Diskreetti matematiikka Tehtävä 10

Algoritmit

51.

Kauppamatkustajan ongelma: Myyntiedustaja halusi käydä kaikissa oheisen kuvion kaupungeissa käyttäen mahdollisimman lyhyttä reittiä. Myyntiedustajalla oli 2 kriteeriä reitin suhteen

a. Lähdetään ja palataan kaupunkiin A.
b. Jokaisessa kaupungissa käydään vain kerran.

Mitä reittiä kauppamatkustajan kannattaa kulkea? Kuinka pitkä tämä reitti on? Huomaathan myös, että ko. reitin voi kulkea myös toisinpäin, jolloin saadaan toinen yhtä hyvä ratkaisu.

Vastaus: A -> B -> C -> D -> A, pituus 128

52.

Kuinka monta erilaista reittiä edellisessä tehtävässä on? 24 a. Entä jos mukaan tulee viides kaupunki? : 120 b. Kuinka monta eri reittiä löytyy 10 kaupungin tapauksessa? : 3 628 800 c. Entä 20 kaupungin ongelmassa? : 2 432 902 008 176 640 000

53.

Tutustu Turingin koneeseen ja kuvaile lyhyesti, miten se toimii.

Turingin kone on abstrakti kone, joka on kehitetty matemaattisesti. Se on abstrakti, koska se ei ole fyysinen kone, vaan se on vain abstrakti malli koneesta. Se on kehitetty matemaattisesti, jotta voidaan määritellä, mitä tarkoittaa koneen toiminta. Turingin koneessa on tiettyjä tiloja, joissa kone voi olla. Koneessa on myös tiettyjä syötteitä, joita se voi lukea. Koneen tiloja ja syötteitä voidaan kutsua myös tiloiksi ja syötteiksi.

Se on myös yksi tietojenkäsittelytieteen peruskäsitteistä ja se on vaikuttanut merkittävästi tietokoneiden kehitykseen ja ohjelmistosuunnitteluun.

54.

Mitä tarkoitetaan äärellisellä automaatilla?

Äärellinen automaatti on matemaattinen malli, joka koostuu tiloista ja siirtymätoiminnoista. Se on yksi teoreettisen tietojenkäsittelyn peruskäsitteistä. Äärellinen automaatti voi olla joko deterministinen (DFA) tai epädeterministinen (NFA). DFA:ssa jokaisessa tilassa on tietty sääntö, joka määrittää, mitä tilaa seuraa, kun tietty merkki luetellaan. NFA:ssa sen sijaan yhdessä tilassa voi olla useita sääntöjä, jotka johtavat eri tiloihin saman merkin tapahtuessa. Äärellinen

automaatti voi käsitellä äärellistä syötettä ja tuottaa äärellisen määrän mahdollisia tulosteita tai tilanteita. Esimerkkejä sen sovelluksista ovat tietojenkäsittelyn ohjelmoinnin kielen analysointi ja automaattinen oikeinkirjoituksen tarkistus. Äärellinen automaatti on peruskäsite teoreettisessa tietojenkäsittelyssä ja sillä on merkittävä rooli esimerkiksi ohjelmistosuunnittelussa, kuten ohjelmistojen testauksessa ja kääntämisessä.

55.

Alan Turing (1912 - 1954) oli vuosisatamme suurimpia matemaatikkoja (ellei suurin). Toisen maailmansodan aikana hän osallistui Bletchley Parkissa 1 saksalaisten salauslaitteiden murtamiseen. Näistä laitteista tunnetuin lienee Enigma. Netistä löytyy erilaisia Enigma-simulaattoreita, esimerkiksi tämä.

a. Mainitse kaksi asiaa, mitkä helpottivat Enigman murtamista.

- Saksalaisten virheelliset käytännöt: Saksalaiset käyttivät Enigma-salauslaitettaan epävarmasti, mikä teki sen murtamisen helpommaksi. He esimerkiksi käyttivät samoja asetuksia useita kertoja, lähettivät toistuvia viestejä, eivätkä käyttäneet satunnaisia asetuksia. Nämä tekijät auttoivat Bletchley Parkin kryptografeja löytämään kaavoja ja toistoja salauksessa.
- Turingin kekseliäisyys: Alan Turingin johtama ryhmä kehitti menetelmiä, jotka auttoivat murtamaan Enigman salauksen. Turing esimerkiksi keksi käyttää mekaanista laitetta, joka tunnettiin nimellä "Bombe", joka pystyi löytämään Enigman salausavaimen. Turing myös kehitti ajatuksen "vastakoneesta", joka kykeni purkamaan saksalaisten käyttämiä monimutkaisia asetuksia ja yksinkertaistamaan salauksen purkamista. Turingin ajattelutapa ja kekseliäisyys auttoivat ratkaisevasti Enigman salauksen murtamisessa.

b. Mikä on Bombe?

- Bombe oli suunniteltu murtamaan natsien käyttämän Enigma-salauslaitteen salausavaimia. Bombe koostui useista pyörivistä levyistä, jotka sisälsivät piirilevyjä ja kytkentöjä, ja joka pyöri sähkömoottorin avulla. Laite käytti yleistä avainta ja koetti sen avulla löytää oikean salausavaimen Enigma-salauslaitteelle. Bombe toimi etsimällä yhteensattumia salauksen ja avaimen välillä, mikä auttoi murtamaan salauksen. Bombe oli erittäin tärkeä apuväline Enigma-salauslaitteen murtamisessa, ja sen avulla brittiläiset kryptoanalyytikot pystyivät lukemaan natsien viestejä ja saamaan tärkeää tiedustelutietoa toisessa maailmansodassa.

c. Enigman lisäksi Bletchley Parkissa murrettiin muitakin saksalaisten salauslaitteita. Mainitse yksi muu.

- Yksi Bletchley Parkissa murretuista saksalaisten salauslaitteista oli Lorenz-salauslaitteisto, jota käytettiin korkean tason sähkeviestinnässä natsien armeijan ja hallinnon välillä. Lorenz-salauslaitteisto oli monimutkaisempi ja

turvallisempi kuin Enigma, ja sen salauksen purkamiseen tarvittiin huomattavasti enemmän resursseja ja kekseliäisyyttä. Brittiläinen matemaatikko William Tutte kehitti menetelmiä, jotka auttoivat Lorenzin salauksen murtamisessa. Tutten kehittämät menetelmät ovat olleet tärkeitä myös modernin tietokoneiden teorian kehittämisessä.

Aman Mughal 28/03/2023