Tóth Bálint
A kártyakeverés matematikája

2006. május 23-ai előadása alapján írta
Lovász László, Nagy Gergely, Surányi László

Az előadás címéről

Tegyük fel, hogy négyen valamilyen kártyajátékot szeretnének játszani, például francia kártyával bridzselni. Nem a szabályok érdekelnek minket, összesen annyit kell tudnunk, hogy a bridzset az 52 kártyás, tehát egy pakli, joker nélküli francia kártyával játssza négy játékos, mindegyiküknek 13 lapot osztanak rögtön az elején. Minket most csak az a kérdés érdekel, hogy hogyan osszuk ki a lapokat úgy, hogy elég véletlenszerű legyen a leosztás. Nyilván nem felelne meg a célnak, ha egy frissen vásárolt kártyacsomagból egyből osztani kezdenénk (miután a jokereket kitettük), hiszen a boltban vásárolt pakli még „rendezett", a kártyák „sorban" jönnek: először a treffek, aztán a többi szín, ráadásul mindegyik szín sorba rendezve a kettestől az ászig. Előbb „jól meg kell kevernünk" a kártyát, például úgy, hogy ketté választjuk a kártyacsomagot és az egyik felét belekeverjük a másik felébe, majd ezt párszor megismételjük? De hányszor? Ha egyszer csináljuk, akkor nagy valószínűséggel többen is hosszú egyszínű sorokat fognak kapni, tehát korántsem lesz „véletlenszerű" a keverés. Viszont ha 15-ször megismételjük ezt a keverést, akkor már mindenki úgy fogja érezni, hogy elég véletlenszerű lesz a leosztás. A kérdés az, hogy ***hányszor*** kell a műveletet megismételnünk ahhoz, hogy az eredmény már „véletlenszerű" legyen.

Már a kérdés pontos feltevéséhez is szükség van fogalmak tisztázására. Miután a középiskolában csak nagyon érintőlegesen tananyag a véletlen matematikája, azaz a valószínűségszámítás, szükséges az alapfogalmaktól elindulnunk. Nem fogunk minden fogalmat pontosan definiálni, néha az intuícióra kell hagyatkoznunk, de a felépítésre mindenképp szükségünk lesz. Magának az előadásnak a témájához csak az előadásnak kb. a közepén fogunk eljutni, addigra lesz kezünkben minden fogalom, hogy pontosan feltehessük kérdéseinket.

Kezdjük tehát az alapfogalmaknál. Látszólag elkanyarodunk és nem a ***véletlen***, hanem a ***valószínűség*** definiálásával kezdjük. Ez azonban általános eljárás a matematikában, sőt a természettudományban: a valószínűség a véletlen ***mérőszáma***, vagyis megmondja, hogy egy esemény mennyire „véletlen". (Gondoljuk meg: a legtöbb fizikai fogalomnál sem azt mondjuk meg, hogy mi az, hanem azt adjuk meg, hogy hogyan mérjük az illető mennyiséget.) De az épp most mondottakból az is világos, hogy a valószínűség definiálásához szükséges azt is megmondanunk, hogy mi az esemény. És miután az egyes események valószínűségét egymáshoz viszonyítva tudjuk mérni, meg kell adni az „eseménytért" is, tehát az összes olyan eseményt, amit egymáshoz képest mérni akarunk. De – legalábbis abban az esetben, ha véges sok lehetséges esemény van – nyilván vannak összetettebb és tovább nem bontható ***elemi események***. A kártyakeverés esetében ezek az 52 kártya lehetséges sorrendjei (a kiosztás előtt) – és a megfigyelés összes lehetséges eredménye, tehát a kísérlet összes lehetséges kimenetele alkotja az ***eseménytért***. Általában a definíció a következő:

A valószínűség definíciója

Ω egy véges vagy megszámlálhatóan végtelen halmaz, amelynek elemei a kísérlet egyes kimenetelei. Az Ω halmazt **eseménytér**nek, az Ω elemeit **elemi esemény**eknek nevezzük. Az $\omega \in \Omega$ elemi esemény valószínűsége egy 0 és 1 közötti $p(\omega)$ szám. A p függvény értékeinek összege 1, ha minden elemen végigmegyünk:

$$\sum_{\omega \in \Omega} p(\omega) = 1,$$

azaz a biztos esemény valószínűsége 1. **Esemény**nek (E) az eseménytér tetszőleges részhalmazát nevezzük, az esemény **valószínűsége (*P(E)*)** az eseményt alkotó elemi események valószínűségeinek összege:

$$P(E) = \sum_{\omega \in E} p(\omega).$$

Tehát egyrészt a biztos esemény valószínűségét egynek vesszük, ezzel „normáljuk” a valószínűségeket. Minden egyes (tovább nem bontható) elemi eseménynek adunk egy pozitív „súlyt” – hogy hogyan, minek az alapján, ezt minden esetben el kell előbb döntenünk –, és ez lesz az egyes elemi események valószínűsége. Egy összetett esemény valószínűségét ezek után úgy állapítjuk meg, hogy megnézzük: milyen elemi eseményekből tevődik össze és ezek súlyát összeadjuk.

Például a bridzs esetében, ahol az elemi események a pakli egyes sorrendjei, semelyik sorrendet nem tüntetjük ki, minden sorrendet ugyanolyan súllyal látunk el. (Ez látszólag ellentmond annak, hogy „kezdetben” a kártyacsomag rendezett, de éppen egy olyan állapothoz akarunk eljutni, amikor semmit nem tudhatunk a sorrendről, tehát minden sorrend egyformán valószínű.) Miután 52! a lehetséges sorrendek száma, az egyes elemi események – sorrendek – valószínűsége egyformán 1/52! Most megkérdezhetjük, hogy a négy játékos közül – ezeket szokás a négy égtájjal Északnak, Délnek, Nyugatnak és Keletnek nevezni – az egyik, pl. Nyugatnak milyen valószínűséggel lesz három ász a. Ehhez annyit kell tennünk, hogy meg kell számolnunk azokat a sorrendeket, amelyekben Nyugatnak három ász jut. (Persze ehhez tudnunk kell, hogy a sorrendben hanyadik lapokat kapja ő, de ez ismert.)

A definícióból következik pár alapvető tétel:

Valószínűségszámítási alaptétel

Páronként egymást kizáró események uniójának valószínűsége az egyes események valószínűségének összege. Azaz, ha minden $i \neq j$-re $A_i \cap A_j = \emptyset$, akkor

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i).$$

Ez világos, hiszen az unió-esemény valószínűségét úgy kapjuk, hogy a hozzá tartozó összes elemi esemény valószínűségét összeadjuk, ezt az összegzést pedig elvégezhetjük úgy is, hogy az egyes A_i halmazbeli elemi eseményeket összeadjuk, és az így kapott eredményeket összeadjuk, hiszen egyetlen elemi eseményt sem fogunk kétszer számba venni.

Bemelegítésül nézzünk egy elég ismert példát:

1. feladat

Mennyi annak a valószínűsége, hogy egy 23 tagú társaságban semelyik két embernek sem esik ugyanarra a napra a születésnapja?

Az 1. feladat megoldása

Ebben az esetben a „kísérlet” egy 23 emberből álló minta választása. A kísérlet kimenetele az év napjaiból álló 23 elemű sorozat. Az eseménytér az összes ilyen sorozat halmaza. Ha a napokat az 1, 2, 3, ..., 365 számokkal jelöljük (az egyszerűség kedvéért elfeledkezve a szökőévekről), akkor ezt így is írhatjuk:

$$\Omega = \{1, 2, 3, ..., 365\}^{23}.$$

Egy elemi esemény egy konkrét sorozat:

$$\omega = (x_1, x_2, ..., x_{23}),$$

ahol x_i jelöli, hogy az i-edik ember az év melyik napján született.

Azok az ω-k a „jók”, amelyekben különböző emberek, az év különböző napján születtek.

$$E = \{\omega | i \neq j \Rightarrow x_i \neq x_j\}.$$

A valóságot jól közelítjük, hogy ha azzal a p függvénnyel dolgozunk, amely minden elemi eseményhez ugyanazt a számot rendeli (**kombinatorikus valószínűség**), így bármely esemény valószínűsége a jó esetek számának és az összes eset számának hányadosa lesz. Most ez

$$P(E) = \frac{365 \cdot 364 \cdot ... \cdot 343}{365^{23}} = \prod_{i=0}^{22} \left(1 - \frac{i}{365}\right).$$

A kérdés az, hogy vajon ez a valószínűség „nagy” lesz-e, pl. ¾-nél nagyobb, vagy „kicsi” lesz-e, tehát pl. ¼-nél kisebb. Aki nem ismeri még a feladatot, annak érdemes kiszámolnia ezt a szorzatot, elég meglepő eredményt kap.

Természetesen általában, n tagú társaságra is megoldható a feladat, ekkor a megoldás:

$$P(E) = \frac{365 \cdot 364 \cdot ... \cdot (366 - n)}{365^n}.$$

Ez a valószínűség n=366-tól kezdve nulla, ami az egyszerű skatulyaelvből is nyilvánvaló: 366 ember között biztos van kettő, aki azonos napon született (feltéve, hogy senki nem született február 29-én).

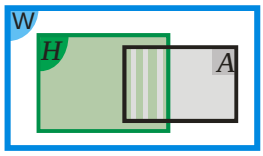
A következő fogalom a *feltételes valószínűség* fogalma. Ez elég egyszerű fogalom, de enélkül nem tudjuk értelmezni sem az előadás címében jelzett kérdést, sem számtalan lényeges más kérdést. Ismét a fenti bridzs-példát használva ismét azt kérdezzük, hogy milyen valószínűséggel fog Nyugat három ászt kapni? Említettük, hogy ezt hogy kell kiszámolni: megszámoljuk, hogy hány olyan sorrend van, amelyben Nyugatnak három ásza van, s ezek számát elosztjuk az összes lehetséges eset számával, 52!-sal.

De tegyük fel, hogy a lapok kiosztása után, még mielőtt Nyugat megnézné a lapját, pl. Észak megsúgja neki, hogy nála pontosan egy ász van. Most nyilván megváltozik annak az esélye, hogy nála három ász lesz. (Nem beszélve arról az esetről, ha azt tudja meg, hogy Északnál két ász van: ekkor nullára csökken annak a valószínűsége, hogy nála három ász legyen.) Mi történt? Nyugat nem kapott ugyan teljes felvilágosítást a kérdésére, de megtudott valami részinformációt, s ez módosítja az esélyeit. Általában is ez a helyzet: egy A esemény valószínűségét szeretnénk megtudni, ha valami H feltételt tudunk, ami ugyan nem ad teljes felvilágosítást. (Persze az információ ad*hat* teljes felvilágosítást, de lehet teljesen irreleváns is az információ. A példánknál maradva: ha Északnál két ász van, ez már a kérdésünk szempontjából teljes felvilágosítást ad, biztosan tudni fogjuk, hogy Nyugatnál nem lehet, azaz nulla valószínűséggel lehet három ász. Másrészt meggondolható, hogy ha például Nyugat azt árulja el, hogy nála van treff, ezzel a kérdésünk vonatkozásában semmit nem árult el.)

Vegyük tehát azt az esetet, amikor az $A \subset \Omega$ esemény valószínűsége érdekel minket, de tudjuk (vagy feltételezzük), hogy a H esemény bekövetkezett. Ennek az információnak (vagy feltevésnek) a figyelembevételével máshogy kell számolnunk a valószínűséget. Erre vonatkozik az alábbi jelölés és képlet.

Feltételes valószínűség

Az A esemény H eseményre vonatkozó feltételes valószínűsége: $P(A \mid H) = \dfrac{P(A \cap H)}{P(H)}$.



1. ábra

Az 1. ábrán szemléltetjük, hogy miről van szó. Kékkel jelöltük a teljes eseménytért, tehát az Ω halmazt. Zölddel jelöljük a H eseményhez tartozó elemi események „terét”, tehát azt a részt, amire figyelmünket fordítjuk, miután feltesszük (vagy megtudjuk), hogy H igaz. A kérdés most az, hogy ezen a részen milyen valószínűséggel következik be (a feketével jelölt) A. Ehhez nyilván tudnunk kell, hogy milyen valószínűséggel következik be az $A \cap H$ esemény, és ezt kell a H esemény bekövetkezésének valószínűségéhez viszonyítanunk, hiszen most ez a „az eseménytér”, ennek kell 1 valószínűséggel bekövetkeznie.

A feltételes valószínűséget időnként egy esemény feltétel nélküli valószínűségének kiszámítására alkalmazzuk valamely teljes eseményrendszer segítségével.

Teljes eseményrendszer
Azt mondjuk, hogy a H_1, H_2, ..., H_n események teljes eseményrendszert alkotnak, ha minden elemi esemény pontosan az egyiküknek eleme. Másképp: a H_i események páronként diszjunktak és uniójuk a biztos esemény.

A teljes valószínűség tétele
Ha A tetszőleges esemény és H_1, H_2, ..., H_n teljes eseményrendszer, akkor

$$P(A) = \sum_{i=1}^{n} P(A \mid H_i) \times P(H_i).$$

Ez az állítás csak kinézetre bonyolult: az összeadandók előző definíciónk alapján éppen az egyes $A \cap H_i$ események bekövetkezésének a $P(A \cap H_i)$ valószínűségével egyenlők, s ezek páronként diszjunkt események, együtt tehát épp az A valószínűségét adják.

Szükségünk lesz még az úgynevezett „toronyszabályra”. Ez időben egymás után következő eseményekkel foglalkozik. Hogy rögtön példát is mondjunk:

2. feladat Tegyük fel, hogy van két urnánk, az egyikben öt kék és három piros golyó van, a másikban négy kék és nyolc piros golyó. A következőt csináljuk: először az elsőből találomra kiveszünk egy golyót és átrakjuk a másodikba. Ezután az ott levő immár 13 golyót egy fakanállal jól összekeverjük és kihúzunk találomra egy golyót és átrakjuk az elsőbe. Most azt is megkeverjük a fakanállal és találomra húzunk az ott levő nyolc golyóból egyet. Mondjuk itt megállunk és azt kérdezzük, hogy mi a valószínűsége annak, hogy egymás után rendre egy piros, egy kék, majd ismét egy kék golyót húztunk.

Ezt nyilván úgy számoljuk ki, hogy először kiszámoljuk annak a valószínűségét, hogy az elsőből pirosat húzunk (3/8). Ezután kiszámoljuk annak a valószínűségét, hogy a másodikból kéket húzunk, de tudva azt, hogy oda egy pirosat raktunk, tehát tudva, hogy az első húzás piros volt (tehát hogy most a második urnában négy kék és kilenc piros golyó van). Ez a feltételes valószínűség P(második húzás kék|első húzás piros) = 4/13. Ezután kiszámoljuk, hogy mennyi annak a valószínűsége, hogy az első urnából ismét kéket húzunk, tudva, hogy onnan először kéket húztunk, tehát hogy négy kék és három piros maradt benne, továbbá tudva, hogy másodszorra pirosat húztunk (tehát hogy most pirosat teszünk vissza, azaz négy kék és négy piros van az elsőben). Ez a feltételes valószínűség P(harmadik húzás piros|első húzás piros és második húzás kék)=1/2. A keresett valószínűség e három valószínűség szorzata lesz:

P(sorra pirosat, kéket, pirosat húzunk) =
= P(1. húzás piros) ×P(2. húzás kék|1. húzás piros) ×P(3. húzás piros|1. húzás piros és 2. húzás kék).

Ennek alapján érthető az úgynevezett

toronyszabály:

$$P\left(\bigcap_{i=1}^{n} A_i\right) = P(A_1)\times P\left(A_2 \middle| A_1\right)\times P\left(A_3 \middle| A_2 \cap A_1\right)\times \ldots \times P\left(A_n \middle| \bigcap_{i=1}^{n-1} A_i\right)$$

A toronyszabály tehát azt mondja ki, adja meg, hogy hogyan számolható ki annak a valószínűsége, hogy egymás után az A_1, A_2, …, A_n események következnek be. Kiszámoljuk, hogy az i-edik esemény milyen valószínűséggel következik be, feltéve hogy előtte az A_1, A_2,…,A_{i-1} események következtek be, majd ezeket a feltételes valószínűségeket összeszorozzuk.

A következő fogalom az események függetlensége.

Függetlenség, naív definíció

Eseményeket akkor nevezünk egymástól függetlennek, ha hiába van információnk néhánynak a bekövetkezéséről vagy be nem következéséről, ettől a többi esemény bekövetkezésének vagy be nem következésének esélyéről nem tudunk többet, tehát ezek valószínűsége nem változik.

Két esemény esetén ez azt jelenti, hogy az A esemény valószínűsége nem változik, ha tudjuk, hogy B bekövetkezik, azaz $P(A) = P(A|B)$. Ez a definíció formálisan nem szimmetrikus. Vagyis: mi két esemény függetlenségéről beszéltünk, de itt csak azt mondtuk meg, hogy A mikor független B-től. Ám ha ide beírjuk a feltételes valószínűség fenti definícióját és átszorzunk a nevezővel, akkor azt kapjuk, hogy $P(A\cap B)=P(A)P(B)$. Szavakban ez azt jelenti, hogy a két esemény együttes bekövetkezésének valószínűsége megegyezik a két esemény valószínűségének szorzatával. Ebből viszont következik, hogy ha A független B-től, akkor B is független A-tól, tehát valóban beszélhetünk a két esemény egymástól való függetlenségéről.

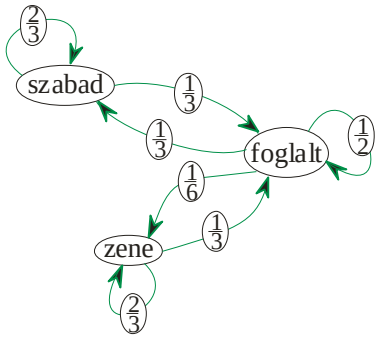
Több esemény függetlenségével kapcsolatban azonban fontos eloszlatni egy tévedést: ehhez nem elég, hogy bármely két esemény független legyen. Mondok egy példát rögtön, amit egy életre meg kell jegyezni, hogy ne kövessük el az említett a hibát, amit még könyvben is láttam elkövetni. Tehát tegyük fel, hogy két kockával dobunk, az egyik zöld, a másik piros. Az A esemény legyen az, hogy a zöld kockán párosat dobunk, a B esemény az, hogy a piros kockán párosat dobunk, a C pedig az, hogy a két dobott szám összege páros. Mármost nyilvánvaló, hogy mindhárom esemény 1/2 valószínűséggel következik be, bármely kettő pedig független, mert együttes bekövetkezésük valószínűsége ¼. Ám a három esemény egyáltalán nem független egymástól, mert ha bármely kettő bekövetkezéséről van információnk, abból el tudjuk dönteni, hogy a harmadik bekövetkezik-e. Ha például A is, B is bekövetkezik, akkor C is biztosan bekövetkezik, ha egyik sem következik be, C akkor is biztos, stb. Tehát

Függetlenség, matematikai definíció

N eseményt akkor nevezünk függetlennek, ha bárhogy választunk közülük néhányat, azok együttes bekövetkezésének valószínűsége a külön-külön bekövetkezésük valószínűségének szorzata.
Képlettel kifejezve:

Minden $1\le i_1<i_2<\ldots<i_k\le n$-re teljesül, hogy $P\left(\bigcap_{j=1}^{k} A_{i_j}\right) = \prod_{j=1}^{k} P(A_{i_j})$.

Ezután már rátérhetünk a *Markov-láncokra*, ezek lesznek segítségünkre eredeti, kártyakeverési problémánk megválaszolásában. Valami véletlen mozgásáról van szó, amely véges – vagy néhány később sorra kerülő példában megszámlálhatóan sok, de mindenképp diszkrét – állapotban lehet. Diszkrét időegységenként változtatja állapotát. Az állapotok véges vagy megszámlálhatóan végtelen halmazát S-sel jelöljük. A később terítékre kerülő 2. példa állapotainak rendszere látható a 2. ábrán.



2. ábra
A 2. példa állapotai és az átmeneti valószínűségek $\left(p=\frac{1}{2},\ q=\frac{1}{3}\right)$

Az egyes pontok az állapotokat (megengedett állapotokat) jelölik, a zöld nyílak azt mutatják, hogy melyik állapotból melyikbe mehet át (közvetlenül, tehát egy időegység múltán) a véletlen mozgás. Ezekre rá van írva egy-egy pozitív szám, az a állapotból a b állapotba mutató nyíl jelöli, hogy a mozgás milyen valószínűséggel fog az a állapotból a b állapotba átmenni (egy időegység múltán). Ezt a mennyiséget p_{ab}-val jelöljük. Ez az átmeneti valószínűség. Tehát itt nem-determinisztikus mozgásról van szó, mintegy sorshúzás dönti el, hogy egy adott állapotból hogyan megy tovább a mozgás (vagy folyamat). Ha például veszünk a boltban egy pakli kártyát, akkor a kiinduló állapot még nagyon rendezett, mint mondtuk. A következő (egy keverési művelet utáni) állapot már nem eldönthető (nem determinált) és aránylag rendezetlenebb, véletlenszerűbb lesz. Éppen azt kérdezzük, hogy hány lépés (azaz: hány keverési művelet) után lesz már „tényleg véletlen” a sorrend.

Mármost ilyen véletlen mozgás még nagyon sokféle van és nagyon bonyolult a kezelésük is. A p_{ab} átmeneti valószínűség általában sok mindentől függ, például az összes azt megelőző állapottól. Ez nagyon bonyolulttá teszi az általános esetet. A Markov-láncok esetében azonban van egy lényeges egyszerűsítés, nevezetesen feltesszük, hogy a p_{ab} valószínűség csak a pillanatnyi állapottól függ, a korábbiaktól nem! Feltesszük tehát, hogy a mozgásnak ilyen értelemben nincs memóriája, tehát az, hogy mi fog történni, csak a pillanatnyi állapottól függ, teljesen mindegy, hogy a folyamat hogyan jutott ebbe az állapotba. Ez nagyon erős feltétel, mégis természetes, és jól alkalmazható sok esetben, például a kártyakeverésnél, de a genetikában is. Képletben ez azt jelenti, hogy $p_{ab}=P(b|a)$ és ez a b állapot csakis a pillanatnyi állapotot jelöli. Analógia lehet a fizikai differenciálegyenletek példája, ahol csak egy pillanatnyi állapottól (pl. a rendszerben levő részecskék pillanatnyi helyzetétől és sebességétől) függ, hogy utána mi fog történni – de csak analógia, hiszen ott determinisztikus folyamattal van dolgunk!

Jelöljük *S*-sel a Markov-lánc lehetséges állapotainak halmazát és tegyük fel, hogy *S* alemainek száma *n*. A Markov-lánchoz tartozik tehát egy $n\acute{}\,n$-es négyzetes mátrix (a mátrixokról lásd a KöMaL 2006. májusában megjelent cikket Hermann Pétertől – sajnos egyelőre nem érhető el a neten –). Ennek a mátrixnak például a második sor és ötödik oszlop metszéspontjában álló eleme azt adja meg, hogy milyen valószínűséggel jut a mozgás a második állapotból az ötödikbe. Nyilvánvaló, hogy egy ilyen mátrix minden eleme egy-egy nemnegatív szám, s az egy sorban álló számok összege egy. Hiszen egy adott állapotból csak a véges sok adott állapot egyikébe kerülhet a mozgás és ezek az állapotok páronként kizárják egymást. Tehát a fent mondott értelemben teljes eseményrendszert alkotnak.

Markov-mátrix
Ha egy négyzetes mátrix teljesíti a mondott feltételt (csupa nem negatív elem és minden sorösszeg egy), akkor **Markov-mátrix**nak, **sztochasztikus mátrix**nak nevezzük.
Képlettel kifejezve olyan *nxn*-as (négyzetes) mátrixról van szó, amelynek minden elemére $0 \le p_{ab} \le 1$ és

$$\sum_{b=1}^{n} p_{ab} = 1.$$

A továbbiakban csak olyan Markov-láncokkal foglalkozunk, amelyekre teljesül a következő feltétel. Tekintsük azt az irányított gráfot, amelyet úgy kapunk, hogy a nem-nulla elemeket irányított élként behúzzuk, azaz ha p_{ab} nem nulla, akkor a-ból b-be húzunk egy irányított élt. Erről a gráfról feltesszük, hogy bármelyik pontjából bármelyik pontjába eljuthatunk irányított út mentén. Ilyen esetben a Markov-láncot **irreducibilisnek** nevezzük.

Ez utóbbi feltevés azt jelenti, hogy a gráf „nem esik szét”, sem az nem történik meg, hogy ha eljutunk egy részébe, onnan nem tudunk visszajutni egy másik részébe. Ez a kikötés nem nagyon szorítja meg a vizsgálódásainkat. Ha ugyanis egy Markov-láncra nem teljesül, nem nehéz belőle egy másikat csinálni, ami ugyanúgy megfelel céljainknak, de teljesül rá az irreducibilitás feltétele.

A legtöbb esetben még egy megkötéssel élünk (bár látni fogunk olyan példát is, ahol ez nem teljesül): feltesszük, hogy nincs benne periódus. Ez a következőt jelenti: a gráf egy tetszőleges pontjából kiinduló körök hosszának legnagyobb közös osztója egy. Ez egy páros gráfra például nem teljesül, hiszen ott egy tetszőleges adott állapotból csak minden párosadik lépésben juthatunk vissza ugyanabba az állapotba. Páros gráfban minden kör hossza páros, tehát a hosszak legnagyobb közös osztója is legalább kettő. Ezt, mint mondtam, a legtöbb esetben kizárjuk.

Ha egy véletlen folyamatban adott egy rögzített, most tehát határozott, determinisztikus, nem véletlen útvonal, és azt kérdezzük, hogy mi ennek *trajektóriának* a valószínűsége, akkor ezt általában a toronyszabállyal számíthatjuk ki. Ez tehát így szólt: Ha adva van egy $\alpha_0, \alpha_1, \ldots, \alpha_n$ rögzített útvonal, akkor annak a valószínűsége, hogy az $X_0, X_1, \ldots, X_n$ útvonal ezzel megegyezik a torony-szabály szerint:

$$P\left(\bigcap_{i=1}^{n} A_i\right) = P(X_1 = a_1) \times P\left(X_2 = a_2 \middle| X_1 = a_1\right) \times P\left(X_3 = a_3 \middle| X_2 = a_2, X_1 = a_1\right) \times \ldots \times$$

$$\times P\left(X_n = a_n \middle| X_{n-1} = a_{n-1}, X_{n-2} = a_{n-2}, \ldots, X_1 = a_1\right).$$

Csakhogy a Markov-lánc esetében a mozgásnak nincs memóriája, tehát már a második feltételes valószínűség egyszerűsödik, s ugyanígy minden utána következő is:

$$P\left(\bigcap_{i=1}^{n} A_i\right) = P(X_1 = a_1) \times P\left(X_2 = a_2 \middle| X_1 = a_1\right) \times P\left(X_3 = a_3 \middle| X_2 = a_2\right) \times \ldots \times$$

$$\times P\left(X_n = a_n \middle| X_{n-1} = a_{n-1}\right) = P(X_1 = a_1) P_{a_1 a_2} P_{a_2 a_3} \ldots P_{a_{n-1} a_n}.$$

Ezt hívjuk Markov-tulajdonságnak.

S most lássunk pár konkrét példát a Markov-láncokra, a nagyon egyszerűekből indulva.

1. példa: primitív telefonközpont.

Kezdjük egy primitív telefonközponttal: ez egyszerre csak egy hívást tud fogadni. A következőket tesszük fel:

a) a központba minden időegységben a múlttól függetlenül $0<p<1$ valószínűséggel érkezik hívás, b) ha a központ éppen foglalt, akkor a hívás elvész, ha szabad, akkor értelemszerűen foglaltra vált, c) ha foglalt, akkor a folyamatban lévő beszélgetés – ismét a múlttól függetlenül – $0<q<1$ valószínűséggel véget ér.

Végül feltesszük azt is, hogy

d) az, hogy érkezik-e új hívás az időegység alatt, az független attól, hogy jelenleg folyik-e beszélgetés.

Az a) feltétel azt is magában foglalja, hogy olyan kis időegységeket veszünk, amelyeken belül nem érkezik egyszerre több hívás, ezt vehetjük reális feltevésnek. A b) feltétel fejezi ki a telefonközpont „primitív"-voltát: nincs várakoztatás, ha mással beszél, akkor nekünk foglaltat jelez és kész. A c) feltétel csak némely esetekben reális: a végtelen beszélgetésekbe bonyolódó telefonálóknál.

Itt tehát két állapot van: $S=\{0,1\}$, 0-val jelezzük, hogy szabad a vonal, 1-gyel, hogy foglalt. A Markov-mátrix most a következő:

$$M=\begin{pmatrix} 1-p & p \\ q(1-p) & pq+(1-q) \end{pmatrix}.$$

Itt az első sorral nincs gond. Az első elem azt fejezi ki, milyen valószínűséggel marad szabad egy szabad állapot. Ez akkor történik, ha nem érkezik hívás az időegység alatt. Ennek valószínűsége $1–p$. Ugyanígy az első sor második eleme azt fejezi ki, hogy milyen valószínűséggel lesz foglalt a szabad állapot. Ehhez az kell, hogy érkezzen egy hívás, ennek valószínűsége p. A második sor már bonyolultabb: itt a vonal foglalt. Mikor lesz szabad? Ha egyrészt befejeződik a hívás, ennek q a valószínűsége, másrészt nem érkezik új hívás, ennek valószínűsége $1–p$. Az eredmény a kettő szorzata, hisz feltettük, hogy az aktuális beszélgetés befejezése és az új hívás érkezése egymástól független események. Valamivel még ennél is bonyolultabb a második sor második elemének kiszámolása: itt az időegység elején foglalt és a végén is foglalt a vonal. Ez kétféleképp is lehetséges: a) befejeződik a „régi" beszélgetés (q valószínűséggel) és érkezik új (p valószínűséggel), ennek az eseménynek a valószínűsége a függetlenség miatt pq, b) nem fejeződik be a régi $(1–q)$ és ekkor mindegy, hogy érkezik-e új hívás vagy sem, hiszen ha érkezik, az „kárba megy". Az utóbbi esemény valószínűsége tehát $1–q$. Könnyen ellenőrizhető, hogy a Markov-mátrixra kirótt feltételek teljesülnek.

2. példa: telefonközpont egy „Vangelis vonallal".

Nézzünk egy kicsit bonyolultabb példát! Az előző példához hozzáveszünk még egy „Vangelis vonal"-at, amin egy ember várakozhat a hívás kapcsolására (miközben nyilván Vangelis zenéjét hallgatja). Továbbra is olyan kicsi az időegység, ahogy azalatt csak egy hívás érkezhet, továbbra is p valószínűséggel, a beszélgetés befejezésének valószínűsége továbbra is q és továbbra is független egymástól e két esemény.

Most tehát három állapot van: $S=\{0,1,2\}$, ahol 0=szabad, 1=foglalt és nincs várakozó, 2=foglalt és van várakozó.

3. feladat: Számítsuk ki most a folyamat mátrixát!

Megoldás:
Most a mátrix a következőképpen alakul:

$$M = \begin{pmatrix} 1-p & p & 0 \\ q(1-p) & (1-p)(1-q)+pq & (1-q)p \\ 0 & q(1-p) & qp+(1-q)(1-p) \end{pmatrix}.$$

A második oszlopot magyarázzuk meg, mert az a legbonyolultabb. A második oszlop első eleme azt jelzi, hogy milyen valószínűséggel lesz a szabad állapotból foglalt, ez egyszerű: p. A második sor és második oszlop metszéspontjában annak az eseménynek a valószínűsége áll, hogy a központ foglalt volt várakozó nélkül és ebben az állapotban is marad. Ez kétféleképp lehetséges: a) nem ér véget a beszélgetés ($1–q$) és nem érkezik új hívás ($1–p$), ennek valószínűsége tehát $(1–p)(1–q)$ a függetlenség miatt, b) véget ér a beszélgetés (q) és új hívás érkezik (p), ennek valószínűsége pq. Itt tehát $(1–p)(1–q)+pq$ áll. A harmadik sorban álló elem azt fejezi ki, hogy milyen valószínűséggel lesz a foglalt plusz várakozó állapotból egyszerűen foglalt. Ehhez az kell, hogy a folyó beszélgetés befejeződjék (q) és új hívás ne érkezzék ($1–p$). Ennek valószínűsége tehát $q(1–p)$ a függetlenség miatt.

3. példa: Ehrenfest urna modell.

Az Ehrenfest urna modell valójában egy Markov-lánc, a fizikában van rá szükség. Amikor ezt a modellt felállították, még nem volt tisztázva, hogy mi is a Markov-lánc. A modellt a következőképp lehet szemléltetni. Van két kutya és a két kutyán összesen N bolha. Egy lépésben pontosan egy bolha átugrik a másik kutyára. Az első kutyán lévő bolhák számát – pontosabban ennek változását – vizsgáljuk.

Most tehát az állapotok: $S=\{0,1,2,\ldots,N\}$. Az átmeneti valószínűségek is könnyen kiszámíthatók. Ha épp n bolha van az első kutyán, akkor a következő lépésben csak $n+1$ vagy $n–1$ bolha lehet rajta. Ennek valószínűsége $P_{n,n-1} = \frac{n}{N}$ (hiszen ennyi a valószínűsége, hogy egy a rajta levő n bolhából ugrik az adott időegységben, illetve $P_{n,n+1} = \frac{N-n}{N}$.

Ez a Markov-lánc azonban nem teljesíti az aperiodicitási feltételt, hiszen a gráfja páros gráf. Ha például éppen nincs bolha a kutyán, akkor a következő lépésben biztos lesz, és legközelebb a második, a negyedik vagy általában valamelyik párosadik lépésben szabadulhat meg megint az összes bolhájától. Tehát az innen induló körök hosszának legnagyobb közös osztója kettő. És nyilván minden állapotra igaz, hogy csak páros lépésben léphet újra fel.

4. példa: Wright-Fischer genetikai modell.

Ez a modell a génreprodukciót van hivatva modellezni. Ezt a következőképp teszi: a gént egy urnának képzeli, amiben mondjuk kék és piros golyók vannak, összesen N darab. A következő urnát (gént) úgy kapjuk, hogy N-szer húzunk ebből az urnából visszatevéssel – minden húzás független a többitől – és olyan színű golyót teszünk a következő urnába, amilyen színűt az előzőből húztunk. Mondjuk a piros golyók számát figyeljük.

A piros golyók számának lehetséges állapotai $S=\{0,1,2,\ldots,N\}$. Az átmeneti valószínűség a k-piros állapotból az l piros állapotba: $P_{k,l} = \binom{N}{l}\left(\frac{k}{N}\right)^l\left(1-\frac{k}{N}\right)^{N-l}$. Aki ismeri a binomiális eloszlást, annak ebben semmi meglepő nincsen. Az N húzásból ki kell választanunk azt az l-et, amikor pirosat húzunk, ezt $\binom{N}{l}$-féleképp lehet. Ha már rögzítettük a helyeket, ezeken $\left(\frac{k}{N}\right)^l$ valószínűséggel fogunk piros golyót húzni az első urnából. A többi helyen viszont kék

golyót kell húznunk, ennek valószínűsége $(1-\frac{k}{N})^{N-l}$. A húzások visszatevéssel történnek, és függetlenek egymástól, tehát annak valószínűsége, hogy pont a rögzített *l* helyen húzunk pirosat éppen $(\frac{k}{N})^{l}(1-\frac{k}{N})^{N-l}$.

Megjegyezzük még, hogy ennek a folyamatnak két elnyelő állapota van, ahonnan nem lehet máshova eljutni: az egyik a csupa-piros, a másik a csupa-kék.

4. feladat Próbáljuk meg a mutációt is hasonlóan modellezni. Tehát tegyük fel, hogy pl. 0,99 valószínűséggel a húzott színű golyót helyezünk a második urnába, de 0,01 valószínűséggel ellenkező színűt. Írjuk fel most az átmeneti valószínűségeket!

Ajánló

Nemetz Tibor és Wintsche Gergely: Valószínűségszámítás és statisztika mindenkinek, Polygon, 1998, http://www.math.u-szeged.hu/polygon/

William Feller: Bevezetés a valószínűségszámításba és alkalmazásaiba, Műszaki Kiadó, Budapest, 1978.

Orosz Gyula: Markov láncok, http://matek.fazekas.hu/portal/tanitasianyagok/Orosz_Gyula/Mar/markov.html

Sztrik János: Bevezetés a sorbanállási elméletbe és alkalmazásaiba, http://irh.inf.unideb.hu/user/jsztrik/education/08/index.html

Hosszú idejű várakozás.

Sokszor az érdekel minket, hogy hogyan viselkednek „hosszú távon” a Markov-láncok, tehát mi történik, ha sokáig várunk. Ez érdekel a kártyakeverésnél is. Tehát az érdekel minket, hogy egy bizonyos b állapotot nagyon sok lépés után milyen valószínűséggel ér el az állapot.

Jelöljük tehát $P_{ab}^{(n)}$-nel annak valószínűséget, hogy az állapot *n* lépés után a b állapotban lesz, ha most éppen az a állapotban van.

Nyilvánvaló, hogy $P_{ab}{}^{(0)} = \begin{matrix}1\\0\end{matrix}$, annak megfelelően, hogy b=a vagy nem. Másrészt definíció szerint $P_{ab}{}^{(1)} = p_{ab}$. Általában azt állítjuk, hogy

$P_{ab}^{(n)} = P_{ab}^{n}$, ahol P^n az eredeti *P* mátrix mátrixszorzás szerinti *n*-edik hatványát jelenti, P_{ab}^{n} pedig ennek a mátrixnak a megfelelő (a-adik sor és b-edik oszlop metszéspontjában álló) elemét.

Állításunk bizonyítása teljes indukcióval történhet. Láttuk, hogy igaz az állítás *n*=0-ra és 1-re. Tegyük fel, hogy *n*-re igaz és írjuk fel a valószínűséget *n*+1-re. Aki tisztában van a mátrixszorzás fogalmával és a teljes valószínűség tételét megértette, az könnyen megérti az alábbi bizonyítást:

$$P_{ab}^{(n+1)} = P(X_{n+1}=b \mid X_0=a) = \sum_g P(X_{n+1}=b, X_n=g \mid X_0=a) =$$

$$= \sum_g P(X_{n+1}=b \mid X_n=g)P(X_n=g \mid X_0=a) = \sum_g P_{gb}P_{ag}^{(n)} = \sum_g P_{gb}P_{ag}^{n} = P_{ab}^{n+1}.$$

A második lépésben kihasználtuk a Markov-tulajdonságot. Tehát minden *n*-re igaz az állítás.

Az érdekel minket, hogy mi történik hosszú idő után egy Markov-lánccal. Kialakul-e egyfajta állandóság és egyenletesség. A kártyakeverés esetében például az a kérdés, hogy ha hosszú ideig keverünk, előbb-utóbb kialakul-e egy olyan állapot, amelyben minden sorrend egyformán

valószínű. Matematikailag kicsit pontosabb formában így fogalmazhatjuk meg a kérdést: ha a lépésszám, *n* a végtelenhez tart, akkor stabilizálódik-e – konvergál-e – az egyes állapotok valószínűsége? Vagyis: ha elég sok lépést teszünk, tetszőlegesen megközelíthetjük-e azt a helyzetet, amikor minden állapot (sorrend) egyformán valószínű? Ez a következőt jelenti:
Tegyük fel, hogy felrajzoltuk az állapotok gráfját, s ezután a gráfon elkezdődik egyfajta „véletlen bolyongás". Igaz-e, hogy ha elég sokáig tart ez a bolyongás, akkor valamilyen eloszlás stabilizálódik? A kártyakeverés esetén azt kérdezzük, hogy igaz-e, hogy egy idő után minden sorrend nagyjából (közel) egyenlő valószínűségű lesz?

A kártyakeverés matematikai modellje
Szükségünk van egy *matematikai modellre*, ez a következő:
Tekintsük az 52 kártya összes sorrendjét, ezt a halmazt – az összes 52-edrendű permutációk halmazát – a matematikában $\mathbf{S}_{52}$-vel jelöljük. Tehát $S = S_{52}$.
Ismeretes, hogy ilyen permutációból 52! darab van, ami irdatlanul nagy szám, kb. $6{,}5\times10^{67}$. Ha ennyi aranyatomot vennénk és azt egy kocka alakú aranytömbbe öntenénk, ennek az aranykockának az oldalhossza csillagászati méretű lenne. Ezt a mennyiséget tehát gyakorlatilag végtelennek is tekinthetjük. A Markov-láncnak tehát ennyi állapota lesz.
Megjegyzem, hogy a továbbiak matematikájához felhasználjuk, hogy a permutációk csoportot alkotnak, de erre csak utalni fogok. (A permutációk egy véges halmazon végzett transzformációk, ugyanúgy, ahogy például a sík egybevágósági transzformációi a sík pontjainak halmazán végzett transzformációk. Ezeket a transzformációkat alkalamazhatom egymás után, s akkor újra egy permutációt – illetve egy egybevágóságot – kapok. Az egymás után alkalmazást nevezik a transzformációk szorzásának. Erre mint műveletre alkotnak csoportot a permutációk.)
A keverés egy lehetséges matematikai modellje a következő: A kártyacsomag tetejéről valahány lapot leemelünk („emelés"), a jobb kezünkbe fogjuk a leemelt *j* darab lapot, a bal kezünkbe a *b* darab megmaradt lapot ($j+b=52$), és valamilyen véletlen sorrendben összefésüljük a két kupacot. Így kapjuk az új sorrendet.
Először számoljuk ki, hogy egy sorrendből hány másikhoz tudunk így eljutni, vagy másképp: egy adott sorrendnek hány ilyen keverése van? Egyszerű kombinatorikai feladat annak belátása, hogy ha *b* lap marad a bal kezünkben, azt $\binom{52}{b}-1$ féle különböző sorrendben rakhatjuk a többi közé, oly módon, hogy ne az eredeti sorrendet kapjuk vissza éskülönböző *b*-kre ezek a sorrendek mind különbözőek. (Gondoljunk arra a helyzetre, amikor már összefésültük a két kupacot, és írjuk fel a sorrendet úgy, hogy csak azt jelöljük, hogy melyik kártya melyik kezünkből „származik". A *b* darab „balkezes" kártyának éppen ennyiféle elrendezése lehetséges, ha a kiinduló helyzetet nem engedjük meg. A „balkezes" kártyák egymáshoz viszonyított sorrendje viszont adott, az a keverés során nem változik.) Ezt a mennyiséget kell tehát minden *b*-re összeadni és az összeghez még hozzáadni 1-et, ami a az eredeti sorrend visszaállítását képviseli. Tehát az összes elérhető sorrend száma:

$$\sum_{b=0}^{52}\left(\binom{52}{b}-1\right)+1=2^{52}-52\approx 4{,}5\times10^{15}.$$

(Megengedjük, hogy ne emeljünk egyetlen lapot sem és azt is, hogy minden lapot leemeljünk, ezért megy az összegzés 0-tól és tart 52-ig.) A keveréssel megkapható sorrendek száma az összes lehetséges sorrendhez képest nagyon kicsi. Mondhatjuk:
Valóságos csoda, hogy mégis meg tudjuk keverni a kártyacsomagot, sőt: az összes sorrendet megkaphatjuk, méghozzá elég gyorsan.
Be lehet bizonyítani, hogy

$\log_2 52$ lépésben megkaphatunk minden permutációt!

Persze ez egy általános tétel speciális esete, s mivel a keverések száma egész, ez azt jelenti, hogy legfeljebb hat keveréssel megkaphatunk minden permutációt. Jól értsük meg: ez az állítás arra az esetre vonatkozik, amikor előre meghatározhatjuk, hogy mikor hogyan emelünk és keverünk. Tehát ha determinisztikus módon hajtjuk végre a keveréseket, akkor ennyi lépésben eljuthatunk minden keveréshez. Ez még így is valóságos csoda, hiszen a gráfnak irdatlan sok pontja van, kb. $6,5\times10^{67}$. Ehhez képest minden pont foka elenyészően kicsi: $4,5\times10^{15}$. A gráf tehát nagyon ritka. Állításunk azt mondja, hogy mégis minden pontjából minden pontjába „hamar" el lehet érni. Gráfelméleti nyelven: az átmérője kicsi, pontosan: hat, azaz bármely két pont távolsága – a legrövidebb út hossza az egyik pontból a másikba – legfeljebb hat hosszúságú.

Egyelőre tehát ott tartunk, hogy tudjuk, hány pontja van a Markov-láncunkhoz tartozó gráfnak és tudjuk azt is, hogy egy pontból hány él indul. Most azt is meg kell állapítanunk, hogy egy adott sorrendből egy másikba milyen valószínűséggel jutunk el. Ezt a következőképpen számoljuk ki:

– Annak a valószínűsége, hogy pontosan *b* kártyát emelek le, $P(b)=\binom{52}{b}2^{-52}$.

– Az emelés és az összefésülés egymástól független műveletek.

– Az, hogy az összefésülésnél a következő kártyát melyik kezemből veszem, arányos azzal, ahány kártya van éppen ebben a kezemben. Tehát például legyen a jobb kezemben 20 kártya, a bal kezemben 32. Ekkor az, hogy az első négy lapot *jbbj* sorrendben fogom összefésülni: $\frac{20}{52}\frac{32}{51}\frac{31}{50}\frac{19}{49}$.

Ha így kiszámolom a valószínűségeket, akkor minden, egy keverési művelettel megvalósítható („kikeverhető") és a kiindulótól különböző sorrend valószínűsége egyaránt 2^{-52}, míg a kiinduló sorrend visszaállításának valószínűsége $53x\,2^{-52}$ lesz.

Hogy miért jó ez a modell, az jobban látszik, ha a fordított műveletet, ennek a keverésnek az **inverz műveletét** nézem.

Mi a fordított művelet? Veszem az egyes lapokat sorban, és egy érme feldobásával döntöm el, hogy a soron következő lapot a bal (írás) vagy a jobb (fej) kezemnek megfelelő kupacba teszem, majd a végén a bal kupacot a jobb kupac alá helyezem.

Könnyen belátható, hogy ez tényleg az inverzkeverés. Matematikai szempontból lényegtelen, hogy az eredeti keverést vagy annak az inverzét vizsgáljuk. Ez csak annyit változtat a dolgon, hogy időben visszafele nézzük a folyamatot. És így minden lépés természetes, az érme feldobása is, az egymás alá helyezés is. (Ha az inverz művelettel *minden* állapotból *d* állapotba juthatunk el, az eredeti művelettel is minden állapotból *d* állapotba juthatunk el, és minden lépés egyformán valószínű, akkor ez azt jelenti, hogy az eredeti állapotból is minden elérhető állapotba ugyanolyan valószínűséggel juthatunk el.)

Most már kész a gráf, persze felrajzolni nem fogom, és a mátrixot sem írom fel: mindkettő irdatlanul nagy lenne.

Azt állítom, hogy az egyes állapotok valószínűsége idővel stabilizálódik. Vagyis van egy stacionárius állapot. Azt állítom, hogy

a kártyakeverésnél az egyenletes eloszlás a stacionárius állapot.

Elvileg elképzelhető volna, hogy nem az egyenletes eloszlás a stacionárius állapot, hanem például egy olyan állapot, ahol a pikkek inkább a középen helyezkednek el, vagy az ászok aránylag közel vannak egymáshoz. Persze, nem így van, de ezt bizonyítanunk kell. A bizonyítás tulajdonképpen egyszerű, csak szükséges hozzá pár fogalom. Először p-vel fogjuk jelölni az állapotok **valószínűségi eloszlását**. Ezen a következőt értjük: p egy olyan függvény, amely minden állapothoz hozzárendel egy pozitív valós számot, ennek az állapotnak a valószínűségét. Az összes állapotokra összeadva ezeket az értékeket pontosan egyet kapunk:

$$\sum_a p(a) = 1,$$

ahol az összegzés az összes állapotra történik. A mi esetünkben az összes sorrendre összegzünk, vagyis ez az összeg 52! tagból áll.

A p eloszlást tekinthetem egy 52! hosszú sorvektornak is:

$$p=(p(a_1), p(a_2), \ldots, p(a_{52!})).$$

Érdemes meggondolni, hogy ha ezt a sorvektort jobbról megszorzom a keverés Markov-mátrixával, az $\mathbf{M}=\left(P_{a_i a_j}\right)$ mátrixszal, akkor a kapott sorvektor épp azt mutatja, hogy, feltéve, hogy jelenleg az állapotok eloszlása p, milyen eloszlású lesz az állapotok valószínűsége egy lépés múlva. Hiszen az *i*-edik állapotba, azaz a_i állapotba éppen $\sum_{j=1}^{52!} p(a_j) P_{a_j a_i}$ valószínűséggel jut a folyamat, s ez éppen a p sorvektornak és az $\mathbf{M}$ mátrix *i*-edik oszlopának szorzata, tehát a $p\mathbf{M}$ sorvektor *i*-edik eleme.

Azt kell még észrevennünk, hogy

a stacionárius állapothoz tartozó sorvektornak ki kell elégítenie a

$$\mathbf{vM}=\mathbf{v}$$

egyenletet.

Az előbb mondottak szerint ez éppen azt fejezi ki, hogy az időben nem változik az állapotok eloszlása.

Azt állítjuk, hogy

a kártyakeverésnél épp az egyenletes eloszlás az egyetlen megoldása ennek az egyenletnek.

Az előbb már láttuk, hogy **minden keverésnek van inverze**. (Ez nem minden Markov-láncra igaz, de a Markov-láncok egy nagy osztályára igaz.) Ez pontosan azt jelentette, hogy minden állapotba ugyanannyi féleképp lehet eljutni, ahány állapot elérhető belőle és mindegyiknek egyforma a valószínűsége. Ebből viszont következik, hogy

a Markov-lánc mátrixában nemcsak az egy sorban álló elemek összege egy, hanem az egy oszlopban álló összegeké is:

$$\sum_a P_{ab} = \sum_b P_{ab} = 1.$$

Azokat a mátrixokat, amelyekben minden sorösszeg és minden oszlopösszeg egyenlő, duplán **sztochasztikus mátrix**nak vagy **bisztochasztikus mátrix**nak nevezzük.

Most használtuk, hogy a permutációk csoportot alkotnak, ezért a kártyakeverés mátrixa bisztochasztikus mátrix. Könnyen ellenőrízhetjük, hogy bisztochasztikus $\mathbf{M}$ mátrix esetében az

egyenletes eloszlásnak megfelelő konstans **v** vektor kielégíti az egyenletet. Ez jelen esetben 52! darab 1/52!-ból áll. Hiszen minden eleme egyenlő és összességében egy oszlopnyi P_{ab}-val szorozzuk, ezek összege pedig egy.

„Végtelenül sok” idő után egyre közelebb kerülünk a stacionárius állapothoz, ami jelen esetben az egyenletes eloszlás. Vagyis nagyon sok keverés után közelítőleg egyforma lesz minden sorrend valószínűsége.

Hány keverés elég?

Befejezésül még felvethető az a kérdés, hogy akkor hány keverés elég? Hány keverés után mondhatjuk, hogy már „majdnem” egyenletes az egyes sorrendek valószínűsége?
A választ itt csak jelezni tudom, akit érdekel, erről a témáról az egyetemen egy speciálelőadást tartok, ott majd szeretettel várom.

Bevezetjük a d_n számot, amely azt mutatja, hogy n keverés utáni eloszlás milyen „messze” van a stacionárius eloszlástól.

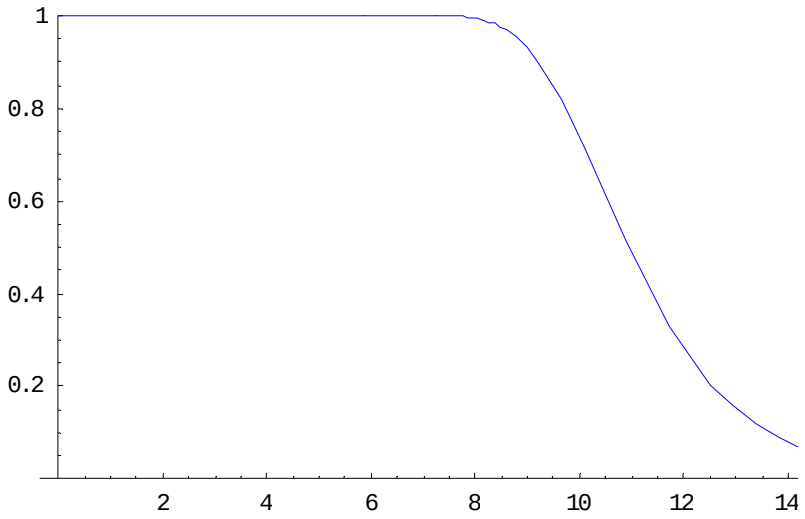
$d_n = \frac{1}{2}\sum_b |p(b) - M_{ab}^n|$, ahol az a az indulási állapot, p a stacionárius állapot és M_{ab}^n azt jelzi, hogy milyen valószínűséggel leszünk a b állapotban n lépés után. Ez a d_n egy 0 és 1 közötti szám. Azt akarjuk, hogy ez a szám nagyon kicsi, azaz nullához közeli szám legyen. A kérdés az, hogyan kell ehhez n-et (a lépésszámot) megválasztanunk. Erre egy nevezetes cikk válaszol, már a címével is: „Seven shuffles suffice!” Hét(-nyolc) keverés elég. S valóban: ha egy pókerpartiban valaki 15-ször megkeveri a paklit, azt társai idővel kirakják, mert túl sokat kell rá várni.

Mit jelent ez matematikailag? Tegyük fel, hogy nem 52, hanem m lapból álló kártyacsomagot akarunk megkeverni. Bonyolult számolással belátható, hogy a fenti d_n érték $n < c\log m$ lépésig (itt c egy pontosan kiszámítható konstans) nagyon közel van 1-hez, ennél az értéknél hirtelen nagyon közel kerül 0-hoz, és nagyobb n-ekre már közel marad. Ez az érték 52 lapnál 7 körül van, tehát valóban: **hét-nyolc keverés elég**.

Igaz az alábbi felső becslés:

$$d_n \le 1 - e^{-2^{\left(\log_2 m - \frac{1}{2}\right)(n+1)}},$$

ahol tehát m a pakli lapjainak számát, n pedig a keverések számát jelöli. A felső korlátot adó jobb oldali függvény grafikonja m=52 esetén a 3. ábrán látható. Ez a felső becslés a jó keverést csak 7-8-nál több lépés esetén garantálja, de a d_n függvény hirtelen lecsökkenő alakja már ebből a közelítésből is látható.



3. ábra
A grafikon a Mathematica szoftver segítségével készült.

Tóth Bálint weboldala: http://www.math.bme.hu/~balint/

Ajánlott írások a kártyakeverésről
Angol nyelvű viszonylag egyszerű nyelvezetű összefoglaló:
Brad Mann: How many times should you shuffle a deck of cards?
http://www.dartmouth.edu/~chance/teaching_aids/books_articles/Mann.pdf

Tudományos összefoglaló a felfedezőtől:
Persi Diaconis: Mathematical developments from the analysis of riffle shuffling,
http://www-stat.stanford.edu/~cgates/PERSI/papers/Riffle.pdf

Persi Diaconis weboldala: http://www-stat.stanford.edu/~cgates/PERSI/index.html