Block Codes

block code A code C that consists of words of the form $(c_0, c_1, \ldots, c_{n-1})$, where n is the number of *coordinates* (and is said to be the *length* of the code).

q-ary code A code whose coordinate values are taken from a set (alphabet) of size q (unless otherwise stated, GF(q)).

encoding Breaking the data stream into blocks, and mapping these blocks onto codewords in C.

The encoding process is depicted in [Wic, Fig. 4-1].

Redundancy

If the data blocks of a q-ary code are of length k, then there are $M = q^k$ possible data vectors. (But all data blocks are not necessarily of the same length.)

There are q^n possible words of length n, out of which $q^n - M$ are not valid codewords. The **redundancy** r of a code is

$$r = n - \log_q M,$$

which simplifies to $r = n - k$ if $M = q^k$.

Code Rate

The redundancy is frequently expressed in terms of the code rate. The **code rate** R of a code C of size M and length n is

$$R = \frac{\log_q M}{n}.$$

Again, if $M = q^k$, $R = k/n$.

Transmission Errors

The corruption of a codeword by channel noise, modeled as an additive process, is shown in [Wic, Fig. 4-2].

error detection Determination (by the error control decoder) whether errors are present in a received word.

undetectable error An error pattern that causes the received word to be a valid word other than the transmitted word.

error correction Determine which of the valid codewords is most likely to have been sent.

decoder error In error correction, selecting a codeword other than that which was transmitted.

Error Control

The decoder may react to a detected error with one of the following three responses:

automatic repeat request (ARQ) Request a retransmission of the word. For applications where data reliability is of great importance.

muting Tag the word as being incorrect and pass it along. For applications in which delay constraints do not allow for retransmission (for example, voice communication).

forward error correction (FEC) (Attempt to) correct the errors in the received word.

Weight and Distance (1)

The **(Hamming) weight** of a word $\mathbf{c}$, denoted by $w(\mathbf{c})$ (or $w_H(\mathbf{c})$), is the number of nonzero coordinates in $\mathbf{c}$.

Example. $w((0, \alpha^3, 1, \alpha)) = 3$, $w(0001) = 1$.

The *Euclidean distance* between $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ and $\mathbf{w} = (w_0, w_1, \ldots, w_{n-1})$ is

$$d_E(\mathbf{v}, \mathbf{w}) = \sqrt{(v_0 - w_0)^2 + (v_1 - w_1)^2 + \cdots + (v_{n-1} - w_{n-1})^2}.$$

Weight and Distance (2)

The **Hamming distance** between two words, $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ and $\mathbf{w} = (w_0, w_1, \ldots, w_{n-1})$, is the number of coordinates in which they differ, that is,

$$d_H(\mathbf{v}, \mathbf{w}) = |\{i \mid v_i \neq w_i, 0 \leq i \leq n-1\}|,$$

where the subscript H is often omitted. Note that $w(\mathbf{c}) = d(\mathbf{0}, \mathbf{c})$, where $\mathbf{0}$ is the all-zero vector, and $d(\mathbf{v}, \mathbf{w}) = w(\mathbf{v} - \mathbf{w})$.

The **minimum distance** of a block code C is the minimum Hamming distance between all pairs of distinct codewords in C.

Minimum Distance and Error Detection

Let $d_{\min}$ denote the minimum distance of the code in use. For an error pattern to be undetectable, it must change the values in at least $d_{\min}$ coordinates.

▷ A code with minimum distance $d_{\min}$ can detect *all* error patterns of weight less than $d_{\min}$.

Obviously, a large number of error patterns of weight $w \geq d_{\min}$ can also be detected.

Forward Error Correction

The goal in FEC systems is to minimize the probability of decoder error given a received word $\mathbf{r}$. If we know exactly the behavior of the communication system and channel, we can derive the probability $p(\mathbf{c} \mid \mathbf{r})$ that $\mathbf{c}$ is transmitted upon receipt of $\mathbf{r}$.

maximum a posteriori decoder (MAP decoder) Identifies the codeword $\mathbf{c}_i$ that maximizes $p(\mathbf{c} = \mathbf{c}_i \mid \mathbf{r})$.

maximum likelihood decoder (ML decoder) Identifies the codeword $\mathbf{c}_i$ that maximizes $p(\mathbf{r} \mid \mathbf{c} = \mathbf{c}_i)$.

Bayes's rule $p(\mathbf{c} \mid \mathbf{r}) = \frac{p_C(\mathbf{c})p(\mathbf{r}|\mathbf{c})}{p_R(\mathbf{r})}$.

Minimum Distance and Error Correction

The two decoders are identical when $p_C(\mathbf{c})$ is constant, that is, when all codewords occur with the same probability. The maximum likelihood decoder is assumed in the sequel.

The probability $p(\mathbf{r} \mid \mathbf{c})$ equals the probability of the error pattern $\mathbf{e} = \mathbf{r} - \mathbf{c}$. Small-weight error patterns are more likely to occur than high-weight ones $\Rightarrow$ we want to find a codeword that minimizes $w(\mathbf{e}) = w(\mathbf{r} - \mathbf{c})$.

▷ A code with minimum distance $d_{\min}$ can correct *all* error patterns of weight less than or equal to $\lfloor (d_{\min} - 1)/2 \rfloor$.

It is sometimes possible to to correct errors with $w > \lfloor (d_{\min} - 1)/2 \rfloor$.

Decoder Types

A **complete error-correcting decoder** is a decoder that, given a received word $\mathbf{r}$, selects a codeword $\mathbf{c}$ that minimizes $d(\mathbf{r}, \mathbf{c})$.

Given a received word $\mathbf{r}$, a ***t*-error-correcting bounded-distance decoder** selects the (unique) codeword $\mathbf{c}$ that minimizes $d(\mathbf{r}, \mathbf{c})$ iff $d(\mathbf{r}, \mathbf{c}) \leq t$. Otherwise, a *decoder failure* is declared.

Question. What is the difference between decoder errors and decoder failures in a bounded-distance decoder?

Example: A Binary Repetition Code

The binary repetition code of length 4 is $\{0000, 1111\}$.

Received	Selected	Received	Selected
0000	0000	1000	0000
0001	0000	1001	0000 or 1111*
0010	0000	1010	0000 or 1111*
0011	0000 or 1111*	1011	1111
0100	0000	1100	0000 or 1111*
0101	0000 or 1111*	1101	1111
0110	0000 or 1111*	1110	1111
0111	1111	1111	1111

*Bounded-distance decoder declares decoder failure.

Error-Correcting Codes and a Packing Problem

A central problem related to the construction of error-correcting codes can be formulated in several ways:

1. With a given length n and minimum distance d, and a given field $\mathrm{GF}(q)$, what is the maximum number $A_q(n,d)$ of codewords in such a code?
2. What is the minimum redundancy for a t-error-correcting q-ary code of length n ?
3. What is the maximum number of spheres of radius t that can be packed in an n-dimensional vector space over $\mathrm{GF}(q)$?

The Hamming Bound

The number of words in a sphere of radius t in an n-dimensional vector space over $\mathrm{GF}(q)$ is

$$V_q(n,t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

Theorem 4-1. The size of a t-error-correcting q-ary code of length n is

$$M \leq \frac{q^n}{V_q(n,t)}.$$

The Gilbert Bound

Theorem 4-2. There exists a t-error-correcting q-ary code of length n of size

$$M \geq \frac{q^n}{V_q(n,2t)}.$$

Proof: Repeatedly pick any word $\mathbf{c}$ from the space, and after each such operation, delete all words $\mathbf{w}$ that satisfy $d(\mathbf{c},\mathbf{w}) \leq 2t$ from further consideration. Then the final code will have minimum distance at least $2t+1$ and will be t-error-correcting. The theorem follows from the fact that at most $V_q(n,2t)$ words are deleted from further consideration in each step. □

Comparing Bounds

Theorems 4-1 and 4-2 say that for the redundancy r of a code,

$$\log_q V_q(n,t) \leq r \leq \log_q V_q(n,2t).$$

These bounds for binary 1-error-correcting codes are compared in [Wic, Fig. 4-3].

Perfect Codes

A block code is **perfect** if it satisfies the Hamming bound with identity.

Theorem 4-4. Any nontrivial perfect code over GF(q) must have the same length and cardinality as a Hamming, Golay, or repetition code.

Note: The sphere packing problem and the error control problem are not entirely equivalent.

List of Perfect Codes

1. $(q, n, k = n, t = 0), (q, n, k = 0, t = n)$: trivial codes.
2. $(q = 2, n$ odd$, k = 1, t = (n-1)/2)$: odd-length binary repetition codes (trivial codes).
3. $(q, n = (q^m - 1)/(q-1), k = n - m, t = 1)$ with $m > 0$ and q a prime power: Hamming codes and and nonlinear codes with the same parameters.
4. $(q = 2, n = 23, k = 12, t = 3)$: the binary Golay code.
5. $(q = 3, n = 11, k = 6, t = 2)$: the ternary Golay code.

Research Problem. Are there other perfect codes over alphabets that are not fields (where q is not a prime power)?

Definitions

With bit error probability p and n bits, there are on average np errors $\Rightarrow$ if the code length n is allowed to increase, the minimum distance $d_{\min}$ must increase accordingly. Let

$$\delta = \frac{d_{\min}}{n},$$

$$a(\delta) = \limsup_{n\to\infty} \left[\frac{\log_q A_q(n, \lfloor \delta n \rfloor)}{n} \right],$$

where $a(\delta)$ is the maximum possible code rate that a code can have if it is to maintain a minimum distance/length ratio δ as its length increases without bound.

Some Bounds

The entropy function:
$H_q(x) = x \log_q(q-1) - x \log_q x - (1-x)\log_q(1-x)$ for $0 < x \leq (q-1)/q$.

The Gilbert-Varshamov (lower) bound: If $0 \leq \delta \leq (q-1)/q$, then $a(\delta) \geq 1 - H_q(\delta)$.

The McEliece-Rodemich-Rumsey-Welch (upper) bound:
$a(\delta) \leq H_2(1/2 - \sqrt{\delta(1-\delta)})$.

Bounds for the binary case are plotted in [Wic, Fig. 4-4].

Linear Block Codes

A q-ary code C is said to be **linear** if it forms a vector subspace over GF(q). The *dimension* of a linear code is the dimension of the corresponding vector space.

A q-ary linear code of length n and dimension k (which then has q^k codewords) is called an (n, k) code (or an $[n, k]$ code).

Linear block codes have a number of interesting properties.

Properties of Linear Codes

Property One The linear combination of any set of codewords is a codeword ($\Rightarrow$ the all-zero word is a codeword).

Property Two The minimum distance of a linear code C is equal to the weight of the codeword with minimum weight (because $d(\mathbf{c}, \mathbf{c}') = w(\mathbf{c} - \mathbf{c}') = w(\mathbf{c}'')$ for some $\mathbf{c}'' \in C$).

Property Three The undetectable error patterns for a linear code are independent of the codeword transmitted and always consist of the set of all nonzero codewords.

Generator Matrix

Let $\{\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}\}$ be a basis of the codewords of an (n, k) code C over GF(q). By Theorem 2-6, every codeword $\mathbf{c} \in C$ can be obtained in a unique way as a linear combination of the words $\mathbf{g}_i$. The *generator matrix* $\mathbf{G}$ of such a linear code is

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix},$$

and a data block $\mathbf{m} = (m_0, m_1, \ldots, m_{k-1})$ is encoded as $\mathbf{mG}$.

Parity Check Matrix

The dual space of a linear code C is called the **dual code** and is denoted by $C^\perp$. Clearly, $\dim(C^\perp) = n - \dim(C) = n - k$, and it has a basis with $n - k$ vectors. These form the **parity check matrix** of C:

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k-1} \end{bmatrix} = \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix}.$$

The Parity Check Theorem

Theorem 4-8. A vector $\mathbf{c}$ is in C iff $\mathbf{cH}^T = \mathbf{0}$.

Proof: $(\Rightarrow)$ Given a vector $\mathbf{c} \in C$, $\mathbf{c} \bullet \mathbf{h} = 0$ for all $\mathbf{h} \in C^\perp$ by the definition of dual spaces.
$(\Leftarrow)$ If $\mathbf{cH}^T = \mathbf{0}$, then $\mathbf{c} \in (C^\perp)^\perp$, and the result follows as $(C^\perp)^\perp = C$, which in turn holds as $C \subseteq (C^\perp)^\perp$ and $\dim(C) = \dim((C^\perp)^\perp)$. $\square$

Parity Check Matrix and Minimum Distance

Theorem 4-9. The minimum distance of a code C with parity check matrix $\mathbf{H}$ is the minimum nonzero number of columns that has a nontrivial linear combination with zero sum.

Proof: If the column vectors of $\mathbf{H}$ are $\{\mathbf{d}_0, \mathbf{d}_1, \ldots, \mathbf{d}_{n-1}\}$ and $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$, we get
$\mathbf{cH}^T = \mathbf{c}[\mathbf{d}_0\ \mathbf{d}_1\ \cdots\ \mathbf{d}_{n-1}]^T = c_0\mathbf{d}_0 + c_1\mathbf{d}_1 + \cdots + c_{n-1}\mathbf{d}_{n-1}$, so $\mathbf{cH}^T = 0$ is a linear combination of $w(\mathbf{c})$ columns of $\mathbf{H}$. $\square$

Singleton Bound

Theorem 4-10. The minimum distance $d_{\min}$ of an (n, k) code is bounded by $d_{\min} \leq n - k + 1$.

Proof: By definition, any $r + 1$ columns of a matrix with rank r are linearly dependent. A parity check matrix of an (n, k) code has rank $n - k$, so any $n - k + 1$ columns are linearly dependent, and the theorem follows by using Theorem 4-9. $\square$