3a. Hamming codes

Coding Technology

Objective

Goal: design a code which can correct any single error.

Motivation: if the channel has good quality, it is enough to have a limited error correcting capability as single errors are the most likely error scenario.

Hamming codes

Hamming codes are capable of correcting any single error.

Hamming codes are perfect codes:

$$n = 2^{n-k} - 1 \quad \Longleftrightarrow \quad \sum_{i=0}^{1} \binom{n}{i} = 2^{n-k}$$

Construction of the $C(n, k)$ Hamming code:

- construct the column vectors of the parity check matrix H such that all column vectors are different and nonzero;
- construct the generator matrix;
- design the "matching gates" for syndrome decoding;
- implement the full scheme.

The $C(7,4)$ Hamming code

$n = 7, k = 4$, so $2^{7-4} - 1 = 7 = n$ holds.

The $C(7, 4)$ Hamming code

$n = 7, k = 4$, so $2^{7-4} - 1 = 7 = n$ holds.

Constructing the parity check matrix:

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

The $C(7,4)$ Hamming code

$n = 7, k = 4$, so $2^{7-4} - 1 = 7 = n$ holds.

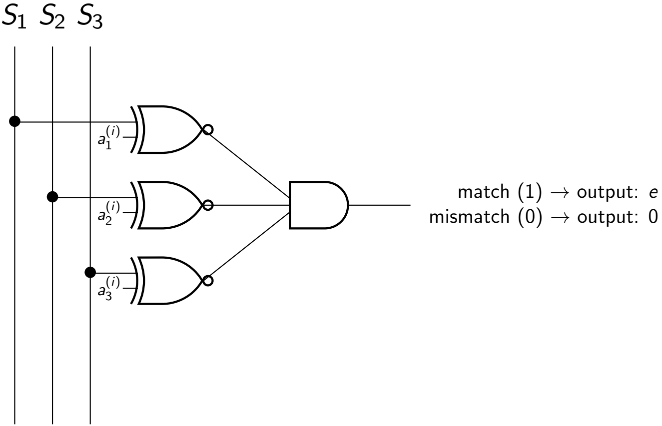
Constructing the parity check matrix:

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

Constructing the generator matrix:

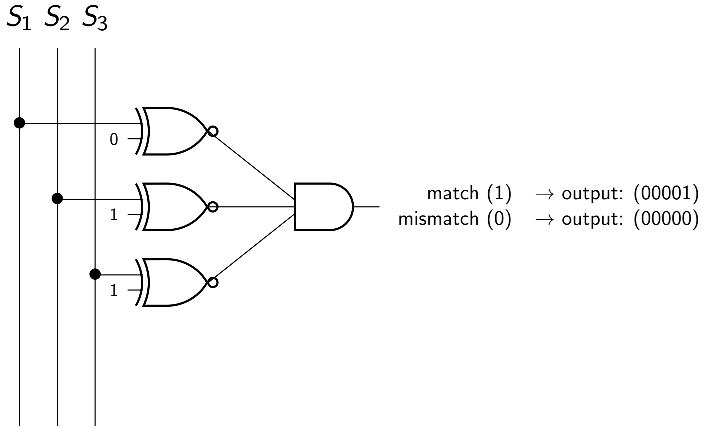
$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Constructing the "Matching System" for decoding



Constructing the "Matching System" for decoding

E.g. $a^{(1)} = (011)$:



Similarly for $a^{(2)} = (101), \ldots, a^{(7)} = (001)$.

Problem 1

A channel has bit error probability $P_b = 0.001$.

(a) We transmit a binary message of length 57 over the channel with no coding. What is the block error probability?

(b) We transmit a binary message of length 57 over the channel using a C(63,57) Hamming code. What is the block error probability?

Problem 1

A channel has bit error probability $P_b = 0.001$.

(a) We transmit a binary message of length 57 over the channel with no coding. What is the block error probability?

(b) We transmit a binary message of length 57 over the channel using a C(63,57) Hamming code. What is the block error probability?

Solution.

(a) With no coding, the message will be received correctly only if all bits are correct, so the probability of correct decoding is

$$(1 - P_b)^{57} \approx 0.9446,$$

and the block error probability is

$$1 - (1 - P_b)^{57} \approx 0.0554.$$

Problem 1

(a) When using a Hamming code, the message will be decoded correctly if there is 0 or 1 errors within the block. Accordingly, the probability of correct decoding is

$$(1-P_b)^{63}+63(1-P_b)^{62}P_b = 0.99^{63}+62\cdot 0.999^{62}\cdot 0.001 \approx 0.99812,$$

and the block error probability is

$$1-(1-P_b)^{63}-63(1-P_b)^{62}P_b \approx 0.00188.$$

Problem 1

(a) When using a Hamming code, the message will be decoded correctly if there is 0 or 1 errors within the block. Accordingly, the probability of correct decoding is

$$(1-P_b)^{63}+63(1-P_b)^{62}P_b = 0.99^{63}+62\cdot 0.999^{62}\cdot 0.001 \approx 0.99812,$$

and the block error probability is

$$1-(1-P_b)^{63}-63(1-P_b)^{62}P_b \approx 0.00188.$$

By using a C(63,57) Hamming code, we reduced the block error probability from 0.0554 to 0.00188, at the cost of decreasing the channel capacity to 57/63 of the original capacity.

Problem 2

(a) A channel has bit error probability $P_b = 0.01$. We transmit a binary message of length 4 over the channel using a C(7,4) Hamming code. What is the block error probability?

(b) A channel has bit error probability P'_b. We transmit a binary message of length 4 over the channel with no coding. Compute the value of P'_b so that the block error probability is the same as in part (a).

Problem 2

(a) A channel has bit error probability $P_b = 0.01$. We transmit a binary message of length 4 over the channel using a C(7,4) Hamming code. What is the block error probability?

(b) A channel has bit error probability P'_b. We transmit a binary message of length 4 over the channel with no coding. Compute the value of P'_b so that the block error probability is the same as in part (a).

Solution.

(a) The block error probability is

$$1 - (1 - P_b)^7 - 7(1 - P_b)^6 P_b \approx 0.00203.$$

Problem 2

(a) A channel has bit error probability $P_b = 0.01$. We transmit a binary message of length 4 over the channel using a C(7,4) Hamming code. What is the block error probability?

(b) A channel has bit error probability P_b'. We transmit a binary message of length 4 over the channel with no coding. Compute the value of P_b' so that the block error probability is the same as in part (a).

Solution.

(a) The block error probability is

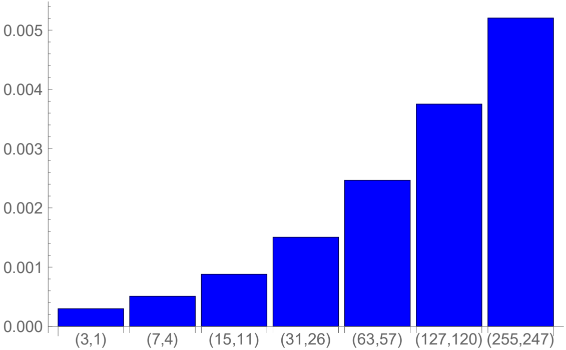
$$1 - (1 - P_b)^7 - 7(1 - P_b)^6 P_b \approx 0.00203.$$

(b) With no coding, the block error probability is

$$1 - (1 - P_b')^4 = 0.00203 \quad \to \quad P_b' \approx 0.000508.$$

Modified bit-error probability

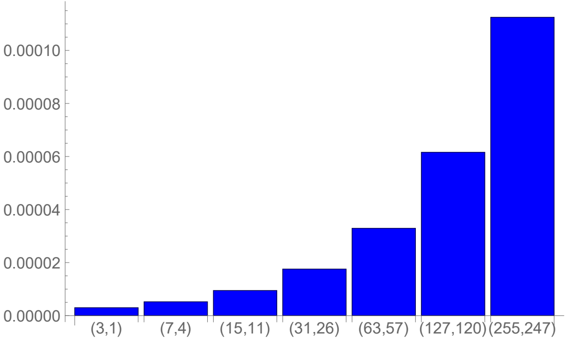
Modified bit-error probability as a function of code parameters for $P_b = 0.01$.



Speed decrease ratios: $1/3; 4/7; 11/15; 57/63; 120/127; 247/255.$

Modified bit-error probability

Modified bit-error probability as a function of code parameters for $P_b = 0.001$.



Speed decrease ratios: $1/3; 4/7; 11/15; 57/63; 120/127; 247/255$.

Code design

Code design from the point of communication engineering.

Problem. Given a BSC with bit-error probability P_b and a desired QoS ε, design a code with $P_b' < \varepsilon$.

Code design

Code design from the point of communication engineering.

Problem. Given a BSC with bit-error probability P_b and a desired QoS ε, design a code with $P_b' < \varepsilon$.

Solution.

(1) Compute k from

$$1 - (1 - P_b')^k = 1 - (1 - P_b)^n - nP_b(1 - P_b)^{n-1}.$$

If $n - k$ is too large or $n > 2^{n-k} - 1$, there is no solution using codes correcting only single errors (so a more powerful code capable of correcting more than a single error is necessary).

Code design

(2) Construct the parity check matrix according to the following rules:

- each column vector is different;
- no column vector is the all-zero vector;
- the code is systematic.

(3) Implement the coding scheme.

Problem 3

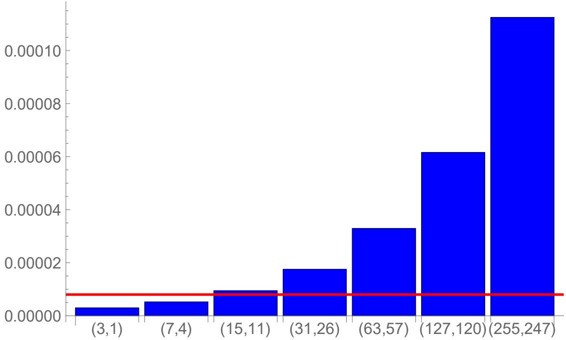
Design an error correcting code for a BSC with $P_b = 0.001$ that achieves $P_b' = 0.000008$.

Problem 3

Design an error correcting code for a BSC with $P_b = 0.001$ that achieves $P_b' = 0.000008$.

Solution.

(1) Identifying the parameters: either $n = 3, k = 1$, or $n = 7, k = 4$ are suitable. Which one should we pick?



Problem 3

(2) Constructing the parity check matrix:

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

Problem 3

(2) Constructing the parity check matrix:

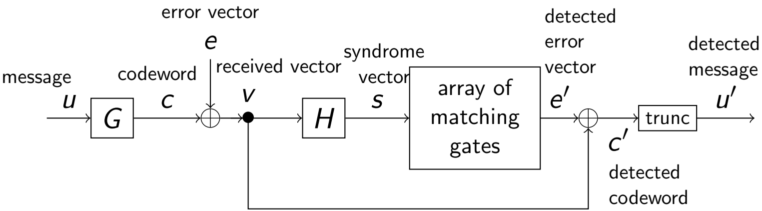
$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Constructing the generator matrix:

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

Problem 3

(3)



error vector
e
message
u
G
codeword
c
received vector
v
H
syndrome
vector
s
array of
matching
gates
detected
error
vector
e'
c'
detected
codeword
trunc
detected
message
u'

Problem 4

A binary linear code has generator matrix

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

Is this a Hamming code?

Problem 4

A binary linear code has generator matrix

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

Is this a Hamming code?

Solution. $n = 5, k = 3$, so this is a $C(5,3)$ code. But

$$n = 5 \neq 2^{n-k} - 1 = 3,$$

so this is not a Hamming code.

Problem 4

A binary linear code has generator matrix

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

Is this a Hamming code?

Solution. $n = 5, k = 3$, so this is a $C(5,3)$ code. But

$$n = 5 \neq 2^{n-k} - 1 = 3,$$

so this is not a Hamming code.

(There is a C(3,1), C(7,4), C(15,11) etc. Hamming code - but no Hamming code in-between!)

Problem 5

For a binary Hamming code with $k = 11$, what is the codeword length n?

Problem 5

For a binary Hamming code with $k = 11$, what is the codeword length n?

From solving

$$n = 2^{n-k} - 1,$$

we get $n = 15$.

Problem 6

A linear binary code has parity check matrix

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

Is this a Hamming code?

Problem 6

A linear binary code has parity check matrix

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

Is this a Hamming code?

Solution. $n = 7, k = 4$, so $n = 2^{n-k} - 1$ holds, but columns 1 and 4 are the same, so this is not a Hamming code.

Problem 7

A systematic binary linear code has parity check matrix

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

(a) What are the parameters of the code?

(b) Is this a Hamming code?

(c) Compute the generator matrix G.

(d) What are the error detecting and correcting capabilities of the code?

(e) Compute the syndrome and error group of the error vector (011).

Problem 7

Solution.

(a) $H = H_{(n-k)\times n}$ is a 2×3 matrix, so $n - k = 2$ and $n = 3$, and this is a C(3,1) code.

Problem 7

Solution.

(a) $H = H_{(n-k)\times n}$ is a 2×3 matrix, so $n - k = 2$ and $n = 3$, and this is a C(3,1) code.

(b) The columns of H are all nonzero binary vectors of length 2, so yes, this is a Hamming code.

Problem 7

Solution.

(a) $H = H_{(n-k)\times n}$ is a 2×3 matrix, so $n - k = 2$ and $n = 3$, and this is a C(3,1) code.

(b) The columns of H are all nonzero binary vectors of length 2, so yes, this is a Hamming code.

(c)

$$H = (B^T, I_{n-k}) = \left[\underbrace{\boxed{\begin{matrix} 1 \\ 1 \end{matrix}}}_{B^T} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}\right].$$

$$G = (I_k, B) = \left[\, 1 \; \underbrace{\boxed{\begin{matrix} 1 & 1 \end{matrix}}}_{B} \right].$$

Problem 7

Solution.

(d) The codewords are

$$(000), \quad (111)$$

so

$$d_{\min} = \min_{c \neq (00\ldots0)} w(c) = 3,$$

and the code can detect $d_{\min} - 1 = 2$ errors and correct $\lfloor (d_{\min} - 1)/2 \rfloor = 1$ error.

Problem 7

Solution.

(d) The codewords are

$$(000), \quad (111)$$

so

$$d_{\min} = \min_{c \neq (00\ldots0)} w(c) = 3,$$

and the code can detect $d_{\min} - 1 = 2$ errors and correct $\lfloor (d_{\min} - 1)/2 \rfloor = 1$ error.

(e) $s^T = He^T = \begin{bmatrix} 110 \\ 101 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$

$E_{(11)} = \{(011), (011) + (111)\} = \{(011), (100)\}$

Problem 8

For a $C(7,4)$ binary systematic Hamming code,

(a) Fill in the missing columns in the parity check matrix:

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

(b) What is the codeword for the message vector (1111)?

Problem 8

Solution.

(a)

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

Problem 8

Solution.

(a)

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

(b)

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

and

$$(1111) \cdot G = (1111111).$$