

**Rozhodnutí děkana FIT č. 13/2018:**  
**Tematické okruhy pro ústní část státní závěrečné zkoušky**  
**v navazujícím magisterském studijním programu**  
**Informační technologie na FIT VUT v Brně**  
**pro akademický rok 2017/18**

**Obor Bioinformatika a biocomputing – MBI**

1. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
2. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
3. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
4. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
5. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
6. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
7. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
8. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
9. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
10. Orientované grafy (orientované sledy, souvislost a silná souvislost, turnaje, eulerovské a hamiltonovské grafy, Dijkstrův a Floyd-Warshallův algoritmus pro hledání cesty minimální délky).
11. Základní pojmy molekulární genetiky: genetická informace, gen, genetický kód.
12. Struktura a funkce genomů prokaryot, eukaryot a virů.
13. Transkripce genů a posttranskripční úpravy.
14. Translace a posttranslační úpravy.
15. Základní principy regulace genové exprese.
16. Změny genetické informace: mutace, rekombinace, reparace DNA, transpozice.
17. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
18. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
19. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
20. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
21. Transformace a normální formy bezkontextových gramatik.
22. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
23. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
24. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
25. Parciální rekurzivní funkce.
26. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
27. Zarovnání sekvencí (dynamického programování, BLAST).
28. Vícenásobné zarovnání sekvencí (dynamické programování, CLUSTAL).
29. Konstrukce fylogenetických stromů (metody založené na vzdálenosti, metody založené na znacích, maximum likelihood).

30. Metody sekvenace DNA a sestavování fragmentů.
31. Rozpoznávání genů (statistické metody, skryté Markovovy modely).
32. Predikce struktury proteinů (struktura proteinů, predikce elementů sekundární struktury, predikce celkového tvaru proteinů).
33. Predikce struktury RNA (strukturní elementy v RNA, Nussinin algoritmus, další metody predikce struktury RNA).
34. Entropie ve fyzice a informatice, emergence, chaotický systém, disipativní struktura.
35. Rekonfigurovatelná výpočetní zařízení pro evolvable hardware (požadavky, princip funkce).
36. Evoluční návrh a evoluční optimalizace (typické algoritmy, aplikace, způsob vyhodnocení experimentů).
37. Kartézské genetické programování (reprezentace problému, prohledávací algoritmus, fitness funkce).
38. Evoluční návrh obvodů (fitness funkce, problém škálovatelnosti a jeho řešení).
39. Výpočetní development (princip, modely), celulární automaty (v 1D a 2D, Wolframovy třídy, sebepublikace).
40. DNA počítače (Adlemanův experiment, SAT problém, důsledky pro informatiku).
41. Klasifikace a vlastnosti paralelních a distribuovaných architektur.
42. Základní typy topologií paralelních a distribuovaných architektur a jejich vlastnosti.
43. Distribuované a paralelní algoritmy - algoritmy řazení, select.
44. Distribuované a paralelní algoritmy - algoritmy vyhledávání.
45. Model PRAM, suma prefixů a její aplikace.
46. Distribuované a paralelní algoritmy - algoritmy nad seznamy, stromy a grafy.
47. Interakce mezi procesy a typické problémy paralelismu (synchronizační a komunikační mechanismy).
48. Distribuované a paralelní algoritmy - předávání zpráv a knihovny pro paralelní zpracování (MPI).
49. Distribuovaný broadcast, synchronizace v distribuovaných systémech.
50. Informace o genomech (sekvence, anotace) a související výpočetní nástroje.
51. Závislost tvorby duplexů DNA a struktur RNA na sekvenci a teplotě a související algoritmy a nástroje.
52. Popis funkce genových produktů ("Gene Ontology") a související výpočetní nástroje.
53. Biologické sekvence pohledem statistiky, pravděpodobnosti, informační teorie a strojového učení.
54. Bayesovské sítě (princip, exaktní inference, přibližná inference).
55. Hrubé množiny (definice, aproximační prostory).
56. Neuronové sítě: Hopfieldova, Kohonenova, RCE, LVQ, ART (učení, odezva, možné aplikace).
57. Neuronové sítě: Back-propagation, Boltzmannův stroj, konvoluční sítě (učení, odezva, možné aplikace).
58. Fuzzy množiny a fuzzy logika. Fuzzy řízení (fuzzyfikace, inference, defuzzyfikace).
59. Předzpracování dat v procesu získávání znalostí (popisné charakteristiky dat; metody čištění; normalizace a redukce dat).
60. Dolování asociačních pravidel (pojmy frekventovaná množina; asociační pravidlo; podpora; spolehlivost; algoritmy pro dolování asociačních pravidel).
61. Dolování textu (základní charakteristika, předzpracování textových dokumentů a jejich reprezentace; vyhledávání informací).
62. Klasifikace a predikce (princip a fáze klasifikace; rozdíl mezi klasifikací a predikcí; princip klasifikace rozhodovacím stromem, bayesovské naivní klasifikace, klasifikace neuronovou sítí, lineární regrese, nelineární regrese).
63. Shluková analýza (Princip shlukové analýzy; vzdálenostní funkce; princip rozdělovacích metod k-means a k-medoids, princip hierarchických metod; princip metod založených na hustotě).
64. Dolování v netradičních datech (v proudu dat, sekvencích, grafech - specifika a přístupy k řešení).

## Obor Bezpečnost informačních technologií - MBS

1. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
2. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
3. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
4. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
5. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
6. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
7. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
8. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
9. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
10. Orientované grafy (orientované sledy, souvislost a silná souvislost, turnaje, eulerovské a hamiltonovské grafy, Dijkstrův a Floyd-Warshallův algoritmus pro hledání cesty minimální délky).
11. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
12. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
13. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
14. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
15. Transformace a normální formy bezkontextových gramatik.
16. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
17. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
18. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
19. Parciální rekurzivní funkce.
20. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
21. Lambda kalkul (definice všech pojmů, operací...).
22. Práce v lambda kalkulu (reprezentace čísel a pravdivostních hodnot a operací nad nimi).
23. Haskell - lazy evaluation (typy v jazyce včetně akcí, význam typových tříd, demonstrace lazy evaluation).
24. Prolog - způsob vyhodnocení (základní princip, unifikace, chování vestavěných predikátů, operátor řezu - vhodné a nevhodné užití).
25. Prolog - změna DB/programu za běhu (demonstrace na prohledávání stavového prostoru, práce se seznamy).
26. Klasifikace metod komprese dat (ztrátové, bezztrátové, intuitivní, algoritmické, četnost výskytu, pravděpodobnost výskytu), princip kódování délek sledů, kódování "přesuň na začátek."
27. Kódy s proměnnou délkou - princip, zdůvodnění, Huffmanovy kódy - různé typy, kanonický Huffmanův kód, adaptivní Huffmanův kód, aritmetický kód.
28. Slovníkové metody (LZ77, LZ78, práce se slovníkem, pohyblivé okno, prodlužování položek).
29. Základní funkce směrovače, zpracování paketů ve směrovači, typy přepínání a architektury.
30. Formální metody v počítačových sítích: modelování protokolů pomocí konečných automatů a temporálních logik.
31. Řízení toku dat (flow-control) a prevence zahlcení (congestion-control) na transportní vrstvě (MP-TCP, QUIC, SCTP, DCCP).
32. Identifikace síťového provozu (signatury, statistické metody), důvěra na Internetu (reputační systémy).
33. Sítě Peer-to-Peer: vlastnosti, chování, způsoby směrování. Strukturované a nestrukturované sítě.
34. Distribuované a paralelní algoritmy - algoritmy řazení, select.

35. Distribuované a paralelní algoritmy - algoritmy vyhledávání.
36. Model PRAM, suma prefixů a její aplikace.
37. Distribuované a paralelní algoritmy - algoritmy nad seznamy, stromy a grafy.
38. Distribuované a paralelní algoritmy - předávání zpráv a knihovny pro paralelní zpracování (MPI).
39. Distribuovaný broadcast, synchronizace v distribuovaných systémech.
40. Hodnocení spolehlivosti biometrických systémů (chybové míry, metriky apod.).
41. Rozpoznávání otisků prstů (předzpracování, metody, markanty, třídy apod.).
42. Metody detekce živosti na prstech.
43. Rozpoznávání 2D/3D geometrie ruky (předzpracování, metody apod.).
44. Rozpoznávání duhovky a sítnice oka (předzpracování, metody apod.).
45. Rozpoznávání 2D/3D obličeje a termogramů obličeje (předzpracování, metody apod.).
46. Rozpoznávání dynamických vlastností člověka (dynamika stisku kláves, chůze apod.).
47. Rozpoznávání podpisu (předzpracování, metody apod.).
48. Rozpoznávání DNA (metody, extrahované rysy apod.).
49. Klasická kryptografie, substituční a transpoziční šifry, rotorové stroje.
50. Symetrická kryptografie. Vlastnosti, vlastnosti bezpečného algoritmu, délka klíče, útok silou, příklady symetrických algoritmů, Feistelovy šifry, DES, režimy činnosti, proudové šifry.
51. Asymetrická kryptografie, vlastnosti, způsoby použití, poskytované bezpečnostní funkce, elektronický podpis a jeho vlastnosti, hybridní kryptografie, algoritmus RSA, generování klíčů, šifrování, dešifrování.
52. Hašovací funkce, klíčovaný haš a MAC a jejich použití a vlastnosti.
53. Správa klíčů v asymetrické kryptografii (certifikáty X.509).
54. Správa a distribuce klíčů v symetrické kryptografii (KDC, KTC a navazující protokoly).
55. Řízení přístupu k síti (bezpečnostní politika, AAA, RADIUS, TACACS+, 802.1x, Kerberos, OTP).
56. Bezpečnost v operačních systémech (správa OS, ACL, Audit, BSM, MAC, Capabilities).
57. Systémy IDS a IPS, signatury.
58. Útoky v počítačových sítích a ochrana před nimi (útoky na DHCP, ARP, tabulku CAM).
59. Zabezpečení síťové komunikace pomocí VPN.
60. Hrozby, slabá místa, aktiva, škodlivý software (malware), funkce prosazující bezpečnost (řízení přístupu, autentizace, skryté kanály, audit, přenos dat).
61. Kritéria hodnocení bezpečnosti informačních systémů, historie, kritéria CC (Common Criteria), standardy pro management bezpečnosti.
62. Analýza rizik bezpečnosti informačních systémů (vstupy, výstupy, jednotlivé generace).
63. Bezpečnost webových aplikací, typické útoky.
64. Bezpečnost bezdrátových sítí, útoky, způsoby kryptografického zabezpečení.
65. Objektově-orientované databázové systémy - kolekce a struktura, objekt, dědičnost, vztahy, role, systém Cache, architektura Java Enterprise Edition.

## Obor Počítačová grafika a multimédia - MGM

1. Metodika návrhu HW/SW codesign, platformy, programovatelné obvody.
2. Výpočetní modely (StateCharts, Kahnova síť procesů, synchronní dataflow).
3. Specifikace (chování, struktura), syntéza (alokace, přidělení, plánování) a integrace systémů (rozhraní, synchronizace, komunikace).
4. Syntéza HW z vyšších programovacích jazyků (reprezentace, alokace, plánování, přiřazení) a jazyk Catapult C.
5. Odhady (přesnost, věrnost, metriky, metody) a optimalizace vlastností systému (příkon, energie).
6. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
7. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
8. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
9. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
10. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
11. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
12. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
13. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
14. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
15. Orientované grafy (orientované sledy, souvislost a silná souvislost, turnaje, eulerovské a hamiltonovské grafy, Dijkstrův a Floyd-Warshallův algoritmus pro hledání cesty minimální délky).
16. Postrelační SRBD (definice, vymezení problematiky a specifik pro O-R, prostorové, temporální, XML a deduktivní DB).
17. Metody indexování bodových a plošných útvarů - typicky obalujících hyperobdélníků - v prostorových DB (principy, metody, postupy, ke každé třídě typický algoritmus, minimálně (adaptivní) kD strom, Grid File, R strom, R+ strom).
18. Temporální DB (modely času, generičnost dotazu a shlukování, [integritní] omezení v historii).
19. Objektově-relační databáze (charakteristika, porovnání s relačními, podpora v SQL:1999 a SQL:2003).
20. XML databáze (typy XML dokumentů, klasifikace úrovně podpory, XML typ v SQL a jeho použití).
21. Grafická knihovna OpenGL: vykreslovací řetězec (funkční bloky, možnosti nastavení), frame buffer, stencil buffer.
22. Afinní 3D transformace, kamera, projekce, skládání transformací.
23. Osvětlení: způsob výpočtu, osvětlovací modely, stínování, materiály.
24. Realistické zobrazování: metoda sledování paprsku, radiozita, distribuované sledování paprsku, sledování cest.
25. Textury a texturování: texturování, MIP mapping, procedurální textury, mřížkové šумы.
26. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
27. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
28. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
29. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
30. Transformace a normální formy bezkontextových gramatik.
31. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
32. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
33. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
34. Parciální rekurzivní funkce.
35. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).

36. Interference světla (skládání dvou a více koherentních vln, intenzita složené vlny, interferenční člen, konstruktivní a destruktivní interference, princip interferometru).
37. Difrakce světla (rozložení intenzity světla za obdélníkovou a kruhovou šěrbinou, Airyho obrazec, rozlišovací schopnost optických přístrojů, oka).
38. Polarizace světla (přirozené a lineárně polarizované světlo, polarizační rovina, způsoby polarizace světla, elipticky polarizované světlo, polarizační filtry).
39. Holografie a laser (holografický kód, jeho dekódování, mimooosový hologram, objemový hologram, vztah holografie a laseru).
40. Vztah zpracování signálu a multimédií (proč je zpracování zvukového a obrazového signálu pro multimédia důležité, typické operace při zpracování zvukového a obrazového signálu).
41. Komprese zvuku (základní postupy při kompresi zvuku, jak se liší od obecné komprese dat, vztah k vlastnostem lidského sluchu, dosahovaný kompresní poměr).
42. Komprese obrazu (základní postupy při kompresi obrazu, jak se liší od obecné komprese dat, vztah k vlastnostem lidského zraku, dosahovaný kompresní poměr).
43. Komprese videosekvencí (základní postupy při kompresi videa, jak se liší od komprese obrazu a od obecné komprese dat, vlastnosti a dosahovaný, kompresní poměr).
44. Informace a entropie, Shannova věta o kódování.
45. Bezpečnostní kódy: lineární, Hammingovy, cyklické. Detekce a oprava chyb.
46. Základní architektury přepínačů, algoritmy pro plánování, řešení blokování, vícestupňové přepínací sítě.
47. Základní funkce směrovače, zpracování paketů ve směrovači, typy architektur.
48. Formální metody v počítačových sítích: modelování protokolů pomocí konečných automatů a temporálních logik.
49. Obrazová data, jejich pořizování a možná poškození (možné reprezentace obrazu, obrazové snímáčí čipy a zařízení, jejich vlastnosti, vady pořízeného obrazu, šumy, optimální filtrace obrazu).
50. Transformace obrazu (jaké transformace se používají při zpracování obrazu, typické příklady a důvody použití transformací při zpracování obrazu).
51. Filtrace obrazu (definice lineární filtrace, typické příklady použití filtrů, použití rychlé konvoluce s využitím FFT, návrh lineárních filtrů, nelineární filtrace).
52. Vodoznaky (watermarks) a jejich využití (vymezení pojmu vodoznak, základní principy a vlastnosti vodoznaků, typické příklady využití a vlastností vodoznaků).
53. Detekce hran, segmentace (vymezení pojmů detekce hran a segmentace, možné aplikace jednotlivých algoritmů a jejich důvody, typické případy nasazení algoritmů).
54. Cepstrum (definice, způsoby výpočtu, Mel-frekvenční cepstrální koeficienty).
55. Lineární predikce (podstata, výpočet parametrů LP filtru, použití lineární predikce).
56. Určení základního tónu (podstata, autokorelace, normalizovaná cross-korelace, metody zlepšení přesnosti).
57. Kódování: waveform (podstata, DPCM), vokodéry, hybridní kodéry (podstata, vektorové kvantování, analýza syntézou, CELP).
58. Rozpoznávání DTW (variabilita v rozpoznávání řeči, lokální vzdálenost, částečná kumulovaná vzdálenost, DTW cesta).
59. Rozpoznávání HMM (architektura, přechodová pravděpodobnost, funkce hustoty pravděpodobnosti ve stavech, sekvence stavů, pravděpodobnost promluvy přes sekvenci stavů, Baum-Welch, Viterbi, podstata trénování).
60. Standardy pro rychlé vykreslování na GPU (OpenGL, Direct3D, Vulkan) - charakteristiky, srovnání, důležité verze.
61. Důležité knihovny pro práci s grafem 3D scény.
62. Standardy ukládání obrazů, 3D objektů a scén - rozdělení podle účelu, důležití zástupci, moderní trendy.
63. Standardy a knihovny ve zpracování videa - standardy kódování, důležité knihovny a nástroje.
64. MIDI a rozhraní pro profesionální práci se zvukem v reálném čase.

## Obor Inteligentní systémy - MIN

1. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
2. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
3. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
4. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
5. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
6. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
7. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
8. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
9. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
10. Orientované grafy (orientované sledy, souvislost a silná souvislost, turnaje, eulerovské a hamiltonovské grafy, Dijkstrův a Floyd-Warshallův algoritmus pro hledání cesty minimální délky).
11. Bayesovské sítě (exaktní inference, přibližná inference).
12. Hrubé množiny (dolní a horní aproximace, pozitivní, negativní a hraniční oblast).
13. Chaos (chaotické řešení, bifurkace, Mandelbrotova množina a Juliovy množiny).
14. Neuronové sítě: Hopfieldova, Kohonenova, RCE, LVQ, ART (učení, odezva, možné aplikace).
15. Vícevrstvé dopředné neuronové sítě Madaline a Back-propagation (učení, odezva, možné aplikace).
16. Genetický algoritmus (ohodnocení jedinců, výběr rodičů, rekombinace, mutace, tvorba nové populace).
17. Optimalizační algoritmy ACO a PSO (základní principy).
18. Fuzzy množiny a fuzzy logika. Fuzzy řízení (fuzzyfikace, inference, defuzzyfikace).
19. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
20. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
21. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
22. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
23. Transformace a normální formy bezkontextových gramatik.
24. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
25. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
26. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
27. Parciální rekurzivní funkce.
28. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
29. Základy argumentace. Argumentační systém a určování přípustných argumentů.
30. Racionální umělý agent, reaktivní agent a agent řízený záměrem.
31. Programování BDI agentů v systémech AgentSpeak(L).
32. Syntaxe a sémantika agentních komunikačních jazyků KQML a ACL.
33. Agentně-orientované programování, systém Agent-0.
34. Abstraktní agentní architektura FIPA, její struktura a funkčnost.
35. Lambda kalkul (definice všech pojmů, operací...).
36. Práce v lambda kalkulu (reprezentace čísel a pravdivostních hodnot a operací nad nimi).
37. Haskell - lazy evaluation (typy v jazyce včetně akcí, význam typových tříd, demonstrace lazy evaluation).

38. Prolog - způsob vyhodnocení (základní princip, unifikace, chování vestavěných predikátů, operátor řezu - vhodné a nevhodné užití).
39. Prolog - změna DB/programu za běhu (demonstrace na prohledávání stavového prostoru, práce se seznamy).
40. Základní typy topologií paralelních a distribuovaných architektur a jejich vlastnosti.
41. Distribuované a paralelní algoritmy - algoritmy řazení, select.
42. Distribuované a paralelní algoritmy - algoritmy vyhledávání.
43. Model PRAM, suma prefixů a její aplikace.
44. Distribuované a paralelní algoritmy - algoritmy nad seznamy, stromy a grafy.
45. Interakce mezi procesy a typické problémy paralelismu (synchronizační a komunikační mechanismy).
46. Distribuované a paralelní algoritmy - předávání zpráv a knihovny pro paralelní zpracování (MPI).
47. Distribuovaný broadcast, synchronizace v distribuovaných systémech.
48. Teorie modelování a simulace, formalismus DEVS (atomický DEVS, DEVN).
49. Modelování diskrétních systémů (procesy, události, celulární automaty).
50. Modelování spojitých systémů (bloková schémata, rovnice, numerické metody a jejich vlastnosti).
51. Modelování kombinovaných systémů (stavové podmínky a stavové události).
52. Bezdrátový přenos dat, kmitočty a plánování, antény, šíření signálu.
53. Systémy mobilní komunikace - GSM, GPRS, HSCSD, EDGE, UMTS, DECT, LTE.
54. Satelitní komunikační systémy.
55. Bezdrátové lokální sítě (Wifi, Bluetooth).
56. Lokalizační systémy GPS.
57. Markovský rozhodovací proces s odměnami, dynamické programování, učení.
58. Distribuované řídicí systémy, SCADA, internet věcí.
59. Předzpracování dat v procesu získávání znalostí (popisné charakteristiky dat; metody čištění; normalizace a redukce dat).
60. Dolování asociačních pravidel (pojmy frekventovaná množina; asociační pravidlo; podpora; spolehlivost; algoritmy pro dolování asociačních pravidel).
61. Dolování textu (základní charakteristika, předzpracování textových dokumentů a jejich reprezentace; vyhledávání informací).
62. Klasifikace a predikce (princip a fáze klasifikace; rozdíl mezi klasifikací a predikcí; princip klasifikace rozhodovacím stromem, bayesovské naivní klasifikace, klasifikace neuronovou sítí, lineární regrese, nelineární regrese).
63. Shluková analýza (Princip shlukové analýzy; vzdálenostní funkce; princip rozdělovacích metod k-means a k-medoids, princip hierarchických metod; princip metod založených na hustotě).
64. Klasifikace Petriho sítí.
65. Metody analýzy C/E a P/T Petriho sítí.



# Obor Informační systémy - MIS

1. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
2. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
3. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
4. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
5. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
6. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
7. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
8. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
9. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
10. Orientované grafy (orientované sledy, souvislost a silná souvislost, turnaje, eulerovské a hamiltonovské grafy, Dijkstrův a Floyd-Warshallův algoritmus pro hledání cesty minimální délky).
11. Postrelační SRBD (definice, vymezení problematiky a specifik pro O-R, prostorové, temporální, XML a deduktivní DB).
12. Metody indexování bodových a plošných útvarů - typicky obalujících hyperobdélníků - v prostorových DB (principy, metody, postupy, ke každé třídě typický algoritmus, minimálně (adaptivní) kD strom, Grid File, R strom, R+ strom).
13. Temporální DB (modely času, generičnost dotazu a shlukování, [integritní] omezení v historii).
14. Objektově-relační databáze (charakteristika, porovnání s relačními, podpora v SQL:1999 a SQL:2003).
15. XML databáze (typy XML dokumentů, klasifikace úrovně podpory, XML typ v SQL a jeho použití).
16. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
17. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
18. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
19. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
20. Transformace a normální formy bezkontextových gramatik.
21. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
22. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
23. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
24. Parciální rekurzivní funkce.
25. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
26. Lambda kalkul (definice všech pojmů, operací...).
27. Haskell - lazy evaluation (typy v jazyce včetně akcí, význam typových tříd, demonstrace lazy evaluation).
28. Prolog - způsob vyhodnocení (základní princip, unifikace, chování vestavěných predikátů, operátor řezu - vhodné a nevhodné užití).
29. Management času a nákladů v rámci projektů (procesy, metody, metoda kritické cesty CPM - Critical Path Method, metoda odhadu pracnosti FPA - Function Point Analysis, řízení dosažené hodnoty projektu EVM - Earned Value Management, prognózování).
30. Management kvality v rámci projektu (procesy, metody, Paretova analýza, diagram příčin a účinků, kvalitativní charakteristiky softwarových produktů).
31. Management rizik v rámci projektů (procesy, metody, rozhodovací strom, matice pravděpodobnosti a dopadu, analýza očekávané peněžní hodnoty, kategorie rizik v projektech IT, eliminace rizik v softwarových projektech).
32. Základní architektury prepínačů, algoritmy pro plánování, řešení blokování, vícestupňové prepínací sítě.
33. Základní funkce směrovače, zpracování paketů ve směrovači, typy prepínání a architektury.

34. Základní principy softwarově definovaných sítí SDN, architektura, technologie OpenFlow.
35. Procesy a vlákna POSIX.
36. Semaforey, vlastnosti a typické použití (binární, obecné).
37. Monitory, vlastnosti, typy a použití v praxi (POSIX vlákna).
38. Uvážnutí při přidělování prostředků, detekce a řešení.
39. Virtualizace paměti, stránkovací a nahrazovací algoritmy.
40. Systémy souborů, přidělování a evidence diskového prostoru.
41. Systémy souborů, metadata a odolnost vůči výpadku.
42. Klasifikace a vlastnosti paralelních a distribuovaných architektur.
43. Základní typy topologií paralelních a distribuovaných architektur a jejich vlastnosti.
44. Distribuované a paralelní algoritmy - algoritmy řazení, select.
45. Distribuované a paralelní algoritmy - algoritmy vyhledávání.
46. Model PRAM, suma prefixů a její aplikace.
47. Distribuované a paralelní algoritmy - algoritmy nad seznamy, stromy a grafy.
48. Interakce mezi procesy a typické problémy paralelismu (synchronizační a komunikační mechanismy).
49. Distribuovaný broadcast, synchronizace v distribuovaných systémech.
50. Moderní modely životního cyklu vývoje software (iterativní model životního cyklu; MDA, agilní vývoj; agilní modelování; Unified Process (UP)).
51. Modelovací techniky UML (charakteristika jazyka UML; rozšiřitelnost jazyka; charakteristika, základní prvky a použití diagramů UML).
52. Získávání a modelování požadavků (evoluce požadavků; model FURPS+; techniky získávání požadavků; artefakty UP související s požadavky; tvorba modelu případů použití).
53. Logická architektura software (pojem logické architektury; vrstvená architektura; závislosti vrstev a balíčků; princip oddělení pohledu; vzor Model-View-Controller, podstata SOA).
54. Objektově-orientovaný návrh (podstata OO návrhu; vstupy a výstupy OO návrhu; návrh řízený zodpovědností; principy návrhu GRASP, principy SOLID).
55. Návrh řízený testem, refaktorizace, vlastnictví a správa zdrojového kódu v týmu (motivace, podstata, souvislosti, přínos pro zajištění kvality software; repositáře a větvení zdrojového kódu).
56. OLAP-určení, rozdíly oproti OLTP, datový model (datová kostka a operace, zobrazení kostky), datové sklady (struktura, komponenty).
57. Objektově-orientované databázové systémy - kolekce a struktura, objekt, dědičnost, vztahy, role, systém Cache, architektura Java Enterprise Edition.
58. Workflow a jeho užití - business proces, WFM systém, referenční model, zdroj, aktivita, úloha, jazyky pro popis workflow.
59. Hrozby, slabá místa, aktiva, škodlivý software (malware), funkce prosazující bezpečnost (řízení přístupu, autentizace, skryté kanály, audit, přenos dat).
60. Kritéria hodnocení bezpečnosti informačních systémů, historie, kritéria CC (Common Criteria), standardy pro management bezpečnosti.
61. Analýza rizik bezpečnosti informačních systémů (vstupy, výstupy, jednotlivé generace).
62. Bezpečnost webových aplikací, typické útoky.
63. Bezpečnost bezdrátových sítí, útoky, způsoby kryptografického zabezpečení.

## Obor Management a IT - MMI

1. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
2. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
3. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
4. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
5. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
6. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
7. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
8. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
9. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
10. Orientované grafy (orientované sledy, souvislost a silná souvislost, turnaje, eulerovské a hamiltonovské grafy, Dijkstrův a Floyd-Warshallův algoritmus pro hledání cesty minimální délky).
11. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
12. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
13. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
14. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
15. Transformace a normální formy bezkontextových gramatik.
16. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
17. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
18. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
19. Parciální rekurzivní funkce.
20. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
21. Lambda kalkul (definice všech pojmů, operací...).
22. Haskell - lazy evaluation (typy v jazyce včetně akcí, význam typových tříd, demonstrace lazy evaluation).
23. Prolog - způsob vyhodnocení (základní princip, unifikace, chování vestavěných predikátů, operátor řezu - vhodné a nevhodné užití).
24. Prolog - změna DB/programu za běhu (demonstrace na prohledávání stavového prostoru, práce se seznamy).
25. Segmentace trhu (podstata a účel segmentace, segmentační kritéria, žádoucí charakteristiky segmentů).
26. Marketingový mix (co to je, které prvky tvoří marketingový mix 4P, 5P a 7P).
27. Cena (faktory ovlivňující výši ceny, metody stanovení ceny a jejich stručná charakteristika).
28. Distribuce (účel distribuce, distribuční cesty/kanály, charakteristika velkoobchodu a maloobchodu).
29. Propagace (podstata a účel komunikace, prvky komunikačního mixu).
30. Životní cyklus projektu z hlediska projektového řízení. Souvislosti projektového řízení (objekty řízení projektu, princip trojího omezení, faktory podnikového prostředí, organizační struktury, zainteresované strany, socioekonomické vlivy).
31. Znalostní oblasti managementu projektů (vyjmenovat, každou oblast stručně charakterizovat). Management rozsahu projektu (procesy, metody, strukturovaná dekompozice práce).
32. Management času a nákladů v rámci projektů (procesy, metody, metoda kritické cesty CPM - Critical Path Method, metoda odhadu pracnosti FPA - Function Point Analysis, řízení dosažené hodnoty projektu EVM - Earned Value Management, prognózování).
33. Management kvality v rámci projektu (procesy, metody, Paretova analýza, diagram příčin a účinků, kvalitativní charakteristiky softwarových produktů).

34. Management rizik v rámci projektů (procesy, metody, rozhodovací strom, matice pravděpodobnosti a dopadu, analýza očekávané peněžní hodnoty, kategorie rizik v projektech IT, eliminace rizik v softwarových projektech).
35. Metoda Logického rámce (LFM - Logical Framework Matrix).
36. Klasifikace a vlastnosti paralelních a distribuovaných architektur.
37. Základní typy topologií paralelních a distribuovaných architektur a jejich vlastnosti.
38. Distribuované a paralelní algoritmy - algoritmy řazení, select.
39. Distribuované a paralelní algoritmy - algoritmy vyhledávání.
40. Distribuované a paralelní algoritmy - algoritmy nad seznamy, stromy a grafy.
41. Interakce mezi procesy a typické problémy paralelismu (synchronizační a komunikační mechanismy).
42. Distribuované a paralelní algoritmy - předávání zpráv a knihovny pro paralelní zpracování (MPI).
43. Obrazová data, jejich pořizování a možná poškození (možné reprezentace obrazu, obrazové snímací čipy a zařízení, jejich vlastnosti, vady pořízeného obrazu, šumy, optimální filtrace obrazu).
44. Transformace obrazu (jaké transformace se používají při zpracování obrazu, typické příklady a důvody použití transformací při zpracování obrazu).
45. Filtrace obrazu (definice lineární filtrace, typické příklady použití filtrů, použití rychlé konvoluce s využitím FFT, návrh lineárních filtrů, nelineární filtrace).
46. Detekce hran, segmentace (vymezení pojmů detekce hran a segmentace, možné aplikace jednotlivých algoritmů a jejich důvody, typické případy nasazení algoritmů).
47. Informační management (základní souvislosti, postup tvorby podnikatelské/business strategie, manažerské informační systémy - MIS).
48. Oceňování a verzování (základní vlastnosti a nákladové charakteristiky informačních produktů, přístupy/strategie k oceňování, verzování - podstata, dimenze použití, východiska pro určení počtu verzí, druhy a formy svazování, cenová diskriminace).
49. Uzamčení a náklady na přechod (pojem, klasifikace uzamčení, cyklus uzamčení, řízení uzamčení - strategie kupujících a prodávajících).
50. Řízení sítí a síťová ekonomika (sít' a síťové struktury, síťové externality a příčiny vzniku, proces vytváření sítí, standardizace a její dopady na řízení sítí).
51. Tržní selhání (pojem a zdroje, externality a jejich členění, možnosti řešení tržního selhání).
52. Management procesů (co je to proces, základní charakteristiky a dělení procesů, charakteristiky procesní organizace a postup jejího zavádění). Analýza a modelování procesů - CASE nástroje (charakteristika, klasifikace, komponenty a přínosy).
53. Business Process Reengineering (pojem a podstata, klíčové charakteristiky, postup implementace).
54. Základní charakteristika ASP, výhody a nevýhody pro zákazníka i dodavatele. Životní cyklus ASP. Využití v současnosti - srovnání se SaaS a dalšími přístupy.
55. Efektivnost IS/IT (efektivita vs. efektivnost, metrika - pojem, atributy, typy, klasifikace výdajů - pojem TCO, hodnocení přínosů).
56. Informační bezpečnost (přístupy k hodnocení, klasifikace hrozeb a zranitelností, postup analýzy rizik IS, porušení bezpečnosti - bezpečnostní incidenty, typy útoků, cíle útoků).
57. Majetková a kapitálová struktura podniku; výnosy, náklady a výsledek hospodaření.
58. Vztah mezi náklady, objemem a ziskem. Bod zvratu početně a graficky.
59. Výrobní činnost podniku, výrobní kapacita, produktivita. Zásoby v podniku.
60. Investiční rozhodování v podniku. Metody hodnocení investic: čistá současná hodnota, doba návratnosti, vnitřní výnosové procento.
61. Finanční plánování. Zdroje financování. Časová hodnota peněz. Řízení oběžného majetku.
62. Popis a charakteristika procesu strategického řízení firmy.
63. Hierarchie firemní strategie - vize, mise, firemní strategie, business strategie, funkční strategie.
64. Princip a struktura strategické analýzy.
65. Analytické nástroje pro hodnocení interních a externích faktorů.

66. Definování strategických obchodních jednotek, využití strategických obchodních jednotek.

## Obor Matematické metody v IT - MMM

1. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
2. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
3. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
4. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
5. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
6. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
7. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
8. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
9. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
10. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
11. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
12. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
13. Transformace a normální formy bezkontextových gramatik.
14. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
15. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
16. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
17. Parciální rekurzivní funkce.
18. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
19. Temporální logiky CTL\*, CTL a LTL.
20. Explicitní CTL model checking.
21. Binární rozhodovací diagramy.
22. Symbolický CTL model checking.
23. Büchiho automaty, varianty, vlastnosti.
24. LTL model checking založený na automatech.
25. Predikátová abstrakce.
26. Redukce na základě částečného uspořádání.
27. Analýza toku dat.
28. Metody řešení SAT problému (DPLL).
29. Grafy a jejich prohledávání do šířky (pojmy: graf, sled, tah, cesta, kružnice, cyklus, algoritmus BFS, strom prohledávání do šířky a jeho vlastnosti).
30. Prohledávání grafu do hloubky (algoritmus DFS, les prohledávání do hloubky, hledání topologického uspořádání, hledání silně souvislých komponent).
31. Hledání minimální kostry obyčejného grafu (pojmy, stromy a kostry, Kruskalův algoritmus, Primův algoritmus).
32. Hledání nejkratších cest ze zdrojového uzlu do všech ostatních uzlů grafu (Bellman-Fordův algoritmus, Dijkstrův algoritmus).
33. Orientované ohodnocené grafy a hledání nejkratších cest ze všech uzlů do všech uzlů (matice sousednosti, Floyd-Warshallův algoritmus).
34. Toky v síti (pojmy, vlastnosti toku v síti, Ford-Fulkersonova metoda, maximální párování v bipartitním grafu).
35. Hranové a vrcholové barvení grafů (Chromatický polynom).

36. Nekooperativní hry v normální formě (hry s nulovým/nenulovým součtem, jejich analýza a koncepty řešení - MNE a CE).
37. Opakované hry (řešení konečně a nekonečně opakovaných her, Folk theorem).
38. Kooperativní hry s přenositelným užitekem ve formě charakteristické funkce (definice, koncepty řešení - imputace, jádro, Shapleyho hodnota).
39. Teorie veřejné volby (volební mechanismy, Condorcetův paradox, strategická manipulace, Arrow's impossibility theorem).
40. Teorie aukcí (formy aukcí, ekvilibria v aukčních situacích, Revenue equivalence theorem).
41. Evoluční teorie her (evolučně stabilní strategie, dynamika v evoluci).
42. Lexikální analýza: lexikální analyzátoři, tabulka symbolů, lex.
43. Obecná syntaktická analýza: přístupy a modely.
44. Deterministická syntaktická analýza shora dolů: definice a konstrukce množin FIRST a FOLLOW, LL tabulky a LL gramatiky, rekurzivní sestup, prediktivní tabulková analýza, zotavení z chyb.
45. Deterministická syntaktická analýza zdola nahoru: precedenční analýza, LR analýza, konstrukce jejich tabulek, zotavení z chyb, yacc.
46. Sémantická analýza a generování vnitřní formy programů: typová kontrola, abstraktní syntaktické stromy, tříadresný kód, polská notace, yacc.
47. Optimalizace a generování cílového kódu: základní bloky vnitřní formy programů, optimalizace vnitřního a cílového kódu, úspěšné užití registrů.
48. Formální modely pro překlad: převodníky a překladové gramatiky.
49. Lambda kalkul (definice všech pojmů, operací...).
50. Práce v lambda kalkulu (reprezentace čísel a pravdivostních hodnot a operací nad nimi).
51. Haskell - lazy evaluation (typy v jazyce včetně akcí, význam typových tříd, demonstrace lazy evaluation).
52. Prolog - způsob vyhodnocení (základní princip, unifikace, chování vestavěných predikátů, operátor řezu - vhodné a nevhodné užití).
53. Prolog - změna DB/programu za běhu (demonstrace na prohledávání stavového prostoru, práce se seznamy).
54. Věty o úplnosti, kompaktnosti a neúplnosti (teorie 1. řádu, bezespornost, model a důsledek teorie, Gödelovy věty o úplnosti, věta o kompaktnosti a věta Herbrandova, Gödelovy věty o neúplnosti).
55. Metody analýzy C/E a P/T Petriho sítí.
56. Podtřídy a rozšíření Petriho sítí.
57. Barvené a hierarchické Petriho sítě.
58. Klasifikace a vlastnosti paralelních a distribuovaných architektur.
59. Základní typy topologií paralelních a distribuovaných architektur a jejich vlastnosti.
60. Distribuované a paralelní algoritmy - algoritmy řazení, select.
61. Distribuované a paralelní algoritmy - algoritmy vyhledávání.
62. Model PRAM, suma prefixů a její aplikace.
63. Distribuované a paralelní algoritmy - algoritmy nad seznamy, stromy a grafy.
64. Interakce mezi procesy a typické problémy paralelismu (synchronizační a komunikační mechanismy).
65. Distribuované a paralelní algoritmy - předávání zpráv a knihovny pro paralelní zpracování (MPI).
66. Distribuovaný broadcast, synchronizace v distribuovaných systémech.
67. Metodika sériového a paralelního výpočtu (zpětnovazební stabilita paralelních výpočtů).
68. Extrémně přesné řešení diferenciálních rovnic metodou Taylorovy řady.
69. Paralelní řešení obyčejných diferenciálních rovnic s konstantními koeficienty, knihovní podprogramy přesných výpočtů.
70. Metoda řešení rozsáhlých soustav algebraických rovnic převodem na obyčejné diferenciální rovnice.

## Obor Počítačové a vestavěné systémy - MPV

1. Metodika návrhu HW/SW codesign, platformy, programovatelné obvody.
2. Výpočetní modely (StateCharts, Kahnova síť procesů, synchronní dataflow).
3. Specifikace (chování, struktura), syntéza (alokace, přidělení, plánování) a integrace systémů (rozhraní, synchronizace, komunikace).
4. Syntéza HW z vyšších programovacích jazyků (reprezentace, alokace, plánování, přiřazení) a jazyk Catapult C.
5. Odhady (přesnost, věrnost, metriky, metody) a optimalizace vlastností systému (příkon, energie).
6. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
7. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
8. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
9. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
10. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
11. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
12. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
13. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
14. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
15. Orientované grafy (orientované sledy, souvislost a silná souvislost, turnaje, eulerovské a hamiltonovské grafy, Dijkstrův a Floyd-Warshallův algoritmus pro hledání cesty minimální délky).
16. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
17. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
18. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
19. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
20. Transformace a normální formy bezkontextových gramatik.
21. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
22. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
23. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
24. Parciální rekurzivní funkce.
25. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
26. Ukazatele a zákony paralelního zpracování. Funkce konstantní účinnosti a škálovatelnost.
27. Paralelizace programů: vzory programových a datových struktur.
28. Paralelní zpracování v OpenMP, SPMD, smyčky, sekce a tasky. Synchronizační prostředky.
29. Architektury se sdílenou pamětí, UMA i NUMA, zajištění koherence paměti cache.
30. Architektura a použití současných superpočítačů a výpočetních uzlů (Anselm a Salomon).
31. Blokující a neblokující párové (point-to-point) komunikace v MPI.
32. Kolektivní komunikace v MPI, paralelní vstup a výstup.
33. Propojovací sítě: Topologie a směrovací algoritmy, přepínání a řízení toku.
34. Klasifikace metod komprese dat (ztrátové, bezztrátové, intuitivní, algoritmické, četnost výskytu, pravděpodobnost výskytu), princip kódování délek sledů, kódování "přesuň na začátek."
35. Kódy s proměnnou délkou - princip, zdůvodnění, Huffmanovy kódy - různé typy, kanonický Huffmanův kód, adaptivní Huffmanův kód, aritmetický kód.



36. Slovníkové metody (LZ77, LZ78, práce se slovníkem, pohyblivé okno, prodlužování položek).
37. Informace a entropie, Shannova věta o kódování.
38. Bezpečnostní kódy: lineární, Hammingovy, cyklické. Detekce a oprava chyb.
39. Základní architektury prepínačů, algoritmy pro plánování, řešení blokování, vícestupňové prepínací sítě.
40. Základní funkce směrovače, zpracování paketů ve směrovači, typy architektur.
41. Formální metody v počítačových sítích: modelování protokolů pomocí konečných automatů a temporálních logik.
42. Základní principy softwarově definovaných sítí SDN, architektura, technologie OpenFlow.
43. Konflikty a závislosti při řetězovém zpracování instrukcí a jejich HW/SW ošetření.
44. Architektura superskalárních procesorů a algoritmy OOO zpracování instrukcí.
45. Procesory VLIW a používané optimalizační techniky s HW podporou.
46. Multivláčkové procesory, hrubý, jemný a simultánní MT.
47. Datový paralelismus SIMD a SIMT, HW implementace a SW podpora.
48. Architektura grafických procesorů, odlišnosti od superskalárních procesorů.
49. Programovací jazyk CUDA, model vláken a paměťový model.
50. Základní rysy nízkopříkonových procesorů (požadavky, architektura, výkonnost).
51. Jazyky pro popis obvodů (VHDL, behaviorální a strukturní popis) a cílové technologie ASIC a FPGA (charakteristika, srovnání).
52. Logická syntéza obvodů (návrh pro technologie FPGA a ASIC, fáze syntézy, optimalizace, mapování, techniky zřetězení a vyvážení).
53. Moderní přístupy k syntéze číslicových obvodů (reprezentace obvodu pomocí AIG, techniky odstraňování funkční redundance v AIG, tradiční mapování AIG do LUT).
54. Aplikace omezujících podmínek (časová a fyzická omezení).
55. Verifikace číslicových obvodů (metodologie OVM).
56. Metody snižování příkonu číslicových zařízení (statický a dynamický příkon v technologii CMOS, metody redukce příkonu).
57. Vestavěný počítačový systém (shody a odlišnosti s běžným univerzálním počítačovým systémem).
58. Implementace funkcí vestavěného systému SW a HW prostředky (výhody a nevýhody - dopady SW a HW implementace konkrétní funkce na vlastnosti systému, příklad).
59. Číslicové vstupy a výstupy vestavěných systémů (problémy a jejich řešení, přizpůsobení napěťových úrovní, snímání stavu mechanického kontaktu, ovládání zátěže, posílení výstupu, H-můstek).
60. Architektura SW pro vestavěné systémy (hlavní smyčka, implementace stavového automatu, obsluha přerušení).
61. Konstrukce adaptéru systémové sběrnice: návrh adresového dekodérů, obsluha čtecí a zápisové transakce.
62. Architektura sběrnice PCI-Express a USB: typy transakcí, způsob komunikace a směrování transakcí, detekce chyb a způsob zotavení.

## Obor Počítačové sítě a komunikace - MSK

1. Grafy a jejich prohledávání do šířky (pojmy: graf, sled, tah, cesta, kružnice, cyklus, algoritmus BFS, strom prohledávání do šířky a jeho vlastnosti).
2. Prohledávání grafu do hloubky (algoritmus DFS, les prohledávání do hloubky, hledání topologického uspořádání, hledání silně souvislých komponent).
3. Hledání minimální kostry obyčejného grafu (pojmy, stromy a kostry, Kruskalův algoritmus, Primův algoritmus).
4. Hledání nejkratších cest ze zdrojového uzlu do všech ostatních uzlů grafu (Bellman-Fordův algoritmus, Dijkstrův algoritmus).
5. Orientované ohodnocené grafy a hledání nejkratších cest ze všech uzlů do všech uzlů (matice sousednosti, Floyd-Warshallův algoritmus).
6. Toky v síti (pojmy, vlastnosti toku v síti, Ford-Fulkersonova metoda, maximální párování v bipartitním grafu).
7. Metodika návrhu HW/SW codesign, platformy, programovatelné obvody.
8. Výpočetní modely (StateCharts, Kahnova síť procesů, synchronní dataflow).
9. Specifikace (chování, struktura), syntéza (alokace, přidělení, plánování) a integrace systémů (rozhraní, synchronizace, komunikace).
10. Odhady (přesnost, věrnost, metriky, metody) a optimalizace vlastností systému (příkon, energie).
11. Jazyk a sémantika predikátové logiky (termy, formule, realizace jazyka, pravdivost formulí).
12. Formální systém predikátové logiky (axiomy a odvozovací pravidla, dokazatelnost, model a důsledek teorie, věty o úplnosti a kompaktnosti, prenexní tvar formulí).
13. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Boolovy algebry, univerzální algebry).
14. Základní algebraické metody (podalgebry, homomorfismy, přímé součiny, kongruence a faktorové algebry, normální podgrupy a ideály okruhů).
15. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy).
16. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).
17. Metrické prostory (příklady, konvergence posloupností, spojitá a izometrická zobrazení, úplnost, Banachova věta o pevném bodu).
18. Normované a unitární prostory (základní vlastnosti a příklady, normované prostory konečné dimenze, uzavřené ortonormální systémy a Fourierovy řady).
19. Obyčejné grafy (stupně uzlů, sledy, souvislost, izomorfismy, stromy, kostry, Kruskalův a Primův algoritmus pro hledání minimální kostry ohodnoceného grafu, eulerovské a hamiltonovské grafy, planarita a obarvitelnost).
20. Popište principy komunikačního protokolu SCTP.
21. Popište protokol HDLC, jaké jsou režimy přenosu, typy rámců.
22. Popište architekturu ADSL sítě a k čemu jednotlivé prvky slouží.
23. Popište princip ISDN BRI přípojky, možné topologie, komunikační kanály.
24. Klasifikace gramatik, formálních jazyků a automatů přijímajících jazyky.
25. Vlastnosti formálních jazyků (typické vlastnosti a jejich rozhodnutelnost).
26. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
27. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
28. Transformace a normální formy bezkontextových gramatik.
29. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
30. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, univerzální TS).
31. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
32. Parciální rekurzivní funkce.
33. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
34. Ukazatele a zákony paralelního zpracování. Funkce konstantní účinnosti a škálovatelnost.

35. Paralelizace programů: vzory programových a datových struktur.
36. Architektury se sdílenou pamětí, UMA i NUMA, zajištění koherence paměti cache.
37. Blokující a neblokující párové (point-to-point) komunikace v MPI.
38. Propojovací sítě: Topologie a směrovací algoritmy, přepínání a řízení toku.
39. Základní architektury přepínačů, algoritmy pro plánování, řešení blokování, vícestupňové přepínací sítě.
40. Základní funkce směrovače, zpracování paketů ve směrovači, typy přepínání a architektury.
41. Formální metody v počítačových sítích: modelování protokolů pomocí konečných automatů a temporálních logik.
42. Základní principy softwarově definovaných sítí SDN, architektura, technologie OpenFlow.
43. Řízení toku dat (flow-control) a prevence zahlcení (congestion-control) na transportní vrstvě (MP-TCP, QUIC, SCTP, DCCP).
44. Identifikace síťového provozu (signatury, statistické metody), důvěra na Internetu (reputační systémy).
45. Sítě Peer-to-Peer: vlastnosti, chování, způsoby směrování. Strukturované a nestrukturované sítě.
46. Základní typy topologií paralelních a distribuovaných архитектур a jejich vlastnosti.
47. Distribuované a paralelní algoritmy - algoritmy řazení, select.
48. Distribuované a paralelní algoritmy - algoritmy vyhledávání.
49. Model PRAM, suma prefixů a její aplikace.
50. Distribuované a paralelní algoritmy - algoritmy nad seznamy, stromy a grafy.
51. Interakce mezi procesy a typické problémy paralelismu (synchronizační a komunikační mechanismy).
52. Distribuovaný broadcast, synchronizace v distribuovaných systémech.
53. Hrozby, slabá místa, aktiva, škodlivý software (malware), funkce prosazující bezpečnost (řízení přístupu, autentizace, skryté kanály, audit, přenos dat).
54. Bezpečnost webových aplikací, typické útoky.
55. Bezpečnost bezdrátových sítí, útoky, způsoby kryptografického zabezpečení.
56. Systémy mobilní komunikace - GSM, GPRS, HSCSD, EDGE, UMTS, DECT, LTE.
57. Klasifikace algoritmů volby koordinátora, algoritmus Bully a jeho složitost.
58. Skalární, vektorový a maticový logický čas.
59. Podmínky konsistentního globálního stavu distribuovaného systému.
60. Skupinová komunikace v distribuovaném systému (algoritmy, modely skupinové komunikace).
61. Principy distribuovaného zpracování MapReduce a jeho základní operace.
62. Modely distribuovaného provádění a jejich vlastnosti.

Schválila Rada navazujícího magisterského studijního programu dne 28. 3. 2018.

V Brně dne 4. 4. 2018

prof. Dr. Ing. Pavel Zemčík  
děkan FIT VUT v Brně