Information Theory and Coding (66.24)
Arithmetic in GF(2)

Group

A set G on which a binary operation * is defined is called a Group if:

1. * is associative
2. G contains an element such that, for any a in G $a * e = e * a = a$ (identity)
3. For any element a in G exits a' shuch that $a * a' = a' * a = e$ (inverse)

i) The identity is unique. ii) The inverse is unique. Prove.

Rings

A set of elements R on which two binary operations, called addition "+" and multiplication "." are defined satisfying the following conditions:

1. R is a commutative group under +
2. Multiplication is associative
3. Multiplication is distributive over addition $a.(b + c) = a.b + a.c$

Fields

A set of elements F forming a ring satisfying the following condition:

1. The set of nonzero elements in F is a commutative Group under "."

The characteristic λ of the field GF(q) is the smallest positive integer shuch that $\sum_{i=1}^{\lambda} 1 = 0$

1. The characteristic λ is prime.
2. GF(λ) is also a field, then, is a subfield of GF(q)

Table 1: Module-2 Addition

+	0	1
0	0	1
1	1	0

Table 2: Module-2 Multiplication

.	0	1
0	0	0
1	0	1

3. The characteristic of GF(2) is 2

The order of a field element a is the smallest integer n shuch that $a^n = 1$
i) Being a a non zero element in GF(q), then $a^{q-1} = 1$
ii) Let n be the order of a, then n divides $q - 1$

Fundamental Definition

In a field GF(q), a nonzero element a is said to be *primitive* if the order of a is $q - 1$.

Fundamental Property

Every finite field has a primitive element. The powers of a primitive element generate all the nonzero elements of GF(q).

Vector Spaces

Let V be a set of elements on which a binary operation "+" is defined. Let F be a field. A multiplication operation "." between F an V is also defined. The set V is called a *vector space* if:

1. V is a commutative Group under +
2. For any element a in F and any element $\mathbf{v}$ in V, $a.\mathbf{v}$ is an element in V
3. $a.(\mathbf{u} + \mathbf{v}) = \mathbf{a.u} + \mathbf{a.v}$, $(a + b).\mathbf{v} = \mathbf{a.v} + \mathbf{b.v}$
4. $(a.b)\mathbf{v} = \mathbf{a.(b.v)}$
5. $1.\mathbf{v} = \mathbf{v}$

Linear Codes

Linear block codes are a vector space on GF(2)
Block codes in *systematic* form

$$\begin{aligned} \mathbf{c} &= \underbrace{b_0\ b_1 \cdots b_{n-k-1}}_{\text{Parity bits}}\ \underbrace{m_0\ m_1 \cdots m_{k-1}}_{\text{Message bits}} \\ &= (\mathbf{b}\ \mathbf{m}) \end{aligned} \tag{1}$$

$$\mathbf{b} = \mathbf{m}\mathbf{P}$$

$$\begin{aligned} \mathbf{c} &= \mathbf{m}\ (\mathbf{P}\ \mathbf{I_k}) \\ &= \mathbf{m}\ \mathbf{G} \end{aligned} \tag{2}$$

Closure

$$\begin{aligned} \mathbf{c_i} + \mathbf{c_j} &= \mathbf{m_i}\ \mathbf{G} + \mathbf{m_j}\ \mathbf{G} \\ &= (\mathbf{m_i} + \mathbf{m_j})\ \mathbf{G} \end{aligned} \tag{3}$$

$$H = (I_{n-k}\ P^T)$$

$$H^T = \begin{pmatrix} I_{n-k} \\ P \end{pmatrix}$$

$$\begin{aligned} H\ G^T &= \left(I_{n-k}\ P^T\right) \begin{pmatrix} P^T \\ I_k \end{pmatrix} \\ &= P^T + P^T \\ &= 0 \end{aligned} \tag{4}$$

$$\begin{aligned} \mathbf{c}\ \mathbf{H^T} &= \mathbf{m}\ \mathbf{G}\ \mathbf{H^T} \\ &= 0 \end{aligned} \tag{5}$$

Syndrome

$$\mathbf{r} = \mathbf{c} + \mathbf{e}$$

$$\mathbf{s} = \mathbf{r}\ \mathbf{H^T}$$

Property 1

$$\mathbf{s} = \mathbf{e}\,\mathbf{H^T}$$

Property 2
All error patterns that differ by a code have the same syndrome

$$\mathbf{e_i} = \mathbf{e} + \mathbf{c_i}$$

$$\mathbf{e_i}\,\mathbf{H^T} = \mathbf{e}\,\mathbf{H^T}$$

Hamming distance

$$d(\mathbf{c_1}, \mathbf{c_2}) \text{ number of bits of difference}$$

Hamming weight

$$w(\mathbf{c_i}) \text{ number of nonzero bits}$$

Hamming minimum distance d_{min}, the smallest Hamming distance between pairs.

1. **The minimum distance coincides with the smallest Hamming weight of the nonzero code vectors** Why?
2. **The minimum distance is related to the number of linearly independendent column vectors of H** Why (Hint: see (5))?
3. **A linear block code $\{n, k\}$ of minimum distance d_{min} can detect error patterns of weight $d_{min} - 1$ or less**
4. **A linear block code $\{n, k\}$ can correct pattern errors of weight t or less iif $t \leq \lfloor \frac{1}{2}(d_{min} - 1) \rfloor$** Why? Remember jointly typical sequences decoding.

Syndrome decoding:
The set of 2^n possible outcomes is partitioned in 2^k disjoint subsets $\mathcal{D}_1, \mathcal{D}_2, \cdots, \mathcal{D}_{2^k}$. Each $\mathcal{D}_i$ is built by adding each error pattern of weight t or less to the codword $\mathbf{c_i}$.

In the same way, *cosets* are defined by adding each codeword $\mathbf{c_i}$ to the error pattern $\mathbf{e_i}$ corresponding to one of the 2^{n-k} syndromes. The error pattern correspondig to each coset is called *coset leader*.

Decoding procedure: Given a received syndrome, identify the coset, then choose the coset leader $\mathbf{e_0}$. The estimated codewrod is $\mathbf{r} + \mathbf{e_0}$.

Example: Hamming Codes (See [1], p. 639)

Further reading. [2] Chap. 2, [1] Chap.10, [3] Chap. 2-3.

References

[1] Simon Haykin. *Communications Systems*. John Wiley & Sons Inc., 2001.

[2] Shu Lin and Daniel J. Costello Jr. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.

[3] Jorge Castiñeira Moreira and Patrick Guy Farrel. *Essentials of Error-Control Coding*. John Wiley & Sons Ltd., 2006.