



INFORMATIONSTEORI

Information Theory

EIT080

Antal högskolepoäng: 7,5. **Betygskala:** TH. **Nivå:** G2 (Grundnivå, fördjupad).
Undervisningsspråk: Kursen ges på svenska. **Obligatorisk för:** D3sst. **Valfri för:** C3, C3ks, C3sd, D3, D3ks, E3, MWIR2, Pi3sbs. **Kursansvarig:** Univ.lektor Mats Cedervall, mats.cedervall@it.lth.se, Inst f informationsteknologi. **Prestationsbedömning:** Tentamen (5 tim) är skriftlig och omfattar normalt fem uppgifter av problemtyp. **Hemsida:** <http://www.it.lth.se/courses/informationsteori>.

Syfte

Kursen skall förmedla kunskap om de grundläggande principerna för lagring och överföring av information och om (Shannons insikt) att de binära symbolerna, representerade som nollor och ettor, kan tas till grund för all representation av information. Kursen ger en bredd och ett djup som gör att många av de idag förekommande metoderna samt en stor del av morgondagens kan förstås.

Mål

Kunskap och förståelse

För godkänd kurs skall studenten

- kunna identifiera och formulera problem inom området Informationsteori.
- kunna klassificera problemens svårighetsgrad i förhållande till den egna kunskapsnivån.

Färdighet och förmåga

För godkänd kurs skall studenten

- kunna visa prov på förmåga att hantera för studenten nya metoder och resultat.
- på egen hand kunna realisera system för de i kursen presenterade algoritmerna.

Värderingsförmåga och förhållningssätt

För godkänd kurs skall studenten

på egen hand kunna klassificera problemens svårighetsgrad i förhållande till den egna kunskapsnivån

Innehåll

Shannon gav 1948 en kvantitativ definition av information. Med denna definition kan vi ge gränser för antalet meddelanden som kan överföras eller lagras. Såväl perfekta som

störda överförings- och minnesmedia behandlas. Vi behandlar först fallet med en källa och en mottagare. Teorin generaliseras därefter till en fleranvändarsituation i vilken vi har ett nätverk med flera källor och/eller mottagare.

Informationsteori ☒ vad är det?

Informationsteorins grunder: Shannons informationsmått, Fanos lemma, data processing lemma.

Tre fundamentala kommunikationssatser: Typiska följder, källkodningssatsen, kanalkodningssatsen, starkt symmetriska och symmetriska kanaler, summakanaler, rate-distortion-satsen.

Källkodning: Prefixfri kodning och Krafts olikhet, Huffmankodning, Tunstallkodning. Universell källkodning (Willems☒ algoritm, Ziv-Lempel-kodning), testalgoritmer.

Kanalkodning: Blockfelsannolikhet och avkodningskriterier (maximum a posteriori och maximum likelihood), Bhattacharyyas och Gallagers gränser, Gallagers version av kanalkodningssatsen, träd- och trelliskoder. Fleranvändarkommunikation.

Gausskanalen: Differentiell entropi, tidsdiskret Gausskanal, bandbegränsad Gausskanal, en fundamental gräns.

Kryptering: Grundläggande begrepp, några klassiska system, Shannons teori för sekretess, öppen nyckel-system, Simmons☒ teori för autentisering.

Litteratur

Johannesson R: Informationsteori ☒ grundvalen för (tele-)kommunikation, Studentlitteratur 1988