

Osnovi teorije informacija i kodovanja

Prof. Milan Milosavljević, predavanja

mmilosavljevic@singidunum.ac.rs

Prof. Marina Marjanović-Jakovljević, vežbe

mjakovljevic@singidunum.ac.rs

Sadržaj kursa

1. Informacione mere (entropija, informacija, uzajamna informacija)
2. Efikasno kodovanje (kodovanje bez prisustva šuma)
3. Kodovanje sa ciljem prenosa po kanalima sa šumom
4. Kodovanje izvora (kompresija govora, muzike, slike, videa)
5. Kodovi za ispravljenje grešaka

Stranica predmeta

<http://predmet.singidunum.ac.rs/course/view.php?id=185>



Stranice predmeta

[Početna strana](#) ▶ [Kursevi](#) ▶ [Fakultet za informatiku i računarstvo](#) ▶ [III godina](#) ▶ [Informatika i računarstvo](#) ▶ [Osnovi teorije informacija i kodovanja](#)

Osnovi teorije informacija i kodovanja

Savremeni razvoj bezbednosnih servisa na Internetu, pokazuje da je informaciono teorijski pristup koji je izložen na ovom predmetu, upravo na frontu najnovijih pravaca razvoja koji već danas mogu obezbediti sisteme zaštite, kontrolisane i izmerljive snage. Time je potpuno osiguran bezbedan sadašnji i svaki budući razvoj Interenta, kao opšte računarsko komunikacione infrastrukture, ključne za razvoj digitalne ekonomije i nove globalne digitalne civilizacije. Pored osnovnog teorijskog pristupa za razumevanje informacionih procesa koje susrećemo u svakom računarsko komunikacionom sistemu, u udžbeniku iz ovog predmeta je predstavljen snažan praktični aparat koji savremenom informatičaru olakšava rešavanje problema koje mu nameće sve složenija i zahtevnija praksa.

Važni datumi:

1 kol: 17.11.2015.

2 kol: 23.12.2015.

Studentske prečice

- [Silabus](#)
- [Podaci o predmetu](#)
- [Obaveštenja](#)
- [Rezultati ispita i kolokvijuma](#)
- [Arhiva](#)

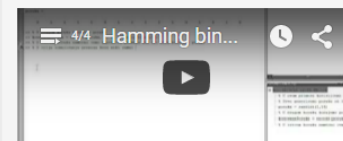
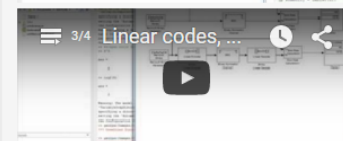
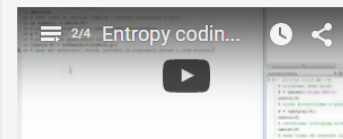
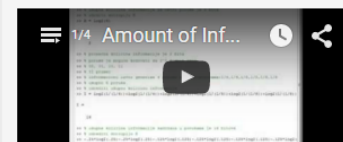
Predavanja

- [Gradivo za I kolokvijum](#)
- [Gradivo za II kolokvijum](#)
- [Gradivo za završni ispit](#)
- [Dodatni materijal](#)

Vežbe

- [Gradivo za I kolokvijum](#)
- [Gradivo za II kolokvijum](#)
- [Gradivo za završni ispit](#)
- [Dodatni materijal](#)

VIDEO MATERIJALI

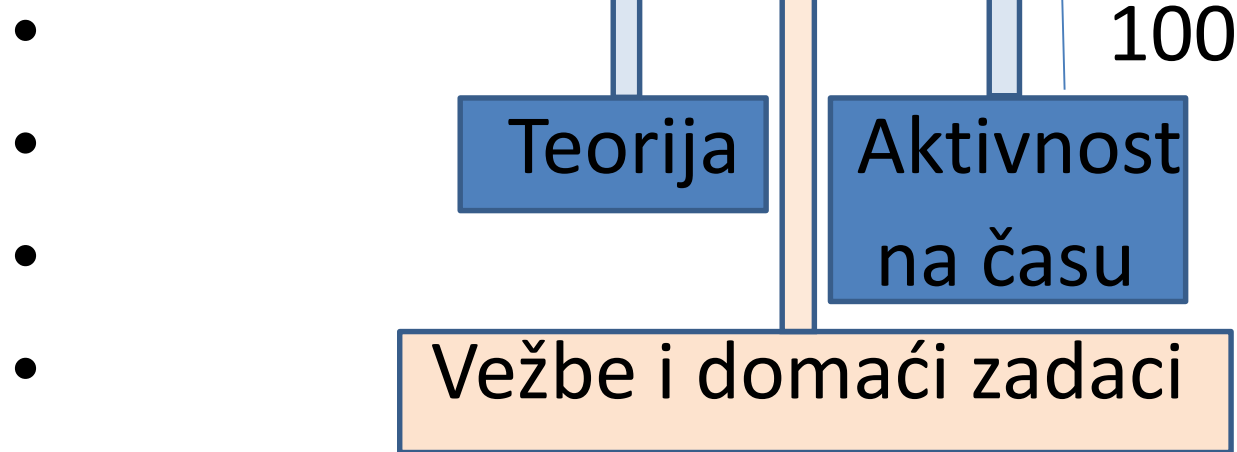


NEDAVNE AKTIVNOSTI

Aktivnost od [utorak, 13. oktobar 2015., 13:26](#)
[Potpuni izveštaj o nedavnim aktivnostima...](#)
Nema skorašnjih aktivnosti

Način polaganja

• I kolokvijum	20 + 10	30
• II kolokvijum	20 + 10	30
• Završni ispit	20 + 10 + 10	40



Raspored predavanja i konsultacija

- Predavanja: Ponedjeljak, 14:00 – 17:00
Kumodraška, sala 110
- Vežbe: Četvrtak, 14:00-16:00
Kumodraška, sala 118
- Konsultacije: Ponedjeljak, 17:00 – 18:00
Danijelova 32, II sprat sala za konsultacije

Zašto je ovaj predmet deo vašeg obrazovanja

- U samom nazivu oblasti kojom ćete se baviti pojavljuje se termin Informatičar, dakle neko ko se služi informatičkim tehnologijama u cilju obrade, memorisanja i prenosa svih vidova informacionih sadržaja u okviru savremenih računarsko komunikacionih sistema
- Već u samoj definiciji informatičara susrećemo tri pojma – obrada, memorisanje i prenos informacija (informacionih sadržaja)

Zašto je ovaj predmet deo vašeg obrazovanja

- Zamislimo da ste prvi dan na poslu u jednoj velike kompaniji. Posao ste dobili nakon mnogo napora i rešeni ste da date sve od sebe.
- Šef vam zadaje sledeći zadatak: Napišite program za saldiranje dnevnih rezultata poslovanja filijala, i dostavite izveštaj centrali kompanije u što kraćem roku.

Zašto je ovaj predmet deo vašeg obrazovanja

- Zadatak br.1: Pisanje programa
- Ako želim da ostavim snažan utisak moj program mora biti najbolji, a to znači da korektno radi i da je pri tome najkraći mogući (najefikasniji)
- Zadatak br.2: Obrada podataka
- Ako želim da ostavim snažan utisak morao bih da znam koji podaci su bitni ili bitniji za moj proraračun, a koji možda uopšte nisu bitni. Time bih ukazao kompaniji na nepotrebno prikupljanje nekih podataka

Zašto je ovaj predmet deo vašeg obrazovanja

- Zadatak br.3: Slanje podataka u centralu kompanije
- Ako želim da ostavim snažan utisak morao bih da znam koji je najefikasniji način dostave, odnosno kako da u što kraćem roku pošaljem podatke koji će biti primljeni bez greške.
- Moja bi se pozicija još više učvrstila ako bih znao da kažem da li podatke treba zaštititi, i ako treba, kojim metodama iz skupa bezbednosnih servisa.

Zašto je ovaj predmet deo vašeg obrazovanja

- Zasigurno bih postao zvezda kompanije ako bih na zahtev šefa da podatke pošaljem apsolutno tajno (dakle da primenjenu šifru niko ne može ni sa kakvim računarskim resursima nikada razbiti) to znao i da uradim i da pri tome garantujem apsolutnu tajnost.
- Promocija bi mi bila osigurana ako bih znao da generišem veliku količinu šifarskih ključeva i da pri tome poznajem metode za njihovu sigurnu distribuciju.

Zašto je ovaj predmet deo vašeg obrazovanja

- Šta je neophodno da znam da bih sve ove zadatke uspešno obavio?
- Šta je informacija, kako se meri?
- Šta je algoritamska složenost i kako se meri?
- Šta su granice kompresije jednog skupa podataka ispod koje se ne može ići bez gubitka dela informacije?
- Šta je uzajamna informacija između dva skupa podataka, odnosno koliko jedan skup podataka sadrži u sebi informacije o onom drugom?

Zašto je ovaj predmet deo vašeg obrazovanja

- Šta je redundansa (suvišnost) jednog izvora informacija i kako se ona može iskoristiti?
- Kako mogu da konstruišem transformaciju podataka koje šaljem ili memorišem, tako da na prijemu ili prilikom očitavanja mogu da ispravljam greške u prenosu ili prilikom memorisanja?

Pojam informacije

- U Teoriji informacija centralni pojam zauzima pojam informacije kao fenomen i komunikacija kao proces.
- Intuitivna predstava pojma informacije je gotovo svima nama bliska, ali naučna zasnovanost i interpretacija informacije utemeljen je tek polovinom prošlog veka radjanjem nove naučne discipline Teorije informacija.
- Informacija je postala relevantan pojam za sve nauke koje se bave simboličkom komunikacijom u rasponu od matematike do računarske nauke, ili od logike do lingvistike, odnosno od elektronike do bibliotekarstva, kao i od humanističkih nauka i umetnosti do dokumentalistike, ali i od društvenih nauka do medicine i dr.

Pojam informacije

- To je informaciji dalo interdisciplinarnu dimenziju, jer je svaka nauka pokušala i još pokušava da protumači taj kompleksan pojam.
- Sve ovo ukazuje da pojam informacija nije lako shvatiti niti jednostavno protumačiti.
- Informacija je reč latinskog porekla *in formare* i izvorno je značila stavljanje u određenu formu, odnosno, davanje oblika nečemu, ali je tokom vremena izgubila prvobitno značenje.

Pojam informacije

- Danas nema jedinstvenog pristupa fenomenu informacije, a još manje jednoznačne i opšte prihvaćene definicije informacije:
- "Ljudi su tvorci i nosioci informacija",
- "Informacija mora, pre svega, da ima određeni smisao, ona mora biti nosilac značenja",
- "Informacija je sve ono što daje nove podatke, ili nova obaveštenja o nekoj činjenici ili nekom događaju, koji nisu bili ranije poznati",

Pojam informacije

- "Informacije su oni delovi vesti koji za primaoca imaju vrednost novosti i koji mu omogućavaju da bolje izvrši svoje zadatke",
- "Informacije su saznanja koja postaju dostupna pomoću sredstava komunikacija, a poseduju obaveštajnu vredenost",
- "... sadržaj onog što razmenjujemo sa spoljnim svetom dok mu se prilagođavamo i dok utičemo na njega",
- "... svesna ili ciljna organizovanost podataka"...

Pojam informacije

- U univerzitetskoj literaturi najčešće definicije pojma informacija su :
- "Informacija je inkrement znanja", njenim postojanjem je naše znanje o nečemu uvećano
- "Informacija je značenje koje dodeljujemo podatku"
- "Informacija je skup podataka u nekom kontekstu,,
- "Informacija je primljena i shvaćena poruka"

Razlika izmedju podatka i informacije

- Važno je napraviti razliku između podatka i informacije, pojmova koji se često poistovećuju.
- Na primer broj 17 je podatak i on kao takav nema posebno značenje.
- "Sada je 17 časova" je informacija jer je podatku dodeljeno neko značenje.
- Tako možemo uvideti da se informacija sastoji od podatka i značenja koje mu je dodeljeno.

Informacioni sadržaj

- Informacija je uvek nošena nekim specifičnim nosiocem (npr. slova, brojevi, specifični simboli, nizovi simbola)
- Informacija se materijalizuje kroz poruke.
- Šta je informacioni sadržaj svake poruke?
- Šenonov odgovor: Informacioni sadržaj poruka se sastoji jednostavno od jedinica (1) i nula (0) upotrebljenih u cilju prenosa.

Informacioni sadržaj

- Stoga je elementarna jedinica informacije binarna jedinica – bit, koja može biti ili 1 ili 0;
istina ili laž; da ili ne; crno ili belo, i sl.
- Jedan od osnovnih postulata teorije informacijaje da se informacija tretira kao merljiva fizička veličina, kao što je masa ili brzina.
- Primer: Zamislimo da bacamo novčić milion puta i pri tome zapisujemo rezultat bacanja. Koliko bita informacija je potrebno prilikom prenosa ovog zapisa nekoj drugoj osobi?
- Ako je verovatnoća svakog ishoda $p=0.5$ (fer bacanje), svako bacanje nosi 1 bit informacije. Za slanje ovog zapisa potrebno je 1 milion bita.

Informacioni sadržaj

- Pretpostavimo da je verovatnoća pisma= $1/4$, a glave $3/4$, tada se celokupna sekvenca može poslati u proseku sa 811 300 bita. Izgleda kao da svako bacanje novčića zahteva samo 0.8113 bita u cilju prenosa.
- Kako je uopšte moguće preneti ishod jednog bacanje novčića sa manje od 1 bita, kada je jedina mogućnost prilikom prenosa da šaljemo samo nule ili jedinice?
- Odgovor je da, naravno, ishod jednog bacanja ne možemo preneti sa manje od jednog bita, ali pošto je cilj prenos celokupne sekvence ishoda bacanja, teorija informacija nam daje rešenje kako se konstruišu kodovi koji omogućavaju efikasan prenos.
- Ovaj primer možemo interpretirati i tako što sekvenca ishoda u drugom slučaju nosi manje informacija od sekvence ishoda u prvom slučaju, tako da je za njen prenos potrebno manje bita.

Informaciono društvo

- Znanje je rezultat učenja.
- Povećanje nivoa znanja dovodi do boljeg odlučivanja.
- Nove informacione tehnologije dovode do ubrzanja i sve većih količina podataka i informacija.

Informaciono društvo

- Sveprisutnost informacija dovela je do toga da savremeno društvo već označavamo kao informaciono društvo.
- Razlog za to ne leži samo u sveprisutnosti, već i ključnom značaju informacija u funkcionisanju gotovo svih ljudskih delatnosti.
- Danas već imamo informacionu teoriju sistema, informacionu teoriju odlučivanja, informacionu ekonomiju, informacionu filozofiju, informacionu teoriju svega u okviru teorijske fizike, informacionu medicinu i tako redom.
- Eksperimentalno je potvrđen revolucionarni novi pristup lečenju, po kome se uzročnicima bolesti, npr. virusima šalje informacija da izvrše sopstveno samouništenje.

Informaciono društvo

- Razvoj tehničkih sistema za prenos i memorisanje informacionih sadržaja, kao što su računari, internet i savremeni digitalni telekomunikacioni sistemi, nisu na adekvatan način praćeni teorijskim rezultatima i relevantnim studijama fenomena informacija, kao i sistema za njeno efikasno kodovanje, prenos, memorisanje i zaštitu.
- Savremena ekonomija pomera svoje težište ka informacionoj ekonomiji. Šta to zapravo znači?

Informaciono društvo

- U klasičnoj ekonomiji cenu robe čine komponente kao što su utrošene sirovine i energija, ljudski rad, amortizacija sredstava za proizvodnju i profit.
- Razvoj sredstava za proizvodnju ide ka tome da će osnovnu komponentu u ovoj ceni sve više da preuzima informacija kako nešto napraviti, a ne neposredna materijalna osnova proizvoda (rad, sirovine, energija).

Informaciono društvo

- Pojavom fuzionih reaktora u kojima se može sintetizovati bilo koja sirovina uz utrošak energije i sirovina zanemarljive cene, dovodi nas u do sada nezamislivi scenario po kome će cena jednog proizvoda biti jednaka ceni informacije potrebne za pravljenje programa koji upravlja sintezom u fuzionom reaktoru.
- Ovo je samo jedan primer koji potvrđuje već postojeće stanje stvari po kome je informacija izborila status resursa, istog kao što je u klasičnoj privrednoj delatnosti to sirovina, energija ili ljudski rad.

Informaciono društvo

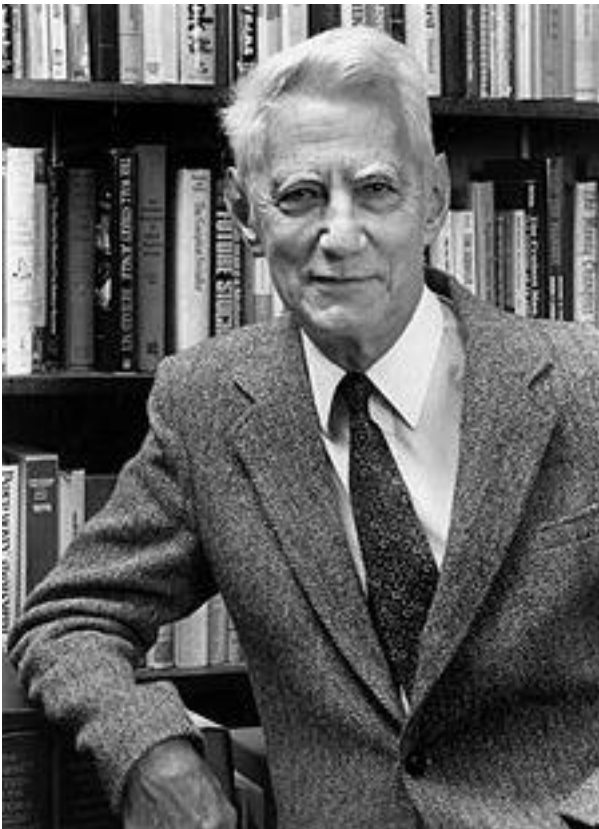
- Ako informacija postaje dominantni resurs privredne delatnosti, onda se tim resursom mora pažljivo rukovati.
- Stoga prenos, memorisanje i zaštita informacija dolaze na prvo mesto, kao kritične tehnologije kojima se obezbedjuje stabilan razvoj i u krajnjoj liniji opstanak jedne društvene zajednice.
- Upravo teorija informacija daje teorijske i praktične okvire za sintezu sistema koji obezbeduju efikasnost i raspoloživost informacionih resursa, shvaćenih na gore pomenuti način.

Informaciono društvo

- Teorija informacija u tehničkom smislu, kako se danas razume i tumači, vodi poreklo od radova Kloda Šenona objavljenih neposredno nakon drugog svetskog rata.
- Šenon je definisao ovu disciplinu kao teoriju za rešavanje problema prenosa signala preko komunikacionih kanala.
- Iako je ovakav pristup danas suviše uzak, pogotovu ako se ima u vidu merenje informacionog (semantičkog) sadržaja poruka koje se memorišu ili prenose, Šenonov pristup predstavlja i dalje centralno jezgro ove teorije.

Teorija informacija kao akademska disciplina

- Teoriju informacija je zasnovao Klod Šenon



Claude Shannon
(1916 - 2001)

- Bell Laboratories (1941-1956)
- Massachusetts Institute of Technology (1956-1978)
- Institute for Advanced Study (1940)

Teorija informacija kao akademska disciplina

- Šenon je tražio odgovor na dva fundamentalna pitanja teorije komunikacija:
 1. Do koje mere se neki skup podataka može komprimovati (odgovor: entropija izvora H)
 2. Šta je krajnja brzina komuniciranja za zadati komunikacioni kanal (odgovor: kapacitet kanala C)

Odnos teorije informacija sa drugim disciplinama-telekomunikacije

- Elektrotehnika (Telekomunikacije)
- Do Šenonovih radova smatralo se da je nemoguće slati informacije pozitivnom brzinom sa zanemarljivom verovatnoćom greške
- Šenon je u svom fundamentalnom radu iz 1948 godine iznenadio celokupnu naučnu zajednicu iz domena telekomunikacija dokazavši da je grešku prenosa moguće smanjiti proizvoljno za sve brzine prenosa ispod kapaciteta kanala.

Odnos teorije informacija sa drugim disciplinama-telekomunikacije

- C. E. Shannon: *A mathematical theory of communication*. Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October, 1948
- Shannon, Claude (1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal 28 (4): 656–715.

Odnos teorije informacija sa drugim disciplinama-telekomunikacije

- Šenon je dalje pokazao da informacioni izvori kao što su muzika ili govor poseduju kompleksnost ispod koje se signali ovih izvora ne mogu dalje komprimovati bez gubitaka.
- Ovu kompleksnost je nazvao *entropija* i razlikovao je od pojma entropije uvedenog mnogo ranije u oblasti termodinamike.
- Dakle, ako je entropija izvora manja od kapaciteta kanala, moguće je dizajnirati komunikacionu šemu koja je asimptotski bez greške prenosa.

Odnos teorije informacija sa drugim disciplinama-telekomunikacije

- Pojava LDPC kodova približava nas Šenonovoj granici (dakle komunikaciji sa maksimalno mogućom brzinom-u blizini kapaciteta kanala, sa nultom greškom prenosa)
- Pojavom Polarnih kodova (Erdal Arikan, 2009) ova magična granica je i dostignuta.
- Front oblasti je danas dominantno tzv. Network coding (mrežno kodovanje), odnosno teorija simultanog komuniciranja više čvorova u jednoj mreži različitim brzinama u prisustvu šumova i interferencija.

Odnos teorije informacija sa drugim disciplinama-računarske nauke

- Kolmogorov, Čaitin i Solomonov su razvili ideju da je kompleksnost jednog niza jednaka dužini najkraćeg računarskog programa koji generiše date podatke.
- Kompleksnost je dakle jednaka dužini minimalnog opisa. (Deskriptivna kompleksnost)
- Pokazalo se da je ideja Kolmogorovljeve kompleksnosti univerzalna i nezavisna od konkretnog računara



Erdal Arikan (1958 -)

Odnos teorije informacija sa drugim disciplinama-računarske nauke

- Kolmogorovljeva kompleksnost K je približno jednaka Šenonovoj entropiji H , ukoliko je posmatrana sekvenca za koju se ona računa izvučena slučajno u skladu sa nekom raspodelom verovatnoća koja ima entropiju H .
- Stoga je veza između Šenonove teorije informacija i Kolmogorovljeve kompleksnosti gotovo perfektna.

Odnos teorije informacija sa drugim disciplinama-fizika

- Statistička mehanika je mesto rođenja entropije i drugog zakona termodinamike. Entropija uvek raste.
- Drugi zakon termodinamike daje teorijsku osnovu za odbacivanje svake tvrdnje o egzistenciji perpetumobila.

Odnos teorije informacija sa drugim disciplinama-matematika

- Fundamentalne veličine teorije informacija: entropija, relativna entropija, uzajamna informacija su definisane kao funkcionali raspodela verovatnoća.
- Sa svoje strane ove veličine dobro opisuju ponašanje dugačkih sekvenci slučajnih veličina i omogućavaju nam procenu verovatnoća retkih događaja (teorija velikih devijacija), kao i ocene error eksponenta pri testiranju hipoteza.

Odnos teorije informacija sa drugim disciplinama-filozofija nauka

- Okamov sekač: Najjednostavnije objašnjenje je najbolje
- Solomonov i Čaitin su ubedljivi u dokazu da je univerzalno najbolja procedura predikcije ona koja uzima težinsku sumu predikcija svih programa koji dobro objašnjavaju podatke.
- Naravno da je ova univerzalna procedura nepraktična, budući da je pronalaženje svih programa koji mogu da objasne date podatke vremenski zahtevan postupak.

Odnos teorije informacija sa drugim disciplinama-ekonomija

- Repetitivne investicije u stacionarno berzansko tržište rezultuje u eksponencijalnom rastu dobitka.
- Rast dobitka je dualan entropiji berzanskog tržišta.
- Postoji jednoznačna veza između teorije optimalnog investiranja u berzansko tržište i teorije informacija.

Odnos teorije informacija sa drugim disciplinama-računarstvo vs. komunikacije

- Pravljenjem velikih računara na osnovu malih komponenti dovodi nas i do računarskih i do komunikacionih limita.
- Računarstvo je limitirano komunikacijom, dok su komunikacije računarski limitirane.
- Stoga su svi rezultati teorije informacija u domenu komunikacija od direktnog uticaja i na računarstvo.