TMA 055 : Diskret Matematik

Inlämningsuppgift 5

Följande allmäna regler gäller för alla inlämningsuppgifterna (se också Kurs PM:et) :

1. Motivera (bevisa) alla svar.
2. Uppge vilka du samarbetet med.
3. Spara uppgifterna (med kommentarer) när du får tillbaka dem.

Att lämna in måndag den 21 oktober

OBS !! A. A couple more exercises will be added after the lecture on Tuesday, October 15. All exercises are worth 8 points, except for the bonus problem, which is worth 16 points.

1. Let p be a prime. Verify that the numbers $0, 1, ..., p-1$ form a field under addition and multiplication modulo p (that is, you must verify that all the field axioms are satisfied).

2. Which of the following are fields ?

(i) The integers $0, 1, 2, ..., 8$, under addition and multiplication modulo 9.
(ii) The vectors in the vector space $\mathbf{F}_2^4$, under componentwise addition and multiplication.

Obs : If your answer is 'yes, this is a field', then you must verify that all the field axioms are satisfied. Otherwise, you must indicate by means of examples which axioms are not satisfied.

3. Describe explicitly a finite field with 4 elements : that is, give the set, the addition and multiplication tables, and verify that all the field axioms are satisfied.

(Generous hints will be given for this exercise to those who ask for them !).

4. For any BSC, prove that the entropy

$$E = -\left(p \log_2 p + q \log_2 q\right)$$

of the channel is a real number between 0 and 1.

5. Use a simple example to illustrate that Shannon's Theorem breaks down for rates $R > 1 - E$.

(Hint : Consider a channel with $p = 1/2$).

6. Consider a BSC with parameter p. Suppose we send n bits along this channel. For $k = 0, 1, ..., n$, let $\mathcal{P}(k)$ denote the probability that k bits are changed during transmission. Find the maximum possible value of p for which $\mathcal{P}(k)$ is a non-increasing function of k.

(OBS! The answer depends on n).

7. Compute the probability of error for the rate 2/5 Hamming code discussed in class, if we use a channel with $p = 1/10$.

OBS! Om du har problem att lösa uppgift **8** då kan det hjälpa att kika på uppgift **9** först.

8. Låt C vara en linjär kod av längd n och dimension k. Låt paritetsmatrisen för C vara given på formen

$$H = \left[\begin{array}{cc} \mathbf{P} & \mathbf{E}_{n-k} \end{array} \right] \tag{1}$$

där $\mathbf{P}$ är en $(n-k) \times k$ matris och $\mathbf{E}_{n-k}$ är enhetsmatrisen av storlek $n-k$.

OBS! Detta är inte formen som gavs på föreläsningen. I formen ovan så placeras informationsbitarna i de FÖRSTA k positionerna i kodorden, snarare än de sista k.

Ange nu formen på en generator matris for C.

9. OBS! For full points on this exercise, you should solve it without writing out any codewords.

Let C be the code which takes 3-bit information blocks (a_1, a_2, a_3) and encodes them as 6-bit codewords $(a_1, a_2, a_3, a_4, a_5, a_6)$ such that

$$\begin{aligned} a_4 &= a_2 + a_3, \\ a_5 &= a_1 + a_3, \\ a_6 &= a_1 + a_2. \end{aligned}$$

Write down a parity-check matrix H for this code of the form (1) above, and a corresponding generator matrix. What is the dimension, rate and minimal distance of C ? Show that C corrects one error.

Bonus problem

10. Repeat **Q.5** but this time illustrate the breakdown using a channel with parameter $p = 1/4$.