12. 循环码

目录

- 定义12.1: 若 $(v_0, v_1, \ldots, v_{n-1}) \in C$,

  有 $(v_{n-1}, v_0, \ldots, v_{n-2}) \in C$,

  则称线性分组码C为循环码.

- 循环码C的码字可以写作GF(q)上的多项式:

  $(v_0, v_1, \ldots, v_{n-1}) \rightarrow$

  $v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}$

  或 $v_{n-1} x^{n-1} + \ldots + v_1 x + v_0$

- 例： （7，4）循环Hamming Code

0000000

1010001 0100011 0110100 1000110 1101000 0011010 0001101

1110010 1100101 0010111 0111001 1001011 1011100 0101110

1111111

0

$1+x^2+x^6$ $x+x^5+x^6$ $x+x^2+x^4$ $1+x^4+x^5$ $1+x+x^3$ $x^2+x^3+x^5$ $x^3+x^4+x^6$

$1+x+x^2+x^5$ $1+x+x^4+x^6$ $x^2+x^4+x^5+x^6$ $x+x^2+x^3+x^6$

$1+x^3+x^5+x^6$ $1+x^3+x^5+x^6$ $x+x^3+x^4+x^5$

$1+x+x^2+x^3+x^4+x^5+x^6$

- 码字 $(v_0, v_1, \cdots, v_{n-1})$ 的i次循环移位 $(v_{n-i}, v_{n-i+1}, \cdots, v_{n-i-1})$ 可以表示为：

$$(v_0, v_1, \cdots, v_{n-1}) \rightarrow v(x),$$

$$(v_{n-i}, v_{n-i+1}, \cdots, v_{n-i-1}) \rightarrow v^{(i)}(x),$$

$$v^{(i)}(x) = x^i v(x) \bmod (x^n+1)$$

$$x^i v(x) = v^{(i)}(x) + q(x)(x^n+1)$$

$v_0, v_1, \cdots, v_{n-1}$

$v_0, v_1, \cdots, v_{n-1}$

$v_{n-i}, v_{n-i+1}, \cdots, v_{n-i-1}$

例： $1010001 \rightarrow$ 循环移位6次$\rightarrow 0100011$

$$[x^6(1+x^2+x^6)] \bmod (x^7+1) = x+x^5+x^6$$

目录

- 数学描述
- 生成多项式和校验多项式
- 生成矩阵和校验矩阵
- 编码电路
- 译码电路
- 常见的循环码

- **生成多项式g(x)**

定义12.2: 循环码C中阶次最低、最高次项系数为1的码多项式称为生成多项式g(x).

g(x)中常数项是非零的, 即$g_0 \neq 0$.

例: (7, 4)循环Hamming Code, $g(x)= 1+x+x^3$

- **生成多项式g(x)**

定理12.1:循环码的生成多项式$g(x)$是唯一的.

定理12.2: 设$g(x)$是循环码C的生成多项式, 码多项式$v(x) \in C$的充要条件是 $g(x) \mid v(x)$.

- **生成多项式g(x)**

定理12.2证明:

充分性: 若$g(x) \mid v(x)$,

$v(x) = q(x)\, g(x) = (q_{k-1}\, x^{k-1} + \ldots + q_1\, x + q_0)\, g(x)$,

由循环码的定义和线性码性质可知,

$v(x)$必为循环码C的码多项式.

必要性: 若$v(x) \in C$, 而$g(x) \mid v(x)$不成立,

有$v(x) = q(x)g(x) + r(x)$, $\deg[r(x)] < \deg[g(x)]$

由于$v(x), g(x) \in C$, $q(x)g(x) \in C$, 有$r(x) \in C$

这与$g(x)$ 定义相矛盾,

因此必有$g(x) \mid v(x)$.

- **生成多项式g(x)**

定理12.3: 设$g(x)$是码长为n的循环码C的生成多项式,

则$g(x) \mid x^n+1$.

证明: 由 $v(x) \in C$, $v^{(i)}(x) \in C$

有 $g(x) \mid v(x)$, $g(x) \mid v^{(i)}(x)$

而$v^{(i)}(x) + q(x)(x^n+1) = x^i\, v(x)$

则有 $g(x) \mid x^n+1$

- **生成多项式g(x)**

定理12.4: g(x)是 (n, k) 循环码C的生成多项式,

则 deg[g(x)] = n-k

v(x)=u(x)·g(x)

u(x)—信息多项式

deg[u(x)]≤k-1

- **校验多项式h(x)**

定义12.3: 校验多项式$h(x) = (x^n+1)/g(x)$

性质(1)：校验多项式的阶次：

由 $g(x)h(x)=x^n+1$

$\deg[g(x)] = n-k$

有 $\deg[h(x)] = k$

- 例： (7, 4) 循环Hamming Code：

$g(x) = x^3 + x + 1$

$h(x) = (x^7+1) / g(x) = x^4 + x^2 + x + 1$

- **校验多项式h(x)**

性质(2)：码多项式v(x)系数的递推关系：

若v(x) ∈ C

则 v(x) h(x) = u(x) g(x) h(x)

= u(x) (x^n+1)

展开式中i次项系数为零

i = k, k+1, …n-1 共 n-k 项

即 $\sum_{j=0}^{k} h_j v_{i-j} = 0 \quad i = k, k+1, \cdots, n-1$

目录

- 数学描述
- 生成多项式和校验多项式
- 生成矩阵和校验矩阵
- 编码电路
- 译码电路
- 常见的循环码

- 系统码生成矩阵

$$\mathbf{G}=\begin{bmatrix} r_{0,0} & r_{0,1} & \cdots & r_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ r_{1,0} & r_{1,1} & \cdots & r_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ & & \cdots & & & & \cdots & \\ r_{k-1,0} & r_{k-1,1} & \cdots & r_{k-1,n-k-1} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

其中 $r_i(x)=\sum_{j=0}^{n-k-1} r_{i,j}x^j$ 是g(x)除x^{n-k+i}所得余式.

- **系统码生成矩阵**

例: (7, 4)循环Hamming Code

$$g(x) = 1 + x + x^3$$

$$x^3 \bmod (1 + x + x^3) = 1 + x$$

$$x^4 \bmod (1 + x + x^3) = x + x^2$$

$$x^5 \bmod (1 + x + x^3) = 1 + x + x^2$$

$$x^6 \bmod (1 + x + x^3) = 1 + x^2$$

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

- 系统码校验矩阵

$$\mathbf{H}=\begin{bmatrix} 1 & 0 & \cdots & 0 & r_{0,0} & r_{1,0} & \cdots & r_{k-1,0} \\ 0 & 1 & \cdots & 0 & r_{0,1} & r_{1,1} & \cdots & r_{k-1,1} \\ & & \cdots & & & & \cdots & \\ 0 & 0 & \cdots & 1 & r_{0,n-k-1} & r_{1,n-k-1} & \cdots & r_{k-1,n-k-1} \end{bmatrix}$$

- **系统码校验矩阵**

例: (7, 4)循环Hamming Code

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

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

- 由g(x)构成的生成矩阵

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & & \\ & g_0 & g_1 & \cdots & g_{n-k} & \\ & & \cdots & & & \cdots \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

生成多项式g(x)为：

$$g(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_1 x + g_0$$

- **由g(x)构成的生成矩阵**

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & & \\ & g_0 & g_1 & \cdots & g_{n-k} & \\ & & \cdots & & \cdots & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix} \Rightarrow \begin{bmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{bmatrix}$$

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G}$$

$$\Rightarrow \begin{pmatrix} u_0 & u_1 & \ldots & u_{k-1} \end{pmatrix} \cdot \begin{pmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{pmatrix}$$

$$= u_0 g(X) + u_1 X g(X) + \cdots u_{k-1} X^{k-1} g(X)$$

$$= u(X) \cdot g(X)$$

- **由g(x)构成的生成矩阵**

  例: (7, 4)循环Hamming Code

  $g(x) = 1 + x + x^3$

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

- **由h(x)构成的校验矩阵**

$$\mathbf{H}=\begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & & \\ & h_k & h_{k-1} & \cdots & h_0 & \\ & & \cdots & & & \cdots \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

校验多项式h(x)为：

$$h(x)=h_k x^k+h_{k-1}x^{k-1}+\cdots+h_1 x+h_0$$

$$\mathrm{H}\cdot\mathrm{G}=0$$

$$h(x)\cdot g(x)=x^n+1$$

- **由h(x)构成的校验矩阵**

例: (7, 4)循环Hamming Code

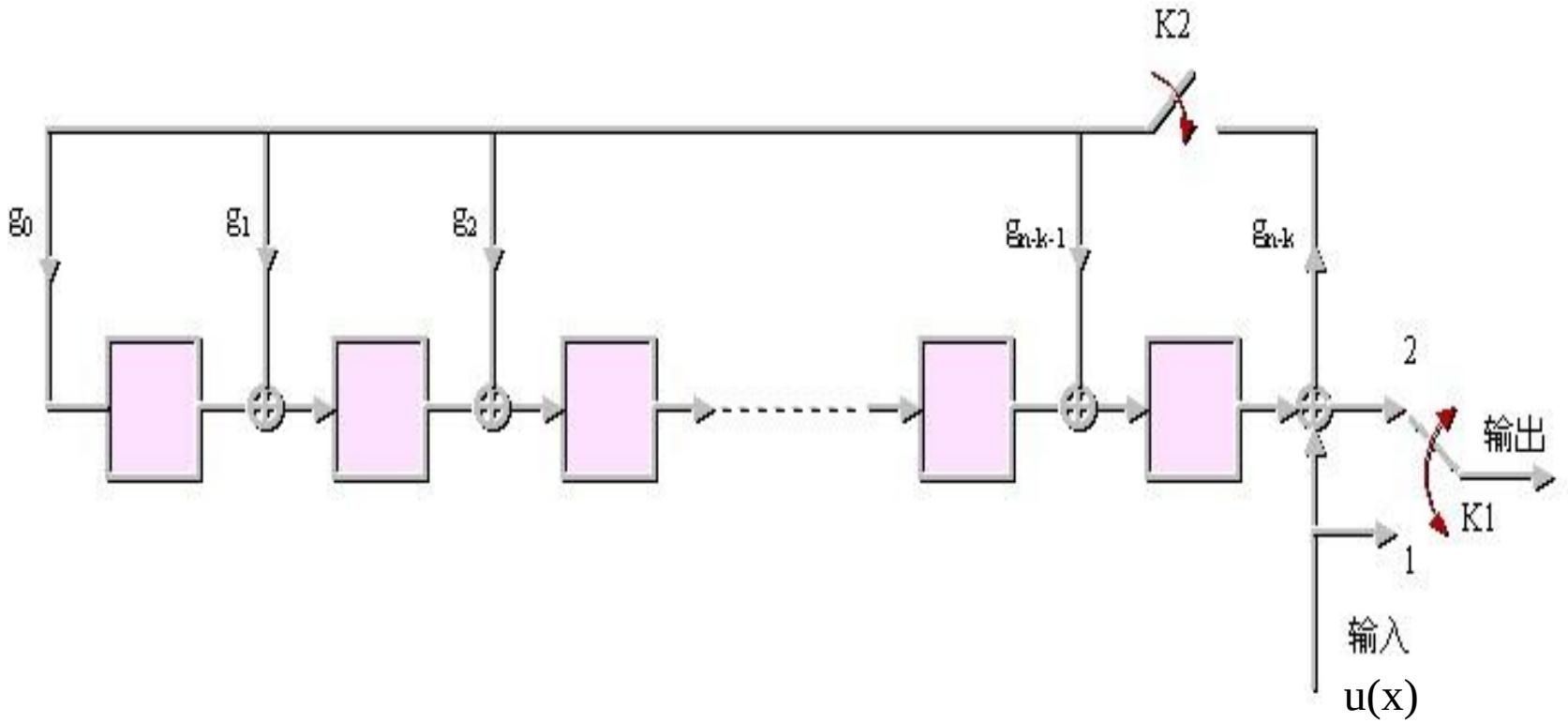
$$h(x) = (x^7+1) / g(x) = x^4 + x^2 + x + 1$$

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

目录

- 数学描述
- 生成多项式和校验多项式
- 生成矩阵和校验矩阵
- 编码电路
- 译码电路
- 常见的循环码

- 按g(x)构造的系统码编码电路



- **按g(x)构造系统码编码电路**
  - 输入信息多项式u(x)，编码器循环反馈移位并同时输出
  - 经过k拍后，在移位寄存器中得到n-k位余式系数，对应码字多项式v(x)的低n-k项系数
  - 停止输入，经过n-k拍输出移位寄存器中的n-k位余式系数
  - 完成k位信息的编码，输出n位编码码字

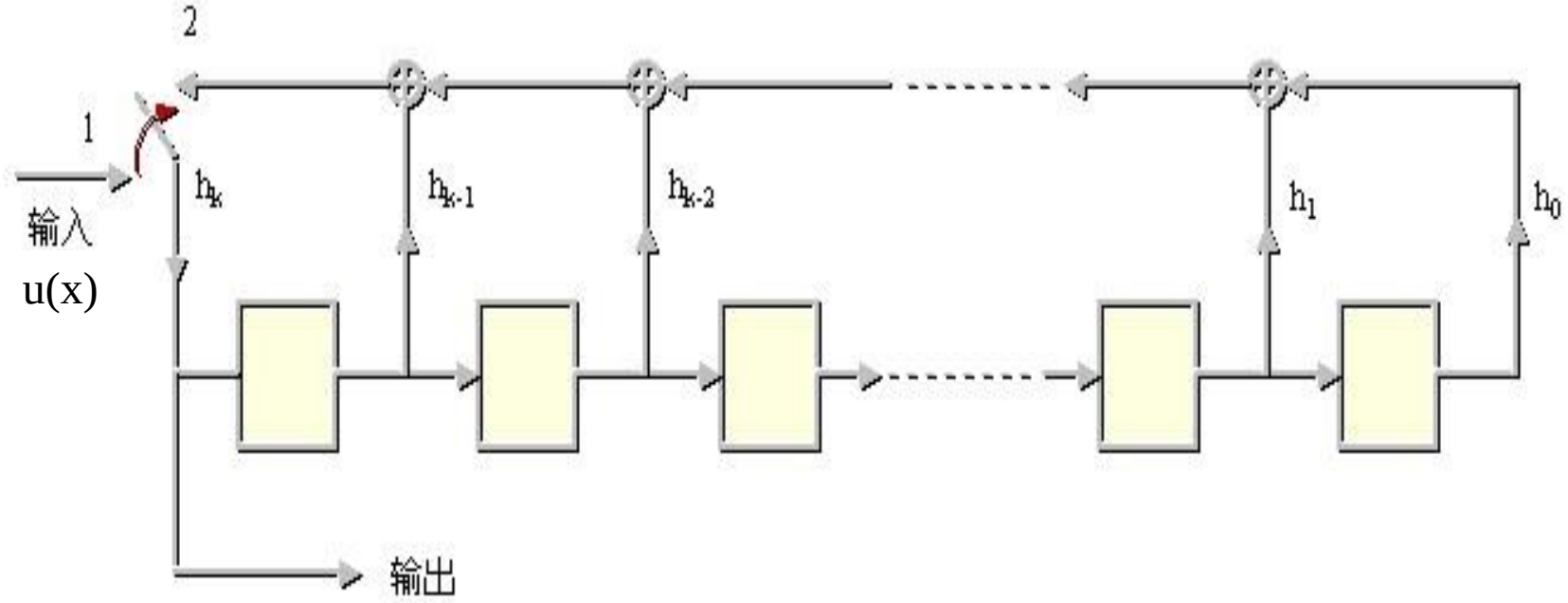
- **按h(x)构造系统码编码电路**

根据递推公式 $\sum_{j=0}^{k} h_j v_{i-j} = 0 \quad i = k, k+1, \cdots, n-1$

因为$h_k = 1$, $v_{i-k} = \sum_{j=0}^{k-1} h_j v_{i-j} \quad i = k, k+1, \cdots, n-1$

即
$$\begin{aligned} v_{n-k-1} &= h_0 v_{n-1} + h_1 v_{n-2} + \cdots + h_{k-1} v_{n-k} \\ &= h_0 u_{k-1} + h_1 u_{k-2} + \cdots + h_{k-1} u_0 \\ v_{n-k-2} &= h_0 v_{n-2} + h_1 v_{n-3} + \cdots + h_{k-1} v_{n-k-1} \\ &\vdots \\ v_0 &= h_0 v_k + h_1 v_{k-1} + \cdots + h_{k-1} v_1 \end{aligned}$$

- 按h(x)构造系统码编码电路



- **按h(x)构造系统码编码电路**
  - 输入的信息多项式u(x)在全部移入寄存器的同时输出
  - 经k拍移位后，再断开输入并接通反馈开关
  - 经过n-k拍的循环反馈移位，得到并输出码字多项式v(x)的后n-k位系数（校验位）

上述的编码电路也可以用来计算相应**H**矩阵的伴随式.

- **系统码编码电路举例**

例：（7，4）循环Hamming Code

$g(x) = x^3 + x + 1$

$h(x) = (x^7 + 1) / (x^3 + x + 1) = x^4 + x^2 + x + 1$

设信息矢量 $\mathbf{u} = (1\ 0\ 1\ 1)$

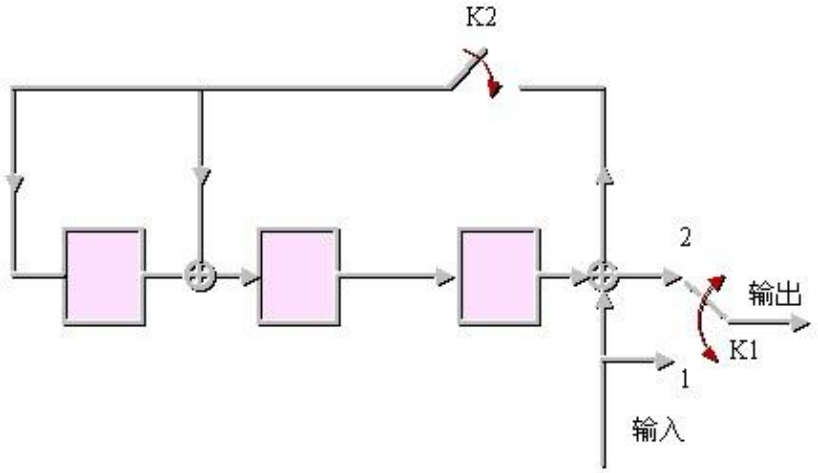
用$g(x)$去除$u(x) \cdot x^{n-k} = (1 + x^2 + x^3) \cdot x^{n-k}$

得余式 $r(x) = 1$

编码码字：$v(x) = u(x) \cdot x^{n-k} + r(x) = 1+x^3+x^5+x^6$

$\mathbf{v} = (1\ 0\ 0\ 1\ 0\ 1\ 1)$

- 例(cont.):

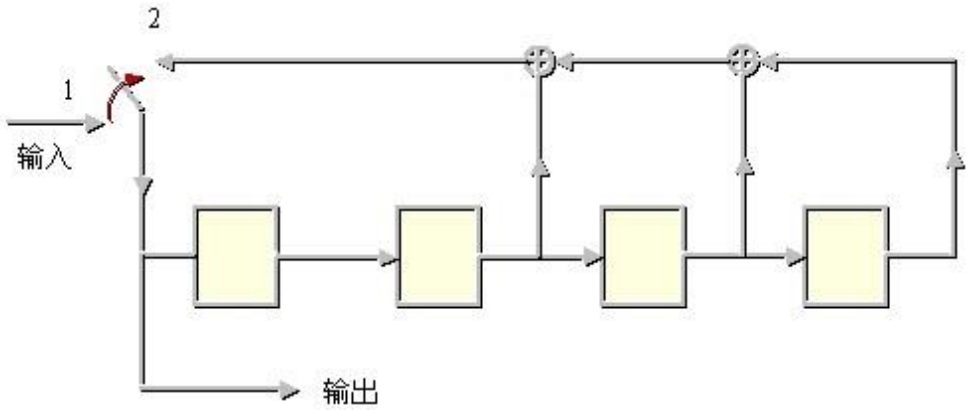


前4拍：K1在位置1，K2闭合

后3拍：K1在位置2，K2打开

输入	反馈	移存器内容	输出
		0 0 0	
1	1	1 1 0	1
1	1	1 0 1	1
0	1	1 0 0	0
1	1	1 0 0	1
			0
			0
			1

- **例(cont.)：**



根据差分方程

$$v_{3-i} = 1\times\ v_{7-i} + 1 \times\ v_{6-i} + 1 \times\ v_{5-i} + 0 \times\ v_{4-i} \qquad i = 1, 2, 3$$

由 $\mathbf{u} = (1\ 0\ 1\ 1)$，得 $v_3 = 1,\ v_4 = 0,\ v_5 = 1, v_6 = 1$

$$v_2 = v_6 + v_5 + v_4 = 0$$

$$v_1 = v_5 + v_4 + v_3 = 0$$

$$v_0 = v_4 + v_3 + v_2 = 1$$

$\mathbf{v} = (1\ 0\ 0\ 1\ 0\ 1\ 1)$

目录

- 数学描述
- 生成多项式和校验多项式
- 生成矩阵和校验矩阵
- 编码电路
- 译码电路
- 常见的循环码

- **译码步骤**

  (1) 计算伴随多项式 s(x)

  (2) 由s(x)确定错误图案多项式 e(x)

  (3) 输出 $\hat{v}(x) = r(x) - e(x)$

- **伴随多项式**

  按$g(x)$构造的伴随多项式:

  若$v(x) \in$循环码C, 则$g(x) \mid v(x)$

  定义接收多项式$r(x)$的伴随多项式

  $$s(x) \equiv r(x) \bmod g(x)$$

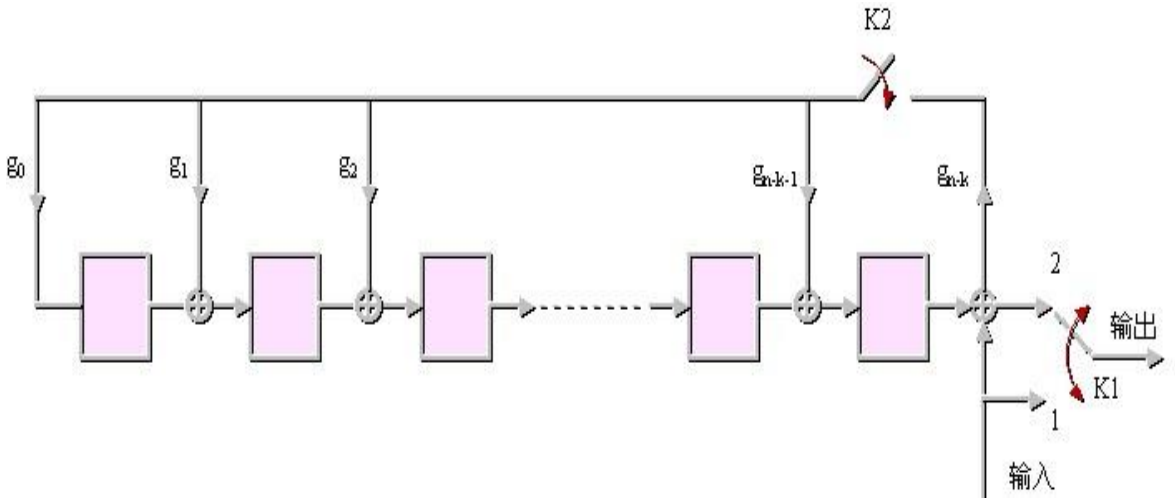
  $$\deg[s(x)] \leq n-k-1$$

- **伴随多项式**

性质1：在以g(x)为除式的除法电路中，输入 r(x)做n次循环反馈移位后相当于

$r(x) \bmod g(x)$　　若r(x) 从最低位（左侧）输入

$r(x)\cdot x^{n-k} \bmod g(x)$　　若r(x) 从最高位（右侧）输入



- **伴随多项式**

性质2：g(x)除法电路中寄存的 $s(x) = r(x) \bmod g(x)$ 作一次循环反馈移位得到

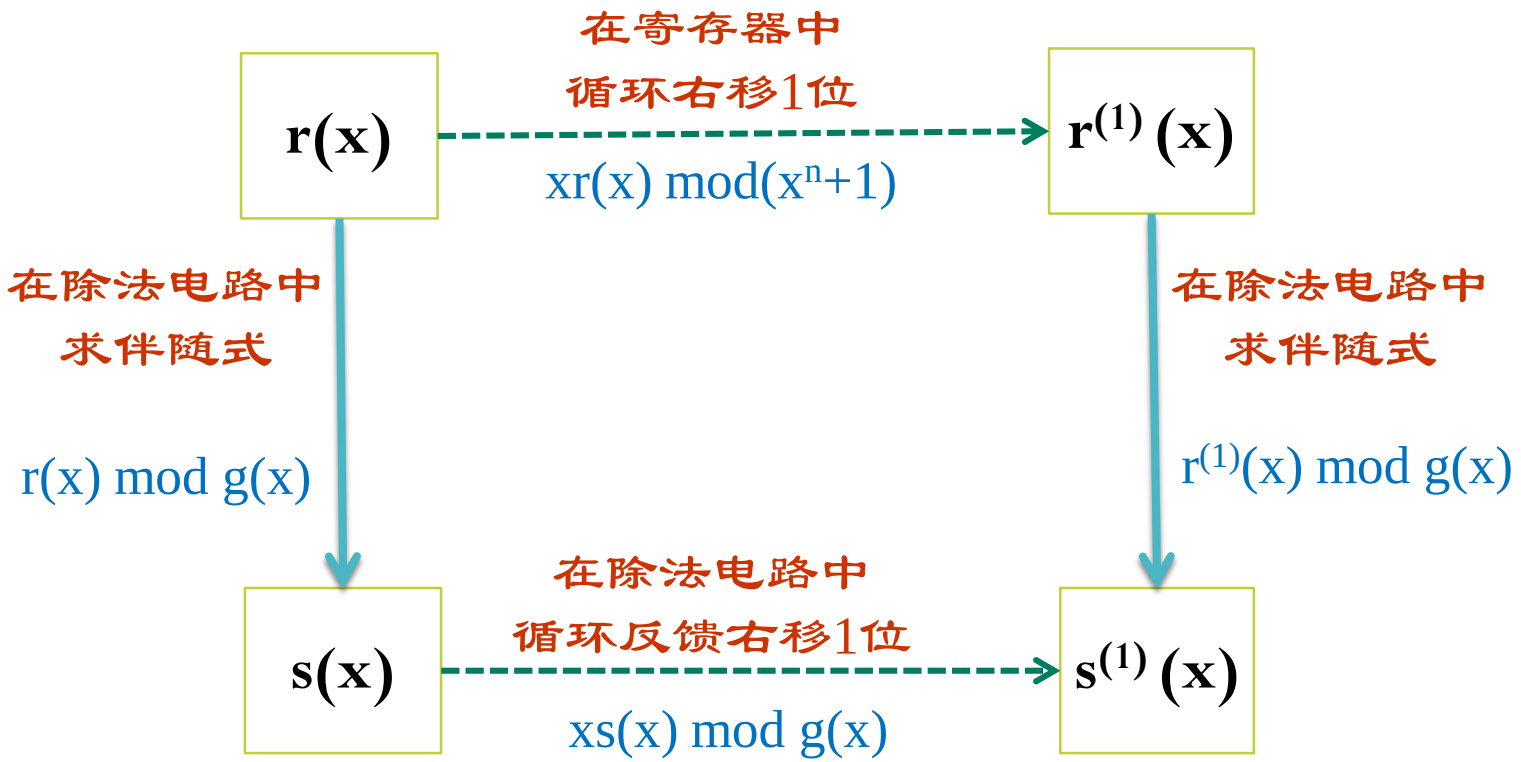
$$s^{(1)}(x) = x\, s(x) \bmod g(x)$$

$$= x\, r(x) \bmod g(x) = r^{(1)}(x) \bmod g(x)$$

其中$r^{(1)}(x)$为r(x)的一次循环移位.

$$\mathbf{x^i v(x) = v^{(i)}(x) + q(x)(x^n+1)}$$

- 伴随多项式

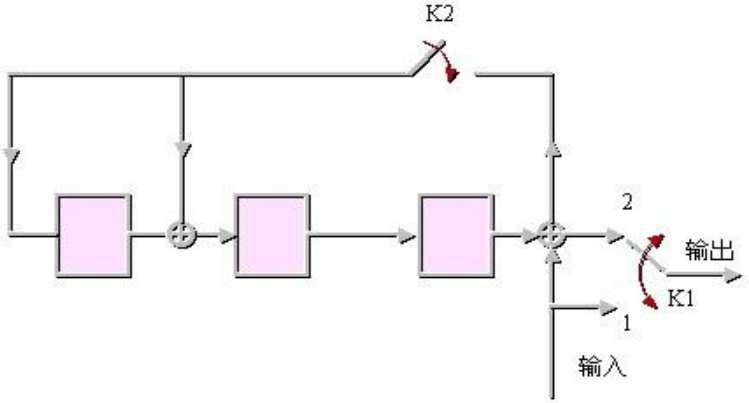

在寄存器中
循环右移1位
r(x)
xr(x) mod(x^n+1)
r^(1) (x)
在除法电路中
求伴随式
r(x) mod g(x)
在除法电路中
求伴随式
r^(1)(x) mod g(x)
在除法电路中
循环反馈右移1位
s(x)
xs(x) mod g(x)
s^(1) (x)

- **捕获错误图案**

  循环移位等价的错误图案多项式，

  其伴随多项式也可通过循环反馈移位得到，

  简化了 $s(x) \rightarrow e(x)$ 的计算.



- **捕获错误图案**

例：

错误图样	伴随式 S(X)	(S_0, S_1, S_2)
$e_6(x)=x^6$	$1+x^2$	(1 0 1)
$e_5(x)=x^5$	$1+x+x^2$	(1 1 1)
$e_4(x)=x^4$	$x+x^2$	(0 1 1)
$e_3(x)=x^3$	$1+x$	(1 1 0)
$e_2(x)=x^2$	x^2	(0 0 1)
$e_1(x)=x^1$	x	(0 1 0)
$e_0(x)=x^0$	1	(1 0 0)

- **捕获错误图案**
  - 如果循环码能纠正单个错误,

若$s(x)=0$，　则$e(x)=0$；

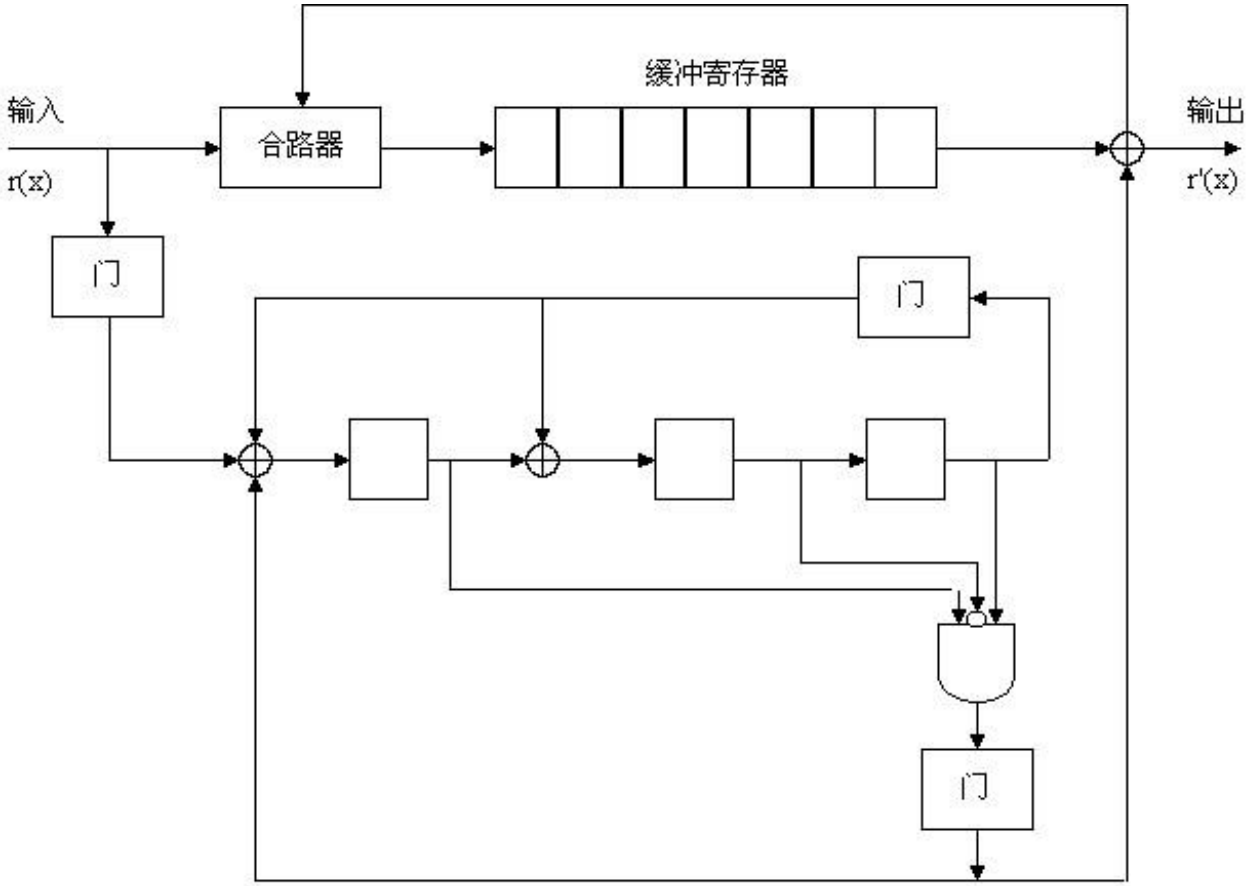
若$s(x)\neq 0$, 已知$e_{n-1}(x)=x^{n-1}$对应的$s_{n-1}(x)$

　　如果某个错误图案$e(x)$对应的伴随式$s(x)$循环反馈移位i次后，$s^{(i)}(x)=s_{n-1}(x)$，

　　则相应的单个错误发生在$(n-1-i)_{\bmod n}$位上.

- **译码电路举例**

例：（7,4）循环汉明码



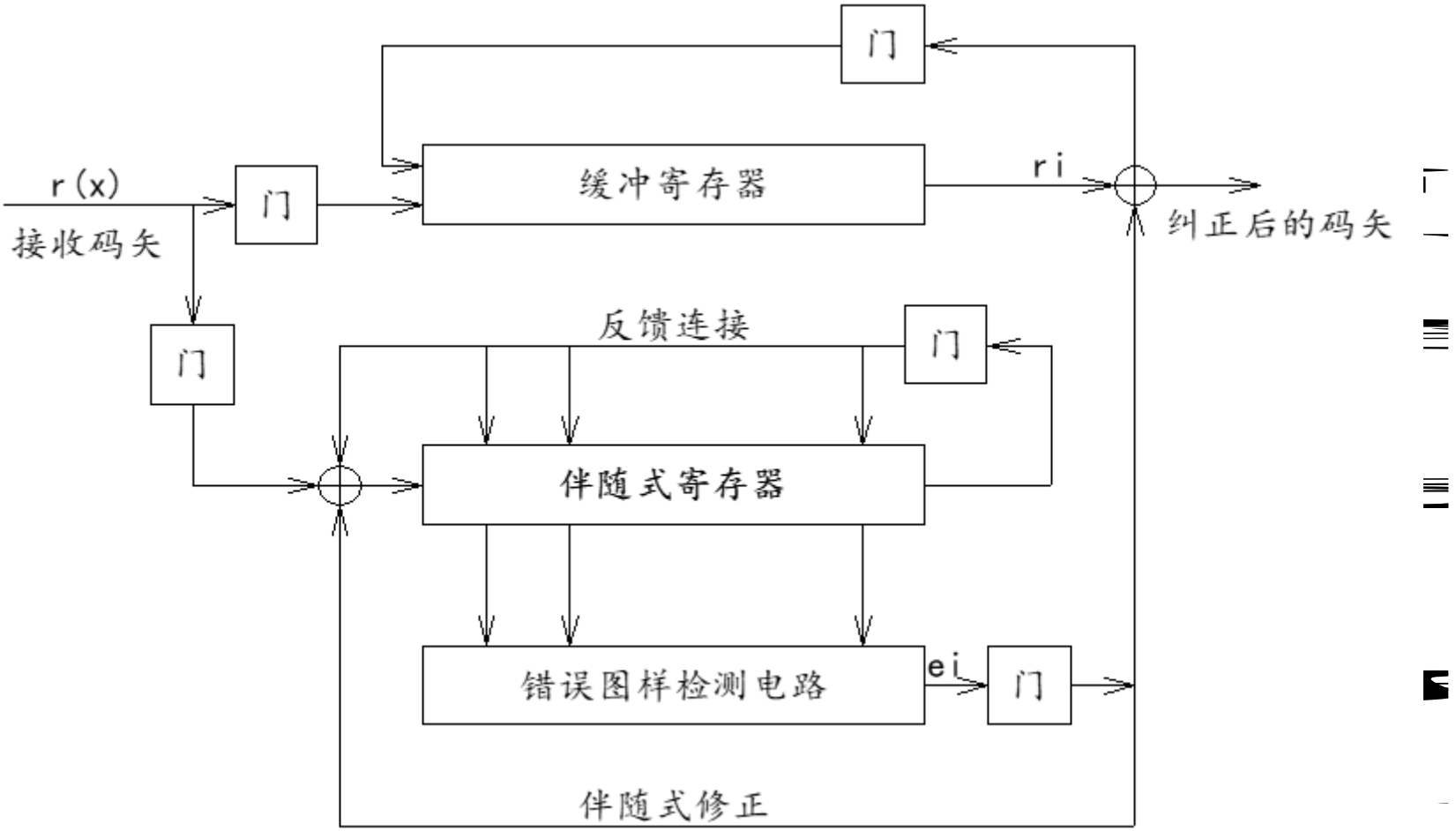
- **译码电路举例**

例：设发码 $\mathbf{v}=(1001011)$，$v(x)=1+x^3+x^5+x^6$

收码 $\mathbf{r}=(1011011)$，$r(x)=1+x^2+x^3+x^5+x^6$

	伴随式寄存器	缓冲寄存器	纠错
经过7拍移位后	0 0 1	1 0 1 1 0 1 1	0
第1次移位	1 1 0	1 1 0 1 1 0 1	0
第2次移位	0 1 1	1 1 1 0 1 1 0	0
第3次移位	1 1 1	0 1 1 1 0 1 1	0
第4次移位	1 0 1	1 0 1 1 1 0 1	1
第5次移位	0 0 0	0 1 0 1 1 1 0	0
第6次移位	0 0 0	0 0 1 0 1 1 1	0
第7次移位	0 0 0	1 0 0 1 0 1 1	0

- “捕获”译码电路基本结构



目录

- 数学描述
- 生成多项式 和校验多项式
- 生成矩阵和校验矩阵
- 编码电路
- 译码电路
- 常见的循环码

- **循环Hamming Code**
  - 主要参数

    码长 $n = 2^m-1$

    信息位数 $k = 2^m-1-m$

    生成多项式是GF(2)上m次本原多项式

  - 例： (7, 4) 循环Hamming Code：

    $g(x) = x^3 + x + 1$，

    $h(x) = (x^7+1) / g(x) = x^4 + x^2 + x + 1$

- **循环Golay 码**

（23，12）循环Golay码的生成多项式为：

$$g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

码间最小距离 $d_{min} = 7$

重　　量	码字数目 （23，12）码	码字数目 （24，12）码
0	1	1
7	253	0
8	506	759
11	1288	0
12	1288	2576
15	506	0
16	253	759
23	1	0
24	0	1

- **极长码**
  - 定义14.2: 对于任意整数 $m \geq 3$, 都存在具有下列参数的极长码:

    码长: $n = 2^m - 1$

    信息位: $k = m$

    最小距离: $d = 2^{m-1}$

    生成多项式: $g(x) = (x^n+1)/p(x)$

    p(x)是m阶本原多项式

    极长码由一个全零码字和$2^m - 1$个重量为2^{m-1} 的码字组成

- **极长码**
  - 极长码的对偶码
    - 极长码的校验多项式p(x)是m次本原多项式
    - 以 $p^*(x) = x^m p(x^{-1})$

      为生成多项式可生成一个$(2^m-1, 2^m-m-1)$循环汉明码
      - $(2^m-1, m)$极长码的对偶码是$(2^m-1, 2^m-m-1)$循环汉明码

- 极长码

$$\mathbf{G}=\begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & & \\ & g_0 & g_1 & \cdots & g_{n-k} & \\ & & \cdots & & & \cdots \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

$$\mathbf{G}^{\perp}=\begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & & \\ & h_k & h_{k-1} & \cdots & h_0 & \\ & & \cdots & & & \cdots \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

$$\mathbf{H}=\begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & & \\ & h_k & h_{k-1} & \cdots & h_0 & \\ & & \cdots & & & \cdots \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

$$g^{\perp}(x) = h_0 x^k + h_1 x^{k-1} + \cdots + h_{k-1} x + h_k$$
$$== x^k h(x^{-1}) = h^*(x)$$

$$h(x) = h_k x^k + h_{k-1} x^{k-1} + \cdots + h_1 x + h_0$$

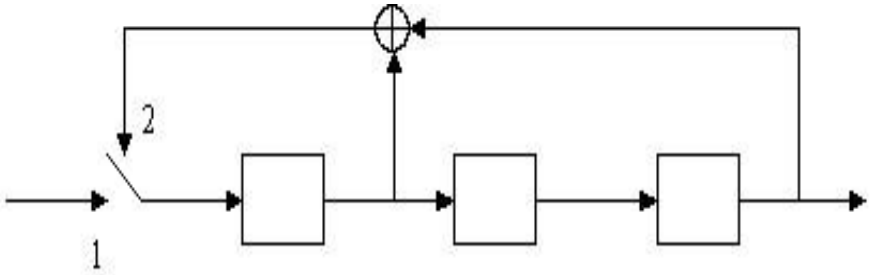
	循环码C	对偶码$C^{\perp}$
生成矩阵	**G**	$\mathbf{G}^{\perp}=\mathbf{H}$
校验矩阵	**H**	$\mathbf{H}^{\perp}=\mathbf{G}$
生成多项式	g(x)	$g^{\perp}(x)=h^{*}(x)$
校验多项式	h(x)	$h^{\perp}(x)=g^{*}(x)$
举例	循环汉明码 $n=2^{m}-1$ $k=2^{m}-m-1$ 生成多项式为m次本元多项式	极长码 $n=2^{m}-1$ $k=m$ 校验多项式为m次本元多项式

- **极长码**
  - 编码器：由 h(x)构造的m级循环反馈移位寄存器
  - 应用：用作PN码，应用于扰码及扩展频谱信号的产生

- **极长码**

例： （7，3）极长码，m=3

取$h(x) = x^3 + x^2 + 1$



	移存器内容			输出
初值	1	0	0	-
1	1	1	0	0
2	1	1	1	1
3	0	1	1	1
4	1	0	1	1
5	0	1	0	0
6	0	0	1	1
7	1	0	0	0

作业

- 习题12.1，12.2，12.3，12.8