Quasi-cyclic codes

Jay A. Wood

Department of Mathematics
Western Michigan University
http://homepages.wmich.edu/∼jwood/

Algebra for Secure and Reliable Communications Modeling
Morelia, Michoacán, Mexico
October 12, 2012

Introduction

- This will be an elementary introduction to cyclic and quasi-cyclic codes from the point of view of ring theory.
- At least I hope so!

Cyclic codes

- Let A be an alphabet.
- The shift operator on A^n is the map $T : A^n \to A^n$ given by

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \mapsto (a_{n-1}, a_0, a_1, \ldots, a_{n-2}).$$

- A linear code $C \subset A^n$ is a *cyclic code* if $T(C) \subset C$. That is, the shift of any codeword is again a codeword.

Examples

- $A = \mathbb{F}_2$, $n = 7$
- Let C be the code spanned by the row vectors:

$$\begin{array}{c} 1011100 \\ 0101110 \\ 0010111 \end{array}$$

- T of row 1 is row 2; T of row 2 is row 3. T of row 3 is the sum of rows 1 and 3. Use linearity in general.

Viewing codewords as polynomials

- Suppose the alphabet is a finite commutative ring R.
- View a codeword as a polynomial:

$$\begin{array}{c}(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \\ \updownarrow \\ a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}\end{array}$$

Shift as multiplication by x

- In the 1950s, Prange observed: if we consider the polynomials modulo $x^n - 1$, then the shift operator corresponds to multiplication by x.

$$
\begin{gathered}
x(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}) \\
= a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} + a_{n-1} x^n \\
\equiv a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} \bmod (x^n - 1) \\
\updownarrow \\
(a_{n-1}, a_0, a_1, \ldots, a_{n-2})
\end{gathered}
$$

Cyclic codes as ideals

- This establishes an isomorphism

$$R^n \cong R[x]/(x^n - 1)$$

  as (free) R-modules such that the shift operator T corresponds to multiplication by x in the ring structure of $R[x]/(x^n - 1)$.
- Linear cyclic codes in R^n correspond to ideals in $R[x]/(x^n - 1)$.

Structure of $R[x]/(x^n - 1)$

- For R a finite commutative ring, about all we can say about $R[x]/(x^n - 1)$ is that it too is a finite commutative ring, of order $|R|^n$.
- Every finite commutative ring splits (as rings) as the direct sum of local rings.
- If $R[x]/(x^n - 1) \cong \oplus R_i$, with R_i local, then the ideals of $R[x]/(x^n - 1)$ are direct sums of ideals of the R_i.
- Structure of ideals of local rings is worth studying in general. We look at a special example.

Finite fields

- Let $R = \mathbb{F}_q$, a finite field.
- $\mathbb{F}_q[x]$ is a principal ideal ring.
- The ideals of $\mathbb{F}_q[x]/(x^n - 1)$ correspond to the ideals of $\mathbb{F}_q[x]$ that contain the ideal $(x^n - 1)$.
- An ideal $(g) \subset \mathbb{F}_q[x]$ contains $(x^n - 1)$ iff the polynomial g divides $x^n - 1$.

Factoring $x^n - 1$

- In the principal ideal ring $\mathbb{F}_q[x]$ there is unique factorization into irreducibles.
- Factor
$$x^n - 1 = f_1^{s_1} f_2^{s_2} \cdots f_k^{s_k},$$
where the f_i are distinct monic irreducible polynomials. The s_i are positive integers.

Chinese remainder theorem

- There is a natural ring homomorphism
$$\frac{\mathbb{F}_q[x]}{(x^n - 1)} \to \bigoplus_{i=1}^{k} \frac{\mathbb{F}_q[x]}{(f_i^{s_i})},$$
given by reduction mod $f_i^{s_i}$.
- The Chinese remainder theorem (CRT) says that this homomorphism is an isomorphism. (Exercise.)
- Ideals on the left (cyclic codes) are sums of ideals from the right.

Examples

- Let $q = 2$, so that $- = +$.

$$
\begin{aligned}
x^2 - 1 &= (x+1)^2 \\
x^3 - 1 &= (x+1)(x^2+x+1) \\
x^4 - 1 &= (x+1)^4 \\
x^5 - 1 &= (x+1)(x^4+x^3+x^2+x+1) \\
x^6 - 1 &= (x+1)^2(x^2+x+1)^2 \\
x^7 - 1 &= (x+1)(x^3+x+1)(x^3+x^2+1) \\
x^8 - 1 &= (x+1)^8
\end{aligned}
$$

Multiplicity one

- When does $x^n - 1$ factor over $\mathbb{F}_q$ into distinct irreducibles, all of multiplicity one?
- This happens when n, q are relatively prime.
- q is a unit in $\mathbb{Z}/n\mathbb{Z}$, so $q^\ell \equiv 1 \bmod n$ for some smallest positive integer ℓ. Then $n|(q^\ell - 1)$.
- There is a cyclic n-subgroup in the multiplicative group of $\mathbb{F}_{q^\ell}$, so $x^n - 1$ splits into distinct linear factors over $\mathbb{F}_{q^\ell}$.
- Multiply factors in Frobenius orbits to get distinct factors over $\mathbb{F}_q$. (Cyclotomic cosets.)

Relatively prime case (a)

- When $\gcd(q, n) = 1$, $x^n - 1$ factors as $x^n - 1 = f_1 f_2 \cdots f_k$, distinct irreducibles.
- Chinese remainder theorem gives

$$\frac{\mathbb{F}_q[x]}{(x^n - 1)} \to \bigoplus_{i=1}^{k} \frac{\mathbb{F}_q[x]}{(f_i)}.$$

- The rings on the right are all field extensions of $\mathbb{F}_q$, because the f_i are irreducible.

Relatively prime case (b)

- The only ideals in a field are 0 and the field itself.
- Ideals on the left (cyclic codes) are generated by g of the form
$$g = f_1^{\delta_1} f_2^{\delta_2} \cdots f_k^{\delta_k},$$
where each $\delta_i = 0$ or 1.
- There are 2^k such cyclic codes.
- Write then down for $q = 2$, $n = 7$ ($k = 3$).

General case for fields

- The Chinese remainder theorem gives

$$\frac{\mathbb{F}_q[x]}{(x^n - 1)} \to \bigoplus_{i=1}^{k} \frac{\mathbb{F}_q[x]}{(f_i^{s_i})}.$$

- The rings $\mathbb{F}_q[x]/(f_i^{s_i})$ are chain rings, because the ideals of $\mathbb{F}_q[x]/(f_i^{s_i})$ correspond to ideals of $\mathbb{F}_q[x]$ that contain $(f_i^{s_i})$. That is, to (g) where $g | f_i^{s_i}$. Since f_i is irreducible, $g = f_i^{j_i}$ for $j_i \le s_i$.
- There are $\prod_{i=1}^{k}(s_i + 1)$ such cyclic codes.

Examples $q = 2$, $n = 4$

- Over $\mathbb{F}_2$, $x^4 - 1 = (x+1)^4$. For $g = (x+1)^j$, here are the first rows of the cyclic codes.

j	$(x+1)^j$	first row
0	1	1000
1	$1 + x$	1100
2	$1 + x^2$	1010
3	$1 + x + x^2 + x^3$	1111
4	$1 + x^4 \equiv 0$	0000

Examples $q = 2$, $n = 6$

- Over $\mathbb{F}_2$, $x^6 - 1 = (x+1)^2(x^2+x+1)^2$. There are now $3^2 = 9$ cyclic codes. First rows:

jk	first row
00	100000
10	110000
20	101000
01	111000
11	100100
21	110110
02	101010
12	111111
22	000000

Quasi-cyclic codes

- Work over $\mathbb{F}_q$, and suppose $n = \ell m$.
- A linear code $C \subset \mathbb{F}_q^n = \mathbb{F}_q^{\ell m}$ is *quasi-cyclic of index* ℓ or ℓ*-quasi-cyclic* if $T^\ell(C) \subset C$.
- Example: $q = 2$, $\ell = 2$, $m = 4$, $n = 8$. All the codewords (left column is a quasi-cyclic subcode):

00000000	01010101
10001000	11011101
00100010	01110111
10101010	11111111

Quasi-cyclic codes as codes over a ring

- Set $R = \mathbb{F}_q[x]/(x^m - 1)$. Label a vector in $\mathbb{F}_q^{\ell m}$ by

$$\begin{aligned} a = \big(&a_{00}, a_{01}, \ldots, a_{0,\ell-1},\\ &a_{10}, a_{11}, \ldots, a_{1,\ell-1}, \ldots,\\ &a_{m-1,0}, a_{m-1,1}, \ldots, a_{m-1,\ell-1}\big). \end{aligned}$$

- Set $A_j = \sum_{i=0}^{m-1} a_{ij}x^i \in \mathbb{F}_q[x]$.
- Map $\mathbb{F}_q^{\ell m} \to R^\ell$ by $a \mapsto (A_0, A_1, \ldots, A_{\ell-1})$.
- Then ℓ-quasi-cyclic codes correspond to R-linear codes in R^ℓ.

Work of Ling and Solé

- As for cyclic codes, the ring R can be decomposed via the Chinese remainder theorem.
- This allows R-linear codes in R^ℓ to be decomposed into codes over local rings (fields and chain rings, here).
- Ling and Solé, in a series of papers, 2001–2006, describe the structure of quasi-cyclic codes with coefficients in $\mathbb{F}_q$ or in chain rings. They describe the dual codes and characterize self-dual codes.

Another direction

- The ring $R = \mathbb{F}_q[x]/(x^m - 1)$ is isomorphic to $\mathbb{F}_q[C_m]$, the group algebra of the cyclic m-group with coefficients in $\mathbb{F}_q$.
- Write C_m multiplicatively, as $C_m = \{e, g, g^2, g^3, \ldots, g^{m-1}\}$, with $g^m = e$.
- An element $a \in \mathbb{F}_q[C_m]$ has the form $a = \sum_{i=0}^{m-1} a_i g^i$, with $a_i \in \mathbb{F}_q$.
- $\mathbb{F}_q[C_m] \cong \mathbb{F}_q[x]/(x^m - 1)$ by sending g to x.

$\mathbb{F}_2 + u\mathbb{F}_2$

- Multiply in the ring $\mathbb{F}_2 + u\mathbb{F}_2$, with $u^2 = 0$, by

$$(a_0 + a_1 u)(b_0 + b_1 u) = a_0 b_0 + (a_0 b_1 + a_1 b_0) u.$$

- Set $v = 1 + u$. Notice that $v^2 = 1 + u^2 = 1$.
- Use $1, v$ as basis instead. Then

$$\begin{aligned}(c_0 + c_1 v)(d_0 + d_1 v) &= c_0 d_0 + (c_0 d_1 + c_1 d_0) v + c_1 d_1 v^2 \\ &= (c_0 d_0 + c_1 d_1) + (c_0 d_1 + c_1 d_0) v.\end{aligned}$$

$\mathbb{F}_2 + u\mathbb{F}_2 \cong \mathbb{F}_2[C_2]$

- Compare this with the multiplication in the group algebra $\mathbb{F}_2[C_2]$:

$$\begin{aligned}(c_0e + c_1g)(d_0e + d_0g) &= c_0d_0e + (c_0d_1 + c_1d_0)g + c_1d_1g^2 \\ &= (c_0d_0 + c_1d_1)e + (c_0d_1 + c_1d_0)g\end{aligned}$$

- We see that $\mathbb{F}_2 + u\mathbb{F}_2 \cong \mathbb{F}_2[C_2]$. The same proof works for $q = 2^t$. (Not true for odd q.)

Maschke's theorem (a)

- The fact that $\mathbb{F}_q[x]/(x^n - 1)$ splits into a sum of fields when $\gcd(q, n) = 1$ is a special case of Maschke's theorem in group representation theory.
- Suppose k is a field of characteristic p and G is a finite group. If p does not divide the order of G (always true for characteristic zero), then the group algebra $k[G]$ is a semisimple ring (a sum of matrix rings over division algebras over k).

Maschke's theorem (b)

- For $G = C_n$, the group is abelian. Then $\mathbb{F}_q[x]/(x^n - 1) \cong \mathbb{F}_q[C_n]$ is a commutative ring. If $\gcd(q, n) = 1$, then Maschke's theorem applies, and $\mathbb{F}_q[x]/(x^n - 1)$ splits as a sum of matrix rings.
- In order to be commutative and finite, the matrix rings must be 1×1, hence just fields (extensions of $\mathbb{F}_q$).

Codes over group algebras

- This leads one to contemplate codes over group algebras.
- Compare to "group codes" in the literature.
- Even more generally: codes over algebras. By fixing a vector space basis for an algebra R over $\mathbb{F}_q$, one can view R-linear codes $C \subset R^n$ as $\mathbb{F}_q$-codes of length $n \cdot \dim_{\mathbb{F}_q} R$, with additional symmetry coming from the R-module structure.
- This area should be wide open for investigation.