Exercise Sheet 1 Combinatorics
2014/15

Ex. 1
Let $\mathrm{ex}(n, C_3)$ denote the maximum number of edges a graph on n vertices can have, without containing a triangle (=cyclic graph of length 3) as a subgraph. Determine $\mathrm{ex}(n, C_3)$ as good as possible.

Ex. 2
Let $\mathrm{ex}(n, C_4)$ denote the maximum number of edges a graph on n vertices can have, without containing a cyclic graph of length 4.
Let p be prime, and let the set of vertices V be $V = \mathbb{Z}_p \times Z_p$. The vertices (x, y) and (x', y') are joined by an edge if $x + x' = yy'$. Show that (x, y) has at least $p - 1$ neighbours. From this, show that $|E| \geq \frac{1}{2}p^2(p-1)$. Show that there is no 4-cycle. (Suppose that (x, y) has two distinct neighbours $(x_1, y_1) \neq (x_2, y_2)$, (say). Show that, by the definition of the edges, y and then also x is uniquely defined.)
Would the same type of proof work if p is not a prime? (if yes, for which other values does it work?, if no, why not?)
Compare the new result on $\mathrm{ex}(n, C_4)$ with the previous ones.

Ex. 3
Given a set of n distinct points $p_1, \ldots p_n \in P$ in the Euclidean plane, and a set of n distinct lines $l_1, \ldots, l_n$. Prove that the number of point-line incidences (p_i, l_j) with $p_i \in l_j$ is $O(n^{3/2})$.
Hint: use the graph theoretic results we studied so far.

Ex. 4
Verify the number theoretic details (Lemma 1.8) of the proof of the Bruck-Ryser-Chowla theorem, see e.g. lecture notes by Simeon Ball, Zsuzsa Weiner, linked to on webpage.

Ex. 5 (Maybe with computer)
Give a list of 4 mutually orthogonal Latin squares of order 5.

Now let $p = 3$. Find an irreducible quadratic polynomial over $\mathbb{F}_3$. From this construct a finite field of 9 elements. (give its addition and multiplication table). From this, maybe with computer, give a list of 8 mutually orthogonal latin squares of order 9.

Ex. 6 (With computer)
Determine the number of Latin squares of order 6, which are essentially distinct. (Think about "normalizing" the Latin squares.) Try to prove: There are no two orthogonal Latin squares of order 6.

[Maybe you should start counting problems which are way too hard and tell me later the result...]
Please cross the problems you did in the Kreuze-system, link at webpage below. Deadline, Tuesday 21st October, 10am.

http://www.math.tugraz.at/∼elsholtz/WWW/lectures/ws14/kombinatorik/vorlesung.html

Please note that by Nawi-regulatations, everybody who takes part in the exercise programme will receive a grade. (Deregistration from the Übungen is possible during October).

Exercise Sheet 2 COMBINATORICS
2014/15

Ex. 7
Study the affine and the projective plane of order 4, i.e. give a list of all lines, and try to visualize them.
(Hint: you have to work with the finite field $\mathbb{F}_4$, not with $\mathbb{Z}_4$).

Ex. 8
A projective space satisfies the following axioms:

P1) For any pair of two points, there is a unique line going through it.

P2) Let p, q, r, s be four distinct points. If the lines pq and rs intrsect, then the lines pr and qs intersect as well.

P3) Each line contains at least three points.

P4) There exist three points, not all on one line.

Further, let V be a vector space of dimension $d \geq 3$ over a field of q elements. Let $U_1(V)$ and $U_2(V)$ denote the one- and two-dimensional subspaces of V. Let $P(V) = (U_1(V), U_2(V), \subseteq)$ denote a geometry, where the points are the one-dimensional subspaces, the lines are the two-dimensional subspaces, with canonical subset-inclusion.
a) Discuss the difference to a projective plane.
b) Prove that $P(V)$ is a projective space.
c) Prove that $P(V)$ is a $2 - (q^{d-1} + q^{d-2} + \cdots + q + 1, q + 1, 1)$ design.

Ex. 9
Study a three-dimensional projective space over $\mathbb{F}_2$, i.e. determine the number of points, lines, and describe the lines. (How do the planes look like? How many are there?)

Ex. 10
Prove the existence of a Hadamard-matrix of order 2^n by verifying the construction below: Let $X = \{1, \ldots, n\}$. Let $S_1, \ldots, S_{2^n}$ be the 2^n subsets of X, (in any order). Define $H = (h_{ij})$ by:

$$h_{ij} = (-1)^{|S_i \cap S_j|}.$$

Ex. 11
a) Prove: if Hadamard matrices of order n_1 and n_2 exist, then a Hadamard matrix of order $n_1 n_2$ exists.

b) Find a Hadamard matrix of order 12.

Ex. 12 (Small excursion to coding theory)
Let C be the set of words of length 8, consisting of all cyclic shifts of the three words below $11010000, 11100100, 10101010$, and of $00000000, 11111111$. (What

is $|C|$?).
a) Show that any two words differ in at least two positions. How many comparisons are required to do this? (The real answer is smaller than the trivial upper bound).
b) Try the following:
b1) either find a set with more than $|C|$ words, where any two elements differ in at least three positions.
b2) or prove that the number $|C|$ is the maximum number with this property.

Exercise Sheet 3 COMBINATORICS
2014/15

Ex. 13
Let $(G, +)$ be a finite abelian group. A family of sets $B_i \subset G$ is called a difference family, if for each $d \in G\backslash\{0\}$ there is a triple (i, b, b') with $i \in \{1, \ldots, s\}$ and $b, b' \in B_i$ such that $d = b - b'$. If $|G| = v$ and $|B_i| = k$, for all i, this is called a (v, k)-difference family.
Prove that $D = (G, B_i + g : g \in G, i \in \{1, \ldots, s\}, \in)$ defines a $2-(v, k, 1)$ design.
Let $v = 18n + 1$. Define
$B_i = \{0, 3i - 2, 4n + 2i\}, i = 1, \ldots, n$
$B_{n+i} = \{0, 3i - 1, 8n + 2i\}, i = 1, \ldots, n$
$B_{2n+i} = \{0, 3i, 6n + 1 + i\}, i = 1, \ldots, n - 1$
$B_{3n} = \{0, 3n, 6n + 1\}$.
Show that this is a $(18n + 1, 3)$-difference family in $(\mathbb{Z}_{18n+1}, +)$.

Ex. 14
Construct a $2 - (21, 3, 1)$ design. Show that there is no such construction based on difference designs.

Ex. 15
Prove the existence of $2 - (6n + 1, 3, 1)$ designs.

Ex. 16
Prove necessary conditions on v for the existence of a $2 - (v, 4, 1)$ design.

Ex. 17
Inform yourself about results of Teirlinck on designs, (e.g. "Non-trivial t-designs without repeated blocks exist for all t")
Inform yourself about results of Betten, Kerber, (and maybe other colleagues from Bayreuth) about t-designs, particularly $t = 6, 7$.
Inform yourself about "Wilson's theorem", (no proof needed...).
Inform yourself abot Peter Keevash very recent result on designs "The existence of designs", (no proof needed...).
(No proofs needed at all, but list a few highlights of the development of modern results on t-designs.)

Ex. 18
Prove that the $2 - (4n - 1, 2n - 1, n - 1)$-design (i.e. a Hadamard design) can be extended to a $3 - (4n, 2n, n - 1)$-design.

Ex. 19
Study Theorem 4.9 of the lecture notes of Anderson and Honkola, (A Short Course in Combinatorial Designs.)
http://www.utu.fi/fi/yksikot/sci/yksikot/mattil/opiskelu/kurssit/Documents/comb2.pdf
Verify (or correct) the details.

Ex. 20
Let C be the (linear) code over $\mathbb{F}_2^8$, defined by all 16 subsums over the 4 rows of the generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$. Prove that 14 words have weight 4, (all words apart from 00000000 and 11111111). Show that these 14 words define a $3-(8,4,1)$ design .

Ex. 21
Let C be the (linear) code $C \subset \mathbb{F}_3^{12}$, defined by all $3^6 = 729$ linear combinations over the 6 rows of the generator matrix

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

Prove (possibly by a computer check) that the minimal non-zero weight (of all codewords) is 6. How many words have weight 6? (Note that they come in pairs, c and $-c$, Now, from this one finds 132 codewords which are the block of a $5-(12,6,1)$ design, the so-called Mathieu 5-design on 12 points. (Using a computer it can be easily tested that each subset of 5 of the 12 positions occurs exactly once).
How often do quadruples, triples, pairs, single elements occur, respectively?

Do these 132 words form an e-error correcting code? If yes, for which e? Is it a perfect code?
Now, delete the first column of G. What does it mean in terms of a code (parity check). Does this give a $4-(11,5,1)$ design? Is the corresponding code perfect?
((For comparison, the quite similar matrix

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

does not work, the minimum (non-zero) weight is 5 etc.))

Exercise Sheet 4 COMBINATORICS
2014/15

Ex. 22
On comet 67P/Churyumov-Gerasimenko there are 100 football clubs in the comet-league. Each pair of clubs plays each other once.
Show that the following is possible:
i) for each $n \in \{0, \ldots, 99\}$ there is one club, winning exactly n times.
ii) for each triple $\{x, y, z\}$ of three clubs there is one other club $c(x, y, z)$ beating x, y and z. (You can try to find an explicit solution, maybe starting with smaller numbers, but this seems complicated.) Complete the following outline: Let's assume that all games are played by tossing a fair coin. Show: the probability that there is some triple $\{x, y, z\}$ such that there is no club beating them all is: $p = \binom{100}{3}(\frac{7}{8})^{97}$. Show that $p < 1$, and think about what this means!

Ex. 23
Revise the notion of group action:
If G is a group and X is a set, then a (left) group action φ of G on X is a function

$$\varphi : G \times X \to X : (g, x) \mapsto \varphi(g, x)$$

that satisfies the following two axioms (where we denote $\varphi(g, x)$ as $g \cdot x$).
1. Compatibility: $(\forall g, h \in G) \quad (\forall x \in X) : (gh) \cdot x = g \cdot (h \cdot x)$.
2. Identity: $\forall x \in X : \quad e \cdot x = x$. (Here, e denotes the identity of the group G.)
(The set X is called a (left) G-set. The group G is said to act on X (on the left)).
Verify that the following examples are group actions:
a) G is an arbitrary group. Conjugation is an action of G on $G: \quad g \cdot x = gxg^{-1}$.
One often writes for the right-action: $x^g = g^{-1}xg$; it satisfies $(x^g)^h = x^{gh}$.
b) The symmetric group S_n and its subgroups act on the set $\{1, \ldots, n\}$ by permuting its elements.

Ex. 24
Determine the cycle index of $S_2, \ldots, S_4$. (Think about the possible cycle types of the permutations).

Ex. 25 (Isaacs, Finite group theory, 1A.8.)
Let G be a finite group, let $n > 0$ be an integer, and let C be the additive group of the integers modulo n. Let Ω be the set of n-tuples $(x_1, x_2, ..., x_n)$ of elements of G such that $x_1 \cdot x_2 \cdots x_n = 1$.
(Here 1 is the identity in G).
(a) Show that C acts on Ω according to the formula $(x_1, x_2, \ldots, x_n) \cdot k = (x_{1+k}, x_{2+k}, \ldots, x_{n+k})$, where $k \in C$ and the subscripts are interpreted modulo n.

(b) Now suppose that $n = p$ is a prime number that divides $|G|$. Show that p divides the number of C-orbits of size 1 on Ω, and deduce that the number of elements of order p in G is congruent to $-1 \mod p$.
Note. In particular, if a prime p divides $|G|$, then G has at least one element of

order p. This is a theorem of Cauchy, and the proof in this problem is due to J. H. McKay. Cauchy's theorem can also be derived as a corollary of Sylow's theorem. Alternatively, a proof of Sylow's theorem can be based on Cauchy's theorem.

Ex. 26
An involution is a map $f : S \to S$ with $f^2 = \mathrm{id}$.
A beautiful example of the power of an involution is here: Don Zagier: A one-sentence proof that every prime $p \equiv 1 \bmod 4$ is a sum of two squares (Amer. Math. Monthly 97 (1990), p. 144).
http://people.mpim-bonn.mpg.de/zagier/files/doi/10.2307/2323918/fulltext.pdf
"The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \to (x, z, y)$ also has a fixed point. $\square$"
Work through it and make sure that you understand all(!) details of the proof. In particular verify the implicitly made claims that the maps are well defined and are involutions.

Ex. 27

a) Use a book or the internet to get information about the 5 Platonic solids. How many faces, edges, corners do these have? How many rotations are there? (which angle, which axis?) Which group is the group of rotations? (No need to prove this here, this is a rather algebraic question).

b) Study the rotations of the dodecahedron. How many are there? How many of these have which order? Use the orbit stabilizer theorem, applied to a) the corners, b) the faces, c) the edges.