Designs and Codes
Martin Aigner

So 2017
Shagnik Das

Exercise Sheet 5

Due date: 12:30, Jun 28th, at the beginning of the exercise class.
Late submissions will be forever lost somewhere in my dungeon.

You should try to solve all of the exercises below, and submit three solutions to be graded — each problem is worth 10 points. We encourage you to submit in pairs, but please remember to indicate the author of each individual solution.

Exercise 1 We imagine that a sender is using some code $C \subseteq A^n$ to transmit messages to a receiver through a noisy channel, and that she sends the codeword one letter at a time. We further assume that there is some $0 < p < 1$ such that, independently for each letter, the noisy channel changes the letter being sent with probability p.

(a) Suppose C has length n, and that the sender is sending some codeword $c \in C$. What is the probability that there are exactly i errors in the word the receiver gets, for $0 \leq i \leq n$?

(b) The receiver gets a word $\tilde{c} \in A^n$, which, because of the noise in the channel, may not be the codeword c that the sender sent. The receiver must try to determine what c actually was. Assuming the error probability p is reasonably small, justify (mathematically) why the receiver should choose the closest codeword to $\tilde{c}$ if this codeword is unique.

Exercise 2 Let $C \leq \mathbb{F}_2^n$ be an $[n, k, d; 2]$-code for some $d \geq 2$.

(a) Denote by $C^{(i)}$ the code obtained by deleting the ith coordinate from each codeword. Show that $C^{(i)}$ is an $[n-1, k, d-1; 2]$-code.[1]

(b) Let $\hat{C} \subset \mathbb{F}_2^{n+1}$ be the code consisting of words of the form $(\vec{c}, y)$, where $\vec{c} \in C$ and $y \in \mathbb{F}_2$ is such that $\sum_{i=1}^{n} c_i + y = 0$.[2] Show that $\hat{C}$ is an $[n+1, k, \hat{d}; 2]$-code, where $\hat{d} = d$ if d is even, and $\hat{d} = d + 1$ if d is odd.

Exercise 3 Let C be a (not necessarily linear) $(n, d; q)$-code.

(a) Show that $|C| \leq q^{n-d+1}$.

(b) How does this bound compare to the Hamming bound?

[1] $C^{(i)}$ is called the *punctured code*. Recall that an $[n, k, d; q]$-code C has $d(C) \geq d$.
[2] $\hat{C}$ is called the *extended code*, and the extra letter y is often called a *check digit*.

Exercise 4

(a) Prove Proposition 2 by showing that a linear code C has $d(C) \geq d$ if and only if any $d-1$ columns of its control matrix H are linearly independent.

(b) Let C be a linear code over $\mathbb{F}_2$ with control matrix

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

For which values of n, k and d is C an $[n, k, d; 2]$-code? Is the code perfect?

Exercise 5

(a) Suppose one has a 1-error-correcting binary code[3] C. Explain how one can use the control matrix H to decode a message. That is, the recipient of the message should be able to identify and correct any single mistake in the transmission.

(b) A friend of yours suggests you communicate with each other using the code from Exercise 4(b).[4] Unfortunately, the code is not large enough to cover all letters in the English alphabet, so you decide to omit the least frequently used letters, using the encoding given in the table below.

Codeword	Letter	Codeword	Letter	Codeword	Letter
0000000	a	1100001	h	1001100	r
0111000	c	0011110	i	0110011	s
1000111	d	0010101	l	0001011	t
0100110	e	1101010	m	1110100	u
1011001	f	1010010	n	1111111	[space]
		0101101	o		

A short while later, you receive the following message from your friend. What is your friend trying to say?

```
10111100001011101111100101100111011111111101000010000010100111010001111
11111110000011000110111111011011011010110110011001101110111111111110011
01001101010010010101101011101010010011100001000100110011111011101111101
11101000001011111111100011011011011111111100010111100101010011001100010
01001101111111001010101001000001011000101101001101001100011001111111111
01000001010000100011111111111011010010110100010111101111010101111000000
01001101110111010110100010111101001010011010111000110011
```

[3] Recall that an R-error-correcting code C is one with $d(C) \geq 2R + 1$.

[4] If this doesn't sound like something your friends would suggest, you need better friends. Like these guys: `https://www.youtube.com/watch?v=CTjolEUj00g`.

Exercise 6 You and six of your friends enter a dark room, excited to take part in the newest "Escape" game in Berlin. That is the last thing you remember, though, when you wake up in a brightly-lit dungeon. Confused, you hear the only door being unlocked, and see someone walk in.

> "Welcome to Dungeon Escape II," she says.[5] "As you can see, while we drugged you and brought you to this secret location, we put hats on your heads. Each hat is either red or blue. You can see everyone else's hat, but you cannot see your own." You look around and see that she is telling the truth — all of your friends are wearing coloured hats, and you can feel one on top of your head too. However, the handcuffs and chains that are binding you to the wall make it impossible for you to reach or see your own hat.
>
> "In just a minute, I am going to ask you to guess what colour your hat is. You can either guess red or blue, or you can choose to pass.[6] If somebody answers correctly *and* nobody answers incorrectly, then I will let you all go free. However, if somebody guesses wrong, or if you all pass, nobody will ever see any of you again." After a brief pause for effect, the ominous silence is broken by her shrill and evil cackle. You would shudder at the thought of the evil fate that awaits you, but the chains are far too tight to allow such an expression of horror.
>
> "You are not allowed to communicate in any way, and you must answer simultaneously, right when I ask you. If there is any illegal communication, you will be stuck here forever." She immediately breaks out into another terrifying laugh. Given the drugging and the handcuffs, you have no doubt that she is serious about this threat. You can only base your guess on the colours of your friends' hats, and the same holds true for them. In particular, you will have no chance to hear what they are guessing before you make your own guess.
>
> "I have also made sure you cannot cheat by knowing about the hats in advance, since their colours were chosen independently and uniformly at random while we brought you here. So, that's enough of that — what colour is the hat on your head?"

It seems like a hopeless situation, but fortunately you and your friends have come prepared,[7] and play this game optimally. What is the probability that you will get to go home?

[Hint at `http://discretemath.imp.fu-berlin.de/DMIII-2017/hints/S5.html`.]

[5] "Not the most original of names," you think to yourself, but you are not too disappointed, for you prefer that they save their creativity for the puzzles themselves.

[6] Not being a fan of the red or blue options, you briefly consider guessing a third-party colour instead (say, green), but realise that it would be irresponsible to exercise the luxury of a protest guess that has no chance of being correct, which would leave you and all your friends stuck in a terrible situation that could possibly have been avoided had you guessed correctly.

[7] After all, you've been in similar situations before: `http://discretemath.imp.fu-berlin.de/DMI-2016/Sheet0.pdf`.[7]

[7] It would appear that your tendency to end up chained in dungeons has adversely affected your popularity.