Poglobljeni predmeti BDR-RI v š. l. 2017/18

Nosilec-predstojnik katedre / (izvajalec)	Šifra pred.	Predmet	Št. kred. točk	Št. semestrskih ur	
				zim.	pol.
Borut Robič	63824	**Izbrana poglavja iz arhitektur in algoritmov 1 (Contemporary Approaches to Algorithm Design)** Pri predmetu bomo spoznali sodobne pristope k snovanju algoritmov. Ti pristopi vključujejo razne tehnike analiziranja, metode snovanja in računske modele. Spoznali bomo: • proces inženiringa algoritmov (proces, ki se trudi premoščati razlike med teorijo in prakso), • algoritme za večnivojsko pomnilniško hierarhijo (algoritme, ki upoštevajo značilnosti predpomnilnikov ipd.), • načine za pohitritev natančnih eksponentnih algoritmov (npr. rezanje prostora iskanja ipd.), • parametrične algoritme (algoritme, ki so hitri pri določenih vrstah vhodnih podatkov), • aproksimacijske algoritme (algoritme, ki hitro vrnejo približen, toda kakovosten rezultat),	5		15-20-15

		• verjetnostne algoritme (algoritme, ki hitro vrnejo negotov, toda verjetno pravilen rezultat), • kvantne algoritme (algoritme, ki izkoriščajo načela kvantne fizike). Vse našteto bomo podkrepili s sodobno analizo algoritmov in problemov (npr. analizo najslabšega primera). The subject explains the main contemporary approaches to the design of algorithms. These approaches include various analysis techniques, design methods and computation models. We describe how we can: • apply algorithm engineering (which aims to bridge the gap between theory and practice), • use multi-level memory hierarchy and design cache-oblivious algorithms, • speed up exact exponential algorithms (e.g., by branching techniques), • design parameterized algorithms (algorithms that take advantage of specific inputs bound to a parameter), • design approximation algorithms (fast algorithms that return approximate results of good quality),			

		• design randomized algorithms (fast algorithms that return uncertain results of good confidence), • design quantum algorithms (algorithms that integrate quantum reality into computation). Finally, we describe the concept of the realistic (as opposed to the worst-case) complexity of algorithms and computational problems.			
Nežka Mramor Kosta (Polona Oblak)	63828A	**Izbrana poglavja iz matematičnih metod v računalništvu 1 (Mathematics for Machie Learning)** In this course, we'll study the theory of matrices behind the basic concepts of maching learning. We'll present the matrix algebra and derivations of and over matrices. These definitions are crucial to understand the optimization methods in machine learning. A detailed description of the course content, divided into weekly lectures. Week 1 Introduction. Weeks 2-5 Trace, norm, distance, angle,	5	30-15-15	

		orthogonality. Kronecker product, vec operator, Haddamard product. Linear systems and generalized inverses. Moore-Penrose inverse. Determinants. Linear, bilinear and quadratic forms. Eigenvalues and eigenvectors of matrices. Week 6 -11 Matrix differentiation. Polar decomposition. Hessian. Week 12 Minimization of a second-degree n-variable polynomial subject to linear constraints. Weeks 13-14 Applications to machine learning.			
Nežka Mramor Kosta (Aleksandar Jurišić)	63828B	**Izbrana poglavja iz matematičnih metod v računalništvu 1 (Selected topics on Cryptography and Computer Security)** The course will cover selected topics from the following list: Symmetric cryptography - classical Ciphers and History of Cryptography - Kerckho Principle and various attacks on cryptosystems - Shannon Theory of Information (Perfect, Computational and Provable Security) - Block Ciphers (DES/IDEA, AES and nalists, Linear and Di	5		30-15-15

		erential Analysis) - Stream Ciphers/PRNG (LFSR and Berlekamp-Massey algorithm, RC4,...), - Cryptoanalysis and Statistical Methods - Hash Functions (MD/SHA, HMAC, ...), - Authentication Codes (MAC), - Birthday Paradox Attacks, new attacks,... Public-key cryptography (Asymmetric Cryptography) - Perfect Security (Computational, Unconditional and Provable Security) - Public-Key Cryptosystems, One-Way Functions and related problems in Number Theory - Primality Testing, Integer Factorization, Discrete Logarithem Problem) - Digital Signatures (RSA, DSA, one-time, blind, group etc.) - Key Agreement Protocols (Die-Hellman, ElGamal, Kerberos, STS) - Identication Schemes for humans and devices (challenge/response, ...) - Other protocols (head/tail over the phone, mental poker, Secret Sharing Schemes, Authentication Schemes, Timestamps, Visual Cryptography, Zero-Knowledge Proofs) - Quantum cryptography			

		Computer and information security - Security of programs (bugs, viruses, malicious code) - Security of databases (anonymization, homomorphic encryption) - Security of OS (MS Win, Unix/Linux, liveCD) - Security of network communication (rewalls, VPN, IPSec, SSL) A detailed description of the course content, divided into weekly lectures (15W, 45h) Week 1 Introduction Week 2-5 (A) Funamentals of Cryptography (Project proposal) Week 6-11 (B) Advanced topics in Cryptography and Computer Security (Milestone presentations) Week 12 (C) Applied Projects Week 13-15 (D) Research topics (Project Presentation)			
Marko Robnik Šikonja (Zoran Bosnić)	63834	**Izbrana poglavja iz umetne inteligence 1 (Incremental Learning from Data Streams)** Tema predmeta so sodobni algoritmi za učenje iz podatkovnih tokov. Učili se bomo o odprtih izzivih na področju (inkrementalni modeli za nadzorovano učenje, stiskanje podatkov, odkrivanje spremembe v porazdelitvi toka	5	15-20-15	

		(concept drift), gručenje iz podatkov, specializirane statistike za vrednotenje uspešnosti). S pridobljenim znanjem bo študent sposoben uporabljati svoje znanje o strojnem učenju pri aplikacijah, ki so povezane z obilico vsakdanjih podatkov (finančne in bančne transakcije, vremenski podatki, senzorski podatki itd.). Predmet bo organiziran kot kombinacija predavanj in laboratorijskih vaj (te bodo izvedene z uporabo statističnega paketa R). V okviru vaj bodo študenti znanje aplicirali na izbranem problemu, ki je lahko direktno povezan tudi s tematiko doktorske naloge. V preostanku semestra bo organizirano tudi medsebojno tekmovanje za izdelavo najbolj točnega napovednega modela na podanih podatkih. The goal of the proposed course is to teach the students about the state-of-the-art algorithms that are used to perform learning from data streams. The course will guide the students through the major open challenges in the field (supervised learning, data compression, concept drift detection, clustering from streams, specialized evaluation statistics). With this knowledge, the students will be able to apply their machine learning skills to a			

		specialized and useful area that is connected to the abundance of data in our everyday lives (bank/weather/financial transactions, sensor readings etc.). The course will be organized by mixing lectures with hands-on lab exercises that the students will do in the Statistical package R. The lab exercises will include applying the acquired knowledge on their own problem and stimulating a competition between students to achieve the best possible learning results.			
Marko Robnik Šikonja (Anand Paul, KNU)	63834C	**Izbrana poglavja iz umetne inteligence 1 (Big Data); izvajanje v bloku feb. 2018** In this course you will develop your knowledge of big data analytics and enhance your programming and mathematical skills. Starting with fundamental data analysis and data visualization suing Power BI and later you will learn to use essential analytic tools such as Hadoop, R, you will also learn about predictive analytics including probabilistic and statistical models. Finally some machine learning methods will also be explored during the	5		15-20-15

		course of this course. By the end of this course, you will be able to approach large-scale data science problems with creativity.			
Marko Robnik Šikonja (Lovro Šubelj)	63835A	**Izbrana poglavja iz umetne inteligence 2 (Napredna poglavja iz omrežne znanosti /Advanced Topics in Network Science)** Omrežja ali grafi so prisotna na vsakem koraku. Primeri vključujejo družabna omrežja, svetovni splet, nevronsko mrežo, sklicevanja med WikiLeaks depešami, Supervizor, pripadnost teroristov, shemo linij LPP, vodovod in človeške možgane. Pri tem pa je v številnih realnih omrežjih moč opaziti karakteristične vzorce povezovanja, ki jih značilno ločijo od regularnega ali naključnega sveta. Omrežja tako predstavljajo pomembno orodje za preučevanje realnih sistemov že od 18. stoletja dalje. Dočim pa lahko manjša omrežja narišemo z roko in preučujemo s prostim očesom, smo pri realnih omrežjih primorani k uporabi specializiranih računalniških algoritmov, tehnik in modelov. Slednje je pred približno 15 leti vodilo k nastanku novega področja imenovanega omrežna znanost.	5		15-20-15

		Predmet bo najprej predstavil jezik omrežij ter podal pregled temeljnih konceptov in tehnik za analizo velikih realnih omrežij. V glavnem delu predmeta bodo študentje spoznali izbrana napredna poglavja omrežne znanosti s posebnim poudarkom na praktični uporabnosti predstavljenih pristopov. Poglavja bodo vključevala metrike vozlišč, vzorce in skupine, globalno zgradbo omrežij ter vzorčenje, primerjavo, modeliranje, rudarjenje, inferenco, prikaz in dinamiko omrežij. Zadnji del predmeta bo namenjen vabljenim predavanjem o omrežni znanosti z vidika matematikov, fizikov, sociologov in drugih. Cilj predmeta ni podati obsežno teoretično diskusijo ali poglobljen pregled izbranih poglavij, ampak predstaviti bogat nabor pristopov omrežne znanosti, ki bi jih študentje lahko uporabili v okviru lastnega doktorskega dela. Slednje bo predstavljalo glavni del obveznosti pri predmetu. Razen jasno zastavljene doktorske teme, predmet ne zahteva posebnega predznanja. Kljub temu pa bo študentom koristilo dobro poznavanje teorije grafov, teorije verjetnosti in linearne algebre, trdno programersko znanje v jeziku po lastni izbiri ter veščine raziskovalnega dela in znanstvenega pisanja.			

		Predmet se izvaja v poletnem semestru z začetkom 29. februarja 2016 in traja štirinajst tednov. Predavanja in vaje bodo potekala v angleščini ali slovenščini. Za več glej eUčilnica. Networks or graphs are ubiquitous in everyday life. Examples include online social networks, the Web, wiring of a neural system, references between WikiLeaks cables, Supervizor, terrorist affiliations, LPP bus map, plumbing systems and your brain. Many such real-world networks reveal characteristic patterns of connectedness that are far from regular or random. Networks have thus been a prominent tool for investigating real-world systems since the 18th century. However, while small networks can be drawn by hand and analyzed by a naked eye, real-world networks require specialized computer algorithms, techniques and models. This led to the emergence of a new scientific field about 15 years ago denoted network science. The course will first introduce the language of networks and review the fundamental concepts and techniques for the analysis of			

		large real-world networks. In the main part of the course, the students will learn about selected advanced topics in network science with special emphasis on the practical applicability of the presented approaches. The topics will include node metrics, groups and patterns, large-scale network structure, network sampling, comparison, modeling, mining, inference, visualization and dynamics. The last part of the course will be devoted to invited talks on network science from the perspective of mathematicians, physicists, social scientists and other. The objective of the course is not to give a comprehensive theoretical discussion or in-depth review on any of the topics, but to present a rich set of network science tools that students could use in their own PhD work. The latter will be the main part of the coursework. Except for a clearly identified PhD topic, there are no specific prerequisites for the course. However, the students will benefit from a solid knowledge in graph theory, probability theory and linear algebra, good programming skills in a language of their choice, and familiarity with research work and scientific writing.			

		The course is offered in the summer semester starting on February 29th, 2016 and lasts for fourteen weeks. Lectures and practice will be held in either English or Slovene. For more see eUcilnica.			
Marko Robnik Šikonja (Sašo Džeroski)	63835B	**Izbrana poglavja iz umetne inteligence 2 (Predictive Analytics for Structured Data)** Študentje se bodo pri predmetu seznanili z različnimi nalogami napovedovanja strukturiranih izhodnih spremenljivk in z različnimi pristopi za njihovo reševanje. Spoznali bodo nekaj najsodobnejših orodij za reševanje te vrste nalog in jih uporabili na praktičnih problemih. Naučili se bodo tudi uporabljati metode napovedne analize strukturiranih podatkov v kontekstu lastnega raziskovalnega dela. Predmet bo zajemal naslednje tematske sklope: 1. Opis različnih nalog napovedovanja strukturiranih izhodnih spremenljivk, kot so uvrščanje/ klasifikacija in regresija z več ciljnih spremenljivk ter (hierarhično) večoznačno uvrščanje.	5		15-20-15

		2. Metode napovednega razvrščanja (na osnovi dreves in pravil) za napovedovanje različnih vrst strukturiranih izhodnih spremenljivk. 3. Ontologije za rudarjenje podatkov in njihova uporaba za opisovanje napovedovanja strukturiranih izhodnih spremenljivk. 4. Ansambelske metode za napovedovanje strukturiranih izhodnih spremenljivk (ansambli dreves in pravil). 5. Uporaba metod za napovedovanje strukturiranih izhodnih spremenljivk pri reševanju različnih praktičnih problemov na področjih kot so znanosti o življenju in okolju ter označevanje in iskanje slik. The course will introduce the students to different tasks of structured output prediction and describe a variety of approaches for solving such tasks. The students will get to know some state-of-the-art tools for solving such tasks and examples of their use in practice. Within the course, the students will learn to apply predictive analytics methods for structured data in the context of their research.			

		The course will cover the following topics: 1. The different tasks of structured output prediction, such as multi-target classification/ regression and (hierarchical) multi-label classification. 2. Predictive clustering methods (tree and rule-based) for structured output prediction. 3. Ontologies for data mining and their use for describing structured output prediction. 4. Ensemble methods for structured output prediction (tree and rule ensembles). 5. Applications of structured output prediction to different practical problems, from areas such as environmental/ life sciences and image annotation/ retrieval.			