Advanced Communication Systems

ELEN90051 (Lecturer Margreta Kuijper)

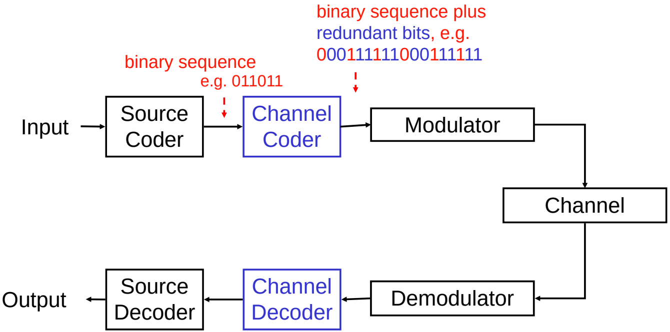
Basic theory of linear block codes; algebraic codes; LDPC codes

1st Semester 2018

Written by Margreta Kuijper; see Chapter 7 and Chapter 8 pp.558-571 of "Digital Communications" by Proakis & Salehi, 2008

All scanned tables and text are from the textbook "Digital Communications" by Proakis and Salehi, 2008

RECALL:


binary sequence plus
redundant bits, e.g.
0001111110001111111
binary sequence
e.g. 011011
Input
Source Coder
Channel Coder
Modulator
Channel
Output
Source Decoder
Channel Decoder
Demodulator

RECALL: THREE DIFFERENT TYPES OF CHANNEL CODING:

- block codes– every block of k information bits is mapped into a block of n coded bits
- convolutional codes– k streams of information bits are convoluted into n streams of coded bits
- trellis coded modulation– error control is combined with modulation

TWO DIFFERENT WAYS OF DESCRIBING CODES:

- via matrices and/or polynomials (= [Ch. 7 PS08])
- via trellises and/or graphs (= [Ch. 8 PS08])

Up till now restricted to bits. Let's now operate more generally and deal with information symbols, coded symbols, etcetera.

We assume that symbols are from a field $\mathbb{F}$

- $\mathbb{F} = \{0, 1\}$ (considered up till now)
- $\mathbb{F} = \{0, 1, 2, \ldots, 9, X\}$
- $\mathbb{F} = \{000, 100, 010, 001, 110, 011, 111, 101\}$
- and many more....

DEFINITION

A (n, k) **block code** C is defined as the set of all codewords $\boldsymbol{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}^n$ resulting from encoding information words $\boldsymbol{u} = (u_0, u_1, \dots, u_{k-1}) \in \mathbb{F}^k$.

DEFINITION

A block code C is **linear** if for all $\lambda_1, \lambda_2 \in \mathbb{F}$ and all $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$ we have that

$$\lambda_1 \boldsymbol{c}_1 + \lambda_2 \boldsymbol{c}_2 \in C.$$

Note: This means that a (n, k) linear block code is a subspace of dimension k of the vector space $\mathbb{F}^n$.

TUTORIAL QUESTION 6.1

How many codewords are there in a (n, k) binary linear block code?

Example

The $(3,1)$ binary repetition code C is given by

$$C = \{(0,0,0),(1,1,1)\}.$$

We can also write this as

$$C = \{(c_0,c_1,c_2) \mid (c_0,c_1,c_2) = uG\}$$

where $G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$, or as

$$C = \{(c_0,c_1,c_2) \mid (c_0,c_1,c_2)H^T = 0\}$$

where $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

Definition

Let a (n, k) block code C be given by

$$C = \{\boldsymbol{c} \in \mathbb{F}^n \mid \boldsymbol{c} = \boldsymbol{u}G \text{ for some } \boldsymbol{u} \in \mathbb{F}^k\}$$

where $G \in \mathbb{F}^{k \times n}$.
Then G is called a **generator matrix** of C.

Definition

Let a (n, k) block code C be given by

$$C = \{\boldsymbol{c} \in \mathbb{F}^n \mid \boldsymbol{c}H^T = 0\}$$

where $H \in \mathbb{F}^{(n-k) \times n}$.
Then H is called a **parity check matrix** of C.

Note: $GH^T = 0$; also note that a parity check matrix is not unique—there are many matrices H such that $GH^T = 0$.

Tutorial question 6.2

Consider the $(k+1,k)$ binary parity check code

$$C = \{(p, u_0, u_1, \ldots, u_{k-1}) \mid p = 0 \;\text{ if }\; \sum_{i=0}^{i=k-1} u_i = 0$$

$$\text{or } p = 1 \;\text{ if }\; \sum_{i=0}^{i=k-1} u_i = 1\}$$

Give the corresponding generator matrix G and write down a parity check matrix H.

Definition

Two codes are called **equivalent** if they are the same up to a permutation of codeword components.

Recovering the message word from the decoded codeword is easy when a systematic generator matrix is used:

Definition

The generator matrix G of a (n, k) linear code is called **systematic** if G is of the form

$$G = \begin{bmatrix} A & I_k \end{bmatrix}.$$

Quiz 1: Show that any (n, k) linear code is equivalent to a (n, k) linear code with a systematic generator matrix.

EXAMPLE 7.2–1. Consider a (7, 4) linear block code with

$$G = [I_4 \mid P] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{7.2–8}$$

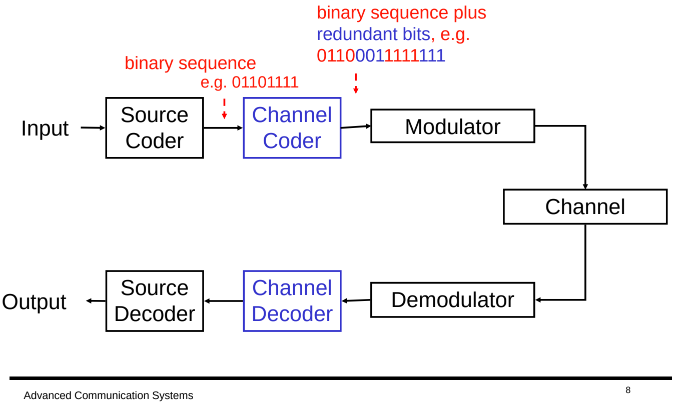
Obviously this is a systematic code. The parity check matric for this code is obtained from Equation 7.2–7 as

$$H = \left[P^t \mid I_{n-k}\right] = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{7.2–9}$$

If $u = (u_1, u_2, u_3, u_4)$ is an information sequence, the corresponding codeword $c = (c_1, c_2, \ldots, c_7)$ is given by

$$\begin{aligned} c_1 &= u_1 \\ c_2 &= u_2 \\ c_3 &= u_3 \\ c_4 &= u_4 \\ c_5 &= u_1 + u_2 + u_3 \\ c_6 &= u_2 + u_3 + u_4 \\ c_7 &= u_1 + u_2 + u_4 \end{aligned} \tag{7.2–10}$$

Previous example put into context:



Tutorial question 6.3

Consider a linear code C with generator matrix

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

A) Give a systematic generator matrix for C.

B) Determine a parity check matrix H for C

DEFINITION

Let C be a (n, k) code with $(n-k) \times n$ parity check matrix H. Then the **dual code** $C^{\perp}$ is the $(n, n-k)$ code that has H as its generator matrix.

TUTORIAL QUESTION 6.4

What is the dual code of the $(k+1, k)$ binary parity check code of Tute Q6.2?

TUTORIAL QUESTION 6.5

A code is **self-dual** if $C = C^{\perp}$. Show that for a (n, k) self-dual code we must have n even and the rate k/n equal to $1/2$.

Suppose our channel is a BSC with cross-over probability $p < 0.5$.

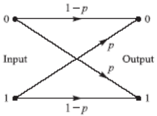


FIGURE 6.5–2
Binary symmetric channel.

Question: When we use a channel code, what do we want from the channel decoder?

Answer: decoder should minimize P(decoder error | received word $\boldsymbol{y}$).

- a Maximum A Posteriori (MAP) decoder maximizes P(codeword $\boldsymbol{c}$ was sent | $\boldsymbol{y}$ received) over all possible codewords $\boldsymbol{c}$.
- a Maximum Likelihood (ML) decoder maximizes $P(\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ received $\mid \boldsymbol{c}$ transmitted$)$ over all possible codewords $\boldsymbol{c}$.

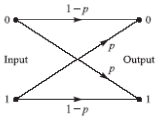


FIGURE 6.5–2
Binary symmetric channel.

- $P(\boldsymbol{c}|\boldsymbol{y}) = \frac{P(\boldsymbol{y}|\boldsymbol{c})P(\boldsymbol{c})}{P(\boldsymbol{y})}$, so MAP decoder and ML decoder give the same result if all codewords are equally likely to be transmitted
- For hard-decision decoding the ML decoder chooses the sparsest error pattern $\boldsymbol{e}$. **Quiz 2:** Why? (use that $\frac{p}{1-p} < 1$)
- The ML decoder chooses $\boldsymbol{c}$ such that $\boldsymbol{c}$ is "closest to" $\boldsymbol{y}$
- Thus ML decoding = minimum distance decoding

We need to define "distance" more precisely....

Definition

The **weight** of a word $\boldsymbol{v} \in \mathbb{F}^n$ is defined as

$$w(\boldsymbol{v}) := \#\text{nonzero components in } \boldsymbol{v}.$$

Definition

The **Hamming distance** between two words $\boldsymbol{v}$ and $\tilde{\boldsymbol{v}}$ is defined as

$$d(\boldsymbol{v}, \tilde{\boldsymbol{v}}) := w(\boldsymbol{v} - \tilde{\boldsymbol{v}}).$$

DEFINITION

The **minimum distance** of a code C is defined as

$$d_{min}(C) := \min \{d(\boldsymbol{c}, \tilde{\boldsymbol{c}}) \mid \boldsymbol{c}, \tilde{\boldsymbol{c}} \in C \ \text{ and } \ \boldsymbol{c} \neq \tilde{\boldsymbol{c}}\}.$$

For a linear code C we have

$$d_{min}(C) = \min \{w(\boldsymbol{c}) \mid \boldsymbol{c} \in C \ \text{ and } \ \boldsymbol{c} \neq 0\}.$$

Quiz 3: Why?

Example: consider the $(5,2)$ linear code
$C = \{00000, 10110, 11101, 01011\}$; check for this code that
$d_{min}(C) = \min \{w(\boldsymbol{c}) \mid \boldsymbol{c} \in C \ \text{ and } \ \boldsymbol{c} \neq 0\}$.

Consider a linear code C with parity check matrix H. With every codeword in C of weight w, we can associate a set of w linearly dependent columns of H (check this for yourself!). Therefore

$$d_{min}(C) = \text{ min \#columns of } H \text{ that are linearly dependent.}$$

Quiz 4: Show that $d_{min}(C) \leq n - k + 1$ (= Singleton bound)

Definition

A code C that meets the above bound, that is,

$$d_{min}(C) = n - k + 1$$

is called a **Maximum Distance Separable (MDS)** code.

Later we will see that the ISBN code is an MDS code over GF(11).
Quiz 5: can you think of any binary MDS codes, that is, can you think of any MDS codes over GF(2)? Is the Hamming code an MDS code?

In general it is hard to list the number of codewords of weight d_{min}. However, for a MDS code of length n over GF(q) we have an expression, namely

$$\#\text{ codewords of weight } d_{min} = \binom{n}{d_{min}}(q-1)$$

Let us now assume that a codeword $\boldsymbol{c}$ was sent through a BSC and a word $\boldsymbol{y}$ was received. Then

- errors are undetectable if and only if $\boldsymbol{y} \in C$.
- all error patterns of weight $< d_{min}(C)$ are detectable.
- all error patterns of weight $< \frac{d_{min}(C)}{2}$ are correctable. **Quiz 6:**Why? (show that for such error patterns $d(y, \tilde{\boldsymbol{c}}) > \frac{d_{min}(C)}{2}$ must hold for $\tilde{\boldsymbol{c}} \neq \boldsymbol{c}$)

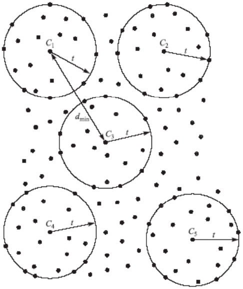


FIGURE 7.5–1
A representation of codewords as center of spheres with radius $t = \left\lfloor \frac{1}{2}(d_{\min} - 1) \right\rfloor$.

QUESTION:

Is it possible that correctable error patterns of weight $\geq \frac{d_{min}}{2}$ exist?

ANSWER:

Yes, so it may pay off to do list decoding rather than unique decoding. Of course we hope that the list size turns out to be 1.

In list decoding we fix an integer $\tau \geq \frac{d_{min}}{2}$ and then aim to find all $\boldsymbol{c} \in C$ for which $d(\boldsymbol{y}, \boldsymbol{c}) \leq \tau$.

Since the early 90's this is a very active research area, especially for MDS codes. Such codes have been implemented in, for example, CD, DVD, hard disk drives.

QUESTION:

Do block codes with low d_{min} necessarily perform badly?

ANSWER:

No, it depends on the type of decoder. There exist binary block codes with low d_{min} that perform spectacularly well with soft-decision decoding, particularly in high noise environments. These are the Low Density Parity Check (LDPC) codes, see later.

Since the early 00's this is a very active research area. LDPC codes have been implemented in, for example, digital video broadcasting; hard disk drives.

EXAMPLE

The ISBN code is an example of a nonbinary code. It is a $(10, 9)$ code over the field $\mathbb{Z}_{11} = \{0, 1, 2, \ldots, 9, X\}$ with parity check matrix

$$H = \left[\begin{array}{cccccc} 1 & 2 & 3 & \cdots & 9 & X \end{array}\right].$$

Here the operations "addition" and "multiplication" all need to take place modulo 11. **Quiz 7:** Is this a single-error detecting code? Is this a single-error correcting code? Is this code MDS??

Quiz 8: Repeat the previous quiz for the $(10, 8)$ code over $\mathbb{Z}_{11}$, given by parity check matrix

$$H = \left[\begin{array}{cccccc} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 3 & \cdots & 9 & X \end{array}\right].$$

Several types of error probability at play:

- p := transmission bit error probability (= a channel parameter)
- P_e := codeword error probability. Useful fact: if codewords are equally likely to be transmitted and the code is linear then

$$P_e = P\,(\text{decoder decides nonzero codeword} \mid \text{zero codeword transmitted})$$

- P_b := information bit error probability

Note: bit errors at different locations of an information word of length k may have different probabilities, let's call these $P_{b,j}$ for $j = 1, \ldots, k$. The code's bit error probability P_b is the average of these probabilities:

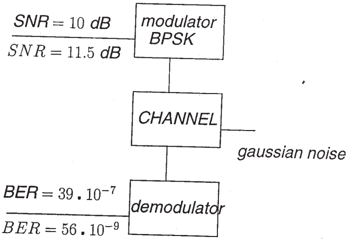
$$P_b = \frac{1}{k}\sum_{j=1}^{k} P_{b,j}$$

Quiz 9: Show that $\frac{1}{k}P_e \le P_b \le P_e$

- Recall that error control is used to achieve a lower information bit error probability P_b.
- Put differently: error control is used to achieve a desired P_b at reduced transmitter power levels
- Crucial in case of power limitations, e.g. satellite applications, mobile communications

Example

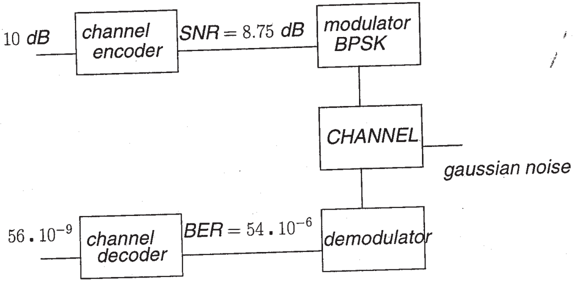
The following figure shows two scenarios where no coding is used:



Now suppose we start using a binary $(15, 11)$ code C, given by

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Then we get a better performance:



Definition

Let a SNR of γ dB lead to a bit error probability P_b at the decoder output in the coded system. Let $\tilde{\gamma}$ dB be the required SNR to achieve P_b at the demodulator output of the uncoded system. Then the **coding gain** at P_b is defined as $\tilde{\gamma} - \gamma$ dB.

In the previous example the coding gain at $P_b = 56 \cdot 10^{-9}$ equals $11.5 - 10 = 1.5$ dB.

This Hamming code is not a particularly good code; it can be proven from Shannon's theory that

- a coding gain of $11.5 - 0.4 = 11.1$ dB at $P_b = 56 \cdot 10^{-9}$ is theoretically possible with hard-decision decoding
- a coding gain of $11.5 + 1.6 = 13.1$ dB at $P_b = 56 \cdot 10^{-9}$ is theoretically possible with soft-decision decoding

Research in this area focuses on finding good codes that are practically implementable.

RECALL:

- An (n, k) block code maps blocks of k information bits into blocks of n coded bits, there is no memory between blocks
- Its code rate is defined as k/n.
- We'll now look at some practical linear block codes:
  - family of Hamming codes
  - family of maximum length codes

  We'll describe them via matrices, later we'll look at some linear block codes described via graphs....

Let H be the $r \times n$ matrix whose columns are all nonzero binary vectors of length r. So for $r = 3$ for example:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Let C be the $(2^r - 1, 2^r - r - 1)$ binary code that has H as a parity check matrix. **Quiz 10:** Show that $d_{min}(C) = 3$.

Definition

The above code C is called a **Hamming code**

Properties:

- $d_{min} = 3$, so single-error correcting
- easy to decode
- optimal sphere packing property (code is then called **perfect**)

How to decode

Consider again our example of the $(7,4)$ Hamming code with

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Suppose $\boldsymbol{c}_0$ is sent and $\boldsymbol{y}$ is received. We can decode by calculating the received word's **syndrome**, given as

$$\begin{bmatrix} S_1 & S_2 & S_3 \end{bmatrix} := \boldsymbol{y}H^T$$

- If $S_1 = S_2 = S_3 = 0$ then decide: no errors
- Otherwise: suppose $\begin{bmatrix} S_1 & S_2 & S_3 \end{bmatrix}^T$ equals the i'th column of H. Now decide: single error in position i.

Tutorial question 6.6

1. Show that the above procedure is single-error correcting.
2. Let the probability of a bit transmission error be denoted by p. Calculate the probability of a decoder error in the above example.

Definition

The dual of a Hamming code is called a **maximum-length code**.

Tutorial Question 6.7

1. show that a maximum-length code is a $(2^r - 1, r)$ code (with r any integer > 2)
2. (advanced!) show that its nonzero codewords all have the same weight, namely 2^{r-1}.

DEFINITION

A (n, k) code is **shortened** to a $(n-1, k-1)$ code by deleting an information component.

Note: Shortening can be achieved by deleting a column of the parity check matrix (without changing its rank).

DEFINITION

A (n, k) code is **extended** to a $(n+1, k)$ code by adding a check component.

Note: Extending can be achieved by adding a column to the generator matrix. **Quiz 11:** Can d_{min} decrease when a code is extended?

Example

An extended binary $(n+1, k)$ code can be obtained by adding a parity check bit, thus requiring that all codewords have even weight. The parity check matrix then becomes

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & & H_{old} & \\ \vdots & & & \\ 0 & & & \end{bmatrix}.$$

Some further modifications that occur in practice:

- **puncturing** (= inverse operation to “extending”)
- **lengthening** (= inverse operation to “shortening”).

Example

The extended $(8,4)$ Hamming code C has parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Now $d_{min}(C) = 4$ and C is not only single-error correcting but also triple-error detecting.

Correction & detection method:

Calculate

$$\begin{bmatrix} S_1 & S_2 & S_3 & S_4 \end{bmatrix} := \boldsymbol{y}H^T$$

- If $S_1 = S_2 = S_3 = S_4 = 0$ then decide: no errors
- If $\begin{bmatrix} S_1 & S_2 & S_3 & S_4 \end{bmatrix} \neq (0,0,0,0)$ and $S_1 = 1$: suppose $\begin{bmatrix} S_1 & S_2 & S_3 & S_4 \end{bmatrix}^T$ equals the i'th column of H. Now decide: single error in position i.
- Otherwise detect: ≥ 2 errors have occurred.

General error correction method for a binary (n, k) code:

STANDARD ARRAY DECODING

Construct a look-up table of size $2^{n-k} \times 2^k$ as follows

1. Write down all codewords of C in the first row, starting with $00 \cdots 0$.
2. Select a pattern of lowest weight (not listed before) as row leader of the next row. In every column write the sum of that pattern and the column leader.
3. Repeat the previous step until all possible 2^n words have been listed.
4. If $\boldsymbol{y}$ is received, locate $\boldsymbol{y}$ in the jth column of the table. Then choose the jth column leader as the decoded codeword.

Note: if $\boldsymbol{y}$ is in the (i, j)th position of the table, then this procedure declares the ith row leader as the error word $\boldsymbol{e}$; the rows of the above array constitute the so-called **cosets** of C. A row leader $\boldsymbol{e}$ is also called a **coset leader**; by construction, it is the word of smallest weight in the coset.

There exists a more efficient table lookup decoding method. First we need:

DEFINITION

Let H be a $(n-k) \times n$ parity check matrix of C and let $\boldsymbol{y}$ be a received word. Then

$$\boldsymbol{s} = (\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_{n-k}) := \boldsymbol{y}H^T$$

is called the **syndrome** of $\boldsymbol{y}$.

Note: if $\boldsymbol{y}_1 - \boldsymbol{y}_2$ equals a codeword, then their syndromes are the same. In particular, each coset gives rise to a single syndrome and we can condense each row in the standard array to a row of only 2 elements: the error word and its corresponding syndrome, see next method.

Syndrome table decoding

1. Write down the zero error pattern as the first element of the second column; write its syndrome $00\cdots0$ as the first element of the first column.
2. Select an error pattern of lowest weight whose syndrome is not listed before as the next element in the second column; write its syndrome as the next element in the first column.
3. Repeat the previous step until all possible 2^{n-k} syndromes are listed.
4. If $\boldsymbol{y}$ is received, compute its syndrome $\boldsymbol{s} = \boldsymbol{y}H$ and locate $\boldsymbol{s}$ in the ith row of the first column. Then choose the error pattern in the ith row as the error word $\boldsymbol{e}$ and compute $\boldsymbol{y} - \boldsymbol{e}$ as the decoded codeword.

EXAMPLE

Consider the $(5,2)$ code C with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Quiz 12: What is $d_{min}(C)$?

TABLE 7.5–1
The Standard Array for Example 7.5–1

00000	01011	10101	11110
00001	01010	10100	11111
00010	01001	10111	11100
00100	01111	10001	11010
01000	00011	11101	10110
10000	11011	00101	01110
11000	10011	01101	00110
10010	11001	00111	01100

Note: all error patterns of weight 1 are coset leaders as expected (**Why?**) but there is only room for two error patterns of weight 2.

Example–continued

Show that a parity check matrix for C is given by

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

TABLE 7.5–2
Syndromes and Coset Leaders for Example 7.5–2

Syndrome	Error Pattern
000	00000
001	00001
010	00010
100	00100
011	01000
101	10000
110	11000
111	10010

Suppose the zero codeword was transmitted but $\boldsymbol{y} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \end{bmatrix}$ is received. The syndrome $\boldsymbol{s}$ is then computed as $\boldsymbol{s} = \boldsymbol{y}H^t = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$. The above syndrome table results in a decoder error (**check this for yourself**).

Tutorial Question 6.8

Construct the standard array for the $(7,3)$ binary code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Also determine the correctable error patterns, their corresponding syndromes and then construct a syndrome table.

The class of cyclic codes is an important class that allow for algebraic encoding/decoding methods—a prime example is the family of Reed-Solomon codes.

Definition

A Reed-Solomon code is a $(q-1, q-1-r)$ code over GF(q) = $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ with parity check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{q-2} \\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{q-2} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha^r & (\alpha^r)^2 & \cdots & (\alpha^r)^{q-2} \end{bmatrix}.$$

Note that the above matrix H is just a chunk of the Discrete Fourier Transform (DFT) matrix Φ, wellknown to you from Signals & Systems. But this time the DFT is taken over the finite field GF(q).

In more detail: the $(q-1)\times(q-1)$ DFT matrix Φ is given by

$$\Phi = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{q-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^r & (\alpha^r)^3 & \cdots & (\alpha^r)^{q-2} \\ 1 & \alpha^{r+1} & (\alpha^{r+1})^3 & \cdots & (\alpha^{r+1})^{q-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{q-2} & (\alpha^{q-2})^2 & \cdots & (\alpha^{q-2})^{q-2} \end{bmatrix}.$$

Suppose that $q = 2^m$ for some positive integer m and define $\beta := \alpha^{-1}$. Then $\beta = \alpha^{q-2}$ and the inverse DFT is written as

$$\Phi^{-1} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \beta & \beta^2 & \cdots & \beta^{q-2} \\ 1 & \beta^2 & (\beta^2)^2 & \cdots & (\beta^2)^{q-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^r & (\beta^r)^3 & \cdots & (\beta^r)^{q-2} \\ 1 & \beta^{r+1} & (\beta^{r+1})^3 & \cdots & (\beta^{r+1})^{q-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{q-1} & (\beta^{q-1})^2 & \cdots & (\beta^{q-1})^{q-2} \end{bmatrix}.$$

From Φ times Φ^{-1} = identity matrix, we can easily obtain the generator matrix G of the above RS code.

Properties of a Reed-Solomon code

- nonbinary, in practice often defined over the alphabet of bytes ($q = 2^8$)
- reaches Singleton bound, so is MDS
- used in many practical applications (CD, DVD etc.)
- good at correcting burst errors
- dual code is again a Reed-Solomon code

Hamming codes can also be formulated as cyclic codes and then decoded via algebraic encoding and decoding methods. Cyclic Redundancy Check (CRC) codes are also cyclic codes, used in many applications, particularly for error detection. Examples: electronic tolling communication; medical devices.

Low Density Parity Check (LDPC) codes

- are block codes; with sparse parity check matrix represented by a graph
- invented by Gallager in his 1963-PhD thesis
- re-invented several times since then
- late 90's: performance close to Shannon limit
- very fast encoding and decoding algorithms
- used in many modern standards (Ethernet, WLAN, WiMAX, DVB etc)

Definition

A binary block code is called a **Low Density Parity Check (LDPC) code** if it has a parity check matrix H with only a small number of ones in each row and column (Here H not necessarily of full row rank); furthermore, a (γ, ρ)-regular LDPC code has exactly γ ones in each column and exactly ρ ones in each row of H.

Example:

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

(from "Error control coding" by Lin and Costello, 2nd edition, 2004)

Note that in this example H does not have full row rank.

Tanner graphs

Definition

A Tanner graph of a binary code C with parity-check matrix H is a graph $\mathcal{G} = (\mathcal{V}_1, \mathcal{V}_2, \mathcal{E})$ with nodes in two disjoint subsets $\mathcal{V}_1$ and $\mathcal{V}_2$, such that

- each coded symbol i is represented by a variable node $v_i \in \mathcal{V}_1$;
- each parity-check equation j is represented by a check node $s_j \in \mathcal{V}_2$;
- there exists an edge between a variable node v_i and a check node s_j if and only if $h_{ji} = 1$.

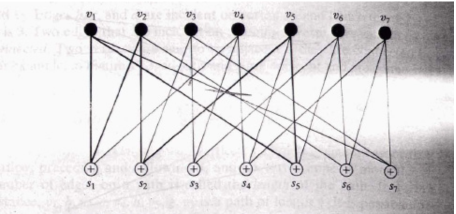


FIGURE 17.6: The Tanner graph of a (7, 3) linear block code.

(from "Error control coding" by Lin and Costello, 2nd edition, 2004)

EXAMPLE:

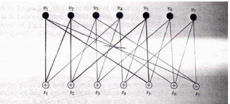


FIGURE 17.6: The Tanner graph of a (7, 3) linear block code.

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

(from “Error control coding” by Lin and Costello, 2nd edition, 2004)

- There are 7 coded symbols and 7 parity-check equations.
- Each coded symbol participates in $\gamma = 3$ parity-check equations
- Each parity-check equation contains $\rho = 3$ coded symbols
- H^T is incidence matrix of Tanner graph

Another example:

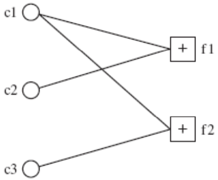


FIGURE 8.10–3
The Tanner graph for the (3, 1) repetition code.

Quiz:

Find the Tanner graph of the $(4, 1)$ binary code given by parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

Decoding of LDPC codes

- A simple hard decision decoding method is called bit flipping algorithm
- see bit flipping example for code of the above Quiz, downloadable under LMS-"Additional Material" (Lara Dolecek slides)
- bit flipping algorithm is iterative and involves messages being passed between check nodes and variable nodes of the code's Tanner graph
- the soft decision version is called message passing algorithm

Performance of LDPC codes

- LDPC codes achieve very good performance with message passing decoding, for example at a BER of 10^{-5}, there exists a $(65520, 61425)$ LDPC code of rate 0.9375 that is less than 0.5dB away from the Shannon limit of 3.91dB.

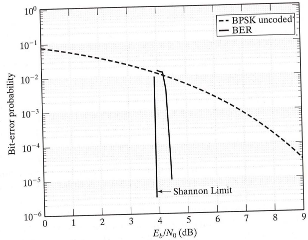


FIGURE 1.12: Bit-error performance of a (65520,61425) low-density parity check code decoded with a soft-decision near-MLD algorithm.

(from "Error control coding" by Lin and Costello, 2nd edition, 2004)

Random LDPC codes

- some randomly generated regular LDPC codes have very good error correcting performance (MacKay '99)
- for example $(3,6)$-regular $(504,252)$ EG-Gallager code
- large encoding complexity because of lack of algebraic structure
- some very long ($n \approx 10^7$) random LDPC codes perform very well, only 0.0045 dB away from Shannon limit (Chung, Fornay, Richardson, Urbanke 2001)
- some random irregular LDPC codes perform also very well
  - randomly choose γ_i's and ρ_i's from designed degree distributions $\gamma(x)$ and $\rho(x)$
  - for example (see Lin and Costello, 2004, page 925):
    $n = 4000$; rate = 0.82;
    $\gamma(x) = 0.4052x + 0.3927x^2 + 0.1466x^6 + 0.0555x^7$;
    $\rho(x) = 0.3109x^{18} + 0.6891x^{19}$