5. Algebra over GF(p^m) and Reed–Solomon codes over GF(p^m)

Coding Technology

Algebra over GF(p^m)

q can be either a prime or p^m (with p prime and $m \geq 2$). **Now we focus on the case when $q = p^m$.**

$$GF(q) = \{0, 1, \ldots, q-1\}$$

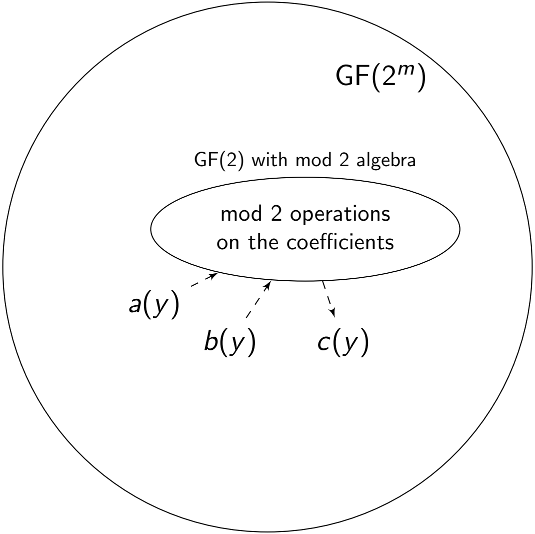
Each element of GF(p^m) has 3 representations:

element	p-ary	polynomial
0	$(0\ldots00)$	0
1	$(0\ldots01)$	1
$\vdots$	$\vdots$	$\vdots$
α	$(\alpha_{m-1},\ldots\alpha_1,\alpha_0)$	$a(y) = \alpha_{m-1}y^{m-1} + \cdots + \alpha_1 y + \alpha_0$
$\vdots$	$\vdots$	$\vdots$

Addition is p-ary addition mod p, equivalent to polynomial addition mod p.

For multiplication, fix an irreducible polynomial $p(y)$ with degree m. Multiplication is polynomial multiplication mod $p(y)$.

"Big field" and "small field"



Algebra over GF(4)

Irreducible polynomial: $p(y) = y^2 + y + 1$.

Elements of GF(4):

element	binary	polynomial
0	(00)	$0 \cdot y^1 + 0 \cdot y^0 = 0$
1	(01)	$0 \cdot y^1 + 1 \cdot y^0 = 1$
2	(10)	$1 \cdot y^1 + 0 \cdot y^0 = y$
3	(11)	$1 \cdot y^1 + 1 \cdot y^0 = y + 1$

Examples for addition:

$$y + (y + 1) = 2y + 1 = 0 \cdot y + 1 = 1,$$
$$1 + (y + 1) = y + 2 = y.$$

Algebra over GF(4)

Irreducible polynomial: $p(y) = y^2 + y + 1$.

Elements of GF(4):

element	binary	polynomial
0	(00)	$0 \cdot y^1 + 0 \cdot y^0 = 0$
1	(01)	$0 \cdot y^1 + 1 \cdot y^0 = 1$
2	(10)	$1 \cdot y^1 + 0 \cdot y^0 = y$
3	(11)	$1 \cdot y^1 + 1 \cdot y^0 = y + 1$

Examples for multiplication:

$$y * y = y^2 = 1(y^2 + y + 1) + y + 1 = y + 1,$$
$$y * (y + 1) = y^2 + y = 1(y^2 + y + 1) + 1 = 1.$$

Algebra over GF(4)

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

+	0	1	y	y+1
0	0	1	y	y+1
1	1	0	y+1	y
y	y	y+1	0	1
y+1	y+1	y	1	0

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

*	0	1	y	y+1
0	0	0	0	0
1	0	1	y	y+1
y	0	y	y+1	1
y+1	0	y+1	1	y

GF(4) primitive element and power table

Irreducible polynomial: $p(y) = y^2 + y + 1$.

Elements of GF(4):

element	binary	polynomial
0	(00)	$0 \cdot y^1 + 0 \cdot y^0 = 0$
1	(01)	$0 \cdot y^1 + 1 \cdot y^0 = 1$
2	(10)	$1 \cdot y^1 + 0 \cdot y^0 = y$
3	(11)	$1 \cdot y^1 + 1 \cdot y^0 = y + 1$

y is the primitive element. Power table:

y^0	1
y^1	y
y^2	$y + 1$

(It is also customary to write $0 = y^{-\infty}$.) Examples:

$$y^2 = 1(y^2 + y + 1) + y + 1 = y + 1,$$
$$y^3 = y^2 \cdot y = (y + 1)y = y^2 + y = 1 \cdot (y^2 + y + 1) + 1 = 1.$$

GF(8) representations

Irreducible polynomial: $p(y) = y^3 + y + 1$.

Elements of GF(8):

element	binary	polynomial
0	(000)	0
1	(001)	1
2	(010)	y
3	(011)	$y + 1$
4	(100)	y^2
5	(101)	$y^2 + 1$
6	(110)	$y^2 + y$
7	(111)	$y^2 + y + 1$

Power table of GF(8)

Irreducible polynomial: $p(y) = y^3 + y + 1$.

y is the primitive element. Power table:

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Examples:

$$y^3 = 1(y^3 + y + 1) + y + 1 = y + 1,$$
$$y^4 = y \cdot y^3 = y(y^3 + y + 1) + y^2 + y = y^2 + y.$$

Multiplication using the power table

Irreducible polynomial: $p(y) = y^3 + y + 1$.

y is the primitive element. Power table:

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Examples:

$$\begin{aligned} 2*6 &= y * y^4 = y^5 = 7 (= y^2 + y + 1), \\ 3*3 &= y^3 * y^3 = y^6 = 5, \\ 4*5 &= y^2 \cdot y^6 = y^8 = y = 2. \end{aligned}$$

Multiplication with shift registers over GF(8)

Example. We want to multiply
$\alpha(y) = a_0 + a_1 y + a_2 y^2$ by y.

$y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$
$a_0 y + a_1 y^2 + a_2 (y + 1) = a_2 + (a_0 + a_2) y + a_1 y^2$.

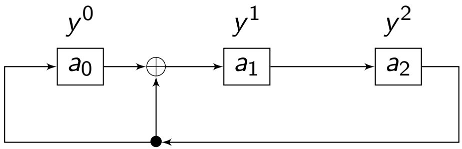
1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Multiplication with shift registers over GF(8)

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Example. We want to multiply $\alpha(y) = a_0 + a_1 y + a_2 y^2$ by y.

$y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$
$a_0 y + a_1 y^2 + a_2(y+1) = a_2 + (a_0 + a_2)y + a_1 y^2.$



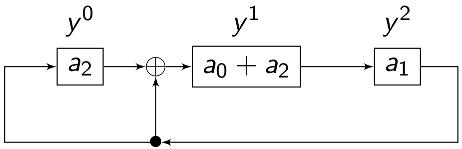
Multiplication with shift registers over GF(8)

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Example. We want to multiply $\alpha(y) = a_0 + a_1 y + a_2 y^2$ by y.

$y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$
$a_0 y + a_1 y^2 + a_2 (y+1) = a_2 + (a_0 + a_2) y + a_1 y^2.$

At the next time instance:



Multiplication with shift registers over GF(8)

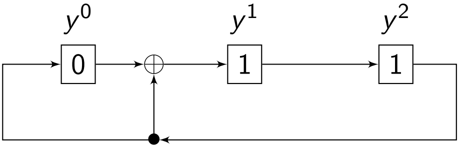
Example. We want to multiply $y^2 + y$ by y.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

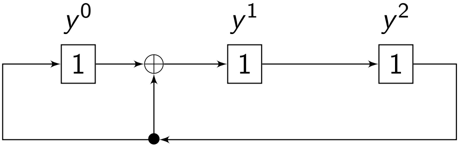
Multiplication with shift registers over GF(8)

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Example. We want to multiply $y^2 + y$ by y.



At the next time instance:



So $(y^2 + y) * y = y^2 + y + 1$.

Multiplication with shift registers over GF(8)

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Example. Multiplication by 4. ($4 = y^2$.)

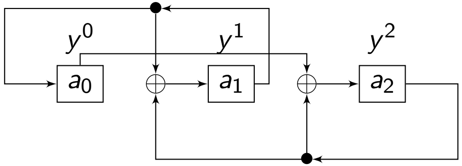
$$y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 =$$
$$a_0 y^2 + a_1(y+1) + a_2(y^2+y) =$$
$$a_1 + (a_1 + a_2)y + (a_0 + a_2)y^2.$$

Multiplication with shift registers over GF(8)

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Example. Multiplication by 4. ($4 = y^2$.)

$$y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 =$$
$$a_0 y^2 + a_1(y+1) + a_2(y^2+y) =$$
$$a_1 + (a_1 + a_2)y + (a_0 + a_2)y^2.$$



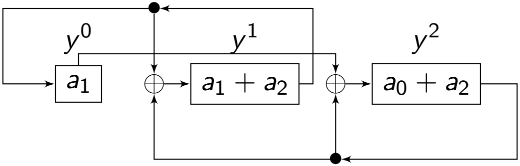
Multiplication with shift registers over GF(8)

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Example. Multiplication by 4. ($4 = y^2$.)

$$y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 =$$
$$a_0 y^2 + a_1(y+1) + a_2(y^2+y) =$$
$$a_1 + (a_1 + a_2)y + (a_0 + a_2)y^2.$$

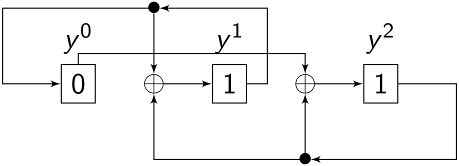
At the next time instance:



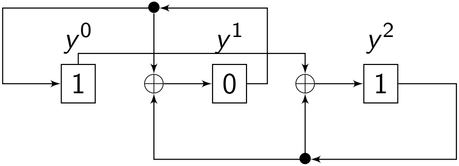
Multiplication with shift registers over GF(8)

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Example. We want to compute $6 * 4$.
($6 = y^2 + y$, $4 = y^2$.)



At the next time instance:



So $(y^2 + y) * y^2 = y^2 + 1$.

Problem 1

(a) Compute $3 * 4$ in GF(8).

(b) Depict the corresponding shift register architecture.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Problem 1

(a) Compute $3 * 4$ in GF(8).

(b) Depict the corresponding shift register architecture.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Solution.

(a) According to the power table:
$3 * 4 \rightarrow y^3 * y^2 = y^5 = y^2 + y + 1$

Problem 1

(a) Compute $3 * 4$ in GF(8).

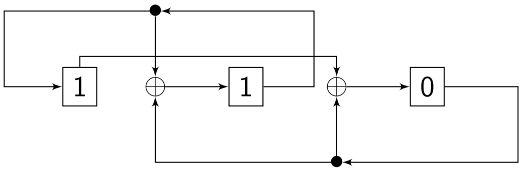
(b) Depict the corresponding shift register architecture.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Solution.

(a) According to the power table:
$3 * 4 \rightarrow y^3 * y^2 = y^5 = y^2 + y + 1$

(b)



Problem 1

(a) Compute $3 * 4$ in GF(8).

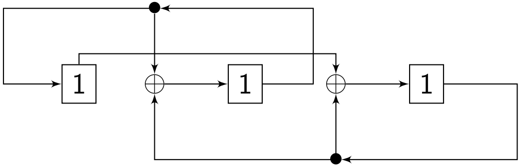
(b) Depict the corresponding shift register architecture.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Solution.

(a) According to the power table:
$3 * 4 \to y^3 * y^2 = y^5 = y^2 + y + 1$

(b) At the next time instance:



Reed–Solomon codes over $\mathrm{GF}(p^m)$

Reed–Solomon codes over $\mathrm{GF}(p^m)$ work basically the same as RS codes over $\mathrm{GF}(q)$ when q is a prime. $n = q - 1$, and the primitive element is always y, so the $C(n, k)$ Reed-Solomon code over $\mathrm{GF}(p^m)$ has generator polynomial and parity check polynomial

$$g(x) = \prod_{i=1}^{n-k}(x - y^i), \qquad h(x) = \prod_{i=n-k+1}^{n}(x - y^i).$$

Reed–Solomon codes over $\mathrm{GF}(p^m)$

Reed–Solomon codes over $\mathrm{GF}(p^m)$ work basically the same as RS codes over $\mathrm{GF}(q)$ when q is a prime. $n = q - 1$, and the primitive element is always y, so the $\mathrm{C}(n,k)$ Reed-Solomon code over $\mathrm{GF}(p^m)$ has generator polynomial and parity check polynomial

$$g(x) = \prod_{i=1}^{n-k}(x - y^i), \qquad h(x) = \prod_{i=n-k+1}^{n}(x - y^i).$$

The code can

- detect $n - k$ errors, and
- correct $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors.

Problem 2

Determine the parity check polynomial of the Reed-Solomon code capable of correcting every double error over GF(8).

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Problem 2

Determine the parity check polynomial of the Reed-Solomon code capable of correcting every double error over GF(8).

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Solution. Code parameters:

$$n = 8 - 1 = 7, \qquad t = 2 = \left\lfloor \frac{n-k}{2} \right\rfloor \quad \to \quad k = 3.$$

$$h(x) = \prod_{i=n-k+1}^{n} (x - y^i) = (x - y^5)(x - y^6)(x - y^7) =$$

$$(x + y^5)(x + y^6)(x + y^7) = (x^2 + yx + y^4)(x + 1) =$$

$$x^3 + yx^2 + y^4x + x^2 + yx + y^4 = x^3 + y^3x^2 + y^2x + y^4.$$

Problem 3

A code over GF(8) has generator polynomial

$$g(x) = x^3 + y^6 x^2 + yx + y^6.$$

(a) What are the code parameters?

(b) What is the codeword for the message vector u containing all 1's in binary form?

(c) Is this a RS code?

Problem 3

A code over GF(8) has generator polynomial

$$g(x) = x^3 + y^6x^2 + yx + y^6.$$

(a) What are the code parameters?

(b) What is the codeword for the message vector u containing all 1's in binary form?

(c) Is this a RS code?

Solution. If we knew it is a RS code, then we would also know $n = q - 1 = 7$. So start with (c) instead of (a).

(c) RS codes have generator polynomials of the form $\prod_{i=1}^{n-k}(x - y^i)$, so we need to decide if $g(x)$ is of this form.

Problem 3

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

(c) The given $g(x)$ has degree 3 (we need to consider the exponent of x, the y terms are coefficients, 'numbers' from GF(8)).

$$g(x) = (x-y)(x-y^2)(x-y^3) =$$
$$= (x^2 - \underbrace{(y+y^2)}_{y^4} x + y^3)(x-y^3) =$$
$$= x^3 + x^2 \underbrace{(-y^3 - y^4)}_{(y+1)+(y^2+y)} + x \underbrace{(-y^7 + y^3)}_{1+(y+1)=y} + y^6 =$$
$$x^3 + y^6x^2 + yx + y^6,$$

which matches the given $g(x)$, so yes, this is a RS code, and $n = q - 1 = 7$.

Problem 3

(c) The given $g(x)$ has degree 3 (we need to consider the exponent of x, the y terms are coefficients, 'numbers' from GF(8)).

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

$$g(x) = (x-y)(x-y^2)(x-y^3) =$$
$$= (x^2 - \underbrace{(y+y^2)}_{y^4} x + y^3)(x-y^3) =$$
$$= x^3 + x^2 \underbrace{(-y^3 - y^4)}_{(y+1)+(y^2+y)} + x \underbrace{(-y^7 + y^3)}_{1+(y+1)=y} + y^6 =$$
$$x^3 + y^6 x^2 + yx + y^6,$$

which matches the given $g(x)$, so yes, this is a RS code, and $n = q - 1 = 7$.

(a) $\deg(g(x)) = 3 = n - k \rightarrow C(7,4)$.

Problem 3

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Solution.

(b) The message vector u is $(111, 111, 111, 111)$ as $k = 4$. $(111) = y^5$, so u has polynomial form

$$u(x) = y^5 + y^5x + y^5x^2 + y^5x^3.$$

Then

$$c(x) = g(x)u(x) =$$
$$= (y^6 + yx + y^6x^2 + x^3)(y^5 + y^5x + y^5x^2 + y^5x^3) =$$
$$= \cdots = (y^2 + y) + y^3x + y^6x^2 + yx^3 + y^2x^4 + x^5 + y^5x^6$$
$$\to c = (6\,3\,5\,2\,4\,1\,7).$$