Číslo cvičení: 1
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. $h(C) = 4$, $s(C) = 3$, $t(C) = 1$.
   C is equivalent to code $D = \{0000000, 1111000, 1100111, 001111\}$. (The last bit of all codewords is negated.)

2. Let the first codeword WLOG be 00000. The other codewords must differ in at least 4 bits, therefore can be from $A = \{01111, 10111, 11011, 11101, 11110, 11111\}$.
   $max\{h(x, y)|x, y \in A\} = 2 \implies$ the third codeword can only have a distance of 2 from the first two $\implies$ a binary $(5, 3, 4)$ code does not exist.

3.

4. The code is defined by the following table.

A	B	C	D	E
1	2	3	44	43

   The second symbol for the D and E characters could be chosen. It is probably better to choose the symbols that are statistically least used in the rest of the code.

5. For any codeword of length $n - 1$, there is exactly 1 symbol that can be put on the last position so that the resulting codeword of length n is in $C \implies M = q^{(n-1)}$. Because of that, if one symbol is changed, another must also be changed. Such change can be always made $\implies d = 2$.

6. (a) 8 distinct messages $\implies n \geq 3$. $n = 3$ does not provide room for any error correction. For $n = 4$, one additional bit is not enought to correct a shift of two bits. The following code provides the requested correction for $n = 5$.

Msg	unchanged	p_l	p_r
A	00000		
B	11111		
C	10000	00001	01000
D	11000	10001	01100
E	11100	11001	01110
F	11110	11101	01111
G	10100	01001	01010
H	10101	01011	11010

   The unchanged message is sent. The receiver decodes it using any of unchanged, p_l, p_r.

   (b) In a 4-bit code, there are 16 total codewords, 4 are symmetric and are always transmitted correctly. For the reamining $16 - 4 = 12$ we need two codewords for each message $\implies$ the total maximum is $4 + (16 - 4)/2 = 10$.

7. Only (b) is a possible Huffman code. (a) is not a prefix code. (c),(d) unnecessarily add a trailing 0 to their last codeword.

8. $x = 9$, Cryptography: An Introduction.