582204 Kandidaatintutkielma-kurssi (Tieteellisen kirjoittamisen kurssi), kevät 2017
Aiheita, 16. tammikuuta 2017

1 Ohjeita

Tässä listassa on ehdotuksia kandidaatintutkielma-kurssin aiheiksi. Valitse listalta joitain kandidaattiaiheita. Listan aiheet ovat suuntaa-antavia; lopullinen rajaus ja otsikko sovitaan kurssin kuluessa. Voit myös ehdottaa omaa aihettasi. Oma aihe on kaikkein paras vaihtoehto, kunhan se sopii 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 silmäillä läpi esimerkiksi yksi lähdeartikkeli ennen kuin 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 Koneoppimista, tekoälyä, data-analyysia ja tiedon louhintaa

Ohjaajan arvio: A. *Liittyy:* Todennäköisyyslaskentaa. *Kursseja:* Johdatus koneoppimiseen, Johdatus tekoälyyn, Todennäköisyysmallit, Tiedon louhinta, Laskennallinen data-analyysi, Kolme käsitettä -kurssit, Graphical models, todennäköisyyslaskennan ja tilastotieteen 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.

Liittyy: Algebra.

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 epälineaarisena 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, tiedon louhintaa.

Ei-negatiiviset matriisihajotelmat [LS99]

Ei-negatiivisissa matriisihajotelmissa ei-negatiivinen matriisi hajotetaan kahden ei-negatiivisen matriisin tuloksi. Näin saadaan joissain tilanteissa helpommin tulkittavia hajotelmia kuin esimerkiksi riippumattomien komponenttien analyysillä. Valitettavasti ei-negatiivisten hajotelmien laskeminen on melko vaikeaa.

Liittyy: Matriisilaskentaa, tiedon louhintaa.

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 olivat 1990-luvun loppupuolen kuumin koneoppimisparadigma. 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, ORSS06, AV07]

Ryvästämisessä *(clustering)* suuri joukko pisteitä jaetaan pieneen määrään *rypäitä* siten, että samaan rypääseen 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.

Paikkatiedon ryvästäminen [NM04]

Assosiaatiot paikkatiedossa [HSX04]

Liittyy: Tiedonlouhinnan kurssit, assosiaatiosäännöt.

Emerging pattens, change patterns [DL99]

Ryvästäminen korkeaulotteisissa avaruuksissa [AGGR98]

Ryvästettäessä hyvin korkeaulotteista dataa kaikkia datan ulottuvuuksia käyttävät metriikat toimivat usein huonosti. Ongelmaan on esitetty ratkaisuksi algoritmeja, jotka tunnistavat ryppäitä alkuperäisen avaruuden aliavaruuksissa.

Tiedon louhinta verkoista [KK01]

Usein datan rakenne on kuvattavissa luontevasti verkkona, jolloin usein toistuvien hahmojen etsiminen muuttuu verkossa usein toistuvien aliverkkojen etsimisiksi. Ongelmien muotoilussa ja algoritmeissa on huomioitava klassisia verkkoteorian kysymyksiä kuten verkkojen isomorfisuus.

Parametriton tiedon louhinta [KLR04]

2.2 Laskennan teoriaa

Ohjaajan arvio: B. *Kursseja:* Laskennan mallit, Laskennan vaativuus, Laskennan teoria, logiikan kurssit.

Kvantifioidut Boolen kaavat *(quantified Boolean formulae, QBF)* [CSGG02, GW99, Rin99]

Kvantifioidut Boolen 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 $O(f(k)\,\mathrm{poly}(n))$, missä n on syötteen koko, k ongelman parametri (esimerkiksi solmupeitteen koko), $f(k)$ on funktio, joka ei riipu parametrista n ja $\mathrm{poly}(\cdot)$ on polynomi. Tälläiset algoritmit pystyvät käsittelemään suuriakin syötteitä, jos parametri k on kiinnitetty riittävän pieneksi.

Laskentapiirien 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 pariteettifunktioille. 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 tietyssä mielessä tehokkaasti rinnakkaistuvia.

Satunnaislaskennan vaativuusteoriaa [Joh84, Joh90a]

Satunnaisuus on tärkeä algoritminen tekniikka, jota käytetään monella lailla eri tyyppisten ongelmien ratkaisussa. Tämän aiheen tarkoituksena on tarkastella satunnaisalgoritmien yleistä teoriaa: millaisia vaativuusluokkia satunnaislaskennassa voidaan määritellä 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.

2.3 Tietorakenteita ja algoritmeja

Ohjaajan arvio: B. *Kursseja:* Tietorakenteet, Algoritmien suunnittelu ja analyysi, Merkkijonomenetelmät, Tiedon tiivistämisen tekniikat, Advanced data structures.

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 [Cla97, Jac89]

Tiedon tiivistyksessä on tavoitteena esittää tieto (esim. tekstidokumentti) mahdollisimman pienessä tilassa siten, että alkuperäinen tieto voidaan palauttaa virheettä. 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.

Hahmonsovitus merkkijonoissa [CR02, KMP77]

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

Staattisen tekstin indeksointi loppuosatietorakenteilla [MM93]

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

Muistihierarkia-algoritmit [BDFC05, FLPR99]

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

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].

2.4 Kombinatorista optimointia

Ohjaajan arvio: B. *Liittyy:* Kombinatoriikka, verkot, puut, lineaarinen ohjelmointi. *Kursseja:* Algoritmien suunnittelu ja analyysi, Diskreetti optimointi, Kombinatorinen optimointi, Approksimointialgoritmit, Satunnaisalgoritmit, diskreetin matematiikan kurssit.

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 virittävä 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]

Murtolukuvärityksongelmat ovat muunnoksia tunnetuista verkonvärityksongelmista. 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 approksimointialgoritmeja.

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

Mitä nykyään tiedetään Steiner-puihin liittyvien optimointiongelmien approksimoituvuudesta ja ei-approksimoituvuudesta?

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

Simuloitu jäähdytys on yleiskäyttöinen satunnaisuuteen perustuva menetelmä, jota voidaan käyttää erilaisten optimointiongelmien heuristiseen ratkaisemiseen.

Geneettiset algoritmit [SP94, 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.

Siirtostrategia *(shifting strategy)* [HM85, Bak94, HMR+98]

Yleiskäyttöinen tekniikka, jota voidaan käyttää polynomiaikaisen approksimointiskeeman laatimiseen lukuisiin NP-koviin ongelmiin geometrisissa verkoissa (esim. yksikkökiekkoverkossa tai tasoverkossa).

2.5 Laskennallista geometriaa

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

Leikkaavien janojen ongelma [Bal95]

Monikulmioiden kolmiointialgoritmit [AGR01]

Äärellisen tarkkuuden geometriaa [GGHT97, GM98, Hob99, HP02, Pac08, CKNT08, Buz07]

Käytännön laskennassa geometristen kappaleiden koordinaatteja ei käsitellä mielivaltaisen tarkkoina reaalilukuina. Miten koordinaatit voidaan pyöristää rajalliseen tarkkuuteen? Millaisia vaatimuksia pyöristämiselle asetetaan sovelluksissa? Millaisilla algoritmeilla nämä vaatimukset saadaan täytettyä?

Ydinjoukot ja geometriset approksimointialgoritmit [AHPV04, HP05]

Monet laskennallisen geometrian ongelmat liittyvät isoihin pistejoukkoihin: on esimerkiksi löydettävä pienin pistejoukkoa ympäröivä pallo tai laatikko. Tällaisten ongelmien tehokkaaseen likimääräiseen ratkaisemiseen on olemassa kohtalaisen yleinen menetelmä: (1) etsitään pistejoukosta ns.

ydinjoukko *(coreset)*, joka on tarkasteltavan ongelman kannalta mahdollisimman edustava; (2) ratkaistaan ongelma tässä huomattavasti pienemmässä pistejoukossa. Mihin ongelmiin tämä lähestymistapa soveltuu ja mihin ei?

Konveksin peitteen yleistyksiä [EKS83, EM94, Ede98]

Ns. α-muodot ovat pistejoukon konveksin peitteen yleistyksiä.

Liittyy: Mahdollisesti varsin matemaattinen aihe.

Näkyvyysverkot [Eve90, CSC95, Gho97, AK02]

Monikulmion näkyvyysverkko *(visibility graph)* kuvaa, minkä nurkkapisteiden välillä on esteetön näköyhteys. Jos monikulmio on annettu, näkyvyysverkon muodostaminen on suoraviivaista. Mutta jos on annettu verkko, voidaanko tunnistaa, onko se jonkin monikulmion näkyvyysverkko?

2.6 Logiikkaa; ohjelmointikielten syntaksia ja semantiikkaa

Ohjaajan arvio: C. *Kursseja:* Johdatus funktionaaliseen ohjelmointiin, Johdatus lambda-kalkyyliin, Spesifioinnin ja verifioinnin perusteet, logiikan kurssit.

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.

Spesifikaatiot ovat väitteitä, ohjelmat niiden todistuksia [Bac90, CNSvS94, Wad00]

Formaali looginen ohjelmankehitys.

Liittyy: Logiikkaa, spesifiointia ja verifiointia.

Ohjelmien aksiomaattinen semantiikka [Hoa69]

Heikoimman ennakkoehdon semantiikka, todistetusti oikeellisten ohjelmien kehittäminen.

Liittyy: Logiikkaa, spesifiointia ja verifiointia.

2.7 Hajautettuja algoritmeja

Ohjaajan arvio: C. *Konferensseja:* PODC, SPAA, DISC.

Hajautettu verkon väritys [CV86, Lin92], [CLR90, luku 30.5]

Verkkoa ei voi värittää hajautetulla algoritmilla vakioajassa, ei edes siinä yksinkertaisessa erikoistapauksessa, että kyseessä on n:n solmun rengas, jossa jokaisella solmulla on yksilöllinen tunniste. Sen sijaan renkaan värittämiseen on olemassa algoritmi, joka toimii ajassa $O(\log^* n)$; tämä on erittäin hitaasti kasvava funktio. Miten nämä tulokset yleistyvät muihin verkkoihin kuin renkaisiin? Mikä on yhteys muihin kombinatorisiin ongelmiin, esimerkiksi riippumattoman joukon etsimiseen?

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.

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.

Mustan aukon etsintää [FIS08]

Musta aukko on verkon solmu, johon astuva agentti katoaa jälkiä jättämättä. Missä tapauksessa usean agentin joukkue voi paikantaa mustan aukon (uhraamalla osan jäsenistään)?

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

2.8 Tietoturva

Ohjaajan arvio: C. *Kursseja:* Tietoturva.

Julkisen avaimen salakirjoitus [RSA78]

RSA-algoritmi yms.

Liittyy: Kryptografiaa, algebraa, lukuteoriaa.

Diffie-Hellman-avaimenvaihtoprotokolla [DH76]

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

Melko tekninen

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 itsekkään “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 itsekkään 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 tälläisten verkostojen syntyä selittää algoritmisesti?

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

Liittyy: Fourier-muunnosta käsitellään signaalinkäsittelyn kursseilla.

Viitteet

[ABM04] Dimitris Achlioptas, Paul Beame, and Michael S. O. Molloy. A sharp threshold in proof complexity yields lower bounds for satisfiability search. *Journal of Computer and System Sciences*, 68(2):238–268, 2004.

[AGGR98] Rakesh Agrawal, Johannes Gehrke, Dimitrios Gunopulos, and Prabhakar Raghawan. Automatic subspace clustering of high dimensional data for data mining applications. In *Proc. 1998 ACM SIGMOD International Conference on Management of Data*, pages 94–105. ACM Press, 1998.

[AGR01] Nancy M. Amato, Michael T. Goodrich, and Edgar A. Ramos. A randomized algorithm for triangulating a simple polygon in linear time. *Discrete & Computational Geometry*, 26(2):245–265, 2001.

[AHPV04] Pankaj K. Agarwal, Sariel Har-Peled, and Kasturi R. Varadarajan. Approximating extent measures of points. *Journal of the ACM*, 51(4):606–635, 2004.

[AHV95] Serge Abiteboul, Richard Hull, and Victor Vianu. *Foundations of Databases*. Addison-Wesley, 1995.

[AK89] Emile Aarts and Jan Korst. *Simulated Annealing and Boltzmann Machines: a Stochastic Approach to Combinatorial Optimization and Neural Computing*. Wiley, 1989.

[AK02] James Abello and Krishna Kumar. Visibility graphs and oriented matroids. *Discrete & Computational Geometry*, 28(4):449–465, 2002.

[AKNRT04] Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, and Gene Tsudik. On the performance of group key agreement protocols. *ACM Transactions on Information and System Security*, 7(3):457–488, 2004.

[AM00] Srinivas M. Aji and Robert J. McEliece. The generalized distributive law. *IEEE Transactions on Information Theory*, 46(2):325–343, 2000.

[AMS99] Noga Alon, Yossi Matias, and Mario Szegedy. The space complexity of approximating the frequency moments. *Journal of Computer and System Sciences*, 58(1):137–147, 1999.

[Aro98] Sanjeev Arora. Polynomial time approximation schemes for Euclidean traveling salesman and other geometric problems. *Journal of the ACM*, 45(5):753–782, 1998.

[Aue02] Peter Auer. Using confidence bounds for exploitation-exploration trade-offs. *Journal of Machine Learning Research*, 3:397–422, 2002.

[AV91] Baruch Awerbuch and George Varghese. Distributed program checking: A paradigm for building self-stabilizing distributed protocols. In *Proc. 32nd Annual Symposium on Foundations of Computer Science*, pages 258–267. IEEE, 1991.

[AV07] David Arthur and Sergei Vassilvitskii. k-means++: the advantages of careful seeding. In *Proc. 18th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1027–1035. Society for Industrial and Applied Mathematics, 2007.

[Bac90] Roland C. Backhouse. Constructive type theory: A perspecive from computing science. In Edsger W. Dijkstra, editor, *Formal Development of Programs and Proofs*, chapter 1, pages 1–32. Addison-Wesley, 1990.

[Bak94] Brenda S. Baker. Approximation algorithms for NP-complete problems on planar graphs. *Journal of the ACM*, 41(1):153–180, 1994.

[Bal95] Ivan J. Balaban. An optimal algorithm for finding segments intersections. In *Proc. 11th Annual Symposium on Computational Geometry*, pages 211–219. ACM Press, 1995.

[BDFC05] Michael A. Bender, Erik D. Demaine, and Martin Farach-Colton. Cache-oblivious B-trees. *SIAM Journal on Computing*, 35(2):341–358, 2005.

[BDGJ99] Russ Bubley, Martin Dyer, Catherine Greenhill, and Mark Jerrum. On approximately counting colorings of small degree graphs. *SIAM Journal on Computing*, 29(2):387–400, 1999.

[Ben99] Yoshua Bengio. Markovian models for sequential data. *Neural Computing Surveys*, 2:129–162, 1999.

[BIN06] Jacir Luiz Bordim, Yasuaki Ito, and Koji Nakano. Randomized leader election protocols in noisy radio networks with a single transceiver. In *Proc. 4th International Symposium on Parallel and Distributed Processing and Applications*, volume 4330 of *Lecture Notes in Computer Science*, pages 246–256. Springer-Verlag, 2006.

[BL00] Michael Benedikt and Leonid Libkin. Relational queries over interpreted structures. *Journal of the ACM*, 47(4):644–680, 2000.

[BL02] Michael Benedikt and Leonid Libkin. Aggregate operators in constraint query languages. *Journal of Computer and System Sciences*, 64(3):628–654, 2002.

[BM03] Colin Boyd and Anish Mathuria. *Protocols for Authentication and Key Establishment.* Springer-Verlag, 2003.

[Bor77] Allan Borodin. On relating time and space to size and depth. *SIAM Journal on Computing*, 6(4):733–744, 1977.

[BR97] Michel Balinski and Guillaume Ratier. Of stable marriages and graphs, and strategy and polytopes. *SIAM Review*, 39(4):575–604, 1997.

[BS90] Ravi B. Boppana and Michael Sipser. The complexity of finite functions. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume A: Algorithms and Complexity, pages 757–804. Elsevier, 1990.

[Buz07] Lilian Buzer. Optimal simplification of polygonal chain for rendering. In *Proc. 23rd Annual Symposium on Computational Geometry*, pages 168–174. ACM Press, 2007.

[BW94] Michael Burrows and David Wheeler. A block sorting lossless data compression algorithm. Technical Report 124, Digital Equipment Corporation, 1994.

[Cha00] Bernard Chazelle. A minimum spanning tree algorithm with inverse-Ackermann type complexity. *Journal of the ACM*, 47(6):1028–1047, 2000.

[CKJ01] Jianer Chen, Iyad A. Kanj, and Weijia Jia. Vertex cover: Further observations and further improvements. *Journal of Algorithms*, 41(2):280–301, 2001.

[CKNT08] J. Chun, M. Korman, M. Nöllenburg, and T. Tokuyama. Consistent digital rays. In *Proc. 24th Annual Symposium on Computational Geometry*, pages 355–364. ACM Press, 2008.

[Cla97] David Clark. *Compact PAT Trees.* PhD thesis, University of Waterloo, 1997.

[CLR90] Thomas H. Cormen, Charles E. Leiserson, and Ronald L. Rivest. *Introduction to Algorithms.* The MIT Press, 1 edition, 1990.

[CLRS01] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms.* The MIT Press, 2 edition, 2001.

[CM05] Graham Cormode and S. Muthukrishnan. An improved data stream summary: The count-min sketch and its applications. *Journal of Algorithms*, 55(1):58–75, 2005.

[CNSvS94] Thierry Coquand, Bengt Nordström, Jan M. Smith, and Björn von Sydow. Type theory and programming. *Bulletin of the EATCS*, 52:203–228, 1994.

[Col90] Alain Colmerauer. An introduction to Prolog III. *Communications of the ACM*, 33(7):69–90, 1990.

[CR02] Maxime Crochemore and Wojciech Rytter. *Jewels of Stringology.* World Scientific, Singapore, 2002.

[CSC95] Seung-Hak Choi, Sung Yong Shin, and Kyung-Yong Chwa. Characterizing and recognizing the visibility graph of a funnel-shaped polygon. *Algorithmica*, 14(1):27–51, 1995.

[CSGG02] Marco Cadoli, Marco Schaerf, Andrea Giovanardi, and Massimo Giovanardi. An algorithm to evaluate quantified Boolean formulae and its experimental evaluation. *Journal of Automated Reasoning*, 28(2):101–142, 2002.

[CV86] Richard Cole and Uzi Vishkin. Deterministic coin tossing with applications to optimal parallel list ranking. *Information and Control*, 70(1):32–53, 1986.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, September 1976.

[Dij74] Edsger W. Dijkstra. Self-stabilizing systems in spite of distributed control. *Communications of the ACM*, 17(11):643–644, 1974.

[Dij86] Edsger W. Dijkstra. A belated proof of self-stabilization. *Distributed Computing*, 1(1):5–6, 1986.

[DL99] Guozhu Dong and Jinyan Li. Efficient mining of emerging patterns: Discovering trends and differences. In *Proc. 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 43–52. ACM Press, 1999.

[DL05] Sanjoy Dasgupta and Philip M. Long. Performance guarantees for hierarchical clustering. *Journal of Computer and System Sciences*, 70(4):555–569, 2005.

[Dol00] Shlomi Dolev. *Self-Stabilization.* The MIT Press, 2000.

[Ede98] H. Edelsbrunner. Shape reconstruction with Delaunay complex. In *Proc. 3rd Latin American Symposium on Theoretical Informatics*, volume 1380 of *Lecture Notes in Computer Science*, pages 119–132. Springer-Verlag, 1998.

[EKS83] H. Edelsbrunner, D. G. Kirkpatrick, and R. Seidel. On the shape of a set of points in the plane. *IEEE Transactions on Information Theory*, 29(4):551–559, 1983.

[EM94] H. Edelsbrunner and E. P. Mücke. Three-dimensional alpha shapes. *ACM Transactions on Graphics*, 13(1):43–72, 1994.

[Eve90] H. J. Everett. *Visibility Graph Recognition.* PhD thesis, University of Toronto, 1990.

[FIS08] Paola Flocchini, David Ilcinkas, and Nicola Santoro. Ping pong in dangerous graphs: Optimal black hole search with pure tokens. In *Proc. 22nd International Symposium on Distributed Computing*, volume 5218 of *Lecture Notes in Computer Science*, pages 227–241. Springer-Verlag, 2008.

[FLPR99] Matteo Frigo, Charles E. Leiserson, Harald Prokop, and Sridhar Ramachandran. Cache-oblivious algorithms. In *Proc. 40th Annual Symposium on Foundations of Computer Science*, pages 285–298. IEEE Computer Society Press, 1999.

[GGHT97] M. Goodrich, L. J. Guibas, J. Hershberger, and P. Tanenbaum. Snap rounding line segments efficiently in two and three dimensions. In *Proc. 13th Annual ACM Symposium on Computational Geometry*, pages 284–293. ACM Press, 1997.

[Gho97] Subir Kumar Ghosh. On recognizing and characterizing visibility graphs of simple polygons. *Discrete & Computational Geometry*, 17(2):143–162, 1997.

[GK98] Naveen Garg and Jochen Könemann. Faster and simpler algorithms for multicommodity flow and other fractional packing problems. In *Proc. 39th Annual Symposium on Foundations of Computer Science*, pages 300–309. IEEE Computer Society Press, 1998.

[GM98] Leonidas Guibas and David Marimont. Rounding arrangements dynamically. *International Journal of Computational Geometry and Applications*, 8:157–176, 1998.

[Gol89] David E. Goldberg. *Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison-Wesley, 1989.

[GS68] D. Gale and L. S. Shapley. College admissions and the stability of marriage. *The American Mathematical Monthly*, 69(1):9–15, 1968.

[GS85] David Gale and Marilda Sotomayor. Some remarks on the stable matching problem. *Discrete Applied Mathematics*, 11(3):223–232, 1985.

[GV99] Alexander Gammerman and Vladimir Vovk. Kolmogorov complexity: Sources, theory and applications. *The Computer Journal*, 42(4):252–255, 1999.

[GW99] Ian P. Gent and Toby Walsh. Beyond NP: the QSAT phase transition. In *Proc. 16th National Conference on Artificial Intelligence*, pages 648–653. AAAI Press, July 1999.

[HGL93] Abdollah Homaifar, Shanguchuan Guan, and Gunar E. Liepins. A new approach on the traveling salesman problem by genetic algorithms. In *Proc. 5th International Conference on Genetic Algorithms*, pages 460–466. Morgan Kaufmann, 1993.

[HM85] Dorit S. Hochbaum and Wolfgang Maass. Approximation schemes for covering and packing problems in image processing and VLSI. *Journal of the ACM*, 32(1):130–136, 1985.

[HMR+98] Harry B. Hunt, III, Madhav V. Marathe, Venkatesh Radhakrishnan, S. S. Ravi, Daniel J. Rosenkrantz, and Richard E. Stearns. NC-approximation schemes for NP- and PSPACE-hard problems for geometric graphs. *Journal of Algorithms*, 26(2):238–274, 1998.

[Hoa69] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, 1969.

[Hob99] J. D. Hobby. Practical segment intersection with finite precision output. *Computational Geometry: Theory and Applications*, 13(4):199–214, 1999.

[HP02] D. Halperin and E. Packer. Iterated snap rounding. *Computational Geometry: Theory and Applications*, 23(2):209–225, 2002.

[HP05] Sariel Har-Peled. No coreset, no cry. In *Proc. 24th International Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 3328 of *Lecture Notes in Computer Science*, pages 324–335. Springer-Verlag, 2005.

[HS88] Bruce Hajek and Galen Sasaki. Link scheduling in polynomial time. *IEEE Transactions on Information Theory*, 34(5):910–917, 1988.

[HSX04] Huang, Shekhar, and Xiong. Discovering colocation patterns from spatial data sets: A general approach. *IEEE Transactions on Knowledge and Data Engineering*, 16(12):1472–1485, 2004.

[Hås89] Johan Håstad. Almost optimal lower bounds for small depth circuits. In Silvio Micali, editor, *Advances in Computing Research*, volume 5: Randomness and Computation, pages 143–170. JAI Press, 1989.

[IMMM99] Kazuo Iwama, David Manlove, Shuichi Miyazaki, and Yasufumi Morita. Stable marriage with incomplete lists and ties. In *Proc. 26th International Colloquium on Automata, Languages and Programming*, volume 1644 of *Lecture Notes in Computer Science*, pages 443–452. Springer-Verlag, 1999.

[Jac89] Guy Jacobson. *Succinct Static Data Structures*. PhD thesis, Carnegie Mellon University, 1989.

[Jan03] Klaus Jansen. Approximate strong separation with application in fractional graph coloring and preemptive scheduling. *Theoretical Computer Science*, 302(1–3):239–256, 2003.

[JLV99] Tao Jiang, Ming Li, and Paul M. B. Vitányi. New applications of the incompressibility method. *The Computer Journal*, 42(4):287–293, 1999.

[JLV00] Tao Jiang, Ming Li, and Paul M. B. Vitányi. Average-case analysis of algorithms using Kolmogorov complexity. *Journal of Computer Science and Technology*, 15(5):402–408, 2000.

[Joh84] David S. Johnson. The NP-completeness column: An ongoing guide. *Journal of Algorithms*, 5(3):433–447, 1984.

[Joh90a] David S. Johnson. Catalog of complexity classes. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume A: Algorithms and Complexity, pages 67–162. Elsevier, 1990.

[Joh90b] David S. Johnson. Local optimization and the traveling salesman problem. In *Proc. 17th International Colloquium on Automata, Languages and Programming*, volume 443 of *Lecture Notes in Computer Science*, pages 446–461. Springer-Verlag, 1990.

[KCHP01] Eamonn J. Keogh, Selina Chu, David Hart, and Michael J. Pazzani. An online algorithm for segmenting time series. In *Proc. 1st IEEE International Conference on Data Mining*, pages 289–296. IEEE Computer Society Press, 2001.

[Ken92] Robert Kennes. Computational aspects of the Möbius transformation of graphs. *IEEE Transactions on Systems, Man, and Cybernetics*, 22(2):201–223, 1992.

[KGV83] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi. Optimization by simulated annealing. *Science*, 220(4598):671–680, 1983.

[KK01] M. Kuramochi and G. Karypis. Frequent subgraph discovery. In *Proc. 1st IEEE International Conference on Data Mining*, pages 313–320. IEEE Computer Society Press, 2001.

[KKL+00] Teuvo Kohonen, Samuel Kaski, Krista Lagus, Jarkko Salojarvi, Jukka Honkela, Vesa Paatero, and Antti Saarela. Self organization of a massive document collection. *IEEE Transactions on Neural Networks*, 11(3):574–585, 2000.

[Kle00] Jon M. Kleinberg. The small-world phenomenon: An algorithm perspective. In *Proc. 32nd Annual ACM Symposium on Theory of Computing*, pages 163–170. ACM Press, 2000.

[KLM96] Leslie Pack Kaelbling, Michael L. Littman, and Andrew P. Moore. Reinforcement learning: A survey. *Journal of Artificial Intelligence Research*, 4:237–285, 1996.

[KLR04] Keogh, Lonardi, and Ratanamahatana. Towards parameter-free data mining. In *Proc. 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 206–215. ACM Press, 2004.

[KMP77] Donald E. Knuth, James H. Morris, and Vaughan R. Pratt. Fast pattern matching in strings. *SIAM Journal on Computing*, 6(2):323–350, 1977.

[KMW06] Fabian Kuhn, Thomas Moscibroda, and Roger Wattenhofer. The price of being near-sighted. In *Proc. 17th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 980–989. ACM Press, 2006.

[KW05] Fabian Kuhn and Roger Wattenhofer. Constant-time distributed dominating set approximation. *Distributed Computing*, 17(4):303–310, 2005.

[Lib99] Leonid Libkin. Query languages with arithmetic and constraint databases. *SIGACT News*, 30(4):41–50, 1999.

[Lin92] Nathan Linial. Locality in distributed graph algorithms. *SIAM Journal on Computing*, 21(1):193–201, 1992.

[LS99] Daniel D. Lee and H. Sebastian Seung. Learning the parts of objects by non-negative matrix factorization. *Nature*, 401:788–791, 1999.

[LY94] Carsten Lund and Mihalis Yannakakis. On the hardness of approximating minimization problems. *Journal of the ACM*, 41(5):960–981, 1994.

[Lyn96] Nancy Lynch. *Distributed Algorithms*. Morgan Kaufmann, 1996.

[Man01] Giovanni Manzini. An analysis of the Burrows–Wheeler transform. *Journal of the ACM*, 48(3):407–430, 2001.

[MM93] Udi Manber and Eugene W. Myers. Suffix arrays: A new method for on-line string searches. *SIAM Journal on Computing*, 22(5):935–948, 1993.

[MR95] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[MT99] Dov Monderer and Moshe Tennenholtz. Distributed games: From mechanisms to protocols. In *Proc. 16th National Conference on Artificial Intelligence*, pages 32–37. AAAI Press, July 1999.

[Nis99] Noam Nisan. Algorithms for selfish agents. In *Proc. 16th Annual Symposium on Theoretical Aspects of Computer Science*, volume 1563 of *Lecture Notes in Computer Science*, pages 1–15. Springer-Verlag, 1999.

[NM04] Neill and Moore. Rapid detection of significant spatial clusters. In *Proc. 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 256–265. ACM Press, 2004.

[NM07] Gonzalo Navarro and Veli Mäkinen. Compressed full-text indexes. *ACM Computing Surveys*, 39(1):2, 2007.

[NS95] Moni Naor and Larry Stockmeyer. What can be computed locally? *SIAM Journal on Computing*, 24(6):1259–1277, 1995.

[ORSS06] Rafail Ostrovsky, Yuval Rabani, Leonard J. Schulman, and Chaitanya Swamy. The effectiveness of Lloyd-type methods for the k-means problem. In *Proc. 47th Annual IEEE Symposium on Foundations of Computer Science*, pages 165–176. IEEE, 2006.

[Pac08] Eli Packer. Iterated snap rounding with bounded drift. *Computational Geometry: Theory and Applications*, 40(3):231–251, 2008.

[Pap01] Christos H. Papadimitriou. Algorithms, games, and the Internet. In *Proc. 33rd Annual ACM Symposium on Theory of Computing*, pages 749–753. ACM Press, 2001.

[PR04] Toniann Pitassi and Ran Raz. Regular resolution lower bounds for the weak pigeonhole principle. *Combinatorica*, 24(3):503–524, 2004.

[PR07] Michal Parnas and Dana Ron. Approximating the minimum vertex cover in sublinear time and a connection to distributed algorithms. *Theoretical Computer Science*, 381(1–3):183–196, 2007.

[Pre93] Bart Preneel. *Analysis and Design of Cryptographic Hash Functions*. PhD thesis, Katholieke Universiteit Leuven, 1993.

[PY91] Christos H. Papadimitriou and Mihalis Yannakakis. On the value of information in distributed decision-making. In *Proc. 10th Annual ACM Symposium on Principles of Distributed Computing*, pages 61–64. ACM Press, 1991.

[PY93] Christos H. Papadimitriou and Mihalis Yannakakis. Linear programming without the matrix. In *Proc. 25th Annual ACM Symposium on Theory of Computing*, pages 121–129. ACM Press, 1993.

[Qui86] J. Ross Quinlan. Induction of decision trees. *Machine Learning*, 1(1):81–106, 1986.

[Rin99] Jussi Rintanen. Improvements to the evaluation of quantified boolean formulae. In *Proc. 16th International Joint Conference on Artificial Intelligence*, pages 1192–1197. Morgan Kaufmann, 1999.

[RR97] Alexander A. Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[RZ05] Gabriel Robins and Alexander Zelikovsky. Tighter bounds for graph Steiner tree approximation. *SIAM Journal on Discrete Mathematics*, 19(1):122–134, 2005.

[Sán02] V. David Sánchez. Frontiers of research in BSS/ICA. *Neurocomputing*, 49(1–4):7–23, 2002.

[Sch93] Marco Schneider. Self-stabilization. *ACM Computing Surveys*, 25(1):45–67, 1993.

[SH96] Richard Edwin Stearns and Harry B. Hunt. An algebraic model for combinatorial problems. *SIAM Journal on Computing*, 25(2):448–476, 1996.

[SP94] M. Srinivas and Lalit M. Patnaik. Genetic algorithms: a survey. *Computer*, 27(6):17–26, 1994.

[SS02] Bernhard Schölkopf and Alex J. Smola. A short introduction to learning with kernels. In Shahar Mendelson and Alex J. Smola, editors, *Advanced Lectures on Machine Learning, Machine Learning Summer School 2002*, volume 2600 of *Lecture Notes in Artificial Intelligence*, pages 41–64. Springer-Verlag, 2002.

[ST85] Daniel Dominic Sleator and Robert Endre Tarjan. Self-adjusting binary search trees. *Journal of the ACM*, 32(3):652–686, 1985.

[Sta03] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 3 edition, 2003.

[Ste03] Richard Edwin Stearns. Deterministic versus nondeterministic time and lower bound problems. *Journal of the ACM*, 50(1):91–95, 2003.

[Tar83] Robert Endre Tarjan. *Data Structures and Network Algorithms*. Society for Industrial and Applied Mathematics, 1983.

[Tes95] Gerald Tesauro. Temporal difference learning and TD-Gammon. *Communications of the ACM*, 38(3):58–68, 1995.

[Thr98] Sebastian Thrun. Learning metric-topological maps for indoor mobile robot navigation. *Artificial Intelligence*, 99(1):21–71, 1998.

[TvL84] Robert Endre Tarjan and Jan van Leeuwen. Worst-case analysis of set union algorithms. *Journal of the ACM*, 31(2):245–281, 1984.

[TWL05] Wade Trappe, Yuke Wang, and K. J. Ray Liu. Resource-aware conference key establishment for heterogeneous networks. *IEEE/ACM Transactions on Networking*, 13(1):134–146, 2005.

[Urr07] Jorge Urrutia. Local solutions for global problems in wireless networks. *Journal of Discrete Algorithms*, 5(3):395–407, 2007.

[Vaz03] Vijay V. Vazirani. *Approximation Algorithms*. Springer-Verlag, 2003.

[Wad00] Philip Wadler. Old ideas form the basis of advancements in functional programming, December 2000.

[WT89] Jeffery Westbrook and Robert Endre Tarjan. Amortized analysis of algorithms for set union with backtracking. *SIAM Journal on Computing*, 18(1):1–11, 1989.

[WY05] Xiaoyun Wang and Hongbo Yu. How to break MD5 and other hash functions. In *Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3494 of *Lecture Notes in Computer Science*, pages 19–35. Springer-Verlag, 2005.