中国科学技术大学

信息论复习宝典

学　　院：信息科学技术学院

课　　程：信息论基础

主　　编：高源

定稿日期：2023 年春

目录

前言

亲爱的读者：

你好！

如果你正在学习信息论课程，或者正在准备信息论课程的期末考试，那这本书可能会对你有所帮助。作者基于三年担任信息论课程助教期间答疑、批改作业等过程中收获的反馈，考虑到同学们考前复（预）习时候的需求，特别编著了这本《信息论复习宝典》。

这本书包括信息论解题模型、考点总结、专题复习计划、模拟试卷。信息论解题模型为作者基于对课程的理解总结而成，如果能够熟练掌握该模型，可以顺利解决信息论课程中的各种常见题目，在 2023 年信息论第一次习题课上作者也向班级同学验证了这一点。考点总结部分针对同学们在学习、复习以及考试中经常出现的问题进行总结，同时结合对课程的理解梳理了课程中的重要考点，并对难点进行讲解。如果读者处于复（预）习初期，可以对照着考点总结，筛选目前以及掌握的、还未熟练掌握的、不了解的，然后根据掌握程度安排复习计划。如果读者已经完成了复习，可以对照考点总结检查自己是否存在疏漏。专题复习计划专门针对考试题目对不同考点的考察方式进行设计，读者可以按照自己规划好的节奏对照着专题复习计划中的题目完成复习，这里特别提示，专题复习计划中的题目是作者模拟出题人的视角充分归纳不同的考点对应的考察形式，其中包括作者在习题课上反复强调的易错点等，建议读者在使用的时候主要检查自己在面对每道题目的时候是否有处理思路。模拟试卷主要包含近两年考前准备的模拟题目，建议需要做模拟考试练习的读者使用。

本书包括不同形式的复习材料，供不同需求的读者使用。将这些材料整理成这本书，也是作为对作者三年课程助教经历的总结，同时为学习信息论课程的同学提供可能的帮助。除此外，本书也可以作为将来担任信息论课程的助教同学们准备习题课的参考。作者谨祝愿学习信息论课程的同学都能有满意的收获，祝愿信息安全专业信息论课程教学工作越来越好！

祝好！

高源

2023 年春

信息论解题模型

作者在 2023 年春季学期任助教期间，通过在批改作业和答疑中获得的反馈，决定系统地给班级同学总结出信息论课程常用解题方法组合成的信息论解题模型。本质上，是在熟练掌握各个重点内容后的比较、凝练以及在解决具体题目时的经验总结。

读者可以在《信息论学习指导》中找到这里的总结所对应的具体内容，并可以从每一道作业题中检验该模型的使用方法和价值。

1. 定义。定义是最朴素也是在很多时候最有效的解决方法。作者在答疑过程中发现同学们解题遇到困难往往都是由于没有弄清楚题目中所对应的概率模型。作者建议，如果遇到一个题目不知道从何处切入的时候，首先问一下自己，**概率分布是否搞清楚了**。

2. 性质。信息量的一些重要性质，例如离散情形熵、相对熵、互信息非负性，熵的极值性、独立界等等。要注意的是，每一条性质的完整描述，例如“条件使得熵减少”中条件是“随机变量”而非“事件”。

3. 链式法则。信息量的展开处理是处理二元乃至多元问题的常用手段. 这一点也不难解释，我们常用的结论往往都是关于单个变量之间的关系。

4. 重要不等式。Jesen 不等式、数据处理不等式、费诺不等式等重要不等式，是这门课程中常用的解题手段。

5. 信息论常用技巧。遇到“随机变量依概率选择”问题时往往需要引入示性变量（费诺不等式的证明）。构造一个信息量的不同展开式也是一种非常常见的技巧（数据处理不等式、费诺不等式的证明）。

6. 一般性的解题技巧。例如利用上界和上确界的关系：题目要求求解最大值，直接求解往往需要建模成函数极值问题，如果发现求解起来有些麻烦，可以考虑先利用信息论的技术对其进行放缩（例如用性质、重要不等式），然后给出等号成立条件，也就是举例子说明这个上界能取到，即为上确界（这个是必要的，不然前面的过程只能得到上界，而不是上确界。关于例子，可以通过观察题目前几问提供的信息、基于性质的猜测等等得到）。一些具有多个小问的题目不同的小问之间可能是存在一定的关系的，有时候前面的小问会是给后面问题的辅助。要学会猜测

出题人意图，比如作业题目中有一道题给了一个情景并要求计算估计量和验证费诺不等式，那出题人可能是会希望你给出紧致的结论，所以要考虑费诺不等式的加强版本。

这个信息论解题模型是作者在课程学习和三个学期担任助教期间的经验总结，并在 2023 年春季学期的习题课中分享给班级同学，在讲解每一道题目的时候都展示了该模型是如何使用的. 作者希望这个模型能够给读者带来帮助，或是把作者总结的模型消化吸收，或者以此为参考自己总结适合自己学习的模型，或者以此为参考自己选择合适的信息论学习方法。

考点总结

3.1 第二章 熵、相对熵、互信息

这一章的考题往往是包含一道选择题（判断信息量不等式是否成立），一道填空题（可能正向考察信息量的计算，也可能逆向考察基于已知信息量推导概率分布），判断题加大题共两道（判断题主要考察对信息量数学性质的理解，大题主要考察信息量不等式的证明或者计算）。

1. 信息量定义。例：比较 $H\left(p_1, p_2, \ldots, p_n\right)$ 和 $H\left(p_1, p_2, \ldots, p_m, q_m\right) + q_m \log(n-m)$ 的大小，其中 $q_m = \left(1 - \sum_{i=1}^{m} p_i\right)$。
   - 虽然解题的时候往往会采用更高效的方法，如性质、链式法则等，但要时刻记得最基本的定义，如果其他方法都失效的时候就需要用定义来解决问题。
   - 一般来说，熵的定义式比较常用，二元相对熵的定义式 $H(Y \mid X) = \sum_{x \in \mathcal{X}} p(x) H(Y \mid X = x)$ 比较常用，相对熵的定义式在解决含相对熵的问题时较为常用，联合熵、互信息的定义式应用较少（往往是利用链式法则等进行展开处理）。
   - 关于熵的定义式有一个易错点，$H(p)$ 表示参数为 p 的伯努利分布的熵，其定义式为 $H(p) = -p \log p - (1-p) \log(1-p)$，而非 $-p \log p$。
   - 注意信息量的单位。
2. 信息量性质。例：比较 $H(Y \mid X = x)$ 与 $H(Y)$ 的大小。
   - 常用的性质参见作者编著的另一本教材《信息论学习指导》。
   - 信息量的性质往往应用于讨论信息量不等式，这时候就要关注不等号的方向问题，建议读者熟练掌握不同性质中不等号的方向，便于快速选择合适的性质用于解题。
   - 建议读者熟练掌握每条性质的完整内容（包括使用条件、具体数学描述以及等号成立条件等）。关于使用条件的问题，存在一些常见的易错点，例如“条件使得熵减少”中的“条件”应该为随机变量（即，条件熵）而非随机事件（随机变量固定了某个取值），“条件使得互信息减少”的成立条件是“构成了马尔科夫链”等。

- 一类常见的考试题是基于信息量的取值推导随机变量的概率分布，例如有三个二元离散随机变量 X, Y, Z 均服从伯努利分布，若要使得 $I(X;Y) = 1$ bit，$I(X;Y \mid Z) = 0$ bit，推导 X, Y, Z 的联合概率分布（往往是填空题）。这类题目就需要考生熟练掌握信息量的性质。

3. 重要的不等式。例：若 $X \to Y \to Z$，比较 $I(Y;Z)$ 与 $I(X;Z)$ 的大小。

- 三个重要的不等式包括 Jesen 不等式、数据处理不等式和费诺不等式。
- Jesen 不等式主要用于证明信息量的一些性质（例如熵的极值性），数据处理不等式用于处理马尔科夫链的相关问题，费诺不等式主要用于处理离散均匀分布信源在汉明失真下的率失真问题。
- 数据处理不等式的证明方法中所蕴含的技巧非常重要，在信息论解题模型中有总结。
- 注意每个不等式的成立条件。

4. 信息量的物理含义。例：已知 X, Y 的联合分布，通过测定 X 可以消除关于 Y 的不确定度是多少。

- 作业题目中涉及信息量计算的问题往往直接给出待计算的对象，但如果题目通过信息量的物理含义进行考察，读者也应理解待求解对象具体是什么。
- 信息量特殊取值的物理含义往往会用于解题，例如 $I(X;Y) = 0$ 表示随机变量 X, Y 独立，$H(Y \mid X) = 0$ 表示 $Y = f(X)$。

3.2 第三章 渐进均分性

这一章在近几年的期末考试题中没有出现，掌握作业题目中的三类问题即可。

1. 弱大数定理和渐进均分性定理。例：作业 3.9 题。

- 掌握定理的内容即可。

2. 给定集合的大小上下界证明。例：作业 3.4 题后两问。

- 采用和典型集大小的上下界证明相同的方法。详见《信息论学习指导》。

3. 典型集相关计算。例：作业 3.13 题。

- 掌握典型集的基本概念即可。

3.3 第四章 随机过程的熵率

这一章往往就是一道大题计算熵率，其中主要考察存在平稳分布的马尔科夫链的熵率计算。

1. 马尔科夫链平稳及其判断。
    - 理解平稳分布的含义，掌握不可约、非周期的判断方法。
2. 存在平稳分布的马尔科夫链的熵率计算。例：已知马尔科夫链状态转移概率矩阵，计算熵率。
    - 首先根据转移概率矩阵判断是否满足不可约、非周期。
    - 考试时候过程书写，第一步要写上"由题意知，马尔科夫链有限状态、不可约、非周期，因此平稳分布存在"。然后后面继续求解平稳分布，代入公式计算熵率。
    - 注意，题目中可能给出初始分布，这个往往是迷惑你的（但不排除，有可能会用于其他计算，比如计算初始条件下熵的大小），平稳马尔科夫链的熵率计算公式中一定要用平稳分布。
3. 加权图上随机移动问题。例：作业 4.22。
    - 这类问题如果考试出现，直接用公式。因此，需要读者记住公式，并且注意理解公式中每一项的含义。
4. 一般随机过程的熵率计算。例：作业 4.18。
    - 这类问题如果考试出现，只能用定义计算。考察可能性不大，不过还是建议读者记住熵率定义式。

3.4 第五章 数据压缩

这一章可能考察一道选择题（下列码字长度符合即时码要求的是、以下编码不可能是二元哈夫曼编码的是，也可能出成判断题），一道填空题（给出哈夫曼编码判断信源概率大小关系、计算期望码长等），一道大题（主要是给出概率分布进行哈夫曼编码）。

1. 唯一可译码、及时码、前缀码等概念。例：作业 5.37。
    - 掌握基本概念即可
2. Kraft 不等式。例：下列码字长度符合即时码要求的是。

- 掌握 Kraft 不等式的内容。
- 注意不等式是即时码存在的充要条件，也是即时码的必要条件。换句话说，给了一个符合不等式的码长，说明存在即时码满足该码长，但不能说明满足该码长的都是即时码。

3. 最优码长理论。例：若某信源有一个三元前缀码满足平均码长 $L = H_3(X)$，则其码字空间大小一定为奇数。

   - 掌握理论内容 $H_D(X) \leqslant L^* < H_D(X) + 1$。
   - 记住哈夫曼编码是最优码。这一性质往往会用于解题，例如上述问题的一种解法是"由于存在三元前缀码满足平均码长 $L = H_3(X)$，则可知该三元前缀码为最优码，又由于哈夫曼编码是最优码，因此该信源的三元哈夫曼编码的平均码长也是 $L_{huffman} = H_3(X)$，所以可知三元哈夫曼编码不需要增加零概率项。由哈夫曼编码的性质可知其码字空间大小 $|\mathcal{X}| = 1 + k(D-1)$，因此可知码字空间大小一定为奇数（$(3-1)k + 1 = 2k + 1$ 一定是奇数）"。

4. 哈夫曼编码。例：根据给定的信源概率分布进行哈夫曼编码。

   - 掌握哈夫曼编码的基本方法。
   - 掌握哈夫曼编码的性质 $|\mathcal{X}| = 1 + k(D-1)$。
   - 首先检查是否需要增加零概率项，然后再进行概率合并过程。
   - 若题目要求给出两种编码方案，具有相同的平均码长和不同的方差，其产生方法是，在概率合并的时候改变相同概率项合并的顺序。
   - 若题目增加约束。不要慌，认真分析一下约束到底是什么含义。例如，要求三元哈夫曼编码的第一位可以从 3 个字母中选取，后续编码只能从其中的两个字母中选取，这也就是要求我们先进行二元哈夫曼编码，对最后 3 个待合并的概率项进行三元哈夫曼编码。

5. Shannon-Fano-Elias 编码及其相关的前缀码证明方法。例：作业 5.28。

   - 掌握 Shannon-Fano-Elias 编码的基本方法。
   - 掌握 Shannon-Fano-Elias 编码中证明前缀码的方法（码字空间不重叠）。

3.5 第七章 信道容量

这一章一般会是一道大题（考察给定信道的信道容量计算），偶尔会出现一道小题比如判断题（考察对信道容量的理解，例如某一年一道判断题问"达到信道容量的输入概率分布是唯一的"）。

1. 信道容量计算。例：给定信道转移概率矩阵，计算信道容量。

    - 一般情况下会直接给出信道的数学描述（转移概率图或者矩阵），但也有时候会以应用题形式考察。遇到应用题不要慌，关键是从中抽象出信道概率模型，具体地，首先确定输入字母表，接着确定输出字母表，最后确定他们之间的对应关系。
    - 信道容量的一般求解方法见《信息论学习指导》。
    - 弱对称信道是常用模型，相关结论建议记住。

2. 并联信道的信道容量。例：作业 7.32。

    - 关于并联信道的信道容量的结论在《信息论学习指导》中有讲解。如果考试的时候担心不能直接用，可以根据《学习指导》中的推导过程进行简化，省略中间求解过程，“经过计算得到，并联信道的信道容量满足”后面写上结论，然后就可以用了。

3.6 第八章 微分熵

这一章一般会有一道选择题（和第二章一起组成一道选择），一道判断题（考察性质，往往是和离散情形不同的结论），一道大题（给定概率密度函数计算微分熵）。

1. 和第二章类似，信息量的定义、性质和链式法则等。

    - 定义、性质、链式法则等请参考《信息论学习指导》。
    - 注意，这一块容易和正态分布的性质结合考察，建议读者熟练掌握正态分布常用性质。

2. 连续情形下的渐进均分性定理和典型集。

    - 掌握基本概念和定义即可。

3. 不同约束下最大微分熵对应的分布。

    - 相关结论见《信息论学习指导》。

3.7 第九章 高斯信道

这一章主要是一道填空题（考察带宽有限信道的结论或者并联高斯信道注水法）和一道大题（和填空题考察的内容互补）。

1. 高斯信道的信道容量计算及其变形。例：计算在同时给定功率约束和均值约束条件下的信道容量。

    - 掌握典型高斯信道的信道容量计算方法，详见《信息论学习指导》。
    - 针对不同的约束，例如把输入功率约束变成输出功率约束，或者在输入功率约束基础上增加均值约束（这种就要考虑均值约束的影响，其实简单来说就是均值非零的时候方差和功率不再相等）。

2. 并联高斯信道注水法。例：给出独立并联高斯信道各个子信道噪声方差，求解总信道容量。

    - 理解并掌握注水法，详见《信息论学习指导》。
    - 其中一种常见的问法是，并联高斯信道中输入功率约束为何值时，该信道不再像一个信道而开始像一对信道。这类问法，本质上还是考察对注水法本身的理解。

3. 带宽有限信道。例：给出带宽限制和信噪比，计算信道容量。

    - 记住结论 $C = W\log\left(1+\frac{P}{N_0W}\right)$ 比特/ 秒，注意单位。
    - 无限带宽下 $C \to W \cdot \frac{P}{N_0W} \cdot \log_2 e = \frac{P}{N_0}\log_2 e$ 比特/ 秒。
    - 注意信噪比的概念，填空题可能出现，详见《信息论学习指导》。

4. 反馈的影响。

    - 了解无记忆噪声不会影响，有记忆噪声会产生影响，其中两个约束的结论可以记住。

3.8 第十章 率失真理论

这一章是这门课最难的部分，考察往往是作业题直接改编。这一部分可能会考察一道填空题（考察带失真的信源信道分离定理 $C > R(D)$），以及一道大题（常见是率失真函数计算，偶尔会考察信息价值计算）。

1. 率失真理论研究内容的理解。

    - 作者在答疑的时候也反复强调过，建议理解一下这一章到底在研究什么事情。为什么会考虑允许失真这件事情？对于连续情形，这个比较容易接受，毕竟用离散量编码连续量不可避免存在失真，但是如果离散信源为什么还要讨论率失真呢？这个问题可以结合带失真的信源信道分离定理一起理解，或者说，建议读者在学到这一章的时候能建立一个完整的从发送方发送的消息作为起

点出发到接收方接收消息的模型。虽然不会直接考，但是理解这个问题有助于这一章的解题。

2. 率失真函数计算的理解。例：给定信源分布和失真度量，假设在再生字母表中增加一个元素，证明率失真函数不会增加。
   - 率失真函数计算有两个要素，一个是信源分布，一个是失真度量，二者缺一不可。
   - 通过《信息论学习指导》中介绍的几种常见模型，来理解不同信源分布在常见失真度量下的处理技巧。
   - 失真度量线性变换对率失真函数的影响的结论的推导过程可以了解一下，详见《信息论学习指导》。
3. 率失真函数计算。例：二维信源由两个独立且已知分布的伯努利信源组成，每个信源的失真度量都是汉明失真，失真限制是总的失真限制，求二维信源的率失真函数。
   - 详见《信息论学习指导》。
4. 从信息的价值理解率失真。
   - 详见《信息论学习指导》。

专题复习计划

4.1 第一关

1. 选择题。

(a) 设 X, Y, Z 为离散随机变量，则以下不等式正确的是 (　)

$$
\begin{aligned}
&(A) H(Y \mid X = x) \leqslant H(Y)\\
&(B) I(X, Y) \geqslant I(X, Y \mid Z)\\
&(C) H(X) < H(2X)\\
&(D) I(X, Y; Z) \geqslant (X; Z) + I(Y; Z)
\end{aligned}
$$

(b) 设 X, Y, Z 均为离散随机变量, 则以下等式或不等式成立的是 (　)

$$
\begin{aligned}
&(A) H(X + Y) \geqslant H(X)\\
&(B) H(X \mid Y) = H(Y \mid X)\\
&(C) H(g(X)) \leqslant H(X)\\
&(D) H(f(X) \mid g(X)) = 0
\end{aligned}
$$

(c) 以下编码不可能是二元哈夫曼编码的是 (　)

$$
\begin{aligned}
&(A) \{0, 10, 11\}\\
&(B) \{00, 01, 10, 110\}\\
&(C) \{01, 10\}\\
&(D) \{1, 01, 10\}
\end{aligned}
$$

(d) 以下 D 元字母表上的码字长度符合即时码要求的是 ( )

$$(A)D=2, l_i=1,2,3,3,3$$
$$(B)D=3, l_i=1,2,2,2,3,3,3,3$$
$$(C)D=4, l_i=1,1,1,2,2,3,3,3,4,4$$
$$(D)D=5, l_i=1,1,2,2,3,3,4,4$$

2. 填空题。

(a) 有三个伯努利分布的离散随机变量 X, Y, Z, 若要使得 $I(X;Y)=0$ 比特,$I(X;Y\mid Z)=1$ 比特, 则 X, Y, Z 的联合概率分布为__________________。

(b) 设 $\{X_n\}$ 为平稳的马尔可夫链。则存在 $k=$ ______________ 满足

$$H\left(X_{-n} \mid X_0, X_1\right)=H\left(X_k \mid X_0, X_1\right) \quad (n>1)$$

(c) 设 X 是 $\{0,1,2\}$ 上均匀分布的随机变量，随机变量 Y 的字母表为 $\{0,1\}$。互信息 $I(X;Y)$ 的最大值为_________ 。

(d) 已知信源概率分布 $p=\left(\frac{1}{100}, \frac{1}{100}, \ldots, \frac{1}{100}\right)$，则其最优二元编码的期望长度为_________ 。

3. 判断题。

(a) 存在两个互不相同的概率分布 p, q 使得 $D(p\|q)=D(q\|p)$。

(b) 考虑平稳随机过程 $X_1, X_2, \cdots, X_n$ 。对某个函数 ϕ, 定义 $Y_1, Y_2, \cdots, Y_n$ 为 $Y_i=\phi\left(X_i\right), i=1,2, \cdots$。则有

$$H(\mathcal{Y}) \leqslant H(\mathcal{X})$$

(c) 对平稳随机过程 $X_1, X_2, \cdots, X_n$, 有

$$\frac{H\left(X_1, X_2, \cdots, X_n\right)}{n} \leqslant \frac{H\left(X_1, X_2, \cdots, X_{n-1}\right)}{n-1}$$

(d) 设随机变量 X 的字母表为 $\{0,1,2\}$，对应的概率为 $(0.6,0.3,0.1)$，则使得 D 元字母表上的香农码为最优码的最小整数 D 不小于 9。

(e) 对于离散无记忆信道, 达到信道容量时的输入概率分布 $p(X)$ 是唯一的。

(f) 添加一行到信道转移矩阵不会降低容量。

(g) 设信道 1 的转移概率矩阵为

$$p(y \mid x)=\left[\begin{array}{cc}1-p & p \\ p & 1-p\end{array}\right]$$

其信道容量记为 C_1，信道 2 的转移概率矩阵为

$$p(y \mid x) = \begin{bmatrix} 1-q & q & 0 \\ 0 & q & 1-q \end{bmatrix}$$

其信道容量记为 C_2，信道 3 的转移概率矩阵为

$$p(y \mid x) = \begin{bmatrix} 1-p & p & 0 & 0 & 0 \\ p & 1-p & 0 & 0 & 0 \\ 0 & 0 & 1-q & q & 0 \\ 0 & 0 & 0 & q & 1-q \end{bmatrix}$$

其信道容量记为 C_3。则有 $C_3 \geqslant C_1 + C_2$。

4. 随机变量 X_1、X_2、X_3、X_4 构成了马尔科夫链 $X_1 \to X_2 \to X_3 \to X_4$. 证明：

$$I\left(X_1;X_3\right)+I\left(X_2;X_4\right)\leqslant I\left(X_1;X_4\right)+I\left(X_2;X_3\right)$$

5. 设 $\{X_i, i=1,2,\cdots\}$ 为时间不变的马尔可夫链，初始状态的概率分布为 $P(X_1=1)=0.33$，$P(X_1=2)=0.46$，$P(X_1=3)=0.21$. 转移概率矩阵为

$$P=\begin{bmatrix} 5/12 & 1/4 & 1/3 \\ 1/4 & 7/12 & 1/6 \\ 1/2 & 1/2 & 0 \end{bmatrix}$$

请计算：

(a) 联合熵 $H(X_1, X_2, X_3)$。

(b) 马尔可夫链的熵率。

6. 设一离散信源只能产生“黑色”和“白色”两种消息，“黑色”出现的初始概率 p(黑色)=0.7，白色出现的初始概率是 p(白色)=0.3。

   (a) 假设消息出现前后没有关联，求该信源的熵率。

   (b) 假设消息出现前后有关联，其依赖关系为 p(白 | 白)=0.7，p(黑 | 白)=0.3，p(白 | 黑)=0.2，p(黑 | 黑)=0.8。求该信源的熵率。

   (c) 求当信源进入平稳状态后，以上两个信源的平均冗余度。

7. 设离散信源的概率分布为

$$\begin{bmatrix} S \\ P(S) \end{bmatrix} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 \\ 0.3 & 0.3 & 0.1 & 0.1 & 0.05 & 0.05 & 0.05 & 0.05 \end{bmatrix}$$

请给出该信源的三元哈夫曼编码，并计算平均码长。要求给出两种编码方案，平均码长相同，但码长方差不同。

8. 已知某信道的转移概率矩阵为

$$p(y \mid x) = \begin{bmatrix} 1-p & p & 0 & 0 \\ p & 1-p & 0 & 0 \\ 0 & 0 & 1-\varepsilon & \varepsilon \\ 0 & 0 & \varepsilon & 1-\varepsilon \end{bmatrix}$$

试求解其信道容量。

9. 胶片是由碘酸银晶体按照泊松分布组成，每平方英寸的粒子密度 λ 已知。在不知道碘化银粒子位置的情况下对该胶片随机地进行光照。当碘酸银粒子感光 (接受光照) 后，其所在的区域被点亮，没有碘酸银粒子的区域和有碘酸银粒子但没有感光的区域未被点亮。我们做如下的假设，将胶片的区域划分为若干小格子，大小为 dA。假设每个格子中至多一个碘酸银粒子并且不在格子的边界上。于是，胶片可以看作是一系列具有交叉概率 $1-\lambda dA$ 的并联二元非对称信道。通过必要的近似，计算该胶片的信道容量 (量纲为比特/平方英寸)。

10. 离散信源 X 发出消息经过有噪声信道输出为 Y，且 $Y = X + Z \pmod 2$，其中 Z 为干扰噪声，X 和 Z 相互独立，取值空间为 $\{0,1\}$，$p(X=0)=\omega$，$p(Z=0)=\varepsilon$。发送方功率受限，有 $E(X^2) \leqslant 1/2$；干扰方功率也受限，有 $E(Z^2) \leqslant 1/4$。

    (a) 求平均互信息 $I(X;Y)$。

    (b) 当信道噪声分布给定时，求使得 $I(X;Y)$ 最大的信源 X 分布。

    (c) 当信源分布给定时，求使得 $I(X;Y)$ 最小的信道噪声 Z 分布。

4.2 第二关

1. 填空题。

   (a) 由四个子信道构成的独立并联高斯信道的各子信道的噪声方差分另为 1,3,6,9, 总功率限制为 $P=8$, 则总信道容量为 C=______________ 。

   (b) 设一带宽有限信道的带宽为 5kHZ ，信噪比 (P/N_0W) 为 10 dB, 则该信道的信道容量为 C=______________ 。

2. 判断题。

   (a) 对任意连续随机变量 X 和 $a \neq 1, h(aX) \neq h(X)$ 。

   (b) 反馈不会对信道容量产生影响。

   (c) 高斯信源采用失真度量 $d(u,v)=|u-v|$，其率失真函数为

$$R(D)=\begin{cases} \frac{1}{2}\log\frac{\sigma^2}{D}, & 0 \leqslant D \leqslant \sigma^2, \\ 0, & D > \sigma^2. \end{cases}$$

   (d) 完善保密性的条件是 $I(K;E)=H(E)-H(M \mid E)$，其中 M,K,E 分别表示明文、密钥和密文。

3. 给定两个连续随机变量 X 和 Y，它们的联合概率密度函数为

$$f(x,y)=\frac{1}{2\pi\sigma_x\sigma_y}\exp\left[-\frac{(x-m_x)^2}{2\sigma_x^2}-\frac{(y-m_y)^2}{2\sigma_y^2}\right],-\infty<x,y<\infty$$

设 $U=X+Y$，$V=X-Y$. 请计算 $h(U)$，$h(V\mid U)$，$D(U\|V)$，$I(U;V)$.

4. 假设有一无记忆加性指数噪声信道，输入随机变量 X 是非负的，输出为 $Y = X + Z$ ，其中随机变量 Z 为独立于输入的指数分布噪声

$$f(Z) = \frac{1}{\mu}\exp(-z/\mu)$$

如果对信道输入的均值进行限制，即 $E[X] \leqslant \lambda$，求该信道的信道容量。

5. 已知信道的带宽为 5kHz。试求：

(1) 接收端信噪比 P/N 为 30dB 时候的信道容量。

(2) 若要求该信道能够传输 20kb/s 的数据，则接收端最小的信噪比应该为多少。

6. 一个三维独立并联高斯信源 (X_1, X_2, X_3)，其中 X_1，X_2，X_3 均值都为零，方差分别是 2、8 和 4. 采用平方误差失真度量，$D = \sum_{i=1}^{3} D_i = \sum_{i=1}^{3} (x_i - \hat{x}_i)^2$，求该信源的信息率失真函数 $R(D)$。

7. 设有一个均匀分布的离散无记忆信源的失真度量矩阵如下，求解其率失真函数。

$$d(x,\hat{x}) = \begin{bmatrix} 0 & \infty & \infty & 1 \\ \infty & 0 & \infty & 1 \\ \infty & \infty & 0 & 1 \end{bmatrix}$$

8. 设有一个离散无记忆信源 X，概率分布为 $p(X=0)=p(X=1)=2/5, p(X=2)=1/5$，失真度量采用汉明失真，求解其率失真函数。

$$d(x,\hat{x})=\begin{cases}0, \text{ 如果} x=\hat{x}\\ 1, \text{ 如果} x\neq\hat{x}\end{cases}$$

9. 设 $X \sim \mathcal{N}(0,\sigma^2)$, 失真度量为平方误差。不允许分组描述。试证明: 1 比特量化的最佳再生点为 $\pm\sqrt{\frac{2}{\pi}}\sigma$, 且 1 比特量化的期望失真为 $\frac{\pi-2}{\pi}\sigma^2$ 。将此与 $R=1$ 时的失真率上界 $D=\sigma^2 2^{-2R}$ 作比较。

模拟试卷

1. (每题 4 分，共 8 分) 选择题 (多选题)

   (a) 设 X, Y, Z 均为离散随机变量，U, V 为连续随机变量，则以下等式或不等式成立的是 (　)

   $$(A) H(X,Y,Z) \leqslant H(X,Z) + H(Y \mid X) - I(Z;Y)$$
   $$(B) h(U,V) = h(U+V, U-V)$$
   $$(C) h(f(U)) \leqslant h(U)$$
   $$(D) H(X,Y) \geqslant H(X+2Y, 2X-Y)$$

   (b) 以下编码不可能是二元哈夫曼编码的是 (　)

   $$(A)\{0, 10, 11\}$$
   $$(B)\{00, 01, 10, 110\}$$
   $$(C)\{1, 01, 10\}$$
   $$(D)\{001, 010, 011\}$$

2. (每题 4 分，共 8 分) 判断题 (若判断为对，简要说明或证明；若判断为错，简要说明或举出反例)

   (a) 设 X, Y 均为离散随机变量，则有 $H(X+Y) \leqslant H(X) + H(Y)$，且当两个随机变量都只有 2 个可能取值的时候，上述不等式是紧致的.

   (b) 设一离散信源 X 概率分布为 $\{p_1, p_2, p_3, \ldots, p_n\}$，且 $p_1 > p_2$. 考虑另一离散信源 Y，概率分布为 $\{p_1', p_2', p_3, \ldots, p_n\}$，其中 $p_1' = p_1 - \varepsilon$，$p_2' = p_2 + \varepsilon$，$0 < 2\varepsilon \leqslant p_1 - p_2$. 则有 $H(Y) \geqslant H(X)$.

3. (每题 4 分，共 12 分) 填空题

(a) 有三个服从伯努利分布的离散随机变量 X, Y, Z, 若要使得 $I(X;Y) = 1$ 比特，$I(X;Y \mid Z) = 1$ 比特，则 X, Y, Z 的联合概率分布为__________________ .

(b) 设一随机变量 X 有四个可能取值，对应概率分布 $\{p_1, p_2, p_3, p_4\}$，且 $p_1 \geqslant p_2 \geqslant p_3 \geqslant p_4$. 若该信源的二元哈夫曼编码为 (0,10,110,111)，则概率分布 $\{p_1, p_2, p_3, p_4\}$ 应满足的必要条件是__________________ .

(c) 有一伯努利分布的信源 X，$p(X=0) = 1/3$，该信源每 2 秒发出 3 个符号，通过一个错误概率 $\varepsilon < 0.5$ 的二元对称信道进行传输，信道每秒使用 2 次. 假设该信源能在允许失真 D 的前提下在该信道中进行传输，则失真 D 要满足的条件是：__________________ .

4. (10 分) 设 X, Y 均为二元离散随机变量，且 $p(X=0, Y=0) = p(X=1, Y=1) = p(X=0, Y=1) = \dfrac{1}{3}$. 求：

(a) $H(X), H(Y), H(X \mid Y), I(X+Y; X-Y)$；

(b) 若 X, Y, Z 均服从参数 1/2 的伯努利分布,且满足 $I(X;Y) = I(X;Z) = I(Y;Z) = 0$，试求解 $H(X, Y, Z)$ 的最小值.

5. (10 分) 设 $\{X_i, i = 1, 2, \cdots\}$ 为时间不变的马尔可夫链，初始状态的概率分布为 $P(X_1 = 1) = 0.5$，$P(X_1 = 2) = 0.25$，$P(X_1 = 3) = 0.25$. 转移概率矩阵为

$$P = \begin{bmatrix} 1/3 & 1/3 & 1/3 \\ 2/3 & 0 & 1/3 \\ 2/3 & 1/3 & 0 \end{bmatrix}$$

请计算：

(a) 联合熵 $H(X_1, X_2, X_3)$.

(b) 马尔可夫链的熵率.

6.（12 分）设离散信源的概率分布为

$$\begin{bmatrix} S \\ P(S) \end{bmatrix} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 \\ 0.24 & 0.12 & 0.03 & 0.06 & 0.4 & 0.06 & 0.03 & 0.06 \end{bmatrix}$$

(a) 请给出该信源的三元哈夫曼编码并计算平均码长（要求给出两种编码方案，平均码长相同，但码长方差不同. ）;

(b) 假设我们对该信源的三元编码增加一个约束，要求信源编码输出码字的第一位可以从 $\{0,1,2\}$ 中选取，但后续位数都只能从 $\{0,1\}$ 中选取，例如 210,011 是合法码字，12,002 是非法码字. 请给出在这个约束下该信源的三元最优编码.

(c) 若有另一离散信源 X，该信源有一个三元前缀码满足平均码长

$$\bar{L} = \frac{H(X)}{\log 3} = H_3(X)$$

请证明该信源的取值空间大小和 S 的大小一定不同.

7. (10 分) 一名间谍按下述方式与他的联系人通信：每个小时，该间谍要么不打电话，要么打电话并只允许电话响一定的次数 (不多于 N 次). 他的联系人不接听电话，只记录电话是否响起，以及响起次数. 由于电话系统的不足，每次打电话，电话正常连通的概率为 $p(0<p<1)$，且在不同通话中是独立的. 由于联系人不接听电话，间谍并不知道哪个电话正常连通了. 设该间谍打电话的概率为 q，请计算该通信系统的信道容量 (写成 p 和 q 的函数).

8. (10 分) 设有连续随机变量 X, Y, Z，其中 X 的概率密度函数为 $f(x)=\frac{1}{2}\lambda e^{-\lambda|x|}$，$Y, Z$ 的联合概率密度函数为

$$f(y,z)=\frac{1}{2\pi\sigma_y\sigma_z}\exp\left[-\frac{(y-m_y)^2}{2\sigma_y^2}-\frac{(z-m_z)^2}{2\sigma_z^2}\right], -\infty<y,z<\infty$$

(a) 计算 $h(X), h(Y), h(Z \mid Y), h(Y+Z)$；

(b) $U=Y+Z$，$V=Y-Z$. 请计算 $I(U;V)$.

9. (10 分) 设随机变量 X 服从区间 $[-1/2, 1/2]$ 上的均匀分布，信道为加性噪声信道 $Y = X + Z$，噪声 Z 服从区间 $[-a/2, a/2]$ 上的均匀分布.

   (a) 求 $I(X;Y)$.

   (b) $a = 1$ 时，X 取值限制在区间 $[-1/2, 1/2]$ 内，求信道容量. 并说明达到信道容量时的输入概率分布.

10. (10 分) 考虑在集合 $\{1, 2, \ldots, N\}$ 上均匀分布的信源 X. 若失真度量为汉明失真，即

$$d(x, \hat{x}) = \begin{cases} 0, & \text{如果} x = \hat{x} \\ 1, & \text{如果} x \neq \hat{x} \end{cases}$$

求信源的率失真函数 $R(D)$. 现假设我们在 $\hat{\mathcal{X}}$ 中增加一个新的元素 $\hat{x}_0$，真函数 $\tilde{R}(D)$ 必然不大于原来的率失真函数，即 $\tilde{R}(D) \leqslant R(D)$.

后记

这个学期也许是作者最后一次担任信息论课程的助教了。在过去的几年里，有三次担任信息论课程助教，在整个过程中积累的经验都凝结在本书和《信息论学习指导》中，希望能够给信息安全专业的教学工作做一些贡献，也希望能够吸引一些有能力的学弟学妹一起加入助教团队，一起丰富课程的教学资源并提升课程质量。

不得不承认，在 2023 年春季学期的助教工作中有一些失望。基础问题、能力问题、态度问题，以及最难以接受的人品问题。基础问题主要体现在概率论课程上，这是信息论课程最重要的数学基础，但是从答疑情况来看，近年来班级同学的平均水平呈现一定的下降趋势，作者有思考过解决方案，比如在课程初发布一些学习材料并提醒同学们抽空补足一下，但效果并不理想，这个问题希望读者能够给出一些建议，以帮助以后学习该课程的同学们。关于学习能力问题，作者希望能通过“信息论解题模型”等方式作为辅助，引导同学们去提升学习能力。态度问题主要是在作业和答疑过程中，在课程 QQ 群中经常遇到一些同学不愿意自主思考，即使给了提示也不愿意，只希望助教能够把答案直接讲出来。至于人品问题，我很认同老师的一句话，该着急的应该是学生的父母，而非老师。

除此以外，对助教管理体制以及改革也很失望。对于助教来说，激励体制很朴素，但也存在一些令人疑惑的地方。激励体制的用意应该是鼓励更多助教提高工作的质量，以辅助提升课程教学质量。但目前看来，其评价体制也许存在一些不合理的地方。例如，如何解决课程本身的难易程度对同学们主观评价的影响，一些评价指标例如随堂率是否是必要的，以及是否可以改善评价方式，比如给出一些高分或者低分的时候需要提供一些文字性的理由描述。作者曾经在 2020 年获得过两次“优秀助教”荣誉称号，提出上述反馈并不只是因为某一次没有获得，而是希望能够有更完善的激励体制，以期吸引更多优秀的助教能够加入助教团队。助教管理团队也许也有其难处，但还是希望在未来，能够有一些改善。

虽然有失望，但回望过去，这一路走来，还是快乐更多一些。最美的回忆留在了 2020 年的春天，感谢和你们的相遇。山海自有归期，风雨自有相逢。期待重逢时繁花似锦，期待我们都有好故事有可以说。

也感谢一路走来其他美好的遇见，编写这些教材一方面是你们给的动力，也有你们给的素材。啰嗦了很多，就先这样结尾吧。另外，由于作者能力有限，难免会存在一些疏漏。如果有错误指正等，欢迎和作者联系，同时也欢迎交个朋友。QQ：2209823112。