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 0 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.

Solution: The adjacency matrix of G is a $|V| \times |V|$ matrix with $a_{ij} = 1$ if v_i is adjacent to v_j and $a_{ij} = 0$ otherwise. The adjacency matrix is:

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

(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.

Solution:

By Theorem 8.19 of Aigner a graph G is Eulerian if and only if it is connected and every vertex is of even degree. Only the vertex corresponding to the 4th column of the incidence matrix is of even degree, therefore G is not Eulerian.

(Continued on page 2.)

We are asked to find a "tour" in G, following page 172 of Aigner this means a circuit in G traversing every edge of G at least once. Following the algorithm to solve An Ya-Ren's postal worker problem we insert the edges v_1v_2 and v_3v_5 to obtain a multigraph G'. This multigraph is then Eulerian and an Eulerian tour is given by $v_1v_2v_3v_5v_4v_3v_5v_2v_1$, the edges v_1v_2 and v_3v_5 are traversed twice.

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.

Solution:

Fix $n \geq 3$ and consider the set of all the graphs with n vertices which satisfy the above assumption and are not Hamiltonian. If this set is non-empty we can choose a graph $H = (V, E)$ in this set such that adding any edge $uv \notin E$ for $u, v \in V$ makes the graph Hamiltonian. We will derive a contradiction from the existence of H, therefore the set of graphs satisfying the hypothesis which are not Hamiltonian must be empty and the statement in the problem is true.
Firstly the graph H must contain a Hamiltonian path (not closed), this is because if we add any edge there would exist a Hamiltonian circuit and upon removing the edge we have a Hamiltonian path. Suppose the path is $u = u_1, u_2, \ldots, u_n = v$. Now consider the sets

$$A = \{u_i \mid uu_{i+1} \in E\} \quad \textbf{and} \quad B = \{u_j \mid u_jv \in E\}.$$

By assumption:

$$n \leq d(u) + d(v) = |A| + |B| = |A \cup B| + |A \cap B|$$

However, $v \notin |A \cup B|$ so $|A \cup B| < n$ and $A \cap B \neq \emptyset$. Take $u_k \in A \cap B$ and form the closed Hamiltonian circuit $u = u_1, \ldots, u_k, v = u_n, u_{n-1}, \ldots, u_{k+1}, u$. This provides the contradiction we were after and completes the proof of the statement.

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)

   Solution
   i) The code is not linear since $|C| = 5 \neq 2^k$ for some k. Also $011110 = 111000 + 100110 \notin C$.

(Continued on page 3.)

ii)The distance of the code is the minimum over all Hamming distances between distinct elements in C. Firstly, $\Delta(000000, b) = 3$ for all $b \in C, b \neq 000000$. Checking the remaining 6 pairs of distinct elements of C we see that $\Delta(a, b) = 4$ for $a, b \neq 000000$ and $a \neq b$. Therefore $d(C) = 3$.
iii) Since $d(C) = 3 = 2t + 1$ the code C is 1-error correcting. The code is not perfect since it does not attain Hamming's bound. Since $q = 2$ we have for Hamming's bound

$$\frac{q^n}{1 + \binom{n}{1}(q-1)} = \frac{2^6}{7} > 5.$$

Alternatively, we see that C is not 1-perfect since the word 111111 is not in a ball of radius 1 around an element of C.

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.

Solution
From Aigner, the parity check matrix for C is

$$\begin{pmatrix} 0 & 0 & 0 & h_0 & h_1 & \dots & 1 \\ 0 & 0 & h_0 & h_1 & \dots & 1 & 0 \\ \dots & & \dots & & \dots & & 0 \\ h_0 & h_1 & \dots & h_{r-1} & 1 & 0 & 0 \end{pmatrix}$$

This matrix is the generator matrix of the dual code $C^\perp$. Dividing each row by $h_0 \neq 0$ is still a generating matrix and each row is a vector corresponding to the monic polynomial $x^j\tilde{h}(x)$.
To see that $C^\perp$ is indeed cyclic we must check that $\tilde{h}(x)$ divides $x^n - 1$. One way to do this is to see that $h(x)g(x) = x^n - 1$ and if $\tilde{g}(x)$ is the polynomial $g(x)$ with coefficients written backwards then $-h_0\tilde{g}(x)\tilde{h}(x)$ is $x^n - 1$. So $\tilde{h}(x)$ divides $x^n - 1$.

Problem 3

1. Why is there no 2-design with parameters $v = 9$, $k = 5$ and $\lambda = 1$?

Solution
By Theorem 12.9 of Aigner, for a t-design with parameters v, k, λ we have $|\mathcal{B}| = \lambda\frac{\binom{v}{t}}{\binom{k}{t}} = \frac{9\cdot 8}{5\cdot 4}$. But $|\mathcal{B}|$ is the number of blocks which must be a natural number, so no such 2-design exists.

(Continued on page 4.)

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.

   Solution

   We must show that M satisfies the following three axioms.

   (a) $\emptyset \in \mathcal{U}$

   (b) if $B \in \mathcal{U}$ and $A \subset B$ then $A \in \mathcal{U}$.

   (c) if $A, B \in \mathcal{U}$ and $|B| = |A| + 1$ then $A \cup b \in \mathcal{U}$ for some $b \in B$.

   Since $|\emptyset| = 0 < 2$ we have $\emptyset \in \mathcal{T} \subset \mathcal{U}$ and a) is satisfied.
   If $B \in \mathcal{U}$ and $A \subset B$ then $|A| \leq 2$ so $A \in \mathcal{T} \subset \mathcal{U}$ and b) is satisfied. Finally, if $A, B \in \mathcal{U}$ and $|A| + 1 = |B| = |2|$ then $|A| = 1$ and any $b \in B$ such that $b \notin A$ satisfies $A \cup b \in \mathcal{U}$. In the same situation, if $|B| = 3$ then $A = 2$. By the axioms of a finite projective plane, there is a unique line L in $\mathcal{P}$ incident to the two points in A. Since the three points in B are not all collinear there must exist a $b \in B$ not contained on L. Then $A \cup b \in \mathcal{U}$ since the three points are not collinear.
   Therefore, M is a matroid.

3. How many independent sets are there in the matroid constructed above in the case of the Fano plane?

   Solution

   There are exactly three points on each line in the Fano plane and there are exactly 7 lines. The independent subsets of M in this case are all subsets of the 7 points of size less than or equal to 3 with the exception of these 7. Therefore, there are

   $$\binom{7}{0} + \binom{7}{1} + \binom{7}{2} + \binom{7}{3} - 7 = 57$$

   independent subsets in the matroid.

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).

   Solution

   1. We need to solve the discrete log problem for $p = 11$ and base 7. There is even a table in Aigner. $7^2 \equiv 5 \mod 11$ and $7^5 \equiv 10 \mod 11$. Therefore, Alice's key is 3 and Bob's is 5.

(Continued on page 5.)

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.

Solution

We begin by factoring $91 = 7 * 13$. **Then we can compute** $(p-1)(q-1) = 72$. **The public and private keys satisfy** $gk \equiv 1 \mod (p-1)(q-1)$ **and** g, k **must be relatively prime to** 72. **We wish to find the unique** g **such that**

$$gk + m(p-1)(q-1) = 1.$$

Running the Eulclidean algorithm backwards we find that $5 * 29 + (-2)91 = 1$**, so that** $5 * 29 \equiv 1 \mod 72$. **The secret key is then** 29.

3. To encrypt the message Bob computed $T^5 \mod 91$ **for each number** T **corresponding to a letter he wished to send. To decrypt Alice must now compute** $C^{29} \mod 91$ **for each number received from Bob and find the corresponding letter of the alphabet.**

Using a modular arithmetic calculator online (Wolfram for instance) we obtain:

$$63^{29} \equiv 7 \quad 71^{29} \equiv 15 \quad 23^{29} \equiv 4 \quad 0^{29} \equiv 0 \quad 80^{29} \equiv 19$$
$$71^{29} \equiv 15 \quad 13^{29} \equiv 13 \quad 31^{29} \equiv 5 \quad 44^{29} \equiv 18.$$

The message is GOD SOMMER.

(Continued on page 6.)