

58110 Tieteellisen kirjoittamisen kurssi, kevät 2008
Algoritmiaiheita, 5.1.2008

1 Ohjeita

Tässä listassa on ehdotuksia tieteellisen kirjoittamisen kurssin algoritmiryhmän aiheiksi. Valitse listalta joitain kandidaattiaiheita. Listan aiheet ovat suuntaa-antavia; lopullinen rajaus ja otsikko sovitaan kurssin kuluessa. Voit myös ehdottaa omaa aiheitasi. Oma aihe on kaikkein paras vaihtoehto, kunhan se sopii algoritmiryhmän aihepiiriin ja siitä löytyy riittävästi sopivaa materiaalia.

Kukin aihe tai aihepiiri on varustettu listalla avainsanoja, jotka kuvaavat aiheeseen liittyviä matematiikan ja tietojenkäsittelyn osa-aloja tai hyödyllisiä kursseja. Nämä eivät ole esitietovaatimuksia, mutta on selvää että taustatiedot ja menetelmiin liittyvä kiinnostus saattavat nopeuttaa artikkelien ymmärtämistä ja kirjoitustyötä. Peruslähtökohta on kuitenkin se, että opinto-oppaassa mainitut esitietovaatimukset antavat riittävät valmiudet kaikkiin aiheisiin.

Listalla on kustakin aiheesta mainittu muutama lähdeartikkeli tai kirja, joiden kautta voi päästä helpommin aihepiiriin kiinni. Valintariskin minimoimiseksi kannattaa silmällä läpi esimerkiksi yksi lähdeartikkeli ennenkuin kiinnität valintasi.

Aiheisiin tai aihepiireihin on merkitty myös ohjaajan arvio kirjaimilla A–C. Kirjain A tarkoittaa aihepiiriä, joka on lähempänä ohjaajan omaa tutkimusta, ja kirjain C taas aihepiiriä, jossa ohjaajakin varmasti oppii uutta. Kaikista aiheista saa toki ohjausta, myös omasta aiheestasi.

2 Aiheita

2.1 Laskennan teoriaa

Ohjaajan arvio: A. *Kursseja:* Laskennan mallit, Laskennan vaativuus, Logiikka I, Matemaattinen logiikka.

Kvantifoidut Boolean kaavat (*quantified Boolean formulae, QBF*)

[CSGG02, GW99, Rin99]

Kvantifoidut Boolean kaavat laajentavat propositiologiikkaa sallimalla eksistentiaali- ja universaalikvanttorit. Lähdeartikkeleissa tarkastellaan esimerkiksi QBF-kaavojen SAT-ongelmaa eli kaavojen toteutuvuutta.

Resoluutiotodistusten vaikeus [ABM04, PR04]

Toteutuvuusongelma on tutkituimpia NP-täydellisiä ongelmia. Viime aikoina on saatu uusia tuloksia toteutuvuustodistusten vaikeudesta.

Kiintoparametrivaativuus (*fixed-parameter complexity*) [CKJ01]

Tietyille NP-täydellisille ongelmille on olemassa algoritmeja, joiden aikavaativuus on $O(f(k) \text{ poly}(n))$, missä n on syötteen koko, k ongelman parametri (esimerkiksi solmupeitteen koko), $f(k)$ on funktio, joka ei riipu parametrasta n ja $\text{poly}(\cdot)$ on polynomi. Tällaiset algoritmit pystyvät käsittelemään suuriakin syötteitä, jos parametri k on kiinnitetty riittävän pieneksi.

Approksimointiongelmiin vaativuus [ALM⁺98, Din06]

Eräs merkittävimmistä viimeaikaisista vaativuusteorian tuloksista on luokan NP karakterisointi satunnaisesti tarkastettavien todistusten avulla (*probabilistic checking of proofs, PCP*). Tuloksesta seuraa mielenkiintoisia mahdotto- muustuloksia optimointiongelmiin approksimoimiselle.

Laskentapiiriin teoriaa [BS90, Hås89, RR97]

Laskentapiirit ovat laskennan malli, joka jäljittelee loogisista peruskomponenteista muodostuvaa elektronista piiriä. Laskennan piirivaativuus on mielenkiintoista etenkin alarajojen kannalta. Klassinen esimerkki on Håstadin tulos pariteettifunktiolle. Ikävä kyllä epätriviaalien alarajojen todistaminen on tässäkin mallissa osoittautunut hyvin vaikeaksi.

Helppojen ongelmien vaativuus [Bor77, Joh90a]

Vaativuusteoriassa ollaan yleensä ensisijaisesti kiinnostuneita siitä, mitkä ongelmat kuuluvat luokkaan P. Kuitenkin myös luokkaan P kuuluvien ongelmien välisiä eroja voidaan tutkia. Eräs mielenkiinnon kohde on logaritmisessa työtilassa ratkeavat ongelmat, joiden voidaan osoittaa olevan tiettyssä mielessä tehokkaasti rinnakkaistuvia.

Satunnaislaskennan vaativuusteoriaa [Joh84, Joh90a]

Satunnaisuus on tärkeä algoritmien tekniikka, jota käytetään monella lailla eri tyyppisten ongelmien ratkaisussa. Tämän aiheen tarkoituksena on tarkastella satunnaisalgoritmien yleistä teoriaa: millaisia vaativuusluokkia satunnaislaskennassa voidaan määrittellä ja miten ne suhtautuvat toisiinsa ja deterministisiin vaativuusluokkiin.

Kolmogorov-kompleksisuus [GV99, JLV99, JLV00]

Kolmogorov-kompleksisuus on eräänlainen satunnaisuuden mittari. Bittijonon monimutkaisuus on yhtä kuin lyhimmän sellaisen tietokoneohjelman pituus, jonka tulosteena on kyseinen bittijono. Toisin sanoen, jos ohjelma on olennaisesti ”yhtä pitkä” kuin bittijono itse, bittijonoa voidaan pitää ”satunnaisena” siinä mielessä ettei sen rakenteessa ollut mitään säännönmukaisuutta, jonka perusteella ohjelma voisi tehdä muuta kuin muistaa bittijonon suoraan sellaisena kuin se tulostetaan.

2.2 Tietorakenteita ja algoritmeja

Ohjaajan arvio: A. *Kursseja:* Tietorakenteet, Algoritmien suunnittelu.

Joukkojen erilliset yhdisteet [TvL84, WT89]

Joukkojen yhdisteiden säilyttäminen ja purkaminen.

Binääriset etsintäpuut [ST85]

Splay-puu on itsesäätyvä versio perinteisestä binäärisestä hakupuusta.

Liittyy: Tasoitettua analyysiä.

Tietorakenteiden tiivistys [Cla98, Jac89]

Tiedon tiivistyksessä on tavoitteena esittää tieto (esim. tekstidokumentti) mahdollisimman pienessä tilassa siten, että alkuperäinen tieto voidaan palauttaa virheettää. Tietorakennetta tiivistettäessä lisätavoitteena on säilyttää tietorakenteen toimintakyky. Esimerkki: Binääripuu halutaan esittää muodossa, jossa kullekin solmulle löydetään vakioajassa sen vasen ja oikea lapsi. Perinteinen linkein esitetty puu vie $O(n \log n)$ bittiä tilaa, missä n on puun solmujen määrä (jokaiseen solmuun on talletettu 2 linkkikenttää, kukin luokkaa $\log n$ bittiä). On kuitenkin mahdollista esittää puu $O(n)$ bitillä siten, että vasen ja oikea lapsi löytyvät vakioajassa.

Liittyy: Informaatioteoriaa.

Hahmonsovitukset merkkijonoissa [CR02, KMP77]

Merkkijonomenetelmien avulla pyritään löytämään tekstistä hahmon osumia eli paikkoja, joissa hahmo esiintyy osin tai kokonaan.

Kursseja: Merkkijonomenetelmät.

Staattisen tekstin indeksointi loppuosatietorakenteilla [MM93]

Suuri osa internetin sisällöstä on tekstiä, joka muuttuu suhteellisen hitaasti. Tällaiselle staattiselle tekstile on kehitetty indeksirakenteita, jotka mahdollistavat erittäin nopeat tekstihaut. Loppuosatietorakenteet kuten suffiksipuut ja -taulukot ovat perusesimerkkejä tällaisista rakenteista.

Kursseja: Merkkijonomenetelmät.

Muistihierarkia-algoritmit [BDFC05, FLPR99]

Välimuistin käyttö vaikuttaa usein merkittävästi algoritmien käytännön tehokkuuteen. Eräs mielenkiintoinen idea on suunnitella algoritmit sellaisiksi, että ne käyttävät välimuistia suunnilleen optimaalisesti ilman, että niiden tarvitsee ennakolta tietää välimuistin kokoa. B-puut ovat tuore esimerkki mallin soveluksista.

Burrows–Wheeler-muunnos [BW94, Man01, NM07]

Burrows–Wheeler-muunnos [BW94] on tärkeä tekstin esikäsittelymenetelmä, jota voidaan käyttää esim. hakemistojen tiivistämisessä [NM07]. Aiheesta on tehty myös matemaattisia analyyseja [Man01].

2.3 Kombinatorista optimointia

Ohjaajan arvio: A. *Liittyy:* Kombinatoriikka, verkot, puut. *Kursseja:* Diskreetti matematiikka 2, Kombinatorinen optimointi, Laskennan vaativuus.

Kauppamatkustajan ongelma (*travelling salesman problem, TSP*)

[Aro98, Joh90b]

Kauppamatkustajan ongelma on yksi yleisimmistä NP-täydellisistä ongelmista. Sille tunnetaan erilaisia ratkaisuheuristiikkoja ja erikoistapauksille myös approksimointialgoritmeja.

Pienin virittävän puu (*minimum spanning tree*) [Cha00], [Tar83, luku 8]

Pienimmän virittävän puun laskenta on klassinen optimointiongelma. Siihen on löydetty myös uudempia lähestymistapoja.

Avioliitto-ongelma (*stable marriage problem*) [BR97, GS68, GS85, IMMM99]

Avioliitto-ongelmassa pitää parittaa annetut naiset ja miehet toisilleen siten, etteivät he tee syrjähyppyjä, kun kaikkien mieltymykset tunnetaan. Tämän jo klassisen algoritmisen ongelman perustapaus ratkeaa polynomisessa ajassa, mutta laajennuksissa on törmättykin vaikeuksiin.

Verkon murtolukuväritys (*fractional graph coloring*) [HS88, Jan03, LY94]

Murtolukuväritysongelmat ovat muunnoksia tunnetuista verkonväritysongelmista. Murtolukuväritystä voi soveltaa esimerkiksi tiedonsiirron ajoittamiseen langattomassa verkossa. Kaarivärityksen murtolukuversio ratkeaa polynomisessa ajassa, mutta solmuvärityksen approksimointikin on vaikeaa millä tahansa vakiosuhteella. Monille verkkojen luokille voidaan kuitenkin löytää approksimaatioalgoritmeja.

Liittyy: Approksimaatioalgoritmit.

Steiner-puut (*Steiner tree*) [RZ05, Vaz03]

Mitä nykyään tiedetään Steiner-puihin liittyvien optimointiongelmiä approksimoitavuudesta ja ei-approksimoitavuudesta?

Liittyy: Approksimaatioalgoritmit.

Simuloitu jäähtytys (*Simulated annealing*) [AK89, KGV83]

Simuloitu jäähtytys on yleiskäyttöinen satunnaisuuteen perustuva menetelmä, jota voidaan käyttää erilaisten optimointiongelmiä heuristiseen ratkaisuun.

Geneettiset algoritmit [Gol89, HGL93]

Geneettiset algoritmit ovat toinen satunnaisuuteen perustuva optimointimenetelmä.

Nopeasti sekoittuvat Markovin ketjut (*rapidly mixing Markov chains*) [BDGJ99], [MR95, luvut 6.7 ja 11]

Nopeasti sekoittuvat Markovin ketjut tarjoavat keinon vaikeiden laskentaongelmien likimääräiseen ratkaisemiseen suurella todennäköisyydellä. Tyypillisesti algoritmit ovat yksinkertaisia, mutta niiden tehokkuuden todistaminen on mutkikasta.

Liittyy: Markovin prosesseja. *Kursseja:* Satunnaisalgoritmit.

Peitto- ja pakkaus-LP [GK98]

Peitto- ja pakkaustyyppisten LP-ongelmien sovelluksia ja approksimatiivista ratkaisemista.

Liittyy: Approksimaatioalgoritmit, lineaarinen ohjelmointi.

2.4 Laskennallista geometriaa

Ohjaajan arvio: C. *Kursseja:* Geometriset menetelmät.

Leikkaavien janojen ongelma [Bal95]**Monikulmioiden kolmiointialgoritmit** [AGR01]**2.5 Logiikkaa; ohjelmointikielten syntaksia ja semantiikkaa**

Ohjaajan arvio: B. *Kursseja:* Johdatus funktionaaliseen ohjelmointiin, Logiikka I, Spesifioinnin ja verifioinnin perusteet.

Rajoitetietokantojen kyselykielet (*constraint query languages*) [AHV95, sivut 94–98], [BL00], [BL02], [Lib99]

Rajoitetietokantojen kyselykielet käsittelevät sellaisia tietokantoja, joihin on talletettu informaatiota jostakin äärettömästä rakenteesta äärellisenä kokoelmana sitä rajoittavia lauseita. Esimerkiksi kolmiulotteinen avaruus on periaatteessa ääretön, mutta sen osia voidaan kuvailla sellaisilla lauseilla kuin ”kaikki ne pisteet joiden x -koordinaatti on positiivinen”. Mutta miten näin esitetystä informaatiosta vastataan käyttäjän kysymyksiin?

Liittyy: Tietokannat, logiikka.

Rajoitelogiikkaohjelmointi [Col90]

Rajoitelogiikkakielet.

Liittyy: Prolog-ohjelmointi.

Funktionaalisen ohjelmointikielen suoritusmalli

[ACM04, BAJ00, BJdM97, Lei99, Pip97]

Funktionaalisen ohjelmointikielen suoritusmalli on λ -lausekkeiden β -sievittäminen. Mitä se maksaa algoritmisenä ilmaisuvoimana ja laskentaresursseina?

Liittyy: Jonkin funktionaalisen kielen (esim. Haskell, Lisp) osaaminen eduksi.

Spesifikaatiot ovat väitteitä, ohjelmat niiden todistuksia

[Bac90, CNSvS94, Wad00]

Formaali looginen ohjelmankehitys.

Liittyy: Logiikkaa, spesifointia ja verifointia.

Ohjelmien aksiomaattinen semantiikka [Hoa69]

Heikoimman ennakkoehdon semantiikka, todistetusti oikeellisten ohjelmien kehittäminen.

Liittyy: Logiikkaa, spesifointia ja verifointia.

2.6 Koneoppimista, tekoälyä ja data-analyysia

Ohjaajan arvio: B. *Liittyy:* Todennäköisyyslaskentaa. *Kursseja:* Koneoppiminen, todennäköisyyslaskennan ja tilastotieteen kurssit, Tekoäly, Kolme käsitettä -kurssit.

Algoritmeja tietovirroille (*data stream algorithms*) [AMS99, CM05]

Sensori tai muu reaaliaikainen datalähde voi tuottaa dataa niin paljon ja nopeasti, että sitä ei ole mahdollista kokonaan tallettaa myöhempää käsittelyä varten. Erilaisia koko dataa koskevia tilastoja voidaan kuitenkin laskea luomalla siitä muistiin vain ”hahmotelma” (*sketch*), joka on kooltaan esim. logaritminen syötteen koon suhteen.

Tulon summaus -ongelma (*sum-product problem*) [AM00, Ste03, SH96]

Tulon summaus -ongelmassa tehtävänä on laskea moniulotteinen summa funktiosta, joka voidaan esittää alempiulotteisten funktioiden tulona.

Ohjaajan arvio: B. *Liittyy:* Algebra. *Kursseja:* Graphical models, Research seminar on algorithms: sums of products.

Tilastollinen oppimisteoria [BEHW89, Hau92, Vap98]

Tilastollinen oppimisteoria on tekoälytutkimukseen läheisesti liittyvä alue, joka tarkastelee esimerkkien perusteella tehtävien yleistysten luotettavuutta. Klassinen tulos on opittavuuden karakterisointi ns. PAC-mallissa opittavien käsitteiden monimuotoisuutta mittaavan Vapnik–Chervonenkis-dimension avulla. Perus-PAC-malli on kuitenkin melko rajoittunut, ja sitä on tarpeen yleistää mm. virheiden sallimiseksi esimerkeissä.

Päätöspuiden oppiminen [Qui86]

Heuristiikkoja päätöspuiden muodostamiseen, päätöspuiden oppiminen.

Liittyy: Informaatioteoriaa.

Robottien navigointi [Thr98]

Oppiminen robottien navigoinnissa, robottien navigointialgoritmit.

Liittyy: Matriisilaskenta, Markovin prosessit, Kalman-suodattimet, particle filtering -tyyppiset tilasiirtymäjärjestelmiin liittyvät tilastolliset estimointimenetelmät.

Itseorganisoivat kartat ja niiden sovellukset [KKL⁺00]

Itseorganisoivan kartan tarkoituksena on projisoida suuriulotteisessa vektoriavaruudessa sijaitseva data pieniulotteiseen (esim. kaksiulotteiseen) vektoriavaruuteen esimerkiksi datan visualisointia varten tai siksi että tyypilliset etäisyysmitat käyttäytyvät huonosti suuriulotteisissa avaruuksissa.

Itseorganisoivat kartat voidaan nähdä myös pääkomponenttianalyysin epälineaarisenä vastineena (ei suoria ominaisvektoreita eikä ortogonaalista kantaa).

Liittyy: Matriisilaskentaa.

Riippumattomien komponenttien analyysi [Sán02]

Sokeassa lähteiden erottelussa havaittu signaalivektori x oletetaan toisitaan riippumattomien lähdesignaalien s sekoitteeksi ($x = As$). Tehtävänä on selvittää alkuperäinen signaalivektori S oletusten ja havaitun signaalivektorin perusteella niin pitkälle kuin mahdollista ($s = Wx$). Sovelluksia on mm. laskennallisessa neurotieteessä.

Liittyy: Matriisilaskentaa, informaatioteoriaa.

Palauteoppiminen (*reinforcement learning*) [Aue02, KLM96, Tes95]

Palauteoppimisessa oppija yrittää muodostaa tehokkaan toimintastrategian ympäristössä, jossa suoritettujen valintojen edut ja haitat näkyvät vasta myöhemmin. Algoritmeja on sovellettu menestyksellä mm. peleissä. Myös erilaisia teoreettisia analyyseja on mahdollista tehdä.

Liittyy: Markovin prosesseja.

Tukivektorikoneet (*support vector machines, SVM*) [SS02]

Tukivektorikoneet ovat 1990-luvun loppupuolen kuumiin koneoppimisparadigmiin. Tukivektorikoneita ja muita ydinfunktioihin (*kernel function*) perustuvia data-analyysimenetelmiä on sovellettu menestyksellisesti moniin tehtäviin, joihin aiemmin käytettiin etupäässä neuraaliverkkoja.

Liittyy: Optimointia.

Segmentointi [KCHP01]

Segmentoinnin tarkoituksena on sekvenssidatan jakaminen segmentteihin s.e. kunkin segmentin sisältämä data on keskenään samankaltaista ja eroaa naapurisegmenteistä. Algoritmisia kysymyksiä liittyy mm. datan esikäsittelyyn, oikean segmenttimäärän löytämiseen sekä segmenttien kuvauksen määrittelyyn. Sovelluksia esim. DNA-sekvenssin jakaminen geeneihin ja ei-koodaaviin alueisiin, sensoridatan jakaminen systeemin eri tiloja vastaaviin segmentteihin.

Piilo-Markov-mallit (*hidden Markov models, HMM*) [Ben99]

Piilo-Markov-malleja käytetään moniin tietojenkäsittelyongelmiin puheentunnistuksesta geenisekvenssien analysointiin.

Liittyy: Markovin prosesseja. *Kursseja:* Graphical models.

Ryvästämisen algoritmistiikkaa [DL05]

Ryvästämisessä (*clustering*) suuri joukko pisteitä jaetaan pieneen määrään *rypäitä* siten, että samaan rypäeseen tulevat pisteet ovat jonkin metriikan mukaan lähellä toisiaan ja eri rypäisiin kuuluvat kaukana toisistaan. Ryvästämisestä on useita muunnelmia ja niitä varten erilaisia algoritmeja. Ongelmien tarkka ratkaiseminen on laskennallisesti vaativaa, mutta joitakin approksimointialgoritmeja tunnetaan.

2.7 Hajautettuja algoritmeja

Ohjaajan arvio: A.

Paikalliset algoritmit (*local algorithm*)

[KMW06, KW05, Lin92, NS95, PR07, PY91, PY93, Urr07]

Paikallinen algoritmi on hajautettu algoritmi, joka ratkaisee ongelman vakioajassa riippumatta syötteenä olevan verkon koosta. Verkon kukin solmu suorittaa laskentaa itsenäisesti. Vakioajassa informaatiota voidaan kerätä vain vakioetäisyydeltä; kunkin solmun tekemä päätös on siis funktio syötteestä, joka oli alkutilanteessa saatavilla solmun lähiympäristössä enintään tietyllä etäisyydellä solmusta. Tällainen laskennan malli on luonnollisesti hyvin rajoitettu. Vain harvoja kombinatorisia ongelmia voidaan ratkaista tarkasti paikallisilla algoritmeilla: paikallisella algoritmilla ei voi edes värittää rengasta kolmella värillä. Jos tyydytään approksimaatioalgoritmeihin, tilanne on kuitenkin vähemmän synkkä.

Itsestabiloivat algoritmit (*self-stabilising algorithm*)

[AV91, Dij74, Dij86, Dol00, Sch93]

Hajautettu järjestelmä on itsestabiloiva, jos se palautuu äärellisessä ajassa kelvolliseen suoritukseen riippumatta siitä, mikä on järjestelmän alkutila.

Kursseja: Hajautettujen algoritmien seminaari syksyllä 2007.

Johtajan valinta [BIN06], [Lyn96, luku 3]

2.8 Tietoturva

Ohjaajan arvio: C.

Julkisen avaimen salakirjoitus [RSA78]

RSA-algoritmi yms.

Liittyy: Kryptografiaa, algebraa, lukuteoriaa.

Tiivistefunktiot kryptografiassa [Pre93], [Sta03, luku 12], [WY05]

Monen osapuolen protokollat [AKNRT04], [BM03, luku 6], [TWL05]

2.9 Muita aiheita

Ohjaajan arvio: C.

Mekanismisuunnittelu (*mechanism design*)

[BR97, luku 7], [MT99], [Nis99], [Pap01]

Mekanismisuunnittelu on “pelien suunnittelua” peliteoreettisessa mielessä. Toisin kuin tyypillisessä peliteorian ongelmassa, tässä ei asetuta itsekään “pelaajan” asemaan ratkaisemaan optimaalista tapaa pelata peliä, vaan asetutaan “keskusjohdon” asemaan suunnittelemaan pelin säännöt siten että itsekkäiden pelaajien omaa hyötyä maksimoivasta käytöksestä seuraa keskusjohdon haluama lopputulos. Esim. hyvin suunnitelluista pelisäännöistä voi seurata ettei itsekään pelaajan kannata petkuttaa tai vahingoittaa muita pelaajia.

Tunnettuna esimerkkinä mekanismisuunnittelusta voidaan mainita *Vickreyn huutokauppasääntö*, jota käytettiin esim. Googlen listausannissa.

Tietojenkäsittelytieteellä on liittymäkohtansa taloustieteisiin ja peliteoriaan. Mekanismisuunnittelua voi soveltaa myös Internetiin [Pap01]. Toistuvien pelien tapauksessa peliteoreettisilla aiheilla on liittymäkohtia koneoppimiseen: TD-oppiminen, palauteoppiminen, ja Markovin prosessit.

Onpa maailma pieni -ilmiö (*small world phenomenon*) [Kle00]

Analysoitaessa erilaisia verkostoja on havaittu, että useimmiten mitä tahansa kahta verkon solmua yhdistää lyhyt polku. Esimerkiksi lentoreiteissä, internetissä, geenisäätelyssä ja ihmisten tuttavuuspiireissä tämä ilmiö on havaittavissa. Mutta voidaanko tällaisten verkostojen syntyä selittää algoritmisesti?

Nopea Fourier- ja Möbius-muunnos [CLRS01, luku 30], [Ken92]

Liittyy: Fourier-muunnosta käsitellään signaalinkäsittelyn kurseilla.

Lähteet

- ABM04 Achlioptas, D., Beame, P. ja Molloy, M. S. O., A sharp threshold in proof complexity yields lower bounds for satisfiability search. *Journal of Computer and System Sciences*, 68,2(2004), sivut 238–268.
- ACM04 Asperti, A., Coppola, P. ja Martini, S., (Optimal) duplication is not elementary recursive. *Information and Computation*, 193,1(2004), sivut 21–56.
- AGR01 Amato, N. M., Goodrich, M. T. ja Ramos, E. A., A randomized algorithm for triangulating a simple polygon in linear time. *Discrete & Computational Geometry*, 26,2(2001), sivut 245–265.
- AHV95 Abiteboul, S., Hull, R. ja Vianu, V., *Foundations of Databases*. Addison-Wesley, 1995.
- AK89 Aarts, E. ja Korst, J., *Simulated Annealing and Boltzmann Machines: a Stochastic Approach to Combinatorial Optimization and Neural Computing*. Wiley, 1989.
- AKNRT04 Amir, Y., Kim, Y., Nita-Rotaru, C. ja Tsudik, G., On the performance of group key agreement protocols. *ACM Transactions on Information and System Security*, 7,3(2004), sivut 457–488.
- ALM⁺98 Arora, S., Lund, C., Motwani, R., Sudan, M. ja Szegedy, M., Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45,3(1998), sivut 501–555.
- AM00 Aji, S. M. ja McEliece, R. J., The generalized distributive law. *IEEE Transactions on Information Theory*, 46,2(2000), sivut 325–343.
- AMS99 Alon, N., Matias, Y. ja Szegedy, M., The space complexity of approximating the frequency moments. *Journal of Computer and System Sciences*, 58,1(1999), sivut 137–147.
- Aro98 Arora, S., Polynomial time approximation schemes for Euclidean traveling salesman and other geometric problems. *Journal of the ACM*, 45,5(1998), sivut 753–782.
- Aue02 Auer, P., Using confidence bounds for exploitation-exploration trade-offs. *Journal of Machine Learning Research*, 3(2002), sivut 397–422.
- AV91 Awerbuch, B. ja Varghese, G., Distributed program checking: A paradigm for building self-stabilizing distributed protocols. *Proc. 32nd Annual Symposium on Foundations of Computer Science*. IEEE, lokakuu 1991, sivut 258–267.

- Bac90 Backhouse, R. C., Constructive type theory: A perspective from computing science. Teoksessa *Formal Development of Programs and Proofs*, Dijkstra, E. W., toimittaja, Addison-Wesley, 1990, luku 1, sivut 1–32.
- BAJ00 Ben-Amram, A. M. ja Jones, N. D., Computational complexity via programming languages: Constant factors do matter. *Acta Informatica*, 37,2(2000), sivut 83–120.
- Bal95 Balaban, I. J., An optimal algorithm for finding segments intersections. *Proc. 11th Annual Symposium on Computational Geometry*, New York, NY, kesäkuu 1995, ACM Press, sivut 211–219.
- BDFC05 Bender, M. A., Demaine, E. D. ja Farach-Colton, M., Cache-oblivious B-trees. *SIAM Journal on Computing*, 35,2(2005), sivut 341–358.
- BDGJ99 Bublely, R., Dyer, M., Greenhill, C. ja Jerrum, M., On approximately counting colorings of small degree graphs. *SIAM Journal on Computing*, 29,2(1999), sivut 387–400.
- BEHW89 Blumer, A., Ehrenfeucht, A., Haussler, D. ja Warmuth, M. K., Learnability and the Vapnik–Chervonenkis dimension. *Journal of the ACM*, 36,4(1989), sivut 929–965.
- Ben99 Bengio, Y., Markovian models for sequential data. *Neural Computing Surveys*, 2(1999), sivut 129–162.
- BIN06 Bordim, J. L., Ito, Y. ja Nakano, K., Randomized leader election protocols in noisy radio networks with a single transceiver. *Proc. 4th International Symposium on Parallel and Distributed Processing and Applications*, osa 4330 sarjasta *Lecture Notes in Computer Science*, Berlin, joulukuu 2006, Springer-Verlag, sivut 246–256.
- BJdM97 Bird, R. S., Jones, G. ja de Moor, O., More haste, less speed: Lazy versus eager evaluation. *Journal of Functional Programming*, 7,5(1997), sivut 541–547.
- BL00 Benedikt, M. ja Libkin, L., Relational queries over interpreted structures. *Journal of the ACM*, 47,4(2000), sivut 644–680.
- BL02 Benedikt, M. ja Libkin, L., Aggregate operators in constraint query languages. *Journal of Computer and System Sciences*, 64,3(2002), sivut 628–654.
- BM03 Boyd, C. ja Mathuria, A., *Protocols for Authentication and Key Establishment*. Springer-Verlag, Berlin, 2003.
- Bor77 Borodin, A., On relating time and space to size and depth. *SIAM Journal on Computing*, 6,4(1977), sivut 733–744.

- BR97 Balinski, M. ja Ratier, G., Of stable marriages and graphs, and strategy and polytopes. *SIAM Review*, 39,4(1997), sivut 575–604.
- BS90 Boppana, R. B. ja Sipser, M., The complexity of finite functions. Teoksessä *Handbook of Theoretical Computer Science*, van Leeuwen, J., toimittaja, osa A: Algorithms and Complexity, Elsevier, 1990, sivut 757–804.
- BW94 Burrows, M. ja Wheeler, D., A block sorting lossless data compression algorithm. Tekninen raportti 124, Digital Equipment Corporation, 1994.
- Cha00 Chazelle, B., A minimum spanning tree algorithm with inverse-Ackermann type complexity. *Journal of the ACM*, 47,6(2000), sivut 1028–1047.
- CKJ01 Chen, J., Kanj, I. A. ja Jia, W., Vertex cover: Further observations and further improvements. *Journal of Algorithms*, 41,2(2001), sivut 280–301.
- Cla98 Clark, D. R., *Compact pat trees*. Väitöskirja, University of Waterloo, Waterloo, Ontario, 1998.
- CLRS01 Cormen, T. H., Leiserson, C. E., Rivest, R. L. ja Stein, C., *Introduction to Algorithms*. The MIT Press, Cambridge, MA, toinen painos, 2001.
- CM05 Cormode, G. ja Muthukrishnan, S., An improved data stream summary: The count-min sketch and its applications. *Journal of Algorithms*, 55,1(2005), sivut 58–75.
- CNSvS94 Coquand, T., Nordström, B., Smith, J. M. ja von Sydow, B., Type theory and programming. *Bulletin of the EATCS*, 52(1994), sivut 203–228.
- Col90 Colmerauer, A., An introduction to Prolog III. *Communications of the ACM*, 33,7(1990), sivut 69–90.
- CR02 Crochemore, M. ja Rytter, W., *Jewels of Stringology*. World Scientific, Singapore, 2002.
- CSGG02 Cadoli, M., Schaerf, M., Giovanardi, A. ja Giovanardi, M., An algorithm to evaluate quantified boolean formulae and its experimental evaluation. *Journal of Automated Reasoning*, 28,2(2002), sivut 101–142.
- Dij74 Dijkstra, E. W., Self-stabilizing systems in spite of distributed control. *Communications of the ACM*, 17,11(1974), sivut 643–644.
- Dij86 Dijkstra, E. W., A belated proof of self-stabilization. *Distributed Computing*, 1,1(1986), sivut 5–6.

- Din06 Dinur, I., The PCP theorem by gap amplification. *Proc. 38th Annual ACM Symposium on Theory of Computing*, New York, NY, toukokuu 2006, ACM Press, sivut 241–250.
- DL05 Dasgupta, S. ja Long, P. M., Performance guarantees for hierarchical clustering. *Journal of Computer and System Sciences*, 70,4(2005), sivut 555–569.
- Dol00 Dolev, S., *Self-Stabilization*. The MIT Press, Cambridge, MA, 2000.
- FLPR99 Frigo, M., Leiserson, C. E., Prokop, H. ja Ramachandran, S., Cache-oblivious algorithms. *Proc. 40th Annual Symposium on Foundations of Computer Science*, Los Alamitos, CA, lokakuu 1999, IEEE Computer Society Press, sivut 285–298.
- GK98 Garg, N. ja Könemann, J., Faster and simpler algorithms for multicommodity flow and other fractional packing problems. *Proc. 39th Annual Symposium on Foundations of Computer Science*, Los Alamitos, CA, marraskuu 1998, IEEE Computer Society Press, sivut 300–309.
- Gol89 Goldberg, D. E., *Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison-Wesley, 1989.
- GS68 Gale, D. ja Shapley, L. S., College admissions and the stability of marriage. *The American Mathematical Monthly*, 69,1(1968), sivut 9–15.
- GS85 Gale, D. ja Sotomayor, M., Some remarks on the stable matching problem. *Discrete Applied Mathematics*, 11,3(1985), sivut 223–232.
- GV99 Gammerman, A. ja Vovk, V., Kolmogorov complexity: Sources, theory and applications. *The Computer Journal*, 42,4(1999), sivut 252–255.
- GW99 Gent, I. P. ja Walsh, T., Beyond NP: the QSAT phase transition. *Proc. 16th National Conference on Artificial Intelligence*. AAAI Press, heinäkuu 1999, sivut 648–653.
- Hau92 Haussler, D., Decision theoretic generalizations of the PAC model for neural net and other learning applications. *Information and Computation*, 100,1(1992), sivut 78–150.
- HGL93 Homaifar, A., Guan, S. ja Liepins, G. E., A new approach on the traveling salesman problem by genetic algorithms. *Proc. 5th International Conference on Genetic Algorithms*. Morgan Kaufmann, heinäkuu 1993, sivut 460–466.
- Hoa69 Hoare, C. A. R., An axiomatic basis for computer programming. *Communications of the ACM*, 12,10(1969), sivut 576–580.
- HS88 Hajek, B. ja Sasaki, G., Link scheduling in polynomial time. *IEEE Transactions on Information Theory*, 34,5(1988), sivut 910–917.

- Hås89 Håstad, J., Almost optimal lower bounds for small depth circuits. Teoksessa *Advances in Computing Research*, Micali, S., toimittaja, osa 5: Randomness and Computation, JAI Press, 1989, sivut 143–170.
- IMMM99 Iwama, K., Manlove, D., Miyazaki, S. ja Morita, Y., Stable marriage with incomplete lists and ties. *Proc. 26th International Colloquium on Automata, Languages and Programming*, osa 1644 sarjasta *Lecture Notes in Computer Science*, Berlin, heinäkuu 1999, Springer-Verlag, sivut 443–452.
- Jac89 Jacobson, G., *Succinct Static Data Structures*. Väitöskirja, Carnegie Mellon University, Pittsburgh, PA, 1989.
- Jan03 Jansen, K., Approximate strong separation with application in fractional graph coloring and preemptive scheduling. *Theoretical Computer Science*, 302,1–3(2003), sivut 239–256.
- JLV99 Jiang, T., Li, M. ja Vitányi, P. M. B., New applications of the incompressibility method. *The Computer Journal*, 42,4(1999), sivut 287–293.
- JLV00 Jiang, T., Li, M. ja Vitányi, P. M. B., Average-case analysis of algorithms using Kolmogorov complexity. *Journal of Computer Science and Technology*, 15,5(2000), sivut 402–408.
- Joh84 Johnson, D. S., The NP-completeness column: An ongoing guide. *Journal of Algorithms*, 5,3(1984), sivut 433–447.
- Joh90a Johnson, D. S., Catalog of complexity classes. Teoksessa *Handbook of Theoretical Computer Science*, van Leeuwen, J., toimittaja, osa A: Algorithms and Complexity, Elsevier, 1990, sivut 67–162.
- Joh90b Johnson, D. S., Local optimization and the traveling salesman problem. *Proc. 17th International Colloquium on Automata, Languages and Programming*, osa 443 sarjasta *Lecture Notes in Computer Science*, Berlin, heinäkuu 1990, Springer-Verlag, sivut 446–461.
- KCHP01 Keogh, E. J., Chu, S., Hart, D. ja Pazzani, M. J., An online algorithm for segmenting time series. *Proc. 2001 IEEE International Conference on Data Mining*, Los Alamitos, CA, marraskuu 2001, IEEE Computer Society Press, sivut 289–296.
- Ken92 Kennes, R., Computational aspects of the Möbius transformation of graphs. *IEEE Transactions on Systems, Man, and Cybernetics*, 22,2(1992), sivut 201–223.
- KGV83 Kirkpatrick, S., Gelatt, C. D. ja Vecchi, M. P., Optimization by simulated annealing. *Science*, 220,4598(1983), sivut 671–680.

- KKL⁺00 Kohonen, T., Kaski, S., Lagus, K., Salojarvi, J., Honkela, J., Paatero, V. ja Saarela, A., Self organization of a massive document collection. *IEEE Transactions on Neural Networks*, 11,3(2000), sivut 574–585.
- Kle00 Kleinberg, J. M., The small-world phenomenon: An algorithm perspective. *Proc. 32nd Annual ACM Symposium on Theory of Computing*, New York, NY, toukokuu 2000, ACM Press, sivut 163–170.
- KLM96 Kaelbling, L. P., Littman, M. L. ja Moore, A. P., Reinforcement learning: A survey. *Journal of Artificial Intelligence Research*, 4(1996), sivut 237–285.
- KMP77 Knuth, D. E., Morris, J. H. ja Pratt, V. R., Fast pattern matching in strings. *SIAM Journal on Computing*, 6,2(1977), sivut 323–350.
- KMW06 Kuhn, F., Moscibroda, T. ja Wattenhofer, R., The price of being near-sighted. *Proc. 17th Annual ACM-SIAM Symposium on Discrete Algorithms*. ACM Press, 2006, sivut 980–989.
- KW05 Kuhn, F. ja Wattenhofer, R., Constant-time distributed dominating set approximation. *Distributed Computing*, 17,4(2005), sivut 303–310.
- Lei99 Leivant, D., Applicative control and computational complexity. *Proc. 13th International Workshop on Computer Science Logic*, osa 1683 sarjasta *Lecture Notes in Computer Science*, Berlin, 1999, Springer-Verlag, sivut 82–95.
- Lib99 Libkin, L., Query languages with arithmetic and constraint databases. *SIGACT News*, 30,4(1999), sivut 41–50.
- Lin92 Linial, N., Locality in distributed graph algorithms. *SIAM Journal on Computing*, 21,1(1992), sivut 193–201.
- LY94 Lund, C. ja Yannakakis, M., On the hardness of approximating minimization problems. *Journal of the ACM*, 41,5(1994), sivut 960–981.
- Lyn96 Lynch, N., *Distributed Algorithms*. Morgan Kaufmann, 1996.
- Man01 Manzini, G., An analysis of the Burrows–Wheeler transform. *Journal of the ACM*, 48,3(2001), sivut 407–430.
- MM93 Manber, U. ja Myers, E. W., Suffix arrays: A new method for on-line string searches. *SIAM Journal on Computing*, 22,5(1993), sivut 935–948.
- MR95 Motwani, R. ja Raghavan, P., *Randomized Algorithms*. Cambridge University Press, 1995.

- MT99 Monderer, D. ja Tennenholtz, M., Distributed games: From mechanisms to protocols. *Proc. 16th National Conference on Artificial Intelligence*. AAAI Press, heinäkuu 1999, sivut 32–37.
- Nis99 Nisan, N., Algorithms for selfish agents. *Proc. 16th Annual Symposium on Theoretical Aspects of Computer Science*, osa 1563 sarjasta *Lecture Notes in Computer Science*, Berlin, maaliskuu 1999, Springer-Verlag, sivut 1–15.
- NM07 Navarro, G. ja Mäkinen, V., Compressed full-text indexes. *ACM Computing Surveys*, 39,1(2007), sivu 2.
- NS95 Naor, M. ja Stockmeyer, L., What can be computed locally? *SIAM Journal on Computing*, 24,6(1995), sivut 1259–1277.
- Pap01 Papadimitriou, C. H., Algorithms, games, and the Internet. *Proc. 33rd Annual ACM Symposium on Theory of Computing*, New York, NY, heinäkuu 2001, ACM Press, sivut 749–753.
- Pip97 Pippenger, N., Pure versus impure Lisp. *ACM Transactions on Programming Languages and Systems*, 19,2(1997), sivut 223–238.
- PR04 Pitassi, T. ja Raz, R., Regular resolution lower bounds for the weak pigeonhole principle. *Combinatorica*, 24,3(2004), sivut 503–524.
- PR07 Parnas, M. ja Ron, D., Approximating the minimum vertex cover in sublinear time and a connection to distributed algorithms. *Theoretical Computer Science*, 381,1–3(2007), sivut 183–196.
- Pre93 Preneel, B., *Analysis and Design of Cryptographic Hash Functions*. Väitöskirja, Katholieke Universiteit Leuven, 1993.
- PY91 Papadimitriou, C. H. ja Yannakakis, M., On the value of information in distributed decision-making. *Proc. 10th Annual ACM Symposium on Principles of Distributed Computing*. ACM Press, elokuu 1991, sivut 61–64.
- PY93 Papadimitriou, C. H. ja Yannakakis, M., Linear programming without the matrix. *Proc. 25th Annual ACM Symposium on Theory of Computing*. ACM Press, toukokuu 1993, sivut 121–129.
- Qui86 Quinlan, J. R., Induction of decision trees. *Machine Learning*, 1,1(1986), sivut 81–106.
- Rin99 Rintanen, J., Improvements to the evaluation of quantified boolean formulae. *Proc. 16th International Joint Conference on Artificial Intelligence*, San Francisco, CA, heinäkuu 1999, Morgan Kaufmann, sivut 1192–1197.

- RR97 Razborov, A. A. ja Rudich, S., Natural proofs. *Journal of Computer and System Sciences*, 55,1(1997), sivut 24–35.
- RSA78 Rivest, R. L., Shamir, A. ja Adleman, L. M., A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21,2(1978), sivut 120–126.
- RZ05 Robins, G. ja Zelikovsky, A., Tighter bounds for graph Steiner tree approximation. *SIAM Journal on Discrete Mathematics*, 19,1(2005), sivut 122–134.
- Sán02 Sánchez, V. D., Frontiers of research in BSS/ICA. *Neurocomputing*, 49,1–4(2002), sivut 7–23.
- Sch93 Schneider, M., Self-stabilization. *ACM Computing Surveys*, 25,1(1993), sivut 45–67.
- SH96 Stearns, R. E. ja Hunt, H. B., An algebraic model for combinatorial problems. *SIAM Journal on Computing*, 25,2(1996), sivut 448–476.
- SS02 Schölkopf, B. ja Smola, A. J., A short introduction to learning with kernels. Teoksessa *Advanced Lectures on Machine Learning*, Mendelson, S. ja Smola, A. J., toimittajat, osa 2600 sarjasta *Lecture Notes in Artificial Intelligence*, Springer-Verlag, Berlin, helmikuu 2002, sivut 41–64.
- ST85 Sleator, D. D. ja Tarjan, R. E., Self-adjusting binary search trees. *Journal of the ACM*, 32,3(1985), sivut 652–686.
- Sta03 Stallings, W., *Cryptography and Network Security: Principles and Practice*. Prentice Hall, kolmas painos, 2003.
- Ste03 Stearns, R. E., Deterministic versus nondeterministic time and lower bound problems. *Journal of the ACM*, 50,1(2003), sivut 91–95.
- Tar83 Tarjan, R. E., *Data Structures and Network Algorithms*. Society for Industrial and Applied Mathematics, 1983.
- Tes95 Tesauro, G., Temporal difference learning and TD-Gammon. *Communications of the ACM*, 38,3(1995), sivut 58–68.
- Thr98 Thrun, S., Learning metric-topological maps for indoor mobile robot navigation. *Artificial Intelligence*, 99,1(1998), sivut 21–71.
- TvL84 Tarjan, R. E. ja van Leeuwen, J., Worst-case analysis of set union algorithms. *Journal of the ACM*, 31,2(1984), sivut 245–281.
- TWL05 Trappe, W., Wang, Y. ja Liu, K. J. R., Resource-aware conference key establishment for heterogeneous networks. *IEEE/ACM Transactions on Networking*, 13,1(2005), sivut 134–146.

- Urr07 Urrutia, J., Local solutions for global problems in wireless networks. *Journal of Discrete Algorithms*, 5,3(2007), sivut 395–407.
- Vap98 Vapnik, V. N., *Statistical Learning Theory*. Wiley, 1998.
- Vaz03 Vazirani, V. V., *Approximation Algorithms*. Springer-Verlag, Berlin, 2003.
- Wad00 Wadler, P., Old ideas form the basis of advancements in functional programming. *Dr. Dobbs's Journal*, (2000). <http://www.ddj.com/architect/184404384>. [5.1.2008]
- WT89 Westbrook, J. ja Tarjan, R. E., Amortized analysis of algorithms for set union with backtracking. *SIAM Journal on Computing*, 18,1(1989), sivut 1–11.
- WY05 Wang, X. ja Yu, H., How to break MD5 and other hash functions. *Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, osa 3494 sarjasta *Lecture Notes in Computer Science*, Berlin, toukokuu 2005, Springer-Verlag, sivut 19–35.