The Program of the Spring Colloquium on Discrete Mathematics DSBA

At the beginning of the colloquium, you will take a ticket containing three tasks: a question on understanding definitions, a problem (like a typical problem from seminars and home assignments), and a theorem from the course to be proved. You will have about an hour to prepare your answer. You shall answer orally to one of the examiners, but you shall write your answer during the time for preparation.

The grade for the colloquium is formed as follows. You get your first point as soon as you come to the colloquium, another 2 points for the complete answer to the first question (on understanding the definitions), 3 points for the correct solution of the problem, and the last 4 points for the full proof.

According to the rules of HSE, in the case of detected cheating the student will get 0 points (for the whole colloquium).

1. The List of Definitions

A question on understanding definitions contains a definition (that you shall formulate) and a question on this definition that you shall answer. Example: «Definition of the preimage. Let $f(x) = x^2$ be a function from $\mathbb{Z}$ to $\mathbb{Z}$. Find the preimage of the set $\{1, 2, 3, 4\}$.»

1. Binary relation. Representation via a table and via bipartite graph.
2. Reflexive, symmetric, transitive binary relations
3. Set operations with binary relations and transposition operation.
4. Equivalence relations, classes of equivalence
5. Composition of binary relations
6. Devisability: devisor, quotient, remainder
7. Congruences modulo N
8. Modular arithmetic. Modular multiplicative inverse (modulo N)
9. Fermat's little theorem
10. Totient (Euler's function). Euler's theorem
11. Greatest common divisor. Euclidean algorithm.
12. Extended Euclidean algorithm. Solving linear Diophantine equations with two variables.
13. Prime numbers. Statement of the fundamental theorem of arithmetic.
14. Sets of the same cardinality.
15. Countable set.
16. A set of cardinality continuum.

17. The statement of Schröder-Bernstein theorem (also known as Cantor-Bernstein or Cantor-Bernstein-Schröder theorem).

18. Basic definitions of elementary probability theory: outcomes, probability function, probability space.

19. Basics of elementary probability theory: events, probability of events, rule of sum.

20. The statement of inclusion-exclusion principle (for probabilities).

21. Conditional probability.

22. Independent events. Basic properties.

23. The law of total probability.

24. Random variable. Expectation, linearity property.

25. Markov's inequality.

26. Boolean circuits (general case, arbitrary gates). Graphical representation of boolean circuits.

27. Functional complete basis (set of logical connectivities). Examples of functionally complete and incomplete basises.

28. Zhegalkin polinomial

29. Common basis, $\mathrm{MAJ}(x_1, \ldots, x_n)$.

30. Size of a boolean circuit

31. Big O notation: $f(n) = O(g(n))$. Polynomial circuit.

2. Examples of Problems

Problems from the tickets are similar to the problems below, but not all of them are listed below.

1. Answer the following questions for the binary relation $R \subseteq \{1,2,3\} \times \{1,2,3\}$. Is R reflexive? symmetric? transitive? an equivalence relation? For each relation R draw the corresponding graph. Choose undirected graphs for symmetric relations, in the case of non-reflexive relation use loops.

a) $R = \{(1,2),(2,3),(1,3)\}$

b) $R = \{(1,2),(2,1),(1,1)\}$

c) $R = \{(1,1),(2,2),(3,3)\}$

d) $R = \{(x,y) \mid x,y \in \{1,2,3\}\}$

e) $R = \varnothing$

2. Compute the resulting binary relation. Describe it via math. symbols or in English. Each relation is defined over real numbers.

a) $\overline{(>)}$; **b)** $(>)^{\intercal}$; **c)** $(\geq)\Delta(\leq)$; **d)** $(>) \cap (<)$; **e)** $(=) \circ (>)$; **f)** $(<) \circ (<)$; **g)** $(<) \circ (>)$.

3. Find numbers a, b, c such that $\gcd(ab,c) \neq \gcd(a,c) \cdot \gcd(b,c)$.

4. How many zeroes are there in the tail of decimal representation of the number 16! ?

5. Find the remainder after devision 2^{38} by 37.

6. Find all the solutions of an equation $12x + 19y = 7$ with integer x, y.

7. How many positive divisors of the number 66^{66} are there?

8. A uniform probability space consists of tuples (x_1, x_2, x_3, x_4) of integers $1 \leqslant x_i \leqslant 6$. Find the probability of the event «$x_1 \times x_2 \times x_3 \times x_4$ is even».

9. Give an example of probability space and events A and B such that $\Pr[A \mid B] = \frac{1}{3}\Pr[A]$.

10. Do there exist a probability space and events A an B such that $\Pr[A] = \Pr[B] = \Pr[A \mid B] = 1/2$ and $\Pr[B \mid A] = 1/3$?

11. It is known about events A and B and about a sample space U that $\Pr[A] = \Pr[B] = 4/5$. Can the events $A \cup B$ and B be independent?

12. A uniform probability space consists of tuples (x_1, x_2, x_3, x_4) of integers $1 \leqslant x_i \leqslant 6$. Find the expectation of a random variable $x_1 + x_2 + x_3 + x_4$.

13. Prove that the set of non-intersecting segments $[a,b]$ on a real line is countable.

14. Prove that each infinite set contains infinite number of non-intersecting infinitely countable subsets.

15. Prove that the set of bijections $\mathbb{N} \to \mathbb{N}$ has cardinality continuum.

16. Prove that the set of logical connectivities $\{x_1 \oplus x_2 \oplus x_3,\ x_1 \wedge x_2, 1\}$ is functionally complete.

17. Let a boolean function f have a corresponding boolean circuit of size A and a boolean function g have a corresponding boolean circuit of size B (both in common basis). Prove that there exists a boolean circuit that computes a function $f \oplus g$ of size at most $A + B + 5$.

18. Construct a polynomial circuit that computes MAJ_n.

19. Prove that each monotone boolean function of n variables is computable by a boolean circuit of size $O(n2^n)$ with gates $\{\wedge, \vee\}$.

3. The List of Theorems

1. The main theorem about equivalence relations (part I): if $\sim$ is an equivalence relation on A then the equivalence classes (of $\sim$) form a partition of A.
2. The main theorem about equivalence relations (part II): there exists a bijection between equivalence relations on A and partitions of A.
3. There exists x satisfying congruence $ax \equiv 1 \pmod{N}$ if and only if $\gcd(a, N) = 1$.
4. Euler's theorem.
5. Correctness of Euclidean and extended Euclidean algorithms.
6. Fundamental theorem of arithmetic.
7. Chinese remainder theorem.
8. Properties of Euler's totient function.
9. Any infinite set has an infinitely countable subset. Any subset of a countable set is countable.
10. Countable union of countable sets is countable.
11. Cartesian product of countable sets is countable. The set of rational numbers is countable.
12. Sets $[a, b], [a, b), (a, b], (a, b)$, $[a, +\infty), (a, +\infty), (-\infty, b], (-\infty, b), (-\infty, +\infty)$ are of the same cardinality.
13. The set of (countable) infinite $\{0, 1\}$-sequences is uncountable (Cantor's theorem).
14. Let A and B be events of positive probability. Prove that the following conditions are equivalent: $\mathrm{P}[A \mid B] = \mathrm{P}[A]$, $\mathrm{P}[B \mid A] = \mathrm{P}[B]$, $\mathrm{P}[A \cap B] = \mathrm{P}[A] \times \mathrm{P}[B]$
15. Bayes' Rule. The law of total probability.
16. Equivalence of two definitions of expectation
17. Birthday paradox
18. Lemma: $\min(f) \leqslant \mathrm{E}[f] \leqslant \max(f)$.
19. Markov inequality.
20. Boolean circuit for addition of numbers of linear size.
21. Boolean circuit for multiplication of numbers of quadratic size.
22. Boolean circuit for a graph connectivity testing of size $O(n^4)$.
23. For each boolean function $f(x_1, \ldots, x_n)$ there is a boolean circuit of size $O(n2^n)$.