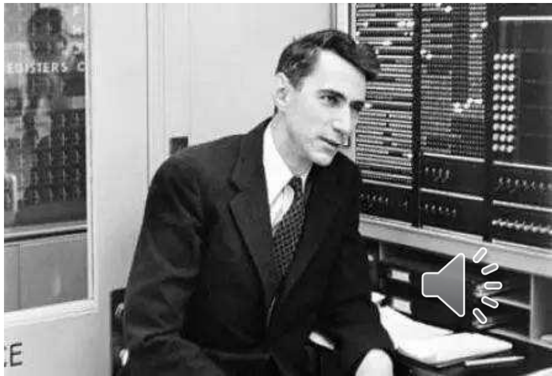
信息论
信号传输与处理的理论基础

线性分组编码及通用ML译码算法

经典编码与现代编码(4)

* 关于**信道编码基本定理**(Shannon, Cover, Verdu, Shimai,…)
*
* **任何信道均存在一个仅与信道的噪声干扰特性有关的正数C(信道容量)，只要分组编码的传输速率$k/n<C$，则对任何充分小的正数ε，都存在某种编码算法$E_{\varepsilon,n,k}$，使得相应的译码算法$D_{\varepsilon,n,k}$在噪声环境中的差错概率$P[D_{\varepsilon,n,k}]<\varepsilon$。**

* 注：分组编码的传输速率$k/n<C$等价于编码的冗余度$>1-k/n$.
* 例：
* (1) 单位差错概率为p的二元对称BSC信道的容量
* $$C = 1 + p\log_2 p + (1-p)\log_2(1-p)$$
* (2) 有限带宽为W、信噪比为SNR的Gauss 信道的容量
* $$C = W\log_e(1+SNR)$$
* (3) MIMO信道的容量
* (4) 多接入信道的容量
* (5) 广播信道的容量……



经典编码与现代编码(5)

* 信道编码基本问题：
* 设计编码算法$E_{\varepsilon,n,k}$和译码算法$D_{\varepsilon,n,k}$，使得:
* (1) $k/n<C$但尽可能地接近C，C是该编码方案所针对的信道的容量.
* (2) 编码和译码算法的计算复杂性尽可能低。

* 信道编码设计方法：
* (1) 基于有限域的代数结构的设计方法
* 典型工具：F_2的N次扩域、本原多项式、有限域上的特征标群等。
* (2) 基于代数曲线的设计方法
* 典型工具：椭圆曲线等
* (3) 基于图结构的编码设计方法
* (4) 上述方法同人工智能相结合的设计方法
*

经典编码与现代编码(6)

* 线性分组码（一）：通用编码结构与译码概述

* 设$\boldsymbol{u}=(u_1,u_2,\ldots,u_k)^T$是原始信息的分组，$u_i=0$或1。
* $n>k$, G是一个n行k列矩阵，矩阵元素$g_{ij}=0$或1，且秩=k。
* 对每个原始信息分组u，$\boldsymbol{x}=\boldsymbol{Gu}$是u的码字，$\boldsymbol{x}=(x_1,x_2,\ldots,x_n)^T$.
* 注:
* (1) 以上比特运算均为二进制算术运算，即域F_2上的加法与乘法。
* (2) G的秩为k(满秩)，故对$u\neq v$必有$Gu\neq Gv$，即：
* 不同的原始信息必有不同的码字。
* (3) G的秩为k，故必存在n-k行、n列矩阵H满足$HG=O$，且H的秩=n-k。
* (4) n维二进制向量x是一个码字，即存在k维二进制向量u使$x=Gu$，
* 当且仅当$Hx=0$.
* (5) ML译码算法：对每个n维接收向量$r=x+e$，计算
* $\hat{e}=\mathit{Argmin}\,\{|e|_H: He=Hr\}$, $\hat{x}=r+\hat{e}$, 其中$|e|_H$: =e的非零分量的个数。

经典编码与现代编码(7)

* 线性分组码（二）：传输方程与等效的差错表示

* **二进制线性分组码的传输差错的等效表示**
* 码字$\mathbf{x}=(x_1,x_2,\ldots,x_n)$的每一位$x_j=0,1$.
* 接收分组$\boldsymbol{r}=(r_1,r_2,\ldots,r_n)$的每一位$r_j=0,1$.
* 第j位发生传输差错，当且仅当$y_j \neq x_j$；
* 设想第j位在传输过程中被一位噪声$e_j \in \{0,1\}$以叠加的形式所干扰：
* $$r_j = x_j + e_j$$
* 【注】该表达式是二元数字传输的传输方程，这里及以下的 + 运算是指二进制运算：
* $1+0=0+1=1, 1+1=0+0=0$. 传输方程的矢量形式为$\boldsymbol{r}=\boldsymbol{x}+\boldsymbol{e}$。
* 因此，码字的第j位发生传输差错的等效条件是：$e_j=1$ 。
* 借助于传输方程，BSC信道差错特性的等效表示归结为：
* (1) 在一个码字的传输过程中，差错图样$e=(e_1,e_2,\ldots,e_n)$的每个比特两两独立；
* (2) 对每个j，$P[e_j=1]=p$.

经典编码与现代编码(8)

* 线性分组码（三）：码字传输的差错概率
*
* 根据传输方程 $y_j = x_j + e_j, j=1,\ldots,n,$ 在BSC信道上接收分组 $\boldsymbol{r}=(r_1,r_2,\ldots,r_n)$
* 相对于码字 $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ 发生特定差错 $\boldsymbol{e}=(e_1,e_2,\ldots,e_n)$ 的概率
* $P[\boldsymbol{e}] = P[e_1]\ldots P[e_n]$
* $= \prod_{j:e_j=1} P[e_j] \prod_{j:e_j=0} P[e_j] = \prod_{j:e_j=1} p \prod_{j:e_j=0} (1-p)$
* $= p^{|e|}(1-p)^{n-|e|}$
* 其中 $|e|$ 是差错图样 $\boldsymbol{e}=(e_1,e_2,\ldots,e_n)$ 中非零比特的个数。
* 定义：二进制向量 $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ 中非零比特的个数，称为x的Hamming重量。
* 结论：BSC信道上的差错概率P[**e**]仅与差错图样e的Hamming重量有关。

【注1】根据这一结论，两个不同的差错图样，虽然差错发生的位置不同，只要其Hamming重量相等，即总的差错比特数相同，则发生的概率就相同。

【注2】从 $P[\boldsymbol{e}] = (1-p)^n(\frac{p}{1-p})^{|e|}$ 可以看到，对 $0<p<1/2$ 的情形，$P[\boldsymbol{e}]$ 随 $|\boldsymbol{e}|$ 的增大而下降。

经典编码与现代编码(9)

* 线性分组码（四）：Hamming重量的基本性质

* 定义：二进制向量 $\mathbf{x}=(x_1,x_2,\ldots,x_n)$的Hamming重量
* $$|\mathbf{x}|_H = \sum_{j:x_j=1} 1$$
* 基本性质：
* (1) $|\mathbf{x}|_H \geq 0$ 且 $|\mathbf{x}|_H = 0$ 当且仅当 x是全零码字。
* (2) 对线性码，码字x和码字y之和x+y仍然是一个码字，且恒有不等式
* $$|\mathbf{x}+\mathbf{y}|_H \leqq |\mathbf{x}|_H + |\mathbf{y}|_H$$

【习题】根据定义验证以上性质。

基于上述性质，定义两个码字x和y之间的Hamming距离为$|\mathbf{x}+\mathbf{y}|_H$. 因此$|\mathbf{x}|_H$实际上是码字x和全零码字的Hamming距离。

【思考】x和y的Hamming距离的实际含义是什么？

该距离反映两个码字在“对应位上不同”这一意义上差异有多大。

练习：码字00011100110和码字01001101101的Hamming距离是多少？

经典编码与现代编码(10)

- 线性分组码（五）：通用译码算法

- ML译码算法初始化：
- 生成译码表DE, 每个表项是一对向量[s,e]，其中e满足方程s=Hz
- 的各种解z中Hamming重量最小的解。

- ML译码算法
- 对每个接收向量$\mathbf{r}=(r_1,r_2,\dots,r_n)$，译码器做以下处理：
- 第一步：用编码方案的(n-k)×n校验矩阵H计算n-k维二进制向量

$$\mathbf{s} = \mathbf{Hr}$$

- 如果s=0，则将r作为正确的码字接受下来，否则转第二步。
- 第二步：检索译码表，找到表项[s,e]，计算$\hat{x} = r + e$, 并将$\hat{x}$作为正确的码字接受。

经典编码与现代编码(11)

* 线性分组码（六）： 对通用译码算法的解释

* ML译码算法初始
* 生成译码表DE,
* 的各种解z中Hamm
*
* ML译码算法
* 对每个接收向量r=(
* 第一步：用编码方
*
* 如果s=0，则将r作
* 第二步：检索译码
* 的码字接

(1) 码字x的接受分组r = x + e，e是差错图样，
因为Hx=H(Gu)=(HG)u=0，所以

$$s = Hr = Hx + He = He$$

即s仅由实际错误图样e确定。

(2) 对给定的s，方程s=Hz 具有多个解z，因此不能简单通过求逆来从s计算出e（H非可逆!）.

(3) ML译码算法选择满足s=Hz 的概率最大的解作为实际差错图样(的估计)。

(4) 根据前面的结果$P[z] = (1\text{-}p)(\frac{p}{1-p})^{|z|}$看到，$0<p<1/2$时，Hamming重量越小的解其P[z]越大。
这就是为什么在译码表中对每个s存储一个表项[s,e]，e是满足方程s=Hz的各种解z中Hamming重量最小的解！

(5) r = x + e，因此x = r + e。

【思考】什么样的传输差错，ML算法永远不可能检测到？

经典编码与现代编码(12)

* 线性分组码（七）：ML译码算法的普遍性能

设(n,k)线性分组编码方案的码字最小距离为$\boldsymbol{d}_{min}$（等价地，该分组码的最小非零码字的Hamming重量为$\boldsymbol{d}_{min}$），则：

（1）任何少于$\boldsymbol{d}_{min}$位的传输差错，都能被明确地检测到。

这是因为在ML译码算法中，如果$|\boldsymbol{e}|<d_{min}$则e不可能是非零码字，因此$s=Hr=He\neq 0$，从而译码器判定存在一个错误。

(2) 任何少于$[(\boldsymbol{d}_{min}-1)/2]$位的传输差错，都能被正确地校正。

注意到不可能存在两个不同的码字x和y均满足$|x+r|\leq[(\boldsymbol{d}_{min}-1)/2]$和$|y+r|\leq[(\boldsymbol{d}_{min}-1)/2]$，否则将有矛盾$|x+y| = |x+r+y+r| \leq |x+r|+|y+r| < \boldsymbol{d}_{min}$。因此，如果实际差错位数少于$[(\boldsymbol{d}_{min}-1)/2]$，这时同$\boldsymbol{r}$的Hamming距离最近的码字只有一个，并且正是$\boldsymbol{r}+\boldsymbol{e}=\boldsymbol{x}$。

【注】由以上结论，码的设计方案(在满足其他约束的条件下)应尽可能追求大的$\boldsymbol{d}_{min}$。

信道编码与Shannon定理

* Shannon定理：
* 分组编码的译码性能与传输效率
* 之关系普遍的结论（定理7.7.1）
* 更现代的成果：
* 网络编码定理：Cover、Shamai、Verdu、…
* MIMO链路/时空编码