MATH 525
Section 3.3: Hamming Codes

October 20, 2020

Motivation

- A block of r bits can be regarded as the binary (or base-2) representation of a decimal integer in the range $[1..2^r - 1]$.
- Each number in the range is uniquely represented by a block of r bits. For example, when $r = 3$, one has $2^r - 1 = 7$ and

decimal	binary representation
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Now let H_3 be the matrix whose rows are the above binary representations. That is,

$$H_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Let $\mathscr{H}_3$ be the linear code with parity-check matrix H_3. The parameters of the code are:

Length $= 7$
Dimension $= 4$
Minimum Distance $= 3$.

Now redo the previous example with $r = 4$. We obtain:

$$H_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Let $\mathscr{H}_4$ be the linear code with parity-check matrix H_4. The parameters of the code are:

Length $= 15$
Dimension $= 11$
Minimum Distance $= 3$.

Definition of Hamming Codes

- It is now not difficult to generalize the previous two examples to any $r \geq 2$. Let H_r be the $2^r - 1 \times r$ matrix whose rows are the r-bit binary representations of the integers $1, 2, \ldots, 2^r - 1$. The rows of H_r are $00\cdots01,\ \ 00\cdots010,\ \ 00\cdots011,\ \ldots,\ \ 11\cdots11$.
- The linear code with parity-check matrix H_r is called a Hamming code and it is denoted by $\mathscr{H}_r$. The parameters of the code are:

  Length $= 2^r - 1$
  Dimension $= 2^r - r - 1$
  Minimum Distance $= 3$.

- Hamming codes are single-error-correcting codes, that is, their error-correcting capability is $t = 1$.
- As an exercise, show that the Hamming code with parameter r (as above) is a perfect code.

Decoding Hamming Codes

- Since Hamming codes are linear codes, they can be decoded using the syndrome decoding array (SDA) (see Section 2.11). However, there is a more efficient method as explained next:
- Suppose the ith coordinate of the sent codeword $\boldsymbol{c}$ is corrupted by channel. Then the received word $\boldsymbol{r}$ is given by

$$\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}_i,$$

  where $\boldsymbol{e}_i$ is the word whose coordinates are all zero, except for the ith coordinate, which is equal to 1.

- Upon receiving $\boldsymbol{r}$, the decoder computes

$$\mathrm{syn}\,\boldsymbol{r} = (\boldsymbol{c} + \boldsymbol{e}_i) \cdot H_r = \boldsymbol{e}_i \cdot H_r = i\text{th row of } H_r,$$

  which in turn is the binary representation of the integer i. In conclusion, converting $\mathrm{syn}\,\boldsymbol{r}$ to decimal yields the error location.

- If no errors occur, then clearly $\mathrm{syn}\,\boldsymbol{r} = \boldsymbol{0}$ and the decoder declares that no error has occurred.