Notebook
Algebraic Coding Theory
Math 525
Stephen Giang

08/24/20 - Introduction

1. This class covers the science of ”error-correcting codes.”
2. Binary Symmetric Channel

08/26/20 - Introduction.pdf + Section 1.1 - 1.6.pdf

1. Example of Coding:
   (a) 0 is encoded as 000, and 1 is 111 - Encoder
   (b) After corruption, the decoder will use the majority vote: $000 \rightarrow \{000, 100, 010, 001, 110, 011, 101, 111\}$
   (c) If the decoder receives a three digit number, it will decode it as which ever number is the majority - ex: $001 \rightarrow 0, 110 \rightarrow 1$
   (d) Probability of $000 \rightarrow 110$ is $qqp = q^2p$, where $q = 1 - p$ is the probability of error, and p is probability of correct conversion.
   (e) The probability of $000 \rightarrow 111, 110, 101, 011$ is $Pr(E) = q^3 + 3q^2p$. When evaluating $p = .9, q = .1$, we get $Pr(E) = .028$.
   (f) For probability of this or that, we add the probabilities.
   (g) In other examples, encoding will always convert the 0 or 1 into a string of odd number 0s or 1s. Ex: $0 \rightarrow 000, 00000, 0000000$
2. Definitions:
   (a) Digits or Bits: 0,1
   (b) Word: Sequence of digits
   (c) Length of word: # of digits a word has
   (d) Channel: Physical Link that connects data source to data sink. In this course, we will model these channels with error characteristics. Refer to the Binary Symmetric Channel
   (e) Binary Channel: Only 0's or 1s are transmitted or received over it
   (f) Binary Code: Set of words. Ex: {00,110,01,11}
   (g) Block Code - Binary Code, but all words have the same length
   (h) Repetition and parity-check codes:
      i. Repetition Codes: {000...0,111...1,...} with n copies.
      ii. Rate is $\frac{1}{n}$
      iii. Rate is for every n bits, the receiver receives 1 bit of information,
      iv. Parity-Check Code: $C = \{(x_1x_2...x_n) | x_1 + ... + x_n \text{ is even}, x_i \text{ are 0s and 1s}\}$

v. $n = 3 : C = \{000, 110, 011, 101\}$

vi. $n = 4 : C = \{0000, 1100, 1010, 0011, 0110, 1001, 0101, 1111\}$

vii. For $n = 4$, the rate is $\frac{3}{4}$

(i) C is Code, and $|C|$ is the number of code words, or words held in the code. Its also known as the size or cardinality of the code.

08/28/20 - Section 1.1 - 1.6

1. For $n = 3$:
   - Given 00 - 001
   - Given 10 - 101
2. Notice that we give it 2, and then it adds an extra number to make sure there are an even number of 1s.
3. So the rate is $\frac{2 \text{ bits info}}{3 \text{ bit word}} = \frac{2}{3}$
4. We will assume that errors occur independently, that is, the occurrence of error during a time slot does not imply anything about the next time slot.
5. Special Case: $p = 1$ and $p = 0$
6. We can always assume that $\frac{1}{2} \leq p < 1$
7. The information rate of a code C is the proportion of digits that convey information.

$$R = \frac{\log_2 |C|}{n} \text{ bits per block,}$$

   where n is the length of C (length of codewords within C)
8. Example:

$$\begin{aligned} C &= \{000, 010, 100, 001, 110, 101, 011, 111\} \\ &\to \{00011, 01001, 10000, 00111, 11001, 10110, 01101, 11111\} \end{aligned}$$

   Notice $|C| = 8$, so $\log_2 |C| = \log_2(8) = 3$. Length of C = 5. Thus $R = \frac{3}{5}$.
9. Example of error-correcting:

   $C_1 = \{00, 01, 10, 11\}$ cannot detect any errors, let alone correct any errors.
   $C_2 = \{000, 011, 101, 110\}$ (Parity Check Code of Length 3) can detect one error (affecting any codeword).
   $C_3 = \{000000, 010101, 101010, 111111\}$

   C_3 can detect up to 2 errors (affecting any codeword). Suppose 110101 is received. The most likely code transmitted is 010101, So we make the correction

08/31/20 - Section 1.7,1.8

1. Let $\phi_p(v, w)$ = probability of receiving w given that v was sent. We have:

$$\phi_p(v, w) = p^{n-d}q^d$$

, where n is the length of the codewords, and d is the number of disagreements or areas of corruption.

2. Ex:

$$v = 1110101$$
$$w = 1010010$$
$$\phi_p(v, w) = pqppqqq = p^{7-4}q^4 = p^3q^4$$

3. Suppose we have a BSC with $\frac{1}{2} \leq p < 1$. Suppose v_1 and w disagree in d_1 positions and v_2 and w disagree in d_2 positions. Then

$$\phi_p(v_1, w) \leq \phi_p(v_2, w) \Longleftrightarrow d_2 \leq d_1$$

4. Proof:

$$\phi_p(v_1, w) \leq \phi_p(v_2, w)$$
$$p^{n-d_1}q^{d_1} \leq p^{n-d_2}q^{d_2}$$
$$\left(\frac{p}{q}\right)^{d_2-d_1} \leq 1$$

Notice that$\frac{1}{2} \leq p < 1$ with $q = 1 - p$, so that makes $\frac{p}{q} \geq 1$, thus making $d_2 \leq d_1$

5. Let $K = \{0, 1\}$ and define two operations on it, $+$ and $\cdot$, as addition and multiplication modulo 2. Endowed with these two operations, K becomes a field.

6. Let n be a positive integer, then:

$$K^n = K \times K \times ... \times K = \{(v_1, ...v_n)|v_i \in K, i = 1, ..., n\}$$

7. In K^n, define addition componentwise, that is:

$$(v_1, v_2, ..., v_n) + (w_1, w_2, ..., w_n) = (v_1 + w_1, v_2 + w_2, ..., v_n + w_n)$$

for all $(v_1, v_2, ..., v_n), (w_1, w_2, ..., w_n) \in K^n$ with $+$ as addition in modulo 2.

8. We define multiplication by scalar as

$$a(v_1, v_2, ..., v_n) = (av_1, av_2, ..., av_n)$$

for all $a \in K$ and for all $(v_1, v_2, ..., v_n) \in K^n$

9. Thus K^n becomes a vector space over K.

10. If v is sent and w is received, then $e = v + w$ is called the error pattern or error vector. The nonzero components of e indicate errors. Ex: $v = 010100$ and $w = 011101$, then $e = 001001$ is the error pattern, where the 1's are the errors.

11. Let $v \in K^n$. The Hamming weight (or just weight) of v, denoted by $wt(v)$ is the number of nonzero components. Ex: $wt(0111001) = 4$

12. Let $v, w \in K^n$. The Hamming distance (or just distance) between v and w, denoted by $d(v, w)$, is the number of postions in which they disagree. Ex: $d(010101, 101001) = 4$.

13. Note that $d(v, w) = wt(v + w)$

14. The Hamming distance is a metric, meaning it has the reflexive, symmetric, and triangle inequality properties.

$$d(v, w) = 0 \iff v = w \tag{Reflexive}$$
$$d(v, w) = d(w, v) \tag{Symmetric}$$
$$d(v, w) \leq d(v, u) + d(u, w) \tag{Triangle Inequality}$$

09/02/20 - Section 1.9, 1.11

1. Complete Maximum Likelihood Decoding (CMLD) - Let $v \in C$. If $d(v, w) < d(v_1, w)$ $\forall v_1 \in C, v_1 \neq v$, then decode w as v. If there is more than one codeword closest to w, select one of them arbitrarily and conclude that it was the sent codeword.

2. Incomplete Maximum Likelihood Decoding (IMLD) - Let $v \in C$. If $d(v, w) < d(v_1, w)$ $\forall v_1 \in C, v_1 \neq v$, then decode w as v. If there is more than one codeword closest to w, request retransmission.

3. Recall that $w = v + e$, where w is the recieved word, v is the sent codeword, and e is the error pattern. Thus,
$$d(v, w) = wt(v + w), wt(e)$$

4. In conclusion, the decoder's strategy is to decode w into the codeword v which yields the error pattern of smallest weight.

5. Ex: Let $C = \{000, 001, 010, 011\}$. Length of codewords ($n = 3$), K^3 = all binary triples. Construct an IMLD table for it:

Recieved w	$w + 000$	$w + 001$	$w + 010$	$w + 011$	Decode v
000	000	001	010	011	000
100	100	101	110	111	000
010	010	011	000	001	010
001	001	000	011	010	001
110	110	111	100	101	010
101	101	100	111	110	001
011	011	010	001	000	011
111	111	110	101	100	011

6. We say that code C detects the error pattern e iff $v + e \notin C, \forall v \in C$
7. Ex: $C = \{00000, 10101, 00111, 11100\}$. Determine whether C detects each of the error patterns: $e = 10101, e = 01010, e = 11011$
   - Notice that if $e = 10101$, We get $00000 \to 10101$. Thus the code C does not detect the error pattern
   - Notice that if $e = 01010$, $v + e \notin C, \forall v \in C$, so C does detect the error pattern
   - Notice that if $e = 11011$, We get $00111 \to 11100 \in C$. Thus the code C does not detect the error pattern

09/04/20 - Section 1.11

1. Minimum distance - $d(C) = \min\{d(u, v) | u, v \in C, u \neq v\}$
2. If $d(C) = d$, then C detects all non-zero error patterns of weight $d - 1$ or less. Moreover, there is at least one error pattern of weight d which C will not detect.
3. A code C is said to be a t-error-detecting code if it detects all error patterns of weight t or less and it does not detect at least one error pattern of weight $t + 1$.
4. Ex: $C = \{000, 111\}$ detects all error patterns of weight two or less

09/09/20 - Section 1.12

1. A code C corrects the error pattern e if $\forall v \in C$,

$$d(v + e, v) < d(v + e, u), \forall u \in C, u \neq v$$

2. A code of distance d will correct all error patterns of weight $\leq \lfloor \frac{d-1}{2} \rfloor$. Moreover, there exists at least one error pattern of weight $1 + \lfloor \frac{d-1}{2} \rfloor$ which C will not correct.

09/11/20 - Section 1.10

1. $\theta_p(C, v)$ = probability that if v is sent over a BSC of reliablity p, then IMLD will correctly conclude that v was sent.

   To evaluate $\theta_p(C, v)$, we construct the set $L(v)$ which consists of all words in K^n that are closer to v than to any other word in C. It follows that

$$\theta_p(C, v) = \sum_{w \in L(v)} \phi_p(v, w)$$

09/14/20 - Section 1.10

1.