Alan Mathiason Turing

10. huhtikuuta 2002

Tietojenkäsittelytieteen Historia –seminaari

Kimmo Palin
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

1 Johdanto

Alan Turing oli tavallinen englantilainen homoseksuaali matemaatikko [4]. Tämä esitelmä käsittelee hänen elämäänsä ja monipuolista antiaan matemaattisten tieteiden historiassa.

Esitelmän rakenne on suurimmalta osaltaan kronologinen. Aluksi kerrotaan Alan Turingin lapsuudesta ja opiskelusta ja sen jälkeen hänen tieteellisistä töistään suurpiirteisen kronologisessa järjestyksessä. Viimeisissä kappaleissa palataan Alan Turingin yksityiselämään ja hänen ennenaikaiseen kuolemaansa.

Tässä esitelmässä on käytetty pääasiallisena lähteenä Andrew Hodges:in kirjoittamaa Alan Turingin elämänkertaa [4] sekä kirjaan liittyvää www–sivustoa [3]. Tieteellisiä tuloksia käsittelevissä luvuissa on käytetty myös alkuperäislähteitä ja erityisesti kalvoesityksen lisämateriaali on saatu Cambridgen King's Collegen Turing arkistosta [2].

Kannen kuva on Alan Turingin virallinen valokuva hänen päästessä Royal Societyn Fellowksi vuonna 1951. Kuvan oikeudet omistaa National Portrait Gallery. Alan Turing sai myös OBE (Officer of British Empire) arvon ansioistann toisen maailmansodan aikana.

2 Lapsuus

Alan Mathiason Turing syntyi Lontoossa, Englannissa, 23. kesäkuuta 1912. Hänen isänsä, Julius Turing (s. 1873), oli korkea virkamies Brittiläisen Intian siirtomaahallinnossa ja hänen äitinsä Ethel (o.s. Stoney) (s. 1881) oli varakkaasta Intiassa vaikuttavaa Brittisukua.

Alan ei itse käynyt milloinkaan Intiassa, vaikka hänen vanhempansa asuivat ja työskentelivät siellä. Alan jäi veljensä Johnin (s. 1908) kanssa vuoden vanhana hoitoon eversti ja rouva Wardille. Turingit kävivät Englannissa niin usein kuin isän lomat ja saksalaiset sukellusveneet (ensimmäisen maailman sodan aikana) sallivat. Tällainen menettely oli varsin tyypillistä Brittiläisen imperiumin virkailijoiden perheissä.

Alan opetteli itsenäisesti lukemaan ja laskemaan mutta hänen vuonna 1918 alkanutta koulu–uraansa varjosti pitkään erittäin huono käsiala ja huono menestys tuon ajan ylemmän keskiluokan sivistykseen kuuluvissa aineissa, kuten latinassa, ranskassa ja urheilussa. Vuonna 1922 Alan siirtyi päiväkoulusta Hazelhurstin sisäoppilaitokseen ja 1926 Hazelhurstista Sherbourneen.

Sisäoppilaitoksissa Alan kohtasi kouluaineisiin liittyvien ongelmien lisäksi ongelmia auktoriteettien kanssa. Alan ei koskaan hyväksynyt mitään perusteetonta valtaa, jollaiseksi hän katsoi asuntolavanhimmat, opettajat, valmentajat, kirkon ja vastaavat. Sherbornessa Alan tapasi ensimmäisen suuren rakkautensa Christopher Morcomin mutta ujo poika ei uskaltanut ajoissa puhua yhteisön halveksimista tunteistaan ja Christopherin kuolema vuonna 1930 jätti häneen suuren vaikutuksen.

3 Opiskelu

Vuonna 1930 Allan haki Cambridgen Trinity Collegeen (mm. Newton, Hawking, Babbage, Russell) mutta ei päässyt. Seuraavana vuonna Alanin kuitenkin pääsi lähes yhtä arvostettuun King's Collegeen (mm. Watson & Crick, Keynes) opiskelemaan matematiikkaa. Vaikka College muistuttikin suurta sisäoppilaitosta kello yhdentoista ulkonaliikkumiskieltoineen, Alan viihtyi siellä huomattavasti paremmin. Ei vähiten King's:in suhteellisen liberaalin ilmapiirin ansiosta.

Collegessa Alan osallistui myös urheiluun: hän souti ja myöhemmin juoksi. Hän jopa pyrki Lontoon olympialaisiin 1948 maratonille mutta loukkaantuminen esti nuo haaveet.. Alan valmistui King's:istä keväällä 1934 ja jatkoi tutkijaopiskelijana. Alan Turingista tuli King's Collegen Fellow vain 22 vuotiaana vuonna 1935 ja tässä virassa hän oli pienissä pätkissä toistakymmentä vuotta.

4 Turingin kone

Vuonna 1928 Kurt Gödel todisti kuuluisan epätäydellisyyslauseensa, että jokaisessa (riittävän laajassa) ensimmäisen kertaluvun loogisessa järjestelmässä on lauseita, joita ei voida todistaa todeksi eikä epätodeksi. Saksalainen matemaatikko David Hilbert esitti tämän epätäydellisyyslauseen kiertämiseksi toisen ongelman, niin sanotun päätäntäongelman (Entscheidungsproblem): "Onko olemassa mekaaninen menetelmä, jolla voidaan päättää onko ongelma todistettavissa vai ei?"

Varsinainen vaikeus päätäntäongelman ratkaisussa oli, että "mekaaninen menetelmä" ei ollut hyvin määritelty käsite. Varhaiskesällä 1935, makaillessaan kedolla Granchesterissa, Alan Turing keksi määritelmän "mekaaniselle menetelmälle": Turingin kone. Turingin koneilla ja erityisesti Universaalilla Turingin koneella Alan pystyi antamaan kielteisen vastauksen päätäntäongelmaan: Turingin koneen pysähtymisongelma voidaan kuvata ensimmäisen kertaluvun logiikassa ja pysähtymisongelmaa ei voida ratkaista Turingin koneella, joten päätäntäalgoritmia ei ole olemassa.

Turingin kone ja erityisesti päätösongelmaan vastaava universaali kone julkaistiin vuonna 1936 artikkelissa: "On Computable Numbers, with an application to the Entscheidungsproblem" [9]. Päätösongelman ratkaisu ei ollut edes julkaisuaikana artikkelin tärkein kontribuutio sillä Alonzo Church ja Emil Post olivat ennakoineet tuloksen, Post usealla vuodella. Artikkelin varsinainen saavutus oli itse Turingin kone, joka oli vuosikymmen myöhemmin teoreettisena, ja vähän käytännöllisenäkin, mallina elektronisille tietokoneille.

5 Kryptografia

Alan kiinnostui salakirjoituksesta ja mekaanisista laskimista 1930 luvun lopulla. Palattuaan vierailultaan Yhdysvalloista, Princeton Institute of Advanced Studiessta (Einstein, von Neumann, Church) vuonna 1938 hänet kutsuttiin osa–aikaiseksi Government Code and Cypher Schooliin (GCCS), jonka tehtävänä oli purkaa ja analysoida kaapattuja vieraiden valtioiden radioviestejä.

Vuonna 1938 GCCS:n suurin haaste oli saksalaisten Enigma salausjärjestelmä. Alkuperäinen Enigma, joka oli julkisesti esitelty jo vuonna 1923 Kansainvälisen postiliiton kokouksessa, oli yleisessä käytössä esimerkiksi pankeissa ympäri maailmaa. Alkuperäisestä Enigmasta oli vuosien saatossa tehty useita muunnelmia kuten Britannian asevoimien Typex ja Saksan asevoimien käyttämä Enigma.

Edes Saksan asevoimien kehittynyt Enigma järjestelmä ei ollut kovin moderni salausmenetelmä. Se yksinkertaisesti vaihtoi viestin kirjaimet pareittain toiseksi jaksollisen säännön mukaan. Tästä huolimatta briteillä ei ollut hajuakaan koodin murtamisesta ja Enigmaa pidettiin murtumattomana vielä kesällä 1939. Tämä muuttui vasta kun britit saivat liittosopimuksen yhteydessä apua Puolalaisilta. Puolalaiset olivat käyttäneet nerokasta algebraa, tilastotiedettä, arvauksia ja mekaniikkaa Enigman murtamisessa. Kuitenkin puolalaisten marraskuussa 1938 valmistuneet sähkömekaaniset Bombe koneet vanhenivat kuukaudessa saksalaisten muuttaessa Enigma koneiden käyttötapaa.

Juuri Enigman käyttötapa ratkaisi salauksen tehon. Huonosti valittu tapa lähettää osa viestistä kahteen kertaan auttoi merkittävästi englantilaisia murtamisessa tarpeellisen tilastoaineiston keräyksessä. Myös eri aselajien välillä oli eroja salauksen laadussa: Luftwaffe käytti Enigmaa varsin huolettomasti kun taas laivaston viestit olivat yleensä paremmin harkittuja ja siten vaikeammin murrettavia.

Alan Turing toimi Blechley Parkiin sodan ajaksi sijoitetussa GCCS:ssä majan 8, eli laivaston Enigman, päällikkönä. Vuonna 1940 GCCS:n menestykset rajoittuivat lähinnä Luftwaffen Enigmaan ja osittain Turingin suunnittelemiin [10] uusiin Bombe laitteisiin.

Keväällä 1941 majan 8 tilanne alkoi parantua. Huhtikuusta lähtien laivaston Enigmaviestejä luettiin säännöllisesti parin viikon viiveellä ja kesäkuusta, radiokuunteluaineiston ja sotasaaliina saadun tiedon lisääntyessä, saksan laivaston viestit luettiin käytännössä välittömästi. Tämä onnellinen tilanne kesti 1. helmikuuta 1942 asti, jolloin laivasto muutti sekä Enigman käyttötapoja että itse laitetta. Uusi Enigma joutui englantilaisten haltuun vasta U-559–sukellusveneen valtauksen yhteydessä 30. lokakuuta Port Saidissa, Egyptissä.

Alan Turingin osuus Enigman tarinassa loppui 7. marraskuuta 1942 kun hän lähti Yhdysvaltoihin pitämään yhteyttä sikäläisiin koodaajiin ja koodin murtajiin. Hänen paluunsa maaliskuussa 1943 osui sodan tuhoisimmalle sukellusvenekuukaudelle: Saksan Beobachter Dienst oli lähestynyt tehokkuudessaan Blechley Parkia. Onneksi Alania kuljettanut Empress of Scotland pääsi huomaamatta Englantiin ja Britannian laivasto sai pikaisesti muutettua salakirjoitusmenetelmiään.

Vuosien 1943–44 aikana Alan siirtyi vähitellen pois koodinmurtoprojekteista koodien suunnittelualalle Hanslopeen. Tuon ajan tulos oli puhetta salaava laite nimeltä Delilah. Laite oli teknisesti vuosikymmeniä aikaansa edellä mutta sodan kannalta auttamattomasti myöhässä. Delilah valmistui vasta sodan loppuessa ja Alan siirtyi

Saksaan suuntautuneen tiedustelumatkan [8] jälkeen siviiliprojekteihin.

6 Fyysinen tietokone

Heinäkuussa 1945 Alan Turingille tarjottiin työtä National Physical Laboratoryssa, jossa aiottiin rakentaa fyysinen universaali kone. Alanin virka alkoi virallisesti lokakuun 1. päivä mutta jo ennen sitä hän rupesi suunnittelemaan koneen toteutusta.

Tuohon aikaan tietokoneen rakentamisen suurin haaste oli muistin toteuttaminen. Elektroniputket olivat nopeita tallennusvälineitä mutta liian kalliita ja virhealttiita suuren muistikapasiteetin rakentamiseen. Saksalaisten uusi keksintö magnetofoni olisi vastannut hyvin universaalin Turingin koneen nauhaa mutta edestakainen kelaus olisi ollut liian hidasta. Harkittuaan monia tallennusmenetelmiä Alan päätti toteuttaa Automatic Computing Enginen (ACE) käyttämällä *akustisia viiveitä* [13]. Tiedon tallennus tapahtui lähettämällä äänisignaali elohopeaa sisältävään putkeen, jolloin tuo elohopeaputki "tallentaa" signaalin siksi aikaa kun ääni kulkee sen läpi.

Turing teki ACE koneesta useita varsin tarkkojakin suunnitelmia ja kirjoitti sille kohtalaisen ohjelmakirjaston. ACE projekti ei kuitenkaan edennyt läheskään niin nopeasti kuin Alan olisi halunnut. Blechleyssä hän oli saanut koko Britannian resurssit käyttöönsä yhdellä kirjeellä pääministerille mutta nyt pääministeri oli vaihtunut, sota loppunut ja valtion talous oli entistäkin huonommassa kunnossa.

Byrokraattiset ongelmat aiheuttivat ACE projektin vesittymisen "pilottikoneeksi" ja Alan menetti kiinnostuksensa NPL:ään. Lukuvuoden 1947–48 Alan oli sapattivapaalla vanhassa Cambridgessa King's:in fellown virassaan. Cambrigessa oli myös rakenteilla tietokone professori Wilkesin alaisuudessa mutta Alan hädin tuskin piipahti Cambridgen tietokonelaboratoriossa koko sapattivuotensa aikana [5]. Keväällä 1948 hän päätti olla palaamatta NPL:ään ja mennä Manchesteriin, jossa Britannian kolmas tietokoneprojekti oli kovassa vauhdissa.

Kesäkuun 21. päivänä 1948 Manchesterin koekone ajoi ensimmäisen ohjelmansa, brute-force algoritmin kokonaisluvun tekijöintiin. Se oli ensimmäinen toimiva, joskaan ei käytännöllinen, universaali tietokone maailmassa. Se voitti jopa Cambridgen EDSAC koneen, joka ajoi ensimmäisen ohjelmansa vasta 6. toukokuuta 1949.

Yksi Turingin tehtävistä Manchesterissa oli suunnitella seuraavasta koneesta (ensimmäinen kaupallinen tietokone Ferranti Mark I) helppokäyttöinen. Ilmeisesti helppokäyttöisyys merkitsi Alan Turingille eri asiaa kuin muille ihmisille, sillä kaikki ohjelmointi [12] Manchesterin tietokoneilla tapahtui 32–kantaisella lukujärjestelmällä, jossa eniten merkitsevä numero oli oikealla (Nykyään tämä merkintätyyliä kuvataan nimellä little-endian). Samaan aikaan Cambridgen tietokoneen käyttäjät kehittelivät jo ensimmäisiä ohjelmointikieliä.

Ajoittain Alan käytti Manchesterin koneita kuin PC:tä: kun ohjelma halusi lisää parametreja, se antoi äänimerkin koneen torvella ja käyttäjä katsoi katodisädeputkelta (joka varsinaisesti oli koneessa keskusmuistina) ohjelman tilan ja antoi tarvittavat parametrit. Koneen torvi teki siitä myös ensimmäisen multimediatietokoneen: se ohjelmoitiin soittamaan "God Save the Queen".

Alan toimi elämänsä loppuun asti Manchesterin tietokonelaboratorion esimiehenä mutta siirsi 1950 luvun alussa tehtävänsä alaisilleen ja oli harvoin henkilökohtaisesti paikalla. Hänen alaisensa eivät pitäneet tilannetta vättämättä huonona, sillä Alan tunnettiin vaikeana ihmisenä.

7 Turingin testi

Alan Turing mietti älykkäitä koneita jo ainakin sota–aikana Blechley Parkissa. Hänen suosikkiesimerkkinsä oli shakkia pelaava kone. Hän oli viehtynyt erityisesti ajatukseen, että kone oppisi jotain jota sille ei ole eksplisiittisesti kerrottu.

Kuuluisin tulos Alan Turingin mietteistä tekoälystä on Mind lehdessä vuonna 1950 julkaistu artikkeli "Computing Machinery and Intelligence" [11]. Tässä artikkelissa Turing ehdottaa peliä, jossa mies ja nainen komunikoivat kirjallisin viestein kuulustelijan kanssa. Kuulustelijan tehtävä on arvata kumpi henkilöistä on mies ja kumpi nainen. Mies yrittää saada kuulustelija erehtymään ja naisen on tarkoitus auttaa kuulustelijaa. Nyt jos mies korvattaisiin tietokoneella ja tulokset pysyisivät samanlaisina voidaan Turingin mukaan sanoa tietokoneen olevan älykäs.

Turing ennusti artikkelissaan myös tekoälyn tulevaa kehitystä:

> Uskon, että viidenkymmenen vuoden kuluttua voidaan ohjelmoida tietokoneita, joiden muistikapasiteetti on noin 10^9 (huom! noin 120MB) siten, että ne pelaavat matkimispelejä niin hyvin, että keskimääräisellä

kysyjällä on korkeintaan 70 prosentin mahdollisuus oikeaan tunnistukseen viiden minuutin kyselemisen jälkeen. Alkuperäinen kysymys "voivatko koneet ajatella?" on mielestäni niin merkityksetön, ettei siitä kannata edes keskustella. Silti uskon, että 1900–luvun lopussa sanojen käyttö ja yleinen oppinut mielipide on muuttunut niin paljon, että ajattelevista koneista voidaan puhua ristiriidoitta.

8 Turing bifurkaatio

Alan Turingin tietojenkäsitteliöille vähemmän tunnettu tieteellinen kontribuutio liittyi teoreettiseen, voisi sanoa jopa laskennalliseen, biologiaan. Alan oli aina ollut kiinnostunut luonnosta ja sodan aikana Joan Clarke oli herättänyt hänen kiinnostuksensa muun muassa Fibonaccin lukujen esiintymiseen luonnossa.

Turingin biologinen mielenkiinto keskittyi erityisesti morfogeneesiin: miten yhdestä symmetrisestä ja lähes tulkoon homogeenisestä solusta voi muodostua jakautumalla epäsymmetrisen muotoinen organismi. Toisin sanoen miten syntyvät seepran raidat. Vaikka samoihin aikoin King's Collegen tutkijat Watson ja Crick olivat paljastamassa DNA:n rakennetta, tämä kysymys (tai lähinnä vastaus) oli erittäin omaperäinen.

Alanin vastaus perustui solun kemiallisen rakenteen hiuksen hienoihin epäsymmetrioihin ja reaktio–diffuusio kaavoille [7]. Näitä kemiallisia differentiaaliyhtälöitä hän laski öisin Manchesterin tietokoneella. Nykyään Turingin artikkeliin "The Chemical Basis of Morphogenesis" on helppo löytää lähes sata viitettä [6]. Haut "Turing instability" ja "Turing bifurcation" tuottavat satoja sivuja Googlesta [1]. Alan Turingin työ teoreettisessa biologiassa katkesi kuitenkin lyhyeen.

9 Homoseksuaalisuus

Alan Turing oli homoseksuaali. Hän ei edes salannut suuntautumistaan erityisen aktiivisesti. Hän ei esimerkiksi mennyt naimisiin (vaikka olikin hetken kihloissa Joan Clarken kanssa vuonna 1941), kuten monet tuon ajan ja yhteiskuntaluokan homomiehet.

Suuria ongelmia hänen homoutensa tuotti alkuvuodesta 1952. Alan oli "pokannut" joulukuussa manchesterilaisen pikkurikollisen ja yhden heidän tapaamisensa jälkeen Alanin luona kävi murtovarkaita. Alan teki varkaista rikosilmoituksen ja poliisit kävivät paikalla tutkimassa ja ottamassa sormenjälkiä.

Alanin epäonneksi poliisi sai varkaan kiinni. Varas oli kuullut Alanista ja Alanin homoudesta Alanin kumppanilta. Jäätyään kiinni varas oli kertonut kaiken poliisille ja miehen homoseksuaalisuus oli tuohon aikaan Englannissa rikos. Maaliskuun 31. päivänä Alan sai tuomion: vuosi ehdollista vankeutta ja organoterapiaa, eli kemiallista kastraatiota.

Hormonihoidon, joka vei häneltä potenssin ja toi rinnat, lisäksi paljastuminen merkitsi turvallisuusluokituksen menettämistä. Valtio pelkäsi, että homoseksuaalisuus altistaa henkilön kiristykselle. Tämä pelko oli ainakin osittain aiheellinen: Alanin luona käynyt varas oli uskonut, ettei homo uskalla ottaa yhteyttä poliisiin.

Paljastumisen jälkeen Alan ei voinut enää toteuttaa itseään Britanniassa, joten hänen ulkomaanlomansa yleistyivät. Erityisesti hän oli kiinnostunut Norjasta, josta hän oli kuullut huhuja vain miehille tarkoitetuista tansseista. Vaikka tanssihuhut osoittautuivat vääriksi, hänen viimeisten vuosien tietokoneohjelmien nimissä esiintyi varsin usein norjalaisia miesten nimiä.

10 Loppu

Alan Turing löydettiin kuolleena kotoaan tiistaina kesäkuun 8. 1954. Hän oli ilmeisesti edellisenä iltana myrkyttänyt itsensä syanidilla. Kuolema luokiteltiin itsemurhaksi eikä missään virallisissa tai epävirallisissa kommenteissa esitetty yhteyksiä homoseksuaalisuusoikeudenkäyntiin tai valtiosalaisuuksiin. Hänen oikeudenkäynnistään oli jo aikaa yli kaksi vuotta ja organoterapiakin oli loppunut jo vuosi sitten. Hän ei jättänyt mitään jäähyväiskirjettä ja hänen teoreettista biologiaa käsittelevät tutkimuksensa jäivät kesken. Turingin äiti uskoi, että Alan oli saanut syanidia vahingossa suuhunsa työskennellessään kemikaaleilla.

Viitteet

[1] Google inc. `http://www.google.com/`.

[2] King's College Cambridge. Turing Digital Archive. `http://www.turingarchive.org/`.

[3] Andrew Hodges. Alan Turing kotisivut. `http://www.turing.org.uk/`.

[4] Andrew Hodges. *Alan Turing: The Enigma*. Walker And Company, New York, 1992. Ilmestyi suomeksi nimellä Alan Turing: Arvoitus, Terra Cognita, 2000.

[5] Karen Sparck Jones. A brief informal history of the computer laboratory, 1999.

[6] Steve Lawrence, C. Lee Giles, and Kurt Bollacker. Digital libraries and Autonomous Citation Indexing. *IEEE Computer*, 32(6):67–71, 1999. `http://www.researchindex.com/`.

[7] A. M. Turing. The Chemical Basis of Morphogenesis. *Phil. Trans. Roy. Soc. London*, B(237):37–72, 1952.

[8] Alan Mathiason Turing. Oletettavasti runsaasti tekstejä vuosilta 1940–1952 on vielä salaisia.

[9] Alan Mathiason Turing. On Computable Numbers, with an application to the Entscheidungsproblem. *Proceedings of London Mathematical Society*, 42(2):230–265, 1936. `http://www.abelard.org/turpap2/tp2-ie.asp`.

[10] Alan Mathiason Turing. NR 964 CBCB55 9024A 19390000 TURING'S TREATISE ON THE ENIGMA. Yhdysvaltain kansallinen turvallisuuspalvelu (NSA) kumosi salassapidon 6. Huhtikuuta 1996., 1940. `http://frode.home.cern.ch/frode/crypto/Turing/index.html`.

[11] Alan Mathiason Turing. Computing Machinery and Intelligence. *Mind*, LIX(236):433–, October 1950. `http://www.abelard.org/turpap/turpap.htm`.

[12] Alan Mathiason Turing. Programmers' Handbook for the Manchester electronic computer. Manchester University Computing Laboratory `http://www.ai.mit.edu/people/rst/turing/`, 1950.

[13] Alan Mathiason Turing. Lecture to the london mathematical society. In B. E. Carpenter and R. W. Doran, editors, *A. M. Turing's ACE Report of 1946 and Other Papers*, volume 10 of *the Charles Babbage Institute reprint series for the History of Computing*. MIT Press, University of Minnesota. Cambridge, MA, 1986.