Error Correcting Codes Notes

Sasank

November 11, 2014

1 Properties of Linear Block Codes

- The minimum distance of a linear block code is equal to the minimum weight of its nonzero codewords
- Let C be a linear block code with parity check matrix H. There exists a codeword of weight w in C iff there exist w columns in H which sum to the zero vector.
- *Singleton Bound:* Let C be an (n, k) binary block code with minimum distance d_{min}.

  $$d_{min} \leq n - k + 1$$

  Prove by puncturing first $d_min - 1$ locations in each codeword and count number of codewords.
- Let A_i be the number of codewords of weight i in C. Probability of undetected error over a BSC is given by

  $$P_{ue} = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$

- *Standard Array:* Rows are cosets of the code and first row in each row is called a coset leader. Any error pattern equal to a coset leader is correctable. So, every (n, k) binary block code can correct 2^{n-k} error patterns.
- *Syndrome Decoding:* Each coset has a unique syndrome $y.H^T$. So, compute syndrome, find coset leader corresponding to that syndrome and add it to the received vector, y.
- Let α_i be the number of coset leaders of weight i in C. Probability of decoding error over a BSC is given by

  $$P_e = 1 - \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}$$

- *Hamming Bound*: Let C be an (n, k) binary linear block code with minimum distance $d_{min} \geq 2t+1$.

  $$2^{n-k} \geq 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}$$

  Prove by counting number of cosets. All patterns with weight less than or equal to t are coset leaders.
- *MacWilliams Identity:* Let A_i be weight distribution of C and B_i be that of $C^{\perp}$.

  $$A(z) = 2^{-(n-k)}(1+z)^n B\left(\frac{1-z}{1+z}\right)$$

  Can be useful in computing P_{ue}

2 Examples of Linear Block Codes

2.1 Hamming Code

For any integer $m \geq 3$, the code with parity check matrix consisting of all nonzero columns of length m is a Hamming code. Some Properties:

- $n = 2^m - 1$
- $k = 2^m - m - 1$
- $d_{min} = 3$

2.2 Reed Muller Code

Let $P(r, m)$ be the set of all boolean polynomials of m variables having degree r or less. Reed Muller code $RM(r, m)$ is given be the vectors

$$\{v(f) | f \in P(r, m)\}$$

Where $v(f)$ is length 2^m vector containing values of f evaluated at each of vector in F_2^m.

- Linear Code
- n = 2^m
- k = $1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$
- ~~read all this. decoding and min distance and all~~

3 Cyclic Code

An (n, k) linear block code C is a cyclic code if every cyclic shift of a codeword in C is also a codeword. Let $V(x)$ denote polynomial representation of V.

3.1 Properties

- Let $v^{(i)}(x)$ denote ith cyclic shift of $v(x)$. Then, $v^{(i)}(x) = x^i v(x) \mod x^n + 1$
- The nonzero code polynomial of minimum degree in a linear block code is unique. For (n, k) cyclic code, constant term of such polynomial $g(x)$ is 1. We call $g(x)$ generator of the code
- A binary polynomial of degree $n - 1$ or less is a code polynomial if and only if it is a multiple of $g(x)$.
- $\deg g(x) = n - k$
- $g(x)$ generates a cyclic code iff $g(x)$ is a factor of $x^n + 1$.
- *Systematic encoding:* Divide $x^{n-k}u(x)$ by $g(x)$ to obtain reminder $b(x)$. Code polynomial is given by $b(x) + x^{n-k}u(x)$

– Some Circuits here –

3.2 Error Detection

Syndrome polynomial $s(x) = r(x) \mod g(x)$

- If $x + 1$ is a factor of $g(x)$, all odd weight error patterns are detected
- A polynomial over F_2 is said to be **irreducible** over F_2 if it has no factors other than 1 and itself. A degree m irreducible polynomial is **primitive** if the smallest value of N for which it divides $x^n + 1$ is $2^m - 1$

4 Finite Groups

Definition 4.1 A set G with binary operation $*$ defined on it is called a group if

1. $*$ is associative
2. There exists a identity element e, $a * e = e * a = a$
3. For every element a, there exists a inverse b, $a * b = b * a = e$

Order of finite group is its cardinality.

4.1 Some Definitons and Properties

- **Cyclic group** $G = (g)$, for some element $g \in G$. It is called generator of G.
- **Group isomorphism** is a bijection between two groups which 'preserves' binary operation
- Every cyclic group of order n is isomorphic to $\mathbb{Z}_n$
- A nonempty subset of S of a group G is called a **subgroup** of G if for all $\alpha, \beta \in S$
  - $\alpha + \beta \in S$
  - $-\alpha \in S$
- If S is a subgroup of a finite group G, then $|S|$ divides $|G|$. For any $g \in G$, the set $S+g = \{s+g | s \in S\}$ is called a **coset** of S.
- Every subgroup of a cyclic group is cyclic. There is a *unique* subgroup for each divisor of order of the cyclic group.
- A cyclic group of order n has $\phi(n)$ generators where $\phi(n)$ is Euler's function. Can use this to prove

$$n = \sum_{d|n} \phi(d)$$

5 Finite Fields

Definition 5.1 A set F together with two binary operations $+$ and $*$ is a field if

1. F is an abelian group under $+$ whose identity is called 0
2. $F^* = F \setminus \{0\}$ is an abelian group under $*$ whose identity is called 1
3. For any $a, b, c \in F$, $a * (b + c) = a * b + a * c$

A finite field is a field with a finite cardinality.

5.1 Some Definitons and Properties

- **Field isomorphism** is a bijection between two fields which 'preserves' binary operations $+$ and $*$
- Every field F with a prime cardinality p is isomorphic to $\mathbb{F}_p$. *(Prove this by observing that $F = (1)$)*
- A nonempty subset of S of a field F is called a **subfield** of F if for all $\alpha, \beta \in S$
  - $\alpha + \beta \in S$
  - $-\alpha \in S$
  - $\alpha * \beta \in S \setminus \{0\}$
  - $-\alpha^-1 \in S \setminus \{0\}$
- Let F be a field with multiplicative identity 1. The **characteristic** of F is the smallest integer p such that $1 + 1 + 1 + \cdots + 1$ (p times) $= 0$. The characteristic of a finite field is prime. *(If not, its divisors will be characteristic contradicting minimality)*
- Every finite field has a prime subfield *($S = (1)$ is one such subfield)*
- Any finite field has p^m elements where p is a prime and m is a positive integer. *(Let p be characterstic of F, observe that F is a vector field over $\mathbb{F}_p$)*

5.2 Polynomials over a Field

Definition 5.2 A nonzero polynomial over a field F is an expression $f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_m x^m$ where $f_i \in F$ and $f_m \neq 0$. If $m = 1$, $f(x)$ is said to be monic. The set of all polynomials over a field F is denoted by $F[x]$.

- A polynomial $a(x) \in F[x]$ is said to be a **divisor** of a polynomial $b(x) \in F[x]$ if $b(x) = q(x)a(x)$ for some $q(x) \in F[x]$. Trivial divisors are α and $\alpha f(x)$, $\alpha \in F \setminus \{0\}$
- An **irreducible polynomial** is a polynomial of degree 1 or more which has only trivial divisors. A monic irreducible polynomial is called a **prime polynomial**.
- Set of reminders when polynomials in $\mathbb{F}_p[x]$ are divided by a prime polynomial $g(x) \in \mathbb{F}_p[x]$ of degree m is a field of order p^m.
- Every monic polynomial $f(x) \in F[x]$ can be *uniquely* written as a product of prime factors $a_i(x) \in F[x]$.
- If $f(x) \in F[x]$ has a degree 1 factor $x - \alpha$ for some $\alpha \in F$, then α is called a **root** of $f(x)$. $f(x)$ of degree m can have at most m roots.
- In any field F, the multiplicative group F^* of nonzero elements has at most one cyclic subgroup of any given order n. If it does, then its elements $\{1, \beta, \beta^2, \dots, \beta^{n-1}\}$ satisfy

$$x^n - 1 = (x-1)(x-\beta)(x-\beta^2)\dots(x-\beta^{n-1})$$

- Elements of a finite field F_q are q distinct roots of $x^q - x$. *($|(\beta)|$ divides $q-1$. So, $\beta^{(q-1)} = 1$ for all nonzero β)*
- F_q^* is cyclic.

~~look at proof if time available~~

6 Minimal Polynomials

Let F_q be finite field with characteristic p. Thus, F_q has a subfield isomorphic to $\mathbb{F}_p$. Consider polynomial $x^q - x \in F_q[x]$, it is also a polynomial in $F_p[x]$. Factorize $x^q - x$ into product of prime polynomials in $F_p[x]$

$$x^q - x = \prod_i g_i(x)$$

$g_i(x)$ are called the **minimal polynomials** of F_q.

Since, $x^q - x = \prod_{\beta \in F_q}(x - \beta) = \prod_i g_i(x)$, $g_i(x) = \prod_{j=1}^{\deg g_i(x)}(x - \beta_{ij})$. So, each $\beta \in F_q$ is a root of exactly one minimal polynomial of F_q, called the minimal polynomial of β.

- Let $g(x)$ be the minimal polynomial of $\beta \in F_q$. $g(x)$ is the monic polynomial of least degree in $F_p[x]$ such that $g(\beta) = 0$. *(If $h(x)$ is such least degree polynomial, prove that it should divide $g(x)$. But $g(x)$ is prime polynomial. So $h(x) = g(x)$)*
- For any $f(x) \in F_p(x)$, $f(\beta) = 0$ iff $g(x)$ divides $f(x)$ *(use previous result)*
- For any $g(x) \in F_q(x)$, $g^p(x) = g(x^p)$ iff $g(x) \in F_p[x]$
- Let $g(x)$ be the minimal polynomial of $\beta \in F_q$, If $q = p^m$, then the roots of $g(x)$ are of the form

$$\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{n-1}}$$

where n is a divisor of m. *(Using previous result, if y is a root, y^p is also a root. If n is smallest integer that $\beta^{p^2} = \beta$, show that n divides m using the fact that $\beta^{p^m} = \beta$. Now show these can be only roots by invoking previous results.)*

7 BCH Codes

Definition 7.1 Let α be a primitive element in F_{2^m}. The generator polynomial $g(x)$ of the t-error-correcting BCH code of length $2^m - 1$ is the least degree polynomial in $\mathbb{F}_2[x]$ that has

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$$

as its roots. If $\phi_i(x)$ is minimal polynomial of α^i, then $g(x)$ is LCM of $\phi_i(x), i = 1, 2, \ldots 2t$

- For BCH code of parameters m and t, we have
  - $n - k \leq mt$
  - $d_{min} \geq 2t + 1$
- A degree m irreducible polynomial in $F_2[x]$ is said to be primitive if the smallest value of N for which it divides $X^N + 1$ is $2^m - 1$. The minimal polynomial of a primitive element is a primitive polynomial. ~~How?~~
- Single error correcting BCH codes are Hamming Codes. *($v(\alpha) = 0$ for code word v. Write α^i as a tuple)*
- degree of generator polynomial $\deg g(x) \leq mt$. i.e, $n - k \leq mt$ *(Observe that even powers of α has same minimal polynomial as some odd power before it. Now, LCM of m minimal polynomials $\leq mt$)*
- $d_{min} \geq 2t + 1$ ~~complete this.~~