内容

什么是信息

1. 信息论是研究什么的？
   信息的存储、传输、处理的一般规律；目的：高效可靠传输。
2. 信息论是研究信息的科学和理论，它定量地描述信息的统计特性。
3. 信息是对认识在传输过程中特性的度量。
4. 消息的知识量固定且巨大、传输目的、传递的信息量随接收者（他们所具有的知识不同）而异。
5. 信息是对在传消息中接收者尚未了解的（不知道的、不掌握的）那部分知识的度量。
6. 接收者知识增加了多少，就获得了多少信息。
7. 信息的特点。
   与接收者的先验知识有关；与主观感受无关；与重要程度无关。

通信系统模型：信源编码与信道编码。

信息量及信息熵的定义，信息的单位

1. 信息量的定义；$I_x \triangleq \log_a \frac{1}{p_x} = -\log_a p_x$
2. 该信息量定义的优缺点；
3. 信息熵的定义及其计算；

$$H(X) \triangleq E\left[I_{x_i}\right] = \sum_{i=1}^{N} p_{x_i} \log \frac{1}{p_{x_i}} = \sum_{x} p(x) \log \frac{1}{p(x)}$$

4. 信息熵的性质
   极值性、对称性、非负性、可加性、强可加性、上凸性。
5. 信息的单位及换算。比特、奈特、笛特（哈特利）

消息的形式与编码

可以通过数值编码剥去消息的形式后，研究所含知识在传输中的统计特性。

1. 常见的消息形式—文字、声音与图像
2. 文字消息的编码
3. 声音或图像信号，抽样与量化。
4. 抽样是可恢复性的。
5. 量化过程是不可恢复的。

信源的种类

从信源消息的取值集合角度看，可分为离散、连续；
从信源消息的统计特性看，可分为无记忆、有记忆；

1. 离散无记忆信源DMC $H(X)=\sum_i p_i \log \frac{1}{p_i} \quad R=rH(X)$
2. 连续无记忆信源

$$H_{abs}(X)=H(X)+\infty \quad H(X)=\int p(x)\log\frac{1}{p(x)}dx$$

连续如何处理，先量化、再让量化台阶无穷小。绝对熵与相对熵。
连续变量所含的信息量是无穷大；绝对熵非负，相对熵可正可负。

3. 离散记忆信源
冗余来自两个方面：符号间不等概或不独立。记忆表现为符号间不独立。联合熵与条件熵
4. 信息率—单位时间内发出的平均信息量。

信息在信道中传送

信息论定量地研究信息在传输过程中的统计特性。
信息在信道中传送，因此要研究

1. 互信息，使用信道一次能够传输多少信息；
2. 互信息熵，信道使用一次平均能够传输多少信息；
3. 信道容量，信道使用一次能够传输的平均信息量的最大值。

信道的模型、分类

1. 从通信过程抽象出信道模型。
强调：输出与输入间不是确定性关系，而是统计依赖关系。
2. 信道的分类。
主要强调：离散、单用户、无记忆、无反馈、固定参数信道。
3. 信道模型举例。
BSC，BEC。

互信息与互信息熵

1. DMC信道，无记忆：信道的输出仅与当前时刻的输入有关。
2. 互信息是消除了的不确定性。互信息与自信息。

$$I(a_k;b_j)\triangleq I(a_k)-I(a_k|b_j)=\log\frac{p(a_k|b_j)}{p(a_k)}$$

3. 互信息具有对称性。
4. 互信息是随机的，引入互信息熵。

$$I(X;Y)=I(Y;X)=\sum_{k,j}p(a_k,b_j)\log\frac{p(a_k|b_j)}{p(a_k)}$$

5. 互信息可正可负，可为零；互信息熵非负。

互信息熵的变形及意义

1. 信源熵减疑义熵：$H(X)-H(X|Y)$;
2. 信宿熵减噪声熵：$H(Y)-H(Y|X)$;
3. 信源熵加信宿熵减联合熵：$H(X)+H(Y)-H(X,Y)$。
4. 用Venn图（文氏图或维拉图）表示各种熵之间的关系。
5. 理想（无噪无损）信道的疑义熵和噪声熵等于零；强噪信道的互信息熵等于零，不能用来传输信息。
6. 无噪有损信道的噪声熵等于零；有噪无损信道的疑义熵等于零。
7. 四种特殊信道互信息熵的计算。
8. 举例计算BSC信道的互信息熵，一般情况下用变形2计算比较方便。
9. 互信息熵的性质：对称、非负。
10. 连续无记忆信道的互信息。
香农公式$I(X;Y)=\frac{1}{2}\log\left(1+\frac{E}{\sigma_n^2}\right)$

信道容量

1. 在可靠的前提下，希望传输得越多越好。
2. 传输信息量的多少与信源分布和信道前向转移概率有关。信道确定后，应该对输入分布求最大。
3. 带约束的极值问题，凸域与凸函数、凸函数的定义、性质及几何意义。
4. 概率向量域是凸域。
5. 任一随机变量的信息熵是严格凸函数。
6. 定义在概率向量域上的凸函数取最大值的充要条件。
7. DMC的互信息熵是输入概率分布的凸函数。
8. DMC互信息熵最大的条件是部分互信息熵相等。
9. 这个相等的部分互信息熵就是信道容量。
10. 对称DMC信道在输入等概分布时达到信道容量。
11. 对称信道的判断，用部分互信息熵求信道容量。

信源编码与信道编码

1. 有了信息的度量、信道及信道容量的概念。从传输的角度，只要需要传输的信息量不超过信道容量，就总可以想办法传过去。信道编码定理就是要证明这一点。
2. 信源编码与信道编码的讨论。
二者的目的不同。研究信源编码时，把信道编解码看作信道的一部分，即把信道编码-信道-信道解码作为一体看作理想信道。
3. 要充分利用信道容量是有条件的。
信道的输入在某种程度上是可以分割组合的。
4. 编码器的结构。
5. 码的属性与分类，分组码、定长编码与变长编码、非奇异码、唯一可译码、即时码。

序列的概率、信息量及熵

编码定理都是通过序列证明的。

1. 离散无记忆信源所产生序列的概率等于序列各符号发生的概率之积。$P(u^L)=\prod_{l=1}^{L}P(u_l)$
2. 离散无记忆信源产生的序列的信息量等于序列各符号携带的信息量之和。$I(u^L)=\sum_{l=1}^{L}I(u_l)$
3. 长为L的离散无记忆序列的熵等于一个符号熵的L倍。
$H(U^L)=LH(U)$
4. 有记忆时序列的熵小于无记忆序列的熵。
5. 序列通过信道。
低进制信道使用多次可以看作高进制信道使用一次，等效信道。
6. 序列通过信道的互信息熵。
7. 信源编码要求输出尽可能等概、尽可能短。

定长编码

1. 无误编码，码序列的个数不少于源序列的个数。

$$D^N \geq K^L \Rightarrow N\log D \geq L\log K, L\log K \geq LH(U).$$

2. 序列长度趋于无穷大时每个符号携带的平均信息量趋于信源熵。
3. 有编码损失（足够小），码序列个数小于源序列个数。
   仅对典型序列编码，即出现概率在下式范围内的序列。

$$2^{-L[H(U)+\delta]} \leq P(U_T^L) \leq 2^{-L[H(U)-\delta]}$$

   这要求$N\log D \geq L[H(U)+\delta]$，此时可以有$L\log K \geq N\log D$
4. Chebyshev不等式。典型序列数上界、下界的估计。
5. 编码效率、编码损失、联合编码长度的计算举例。
   最佳定长编码的效率：

$$\eta = \frac{H(U)}{H(U)+\delta}$$

变长编码

1. 平均码长的定义。$\bar{n} = \sum_{k=1}^{K} P(s_k)n_k$
2. 唯一可解码（唯一可解码很难判断）与异前缀码（一定是唯一可解的）。
   唯一可解不一定是异前缀码，但对任意唯一可解码，可以构造出与其码长分布相同的异前缀码。所以，可以只研究异前缀码。
3. 码树，Kraft不等式与异前缀码。
   唯一可解码与异前缀码的码长一定满足Kraft不等式。满足Kraft不等式一定存在异前缀码。
4. 变长变码定理。

$$\frac{H(U)}{logD} \leq \overline{n} < \frac{H(U)}{logD} + 1.$$

5. 编码效率的定义及计算，通过扩展编码提高编码效率。

Huffman编码

最佳—平均码长最短。

1. 最佳异前缀码必须满足可能性最小（即概率最小）的两个源符所编的码字长度最长且相等。
2. 可以按递归（迭代）编码方法得到最佳的异前缀编码。
3. Huffman编码步骤，平均码长及编码效率的计算。
4. L次扩展编码。
5. 多进制Huffman编码，空枝数的计算。

$$B = D - 2 - R_{(D-1)}(K-2)$$

$$M = D + m(D-1)$$

信道编码的基本概念

信道不理想会带来误码，信道编码的目的就是通过编码来减小因传输错误而造成的误码。希望用尽可能少的保护实现可靠通信。

1. 线路编码与信道编码。
   信息论中的信道编码指差错控制编码（即各种形式的检错码、纠错码）。
2. 编码方式及译码方法对系统误码率有影响。
3. 信道编码中的一对矛盾—误码率与传输效率。
4. 信道编码增加冗余，但不改变信息量，改变的是每符号平均携带的信息量。

信道速率

1. 信道速率的定义。
   信道每用一次所需要传递的信息量。
2. 信道速率没有任何时间的概念，而是次的概念。
3. 与互信息定义的比较。
4. 信源编码理想时:
   $R = \frac{LH(U)}{N} = \frac{L\log K}{N} = \frac{\log K^L}{N} = \frac{\log M}{N}$
5. 编码定理要证明的是：只要信道速率小于信道容量，总存在一种编码使误码率任意小。

解码准则与解码过程

1. 解码规则，解码误差的计算;
2. 最小误差解码（最大后验概率）;
3. 最大似然解码（最大先验概率）;
4. 输入等概时二者一致。
5. 译码过程，输出子集的划分。

二元编码误差

1. 发某个码字时的误码率
   $$P_{e,m} \le \sum_{y^N} p\left(y^N|x_1^N\right)^{1-s} p\left(y^N|x_2^N\right)^s \quad m=1,2 \quad 0<s<1$$
2. DMC信道
   $$P_{e,m} \le \prod_{n=1}^{N} g_n(s) \qquad m=1,2 \qquad 0<s<1$$
   其中，$g_n(s) \triangleq \sum_{y_n} p\left(y_n|x_{1,n}\right)^{1-s} p\left(y_n|x_{2,n}\right)^s$
3. 辅助函数$g_n(s)$的性质
   边值$g_n(0) \le 1, g_n(1) \le 1$、凹函数。本质上反映了码字选定后，码字序列中第$n$个码元的区分能力。
4. 不同编码方式下$g_n(s)$的计算及误码率上界的比较
   所有位不同、一半位不同、随机选码。可选码字集合的增加带来误码率的增大。

多元编码误码率上界

1. 随机编码的Gallager界
2. DMC错误概率上界
   $$\overline{P}_e < M^{\rho}\left\{\sum_y\left[\sum_x q(x)p(y|x)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\}^N$$
3. 可靠性函数
   $$\overline{P}_e < \exp\left\{-N\left[E_0\left(\rho\,,\,\mathbf{Q}\right)-R\rho\right]\right\} = \exp\left[-NE_r\left(\rho,\mathbf{Q},R\right)\right]$$
   其中，
   $$E_0(\rho,\mathbf{Q}) = -\ln\sum_y\left[\sum_x q(x)p(y|x)^{\frac{1}{1+\rho}}\right]^{1+\rho}, 0\le\rho\le 1$$

编码指数

$$E_r(R,\mathbf{Q}) \triangleq \max_{0\le\rho\le 1}[E_0(\rho,\mathbf{Q})-\rho R]$$

$$E_r(R) \triangleq \max_{\mathbf{Q}} E_r(R,\mathbf{Q})$$

Holder不等式及变形。
$E_0(\rho,\mathbf{Q})$的性质。

1. 二阶导小于等于零（上凸函数）；
2. 一阶导是个减函数，最大值为互信息熵，最小值大于零;
3. 恒为正。

$E_r(R,Q)$的讨论及曲线绘制，$E_r(R)$曲线。
总结有噪信道编码定理。

率失真理论的基本概念

由前两章的结论，无论是理想的无噪信道还是有噪信道，只要信息率小于信道容量，总能找到一种编码，从而以任意小的错误概率，任意接近信道容量的传输率在信道上传送信息。

反之，如果信息传输率大于信道容量，就不存在能实现无失真传输的编码。因此，需要研究有失真的编码。

信息率失真理论回答了这些问题，论述了在限失真范围内的信源编码问题。它是量化、数模转换、频带压缩和数据压缩等现代通信技术的理论基础。

基本的研究方法：把有失真的信源编码器看作有干扰的信道。

失真度与平均失真度

1. 失真度（函数）的定义。它是一个非负实值函数，其值可以人为规定。
2. 失真矩阵。汉明失真、平方误差失真。
3. 平均失真度。

$$\overline{D}=\sum_{i=1}^{R}\sum_{i=1}^{S}P(a_i,b_j)d(a_i,b_j)=\sum_{i}\sum_{j}P(a_i)P(b_j|a_i)d(a_i,b_j)$$

4. 离散无记忆平稳信源的N次扩展信源通过无记忆编码器编码后的平均失真度。

$$\overline{D}(N)=N\overline{D}$$

率失真函数及其性质

1. 保真度准则。编码器引起的平均失真不能超过某一给定的限定值。
2. D失真许可的试验信道。满足保真度准则的试验信道。
3. 信息率失真函数。
   在满足保真度准则的情况下，寻找信源必须传给信宿的信息率的下限。将该问题转化为寻找满足保真度准则且平均互信息最小的试验信道。即在集合B_D中寻找平均互信息最小的信道。

$$R(D)=\min_{B_D} I(\mathbf{X};\mathbf{Y})$$

4. 信息率失真函数的物理意义：对给定信源，在满足一定失真度要求的条件下，信息率可以压缩到的最小值（信源必须输出的最小信息率）。
5. 率失真函数仅取决于信源特性和保真度要求，与信道特性无关。
6. 率失真函数与信道容量的比较。

率失真函数及其性质

1. 率失真函数$R(D)$的定义域$(D_{\min}, D_{\max})$。
   只有当失真矩阵中每行至少有一个零元素时，信源的平均失真度才能达到零。
2. 率失真函数的值域$(R(D_{\max}), R(D_{\min}))$。
   只有当失真矩阵中每行至少有一个零，且每列最多只有一个零时$R(D_{\min}) = R(0) = H(X)$。
3. 信息率失真函数是允许失真度的下凸函数。
4. 信息率失真函数是严格递减的连续函数
5. 限失真信源编码定理。

编码概述

1. 编码目的：提高通信的有效性、可靠性和保密性。
2. 编码问题：搜索好码、编译码方法、性能分析。
3. 纠错码的分类。
4. 分组码举例。
5. 卷积码的特点及描述方式。移位寄存器、树状图、状态转移图、网格图。

近世代数

1. 群的定义及基本性质（恒元、逆元唯一），交换群，举例。
2. 子群和陪集，陪集展开，群元素与陪集展开。
3. 环的定义，交换环，环的性质及举例。
4. 域的定义及基本性质，域的例子（有理数、实数、复数）
5. 伽罗华域$GF(q)$，$q = p^m$为域的阶。
6. 有限域的特征，域元素的阶，本原元素。
7. $GF(2)$域上的多项式，既约多项式与本原多项式。
8. 由$GF(2)$构造$GF(2^m)$，域元素的三种表示。
9. $GF(2)$上多项式的根。共轭元、域元素的最小多项式。

线性分组码的定义及编译码

1. 线性分组码的定义。
   二元分组码是线性的充要条件是两个码字的模2和也是码字。分组码的线性只与选用的码字有关。特殊关系。
2. 码字的重量、最小距离、错误图样。纠错能力与最小重量。
3. 编码。生成矩阵$\mathbf{G}$的行向量张成码字空间（线性子空间、子群）。
4. 一致校验矩阵$\mathbf{H}$，$\mathbf{G}\mathbf{H}^T = 0$。不唯一。
5. 等价码，纠错能力相同。
6. 系统码及标准生成矩阵。
7. $\mathbf{H}$的性质，码字的最小重量与$\mathbf{H}$的列向量之间的关系。
8. 译码。伴随式的定义及性质。
9. 标准阵的定义及构造，性质。
10. 伴随式译码的步骤。译码举例。

分组码的纠错性能及汉明码

1. 分组码的模数表示；编码效率的Plotkin上界。没讲，不考
2. 编码效率的汉明上界，$n-k \geq \log_q \left[\sum_{i=0}^{t} \binom{n}{i}(q-1)^i\right]$。
3. 完备码。$t=1$时，对任意的$n-k \geq 2$均存在完备码，编码效率随$n-k$的增加而增加。
4. 汉明码的定义，可纠一位错的完备的线性分组码。$(2^m-1, 2^m-1-m)$
5. 汉明码的设计。关键是校验矩阵$\mathbf{H}$的设计。
   通过分析纠错能力的要求构造$\mathbf{H}$。
6. 汉明码的伴随式矩阵。

循环码

1. 循环码的特点与定义（线性分组、循环性），举例。
2. 循环码与多项式，多项式的移位与循环移位。
3. 最低次码多项式唯一，且常数项必为1。
4. 码多项式的充要条件，是生成多项式$g(x)$的倍式。
5. 生成多项式$g(x)$的是x^n+1的因式；x^n+1的$n-k$次因式生成(n,k)循环码。举例。
6. 以$n=10, 15$为例讨论循环的生成多项式。
7. 非系统码的生成矩阵。用$x^i g(x), 0 \leq i \leq k-1$作为$\mathbf{G}$的行。
8. 系统循环码。

$$\mathbf{C}(x) = u(x)x^{n-k} + u(x)x^{n-k}\Big|_{\bmod g(x)}$$

9. 系统循环码生成矩阵。

$$x^{n-k+i} + x^{n-k+i}\Big|_{\bmod g(x)}$$

循环码

1. 非系统循环码的编码电路。移位、模2加，卷积。
2. 系统循环码的编码电路。用反馈移位寄存器实现除法运算求得余数。
3. 循环码的伴随式译码。伴随多项式的循环性。
4. 梅吉特译码器。
5. BCH码的特点及定义。
6. 本原BCH码的生成多项式。举例
7. BCH码的结构。用校验矩阵证明最小距离。
8. 多元BCH码。
9. RS码的定义，生成多项式（系数取自$GF(2^m)$）。$(n, n-2t)$
10. RS码的编码，非系统编码、系统编码。

卷积码

1. 卷积码的特点。
2. 卷积码的生成矩阵描述。
3. (n,k,m)的状态数。每种状态可能的输出数。
4. Viterbi译码。最大似然译码。若两条路径在某点汇聚，则这两条路径在此后就合成一条路径。即在汇聚点比较两条路径与比较整个序列的两条路径是一致的。
5. 译码过程的核心操作，加-比-选。举例。