男			
	食物名称及数量	替换项	备注
早餐	燕麦片 30g	玉米（带棒） 80g 红薯 100g 紫薯 70g 豆类（干豆重30g）	早起摄入升糖指数较低的食物，可维持较好的精神状态。
	纯牛奶 250ml	酸奶 200ml 豆浆 250ml	牛奶选择配料只有生牛乳的，酸奶选择配料少的、无糖的（如如实），豆浆选无糖或自榨。若喝咖啡需要加奶，需把早餐的奶算进去。喝纯黑咖啡、手冲或挂耳，根据个人对咖啡因的耐受而选择适当的量，一般不建议超过 3 个 shot
	鸡蛋 2个	鸡胸肉 100g	
	绿叶蔬菜 200g	生菜/菠菜/芥蓝/黄瓜等	可加椰子油炒熟食用
午餐	糙米杂粮饭 250g	意面（生）70g 红薯 400g 紫薯 200g 大南瓜 400g 玉米（带棒）220g	依旧摄入粗纤维类主食，慢速提供能量。
	鸡胸（生）150g	龙利鱼 150g 虾 150g 牛瘦肉 150g 去皮鸡腿 120g 豆腐等豆制品 250g 其他鱼类 150g	适当的蛋白质可以保证足够的饱腹感，让减脂过程更轻松。可与豆制品搭配食用。
	蔬菜(生) 250g	白菜/芹菜/油麦菜/西葫芦/番茄/甘蓝等	可以尽量多一些，选新鲜的蔬菜；充足的膳食纤维促进肠胃蠕动，维护更好的肠道菌群环境，也能维护更好的饱腹感。
晚餐	糙米杂粮饭 200g	意面（生）60g 红薯 300g 紫薯 200g 自制杂粮馒头 100g 玉米（带棒）220g 土豆、芋头 200g	晚餐要尽量避免高盐高油重口味食物，烹饪方式尽可能清淡，同时建议在睡前 3-4h结束进食，以保证良好的睡眠质量，和充足的隔夜空腹时间
	牛瘦肉（生）120g	各种鱼类 120g 虾 120g 鸡胸肉 120g 去皮鸡腿 100g	
	蔬菜(生) 300g	萝卜/空心菜/茼蒿/菜花/莴苣/油菜等	可以尽量多一些，选新鲜的蔬菜；充足的膳食纤维促进肠胃蠕动，维护更好的肠道菌群环境，也能维护更好的饱腹感。
豆制品	豆腐 100g	内脂豆腐 180g 南豆腐、嫩豆腐 120g 豆干、豆腐丝 50g	大豆蛋白食品有很多预防相关疾病的功效，建议每天都能摄入适量大豆制品（非卤制、油炸、熏制等添加制作的豆制品）
豆制品和菌藻类，可以任意安排在午餐或晚餐，或感觉吃不饱的那一餐。			
菌藻类	蘑菇 100g	海带 100g 木耳 80g 杏鲍菇 70g 金针菇 80g	菌菇中多糖物质具有免疫功能，能抑制人体癌细胞增殖。建议每天都能适量摄入
食用油 20g/day（1 可乐瓶盖≈4--5g）			
加餐（一天一次）	苹果 250g	香蕉 150g 荔枝、柿 150g 梨、猕猴桃、蓝莓 250g 桃、桔、橙、柚子、葡萄、李子 250g 草莓 400g 西瓜 350g	都是带皮带核的重量，可作为一天随时的加餐。
	杏仁 12颗	腰果、榛子 10颗 花生米 15颗 核桃 2个 开心果 20颗 碧根果 4个 松子仁 15g	可加在早餐中或其他感到饥饿时。

女

	食物名称及数量	替换项	备注
早餐	燕麦片 30g	玉米（带棒） 80g 红薯 100g 紫薯 70g 豆类（干豆重30g）	早起摄入升糖指数较低的食物，可维持较好的精神状态。
	纯牛奶 250ml	酸奶 200ml 豆浆 250ml	牛奶选择配料只有生牛乳的，酸奶选择配料少的、无糖的（如如实），豆浆选无糖或自榨。若喝咖啡需要加奶，需把早餐的奶算进去。喝纯黑咖啡、手冲或挂耳，根据个人对咖啡因的耐受而选择适当的量，一般不建议超过 3 个 shot
	鸡蛋 1个	鸡胸肉 40g	
	绿叶蔬菜 150g	生菜/菠菜/芥蓝/黄瓜等	可加椰子油炒熟食用
午餐	糙米杂粮饭 220g	意面（生）70g 红薯 330g 紫薯 200g 大南瓜 400g 玉米（带棒）220g	依旧摄入粗纤维类主食，慢速提供能量。
	鸡胸（生）150g	龙利鱼 150g 虾 150g 牛瘦肉 150g 去皮鸡腿 120g 豆腐等豆制品 220g 其他鱼类 150g	适当的蛋白质可以保证足够的饱腹感，让减脂过程更轻松。可与豆制品搭配食用。
	蔬菜(生) 200g	白菜/芹菜/油麦菜/西葫芦/番茄/甘蓝等	可以尽量多一些，选新鲜的蔬菜；充足的膳食纤维促进肠胃蠕动，维护更好的肠道菌群环境，也能维护更好的饱腹感。
晚餐	糙米杂粮饭 150g	意面（生）50g 红薯 250g 紫薯 150g 自制杂粮馒头 80g 玉米（带棒）200g 土豆、芋头 200g	晚餐要尽量避免高盐高油重口味食物，烹饪方式尽可能清淡，同时建议在睡前 3-4h结束进食，以保证良好的睡眠质量，和充足的隔夜空腹时间
	牛瘦肉（生）120g	各种鱼类 120g 虾 120g 鸡胸肉 120g 去皮鸡腿 100g	
	蔬菜(生) 200g	萝卜/空心菜/茼蒿/菜花/莴苣/油菜等	可以尽量多一些，选新鲜的蔬菜；充足的膳食纤维促进肠胃蠕动，维护更好的肠道菌群环境，也能维护更好的饱腹感。

豆制品	豆腐 100g	内脂豆腐 180g 南豆腐、嫩豆腐 120g 豆干、豆腐丝 50g	大豆蛋白食品有很多预防相关疾病的功效，建议每天都能摄入适量大豆制品（非卤制、油炸、熏制等添加制作的豆制品）

豆制品和菌藻类，可以任意安排在午餐或晚餐，或感觉吃不饱的那一餐。

菌藻类	蘑菇 100g	海带 100g 木耳 80g 杏鲍菇 70g 金针菇 80g	菌菇中多糖物质具有免疫功能，能抑制人体癌细胞增殖。建议每天都能适量摄入

食用油 20g/day（1 可乐瓶盖≈4--5g）

加餐（一天一次）	苹果 200g	香蕉 120g 荔枝、柿 150g 梨、猕猴桃、蓝莓 200g 桃、桔、橙、柚子、葡萄、李子 260g 草莓 300g 西瓜 400g	都是带皮带核的重量，可作为一天随时的加餐。
	杏仁 12颗	腰果、榛子 10颗 花生米 15颗 核桃 2个 开心果 20颗 碧根果 4个 松子仁 15g	可加在早餐中或其他感到饥饿时。

第三章 BCH码

本章内容

- **有限域**
- **BCH码的编码**
- **BCH码的译码**
- **戈雷(Golay)码**
- **Reed-Solomon码**

3.1 引言

- BCH码是一类最重要的循环码，能纠正多个随机错误，它是1959年由Bose、Chaudhuri及Hocquenghem各自独立发现的二元线性循环码，人们用他们的名字字头命名为BCH码。
- 在前面的讨论中，我们所做的只是构造一个码，然后计算它的最小距离，从而估计出它的纠错能力，而在BCH码中，我们将采用另外一种方法：先说明我们希望它能纠错的个数，然后构造这种码。

3.2 BCH码简述

- 若循环码的生成多项式具有如下形式：

  $g(x)=LCM[m_1(x),m_3(x),\ldots,m_{2t-1}(x)]$

  其中LCM表示最小公倍式，t为纠错个数，$m_i(x)$为素多项式，则由此生成的循环码称为BCH码，其最小码距$d\geq d_0=2t+1$（d_0称为设计码距），它能纠正t个随机独立差错。

- BCH码的码长$n=2^m-1$或是$n=2^m-1$的因子

本原BCH码

非本原BCH码

- 例3.1: BCH(15,5)码，可纠正3个随机独立差错，即t=3

  $d \geq d_0 = 2t+1 = 7$

  $n=15=2^m-1$, so $m=4$

查不可约多项式表可得

$m_1(x)=(23)_8=010011=x^4+x+1$

$m_3(x)=(37)_8=011111=x^4+x^3+x^2+x+1$

$m_5(x)=(07)_8=000111=x^2+x+1$

这样 $g(x)=LCM[m_1(x),m_3(x),m_5(x)]$

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

$= x^{10}+x^8+x^5+x^4+x^2+x+1$

File: merged_output.pdf

- 例3.2: BCH(31,16)码，可纠正3个随机独立差错，即t=3

$d \geq d_0 = 2t+1 = 7$

$n = 31 = 2^m - 1$, so $m = 5$

查不可约多项式表可得

$m_1(x) = (45)_8 = 100101 = x^5 + x^2 + 1$

$m_3(x) = (75)_8 = 111101 = x^5 + x^4 + x^3 + x^2 + 1$

$m_5(x) = (67)_8 = 110111 = x^5 + x^4 + x^2 + x + 1$

这样 $g(x) = LCM[m_1(x), m_3(x), m_5(x)]$

$= x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$

- 部分不可约多项式表

2阶	1	7				
3阶	1	13				
4阶	1	23	3	37	5	07
5阶	1	45	3	75	5	67

File: merged_output.pdf

n≤ 31的本原BCH码

n	k	t	g(x)
7	4	1	13
15	11	1	23
15	7	2	721
15	5	3	2467
31	26	1	45
31	21	2	3551
31	16	3	107657
31	11	5	5423325
31	6	7	313365047

File: merged_output.pdf

部分非本原BCH码

n	k	d	g(x)
17	9	5	727
21	16	3	43
21	12	5	1663
21	6	7	126357
21	4	9	643215
23	12	7	5343
25	5	5	4102041
27	9	3	1001001
27	7	6	7007007
33	6	7	3043

File: merged_output.pdf

3.3 有限域

- 一个元素个数有限的域称为有限域，或者伽罗华域(Galois field);
- 有限域中元素的个数为一个素数，记为GF(p),其中p为素数;
- 一个大于1的整数，如果它的正因数只有1和它本身，就叫做素数，否则就叫做合数。
- 有限域中运算满足
  - 交换律:a+b=b+a, a·b=b ·a
  - 结合律:(a+b)+c=a+(b+c),a·(b·c)=(a·b) ·c
  - 和分配律:a ·(b+c)=a ·b+a ·c

- 可以将GF(p)延伸为一个含有p^m个元素的域，称为GF(p)的扩展域，表示为$GF(p^m)$，m是一个非零正整数。注意：GF(p)是$GF(p^m)$的子集。
- 二进制域GF(2)是扩展域$GF(2^m)$的一个子域，类似于实数域是复数域的一个子域一样。除了数字0和1之外，在扩展域中还有特殊的元素，用一个新的符号a表示。$GF(2^m)$中任何非0元素都可由a的幂次表示。

- 有限元素的集合$GF(2^m)$，只能含有2^m个元素，并且对乘法封闭，其约束条件为： $a^{(2^m-1)}+1=0$
- 根据这个多项式限制条件，任何幂次等于或超过2^m-1的域元素都可降阶为下述幂次小于2^m-1的元素：

$$a^{(2^m+n)}=a^{(2^m-1)}a^{n+1}=a^{n+1}$$

- 这样，$GF(2^m)$的元素可表示为：

$$GF(2^m)=\{0,a^0,a^1,a^2,\cdots,a^{2^m-2}\}$$

File: merged_output.pdf

扩展域GF(2ᵐ)中的加法

- 在GF(2^m)中，将每个非0元素用多项式$a_i(x)$表示，其系数至少有一个不为0。对于i=0,1, 2,…,2^m-2，有：

  $$a^i = a_i(x) = a_{i,0}+a_{i,1}x+a_{i,2}x^2+\ldots+a_{i,m-1}x^{m-1}$$

- 考虑m=3,有限域表示为GF(2^3),下表为上式描述的基本元素{x^0,x^1,x^2}映射为7个元素{a^i}和一个0元素。表中的各行是二进制数字序列，代表上式中的系数$a_{i,0}$、$a_{i,1}$、$a_{i,2}$的取值。

域元素	基本元素			
		x^0	x^1	x^2
	0	0	0	0
	a^0	1	0	0
	a^1	0	1	0
	a^2	0	0	1
	a^3	1	1	0
	a^4	0	1	1
	a^5	1	1	1
	a^6	1	0	1
	a^7	1	0	0

多项式为$f(x)=1+x+x^3$的GF(8)的元素与基本元素之间的映射

File: merged_output.pdf

- 有限域中两个元素的加法定义为两个多项式中同幂次项系数进行模2加，即

$$a^i+a^j=(a_{i,0}+a_{j,0})+(a_{i,1}+a_{j,1})x+\ldots+(a_{i,m-1}+a_{j,m-1})x^{m-1}$$

- 有限域的本原多项式：因为这些函数用来定义有限域$GF(2^m)$。

一个多项式是本原多项式的充要条件：一个m阶的不可约多项式f(x)，如果f(x)整除x^n+1的最小正整数n满足$n=2^m-1$，则该多项式是本原的。

- 例3.3 本原多项式的辨别

(1) $p_1(x)=1+x+x^4$

(2) $p_2(x)=1+x+x^2+x^3+x^4$

分析: (1)通过验证这个幂次为m=4的多项式是否能够整除 x^n+1,但不能整除$1\le n<15$范围内的x^n+1，就可以确定它是否为本原多项式。经反复计算，$p_1(x)$是本原多项式，$p_2(x)$不是，因为它能整除x^5+1。

部分本原多项式

m		m	
3	$1+x+x^3$	11	$1+x^2+x^{11}$
4	$1+x+x^4$	12	$1+x+x^4+x^6+x^{12}$
5	$1+x^2+x^5$	13	$1+x+x^3+x^4+x^{13}$
6	$1+x+x^6$	14	$1+x+x^6+x^{10}+x^{14}$
7	$1+x^3+x^7$	15	$1+x+x^{15}$
8	$1+x^2+x^3+x^4+x^8$	16	$1+x+x^3+x^{12}+x^{16}$
9	$1+x^4+x^9$	17	$1+x^3+x^{17}$
10	$1+x^3+x^{10}$	18	$1+x^7+x^{18}$

File: merged_output.pdf

考虑一个本原多项式定义的有限域的例子

- 选择$p(x)=1+x+x^3$，多项式的幂次为m=3,所以由p(x)所定义的域中包含了$2^m=2^3=8$个元素。求解p(x)的根就是指找到x使p(x)=0。我们所熟悉的二进制数0和1不能满足，因为p(1)=1,p(0)=1 (运用模2运算)。由基本代数学理论我们知道，对于幂次为m的多项式必然有m个根。对于这个例子，p(x)=0有3个根，由于这3个根不可能位于与p(x)系数相同的有限域中，而是位于扩展域$GF(2^3)$中。用扩展域的元素a来定义多项式p(x)的根，可写成如下形式：p(a)=0

即 $1+a+a^3=0 \Rightarrow a^3=1+a$

这意味着a^3可以表示为更低阶a项的加权和。

类似地有：

$a^4=a*a^3=a*(1+a)=a+a^2$

$a^5=a*a^4=a*(a+a^2)=a^2+a^3=1+a+a^2$

$a^6=a*a^5=a*(1+a+a^2)=a+a^2+a^3=1+a^2$

$a^7=a*a^6=a*(1+a^2)=a+a^3=1=a^0$

所以，有限域GF(2^3)的8个元素为

$\{0,a^0,a^1,a^2,a^3,a^4,a^5,a^6\}$

- 这8个元素中哪些是$p(x)=0$的3个根呢？我们可通过枚举找到！

  $p(a^0)=1$, a^0不是

  $p(a^1)=1+a+a^3=0$, a^1是

  $p(a^2)=1+a^2+a^6=1+a^0=0$, a^2是

  $p(a^3)=1+a^3+a^9=1+a^3+a^2=1+a^5=a^4$, a^3不是

  $p(a^4)=1+a^4+a^{12}=1+a^4+a^5=1+a^0=0$, a^4是

  同理可计算$p(a^5)$、$p(a^6)$都不等于0，所以$p(x)=1+x+x^3$的3个根是a, a^2, a^4

$p(x)=1+x+x^3$, GF(8)加法运算表

+	a^0	a^1	a^2	a^3	a^4	a^5	a^6
a^0	0	a^3	a^6	a^1	a^5	a^4	a^2
a^1	a^3	0	a^4	a^0	a^2	a^6	a^5
a^2	a^6	a^4	0	a^5	a^1	a^3	a^0
a^3	a^1	a^0	a^5	0	a^6	a^2	a^4
a^4	a^5	a^2	a^1	a^6	0	a^0	a^3
a^5	a^4	a^6	a^3	a^2	a^0	0	a^1
a^6	a^2	a^5	a^0	a^4	a^3	a^1	0

File: merged_output.pdf

$p(x)=1+x+x^3$, GF(8)乘法运算表

×	a^0	a^1	a^2	a^3	a^4	a^5	a^6
a^0	a^0	a^1	a^2	a^3	a^4	a^5	a^6
a^1	a^1	a^2	a^3	a^4	a^5	a^6	a^0
a^2	a^2	a^3	a^4	a^5	a^6	a^0	a^1
a^3	a^3	a^4	a^5	a^6	a^0	a^1	a^2
a^4	a^4	a^5	a^6	a^0	a^1	a^2	a^3
a^5	a^5	a^6	a^0	a^1	a^2	a^3	a^4
a^6	a^6	a^0	a^1	a^2	a^3	a^4	a^5

File: merged_output.pdf

- 如果GF(p)上的所有元素(除0外)都可表示为某元素a的幂，则a称为GF(p)上的本原元。
- 例3.4 考虑GF(5)，因为p=5是个素数，模算数可以进行。考虑该域上的元素2，

$2^0=1(\text{mod } 5)=1,\ 2^1=2(\text{mod } 5)=2$

$2^2=4(\text{mod } 5)=4,\ 2^3=8(\text{mod } 5)=3$

因此，所有GF(5)上的非零元素，即{1,2,3,4}都可以表示成2的幂，故2是GF(5)上的本原元；大家可以验证，3也是GF(5)上的本原元。

- **$GF(p^m)$中，在模p(x)运算下的扩域上，x所表示的元素是本原元。**
- **例如：用本原多项式$p(x)=1+x+x^3$ 来构造GF(8)，设GF(8)上的本原元为a, 通过将a的幂模p(a)得到GF(8)上的所有元素。**

a的幂	GF(8)上的元素
a^0	1
a^1	a
a^2	a^2
a^3	$a+1$
a^4	a^2+a
a^5	a^2+a+1
a^6	a^2+1

File: merged_output.pdf

- 定理：设$b_1,b_2,\ldots,b_{p-1}$为GF(p)上的非零域元素，则$x^{p-1}+1=(x+b_1)(x+b_2)\ldots(x+b_{p-1})$
- 从循环码知识我们知道，为了找到分组长度为n的循环码的生成多项式，首先分解x^n+1,因此x^n+1可以表示为多个因子的乘积，即

  $$x^n+1=f_1(x)f_2(x)\ldots f_w(x)$$

- 在扩展域$GF(p^m)$中，$n=p^m-1$

- 例3.5 考虑GF(2)和它的扩展域GF(8)。这里p=2,m=3,对x^7+1进行分解

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

同时我们知道，GF(8)中的非零元素为1, a , a+1, a^2, a^2+1, a^2+a, a^2+a+1,因此我们可以写为

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

$=(x+1)[(x+a)(x+a^2)(x+a^2+a)][(x+a+1)(x+a^2+1)(x+a^2+a+1)]$

而在GF(8)上，有

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

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

极小多项式$f_i(x)$	对应的根	元素用a的幂表示
$x+1$	1	a^0
x^3+x+1	a,a^2和a^2+a	a^1,a^2,a^4
x^3+x^2+1	$a+1$,a^2+1和a^2+a+1	a^3,a^6,a^5

File: merged_output.pdf

3.4 BCH码的编码

- 对一个分组长度$n=p^m-1$、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$GF(p^m)$
2. 求$a^i, i=0,1,2,\ldots n-2$的极小多项式$f_i(x)$
3. 可纠t个错误的码的生成多项式为

$$g(x)=LCM[f_1(x),f_2(x),\ldots,f_{2t}(x)]$$

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$d^* \geq 2t+1$。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。

- 例3.6 考虑GF(2)上的本原多项式$p(a)=a^4+a+1$，我们将以此来构造GF(16),设a为本原元。GF(16)上以a的幂表示形式的元素及它们对应的极小多项式为：

a的幂	GF(16)的元素	极小多项式
a^0	1	$x+1$
a^1	a	x^4+x+1
a^2	a^2	x^4+x+1
a^3	a^3	$x^4+x^3+x^2+x+1$
a^4	$a+1$	x^4+x+1
a^5	a^2+a	x^2+x+1
a^6	a^3+a^2	$x^4+x^3+x^2+x+1$
a^7	a^3+a+1	x^4+x^3+1
a^8	a^2+1	x^4+x+1
a^9	a^3+a	$x^4+x^3+x^2+x+1$
a^{10}	a^2+a+1	x^2+x+1
a^{11}	a^3+a^2+a	x^4+x^3+1
a^{12}	a^3+a^2+a+1	$x^4+x^3+x^2+x+1$
a^{13}	a^3+a^2+1	x^4+x^3+1
a^{14}	a^3+1	x^4+x^3+1

- 我们希望确定纠单错的BCH码的生成多项式，即t=1且n=15。由前面公式可知，一个BCH码的生成多项式由$LCM[f_1(x),f_2(x),\ldots,f_{2t}(x)]$给出，利用前面的表我们可获得极小多项式$f_1(x)$和$f_2(x)$，于是有：

$$g(x)=LCM[f_1(x),f_2(x)]$$
$$=LCM[(x^4+x+1),(x^4+x+1)]$$
$$=x^4+x+1$$

因为deg g(x)=n-k，可得n-k=4，所以k=11,于是我们得到纠单一错误的BCH(15,11)码的生成多项式。该码的设计距离为d=2t+1=3，可以计算该码的实际最小距离d*也是3。

如果希望纠2个错误，且n=15。则其生成多项式为

$g(x)=LCM[f_1(x),f_2(x),f_3(x),f_4(x)]$

$=LCM[(x^4+x+1),(x^4+x+1),(x^4+x^3+x^2+x+1),(x^4+x+1)]$

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

$=x^8+x^7+x^6+x^4+1$

因为deg g(x)=n-k=8，所以k=7,于是我们得到纠2个错误的BCH(15,7)码的生成多项式。该码的设计距离为d=2t+1=5，可以计算该码的实际最小距离d*也是5。

如果希望纠3个错误，且n=15。则其生成多项式为

$g(x)=LCM[f_1(x),f_2(x),f_3(x),f_4(x),f_5(x),f_6(x)]$

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

$= x^{10}+x^8+x^5+x^4+x^2+x+1$

因为deg g(x)=n-k=10，所以k=5,于是我们得到纠3个错误的BCH(15,5)码的生成多项式。该码的设计距离为d=2t+1=7，可以计算该码的实际最小距离d*也是7。

如果希望纠4个错误，且n=15。则其生成多项式为

$$g(x)=LCM[f_1(x),f_2(x),f_3(x),f_4(x),f_5(x),f_6(x),f_7(x),f_8(x)]$$

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

$$= x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

因为deg g(x)=n-k=14，所以k=1。(简单的重复码)。于是我们得到纠4个错误的BCH(15,1)码的生成多项式。该码的设计距离为d=2t+1=9，可以计算该码的实际最小距离d*是15。在此情况下，设计距离不等于实际最小距离，码设计得太过度了，该码实际可纠(d*-1)/2=7个随机错误！

3.5 BCH码的译码

- 根据生成多项式，可以构造出快速的硬件编码器，而对于BCH码的译码，由于它是循环码的一个子类，任何对循环码的标准译码过程都适用于BCH码。下面我们主要讨论专门针对BCH码的更高效的算法:

Gorenstein-zierler译码算法

设c(x)为发送码字多项式，e(x)为错误多项式，则接收到的多项式为r(x)=c(x)+e(x)

设$y_1,y_2,\ldots,y_w$为g(x)在$GF(p^m)$上的根，即$g(y_i)=0,i=1,2,\ldots,w$。因为对某个信息多项式a(x),有c(x)=a(x)g(x),所以$c(y_i)=0$

$r(y_i)=c(y_i)+e(y_i)=e(y_i)$, $i=1,2,\ldots,w$

- 假设BCH码是根据一个域元素a来构造的，考虑错误多项式

$e(x)=e_{n-1}x^{n-1}+e_{n-2}x^{n-2}+\ldots+e_1x+e_0$

其中最多有t个系数为非零(可纠t个错误),假设实际发生了v个错误，其中$0\le v\le t$。设错误发生在位置$i_1,i_2,\ldots,i_v$，则错误多项式可写为

$$e(x)=e_{i_1}x^{i_1}+e_{i_2}x^{i_2}+\ldots+e_{i_v}x^{i_v}$$

其中 e_{i_k} 为第k个错误的大小，对二元码，$e_{i_k}=1$

对纠错问题，我们必须知道两件事：

(1)错误在哪里发生了，即错误的位置

(2)错误程度

因此，未知量为$i_1,i_2,\ldots,i_v$和 e_{i_1}，e_{i_2} ,..., e_{i_v}，它们分别表明错误发生的位置和程度。

伴随式可通过对接收到的关于a的多项式计算得到：

$$S_1 = r(a) = c(a) + e(a) = e(a)$$

$$= e_{i_1} a^{i_1} + e_{i_2} a^{i_2} + \ldots + e_{i_v} a^{i_v}$$

定义错误程度 $Y_k = e_{i_k}$和错误位置 $X_k = a^{i_k}$ ，

$k=1,2,\ldots,v$。其中i_k为第k个错误的位置，X_k是与这个位置相关的域元素。

- 现在伴随多项式可写为

$$S_1=Y_1X_1+Y_2X_2+\ldots+Y_vX_v$$

对j=1,2,…,2t, 我们定义伴随式

$$S_j=r(a^j)=c(a^j)+e(a^j)=e(a^j)$$

于是我们可得到2t个联立方程组，它有v个错误位置未知量 $X_1,X_2,\ldots,X_v$和v个错误程度未知量$Y_1,Y_2,\ldots,Y_v$:

$$\begin{cases} S_1 = Y_1X_1 + Y_2X_2 + \cdots + Y_vX_v \\ S_2 = Y_1X_1^2 + Y_2X_2^2 + \cdots + Y_vX_v^2 \\ \vdots \\ S_{2t} = Y_1X_1^{2t} + Y_2X_2^{2t} + \cdots + Y_vX_v^{2t} \end{cases}$$

File: merged_output.pdf

- 定义错误定位多项式

$U(x)=U_v x^v+U_{v-1}x^{v-1}+\ldots+U_1 x+1$

这个多项式的根是错误位置的逆 X_k^{-1} ,k=1,2,…,v,即

$U(x)=(1-xX_1)(1-xX_2)\ldots(1-xX_v)$

所以，如果我们知道错误定位多项式U(x)的系数，便可以求得错误位置$X_1,X_2,\ldots,X_v$。经过一系列代数变换，我们可得如下矩阵：

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_{v-1} & S_v \\ S_2 & S_3 & \cdots & S_v & S_{v+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ S_v & S_{v+1} & \cdots & S_{2v-2} & S_{2v-1} \end{bmatrix} \begin{bmatrix} U_v \\ U_{v-1} \\ \vdots \\ U_1 \end{bmatrix} = \begin{bmatrix} S_{v+1} \\ S_{v+2} \\ \vdots \\ S_{2v} \end{bmatrix}$$

错误定位多项式的系数可通过对伴随式矩阵M求逆得到！

BCH码的译码步骤

1. 作为测试值，令v=t，计算伴随矩阵M的行列式。如果行列式的值为零，令v=t-1,再一次计算M的行列式。重复这个过程直到找到一个v值，使伴随矩阵的行列式不为0，该v值就是实际产生错误的数目。
2. 求M的逆，并计算错误定位多项式U(x)的系数；
3. 求解U(x)=0的零点，从中可计算错误位置$X_1,X_2,\ldots,X_v$。如果是二元码，就到此为止(因为错误程度为1);
4. 如果不是二元码，回到方程组解这些方程组就得到错误程度

$$\begin{cases} S_1 = Y_1X_1 + Y_2X_2 + \cdots + Y_vX_v \\ S_2 = Y_1X_1^2 + Y_2X_2^2 + \cdots + Y_vX_v^2 \\ \vdots \\ S_{2t} = Y_1X_1^{2t} + Y_2X_2^{2t} + \cdots + Y_vX_v^{2t} \end{cases}$$

File: merged_output.pdf

- 例3.7 考虑纠3个错误的BCH(15,5)码，它的生成多项式为 $g(x)=x^{10}+x^8+x^5+x^4+x^2+x+1$

设传输的是全0码字，接收到的多项式为$r(x)=x^5+x^3$,故有两个错误分别在第4个位置和第6个位置，错误多项式为$e(x)=x^5+x^3$。但译码器并不知道这些，它连实际发生了几个错误都不知道！

解：利用Gorenstein-aierler译码算法，首先用GF(16)上的算术计算出伴随式

$S_1=a^5+a^3=a^{11}$，$S_2=a^{10}+a^6=a^7$

$S_3=a^{15}+a^9=a^7$，$S_4=a^{20}+a^{12}=a^{14}$

$S_5=a^{25}+a^{15}=a^5$，$S_6=a^{30}+a^{18}=a^{14}$

因为这是个纠3个错的码，首先令v=t=3

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} a^{11} & a^{7} & a^{7} \\ a^{7} & a^{7} & a^{14} \\ a^{7} & a^{14} & a^{5} \end{bmatrix}$$

Det(M)=0, 这表明发生的错误数少于3个。

下面令v=2

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} a^{11} & a^{7} \\ a^{7} & a^{7} \end{bmatrix}$$

Det(M) ≠ 0, 这表明实际发生了2个错误。

下面计算M^{-1}

$$M^{-1} = \begin{bmatrix} a^{7} & a^{7} \\ a^{7} & a^{11} \end{bmatrix}$$

File: merged_output.pdf

$$\begin{bmatrix} U_2 \\ U_1 \end{bmatrix} = M^{-1} \cdot \begin{bmatrix} S_3 \\ S_4 \end{bmatrix} = \begin{bmatrix} a^7 & a^7 \\ a^7 & a^{11} \end{bmatrix} \begin{bmatrix} a^7 \\ a^{14} \end{bmatrix}$$

求解U_1和U_2可得$U_2=a^8$及$U_1=a^{11}$, 从而

$U(x)=a^8x^2+a^{11}x+1=(1+xa^5)(1+xa^3)$

因此恢复出来的错误位置为a^5和a^3。因为该码是二元码，错误程度为1，故$e(x)=x^5+x^3$。

#

3.6 戈雷(Golay)码

- 在第9页中，我们曾给出一些部分非本原BCH码的列表，Golay码就是(23,12)码。由表可查出，其生成多项式

$(5343)_8$=101 011 100 011

即 $g_1(x)=x^{11}+x^9+x^7+x^6+x^5+x+1$ ⟹

或$g_2(x)=x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$ ⟸

它们都是$x^{23}+1$的因式，即$x^{23}+1=(x+1)g_1(x)g_2(x)$

其最小码距为7，可纠正不大于3个的随机错误。

- Golay码是一个完备码。如果r 位监督位所组成的校正子与误码图样一一对应，这种码组称为完备码.

- **定理：一个有M个码字，最小距离为2t+1的q-元(n,k)码，满足**

$$M\left\{\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{t}(q-1)^t\right\}\le q^n$$

其中q^n这个界称为汉明界，一个能到达汉明界的码称为完备码，即上式取等号。

- **容易证明：**

$$2^{12}\left\{\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}\right\}=2^{23}$$

3.7 Reed-Solomon (RS)码

- **1960年MIT Lincoln实验室的S. Reed和G. Solomon在*Journal of the Society for Industrial and Applied Mathematics*上发表的一篇论文: Polynomial Codes over Certain Finite Fields (某些有限域上的多项式码)**
- **RS码的编码系统是建立在比特组基础上的，即字节，而不是单个的0和1，因此它是非二进制BCH码，这使得它处理突发错误特别好。**

备注：在许多现实生活的信道中，错误不是随机的，而是突发的。例如，在一个移动通信信道中，信号衰退导致突发错误。当错误连续发生时，我们称它们为突发错误。

- 对于任意选取的正整数s，可构造一个相应码长为$n=q^s-1$的q进制BCH码，其中码元符号取自有限域GF(q)，而q为素数的幂。当s=1，q>2时所建立的码长为n=q-1的q进制BCH码，称为RS码。当$q=2^m(m>1)$，码元符号取自域$GF(2^m)$的二进制RS码可用来纠正突发错误。
- 输入信息分为k*m比特一组，即每个符号有m比特，k个符号形成一组。
- 一个可纠t个符号错误的RS码，有如下参数

码长：$n=2^m-1$　　符号　或　$m(2^m-1)$ bit

信息段：k　　符号　或　km bit

监督段：$n-k=2t$　　符号　或　$m(n-k)=2mt$ bit

最小码距：$d=2t+1$ 符号　或　$md=m(2t+1)$ bit

例3.8 试构造一个能纠3个错误符号，码长n=15,m=4的RS码。

解：已知t=3,n=15,m=4, 所以有

码距：d=2t+1=7个符号(28bit)　监督段：2t=6个符号(24bit)

信息段：n-6=9个符号(36bit)　码长：n=15个符号(60bit)

因此该码是(15,9)RS码，也可看作是(60,36)二进制码；

最小距离为d的RS码生成多项式应具有如下形式：

$$g(x)=(x+a)(x+a^2)\ldots(x+a^{d-1})$$

本例中，d=7

$$g(x)=(x+a)(x+a^2)\ldots(x+a^6)$$

$$=x^6+a^{10}x^5+a^{14}x^4+a^4x^3+a^6x^2+a^9x+a^6$$

其中a^i是GF(q)中的一个元素。

RS码生成多项式的次数总是2t！