MT361/461/5461 Error Correcting Codes: Preliminary Sheet

Solutions to this sheet will be posted on Moodle on 14th January so you can check your answers. Please do Question 2 by 14th January. You are welcome to ask the lecturer about the questions during an office hour.

1. The purpose of this question is to compare the two communication schemes in Example 1.2. The channel is the binary symmetric channel with cross-over probability p. We shall assume that Alice wants to send Bob the message 'Yes'.

(a) Why is it reasonable to assume that $p < 1/2$?

(b) Suppose that Alice and Bob use *Scheme 1*, so Alice sends 11 down the channel. If Bob receives 01 or 10, he requests retransmission.

(i) Explain why the probability that Bob receives 00 is p^2.

(ii) Let c be the probability that Bob receives either 01 or 10. Find c.

(iii) Let $r \in \mathbf{N}$. Show that the probability that Bob decodes Alice's message as 'No' after r attempts at transmission is $c^{r-1}p^2$.

(iv) Hence show that the probability that Bob decodes Alice's message wrongly is

$$\frac{p^2}{1-2p(1-p)}.$$

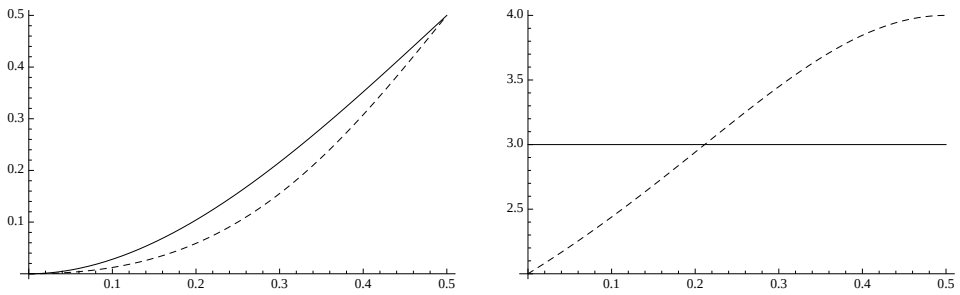
(v) Let b be the average total number of bits that Alice sends to Bob in Scheme 1. Explain why $b = 2(1-c) + (2+b)c$. Hence show that

$$b = \frac{2}{1-2p(1-p)}.$$

(c) Using *Scheme 2*, the probability that Bob decodes Alice's message wrongly was found to be $3p^2 - 2p^3$. How many bits does Alice send to Bob when this scheme is used?

(d) Compare the relative merits of Schemes 1 and 2 when $p = 0.1$ and $p = 0.25$. Why might Scheme 2 be used even when $p = 0.1$?

To confirm your answers in (d) you can use the graphs below which show the probability of incorrect decoding, and the average number of bits sent, for p between 0 and 1/2. The dashed line shows Scheme 1, the solid line shows Scheme 2.



2. Let $\mathbf{Z}_2$ denote the alphabet of binary digits $\{0, 1\}$ with addition modulo 2. So

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0.$$

The *square code* is the binary code of length 8 with codewords

$$\big\{(u_1, u_2, u_3, u_4, u_1 + u_2, u_3 + u_4, u_1 + u_3, u_2 + u_4) : u_1, u_2, u_3, u_4 \in \mathbf{Z}_2\big\}.$$

The name comes from the representation of the codewords as a square of four message bits, (u_1, u_2, u_3, u_4), surrounded by four check bits.

u_1	u_2	$u_1 + u_2$
u_3	u_4	$u_3 + u_4$
$u_1 + u_3$	$u_2 + u_4$	

In general, a received word $(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8)$ may usefully be represented by the square diagram

v_1	v_2	v_5
v_3	v_4	v_6
v_7	v_8	

(a) Show that 11000011 is a codeword in the square code. Draw it as a square diagram.

(b) Suppose that Alice sends 11000011 down a noisy channel, and Bob receives 01000011, which he represents by the square

0	1	0
0	0	0
1	1	

(i) Explain why Bob knows that an error has occurred in the channel.

(ii) Suppose Bob assumes that exactly one error has occurred. Explain how he can work out that Alice sent 11000011.

(c) Assume that the channel behaves as in Question 1. For each of the received words 00100110, 01001100 and 01101110, decide which codeword you think Alice is most likely to have sent.

(d) Write down the length, size and rate of the square code.

MT361/461/5461 Error Correcting Codes: Sheet 1

Hand in your answers to Questions 2, 3, 4 and 5.

If you are an MSc or MSci student please also do Question 6. All other questions are optional for everyone. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 11am on Thursday 24th January or handed in at the Thursday lecture.

1. Find all words $v \in \{0,1\}^5$ such that $d(v, 11011) = 3$.

2. Let C be the binary code with codewords 001, 010, 100 and 111.

(a) What are the length and size of C?

(b) Draw a diagram showing $\{0,1\}^3$ making it clear which words lie in C. (For one way to draw $\{0,1\}^3$, see page 6 of the lecture notes.)

(c) Explain why if a single error occurs when a codeword in C is sent, the receiver will know that something has gone wrong.

(d) What is the probability that when $001 \in C$ is sent on a binary symmetric channel with cross-over probability p, a different codeword $u' \in C$ is received?

3. Let C be the code below

$$00000, \quad 11100, \quad 00111, \quad 11011.$$

(a) Decode the received words 00111, 10111 and 11111 using nearest neighbour decoding.

(b) Give two examples to show that if two errors occur in the channel then nearest neighbour decoding may (i) not give the sent word; (ii) fail. [*Hint:* 'fail' has a technical meaning: see Definition 2.5.]

4. Let $q \in \mathbf{N}$ with $q \geq 2$ and let A be the q-ary alphabet $\{0, 1, \ldots, q-1\}$.

(a) By analogy with Definition 1.6, define a *q-ary symmetric channel* in which the probability that a sent symbol is incorrectly received is p. (Be careful!)

(b) Draw a diagram like the one on page 7 for the ternary case $q = 3$.

5. (a) Using the Square Code find an eight question strategy for the Liar Game (see the second exercise on page 8), in which you can write down, in advance, the eight questions you will ask during the game.

[*Hint: in Lecture 4 we turned a nine question strategy for the Liar Game into a codes of length 9 and size 16. You need to reverse this process.*]

Please state your questions so that are intelligible to someone who knows nothing about the Square Code.

(b) Give an example of a game where Alice lies exactly once, showing how you deduce her number from her answers to your questions.

6. Suppose that C is a binary code of length 5 such that $d(u, u') \geq 3$ for all distinct codewords u, $u' \in C$. Show that C has size at most 4.

7. The purpose of this question is to give a more algebraic proof of the triangle inequality for Hamming distance (proved in lectures in Theorem 2.3). Let A be an alphabet and let u, v, w be words over A of length n.

(a) Let $i \in \{1, 2, \ldots, n\}$. Thinking of u_i, v_i, w_i as words of length 1, prove that

$$d(u_i, w_i) \leq d(u_i, v_i) + d(v_i, w_i).$$

(b) Deduce the triangle inequality by summing the inequality in (a) over all i.

8. I have an important decision 'Yes' or 'No' that I wish to communicate to a friend across a crowded room. I can shout to him up to three times. The probability that he mishears on the first shout is p, and on the second and third it is $r > p$. Assume that $r < 1/2$.

(a) Explain a three shout strategy, making it clear how my friend will decode what he hears.

(b) Calculate the probability that the three shout strategy will successfully communicate the message.

(c) If $p = 1/5$ show that the three shout strategy is superior to a single shout if and only if $r < 1/3$.

(d) ($\star$) Show more generally that there is a function $f : [0, 1/2] \to [0, 1/2]$ such that three shouts are superior to a single shout if and only if $r < f(p)$. Sketch the graph of f.

9. In Lewis Carroll's 'Doublets Game', the aim is to turn one word into another, changing one letter at a time, while staying within the English language.

(a) Show that $d(\mathrm{WARM}, \mathrm{COLD}) = 4$ and find a solution to the Doublet puzzle starting at WARM and ending at COLD using just 3 intermediate words.

(b) Find $r \in \mathbf{N}$ and English words u and w such that $d(u, w) = r$ but there is no r-step solution to the Doublet puzzle.

(c) Suggest an efficient algorithm for solving Doublet puzzles.

10. Do there exist binary words u, v, w of the same length such that $d(u, v) = 3$, $d(v, w) = 4$ and $d(w, u) = 6$? Now answer the same question for words over the ternary alphabet $\{0, 1, 2\}$.

11. Consider the binary code $C = \{00, 01\}$ of length 2. Show that, if we take a **wrong** version of Definition 3.1 in which $d(u, v) = t$, rather than $d(u, v) \leq t$, then C would be 2-error detecting but not 1-error detecting.

MT361/461/5461 Error Correcting Codes: Sheet 2

Hand in your answers to Questions 1, 2, 3, 4 and 6.

If you are an MSc or MSci student please also do Question 10. All other questions are optional for everyone. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 11am on Thursday 31st January or handed in at the Thursday lecture.

1. Let C be a code such that $d(u, u') \geq 3$ for all u, $u' \in C$ with $u \neq u'$. Arguing directly from Definition 3.1,

(a) Show that C is 2-error detecting;

(b) Show that C is 1-error correcting.

[*Hint:* your argument should use only the given hypothesis on C: do not assume that C is any particular code. Also please do not use Theorem 4.5.]

2. Let A be a q-ary alphabet where $q \geq 2$. Let $m \in \mathbf{N}$ and let C be the repetition code of length $2m$ over A. Prove Lemma 3.3(iii), that C is $(m-1)$-error correcting, but not m-error correcting.

3. Let C be the binary code of length 9 seen in Lecture 4 whose codewords are all binary words of the form

$$(u_1, u_2, u_3, u_4, u_1, u_2, u_3, u_4, e)$$

where e is chosen to make the total number of 1s in (u_1, u_2, u_3, u_4, e) even.

(a) Find codewords $u, w, u', w' \in C$ such that $d(u, w) = 3$ and $d(u', w') = 4$.

(b) Let

$$u = (u_1, u_2, u_3, u_4, u_1, u_2, u_3, u_4, x)$$
$$v = (v_1, v_2, v_3, v_4, v_1, v_2, v_3, v_4, y)$$

be codewords in C.

(i) Show that if $d(u_1u_2u_3u_4, v_1v_2v_3v_4) = 1$ then $d(u, v) = 3$.

(ii) Show that if $d(u_1u_2u_3u_4, v_1v_2v_3v_4) \geq 2$ then $d(u, v) \geq 4$.

(iii) Hence find the minimum distance of C.

(c) Deduce that C is 2-error detecting and 1-error correcting. [*You may use Question 1, or Theorem 4.5.*]

4. Let C be the ternary repetition code of length 6 considered in Example 2.6. Given $v \in \{0, 1, 2\}^6$ define the *distance of v from C* to be the minimum of $d(v, u)$ for $u \in C$. What is the maximum possible distance of a word v from C?

5. (a) Which of the following are ISBNs:

1-84628-040-0, 1-84628-400-0, 0-486-68735-X?

(b) Show that if two unequal adjacent symbols are interchanged when writing down an ISBN then the result is not an ISBN.

6. Let C be a t-error correcting code over the alphabet A. Suppose that you receive the word $v \in A^n$ and, after some hunting through the code, you find a codeword $u \in C$ such that $d(u, v) \leq t$. Show that if u is not the sent codeword then at least $t + 1$ errors have occurred in the channel.

7. Let C be the length 12 binary code

$$C = \{u_1u_2u_3u_4\, u_1u_2u_3u_4\, u_1u_2u_3u_4 : u_1, u_2, u_3, u_4 \in \{0, 1\}\}.$$

Show that no matter how many errors occur in the channel, there is always a unique nearest codeword to any received word. (So nearest neighbour decoding never fails for C: of course it might give the wrong answer.)

8. Let $p < 1/2$. A jury consists of three people. Two of them get the verdict wrong with probability p, while the third flips a coin to decide. What is the probability that the majority verdict of the jury is correct? Comment on your answer.

9. Suppose that Alice wishes to send a message 'Yes' or 'No' to Bo through the binary symmetric channel with crossover probability p. She sends 'Yes' with probability 3/4 and 'No' with probability 1/4. They agree to use the length 3 binary repetition code, encoding 'Yes' as 111 and 'No' as 000.

(a) Find $\mathbf{P}[001 \text{ received} \mid 000 \text{ sent}]$ and $\mathbf{P}[001 \text{ received} \mid 111 \text{ sent}]$.

(b) Hence find $\mathbf{P}[000 \text{ sent} \mid 001 \text{ received}]$.

(c) Find $\mathbf{P}[111 \text{ sent} \mid 001 \text{ received}]$.

(d) Show that if $p > 1/4$ then

$$\mathbf{P}[111 \text{ sent} \mid 001 \text{ received}] > \mathbf{P}[000 \text{ sent} \mid 001 \text{ received}].$$

and comment on the implications for nearest neighbour decoding.

10. (**MSc/MSci**) Let C be the Reed–Solomon code with alphabet $\mathbf{F}_5$ defined in Example 2.2(2) of the MSc lecture notes.

(a) Show that C is a vector subspace of $\mathbf{F}_5^4$ and find a basis for C. What is $\dim C$?

(b) Suppose that the word $v = 1312$ is received. Show that $v \notin C$ and decode v using nearest neighbour decoding.

(c) Show that if $u \in C$ is sent down a noisy channel, and v is received such that $d(u, v) \leq 2$, then either $v = u$ or $v \notin C$. What is the maximum t such that C is t-error detecting?

MT361/461/5461 Error Correcting Codes: Sheet 3

Hand in your answers to Questions 2, 3, 4 and 5.

If you are an MSc or MSci student please also do Questions 8 and 9. All other questions are optional for everyone. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 11am on Thursday 7th February 2012 or handed in at the Thursday lecture.

1. Let C be the binary code defined by

$$C = \{u_1u_2u_3u_4\, u_1u_2u_3u_4\, u_1u_2u_3u_4 : u_1, u_2, u_3, u_4 \in \{0, 1\}\}.$$

Find the length, size, rate and minimum distance of C. How many errors can C detect and correct? (**Optional but instructive:** find a code of the same length and minimum distance of C and strictly greater size.)

2. As in Example 2.10, define an *ISBN* to be any word u of length 10 over the alphabet $\{0, 1, \ldots, 9, \mathrm{X}\}$, where X stands for 10, such that the *check sum* $\sum_{j=1}^{10}(11-j)u_j$ is divisible by 11.

(a) Suppose that u is an ISBN and that when written down, a mistake is made in position k, so the 'received' word is

$$v = u_1u_2 \ldots u_{k-1}\, s\, u_{k+1} \ldots u_{10}$$

where $s \in \{0, 1, 2, 3, \ldots, 9, \mathrm{X}\}$ and $s \neq u_k$. Compute the difference between the check sums for u and v. Hence show that v is not an ISBN.

[*Hint:* if $r, s \in \mathbf{Z}$ are not divisible by a prime p then neither is rs.]

(b) Explain, with reference to Definition 3.1, why the ISBN code is 1-error detecting.

(c) Give examples to show that the ISBN code is not 2-error detecting or 1-error correcting.

3. Let C be the code over the ternary alphabet $\{0, 1, 2\}$ with codewords

$$0000 \quad 0111 \quad 0222 \quad 1012 \quad 1120 \quad 1201 \quad 2021 \quad 2102 \quad 2210.$$

(a) Decode the received words 1201, 2121, 2222 using nearest neighbour decoding. In each case, write down how many errors must have occurred in the channel if your answer is not the sent word.

(b) Write down the words in $B_1(0000)$. How would these words be decoded using nearest neighbour decoding?

(c) What is the size of $B_2(0000)$?

4. Let u and w be binary words of length n.

(a) Thinking of u_i and w_i as words of length 1, explain why

$$d(u, w) = \sum_{i=1}^{n} d(u_i, w_i)$$

is true.

(b) Let $1 \leq k \leq n$ and let u' and w' be the binary words obtained by flipping the bits in position k of u and w, respectively. Show that $d(u, w) = d(u', w')$.

(c) Let $1 \leq j \leq k \leq n$, let u' be the word obtained by swapping the bits in positions i and j of u, and let w' be the word obtained by swapping the bits in positions i and j of w. Show that $d(u, w) = d(u', w')$.

(d) Give an example to illustrate either (b) or (c).

5. Let C a binary code. For each codeword $u = u_1 u_2 \dots u_n \in C$, let $D(u)$ be the word of length $2n$ defined by

$$D(u) = u_1 u_2 \dots u_n u_1 u_2 \dots u_n.$$

Let $D(C) = \{D(u) : u \in C\}$. Prove that if C is an (n, M, d)-code then $D(C)$ is a $(2n, M, 2d)$-code.

[*Hint: please do not assume that C is a repetition code, or any other special type of code. The only thing you may assume about C is that it is a binary code with parameters (n, M, d).*]

6. Alice knows a polynomial f with coefficients in the natural numbers, of unknown degree. Bob can pick any number $x \in \mathbf{Z}$ and ask Alice to tell him $f(x)$. After hearing Alice's answer, Bob may then pick $y \in \mathbf{Z}$ and ask for $f(y)$, and so on. Find a strategy for Bob that will determine f in as few questions as possible.

7. Show that the maximum size of a ternary 1-error correcting code of length 4 is 9.

8. (**MSc/MSci**) Let C be the Reed–Solomon code with parameters $p = 7$, $n = 5$, $k = 3$ where polynomials are evaluated at $0, 1, 2, 3, 4 \in \mathbf{F}_7$.

(a) Using polynomial interpolation, or otherwise, find a codeword $u \in C$ such that the first three positions of u are $(1, 0, 4)$.

(b) Suppose that the word $v = (1, 4, 1, 1, 2)$ is received. Explain why there is at most one codeword within distance 1 of v. Find such a codeword.

9. (**MSc/MSci**) Prof. X is heard to say 'I really can't see the point of using Reed–Solomon codes over the finite field $\mathbf{F}_{2^8}$. Since 257 is prime we could just as well work in $\mathbf{F}_{257}$ and all the operations would be easier because no field theory is required: we just work modulo 257.' Criticize Prof. X's argument.

MT361/461/5461 Error Correcting Codes: Sheet 4

Hand in your answers to Questions 1, 2 and 3(a), (b).

If you are an MSc or MSci student please also do Questions 4 and 5. All other questions are optional for everyone. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 11am on Thursday 14th February 2012 or handed in at the Thursday lecture.

1. Consider the five binary codes below:

$$C_1 = \{0000, 1100, 1010, 0110\}$$
$$C_2 = \{0111, 0100, 0010, 0001\}$$
$$C_3 = \{1000, 0100, 0010, 0001\}$$
$$C_4 = \{0000, 1100, 0110, 0011\}$$
$$C_5 = \{0110, 1100, 1001, 0011\}.$$

(a) Show that C_1 is equivalent to C_2.

(b) Show that C_1 is not equivalent to C_3. Is C_2 equivalent to C_3?

(c) Show that C_4 and C_5 are not equivalent. Is either equivalent to C_1, C_2 or C_3?

(d) (**Optional**) Classify all binary codes of length 4, size 4 and minimum distance 2, up to equivalence.

2. (a) Use Lemma 6.6 to show that $A_2(n, d) = 2$ whenever $d > 2n/3$.

(b) By adapting the proof of Lemma 6.5, and using Lemma 6.6 in your version of Step (2), show that $A_2(8, 5) \leq 4$.

(c) Hence prove Theorem 6.7, that $A_2(8, 5) = 4$.

3. A binary code C of length n is said to be *perfect* if there exists $e \in \mathbf{N}$ such that

$$\{0, 1\}^n = \bigcup_{u \in C} B_e(u)$$

where the union is disjoint. (In words: the Hamming balls of radius e about codewords are disjoint, and every binary word of length n is in one of these balls.)

(a) Show that if n is odd then the binary repetition code of length n is perfect.

(b) Show that if C is a perfect binary code of length n with $e = 1$ then C is 1-error correcting and $n = 2^m - 1$ for some $m \in \mathbf{N}$. Express $|C|$ in terms of m. [*You may use any general results proved earlier in the course.*]

(c) (**Optional**) Show that any perfect binary code has odd minimum distance.

4. (**MSc, MSci**) Consider the Reed–Solomon code $RS_{5,4,2}$ over $\mathbf{F}_5$ where polynomials are evaluated at $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 3$. Suppose that you receive the words

$$\text{(i) } 2413, \quad \text{(ii) } 1033, \quad \text{(iii) } 1032.$$

In each case find a solution to the Key Equation for $Q(x)$ and $E(x)$ and decode, where possible, the received word.

5. Read the introduction, Section 6, and at least one other section from Hamming's original paper, *Error Detecting and Error Correcting Codes*, Bell Systems Technical Journal, **2** (1950) 147–160. (See `http://www.lee.eng.uerj.br/~gil/redesII/hamming.pdf`.)

Think critically about how Hamming writes and identify at least two strengths or weaknesses of his paper.

6. Let $n, d \in \mathbf{N}$ where $n \geq d$. Let C be a code of length $n+1$ and minimum distance $d+1$.

(a) Suppose that two codewords at distance $d+1$ in C differ in position i. Show that the code $C^\star$ of length n obtained by removing position i from all codewords in C has minimum distance d.

(b) Deduce that $A_q(n+1, d+1) \leq A_q(n, d)$ for any $q \geq 2$.

7. Let $n, d \in \mathbf{N}$ where $n \geq d$. Suppose that C is a binary code of length n and minimum distance d. Define a new code C^+ of length $n+1$ by appending a final bit to each codeword in C so that each codeword in C^+ has an even number of 1s.

(a) Show that the distance between any two codewords in C^+ is even.

(b) Use the previous question to show that if d is odd then

$$A_2(n, d) = A_2(n+1, d+1).$$

8. Let $q \geq 2$ and let A be a q-ary alphabet.

(a) Show that if $u \in A^n$ then the number of words in the Hamming ball of radius t about u is

$$\sum_{k=0}^{t} \binom{n}{k} (q-1)^k.$$

(b) Hence generalize Theorem 5.4 by showing that if C is a q-ary (n, M, d)-code then

$$M \leq q^n \Big/ \sum_{k=0}^{e} \binom{n}{k} (q-1)^k$$

where $e = \lfloor (n-1)/2 \rfloor$.

MT361/461/5461 Error Correcting Codes: Sheet 5

Hand in your answers to Questions 1, 2 and 3.

If you are an MSc or MSci student please also do Question 5. All other questions are optional for everyone. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 11am on Thursday 21st February 2013 or handed in at the Thursday lecture.

1. Suppose that C is a $(4, q^2, 3)$-code over the alphabet $A = \{0, 1, \ldots, q-1\}$.

(a) Show that if $u = (u_1, u_2, u_3, u_4)$ and $u' = (u'_1, u'_2, u'_3, u'_4) \in C$ are distinct codewords then $(u_1, u_2) \neq (u'_1, u'_2)$.

(b) Deduce that for all i, $j \in A$ there is a unique codeword, say (i, j, X_{ij}, Y_{ij}), whose first two positions are (i, j). [*Hint: C has size q^2.*]

(c) By (b) we have
$$C = \{(i, j, X_{ij}, Y_{ij}) : i, j \in A\}.$$

(i) Prove that the rows of the matrix X have distinct entries. [*Hint: suppose row i has a repeated entry, so $X_{ij} = X_{ij'}$ where $j \neq j'$. What does this imply about the codewords whose first two positions are (i, j) and (i, j')?*]

(ii) Prove that the columns of X have distinct entries.

(iii) Deduce that X is a Latin square.

(iv) Prove that X and Y are MOLs.

2. Let C be the ternary code with codewords $000, 111, 222, 012, 021, 120, 102, 201, 210$. Let $C^\star$ be the code obtained from C by puncturing it in its final position. Write down the codewords in $C^\star$ and find the length, size, and minimum distance of $C^\star$.

3. Let $q \geq 2$ and let $A = \{0, 1, \ldots, q-1\}$. Suppose that C is a q-ary code of length $n \geq 2$ and minimum distance $n - 1$.

(a) Show that if $u = u_1 u_2 \ldots u_n$ and $v = v_1 v_2 \ldots v_n$ are distinct codewords in C then
$$d(u_1 u_2, v_1 v_2) \geq 1.$$

(b) By putting codewords into pigeonholes according to their first two symbols, show that $|C| \leq q^2$.

(c) Deduce that $A_q(n, n-1) \leq q^2$. (This is a special case of the Singleton bound. The case $n = 4$ shows that codes constructed from mutually orthogonal Latin squares are as large as possible.)

4. What does it mean to say that a binary code is an (n, M, d)-code?

For which of the following parameters either give a binary code with these parameters, or show that no such code can exist:

(i) $(5, 2, 5)$; (ii) $(5, 3, 4)$; (iii) $(5, 4, 3)$; (iv) $(5, 16, 2)$.

5. (**MSc/MSci**) Let p be a prime and let $n \leq p$.

(a) Show that the repetition code of length n over $\mathbf{F}_p$ is a Reed–Solomon code.

(b) Show that the code consisting of all words over $\mathbf{F}_p$ of length n is a Reed–Solomon code.

6. (**MSc/MSci**) Is it possible for the Key Equation method for decoding Reed–Solomon codes to fail because the Key Equation has no solutions?

7. By generalizing the steps in Question 3, give an alternative proof of the Singleton bound $A_q(n, d) \leq q^{n-d+1}$.

8. (For people who know some basic group theory.) Let G be a finite group of order n with group operation $\circ$. Suppose that $G = \{g_1, g_2, \ldots, g_n\}$. Show that the matrix X defined by $X_{ij} = g_i \circ g_j$ is a Latin square over the alphabet G.

9. The Grand-Vizier and his fifty servants are planning a banquet. Owing to an administrative error, one of the 1000 barrels of wine in his wine-cellar been poisoned with a deadly but slow-acting poison: anyone who drinks from the poisoned barrel will die at a random time in the next day.

(a) Devise a tasting strategy that will identify the poisoned barrel within one day.

(b) One of the Vizier's servants has been replaced with an assassin who is immune to all poisons. Propose a new tasting strategy.

MT361/461/5461 Error Correcting Codes: Sheet 6

Hand in your answers to Questions 1 and 2.

If you are an MSc or MSci student please also do Question 4. All other questions are optional for everyone. Question 3 gives some extra practice on MOLS. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 11am on Thursday 28th February 2013 or handed in at the Thursday lecture.

1. Let X, Y, Z be the Latin squares shown below

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \qquad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{array} \qquad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{array}$$

You may assume that any two of X, Y, Z are a pair of MOLS.

(a) By generalizing the construction in Theorem 7.7, write down the codewords in a code C of length 5 and size 16 over the alphabet $\{0, 1, 2, 3\}$.

(b) Show that if $u, w \in C$ agree in (at least) two positions then $u = w$. [*Hint: puncture and then apply Theorem 7.7 '$\Longrightarrow$'*]

(c) Hence find the minimum distance of C.

2. (a) Let H be a Hadamard matrix of order n. Show that the $2n \times 2n$ matrix

$$K = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

is a Hadamard matrix of order $2n$.

(b) Starting from the 2×2 Hadamard matrix

$$\begin{pmatrix} + & + \\ + & - \end{pmatrix}$$

use (a) to construct Hadamard matrices with orders 4 and 8. Hence write down the codewords in (i) a binary $(4, 8, 2)$ code and (ii) a binary $(8, 16, 4)$-code.

(c) Use nearest neighbour decoding to decode (where possible) the received words 01010111, 10011110 and 11000000 sent using the code in (b)(ii).

(d) Use (b)(ii) to show that there is a binary $(7, 16, 3)$-code. Deduce from the Hamming Packing Bound that $A_2(7, 3) = 16$.

(e) Using (b)(ii) and the Plotkin bound, prove that $A_2(7, 4) = 8$.

3. Use the construction in Lemma 7.6 to write down two mutually orthogonal Latin squares of order 3. Hence construct a $(4, 9, 3)$-code over the alphabet $\{0, 1, 2\}$ containing the codeword 0000.

4. (**MSc/MSci**) Explain how an $RS_{p,n,k}$ code can be used with polynomial interpolation to encode p^k different messages so that the codeword encoding $(b_1, b_2, \ldots, b_k) \in \mathbf{F}_p^k$ has $b_1, b_2, \ldots, b_k$ as its first k positions. Illustrate your answer by encoding $(4, 2) \in \mathbf{F}_5^2$ in a $RS_{5,4,2}$ code of your choice.

5. Show that a Hadamard matrix of order ≥ 4 has order divisible by 4. [*Hint: let r, r' and r'' be three rows of H. By reordering columns, assume that r and r' agree in their first $n/2$ positions and differ elsewhere. What does this say about r''?*]

6. The purpose of this question is to give a geometric proof of the Plotkin bound (Theorem 9.6). Let C be a binary (n, M, d)-code where $2d > n$. For each codeword $u \in C$ define an associated vector $x(u) \in \mathbf{R}^n$ by

$$x(u)_i = \begin{cases} 1 & \text{if } u_i = 0, \\ -1 & \text{if } u_i = 1. \end{cases}$$

Let $x \cdot y$ be the usual dot product of vectors $x, y \in \mathbf{R}^n$.

(a) Show that $x(u) \cdot x(u) = n$ for all $u \in C$.

(b) Let $u, u' \in C$ be distinct codewords. Show that $x(u) \cdot x(u') = n - 2d(u, u')$ and deduce that $x(u) \cdot x(u') \leq -(2d - n)$.

(c) Let $z = \sum_{u \in C} x(u)$. By considering $z \cdot z$ prove the Plotkin bound.

(d) Find z if C is a binary $(5, 4, 3)$-code.

7. Let C be a binary (n, M, d)-code where $n \geq 2d$. By putting the codewords in C into pigeonholes according to their final $n - 2d$ positions, and then applying Corollary 9.7 to each code of length $2d$ obtained by repeatedly puncturing the codewords in each pigeonhole, prove the asymptotic Plotkin bound

$$|C| \leq 2^{n-2d+1} n.$$

Compare this bound with the Singleton bound for binary codes.

8. Let p be a prime such that $p \equiv 3 \bmod 4$ and let $\mathbf{F}_p$ be the finite field with p elements. We say that $x \in \mathbf{F}_p$ is a *square* if there exists $y \in \mathbf{F}_p$ such that $x = y^2$.

Let Q be the $p \times p$ matrix Q whose rows and columns are indexed by $i, j \in \{0, 1, \ldots, p-1\}$ and where

$$Q_{ij} = \begin{cases} -1 & \text{if } i - j \text{ is a square in } \mathbf{F}_p \\ 1 & \text{otherwise.} \end{cases}$$

It is known that the matrix H obtained from Q by adding an extra row and an extra column consisting entirely of 1s is a Hadamard matrix of order $p + 1$. Use this to find a Hadamard matrix of order 12.

MT361/461/5461 Error Correcting Codes: Sheet 7

Hand in your answers to Questions 1 and 2.

If you are an MSc or MSci student please also do Question 4. If you an MSc student (or did MT441 Channels) please also do Question 3. All other questions are optional for everyone. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 11am on Thursday 7th March 2013 or handed in at the Thursday lecture.

1. Let C be the square code consisting of all codewords of the form

$$(u_1, u_2, u_3, u_4, u_1 + u_2, u_3 + u_4, u_1 + u_3, u_2 + u_4)$$

where $u_1, u_2, u_3, u_4 \in \mathbf{Z}_2$.

(a) Show that if $u, w \in C$ then $u + w \in C$, and so C is linear.

(b) Suppose we agree to encode the binary number $b_3b_2b_1b_0$ as the codeword starting $(b_3, b_2, b_1, b_0, \ldots)$. Find the codewords encoding 1, 2, 3 and 4.

(c) Find, with proof, a basis for C. [*Hint: one basis consists of exactly three of the codewords from (b), together with one other codeword.*]

(d) Let C_{ext} be the parity check extension of C. Write down a general form for the codewords in C_{ext}. Prove that the minimum distance of C_{ext} is 4. What is the maximum number of errors that C_{ext} can detect and correct? [*You may use Lemma 11.4 and any other general results proved in the course.*]

2. Let $n \in \mathbf{N}$. Given binary words $u = u_1u_2 \ldots u_n$ and $v = v_1v_2 \ldots v_n$ of length n, we write $(u \mid v)$ for the word $u_1u_2 \ldots u_nv_1v_2 \ldots v_n$ of length $2n$. Let $\mathbf{1}$ stand for the all-ones word of length n, i.e. $\mathbf{1} = 11 \ldots 1$.

If C is a linear binary code of length n then we define $E(C)$ to be the code of length $2n$ consisting of all words of the form $(u \mid u)$ and $(u \mid u + \mathbf{1})$ for $u \in C$.

(a) Write down the codewords in $E(\{00, 01, 10, 11\})$. Find the length, size and minimum distance of $E(\{00, 01, 10, 11\})$

Let C be a linear binary code. [*Hint: do not assume C is any particular code!*]

(b) Show that $E(C)$ is linear.

(c) Suppose that $u(1), \ldots, u(k)$ is a basis for C. Show that

$$\big(u(1)|u(1)\big), \ldots \big(u(k)|u(k)\big), \big(\mathbf{0}|\mathbf{1}\big)$$

is a basis for $E(C)$.

(d) Show that $|E(C)| = 2|C|$.

(e) Suppose that C has minimum distance $d \leq n/2$. Show that $E(C)$ has minimum distance $2d$. [*You may either use Lemma 11.4, or argue directly.*]

3. (**MSc/MSci**) Prof. X is heard to issue the following monologue:

> 'I want to communicate using the binary symmetric channel with crossover probability $\frac{1}{5}$. If I use a code of length n, then I can expect that about $\frac{n}{5}$ positions in any sent codeword will be flipped in the channel. So the code I use must be at least $\frac{n}{5}$-error correcting. If C is such a code then $d(C) \geq 2n/5$. By the asymptotic Plotkin bound, the rate of C is at most
> $$\frac{\log(2^{n-2d(C)+1}n)}{n} \approx 1/5.$$
> However the capacity of the channel is $1 - H(\frac{1}{5}) \approx 0.278$, where H is Shannon's entropy function, so by Shannon's Noisy Coding Theorem, I should be able to communicate reliably at a rate of $0.278 > \frac{1}{5}$. Therefore the asymptotic Plotkin bound contradicts Shannon's Noisy Coding Theorem.'

Explain to Prof. X where he has gone wrong.

4. (**MSc/MSci**)

(a) Let $f(x) = 1 + x + x^3$ and let $g(x) = 1 + x^2 + x^3$ be polynomials in $\mathbf{F}_2[x]$ corresponding (as in Definition 4.4) to codewords of length 7 in a cyclic binary code. For example, $f(x)$ corresponds to 1101000. Write down the codewords corresponding to

(i) $g(x)$ (ii) $x^5 f(x)$ (iii) $f(x)g(x)$ (iv) $f(x)g(x)(1+x)$ (v) $f(x)^3$.

(b) Let C be the ternary code of length 6 defined by

$$C = \{(u_0, u_1, u_2, u_3, u_4, u_5) \in \mathbf{F}_3^6 : u_0 + u_2 + u_4 = 0, u_1 + u_3 + u_5 = 0\}.$$

Show that C is cyclic and find a generating polynomial for C.

5. Let C be a linear binary code of length n and let $1 \leq i \leq n$. Show that either all codewords in C have 0 in their ith position, or half of the codewords have 0 in their ith position and half have 1. [*Hint: if u is a codeword with $u_i = 1$, consider the map $C \to C$ defined by $v \mapsto v + u$.*]

6. Suppose that C is a binary code of length n and minimum distance at least δn where $0 < \delta < 1$. Show that if $\delta = 1/2$ then $|C|$ can be arbitrarily large, but if $\delta > 1/2$ then $|C|$ is bounded as n tends to infinity.

7. (a) By generalizing the square code S, define a linear binary $[n^2 + 2n, n^2, 3]$-code for each $n \in \mathbf{N}$. Show that the rate of these codes tends to 1 as $n \to \infty$.

(b) Define a *cube code* by analogy with the square code. By extending these codes, find a family of two-error correcting linear binary codes whose rate tends to 1 as their length tends to infinity.

MT361/461/5461 Error Correcting Codes: Sheet 8

Hand in your answers to Questions 1 and 2.

If you are an MSc or MSci student please also do Questions 4 and 5. All other questions are optional for everyone. The lecturer will be happy to discuss any of the questions in office hours.

To be returned to McCrea 240 by 4pm on Tuesday 19th March 2013 or handed in at the Tuesday lecture. (Note change from the usual Thursday deadline.)

1. Let C be the binary code of length 8 with generator matrix

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

(a) Put G into reduced row-echelon form. (Remember that swapping rows is an admissible row operation.)

(b) Find a code C' and a generator matrix G' for C' such that C' is equivalent to C and G' is in standard form.

(c) Using the generator matrix G', encode 7 as a codeword in C'. Which codeword in C' encodes the number $8b_3 + 4b_2 + 2b_1 + b_0$ where $b_i \in \{0, 1\}$ for each i?

(d) Is C equivalent to the square code by a shuffle of positions?

2. Let $C = \{0000, 1111\}$ be the repetition code of length 4.

(a) Construct a standard array for C.

(b) Use your standard array to decode the received words 0000, 0010, 1010, 0101.

(c) Suppose that 0000 is sent through a noisy channel in which each bit flips independently with probability $p < 1/2$.

(i) Explain why the probability that 0000 is received is $(1-p)^4$.

(ii) Show that the probability that a word of weight 1 is received is $4p(1-p)^3$.

(iii) Which words of weight 2 will be decoded to 0000 using your standard array? Find the probability that one of these words is received.

(iv) Hence find the probability that the receiver decodes the received word as 0000. Evaluate this probability when $p = 1/5$.

3. Let C be a linear binary code of length n. Show that if a word $u \in C$ is sent, and $v \in \mathbf{Z}_2^n$ is received, then v is correctly decoded under standard array decoding if and only if $u + v$ is the chosen coset leader in the coset $C + v$.

4. (MSc, MSci) Let p be prime and let $p \geq n \geq k$.

(a) Find a generator matrix for the $RS_{p,n,k}$ code in which polynomials are evaluated at $a_1, a_2, \ldots, a_n \in \mathbf{F}_p$.

(b) Check that your answer is correct for the code $RS_{5,4,2}$ where polynomials are evaluated at $0, 1, 2, 3 \in \mathbf{F}_5$.

5. (MSc/MSci)

(a) Show that if $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_r x^r \in \mathbf{F}_2[x]$ then

$$f(x)^2 = a_0 + a_1 x^2 + a_2 x^4 + \cdots + a_r x^{2r} = f(x^2).$$

(b) Hence, or otherwise, show that $x^8 + 1 = (x + 1)^8$ in $\mathbf{F}_2[x]$.

(c) Find all cyclic binary codes of length 8. Where it seems sensible, give a concrete description of each code, not using generating polynomials.

(d) Give an example of a cyclic binary code C with generator polynomial $g(x)$ such that the minimum distance of C is strictly less than the weight of $g(x)$.

(e) (**Optional**) Solve the 'Candles' problem on the sheet of challenge problems. [*Hint: there is a connection with cyclic codes. It might be good to start by solving the analogous two or four candles problem.*]

6. (MSc/MSci) Let $g(x) \in \mathbf{F}_2[x]$ be a generating polynomial for a cyclic binary code C of length n.

(a) Show that $g(1) \neq 0$ if and only if C contains a word of odd weight.

(b) Let C_{even} be the code containing all codewords in C of even weight. Show that C_{even} is cyclic and find a generator polynomial for C_{even} in terms of g.

7. Show that if C is a linear binary code of length n then the code $C^\star$ obtained by puncturing C in its final position is also linear.

8. Let C be a linear binary code of length n. For $i \in \{1, 2, \ldots, n\}$ let $e(i)$ be the word with 1 in position i and 0 in all other positions.

(a) Show that C is one-error correcting if and only if the cosets

$$C,\ C + e(1),\ \ldots,\ C + e(n)$$

are pairwise disjoint.

(b) Suppose that H is a parity check matrix for C. Show that if v, $v' \in \mathbf{Z}_2^n$ then $C + v = C + v'$ if and only if $vH^{tr} = v'H^{tr}$. Hence show that C is one-error correcting if and only if the columns of H are distinct and non-zero.

9. Use the Singleton bound to show that if C is a linear binary $[n, k, d]$-code then $k \leq n - d + 1$. What result does the asymptotic Plotkin bound give?

MT361/461/5461 Error Correcting Codes: Sheet 9

Questions 1 and 2 cover the material in the final week of lectures. An extra page of questions on the MSc/MSci course will be issued on Thursday (or can be obtained now from Moodle). The lecturer will be happy to answer questions over the vacation sent by email to `mark.wildon@rhul.ac.uk`.

1. Let C be the linear binary code of length 6 with generator matrix

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

(a) Find a code C' equivalent to C by a shuffle of positions such that C' has a generator matrix in standard form.

(b) Use Theorem 14.3 to find a parity check matrix H' for C'.

(c) Hence find a parity check matrix for C. [*Hint: undo the shuffle you performed to turn C into C'.*]

(d) Using the parity check matrix found in (c), make a syndrome / coset-leader table for C.

(e) Check that the syndromes of the six errors affecting just one position are distinct. Explain why this shows that C is 1-error correcting.

(f) Decode the received words 011100, 110111, 000011 using syndrome decoding.

2. Let C be the Hamming $[7, 4, 3]$-code defined in Example 14.6.

(a) Explain how C can be used to encode numbers between 0 and 15. Illustrate your answer by encoding the number 9.

(b) Use syndrome decoding to decode the received words 1011010, 0011011, 1100111 as numbers between 0 and 15.

(c) Show that the Hamming balls $B_1(u)$ of radius 1 about codewords are disjoint. Deduce that $\mathbf{Z}_2^7 = \bigcup_{u \in C} B_1(u)$. (This shows that C is perfect, in the sense defined in Question 3 of Sheet 4.)

(d) Suppose that C is used as a 1-error correcting code to send messages through a binary channel in which each bit of a sent word flips independently with probability $p < 1/2$.

(i) Show that the probability that a message is decoded correctly is

$$(1-p)^7 + 7p(1-p)^6.$$

(ii) Evaluate this probability when $p = 1/20$. Compare this probability with the probability of successful decoding if messages are sent directly as binary words of length 4.

3. (a) Show that there is a linear ternary one-error correcting code of length 12 with a 3×12 ternary parity check matrix all of whose row sums are 0.

(b) You have 12 pennies, one of which *might* be counterfeit, and of a different weight to the others. Using three weighings on a balance find out whether there is a counterfeit penny, and if so, determine whether it is heavy or light. (This is the 'Weighing Pennies' problem on the sheet of challenge problems.)

4. Show that if there is a linear binary $[n, k, d]$-code then there is a linear binary $[n - s, k - s, d]$-code for each $s \leq k - 1$. [*Hint: Question 5 on Sheet 7 is relevant.*]

5. The purpose of this question is to generalize the construction in Example 14.6. Let $r \in \mathbf{N}$ and let H be the $(2^r - 1) \times r$ matrix whose columns are all non-zero binary words of length r. Let

$$C = \{u \in \mathbf{Z}_2^{2^r - 1} : uH^{tr} = 0\}.$$

(a) Show that C is a linear binary code with parity check matrix H.

(b) Show that C is 1-error correcting, and that C contains a codeword u of weight 3. Deduce that C is a $[2^r - 1, 2^r - 1 - r, 3]$-code.

(c) Show that C is perfect.

(d) Deduce from Question 4 that if $2^k \leq 2^n/(1 + n)$ then there is a linear binary $[n, k, 3]$-code.

6. Let C be a linear binary $[n, k, d]$-code with parity check matrix H. Show that any $d - 1$ columns of H are linearly independent, and that there exist $i_1, \ldots i_d$ such that the sum of columns $i_1, \ldots, i_d$ of H is zero. Deduce Theorem 14.7.

7. Consider the Hadamard code $C = \{0000, 1111, 1010, 0101, 1100, 0011, 1001, 0110\}$ of length 4.

(i) Prove that C is a linear code and give a basis for it.

(ii) Write down a generator matrix G and find the corresponding parity check matrix H for C.

(iii) Construct a standard array for C.

8. Let C be a linear binary code of length n and dimension k. Given $u, v \in \mathbf{Z}_2^n$, let $\langle u, v \rangle = \sum_{i=1}^n u_i v_i$. Let $C^\star$ denote the dual space to C consisting of all linear maps from C to $\mathbf{Z}_2$. Let $f : \mathbf{Z}_2^n \to C^\star$ be defined so that $f(v) \in C^\star$ is the map $u \mapsto \langle u, v \rangle$, for $u \in C$.

(a) Show that f is linear.

(b) Show that the image of f is $C^\star$.

(c) Show that the kernel of f is $C^\perp$. (So $C^\perp$ can be defined in way that avoids the choice of a parity check matrix for C.)

(d) Deduce from the rank-nullity theorem that $\dim C^\perp = n - k$.

(e) Show that $(C^\perp)^\perp = C$. (This was suggested by Example 14.5.)

Questions 9 and 10 cover the final examinable material in the MSc/MSci course.

9. (MSc, MSci) Let C be the cyclic code of length 4 over $\mathbf{F}_5$ with generator polynomial $g(x) = (x+3)(x+1)$.

(a) Let $f(x) \in \mathbf{F}_5$. Show that $f(x)$ corresponds to a codeword in C if and only if $f(2) = f(4) = 0$.

(b) Let $u \in \mathbf{F}_5^4$. Show that $u \in C$ if and only if $uH^{tr} = \mathbf{0}$ where

$$H = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \end{pmatrix}.$$

(c) Show that C is equal to the Reed–Solomon code $RS_{5,4,2}$ where polynomials are evaluated at $1, 2, 4, 3 \in \mathbf{F}_5$.

10. (**MSc, MSci**) Let C be the binary cyclic code of length 7 with generator polynomial $g(x) = 1 + x + x^3$.

(a) Write down a generator matrix for C.

(b) Show that

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

is a parity check matrix for C. (For a more general result see Question 12.)

(c) Show that C is equivalent to the Hamming $[7, 4, 3]$-code, as defined in Example 14.6. [*Hint:* compare the parity check matrix above with the one in Example 14.6. Both have all non-zero words in $\mathbf{F}_2^3$ as their columns.]

(d) Let C^- be the binary code consisting of all codewords in C whose weight is even. Show that C^- is cyclic and find a generator polynomial for C^-.

(e) Does C properly contain any other cyclic codes?

In (d) and (e) you may find it helpful to note that $x^7 + 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$ where the factors are irreducible.

11. (**MSc, MSci**). Let $n \in \mathbf{N}$ and suppose that r divides n.

(a) Show that $g(x) = x^r + 1 \in \mathbf{F}_2[x]$ divides $x^n + 1$.

(b) Find an explicit basis for the the cyclic binary code C of length n with generator polynomial $g(x)$ and determine its dimension and minimum distance.

(c) Show that the dual code of C is cyclic and find its generator polynomial.

12. (**MSc, MSci**) Let C be a cyclic code over $\mathbf{F}_p$ with generator polynomial $g(x) \in \mathbf{F}_p[x]$. Let $g(x)h(x) = x^n - 1$ where $h(x) = h_0 + h_1x + \cdots + h_kx^k$. Show that the $(n-k) \times n$ matrix

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_1 & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & h_k & \dots & \dots & h_1 & h_0 \end{pmatrix}$$

is a parity check matrix for C.

13. (**MSc, MSci**) Let C be the cyclic code over $\mathbf{F}_{11}$ with generator polynomial $g(x) = (x-2)(x-2^2)(x-2^3)(x-2^4)$. Note that 2 is a primitive root in $\mathbf{F}_{11}$ so, by Corollary 5.4, C is the Reed–Solomon code $RS_{11,10,6}$.

(a) Use Theorem 5.3 to write down a parity check matrix for C.

(b) Suppose that $u \in C$ is sent and that errors of $\beta, \gamma \in \mathbf{F}_{11}$ occur in positions j and k where $0 \leq j < k < 11$. Show that if the syndrome of the received word is (S_1, S_2, S_3, S_4) then

$$S_1 + S_2x + S_3x^2 + S_4x^3 = \frac{\beta 2^j}{1 - 2^j x} + \frac{\gamma 2^k}{1 - 2^k x}$$

where we work modulo x^4. [*Hint:* expand $1/(1-2^jx)$ as a geometric series.]

(c) Show that if $S(x) = (A_0 + A_1x)/(1 + B_1x + B_2x^2)$ then

$$S_3 + B_1S_2 + B_2S_1 = 0$$
$$S_4 + B_1S_3 + B_2S_2 = 0.$$

(d) Describe a Linear Feedback Shift Register (LFSR) with the property that if the initial fill is (S_1, S_2) then stepping the register gives (S_2, S_3) and then (S_3, S_4).

(e) Decode the received words $(1, 10, 4, 10, 1, 5, 1, 0, 1, 0)$, $(0, 1, 0, 0, 0, 1, 8, 5, 3, 1)$.

14. **(Another link with the Channels course)** Let $n \in \mathbf{N}$ and let $1 \leq e \leq n/2$. Use the identity

$$1 = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k}$$

to show that

$$\sum_{k=0}^{e} \binom{n}{k} \geq \frac{1}{n(1-e/n)^{n-e}(e/n)^e}.$$

Hence deduce from Hamming's Packing Bound that if C is an e-error correcting binary code of length n then the rate of C is at most $1 - H(e/n) + (\log_2 n)/n$.