ELG 5372 Error Control Coding

Lecture 6: (a) Factoring X^n-1 and (b) Introduction to Linear Block Codes: Vector Spaces

uOttawa

L'Université canadienne
Canada's university

Université d'Ottawa | University of Ottawa

uOttawa.ca

Factoring X^n-1

- In GF(p^m), the expression X^n-1 has n roots, β_1, β_2, …, β_n.
- The order of these roots, ord(β_i) must divide n and n must divide p^m-1.
- If we wish to factor X^n-1 in GF(p), we need to find the minimal polynomials in GF(p^m) wrt GF(p).
- Consider X^7+1 in GF(2).
- We need to determine the extension field of GF(2) in which there are at least 7 roots of this equation with order that divides 7. -> GF(8).

Factoring X^n-1

- Since all nonzero elements of GF(8) have order 1 or 7, then $\beta^7-1=0$ for β = any non-zero element in GF(8).
- The minimal polynomials of GF(8) wrt to GF(2) are polynomials in GF(2) but have the nonzero elements of GF(8) as roots in GF(8).
  - $\{1\}$ -> $X+1$
  - $\{\alpha, \alpha^2, \alpha^4\}$ -> $(X+\alpha)(X+\alpha^2)(X+\alpha^4)=X^3 + (\alpha+\alpha^2+\alpha^4)X^2 + (\alpha^3+\alpha^5+\alpha^6)X + \alpha^7 = X^3+X+1$.
  - $\{\alpha^3, \alpha^5, \alpha^6\}$ -> $(X+\alpha^3)(X+\alpha^5)(X+\alpha^6)=X^3 + (\alpha^3+\alpha^5+\alpha^6)X^2 + (\alpha+\alpha^2+\alpha^4)X + \alpha^7 = X^3+X^2+1$.
  - $(X^3+X^2+1)(X^3+X+1)(X+1) = X^7+1$.

Factoring X^n-1

- Factoring X^n-1 when $n = p^m$-1 is simple as we only need to find the minimal polynomials of GF(p^m) wrt to GF(p).
  - For example X^{15}+1 is equal to the multiplication of all minimal polynomials of GF(16) wrt GF(2).
- However, it is a little more complicated to factor X^n-1 when $n \neq p^m$-1.
- For example to factor X5+1 in GF(2), we need to find an extension field in which there are nonzero elements of order 5, or that divide 5.
  - In GF(16), elements must have order 15, 5, 3, or 1.
  - Therefore we choose this field in which to find the roots of X^5+1.

Factoring X^n-1

- We find an element of GF(16) that has order 5.
  - The element α^3 has order 5.
  - The conjugacy class of a3 is $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$.
  - The minimal polynomial corresponding to this group is $X^4+X^3+X^2+X+1$.
  - There are no other elements in GF(16) that have order 5.
  - The element 1 has order 1 which divides 5. Therefore $X+1$ must divide X^5+1.
  - $X^5+1 = (X^4+X^3+X^2+X+1)(X+1)$.

Squaring Polynomials in GF(2)

- Let $p(X) = a_0 + a_1X + a_2X^2 + \ldots + a_mX^m$.
- $p^2(X) = ?$
- In GF(2), $(a)^2 = a$. Furthermore $(a+b)^2 = a^2+b^2+ab+ab = a^2+b^2$
- $[a_0+(a_1X+ a_2X^2+\ldots+a_mX^m)]^2 = a_0^2+(a_1X+ a_2X^2+\ldots+a_mX^m)^2=a_0+.$
- $+(a_1X+ a_2X^2+\ldots+a_mX^m)^2$
- $[a_1X+ (a_2X^2+\ldots+a_mX^m)]^2 = a_1X^2 + (a_2X^2+\ldots+a_mX^m)^2$.
- Until we find $(a_0 + a_1X+ a_2X^2+\ldots+a_mX^m)^2 = a_0 + a_1X^2+ a_2X^4+\ldots+a_mX^{2m}$.
- For example $X^5+1 = X^{10}+X^5+X^5+1 = X^{10}+1$.

List of Primitive Polynomials of Degree *m*

- $m=2$
  - X^2+X+1
- $m=3$
  - X^3+X+1, X^3+X^2+1
- $m=4$
  - X^4+X+1, X^4+X^3+1
- $m=5$
  - X^5+X^2+1, X^5+X^3+1, $X^5+X^3+X^2+X+1$, $X^5+X^4+X^2+X+1$
  - $X^5+X^4+X^3+X+1$, $X^5+X^4+X^3+X^2+1$
- $m=6$
  - X^6+X+1, $X^6+X^4+X^3+X+1$, X^6+X^5+1, $X^6+X^5+X^2+X+1$
  - $X^6+X^5+X^3+X^2+1$, $X^6+X^5+X^4+X+1$

Introduction to Linear Block Codes: Vector Spaces

- Let V be a set of elements called vectors and let F be a field of elements called scalars. The addition operation + is defined between vectors. A scalar multiplication operation · is defined such that for any a in F and $\mathbf{v}$ in V, $a \cdot \mathbf{v}$ is also in V. We say that V is a vector space over F if + and · satisfy the following conditions:
  1. V forms a commutative group under +
  2. For any a in F and $\mathbf{v}$ in V, $a \cdot \mathbf{v}$ is also in V ($a \cdot \mathbf{v} + b \cdot \mathbf{w}$ in also in V if a,b are in F and $\mathbf{v}$ and $\mathbf{w}$ are in V (from 1 and 2)).
  3. + and · distribute $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$ and $a \cdot (\mathbf{v}+\mathbf{w}) = a \cdot \mathbf{v} + a \cdot \mathbf{w}$.
  4. The operation · is associative $(a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$.

Example

- Let V be the set of all length 2 vectors over GF(4).
- F={0,1 α, α^2}
- V={(0,0), (0,1), (0,α), (0, α^2), (1,0), (1,1), (1,α), (1,α^2), (α,0), (α, 1), (α, α), (α, α^2), (α^2,0), (α^2, 1), (α^2, α), (α^2, α^2)}
- Vector addition is done according to GF(4) addition and $(a,b)+(c,d) = (a+c, b+d)$
- Scalar multiplication is done $a \cdot (b,c) = (a \cdot b, a \cdot c)$ and is done according to GF(4) multiplication.
- Therefore it is easy to show that V forms a commutative group over addition, that $a \cdot \mathbf{v}$ is also in V, that addition and multiplication distribute and that multiplication is associative.

Linear Combinations

- Let $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_k$ be vectors in vector space V on field F.
- Let a_1, a_2, …, a_k be scalars in field F.
- $a_1\mathbf{v}_1+a_2\mathbf{v}_2+\ldots+a_k\mathbf{v}_k$ is a linear combination of the vectors.

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{mG}$$

$$\mathbf{m} = [a_1 \quad a_2 \quad \cdots \quad a_k]$$

$$\mathbf{G} = \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_k \end{bmatrix}$$

Spanning Sets

- Let V be a vector space
- Let G = {$\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_k$}, each in V, be a spanning set of V.
- G is a spanning set if all vectors in V can be written as a linear combination of the vectors in G.
  - The set of all vectors obtained from linear combinations of G is called the span of G = span(G).

Example of Spanning Sets

- W = {$\mathbf{v}_1$=(0,0,0), $\mathbf{v}_2$=(0,1,1), $\mathbf{v}_3$=(1,0,0) and $\mathbf{v}_4$=(1,1,1)} on GF(2)
- G={(0,1,1), (1,0,0)} = {$\mathbf{v}_2$, $\mathbf{v}_3$}
- $0\mathbf{v}_2+0\mathbf{v}_3 = \mathbf{v}_1$
- $0v_2+1\mathbf{v}_3 = \mathbf{v}_3$
- $1\mathbf{v}_2+0\mathbf{v}_3 = \mathbf{v}_2$
- $1\mathbf{v}_1+1\mathbf{v}_3 = \mathbf{v}_4$
- Therefore G is a spanning set of W since span(G) = W.

Example 2

- Let $G_2 = \{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$. This is also a spanning set of W because $\text{span}(G_2) = W$.
- However, there are multiple ways to express a vector in W as a linear combination of vectors in G_2.
  - For example $\mathbf{v}_4 = 0\mathbf{v}_2+0\mathbf{v}_3+1\mathbf{v}_4$ or $\mathbf{v}_4=1\mathbf{v}_2+1\mathbf{v}_3+0\mathbf{v}_4$.
- This is because G_2 contains vectors that are linearly dependent.
- Definition:
- The vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ are linearly dependent if there exists a set of scalars $\{a_1, a_2, \ldots, a_k\}$ (except for the all 0 case) for which $a_1\mathbf{v}_1+ a_2\mathbf{v}_2+\ldots+ a_k\mathbf{v}_k=0$.

Basis

- A spanning set for vector space V that has the smallest possible number of vectors in it is called a basis for V.
  - A basis is formed by using only linearly independent vectors
  - If one vector in G is linearly dependent on others in G, it can be removed from the set and the set still spans V.
- Example: V is the set of all binary vectors of length 3.
- V={(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)}.
- Let G_1 = {(0,0,1), (0,1,0), (1,0,0)}
- Let G_2 = {(0,1,1), (1,1,0), (1,1,1)}
- Both G_1 and G_2 each form a basis for V.

Dimension of a Vector Space

- Dim(V) = number of vectors that form a basis for V.
- In the previous example. Dim(V) = 3.
- In the first example Dim(W) = 2.

Vector Subspace

- Let V be a vector space on F and let W be a subset of V.
- If W forms a vector space, then W is a vector subspace of V.
- In the previous examples W is a subspace of V.