Tietojenkäsittelyn perusteet

Lasse Lensu

2010-11-26

1 (a) Tietojenkäsittely on monimerkityksinen käsite, joten sillä on useita alkuperäiskielisiä vastineita. Se voi tarkoittaa lähes mitä tahansa tietotekniikan soveltamiseen liittyviä toimenpiteitä. Tietojenkäsittelytiede on alaan liittyvää tutkimusta ja sen soveltamista.

2 (b) Computer science (tietojenkäsittelytiede)

3 (c) Information processing (tietojenkäsittely)

4 (d) Artificial science (tekotiede, Herbert A. Simon, 1996); vrt. natural science (luonnontiede)

5 (e) Algorithmics (algoritmiikka, Donald E. Knuth, 1968)

6 Algoritmiikka

- Algoritminen ratkeavuus
  - Laskettavuus
    - (a) Ongelman algoritminen ratkeavuus. (JBo)
    - Osittainen laskettavuus
      - (a) Algoritmi antaa vastauksen, jos se on "kyllä" tai "ei".
  - Churchin ja Turingin teesit
    - 1. Kaikki tunnetut, järkevät algoritmin määritelmät ovat keskenään ekvivalentteja (yhtäpitäviä). (JBo)
    - 2. Mikä tahansa järkevä algoritmin määritelmä ikinä keksitäänkin, se on ekvivalentti (yhtäpitävä) tunnettujen määritelmien kanssa. (JBo)
  - (Algoritmisesti) ratkeamattomat ongelmat
    - 1. Pysähtymisongelma
    - 2. Totaalisuusongelma
    - 3. Ekvivalenssiongelma
- Kompleksisuus
  - Algoritmin kompleksisuus
    - (a) Algoritmin suoritukseen tarvittavien resurssien määrän riippuvuus tehtävän koosta huonoimmassa tapauksessa. (JBo)
  - Asymptoottinen kompleksisuustarkastelu
    - (a) Algoritmin käyttäytyminen (suoritukseen tarvittavat tietokoneresurssit, esim. suoritusaika), kun tehtävän (syötteen) koko n kasvaa suuremmaksi. (JBo)

        - Kompleksisuuden suuruusluokka
            - (a) Algoritmin kompleksisuus on samaa suuruusluokkaa kuin funktio f(n); vrt. kompleksisuuden kertaluokat. (JBo)
        - Kompleksisuuden yläraja
            - (a) Algoritmin kompleksisuus on enintään f(n); vrt. kompleksisuuden kertaluokat. (JBo)
    - Kompleksisuuden kertaluokat
        - 1. Vakioaikainen
        - 2. Logaritminen
        - 3. Lineaarinen
        - 4. Polynomiaalinen
        - 5. Eksponentiaalinen
    - Tehtävän kompleksisuus
        - (a) Parhaan (tunnetun) algoritmin suoritukseen tarvittavien resurssien määrän riippuvuus tehtävän koosta. (JBo)
    - Tärkeimmät tietokoneresurssit
        - 1. Aika
        - 2. Muistitila
        - 3. Laitteisto
- Oikeellisuus
    - Testaus
    - Oikeaksi todistaminen
        - 1. Induktioperiaate
        - 2. Invariantit
        - 3. Peräkkäiset väitteet
        - 4. Terminoituvuus

7 Algoritminen ongelmanratkaisu

- Algoritmi
    - (a) Jonkin tehtävän suorittamiseksi tarvittavien toimenpiteiden kuvaus. (JBo)
    - (b) Algoritmi on äärellinen käskyjoukko, jonka seuraaminen toimittaa tietyn tehtävän. (Eho)
    - 1. Ominaisuudet
        - 1. Yleisyys
            - (a) Algoritmi soveltuu määritellyn tehtävän kaikkiin tapauksiin. (Jorma Boberg, 2010)
        - 2. Deterministisyys
            - (a) Tehtävän ratkaisu on yksikäsitteisesti määritelty. (JBo)
            - (b) Algoritmin jokaisessa vaiheessa tiedetään, mitä tehdään ja mitä seuraavaksi tehdään. (JBo)
        - 3. Tuloksellisuus
            - Oikeellisuus
                - (a) Algoritmin antama tulos on oikein kaikissa tehtävän määrittelyn mukaisissa tapauksissa. (JBo)
            - Terminoituvuus
                - (a) Algoritmin suoritus päättyy aina. (JBo)
        - 4. Syöte
            - (a) Algoritmi (voi) käyttää ulkopuolista tietoa suorituksensa aikana. (EHo)
        - 5. Tehokkuus

- (a) Jokainen algoritmin toimenpide on riittävän yksinkertainen ja siten toteuttamiskelpoinen. (EHo)

- 2. Laadinta/suunnittelu
  - Asteittainen tarkentaminen
    - (a) Ongelman ratkaisevan algoritmin kehittäminen reduktioperiaatteella aloittaen karkeasta ratkaisun kuvauksesta.
  - Esitystapa
    - Kuva
    - Vuokaavio
    - Kieli
      - 1. Syntaksi #ID_1139024424
        - (a) Kielioppi
      - 2. Semantiikka
        - (a) Merkitys
      - 3. Pragmatiikka
        - (a) Kielen käytön taito
        - (b) Asiayhteyden vaikutus merkitykseen
      - Formaali
        - C
        - C++
        - Java
        - Python
      - Luonnollinen
        - Suomi
      - Puoliformaali
        - Pseudokieli http://staff.cs.utu.fi/staff/jorma.boberg/Mat/Syntaksi.pdf
          - (a) Tarkoitus on kiinnittää huomio algoritmien toteutusperiaatteisiin ja lauseiden merkitykseen.
  - Luovuutta vaativa tehtävä; ei voida automatisoida. (JBo)
  - Modulaarisuus
    - (a) Kunkin osaongelman ratkaisu kootaan itsenäiseksi moduuliksi. (JBo)
  - Reduktio
    - 1. Ongelman jakaminen osiin. (JBo)
    - 2. Osaongelmien ratkaisu erikseen. (JBo)
    - 3. Osaratkaisujen kokoaminen koko ongelman ratkaisuksi. (JBo)
  - Vaatimuksena kattava ja yksiselitteinen tehtävänmäärittely. (JBo)
  - Ratkaisustrategia
    - Iteraatio
      - (a) Iteratiivinen moduuli sisältää päättyvän toistorakenteen. (JBo)
      - (b) Jotakin toimenpidettä toistamalla päästään lähemmäksi ratkaisua. (JBo)
      - 1. Ratkaisuun liittyvät väliarvot
      - 2. Toimenpiteet edetä kohti ratkaisua
      - 3. Kyky tunnistaa ratkaisu
    - Rekursio
      - (a) Rekursiivinen moduuli kutsuu itseään alkuperäisestä poikkeavin parametrein. (JBo)
      - 1. Moduulissa tulee kuvata ongelman ratkaisu ainakin

yhdessä triviaalitapauksessa.
        - 2. Rekursiivisten kutsujen tulee lähestyä jotakin triviaalitapausta.
    - Raaka voima
        - (a) Kokeillaan kaikki vaihtoehdot ja valitaan paras. (SAl)
    - Inkrementaalinen algoritmi
        - (a) Ongelman ratkaisua rakennetaan pala kerrallaan; vrt. iteraatio. (SAl)
    - Ahne algoritmi
        - (a) Jokaisessa vaiheessa valitaan paras tarjolla olevista vaihtoehdoista. (SAl)
    - Perääntyminen
        - (a) Perääntymisessä palataan edelliseen valintatilanteeseen ja valitaan jokin toinen vaihtoehto, josta jatketaan eteenpäin. (SAl)
    - Hajoita ja hallitse
        - (a) Hajoita ongelma osiin, ratkaise osaongelmat rekursiivisesti ja kokoa ongelman ratkaisu osista. (SAl)
    - Dynaaminen ohjelmointi
        - (a) Välituloksia talletetaan laskennan aikana taulukkoon, jolloin samaa
          tulosta ei tarvitse laskea montaa kertaa. (SAl)
    - Satunnaisalgoritmi
        - (a) Valinnan perusteena käytetään satunnaislukua. (SAl)
- 3. Ohjelmointi
    - Imperatiivinen ohjelmointisuuntaus
        - (a) Algoritmin kukin toimenpide esitetään käskymuodossa.
        - Moduuli
            - Parametri(t)
                - (a) Syötetieto algoritmin moduulille.
                - Muodollinen parametri
                    - (a) Muuttujan nimi funktion/proseduurin määrittelyssä
                - Todellinen parametri
                    - (a) Muuttujan arvo funktiota/proseduuria kutsuttaessa
            - Proseduuri
                - (a) Algoritmin moduuli, joka ei palauta arvoa.
            - Funktio
                - (a) Algoritmin moduuli, joka palauttaa arvon.
        - Muuttuja
            - (a) Jollekin tiedolle varattu muistipaikka.
        - Ohjausrakenne
            - Valinta
                - (a) Ehtolausekkeen arvo määrää haarautumisen algoritmissa.
            - Toisto
                - Definiitti toisto
                    - (a) Toistokertojen lukumäärä tiedetään etukäteen (JBo)
                    - Askeltava toisto
                        - (a) Tietty joukko askelletaan läpi määritellyllä tavalla
                    - Yksinkertainen toisto
                        - (a) Ilmoitetaan suoraan toistokertojen lukumäärä (JBo)

            - Indefiniitti toisto
                - (a) Toistokertojen lukumäärää ei tiedetä etukäteen, vaan sen määrää toistoehto (JBo)
                - Alkuehtoinen toisto
                    - (a) Toistoehto arvioidaan heti ennen yhdenkään toiminnon suoritusta
                - Loppuehtoinen toisto
                    - (a) Toistoehto arvioidaan toiston toimintolohkon yhden suorituksen jälkeen
        - Ohjelmointikieli
            - Syntaksi
                - (a) Säännöt kieleen kuuluville sanoille ja rakenteille.
                - Backus-Naur -muoto (BNF).
                - Syntaksikaavio
    - 4. Kääntäminen suorittajan ymmärtämälle kielelle
        - 1. Selaaminen eli leksikaalinen analyysi
            - (a) Tekstialkioiden ja niiden (tieto)tyyppien selvittäminen.
            - Tuottaa tekstialkioiden listan ja symbolitaulun (tunnukset)
        - 2. Jäsentäminen eli syntaktinen analyysi
            - (a) Lähdekielisen esityksen syntaktisen rakenteen selvittäminen.
            - Kokoava jäsennys (bottom-up)
            - Osittava jäsennys (top-down)
            - Tuottaa jäsennyspuun
        - 3. Kohdekielen tuottaminen
            - (a) Tuotetaan kohdekieltä jäsennyspuun ja symbolitaulun avulla.
            - Kohdekielen lauseiden/käskyjen tuottaminen
            - Koodin optimointi
            - Muistin varaaminen muuttujille ja tietorakenteille
            - Tuottaa kohdekielisen esityksen
        - Kielten määrittely
            - Sanojen/rakenteiden ominaisuudet
                - (a) Kuvataan kieleen kuuluvat sanat esim. matemaattisen lausekkeen avulla.
            - Automaatti
                - (a) Kielen hyväksyvä automaatti, joka koostuu tiloista ja tilasiirtymistä.
            - (Chomskyn) kielioppi
                - (a) Säännöt kieleen kuuluville sanoille ja rakenteille.
                - Päätesymbolit eli terminaalit
                    - (a) Kielessä sallittuja ilmaisuja.
                - Välisymbolit eli nonterminaalit
                    - (a) Kieliopin "muuttujia", jotka korvautuvat tulkittaessa toisilla väli- tai päätesymboleilla.
                - Produktiosäännöt
                    - Johtopuu
                        - (a) Kielen ilmaisujen johtamisen tulos.
                - Alkusymboli
                    - (a) Välisymboli, josta ilmaisun tulkinta tai tuottaminen alkaa.
        - Kielityypit
            - 0. Tyypin 0 Kieli
                - (a) Laajin mahdollinen kieli.

        - 1. Yhteysriippuva kieli
            - (a) Kielen ilmaisujen tulkinta riippuu asiayhteydestä; sanojen tulkinta ympärillä olevista sanoista.
        - 2. Yhteysvapaa kielioppi
            - (a) Kielen ilmaisut tulkitaan huomioiden vain ko. ilmaisu; ympäristö ei vaikuta.
        - 3. Säännöllinen kieli
            - (a) Vain yksinkertaiset ilmaisut mahdollisia.
        - 4. Äärellinen kieli
            - (a) Kieleen kuuluvat sanat/rakenteet voidaan luetella.
    - 5. Suoritus
        - Lataus
            - (a) Käännetty ohjelma ladataan oheismuistista keskusmuistiin ja alustetaan suoritusta varten.
        - Suoritusjärjestys
            - Peräkkäinen
                - (a) Algoritmin suoritus yhden suorittajan toimesta etenee yksi käsky kerrallaan ohjausrakenteiden mukaisesti.
            - Rinnakkainen
                - (a) Algoritmia suoritetaan samanaikaisesti usean suorittajan toimesta.
            - Vapaajärjesteinen
                - (a) Algoritmin osia sovelletaan tarpeen mukaan eri järjestyksessä ongelman ratkaisemiseksi.
                - Perustuu tyypillisesti itse ongelman kuvaukseen sen ratkaisun kuvauksen sijaan.
        - Tietokone
          #ID_116372176
        - Tulkkaus
            - (a) Jokainen lause/käsky tulkitaan (ilman kääntämisvaihetta) ja suoritetaan välittömästi.
- (a) Tehtävän määrittely, algoritmin laadinta, ohjelmointi ja suoritus sekä ratkaisun tulkinta. (JBo)
- Algoritminen ongelmanratkaisuprosessi
    - 1. Ongelman ymmärtäminen
    - 2. Algoritmin ideointi
    - 3. Algoritmin laadinta ja sen esittäminen ohjelmana
    - 4. Algoritmin tarkkuuden ja sen yleistettävyyden arviointi

8 Käsitekartan lähdeluettelo

- EHo: Ellis Horowitz et al. Fundamentals of Data Structures in C. Computer Science Press, 1993.
- EOj: Erkki Oja, Logiikka tietämyskielenä, LUT.
- GPo: George Polya, How to Solve It, 1945.
- JBo: Jorma Boberg, Johdatus tietojenkäsittelytieteeseen, Turun yliopisto, 2010.
- JKo: Jukka Koskinen, Logiikkaa ja Boolen algebrat, LUT.
- OED: Oxford English Dictionary.
- SAl: Satu Alaoutinen, LUT, 2008.
- SSi: Simon Singh, Koodikirja, Tammi, 1999.
- VVo: Vilkko Virkkala, Luova ongelmanratkaisu, Vilkko Virkkala, 1994.

9 Ongelma

- Deterministininen
  - (a) Suorituksen jokaisessa vaiheessa on tarkkaan tiedossa, millä tavalla suoritusta jatketaan. (JBo)
  - (b) Sama syöte saa aikaan aina samojen valintojen tekemisen. (JBo)
- Epädeterministinen
  - (a) Hakuongelmissa toimenpiteiden joukko etukäteen tiedossa. (JBo)
  - (b) On epäselvää, mistä vastaus löytyy (mihin suuntaan haussa edetään). (JBo)
  - Esimerkiksi peli, jossa sen kulku alkutilanteesta päätökseen ei ole etukäteen tiedossa.
- Hakuongelma
  - (a) Kuvataan tilaesityksen avulla.
  - Hakuavaruus
    - (a) Graafi, jossa on kaikki mahdolliset tilat ja niitä yhdistävät siirrot. (JBo)
  - Hakupuu
    - (a) Talletuspaikka siirroille, joita kokeillaan hakuavaruudessa lopputilaa haettaessa. (JBo)
  - Ratkaisupolku
    - (a) Hakupuun polku puun juuresta (alkutilasta) puun lehteen, jossa on lopputila. (JBo)
  - Äärellinen hakuongelma
    - (a) Hakuavaruus äärellinen, joten se voidaan muodostaa kokonaisuudessaan haun aikana. (JBo)
  - Ääretön hakuongelma
    - (a) Hakuavaruus ääretön, joten graafia ei koskaan pystytä muodostamaan kokonaan. (JBo)
  - Leveyshaku
    - (a) Haku etenee leveänä rintamana joka suuntaan yhtä pitkälle. (JBo)
    - (b) Käyttää tilojen säilyttämiseksi jonoa. (JBo)
  - Syvyyshaku
    - (a) Haku lähtee parhaana pidettyyn suuntaan; suuntaa muutetaan ainoastaan, jos joudutaan perääntymään. (JBo)
    - (b) Käyttää tilojen säilyttämiseksi pinoa. (JBo)
  - Heuristiikka
    - (a) Missä järjestyksessä tutkimattomat tilat viedään jonoon/pinoon: järjestys, jossa tilat läpikäydään.
    - (b) Merkitystä vain syvyyshaussa. (JBo)
    - Esimerkiksi pelin pelaaminen heuristisen arviofunktion ohjaamana.

10 Tieto

- Data
  - (a) Asian säännönmukainen esitys viestitettävässä tai käsittelykelpoisessa muodossa. (JBo)
  - (b) The quantities, characters, or symbols on which operations are performed by computers and other automatic equipment, and which may be stored or transmitted in the form of electrical signals, records on magnetic tape or punched cards, etc. (OED)

- Informaatio
  - (a) Datan ihmiselle tuottama mielle tai merkitys. (JBo)
  - (b) As a mathematically defined quantity divorced from any concept of news or meaning; spec. one which represents the degree of choice exercised in the selection or formation of one particular symbol, message, etc., out of a number of possible ones, and which is defined logarithmically in terms of the statistical probabilities of occurrence of the symbol or the elements of the message. (OED)
  - (c) Separated from, or without the implication of, reference to a person informed: that which inheres in one of two or more alternative sequences, arrangements, etc., that produce different responses in something, and which is capable of being stored in, transmitted by, and communicated to inanimate things. (OED)
  - (d) That which is obtained by the processing of data. (OED)
  - Informaatioteoria
    - (a) Tuloksen (epä)todennäköisyys eli todennäköisimmät tapahtumat ovat vain vähän informatiivisia.
    - Liittyy kommunikaatioon osapuolten välillä.
    - Entropia
      - (a) Tapahtumasarjan keskimääräinen informaatio.
      - (b) Lyhin keskimääräinen viestin pituus, jolla satunnainen data voidaan välittää.
- Päättely
  - (a) Matemaattisen logiikan hyödyntäminen tietoon (väittämiin) perustuvien totuuksien ja johtopäätösten muodostamisessa.
  - 1. Propositiologiikka
    - (a) Propositioita käsittelevä formaalinen kieli.
    - (b) Yksinkertaisin klassisen logiikan muoto.
    - (c) Synonyymejä: lauselogiikka, nollannen kertaluvun logiikka.
    - 1. Propositiokirjaimet
      - (a) Äärellinen joukko symboleja, jotka edustavat jakamattomia väitteitä (atomilauseita) ja joilla on totuusarvo tosi (T) tai epätosi (E).
    - 2. Logiikan konnektiivit
      - Negaatio
        - (a) "Ei"
      - Disjunktio
        - (a) "Tai"
      - Konjunktio
        - (a) "Ja"
      - Konditionaali
        - (a) "Jos, niin"
      - Bikonditionaali
        - (a) "Jos ja vain jos"
      - Peircen viiva
        - (a) "Ei, eikä"
      - Shefferin viiva
        - (a) "Ei sekä että"
      - Ekskluviivinen disjunktio
        - (a) "Joko tai"
    - 3. Päättelymenetelmät
      #ID_1024884479

- 2. Predikaattilogiikka
- 3. Intensionaalinen logiikka
- 4. Moniarvoinen logiikka
- 5. Sumea logiikka
- Asiantuntijajärjestelmät
- Formalisointi
  - (a) Luonnollisella kielellä esitettyjen väittämien muuntaminen matemaattisen logiikan formaaliin esitykseen.
- Päätelmä
- Päättelymenetelmät
  - (a) Säännöt sille, millainen johtopäätös voidaan tehdä annetuista premisseistä eli oletuksista.
  - Semanttinen menetelmä
    - (a) Täytetään propositiosta totuustaulu kattaen kaikki totuusarvoyhdistelmät: jos tautologia, niin pätevä päättely.
    - (b) Sievennetään propositio todeksi käyttäen sievennyssääntöjä eli lauseiden välisiä loogisia ekvivalensseja ja implikaatioita.
  - Syntaktinen menetelmä
    - (a) Käytetään valmiiksi päteviksi osoitettuja päättelysääntöjä muuntamaan propositiota kohti haluttua muotoa.
    - Suorassa todistuksessa tuotetaan uusia propositioita premisseistä ja aikaisemmin tuotetuista propositioista hakien todistettavaa propositiota.
    - Ristiriitatodistuksessa muuntelulla haetaan ristiriitaa todistettavan proposition kanssa.
  - Resoluutiomenetelmä
    - (a) Resoluutiosääntöä hyödyntävä iteratiivinen menetelmä.
    - 1. Muunnetaan premissit normaalimuotoon ja muodostetaan niistä klausuulijoukko.
    - 2.a) Suorassa todistuksessa sovelletaan resoluutiosääntöä täydentäen klausuulijoukkoa ja hakien todistettavaa klausuulia.
    - 2.b) Ristiriitatodistuksessa lisätään klausuuleihin todistettavan negaatio ja sovelletaan resoluutiosääntöä täydentäen klausuulijoukkoa ja hakien tyhjää joukkoa.
    - Normaalimuodot
      - Disjunktiivinen normaalimuoto
        - (a) Alkeiskonjunktioita yhdistävät disjunktiot.
      - Konjunktiivinen normaalimuoto
        - (a) Alkeisdisjunktioita yhdistävät konjunktiot.
- Tekoäly
- Totuusarvo
  - (a) Tosi (T, 1, True)
  - (b) Epätosi (E, 0, False)
  - Tautologia
    - (a) Propositio (logiikan lause) on tosi riippumatta atomilauseiden totuusarvoista.
    - (b) Looginen ekvivalenssi.
  - Kontingentti
    - (a) Propositio ei ole tautologia eikä kontradiktio eli se on toteutuva tai kumoutuva riippuen atomilauseiden totuusarvoista.
  - Kontradiktio

            - (a) Propositio (logiikan lause) on epätosi riippumatta atomilauseiden totuusarvoista.
- Tiedon koodaus
    - Lukujärjestelmät
        - Binäärijärjestelmä
            - Kantaluku: 2
        - Kantaluku
            - (a) Luvun esittämiseen käytettävissä olevien numerosymbolien lukumäärä. (JBo)
        - Oktaalijärjestelmä
            - Kantaluku: 8
        - Kymmenjärjestelmä
            - Kantaluku: 10
        - Heksadesimaalijärjestelmä
            - Kantaluku: 16
        - Desimaaliluvut
            - Kiinteä (desimaali)pilkku
            - Liukuluku
                - Etumerkki
                - Mantissa
                - Eksponentti
    - Merkkijärjestelmät
        - ASCII
            - 7 bittiä merkkiä kohti.
        - Latin-1, 2, ...
            - 8 bittiä (1 tavu) merkkiä kohti.
            - ISO 8859 -standardi
        - Unicode transformation format (UTF)
            - 8-32 bittiä (1-4 tavua) merkkiä kohti.
        - Universal character set (UCS)
            - 8-32 bittiä (1-4 tavua) merkkiä kohti.
            - ISO 10646 -standardi
    - Muunnokset
    - Tietotyypit
        - Kokonaisluvut
            - Etumerkittömät kokonaisluvut
                - Esitetään suoraan binäärijärjestelmässä.
            - Etumerkilliset kokonaisluvut
                - 1. Etumerkki ja luvun itseisarvo
                - 2. Yhden komplementti
                    - (a) Kaikki bitit käännetään niiden komplementeiksi.
                - 3. Kahden komplementti
                    - (a) Kaikki bitit käännetään niiden komplementeiksi + 1.
        - Liukuluvut
        - Merkit
        - Totuusarvot
    - Tietorakenteet
        - (a) Abstrakti tapa tallettaa tietoa rakenteisessa muodossa.
        - Lista
            - (a) Peräkkäinen kokoelma tietoalkioita.
            - Jono
                - (a) Lista, jossa tiedon lisäys ja poisto tapahtuu eri päähän.

        - Linkitetty lista
            - (a) Tietoalkioiden kokoelma, jossa alkioiden väliset viittaukset on toteutettu osoittimilla.
        - Pino
            - (a) Lista, jossa tiedon lisäys ja poisto tapahtuu samaan päähän.
        - Taulukko
    - Puu
        - Binääripuu
            - (a) Kullakin puun solmulla voi olla vain kaksi lapsisolmua.
        - (a) Kokoelma hierarkkisesti järjestettyä tietoa.
    - Taulukko
        - (a) Samantyyppisten alkioiden vakiomääräinen kokoelma.
    - Tietue
        - (a) Erityyppisten kenttien kokoelma.
- Tiedon tiivistäminen
    - (a) Tiedon uudelleen koodaus siten, että sen tallettamiseen tai siirtämiseen tarvitaan vähemmän kapasiteettia.
    - Tiivistämissuhde
        - (a) Kuinka suuren osuuden tiivistetty tieto vaatii alkuperäiseen verrattuna.
    - Kiinteäpituinen koodi
        - (a) Jokainen alkuperäinen symboli saa samanpituisen koodin.
    - Muuttuvapituinen koodi
        - (a) Alkuperäiset symbolit voivat saada eripituisia koodeja.
    - Häviöllinen tiivistys
        - (a) Alkuperäistä tietoa menetetään.
        - Differentiaalinen pulssikoodimodulaatio
            - Koodattava tieto määräytyy tietoalkion ja sen edeltäjien perusteella.
        - Muunnoskoodaus
            - Diskreetti Fourier-muunnos
                - Muunnettu kuva kertoo, mitä taajuuksia (minkä kokoluokan yksityiskohtia) kuvassa on.
            - Diskreetti kosinimuunnos
    - Häviötön tiivistys
        - (a) Alkuperäinen tieto säilytetään.
        - Entropia määrää rajan tiivistämissuhteelle.
        - Huffman-koodi
            - Useimmin esiintyville merkeille lyhin bittikuvio.
        - Jononpituuskoodaus
            - (a) Koodataan alkuperäisten symbolien peräkkäisiä jonopituuksia.
        - Lempel-Ziv-Welch -koodi
            - Muodostaa taulukkoa esiintyneistä sanoista.
        - Q-koodi
            - Käyttää koodattavan merkin todennäköisyyden laskemiseen lähiympäristön merkkejä.
- Tiedonlähteet
    - Asiantuntijat
    - Kirjallisuus ja muu historiatieto
    - Mittaukset

        - Suureet
            - Aika
            - Kulma
            - Lukumäärä
            - Paino ja tiheys
            - Pinta-ala ja tilavuus
            - Pituus, etäisyys ja paikka
            - Raha ja arvo
            - Yksiköt
                - Metrinen järjestelmä
                - SI-järjestelmä
        - Kohteet
            - Luonto
            - Ihminen
        - Ominaisuudet
            - Tarkkuus
                - (a) Mittaustuloksen poikkeama suureen todellisesta arvosta.
            - Täsmällisyys
                - (a) Mittauksen toistettavuus eli tuloksen yhtenevyys muiden mittausten kanssa.
            - Virhe
                - (a) Mittaustuloksen ja suureen todellisen arvon erotus.
            - Epävarmuus
                - (a) Mittauksen toistamisesta huolimatta tulokseen jäävä epätietoisuus haluttaessa tulokselle tietty tilastollinen luotettavuus.
        - Kalibrointi
            - Jäljitettävyys
        - Analogiset
            - Jatkuva-aikaiset mittaukset/signaalit
            - Jatkuva-arvoiset mittaukset/signaalit
        - Digitaaliset
            - Diskreettiaikaiset mittaukset/signaalit
                - Näytteistystaajuus
            - Diskreettiarvoiset mittaukset/signaalit
                - Signaalinvoimakkuustasojen lukumäärä näytettä kohti
- Tietokone
    - (a) Algoritmien "mekaaninen" suorittaja.
    - Turingin kone
        - (a) Abstrakti tietokoneen malli, jolla voidaan suorittaa kaikki mahdolliset algoritmit.
        - (b) Algoritmi on Turingin kone, joka syötteen saatuaan pysähtyy äärellisen ajan kuluessa.
        - Luku-/kirjoituspää
            - (a) Nauhan muistipaikan luku- ja kirjoitusväline.
        - Nauha(t)
            - (a) Äärettömän pitkä soluja sisältävä muisti.
            - Nauhan solu
                - (a) Muistipaikka, joka voi sisältää minkä tahansa symbolin sallittujen nauhasymbolien joukosta.
            - Nauhasymbolien joukko
                - (a) Mitä symboleja nauhalla voi esiintyä.

        - Syötesymbolien joukko
            - (a) Mistä symboleista syöte voi muodostua.
        - Tyhjä symboli
            - (a) Erotinmerkki.
    - Ohjausyksikkö
        - (a) Ohjaa nauhan lukua ja kirjoittamista sekä luku-/kirjoituspään siirtämistä tilasiirtymäkaavion mukaisesti.
        - Mahdollisten tilojen joukko
            - Alkutila
            - Lopputila(t)
                - (a) Hyväksyvien lopputilojen joukko (Turingin kone on automaatti).
            - Siirtymäfunktio
                - (a) Kuvaus tilojen ja nauhasymbolien joukosta tilojen, nauhasymbolien ja luku-/kirjoituspään ohjauskomentojen joukkoon.
- Tietoturva
    - Avaaminen
        - (a) Kooditekstin purkaminen alkuperäiseksi selväkieliseksi tekstiksi. (SSi)
    - Avain
        - (a) Salaamista tai allekirjoitusta varten tuotettu tekijä, joka muuttaa yleisen salausalgoritmin määritellyksi salaamismenetelmäksi. (SSi)
        - Julkinen avain
            - (a) Salaukseen liittyvä tekijä, joka on kaikkien tiedossa.
        - Salainen avain
            - (a) Salaukseen liittyvä tekijä, joka on vain kommunikoivien osapuolten tiedossa.
    - Kryptoanalyysi
        - (a) Oppi selväkielisen tekstin, salausmenetelmän tai avaimen päättelemiseksi kooditekstistä ilman tietoa yksityiskohdista. (SSi)
        - (Mikroskopia)
        - Kielitiede
        - Frekvenssianalyysi, todennäköisyyslasku ja matematiikka
        - Salatekstihyökkäys
        - Tunnettu selväteksti -hyökkäys
        - Valittu selväteksti -hyökkäys
        - Mukautuva valittu selväteksti -hyökkäys
        - Valittu kooditeksti -hyökkäys
        - Valittu avain -hyökkäys
        - Kumiletku- tai avaimenhankintahyökkäys
    - Kryptografia
        - (a) Tieteenala, jolla viestit pidetään turvallisina. (SSi)
    - Kryptologia
        - (a) Salaustekniikkaan ja kooditekstin avaamiseen liittyvä tiede.
    - Salaaminen
        - (a) Selväkielisen viestin salakirjoittaminen tai koodaaminen kooditekstiksi. (SSi)
        - Salaiset menetelmät
            - (a) Algoritmi vain kommunikoivien osapuolten tiedossa.
        - Symmetrisen avaimen menetelmät

            - (a) Viestien salaaminen tunnetulla tai salaisella algoritmilla hyödyntäen samaa lisätietoa eli avainta sekä salaamisessa että avaamisessa.
            - Jonomenetelmät
                - (a) Salaus tapahtuu bitti tai tavu kerrallaan.
            - Lohkomenetelmät
                - (a) Salaus tapahtuu tietolohko kerrallaan.
        - Epäsymmetrisen avaimen menetelmät
            - (a) Viestien salaamisessa ja avaamisessa käytetään eri avaimia.
            - Julkisen avaimen menetelmät
                - RSA
        - Korvaussalakirjoitus
            - (a) Salakirjoitusjärjestelmät, jossa viestin kirjaimet vaihdetaan toisiin symboleihin, mutta niiden paikkaa viestissä ei muuteta. (SSi)
            - Yksinkertainen menetelmä
                - (a) Viestin merkit korvataan toisilla samasta aakkostosta.
                - Caesar
                - ROT13
            - Homofoninen menetelmä
                - (a) Viestin merkin korvaamiseen on useita vaihtoehtoja.
            - Polygrammimenetelmä
                - (a) Viestin merkkijonot korvataan toisilla merkkijonoilla.
            - Moniaakkosinen menetelmä
                - (a) Monen yksiaakkostoisen salakielen yhdistelmä.
        - Sekoitussalakirjoitus
            - (a) Salakirjoitusjärjestelmät, joissa viestin kirjaimet vaihtavat paikkaa viestin sisällä, mutta eivät muuta muotoaan. (SSi)
            - Siirtosalakielet
                - (a) Viestin merkkien paikat vaihdetaan toisiin.
                - ADFGVX
            - Roottorikoneet
                - (a) Monivaiheinen merkkiensekoitusmenetelmä.
                - Enigma
        - Kerta-avain
            - (a) Satunnainen avain, jota käytetään vain kerran.
            - Kryptoanalyysissä kaikki kooditekstin tuottaneet selväkieliset viestit ovat yhtä todennäköisiä.
            - Täydellinen salausmenetelmä, kun avainta käytetään vain kerran ja se on yhtä pitkä itse viesti.
    - Steganografia
        - (a) Viestien piilottaminen. (SSi)
- Tietämys
    - (a) Ihmisen ajattelun kohde tai tulos. (JBo)
    - (b) Acquaintance with facts, range of information. (OED)
    - (c) Knowledge of a person, thing, or perception gained through information or facts about it rather than by direct experience. (OED)
    - (d) The fact or condition of being instructed, or of having information acquired by study or research; acquaintance with ascertained truths, facts, or principles; information acquired by study; learning; erudition. (OED)

11 Yleinen ongelmanratkaisu

- (a) Tiedon yhdistely toimiviksi kokonaisuuksiksi (VVo)
- Dokumentointi
- Luovuus
  - Luova organisaatio
  - Motivaatio
  - Palkitseminen
  - Ympäristötekijät
- Ongelmalähtöinen oppiminen
  - (a) Problem-based learning (PBL); syn. ongelmaperustainen oppiminen
  - 1. Käsitteiden selventäminen
  - 2. Ongelman määrittäminen
  - 3. Aivoriihi
  - 4. Ongelman analysointi ja selitysmallin rakentaminen
  - 5. Oppimistavoitteiden muodostaminen
  - 6. Itseopiskelu
  - 7. Purku ja arviointi
  - Ongelmanratkaisutaidot
  - Ongelmavirike
  - Ryhmätyötaidot
  - Viestintätaidot
- Ongelmanratkaisuprosessi (GPo)
  - 1. Ongelman ymmärtäminen
  - 2. Ratkaisusuunnitelman laatiminen
  - 3. Suunnitelman toteutus
  - 4. Ratkaisun arviointi
- Ongelmanratkaisuprosessi (VVo)
  - 1. Ongelma
  - 2. Tosiasiat
  - 3. Ideat
    - Aivoriihi
    - Ideaalitavoitteen käyttö
    - Idean muuntelu kysymyslistan avulla
    - Kaukaiset ajatusmallit
    - Synektiikkakokous
    - Tehostettu alitajuinen käsittely
    - Tunnettujen vaihtoehtojen läpikäynti
    - Tuplatiimi
    - Tuumatalkoot
    - ...
  - 4. Ratkaisu
  - 5. Hyväksyttäminen
  - 6. Viimeistely ja toteutus
- Ongelmatyypit
  - 1. Analyysiongelmat
  - 2. Synteesiongelmat
  - 3. Arvostusongelmat
  - Formalisodut ongelmat
  - Todellisen maailman ongelmat
- Tieto
  - Kvalitatiivinen tieto

- Kvantitatiivinen tieto
- Tiedonlähteet
  - Asiantuntijat
  - Internet
  - Kirjallisuus
  - Lähdekritiikki
    - Asiantuntijasuodin
    - Myyjäsuodin
    - Numerosuodin
    - Tutkimussuodin
    - Ennakkokäsityssuodin
    - Oman pätevyyden todistamissuodin
  - Mediat