Ústní část SZZ oboru MIT: neoficiální rozpis témat

David Stanovský, garant oboru MIT *14.5.2019*

Oficiální zkušební okruhy jsou formulovány v karolince a dostupné na webu fakulty. Tento rozpis berte jako informativní. Snažil jsem se o úplný výčet tradičně zkoušených témat, ale mohl jsem na něco zapomenout a je třeba brát v úvahu, že zkouší komise a na důležitost jednotlivých témat mohou mít různí zkoušející různý názor.

Ústní část státní závěrečné zkoušky

Oficiální popis: Zkouška má přehledový charakter. Žádá se, aby posluchač prokázal pochopení základních pojmů, principů a výsledků, byl schopen je ilustrovat na příkladech a předvedl určitou míru syntézy. Ústní část státní závěrečné zkoušky se skládá ze tří tematických okruhů. Z každého tematického okruhu 1-2 dostane student jednu otázku. Z tematického okruhu 3 si student volí jednu z variant 3A nebo 3B, ze které dostane také jednu otázku.

1. tematický okruh: Matematická analýza a lineární algebra.

Oficiální popis: Posloupnosti a řady čísel a funkcí, diferenciální počet, integrální počet. Matice a determinanty, soustavy lineárních rovnic, vektorové prostory, skalární součin, lineární a bilineární formy.

Neoficiální upřesnění:

1. Posloupnosti a řady čísel a funkcí
Limity posloupností a součty řad. Kritéria absolutní a neabsolutní konvergence číselných řad. Stejnoměrná konvergence posloupností a řad funkcí. Mocninné řady.

2. Diferenciální počet
Spojitost a derivace funkcí jedné reálné proměnné. Hlubší věty o spojitých funkcích. Věty o střední hodnotě a jejich důsledky. Vztahy monotonie a znaménka derivace. Konvexita. Taylorův polynom. Taylorovy řady.

3. Integrální počet
Primitivní funkce, určitý integrál. Základní vlastnosti, vztah k primitivní funkci. Metody výpočtu, věty o substituci a integrace per partes. Základní kritéria existence.

4. Matice a determinanty, soustavy lineárních rovnic
Základní pojmy a operace s maticemi a jejich vlastnosti. Hodnost matice. Soustavy lineárních rovnic, Gaussova eliminace, podmínky rešitelnosti. Determinanty a metody jejich výpočtu.

5. Vektorové prostory
Pojem vektorového prostoru, lineární nezávislost, lineární obal, báze a dimenze. Steinitzova věta o výměně. Podprostory a jejich dimenze. Skalární součin, ortogonalizační proces, ortonormální báze. Ortogonální projekce, metoda nejmenších čtverců a pseudoinverze. Diagonalizace a ortogonální diagonalizace. Různé typy rozkladů matic.

6. Lineární a bilineární formy
Lineární, bilineární a kvadratické formy, matice lineárních zobrazení, vlastní čísla lineárních zobrazení a matic, charakteristický polynom. Polární báze a zákon setrvačnosti pro kvadratické formy. Matice jednoduchých geometrických zobrazení.

2. tematický okruh: Algebra.

Oficiální popis: Grupy. Teorie dělitelnosti v komutativních okruzích a speciálně v oborech polynomů, základy teorie těles (včetně konečných).

Neoficiální upřesnění:

1. Grupy
Základní vlastnosti permutací. Příklady grup. Podgrupy, Lagrangeova věta. Homomorfismy, normální podgrupy a faktorgrupy.

2. Komutativní okruhy
Základy dělitelnosti v okruzích, ireducibilní prvky, největší společný dělitel. Gaussovy obory, obory hlavních ideálů, Eukleidovy obory a rozšířený Eukleidův algoritmus.

3. Polynomy
Dělitelnost v okruzích polynomů jedné i více proměnných. Rozklady a kořeny polynomů. Gaussovo lemma. Polynomy více proměnných a afinní variety. Hilbertova věta o bázi.

4. Tělesa
Minimální polynom a stupeň rozšíření. Faktorokruhy. Kořenová a rozkladová rozšíření. Konstrukce a klasifikace konečných těles. Cykličnost konečných multiplikativních grup v tělesech.

3. Výběr jednoho ze dvou tématických okruhů:

Oficiální popis:

3A. Matematika pro informační bezpečnost: Cyklické grupy, základní poznatky teorie čísel, prvočísla. Základní algoritmy počítačové algebry. Samoopravné kódy. Symetrická a asymetrická kryptografie, booleovské funkce, lineární posuvné registry, základní kryptoanalytické útoky.

3B. Počítačová geometrie: Afinní a projektivní geometrie. Bézierovy křivky a plochy, splajny, základní algoritmy geometrického modelování. Diferenciální geometrie křivek a ploch, křivosti. Bezoutova věta. LU-rozklad, QR-rozklad, singulární rozklad.

Neoficiální upřesnění:

1A. Teorie čísel
Struktura cyklické grupy (podgrupy, generátory, endomorfismy a automorfismy). Grupa invertibilních prvků, Eulerova funkce. Rabinův-Millerův algoritmus. Hustota prvočísel.

2A. Počítačová algebra.
Základní operace s celými čísly a polynomy a jejich složitost: násobení, dělení, největší společný dělitel. Diskrétní Fourierova transformace a rychlé násobení polynomů. Algoritmy na Čínskou větu o zbytcích, interpolace.

3A. Samoopravné kódy
Přenos informace, entropie, Shannonova věta. Lineární kódy: Hammingovy kódy, MDS kódy. Hammingův odhad a perfektní kódy. Cyklické kódy a jejich algebraická interpretace.

4A. Kryptologie
Symetrická a asymetrická kryptografie, základní metody, systémy a postupy. Booleovské funkce, algebraický normální tvar, korelace a korelační matice. Lineární posuvné registry a lineární rekurentní posloupnosti. Útoky hrubou silou, diferenční a lineární kryptoanalýza.

1B. Geometrické modelování
Polynomiální a racionální Bézierovy křivky a jejich vlastnosti, DeCasteljau algoritmus, B-spline funkce, Fergusnovy kubiky, Coonsovy pláty.

2B. Diferenciální geometrie
křivost a torze křivky, Frenetovy vzorce, znaménková křivost, první a druhá forma plochy, hlavní křivosti, Gaussova křivost.

3B. Projektivní algebraická geometrie.
Homogenní souřadnice, homogenizace a vztah afinních a projektivních algebraických křivek. Formulace Bézoutovy věty.

4B. Výpočetní aspekty lineární algebry
Algoritmy na výpočet LU-rozkladu, QR-rozkladu, singulárního rozkladu.