



INFORMATIONSTEORI

EIT080

Information Theory

Antal poäng: 5. **Betygskala:** TH. **Obligatorisk för:** Pi3XSi. **Valfri för:** C3, D3, E3.

Kursansvarig: Univ.lektor Mats Cedervall, mats.cedervall@it.lth.se, Inst f informationsteknologi. **Prestationsbedömning:** Tentamen (5 tim) är skriftlig och av problemlösningstyp. Som ett alternativ erbjuds möjligheten till muntlig tentamen.

Hemsida: <http://www.it.lth.se/courses/informationsteori>.

Mål

Kunskapsmål

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.

Färdighetsmål

Studenten skall kunna formulera gränser som på ett tydligt sätt anger vilka prestanda som kan uppnås i termer av transmissionshastighet, felsannolikhet, tillgänglig signaleffekt och erforderligt frekvensutnyttjande.

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