

Kursuseprogramm

Ainekood IFI6057	NIMETUS KRÜPTOLOOGIA MEETODID ANDMETURBES		
Maht 4.0 EAP	Kontaktitudide maht: 56	Õppesemester: S	Eksam
Eesmärk:	Luua eeldused teadmiste ja intellekti olemuse mõistmiseks struktuuriteoreetilise ning matemaatilise loogika vahenditega.		
Aine lühikirjeldus: (sh iseseisva töö sisu kirjeldus vastavuses iseseisva töö mahule)	Aine jaguneb järgmisteks osadeks: 1. Sissejuhatus ainesse. Esitatakse valdkonna kirjeldus ja käsitletavate probleemide ning teemade iseloomust. Formuleeritakse olulisemad probleemid ja aine ülesehituse kirjeldus. 2. Matemaatilised käsitusvahendid. Antakse lühike ülevaade vajalikest mõistetest ja tulemustest, mis pärinevad hulgateooriast, matemaatilisest loogikast, algoritmiteooriast ning algebrast. 3. Teadmised ja intellekt. Käsitletakse teadmiste, andmete, saladuste ja informatsiooni mõistet tuginedes tähiseks-tähenduseks olemise relatsioonile. Esitatakse teadmiste ja süsteemi mõistele tuginev intellekti määratlus ning intellekti liigitamise alused. 4. Formaliseerimine. Selgitatakse sarnasuse ja seotuse metapredikaatide abil, milles seisneb olemuslikult mingi valdkonna tundmaõppimise selline faas, mida võiks nimetada vaadeldava valdkonna range käsitluse ehk formalismi loomiseks. Iseseisva töö alla kuulub kordamine ja harjutamine, kohustusliku kirjanduse läbitöötlemine. Kontrolltöö ja eksam sisaldavad küsimusi, mis on seotud ka kohustusliku kirjanduse teemadega. Näidiskontrolltöö (nr1 ja nr2) ja näidiseksam asuvad kursuse lehel : www.tlu.ee/~matsak/is		
Õpiväljundid:	Tunneb intellekti teadmiste, andmete ja informatsiooni olemusega seotud mõisteteaparaati ning olulisemaid tulemusi. Oskab teadmiste ja intellektiga seotud väiteid seostada matemaatilise loogika, algoritmiteooria ning (algebralise) süsteemiteooria asjakohaste mõistete, tulemuste ning meetoditega. Tunneb ja oskab formuleerida intelligentsetele süsteemidele püstitavaid ülesandeid viisil, mis võimaldab hinnata nende põhimõttelist lahendatavust või mittelahenduvust, tõestatavust või mittetõestatavust.		
Hindamismeetodid:	Eksam		
Õppejõud:	Prof Peeter Lorents, PhD		
Inglisekeelne nimetus:	<i>Intelligent Systems</i>		

Eeldusaine:	MLM6202, IFI6012
Kohustuslik kirjandus:	Lorents P. (2001). Informaatika teoreetilised alused. Kirjastus EBS Print. Tallinn. Lorents P. (2002). Hulgad, valemid, algoritmid. Kirjastus EBS Print. Tallinn.
Asenduskirjandus: (üliõpilase poolt läbi töötatava kirjanduse loetelu, mis katab ainekursuse loengulist osa)	Lorents P. (2000). Keel ja loogika. Kirjastus EBS Print. Tallinn. Tyugu E. (2007). Algorithms and Architectures of Artificial Intelligence. IOS Press. Amsterdam. Berlin. Oxford. Tokyo. Washington, DC
Õppetöös osalemise ja eksamile/arvestusele pääsemise nõuded	Eksamile pääsemise eeltingimuseks on eelnevalt sooritatud kontrolltööd nr 1 ja nr 2. Kontrolltöö sooritamiseks tuleb esitada õiged vastused rangelt enam kui pooltele küsimustele/ülesannetele. Õigel ajal mitte sooritatud kontrolltöid saab järele teha nädalal, mis vahetult eelneb eksamiks ette nähtud nädalale. Järeleksamit saab sooritada ainult järelvastamiseks ettenähtud nädalatel eelnevalt välja kuulutatutel kuupäevadel.
Iseseisva töö nõuded	Kodus kordamine ja harjutamine, kohustusliku kirjanduse läbitöötlemine
Eksami hindamiskriteeriumid või arvestuse sooritamiseks vajalik miinimumtase	Hindamiskriteeriumid, millest hindamisel lähtutakse: A – Oskab 91-100% ulatuses vastata intelligentsete süsteemide olemust ja aluseid käsitlevatele küsimustele sh hulkade ja süsteemide kirjeldamine; väiteid esitavate valemite tõlevastavuse ja mittevasturääkivuse tuvastamine; tuletussammude korrektsuse kontrollimine; teadmiste, andmete ja info määratlemine; teadmistega opereerimine ja eelnimetatu seostamine intellekti olemasolu või puudumisega vastavas süsteemis. Oskab rakendada transformeerimise protseduuri loomulikus keeles esitatud väidete esitamiseks valemite abil. Oskab 91-100% ulatuses vastata süsteemide selitamise protseduuri olemuse ja rakendamisega seotud küsimustele. Oskab vastata programmide struktuurse sünteesi olemust ja rakendamist käsitlevatele küsimustele. Oskab 91-100% ulatuses vastata intellekti olemasolu ja rakendamist vajavate valdkondi käsitlevatele küsimustele (sh autonoomsed süsteemide,

automaatne otsustamine, automaatne olukorra kirjeldamine jms).

B – Oskab 81-90% ulatuses vastata intelligentsete süsteemide olemust ja aluseid käsitlevatele küsimustele sh hulkade ja süsteemide kirjeldamine; väiteid esitavate valemite tõlevastavuse ja mittevasturääkivuse tuvastamine; tuletussammude korrektsuse kontrollimine; teadmiste, andmete ja info määratlemine; teadmistega opereerimine ja eelnimetatu seostamine intellekti olemasolu või puudumisega vastavas süsteemis. Oskab rakendada transformeerimise protseduuri loomulikus keeles esitatud väidete esitamiseks valemite abil. Oskab 81-90% ulatuses vastata süsteemide selitamise protseduuri olemuse ja rakendamisega seotud küsimustele. Oskab vastata programmide struktuurse sünteesi olemust ja rakendamist käsitlevatele küsimustele. Oskab 81-90% ulatuses vastata intellekti olemasolu ja rakendamist vajavate valdkondi käsitlevatele küsimustele (sh autonoomsed süsteemide, automaatne otsustamine, automaatne olukorra kirjeldamine jms).

C – Oskab 71-80% ulatuses vastata intelligentsete süsteemide olemust ja aluseid käsitlevatele küsimustele sh hulkade ja süsteemide kirjeldamine; väiteid esitavate valemite tõlevastavuse ja mittevasturääkivuse tuvastamine; tuletussammude korrektsuse kontrollimine; teadmiste, andmete ja info määratlemine; teadmistega opereerimine ja eelnimetatu seostamine intellekti olemasolu või puudumisega vastavas süsteemis. Oskab rakendada transformeerimise protseduuri loomulikus keeles esitatud väidete esitamiseks valemite abil. Oskab 71-80% ulatuses vastata süsteemide selitamise protseduuri olemuse ja rakendamisega seotud küsimustele. Oskab vastata programmide struktuurse sünteesi olemust ja rakendamist käsitlevatele küsimustele. Oskab 71-80% ulatuses vastata intellekti olemasolu ja rakendamist vajavate valdkondi käsitlevatele küsimustele (sh autonoomsed süsteemide, automaatne otsustamine, automaatne olukorra kirjeldamine jms).

D – Oskab 61-70% ulatuses vastata intelligentsete süsteemide olemust ja aluseid käsitlevatele küsimustele sh hulkade ja süsteemide kirjeldamine; väiteid esitavate valemite tõlevastavuse ja mittevasturääkivuse tuvastamine; tuletussammude korrektsuse kontrollimine; teadmiste, andmete ja info määratlemine; teadmistega opereerimine ja eelnimetatu seostamine intellekti olemasolu või puudumisega vastavas süsteemis. Oskab rakendada transformeerimise protseduuri loomulikus keeles esitatud väidete esitamiseks valemite abil. Oskab 61-70% ulatuses vastata süsteemide selitamise protseduuri olemuse ja rakendamisega seotud küsimustele. Oskab vastata programmide struktuurse sünteesi olemust ja rakendamist käsitlevatele küsimustele. Oskab 61-70% ulatuses vastata intellekti olemasolu ja rakendamist vajavate valdkondi käsitlevatele küsimustele (sh autonoomsed süsteemide, automaatne otsustamine, automaatne olukorra kirjeldamine jms).

	E – Oskab 51-60% ulatuses vastata intelligentsete süsteemide olemust ja aluseid käsitlevatele küsimustele sh hulkade ja süsteemide kirjeldamine; väiteid esitavate valemite tõlevastavuse ja mittevasturääkivuse tuvastamine; tuletussammude korrektsuse kontrollimine; teadmiste, andmete ja info määratlemine; teadmistega opereerimine ja eelnimetatu seostamine intellekti olemasolu või puudumisega vastavas süsteemis. Oskab rakendada transformeerimise protseduuri loomulikus keeles esitatud väidete esitamiseks valemite abil. Oskab 51-60% ulatuses vastata süsteemide selitamise protseduuri olemuse ja rakendamisega seotud küsimustele. Oskab vastata programmide struktuurse sünteesi olemust ja rakendamist käsitlevatele küsimustele. Oskab 51-60% ulatuses vastata intellekti olemasolu ja rakendamist vajavate valdkondi käsitlevatele küsimustele (sh autonoomsed süsteemide, automaatne otsustamine, automaatne olukorra kirjeldamine jms).
Informatsioon kursuse sisu kohta, kursuse jaotumine teemade kaupa sh kontakttundide ajad	Läbitavad teemad nädalate või loengute kaupa. 1. (4.sept) Sissejuhatus Loeng: Intellekti määratluste mõned näited. Selgitused „võrdusele“ intelligentsed süsteemid = süsteemid + intellekt. Kursuse ülesehituse olulisemate koostisosade ja seoste ülevaade. Fundamentaalsusest. Fundamentaalmõistetest. Fundamentaalsprintsiipidest. Tähisted ja tähendused ning nende vaheline seos. Tähisteks-tähenduseks olemise seose olemuse mõistmiseks vajalikud alusprintsiibid. Harjutus: Veel mõned intellekti määratlused. Erinevate määratluste võrdlemine ning mõtestamine. Näited (sh õppurite poolt auditooriumis esitatavad) intellekti olemasolu ning avaldumisvormide kohta eluslooduses, inimolendite korral ning tehnilises keskkonnas. Tähisteks-tähenduseks olemise seose omadustega seotud harjutusülesanded. 2. (11.sept) Hulgad ja nende kirjeldamise vahendid (hulgateooria valemid). I. Osa. Loeng: Püüdlustest esitada hulga mõiste määratlusi. Hulgaks ja hulga elemendiks olemise fundamentaalsus. Hulkade kirjeldamiseks vajalikud sümbolid. Hulkade kirjeldamiseks vajalikud väited ning nende täpsed „üleskirjutused“ – hulgateooria valemid. Hulkade kirjeldamiseks kasutatavate väidete õigsuse tuvastamine: klassikaline interpretatsioon. Hulgaks ning hulga elemendiks olemist reguleerivad alusväited ehk hulgateooria aksioomid. Esimesed olulised hulkadevahelised seosed: elemendiks olemise ja

	osahulgaks olemise seosed. Astmehulgad. Harjutus: Hulkade kohta käivate väidete kirja panemine hulgateooria valemite abil. Ülesanded hulgateooria aksioomide olemuse (mis on, mis tundub olevat) selgitamiseks. Ülesanded hulgateooria valemite klassikaliseks interpreteerimiseks 3. (18.sept) Hulgad ja nende kirjeldamise vahendid (hulgateooria valemid). II. Osa. Loeng: Zermelo-Fraenkeli aksiomaatika. Mõned lihtsamad tehted olemasolevatest hulkadest uute moodustamiseks (sh osahulkade väljaeraldamine) ning uute olemasolu põhjendamine (kas n-ö otse aksioomidest või n-ö kaudselt – st järeldustena aksioomidest). Harjutus: Ülesanded lihtsamate hulgateoreetiliste tehete (sh osade väljaeraldamine) sooritamiseks ning tulemuste olemasolu tõestamiseks. 4. (25.sept) Hulgad ja nende kirjeldamise vahendid (hulgateooria valemid). III. Osa. A. Loeng: Lõplikud ja lõpmatud hulgad. Naturaalarvud, ordinaalarvud ja nende rollist intelligentsetes süsteemides. B. Loeng: Omaduste olemus: osahulgaks olemine, osahulka kuulumine. Järjestatud paari mõiste ja selle olemasolu. Naturaalarvudest moodustatud järjestatud paarid ja nende nummerdamine. Gödeli numbrid. Cantori numbrid. Korteežide mõiste ja nende olemasolu. Cartesiuse korrutised. Seosed kui Cartesiuse korrutise osahulgad. Funktsionaalsed seosed. Vastavused: ühene ja üks-ühene vastavus. A. Harjutus: Ülesanded naturaalarvude ja ordinaalide kohta: elemendiks ja osahulgaks olemine. Naturaalarvude ordinaalarvudeks olemine. Naturaalarvude esitamine algarvude astmete korrutistena. B. Harjutus: Naturaalarvude omaduste ja vastavate osahulkade seostamine. Järjestatud paaride ning kolmikute elemendid. Korteežide võrdsuse ning mittevõrdsuse näited. Cartesiuse korrutised ning astmed. Näited tegurite järjekorra olulisuse kohta. Ülesanded naturaalarvude vaheliste binaarsete ja ternaarsete seoste kui vastava Cartesiuse astme osahulkade kohta. Seoste funktsionaalsuse tuvastamine. Funktsionaalsete seoste määramis- ja muutumiskiirkonnad. Ühesed ja üks-ühesed vastavaused. Ülesanded ühese vastavuse olemasolu ning samal ajal üks-ühese vastavuse puudumise kohta.
--	--

5. (2.okt) Binaarsed seosed ja nende olulisimad omadused

Loeng: Refleksiivsus ja refleksiivsed ning mitte-refleksiivsed binaarsed seosed. Transitiivsus ja transitiivsed ning mitte-transitiivsed binaarsed seosed. Sümmeetria ja sümmeetrilised ning mitte-sümmeetrilised seosed. Antisümmeetria ja antisümmeetrilised ning mitte-antisümmeetrilised binaarsed seosed. Lineaarsus ning lineaarsed ning mitte-lineaarsed binaarsed seosed. Totaalsus ja totaalsed ning mitte-totaalsed seosed. Fundeeritus ja fundeeritud ja mitte-fundeeritud seosed. Minimaalne element. Minitingimus ja minitingimust rahuldavad ning mitte-rahuldavad binaarsed seosed. Esimene element. Esitingimus ja esitingimust rahuldavad ning mitte-rahuldavad binaarsed seosed. Induktsioonitingimus ja induktsioonitingimust rahuldavad ning mitte-rahuldavad binaarsed seosed. Induktsioonitingimus, minitingimuse ja fundeerituse samaväärsus, IMF teoreem. Induktsiooni rollist intelligentsetes süsteemides. Ekvivalentsuse olemus. Järjestuse olemus. Osaline järjestus, lineaarne järjestu, täielik järjestus. Täielik järjestus ja ordinaalarvud. Hulkade täielikust järjestatavusest: Zermelo ja von Neumanni teoreemid. Järjestamise algoritmidest ja probleemidest.

Harjutus: Ülesanded binaarsete seoste olemasolu või puudumise tuvastamiseks. Ülesanded induktsiooni rakendamiseks. Ülesanded minimaalsete elementide leidmiseks. Ülesanded minimaalse elemendi ja esimese elemendi puudumise kohta. Ülesanded järjestuse liigi määratlemiseks. Ülesanded täieliku järjestuse ning ordinaalarvu seostamise kohta. Hulkade (ümber)järjestamine täielikult järjestatud hulgaks.

6. (9.okt) Süsteemid

Loeng: Süsteemi mitteformaalne määratlemine. Põhihulk ja signatuur. Süsteemide leidmine – väljakutse intellektile. Süsteemide selitamise (“väljakaevamise”) protseduur. Mitme põhihulgaga süsteemid. Süvasüsteemid.

Harjutus: Näited süsteemide mitteformaalse määratluse kohta (üliõpilaste pered, sõpruskonnad, meeskonnad, arvuti riistvara mõned alad jms). Seotuse ja sarnasuse metapredikaatide rakendamine. Süsteemide (sarnasuse ja seotuse metapredikaatidele toetuva) „väljakaevamise“ protseduuri rakendatavus ja mitterakendatavus.

7. (16.okt) Süsteemide sarnasus ja modelleerimise olemus. Aeg ja ajast olenemine. Simuleerimise olemus.

Loeng: Süsteemide sarnasuse mitteformaalne määratlemine. Homomorfism ja isomorfism. Modelleerimise olemus. Aeg kui süsteem. Ajad. Ajast olenevad süsteemid. Situatsioonid ning sündmused. Arengud ja protsessid. Ajast olenevusega seotud alusprintsüübid: ajast olenevuse vältimatus, arenguvõimaluste paljusus, ettemääramatus, arengud ja deduktsioon. Simuleerimise olemus. Modelleerimise ja simuleerimise vahendite näiteid. Intelligentne simulatsioonitarkvara.

Harjutus: Näited süsteemide sarnasuse mitteformaalse määratluse kohta (üliõpilaste pered, sõpruskonnad, meeskonnad, asutused või nende osakonnad, kujundid ja kehad, asumid ja plaanid, kaardid jms). Ülesanded isomorfismi ning homomorfismi olemasolu ja puudumise tuvastamise kohta. Aegade käsitlemine süsteemina: kontoriaeg, ajaloolase aeg, koolifüüsika aeg. Süsteemide arengu näited (mõne üliõpilase pere, meeskond vms). Näited üliõpilaste poolt ajast olenevuse printsüüpide illustreerimiseks. Modelleerimise ja simuleerimise tarkvara demo-ülesanded.

**8. (30.okt) Kordamine kontrolltööks
Kontrol töö nr 1.**

9. (6.nov) Süsteemide ja situatsioonide kirjeldamine.

Loeng: Süsteemide ja situatsioonide kirjeldamine väidete abil. Süsteemide ja situatsioonide kirjeldamiseks vajalikud sümbolid. Süsteemide ja situatsioonide kirjeldamiseks vajalike väidete esitamine valemite abil. Loomulikus keeles esitatud väidete transformeerimine valemiteks. Süsteemide ja situatsioonide kirjeldamiseks kasutatavate valemite tõeväärtuste hindamine. Süsteemide ja situatsioonide kirjeldamise deduktiivne vorm. Aksiomid, tuletussammud ja tuletusreeglid. Tuletussammude ja reeglite korrektsus. Tuletatud valemid ehk teoreemid. Vastuolulisus ja mittevastuolulisus. Vastuolulisusega seotud ohud. Süsteemide ja situatsioonide kirjelduste mittevastuolulisuse tuvastamine.

Harjutus: Süsteemide ja situatsioonide kirjeldavate väidete koostamine loomulikus keeles. Väidete transformeerimine valemiteks. Valemite tõeväärtuste hindamine. Tuletussammude korrektsuse tuvastamine. Tuletuste konstrueerimine. Valemite kogumite vastuolulisuse/mittevastuolulisuse tuvastamine.

10. (13.nov) Konstruktsioonid ja konstrueerimine.

Loeng: Konstruktsioonide ja konstrueerimise mitteformaalne kirjeldamine. Süsteemid ja konstruktsioonid. Konstruktsioonide esitused. Ühekohaliste funktsioonide algebrad (funktsioonide hulk ja seosed funktsioonide vahel). Ühekohaliste algoritmiliselt arvutatavate funktsioonide konstrueerimine (operaatortermid). Church'i tees. Algoritmiline karakteriseeritavus (mittekarakteriseeritavus) ja genereeritavus (mittegenereeritavus). Probleemide algoritmiline taandatavus ja selle rakendamine. Valemite konstrueerimine. Seosed valemite vahel – tuletusreeglid. Tuletuste konstrueerimine. Tuletused ja tõestused. Tuletuse otsimise (tarkvaralistest) vahenditest. Tuletuste ja termide seotusest: programme struktuurne süntees. Täielikkus. 1-järku klassikalise predikaatarvutuse täielikkus. Aritmeetika mittetäielikkus. Intellekti suutlikkuse piiratusest.

Harjutus: Lihtsamate aritmeetiliste arvutuste esitamine konstruktsioonidena. Lihtsamate põhjenduste esitamine konstruktsioonidena. Mõnede funktsioonide algoritmilise arvutatavuse tõestamine. Algoritmilise mittelahenduvuse ja mittegenereeritavuse näited. Tuletuste kui konstruktsioonide ehitamise näited. Struktuurse sünteesi reeglite süsteemi rakendamise näited. Teoreemide automaatse tõestamise süsteemide näited.

11. (20.nov) Teadmised ja nende esitamine

Loeng: Teadmusaatomid. teadmised, andmed ja informatsioon. Teadmised ning asjade informatsiooniline väärtus. Informatsioonilise relatiivsuse printsiip. Teadmised ja freimid. Teadmised ja semantilised võrgud. Tõugu arvutusmodelid. Teadmised ja neuronite võrgud. Teadmised ja digiskeemid.

Harjutus: Näited teadmistest teatmeteostes (tekstides sisalduvate tähiste ja tähenduste esiletoomise ülesanded). Teadmiste „mittetekstilised“ näited (näidete esitamine üliõpilaste poolt ja esitatud näidete analüüs). Lihtsamate freimide koostamine. Semantiliste võrkude näited. Arvutusmodelite näited. Neuronite ja võrkude näited. Digiskeemide näited (tutvustamise ja elementaartaseme selgituste tasemel).

12. (27.nov) Intellekt – opereerimine teadmistega

Loeng: Teadmised ja interpreteerimine. Teadmised ja (loogilised) tuletused. Teadmussüsteemid. Ekspertsüsteemid.

Harjutus: Tekstina esitatud tähistele tähenduste otsimine – interpreteerimine süsteemidel. Ekspertsüsteemi kasutamise näited.

	13. (4.dets) Intellekti vajavad valdkonnad. Loeng: Autonoomsed süsteemid. Autonoomne juhtimine. Autonoomne otsustamine. Autonoomne planeerimine. Autonoomne tarkvara loomine. Autonoomne arutlemine ja õppimine. Autonoomne diagnostika (sh inimeste tervise monitooring ja haiguste/vigastuste diagnoosimine). Autonoomne informatsiooni seostamine ja aru saamine. Autonoomne situatsioonide kirjeldamine. Harjutus: Üliõpilaste poolt otsitud teemakohaste näidete esitamine ja analüüs. Seostamine eelnevalt käsitletud teemadega.
	14. (11.dets) Kordamine kontrolltööks Kontrolltöö nr 2.

Õppeainet kureeriv üksus:	Informaatika instituut
Kursuseprogrammi koostaja	
Allkiri:	
Kuupäev:	

Kursuseprogramm registreeritud akadeemilises üksuses

Kuupäev	
Õppeassistendi nimi	
Allkiri	