UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in:	MAT2250 — Discrete Math
Day of examination:	Wednesday 12. June 2024
Examination hours:	15:00 – 17:00
This problem set consists of 3 pages.	
Appendices:	none
Permitted aids:	none

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

Problem 1 25 points

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

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

1. (5 points) Draw the graph G.
2. (10 points) Define a weight function on the edges of the above graph G by setting $w(e_{ij}) := i + j$, where e_{ij} is the weight of the edge between vertices corresponding to columns i and j (if the edge exists). Find a minimal weight spanning tree of the weighted graph and explain the algorithm you used to do so.
3. (10 points) For which n is the complete graph K_n Eulerian? Describe the Hamiltonian circuits in the complete graph K_n. Justify your answers.

Problem 2 25 points

1. (5 points) Are the two latin squares of size 5 orthogonal? Justify your answer.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \\ 3 & 5 & 1 & 2 & 4 \\ 4 & 3 & 2 & 5 & 1 \\ 5 & 1 & 4 & 3 & 2 \end{bmatrix}$$

(Continued on page 2.)

2. (10 points) A triangle in a finite projective plane consists of three points which are not all contained on a common line. How many triangles are there in the Fano plane (the finite projective plane of order 3)?

3. (10 points) Let $(S, \mathcal{B})$ be a t-design with $|S| = v$, $|B| = k$, for all $B \in \mathcal{B}$ and $\lambda = 1$. Define a code

$$C = \{c_B \mid B \in \mathcal{B}\} \subseteq \{0,1\}^v,$$

where c_B is the vector of zeros and ones with i-th coordinate equal to 1 if $i \in B$ and 0 otherwise.

Show that

$$d(C) \geq 2(k - t + 1),$$

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

Hint: $\Delta(c_{B_1}, c_{B_2})$ is the size of the symmetric difference of the sets B_1 and B_2.

Problem 3 25 points

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

$$C = \{000000, 111000, 100110, 011110\}.$$

   (a) (5 points) Is C a linear code? Is C a cyclic code? (Justify your answers)

   (b) (5 points) Determine $d(C) = \min_{a \neq b \in C} \Delta(a, b)$. For what t is the code t-error correcting?

   (c) (5 points) Suppose that, over a channel which produces at most one error, the message 010110 was received. Correct the error and determine which codeword was sent.

2. (10 points) Let $C \subseteq \{0,1\}^7$ be the binary cyclic code with generating polynomial

$$g(x) = x^3 + x^2 + 1$$

and let $C' \subseteq \{0,1\}^7$ be the binary cyclic code with generating polynomial

$$h(x) = x^4 + x^2 + x + 1.$$

Write down generating matrices for both C and C' and show that $C^\perp = C'$.

Problem 4 25 points

1. (5 points) Compute 3^{302} modulo 5.

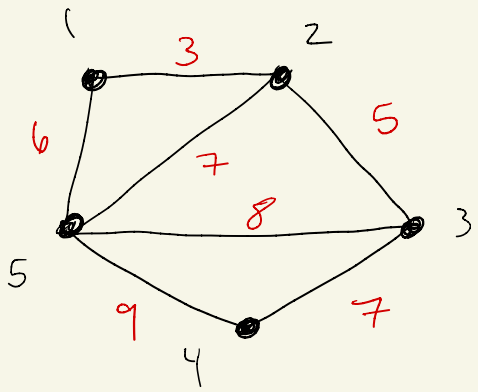
2. (5 points) Show that 2 is a primitive root modulo 11.

3. (5 points) In a Diffie-Hellman key exchange Alice and Bob share the public key $p = 11$ and $a = 2$. Alice sends $A = 5$ to Bob and Bob sends $B = 9$ to Alice. What is their shared secret key K?

(Continued on page 3.)

4. (10 points) Alice publishes the RSA public key $n = 55$ and $k = 27$. Bob sends a secret meeting time to Alice using her public key. Eve manages to intercept the message "28" and decode it after cracking Alice's private key. What is Alice's private key and what is the secret meeting time?

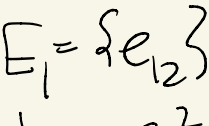
1.



2. The weight function $w(e_{ij}) = i + j$ is drawn in red on the edges of G above

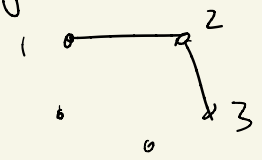
3. We use Kruskal's greedy algorithm to find a minimal weight spanning tree. The algorithm constructs a spanning tree by selecting at each step the edge of minimal weight which does not create a cycle with the previously selected edges.

Step 1: select edge e_{12} $E_1 = \{e_{12}\}$



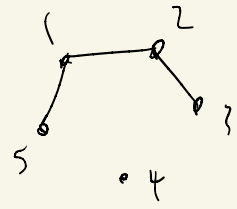
Step 2: select edge e_{23}

$E_2 = \{e_{12}, e_{23}\}$



Step 3: select edge e_{15}

$E_3 = \{e_{12}, e_{23}, e_{15}\}$

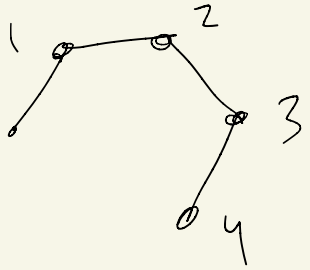


Step 4: there are two edges of minimal weight e_{25}, e_{34}. adding e_{25} produces a cycle. So we add e_{34}

$E_4 = \{e_{12}, e_{23}, e_{15}, e_{34}\}$.

The spanning tree of minimal weight is

$T =$



3. A graph is Eleian if it contains an Eulerian circuit, a circuit which traverses each edge exactly once.

A graph is Eulerian if and only if every vertex has even degree

For $G = K_n$ $\deg(v) = n-1$ for every vertex. Hence, K_n is Eulerian if and only if n is odd.

Problem 2

1) A pair of orthogonal Latin squares is orthogonal if the map

$$L \times L' : \{1 \dots n\}^2 \longrightarrow \{1, \dots n\}^2$$

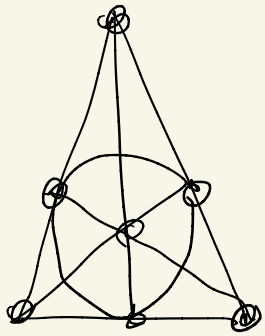
$$(i,j) \longmapsto (L(i,j), L'(i,j))$$

is a bijection.

Notice that

$$L \times L'(1,i) = (i,i) = L \times L'(i,1)$$

Hence the map is not injective so L, L' are not orthogonal.

2) 

The Fano plane consists of 7 points and 7 lines. Each line contains exactly 3 points.

$$\#\text{Triangles} = \#\text{triples of points} - \#\text{triples of collinear points.}$$

$$\#\text{Triangles} = \binom{7}{3} - 7$$

$$= 35 - 7.$$

$$= 28$$

3. For two code words C_{B_1}, C_{B_2}

$$\Delta(C_{B_1}, C_{B_2}) = |\{i \in S \mid i \in B_K \; i \notin B_\ell\}|$$

$$= |B_1 \cup B_2| - |B_1 \cap B_2|$$

$$|B_1 \cup B_2| = |B_1| + |B_2| - |B_1 \cap B_2|.$$

Note that $|B_i| = K$ and since every set of size t is contained in at most one block $|B_1 \cap B_2| \leq t-1$.

$\Rightarrow$

$$\Delta(C_{B_1}, C_{B_2}) \geq 2K - 2(t-1).$$

Therefore, $d(C) \geq 2(K-t+1)$.

Problem 3

1 a) $C = 000000$

and $111000 + 100110 = 011110$

so C is linear.

b) Since C is linear

$$d(C) = \min_{c \neq 0} w(c) = 3.$$

so C is 1-error correcting.

c) Since C is 1-error correcting and the channel produces at most one error the message sent is the unique element a in C which has

$$\Delta(a, 010110) = 1 \Rightarrow a = 011110.$$

2) The generating matrix for the code C is

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

The generating matrix for $C^{\perp}$ is

$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Recall that $C^{\perp} \leq \{0,1\}^7$ is the set

$$C^{\perp} = \{ a \in \{0,1\}^7 \mid \langle a, c \rangle = 0 \ \forall c \in C \}$$

To see that $C^{\perp} = C$ we check that each row of H has inner product 0 with each row of G.

By the cyclic nature of the rows it suffices to check one row of H with every row of G:

$$0001101 \cdot 0010111 = 1+1 = 0$$
$$0011010 \cdot 0010111 = 1+1 = 0$$
$$0110100 \cdot 0010111 = 1+1 = 0$$
$$1101000 \cdot 0010111 = 0$$

Therefore, $C^{\perp} = C$.

Problem 4

1. 5 is prime so $3^4 \equiv 1 \mod 5$ by Fermat's Little Theorem.

$$\Rightarrow 3^{302} \equiv 3^{4 \cdot 15 + 2} \equiv 3^2 \equiv 9 \equiv 4 \mod 5.$$

2. We compute all powers of 2 mod 11

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^3 \equiv 8$

$2^4 \equiv 5$

$2^5 \equiv 10$

$2^6 \equiv 9$

$2^7 \equiv 7$

$2^8 \equiv 3$

$2^9 \equiv 6$

$2^{10} \equiv 1$

The powers of 2 are $\{1, \ldots, 10\}$

Hence 2 is a primitive root mod 11.

3. Alice's public key is $5 \equiv 2^4 \mod 11$

So her public key is $a = 4$

Bob's public key is $9 \equiv 2^6$

So his public key is $b = 6$.

Their shared private key is

$$2^{4 \cdot 6} \equiv 2^{2 \cdot 10} \cdot 2^4$$

$$K \equiv 5 \mod 11$$

4. $n = 55 = 5 \cdot 11$ $K = 27$.

Alice's private key is the multiplicative inverse of 27 mod $40 = (p-1)(q-1)$

Use Euclidean algorithm:

$40 = 1 \cdot 27 + 13$.

$27 = 2 \cdot 13 + 1$

$1 = 27 - 2 \cdot 13$

$= 27 - 2(40 - 27)$

$1 = 3 \cdot 27 - 2 \cdot 40$.

$\Rightarrow 3 \cdot 27 \equiv 1 \mod 40$.

Therefore Alice's private key is 3.

Eve uses the private key to decode the message 28.

The sent secret message is

$$28^3 \mod 55$$

Notice $2 \cdot 28 = 56 \equiv 1 \mod 7$.

$$28^3 \equiv 14 \cdot (2 \cdot 28) \cdot 28 \equiv 7 \cdot 2 \cdot 28 \equiv 7 \mod 5$$

(the $(2 \cdot 28)$ term is $\equiv 1$, and $2 \cdot 28 \equiv 1$)

Therefore the secret meeting time is 7.