# VLSI数字通信原理

# 信道编码

上海交通大学电子信息与电气工程学院

# 提纲

- 循环码
- 常用分组码

# 循环码的基本概念

定义 对线性分组码U，如对任意 $U_i \subset U$， $U_i$ 循环左移或循环右移任意位后得到的码组$U_i'$仍然有$U_i' \subset U$，则称U为**循环码**。

码多项式

用代数理论研究循环码，可将码组用多项式表示，多项式称为**码多项式**。

一般地，长为n的码组$U_{n-1}U_{n-2}...U_1U_0$，对应码多项式T(X)

$$U(x) = u_{n-1}X^{n-1} + u_{n-2}X^{n-2} + ... + u_1X + u_0$$

式中，$X^i$系数对应码字中$U_i$的取值。

# 循环码的基本概念

例： （7, 3）码字：0111001 对应 $1+x^3+x^4+x^5$

对二进制码组，U(x)的系数只在二元域上取值，二元域上加、乘运算规则如下：

加运算：

$$0\oplus 0=0 \qquad 0\oplus 1=1 \qquad 1\oplus 0=1 \qquad 1\oplus 1=0$$

乘运算：

$$0\cdot 0=0 \qquad 0\cdot 1=0 \qquad 1\cdot 0=0 \qquad 1\cdot 1=1$$

减法和除法可由加法和乘法定义。

# 同余类的概念

在整数除法中，取定除数n，可将所有整数按除以n所得余数进行分类，余数相同的数称为关于n的同余类。

一般地，若

$$\frac{m}{n} = Q + \frac{p}{n}$$

（Q为整数，p ＜ n）（模 n）

则记为：

$$(m)_n \equiv (p)_n$$

所有余数为p的整数属于关于模n的一个同余类。

# 同余类的概念

类似地，可以定义关于**多项式N(x)的同余类**，若

$$\frac{F(x)}{N(x)} = Q(x) + \frac{R(x)}{N(x)}$$

式中Q(x)为整式，余式R(x)的幂 ＜ N(x)的幂。

上式可写成：

$$F(x) = Q(x)N(x) + R(x)$$

记为： $F(x) \equiv R(x) \quad \mathrm{mod} N(x)$

例：在系数为二元域的多项式中，有

$$1 \equiv x^n \quad \mathrm{mod}\left(x^n + 1\right)$$

因为：

$$\frac{x^n}{x^n+1} = \frac{x^n+1+1}{x^n+1} = 1 + \frac{1}{x^n+1}$$

从而有上述结论。

# 循环码的代数结构

**定理1** 若U(X)是长度为n的循环码中的一个码多项式，则$X^iU(X)$（i为不等于0的整数）按模 $X^n+1$运算的余式必为循环码中的另一码多项式。

证明：设i＝1，有

$$XU(X)=u_{n-1}X^n+u_{n-2}X^{n-1}+\ldots+u_1X^2+u_0X$$

$$\frac{XU(X)}{X^n+1}=\frac{u_{n-1}X^n+u_{n-2}X^{n-1}+\ldots+u_1X^2+u_0X}{X^n+1}=$$

$$=\frac{u_{n-1}\left(X^n+1\right)+u_{n-2}X^{n-1}+\ldots+u_1X^2+u_0X+u_{n-1}}{X^n+1}=$$

$$=u_{n-1}+\frac{u_{n-2}X^{n-1}+\ldots+u_1X^2+u_0X+u_{n-1}}{X^n+1}$$

# 循环码的代数结构

余式为

$$u_{n-2}X^{n-1}+\ldots+u_1X^2+u_0X+u_{n-1}$$

对应码组$u_0$ $u_1$ …$u_{n-2}$ $u_{n-1}$右循环一位之后的得到的码组：

$u_{n-1}$ $u_0$ $u_1$ … $u_{n-2}$ 。

若i＝2

$$\frac{X^2U(X)}{X^n+1}=\frac{X\left(XU(X)\right)}{X^n+1}=\frac{X\left(u_{n-1}\left(X^n+1\right)+u_{n-2}X^{n-1}+\ldots+u_1X^2+u_0X+u_{n-1}\right)}{X^n+1}$$

$$=u_{n-1}X+\frac{u_{n-2}X^n+\ldots+u_1X^3+u_0X^2+u_{n-1}X}{X^n+1}=$$

$$=u_{n-1}x+u_{n-2}+\frac{u_{n-3}X^{n-1}+\ldots+u_1X^3+u_0X^2+u_{n-1}X+u_{n-2}}{X^n+1}$$

# 循环码的代数结构

显然，余式为对应码组$u_0\ u_1\ ...u_{n-2}\ u_{n-1}$右循环两位之后的得到的 码组。一般地，对任意i有：

$$\frac{X^iU(X)}{X^n+1}=Q(X)+\frac{u_{n-i-1}X^{n-1}+\ldots+u_0X^i+u_{n-1}X^{i-1}+u_{n-2}X^{i-2}+\ldots+u_{n-i}}{X^n+1}$$

余式对应$u_0\ u_1\ ...u_{n-2}\ u_{n-1}$右循环i位之后的得到的码组。

证毕

**例** 已知码组的长度为n＝4，其中一码字：U＝1101(高位在右)，求该码字循环移位3位后得到的码字。

a. 由1101直接(右)循环移3位得：$U^{(3)}=1011$

b. 根据多项式关系求解，当i＝3时，

$$\mathbf{U}(X) = 1 + X + X^3$$
$$X^i\mathbf{U}(X) = X^3 + X^4 + X^6$$

关于$X^4+1$的余式$U^{(3)}(X)$ $\rightarrow$ 1011

$$\begin{array}{r l}
 & X^2 + 1 \\
X^4 + 1 \,\big) & \overline{X^6 + X^4 + X^3} \\
 & X^6 \qquad\qquad\quad + X^2 \\
 & \overline{\qquad X^4 + X^3 + X^2} \\
 & \qquad X^4 \qquad\qquad + 1 \\
 & \overline{\qquad\qquad X^3 + X^2 + 1}
\end{array}$$

remainder $\mathbf{U}^{(3)}(X)$

# 循环码的生成多项式g(x)及生成矩阵

## 循环码的生成多项式

一般地，线性分码组可表示为

$$U=[m_{n-1}m_{n-2}\dots m_{n-k}]G=[m_{n-1}m_{n-2}\dots m_{n-k}][I_k\,|\,P]$$

**矩阵G中每一行均为一许用码组**，如第i行对应第i个信息位为1，其余为0时的信息码生成的码组。

由于G中包含一个$I_k$分块，所以G为k个独立的码组组成的矩阵。

即：**任一线性分组码码组均可由k个线性无关的码组组合而成**。

# 循环码的生成多项式g(x)及生成矩阵

利用上述线性分组码

**任一线性分组码码组均可由k个线性无关的码组组合而成**

这一性质，寻求循环码生成矩阵的构建方法。

设存在一个幂次数为n－k，且常数项不为0的**码多项式**g(X)，

则由循环码的性质（定理1）

$g(X)$，$Xg(X)$, ……，$X^{k-2}g(X)$，$X^{k-1}g(X)$　（最高次幂等于n－1）

也是码多项式，这k个码多项式对应独立的k个码字，由此可构成循环码生成矩阵G(X)。

# 循环码的生成多项式g(x)及生成矩阵

循环码生成矩阵G(X)

$$G[X]=\begin{bmatrix} X^{k-1}g(X) \\ X^{k-2}g(X) \\ \cdots\cdots \\ Xg(X) \\ g(X) \end{bmatrix}$$

其中，g(X)称为循环码**码生成多项式**。G(X)对应的系数矩阵G右侧的子方阵具有主对角线元素均不为0的形式。该子阵行列式不为0，因而子阵满秩，因而行向量是线性无关的。

利用码生成矩阵G(X)，任一码字多项式可以表示为：

$$U(X)=\left(m_{k-1}X^{k-1}+\ldots+m_2X^2+m_1X+m_0\right)g(X)$$

或：
$$U(X)=\left(m_0+m_1X+m_2X^2+\ldots+m_{k-1}X^{k-1}\right)g(X)$$

# 循环码的生成多项式g(x)及生成矩阵

例（7，3）生成多项式 $g(X)=X^4+X^3+X^2+1$ 对应生成矩阵G[X]

矩阵为：

$$G[X]=\begin{bmatrix} X^{3-1}g(X) \\ X^{2-1}g(X) \\ g(X) \end{bmatrix}=\begin{bmatrix} X^6+X^5+X^4+X^2 \\ X^5+X^4+X^3+X \\ X^4+X^3+X^2+1 \end{bmatrix}$$

$$G=\begin{bmatrix} 1110100 \\ 0111010 \\ 0011101 \end{bmatrix}=\begin{bmatrix} 111\ \ 0100 \\ 011\ \ 1010 \\ 001\ \ 1101 \end{bmatrix}$$

因为矩阵G左侧的子方阵满秩，因此容易判断该矩阵中的行向量是线性无关的。

# 循环码的生成多项式g(x)及生成矩阵

**定理 2** 在循环码中，n－k次的码多项式g(X)有一个且只有一个。

**证明：**

（a）在含k个信息位的循环码中，除全0码外，其它码组最多只有k-1个连0。否则，经循环移位后前面k个信息码元为0，而监督码元不全为0的码组，这在线性分组码中是不可能的。所以一定有一个n－k次的多项式。

（b）n－k次的码多项式g(X)的常数项不能为0，否则该多项式移一位就会出现k个连0的情况。

# 循环码的生成多项式g(x)及生成矩阵

（c） n－k次的码多项式g(X)只可能有一个，若有两个，两多项式相加后由线性分组码的封闭性仍为码多项式，但由于n－k次项和常数项相消，会产生k＋1连0的情况，由（a）分析，这是不可能的。

综上（a）、（b）和（c），**证毕**。

# 循环码的生成多项式g(x)及生成矩阵

**定理 3** 在循环码中，所有的码多项式U(x)都能被g(X)整除。

**证明：** 因为任一码多项式都可由其信息码元和生成矩阵G[x]确定：

$$U(X)=\left[m_{k-1}m_{k-2}\ldots m_0\right]G[x]=\left[m_{k-1}m_{k-2}\ldots m_0\right]\begin{bmatrix} X^{k-1}g(X) \\ X^{k-2}g(X) \\ \cdots\cdots \\ Xg(X) \\ g(X) \end{bmatrix}$$

$$=m_{k-1}X^{k-1}g(X)+m_{k-2}X^{k-2}g(X)+\ldots+m_0 g(x)$$

$$=\left(m_{k-1}X^{k-1}+m_{k-2}X^{k-2}+\ldots+m_0\right)g(X)=m(X)g(X)$$

g(X)为码多项式U(x)的一个因式，所以U(x)可被g(X)整除。

**证毕**

# 循环码的生成多项式g(x)及生成矩阵

**推论**：次数不大于k－1次的任何多项式与g(X)的乘积都是码多项式。

# 循环码的生成多项式g(x)及生成矩阵

**定理 4** 循环码（n，k）的生成多项式g(X)是$X^n+1$的一个因式。

**证明**：因为g(X)幂为n−k，因而可得

$$\frac{X^k g(X)}{X^n+1}=1+\frac{R(X)}{X^n+1}$$

其中R(X)的幂小于n。由定理1，R(X)是码多项式，又由定理3，有R(X)=m(X)g(X)，即有

$$X^k g(X)=\left(X^n+1\right)+R(X)=\left(X^n+1\right)+m(X)g(X)$$

移项整理得：

$$X^n+1=X^k g(X)+m(X)g(X)=\left[X^k+m(X)\right]g(X)=h(X)g(X)$$

即g(X)是$X^n+1$的一个因式。**证毕**

# 循环码的生成多项式g(x)及生成矩阵

称 $h(X)=\dfrac{X^n+1}{g(X)}$ 为循环码的一致效验多项式。

对任一码多项式，U(X)＝m(X)g(X)，有

$h(X)U(X)=h(X)[m(X)g(X)]=[h(X)g(X)]m(X)=(X^n+1)m(X)$

即若U(X)是许用码组对应的多项式，其**乘积h(X)U(X)一定可被$X^n$＋1整除**。

生成多项式g(X)的**三个性质**（充要条件）：

（a）g(X)是n－k次多项式；

（b）g(X)的常数项不等于0；

（c）是$X^n$＋1的一个因式。

# 循环码的生成多项式g(x)及生成矩阵

采用前面定义的循环码生成矩阵：

$$G[x]=\begin{bmatrix} x^{k-1}g(x) \\ \cdots\cdots \\ g(x) \end{bmatrix}$$

对应的系数矩阵G一般**不**符合

$$G=[I_k, P]$$

形式。编码输出结果相当于m(x)g(x)，所得码组为非系统码结构。信息码和监督码不容易区分。

# 循环码的生成多项式g(x)及生成矩阵

**例：** 线性分组码（7，4）生成多项式 $g(x)=x^3+x^2+1$ 对应生成矩阵G[x]对应的系数矩阵为：

$$G[x]=\begin{bmatrix} x^{4-1}g(x) \\ x^{3-1}g(x) \\ x^{2-1}g(x) \\ g(x) \end{bmatrix} \leftrightarrow \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

为非系统码结构的生成矩阵。

# 例题——构造循环码

- 例：构造一个（7，3）循环码
- 解：

由于$n=7$,对$(x^7+1)$因式分解得：

$$x^7+1=(x+1)(x^3+x^2+1)(x^3+x+1)$$

由于$k=3$,则$n-k=4$,因此(7,3)循环码的两个可选生成多项式为：

$$g_1(x)=(x+1)(x^3+x^2+1) \quad g_2(x)=(x+1)(x^3+x+1)$$

取生成多项式为：

$$g(x)=g_1(x)=(x+1)(x^3+x^2+1)=(x^4+x^2+x+1)$$

# 例题——校验矩阵和生成矩阵

- 例：对上例的（7，3）循环码，求其校验矩阵和生成矩阵。
- 解　**生成多项式矩阵为$G(x)$、生成矩阵为$G$**

$$G(x)=\begin{bmatrix} x^2g(x) \\ xg(x) \\ g(x) \end{bmatrix}=\begin{bmatrix} x^6+x^4+x^3+x^2 \\ x^5+x^3+x^2+x \\ x^4+x^2+x+1 \end{bmatrix};$$

$$G=\begin{bmatrix} \boxed{1 & 0 & 1 & 1 & 1} & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

# 例题——校验矩阵和生成矩阵

- 例：对上例的（7，3）循环码，求其校验矩阵和生成矩阵。
- 解

**校验多项式为**$h(x) = (x^7+1)/g(x) = (x^3+x+1)$

$$\text{校验矩阵为} H = \begin{bmatrix} \boxed{1 \quad 0 \quad 1 \quad 1} & 0 & 0 & 0 \\ 0 \quad 1 \quad 0 \quad 1 & 1 & 0 & 0 \\ 0 \quad 0 \quad 1 \quad 0 & 1 & 1 & 0 \\ 0 \quad 0 \quad 0 \quad 1 & 0 & 1 & 1 \end{bmatrix}$$

# 例题——循环码的生成

- 例：对上例的（7，3）循环码，若输入信息码字为110，求其循环码。
- 解：

**循环码字为110的码式为** $m(x) = x^2 + x$

**得循环码式为**

$$c(x) = m(x)g(x) = (x^2 + x)(x^4 + x^2 + x + 1)$$
$$= x^6 + x^5 + x^4 + x$$

**则其循环码字为1110010**

# 例题——循环码的检错

- 例：对于上例的（7，3）循环码，若接收码字为1100100，判断是否为许用码字。
- 解：接收码字1100100的码式为$R(x)=x^6+x^5+x^2$

由伴随式$S(x)=e(x)\bmod g(x)=R(x)\bmod g(x)$

$$S(x)=(x^6+x^5+x^2)\bmod(x^4+x^2+x+1)=1$$

因为$S(x)\neq 0$,因此该码字不是（7,3）循环码的许用码字

# 系统循环码的编码方法

a.以$X^{n-k}$乘信息多项式m(X)，m(X) → $X^{n-k}$ m(X)；（幂 < n）

b.用g(X)除$X^{n-k}$ m(X)得余式p(X) ( 幂 < n-k ) 即

$$X^{n-k} m(X) = q(X)g(X)+p(X),$$ q(X)的幂次数小于k

取码多项式

$$U(X) = X^{n-k} m(X)+p(X) \qquad (*)$$

**分析上述编码方式的合理性：**

$$U(X) = X^{n-k} m(X)+p(X) = [q(X)g(X)+p(X)]+p(X) = q(X)g(X)$$

因为q(X)的幂次数小于k，由定理3推论，q(X)g(X)一定是循环码的码多项式，显然（*）定义的U(X)为一种系统码结构的循环码。

# 循环码编码器的电路实现

由系统码结构循环码的编码方法可知

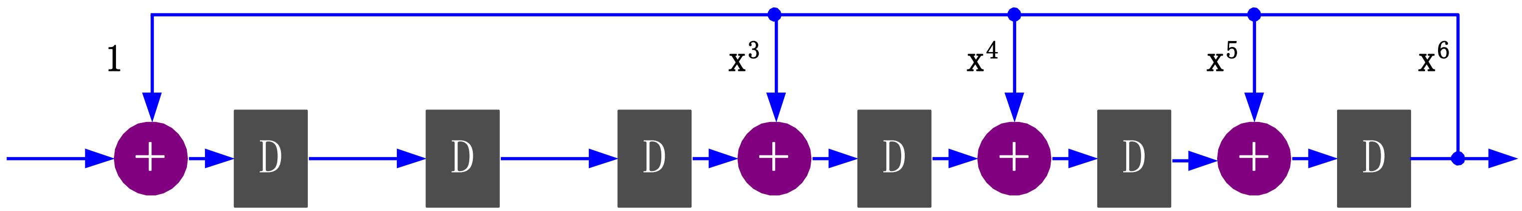
循环码编码器的实现需要用到以生成多项式g(x)为除式的除法器计算余式p(x)：

$$\frac{x^{n-k}m(x)}{g(x)}=q(x)+\frac{p(x)}{g(x)}$$

# 循环码编码器的电路实现

<u>多项式除法</u>　多项式除法可用带反馈的移位寄存器实现。

**例**：除数为 $g(X)=X^6+X^5+X^4+X^3+1$ 除法电路如下图，反馈的接入由g(X)确定




## 除法运算的实现

先将移位寄存器清“0”；

进行n次移位，将被除数全部送入除法器后，在寄存器内即可得到相应的余式。

## (接上例)计算C(X)/g(X)，其中$C(X)=X^{13}+X^{11}+X^{10}+X^{7}+X^{4}+X^{3}+X+1$

| 移位序号 | 输入 | 移位寄存器内容 | 输出商 | 反馈信号 |
|---|---|---|---|---|
| 0 | 0 | L 000000 H | 0 | 000000 |
| 1 | 1 | 100000 | 0 | 000000 |
| 2 | 0 | 010000 | 0 | 000000 |
| 3 | 1 | 101000 | 0 | 000000 |
| 4 | 1 | 110100 | 0 | 000000 |
| 5 | 0 | 011010 | 0 | 000000 |
| 6 | 0 | 001101 | 1 | 000000 |
| 7 | 1 | 000001 | 1 | 100111 |
| 8 | 0 | 100111 | 1 | 100111 |
| 9 | 0 | 110100 | 0 | 100111 |
| 10 | 1 | 111010 | 0 | 000000 |
| 11 | 1 | 111101 | 1 | 000000 |
| 12 | 0 | 111001 | 1 | 100111 |
| 13 | 1 | 011011 | 1 | 100111 |
| 14 | 1 | 001010 | 0 | 100111 |
| | | 余数 | | |

得余式： $p(x)=x^4+x^2$ （容易通过长除法验证）

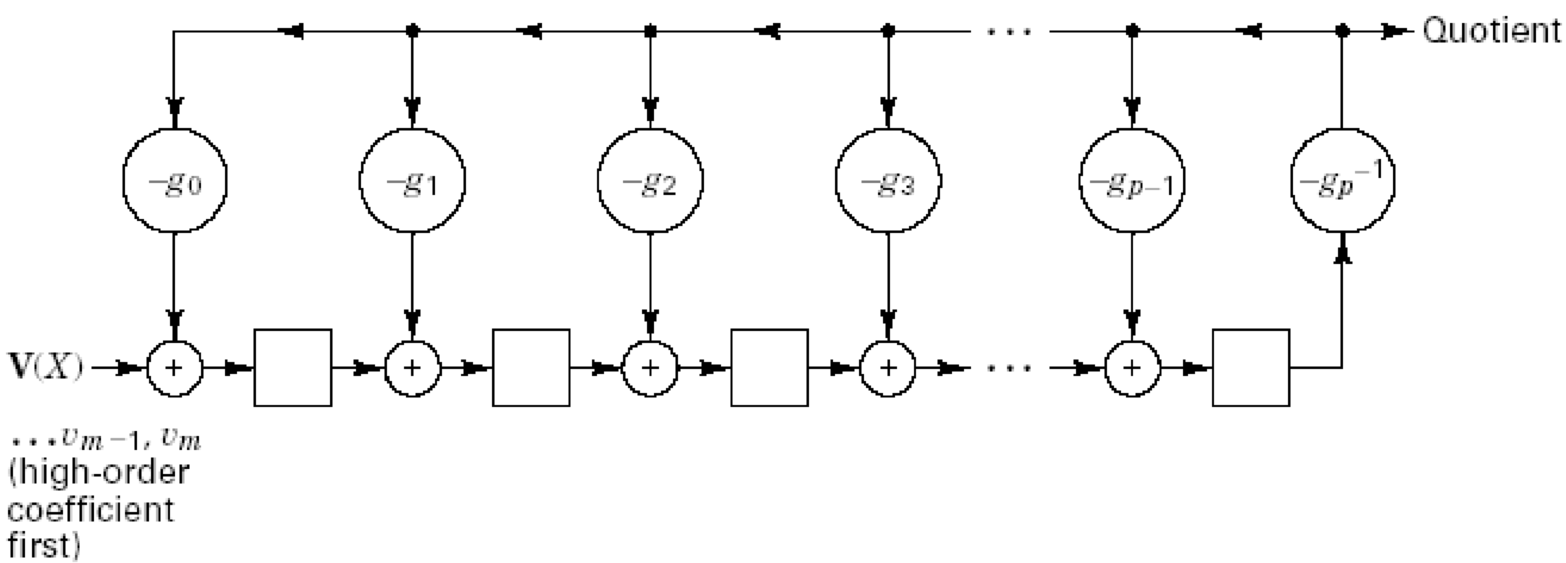
# 循环码编码器的电路实现

## 多项式除法电路的一般形式

被除式： $\mathbf{V}(X) = v_0 + v_1X + v_2X^2 + \cdots + v_mX^m$

除式： $\mathbf{g}(X) = g_0 + g_1X + g_2X^2 + \cdots + g_pX^p$

相应实现电路：



# 循环码译码电路

## 循环码的译码过程

1) 由收到的多项式r(X)计算校正子多项式S(X)：S(X)＝r(X)/g(X)

2) 由S(X)确定误码的错误图样E(X)；（无误码时显然有S(x)=0）

3) 将E(X)与r(X)相加，纠正错误（若在纠错范围内）。

一般地，对矩阵形式的线性分组码，校正子S为：

$$S = rH^T = (U \oplus E)H^T = UH^T \oplus EH^T = EH^T$$

对于循环码，校正子对应的多项式S(x)为：

$$S(X) \equiv r(X) = U(X) + E(X) \quad \bmod\big(g(X)\big)$$

$$\equiv E(X) \qquad\qquad \bmod\big(g(X)\big)$$

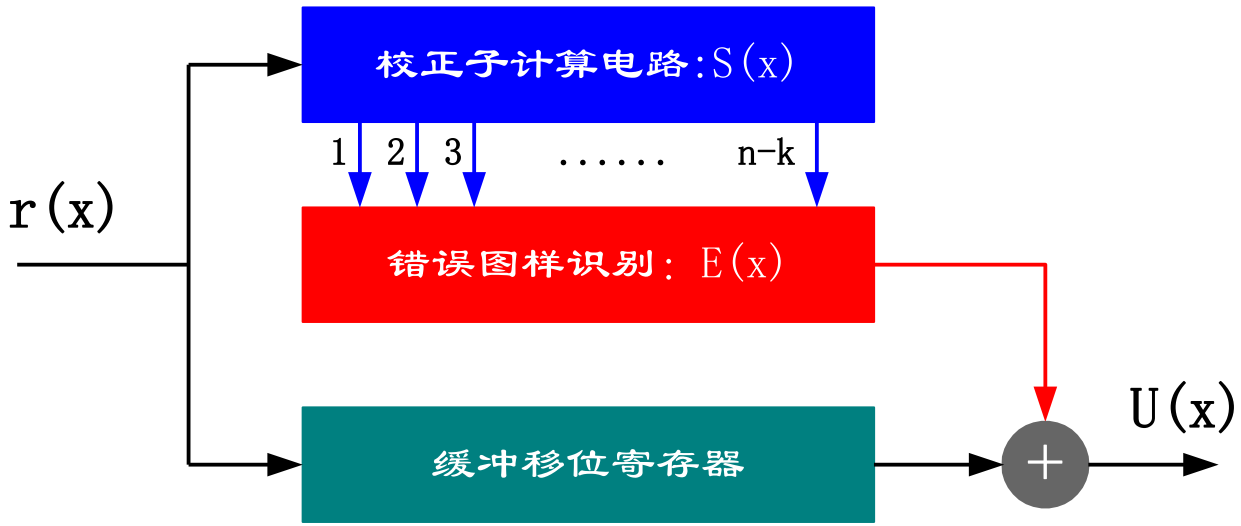
# 循环码译码电路

## 纠错译码步骤

a. 计算S(X)＝r(X)/g(X)

b. 确定错误图样S(X)→E(X)

c. 根据E(X)纠错。



[例] 已知（7，4）码是纠正一位错的汉明码，且$g(x)$ = $x^3+x+1$；请为$R$ = 0110010（高位在前）纠错。

解：设接收码为$R = (r_6 r_5 r_4 r_3 r_2 r_1 r_0)$；由

$S(x) = E(x) \bmod g(x)$；可列出$S(x)$—$E(x)$ 对照表：

| 误码位置 | $r_0$ | $r_1$ | $r_2$ | $r_3$ | $r_4$ | $r_5$ | $r_6$ |
|---|---|---|---|---|---|---|---|
| $E(x)$ | 1 | $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ |
| $S(x)$ | 1 | $x$ | $x^2$ | $x+1$ | $x^2+x$ | $x^2+x+1$ | $x^2+1$ |

若$R = (0110010)$，$R(x) = x^5+x^4+x$；

$S(x)$=（$x^5+x^4+x$）mod（$x^3+x+1$）= $x+1$；

查表知：$E(x) = x^3$；

于是：　$C(x) = R(x) + E(x) = x^5+x^4+x^3+x$；

即：　$C = (0111010)$；

# 提纲

- 循环码
- 常用分组码

# 汉明码（Hamming码）

- 是一种纠正单个错误的线性分组码。
- 特点：　码长　$n = 2^m-1$

  信息码位　$k = 2^m-m-1$

  监督码位　$r = n-k = m$

  最小码距　$d = 3$

  纠错能力　$t = 1$
- 扩展的汉明码：将监督码位由m增至m+1，信息位不变，这时最小码距增加到$d = 4$，能纠正1位错误同时检查出2位错误。

# 汉明码

**汉明码**：能纠正一个任一错误的具有参数

（n，k）＝（2ᵐ—1，2ᵐ—1—m）的线性分组码。

汉明码的特点：

- 码字的最小距离为3，能纠正单个的错误；
- 汉明码是一种完备码，对应 $2^{n-k}=\left[1+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}\right]$

$$2^{n-k}=2^{(2^m-1)-(2^m-1-m)}=2^m,\quad 而\left[1+\binom{n}{1}\right]=\left[1+\binom{2^m-1}{1}\right]=1+\left(2^m-1\right)=2^m$$

- 汉明码的编码效率 $\dfrac{k}{n}=\dfrac{2^m-1-m}{2^m-1}\xrightarrow{m\Rightarrow\infty}1$

# 汉明码

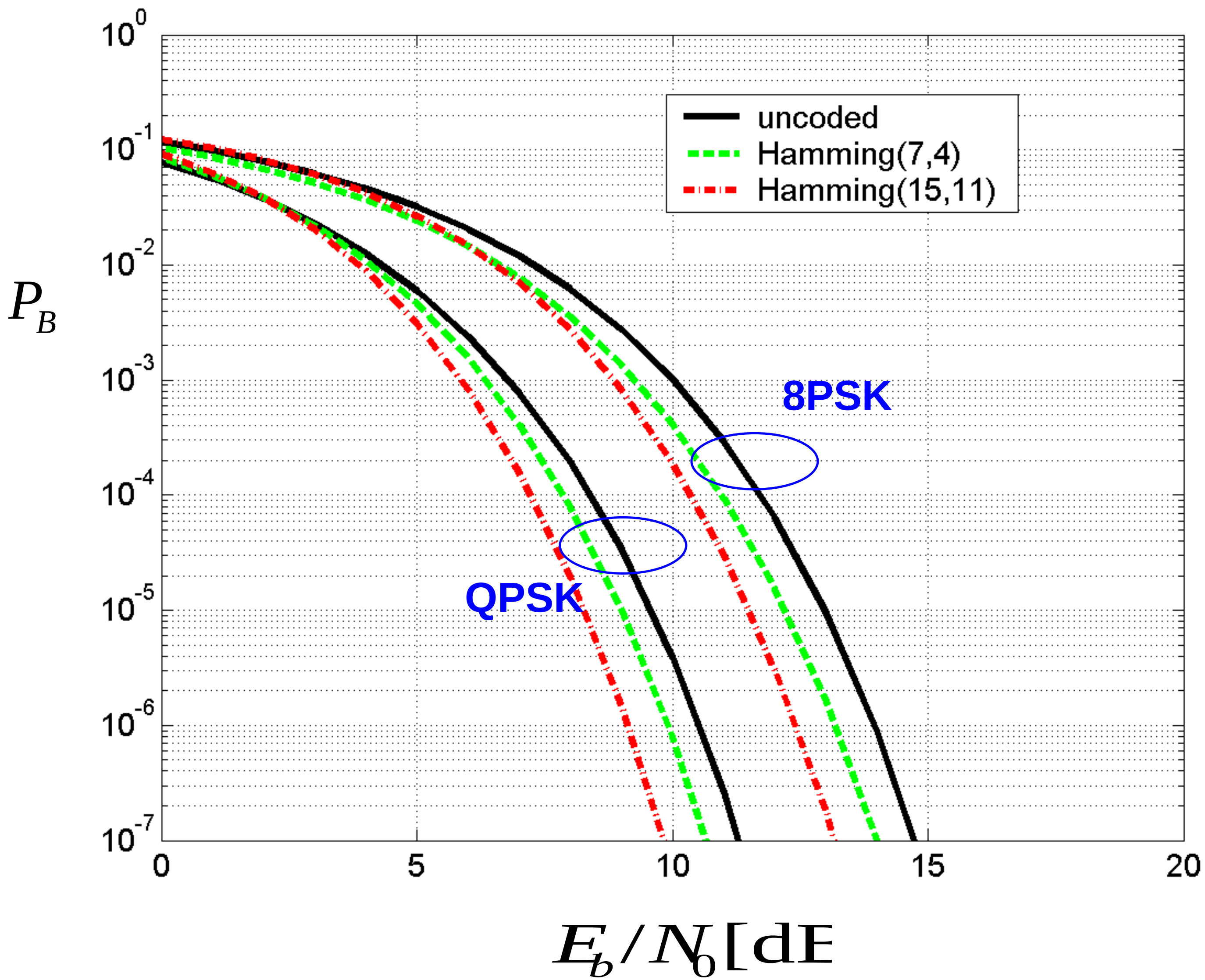
## 汉明码的误比特率

$$P_B \approx \frac{1}{n}\sum_{j=2}^{n} j\binom{n}{j} p^j(1-p)^{n-j} \approx p - p(1-p)^{n-1}$$

例，具有如下监督矩阵的线性分组码（7，4）是汉明码。

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

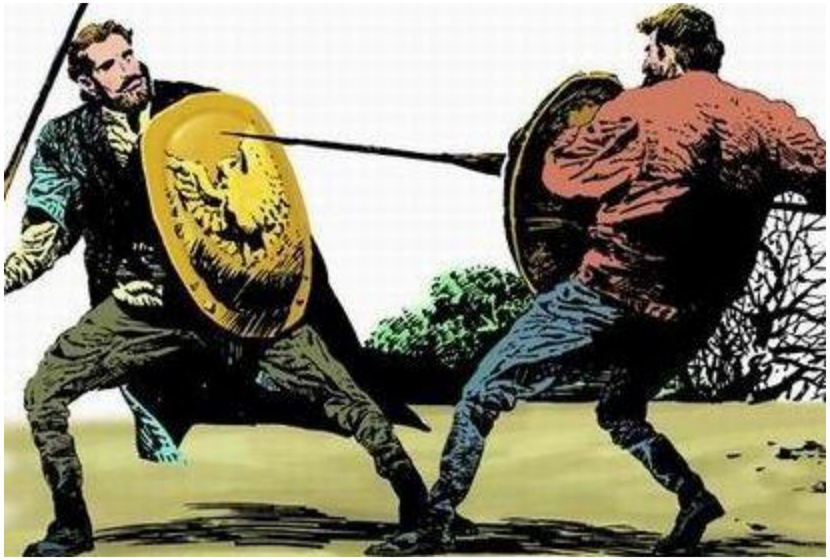
# 汉明码性能



uncoded
Hamming(7,4)
Hamming(15,11)
8PSK
QPSK
$P_B$
$E_b/N_0$[dB
$10^0$
$10^{-1}$
$10^{-2}$
$10^{-3}$
$10^{-4}$
$10^{-5}$
$10^{-6}$
$10^{-7}$
0
5
10
15
20

# 循环冗余校验码CRC产生背景

可靠性



快速性

**在数字通信系统中可靠与快速往往是矛盾的。**
**如何合理地解决可靠与速度这一对矛盾呢？**

# 循环冗余校验码(CRC)

- 循环冗余校验码是截短循环码的一个典型应用。
- 在数据通信和软盘、光盘存储器中，常常需要对较多信息（一个数据帧或一个记录轨道中的数据）进行差错监督。数据的长短往往不确定，但校验位的长度*r*却是固定的。
- 根据$n=2^r-1$设计出一个 $(n, k)$ 循环码后，当信息长度小于*k*时，只要同时截短信息位和码字的长度，而保持监督位不变，便得到一个$(n-i,\ k-i)$截短循环码，这就是循环冗余校验码（CRC）。

# CRC应用

CRC的主要特点

- 检错能力极强
- 开销很小
- 易于实现

**应用范围广**

1. ARJ,LHA,ZIP等压缩软件采用的是CRC-32;
2. GIF,TIFF等图像存储格式;
3. 所有链路层或网络接口层协议中，例如HDLC、DDCMP等众多领域。

# CRC原理

将待发送的位串看成系数为 0 或 1 的多项式；

例1： C = 1100101

$C(x) = 1x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 0x + 1$

$= x^6 + x^5 + x^2 + 1$

收发双方约定一个生成多项式 G(x)（其最高阶和最低阶系数必须为1），发送方用位串及 G(x) 进行某种运算得到校验和，并在帧的末尾加上校验和，使带校验和的帧的多项式能被 G(x) 整除；接收方收到后，用 G(x) 除多项式，若有余数，则传输有错。

# 循环冗余校验码(CRC)

- 常取 $r$ =16， 这时 $g(x) = x^{16}+x^{12}+x^5+1$

  =10001000000100001(B)=11021(H)

- $g(x)$作为最轻的码字，它的重量为4，表明该码组中最小汉明距离$d_0$= 4，能纠正1位差错同时还能检查到第2位差错。

- 例如信息为$K(x)$=4D6F746F(H) ，则可以在信息后面添上CRC监督码：$R(x)=x^{16}K(x) \bmod g(x)$ =

  =4D6F746F0000(H) mod 11021(H)= B944(H)

- 有时也取32位的CRC校验码，生成多项式为：

  $g(x)=(x^{16}+x^{15}+x^2+1)\cdot(x^{16}+x^2+x+1)$

# 生成多项式 G(x) 的国际标准

- CRC-8 : $x^8+x^2+x+1$
- CRC-10： $x^{10}+x^9+x^5+x^4+x^2+1$
- CRC-12： $x^{12}+x^{11}+x^3+x^2+x+1$
- CRC-16： $x^{16}+x^{15}+x^2+1$
- CRC-CCITT： $x^{16}+x^{12}+x^5+1$
- CRC-32： $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

# 循环冗余校验码(CRC)

- 循环冗余校验码不仅实现起来比较简单，而且具有很强的检测能力。它能检测出：

（1）绝大部分连续长度不大于$n$-$k$+1的突发错误。

（2）相当一部分连续长度大于$n$-$k$+1的突发错误。

（3）所有许用码字汉明距离不大于$d_0$-1的错误。

（4）所有奇数个错位。

- 当错位较少时，它能自动纠正，当差错超过纠错能力时，根据校验位很容易进行检错，采用重发反馈 (ARQ) 方式保证数据的正确性。

- 习题6.19，6.21