信道编码理论

刘景伟

jwliu@mail.xidian.edu.cn

2019年度

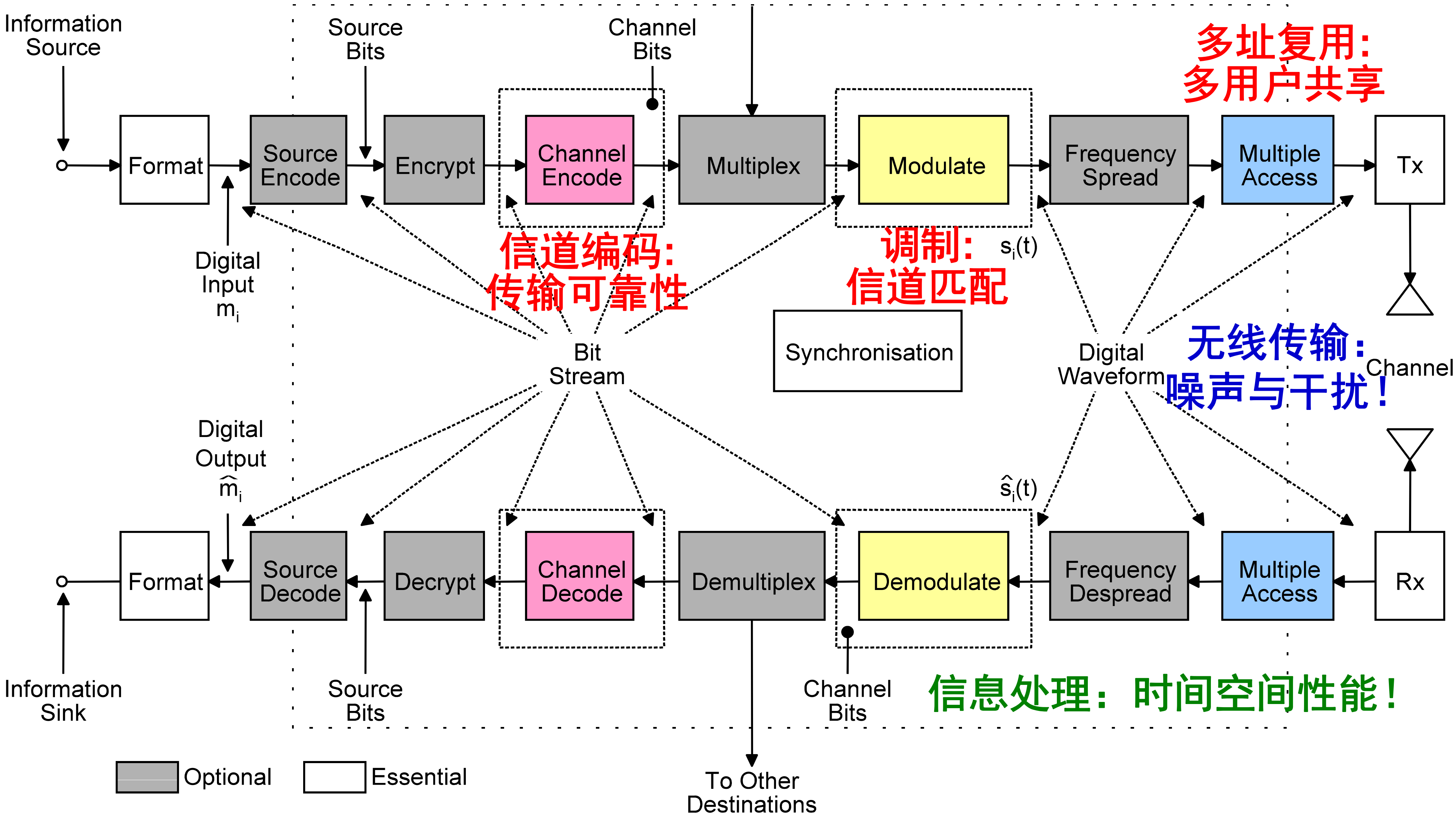
Lecture 1

基本概念

内容

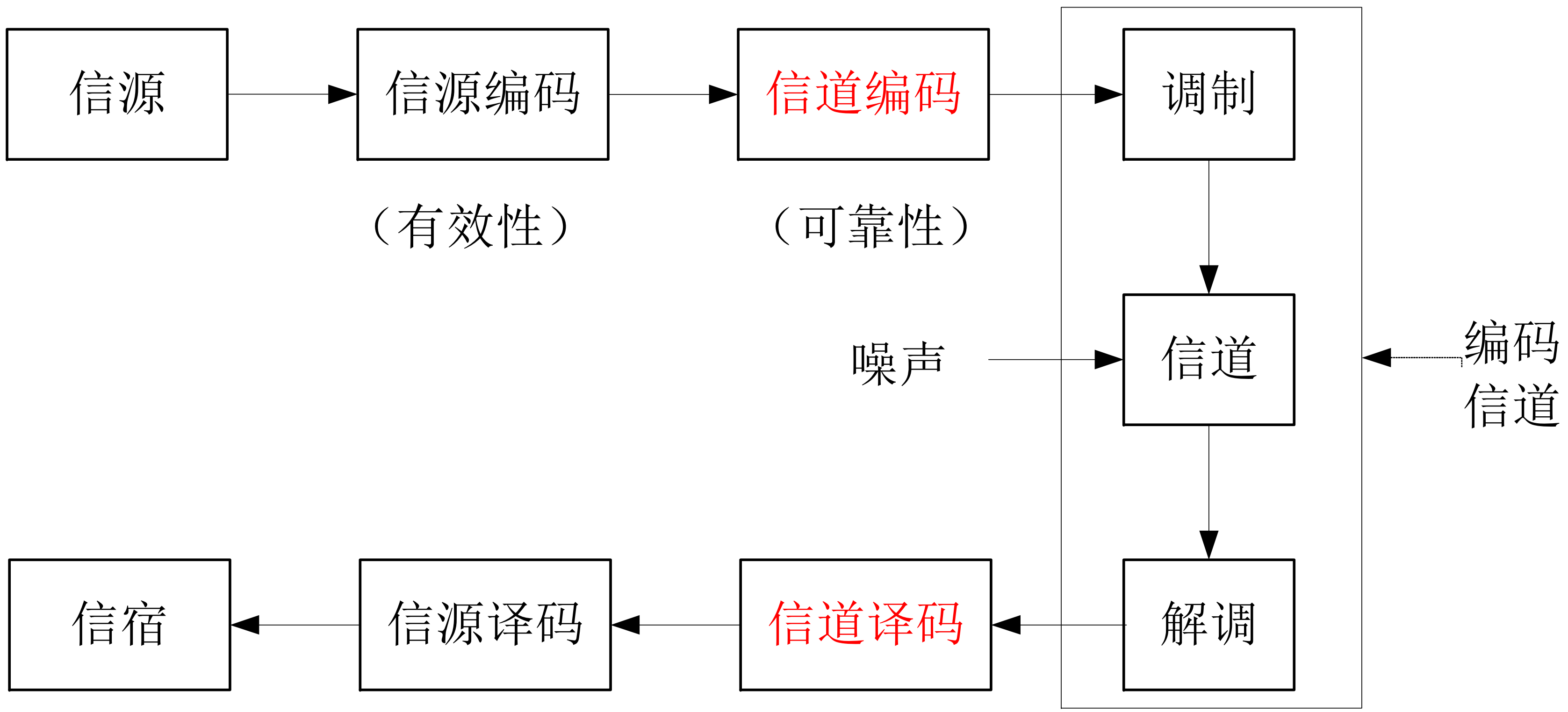
- 数字通信系统模型
- 信道模型与错误图样
- 纠错码的分类与发展历程
- 纠错码的基本原理
- 纠错码的纠错能力
- 纠错码的编码增益
- 基本译码方法
- 信道编码定理
- 信道容量

数字通信系统模型



Information Source
Source Bits
Channel Bits
多址复用：
多用户共享
Format
Source Encode
Encrypt
Channel Encode
Multiplex
Modulate
Frequency Spread
Multiple Access
Tx
Digital Input m_i
信道编码：
传输可靠性
调制：
信道匹配
$s_i(t)$
Bit Stream
Synchronisation
Digital Waveform
无线传输：
噪声与干扰！
Channel
Digital Output $\hat{m}_i$
$\hat{s}_i(t)$
Format
Source Decode
Decrypt
Channel Decode
Demultiplex
Demodulate
Frequency Despread
Multiple Access
Rx
Information Sink
Source Bits
Channel Bits
信息处理：时间空间性能！
Optional
Essential
To Other Destinations

数字通信系统模型



信道模型

离散输入连续输出信道

- 假定信道编码器的输出符号取自 $\boldsymbol{X}=\{x_0,x_1,\cdots,x_{q-1}\}$，译码器输入为连续值*Y*=*R*，我们称这类信道为离散输入连续输出信道，典型的有：二元输入高斯白噪声信道（BIAWGN）和二元拉普拉斯(Laplace)信道
- BIAWGN输入输出可表示为

$$Y=X+N$$

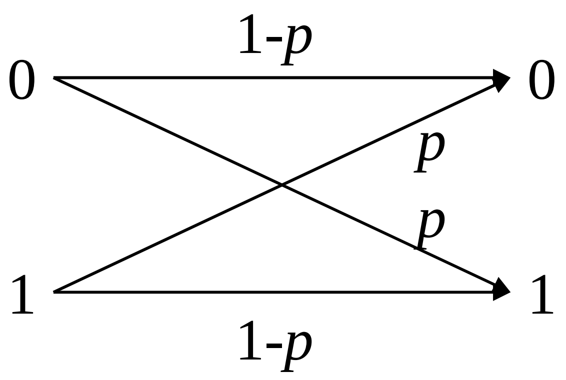
其中，*N*为加性高斯白噪声，其均值为零，方差为 σ^2 。给定一个输入 $X=x_k$，$k=0,1,\cdots,q-1$，则*Y*是均值为 x_k，方差为 σ^2 的高斯变量

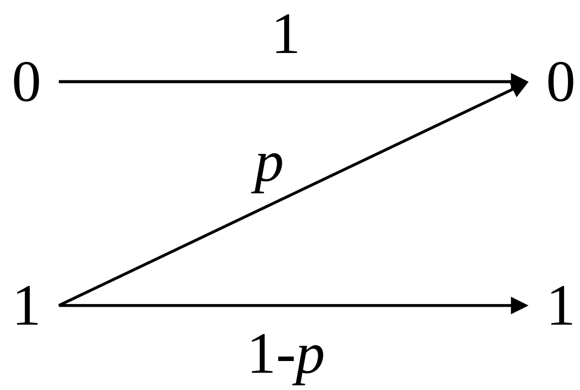
$$p(y\mid X=x_k)=\frac{1}{\sqrt{2\pi}\sigma}\exp\{-(y-x_k)/2\sigma^2\}$$

离散无记忆（随机）信道（DMC），有记忆（突发）信道，组合信道

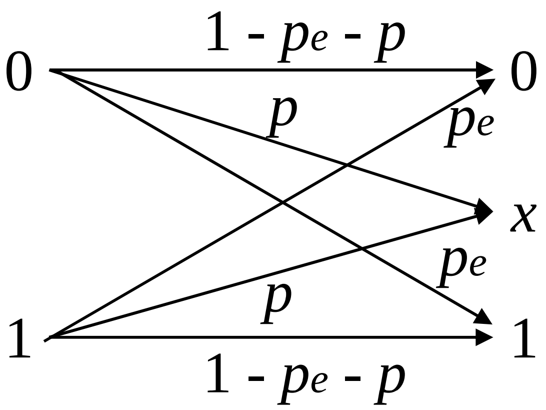
信道模型

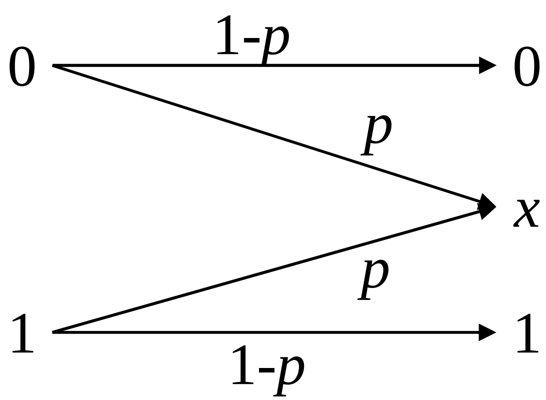
- 二进制对称信道(BSC)与Z信道





- 二进制删除信道（BEC）和二进制纯删除信道





错误类型

- 随机错误——随机错误信道：深空信道，卫星信道等
- 突发错误——突发错误信道：无线信道，电缆传输（开关脉冲噪声，串音），磁记录信道
- 混合错误——混合信道

错误图样

例子

- 发送序列C: (1111011000)
- 错误图样E: (1001001110)
- 接收序列R: (0110010110)
- R=C+E 或 E=C+R
- 突发图样: (100100111)；突发长度：9

二进制运算规则

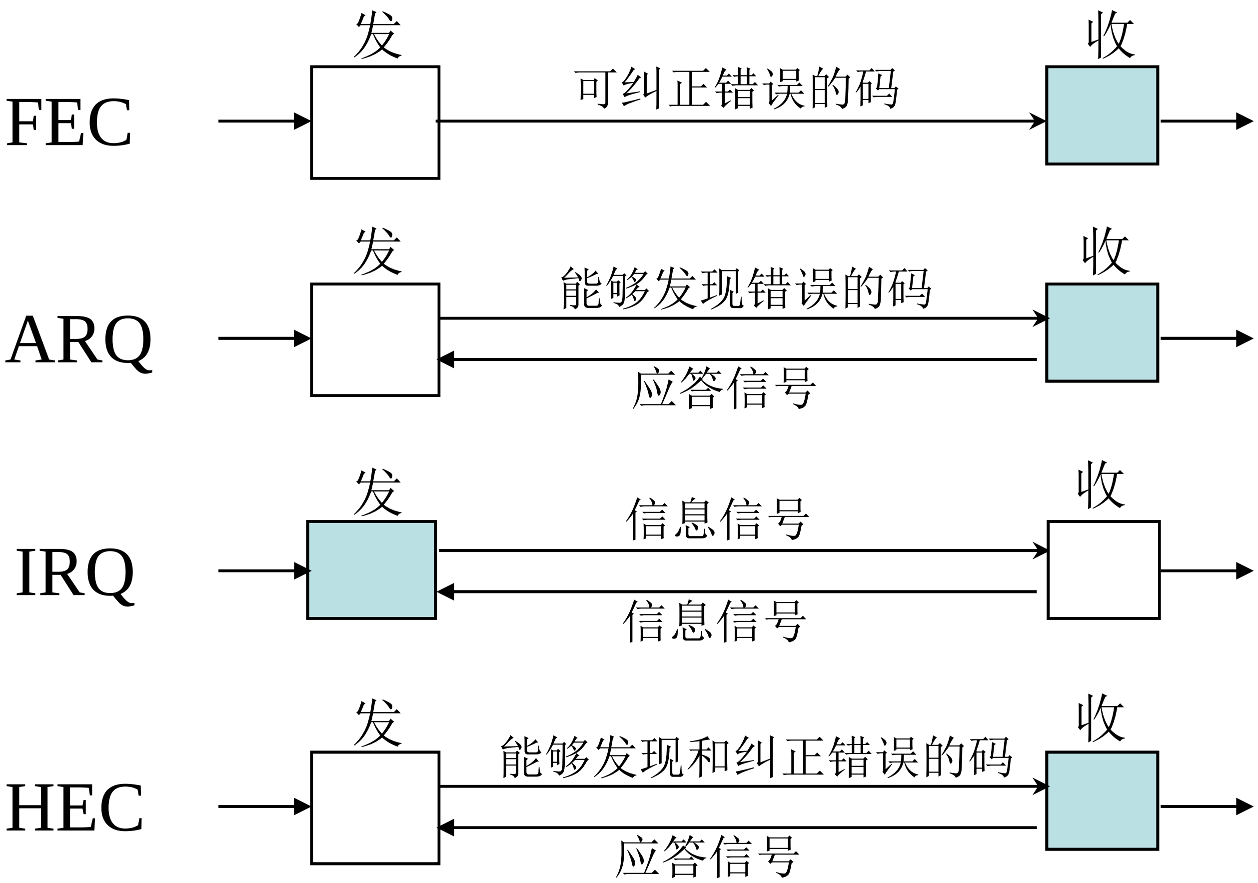
模2加

$\oplus$	0	1
0	0	1
1	1	0

模2乘

$\odot$	0	1
0	0	0
1	0	1

差错控制的基本方式



FEC: Forward Error Control； **ARQ**: Automatic Retransmission Request
IRQ: Information Retransmission Request; **HEC**: Hybrid Error Control

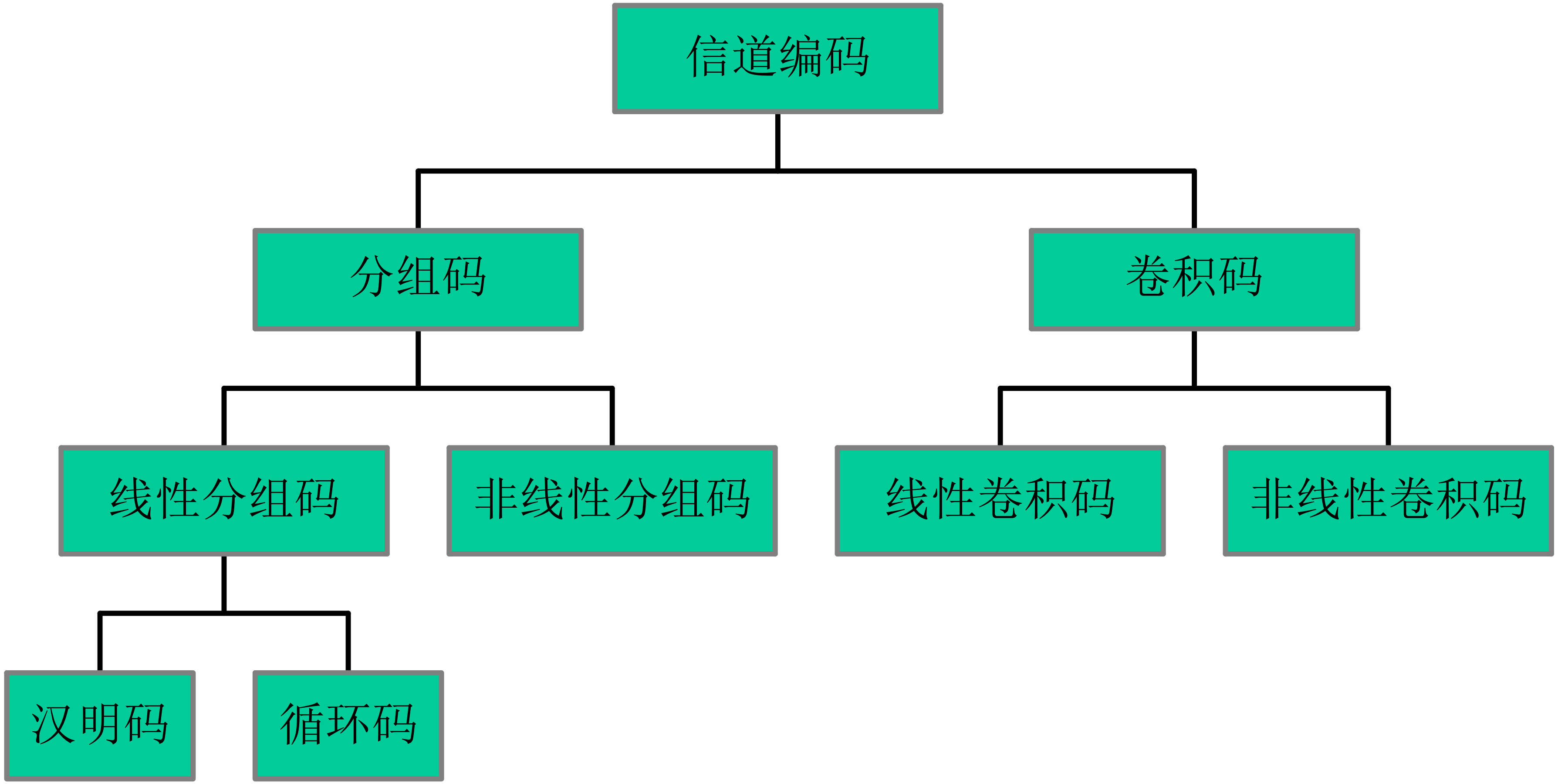
纠错码的基本原理

——纠错码如何纠正错误？

引入信道编码

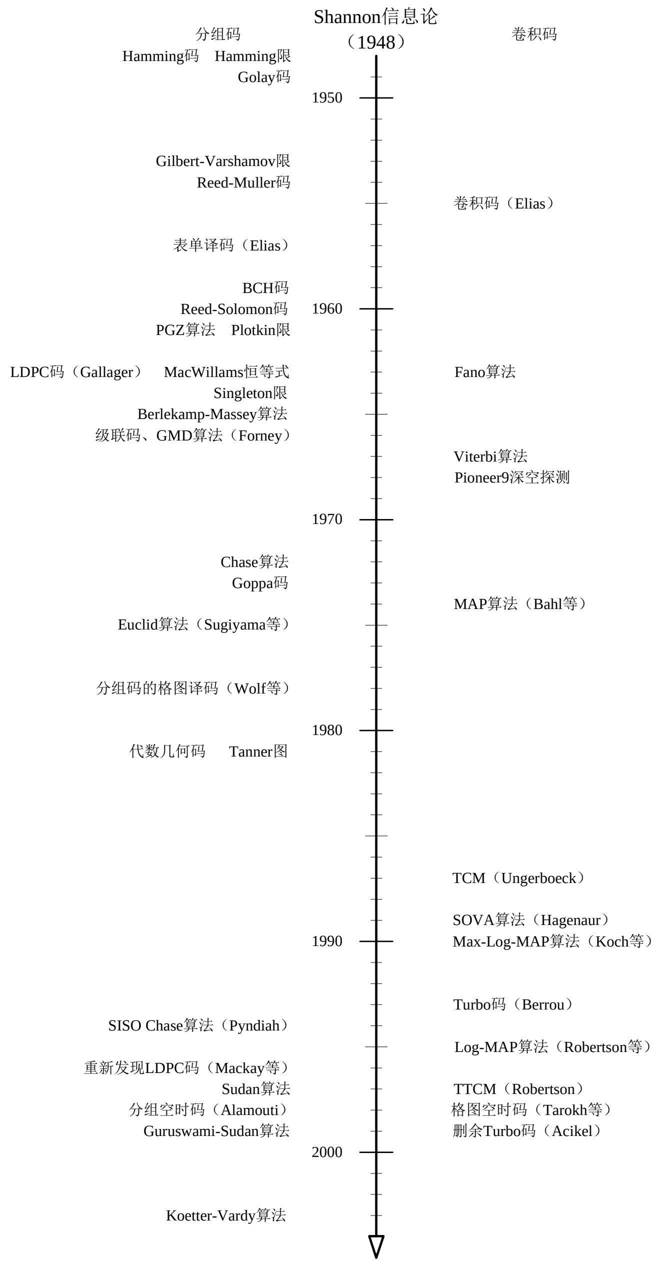
- 检错和纠错：对付信道引入的差错
  - 直观的译码准则：最小距离译码
- Shannon第二定理
  - 当信息速率R小于信道容量C时，总存在一种编码方式使差错率低于任一给定值ε
- 接近信道容量

纠错码的分类



纠错码发展历程

- 通信的数学理论，**Shannon(1948)**
- 汉明码，**Hamming (1950)**
- 级连码，**Forney(1966)**
- 卷积码及有效译码，**(60年代)**
- **RS码及BCH码的有效译码，(60年代)**
- **TCM，Ungerboeck (1982)，Forney(1984)**
- **Turbo码，Berrou (1993)**
- **LDPC 码，Gallager (1963)，Macky (1996)**
- 空时编码，**Tarokh (2000)**



纠错码的基本原理

- **译码失败**：译码器根据接收到的信号无法作出明确判断,不完备译码;
- **译码错误**：译码器根据接收到的信号作出错误判断;
- **完备译码**：根据接收信号，译码器一定能作出是哪一组信息的判断

- **纠错码的基本原理：**
  - **在信息序列之后按照一定的规则添加一定长度的保护比特(校验比特或监督比特)**

纠错码的基本原理

- 以重复码为例
  - $0 \to 0 \ldots 00$ 许用码组(字)
  - $1 \to 1 \ldots 11$
  - 其他所有二进制组合为禁用码组 (字)
  - 若将每个比特重复 n 次，则构成一个码长为 n，信息位长度为 1 的 $(n,1)$ 重复码,且编码效率(码率) $R = 1/n$
  - n=2时

    许用码组：00, 11

    禁用码组：01, 10

    可能接收码字：00, 01, 10, 11

    （能够发现一个错误，但不能纠正错误）

纠错码的基本原理

- n=3

  许用码组：000, 111

  禁用码组：001, 010, 100, 101, 110, 011

  可能接收码字： 000, 001, 010, 100, 101, 110, 011, 111

  能够发现两个错误，纠正一个错误

- n=4

  许用码组：0000，1111

  假定发送码字为：0 → 0000

  禁用码组：0001, 0010, 0100, 1000　　译码正确

  0011, 0101, 0110, 1100, 1001, 1010　　译码失败

  0111, 1101, 1110, 1011　　译码错误

  能够纠正一个错误，同时发现两个错；或发现三个错误

Hamming距离与重量

- **汉明（Hamming）距离：**给定两个序列C1和C2，它们对应位取值不同的个数称为 C1 和 C2 的汉明距离。若 C1=10101, C2=01111; 则 $d(C1,C2) = 3$

- **汉明重量：**序列C中非零码元的个数

  $w(C1) = 3, w(C2) = 4$

- **最小汉明距离：**(n, k)分组码中，设任意两个码字之间距离的最小值为 d_0, 则 d_0 定义为该分组码的最小汉明（Hamming）距离

码纠错能力及编码增益

- 任一(***n, k***)分组码，若要在码字内：

  1) 检测e个随机错误，则要求码的最小汉明距离d_0 >= e+1

  2) 纠正t个随机错误，则要求d_0 >= 2t+1

  3) 纠正t个随机错误，同时检测e (e >= t)个错误，则要求d_0 >= e+t+1

  4) 纠正t个随机错误和ρ个删除，则要求 d_0 >= 2t+ρ+1

- 编码增益：

  - 给定性能前提下，

编码增益=未编码时需要的信噪比(dB) – 编码时需要的信噪比(dB)

例如，未编码时，达到**bit**错误概率**10-5**，需要信噪比**9.6dB**；

采用**1/2**码率的某种卷积码，信噪比大约需要**3.5dB**左右，编码增益**6dB**。

信道编码的作用

- 信道编码的作用：在资源、可靠性和传信量之间选择一个好的工作点（有时还要考虑延时）。
- 资源指的提供信息传输所付出的代价
  - 包括频率、时间、空间、功率等等。但不包括实现复杂度
  - 一个好的编码就是要充分利用资源，传递尽可能多的信息

基本译码方法

- **译码问题**
  - M→C →R：如何根据接收信号 R 估计发送序列 C’，进而估计信息序列 M’
  - 设计译码算法的原则：使译码错误概率最小

$$P_E = \sum_R P(E|R)P(R) \qquad P(E|R) = P(C \neq C'|R)$$

- **最大后验概率(MAP: Maximum Posterior Probability)译码**

$$MinP_E = MinP(E|R) = MinP(C \neq C'|R)$$

$$MinP(C \neq C'|R) = Min(1 - P(C = C'|R))$$

$$\Rightarrow MaxP(C = C'|R)$$

基本译码方法

- 最大似然 **(ML: Maximum Likelihood)**译码

$$P\left(C_i \middle| R\right) = \frac{P(C_i, R)}{P(R)} = \frac{P(C_i) \cdot P\left(R \middle| C_i\right)}{P(R)}$$

$$Max P\left(C_i \middle| R\right) \Rightarrow Max P\left(R \middle| C_i\right)$$

$$\text{if } P\left(C_i\right) = P\left(C_j\right), \text{ for all } i \neq j$$

- 在先验等概的情况下，**MAP**简化为**ML**

信道编码定理

信道编码定理

- 任意离散输入无记忆平稳有噪信道都有一个被称为**信道容量**的值C，它标志着信道传输能力的**上限**，**只要信息传输速率R ≤ C，就存在一种编码方式，当平均码长足够大时，译码错误概率可以做到任意小；反之，则无论采用何种编码方式也不可能保证错误概率任意小。**

信道容量

- 信道容量定义为**信道输入与信道输出的互信息**，它表征了信道可靠传输的最大速率。最常见的信道容量计算式就是带宽、功率受限下的加性高斯白噪声（AWGN）信道容量计算式。设AWGN信道带宽受限于［-W，W］，噪声双边功率谱密度为$N_0/2$，信号功率为P，则

$$C = W\log(1+\frac{P}{N_0 W})\ bits/s$$

- 这个容量仅在**输入服从高斯分布的情况下**可以达到。如果输入信号调制受限，那么容量将会小于上面这个值。

信道容量

- **BSC**
  - 对转移概率为 p 的二进制对称信道而言，当输入等概时，互信息取得最大值，信道容量为

$$C = 1 + p\log_2 p + (1-p)\log_2(1-p) = 1 - H(p)$$

其中 $H(p)$ 是二元熵函数。

- **BEC** $C = 1 - p$

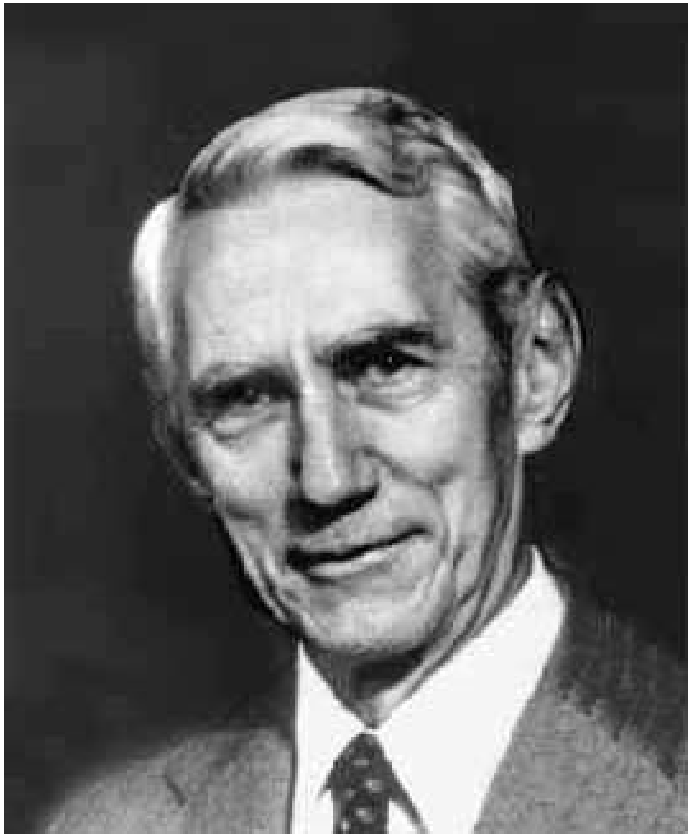
- **BIAWGN**

$$C = \frac{1}{2}\int_{-\infty}^{+\infty} p(y|\sqrt{E_s})\log_2\frac{p(y|\sqrt{E_s})}{p(y)}dy + \frac{1}{2}\int_{-\infty}^{+\infty} p(y|-\sqrt{E_s})\log_2\frac{p(y|-\sqrt{E_s})}{p(y)}dy$$

Claude E. Shannon

- 著名信息论和编码学者Dr. Richard Blahut在Shannon塑像的落成典礼上这样评价Shannon：

“在我看来，两三百年之后，当人们回过头来看我们这个时代的时候，他们可能不会记得谁曾是美国总统，他们也不会记得谁曾是影星或摇滚歌星，但是仍然会知晓Shannon的名字，学校里仍然会讲授信息论。”



C. E. Shannon