UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in: MAT2250 — Discrete Mathematics

Day of examination: Wednesday 2. June 2021

Examination hours: 9:00 – 13:00

This problem set consists of 7 pages.

Appendices: none

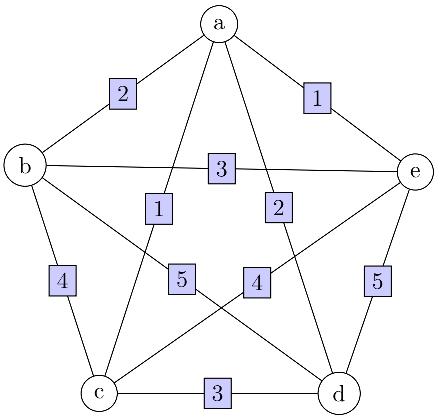
Permitted aids: all

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

Justification must be provided for all solutions. Solutions can be submitted in English or Norwegian. The format may be in Latex or as scanned handwritten notes.

Problem 1

Consider the traveling salesperson problem (TSP) on the following graph where the number on an edge indicates its weight.



1. (5 points) Is this a metric TSP?

   Solution

   A TSP is *metric* if for all triples of distinct vertices i, j, k we have $w_{ij} \leq w_{ik} + w_{kj}$. The above TSP is not metric since $w_{bc} = 4$, yet $w_{ab} + w_{ac} = 2 + 1 = 3$ so $w_{bc} > w_{ab} + w_{ac}$.

   Other solutions are possible! For example $w_{ed} > w_{ad} + w_{ae}$.

2. (20 points) Run the Christofides heuristic to provide a route for a traveling salesperson. Explain each step of the heuristic and name the graph algorithms that you use as they arise.

(Continued on page 2.)

Solution

Step 1: Run Kruskal's algorithm to find a minimal spanning tree. The tree has edges $a-b$, $a-c$, $a-d$, $a-e$.

Step 2: Build complete graph on vertices of odd degree and find a maximal matching with minimal weight. The graph is the complete graph on b, c, d, e and the matching to be found is $b-e$ $c-d$. We didn't learn a matching algorithm for K_n, only for $K_{n,n}$. Here the matching is found by brute force.

Step 3: Add these edges to T to obtain an Eulerian multigraph. Use Algorithm 8.2 from Aigner to produce an Eulerian circuit. There are many possibilities here.

Step 4: The Eulerian circuit “contains" a Hamiltonian cycle. This is found by following the skipping over vertices that would otherwise be repeated. (The solution unfortunately cannot be unique).

Grading There were 5 points for each step. If the explanations were weak or the algorithm of a step was not mentioned 1-2 were removed.

Problem 2

1. (5 points) Consider the 2-design with $v = 7$ and $b = 7$ consisting of the blocks

$$\mathcal{B} = \{\{124\}, \{137\}, \{156\}, \{235\}, \{267\}, \{346\}, \{457\}\}.$$

Write down the $v \times b$ incidence matrix of the 2-design.

Solution

Index the rows of a 7×7 matrix with the elements $1, \ldots, 7$ in increasing order and the columns of the matrix by the blocks as they appear in the list. Then the incidence matrix for the design is:

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

2. (10 points) Show that the columns of the incidence matrix of an arbitrary t-design $(S, \mathcal{B})$ with parameters $v, k \in \mathbb{Z}_{\geq 1}$ and $\lambda = 1$ give a code $C \subseteq \{0,1\}^v$ with $|C| = |\mathcal{B}|$ and satisfying $d(C) \geq 2(k - t + 1)$ when $|\mathcal{B}| \geq 2$.

Solution

The columns of the incidence matrix give a set C of $|\mathcal{B}|$ vectors in $\{0,1\}^v$. Denote the vector in $C \subset \{0,1\}^v$ corresponding to the block B_i by b^i. Each code word b^i has weight $w(b_i) = k$.

The distance of a code C is defined as

$$d(C) = \min_{b^i, b^j} \Delta(b^i, b^j),$$

(Continued on page 3.)

where the minimum is over distinct b^i, b^j. Therefore, we need to bound the Hamming distance of the vectors of two distinct blocks b^i and b^j.

$$\Delta(b^i, b^j) = \{k \mid b^i_k \neq b^j_k\} = |\{k \mid k \in B_i \cup B_j \text{ and } k \notin B_i \cap B_j\}|.$$

In other words $\Delta(b^i, b^j)$ is the size of the symmetric difference of B_i and B_j, namely $\Delta(b^i, b^j) = |(B_i \cup B_j) \backslash (B_i \cap B_j)|$. By inclusion-exclusion

$$|B_i \cup B_j| = |B_i| + |B_j| - |B_i \cap B_j|.$$

and therefore,

$$|(B_i \cup B_j) \backslash (B_i \cap B_j)| = |B_i| + |B_j| - 2|B_i \cap B_j|$$

Each B_i has the same size, namely $|B_i| = |B_j| = k$, so it remains to bound the size of $B_i \cap B_j$.

We claim that $|B_i \cap B_j| \leq t - 1$. Since $\mathcal{B}$ is a t-design with $\lambda = 1$, every subset of size t is contained in exactly one block. Therefore, $|B_i \cap B_j| \geq t$ then there is a subset of size t contained in the two blocks contradicting $\lambda = 1$. The claim is proved.

Combining this into the inequality we obtain: $\Delta(b^i, b^j) \geq 2(k - t + 1)$ for all $b^i \neq b^j \in C$ and therefore $d(C) \geq 2(k - t + 1)$.

Grading The key here was to use that $\lambda = 1$. Maybe people wrote arguments that didn't use this these were incomplete/misleading proofs and received up to 6 points depending on what other details were included.

3. (10 points) For $a \in \{0,1\}^n$ find and prove a formula for the number of points in

$$B_t(a) = \{b \in \{0,1\}^n \mid \Delta(a,b) \leq t\} \subseteq \{0,1\}^n$$

where $\Delta(a,b)$ denotes the Hamming distance between a and b and $t \in \mathbb{Z}_{\geq 0}$.

Use inclusion-exclusion to determine the number of points in

$$B_1((0,0,0)) \cup B_1((1,0,0)) \cup B_1((0,1,0)).$$

Solution

For the number of points in the ball of radius t about a we can partition the set $B_t(a)$ into disjoint subsets:

$$B_t(a) = \bigsqcup_{i=0}^{t} \{b \in \{0,1\}^n \mid \Delta(a,b) = i\}.$$

Using the summation law we have

$$|B_t(a)| = \sum_{i=0}^{t} |\{b \in \{0,1\}^n \mid \Delta(a,b) = i\}|.$$

(Continued on page 4.)

To determine the size of the set $A_i = \{b \in \{0,1\}^n \mid \Delta(a,b) = i\}$, notice that there is a bijection

$$f \colon A_i \to \{i\text{-subsets of size of } \{1,\dots,n\}\}.$$

For an element $b \in A_i$ we assign the subset $f(b) = \{j \mid a_j \neq b_j\}$. The inverse is then $f^{-1}(I) = a + v^I$, where v^I is the vector defined by $v^I_i = 1$ if $i \in I$ and $v^I_i = 0$ otherwise. By the rule of equality we obtain $|A_i| = \binom{n}{i}$. Combining this with the summation rule above we have:

$$B_t(a) = \sum_{i=0}^{t} \binom{n}{i}.$$

For the second task, we use inclusion-exclusion to determine the number of points in

$$A = B_1((0,0,0)) \cup B_1((1,0,0)) \cup B_1((0,1,0)).$$

$$|A| = |B_1((0,0,0))| + |B_1((1,0,0))| + |B_1((0,1,0))|$$
$$-|B_1((0,0,0)) \cap |B_1((1,0,0))| - |B_1((0,0,0)) \cap B_1((0,1,0))| - |B_1((1,0,0)) \cap B_1((0,1,0))|$$
$$+|B_1((0,0,0)) \cap B_1((1,0,0)) \cap B_1((0,1,0))|$$

By our above calcuation each ball $B_1(v) \subset \{0,1\}^3$ contains exactly 4 points. Moreover we have:
$B_1((0,0,0)) \cap |B_1((1,0,0)) = \{(0,0,0),(1,0,0)\}$
$B_1((0,0,0)) \cap |B_1((0,1,0)) = \{(0,0,0),(0,1,0)\}$
$B_1((1,0,0)) \cap |B_1((0,1,0)) = \{(1,1,0),(0,0,0)\}$
Lastly we see that $B_1((0,0,0)) \cap B_1((1,0,0)) \cap B_1((0,1,0)) = (0,0,0)$. Combining this and the above inclusion-exclusion formula we obtain:

$$B_1((0,0,0)) \cup B_1((1,0,0)) \cup B_1((0,1,0)) = 3 \cdot 4 - 3 \cdot 2 + 1 = 7.$$

Grading The most common thing here was a not very well justified or explained counting argument for the number of points in the ball (1 to 2 points were removed for lack of justification). I was looking for things like the summation rule (breaking a set into disjoint subsets and counting parts), and the rule of equality (finding a bijection with words of distance exactly t and subsets of size t).

Problem 3

1. (5 points) Let $C \subset \{0,1\}^5$ be the binary linear code

$$C = \{00000, 11100, 11111, 00011\}.$$

Write down a generating matrix for C.

Solution

(Continued on page 5.)

Since $|C| = 4 = 2^2$ the dimension of C is 2 so the generating matrix is a 2×5 matrix consisting of two linearly independent vectors in C. For example,

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

There are other solutions possible. As rows of the matrix you can take two any non-zero elements of C.

2. (10 points) Let $C \subset \{0,1\}^8$ be the binary cyclic code of dimension 4 with generating polynomial:

$$g(x) = x^4 + 1.$$

While using the above cyclic code, you receive the transmission $(0,1,1,0,1,1,1,0) \in \{0,1\}^8$. Use the fact that the code is cyclic to show that an error has occurred.

Solution

The element $b = (0,1,1,0,1,1,1,0) \in \{0,1\}^8$ translates to the polynomial

$$b(x) = 0x^7 + x^6 + x^5 + 0x^4 + x^3 + x^2 + x + 0.$$

Then $b \in C$ if and only if $b(x) = g(x)a(x)$ for some polynomial $a(x)$. Since $\deg g(x) = 4$ and $\deg b(x) = 6$ the degree of the polynomial $a(x)$ is would have to be two. Letting $a(x) = x^2 + a_1 x + a_0$ we can attempt to solve for a_1, a_0. $a(x)g(x) = (x^2 + a_1 x + a_0)(x^4 + 1) = x^6 + a_1 x^5 + a_0 x^4 + x^2 + a_1 x + a_0$. It is impossible for a product of the above form to be equal to $b(x)$ since there is no degree 3 term. Therefore, $b(x) \neq g(x)a(x)$ for some $a(x)$, and b is not in C and an error has occurred.

Alternatively, perform polynomial long division and see that a remainder of x^3 is obtained. If a polynomial calculator was used as an aid without explanation of which one, 1 to 2 points were deducted.

Some people used error detection for linear codes (syndromes). I didn't deduct any marks as long as it was done correctly.

3. (10 points) Show that the cyclic code from Problem 3.2 is self-dual, namely that $C = C^\perp$.

Solution

The dual code is defined by

$$C^\perp = \{b \in \{0,1\}^8 \mid b \cdot c = 0 \forall c \in C\}.$$

Firstly, both $\dim C = 4$ and $\dim C^\perp = 8 - \dim C = 4$. Therefore, both codes have the same dimension.

To show that $C \subset C^\perp$ it is sufficient to verify that $b_i \cdot b_j = 0$ for all pairs i, j (possibly equal) where $b_1, \ldots, b_4$ is a basis of C.

(Continued on page 6.)

For a basis of C we can take the vectors $b_1, \dots, b_4$ coming from the polynomials x^4+1, $x(x^4+1)$, $x^2(x^4+1)$, and $x^3(x^4+1)$. These translate to vectors:

$$(0,0,0,1,0,0,0,1),(0,0,1,0,0,0,1,0),(0,1,0,0,0,1,0,0),(1,0,0,0,1,0,0,0)$$

It is easily verified that the inner product of any two distinct vectors above is 0. The inner product of any vector above with itself is also 0 since there are an even number of 1's in each vector.

Now since $\dim C = \dim C^\perp$ the fact that $C \subset C^\perp$ lets us conclude that $|C| = |C^\perp|$ and hence that $C = C^\perp$.

Alternative solution

First find a basis for C exactly in the solution above. There is a description of the parity check matrix H of C from Aigner. The parity check matrix of C is the generating matrix of $C^\perp$. In order to write down the parity check matrix we must perform polynomial division to obtain:

$$x^8 - 1 = (x^4+1)(x^4+1)$$

Writing down a parity check matrix for C using the polynomial $h(x) = x^4 + 1$ following Aigner, gives us a basis $a_1, \dots, a_4$ of $C^\perp$. This basis is exactly the same (up to reordering) as the basis $b_1, \dots, b_4$ found for C above. The two linear codes have equal bases therefore they are the same, $C = C^\perp$.

Grading Some students used a problem from a practice exam which states that the check polynomial of the dual code is related to $h(x)$. I was somewhat ok with this but deducted some marks if the explanations. Some stated that $h(x)$ was the check polynomial, which is not correct. Some marks were deducted for this.

Problem 4

1. (5 points) Solve the discrete logarithm problem

$$3 \equiv 7^x \mod 11$$

for $x \in \{0, 1, \dots, 10\}$.

We know from page 313 of Aigner that 7 is a primitive root mod 11, so the discrete logarithm problem has a solution. We can also use the table from the same page of Aigner where the powers of 7 mod 11 are computed to see that $3 \equiv 7^4 \mod 11$.

Alternatively, we can compute powers of 7 mod 11. Firstly, $7^2 = 49 \equiv 5 \mod 11$, then $7^3 \equiv 5 \cdot 7 \equiv 2 \mod 11$ and $7^4 \equiv 5 \cdot 5 \equiv 3 \mod 11$.

2. (5 points) Find an $a \in \{2, 3, 4\}$ and a $y \in \mathbb{Z}_5$ such that

$$y \equiv a^x \mod 5$$

does not have a unique solution for $x \in \{0, 1, 2, 3\}$.

(Continued on page 7.)

The above discrete logarithm problem has a unique solution whenever a is a primitive root mod 5. In the above list only $a = 4$ is not a primitive root mod 5.

We compute the powers of 4 mod 5 to see that: $4^1 \equiv 4 \mod 5$, $4^3 \equiv 44^2 \equiv 1 \mod 5$, $4^3 \equiv 4 \mod 5$ $4^4 \equiv 1 \mod$ Therefore, $4^2 \equiv 4^4$ mod 5 and the discrete logarithm does not have a unique solution for $a = 4$ and $y = 4$.

Grading There was a typo in the statement that was only corrected with about an hour left of the exam. The typo just made the problem easier to solve. No deductions were made if the easier solution was given as long as it was well explained.

3. (15 points) Alice and Bob exchange encrypted messages using the RSA protocol. However, Eve and Iver set out to interfere with the transmission. Using Alice's public key $n = 187$ and $k = 7$, Bob sends an encrypted message to Alice asking if she wants to meet.

   - First Eve cracks Alice's private key by factoring $n = 187$. Find Alice's private key using the same method as Eve.

     First Eve factors $n = 187 = 11 \cdot 17$. In the notation for RSA we have $p = 11$ and $q = 17$. Alice's public key $k = 7$ is relatively prime to $(p - 1)(q - 1) = 10 \cdot 16 = 160$. Alice's private key is a number g such that $kg \equiv 1 \mod 160$. We can find this by brute force (guessing and checking) or by running the Euclidean algorithm in reverse. We find that $23 \cdot 7 = 161 \equiv 1 \mod 160$. Therefore, Alice's secret key is 23.
   - Using the private key they decode the message, then using Bob's public key $n' = 221$ and $k' = 5$, Iver poses as Alice and encrypts the message "NO" using the encoding $N = 14, O = 15$. What numbers does Iver send to Bob?

   For RSA encryption, Iver must use Bob's public key to encrypt the message by computing $T^{k'} \mod n'$ where T is the text. Therefore, Iver sends the numbers $131, 19$ since:

$$14^5 = 131 \mod 221$$
$$15^5 = 19 \mod 221$$

Problem 5

(10 points) Provide an example of where we borrowed tools from other areas of mathematics (for example, linear algebra, analysis, or abstract algebra) to solve discrete problems. Describe how the theorem/fact/construction borrowed from the other area produced results about discrete objects.

Grading There were many solutions here. Common ones were linear algebra and finite fields. If the solution did not point to why the connections to other fields had about 4 points deducted depending on the quality of the other explanations. Otherwise most solutions received between $8 - 10$ as long as they didn't contain any incorrect statements.