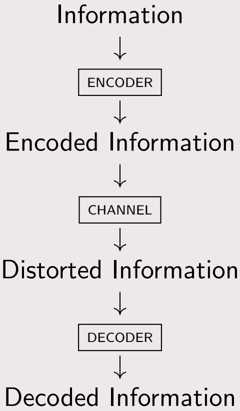
Block Code Basics

Communications Channel



Information

ENCODER

Encoded Information

CHANNEL

Distorted Information

DECODER

Decoded Information

Channel Coding

The basic idea of channel coding is to take data to be transmitted and add some extra information (known as redundancy) in hopes of being able to recover the original data after transmission.

Block Codes

Let F be a finite set of symbols. Let F^n denote the set of n length vectors with components from F. A **block code** C is a subset of F^n where n is the code length.

Let F be a finite field. A **linear block code** C is an F-subspace of F^n where n is the code length.

Let C be a linear code. Since C is an F-subspace it has an F-basis. A matrix whose rows form a basis for C is as a **generator matrix** for C. A matrix whose row space is C is simply a **generating matrix** for C. The dual space of C is denoted by $C^\perp$ is

$$C^\perp = \{v \in F^n | c.v = 0 \text{ for all } c \in C\}.$$

Since $C^\perp$ is also F-subspace it has an F-basis. A matrix whose rows form a basis for $C^\perp$ is a **parity check matrix** for C. Notice $C = \{v \in F^n | vH^T = 0\}$.

Hamming Distance

Hamming Distance - Block Code

$$d(C) = \min_{a,b \in C, a \neq b} d(a,b)$$

where $d(a,b)$ is the number of entries where a and b differ.

In a linear block code,

$$d(C) = \min_{a,b \in C, a \neq b} d(a,b) = \min_{a,b \in C, a \neq b} w(a-b) = \min_{a \in C \setminus 0} w(a)$$

where $w(a)$ is the number of non-zero entries in a.

The function d on F^n is a metric on the space. The idea is to find codes where $d(C)$ is large. This is essentially choosing codewords that are “far” apart in the space. This allows for better error detection and correction.

Packing and Covering radius

Let $C \subset F_q^n$ be a block code and $c \in C$. A sphere V of radius r around c contains

$$\sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

vectors i.e. the number of vectors v s.t. $d(v, c) \leq r$.

The **packing radius** of a code C is the largest t s.t. if there is a sphere of radius t around each codeword of C, the spheres do not overlap. Let $d = d(C)$. Then the packing radius t of C satisfies $t = \lfloor \frac{d-1}{2} \rfloor$. (The packing radius of a code is the maximum number of errors that a code can correct).

Proof: Let $c_1, c_2 \in C$ s.t. $c_1 \neq c_2$ and $v_1, v_2 \in F_q^n$ s.t. $d(c_1, v_1) \leq t$ and $d(c_2, v_2) \leq t$. Since t is the packing radius, $d(v_1, v_2) \geq 1$. Hence, $d(c_1, c_2) \geq 2t + 1$. So, $t \leq \lfloor \frac{d(c_1,c_2)-1}{2} \rfloor$.

The **covering radius** of a code C is the smallest s s.t. if there is a sphere of radius s around each codeword of C, the spheres completely cover F_q^n.

Sphere Packing Bound

Let $C \subset F_q^n$ be a code and t the packing radius of C. Then

$$|C| \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n$$

so,

$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}.$$

This is known as the **sphere packing bound**.Notice if for the covering radius s of C, $s = t$, the spheres will be "perfectly" packed.A code C is **perfect** if its packing radius coincides with its covering radius.

Gilbert Bound

Let $A_q(n,d)$ $(B_q(n,d))$ be the number of codewords in the largest q-ary (linear) block code of length n and minimum distance d. Clearly, $A_q(n,d) \geq B_q(n,d)$.

The **Gilbert Bound** is

$$A_q(n,d) \geq B_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}$$

Proof: Let $C \subset F_q^n$be a linear code with $d = d(C)$ where $|C| = B_q(n,d)$. Assume the covering radius of C is d or greater. Centered at every codeword of C, place a sphere of radius $d-1$. Since the covering radius of C is greater than $d-1$ there is $v \in F_q^n$ not covered by one of the spheres. For any $c \in C$, $d(v,c) \geq d$. But the subspace spanned by C and v would be a subspace with minimum distance d. This contradicts the definition of $B_q(n,d)$ so the covering radius is strictly less than d. Hence we have

$$B_q(n,d) \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \geq q^n.$$