来南开实验室大概有两个月了，中途回去跑回去休息不少，马上就要回家，想一想总结来这里的收获吧。这一阶段主要是编码相关的，了解了编码用到的有限域，生成矩阵，校验矩阵等等

# 编码

熟悉了添加冗余来修正突发的错误

了解了几种码的构造，比如说BCH和Hamming和RS码

两个等长码组之间相应位取值不同的数目称为这两个码组的汉明距离（Hamming Distance），简称码距。记为d(c1,c2),可得d(c1,c2)=w(c1-c2);

码组集中任意两个码字之间距离的最小值称为最小码距（dmin），它关系着这种编码的检错和纠错能力。

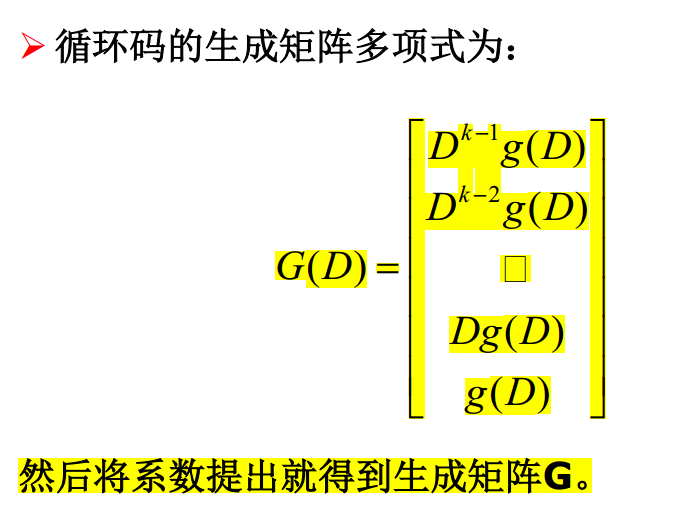
 为检测出e个错码， dmin >= e + 1

 为纠正t个错码，dmin >= 2 \* t + 1

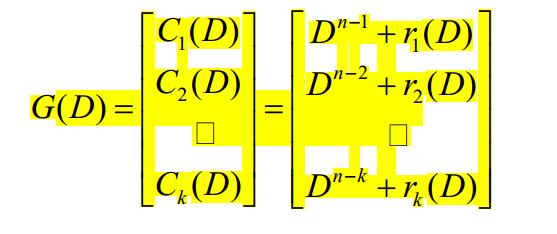
 为检测出e个错码,同时纠正t个错码，dmin >= e + t + 1 且 e >= t

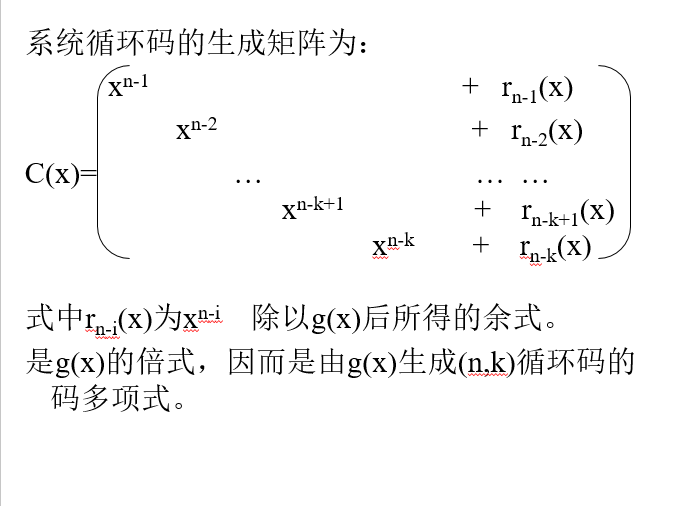
## 循环码

**循环码的非系统矩阵为：**



**由于典型生成矩阵**G = [Ik Q]**形式，与单位矩阵**Ik**每行对应的信息多项式为：**  
Dn-kmi(D)=Dn-kDk-i =Dn-i **，** i**＝**1,2,…,k  
ri(D) = Dn-i mod g(D)  
**由此得到生成矩阵中每行的码生成多项式为：**  
Ci(D) = Dn-i + ri(D), i = 1,2,…,k  
**这样系统循环码生成矩阵多项式的一般表示式为**





## BCH码

构造方式：用构造循环码的方式来构造。

**其中生成多项式为：g(x)=LCM[m1(x),m3(x),…,m2t-1(x)]**

**其中LCM表示最小公倍式， t为纠错个数， mi(x)为素多项式，**

**则由此生成的循环码称为BCH码， 其最小码距d≥d0=2t+1**

**(d0称为设计码距)， 它能纠正t个随机独立差错**

**GF(2m) = {0,a0,a1,a2,。。。,a2m -2} 如GF(23) 可映射为7个元素{ai}和一个0元素**

**P(x)的根 然后即为 a, 通过a^i 生成元素**

**(n,k) 循环码的生成多项式 g(x) 是 (xn+1)的因式，即 xn+1=h(x)•g(x)。**

**对一个分组长度**n=pm-1**、确定可纠**t**个错误的**BCH**码的生成**  
**多项式的步骤：**  
1. **选取一个次数为**m**的素多项式并构造**GF(pm)  
2. **求**ai,i=0,1,2,…n-2**的极小多项式**fi(x)  
3. **可纠**t**个错误的码的生成多项式为**  
g(x)=LCM[f1(x),f2(x),…,f2t(x)]  
**用这种方法设计的码至少能纠**t**个错误， 在很多情况下，这些码能纠多于**t**个错误！！ 因此**d=2t+1**称为码的设计距离，其最小距离**d\*≥ 2t+1**。 注意：一旦确定了**n**和**t**，我们便可以确定**BCH**码的生成多项式**

令ß是GF(2m)中的一个元素，某个形成循环周期并对ß的所有根均满足m(ß)=0的最低多项式m(x),称为ß的最小多项式。

这个最小多项式是既约的。而且根据(6-3)可知，当ß为m(x)的根时， ß2, ß4，ß8，…也比是m(x)的根。

以GF(24)为例，当有根ß＝a时,则a,a2,a2\*2=a4, a2\*3=a8,均为根(a2^4=a16 =a不是新根)。因此，包括全部根的最小多项式为

mi(x)=(x+a)(x+a2) (x+a4) (x+a8)

=x4+ x3 (a+a2 +a4 +a8)+ x2(a3 +a5+a9 +a6+a10 +a12)

+x(a14 +a13+a11 +a7) +a15

**当ß＝a**3 **时，则ß**2**＝ a**6 **， ß**4**＝ a**12**， ß8＝ a**24 **＝ a**9 **，均为根(ß**2^4**＝ a**48 **＝ a**3 **不是新根)。因此，类似地得到**

**m3(x)=(x+a**3**) (x+a**5**) (x+a**9**) (x+a**12**)=x**4**+ x**3 **+ x**2 **+x+1**

**同理ß＝a**5 **时，则ß**2**＝ a**10 **也为根(ß**4**＝ a5 \* 4 ＝ a5 不是新根)。因此m5(x)=(x+a5) (x+a10) = x2 +x+1**

**由于x16 +1＝(x+1)(x2 +x+1)(x4++x+1)(x4+ x3 +1)(x4+ x3 + x2 +x+1)**

**所以m1(x)， m3(x)， m5(x)都是x15 +1＝ x2^4-1 +1的一个既约因式。**

## RS码

**R S(255，223)中，G F(2m ) =G F(28)表示域中有 256 个元素，除 0 ，1 之外 的 254 个元 素 由本原多项式P (x)生成。本原多项式P (x)的特性(X2 ^m - 1 + 1 )/P(x)是得到的余式等于0.**

**R S (N，K )的性质符号的大小， 如 m = 8 表示符号由8位二进制数组成；**

**N 表示码块长度；**

**K 表示码块中的信息长度；**

**k=N - K = 2t 表示校验码的符号数；**

**t 表示能够纠正的错误数目。**

**Eg：t= 2**

**G (x ) = (x – a0 ) (x – a1 ) (x – a2 ) (x – a3 )**

**求（7,3,5）RS码的生成矩阵**

**N = 7, k = 3, -> t = 2; N = 2 m – 1 -> m = 3 -> GF(2^3) –> 即a属于GF（2^3）**

**本原多项式为P(x) = x ^ 3 + x + 1**

**a为P(x)的根 P(a) = a^3 + a + 1 = 0 -> 推出域中的全部元素**

**g（x） = (x – a0 ) (x – a1 ) (x – a2 ) (x – a3 ) = x ^ 4 + a3x3 + x2 + ax + a3;**

**G =[ ] -> 在有限域中换成真实的数即可**

**常常用做 纠删码 而不是 纠错码**

## Hamming码

**Hamming码具有纠一检二的特性**

**设数据位数为m，校验位数为k，则总编码位数为n，所以，n＝m+k，则，**

**有Hamming不等式：**

**2^k-1>=n**

**也可表示为：2^k>=m+k+1，该不等式用于对比运算计算数据位数和检验位数，举个例子假设数据位为64，那么校验位则为（"2^k-k>=65" =>k=7）。**

**校验位数一般指最小值，因为k越小总信息位会越小，传输开销越小。**