ELG 5372 Error Control Coding

Lecture 9: Decoding of Linear Block Codes and Performance Measures

Université d'Ottawa | University of Ottawa

Error Correction with Hard Decisions

- Error Correction
  - Standard Array
  - Syndrome Decoding

Standard Array

- A standard array is a table of all of the possible n-tuples in V_q^n.
  - None are missing and none are repeated.
- In the top row of the table are all of the codewords in C.
- C forms a subspace of V_q^n.
- In the rows beneath are all of the cosets of C.
- The leftmost column contains the coset leader of each row.
- The coset leader can be thought of as the most likely error pattern that when added to each codeword in the code, will produce all of the vectors in the coset.
- Coset leader is thus the lowest weight element of the coset.
- The coset leader for the code itself is the all 0 codeword (it can be viewed as a codeword and a zero weight error pattern.

Example

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

00000	01011	10110	11101

Example

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

00000	01011	10110	11101
00001	01010	10111	11100

Example

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

00000	01011	10110	11101
00001	01010	10111	11100
00010	01001	10100	11111

Example

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

00000	01011	10110	11101
00001	01010	10111	11100
00010	01001	10100	11111
00100	01111	10010	11001

Example

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

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

Decoding using the standard array

- For a given received word **r**, we find it in the standard array then follow the column up to the top and that is our decoded word.
- Note that this code, with d_{min} = 3 can correct two error patterns of weight two.
- If the error pattern is not among the coset leaders, then a decoding error will occur.
- Example **r** = 00110 will be decoded as 10110.
- Example 2: suppose c = 00000 and e = 10111. This will be decoded as 10110 (decoder will assume that the coset leader is the most likely error pattern).
- Lookup is implemented using a memory device where the address specified by **r** contains the decoder output $\mathbf{c}_{dec}$.

Syndrome Decoding

- $\mathbf{S} = \mathbf{r}\mathbf{H}^T = (\mathbf{c}+\mathbf{e})\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$.
- Let $\mathbf{v}_1$ be a coset leader and $\mathbf{v}_2$ be in $\mathbf{v}_1$'s coset. Then if $\mathbf{e} = \mathbf{v}_1$, $\mathbf{S} = \mathbf{v}_1\mathbf{H}^T$.
- If $\mathbf{e} = \mathbf{v}_2$, then $\mathbf{S} = \mathbf{v}_2\mathbf{H}^T = (\mathbf{v}_1+\mathbf{c})\mathbf{H}^T = \mathbf{v}_1\mathbf{H}^T$.
- If $\mathbf{v}_1$ is coset leader, it has lower weight than $\mathbf{v}_2$, therefore it is more likely to occur.
- Decoding algorithm:
  - Compute $\mathbf{S} = \mathbf{r}\mathbf{H}^T$.
  - For a given $\mathbf{S}$, there is a most likely $\mathbf{e}_s$.
  - Compute $\mathbf{c}_{dec} = \mathbf{r}-\mathbf{e}_s$.

Example

- In our previous example,

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

Example: Syndromes ($\mathbf{S=rH}^T$)

row0	00000	01011	10110	11101	000
row1	00001	01010	10111	11100	001
row2	00010	01001	10100	11111	010
row3	00100	01111	10010	11001	100
row4	01000	00011	11110	10101	011
row5	10000	11011	00110	01101	110
row6	01100	00111	11010	10001	111
row7	11000	10011	01110	00101	101

Example

S	e
000	00000
001	00001
010	00010
100	00100
011	01000
110	10000
111	01100 or 10001
101	11000 or 00101

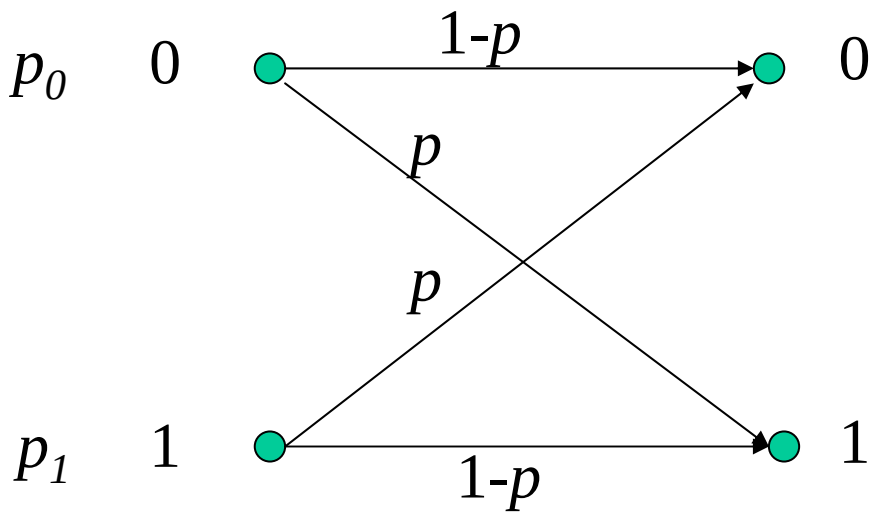
Performance of Linear Block Codes

- $P(E)$ is the probability of decoder error (Word error rate – WER)
  - This is the probability that the codeword at the output of the decoder is not the same as the transmitted codeword.
- P_b is the probability of bit error.
  - Probability that the decoded message bits are not the same as the original message bits.
- $P_u(E)$ is the probability of undetected error.
  - Probability that errors occurring in a codeword are not detected.
- $P_d(E)$ is the probability of detected codeword error.

Performance of Linear Block Codes (2)

- P_{ub} is the probability of message bit error in an undetected codeword error.
- P_{db} is the probability of message bit error in a codeword with a detected error.
- $P(F)$ is the probability of decoder failure. This is the probability that a decoder cannot decode the received vector (it is able to determine that it cannot decode).

Binary Symmetric Channel BSC



The channel is memoryless. In other words, events occurring in one signaling interval do not affect events occurring in the following signaling intervals.

Error Detection Performance

- **r** = **c**+**e**.
- **S** = **r**$\mathbf{H}^T$
- An error is detected if **S** ≠ **0**.
- Therefore an error is undetected if the error pattern **e** is equal to a codeword.
- For the BSC, $P_u(E)$ is given by:

$$P_u(E) = \sum_{i=d_{\min}}^{n} A_i \, p^i (1-p)^{n-i}$$

- Where A_i is the number of codewords of weight I in code C.

Error Detection Performance 2

- The probability of detected error is the probability that the error pattern has weight > 0 and that the error does not go undetected.
  - therefore

$$P_d(E) = 1 - (1-p)^n - P_u(E)$$

Examples

- Suppose p =0.1.
  - For Hamming (7,4), $P_u(E) = 7p^3(1-p)^4+7p^4(1-p)^3+p^7$.
  - Then $P_u(E)$ = 0.0051 or 0.51%.
  - For the (5,2) code given at beginning of lecture, $P_u(E) = 2p^3(1-p)^2+p^4(1-p)$ = 0.0017 = 0.17%.
  - Is this a fair comparison?
- For these two examples, the probability of detected error would be:
  - Hamming (7,4), $P_d(E) = 1-(1-p)^7-P_u(E)$ = 0.5166
  - (5,2) code $P_d(E) = 1-(1-p)^5-P_u(E)$ = 0.4078

Weight Distribution of the Code

- The weight distribution of a code tells us how many codewords there are in the code of weight *i*.
- It is usually expressed as a polynomial.

$$A(x) = 1 + A_{d_{\min}} x^{d_{\min}} + A_{d_{\min}+1} x^{d_{\min}+1} + \ldots + A_n x^n$$

$$= \sum_{i=0}^{n} A_i x^i$$

- Where A_i is the number of codewords of weight *i*.
- For a linear block code $A_0 = 1$ and for any code $A_n = 0$ or 1.

Bounds on $P_u(E)$ and $P_d(E)$

- Calculation of $P_u(E)$ and $P_d(E)$ requires that we know the weight distribution of the code.
- For long block codes, the weight distribution is not always known.
- However, we do know that for error detection, all error patterns of weight d_{min}-1 and less can be detected.
- Although most error patterns of weight d_{min} and more can be detected, we do not know how many. Therefore

$$P_u(E) \le \sum_{i=d_{\min}}^{n} \binom{n}{i} p^i (1-p)^{n-i} = 1 - \sum_{i=0}^{d_{\min}-1} \binom{n}{i} p^i (1-p)^{n-i}$$

$$P_d(E) \ge 1 - (1-p)^n - \sum_{i=d_{\min}}^{n} \binom{n}{i} p^i (1-p)^{n-i} = \sum_{i=1}^{d_{\min}-1} \binom{n}{i} p^i (1-p)^{n-i}$$

Comparing bounds to actual values for our examples

- If we apply the bounds of the previous slide to our examples of Hamming (7,4) and the (5,2) code with $p = 0.1$, then we find:
  - Hamming (7,4): $P_u(E) \leq 1-(1-p)^7-7p(1-p)^6 = 0.15$ (actual is 0.0051) and $P_d(E) \geq 7p(1-p)^6 = 0.372$ (actual is 0.5166).
  - Our (5,2) code $P_u(E) \leq 1-(1-p)^5-5p(1-p)^4 = 0.081$ (actual is 0.0017) and $P_d(E) \geq 7p(1-p)^6 = 0.328$ (actual is 0.4078).

Error Correction Performance

- The probability that the decoder produces the incorrect codeword at its output is the probability that the error pattern is not among the correctable error patterns:
  - For example in Hamming (7,4), the decoder can correct all weight 1 error patterns, therefore the probability of decoder error is the probability that the error pattern has weight greater than 1.
  - Thus for Hamming (7,4),

$$P(E) = \sum_{i=2}^{7} \binom{7}{i} p^i (1-p)^{7-i} = 1 - \sum_{i=0}^{1} \binom{7}{i} p^i (1-p)^{7-i}$$

Error Correction Performance

- As another example, for our (5,2) linear block code, the decoder can correct all error patterns of weight 1 and 2 error patterns of weight 2.

$$P(E) = 1 - \left[\sum_{i=0}^{1} \binom{5}{i} p^i (1-p)^{5-i} + 2p^2(1-p)^3 \right]$$

Error correction performance

- For our examples, if $p = 0.1$,
  - Hamming (7,4), $P(E) = 1-0.9^7-7(0.1)(0.9)^6 = 0.15$
  - (5,2) code, $P(E) = 1-0.9^5-5(0.1)(0.9)^4-2(0.1)^2(0.9)^3 = 0.067$.

- In general

$$P(E) \leq 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}$$