ELG 5372 Error Control Coding

Lecture 12: Ideals in Rings and Algebraic Description of Cyclic Codes

Université d'Ottawa | University of Ottawa

Quotient Ring Example

+	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
S_0	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
S_1	S_1	S_0	S_3	S_2	S_5	S_4	S_7	S_6
S_2	S_2	S_3	S_0	S_1	S_6	S_7	S_4	S_5
S_3	S_3	S_2	S_1	S_0	S_7	S_6	S_5	S_4
S_4	S_4	S_5	S_6	S_7	S_0	S_1	S_2	S_3
S_5	S_5	S_4	S_7	S_6	S_1	S_0	S_3	S_2
S_6	S_6	S_7	S_4	S_5	S_2	S_3	S_0	S_1
S_7	S_7	S_6	S_5	S_4	S_3	S_2	S_1	S_0

Quotient Ring Example

•	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
S_0	S_0	S_0	S_0	S_0	S_0	S_0	S_0	S_0
S_1	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
S_2	S_0	S_2	S_4	S_6	S_1	S_3	S_5	S_7
S_3	S_0	S_3	S_6	S_5	S_5	S_6	S_3	S_0
S_4	S_0	S_4	S_1	S_5	S_2	S_6	S_3	S_7
S_5	S_0	S_5	S_3	S_6	S_6	S_3	S_5	S_0
S_6	S_0	S_6	S_5	S_3	S_3	S_5	S_6	S_0
S_7	S_0	S_7	S_7	S_0	S_7	S_0	S_0	S_7

Quotient Ring

- Recall the quotient ring $R=\{S_0, S_1, \ldots, S_7\}$, where S_i was the set of all polynomials in GF(2)[x] whose remainder is $i = ax^2+bx+c$ when divided by x^3+1.
- Let's identify each coset by its lowest degree polynomial
- $S_0 = 0$, $S_1 = 1$, $S_2 = x$, $S_3 = x+1$, $S_4 = x^2$, $S_5 = x^2+1$, $S_6 = x^2+x$ and $S_7 = x^2+x+1$.
- Let $R_{new} = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ where addition is defined as conventional polynomial addition and multiplication is conventional polynomial multiplication, both followed by computing the remainder modulo x^3+1.
- Then R_{new} is a ring as well.
  - We denote this ring as GF(2)[x]/(x^3+1).

Quotient Ring

- For R_{new}, $(x+1)(x^2+x+1) = 0$ and for R, $S_3 S_7 = S_0$.
  - These rings are called isomorphic rings.

GF(q)[x]/f(x)

- For a field GF(q), the ring of polynomials can be partitioned by a polynoial $f(x)$ of degree m into q_m different equivalence classes
  - One equivalence for each remainder modulo $f(x)$.
- This ring is denoted as GF(q)[x]/f(x).
- It can be a field, but only if $f(x)$ is irreducible in GF(q).
- In our example GF(2)[x]/x^3+1, it is not a field as x^3+1 = (x+1)(x^2+x+1).

Ideals in Rings

- Let *R* be a ring.
- Let *I* be a non empty subset of R
- *I* is an ideal if it satisfies the following conditions:
  1. *I* forms a group under the addition operation of *R*
  2. And any *a* in *I* and any *r* in *R*, *a*•*r* is in *I*.

Example

- Consider ring R (GF(2)[x]/x^3+1).
- Trivial cases: {0} and {R} are ideals.
- I = {S_0, S_7}
  - This set forms a group under addition
  - S_0•any element in R = S_0
  - S_7•any element in R = S_0 or S_7.
- Consider R_{new}
- I = {0, x^2+x+1}
  - Forms a group under addition
  - 0(x^2+x+1) = 0, 1(x^2+x+1) = x^2+x+1, x(x^2+x+1) = x^3+x^2+x mod x^3+1 = x^2+x+1, (x+1)(x^2+x+1) = x(x^2+x+1)+(x^2+x+1) = 0, x^2(x^2+x+1) = x(x(x^2+x+1)) = x(x^2+x+1) = x^2+x+1 etc.

Examples

- In GF(2)[x]/x^3+1, {S_0, S_3, S_5, S_6} also form an ideal.
- Since GF(2)[x]/x^3+1 and R_{new} are isomorphic, we can see that {0, x+1, x^2+1, x^2+x} form an ideal in R_{new}.
- Vectorially, the ideal in R_{new} is {(000), (011), (101), (110)}.
- The above ideal satisfies all the conditions of a cyclic code.

Principal Ideal

- An ideal, I, in ring R is said to be principal if there exists some element g in I such that every element a in I can be expressed as $a=mg$, where m is an element in R. The element g is called the generator element.
  - $I = \{S_0, S_7\}$, S_0 and S_7 can be expressed as multiples of S_7. Therefore $g = S_7$ and this ideal is said to be principal.
  - I = $\{S_0, S_3, S_5, S_6\}$, either S_3, S_5 or S_6 can act as the generator g. This ideal is also said to be principal.

Cyclic Code Theorem 1

- Let *I* be an ideal in GF(q)[x]/x^n-1. Then
  1. There exists a unique monic polynomial $g(x)$ in *I* of minimal degree
  2. *I* is principal with generator $g(x)$.
  3. $g(x)$ divides x^n-1 in GF(q)[x].

– A polynomial of degree m, $g(x) = g_m x^m + g_{m-1} x^{m-1} + \ldots + g_0$, is monic if $g_m = 1$.

Proof of CCT 1

- There is at least one ideal in any ring (since the entire ring is an ideal).
- There is a lower bound on the degrees of the polynomials in the ideal. Hence there is at least one polynomial in the ideal of minimal degree (which may have to be normalized to be monic).
- To show uniqueness, suppose there are two monic polynomials of minimal degree in the ideal, $g(x)$ and $f(x)$. Then $h(x) = g(x)-f(x)$ is also an element in I. $h(x)$ would have a smaller degree than $g(x)$ and $f(x)$, therefore this contradicts the statement that $g(x)$ and $f(x)$ are of minimal degree.

Proof of CCT 1 cont'd

- To show I is principle (all elements of I are multiples of $g(x)$), we assume that there exists a polynomial f(x) in I for which $f(x) = m(x)g(x) + r(x)$, where $m(x)$ and $r(x)$ are in R.
- Since $r(x)$ is the remainder, it has degree less than $g(x)$.
- The definition of an Ideal tells us that $m(x)g(x)$ is in I. Then $r(x) = f(x)\text{-}m(x)g(x)$ must also be in I. But since $r(x)$ has a smaller degree than $g(x)$, it contradicts the statement that $g(x)$ is a polynomial of minimal degree in I. Therefore the only solution is that r(x) = 0 and $f(x)$ is a multiple of $g(x)$.

Proof of CCT 1 cont'd

- To show that $g(x)$ divides x^n-1, we assume that it doesn't
- Then $x^n-1 = h(x)g(x)+r(x)$ where $r(x)$ has degree less than the degree of $g(x)$.
- But $h(x)g(x)$ is in I and $r(x) = x^n-1 - h(x)g(x)$, which is the additive inverse of $h(x)g(x)$, which is also in I, again contradicting the statement that $g(x)$ is a polynomial of minimal degree in I.
- Therefore $r(x) = 0$ and $g(x)$ divides x^n-1.

Example

- Consider the ring GF(2)[x]/x^4+1
- {0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1}
- x^4+1 =(x+1)(x^3+x^2+x+1) or (x^2+1)(x^2+1).
- Therefore we have the following principal Ideals
  - {0}, {0, x+1, x^2+x, x^2+1, x^3+x^2, x^3+x^2+x+1, x^3+1, x^3+x}, {0, x^3+x^2+x+1}, {0, x^2+1, x^3+x, x^3+x^2+x+1}

Example cont'd

- $\{0, x+1, x^2+x, x^2+1, x^3+x^2, x^3+x^2+x+1, x^3+1, x^3+x\} \rightarrow \{(0000), (1100), (0110), (1010), (0011), (1111), (1001), (0101)\}$.
- We can see that the above is a cyclic code.
- **Cyclic codes of length *n* form an ideal in GF(*q*)[*x*]/x^n-1.**
- **They can be described by their generator polynomial *g*(*x*) which is a polynomial that divides x^n-1.**

Algebraic Description of Cyclic Codes

- $c^R(x) = xc(x) \bmod x^n-1$.
- Think of $c(x)$ as an element of GF(q)[x]/x^n-1.
  - Since the arithmetic is done modulo x^n-1, we simply state that $c^R(x) = xc(x)$.
- For an (n,k) cyclic code, the generator polynomial, $g(x)$, is the generator of an ideal in GF(q)[x]/x^n-1.
  - The degree of g(x) is n-k.
- $c(x) = m(x)g(x)$, where $m(x)$ is a polynomial representing a message to be encoded. Deg($m(x)$) < k.
  - If $m(x)$ has degree greater than k-1, then $c(x)$ will have degree greater than n-1 (before dividing by x^n-1 and finding the remainder). After performing the modulo operation, $c(x)$ will not be a distinct codeword.

Example: Binary Cyclic Codes of Length 7

- $x^7-1 = (x+1)(x^3+x+1)(x^3+x^2+1)$.
- (7,6) code: $g(x) = x+1$
- (7,4) code $g_1(x)= x^3+x+1$ or $g_2(x) = x^3+x^2+1$.
- (7,3) code $g_3(x) = (x+1)(x^3+x+1)=x^4+x^3+x^2+1$ or $g_4(x) = (x+1)(x^3+x^2+1) = x^4+x^2+x+1$
- (7,1) code: $g_5(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1$.