信息论

信号传输与处理的理论基础

Shannon信道编码定理(7.7节);

卷积编码和现代编码简介（补充内容）

Shannon定理（1）

* 定理的陈述(Shannon, 1948)
*
* 对一个容量为C的BSC信道，对任何实数0<R<C,都存在一族
* 传输效率k/n=R的(n,k)分组编码方案，使得该组方案的译码
* 差错概率满足 $\lim_{n\to\infty} P_e(n) = 0$.
* 反之，如果一族(n,k)分组编码方案的译码差错概率满足
* $\lim_{n\to\infty} P_e(n) = 0$，那么其传输效率k/n均满足k/n ≦C。

* Shannon定理表明，通过分组冗余编码，可以在BSC信道上（随着码字
* 越来越长）以任意低的差错概率传输信息，条件是每单位比特的传输效率
* k/n不高于信道容量C所界定的极限。
* 在其他类型的复杂信道上，也存在相应的Shannon定理。既然容量C是各种信道上实现可靠通信所伴随的传输效率的极限，因此各类信道上的容量公式就具有格外重要的意义。

Shannon定理（2）

* Shannon定理的证明要点 (详见教程对定理7.7.1的证明)

* 分组编码方案（随机编码）
* 对给定的传输效率R<C，令$k = [nR]$。
* 任取二元随机变量x∈{0,1}的概率分布$p(x)$，以概率分布$p(\mathbf{x})=p(x_1)\ldots p(x_n)$
* 随机生成一组2^k个n位码字$\mathbf{x}=(x_1,\ldots,x_n)$。
* 这些2^k个n位码字的集合记为CW，每个原始的k位信息按任意的方式
* 一一对应地指派到CW中的各个码字。

* 码字传输
* 设BSC信道的差错概率为p(y|x)，则码字$\mathbf{x}=(x_1,\ldots,x_n)$传输到达接收端得到
* 接受分组$\mathbf{y}=(y_1,\ldots,y_n)$的概率
* $$P[\mathbf{y}\,|\mathbf{x}] = p(y_1|x_1)\ldots p(y_n|x_n)$$

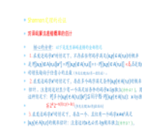
Shannon定理（3）

* Shannon定理的证明要点（详见教程对定理7.7.1的证明）

* 译码方案（随机算法）
* 设$A(n,\varepsilon)$是各码字$(x_1,\ldots,x_n)$和各接受分组$(y_1,\ldots,y_n)$的联合典型集合(7.6节)。
* 对接受分组$\mathbf{y}=(y_1,\ldots,y_n)$，译码算法寻求这样的码字$\mathbf{x}=(x_1,\ldots,x_n)$，使得
* $$(\mathbf{x},\mathbf{y})\in A(n,\varepsilon)$$
* 如果存在且有唯一的码字**x**满足以上性质，则输出**x**所对应的k位原始
* 信息；
* 如果不存在任何码字满足以上条件、或存在多个码字满足以上条件，
* 则报告一个译码差错。

Shannon定理（4）

* Shannon定理的论证
* 对译码算法差错概率的估计
* 核心的分析：以下是发生译码差错的全部情况
* 1. 在发送码字$\mathbf{x}^0$的情况下，不存在任何码字满足$(\mathbf{x},\mathbf{y})\in A(n,\varepsilon)$的概率
* 是$P[(\mathbf{x},\mathbf{y})\notin A(n,\varepsilon)|\mathbf{x}^0] = P[(\mathbf{x},\mathbf{y})\notin A(n,\varepsilon)] = 1 - P[(\mathbf{x},\mathbf{y})\in A(n,\varepsilon)] < \delta$，$\delta$是随$n$
* 的增长趋向于任意小的正数（参见定理7.6.1第一款结论）。
* 2. 在发送码字$\mathbf{x}^0$的情况下，存在多个码字满足条件$(\mathbf{x},\mathbf{y})\in A(n,\varepsilon)$的概率
* 估计。注意到这时至少有一个满足该条件的码字$\mathbf{x}$与$\mathbf{y}$独立(为什么？)，因此这种情况下：$P[\text{多个}(\mathbf{x},\mathbf{y})\in A(n,\varepsilon)|\mathbf{x}^0] \leqq \text{码字数}\cdot P[(\mathbf{x},\mathbf{y})\in A(n,\varepsilon)\text{：}\mathbf{x}\text{与}\mathbf{y}\text{独立}]$
* $\leqq 2^k 2^{-n(I(x;y)-3\varepsilon)}$ (参见定理7.6.1第3款结论)
* 3. 在发送码字$\mathbf{x}^0$的情况下，存在一个、且仅有一个码字$\mathbf{x}\neq\mathbf{x}^0$满足
* $(\mathbf{x},\mathbf{y})\in A(n,\varepsilon)$的概率估计：注意这时$\mathbf{x}$也必然与$\mathbf{y}$概率独立(为什么？)，
* 因此该概率的上界同情况2相同。



Shannon定理（5）

* Shannon定理的论证
* 对译码算法差错概率的估计（续）
* 综合以上分析，在发送码字$\mathbf{x}^0$的情况下，发生译码差错的概率
* $P[\mathbf{x} \neq \mathbf{x}^0 | \mathbf{x}^0]$ 有上界
* $$P[\mathbf{x} \neq \mathbf{x}^0 | \mathbf{x}^0] < \delta + 2 \cdot 2^{-n(I(x;y)-3\varepsilon)+k} \qquad (i)$$
* 其中，第一项δ随n的增长趋向于零；
* 第二项中的$2^{-n(I(x;y)-3\varepsilon)+k}=2^{-n(I(x;y)-R-3\varepsilon)}$当$R<I(x;y)$时随n的增长
* 趋向于零；
* 因此，若$R<I(x;y)$，则有$\lim_{n\to\infty} P[\mathbf{x} \neq \mathbf{x}^0 | \mathbf{x}^0] = 0.$
*

Shannon定理（6）

* Shannon定理的论证

* 对各种分组编码方案的平均译码差错概率上界的估计（参见教程中定理7.7.1的论证）
* 平均差错概率$\overline{P_n}$有与式(i)相似的上界，因此若R<I(x;y)则有$\lim_{n\to\infty}\overline{P_n}=0.$
*
* 最后的结论
* 以上结论对码字的任何概率分布p(x)均成立，特别地，对使得I(x;y)
* 达到最大值的概率分布也成立，因此若R< C = $max_{p(x)}$I(x;y)则有$\lim_{n\to\infty}\overline{P_n}=0.$
* 因为$\lim_{n\to\infty}\overline{P_n}=0$，因此对每个$n$和每个任意小的正数$\mu$，均存在一个
* (n, k)分组编码方案，满足$k/n<$C且$P_e(n)<\mu$。

Shannon定理（7）

* 除7.11之外，7.8-7.13的内容不作要求；
* 7.11内容已扩展为线性分组码的通用译码算法及其性能分析（参见上一讲）。

* 第七章习题：
* 7.1、7.5、7.7、7.11、7.15(a)(b)(c)、7.18(a)、
* 7.20、7.25、7.28、7.34(a)。

* 注：以上习题可分两次提交，可自行划分批次。

* 下节课简介信道编码领域的某些代表性成果与进展，让大家了解信道编码作为信息论
* 也作为通信领域的主流分支之一，应用了哪些有意思的算法的思想，例如有限状态机模型、
* 图的最短路径算法和很多足有优化算法等，都是同学们已经学习过的知识，这些知识有着
* 非常丰富多彩的奇妙应用。

经典编码与现代编码(补充1)

* 线性分组码的补充：特殊的**线性分组码**

* **为什么要寻求特殊的线性分组码?**
* **为了寻求较之通用线性码更高的编码效率和译码速度。**

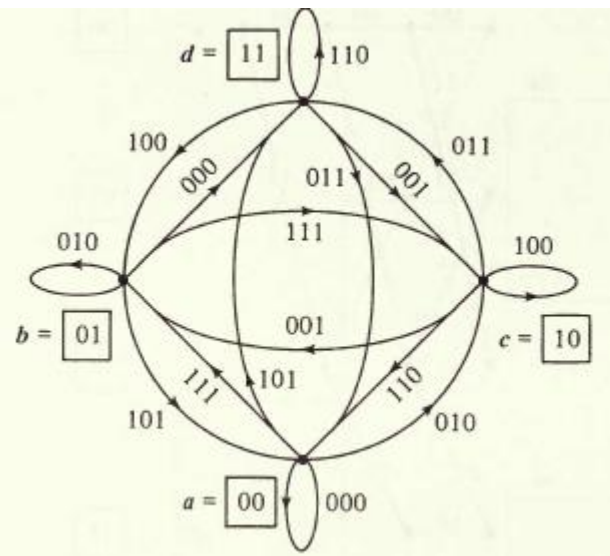
(1) 循环码(Cyclic Codes, Kasami, Omura)

* 编码矩阵G具有这样的性质：每行都是某行g的循环移位。
* 码字特点：每个码字经过特定位数的循环移位后仍然是
* 一个码字。
* 译码特点：基于循环移位寄存器电路高速译码。
* 设计工具：F_2上的素多项式及其相关的域扩张构造。
* (2) **Reed-Solomon码**
* 码字特点：每个码字都是某个代数多项式的零点循环式。
* 译码特点：基于扩域上的运算的高速译码。
* 设计工具：F_2上的特殊代数曲线。

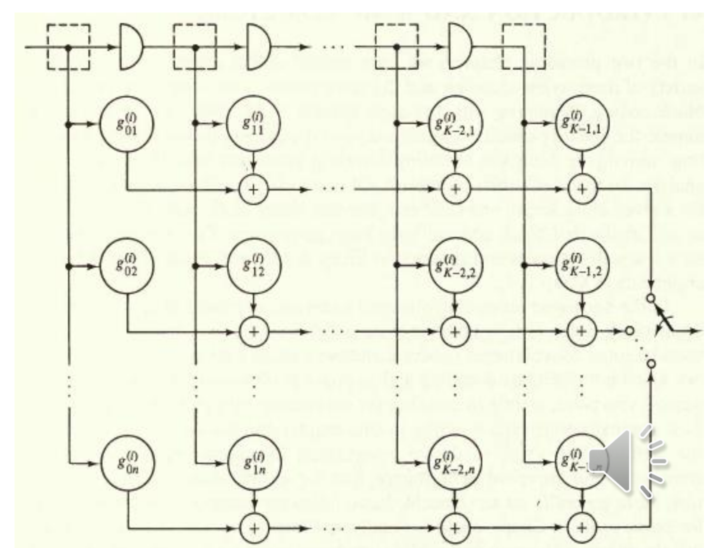
经典编码与现代编码(补充2)

* 卷积码简介（一）：**通用编码结构及状态图**

* (1) 原始信息流u(0)u(1)u(2)…..u(t)….卷积码是一个信息流
* x(0)x(1)x(2)…..x(t)….
* 每个码字x(t)和在其之前的一组原始信息u(t), u(t-1),…, u(t-L)有线性关系:
* $x(t) = G_0u(t)+G_1u(t-1)+\dots+G_Lu(t-L)$, G_j是卷积码的一组编码矩阵。
* (2) 卷积码的上述编码过程等价于一个有限状态机:



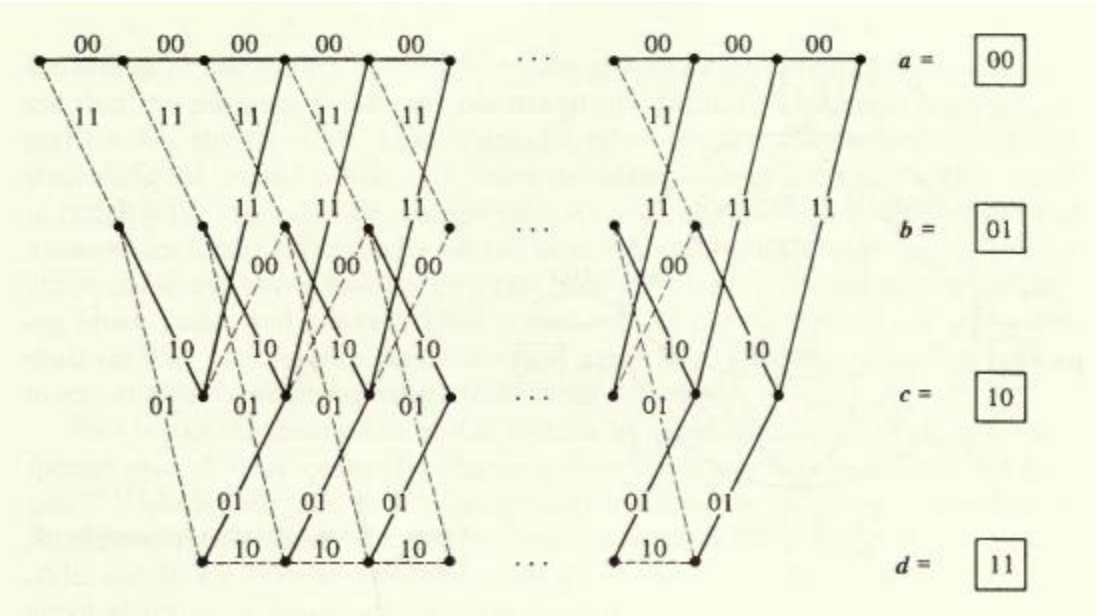
状态：缓存寄存器中的当前数字序列；
事件：原始信息流的u(t);
输出：码字当前分组x(t).



经典编码与现代编码(补充3)

* 卷积码简介（二）：**状态图的动态展开形式**

* (3) 将状态图延时间轴展开，得到卷积编码过程等效的篱笆图模型。
*
* 篱笆图上的每条路径代表一个码字流；
* 每条边上的标记是对应的原始信息分组。



经典编码与现代编码(补充4)

* 卷积码简介（三）： 卷积码的译码 (Viterbi算法)

* (4) 卷积码的译码问题
* 从含噪声的接受比特流**r**=r(0)r(1)r(2)....中求码字流$\hat{\boldsymbol{u}}$= $\widehat{u(0)}\widehat{u(1)}\widehat{u(2)}$...
* 使$\hat{\boldsymbol{u}}$对应的码字流$\hat{\boldsymbol{x}}$= $\widehat{x(0)}\widehat{x(1)}\widehat{x(2)}$... 同r之间的差错度量D($\hat{\boldsymbol{x}}$,r)最小。

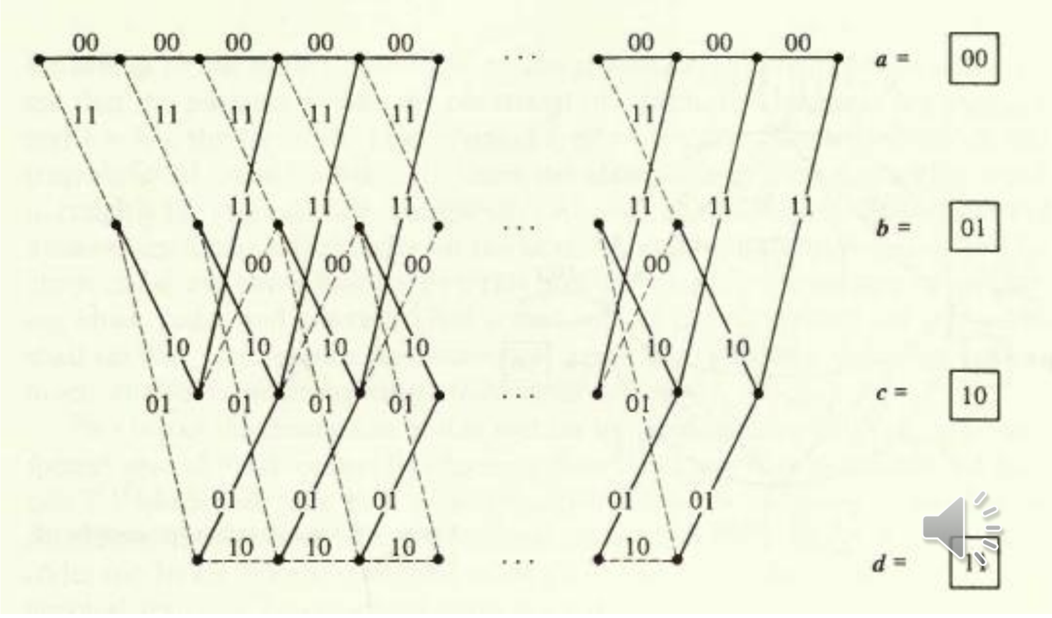
(5) 根据信道的噪声干扰结构将D($\hat{\boldsymbol{x}}$,r)表达为路径上的各边的度量d之和，

即D($\hat{\boldsymbol{x}}$,r)=$\sum_{t=0}^{L-1} d(x\widehat{(t)}, r(t))$

则卷积码的译码问题等价于

求篱笆图上的最短路径问题：

Viterbi算法的核心思想！



经典编码与现代编码(补充5)

* 级联码和Turbo码简介(1990_s -)

* (1) 级联码将多种类型的信道编码组合/嵌套，通常分为内码
* 和外码：
* 内码采用强纠错能力的编码方案，纠正大部分传输差错。
* 外码采用较弱纠错能力的编码方案，纠正剩余的传输错误。

(2) 特点：

内码的译码计算速度慢，纠错能力强；

* 外码的译码纠错能力弱，计算速度快。
* 级联码有能力纠正大批量的猝发错误、校正深度衰落信道上的传输差错。

传输效率接近Shannon容量。

(3) 例：

分组/分组级联码、分组/卷积级联码、Turbo码

经典编码与现代编码(补充6)

时空编码(2000 -)

* 针对多天线/多信道传输结构，同时在空间维和时间维上
* 构造冗余结构。
* 特点：充分利用MIMO信道的高容量特点，同时更灵活地控制
* 译码差错。

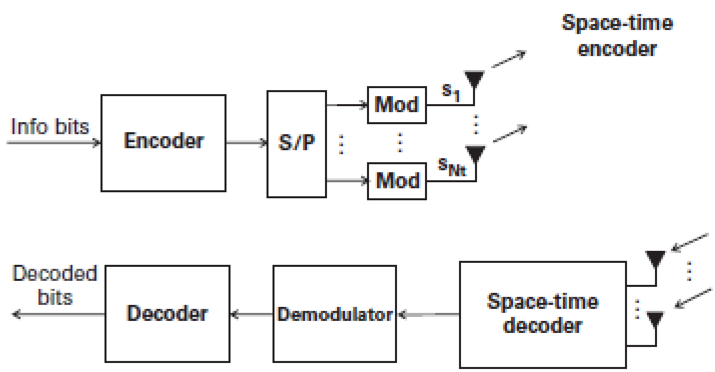


Figure 1.1 A MIMO system for *spatial diversity*.

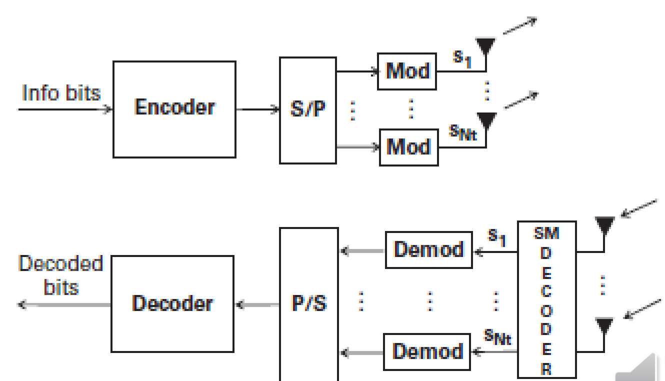


Figure 1.2 A MIMO system for *spatial multiplexing*.

经典编码与现代编码(补充7)

* 适应性编码(2000 -)

* 适应性编码方案有能力在线动态调整和选择最匹配于信道当前状态的编码算法和译码算法。
* 工作方式：
* (1) 接收机对信道状态和噪声特性作出估计。
* (2) 接收机将信道状态反馈会发射机。
* (3) 发射机根据信道当前状态生成近似匹配的编码方案
* 和工作参数，例如在低噪声情状态下提高传输速率、降低码字功率，
* 或者在高噪声/深度衰落状态下降低传输速率、提高码字功率。
* (4) 接收机对译码差错概率进行跟踪监测，向发射机反馈译码质量。
* (5) 发射机根据反馈状态持续调整编码算法和工作参数。

经典编码与现代编码(补充8)

* S.Lin, R.Costello