Exercise 1.2

Show that the error probability is reduced by the use of R_3 by computing the error probability of this code for a binary symmetric channel with noise level f.

Solution:

Without R_3, we have error probability f.
With R_3, we have error probability

$$\binom{3}{2}(1-f)f^2 + f^3 = 3f^2 - 3f^3 + f^3 = 3f^2 - 2f^3$$

Now,

$$\begin{aligned} f - (3f^2 - 2f^3) &= f - 3f^2 + 2f^3 \\ &= f(1-2f)(1-f) > 0 \quad (\because f < \frac{1}{2}) \end{aligned}$$

so $f > 3f^2 - 2f^3$ hence error probability reduced.

Exercise 1.3

(a) Show that the probability of error of R_N, the repetition code with N repetitions, is

$$p_{\mathrm{b}} = \sum_{n=(N+1)/2}^{N} \binom{N}{n} f^n (1-f)^{N-n}, \tag{1.24}$$

for odd N.

(b) Assuming $f = 0.1$, which of the terms in this sum is the biggest? How much bigger is it than the second-biggest term?

(c) Use Stirling's approximation (p.2) to approximate the $\binom{N}{n}$ in the largest term, and find, approximately, the probability of error of the repetition code with N repetitions.

(d) Assuming $f = 0.1$, find how many repetitions are required to get the probability of error down to 10^{-15}. [Answer: about 60.]

Solution:

(a) If N is odd, error when $\frac{N+1}{2}$ or more bits flipped. Hence,

$$p_b = \sum_{n=(N+1)/2}^{N} \binom{N}{n} f^n (1-f)^{N-n}$$

(b) Let each term a_n.

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{N!n!(N-n)!f^{n+1}(1-f)^{N-n-1}}{(n+1)!(N-n-1)!N!f^n(1-f)^{N-n}} \\ &= \frac{(N-n)f}{(n+1)(1-f)} = \frac{N-n}{9(n+1)}\end{aligned}$$

Now,

$$\begin{aligned}&\frac{N-n}{9(n+1)} > 1 \\ \iff& 10n + 9 < n \\ \iff& n < \frac{N-9}{10} \quad (< \frac{N+1}{2})\end{aligned}$$

so ratio < 1 for all $n \geq \frac{N+1}{2}$, meaning the series is decreasing, hence largest term is when $n = \frac{N+1}{2}$.
Ratio is $\frac{N-\frac{N+1}{2}}{9(\frac{N+1}{2}+1)} = \frac{N-1}{9N+11} \simeq \frac{1}{9}$.
The largest term is approximately 9 times larger than second-largest term.

(c)

$$\binom{N}{n} \approx 2^{NH_2(\frac{n}{N})}$$

Now,

$$\begin{aligned}H_2(\frac{\frac{N+1}{2}}{N}) &= \frac{N+1}{2N}\log_2(\frac{2N}{N+1}) + \frac{N-1}{2N}\log_2(\frac{2N}{N-1}) \\ &\simeq \frac{1}{2}\log_2(2) + \frac{1}{2}\log_2(2) = 1\end{aligned}$$

So,

$$p_b \approx p_B = \binom{N}{\frac{N+1}{2}} f^{\frac{N+1}{2}}(1-f)^{N-\frac{N+1}{2}} \quad \simeq 2^N f^{\frac{N}{2}}(1-f)^{\frac{N}{2}} = \{4f(1-f)\}^{\frac{N}{2}}$$

(d)

$$10^{-15} = \{4f(1-f)\}^{\frac{N}{2}}$$
$$N = 2\frac{-15}{\log_{10} 4 \cdot 0.1 \cdot 0.9} = 67.91 \approx 68$$

or more accrately,

$$\begin{aligned}
\ln \binom{N}{n} &\simeq (N-n)\log_2 \frac{N}{N-n} + n\log_2 \frac{N}{n} - \frac{1}{2}\log_2(2\pi\frac{(N-n)n}{N}) \\
&= NH_2(\frac{n}{N}) - \frac{1}{2}\log(2\pi\frac{(N-n)n}{N}) \\
&\xrightarrow{n\simeq\frac{N}{2}} N - \frac{1}{2}\log_2(\frac{\pi N}{2})
\end{aligned}$$

$$\binom{N}{n} \simeq 2^{N-\frac{1}{2}\log_2(\frac{\pi N}{2})} = \frac{2^N}{\sqrt{\frac{\pi N}{2}}}$$

Then,

$$\begin{aligned}
p_b \approx p_B &\simeq \binom{N}{\frac{N+1}{2}} f^{\frac{N+1}{2}}(1-f)^{\frac{N-1}{2}} \\
&\simeq \frac{2^N}{\sqrt{\frac{\pi N}{2}}} f\{f(1-f)\}^{\frac{N-1}{2}} = \frac{2f}{\sqrt{\frac{\pi N}{2}}} f\{4f(1-f)\}^{\frac{N-1}{2}}
\end{aligned}$$

so

$$10^{-15} = \frac{0.2}{\sqrt{\frac{\pi N}{2}}}\{4 \cdot 0.1 \cdot 0.9\}^{\frac{N-1}{2}}$$
$$\frac{N-1}{2} = \frac{-15 - \log_1 0\frac{0.2}{\sqrt{\frac{\pi N}{2}}}}{\log_1 00.36}$$

Iterate from $\hat{N}_1 = 67.6$

$$\frac{\hat{N}_2 - 1}{2} = 29.95$$
$$\hat{N}_2 = 60.90$$
$$\hat{N}_3 = 61.00$$
$$\hat{N}_3 = 61.00$$

which results in 61.

Exercise 1.4

Prove that this is so ($\mathbf{Ht} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$) by evaluating the 3×4 matrix $\mathbf{HG}^{\mathrm{T}}$

Solution:

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

Exercise 1.5

This exercise and the next three refer to the (7, 4) Hamming code. Decode the received strings:

(a) r = 1101011

(b) r = 0110110

(c) r = 0100111

(d) r = 1111111

Solution:

The following are symdrome, unflipped bit and answer.

(a) $z = 011, r_4, 1100011$

(b) $z = 111, r_3, 0100110$

(c) $z = 001, r_7, 0100110$

(d) $z = 000, \text{None}, 1111111$

Exercise 1.6

(a) Calculate the probability of block error p_B of the (7, 4) Hamming code as a function of the noise level f and show that to leading order it goes as $21f^2$.

(b) Show that to leading order the probability of bit error p_b goes as $9f^2$

Solution:

(a)

$$
\begin{aligned}
p_B &= 1 - \sum_{k=0}^{1} \binom{7}{k} f^k (1-f)^{7-k} \\
&= 1 - (1-f)^7 - 7f(1-f)^6 \\
&= 1 - (1+6f)(1-f)^6 \\
&= 1 - (1+6f)(1-6f+15f^2+O(f^3)) \\
&= 1 - (1-6f+15f^2+6f-36f^2+O(f^3)) \\
&= 21f^2 + O(f^3)
\end{aligned}
$$

(b) Let X = the number of bits flipped in a block after decoding.

$$
\begin{aligned}
E[p_b] &= \frac{1}{7} E[X] \\
&= \frac{1}{7} (3 \binom{7}{2} f^2(1-f)^5 + \sum_{3}^{7} a_k \binom{7}{k} f^k (10f)^{7-k}) \\
&= \frac{3}{7} \times \frac{7 \cdot 6}{2 \cdot 1} f^2(1-f)^5 + O(f^3) \\
&= 9f^2(1-f)^5 \\
&= 9f^2 + O(f^3)
\end{aligned}
$$

Exercise 1.7

Find some noise vectors that give the all-zero syndrome (that is, noise vectors that leave all the parity checks unviolated). How many such noise vectors are there?

Solution:

There are $2^4 = 16$ codewords, so 16 such noise vectors. This is because, by definition, codewords are the only vectors that have the property of $\mathbf{Hn} = 0$. This can be seen from the Venn diagram being uniquely filled if the first 4 bits are determined.

Exercise 1.8

I asserted above that a block decoding error will result whenever two or more bits are flipped in a single block. Show that this is indeed so. [In principle, there might be error patterns that, after decoding, led only to the corruption of the parity bits, with no source bits incorrectly decoded.]

Solution:

Assume there is a block error but no decoding error. That is, the source bit is unchanged but the parity bit is changed. The parity bit is deterministic from the source bit, so if the source bit is the same, the parity bit must also be the same, meaning there would be no block error. This contradicts with the assumption that the code has a block error, so if there is a block error, there must also be a decoding error.

Exercise 1.9

Design an error-correcting code and a decoding algorithm for it, estimate its probability of error, and add it to figure 1.18. [Don't worry if you find it difficult to make a code better than the Hamming code, or if you find it difficult to find a good decoder for your code; that's the point of this exercise.]

Solution:

Similar to how (7, 4) Hamming code was derived, we can draw a 4-circle Venn Diagram to create a (15, 11) code.
The generator matrix would be

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

This is a code with a distance of 3 (correct one bit).

Exercise 1.10

A (7, 4) Hamming code can correct any one error; might there be a (14, 8) code that can correct any two errors? Optional extra: Does the answer to this question depend on whether the code is linear or nonlinear?

Solution:

For any code, the space for the received message must be larger than the space for the transmitted message which we are interested in correctly decoding. Now, the space for which we aim to recover in a two-bit correcting code is, (considering that we must recover the original code (and the noise))

$$2^8(\binom{14}{2} + \binom{14}{1} + \binom{14}{0}) = 2^8(91 + 15 + 1) = 2^8 \cdot 106$$

The space for the received message is

$$2^14 = 2^8 \cdot 64 \; < 2^8 \cdot 106$$

so it is impossible to create a (14, 8) two-bit error correcting code. This is regardless of whether the code is linear or non-linear.

Exercise 1.11

Design an error-correcting code, other than a repetition code, that can correct any two errors in a block of size N.

Solution:

Use the bipartite graph to create (30, 11) code which is two-bit error correcting.

Exercise 1.12

Consider the repetition code R_9. One way of viewing this code is as a concatenation of R_3 with R_3. We first encode the source stream with R_3, then encode the resulting output with R_3. We could call this code 'R_3^2'. This idea motivates an alternative decoding algorithm, in which we decode the bits three at a time using the decoder for R_3; then decode the decoded bits from that first decoder using the decoder for R_3. Evaluate the probability of error for this decoder and compare it with the probability of error for the optimal decoder for R_9. Do the concatenated encoder and decoder for R_2^3 have advantages over those for R_9?

Solution:

Note that the error is introduced at the channel, not the encoder.
Considering the dominant term, the error probability for R_9 is

$$p_b(R_9) \simeq \binom{9}{5} f^5(1-f^4) \simeq 126 f^5$$

The error probability for an error for each block in R_3^2 is

$$p_B \simeq \binom{3}{2} f^2(1-f) \simeq 3f^2$$

and so the error probability for the entire procedure is

$$p_b \simeq \binom{3}{2} p_B^2(1-p_B) \simeq 3(3f^2)^2 = 27f^4$$

This means the R_3^2 code is suboptimal in it's error correcting.
Advantages are that the number of bits that needs to be seen is smaller for

each operation, hence cheaper.
Also, the hardware can be reused which makes the design simpler.