Exam for Discrete Mathematics SF1610 for TCOMK, August 16th, 8:00-13:00,

Examinator: Maurice Duits
Course responsible: Stephanie Ziegenhagen

No books/calculators or other forms of help are allowed.

Grading: : (OBS: the total amount of points in this exam is 37p.)

13 points or more gives the Fx grade
15 points or more are required for the grade E
18 points or more are required for the grade D
22 points or more are required for the grade C
28 points or more are required for the grade B
32 points or more are required for the grade A

Note: For getting the full amount of points a fully motivated solution needs to be given for each exercise.

Part I

Each of the exercises 1 to 5 correspond to the Partial Exam with the same number. For x = 1, 2, 3, 4, 5, if you passed Partial Exam x then you immediately receive 3 points for question x below, and you cannot gain any further points on that question.

1. Solve the equation
$$13x + 9 = 5$$
in $\mathbb{Z}/59\mathbb{Z}$.
Solution: We first rewrite the equation to
$$13x = -4.$$
To solve this in $\mathbb{Z}/59\mathbb{Z}$, we solve the diophantine equation
$$13x + 59y = -4.$$
To determine $\gcd(13, 59)$ we use the Euclidean algorithm:
$$\begin{aligned} 59 &= 4 \cdot 13 + 7 \\ 13 &= 1 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \\ 6 &= 6 \cdot 1, \end{aligned}$$

hence $\gcd(13, 59) = 1$. Since 1 divides -4, the equation has solutions. We backtrack the Euclidean algorithm to write $\gcd(13, 59)$ as a linear combination of 13 and 59 and get

$$\begin{aligned} 1 &= 7 - 6 \\ &= 59 - 4 \cdot 13 - (13 - 1 \cdot 7) \\ &= 59 - 4 \cdot 13 - (13 - (59 - 4 \cdot 13)) \\ &= 2 \cdot 59 + (-9) \cdot 13. \end{aligned}$$

Hence

$$\operatorname{lcm}(13, 59) = 13 \cdot 59,$$

and the set of solutions to the diophantine equation above is given by

$$\{(\frac{-4}{1} \cdot (-9) + 59 \cdot k, \frac{-4}{1} \cdot 2 - 13 \cdot k)\}.$$

Hence precisely the x of the form $x = 36 + 59 \cdot k$ satisfy $13 \cdot x = -4$ modulo 59. In $\mathbb{Z}/59\mathbb{Z}$ we hence have only one solution, namely $x = 36$.

2. (3p) You have 6 different plants (for example a rose, a tulip, a cactus, ...) that you want to plant. You want to plant some of them in the backyard, some in the frontyard and some on your balcony. You want to plant at least one plant in each of these places. Furthermore, the cactus and the tulip should be planted in the same place. How many ways are there to do this? (**Your answer should be an integer**).
Solution: Since the cactus and the tulip have to be planted together, we can pretend that we really only have 5 plants to plant. We divide these 5 different plants into three nonempty piles; there are $S(5, 3)$ ways of doing this. Finally, it makes a difference which pile we plant where, so we multiply with the number of possibilities of assigning three different piles to three different places, namely by 3!. Hence the answer is that there are

$$\begin{aligned} S(5,3) \cdot 3! &= (3 \cdot S(4,3) + S(4,2)) \cdot 3! \\ &= (3 \cdot (3 \cdot S(3,3) + S(3,2)) + 2 \cdot S(3,2) + S(3,1)) \cdot 3! \\ &= (3 \cdot (3 \cdot 1 + S(3,2)) + 2 \cdot S(3,2) + 1) \cdot 3! \\ &= (10 + 5 \cdot S(3,2)) \cdot 3! \\ &= (10 + 5 \cdot (2 \cdot S(2,2) + S(2,1))) \cdot 3! \\ &= (10 + 5 \cdot 3) \cdot 3! \\ &= 25 \cdot 6 \\ &= 150 \end{aligned}$$

possibilities of planting the plants given the requirements.

3. Let π be the permutation

$$\pi = (1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7) \circ (1\ \ 3\ \ 5\ \ 7) \circ (2\ \ 4\ \ 6)$$

of the set $\{1, 2, 3, 4, 5, 6, 7\}$. Write π as a product of disjoint cycles and determine if π is an odd or even permutation.

Solution: We use the algorithm from the lecture to write π as a product of disjoint cycles and get that

$$\pi = (1\ \ 4\ \ 7\ \ 2\ \ 5) \circ (3\ \ 6).$$

Since a k-cycle has sign $(-1)^{k-1}$, the permutation π has sign

$$\operatorname{sgn}(\pi) = (-1)^4 \cdot (-1)^1 = -1$$

and hence π is odd.

4. (a) (1p) Find values $x, y \in \{0, 1\}$ such that

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & x & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & y & 1 \end{pmatrix}$$

is the check matrix for a linear 1-error correcting code C. Explain your choice of x and y.

(b) (1p) For your choice of values for x and y from part (a), determine the length of the code C and the number of words in C.

(c) (1p) For your choice of values for x and y from part (a), determine whether the words v=`001110` and w=`101100` can be corrected to words in C, and correct them if possible and necessary.

Solution:

(a) A check matrix for a 1-error correcting code can't have a zero column, so we have to set $x = 1$. It also can't have twice the same column, so we have to set $y = 1$.

(b) Since the matrix has 6 columns, all codewords have length 6. To find out how many codewords C contains, we calculate the row echelon form of H as

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

Hence H has rank 4, and C contains

$$2^{6-4} = 2^2 = 4$$

codewords.

(c) For the first vector, we have that

$$H \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

Hence v is not a code word, but can be corrected to `001111`. For the second vector, we calculate that

$$H \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Hence w is already a codeword and no correction is necessary.

5. Let G be a connected planar graph with 7 vertices. The degrees of these vertices are $1, 2, 3, 3, 3, 4$ and 4. Determine the number of regions of a planar drawing of G, including the outer region.
Solution: According to Eulers formula we know that

$$v + r = e + 2,$$

where v is the number of vertices of G, while e is the number of edges and r is the number of regions in any planar drawing. We know that $v = 7$, and in any graph the degrees of its vertices add up to $2 \cdot e$, hence we can calculate

$$2 \cdot e = 1 + 2 + 3 + 3 + 3 + 4 + 4 = 20.$$

Hence $e = 10$ and

$$r = e - v + 2 = 10 - 7 + 2 = 5.$$

Part II

6. (4p) Recall that the Fibonacci numbers are defined recursively by $f_0 = 1$, $f_1 = 1$ and

$$f_k = f_{k-1} + f_{k-2} \quad \text{for } k \geq 2.$$

Prove by induction on n that

$$f_n = 1 + f_0 + ... + f_{n-2}$$

for all $n \geq 2$.
Solution:

- Base case: For $n = 2$ we calculate directly:

$$f_2 = f_1 + f_0 = 1 + f_0.$$

Hence the claim holds for $n = 2$.

- Inductive assumption: Assume that there is an $s \geq 2$ such that

$$f_s = 1 + f_0 + ... + f_{s-2}.$$

- Inductive step: We prove that the claim holds for $s+1$ under the inductive assumption: By definition, we know that

$$f_{s+1} = f_s + f_{s-1}.$$

We use the inductive assumption and replace f_s by $1 + f_0 + ... + f_{s-2}$ to get that

$$f_{s+1} = 1 + f_0 + ... + f_{s-2} + f_{s-1}.$$

This is what we wanted to prove.

By induction, the claim is true for all $n \geq 2$.

7. (4p) Consider the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 20.$$

Two solutions to this equation are called different if they differ in at least one position, for example

$$x_1 = 20, x_2 = 0, x_3 = 0, x_4 = 0, x_5 = 0$$

and

$$x_1 = 19, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 0$$

are two different solutions.

(a) (2p) Determine the number of different integer solutions to this equation such that

$$0 \leq x_i \leq 3 \quad \text{for } i = 1, 2, 3$$

and

$$0 \leq x_4 \leq 7.$$

(b) (2p) Determine the number of different integer solutions to this equation such that

$$x_i \geq 1 \quad \text{for } i = 1, 2, 3, 4, 5.$$

(Your answer can contain standard notation from the course.)
Solution:

(a) There are 4 choices for x_1, namely $x_1 = 0, 1, 2, 3$. Given a choice for x_1, there are 4 choices for x_2. Given a choice for x_1 and x_2, there are still 4 choices for x_3, and once we have chosen x_1, x_2 and x_3 we still know that

$$x_1 + x_2 + x_3 \leq 12$$

and hence we have 8 choices for x_4, namely $x_4 = 0, ..., 7$. Once we have chosen x_1, x_2, x_3 and x_4 there is precisely one choice for x_5. By the multiplication priciple, this shows that there are

$$4 \cdot 4 \cdot 4 \cdot 8 = 2^9 = 512$$

different solutions.

(b) Since the only condition we have to fulfill is that $x_i \geq 1$ for all $i = 1, ..., 5$, we can imagine the variables $x_1, ..., x_5$ as 'nonempty labeled piles'. We hence have to count the ways of distributing 20 identical objects among 5 nonempty labeled piles. By the stars and bars principle, this amounts to 'cutting the line of 20 identical objects at 4 places inbetween the objects'. There are 19 spaces between the 20 objects, hence there are

$$\binom{19}{4}$$

ways of doing this.

8. (4p) Determine how many boolean functions f in 3 variables exist satisfying the two conditions

$$\begin{cases} f(x, y, z) \cdot (x + \bar{y} + z \cdot \bar{z}) = 0 & \text{for all } x, y, z, \\ f(x, y, z) + \overline{f(y, x, z)} = 1 & \text{for all } x, y, z. \end{cases}$$

Solution: First of all, note that

$$x + \bar{y} + z \cdot \bar{z} = x + \bar{y} + 0 = x + \bar{y}.$$

We determine the functions satisfying the first equation by looking at the corresponding truth table:

x	y	z	$x + \bar{y}$	$f(x, y, z)$ has to be...
0	0	0	1	0
0	0	1	1	0
0	1	0	0	0 or 1
0	1	1	0	0 or 1
1	0	0	1	0
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

Hence there are only 4 boolean functions satisfying the first condition, namely the following 4 functions f_1, f_2, f_3 and f_4:

x	y	z	$f_1(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

x	y	z	$f_2(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

x	y	z	$f_3(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

x	y	z	$f_4(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

One can check directly that f_1 satisfies the second requirement. The functions f_2, f_3 and f_4 do not satisfy the second requirement, by the following counterexamples:

$$f_2(1,0,1) + \overline{f_2(0,1,1)} = 0 + \bar{1} = 0,$$

$$f_3(1,0,0) + \overline{f_3(0,1,0)} = 0 + \bar{1} = 0,$$

$$f_4(1,0,1) + \overline{f_4(0,1,1)} = 0 + \bar{1} = 0.$$

(Part III is on the last page)

Part III

If in this part you wish to use or refer to a theorem from the course, you must give a statement of the theorem. (Your phrasing does not have to match the phrasing in the course word-for-word.)

9. (5p) Recall that a code C can be defined by specifying a check matrix H: A binary word c is in the code C if and only if

$$H \cdot c = 0$$

(where we interpret c as a column vector, and 0 is a column vector which only contains zeroes). In the lecture we discussed which properties the columns of H should have in order to ensure that C is 1-error-correcting.

   (a) (3p) Which properties should the columns of H fulfill in order to make the associated code C a 2-error-correcting code? (Motivate your answer. Particular weight will be placed on your motivations in your answer to this question.)

   (b) (2p) Construct a 2-error-correcting code with 8 words.

Solution:

(a) A code C is 2-error-correcting if and only if the distance between any two different words c and c' is at least 5, meaning that c and c' have to differ in at least 5 digits. If C is defined by a check matrix, the word `00..0` is always in C. Hence in particular any other word c in C needs to have distance at least 5 to the word `00...0`. In terms of digits that means that any word c which is not `00...0` has to contain at least 5 times the digit 1. Now consider what that means in terms of the check matrix H: Multiplying H with a binary vector x amounts to adding up those columns of H corresponding to the digits of x which are 1. Hence the check matrix H should have the property that there is no word x with only 1,2,3 or 4 digits equal to 1 such that

$$H \cdot x = 0.$$

In terms of columns this means that no 1,2,3 or 4 different columns of H should add up to the zero column vector. We hence have proven:

If C is 2-error-correcting, then the sum of 1,2,3 or 4 different columns of H cannot be zero.

We prove that the converse also holds, i.e. that the following is true:

If the sum of 1,2,3 or 4 different columns of H is never zero, then C is 2-error-correcting.

To see this, suppose that there are 4 different columns of H that add up to zero, say the i-th, j-th, k-th, and l-th column, where i, j, k and l are suitable integers. Consider the vector x which has a 1 as a digit exactly at those positions and a 0 as a digit everywhere else. Then

$$Hx = 0,$$

but the distance between `00...0` and x is 4, hence C is not 2-error-correcting. A similar argument can be made in the cases that 1,2 or 3 columns of H add up to 0.

(b) We know that the number of words in a linear code C determined by a matrix H is given by 2^{l-r}, where l is the number of columns of H (i.e. the length of the code C) and r is the rank of H. Hence if H has full rank, the code C will contain 8 words if H has three more columns than rows. To make sure that H has full rank we can imagine that we start with a matrix of the shape

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 & ? & ? & ? \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & ? & ? & ? \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & ? & ? & ? \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & ? & ? & ? \end{pmatrix}$$

and then try to fill in the three missing column vectors according to our criterion that no 1,2,3 or 4 different columns should add up to 0. One way of doing this is the following, for $l = 15$ and $r = 12$ (smaller examples also exist):

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

10. (5p)

(a) (2p) Let G be a group with identitiy element e. Assume that G has no subgroups other than G and $\{e\}$. Prove that G is a cyclic group.

(b) (3p) For a fixed $n \in \mathbb{N}$ consider $G = (\mathbb{Z}/n\mathbb{Z}, +)$, the group of integers modulo n with addition as group operation. Prove the following:

G has no subgroups besides G and $\{e\}$ if and only if n is a prime number.

(Be very careful with explaining your argument and which definitions and results you use!)
Solution:

(a) We distinguish two cases:

- If G consists of a single element, then $G = \{e\}$ is clearly cyclic and is generated by e.
- If G does not consist of a single element, let $x \in G$ be an element different from the identity element e. Then the subgroup $\langle x \rangle$ generated by x is different from $\{e\}$, because it contains x and $x \neq e$. Since $\langle x \rangle$ is a subgroup of G and there are no subgroups besides G and $\{e\}$, the subgroup $\langle x \rangle$ has to be G itself. Hence G is cyclic and generated by x.

(b) We prove the two 'directions' of the statement seperately:

- We prove indirectly that if G has no subgroups other than G and $\{e\}$, then n is prime: Assume that n is not prime. Hence we can write

$$n = a \cdot b$$

for natural numbers a, b with $a, b \geq 2$. Consider the subgroup $\langle a \rangle$ of $\mathbb{Z}/n\mathbb{Z}$ generated by a: By definition, the cardinality of $\langle a \rangle$ equals the order $\text{ord}(a)$ of a. The order of a is the smallest natural number k with $k \cdot a \equiv 0$ modulo n. We know that $k \neq 1$ since $a < n$, and we know that $b \cdot a = n \equiv 0$ modulo n. Hence the order of a satisfies

$$1 < \text{ord}(a) \leq b < n.$$

Hence $\langle a \rangle$ is a subgroup of G whose cardinality is neither 1 nor n, hence the subgroup $\langle a \rangle$ is neither $\{e\}$ nor G.

- We prove that if n is prime, then G has no subgroups besides $\{e\}$ or G: This follows directly from Lagrange's Theorem, since the cardinality $|H|$ of any subgroup H has to divide the order n of G. Since n is prime, we know that either $|H| = 1$ (in which case $H = \{e\}$) or $|H| = n$ (in which case $H = G$).