ELEC 433 Formula Sheet

Coding Approaches and Characteristics

Channel Capacity for Additive White Gaussian for bandwidth W and noise N_0:

$$C = W\log_2\left(1 + \frac{P}{N_0 W}\right)$$

BFSK bit error probability:

$$p = \frac{1}{2}e^{-E_b/2N_0}$$

Binary Linear Block Codes

Number of codewords in a code C:

$$|C| = M = 2^k$$

Code rate:

$$R = \frac{\log_2(M)}{n} = \frac{k}{n}$$

Vector space dimensions:

$$\dim S + \dim S^{\perp} = \dim V$$

Def (*Binary Linear Block Codes*): A subset $C \subseteq V_n$ is a binary linear block code if:

- $\mathbf{u} + \mathbf{v} \in C \quad \forall \mathbf{u}, \mathbf{v} \in C$
- $a\mathbf{u} \in C \quad \forall \mathbf{u} \in C, a \in \{0, 1\}$

Hamming Weight:

$w(\mathbf{x})$ = number of non-zero elements in $\mathbf{x}$

Hamming Distance:

$d(\mathbf{x}, \mathbf{y})$ = number of places in which $\mathbf{x}$ and $\mathbf{y}$ differ

Hamming Distance for binary linear codes:

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$$

Minimum Hamming Distance:

- $d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$
- A code C can detect up to v errors if $d(C) \geq v + 1$
- A code C can correct up to t errors if $d(C) \geq 2t + 1$

Def (*Generator Matrix*): A $k \times n$ matrix whose rows for a basis for a linear (n, k) code of a subspace C is said to be a generator matrix for C.

Groups, Rings, and Fields

Def (*Group*) A group $(G, \cdot)$ is a set of objects G on which a binary operation $\cdot$ is defined: $a \cdot b \in G : \forall a, b \in G$. The operation must satisfy:

- Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Identity: $\exists e \in G \mid \forall a \in G, a \cdot e = a$
- Inverse: $\forall a \in G, \exists$ unique $a^{-1} \in G \mid a \cdot a^{-1} = e$

Def (*Commutative Group*) A group is said to be commutative or abelian if it also satisfies: $\forall a, b \in G, a \cdot b = b \cdot a$

Def (*Ring*) A ring $(R, +, \cdot)$ is a set of objects R on which two binary operations ($+$ and $\cdot$) are defined. It has properties:

- $(R, +)$ is a commutative group under $+$ with identity "0"
- Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Distribution: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Def (*Commutative Ring*) A ring is said to be commutative if it also satisfies: $\forall a, b \in G, a \cdot b = b \cdot a$

Def (*Ring with Identity*) A ring is said to be a ring with identity if the operation $\cdot$ has an identity element "1"

Def (*Division Ring*) Let $(R, +, \cdot)$ be a ring, and $R^* = R - 0$. If the ring is a commutative ring with identity, and $(R^*, \cdot)$ is a group, then the ring is said to be a division ring.

Def (*Field*) A field $(F, +, \cdot)$ is a set of objects F for which two binary operations ($+$ and $\cdot$) are defined. F is said to be a field if and only if:

- $(F, +)$ is a commutative group under $+$ with additive identity "0"
- $(F^*, \cdot)$ is a commutative group under $\cdot$ with multiplicative identity "1"
- Distribution: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Finite Integer Fields:

$S = \{0, 1, \ldots, p - 1\}$ form a finite field if p is prime.

Properties of Finite Fields:

- Order: A field of order q has cardinality $|F| = q$, denoted $\mathrm{GF}(q)$
- Let $\beta \in \mathrm{GF}(q), \beta \neq 0$. The order of β is the smallest positive integer m such that $\beta^m = 1$
- If t is the order of β, then $t \mid (q - 1)$
- In any finite field, there are on or more elements of order $q - 1$ called primitive elements.

Euler's Totient Function:

$\phi(t)$ = number of positive integers less than t that are relatively prime to t

Finite Fields and Euler's Totient Function:

- The number of elements in $\mathrm{GF}(q)$ of order t is $\phi(t)$
- In $\mathrm{GF}(q)$ there are exactly $\phi(q - 1)$ primitive elements
- If α is a primitive element, then $1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$ must be non-zero elements of $\mathrm{GF}(q)$

Def (*Primitive Polynomial*) If an irriducible polynomial $p(x)$ such that the smallest positive integer n for which $p(x)$ divides $x^n - 1$ is $n = p^m - 1$ for a prime p and positive integer m, the polynomial is said to be a primitive polynomial.

Updated February 9, 2022
https://github.com/DonneyF/formula-sheets