UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in: MAT2250 — Discrete Mathematics

Day of examination: 9:00 am May 22, 2020 - 9:00 am May 29, 2020

This problem set consists of 2 pages.

Appendices: none

Permitted aids: all

Please make sure that your copy of the problem set is complete before you attempt to answer anything.

Problem 1

1. Let $G = (V, E)$ be a graph with the $|V| \times |E|$ incidence matrix

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

   (a) Draw the graph G.

   (b) Write down the $|V| \times |V|$ adjacency matrix of G.

   (c) Is the graph G Eulerian? (Justify your answer). If not, find a tour of all of the vertices in G that has the minimal number of edges.

2. Let G be a graph with $n \geq 3$ vertices. Show that if $d(u) + d(v) \geq n$ for every pair of non-neighbouring vertices u and v, then G is Hamiltonian.

Problem 2

1. Let $C \subset \{0, 1\}^6$ be the binary code

$$C = \{000000, 111000, 100110, 010101, 001011\}.$$

   (a) Is C a linear code? (Justify your answer)

   (b) Determine $d(C) = \min_{a \neq b \in C} \Delta(a, b)$.

   (c) Is C t-error correcting for some t? If so, is C a t-perfect code? (Justify your answers)

(Continued on page 2.)

2. Let K be a finite field and $C \subset K^n$ be a cyclic code. Suppose the generating polynomial of C is $g(x) \in K[x]$ and let
$$\frac{x^n - 1}{g(x)} = x^r + h_{r-1}x^{r-1} + \cdots + h_1 x + h_0,$$
for $h_i \in K$. Show that the dual code $C^\perp$ has generating polynomial
$$\tilde{h}(x) = h_0^{-1}(h_0 x^r + h_1 x^{r-1} + \cdots + h_{r-1}x + 1).$$
Conclude that the dual code $C^\perp$ of a cyclic code C is cyclic.

Problem 3

1. Why is there no 2-design with parameters $v = 9$, $k = 5$ and $\lambda = 1$?
2. Let $\mathcal{P}$ be a finite projective plane of order n and let S denote its set of points. Consider the collection of subsets of S defined by
$$\mathcal{T} = \{A \subset S \mid A = \{p, q, r\} \text{ and } p, q, r \text{ are not collinear in } \mathcal{P}\}$$
and
$$\mathcal{U} = \{A \subset S \mid |A| \leq 2 \text{ or } A \in \mathcal{T}\}.$$
Show using the axioms of a finite projective plane that $M = (S, \mathcal{U})$ satisfy the axioms to be the independent sets of a matroid.
3. How many independent sets are there in the matroid constructed above in the case of the Fano plane?

Problem 4

1. Using the Diffie Hellman key exchange Alice and Bob choose the prime $p = 11$ and the primitive root $a = 7$.

   Alice sends $A = 2$ to Bob and Bob sends $B = 10$ back to Alice. What are their private keys? (Use page 313 of Aigner).
2. Alice publishes the public key $n = 91, k = 5$ hoping to receive secret messages via the RSA protocol. Use the fact that n is not very large combined with the Euclidean algorithm in reverse to crack Alice's secret key.
3. Decode the following message that was sent from Bob to Alice using a (modular) calculator:
$$63 \quad 71 \quad 23 \quad 0 \quad 80 \quad 71 \quad 13 \quad 13 \quad 31 \quad 44.$$
Each block represents the encryption of a single letter via space = 0, A = 1, B = 2, C = 3, D = 4.... and then encrypted using RSA with Alice's public key. Explain the computation used to decode.