hyväksymispäivä arvosana

arvostelija

Claude Shannon – informaatioteorian kehittäjä

Hannele Anttonen

Helsinki 2007
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta/Osasto – Fakultet/Sektion – Faculty/Section	Laitos – Institution – Department	
Matemaattis-luonnontieteellinen	Tietojenkäsittelytiede	
Tekijä – Författare – Author		
Hannele Anttonen		
Työn nimi – Arbetets titel – Title		
Oppiaine – Läroämne – Subject		
Tietojenkäsittelytieteen historia -seminaari		
Työn laji – Arbetets art – Level	Aika – Datum – Month and year	Sivumäärä – Sidoantal – Number of pages
Seminaariraportti		

Tiivistelmä – Referat – Abstract

Claude Shannon (1916-2001) oli yhdysvaltalainen matemaatikko ja sähköinsinööri, joka menestyksekkäästi yhdisti käytännön ja teorian työssään. Shannon loi perustan sekä digitaalitekniikalle että informaatiotekniikalle. Hän myös suunnitteli ensimmäisen shakkipeliohjelman ja teki ensimmäisiä kokeiluja tekoälyllä.

Claude Shannonin mielenkiinto kohdistui moneen suuntaan aina käytännön rakentamisesta teoreettiseen tarkasteluun. Hyödyn tavoittelua tärkeämpää hänelle oli ongelman kiinnostavuus. Monet hänen julkaisunsa liittyivätkin hänen harrastuksiin, kuten shakkiin ja jongleeraukseen.

Avainsanat – Nyckelord – Keywords
Säilytyspaikka – Förvaringställe – Where deposited
Muita tietoja – Övriga uppgifter – Additional information

Sisältö

1 Johdanto

Claude Shannon (1916-2001) oli yhdysvaltalainen matemaatikko ja sähköinsinööri, joka menestyksekkäästi yhdisti työssään käytännön ja teorian. Shannon loi perustan sekä digitaalitekniikalle että informaatiotekniikalle. Seminaarityön ensimmäisessä osassa esittelen Claude Shannonin ja kuvailen häntä henkilönä. Toisessa osassa esittelen osan hänen töistään.

2 Claude Shannonin henkilökuva

Claude Shannon oli mielenkiintoinen persoona sekä ammatillisesti että henkilönä.

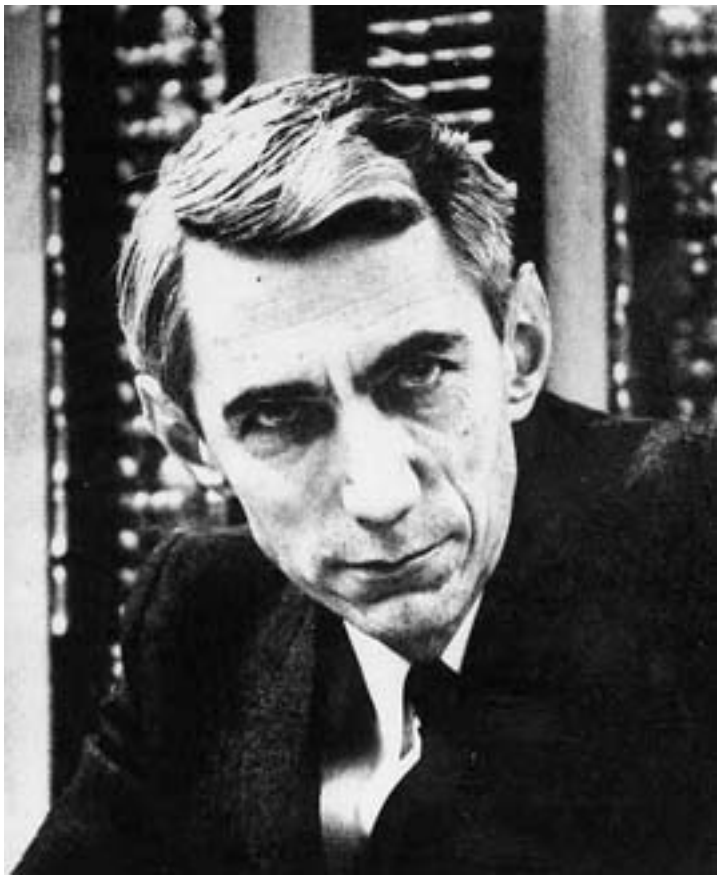
2.1 Elämänkerta

Claude Elwood Shannon syntyi Michiganissa huhtikuun 30. päivä 1916. Shannonin isä oli tuomari ja liikemies, ja hänen äitinsä työskenteli rehtorina ja kieltenopettajana paikallisessa Gaylordin lukiossa, josta Shannon valmistui 16-vuotiaana [Gal01]. Shannon oli etäistä sukua tiedemies Thomas Edisonille [Wik07].

Lukiosta päästyään Shannon suoritti kandidaatin tutkinnon sekä elektroniikassa että matematiikassa University of Michiganissa valmistuen 1936. Vuotta myöhemmin hän suoritti maisterin tutkinnon Massachusetts Institute of Technologyssa (MIT). Shannon väitteli tohtoriksi 1940 aiheenaan teoreettisen perinnöllisyystieteen algebra, mutta tohtorin väitöstyötä ei koskaan julkaistu ja työn tulokset jäivät muille uudelleenkeksittäviksi [Aha04, Wik07]. Shannon siirtyi vuonna 1941 työskentelemään Bell Labsiin tiedon salauksen pariin ja palasi takaisin MIT:iin vuonna 1956 [Wik07].
Bell Labsilta mukaan tarttui vaimo Mary Elizabeth Moore, joka oli samassa paikassa

töissä numeroanalyytikkona. He saivat yhdessä kolme lasta [Aha04]. Shannonin vaimo auttoi miestään tämän työssä tarkastamalla laskelmia ja kirjoittamalla artikkeleita sanelusta [Gal01].

Kuollessaan 84-vuotiaana helmikuun 24. päivä 2001 Shannon sairasti Alzheimerin tautia.



Kuva 1: Claude Shannon 1916-2001 [Kuva1]

Shannonia pidetään yhtenä vuosisadan tärkeimmistä tutkijoista, jossa yhdistyi teoreettinen matemaatikko ja käytännön insinööri. Hänellä oli kyky nähdä ongelmien ytimeen ja usein häntä kiinnosti mielenkiintoinen ongelma sinällään enemmän kuin ongelman ratkaisun soveltaminen johonkin. Hän ei välittänyt saada tunnustusta työlleen ja itse hän väittikin viettäneensä paljon aikaa tehden täysin hyödyttömiä asioita [Aha04, Pri84]. Tämän mahdollisti osaksi henkilökohtainen taloudellinen menestys taitavasti tehtyjen

sijoitusten ansiosta ja osaksi se, että Shannonin työnantaja Bell Labs rohkaisi tutkijoitaan työskentelemään myös tuottamattomien ja turhilta vaikuttavien ongelmien parissa [Gal01, Pie93].

Shannon oli kirjallisesti tuottelias, mutta ei julkaissut kaikkia ideoitaan. Hän ei pitänyt kirjoittamisesta, joten hänellä ei ollut tapana kirjoittaa ajatuksiaan paperille ennen kuin oli saanut kaiken päässään viimeisteltyyn muotoon [Gal01]. Kaiken kaikkiaan Shannonilta on jäänyt 127 julkaistua ja julkaisematonta dokumenttia [Aha04].

2.2 Harrastukset ja kiinnostuksen kohteet

Shannon oli kiinnostunut erilaisista sirkuslajeista kuten jongleerauksesta, hyppykepillä hyppimisestä ja yksipyöräisellä pyöräilystä. Hänen tiedettiin pyöräilevän työpaikkansa käytävillä yksipyöräisellä pyörällään samalla jongleeraten [Gal01]. Shannon harrasti myös shakkia ja musiikkia, ja yhdisti matemaattiset taitonsa harrastuksiinsa suunnittelemalla ja rakentamalla erilaisia laitteita [Aha04].

Jongleeraukseen liittyen Shannon kehitteli jongleerausteoreeman käsien toiminnan ja pallojen aseman välisestä yhteydestä, sekä rakensi koomikko ja näyttelijä W. C. Fieldsin näköisen jongleerauskoneen [Aha04].

Shannon julkaisi vuonna 1950 shakkipelin ohjelmoinnista artikkelin Programming a Computer for Playing Chess [Pie93]. Artikkelissa hän kuvasi, mitä kaikkea koneen pitää tietää ja muistaa ollakseen hyvä vastustaja ihmiselle. Shannon ehdotti minimax-algoritmia seuraavan siirron päätöksentekoon. Shannon teki parannusehdotuksia omaan ohjelmaluonnokseensa, mutta shakkipeliohjelman toteutus jäi muille myöhemmin tehtäväksi silloisten tietokoneiden alkeellisuuden vuoksi.

Shannon rakenteli erilaisia laitteita ja leluja sekä huvin vuoksi että esitelläkseen erilaisia teorioita käytännössä [Pie93]. Eräs hänen laitteistaan oli mekaaninen hiiri, Theseus,

joka liikkui pienessä muunneltavassa labyrintissa etsien 'juustoa'. Kun hiiri oli kerran oppinut reittinsä, se voitiin asettaa mihin tahansa kohtaan labyrintissa, ja se osasi kulkea reitin loppuun oikein. Hiiri oppi myös uuden reitin juuston luo labyrinttia muutettaessa. Theseus-hiiri oli yksi ensimmäisiä yrityksiä toteuttaa oppivia järjestelmiä.

Toinen mainitsemisen arvoinen laite on tietokone, jonka syöte ja tuloste olivat roomalaisia numeroita kuten myös sisäiset operaatiot; yhteen-, vähennys-, jako- ja kertolasku [Pie93]. Tietokonetta kutsuttiin nimellä THROBAC (THRifty Roman numeral BACkward looking computer).

Shannonin huumorintajusta kertoo hänen rakentamansa laatikko, jossa on kytkin ulkopuolella. Kun kytkin laitetaan päälle, laatikosta tulee käsi, joka kääntää kytkimen pois päältä ja vetäytyy takaisin laatikkoon.

3 Ammatilliset saavutukset

Tässä luvussa kerron Shannonin panoksesta digitaalitekniikan ja informaatiotekniikan aloilla.

3.1 Boolen algebra

Suorittaessaan maisterin tutkintoaan MIT:ssä Shannon työskenteli differentiaalianalysaattorin eli eräänlaisen analogisen tietokoneen parissa [Aha04, Wik07]. Opiskellessaan laitetta Shannon tajusi, että Boolen algebrasta voisi olla hyötyä releistä koostuvien piirien analysoinnissa ja suunnittelussa. Maisterin työssään Shannon näytti, kuinka Boolen algebralla ja binääriaritmetiikalla voitaisiin helpottaa piirien suunnittelua ja että asia toimi myös toisinpäin, eli että releistä koostuvilla piireillä voidaan ratkoa Boolen algebran ongelmia [Gal01]. Shannon kirjoitti maisterintyönsä pohjalta ensimmäisen julkaistun artikkelinsa, jolla voitti Alfred Nobelin palkinnon parhaasta alle 30-vuotiaana julkaistusta

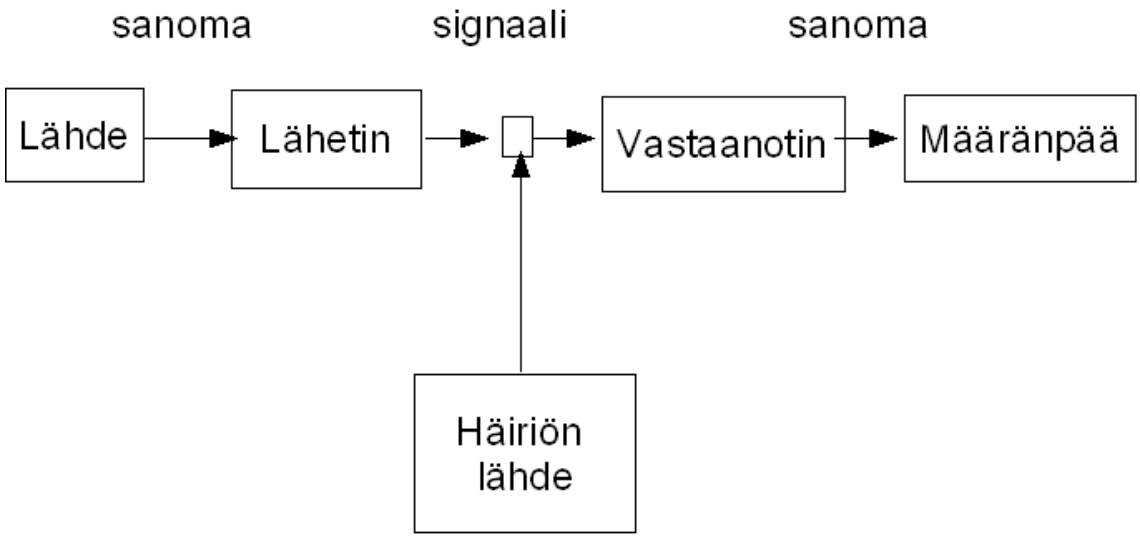
artikkelista [Gal01]. Nimestään huolimatta Alfred Nobelin palkinto on eri asia kuin yleisemmin tunnettu Nobelin palkinto. Shannonin maisterintyö julistettiin kaikkien aikojen tärkeimmäksi ja sitä pidetään pohjana digitaalitekniikalle.

3.2 Informaatioteoria

Shannon aloitti informaatioteorian kehittelyn jo vuonna 1940, mutta julkaisi teoriansa vasta vuonna 1948 laajassa artikkelissaan A Mathematical Theory of Communication [Aha04, Gal01, Sha48]. Näiden kahdeksan vuoden aikana Shannon piti teoriaan liittyvät ajatuksensa päässään, eikä kirjoittanut ainoatakaan luonnosta tai käsikirjoitusta.

Ennen Shannonin julkaisemaa informaatioteoriaa tutkijat osasivat lähinnä lähettää elektromagneettista aaltoa johtoa pitkin ja käsitellä vastaanotettua aaltoa, mutta käsitys siitä, miten sanoma pitäisi muuntaa lähettäväksi aalloksi, oli epämääräinen [Aha04]. Shannon koki, että sanoma on satunnainen valinta jostakin sanomajoukosta. Sanomajoukko oli äärellinen diskreetille kanavalle ja ääretön jatkuvan kanavan tapauksessa. Tämä oli uudenlainen näkemys, mutta erittäin looginen lähetintä rakentavan insinöörin näkökulmasta, koska laitteen rakentaja ei voi tietää, mitä sanomia laitteella lähetetään [Gal01]. Shannon muotoili informaatiojärjestelmän mallin kuvan 2 mukaisesti erottaen sanoman lähteen kanavasta.

Shannonin informaatiojärjestelmän mallissa kuvassa 2 lähetettävä sanoma voi olla hetkellistä, esimerkiksi kirjaimia, tai jatkuvaa, kuten radiolähetys [Sha48]. Lähetin muuntaa sanoman signaaliksi ja lähettää signaalin kanavaa pitkin. Vastaanotin sieppaa signaalin ja muuntaa sen alkuperäistä vastaavaksi sanomaksi sanoman määränpäätä varten. Mallissa näkyy myös kanavassa kulkevaa signaalia häiritsevä kohina, jota aiheuttaa muun muassa johtojen kuumeneminen. Mallia käytetään nykyään lähes kaikissa tietoliikenteen oppikirjoissa.



Kuva 2: Informaatiojärjestelmän malli Claude Shannonin mukaan [Sha48]

Tarkastellessaan sanomaa Shannon yhdisti sanomajoukon vaihtoehtoihin todennäköisyyden. Esimerkkinä artikkelissaan hän käytti englannin kielen rakenteita ja todennäköisyyksiä. Englannin kielessä, kuten muissakin kielissä, tietyt kirjaimet esiintyvät useammin kuin toiset. Toisaalta jotain kirjaimia ei koskaan käytetä yksinään, esimerkiksi 'q'-kirjainta seuraa aina 'u'. Shannonin näkemys tarkoitti, että sanoman sisällöllä tai esityksellä ei ole merkitystä lähetykselle, vaan sanoman käsittely voidaan tehdä erikseen lähettimessä ja vastaanottimessa. Lisäksi Shannonin mukaan kaikki sanomat voidaan esitysmuodostaan riippumatta muuntaa biteiksi eli ykkösiksi ja nolliksi [Sha84]. Bittimuodossa sanoma voidaan generoida uudelleen ja lähettää eteenpäin ilman virheitä.

Shannon tutki artikkelissaan sanoman olemuksen lisäksi kanavaa ja sanoman kulkua kanavassa [Sha48]. Hän määritteli, että kanavan kapasiteetti (C bittiä/sekunnissa) riippuu signaalin voimakkuudesta vastaanottimessa (P), häiriöstä kanavassa (N) ja kaistanleveydestä (W) kaavan

$$C = W * \log_2(\frac{P}{N} + 1)$$

mukaisesti. Shannon todisti matemaattisesti, että jos lähetysnopeus on suurempi kuin

kanavan kapasiteetti, yhteys häiriintyy ja enintään kapasiteetin C verran informaatiota pääsee läpi [Sch06]. Shannon todisti myös, että kaikki sanomat voidaan lähettää kanavaa pitkin halutulla virheprosentilla, jos lähetysnopeus vastaa korkeintaan kanavan kapasiteettia. Virheistä ei pääse kokonaan eroon, mutta niiden määrää voidaan kontrolloida. Virheiden määrää vähennetään suojaamalla sanoma häiriöltä koodaamalla se lähettimessä ja vastaavasti purkamalla koodaus vastaanottimessa häiriön poistamiseksi.

3.3 Tiedonsalauksen teoria

Tiedon salaamisella on yhtäläisyyksiä tiedon lähettämisen teorian kanssa. Shannon julkaisi vuonna 1949 tiedonsalaukseen liittyvän artikkelin Communication Theory of Secrecy Systems [Sha49].

Artikkelissaan Shannon tutki salausjärjestelmiä, joissa sanoman merkitys salataan koodaamalla, mutta joissa sanoman olemassaoloa ei salata. Shannon oletti vihollisen omaavan kaikki tarvittavat laitteet ja taidot sanoman sieppaamiseen ja tallettamiseen [Sha49]. Tarkastelu rajoittui informaatioon, jossa sanoma koostuu diskreeteistä symboleista kuten kirjaimista.

Tärkeä osa tiedon salausta on kielen ominaisuudet. Kieleen kuuluu parametri D, jota kutsutaan kielen toisinnoksi ja joka mittaa, kuinka paljon tekstiä kielestä voidaan poistaa informaatiota hukkaamatta. Tilastollisista rakenteista johtuen englannin kielestä voidaan koodatessa poistaa paljonkin tekstiä.

Esimerkkinä artikkelissaan Shannon esitti tapauksen, jossa käytetään yksinkertaista korvaussalakieltä ja satunnaista avainta. Tällöin englannin kielessä muunnoksia on 26!, eli 26! eri vaihtoehtoa korvata kaikki 26 eri kirjainta. Periaatteessa kaikki vaihtoehdot ovat yhtä todennäköisiä todennäköisyydellä 1/26!, mutta todellisuudessa todennäköisyydet vaihtelevat kirjainten ja sanojen esiintymistiheyden mukaan.

Vihollinen voi sieppaamastaan salakielestä laskea todennäköisyydet erilaisille mahdollisille sanomille ja avaimille, jotka ovat tuottaneet kyseisen salakielen. Shannonin mukaan salaus on täydellinen, jos salakieli ei selviä, vaikka vihollinen saisi siepattua näytteen siitä. Toisin sanoen selväkielen todennäköisyysjakauma ei muutu, vaikka salakieli tunnettaisiin.

Shannon esitti, että vahva ja vaikeasti purettava salausmenetelmä voidaan rakentaa toistamalla yksinkertaisia muunnoksia oikeassa järjestyksessä tarpeeksi monta kertaa tilastollisen analyysin vaikeuttamiseksi. Käytettävät muunnokset ovat diffuusio eli hajottaminen, ja konfuusio eli sekoittaminen.

4 Yhteenveto

Claude Shannonin mielenkiinto kohdistui moneen suuntaan aina käytännön rakentamisesta teoreettiseen tarkasteluun. Hyödyn tavoittelua tärkeämpää hänelle oli ongelman kiinnostavuus. Monet hänen julkaisunsa liittyivätkin hänen harrastuksiinsa.

Shannon loi perustan sekä digitaalitekniikalle että informaatiotekniikalle. Hän myös suunnitteli ensimmäisen shakkipeliohjelman ja teki ensimmäisiä kokeiluja tekoälyllä.

Lähteet

Aha04 Ahammad Parvez, Daskalakis Konstantinos, Etesami Omid, Frome Andrea, Claude Shannon and ”A Mathematical Theory of Communication" lokakuu 2004. http://www.cs.berkeley.edu/~christos/classics/shannon-report.pdf [28.1.2007]

Gal01 Gallager Robert, Claude E. Shannon: A Retrospective on His Life, Work, and Impact. IEEE Transactions on Information Theory, osa 47, numero 7, marraskuu 2001.

Kuva1 http://www.gap-system.org/~history/PictDisplay/Shannon.html [28.1.2007].

Pri84 Price Robert, A Conversation with Claude Shannon – One man's approach to problem solving. IEEE Communications Magazine, osa 22, numero 9, toukokuu 1984.

Pie93 Pierce John R., Looking back – Claude Elwood Shannon. IEEE Potentials, osa 12, numero 4, joulukuu 1993.

Sch06 Schnider Thomas D, Claude Shannon: Biologist. IEEE Engineering in Medicine and Biology Magazine, osa 25, numero 1, 2006.

Sha48 Shannon Claude E., A Mathematical Theory of Communication. The Bell System Technical Journal, osa 27, 1948.

Sha49 Shannon Claude E., Communication Theory of Secrecy Systems. The Bell System Technical Journal, 1949.

http://www.dsm.fordham.edu/~mathai/papers/shannon1949.pdf [25.1.2007].

Sha84 Shannon Claude E., Communication in the Presence of Noise. In the proceedings of the IEEE, syyskuu 1984.

Wik07 Wikipedia, Claude Elwood Shannon. http://en.wikipedia.org/wiki/Claude_Shannon [25.1.2007].