Ústní část SZZ oboru MIT: neoficiální rozpis témat

(platné pro SZZ konané od akademického roku 2025/26 do odvolání)

David Stanovský, garant oboru MIT *verze 8.6.2025*

Oficiální popis ústní části: Zkouška má přehledový charakter, jsou kladeny širší otázky a žádá se, aby posluchač prokázal pochopení základních principů, byl schopen je ilustrovat na konkrétních situacích a osvědčil určitou míru syntézy a hlubšího pochopení. Student dostane po jedné otázce z tematických okruhů 1., 2. a 3., přičemž u okruhů 2., 3. bude otázka zpravidla zahrnovat teorii i nějaké výpočetní aspekty.

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. Pod konkrétním heslem (např. „Struktura cyklických grup“) se typicky rozumí znalost celé stejnojmenné sekce z příslušného učebního materiálu, včetně důkazů, příkladů a základních početních úloh. Očekáváme, že krátké důkazy („rozepiš definice a je to vidět“) student předvede na požádání, a u těch složitějších umí vypíchnout principy, na kterých důkaz stojí.

1. Matematická analýza, geometrie a pravděpodobnost

Oficiální popis:
- Diferenciální a integrální počet funkcí jedné proměnné, diferenciální počet funkcí více proměnných
- Diferenciální geometrie rovinných a prostorových křivek, reprezentace křivek v geometrickém modelování.
- Základy teorie pravděpodobnosti: podmíněná pravděpodobnost, náhodné veličiny a jejich rozdělení, zákon velkých čísel. Entropie náhodné veličiny, vztah entropie a délky kódu, kapacita kanálu.

Neoficiální upřesnění:

1. Diferenciální a integrální počet *[Matematická analýza 1, 2, 3]*
Derivace funkcí jedné reálné proměnné a její vlastnosti. Průběh funkce, vztahy monotonie a znaménka derivace, konvexita a druhá derivace. Taylorův polynom. Primitivní funkce a její výpočet, Newtonův a Riemannův integrál a jejich vztah. Parciální derivace a derivace zobrazení z R^n do R^m, gradient, Jacobiho matice, derivace složeného zobrazení.

2. Geometrie křivek. *[Geometrie 1, Geometrické modelování]*
Diferenciální geometrie křivek: rovinné a prostorové křivky, křivost a znaménková křivost, torze, Frenetovy vzorce, křivkový integrál prvního a druhého druhu. Základy geometrického modelování: polynomiální a racionální Bézierovy křivky a jejich vlastnosti, Fergusonovy kubiky a Hermitova interpolace, B-spline křivky.

3. Základy teorie pravděpodobnosti a informace *[Pravděpodobnost, Teorie informace]*
Pravděpodobnostní prostor. Podmíněná pravděpodobnost, Bayesův vzorec, nezávislost. Náhodné veličiny a jejich rozdělení, základní příklady rozdělení. Charakteristiky náhodných veličin (střední hodnota, rozptyl). Čebyševova nerovnost a slabý zákon velkých čísel. Entropie náhodné veličiny a její vztah k informačnímu obsahu, entropie za podmínky a vzájemná entropie a jejich vztah. Vztah entropie a délky kódu, Shannonův kód. Kapacita kanálu a přenosová rychlost.

2. Lineární algebra a její výpočetní aspekty

Oficiální popis:
- Soustavy lineárních rovnic, eliminační metoda, LU rozklad, iterační metody, numerické aspekty. Maticový počet a determinant.

- Základní algebraické vlastnosti vektorových prostorů. Lineární zobrazení a jejich matice, vlastní čísla a diagonalizace. Aproximace vlastních čísel.
- Prostory se skalárním součinem. Ortogonalizace, QR a SVD rozklad, numerické aspekty výpočtu. Problém nejmenších čtverců a jeho numerické řešení. Ortogonální matice a izometrie.
- Interpolace, diskrétní Fourierova transformace a efektivní algoritmy, aplikace v kryptografii.

Neoficiální upřesnění:

1. Soustavy lineárních rovnic a maticový počet *[Lineární algebra 1, Numerická lineární algebra]*.
Soustavy lineárních rovnic, podmínky řešitelnosti. Gaussova eliminace a LU rozklad, řádové výpočetní náklady, pivotace a numerická stabilita. Stacionární iterační metody pro soustavy lineárních rovnic, konvergence. Základní maticové operace, hodnost matice, výpočet inverzní matice. Determinanty a metody jejich výpočtu, Cramerovo pravidlo.

2. Vektorové prostory *[Lineární algebra 1]*
Pojem vektorového prostoru, lineární nezávislost, lineární obal, báze a dimenze. Steinitzova věta o výměně. Věta o dimenzi součtu a průniku.

3. Lineární zobrazení *[Lineární algebra 1, 2, Numerická lineární algebra]*
Lineární zobrazení a jejich matice, matice základních geometrických zobrazení. Věta o dimenzi jádra a obrazu. Vlastní čísla lineárních zobrazení a matic, algebraická a geometrická násobnost, charakterizace diagonalizovatelných matic. Iterační metody pro řešení částečného a úplného problému vlastních čísel.

4. Prostory se skalárním součinem *[Lineární algebra 2, Numerická lineární algebra, Geometrie 1]*
Vektorové prostory se skalárním součinem, ortogonální projekce, ortogonalizační proces. QR a SVD rozklad matice a metody jeho výpočtu, výpočetní náklady a numerická stabilita. Schurova věta a Schurův rozklad. Využití rozkladů pro řešení soustav lineárních rovnic a problému nejmenších čtverců. Ortogonální matice a izometrie v Eukleidovském prostoru R^n.

5. Interpolace *[Numerická lineární algebra, Počítačová algebra, Úvod do kryptografie]*
Věta o interpolaci. Diskrétní Fourierova transformace, rychlá Fourierova transformace - algoritmus a jeho složitost, aplikace na rychlé násobení polynomů. Shamirovo schéma sdílení tajemství.

3. Obecná algebra a její výpočetní aspekty

Oficiální popis:
- Základy teorie grup, struktura cyklických grup. Základní kryptografické protokoly založené na vlastnostech grup a elementární teorii čísel.
- Klasifikace oborů z hlediska dělitelnosti, Eukleidův algoritmus a jeho složitost.
- Algebraické vlastnosti okruhů polynomů jedné i více proměnných, základní pojmy algebraické geometrie.
- Tělesová rozšíření konečného stupně, rozkladová nadtělesa, klasifikace konečných těles.

Neoficiální upřesnění:

1. Grupy *[Algebra, Úvod do kryptografie]*
Pojem grupy, příklady. Podgrupy, generátory a Lagrangeova věta. Struktura cyklických grup a věta o primitivním prvku (multiplikativní grupy konečných těles jsou cyklické), problém diskrétního logaritmu a jeho využití v kryptografii: Schnorrova grupa a její generátor, Diffie-Hellmanův protokol, Schnorrovo identifikační a podpisové schéma. Eulerova věta a protokol RSA.

2. Dělitelnost v oborech integrity *[Algebra]*
Rozšířený Eukleidův algoritmus, složitost Eukleidova algoritmu v oboru celých čísel. Gaussovské obory, eukleidovské obory, obory hlavních ideálů, vztahy mezi těmito třídami, příklady a protipříklady. Charakterizace gaussovských oborů (ireducibilní rozklady vs. existence NSD).

3. Obory polynomů *[Algebra, Úvod do komutativní algebry, Počítačová algebra]*
Polynomiální okruhy jedné i více proměnných: základní vlastnosti z hlediska dělitelnosti, Gaussova věta.

Hilbertova věta o bázi. Čínská věta o zbytcích pro čísla a polynomy, včetně metod výpočtu. Základní pojmy algebraické geometrie: IV-korespondence a Hilbertova věta o nulách.

4. Tělesová rozšíření *[Algebra]*
Faktorokruhy a konstrukce těles. Minimální polynom a stupeň jednoduchého rozšíření. Existence a jednoznačnost rozkladových nadtěles. Klasifikace konečných těles.