TIETOJENKÄSITTELYTEORIA

Matemaattinen oppi siitä, mitä tietokoneella on mahdollista tehdä ja kuinka tehokkaasti.

Käytännön tietojenkäsittelyn kannalta tarjoaa (valmiiden ratkaisujen lisäksi) matemaattisia käsitteitä ja menetelmiä tietojenkäsittelyjärjestelmien mallintamiseen ja analysointiin sekä selkeiden ja tehokkaiden ratkaisujen laatimiseen.

Tietojenkäsittelyteorian osa-aloja

Laskettavuusteoria
- Mitä tietokoneella voi tehdä periaatteessa?
- Turing, Gödel, Church, Post (1930-luku); Kleene, Markov (1950-luku).

Laskennan vaativuusteoria
- Mitä tietokoneella voi tehdä käytännössä?
- Hartmanis, Stearns (1960-luku); Cook, Levin, Karp (1970-luku); Papadimitriou, Sipser, Håstad, Razborov ym. (1980-).

Automaatti- ja kielioppiteoria
- Tietojenkäsittelyjärjestelmien perustyyppien ominaisuudet ja kuvausformalismit.
- Chomsky (1950-luku); Ginsburg, Greibach, Rabin, Salomaa, Schützenberger ym. (1960-luku)

Ohjelmien oikeellisuus
- Tietojenkäsittelyjärjestelmien matemaattisesti eksakti määrittely ja oikean toiminnan verifiointi.
- Dijkstra, Hoare (1960-luku); Manna, Pnueli, Scott ym. (1970-).

Muuta
- algoritmien suunnittelu ja analyysi (Knuth, Hopcroft, Tarjan ym.)
- kryptologia (Rivest, Shamir, Adleman ym.)
- rinnakkaisten ja hajautettujen järjestelmien teoria (Lamport, Lynch, Milner, Valiant ym.)
- koneoppimisteoria (Valiant ym.)
- jne.

Tällä kurssilla käsitellään ensisijaisesti automaatteja ja kielioppeja sekä hieman laskettavuusteorian alkeita. Laskennan vaativuusteoriasta mainitaan ehkä jotain. Muita aiheita käsitellään Tietojenkäsittelyteorian laboratorion muilla kursseilla.

1. Matemaattisia peruskäsitteitä

1.1 Joukot

Joukko (engl. set) on kokoelma alkioita. Alkiot voidaan ilmoittaa joko luettelemalla, esim.

$$S = \{2, 3, 5, 7, 11, 13, 17, 19\}$$

tai jonkin säännön avulla, esim.

$$S = \{p \mid p \text{ on alkuluku, } 2 \leq p \leq 20\}.$$

Jos alkio a kuuluu joukkoon A, merkitään $a \in A$, päinvastaisessa tapauksessa $a \notin A$. (Esim. $3 \in S$, $8 \notin S$.)

Tärkeä erikoistapaus on *tyhjä joukko* (engl. empty set) $\emptyset$, johon ei kuulu yhtään alkiota.

Jos joukon A kaikki alkiot kuuluvat myös joukkoon B, sanotaan että A on B:n *osajoukko* (engl. subset) ja merkitään $A \subseteq B$. [Kirjallisuudessa esiintyy myös merkintä $A \subset B$.] Jos A *ei* ole B:n osajoukko merkitään $A \nsubseteq B$. Siis esim.

$$\{2,3\} \subseteq S, \qquad \{1,2,3\} \nsubseteq S.$$

Triviaalisti on voimassa $\emptyset \subseteq A$ kaikilla A.

Joukot A ja B ovat samat, jos niissä on samat alkiot, so. jos on $A \subseteq B$ ja $B \subseteq A$. Jos on $A \subseteq B$, mutta $A \neq B$, sanotaan että A on B:n *aito osajoukko* (engl. proper subset) ja merkitään $A \subsetneq B$. Edellä olisi siis voitu myös kirjoittaa $\{2,3\} \subsetneq S$ ja $\emptyset \subsetneq A$ jos $A \neq \emptyset$.

Joukon alkioina voi olla myös toisia joukkoja (tällöin puhutaan usein "joukkoperheestä"), esim.

$$X = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}.$$

Jonkin perusjoukon A kaikkien osajoukkojen muodostamaa joukkoperhettä sanotaan A:n *potenssijoukoksi* (engl. powerset) ja merkitään $\mathcal{P}(A)$:lla; esim. edellä on $X = \mathcal{P}(\{1,2\})$. [Koska n-alkioisen perusjoukon A potenssijoukossa on 2^n alkiota (HT), käytetään kirjallisuudessa potenssijoukolle myös merkintää 2^A.]

Huomaa, että $A \subseteq B$ jos ja vain jos $A \in \mathcal{P}(B)$.

Huomaa myös, että tyhjän joukon käsittelyssä pitää olla huolellinen:

$$\emptyset \neq \{\emptyset\}, \quad \mathcal{P}(\emptyset) = \{\emptyset\}, \quad \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$

Joukkoja voidaan kombinoida *joukko-operaatioilla*, joista tärkeimmät ovat:

yhdiste (engl. union)

$$A \cup B = \{x \mid x \in A \text{ tai } x \in B\},$$

esim.

$$\{1,2,3\} \cup \{1,4\} = \{1,2,3,4\}.$$

leikkaus (engl. intersection)

$$A \cap B = \{x \mid x \in A \text{ ja } x \in B\},$$

esim.

$$\{1,2,3\} \cap \{1,4\} = \{1\}.$$

erotus (engl. difference)

$$A - B = \{x \mid x \in A \text{ ja } x \notin B\},$$

esim.

$$\{1,2,3\} - \{1,4\} = \{2,3\}.$$

[Erotukselle käytetään myös merkintää $A \setminus B$.]

Joukko-operaatioita koskevat tietyt laskulait, joista tärkeimmät ovat yhdisteen ja leikkauksen *liitännäisyys*:

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C$$

ja *vaihdannaisuus*:

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$

sekä näiden *osittelulait*:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Jos kaikki tarkasteltavat joukot ovat jonkin yhteisen "universaalijoukon" U osajoukkoja, sanotaan erotusta $U - A$ joukon A *komplementiksi* (U:n suhteen) ja merkitään $\bar{A}$:lla.

Yhdiste-, leikkaus- ja komplementointioperaatioita yhdistävät tärkeät ns. *de Morganin kaavat*:

$$\overline{A \cup B} = \bar{A} \cap \bar{B},$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}.$$

Lisäksi joukkojen erotus voidaan esittää leikkauksen ja komplementoinnin avulla seuraavasti:

$$A - B = A \cap \bar{B}.$$

Jos joukkoperheen $\mathcal{A}$ jäsenet on *indeksoitu*, esim.

$$\mathcal{A} = \{A_1, A_2, A_3, \dots\},$$

niin yhdisteelle ja leikkaukselle voidaan käyttää lyhennemerkintöjä

$$\bigcup_{i \geq 1} A_i = A_1 \cup A_2 \cup A_3 \cdots$$

ja

$$\bigcap_{i \geq 1} A_i = A_1 \cap A_2 \cap A_3 \cdots$$

Indeksien ei itse asiassa tarvitse olla edes luonnollisia lukuja, vaan *indeksijoukkona* voi olla mikä tahansa joukko I. Tällöin käytetään merkintöjä

$$\mathcal{A} = \{A_i \mid i \in I\}$$

ja

$$\bigcup_{i \in I} A_i, \qquad \bigcap_{i \in I} A_i.$$

1.2 Relaatiot ja funktiot

Olkoot A ja B joukkoja. Alkioiden $a \in A$ ja $b \in B$ *järjestettyä paria* (engl. ordered pair) merkitään (a, b). Huomaa, että joukkoina on aina $\{a, b\} = \{b, a\}$, mutta jos $a \neq b$, niin järjestettyinä pareina on $(a, b) \neq (b, a)$. [Täsmällisesti, mutta epäintuitiivisesti voidaan järjestetty pari määritellä joukkona $(a, b) = \{a, \{a, b\}\}$.]

Joukkojen A ja B *karteesinen tulo* (engl. Cartesian product) määritellään

$$A \times B = \{(a, b) \mid a \in A \text{ ja } b \in B\},$$

esim.

$$\begin{aligned} &\{1, 2, 3\} \times \{1, 4\} \\ &\quad = \{(1, 1), (1, 4), (2, 1), (2, 4), (3, 1), (3, 4)\}. \end{aligned}$$

Relaatio R joukolta A joukolle B on karteesisen tulon $A \times B$ osajoukko:

$$R \subseteq A \times B.$$

Jos $(a, b) \in R$, niin merkitään myös aRb ja sanotaan että alkio a on *relaatiossa (suhteessa)* R alkioon b. Tätä *infix*-merkintää käytetään varsinkin silloin, kun relaation nimenä on jokin erikoismerkki, esim. $\leq$, $\prec$, $\equiv$, $\sim$. [Onhan luontevampaa kirjoittaa "$a \prec b$" kuin "$(a, b) \in \prec$".] Jos relaation R *lähtöjoukko* (engl. domain) A ja *maalijoukko* (engl. range) B ovat samat, so. $R \subseteq A \times A$, sanotaan että R on relaatio *joukossa* A.

Olkoon $R \subseteq A \times B$. Osajoukon $A' \subseteq A$ *kuva* (engl. image) relaatiossa R on

$$R(A') = \{b \in B \mid \exists a' \in A' \text{ s.e. } (a', b) \in R\}$$

ja osajoukon $B' \subseteq B$ *alkukuva* (engl. inverse image) on

$$R^{-1}(B') = \{a \in A \mid \exists b' \in B' \text{ s.e. } (a, b') \in R\}.$$

Relaation $R \subseteq A \times B$ *käänteisrelaatio* (engl. inverse relation) on relaatio $R^{-1} \subseteq B \times A$,

$$R^{-1} = \{(b,a) \mid (a,b) \in R\}.$$

Jos $R \subseteq A \times B$ ja $S \subseteq B \times C$ ovat relaatioita, niin niiden *yhdistetty relaatio* (engl. composite relation) $R \circ S \subseteq A \times C$ määritellään:

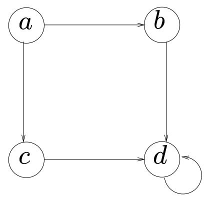
$$R \circ S = \{(a,c) \mid \exists b \in B \text{ s.e. } (a,b) \in R, (b,c) \in S\}.$$

Relaatiota $R \subseteq A \times B$ on usein (varsinkin jos joukot A ja B ovat äärellisiä) havainnollista tarkastella *suunnattuna verkkona* t. *graafina*, jonka *solmuina* ovat joukkojen A ja B alkiot ja solmusta $a \in A$ on *kaari* ("nuoli") solmuun $b \in B$, jos ja vain jos $(a,b) \in R$.

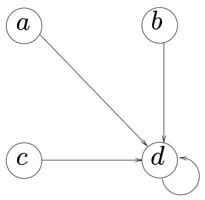
Olkoon esimerkiksi joukossa $A = \{a,b,c,d\}$ määritelty relaatio $R \subseteq A \times A$,

$$R = \{(a,b),(a,c),(b,d),(c,d),(d,d)\}.$$

Tällöin on relaation R graafiesitys:



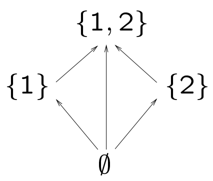
Relaation $R \circ R$ graafiesitys puolestaan on:



Olkoon toisena esimerkkinä joukossa $X = \mathcal{P}(\{1,2\})$ määritelty relaatio $S \subseteq X \times X$,

$$S = \{(A,B) \mid A \subseteq B\}.$$

Tämän graafiesitys on:



Relaatio $f \subseteq A \times B$ on *funktio*, jos kukin $a \in A$ on relaatiossa f täsmälleen yhden $b \in B$ kanssa. Tällöin käytetään yleisten relaatiomerkintöjen sijaan tavallisesti merkintöjä $f : A \to B$ ja $f(a) = b$. Funktioita koskee kaikki mitä edellä yleisesti on todettu relaatioista, mutta historiallisista syistä funktioiden yhdistäminen merkitään toisin päin kuin yleisten relaatioiden: jos $f : A \to B$ ja $g : B \to C$ ovat funktioita, niin niiden yhdistetty funktio määritellään kaavalla $(g \circ f)(a) = g(f(a))$, so. relaatioina

$$g \circ f = \{(a,c) \mid \exists b \in B \text{ s.e. } f(a) = b, g(b) = c\}.$$

Funktio $f : A \to B$ on *surjektio* (engl. onto map), jos jokainen $b \in B$ on jonkin $a \in A$ kuva, so. jos $f(A) = B$, ja *injektio* (engl. one-to-one map), jos kaikki $a \in A$ kuvautuvat eri alkioille, so. jos $a \neq a' \Rightarrow f(a) \neq f(a')$. Funktio f on *bijektio*, jos se on sekä injektio että surjektio, so. jos jokainen $b \in B$ on yhden ja vain yhden $a \in A$ kuva.

1.3 Ekvivalenssirelaatiot

Ekvivalenssirelaatiot ovat matemaattisesti täsmällinen muotoilu sille yleiselle idealle, että oliot ovat keskenään *samankaltaisia* jonkin kiinnostavan ominaisuuden X suhteen. Ominaisuuteen X perustuva ekvivalenssirelaatio osittaa tarkasteltavien olioiden joukon *ekvivalenssiluokkiin*, jotka vastaavat ominaisuuden X eri arvoja. (Kääntäen mielivaltainen olioiden joukon ositus Π määrää tietyn abstraktin samankaltaisuusominaisuuden, nim. sen että oliot ovat samankaltaisia jos ne sijoittuvat samaan osituksen Π luokkaan.)

Osoittautuu, että yleinen "samankaltaisuusrelaation" idea voidaan kiteyttää seuraaviin kolmeen ominaisuuteen.

Määritelmä 1.1 Relaatio $R \subseteq A \times A$ on:
(i) *refleksiivinen*, jos aRa $\forall a \in A$;
(ii) *symmetrinen*, jos $aRb \Rightarrow bRa$ $\forall a, b \in A$;
(iii) *transitiivinen*, jos $aRb, bRc \Rightarrow aRc$ $\forall a, b, c \in A$.

Määritelmä 1.2 Relaatio $R \subseteq A \times A$, joka toteuttaa edelliset ehdot (i)–(iii) on *ekvivalenssirelaatio*. Alkion $a \in A$ *ekvivalenssiluokka* (relaation R suhteen) on

$$R[a] = \{x \in A \mid aRx\}.$$

Ekvivalenssirelaatioita merkitään usein R:n sijaan alkioiden samankaltaisuutta korostavilla symboleilla $\sim$, $\equiv$, $\simeq$ tms.

Esim. Olkoon

$$A = \{\text{kaikki 1900-luvulla syntyneet ihmiset}\}$$

ja aRb voimassa, jos henkilöillä a ja b on sama syntymävuosi. Tällöin R on selvästi ekvivalenssi, jonka ekvivalenssiluokat koostuvat keskenään samana vuonna syntyneistä henkilöistä. Luokkia on 100 kappaletta, ja "abstraktisti" ne vastaavat 1900-luvun vuosia 1900,. . . ,1999.

Lemma 1.3 Olkoon $R \subseteq A \times A$ ekvivalenssi. Tällöin on kaikilla $a, b \in A$ voimassa:

$$R[a] = R[b] \quad \text{joss} \quad aRb.$$

Tod. Helppo; sivuutetaan. □

Lemma 1.4 Olkoon $R \subseteq A \times A$ ekvivalenssi. Tällöin R:n ekvivalenssiluokat muodostavat A:n *osituksen* erillisiin epätyhjiin osajoukkoihin, so.:
(i) $R[a] \neq \emptyset$ kaikilla $a \in A$;
(ii) $A = \bigcup_{a \in A} R[a]$;
(iii) jos $R[a] \neq R[b]$, niin $R[a] \cap R[b] = \emptyset$, kaikilla $a, b \in A$.

Tod. Helppo; sivuutetaan. □

Kääntäen jokainen perusjoukon A ositus erillisiin epätyhjiin luokkiin A_i, $i \in I$, määrää vastaavan ekvivalenssirelaation:

$$a \sim b \quad \Leftrightarrow \quad a \text{ ja } b \text{ kuuluvat samaan luokkaan } A_i.$$

*1.4 Järjestysrelaatiot

Kuten edellä samankaltaisuuden idea, voidaan moninaiset matematiikassa esiintyvät olioiden "järjestykset" kiteyttää seuraavasti:

Määritelmä 1.5 Relaatio $R \subseteq A \times A$ on *antisymmetrinen*, jos kaikilla $a, b \in A$ on voimassa: $aRb, bRa \Rightarrow a = b$.

Määritelmä 1.6 Relaatio $R \subseteq A \times A$, joka on refleksiivinen, antisymmetrinen ja transitiivinen, on joukon A *(osittainen) järjestys* (engl. (partial) order).

Järjestysrelaatioita merkitään usein R:n sijaan symboleilla $\leq$, $\preceq$ tms.

Jos alkioilla $a, b \in A$ on voimassa aRb tai bRa, sanotaan että a ja b ovat *vertailtavia* (engl. comparable).

Jos kaikki perusjoukon A alkiot ovat (pareittain) vertailtavia, järjestys R on *täydellinen* (kokonainen, lineaarinen) (engl. complete, total, linear order).

Järjestetyn joukon $(A, \preceq)$ alkio $a \in A$ on:
(i) *maksimaalinen*, jos $a \preceq x \Rightarrow a = x \quad \forall x \in A$;
(ii) *minimaalinen*, jos $x \preceq a \Rightarrow a = x \quad \forall x \in A$;
(iii) *suurin alkio*, jos $x \preceq a \quad \forall x \in A$;
(iii) *pienin alkio*, jos $a \preceq x \quad \forall x \in A$.

Järjestetty joukko $(A, \preceq)$ on *hyvin järjestetty* (engl. well-ordered), jos jokainen epätyhjä $B \subseteq A$ sisältää järjestyksen $\preceq$ suhteen pienimmän alkion.

Lemma. Jokainen hyvinjärjestys on täydellinen. $\square$

Esimerkkejä.

(i) $(\mathbb{N}, \leq)$ — hyvinjärjestys.

(ii) $(\mathbb{Z}, \leq)$ — täydellinen, mutta ei hyvinjärjestys.

(iii) Olk. X mieliv. joukko. Tällöin $(\mathcal{P}(X), \subseteq)$ on järjestetty joukko, mutta ei täydellinen järjestys jos $|X| \geq 2$.

(iv) Olk. $m, n \in \mathbb{N}$. Merkitään:

$$m \mid n \;\Leftrightarrow m \text{ on } n\text{:n tekijä.}$$

Joukko $(\mathbb{N}, \mid)$ on järjestys, mutta ei täydellinen.

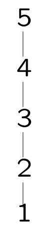
Olkoon $(A, \preceq)$ järjestetty joukko. Merkitään:

$$\begin{aligned} a \prec b &\;\Leftrightarrow\; a \preceq b, a \neq b \\ a \succeq b &\;\Leftrightarrow\; b \preceq a \\ a \succ b &\;\Leftrightarrow\; a \succeq b, a \neq b. \end{aligned}$$

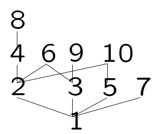
Alkio $a \in A$ on alkion $b \in A$ *välitön edeltäjä* [t. b on a:n *välitön seuraaja*], jos:
(i) $a \prec b$ ja
(ii) $\nexists c \in A$ s.e. $a \prec c \prec b$.

Jokainen äärellinen järjestetty joukko $(A, \preceq)$ voidaan esittää ns. *Hasse-kaaviona*, jonka solmut vastaavat A:n alkioita, ja solmusta $a \in A$ on viivat "ylöspäin" a:n kaikkiin välittömiin seuraajiin.

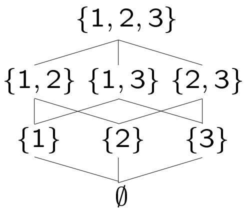
Esim.
(i) Järjestystä $(\{1, 2, \ldots, 5\}, \leq)$ vastaava kaavio:



(ii) Järjestystä $(\{1, 2, \ldots, 10\}, \mid)$ vastaava kaavio:



(iii) Järjestystä $(\mathcal{P}(\{1,2,3,\}),\subseteq)$ vastaava kaavio:



Järjestysrelaation Hasse-kaavio voidaan nähdä myös relaation graafiesityksen "transitiivisena reduktiona," missä graafista on selkeyden vuoksi jätetty pois ne kaaret, joiden olemassaolo voidaan päätellä graafissa esitettyjen kaarten ja tarkasteltavan relaation refleksiivisyyden ja transitiivisuuden nojalla.

1.5 Induktioperiaate

Lause 1.7 Olkoon $(A,\preceq)$ hyvin järjestetty joukko ja $P(a)$ jokin A:n alkioita koskeva väite. Jos voidaan osoittaa kaikilla $a \in A$ induktio-ominaisuus:
(*) $[P(x)$ tosi kaikilla $x \prec a] \Rightarrow P(a)$ tosi,
niin väite $P(a)$ on tosi kaikilla $a \in A$.

Tod. Oletetaan, että ominaisuus (*) on voimassa, mutta silti joukko

$$B = \{a \in A \mid P(a) \text{ on epätosi}\}$$

on epätyhjä. Koska A on hyvin järjestetty, joukossa B on järjestyksen $\preceq$ suhteen pienin alkio $b \in B$. Mutta tällöin on voimassa:

$$[P(x) \text{ tosi kaikilla } x \prec b],$$

joten oletuksen (*) mukaan pitäisi olla myös $P(b)$ tosi.

Saadusta ristiriidasta seuraa, että on oltava $B = \emptyset$, ja siis $P(a)$ tosi kaikilla $a \in A$. □

Seuraus 1.8 [Luonnollisten lukujen vahva induktio.] Olkoon $P(k)$ jokin luonnollisten lukujen ominaisuus. Jos on voimassa:
(i) $P(0)$ ja
(ii) kaikilla $k \geq 0$:

$$[P(0) \& P(1) \& \ldots \& P(k)] \Rightarrow P(k+1),$$

niin $P(n)$ on tosi kaikilla $n \in \mathbb{N}$. □

Seuraus 1.9 [Luonnollisten lukujen heikko induktio.] Olkoon $P(k)$ jokin luonnollisten lukujen ominaisuus. Jos on voimassa:
(i) $P(0)$ ja
(ii) kaikilla $k \geq 0$:

$$P(k) \Rightarrow P(k+1),$$

niin $P(n)$ on tosi kaikilla $n \in \mathbb{N}$. □

Esimerkki.

Väite. Kaikilla $n \in \mathbb{N}$ on voimassa kaava

$$P(n): \quad (1+2+\cdots+n)^2 = 1^3+2^3+\cdots+n^3.$$

Todistus.

(i) Perustapaus: $P(0): \quad 0^2 = 0.$

(ii) Induktioaskel: Oletetaan, että annetulla $k \geq 0$ kaava

$$P(k): \quad (1+2+\cdots+k)^2 = 1^3+2^3+\cdots+k^3$$

on voimassa. Tällöin on myös:

$$\begin{aligned}
&(1+2+\cdots+k+(k+1))^2 \\
&\quad = (1+\cdots+k)^2 + 2(1+\cdots k)(k+1) + (k+1)^2 \\
&\quad = 1^3+\cdots+k^3 + 2\cdot\frac{k(k+1)}{2}\cdot(k+1) + (k+1)^2 \\
&\quad = 1^3+\cdots+k^3 + k(k+1)^2 + (k+1)^2 \\
&\quad = 1^3+\cdots+k^3 + (k+1)^3.
\end{aligned}$$

On siis todettu, että kaavan $P(k)$ totuudesta seuraa kaavan $P(k+1)$ totuus, so. että $P(k) \Rightarrow P(k+1)$, kaikilla $k \geq 0$. Luonnollisten lukujen induktioperiaatteen 1.9 nojalla voidaan nyt päätellä, että kaava $P(n)$ on voimassa kaikilla $n \in \mathbb{N}$. $\square$