

Lecture of January 26th, 2007

Scribe: Frank Kschischang

## 1 Syndrome Decoding

Let  $C$  be a code (not necessarily linear) over a field  $F$ . Assume that we have a channel with input and output alphabet  $F$ . Assume that  $v \in C$  is transmitted and that  $r = v + e$  is received. If  $C = \{v_1, v_2, \dots, v_M\}$  is a code with  $M$  codewords, the set  $E$  of possible error patterns is

$$E = \{r - v_1, r - v_2, \dots, r - v_M\} = \{r - v : v \in C\} = r - C.$$

Given the received vector  $r$ , there is a one-to-one correspondence between the possible error patterns and the codewords, and, in particular,  $|E| = |C| = M$ .

When  $C$  is a linear code, then, since  $-C = \{-v : v \in C\} = C$ , we have

$$E = r - C = r + C = \{r + v : v \in C\},$$

thus the set of possible error patterns corresponding to the received word  $r$  is precisely the coset  $r + C$  of  $C$ . To decode, we must examine this coset to find the appropriate error pattern (for example, the error pattern of least Hamming weight in the coset).

Let  $C$  be a linear  $[n, k]$  code over a finite field  $F$  of size  $q$ . Every coset of  $C$  has  $|C| = q^k$  elements, and these cosets form a disjoint cover of  $F^n$ , thus an  $[n, k]$  linear code has  $q^{n-k}$  cosets in  $F^n$ .

★ **Definition:** Let  $H$  be a parity-check matrix for  $C$ . The *syndrome*  $s$  associated with a received word  $r$  is  $s = rH^T$ .

Observe that

$$s = rH^T = (v + e)H^T = vH^T + eH^T = eH^T,$$

i.e., the syndrome depends only on the error pattern  $e$  and *not* the transmitted codeword  $v$ . Syndromes and cosets of  $C$  are deeply related, as the following theorem shows.

★ **Theorem:** Two vectors  $x, y \in F^n$  yield the same syndrome if and only if they are elements of the same coset of  $C$ .

*Proof:* Suppose that  $x$  and  $y$  are elements of the same coset of  $r + C$ , i.e.,  $x = r + v$  and  $y = r + w$  for some codewords  $v, w \in C$ . We have

$$xH^T = (r + v)H^T = rH^T + vH^T = rH^T,$$

and likewise

$$yH^T = (r + w)H^T = rH^T + wH^T = rH^T;$$

thus,  $x$  and  $y$  yield the same syndrome.

Conversely, suppose that  $x$  and  $y$  yield the same syndrome, i.e.,  $xH^T = yH^T$ . Then  $(x - y)H^T = 0$ , so  $x - y \in C$ . This means that  $x - y = v$  for some  $v \in C$ , so  $x = y + v$ . This shows that  $x$  is an element of the coset  $y + C$ , which necessarily also contains  $y$ . ■

Since the syndrome determines the coset, and the error pattern must be an element of the coset, this theorem tells us that the syndrome is a sufficient statistic for determining the error pattern.

We will illustrate with a simple example.

**Example:** Suppose  $C = \{00000, 11100, 00111, 11011\}$ , a code whose generator and parity-check matrices may be taken as

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \text{ and } H = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

respectively. We can explicitly list the elements of each coset of  $C$  in the following *standard array*:

Identifier	Coset					Syndrome
$C$	<b>00000</b>	11100	00111	11011		000
$10000 + C$	<b>10000</b>	01100	10111	01011		110
$01000 + C$	<b>01000</b>	10100	01111	10011		100
$00100 + C$	<b>00100</b>	11000	00011	11111		010
$00010 + C$	<b>00010</b>	11110	00101	11001		011
$00001 + C$	<b>00001</b>	11101	00110	11010		001
$01001 + C$	<b>01001</b>	10101	01110	<b>10010</b>		101
$10001 + C$	<b>10001</b>	01101	10110	<b>01010</b>		111

Included in this array is the syndrome value associated with each syndrome. The given identifier for a coset is not the only possible one. For example, the reader will verify that  $10000 + C = 01100 + C = 10111 + C = 01011 + C$ . In other words, any of the vectors in a coset can be used as a *coset representative*, and translating  $C$  by any element of the coset yields all the coset elements.

Now, having computed the syndrome, we can narrow the set of possible error patterns to one of those in the corresponding coset of  $C$ . An element in the coset with the highest probability of occurrence is called a *coset leader* (usually an element with the least Hamming weight). In this example the coset leaders are indicated in boldface.

As computation of the syndrome is sufficient for determining the error pattern, the error-correcting decoder structure shown in Fig. 1 is suggested.

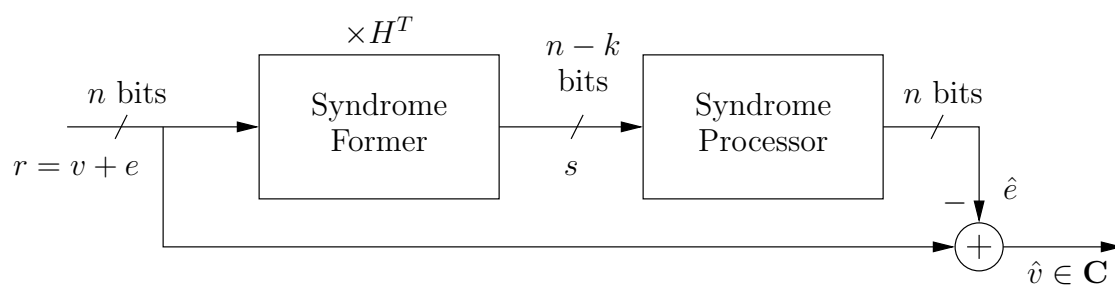
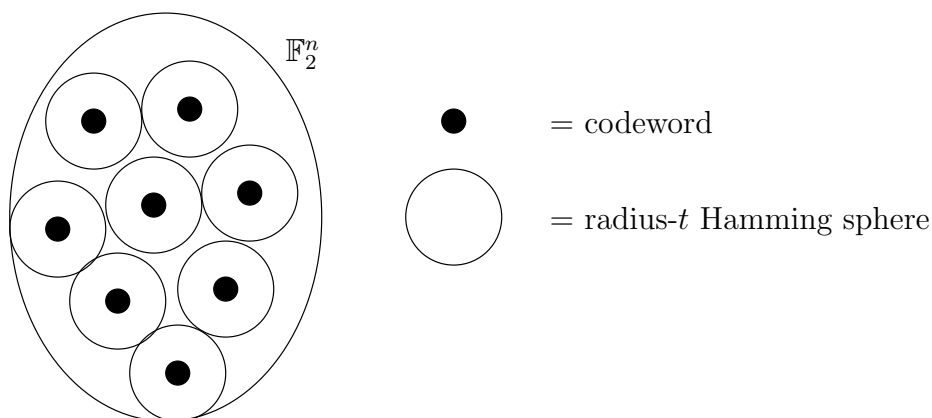


Figure 1: Decoder structure for a linear code.

## 2 Some Simple Bounds

### 2.1 Volume (Hamming) Bound

The geometry of  $F^n$  under the Hamming metric can be used to derive an upper bound on the number of codewords in any binary  $t$ -error correcting code. The fundamental observation is that, if a code is to be  $t$ -error correcting, then the radius- $t$  “Hamming spheres” surrounding the codewords must all be disjoint, as shown schematically in Fig. 2.

Figure 2: The geometry of Hamming space: in a  $t$ -error correcting code, Hamming spheres of radius  $t$  centered at the codewords must be disjoint.

It is easy to show that the number of vectors contained within a Hamming sphere of radius  $t$  is given by

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}.$$

The total number of vectors contained in all these Hamming spheres cannot exceed

the total number of vectors in  $F^n$ , i.e.,

$$|C| \left( 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right) \leq 2^n,$$

and hence

$$|C| \leq 2^n / \left( 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right),$$

a result known as the *Hamming bound* on the cardinality of a  $t$ -error-correcting code.

**Example:** For example, if  $t = 1$  and  $n = 7$ , we have  $|C| \leq 2^7 / (1 + 7) = 16$ , a bound achieved with equality by the (7,4) Hamming code.

★ **Definition:** A code that achieves the Hamming bound with equality is called a *perfect* code.

★ **Theorem:** The binary Hamming codes are perfect.

*Proof:* The binary Hamming codes have  $t = 1$ ,  $n = 2^m - 1$ , and  $k = n - m$ , for  $m \geq 3$ . According to the Hamming bound, such codes cannot have more than

$$\frac{2^n}{1 + n} = 2^{2^m - 1} / (1 + 2^m - 1) = 2^{2^m - m - 1} = 2^{n - m}$$

codewords, but this is precisely the number of codewords in the code. ■

Other examples of binary perfect codes include the repetition codes of odd block length, and the 3-error-correcting (23, 12) binary Golay code. In fact, perfect codes are rare, as these examples are known to be the only ones possible. (There is also a spurious ternary Golay code.) Most codes, and certainly most of those used in practice, are not perfect.