言？什么是汇编语言？
  - 为什么说自然语言的“创造性”过程的本质与计算过程的本质是一致的？
  - 自然语言形式化
    - 图片说明

    - 例
  - 计算机对语言进行处理，首先要解决的是语言的歧义性问题，给出句子“I saw the man on the hill with the telescope”，不可能解释为

计算机导论重要知识点

无向图G存在欧拉通路的充要条件

G为连通图，并且G仅有两个奇度结点（度数为奇数的顶点）或者无奇度结点。

推论1：

1. 当G是仅有两个奇度结点的连通图时，G的欧拉通路必以此两个结点为端点。
2. 当G是无奇度结点的连通图时，G必有欧拉回路。
3. G为欧拉图（存在欧拉回路）的充分必要条件是G为无奇度结点的连通图。

有向图D存在欧拉通路的充要条件

D为有向图，D的基图连通，并且所有顶点的出度与入度都相等；或者除两个顶点外，其余顶点的出度与入度都相等，而这两个顶点中一个顶点的出度与入度之差为1，另一个顶点的出度与入度之差为-1。

推论2：

1. 当D除出、入度之差为1，-1的两个顶点之外，其余顶点的出度与入度都相等时，D的有向欧拉通路必以出、入度之差为1的顶点作为始点，以出、入度之差为-1的顶点作为终点。
2. 当D的所有顶点的出、入度都相等时，D中存在有向欧拉回路。
3. 有向图D为有向欧拉图的充分必要条件是D的基图为连通图，并且所有顶点的出、入度都相等。

简述欧拉回路与哈密尔顿回路的区别

“哈密尔顿回路问题”是访问除原出发结点以外的每个结点一次，而“欧拉回路问题”是访问每条边一次。对任一给定的图是否存在“欧拉回路”前面已给出充分必要条件，而对任一给定的图是否存在“哈密尔顿回路”至今仍未找到满足该问题的充分必要条件.

汉诺塔的搬动次数

2^n - 1

什么是顺序程序设计？什么是并行程序设计？

以教材“证比求易算法”为例，从2开始，一步一步地求48 770 428 433 377 171数的真因子是顺序算法，采用顺序算法进行的程序设计是顺序程序设计。按自然数的顺序给老百姓编号后，求真因子的算法是并行算法，采用并行算法进行的程序设计是并行程序设计。

什么是NP类问题？

在计算复杂性理论中，将所有可以在多项式时间内求解的问题称为P类问题，而将所有在多项式时间内可以验证的问题称为NP类问题.

阿姆达尔定律

设f为求解某个问题的计算存在的必须串行执行的操作占整个计算的百分比，p为处理器的数目，Sp为并行计算机系统最大的加速能力（单位：倍）

Sp <= 1/(f+(1-f)/p)

寻找一个数的真因子

什么叫真因子？
因子是指它所拥有的约数,真因子是指除它本身和1外没有其他约数

RSA公钥密码系统

例1 在一个RSA公钥密码系统中，设公钥为（7，77），请找出其私钥

根据题意，公钥(e, n)=(7,77), 知 e=7,n=77
（1）求p, q
设n = pq =77
对77进行分解，得7×11=77，又7，11为质数
所以p=7, q=11
（2）求d
存在k使得ed = k(p-1) (q-1)+1，因此，必定存在一个k使得
d= (k(p-1) (q-1)+1)/e
将e = 7，p=7,q=11代入上式，有d =(60k+1)/7
当k=1时，d=61/7
当k=2时，d=121/7
当k=3时，d=181/7
当k=4时，d=241/7
当k=5时，d=301/7
=43

根据题意，知d为整数，因此，d=43。
因此，该RSA公钥密码系统的私钥为(43,77)

例2 设p=11, q=13, n=11×13=143，请构建一个RSA公钥密码系统，并对报文9加密和解密。

（1）求e
当p=11, q=13时，(p-1)×(q-1) = (11-1)×(13-1)= 120
根据RSA公钥密码系统的构建，e必须与(p-1)×(q-1)互质，即与120互质。
设e=2，120 mod 2 = 0
设e=3，120 mod 3 = 0
设e=4，120 mod 4 = 0
设e=5，120 mod 5 = 0
设e=6，120 mod 6 = 0
设e=7，120 mod 7 = 1
由上可知，7与120互质，因此，e=7。
（2）求d
存在k使得ed = k(p-1) (q-1)+1，因此，必定存在一个k使得
d= (k(p-1) (q-1)+1)/e
将e = 7，p=11,q=13代入上式，有d =(120k+1)/7
当k=1时，d=121/7
当k=2时，d=241/7
当k=3时，d=361/7
当k=4时，d=481/7
当k=5时，d=601/7
当k=6时，d=721/7
=103
根据题意，知d为整数，因此，d=103。
因此，该RSA公钥密码系统的公钥为(7,143),私钥为(103,143)
（3）用公钥(7,143)对m=9进行加密
c = (mod n) = 97 (mod 143)
= 4782969 (mod 143)
= 48
（4）收到加密报文48，用私钥(103,143)进行解密
(mod n) = 48103 (mod 143)
=(1.4717954286441339093290587459855e+173) (mod 143)
=9

简述停机问题

停机问题是指：针对任意给定的图灵机和输入，寻找一个一般的算法（或图灵机），用于判定给定的图灵机在接收了初始输入后，能否到达终止状态，即停机状态。若能找到这样的算法，我们说停机问题可解，否则，不可解。换句话讲说，就是我们能不能找到这样一个测试程序，它能判断出任意的程序在接收了某个输入并执行后，能不能终止。若能，则停机问题可解，否则，不可解。

简述找零问题、背包问题与贪婪算法

设有不同面值的钞票，要求用最小数量的钞票给顾客找某数额的零钱，这就是通常说的找零问题。
给定n种物品和一个背包，设Wi为物品i的重量，Vi为其价值，C为背包的重量容量，要求在重量容量的限制下，尽可能使装入的物品总价最大，这就是背包问题。
贪婪算法是一种传统的启发式算法，它采用逐步构造最优解的方法，即在算法的每个阶段，都作出在当时看上去最好的决策，以获得最大的“好处”，换言之，就是在每一个决策过程中都要尽可能的“贪”， 直到算法中的某一步不能继续前进时，算法才停止。在算法的过程中，“贪”的决策一旦作出，就不可再更改，作出“贪”的决策的依据称为贪婪准则。贪婪算法是从局部的最优考虑问题的解决方案，具有简单快捷的优点。但是，这种从局部，而不是从整体最优上考虑问题的算法，并不能保证求得的最后解为最优解。

两军问题

两军问题可以这样描述：一支白军被围困在一个山谷中，山谷的两侧是蓝军。困在山谷中的白军人数多于山谷两侧的任一支蓝军，而少于两支蓝军的总和。若一支蓝军对白军单独发起进攻，则必败无疑；但若两支蓝军同时发起进攻，则可取胜。两支蓝军希望同时发起进攻，这样他们就要传递信息，以确定发起攻击的具体时间。假设他们只能派谴士兵穿越白军所在的山谷（惟一的通信信道）来传递信息，那么在穿越山谷时，士兵有可能被俘，从而造成消息的丢失。现在的问题是：如何通信，以便蓝军必胜。

图灵测试和“中文屋子”是如何从哲学的角度反映人工智能本质特征的？

图灵测试”不要求接受测试的思维机器在内部构造上与人脑一样，它只是从功能的角度来判定机器是否能思维，也就是从行为主义这个角度来对“机器思维”进行定义。尽管图灵对“机器思维”的定义是不够严谨的，但他关于“机器思维”定义的开创性工作对后人的研究具有重要意义，因此，一些学者认为，图灵发表的关于“图灵测试”的论文标志着现代机器思维问题讨论的开始。
西尔勒借用语言学的术语非常形象地揭示了“中文屋子”的深刻寓意：形式化的计算机仅有语法，没有语义。因此，他认为，机器永远也不可能代替人脑。作为以研究语言哲学问题而著称的分析哲学家西尔勒来自语言学的思考，的确给人工智能涉及的哲学和心理学问题提供了不少启示。

ER图

ER图分为实体、属性、关系三个核心部分。实体是**长方形**体现，而属性则是**椭圆形**，关系为**菱形**。

ER图的实体（entity）即数据模型中的数据对象，例如人、学生、音乐都可以作为一个数据对象，用长方体来表示，每个实体都有自己的实体成员（entity member）或者说实体对象（entity instance），例如学生实体里包括张三、李四等，实体成员（entity member）/实体实例（entity instance） 不需要出现在ER图中。

ER图的属性（attribute）即数据对象所具有的属性，例如学生具有姓名、学号、年级等属性，用椭圆形表示，属性分为唯一属性（ unique attribute）和非唯一属性，唯一属性指的是唯一可用来标识该实体实例或者成员的属性，用下划线表示，一般来讲实体都至少有一个唯一属性。

ER图的关系（relationship）用来表现数据对象与数据对象之间的联系，例如学生的实体和成绩表的实体之间有一定的联系，每个学生都有自己的成绩表，这就是一种关系，关系用菱形来表示。

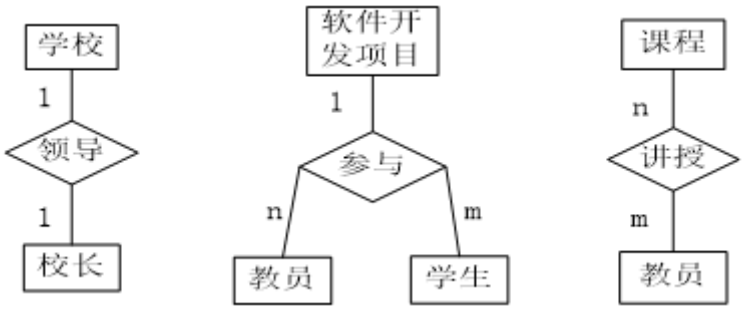
ER图中关联关系有三种：

1对1（1:1）：1对1关系是指对于实体集A与实体集B，A中的每一个实体至多与B中一个实体有关系；反之，在实体集B中的每个实体至多与实体集A中一个实体有关系。

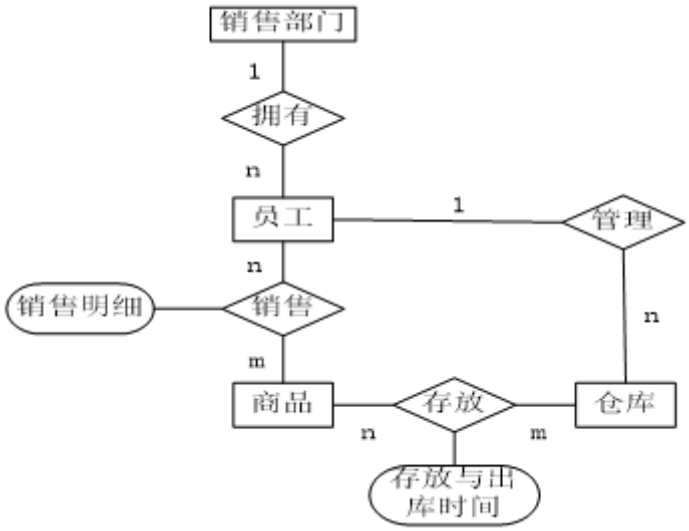
1对多（1:N）：1对多关系是指实体集A与实体集B中至少有N(N>0)个实体有关系；并且实体集B中每一个实体至多与实体集A中一个实体有关系。

多对多（M:N）：多对多关系是指实体集A中的每一个实体与实体集B中至少有M(M>0)个实体有关系，并且实体集B中的每一个实体与实体集A中的至少N（N>0）个实体有关系。

例1：试给出3个实际的E-R图，要求实体之间的关系分别为一对一，一对多，多对多。



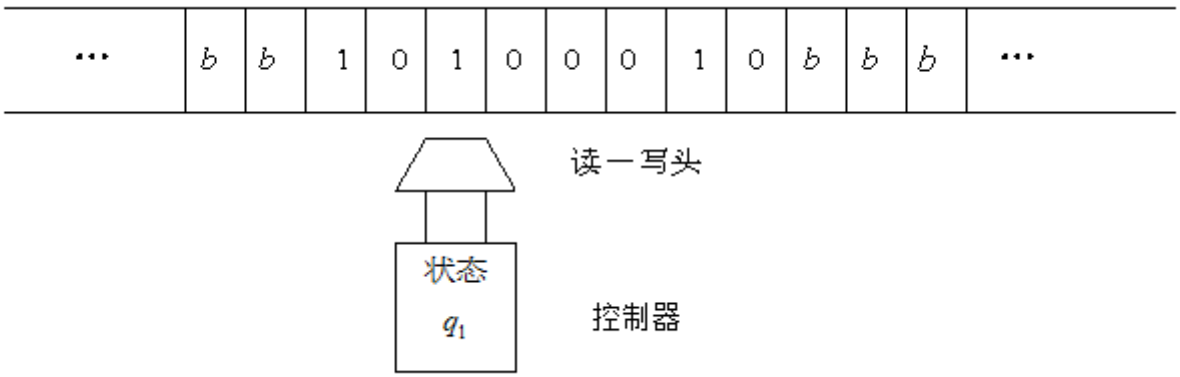
例2： 一个公司有一个销售部门，一个销售部门有若干员工，每位员工都可以销售若干商品，每个商品都可以由若干员工销售，一个商品可以存放在若干不同的仓库中，一个仓库可以存放不同的商品，一个员工可以管理若干仓库，请画出该单位销售部的E-R图（提示：销售时有一个“销售明细”属性；存放时有一个“存放与出库时间”的属性）,请建立该公司销售部门的概念模型。



图灵机

工作原理：

机器的控制状态表为：{q1，q2，…，qm}。通常，将一个图灵机的初始状态设为q1，在每一个具体的图灵机中还要确定一个结束状态qw。
一个给定机器的“程序”认为是机器内的五元组（qiSjSkR（或L或N）ql）形式的指令集，五元组定义了机器在一个特定状态下读入一个特定字符时所采取的动作。5个元素的含义如下：
qi表示机器目前所处的状态；
Sj表示机器从方格中读入的符号；
Sk表示机器用来代替Sj写入方格中的符号；
R、L、N分别表示向右移一格、向左移一格、不移动；
ql表示下一步机器的状态。



例题：

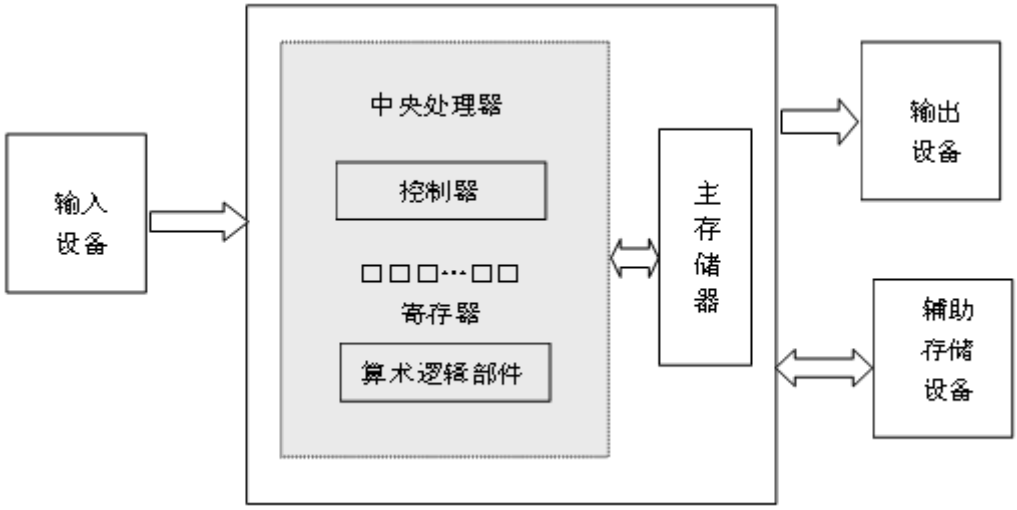
计算题：在图灵的带子机中，设b表示空格，q1表示机器的初始状态，q4表示机器的结束状态，如果带子上的输入信息是11100101，读写头对准最右边第一个为1的方格，状态为初始状态q1。写出执行以下命令后的计算结果。
q1 0 0 L q2

q1 1 0 L q3
q1 b b N q4
q2 0 0 L q2
q2 1 0 L q2
q2 b b N q4
q3 0 0 L q2
q3 1 0 L q3
q3 b b N q4
解：计算结果为00000000或0。

冯·诺依曼型计算机

体系结构及其特点

冯·诺依曼计算机（单指令顺序存储程序式计算机）的体系结构由存储器、控制器、运算器、输入和输出设备等五个基本部件组成的，如图所示：



冯·诺依曼计算机的体系结构，也即存储程序式计算机的体系结构的特点，是将程序与数据一样看待，对程序像数据那样进行适当的编码，然后与数据一起共同存放在存储器中。这样，计算机就可以通过改变存储器中的内容，对数据进行操作。从原来对程序和数据的严格区别到一样看待，这个观念上的转变是计算机史上的一场革命，它反映的正是计算的本质，即符号串的变化。

Vcomputer

例1

设机器从内存地址00开始执行，请用Vcomputer机器指令写一个程序，计算内存单元B1，C1，D1中所有值的和，将结果放入内存地址E1中。

答：

```
地址      内容
00        10
01        B1  ;将B1单元中的内容放入R0中
02        11
03        C1  ;将C1单元中的内容放入R1中
04        12
05        D1  ;将D1单元中的内容放入R2中
06        53
07        01  ;将R0和R1中的内容相加放入到R3中
08        54
09        23  ;将R2和R3中的内容相加放入到R4中
0A        34
0B        E1  ;将R4中的内容放入E1单元中
0C        90
0D        00  ;停机
```

例2：

设机器从内存地址00开始执行，请用Vcomputer机器指令与汇编指令分别实现以下操作。

a．将寄存器1与寄存器2中的值相加，存入内存单元20中。

b．将内存单元25中的值，与寄存器1中的值相加，存入寄存器3中。

c．将寄存器1和寄存器2中的值互换。

答：

```
地址       内容
00          50
01          12  ;将R1和R2中的内容相加放入到R0中
----------
02          30
03          20  ;将R0中的内容存入20单元中
----------
04         10
05         25  ;将单元25中的内容存入R0中
----------
06          53
07          01  ;将R0和R1中的内容相加存入R3中
----------
08          40
09          10  ;将R1中的内容移动到R0中
----------
0A          40
0B          21  ;将R2中的内容移动到R1中
----------
0C         40
0D          02  ;将R0中的内容移动到R2中
----------
0E          90
0F          00  ;停机
```

汇编指令如下：

```
Add R0,R1,R2
Store R0,[20]
Load R0,[25]
Add R3,R0,R1
Move R1,R0
Move R2,R1
Move R1,R2
Halt
```

例3(自修改）：

用自然语言解释以下程序。

地址　内容

00　10

01　0C

02　11

03　0D

04　52

05　01

06　32

07　08

08　72

09　00

0A　90

0B　00

0C　60

0D　30

答：

程序思想：

1） 把0C单元中的内容（60）存放到R0中；（执行）

2） 把0D单元中的内容（30）存放到R1中；（执行）

3） 把RO和R1中的内容相加存入到R2中；（执行）

4） 把R2中的内容存入地址为08单元中；（执行）

5） 对R2中的内容取反；（未执行，停机。即修改自身程序）

6） 停止。（未执行）

由以上分析可知，该程序具有修改自身的功能。

例4(自修改）：

用自然语言解释以下程序。

```
地址    内容
00      10
01      0E
---------
02      70
03      00
---------
04      30
05      08
---------
06      11
07      0F
---------
08      71
09      00
---------
0A      31
0B      10
---------
0C      90
0D      00
---------
0E      6F
0F      52
```

答：

程序思想：

1） 把0E单元中的内容（6F）存入R0中；（执行）

2） 把R0中的内容按位取反；（执行）

3） 把R0中的内容（90）存放到08单元中；（执行）

4） 把0F单元中的内容（52）存入R1中；（执行）

5） 把R1中的内容按位取反；（未执行，停机。即修改自身程序）

6） 把R1中的内容存放到10单元中；（未执行）

7） 停止。（未执行）

由以上分析可知，该程序具有修改自身的功能。

什么是机器语言？什么是汇编语言？

每台数字电子计算机在设计中，都规定了一组指令，这组机器指令集合，就是所谓的机器指令系统。用机器指令形式编写的程序，称为机器语言。

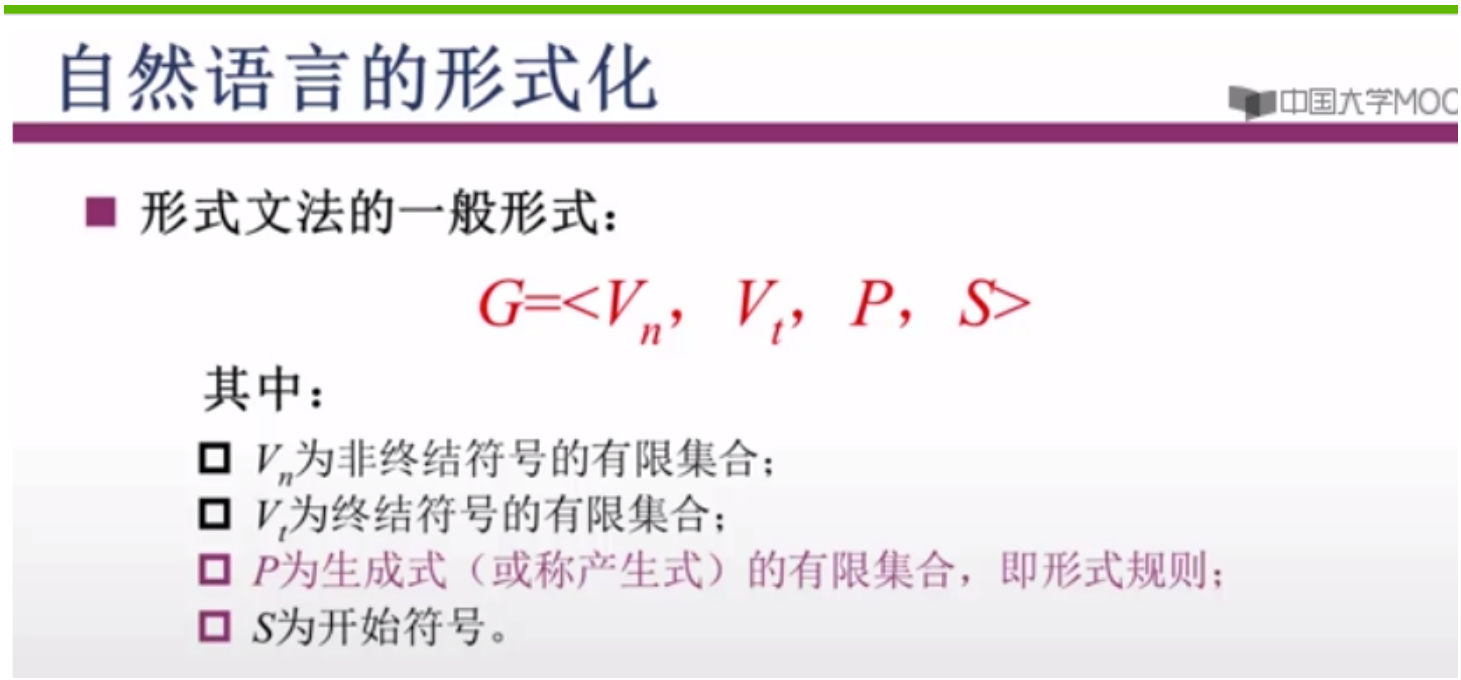
在机器指令的基础上，人们提出了采用字符和十进制数来代替二进制代码的思想，产生了将机器指令符号化的汇编语言。

为什么说自然语言的“创造性”过程的本质与计算过程的本质是一致的？

乔姆斯基把人所具有的创造和理解正确句子的能力称为语言的“创造性”（Creativity）。而语言“创造性”过程的本质，其实就是由有限数量的词根据一定的规则产生正确句子的过程，进一步而言，其实质也就是一个字符串到另一个字符串的变换过程。显然，语言“创造性”过程的本质与计算过程的本质是一致的，因此，可以将自然语言也看作是一种计算，从而自然语言能否实现形式化的争论也就不存在了。

自然语言形式化

图片说明



例

根据本章给出的自然语言形式化例子中的转换规则，给出句子“我教他学汉语”的派生过程。

解：

S
NP VP
N V S
N V NP VP
N V N VP
N V N V NP
N V N V N
我 V N V N
我 教 N V N
我 教 他 V N
我 教 他 学 N
我 教 他 学 汉语

计算机对语言进行处理，首先要解决的是语言的歧义性问题，给出句子**“I saw the man on the hill with the telescope”**，不可能解释为

- A. the hill with the telescope
- B. I with the telescope
- C. I on the hill
- D. the man with the telescope