ENEE626, CMSC858B, AMSC698B

Error Correcting Codes

Part II. Algebraic coding theory

ENEE626 Lecture 10: Finite fields

Euclidean division algorithm
Multiplicative inverse mod p
Irreducible polynomials

In the first part of the course we have studied the main properties of linear codes such as their structure, error correction, decoding, important examples
Here we will prepare way for a detailed study of practical, algebraic families of codes such as Reed-Solomon codes

Example

Roughly speaking, a field is a “number system” with two operations, + and x
Let us look at $\mathbb{F}_7$ ($=\mathbb{Z}/(7\mathbb{Z})$)

The multiplication table is given by

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	2
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Notation: $\mathbb{F}_7^*=\mathbb{F}_7\backslash\{0\}$

For every $a\in\mathbb{F}_7^*$ there is b s.t. ab=1; so $a=b^{-1}$

Properties: a.b mod 7 and a+b mod 7 stay in $\mathbb{F}_7$
$\forall$ $a\neq 0$ $\exists$ b such that ab=1
$\forall$ a $\exists$ b such that a-b=0

Note that $3, 3^2=2, 3^3=6, 3^4=4, 3^5=5, 3^6=1$ exhaust all of $\mathbb{F}_7$.
In such situation we say that 3 is a primitive root mod 7

Definition 10.1: A field F is a set of elements closed under two binary operations, called addition and multiplication

Addition has the following properties
$a+b=b+a$ (commutative)
$a+(b+c)=(a+b)+c$ (associative)
$\exists$ e: $a+e=a$ (called zero)
for any a there is an inverse b: $a-b=0$

Similarly, multiplication is commutative, associative,
distributive: $a(b + c)=ab + ac$
any nonzero element $a \in F$ has an inverse, $b=a^{-1}$, s.t. $ab=1$

Our next goal is to prove that for any prime number, any number r, $0<r<p$, has a unique mult. inverse mod p

Euclidean division algorithm (EDA)

Lemma 10.1. Let r, s $\in \mathbb{Z}$ and let g=GCD(r,s) be their greatest common divisor. There exist integer numbers a and b such that ar+bs=g.

Division with a remainder: For any c, d $\neq$ 0 there exists s, 0 $\leq$ s < |d| such that c = dQ+s. Here Q is called a quotient, s a remainder.

Euclidean division algorithm: Given s,r$\in\mathbb{Z}$, r<s, find GCD(s,r)
Do the following:

$s=Q_1 r+r_1$
$r=Q_2\ r_1+r_2$
$r_1=Q_3\ r_2+r_3$
...
$r_{n-2}=Q_n\ r_{n-1}+r_n$
$r_{n-1}=Q_{n+1} r_n$

The remainder will become 0 in some step, say in step n+1 because
$r>r_1>r_2>\ldots>r_{n-1}>r_n>0$
Clearly, r_n=GCD(s,r) because is $r_n|r$, $r_n|s$, and any divisor of s,r also divides r_n.

Euclidean division algorithm (EDA)

This system of equations can be solved for r_n because from the equation before the last one, $r_n=-Q_n\, r_{n-1}+r_{n-2}$, then from the equation before that one, $r_{n-3}=Q_{n-1}\, r_{n-2}+r_{n-1}$, so

$$r_n=-Q_n\, r_{n-1}+r_{n-2}$$
$$=-Q_n\,(-Q_{n-1}\, r_{n-2}+r_{n-3})+ r_{n-2}= (Q_nQ_{n-1}+1)\, r_{n-2}-Q_n\, r_{n-3}$$
$$=(Q_nQ_{n-1}+1)(-Q_{n-2}\, r_{n-3}+r_{n-4})- Q_n\, r_{n-3}=\ldots$$

Here each step i=1,2,… removes r_{n-i}, so after n steps we get to $r_0=r$ and s

Example: $s=Q_1\, r+r_1$
$r=Q_2\, r_1+r_2$
$r_1=Q_3\, r_2$

Solving, we get
$r_2=-Q_2r_1+r=-Q_2(-Q_1\, r+s)+r=r(Q_2Q_1+1)-Q_2s$

36=2.15+6
15=2.6+3
6=2.3

3=15(2.2+1) – 2.36
=5.15 – 2.36

GCD(18,7)=1
1=2.18-5.7
or
1=2.4 (mod 7)

Corollary 10.2: Let p be a prime and 0<r<p. Then there exists a, 0< a<p such that a.r=1 mod p.
Indeed, GCD(r,p)=1, so ar+bp=1 for some a, b. Reducing this mod p, we get a.r=1 mod p.

Let us extend EDA to polynomials over a field F.
A polynomial $f(x) \in F[x]$ is called irreducible if the equality

$$f(x)=g(x)h(x), \qquad g,h \in F[x]$$

implies that either g or h is a constant polynomial. Irreducible polynomials play the role similar to prime numbers.

Example: $f(x)=x^2+x+1$ is irreducible both over $\mathbb{R}$ and $\mathbb{F}_2$

Division with a remainder for polynomials: Let $c(x),d(x) \in \mathbb{Z}[x]$,
deg c > deg d. Then there exists a polynomial s(x), $0 \leq$ deg s < deg d, s.t.

$$c(x) = d(x)Q(x) + s(x)$$

s(x) can be found by long division. The same is true for polynomials over $\mathbb{F}_p$, i.e., with coefficients 0 ,1,…,p-1 and operations mod p.

Euclidean division algorithm can be extended to polynomials.
Example. Let $f=x^4+x^2+x+1$, $g=x^3+1 \in \mathbb{F}_2[x]$. Find GCD(f,g)

Of course, $x^3+1=(x+1)(x^2+x+1)$

$x^4+x^2+x+1=(x+1)(x^3+x^2+1)$, so GCD(f,g)=x+1

We will use EDA

$x^4 + x^2 + x + 1 = x\,(x^3+1) + x^2+1$ (found by long division)

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

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

$\mathrm{GCD}(x^4 + x^2 + x + 1, x^3+1) = x+1 = x^3+1+ x(x^2+1)$

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

$= (x+1)\, g(x) + x\, f(x)$

Irreducible polynomials over $\mathbb{F}_2$

$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, \ldots$

Lemma 10.3: Let $f(x) \in \mathbb{F}_p[x]$ be irreducible over $\mathbb{F}_p$.
Then every $g(x) \neq 0$ has a unique multiplicative inverse modulo f,
i.e., there exists an h such that $\deg h \leq \deg f - 1$ and $gh = 1 \pmod f$.

Proved similarly to the case of numbers.

Example: Find inverse of x mod $x^4+x+1 \in \mathbb{F}_2[x]$. We need
that $x\, g(x)=1=x^4+x$, so $g(x)=x^3+1$

Algebraic extensions of fields

Complex numbers $\mathbb{C}$ are constructed from $\mathbb{R}$ by adjoining to $\mathbb{R}$ a root of the polynomial x^2+1, denoted i, and considering all linear combinations a+bi where $a,b \in \mathbb{R}$

In this situation we say that $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$ of degree 2, denoted $[\mathbb{C} : \mathbb{R}]=2$

Complex numbers are added as vectors (a+bi)+(c+di)=(a+c)+(b+d)i and multiplied as polynomials in i: (a+bi)(c+di)=ac-bd + (ad+bc)i

The set of complex numbers forms a 2-dimensional vector space over $\mathbb{R}$

Let us construct $\mathbb{F}_{16}$ as a 4^{th} degree extension of $\mathbb{F}_2$ using the irreducible polynomial $f(x)=x^4+x+1$. Let α be a root of f(x), $\alpha^4+\alpha+1=0$ or $\alpha^4+\alpha=1$

Exercise: what are the other 3 roots of f(x)?

Table of the field

vector	polynomial	power of α	logarithm	
0000	0	?	$-\infty$	
0001	1	$\alpha^0=1$	0	
0010	x	α	1	
0100	x^2	α^2	2	
1000	x^3	α^3	3	
0011	x+1	α^4	4	$x^4=x+1 \bmod f$
0110	x^2+x	α^5	5	$\alpha^5=\alpha^4\alpha=(\alpha+1)\alpha=\alpha^2+\alpha$
1100	x^3+x^2	α^6	6	
1011	x^3+x+1	α^7	7	
0101	x^2+1	α^8	8	
1010	x^3+x	α^9	9	
0111	x^2+x+1	α^{10}	10	
1110	x^3+x^2+x	α^{11}	11	
1111	x^3+x^2+x+1	α^{12}	12	
1101	x^3+x^2+1	α^{13}	13	
1001	x^3+1	α^{14}	14	

$\alpha^{15}=1$: $x(x^3+1)=x^4+x=(x+1)+x=1$

We have proved that these 16 elements form a field (check the axioms)

ENEE626 Lecture 11: Finite fields

Basic properties of finite fields
Existence of primitive elements

We have constructed $\mathbb{F}_{16}$ as a degree-4 extension of $\mathbb{F}_2$

Let us prove that this construction is universal: for any prime p and an irreducible polynomial of degree m over $\mathbb{F}_p$ it is possible to construct a finite field of p^m elements

Let F be a finite field. In the sequence of elements

$1+1+1+\ldots+1$ ($t \geq 1$) times

there will be repeated elements (because F is finite). Then for some t_1, t_2, we will have $t_1.1=t_2.1$, or $(t_2-t_1).1=0$

Definition 11.1: The smallest number p such that p.1=0 is called the characteristic of F, denoted char F.

p is always prime. Indeed, if not, then we would have $p.1=(p_1.1)(p_2.1)=0$, which means that one of the two products is 0, contradicting the fact that p is smallest.

Consider a maximal set $\mathcal{B} = \{b_1, b_2, \ldots, b_m\}$ of elements of F which are linearly independent over $\mathbb{F}_p$. It is clear that F contains all p^m linear combinations

$$\lambda_1 b_1 + \ldots + \lambda_m b_m, \quad \lambda_i \in \mathbb{F}_p,\ i=1,..,m$$

and no other elements because otherwise there would be an element linearly independent of $b_1, b_2, \ldots, b_m$
Thus $|F|=p^m$ for any finite field F

The set $\mathcal{B}$ is called a basis of F over $\mathbb{F}_p$

Let $a \in \mathbb{F}_q$. Consider the set $\{a, a^2, a^3, a^4, \ldots\}$. Clearly at some point we will encounter repeated elements $a^i = a^j$, or $a^{j-i}=1$

Definition 11.2: Let $a \in \mathbb{F}_q$. The smallest s such that $a^s=1$ is called the order of a, denoted ord(a). An element of order q-1 is called a primitive element of $\mathbb{F}_q$
An irreducible polynomial whose root is a primitive element is called a primitive polynomial (Exercise: give example of an irreducible, non-prim. polynomial)

Example: In $\mathbb{F}_{16}$, $\text{ord}(\alpha)=\text{ord}(\alpha^2)=\text{ord}(\alpha^4)=15$ (primitive elements); $\text{ord}(\alpha^3)=5$

From the table (next page), the elements $1, \alpha, \alpha^2, \alpha^3$ are linearly independent over $\mathbb{F}_2$, i.e., form a basis. This justifies representation of $\mathbb{F}_{16}$ as a 4-dim. vector space over $\mathbb{F}_2$

Table of the field $\mathbb{F}_{2^4}$

vector	polynomial	power of α	logarithm	
0000	0	?	$-\infty$	
0001	1	$\alpha^0=1$	0	
0010	x	α	1	
0100	x^2	α^2	2	
1000	x^3	α^3	3	
0011	x+1	α^4	4	$x^4=x+1 \bmod f(x)$
0110	x^2+x	α^5	5	$\alpha^5=\alpha^4\alpha=(\alpha+1)\alpha=\alpha^2+\alpha$
1100	x^3+x^2	α^6	6	
1011	x^3+x+1	α^7	7	
0101	x^2+1	α^8	8	
1010	x^3+x	α^9	9	
0111	x^2+x+1	α^{10}	10	
1110	x^3+x^2+x	α^{11}	11	
1111	x^3+x^2+x+1	α^{12}	12	
1101	x^3+x^2+1	α^{13}	13	
1001	x^3+1	α^{14}	14	

$\alpha^{15}=1$: $x(x^3+1)=x^4+x=(x+1)+x=1$

Theorem 11.1: The finite field $\mathbb{F}_{p^m}$ contains a primitive element, i.e., an element of order p^m-1. Thus, the set of nonzero elements of $\mathbb{F}_{p^m}$, denoted $(\mathbb{F}_{p^m})^*$, forms a cyclic group.

Reminder: A commutative group G is a set of elements with a binary operation, called multiplication, that satisfies the following properties:

(i) for any $g_1, g_2 \in G$, $g_1.g_2 \in G$ and $g_1.g_2 = g_2.g_1$

(ii) there exists an element $e \in G$ such that $g.e=g$ for any $g \in G$

(iii) for any $g \in G$ there exists $h \in G$ such that $g.h=1$ (mult. inverse)

(iv) for any g_1, g_2, g_3, $(g_1.g_2)g_3 = g_1(g_2.g_3)$

A finite group G is called cyclic if there exists an element g such that any $h \in G$ is some power of g:

$$G=\{g^0, g^1, \ldots g^{|G|-1}\}$$

We begin with:

Lemma 11.2: Let a,b in $\mathbb{F}_{p^m}$, let ord(a)=r,ord(b)=s, (r,s)=1. Then ord(ab)=rs.

Proof. (a) Let us first prove that a^j=1 if and only if $r \mid j$. We have a^r=1.
It is easy to see that if $j=rk$ then $a^j=(a^r)^k$=1
Assume that $j=(rh+g)$, $g<r$ then $a^j=a^{rh+g}=a^g$=1 but by
assumption g<r, and this contradicts the definition of the order.
Therefore, g=0 and r | j is established.

b) Now prove the lemma. We have $(ab)^{rs}$=1. Hence by part (a), ord(ab) | rs.
Assume that ord(ab)=$l_1 l_2$ and $l_1 \mid r$, $l_2 \mid s$.

$1=(ab)^{l_1 l_2}=a^{rl_2}b^{rl_2}=b^{rl_2}$

Thus $s \mid rl_2$ but s and r are relatively prime, therefore $s \mid l_2$.
Together with $l_2 \mid s$ this implies that $s=l_2$.
Similarly $r=l_1$. and hence we have proved that ord (a,b)=rs.

Theorem 11.3: $\mathbb{F}_{p^m}^* = \mathbb{F}_{p^m} \setminus \{0\}$ is a cyclic multiplicative group of order p^m-1

Proof: (a) Let r = max ord(z) over all $z \neq 0$, let a satisfy ord(a)=r.

Let us first prove that every $b \in \mathbb{F}_{p^m}^*$ satisfies $x^r-1 = 0$.

To show this, it suffices to prove that $\forall\ b \neq 0$, ord(b)|r.

Let ord(b)=l and suppose that ξ is a prime such that $l=\xi^i l'$ and ξ does not divide l (for instance, if l is prime then $\xi=l$). Similarly let $r=\xi^j r'$ where ξ does not divide r'. Since $(\xi,l')=1$, we conclude that ord($b^{l'}$)=ξ^i. Likewise, ord(a^{ξ^j})=r'. Since ξ^j and l' are relatively prime, Lemma 11.2 above implies that ord(a^{ξ^j} $b^{l'}$)=$r'\xi^i$.

Since r is the maximum value of the order in our field, $r'\xi^i \leq r = r'\xi^j$ implying that $i \leq j$.

Since the above argument is true for every prime factor of l, we conclude that $l|r$. Therefore, $b^r=1$, which proves part (a).

Since every $b \neq 0$ satisfies $x^r-1=0$, we obtain

$$\prod_{b \neq 0}(x-b) \mid (x^r-1).$$

Since $\deg(\prod_{b \neq 0}(x-b))=p^m-1$, also $r \geq p^m-1$.

On the other hand, $r \leq p^m-1$ because that's the total number of nonzero elements in the field.

By definition of r, we then get $r=p^m-1$. The powers of a are all distinct and exhaust $\mathbb{F}_{p^m}^*$, which proves that it is a cyclic group.

Basic facts about finite fields:

1. The characteristic of any finite field F is a prime number p.
   Any finite field F consists of p^m elements for some prime p and $m \geq 1$.
   F contains $\mathbb{F}_p$ as its subfield.

2. Given an irreducible polynomial of degree m over $\mathbb{F}_p$, it is possible to construct an mth degree extension of $\mathbb{F}$, namely $\mathbb{F}_{p^m}$. The nonzero elements of $\mathbb{F}_{p^m}$ satisfy the equation $x^{p^m-1} = 1$

3. Over $\mathbb{F}_p$, p prime, there exists an irreducible polynomial of any degree $m \geq 1$. Therefore, for any prime p and any $m \geq 1$ there exists a finite field $\mathbb{F}_{p^m}$

4. The finite field F of size p^m is unique, isomorphic to $\mathbb{F}_{P^m}$ (finite fields of equal size are isomorphic)

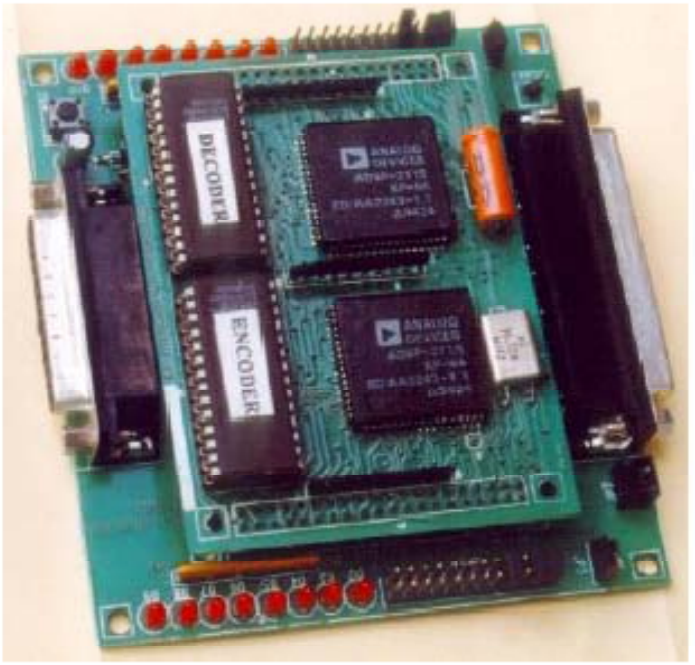
5. The finite field $\mathbb{F}_{P^m}$ contains a primitive element, i.e., an element of order p^m-1. Thus, the set of nonzero elements of $\mathbb{F}_{p^m}$, denoted $\mathbb{F}_{p^m}^*$, forms a cyclic group

ENEE626 Lecture 12: MDS and Reed-Solomon Codes

Definition of RS codes
Main properties of MDS codes
Weight distribution of MDS codes
Extended RS codes

Reed-Solomon codes

Millions of error-correcting codes are decoded **every minute**, with efficient algorithms implemented in custom VLSI circuits.



At least 75% of these VLSI circuits **decode Reed-Solomon codes.**

I.S. Reed and G. Solomon, Polynomial codes over certain finite fields, *Journal Society Indust. Appl. Math.* **8**, pp. 300-304, June 1960.

Reed-Solomon codes are used in...

- ***Magnetic recording*** (all computer hard-disks use RS codes)
- ***Digital video broadcasting*** (ETSI DVB-T and DVB-H)
- ***Digital versatile disks*** (DVDs use products of RS codes)
- ***Third generation (3G) wireless telephony*** (IS-2000, Release D)
- ***Optical fiber networks*** (ITU–T G.795)
- ***Compact disks*** (use cross-interleaved shortened RS codes)
- ***ADSL transceivers*** (ITU–T G.992.1)
- ***Wireless broadband systems – wireless MAN*** (IEEE 802.16)
- ***Intelsat Earth stations*** (IESS–308)
- ***Space telemetry systems*** (CCSDS)
- ***Digital satellite broadcast*** (ETS 300-421S, ETS 300-429)
- ***Frequency-hop communications*** (primarily military)
- ***Deep-space exploration*** (all NASA probes)

And many more applications.

Reed-Solomon codes

Let $q=p^s$, let $\mathbb{F}_q=\{\alpha_0=0,\alpha_1,\ldots,\alpha_{q-1}\}$ be a finite field, let $n \leq q-1$ (typically $q=n+1$)

Let $f(x)\in \mathbb{F}_q[x]$ be a polynomial and let $\mathscr{P}=(\alpha_1,\ldots,\alpha_n) \subset \mathbb{F}_q$
Define the evaluation map eval(f(x)) that maps f to a vector $c \in (\mathbb{F}_q)^n$

$$f \mapsto c=(c_1,c_2,\ldots,c_n) \text{ where } c_i=f(\alpha_i),\ i=1,2,\ldots,n$$

Definition 12.1: An [n,k] q-ary RS code

$$C=\{\text{eval}(f),\ 0 \leq \deg f \leq k-1\}$$

The set $\mathscr{P}$ will be called a defining set of points of C.

Example: $\mathbb{F}_7=\{0,1,2,3,4,5,6\}$. Take $\alpha=3$ to be the primitive element,

Let $\mathscr{P}=\{1,\alpha,\alpha^2,\ldots,\alpha^5\}$ $\quad f(x)=2x+1 \quad$ $\mathbf{c}=\text{eval}(f)=(3,0,5,6,2,4)$
$=\{1,3,2,6,4,5\}$ $\quad f(x)=3x^2+x+2 \quad$ $\mathbf{c}=\text{eval}(f)=(6,4,2,4,5,5)$

C is a linear code: Let $\mathbf{c}_1=\text{eval}(f_1)$ and $\mathbf{c}_2=\text{eval}(f_2)$ where both $f_1(x)$ and $f_2(x)$ are of degrees k-1. Then

$$\alpha\,\mathbf{c}_1+\beta\,\mathbf{c}_2=\text{eval}\,(g),$$

where $g(x)=\alpha\, f_1(x)+\beta\, f_2(x)$, and hence $\deg g \leq k-1$, so $\text{eval}\,(g)\in C$.

RS codes are examples of evaluation codes. They can be generalized to an important class of *algebraic geometry* codes.

Proposition 12.1: The distance of the RS code C d=n-k+1.
Proof: A polynomial of degree $\leq$ k-1 can have at most k-1 zeros.

Theorem 12.2 (Singleton bound) The distance of any code $C \subset \mathbb{F}_q^n$ with |C|=M satisfies

(1) $M \leq q^{n-d+1}$

In particular, if the code is linear, and $M=q^k$, then

(2) $d \leq n-k+1$

Proof: Consider the n x M code matrix. Upon deleting any d-1 columns all the rows will be different. Hence (1). (2) follows from (1).
Alternatively, (2) is proved directly since, denoting by H the parity-check matrix of C, we have

$$d-1 \leq rk(H) \leq n-k.$$

Codes that meet the Singleton bound are called Maximum Distance Separable (MDS). In particular, RS codes are MDS.

Remark: The length of RS codes satisfies $n \leq q-1$. It is also possible to construct extended RS codes of length n=q+1.

General properties of MDS codes

Theorem 12.3: Let C be an [n,k,d] code with generator matrix G and p.-c. matrix H.The following claims are equivalent.

(i) C is MDS

(ii) Every k columns of G are linearly independent

(iii) Every n-k columns of H are linearly independent

(iv) The dual code $C^{\perp}$ =$\{\mathbf{y} \in \mathbb{F}_q^n : \forall\ (\mathbf{c} \in C)\ (\mathbf{y},\mathbf{c})=0\}$ is MDS

(v) If $G=[I_k|A]$ then *every* square submatrix of A has full rank

(vi) The weight distribution of the code C is given by

$$A_0 = 1, A_1 = \ldots = A_{n-k} = 0$$

$$A_l = \binom{n}{l}(q-1)\sum_{j=0}^{l-d}(-1)^j\binom{l-1}{j}q^{l-d-1} \quad (l = d, d+1, \ldots, n)$$

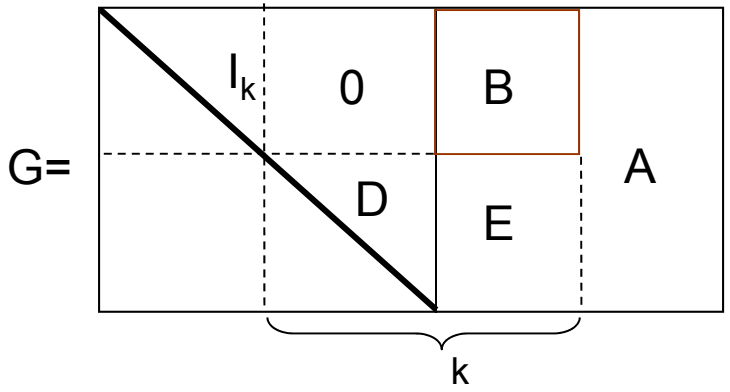
Proof: (i) $\Rightarrow$ (iii) dist(C)=d, so every d-1=n-k columns of H are l.i.

(iii) $\Rightarrow$ (ii) Every n-k columns of H can be reduced to a diagonal matrix I_{n-k}, so these n-k positions can be taken as the positions of check symbols. Hence, the remaining k positions form an information set.

(ii) $\Rightarrow$ (iv) Viewing G as parity-check matrix of $C^{\perp}$, we observe that the distance $d(C^{\perp}) \geq k+1=n-\dim(C^{\perp})+1$. Thus, $C^{\perp}$ satisfies the Singleton bound.

(iv) $\Rightarrow$ (i) By exchanging the roles of C and $C^{\perp}$

(ii) $\Leftrightarrow$ (v) Consider any square submatrix B of A.



If B is k x k then the claim follows from (ii). Otherwise, let B be of order $b \leq$ k-1 and consider the "complementary" submatrix D of I_k with k-b columns as shown. The k x k matrix

$$M = \begin{pmatrix} 0 & B \\ D & E \end{pmatrix}$$

satisfies $0 \neq \det M = \det B$, as required.

(vi) $\Rightarrow$ (i) – obvious

(i) $\Rightarrow$ (vi) - omitted ▲

Note that the error probability of decoding up to half the distance for MDS codes (for instance, for Reed-Solomon codes, to be introduced) is easy to compute exactly.

Fact: The only binary MDS codes are the [n,n-1,2], [n,1,n], [n,n,1] codes.

The definition of RS codes above is slightly more general than the conventional definition, which is given in the following

Theorem 12.4. Let C be an RS code of length n | q-1 and let $\beta \in \mathbb{F}_q$ be an element of order n. Suppose the defining set of points for the code C is $\mathscr{P}=(1,\beta,\ldots,\beta^{n-1})$. Then the parity-check and generator matrices of C are

$$H = \begin{pmatrix} 1 & \beta & \ldots & \beta^{n-1} \\ 1 & \beta^2 & \ldots & \beta^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{n-k} & \ldots & \beta^{(n-k)(n-1)} \end{pmatrix} \qquad G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \beta & \ldots & \beta^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{k-1} & \ldots & \beta^{(n-1)(k-1)} \end{pmatrix}$$

Proof: Let $f(x)=f_0+f_1x+\ldots+f_{k-1}x^{k-1}$ and let $\mathbf{c}=\text{eval}(f)=(f(1),f(\beta),\ldots,f(\beta^{n-1})) \in C$

$c_i=f(\beta^i)$, so $\mathbf{c}= (f_0,f_1,\ldots,f_{k-1})\, G$, i.e. G is a generator matrix

$$(GH^T)_{i,r}=\sum_{j=1}^{n} (\beta^{j-1})^{i-1}\,(\beta^{j-1})^{r} = \sum_j \beta^{(i+r-1)(j-1)}$$

Since $i+r-1 \leq n-1$, $\gamma:=\beta^{i+r-1} \neq 1$. Then

$(GH^T)_{i,r} = \sum_j \gamma^{j-1}=(\gamma^n-1)/(\gamma-1)=0$ since ord (γ) | n.

Extended RS codes, maximum length of MDS codes

Observe that as we defined it, the length of an RS code $n \leq q-1$.

We can construct extended RS codes of length n=q,q+1,
and in some (very few, exceptional) cases n=q+2

It is conjectured that no nontrivial MDS codes longer than these parameters exist (this is called the MDS conjecture and is considered a very difficult problem).

For more on the MDS conjecture see R. Roth's book, pp. 342-346.

Generalized Reed-Solomon codes

Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial, let $\mathscr{P} = (\alpha_1, \ldots, \alpha_n) \subset \mathbb{F}_q$ and let $v_1, v_2, \ldots, v_n$ be nonzero elements of $\mathbb{F}_q$

Definition 12.2: An [n,k] q-ary GRS code

$$C = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n),\ 0 \leq \deg f \leq k-1\}$$

In other words, every coordinate in the code is scaled by a fixed nonzero element of $\mathbb{F}_q$.

Theorem 12.5: The generator matrix of a GRS code C can be written in the form

$$G_{\mathrm{GRS}} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} \begin{pmatrix} v_1 & & & \\ & v_2 & & \\ & & \ddots & \\ & & & v_n \end{pmatrix}$$

Exercise: prove this theorem, find a parity-check matrix of C.

GRS codes form a rather general class of MDS codes; in some cases, there are *no other* MDS codes.

ENEE626 Lecture 13: Decoding RS codes Berlekamp-Welch and Peterson's algorithms

RS codes are optimal with respect to error correction properties
They correct any combination of [(n-k)/2] errors and many error patterns of larger weights

There is a variety of polynomial-time decoding algorithms:

Unique decoding algorithms:
Peterson-Gorenstein-Zierler (1960, 61)
Berlekamp-Massey (1968-69); many versions, most used
Berlekamp-Welch (1984)

List decoding algorithms:
Sudan (1997)
Guruswami-Sudan (1999)

Erasure correction with RS codes

Recall the erasure channel from lecture 1.

Theorem 13.1: An [n,k,d] linear code corrects any combination of t errors and s erasures as long as $2t+s \leq d-1$.

Proof: obvious.

Consider correction of erasures only (t=0) with RS codes

C[n,k,d] RS code. Suppose that $\mathbf{c} \in C$ was transmitted and a vector $\mathbf{r}$ was received. Let $E \subset \{1,2,\ldots,n\}$, $|E|=s$ be a set of erased positions.

$c_i=r_i$ for $i \in E^c$.

Since $s \leq n-k$, the remaining $\geq k$ positions contain an information set.

Thus there is exactly one $\mathbf{c} \in C$ s.t. $\text{proj}_{E^c}\ \mathbf{c} = \text{proj}_{E^c}\ \mathbf{r}$

$\mathbf{c}$ can be found by solving a system of linear equations.

Example: Consider a [7,4,4] RS code over $\mathbb{F}_8$. Let α be a primitive 7th degree root of unity, α is a root of $f(x)=x^3+x+1$
Suppose that $m(x)=x+\alpha\, x^2+\alpha\, x^3$ is the message to be encoded.

Let $c=\text{eval}(m)=(1\alpha^5\alpha 1\alpha^5\alpha^6\alpha^5)$, $\mathbf{r}=(1\alpha^5\alpha 1{*}{*}\alpha^5)$

$\mathbf{h}_1\ \mathbf{h}_2\ \mathbf{h}_3\ \mathbf{h}_4\ \mathbf{h}_5\ \mathbf{h}_6\ \mathbf{h}_7$

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \end{pmatrix}$$

$\mathbf{r} =\ 1\ \alpha^5\ \alpha\ 1\ *\ *\ \alpha^5$

unknowns $\quad c_5\ c_6$

$H.\mathbf{r}^T=\mathbf{h}_1+\alpha^5\,\mathbf{h}_2+\alpha\,\mathbf{h}_3$
$+\mathbf{h}_4+\mathbf{h}_5c_5+\mathbf{h}_6c_6+\alpha^5\,\mathbf{h}_7=0$

Use the first two equations to correct erased

$c_5\alpha^4 + c_6\,\alpha^5=1 + \alpha^6 + \alpha^4=\alpha$ (*)

$c_5\,\alpha + c_6\,\alpha^3=1$ (**)

$$c_5 = \frac{\begin{vmatrix} \alpha & \alpha^5 \\ 1 & \alpha^3 \end{vmatrix}}{\begin{vmatrix} \alpha^4 & \alpha^5 \\ \alpha & \alpha^3 \end{vmatrix}} = \frac{\alpha^4+\alpha^5}{\alpha^2} = \alpha^{-2} = \alpha^5.$$

$$c_6 = \frac{\begin{vmatrix} \alpha^4 & \alpha \\ \alpha & 1 \end{vmatrix}}{\alpha^2} = \frac{\alpha^4+\alpha^2}{\alpha^2} = \alpha^2+1 = \alpha^6.$$

$\mathbb{F}_8$: $\alpha^3=\alpha+1$

000	0
001	1
010	α
100	α^2
011	α^3
110	α^4
111	α^5
101	α^6

Alternatively, assume that we know that coordinates r_4 and r_5 are in error but do not know the values of the errors. Then compute the syndrome $H.\mathbf{r}^T = (S_1\ S_2)^T$ by adding $r_5\alpha^4+r_6\alpha^5$ to right side of (*) and $r_5\alpha+r_6\alpha^3$ to right side of (**), then solve the system

$e_5\alpha^4 + e_6\,\alpha^5=S_1$

$e_5\,\alpha + e_6\,\alpha^3=S_2$

for the unknowns $e_5=r_5-c_5$, $e_6=r_6-c_6$

Conclude: correcting errors with known locations is the same as correcting erasures.

State a general result from the previous example.
Let n|q-1, $\beta \in \mathbb{F}_q$, ord(β)=n

Suppose that we are given the locations of errors but not their values.

We have $c_i+e_i=r_i$, $e_i \neq 0$ only for $i \in$ {error locations}

$S_j = H\, r^T = \sum_{i \in \{\text{error locations}\}} \mathbf{h}_i\, e_i$ ($\mathbf{h}_i$ is the ith col. of H)

Theorem 13.2: Let $i_1,\ldots,i_\nu$ be the error locations. The error values $e_1,\ldots,e_\nu$ can be found from the system

$$\begin{bmatrix} \beta^{i_1-1} & \beta^{i_2-1} & \cdots & \beta^{i_\nu-1} \\ \beta^{2(i_1-1)} & \beta^{2(i_2-1)} & \cdots & \beta^{2(i_\nu-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{\nu(i_1-1)} & \beta^{\nu(i_2-1)} & \cdots & \beta^{\nu(i_\nu-1)} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_\nu \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_\nu \end{bmatrix}$$

Berlekamp-Welch decoding algorithm for error correction with RS codes

C[n,k,d] RS code with defining set $\mathcal{P}=(\alpha_1,\alpha_2,\ldots,\alpha_n)$
received vector $\mathbf{r}=\mathbf{c}+\mathbf{e}$, $e\in \mathbb{F}_q^n$ is the error vector, $wt(\mathbf{e})\leq \tau=[(n-k)/2]$

Lert $Q(x,y)=Q_0(x)+yQ_1(x)\in \mathbb{F}_q[x,y]$ be a nonzero polynomial such that

$$Q(\alpha_i,r_i)=0,\ i=1,2,\ldots,n$$
$$\deg Q_0 \leq n-1-\tau$$
$$\deg Q_1 \leq n-1-\tau-(k-1)$$

A nonzero polynomial with these properties exists. Indeed, the number of unknown coefficients is
$\#\{(Q_{0,0},\ldots,Q_{0,n-1-\tau}),(Q_{1,0},\ldots,Q_{n-1-\tau-(k-1)})\} = 2n-2\tau-k+1 \geq 2n-n+k-k+1=n+1$
These coefficients satisfy n homogeneous equations, so a nonzero solution exists.

Theorem 13.3: If $wt(\mathbf{e})\leq \tau$ and $\mathbf{c}$=eval (f) then $f=-Q_0/Q_1$.
Proof. $\deg(Q(x,f(x)))\leq \max(n-1-\tau,k-1+n-1-\tau-(k-1))=n-1-\tau$.
$Q(\alpha_i,f(\alpha_i))=0$ if $c_i=r_i$, so $Q(x,f(x))$ has $\geq n-\tau$ zeros. Then $Q\equiv 0$, or $Q_0+f\,Q_1=0$. ▲

Algorithm BW: Given $\mathbf{r}=(r_1,\ldots,r_n)$, $l_0=n-1-\tau$, $l_1=n-1-\tau-(k-1)$

1. Find *any* nonzero solution of the system

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{l_0} & r_1 & r_1\alpha_1 & r_1\alpha_1^2 & \ldots & r_1\alpha_1^{l_1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{l_0} & r_2 & r_2\alpha_2 & r_2\alpha_2^2 & \ldots & r_2\alpha_2^{l_1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{l_0} & r_n & r_n\alpha_n & r_n\alpha_n^2 & \ldots & r_n\alpha_n^{l_1} \end{pmatrix} \mathbf{Q}^T = 0$$

where $\mathbf{Q}=((Q_{0,0},Q_{0,1},\ldots,Q_{0,l_0}),(Q_{1,0},Q_{1,1},\ldots,Q_{1,l_1}))$

(complexity $O(n^3)$)

2. Find $f(x)=-\sum_{i=0}^{l_0} Q_{0,i}x^i / \sum_{i=0}^{l_1} Q_{1,i}x^i$

3. If found $f(x) \in \mathbb{F}_q[x]$, decode as $\mathbf{c}=\text{eval}(f)$

Overall complexity is $O(n^3)$; faster implementations are possible

Remarks.

1.

$$Q(x,y) = Q_1(x)y + Q_0(x) = Q_1(x)\left(y + \frac{Q_0(x)}{Q_1(x)}\right) = Q(x)(y - f(x))$$

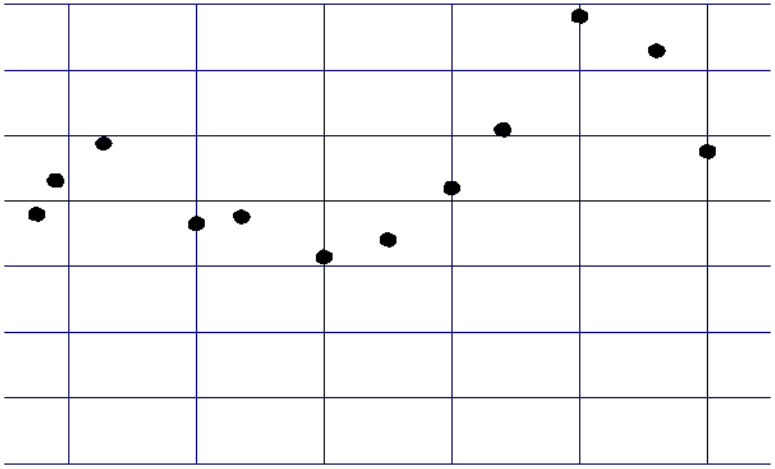
$$Q(\alpha_i, r_i) = Q_1(\alpha_i)(r_i - f(\alpha_i)) \equiv 0$$

Either $r_i = f(\alpha_i)$ ($e_i = 0$, no error) or $Q_1(\alpha_i) = 0$.

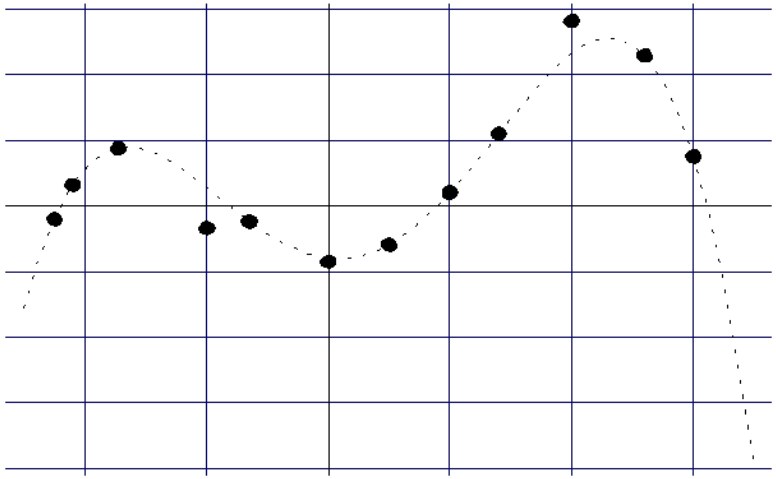
Hence $Q_1(\alpha_i)=0$ if $e_i \neq 0$. Thus the roots of Q_1 locate errors in **r**, so Q_1 is the error locator polynomial.

2. Given a set of points (α_i, r_i), i=1,…,n in the (x,y) plane over $\mathbb{F}_q$, we need to find a polynomial f(x) of degree $\leq$ k-1 that passes through at least $n-\tau \geq (n+k)/2$ of these points. This task is called interpolation or curve fitting. RS decoding $\equiv$ interpolation.

Example (artist's impression): Given a set of 12 points



find a curve of degree ≤ 4 that passes through 10 or more points.
Answer: the curve is $y+0.1x^4-0.2x^3-3x^2+x+8=0$, there are 2 "errors"



Another version of Berlekamp-Welch
(the Peterson-Gorenstein-Zierler algorithm)

Let $n|(q-1)$, $\mathcal{P}=(1,\beta,\ldots,\beta^{n-1})$, where $\text{ord}(\beta)=n$

Let C be a q-ary RS code of length n with defining set $\mathcal{P}$

Let $\mathbf{r}=(r_1,r_2,\ldots,r_n)$ be the received vector (a code vector + τ or fewer errors)

Parity-check matrix

$$H=\begin{pmatrix} 1 & \beta & \ldots. & \beta^{n-1} \\ 1 & \beta^2 & \ldots & \beta^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{n-k} & \ldots & \beta^{(n-k)(n-1)} \end{pmatrix}$$

Compute the syndrome $H\,\mathbf{r}^T=(S_1\ S_2\ \ldots\ S_{n-k})^T$, where

$$S_i=\sum_{j=1}^{n} r_j\,\beta^{i(j-1)}=r(\beta^i) \quad \text{and } r(x)=r_1+r_2x+\ldots+r_n\,x^{n-1}$$

Theorem 11.4:

$$\begin{pmatrix} S_1 & S_2 & \ldots & S_{l_1+1} \\ S_2 & S_3 & \ldots & S_{l_1+2} \\ \vdots & \vdots & \ddots & \vdots \\ S_{l_1} & S_{l_1+1} & \ldots & S_{2l_1} \end{pmatrix} \begin{pmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{pmatrix} = 0$$

Proof: Let

$$A=\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \beta & \dots & \beta^{\ell_0} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{n-1} & \dots & \beta^{\ell_0(n-1)} \end{bmatrix} \qquad B=\begin{bmatrix} r_1 & r_1 & \dots & r_1 \\ r_2 & r_2\beta & \dots & r_2\beta^{\ell_1} \\ \vdots & \vdots & \vdots & \vdots \\ r_n & r_n\beta^{n-1} & \dots & r_n\beta^{\ell_1(n-1)} \end{bmatrix}$$

$\mathbf{Q}_0=(Q_{0,0},Q_{0,1},\dots,Q_{0,l_0})$, $\mathbf{Q}_1=(Q_{1,0},Q_{1,1},\dots,Q_{1,l_1})$

Then the system in the BW algorithm has the form

$$A\mathbf{Q}_0^T+B\mathbf{Q}_1^T=0 \qquad (1)$$

Take

$$D=\begin{pmatrix} 1 & \beta & \dots & \beta^{n-1} \\ 1 & \beta^2 & \dots & \beta^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{\ell_1} & \dots & \beta^{\ell_1(n-1)} \end{pmatrix}$$

Note that DA=0, so the system (1) can be written as

$$DB\mathbf{Q}_1=0 \qquad (2)$$

Compute the (i,j)th element of the matrix DB, $1 \le i \le l_1$,$1 \le j \le l_1+1$: it is

$$\sum_{s=1}^{n} \beta^{i(s-1)} r_s \beta^{(s-1)(j-1)}=\sum_s r_s \beta^{(s-1)(i+j-1)}=r(\beta^{i+j-1})= S_{i+j-1}$$ ▲

Algorithm of Peterson-Gorenstein-Zierler for RS decoding.

Given $r=(r_1,r_2,\ldots,r_n)$.

1. Compute the syndromes $S_1,S_2,\ldots, S_{n-k}$
2. Solve the system

$$\begin{pmatrix} S_1 & S_2 & \cdots & S_{l_1+1} \\ S_2 & S_3 & \cdots & S_{l_1+2} \\ \vdots & \vdots & \ddots & \vdots \\ S_{l_1} & S_{l_1+1} & \cdots & S_{2l_1} \end{pmatrix} \begin{pmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{pmatrix} = 0$$

for the smallest $l_1 \leq \lfloor (n-k)/2 \rfloor$ *that gives a nonzero solution.*

3. Find the error locations as the roots of the polynomial

$$Q_1(x)=Q_{1,0}+Q_{1,1}x+\ldots+Q_{1,l_1}x^{l_1}.$$

This is done by trying all the elements $\{1,\beta,\ldots,\beta^{n-1}\}$ in $\mathcal{P}$.

4. Once the error locations have been found to be $i_1,i_2,\ldots,i_\nu$, solve the system of linear equations to recover the error values
(recall the example earlier in this lecture)

$$\begin{bmatrix} \beta^{i_1-1} & \beta^{i_2-1} & \cdots & \beta^{i_\nu-1} \\ \beta^{2(i_1-1)} & \beta^{2(i_2-1)} & \cdots & \beta^{2(i_\nu-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{\nu(i_1-1)} & \beta^{\nu(i_2-1)} & \cdots & \beta^{\nu(i_\nu-1)} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_\nu \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_\nu \end{bmatrix}$$

Decode as c=r-e, where e has the values $e_1,e_2,..,e_\nu$ in locations $i_1,i_2,\ldots,i_\nu$.

Complexity of the algorithm $O(n^3)$ (naive implementation)

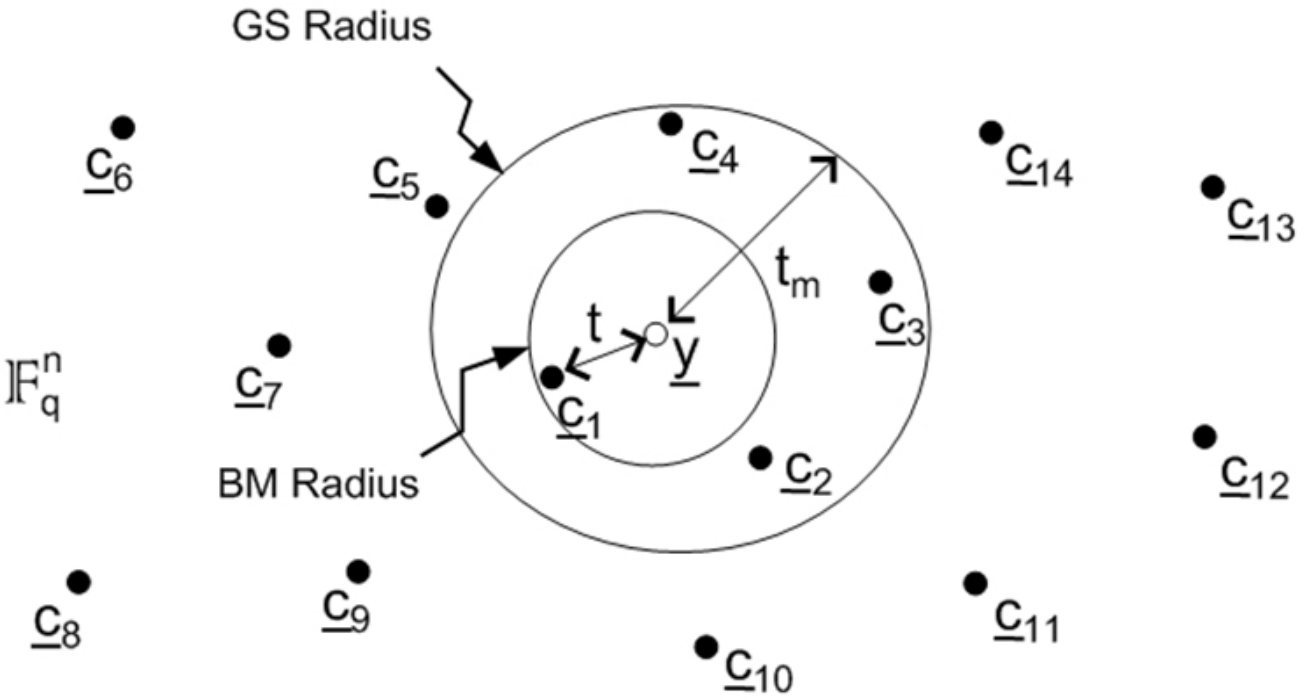
ENEE626 Lecture 14: List Decoding of Codes. Sudan's algorithm

List decoding

C[n,k,d] a linear code

Any t=(d-1)/2 or fewer errors will be corrected

Let $\boldsymbol{y}$ be the received vector. Any sphere of radius t contains ≤ 1 codeword. Some spheres of greater radius contain 2 or more codewords



Definition 14.1: A code C is said to correct r errors under decoding into a list of size l if every sphere of radius r in $\mathbb{F}_q^n$ contains $\leq l$ codewords.

Intuition: The decoder makes a list of all codewords within radius r of the received word. The list is guaranteed to be of size $\leq l$. The case l =1 corresponds to conventional decoding.

Later on, the decoder can select the most plausible codeword from the list (i.e., perform the max-likelihood procedure within the list) at the complexity expense of O(nl) operations.

A code C is said to correct r errors under decoding into a polynomial-size list if every sphere of radius r in $\mathbb{F}_q^n$ contains O(p(n)) codewords, where p(n) is some polynomial.

Note that in some situations both the unique decoding algorithms and list decoding algorithms will find no codewords within their designated error correcting radius (unless the list decoding radius is very large, but this often makes list decoding impractical, reducing it to ML decoding).

C[n,k,d] RS code with defining set $\mathcal{P}=(\alpha_1,\alpha_2,\ldots,\alpha_n)$
received vector **r=c+e, e** $\in \mathbb{F}_q^n$ is the error vector, wt(**e**)$\leq \tau$ (some number)

Let $Q(x,y)=Q_0(x)+Q_1(x)y+Q_2(x)y^2+\ldots+Q_l(x)y^l$ be such that

$Q(\alpha_i,r_i)=0 \quad i=1,\ldots,n$ (a)
$\deg(Q_j(x)) \leq n-\tau-1-j(k-1), \quad j=0,1,\ldots,l$

Lemma 14.1: If c=eval(f) and wt(e) $\leq \tau$ then

$$(y-f(x)) \mid Q(x,y)$$

Proof: deg $Q(x,f(x)) \leq n-\tau-1$

Since $\#\{i: r_i \neq f(\alpha_i)\} \leq \tau$, $Q(\alpha_i,f(\alpha_i))=0$ for $\geq n-\tau$ values of i. Hence $Q(x,f(x))\equiv 0$, or f(x) is a y-root of Q, i.e., $(y-f(x)) \mid Q(x,y)$ ▲

Since $\deg_y Q \leq l$, there are at most l codewords on the list

Remarks:

1. l is (an upper bound on) the size of the list
2. Sometimes one uses notation

$\deg_{1,k-1} f(x,y)$
$=\deg_x f+(k-1)\deg_y f$

So $\deg_{1,k-1} Q \leq n-\tau-1$

Under which conditions does the system (a) have a nonzero solution?

of coefficients in the polynomial Q

$(l+1)(n-\tau) - \sum_{j=1}^{l} j(k-1) = (n-\tau)(l+1) - (k-1)l(l+1)/2$

Thus if $(n-\tau)(l+1) - (k-1)l(l+1)/2 > n$, we can always find a nonzero solution Q

This gives a sufficient condition

$$\tau < \frac{\ell n}{\ell + 1} - (k-1)\frac{\ell}{2} \qquad (1)$$

At the same time we also need deg $Q_j(x) = n-\tau-1-j(k-1)$, $j=0,\ldots,l$ to be nonnegative. This implies

$$n-\tau > l\,(k-1) \qquad (2)$$

The analysis of Sudan's algorithm is performed by juxtaposing (1) and (2)

Sudan's algorithm

Given $\mathscr{P}=(\alpha_i, i=1,\ldots,n)$, $\mathbf{r}=(r_1,\ldots,r_n)$, $\tau \in \mathbb{N}$

1. Solve the system

$$\sum_{j=0}^{\ell} r_i^j \sum_{m=0}^{\ell_j} Q_{j,m} x_i^m = 0$$

where $i = 1, 2, \ldots, n$, $\ell_j = n - \tau - 1 - j(k-1)$,
for the coefficients $\{Q_{j,m}\}$.

2. Find y-roots of $Q(x, y)$, i.e., represent it in the form
$Q(x, y) = \prod_\lambda (y - f_\lambda(x)) P(x, y)$
Discard the roots f with $\deg f \geq k$.

3. For every f left after step 2, verify if
d(eval(f), **r**) $\leq \tau$
If yes, output **c**=eval(f)

Special cases:

$l=1$. From (1), $\tau < (n-k+1)/2$ BW decoding

$l=2$. $l < (2n/3)-k+1$ and $\tau < n-2(k-1)$

Suppose that $n-2(k-1) > (2n/3)-k+1 \Leftrightarrow k/n < (1/3) + 1/n$

Thus if $k/n < (1/3) + 1/n$, the error correction radius $\tau < (2n/3) -k +1$

$\tau/n < -(k/n) + (2/3) +1/n$

On the other hand, if $k/n > (1/3) + 1/n$, then the condition (2) $\tau < n-2(k-1)$ is more restrictive. Indeed, it is $\tau < d-k+1$, Compare this to (d/2):

$(d/2) - (d-k+1)= (n-k)/2 -d+k-1 = (1/2)(-n+3k-4) > 0$,

so $\tau < d/2$, the algorithm does not even reach the d/2 radius

Generally, given l, the number of correctable errors satisfies

$$\frac{\tau}{n} < \left(-\frac{\ell}{2}\frac{k}{n} + \frac{\ell}{\ell+1} + \frac{\ell}{2n}, -\ell\frac{k}{n} + 1 + \frac{\ell}{n} \right)$$

For small R=k/n the first term is more restrictive (R<2/(l(l+1))
The improvement occurs if the number of correctable errors >(n-k)/2.
The first term satisfies this condition for R<$R_1(l) \triangleq$ 1/(l+1)
the second for R<$R_2(l) \triangleq$ 1/(2l-1)

$R_1(2)=R_2(2)$ and $R_1(l)>R_2(l)$ for $l>2$

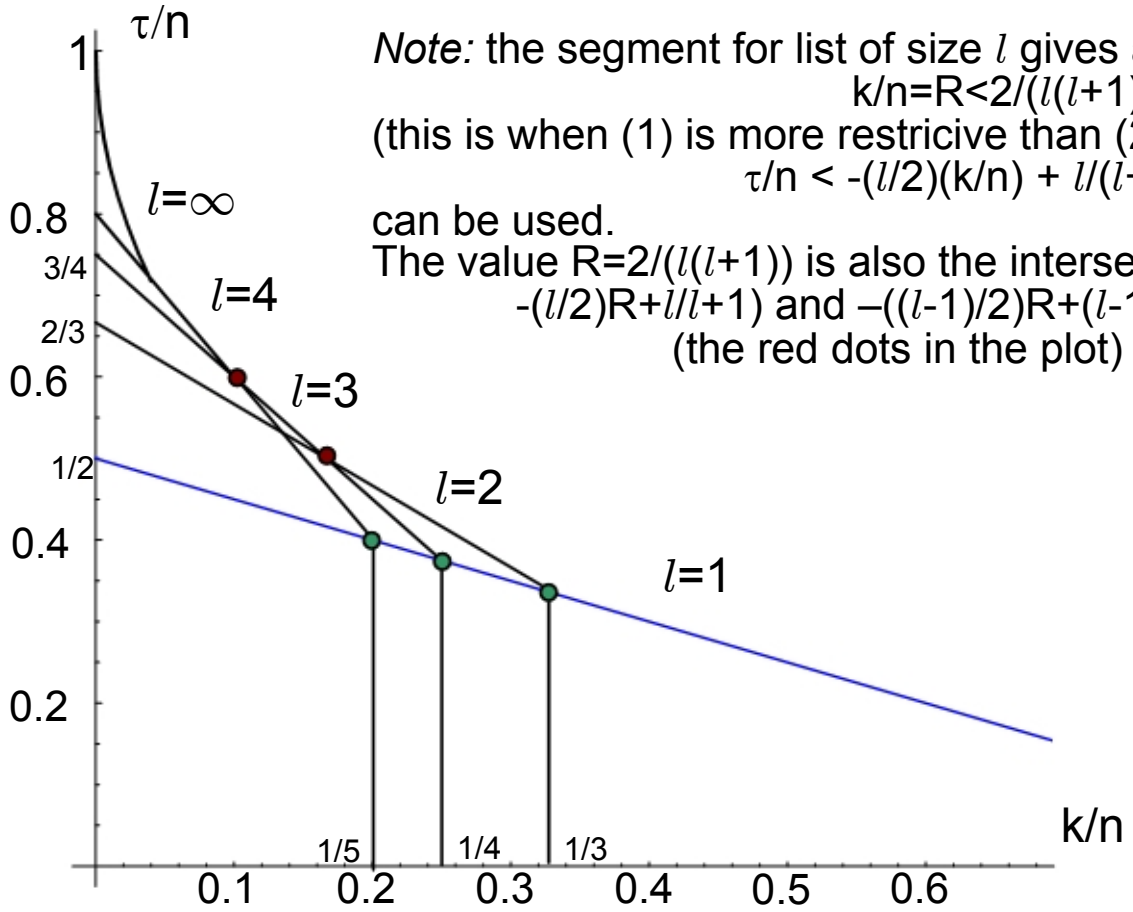
All claims are verified by direct calculations. For instance, let us compute $R_1(l)$:

$$\frac{\ell n}{\ell+1} - (k-1)\frac{\ell}{2} > \frac{n-k+1}{2}$$

$$\Leftrightarrow \frac{2\ell}{\ell+1} n - k\ell + \ell > n - k + 1$$

$$\Leftrightarrow \frac{k}{n} < \frac{1}{\ell+1} + \frac{1}{n}$$

1. l=1 (BW decoding) τ/n < (n-k)/(2n)=(1/2)-k/2n,for all k/n
2. l=2 τ/n < -k/n + 2/3, for k/n < 1/3
3. l=3 τ/n < -1.5 k/n + 3/4, for k/n < 1/4
4. l=4 τ/n < -2k/n + 4/5, for k/n < 1/5



Note: the segment for list of size l gives a valid bounds for
k/n=R<2/(l(l+1))
(this is when (1) is more restricive than (2), so the equation
τ/n < -(l/2)(k/n) + l/(l+1)
can be used.
The value R=2/(l(l+1)) is also the intersection point of
-(l/2)R+l/l+1) and –((l-1)/2)R+(l-1)/l
(the red dots in the plot)

Asymptotic analysis of Sudan's algorithm

Theorem 14.3: Let $n \to \infty$, $l \to \infty$, $2n < l^2(k-1)$; $k/n = R$. The algorithm corrects τ errors under algebraic decoding into a list of size l as long as

$$\tau/n < 1 - \sqrt{2R}$$

Proof: Let

$$\tau_0 = n - \ell(k-1) - 1 \qquad (3)$$

The choice $\tau = \tau_0$ fulfils condition (2). To prove that it also fulfils (1), substitute τ_0 in (1)

$$\tau_0 + (k-1)\frac{\ell}{2} \stackrel{?}{<} \frac{\ell n}{\ell+1}$$

$$n - \ell(k-1) - 1 + (k-1)\frac{\ell}{2} \stackrel{?}{<} \frac{\ell n}{\ell+1}$$

$$2n - \ell^2(k-1) \stackrel{?}{<} \ell(k-1) + 2\ell + 2$$

Hence if $2n < l^2(k-1)$, (1) is satisfied, too. Now, $l(k-1) > \sqrt{2n(k-1)}$, so from (3)

$$\tau_0 < n - \sqrt{2n(k-1)}$$

$$\frac{\tau_0}{n} < 1 - \sqrt{2R - 2/n}$$

■

ENEE626 Lectures 15-16: List Decoding of Codes. The Guruswami-Sudan algorithm

Goal: to correct $\tau > d/2$ errors for all rates $0<R<1$, not just for $R<1/3$.

Idea: Relax the solvability condition (1) of Sudan's algorithm by creating more than n independent linear conditions.

Technical tools:

1. Multiplicity of points

$f(x)=x^2-4x+3=-2(x-1)+(x-1)^2$ has a zero at $x_0=1$
$f(x)=(x-1)^3$ has zero of multiplicity 3 at $x_0=1$ since $f(x_0)=f'(x_0)=f''(x_0)=0$
$f(x)=2x^3-9x^2+12x-5=-3(x-1)^2+2(x-1)^3$ has zero of mult. s=2 at $x_0=1$

$$df/dx|_{x=1}=(6x^2-18x+12)|_{x=1}=0$$

Definition 15.1: A function

$$f(x)=f(x_0)+f'(x_0)(x-x_0)+(1/2)f''(x_0)(x-x_0)^2+\ldots+(1/(m-1)!)\,f^{(m-1)}(x_0)(x-x_0)^{m-1}+\ldots$$

is said to have a zero of multiplicity m at $x=x_0$ if the first m terms of its power series in the neighborhood of x_0 vanish.

A function f(x,y) is said to pass through a point (a,b) with multiplicity s if in the Taylor expansion of f(x,y) in the neighborhood of (a,b) all the monomials x^iy^j with $i+j<s$ vanish.

2. How does this work in finite characteristic?

Let $Q(x,y)=\sum_{i,j} Q_{ij}x^i y^j \in \mathbb{F}_q[x,y]$

$$\bar{Q}(x,y) = Q(x+a,y+b) = \sum_{i,j} Q_{i,j}(x+a)^i(y+b)^j$$

$$= \sum_{i,j} Q_{i,j} \sum_{\alpha=0}^{i} \binom{i}{\alpha} x^\alpha a^{i-\alpha} \sum_{\beta=0}^{j} \binom{j}{\beta} y^\beta b^{j-\beta}$$

$$= \sum_{\alpha,\beta} x^\alpha y^\beta \sum_{\substack{i,j \\ i\geq\alpha, j\geq\beta}} Q_{i,j}\binom{i}{\alpha}\binom{j}{\beta} a^{i-\alpha} b^{j-\beta}$$

$$= \sum_{\alpha,\beta} \bar{Q}_{\alpha,\beta} x^\alpha y^\beta$$

Definition 15.2: A point (a,b) is called a zero of Q(x,y) of multiplicity s if all the monomials of degree $0 \leq \alpha+\beta < s$ in the expression Q(x+a,y+b) are equal to 0.

The quantity

$$\bar{Q}(x,y) = \sum_{\substack{i,j \\ i\geq\alpha, j\geq\beta}} Q_{i,j}\binom{i}{\alpha}\binom{j}{\beta} x^{i-\alpha} y^{j-\beta}$$

is called a Hasse derivative of Q(x,y): $\partial^{\alpha+\beta}Q(x,y)/\partial^\alpha x\, \partial^\beta y$ (of order α on x and β on y).

Example: Let $Q(x,y)=x^2 y+x^2+y+1 \in \mathbb{F}_2[x]$. Since $Q(x+1,y+1)=x^2 y$, the polynomial $Q(x,y)$ has a zero of multiplicity 3 at the point $(x=1,y=1)$.

Idea: Let $\mathscr{P}=(\alpha_1,\ldots,\alpha_n)$ be the defining set of an RS code, let **r** be the received vector.
Let us find a polynomial $Q(x,y)$ such that it passes through the points (α_i,r_i), i=1,..,n *with multiplicity* s.

Thus, let $Q(x,y)=\sum_j Q_j(x)\, y^j$ be a polynomial such that

(i) (α_i,r_i) is its zero of multiplicity s
(ii) $\deg (Q_j(x)) \leq s(n-\tau)-1-j(k-1)$, $\quad j=0,1,\ldots,l$

Lemma 15.1: Let c=eval(f), deg f$\leq$ k-1. Let Q be chosen to satisfy (i)-(ii).
Then (y-f(x)) | Q(x,y)

Proof:

(a) First show that if i is such that $f(\alpha_i)=r_i$ then $(x-\alpha_i)^s \mid Q(x,f(x))$. Let $p(x) = f(x+\alpha_i)-r_i$, then p(0)=0 or x | p(x). Consider $P(x) = Q(x+\alpha_i, p(x)+r_i)$. By definition of Q, 0 is its zero of multiplicity s, or $x^s \mid P(x)$, or $(x-\alpha_i)^s \mid P(x-\alpha_i) = Q(x,f(x))$.

(b) $\deg(Q(x,f(x)) \leq s(n-\tau)-1$. On the other hand, $(x-\alpha_i)^s \mid Q(x,f(x))$ for $\geq n-\tau$ values of i. The number of zeros (counted with multiplicities) is greater than the degree, therefore, $Q(x,f(x)) \equiv 0$.

Conditions for decoding.

1. $s(n-\tau)=l(k-1)+1$ $\quad$ $(\deg(Q_j) >0)$

2. #{coeffs of Q} $=(l+1)s(n-\tau)-(k-1)l(l+1)/2$
The monomials of degree $\alpha+\beta< s$ in $Q(x+\alpha_i,y+r_i)$ are 0, and there are $s(s+1)/2$ of them. This gives $n\, s(s+1)/2$ linear conditions.

Thus if
$$(\ell+1)s(n-\tau)-(k-1)\frac{\ell(\ell+1)}{2} > n\binom{s+1}{2}$$

or
$$\frac{\tau}{n} < -\frac{k}{n}\frac{\ell}{2s}+\frac{2\ell-s+1}{2(\ell+1)}+\frac{\ell}{2sn} \qquad (1)$$

the system $Q(\alpha_i,r_i)=0$ has a nonzero solution.

Our decoding will make sense if the right-hand side of (1) $\geq (1/2n)(n-k+1)$

Lemma 15.2: Assume that s<l. For any k such that

k/n < s/(l+1) + (1/n)

then the upper bound on τ in (1) is greater than d/2

Proof:

$$-k\frac{\ell}{2s} + n\frac{2\ell - s + 1}{2(\ell + 1)} + \frac{\ell}{2s} - \frac{n - k + 1}{2}$$

$$= 1/2\left(- k\frac{\ell}{s} - (n - k + 1) + n\frac{2\ell - s + 1}{\ell + 1} + \frac{\ell}{s}\right)$$

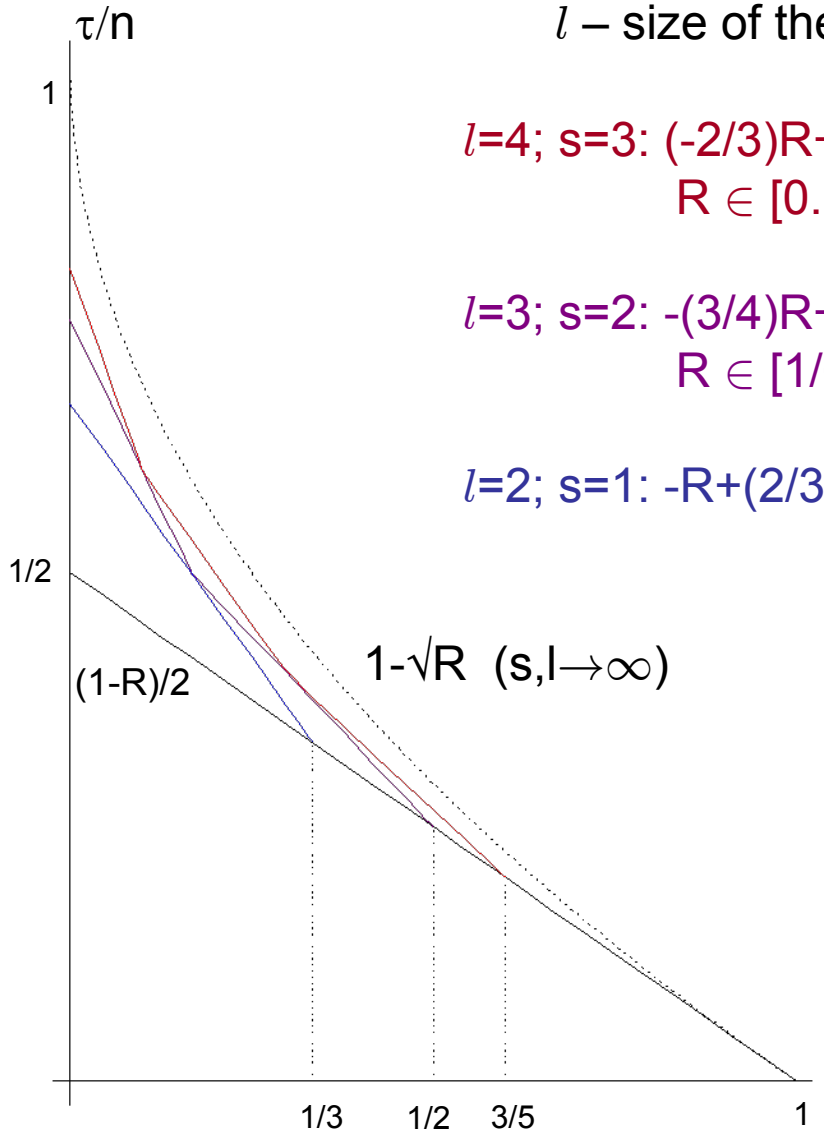
use the condition on k:

$$> 1/2\left[\left(- \frac{sn}{\ell + 1} - 1\right)\left(\frac{\ell}{s} - 1\right) - n - 1 + n\frac{2\ell - s + 1}{\ell + 1} + \frac{\ell}{s}\right]$$

=0 ▲

Next slide: analyze some special cases

Error correction radius of the Guruswami-Sudan algorithm



l – size of the list, s - multiplicity

l=4; s=3: (-2/3)R+(6/10); s=2: -R+(7/10); s=1: -2R+(8/10)
R ∈ [0.3,0.6] R ∈ [0.1,0.3] R ∈ [0,0.1]

l=3; s=2: -(3/4)R+(5/8) s=1: -(3/2)R+(3/4)
R ∈ [1/6,1/2] R ∈ [0,1/6]

l=2; s=1: -R+(2/3), $0 \le R \le 1/3$

Algorithm: Let **r** be the received word. Choose l and find the maximum τ and s that satisfy

$$s(n-\tau) = l(k-1)+1$$

$$s > \frac{n(k-1)+\sqrt{n^2(k-1)^2+4((n-\tau)^2-n(k-1))}}{2(n-\tau)^2-n(k-1)}$$

1. Solve the following system for $Q_{\sigma,\rho}$

$$\sum_{\sigma=0}^{\ell}\sum_{\rho=\alpha}^{\ell_\sigma}\binom{\rho}{\alpha}\binom{\sigma}{\beta}\alpha_i^{\rho-\alpha}r_i^{\sigma-\beta}Q_{\sigma,\rho}=0$$

for all $\alpha\geq 0$, $\beta\geq 0$, $\alpha+\beta < s$, i=1,…,n

2. Form the polynomial

$$Q(x,y)=\sum_{j=0}^{l}\left(\sum_{i=1}^{l_j} Q_{i,j}x^i\right)y^j$$

3. Find all y-roots f(x) of Q(x,y)

4. Output the codewords **c**=eval f that satisfy $d(\mathbf{c},\mathbf{r}) \leq \tau$.

Can be implemented with complexity $O(n^2s^4)$

Proof of consistency

Lemma 15.3: If $(n-\tau)^2 > n(k-1)$, s is chosen as above and l is taken to fulfill $s(n-\tau) = l(k-1) + 1$,

then

$$(\ell+1)s(n-\tau) - (k-1)\frac{\ell(\ell+1)}{2} > n\binom{s+1}{2}.$$

Proof: If $s > \dfrac{n(k-1) + \sqrt{n^2(k-1)^2 + 4((n-\tau)^2 - n(k-1))}}{2((n-\tau)^2 - n(k-1))}.$

then s satisfies

$$\frac{(n-\tau)s-1}{k-1}(s(n-\tau)+1) > n\frac{s(s+1)}{2}.$$

Since $(k-1)l=(n-\tau)s-1$, this implies that

$$\frac{\ell}{2}(\ell(k-1)+2) > n\frac{s(s+1)}{2}$$

The left-hand side of this inequality is less than

$$(\ell+1)s(n-\tau) - (k-1)\frac{\ell(\ell+1)}{2} \qquad \blacktriangle$$

ENEE626 Lecture 17: Structure of finite fields

Plan:

Minimal polynomials
Uniqueness of $\mathbb{F}_q$
Cyclotomic cosets and conjugate elements
Factorization of $x^{p^m}-x$

The purpose of this lecture is to prepare way for the study of BCH codes (an important class of cyclic codes)

Definition 17.1. A polynomial is called *monic* if its leading coefficient =1.

Definition 17.2. The *minimal polynomial* of $\beta \in \mathbb{F}_{p^m}$ *over* $\mathbb{F}_p$ is the lowest-degree monic polynomial m(x) such that $m(\beta)=0$

Let α be a root of $x^4+x+1 \in \mathbb{F}_2$. The minimal polynomial of α^3 over $\mathbb{F}_2$ is

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

Consider $\mathbb{F}_4 \subset \mathbb{F}_{16}$, It is formed of the elements $0,1,\omega,\omega^2$, where ω is an element of order 3 in $\mathbb{F}_{16}$. The minimal polynomial of α over $\mathbb{F}_4$ is

$$x^2+x+\omega$$

(indeed, taking $\omega=\alpha^5$, we observe $\alpha^2+\alpha+\alpha^5=0$)

In this lecture we will establish the following result.

Theorem 17.1: The polynomial $x^{p^m}-x$ factors over $\mathbb{F}_p$ as follows:

$$x^{p^m}-x=\prod_s m_s(x)$$

where the polynomials $m_s(x)$ exhaust all the minimal polynomials over $\mathbb{F}_p$ of degree d|m

Recall the following important fact:

$$a \in \mathbb{F}_q \Leftrightarrow a^q = a$$

Properties of minimal polynomials over $\mathbb{F}_p$

let $q=p^m$

1. m(x) is irreducible
2. Let m(x) be the minimal polynomial of β. If $f(\beta)=0$ then $m(x)|f(x)$
3. $m(x)|(x^{p^m}-x)$
4. deg (m(x)) $\leq$ m
5, The minimal polynomial of a primitive element (an element of order q-1) has degree m.

Proof. 2. For suppose not. Then let $f(x)=q(x)\, m(x)+r(x)$, deg r < deg m. Substitution of β shows that $r(\beta)=0$, contradiction.

3. For any $a \in \mathbb{F}_q^*$, $a^{p^m-1}-1=0$, or a is a root of $x^{p^m}-x$. Now use 2.

4. For any β, the elements $1,\beta,\beta^2,\ldots,\beta^m$ are linearly dependent over $\mathbb{F}_p$. Let $f_0+f_1\beta+\ldots+f_m\beta^m=0$,where some $f_i \neq 0$. Then $f(\beta)=0$, so either deg (m(x))=m or deg(m(x))|m.

5. By definition since $\mathbb{F}_{p^m}$ is an m^{th} degree extension of $\mathbb{F}_p$

Definition 17.3: Two finite fields F and G are called isomorphic if there exists a one-to-one mapping ϕ: F$\rightarrow$ G that satisfies

$$\phi(ab)=\phi(a)\phi(b),\ \phi(a+b)=\phi(a)+\phi(b) \qquad \forall\ a,b\in F \qquad (\mathcal{I})$$

Theorem 17.2: The finite field $\mathbb{F}_{p^m}$ is unique up to isomorphism.

Proof: Let F be a finite field, α primitive element, m(x) its minimal polynomial. $|F|=p^m$; $m(x)|(x^{p^m}-x)$.

Suppose there is another f.f. G, $|G|=p^m$, with primitive element γ.
Find j such that γ^j is a root of m(x). This is possible because the powers of γ exhaust the set of roots of $x^{p^m}-x$.
Now put $\phi(\alpha)=\gamma^j$. Clearly, properties $(\mathcal{I})$ are satisfied.

Example: $F=\mathbb{F}_{2^3}$, $m(x)=x^3+x+1$, $m(\alpha)=0$.
Now let G be a finite field of 8 elements with primitive element γ that satisfies $\gamma^3=\gamma^2+1$. Find j such that $m(\gamma^j)=0$.

j=3 does the job since $(\gamma^3)^3+\gamma^3+1=\gamma^2+(\gamma^2+1)+1=0$. Then put $\phi(\alpha)=\gamma^3$

Definition 17.4: A subfield $G \subset F$ is a subset of F which itself is a field.

Examples: $\mathbb{Q}$ is a subfield of $\mathbb{R}$; $\mathbb{F}_9$ is a subfield of $\mathbb{F}_{81}$, but not of $\mathbb{F}_{27}$
The elements $(0,1,\alpha^5,\alpha^{10})$ form a subfield of $\mathbb{F}_{16}$, which by the previous thm is $\mathbb{F}_4$

Theorem 17.3: $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^m}$ if and only if $s|m$

Lemma: $(x^s-1)|(x^m-1)$ (over any field) if and only if $s|m$.
Proof. If $m=rs$, we can write
$x^m-1=(x^s-1)(x^{m-s}+x^{m-2s}+\ldots+x^{m-(r-1)s}+1)$
Conversely, assuming $(x^s-1)|(x^m-1)$, divide x^m-1 by x^s-1 and argue that $s|m$ ▲

So in particular, $n^s-1|n^m-1$ if and only if $s|m$. ($n \in \mathbb{N}$)

Proof of Theorem: If $s|m$ then $p^s-1|p^m-1$, so $(x^{p^s-1}-1)|(x^{p^m-1}-1)$
This means that elements of $\mathbb{F}_{p^s}$ are contained in $\mathbb{F}_{p^m}$

Conversely, if $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^m}$ then any element $a \in \mathbb{F}_{p^s}$ is a root of $x^{p^m-1}-1$,
and at the same time of $x^{p^s-1}-1$, so $p^s-1|p^m-1$ and $s|m$. ▲

Cyclotimic cosets

Lemma 17.4: Over $\mathbb{F}_p$

$$(x+y)^{p^m}=x^{p^m}+y^{p^m}, \quad m\geq 1$$

Proof: Induction on m. For m=1, all the binomial coefficients p choose i are 0 mod p except for i=0,p. For the induction step, compute $((x+y)^{p^{m-1}})^p$

Theorem 17.5: If $\beta\in \mathbb{F}_{p^m}$ then β and β^p have the same minimal polynomial

Example: $\alpha, \alpha^2,\alpha^4,\alpha^8 \in \mathbb{F}_{16}$ have the minimal polynomial over $\mathbb{F}_2$

$$m_1(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$$
$$=x^4+x+1$$

Elements β and β^{p^i}, $i\geq 0$ are called conjugate over $\mathbb{F}_p$

Definition 17.5: *Cyclotomic coset* C_s is the set of exponents of all the elements conjugate with α^s. It is clear that $|C_s|$ divides m.

$C_0=\{0\}$	$m_0=x+1$
$C_1=\{1,2,4,8\}$	$m_1=m_2=m_4=m_8=x^4+x+1$
$C_3=\{3,6,9,12\}$	$m_3=m_6=m_9=m_{12}=x^4+x^3+x^2+x+1$
$C_5=\{5,10\}$	$m_5=m_{10}=x^2+x+1$
$C_7=\{7,11,13,14\}$	$m_7=x^4+x^3+1=m_{11}=m_{13}=m_{14}$

Theorem 17.6: The coefficients of m(x) are in $\mathbb{F}_p$.

Example: $m(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$.
For instance, compute the coeff of x^2

$$\mu_2=\alpha^{4+8}+\alpha^{2+8}+\alpha^{1+8}+\alpha^{2+4}+\alpha^{1+4}+\alpha^{1+2}$$

$$\mu_2^2=\alpha^{8+1}+\alpha^{4+1}+\alpha^{2+1}+\alpha^{4+8}+\alpha^{2+8}+\alpha^{2+4}=\mu_2$$

Proof: Let

$$m(x)=(x-\alpha^s)(x-\alpha^{sp})\dots(x-\alpha^{sp^{m_s-1}})=\mu_0+\mu_1 x+\dots+\mu_{m_s}x^{m_s}$$

where $m_s=\deg(m(x))$.

$$\mu_{m_s-j}=\sigma_j(\alpha^s,\alpha^{sp},\dots\alpha^{sp^{m_s-1}}),$$

where

$$\sigma_j(z_1,z_2,\dots,z_r)=\sum_{1\le i_1<i_2<\dots<i_j\le m_s} z_{i_1}z_{i_2}\dots z_{i_j}$$

is the j^{th} elementary symmetric function, $\mu_0=1$.

Let us check that $\mu_j^p=\mu_j$. Indeed, raising the coefficient μ_j to the p^{th} power just permutes the exponents:

$$(a^{sp^{i_1}}\alpha^{sp^{i_2}}\dots\alpha^{sp^{i_j}})^p=a^{s(p^{i_1+1})}\alpha^{s(p^{i_2+1})}\dots\alpha^{s(p^{i_j+1})}$$

However, σ_j includes all the monomials of this form (each exactly once), so raising μ_j to power p does not change it ▲

Now compute $g(x)=\prod_s m_s(x)$, where s goes over all representatives of cyclotomic cosets (a representative is the smallest exponent in the coset). g(x) is a monic polynomial of degree p^m that divides $x^{p^m}-x$, so $g(x)= x^{p^m}-x$. Also $\deg(m_s(x))=|C_s|$ divides m.

This proves the Theorem announced in the beginning of the lecture.

ENEE626 Lecture 18-19: Introduction to cyclic codes

Plan:

Cyclic representation of Hamming codes
BCH codes
Factorization of x^n-1 over $\mathbb{F}_q$
BCH and RS codes, subfield subcodes
Nonbinary Hamming code

Motivating Example: Consider the [7,4,3] Hamming code $\mathcal{H}_3$
Its parity-check matrix is formed of all the 7 nonzero 3-columns h_i.

Let α be a primitive element of $\mathbb{F}_8$ that satisfies $\alpha^3=\alpha+1$.

Let us order the columns of H in the order of increasing powers of α
using the basis $(1,\alpha,\alpha^2)$ to represent the elements of $\mathbb{F}_8$

$$H'=\begin{array}{c} \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Now let $\mathbf{c}=(c_0,c_1,\ldots,c_6) \in \mathcal{H}_3$ be a codeword, where the order of the coordinates is consistent with H'. Write $c(x)=\sum_{i=0}^{6} c_i x^i$.

Main observation: $H'\mathbf{c}^T=0 \Leftrightarrow c(\alpha)=0$

Note that if $c(x)\in \mathcal{H}_3$ then $xc(x) \bmod (x^7-1)\in \mathcal{H}_3$. Computing xc(x) corresponds to a right cyclic shift of c(x) by one. We have obtained a *cyclic representation* of the Hamming code.

This example is generalized to any $n=2^m-1$, giving a cyclic Hamming code $\mathcal{H}_m[n,n-m,3]$

Let us extend the previous construction to correcting 2 errors.
We will construct a subcode of $\mathcal{H}_m$ by isolating only those codewords of it that satisfy some additional parity checks,

Try α^2. However $c(\alpha)=0$ implies that $c(\alpha^2)=c(\alpha)^2=0$.
A set of independent checks is given by requiring that

$$c(\alpha^3)=c_0+c_1\alpha^3+c_2\alpha^{2.3}+\ldots+c_{n-1}\alpha^{(2^m-2).3}=0$$

Thus, let us add a row $1,\alpha^3,\alpha^{2.3},\ldots,\alpha^{(2^m-2).3}$ to H'.
Denote this code $BCH_m(2)$ (after Bose and Ray-Chaudhuri; and Hocquenghem)
1960 1959

Proof that the distance of the code is 5. Our proof will be *constructive* in the sense that we show that any 2 errors are correctable.
Number the coordinates of the code by the nonzero elements of $\mathbb{F}_{2^m}$.
Let y(x)=c(x)+e(x), where e(x) has 2 nonzero coefficients in locations

$$X_1=\alpha^i,\ X_2=\alpha^j$$

X_1 and X_2 are called the error locators. Let $y(\alpha)=S_1$, $y(\alpha^3)=S_3$ be the syndromes.

$$S_1=X_1+X_2$$
$$S_3=X_1^3+X_2^3$$

Compute $S_1^3+S_3=X_1X_2(X_1+X_2)$

Thus
$$X_1+X_2=S_1$$
$$X_1X_2=(S_1^3+S_3)/S_1$$

Remark:
X_1,X_2 satisfy the equation
$z^2+S_1z+(S_1^3+S_3)S_1^{-1}=0$

We have the following cases:
(a) $S_1=S_3=0$, no errors
(b) $S_1\neq 0$, $S_3=S_1^3$: one error in location X_1
(c) $S_1\neq 0, S_3\neq 0$, the system has a solution for X_1,X_2: correct the 2 bits
(d) If there are no solutions (this happens when $S_1=0$, $S_3\neq 0$ and in some other cases), we declare that there are more than 2 errors.

The parity-check matrix of $BCH_m(2)$ can be written symbolically as

$$\begin{pmatrix} 1,\alpha,\alpha^2,\ldots,\alpha^{2^m-2} \\ 1,\alpha^3,\alpha^{3.2},\ldots,\alpha^{3.(2^m-2)} \end{pmatrix}$$

where each entry is written as a binary column of m bits.
Thus, the parameters of the code are $[n=2^m-1,k=n-2m,d=5]$.
Since every codeword c(x) satisfies $c(\alpha)=c(\alpha^3)=0$, we say that α, α^3 are zeros of the code.

This generalizes as follows.
Definition 18.1: A primitive BCH code C over $\mathbb{F}_q$ is a cyclic code of length $n=q^m-1$ with zeros $\alpha^b,\alpha^{b+1},\ldots,\alpha^{b+\delta-2}$, where $b\geq 1,\delta\geq 2$.

Theorem 18.1: The parameters of C are $[n=q^m-1,\ k \geq n-m(\delta-1),d \geq \delta]$.
Proof: Let α be primitive in $\mathbb{F}_{q^m}$. The parity-check matrix of C has the form

$$H = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix}.$$

Let D be a submatrix of H formed of columns that start with exponents $i_1 b$, $i_2 b$,..., $i_{\delta-1} b$. $d(C) \geq \delta \Leftrightarrow \det(D) \neq 0$

$$\det(D) = \alpha^{b(i_1+i_2+\ldots+i_{\delta-1})} \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{i_1(\delta-2)} & \alpha^{i_2(\delta-2)} & \cdots & \alpha^{i_{\delta-1}(\delta-2)} \end{bmatrix} \neq 0,$$

since α is a primitive element, all the α^j's are different.
Hence, the Vandermonde determinant is nonzero.

The number of rows in the matrix (after expanding the entries into m-vectors over $\mathbb{F}_q$) has $m(\delta-1)$ rows. Hence, $\dim(C) \geq n - m(\delta-1)$. ▲

Terminology: $\mathbb{F}_q$ is called the symbol field of the code; $\mathbb{F}_{q^m}$ is called the locator field of the code. δ is called the designed (BCH) distance of the code.

Theorem 18.2: A BCH code whose locator field and symbol field coincide, is an [n=q-1,k,d] Reed-Solomon code over $\mathbb{F}_q$.

Proof: Take m=1. The parity-check matrix of the BCH code C has the same form as the RS parity-check matrix of lecture 10. ▲

Factorization of x^n-1 over $\mathbb{F}_q$

We can construct q-ary BCH-like codes not just for n=q-1, but also for any n|(q-1). Hereafter we will assume that (n,q)=1.

To make this work, we need to find the locator field, i.e., a finite field that contains zeros of x^n-1. Clearly, this is the smallest field $\mathbb{F}_{q^m}$ such that $(x^n-1)|\ (x^{q^m-1}-1)$. Therefore, find m such that $n|(q^m-1)$.

Note: this is always possible.

Example: Factor x^9-1 over $\mathbb{F}_2$. m=6: $9|2^6-1$.

The zeros of x^9-1 are called 9th degree roots of unity. They lie in $\mathbb{F}_{64}$

Let $\alpha \in \mathbb{F}_{64}$ be a primitive element.

$\theta=\alpha^7$ is a primitive 9th degree root of unity: $\theta,\theta^2,\ldots\theta^8=\alpha^{56}$ are all different, $\theta^9=1$

Cyclotomic cosets mod 9: {0}, {1,2,4,8,7,5}, {3,6}

Theorem 18.3: $x^n-1=\prod_s m_s(x)$, product of all minimal polynomials.

In the example, $x^9-1=m_0m_1m_3$, where $m_0=x+1$,

$m_1(x)=(x-\theta)(x-\theta^2)(x-\theta^4)(x-\theta^8)(x-\theta^7)(x-\theta^5)=x^6+x^3+1$

$m_3(x):=(x-\theta^3)(x-\theta^6)=x^2+x+1$

Calculations in finite fields can be done using GAP
http://www.gap-system.org/

```
gap> a:=Z(64);;x:=Indeterminate(GF(64),"x");;t:=a^7;;
gap> (x-t)*(x-t^2)*(x-t^4)*(x-t^8)*(x-t^7)*(x-t^5);
x^6+x^3+Z(2)^0
gap> (x-t^3)*(x-t^6);
x^2+x+Z(2)^0
gap>
```

More examples

```
gap> C:=ReedSolomonCode(15,5);
a cyclic [15,11,5]3..4 Reed-Solomon code over GF(16)
gap> GeneratorPol(C);
x_1^4+Z(2^4)^13*x_1^3+Z(2^4)^6*x_1^2+Z(2^4)^3*x_1+Z(2^2)^2
gap> IsCyclicCode(C);
true
```

Cyclic codes

We will number the coordinates of the code from 0 to n-1.

Definition 18.2: A code is called *cyclic* if $(c_0,c_1,\ldots,c_{n-2},c_{n-1})\in C$ implies that $(c_{n-1},c_0,c_1,\ldots,c_{n-2})\in C$

We use a *polynomial representation* of codewords, writing

$$c(x)=\sum_{i=0}^{n-1} c_i x^i$$

The property of being cyclic can be written as follows:

$c(x)\in C$ implies that $xc(x) \bmod (x^n-1) \in C$

Theorem 18.3: Let C be cyclic code.

(i) It contains a unique monic polynomial g(x) such that every $c(x)\in C$ is a multiple of g(x) (generator polynomial of C). $\deg(g(x))=n-k$

(ii) $g(x)|(x^n-1)$

(iii) Generator matrix of C

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ \ldots \\ x^{k-1}g(x) \end{pmatrix}=\begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 \\ 0 & & & & & & & 0 \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-k} \end{pmatrix}$$

Proof: Take $g(x)\neq 0$ a monic polynomial of the smallest degree in C.
Any c(x) is divisible by g because otherwise, the remainder would be of degree smaller than g:

$$c(x)=q(x)g(x)+r(x), \qquad r\neq 0; \deg(r)<\deg(g)$$

Then r(x) is a nonzero codeword of degree less than g, contradiction.
Further, the polynomials

$$g(x),\ xg(x),\ x^2g(x),\ldots,x^{n-\deg(g)-1}g(x) \qquad (\mathcal{B})$$

are linearly independent. So dim $C\geq n-\deg(g)$.
Next, every codeword has the form a(x)g(x) for some a, $0\leq \deg a\leq n-\deg(g)-1$.
It can be represented as a linear combination of the polynomials in $\mathcal{B}$, so dim C, n-deg(g). ▲

Example: $\mathcal{H}_3[7,4,3]$ the Hamming code $m_1(x)=x^3+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$
$c(x)\in\mathcal{H}_3$ iff $c(\alpha)=0$. Since $c(\alpha)=0$, also $c(\alpha^2)=c(\alpha^4)=0$, $m_1|c(x)$
Thus $g(x)=m_1$,

$$G=\begin{pmatrix}1101000\\0110100\\0011010\\0001101\end{pmatrix}$$

Proposition 18.4: The (cyclic) binary Hamming code $\mathcal{H}_m[2^m-1,n-m,3]$ is a cyclic code with generator polynomial m_1.

We write $C=\langle g(x)\rangle$ to refer to the fact that a cyclic code C has generator polynomial g(x).

Definition 18.3: The *check polynomial* $h(x):=(x^n-1)/g(x)$. $\deg(h(x))=\dim(C)$.

For every codeword c(x), $h(x)c(x)=0 \bmod x^n-1$
(Indeed, let $c(x)=a(x)g(x)$, then $h(x)c(x)=a(x)g(x)h(x)=0 \bmod x^n-1$)

Examples:

1.The check polynomial of the Hamming code $\mathcal{H}_m$ is
$h(x)=\prod_{s\neq 1} m_s=m_0m_3\ldots$

2. Binary BCH codes: $g(x)=m_1m_3\ldots m_{2t-1}$
Sometimes we may need fewer minimal polynomials:

n=63	g(x)	δ_{BCH}	true dist	dimension
{1,2,4,8,16,32}	BCH(1) m_1	3	3	57
{3,6,12,24,48,33}	BCH(2) m_1m_3	5	5	51
{5,10,20,40,17,34}	BCH(3) $m_1m_3m_5$	7	7	45
{7,14,28,56,49,35}	BCH(4) $m_1m_3m_5m_7$	9	9	39
{9,18,36}	BCH(5) $m_1m_3m_5m_7m_9$	11	11	36
{11,22,33,25,50,37}	BCH(6) $m_1m_3m_5m_7m_9m_{11}$	13	13	30
{13,26,52,41,19,38}	BCH(7) $m_1\ldots m_{13}$	15	15	24
{15,30,60,57,51,39}	BCH(9) $m_1\ldots m_{15}$	21	21	18

Let C be an [n,k] cyclic code with zeros $\alpha_1,\alpha_2,\ldots,\alpha_s$, gen.pol.g(x) and check polynomial h(x).

$$0=g(x)h(x)=(g_0+g_1x+\ldots+x^{n-k})(h_0+h_1x+\ldots+h_kx^k)$$
$$=\ldots+ x^{n-j}(g_{n-k-j}h_k+g_{n-k-j+1}h_{k-1}+\ldots+g_{n-j}h_0)+\ldots$$

The parity-check matrix of C is

$$00\ldots0h_kh_{k-1}\ldots\ h_1h_0$$
$$00\ldots h_kh_{k-1}\ldots h_1h_00$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$h_kh_{k-1}\ldots h_1h_00\ldots00$$

[7,4,3] $h(x)=x^4+x^2+x+1$

$$H = \begin{matrix}0010111\\0101110\\1011100\end{matrix}$$

Hence, the dual code $C^{\perp}$ is generated by

$$h^*(x)=x^kh(1/x).$$

The zeros of h* are the inverse elements of the zeros of h(x):

$\alpha_{j_1}^{-1},\alpha_{j_2}^{-1},\ldots,\alpha_{j_r}^{-1}$, where $\{j_1,\ldots,j_r\}$ are the *nonzeros* of C

Fact: Zeros of $C^{\perp}$ are reciprocal of the nonzeros of the code C

Example: $x^7-1=m_0m_1m_3$; $m_{-1}=m_3$; $m_{-3}=m_1$

C[7,4,3] $g(x)=m_1=x^3+x+1$, $h(x)=m_0m_3=(x+1)(x^3+x^2+1)$; zeros of C (1,2,4); nonzeros {0,3,6,5}

$C^{\perp}$[7,3,4] Zeros: {0, (-3,-6,-5)=$\mathcal{C}_{-3}$}; $\mathcal{C}_{-j}$=cyclotomic coset that contains α^{-j}

$g(x)=h^*(x)=m_0m_{-3}=(x+1)(x^3+x+1)=x^4+x^3+x^2+1$

Cyclic simplex code is a code with check polynomial $m_{-1}(x)$

Cyclic codes of length n|(q-1) over $\mathbb{F}_p$. Subfield subcodes

$x^n-1=\prod_{s=1}^{r} m_s$ where r is the number of distinct irreducible factors
Any polynomial $g(x)=m_{i_1}m_{i_2}\ldots m_{i_j}$ generates a cyclic code
There are 2^r different cyclic codes of length n

We can construct cyclic codes of length n=q-1 over $\mathbb{F}_q$ or any subfield of it

Example: n=15, q=16.
q-ary cyclic code C_1 of length n with zeros α,α^2 is an RS [15,13,3] code
Binary cyclic code C_2 of length n with zeros α,α^2 must also have all the conjugate zeros: α^4,α^8. Thus, it is a [15,11,3] BCH(1) code generated by $m_1(x)$

Clearly, $C_2 \subset C_1$.
Definition 18.4: Let $q=p^m$. A p-ary *subfield subcode* of a q-ary code C_1 is a linear code $C_2=\{c\in C_1: \forall\, i\in [1,\ldots,n],\ c_i\in \mathbb{F}_p\}$

Proposition 18.4: Let m be the smallest number such that $n|p^m-1$.
A t-error correcting p-ary BCH code C_2 is a subfield subcode of the p^m-ary RS code with zeros $\alpha,\alpha^2,\ldots,\alpha^{2t}$.

q-ary Hamming code

Let $q=p^m$. Consider the code $\mathcal{H}_{q,m}$ with the parity-check matrix formed of all the columns with first entry 1.

$$H=\begin{matrix}0&0&0&0&1&1&1&1&1&1&1&1&1\\0&1&1&1&0&0&0&1&1&1&2&2&2\\1&0&1&2&0&1&2&0&1&2&0&1&2\end{matrix}$$

Code $\mathcal{H}_{3,3}$

The parameters are $n=(q^m-1)/(q-1), k=n-m, d=3$.

Cyclic representation? Not always possible!
Take β, $\beta^n=1$ be a primitive nth degree root of unity in $\mathbb{F}_{q^m}$

$$H'=[1,\beta,\beta^2,\ldots,\beta^{n-1}]$$

H' is not (a permutation of) H because not every power of β expands with the first nonzero =1.
Fact: No two columns of H' are proportional if and only if $(n,q-1)=1$.
If $(n,q-1)>1$ as with $q=4, m=3, n=21$, the distance of the code with the p.-c. matrix H' is 2. No q-ary cyclic Hamming code.

Recap: Cyclic, BCH and RS codes

An q-ary [n,k,d] cyclic code C of length $n|(q^m-1)$ is formed of all the multiples of a polynomial g(x), deg(g)=n-k:

$$C=\{c(x)=a(x)g(x) \bmod x^n-1: a(x)=a_0+a_1x+\ldots+a_{k-1}x^{k-1}\in \mathbb{F}_q[x]\}$$

where the multiplication is over $\mathbb{F}_q$

$\mathbb{F}_q$ is called the symbol field, $\mathbb{F}_{q\{m\}}$ is called the locator field.

The generator polynomial of C is $g(x)=m_{i1}(x)\ldots m_{it}(x)$. Check pol.: $h(x)=x^n-1/g(x)$
If the indices $i_1,\ldots,i_t$ are consecutive, then C is called a BCH code.
Or, a cyclic code is called BCH if its distance is estimated using the BCH bound.

If m=1, C is called an RS code. Thus, RS codes form a subclass of BCH codes.

The dimension of BCH codes is $k\geq n-2mt$. If q=2, $k\geq n-mt$
The true distance can exceed the designed (BCH) distance.

BCH codes can be decoded up to the designed distance using any of the decoding algorithms discussed. For instance, we can decode a q-ary BCH code C by decoding the q^m-ary RS code of which C is a subfield subcode, and then keep only the codewords whose symbols are in $\mathbb{F}_q$.