UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in:	MAT2250 — Discrete Math
Day of examination:	When you like!
Examination hours:	00:00 – 4:00

This problem set consists of 2 pages.

Appendices:	none
Permitted aids:	none

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

Use this practice exam to help you gauge your preparation for the final!

Problem 1 25 points

1. (5 points) How many spanning trees are there of K_4?
2. (5 points) How many vertices are there in the hypercube graph Q_n?
3. (5 points) For what n is the hypercube graph Eulerian?
4. (10 points) Construct a Hamiltonian circuit in Q_3.

Problem 2 25 points

1. (5 points) How many mutually orthogonal latin squares are there of size 9?
2. (10 points) Give the definition of a 2-design $(S, \mathcal{B})$ with parameters $\lambda = 1$, $k = 3$ and $\nu = 7$.

   How many blocks in $\mathcal{B}$ contain a fixed element $i \in S$?
3. (10 points) Let $(S, \mathcal{B})$ be a 2-design with $S = \{1, \ldots, v\}$, $\lambda = 1$, and $|B| = k$ for all $B \in \mathcal{B}$. Suppose $|\mathcal{B}| = b$ and consider the $v \times b$ incidence matrix $B = (b_{ij})$ defined by $b_{ij} = 1$ if $i \in B_j$ and $b_{ij} = 0$ if $i \notin B_j$.

   Calculate the $v \times v$ matrix BB^T, where B^T is the transpose of B.

Problem 3 25 points

1. (10 points) Define the Hamming distance and show that it satisfies the triangle inequality.

(Continued on page 2.)

2. (5 points) Consider the code

$$C = \{00000, 21212, 01010, 20202\} \subset \{0, 1, 2\}^5.$$

What is $d(C) := \min_{\substack{a,b \in C \\ a \neq b}} \Delta(a, b)$?

3. (10 points) Let $C_1, C_2 \subset \{0, 1\}^7$ be two cyclic codes. Suppose that the generating polynomial of C_1 is $g_1(x) = x^5 + x^4 + x^3 + 1$ and the generating polynomial of C_2 is $g_2(x) = x^3 + x^2 + 1$. Show that $C_1 \subset C_2$.

Problem 4 25 points

1. (5 points) Compute 3^7 modulo 13.

2. (10 points) Find the multiplicative inverse of 2 mod 11. Does 6 have a multiplicative inverse modulo 15?

3. (10 points) 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. Find each of their private keys.