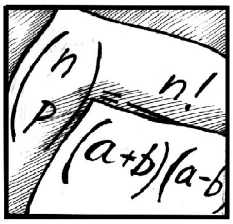

Kolikonheiton todennäköisyys

Jukka Liukkonen
Mat. yo. evp.

Todennäköisyyslaskennan oppikirjoissa kolikonheitto on vakioesimerkki. Symmetristä tai epäsymmetristä kolikkoa heitetään n kertaa ja kysytään, millä todennäköisyydellä saadaan tasan k kruunaa. Sen jälkeen aletaan puhua binomijakaumasta. Mutta onko kukaan heittänyt kolikkoa äärettömän monta kertaa? Onko kukaan toistanut tätä äärettömän pitkää heittosarjaa riittävän monta kertaa niin, että suurten lukujen lain vaikutus alkaisi näkyä, ja satunnaiskokeesta lasketut suhteelliset frekvenssit olisivat edes summittaisia approksimaatioita niille oikeille, pyhille todennäköisyyksille? Veikkaan, että vain harvalla kärsivällisyys riittää tällaisiin suorituksiin. Ensimmäisessä äärettömän pitkässä heittosarjassa ei luulisi olevan vaikeuksia. Olen itse suorittamassa sitä parhaillaan. Varmaan toinenkin sujuu vielä, mutta kolmas äärettömän pitkä kolikonheitto saattaa jo alkaa tuntua puuduttavalta. Sitäpaitsi: mitä ovat ne oikeat, pyhät todennäköisyydet päättymättömän kolikonheiton yhteydessä? Kirjoitelmassa pohjustetaan asian miettimistä. Tekstin ymmärtäminen valitettavasti edellyttää todennäköisyyslaskennan käsitteiden tuntemista lukion kurssin laajuudessa – tai avointa mieltä ja ahkeraa hakukoneella ajelua netissä. Älä ihmettele pientä mustaa kolmiota: se tarkoittaa, että esimerkki, sääntö tms. päättyy juuri sillä kohtaa.

Otosavaruus ja todennäköisyys

Yksinkertaisuuden vuoksi oletetaan, että heitetyt kolikot ovat symmetrisiä, eivät jää pystyyn, eikä varis kaappaa kolikkoa sen ilmalennon aikana. Silloin kruuna tulee todennäköisyydellä 1/2, ja samaten klaava. Eräs tärkeä oletus on, että eri heittokerroilla saadut tulokset ovat toisistaan riippumattomat. Tuntuu luonnolliselta, että riippumattomuusoletus pätee reaalimaailman kolikonheitossa – varmuuden vuoksi mainittakoon, että riittävällä tarkkuudella. Kolikonheittosarjat koodataan bittijonoiksi, joissa 1 edustaa kruunaa ja 0 klaavaa. Bitillä tarkoitetaan asiayhteydestä riippuen joko muuttujaa, jonka arvo voi olla 1 tai 0, tai tällaisen muuttujan arvoa. Päättymättömän kolikonheiton tulos näyttää tältä:

$$(1,0,0,1,0,0,1,0,1,1,1,0,1,0,0,\\ 0,0,1,0,1,0,1,1,1,0,1,1,0,0,\ldots),$$

yleisessä muodossa

$$a=(a_1,a_2,a_3,\ldots),\quad a_i\in\{0,1\}$$

kaikilla $i\in\mathbb{N}=\{1,2,3,\ldots\}$. Alkio a on **alkeistapaus**, ja yksiö $\{a\}$ on **alkeistapahtuma** kaikkien päättymättömien bittijonojen muodostamassa **perusjoukossa** eli **otosavaruudessa** Ω. Kun kolikkoa heitetään n kertaa, tietyn yksittäisen tulosjonon todennäköisyys on 2^{-n}. Heittokertojen lukumäärän n kasvaessa rajatta 2^{-n} lähestyy nollaa. On siis luontevaa sopia, että yhden alkeistapahtuman todennäköisyys päättymättömässä kolikonheitossa on nolla:

$$\mathbb{P}(a)=\mathbb{P}\big(\{a\}\big)=0\quad\text{kaikilla } a\in\Omega.$$

Silloin perusjoukon Ω jokaisen äärellisen tai numeroituvasti äärettömän osajoukon todennäköisyys on nolla. Tämä voidaan perustella todennäköisyyden aksioomilla (aksiooma Tn3), joista on perusteelliset esitykset Solmun numeroissa 1/2003 (T. Kaarakka) ja 2/2004 (T. Sottinen):

Tn1 $\mathbb{P}(A) \geq 0$ kaikilla tapahtumilla A.

Tn2 $\mathbb{P}(\Omega) = 1$.

Tn3 Jos $A_1, A_2, A_3, \ldots$ ovat tapahtumia ja $A_i \cap A_{i+j} = \emptyset$ kaikilla $i, j \in \mathbb{N}$, niin

$$\mathbb{P}\Big(\bigcup_{i=1}^{\infty} A_i\Big) = \sum_{i=1}^{\infty} \mathbb{P}(A_i).$$

On syytä palauttaa mieliin, että **tapahtuman** käsitteellä on todennäköisyyslaskennassa aivan erityinen merkitys. Yleisessä todennäköisyyden teoriassa kaikki perusjoukon osajoukot eivät välttämättä ole tapahtumia. Tapahtumiksi kutsutaan niitä osajoukkoja, joille voidaan määrittää todennäköisyys. Tapahtumien joukko on yhtä kuin todennäköisyysfunktion $\mathbb{P}$ määrittelyjoukko. Sitä merkitään usein symbolilla $\mathcal{F}$, ja sen alkiot ovat otosavaruuden osajoukkoja. Edellä esitetyn mukaisesti äärelliset ja numeroituvat kolikonheiton perusjoukon Ω osajoukot ovat tapahtumia, ja niiden todennäköisyys on nolla. Tämä ei ole ristiriidassa aksiooman Tn2 kanssa, sillä **Cantorin lävistäjämenetelmällä** (engl. *Cantor's diagonal argument*) nähdään, että päättymättömiä bittijonoja on ylinumeroituva määrä.[1]

Kun kolikkoa heitetään vain n kertaa, otosavaruutena on joukko Ω_n, joka koostuu kaikista bittijonoista $(a_1, \ldots, a_n)$. Näin yksinkertaisessa tilanteessa tapahtumia ovat kaikki joukon Ω_n osajoukot U. Tapahtuman U todennäköisyys on

$$\mathbb{P}_n(U) = \frac{|U|}{|\Omega_n|} = \frac{|U|}{2^n}.$$

Yleisen tavan mukaisesti joukon U alkioiden lukumäärää merkitään $|U|$. Vektorin itseisarvo ilmoittaa vektorin suuruuden, joukon "itseisarvo" ilmoittaa joukon suuruuden.

Eräs yksinkertainen tapahtumatyyppi päättymättömässä kolikonheitossa, äärellisten ja numeroituvien tapahtumien lisäksi, on muotoa

$$U^* = \big\{(a_1, \ldots, a_n, a_{n+1}, \ldots) \in \Omega \;\big|\; (a_1, \ldots, a_n) \in U\big\}$$

olevat tapahtumat, missä $n \in \mathbb{N}$ ja $U \subset \Omega_n$, toisin sanoen U on tuttuun n-kertaiseen kolikonheittoon liittyvä tapahtuma. Tapahtumaan U^* kuuluvat siis tasan ne päättymättömät bittijonot, joissa jonon alkupää $(a_1, \ldots, a_n)$ kuuluu tapahtumaan U, ja loppupää saa olla mitä tahansa, "häntä saa heilua vapaasti" kuin Mustin häntä. Tapahtuman U^* tapahtuminen tai tapahtumatta jääminen ratkeaa täysin jo n ensimmäisen heiton aikana, ja myöhempien heittojen tuloksilla ei ole väliä. Tapahtuman U^* todennäköisyydeksi asetetaan luonnollisesti $\mathbb{P}(U^*) = \mathbb{P}_n(U)$. Edistyneemmät todennäköisyyslaskijat samaistavat tapahtumat U ja U^*, mutta asioita ensi kertaa opiskellessa on ehkä hyvä korostaa niiden eroa.

Esimerkki

(a) Jos $U = \{\text{tulee kruuna}\} \subset \Omega_1$, on

$$\begin{aligned} U^* &= \{\text{ensimmäisellä heitolla tulee kruuna}\} \\ &= \big\{(a_1, a_2, a_3, \ldots) \in \Omega \;\big|\; a_1 = 1\big\}, \end{aligned}$$

ja $\mathbb{P}(U^*) = 1/2$.

(b) Jos $V = \{\text{kolmella heitolla tulee tasan 2 klaavaa}\} \subset \Omega_3$, on

$$\begin{aligned} V^* = \{&\text{kolmella ensimmäisellä heitolla tulee} \\ &\text{tasan 2 klaavaa}\} \\ = \big\{&(a_1, a_2, a_3, a_4, \ldots) \in \Omega \;\big|\; a_1 + a_2 + a_3 = 1\big\}, \end{aligned}$$

ja $\mathbb{P}(V^*) = 3/8$. ▲

Mitä muita tapahtumia on olemassa? Kuten jo todettiin, päättyvien heittosarjojen tapauksessa kaikki perusjoukon Ω_n osajoukot U ovat tapahtumia. Tästä ei sovi vetää hätäisiä johtopäätöksiä päättymättömille heittosarjoille. **Vitalin joukko** (engl. *Vitali set*) on tunnettu esimerkki ei-mitallisesta joukosta. Se on välin $[0, 1]$ osajoukko, jolla ei ole Lebesguen mittaa. Seuraavassa yritetään matkia Vitalin joukon yhteydessä normaalisti esitettyä päättelyä sen tutkimiseksi, ovatko päättymättömien heittosarjojen perusjoukon Ω kaikki osajoukot tapahtumia.

Bitit nurin

Olkoon A tapahtuma, jolloin $A \subset \Omega$, ja olkoon k positiivinen kokonaisluku. Jos jokaisen jonon $a \in A$ bitti a_k käännetään nurin, so. nolla korvataan ykkösellä ja ykkönen nollalla, saadaan tapahtuma A', jolla on sama todennäköisyys kuin A:lla, $\mathbb{P}(A) = \mathbb{P}(A')$. Asia voidaan ajatella niin, että jokaisen heittosarjan heitto numero k ja vain se tehdään sellaisella kolikolla, johon on tussilla piirretty kruunapuolelle klaava ja klaavapuolelle kruuna. Jos yhdessä satunnaiskokeessa tulokset tulkitaan kolikon alkuperäisten merkintöjen mukaan ja toisessa kokeessa tussimerkintöjen mukaan, niin ei kai se todennäköisyyksiin vaikuta, vai mitä. Monta bittiä voidaan kääntää nurin yksi kerrallaan. Jos ja kun jokaisessa vaiheessa todennäköisyys säilyy, saadaan seuraava sääntö:

[1] Kun ilman selostusta mainitsen nimeltä Cantorin menetelmän tai jonkin muun yleisesti tunnetun asian, oletan siitä kiinnostuneen lukijan katsovan taustat netistä. Tämän artikkelin lukemista voidaan huoletta jatkaa ilman tällaisten yksityiskohtien selvittämistäkin.

Sääntö

Olkoon $m \in \Omega$ bittijono, jossa on vain äärellinen määrä ykkösbittejä. Tällaista bittijonoa sanotaan **maskiksi**. Jos A' saadaan tapahtumasta A kääntämällä jokaisen alkeistapauksen $a \in A$ bitit nurin maskin m ykkösbittien ja vain niiden kohdalla, joukko A' on tapahtuma ja $\mathbb{P}(A') = \mathbb{P}(A)$. ▲

Esimerkki

Olkoon $U = \{(0,1,1,0),(1,1,0,1),(0,0,1,1)\} \subset \Omega_4$ ja $m = (0,1,0,1,1,0,0,0,\ldots) \in \Omega$. Maskin m bitit kuudennesta eteenpäin ovat nollia. Kun tapahtumalle $A = U^*$ tehdään maskin m mukainen bittien nurinkääntö, saadaan tapahtuma $A' = V^*$, missä $V = \{(0,0,1,1),(1,0,0,0),(0,1,1,0)\} \subset \Omega_4$. Mieti miksi. Huomaa, että maski käskee kääntämään nurin myös viidennen bitin, mutta joukon U jonoissa on vain neljä bittiä. Selvästi $\mathbb{P}(A) = 3/16 = \mathbb{P}(A')$. ▲

Päättymättömiä bittijonoja $a = (a_1, a_2, \ldots)$ ja $b = (b_1, b_2, \ldots)$ sanotaan **melkein samoiksi**, jos ne poikkeavat toisistaan vain äärellisen monen bitin kohdalla. Tällöin voidaan jopa kirjoittaa $a \approx b$. Samanlaista merkintäähän käytetään luvuillekin siinä tapauksessa, että ne ovat suunnilleen yhtäsuuria, esimerkiksi $\pi \approx 3{,}14$. Tässä on kuitenkin se oleellinen ero, että π ja $3{,}14 = 3{,}14000\ldots$ poikkeavat toisistaan äärettömän monen desimaalin osalta. Päättymättömien bittijonojen melkeinsamuus $\approx$ toteuttaa seuraavat ehdot ($a, b, c \in \Omega$):

E1 $a \approx a$.

E2 Jos $a \approx b$, niin $b \approx a$.

E3 Jos $a \approx b$ ja $b \approx c$, niin $a \approx c$.

Lukiossa on saatettu opettaa, että tällaiset ehdot toteuttavaa relaatiota sanotaan **ekvivalenssirelaatioksi**. Matematiikassa ja normaalielämässäkin ekvivalenssirelaatiot ovat erittäin yleisiä. Mieti ehtojen E1–E3 toteutumista vaikka sellaisessa tapauksessa, jossa $a \approx b$ tarkoittaa, että henkilöillä a ja b on samat vanhemmat. Henkilön a **ekvivalenssiluokka**

$$[a] = \{b \mid b \approx a\}$$

koostuu kaikista niistä henkilöistä, joilla on samat vanhemmat kuin henkilöllä a. Luokka $[a]$ on siis henkilön a koko (täys)sisarusparvi a itse mukaan lukien. On selvää, että joukkojen $[a]$ yhdiste kattaa kaikki ihmiset, ja ekvivalenssiluokille $[a]$ ja $[b]$ pätee aina joko $[a] = [b]$ tai $[a] \cap [b] = \emptyset$, muita vaihtoehtoja ei ole. Silloin ihmisten joukko voidaan esittää toisiaan leikkaamattomien sisarusparvien $[a]$ yhdisteenä. Tämä on ekvivalenssirelaatioiden ominaispiirre yleisestikin, eikä sitä ole kovin vaikeaa todistaa (voit kokeilla tai katsoa netistä).

Luokkayhteiskunnan ihmisvilinästä palataan takaisin rauhallisten bittijonojen pariin. Päättymättömien bittijonojen avaruus Ω voidaan, kuten tuli todettua, esittää toisiaan leikkaamattomien joukkojen $[r]$ yhdisteenä

$$\Omega = \bigcup_{r \in \Gamma} [r], \quad [r] = \{a \in \Omega \mid a \approx r\},$$

missä joukko $\Gamma \subset \Omega$ on muodostettu valitsemalla siihen tasan yksi edustaja jokaisesta ekvivalenssiluokasta. Äskeiseen havainnollistukseen liittyen voit ajatella vaikka, että edustaja r on sisarusparven $[r]$ vanhin, joka vastaa koko sisarusparven edesottamuksista. Äkkiä ajatellen tuntuu ilmiselvältä, että jokaisesta ekvivalenssiluokasta voidaan poimia yksikäsitteinen edustaja edustamaan koko luokkaa. Äärettömien joukkoperheiden yhteydessä edustajiston Γ olemassaolo on kuitenkin kaikkea muuta kuin itsestään selvä asia. Olemassaoloa ei pystytä todistamaan tavanomaisista joukko-opin aksioomista, ellei mukaan oteta ns. **valinta-aksioomaa** (engl. *axiom of choice, AC*). Siinä edustajisto yksinkertaisesti oletetaan olemassaolevaksi.

Jotain vialla?

Ennen loppurutistusta ja sitä seuraavaa hämmennystä muistutetaan, että nurinkäännettävät äärellisen monta bittiä ilmoitetaan maskin avulla. Maskissa on käännettävien bittien kohdalla ykkönen, ja muualla pelkkiä nollia. Kaikkien maskien joukkoa merkitään M. Se koostuu nollajonon lisäksi niistä bittijonoista, joissa on vain äärellisen monta ykköstä. Sellaiset voidaan samastaa positiivisten kokonaislukujen binääriesitysten kanssa (luettelemalla maskin kaikki bitit viimeisestä ykkösbitistä taaksepäin). Siis M on numeroituva joukko. Olkoot m ja m' kaksi maskia, $m \neq m'$. Olkoon $m\Gamma$ (vastaavasti $m'\Gamma$) niiden bittijonojen joukko, jotka on saatu edustajistoon Γ kuuluvista bittijonoista kääntämällä maskin m (vastaavasti m') ilmoittamat bitit nurin. Melko vähällä päänvaivaamisella havaitaan, että $m\Gamma \cap m'\Gamma = \emptyset$. Perustele tämä! Näin ollen kaikkien päättymättömien bittijonojen joukko, perusjoukko Ω, voidaan lausua toisiaan leikkaamattomien joukkojen $m\Gamma$ yhdisteenä

$$\Omega = \bigcup_{m \in M} m\Gamma.$$

Edustajisto Γ on otosavaruuden Ω osajoukko. Aikaisemmin perustellun säännön mukaan bitinkääntö ei vaikuta todennäköisyyksiin. Jos Γ on tapahtuma, mainitun säännön nojalla yhtälö $\mathbb{P}(m\Gamma) = \mathbb{P}(\Gamma)$ on voimassa kaikilla maskeilla m, jolloin aksiooman Tn3 perusteella

$$\mathbb{P}(\Omega) = \mathbb{P}\Big(\bigcup_{m \in M} m\Gamma\Big) = \sum_{m \in M} \mathbb{P}(m\Gamma) = \sum_{m \in M} \mathbb{P}(\Gamma)$$
$$= \mathbb{P}(\Gamma) + \mathbb{P}(\Gamma) + \mathbb{P}(\Gamma) + \ldots$$

Aksiooman Tn1 nojalla $\mathbb{P}(\Gamma) \geq 0$. Jos $\mathbb{P}(\Gamma) > 0$, viimeisin päättymätön summa on arvoltaan ääretön. Jos $\mathbb{P}(\Gamma) = 0$, päättymättömästä summasta tulee nolla. Aksiooman Tn2 mukaan $\mathbb{P}(\Omega) = 1$. Missä vika?

Loppuhämmennys

Johtopäätös kaikesta edellisestä on, että päättymättömän kolikonheiton tapauksessa todennäköisyysfunktiota $\mathbb{P}$ ei voida laajentaa kaikille perusjoukon osajoukoille ainakaan siten, että laajennos toteuttaisi luonnollisen vaatimuksen "nurinkääntöinvarianssista", siis yhtälön $\mathbb{P}(mA) = \mathbb{P}(A)$, $m \in M$, $A \subset \Omega$. Tässä mA tarkoittaa niiden bittijonojen joukkoa, jotka on saatu joukkoon A kuuluvista bittijonoista kääntämällä maskin m ilmoittamat bitit nurin. Kuten edellä nähtiin, otosavaruuden Ω osajoukon Γ olettaminen tapahtumaksi johtaa sovittamattomaan ristiriitaan. Edustajisto Γ ei sovellu tapahtumaksi, toisin sanoen otosavaruuden Ω osajoukolla Γ ei ole todennäköisyyttä. Kumma juttu! Kuitenkin Γ on aika iso joukko, sen kopioita tai paremminkin osittain nurinkäännettyjä peilikuvia $m\Gamma$ tarvitaan vain numeroituva määrä täyttämään koko perusjoukko. Tulosjono välttämättä osuu aina yhteen näistä kopioista. Jos tiettyyn kopioon tuleville osumille lasketaan suhteellista frekvenssiä, onko sillä suurten lukujen lain raja-arvon kaltaista rajaa toistojen määrän kasvaessa rajatta? Voidaanko yleensä testata, osuuko tulosjono kyseiseen kopioon? Joukkoa Γ ei missään vaiheessa konstruoitu, se vain oletettiin olemassaolevaksi valinta-aksioomaan vedoten!

Lukijan oman harrastuksen varaan jätetään sen selvittäminen, mitkä kaikki perusjoukon osajoukot lopulta ovat tapahtumia. Tosin se on aika turhaa, sillä kaikki vähänkin tavanomaiset joukko-opilliset konstruktiot ilman valinta-aksiooman käyttöä johtavat tapahtumiin. Käytännön todennäköisyyslaskuissa esiintyvillä bittijonojen otosavaruuden Ω osajoukoilla on aina todennäköisyys. Todennäköisyyslaskennan ja stokastisten prosessien yliopistokursseja suorittamaan aikovalle mainittakoon vihjeeksi, että päättyviin kolikonheittosarjoihin liittyvät **todennäköisyysavaruudet** (engl. *probability space*) voidaan laajentaa päättymättömien heittosarjojen avaruudeksi **Carathéodoryn laajennuslauseen** (engl. *Carathéodory's extension theorem*) avulla.

Harjoitustehtäviä

Kolikkoa heitetään äärettömän monta kertaa, ja heiton tulos koodataan loppumattomaksi bittijonoksi $a = (a_1, a_2, \ldots)$.

1) Millä todennäköisyydellä saadaan äärettömän monta kruunaa?

2) Millä todennäköisyydellä saadaan ainakin kerran miljoona kruunaa peräjälkeen?

3) Tietokoneohjelma on lopulta vain äärellinen bittijono. Ajattele jotain tiettyä tietokoneohjelmaa. Olkoon sen pituus n bittiä. Millä todennäköisyydellä kyseinen n bitin pätkä esiintyy ainakin kerran heittotuloksessa?

4) Millä todennäköisyydellä $\frac{1}{4} \leq \sum_{i=1}^{\infty} \frac{a_i}{2^i} < \frac{1}{2}$?

5) **Häntätapahtuma** on sellainen tapahtuma, jonka tapahtumiselle tai tapahtumatta jäämiselle on täysin yhdentekevää, mitä kolikonheiton alkupäässä tapahtuu, otettiinpa tuo (äärellinen) alkupää miten pitkäksi tahansa. On olemassa nk. **Kolmogorovin 0-1-laki** (engl. *Kolmogorov's zero-one law*), jonka mukaan häntätapahtuman todennäköisyys on aina joko 0 tai 1. Perustele, miksi

$$A = \{a \in \Omega \mid \text{on olemassa } \lim_{n\to\infty} a_n\}$$

on häntätapahtuma. Määritä $\mathbb{P}(A)$.

Jos et saa juonesta kiinni, katso Wikipediasta *infinite monkey theorem.*

Avoimia matematiikan oppikirjoja verkossa

Osoitteesta `http://avoinoppikirja.fi` löytyy avoimia yläkoulun ja lukion matematiikan oppikirjoja.