IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises II.

1. Let A, B be codes over $\mathbb{F}_q^n$. Consider the code $A|B = \{a|a+b \mid a \in A \wedge b \in B\}$. Show that $h(A|B) = \min\{2h(A), h(B)\}$.

2. A code C is called weakly self dual if $C \subset C^{\perp}$. Prove the following.

   (a) If C is a binary weakly self dual code, every codeword is of even weight.

   (b) If each row of the generator matrix of a weakly self dual code C has weight divisible by 4 then so does every codeword.

3. Let C be the linear $[n,k]$-code with parity-check matrix

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

   (a) What is the generator matrix of C? Find out the value n and k? How many codewords are there in C?

   (b) Does the codeword 101010 belong to C?

   (c) Suppose the codeword $x = 001111$ is sent and $y = 000010$ is received. What is the syndrome $S(y)$? According to the syndrome, determine the position of an error? Why the coding system does not work in this case?

4. Consider a linear code C over $\mathbb{F}_q$ with a generator matrix G.

   (a) Show that in a binary code C every codeword has even weight if and only if every row of G has even weight.

   (b) Is the claim in (a) true for $q > 2$?

5. Consider linear codes C_1, C_2 of the same length. Prove the following:

   (a) $(C_1^{\perp})^{\perp} = C_1$,

   (b) $C_1 \subseteq C_2 \iff C_2^{\perp} \subseteq C_1^{\perp}$.

6. Let G_{24} be the extended Golay code with the following generator matrix *(with zeroes at blank positions)*:

$G =$

∞	0	1	2	3	4	5	6	7	8	9	10	∞	0	1	2	3	4	5	6	7	8	9	10	row
1	1												1	1		1	1	1				1		0
1		1												1	1		1	1	1				1	1
1			1										1		1	1		1	1	1				2
1				1										1		1	1		1	1	1			3
1					1										1		1	1		1	1	1		4
1						1										1		1	1		1	1	1	5
1							1						1				1		1	1		1	1	6
1								1					1	1				1		1	1		1	7
1									1				1	1	1				1		1	1		8
1										1				1	1	1				1		1	1	9
1											1		1		1	1	1				1		1	10
												1	1	1	1	1	1	1	1	1	1	1	1	11

More on next page >>>

Show that

(a) $G_{24} = G_{24}^{\perp}$.

(b) Every codeword of G_{24} code has weight divisible by 4.

(c) G_{24} contains the all-ones codeword $\mathbf{1}$.

(d) If G_{24} contains codeword $|L|R|$ with

$$L = a_\infty a_0 a_1 \ldots a_{10}, R = b_\infty b_0 b_1 \ldots b_{10},$$

it also contains codeword $|L'|R'|$ with

$$L' = b_\infty b_0 b_{10} b_9 \ldots b_1, R' = a_\infty a_0 a_{10} a_9 \ldots a_1.$$