Matematikai Lapok

1992/3-4

Szalkai István –
– Dan Velleman:
Rugalmas pénzérmék

RUGALMAS PÉNZÉRMÉK[†]

SZALKAI ISTVÁN[‡] és DAN VELLEMAN

Képzeljünk el egy olyan érmét, amely $\frac{3+\sqrt{3}}{6}$ valószínűséggel[1)] fej, és $1-p=\frac{3-\sqrt{3}}{6}$ valószínűséggel írás. No jó, de lássuk, mire jó egy ilyen érme! Háromszor feldobva annak a valószínűsége, hogy három azonos dobást kapunk (három fej vagy három írás) nem más, mint

$$p^3+(1-p)^3=\frac{9+5\sqrt{3}}{36}+\frac{9-5\sqrt{3}}{36}=\frac{1}{2},$$

azaz, érménk háromszori feldobásával egészen pontosan tudunk egy közönséges (fej=írás=1/2 valószínűséggel) érmét szimulálni. Azonban, ha csak kétszer dobjuk fel az érmét, mi annak a valószínűsége, hogy egy írást és egy fejet kapunk? Pontosan $2p(1-p)=1/3$, azaz érménket egy olyan érmét is tudunk szimulálni, amely 1/3 valószínűséggel fej, 2/3 valószínűséggel írás. A fenti eredményeket úgy is összegezhetnénk, hogy érménkkel a $p=1/2$ és a $p=1/3$ valószínűséggel fejre eső érmék helyett is használhatjuk. Hát ezért nevezhetjük rugalmasnak a $p=\frac{3+\sqrt{3}}{6}$ valószínűséggel fejre eső érmét!

A továbbiakban ezt úgy fogalmazzuk, hogy $\frac{3+\sqrt{3}}{6}$ **szimulálja** mind az 1/2-et, mind az 1/3-ot. Általában pedig mondjuk azt, ha p és q mindketten 0 és 1 közé eső valós számok, hogy **p szimulálja q-t**, ha találunk egy olyan $n\in\mathbb{N}$ természetes számot, és az n hosszúságú fej-írás dobássorozatoknak ki tudjuk jelölni egy olyan E részhalmazát úgy, hogy a p valószínűséggel fej érmét n-szer feldobva a kapott dobássorozat E-nek pontosan q valószínűséggel lesz eleme.

[†] A cikk az American Mathematical Monthlyban jelent meg először (100(1993), 26–33). A szerzők ezért a munkájukért a Mathematical Association of America 1994. évi Lester Ford Díját nyerték el. (Évente öt díjat osztanak ki a Monthlyban megjelent legjobb cikkek szerzőinek.)

[‡] Jelen cikk a Peregrinatio I. Alapítvány 2/1991. sz. támogatásával készült

[1)] A 0 és 1 közötti valós számokat nevezzük valószínűségeknek.

Persze ezt a valószínűséget könnyen ki is tudjuk számolni:

$$P(E) = \sum_{i=0}^{n} a_i p^i (1-p)^{n-i},$$

ahol a_i jelöli E azon elemeinek (azon dobássorozatoknak) a számát, amelyekben a fej i-szer (és így az írás $n-i$-szer) fordul elő. Az elemi valószínűségszámításban jártas Olvasó könnyen látja, hogy bármely dobássorozatban a fejek és írások sorrendje lényegtelen, és hogy az ilyen dobássorozatok valószínűsége pontosan $p^i(1-p)^{n-i}$. Összegezés után kapjuk a fenti képletet. Az is belátható, hogy $a_i \leq \binom{n}{i}$ (binomiális együttható), sőt tetszőlegesen választott ilyen $\{a_i\}_{i=0}^n$ számsorozathoz található dobássorozatok egy megfelelő E halmaza.
Így kimondhatjuk az alábbi definíciót:

0. DEFINÍCIÓ Tetszőleges $p, q \in [0,1]$ valós számok esetén **p szimulálja q-t**, ha található olyan $n \in \mathbf{N}$ természetes szám, és olyan $a_i \leq \binom{n}{i}$ természetes számok $0 \leq i \leq n$, amelyekre

$$q = \sum_{i=0}^{n} a_i p^i (1-p)^{n-i} \qquad \blacksquare$$

Dolgozatunkban a következő kérdést feszegetjük: a $[0,1]$ halmaz mely részhalmazai szimulálhatóak egyszerre (egyetlen p számmal), illetve adott p szám a $[0,1]$ halmaz milyen részhalmazát szimulálja?

Néhány észrevételt máris tehetünk. A „p szimulálja q-t" reláció nyilván reflexív (azaz minden p szimulálja önmagát), és könnyen láthatóan tranzitív (ha p szimulálja q-t n hosszú dobásokkal, és q szimulálja r-et m hosszú dobásokkal, akkor p szimulálni fogja r-et $n \cdot m$ hosszú dobásokkal). Ennek belátását az Olvasóra bízzuk. Az ilyen tulajdonságú relációkat a matematikában **előrendezésnek**, angolul preorder-nek nevezzük. Nyilvánvalóan 0-át és 1-et minden $p \in [0,1]$ valós szám szimulálja, és általában p egyszerre szimulálja (vagy nem szimulálja) q-t és $(1-q)$-t. Továbbá, ha p egyszerre szimulálja q-t és r-et,akkor szorzatukat, $q \cdot r$-et is. A fentiekből az is következik, hogy ha p szimulálja a $q, r, s \in [0,1]$ számokat, akkor a $qr + (1-q)s$ számot is. Ezt a különös tényt a 6. Tétel bizonyításában majd használni fogjuk, ezért nevezzük (@) **tulajdonságnak**. Megemlítjük még azt az önmagában is érdekes algebrai tényt, hogy: tetszőleges $p \in [0,1]$ szám által szimulált valós számok halmaza nem más, mint a $\{0,1\}$ halmaz (algebrai) lezártja egyetlen kétváltozós műveletre, nevezetesen az $f(x,y) := px + (1-p)y$ műveletre nézve.

Mit állíthatunk még a „p szimulálja q-t" relációról? Mint a bevezetőben is látjuk, olyan érméket érdemes terveznünk, melyek egyszerre több, számunkra „hasznos" valószínűséget egyszerre szimulálnak. Mint például az 1/2-et és az 1/3-ot. De miért kellett olyan bonyolult számot választanunk, mint a $\frac{3+\sqrt{3}}{6} \approx 0,7886$? Például, racionális számot nem találhattunk volna? Sajnos nem. Először is: 1/2 nem szimulálja 1/3-ot. Márpedig azért nem, mert az 1/2 által szimulált számok, a $\sum_{i=0}^{n} a_i p^i (1-p)^{n-i}$ alakú kifejezések, olyan racionális számok, melyek nevezői 2-nek hatványai. Másodszor pedig: 1/2-et csak egyetlen racionális szám tudja szimulálni: önmaga. Legyen ugyanis $p = \frac{j}{k}$ olyan racionális szám, mely szimulálja 1/2-et, persze j és k relatív prímek. Ekkor

$$\frac{1}{2} = \sum_{i=0}^{n} a_i p^i (1-p)^{n-i}$$

Ha most $b_i = \binom{n}{i} - a_i$, akkor a binomiális tétel miatt

$$\sum_{i=0}^{n} b_i p^i (1-p)^{n-i} = 1 - \frac{1}{2} = \frac{1}{2}$$

Ne feledjük, hogy $a_0 + b_0 = \binom{n}{0} = 1$, vagyis egyikük 0, mondjuk a_0. Ekkor

$$\frac{1}{2} = \sum_{i=1}^{n} a_i p^i (1-p)^{n-i} = p \sum_{i=1}^{n} a_i p^{i-1} (1-p)^{n-i} = \frac{j}{k} \cdot \frac{\sum_{i=1}^{n} a_i j^{i-1} (k-j)^{n-i}}{k^{n-1}}$$

vagyis $k^n = 2j \cdot \sum_{i=1}^{n} a_i j^{i-1} (k-j)^{n-1}$, azaz $j \mid k^n$ amiből $j = 1$ következik, hiszen k és j relatív prímek. De mivel $1-p = (k-j)/k = (k-1)/k$ szintén szimulálja 1/2-et, így hasonló okoskodással azt is kapjuk, hogy $k - 1 = 1$. Vagyis $j = 1$, $k = 2$, azaz $p = 1/2$, Q.E.D. Végül harmadszor: hasonló, bár kissé hosszadalmasabb gondolatmenettel az is megmutatható,hogy 1/3-ot csak két racionális szám tudja szimulálni: az 1/3 és a 2/3.
A fenti három tényből pedig valóban az látszik, hogy 1/2 és 1/3 semmilyen racionális számmal nem szimulálhatók egyszerre.
(Általában az a tény is a fentiekhez hasonlóan igazolható, hogy tetszőleges 1-nél nagyobb N négyzetmentes szám esetén az $1/N$ számot csak két racionális szám szimulálhatja: $1/N$ és $(N-1)/N$).

A fentiek azt mutatják, hogy a racionális számok által szimulált valószínűségekre nagyon erős (oszthatósági) feltételek kell, hogy teljesüljenek. Azonban irracionális (de még mindig algebrai) számokkal sokkal rugalmasabban lehet akárhány (de véges) számot egyszerre szimulálni, mint azt az alábbi tételek mutatják.

1. TÉTEL *Legyen $F \subseteq \mathbb{Q}$ a racionális számok egy tetszőleges véges részhalmaza, és $F \subseteq [0,1]$. Ekkor létezik egy olyan $p \in [0,1]$ valós szám, amely egyszerre szimulálja F minden elemét.*

A Tétel bizonyítását az alábbi két állításra alapozzuk:

2. ÁLLÍTÁS Tetszőleges $n > 1$ természetes szám esetén $\left(1 - \frac{1}{n}\right)^{n-1} > \frac{1}{e}$

BIZONYÍTÁS: Tekintsük az $f(x) := \left(1 - \frac{1}{x}\right)^{x-1}$ függvényt.
Mivel $\lim_{x\to\infty} f(x) = \frac{1}{e}$ és $\lim_{x\to 0+0} f(x) = +\infty$ könnyen látszik, ezért elegendő azt megmutatnunk, hogy f monoton csökkenő. Ha deriválunk:

$$f'(x) = f(x) \cdot \left[\frac{1}{x} + \ln\left(1 - \frac{1}{x}\right)\right].$$

Mivel $\ln(x) < x - 1$ minden $x \in (0,1)$ valós számra, ezért $\ln\left(1 - \frac{1}{x}\right) < \frac{1}{x}$ ha $x > 1$. Ebből pedig $f'(x) < 0$, vagyis f monoton csökkenése következik. ■

3. ÁLLÍTÁS Tetszőleges $z \in [0, 1/e]$ valós és $n \in \mathbb{N}$ természetes számhoz található olyan $p \in [0,1]$ valós szám, amelyekre

$$np(1-p)^{n-1} = z$$

(azaz az egyenlet p-re megoldható).
BIZONYÍTÁS: $n = 1$ esetén egyszerűen $p = z$. Legyen most $n > 1$. Ekkor $p = 0$ esetén az egyenlet bal oldala 0, ami z-nél kisebb; $p = 1/n$ esetén pedig a bal oldala $1/e$-nél nagyobb (az 1. Állítás alapján), így z-nél is nagyobb. Márpedig a bal oldal p-nek folytonos függvénye, vagyis valóban létezik 0 és $1/n$ között olyan p valós szám, mely kielégíti az egyenletet. ■

Ez utóbbi állítás azt mondja, hogy ha egy érmét, (mely p valószínűséggel fej), n-szer feldobunk, pontosan z annak a valószínűsége, hogy egy fejet dobunk. n-et pedig a Tétel bizonyításában választjuk meg, a szimulálni kívánt racionális számok F halmazától függően.

Az 1. TÉTEL BIZONYÍTÁSA: Legyen F elemei nevezőinek maximuma N, mondjuk $N \geq 4$, és legyen $n = N!/3$. A 3. állítás szerint az $np(1-p)^{n-1} = 1/3$ egyenletnek van $p \in [0,1]$ megoldása. Ebből már következik az, hogy p minden

$$ap(1-p)^{n-1} = \frac{a}{3n} = \frac{a}{N!}$$

alakú racionális számot szimulál, ha $0 \leq a \leq \binom{n}{1} = n = N!/3$. Például az $1/3, 1/4, \ldots, 1/N$ számokat. Mint az 1. Tétel kimondása előtt megállapítottuk, ha p szimulálja q-t, akkor $(1-q)$-t is, sőt ha még r-et is, akkor a qr szorzatot is szimulálja p. Vagyis esetünkben p még a $2/3, 3/4, \ldots, (N-1)/N$ számokat is szimulálja. Sőt, $2/3 \cdot 3/4 = 1/2$-et is. (Itt használtuk ki az $N \geq 4$ feltevést.) Mivel tetszőleges j/k alakú racionális szám előáll az eddig szimulált racionális számok véges szorzataként:

$$\frac{j}{k} = \frac{j}{j+1} \cdot \frac{j+1}{j+2} \cdot \frac{j+2}{j+3} \cdot \ldots \cdot \frac{k-1}{k}$$

(feltéve, hogy $1 \leq j < N$), ezért p valóban minden olyan j/k törtet szimulál, melynek nevezője N-nél nem nagyobb. N választása miatt ez pedig azt jelenti, hogy p valóban szimulálja F minden elemét. ■

Módszerünkkel irracionális valószínűségek bizonyos halmazairól is megmutatható, hogy a halmaz minden eleme szimulálható egyetlen p valószínűséggel: Legyen F tetszőleges olyan véges részhalmaza a $[0, 1/e]$ intervallumnak, hogy F bármely két elemének hányadosa racionális. (Azaz $F \subseteq \mathbb{Q} \cdot \xi$ valamilyen $\xi \in \mathbb{R}$ valós számra, ahol $\mathbb{Q} \cdot \xi := \{r \cdot \xi | r \in \mathbb{Q}\}$.) Legyen F legnagyobb eleme z. Ekkor F minden eleme z-nek racionális többszöröse, azaz valamilyen N közös nevezővel

$$F = \left\{z, \frac{zj_1}{N}, \frac{zj_2}{N}, \ldots, \frac{zj_m}{N}\right\}$$

ahol persze $j_1, j_2, \ldots, j_m$ N-nél kisebb egész számok. Mivel $z \leq 1/e$, így a 3. Állítás miatt az $Np(1-p)^{N-1} = z$ egyenlőség teljesül valamilyen $p \in [0,1]$ valós számra. Ez a p szám minden zj/N számot szimulál, ha $j \leq N$, vagyis p szimulálja F minden elemét.

Az F-re tett $1/e$ felső becslés is kiküszöbölhető. Mi eddig csak az $np(1-p)^{n-1} = z$ egyenlőséget oldogattuk meg p-re, azaz a szimuláláskor *egyetlen* fejet írtunk elő, a többi dobás írás volt. n sajnos elég nagy is lehetett, pl. a nevezők közös többszöröse. Az $1/e$ felső becslés pedig a $\lim_{n\to\infty}\left(1 - \frac{1}{n}\right)^{n-1} = \frac{1}{e}$ egyenlőségből adódott (ld. 2. Állítás). Azonban, ha több fejet is megengedünk, az $1/e$ korlát várhatóan átléphető.
Ezt a

$$\lim_{k\to\infty} \lim_{n\to\infty} \sum_{i=1}^{k} \binom{n}{i} \left(\frac{x}{n}\right)^i \left(1 - \frac{x}{n}\right)^{n-1} = 1 - \frac{1}{e^x}$$

egyenlőség ($x \in \mathbb{R}$ tetszőleges) teszi lehetővé, hiszen így minden $z \in [0,1]$ szám esetén k-t és n_0-át elég nagynak választva ($n_0 > k$) a

$$\sum_{i=1}^{k} \binom{n}{i} p^i (1-p)^{n-i} = z$$

egyenlet minden $n > n_0$ szám esetén megoldható p-re, $p \in [0,1]$, és a fenti bizonyítás gondolatmenete megismételhető. Ez bizonyítja alábbi Tételünket:

4. TÉTEL *Legyen $F \subseteq [0,1]$ egy olyan véges részhalmaz, amelynek bármely két elemének hányadosa racionális. (Azaz $\exists \xi \in \mathbb{R}$ $F \subseteq \mathbb{Q} \cdot \xi$.) Ekkor létezik egy olyan $p \in [0,1]$ valós szám, amely szimulálja F minden elemét.*

A Tételre most egy másik bizonyítást adunk:

BIZONYÍTÁS: A számolások egyszerűsítése végett tegyük fel, hogy $1 \notin F$. Legyen F legnagyobb eleme z, és írjuk fel F elemeit z racionális többszöröseiként:

$$F = \left\{ z, \frac{zj_1}{N}, \frac{zj_2}{N}, \ldots, \frac{zj_m}{N} \right\}$$

ahol $j_1, j_2, \ldots, j_m < n$ és $N \in \mathbb{N}$. $z < 1$ miatt találhatunk olyan elég nagy n egész számot, amelyre

$$1 - \frac{1+nN}{2^n} > z$$

Osszuk el maradékosan $\binom{n}{i}$-t N-el, legyen q_i a hányados, $r_i < N$ pedig a maradék ($i = 1, 2, \ldots, n$), azaz $\binom{n}{i} = N \cdot q_i + r_i$. A bizonyítás kulcsa az a tény, hogy az alábbi (*) egyenletnek van $p \in [0,1]$ valós gyöke:

$$(*) \qquad \sum_{i=1}^{n} N q_i p^i (1-p)^{n-i} = z$$

Ha már megtaláltunk egy ilyen p-t, akkor persze p az összes

$$\frac{zj}{N} = \sum_{i=1}^{n} j q_i p^i (1-p)^{n-i}$$

alakú számot szimulálja, azaz F minden elemét is, q.e.d.

Már csak a (*) egyenletet kell megoldanunk. $p = 0$ esetén a bal oldal 0, ami z-nél kisebb; $p = 1/2$ esetén pedig nem más, mint

$$\sum_{i=1}^{n} \frac{N q_i}{2^n} = \frac{1}{2^n} \sum_{i=1}^{n} \left[\binom{n}{i} - r_i \right] = \frac{1}{2^n} \left[2^n - 1 - \sum_{i=1}^{n} r_i \right]$$
$$> \frac{1}{2^n} [2^n - 1 - nN] = 1 - \frac{1+nN}{2^n} > z$$

Mivel pedig az egyenlet bal oldala p-nek folytonos függvénye, így valóban létezik 0 és 1/2 között olyan p valós szám, mely kielégíti az egyenletet.
Így teljes mértékben beláttuk a 4. Tételt. ■

Vegyük észre, hogy az 1. Tétel bizonyításában szereplő p egy *racionális* együtthatójú polinom gyöke, az ilyen valós számokat *algebrai* számoknak nevezzük. (Közismert, hogy az algebrai számok halmaza testet alkot a szokásos + és · műveletekkel, résztestként tartalmazza $\mathbb{Q}$-t és részteste $\mathbb{R}$-nek. Mivel az 1. Tételben F elemei is racionális számok voltak, így p nem is lehet más, mint algebrai. A „p szimulálja q-t" reláció definíciója miatt ha $p, q \in [0,1]$ és p szimulálja q-t, akkor $f(p) = q$ valamilyen egész együtthatójú polinomra, vagyis ha p és q valamelyike algebrai szám, akkor a másik sem lehet más. Általában még az is igaz: ha $p, q \in [0,1]$ és p szimulálja q-t akkor $\mathbb{Q}[p] = \mathbb{Q}[q]$, ahol tetszőleges $z \in \mathbb{R}$ valós számra

$$\mathbb{Q}[z] = \{r \in \mathbb{R} \mid r \text{ algebrai } \mathbb{Q}(z) \text{ felett}\}$$

és

$\mathbb{Q}(z) = \mathbb{R}$ legkisebb azon részteste, mely tartalmazza $\mathbb{Q} - t$ és $z - t$.

Ebből az is következik, hogy ha p szimulálja valamely $F \subseteq [0,1]$ halmaz elemeit, akkor $F \setminus \{0,1\}$ minden q elemére $\mathbb{Q}[p] = \mathbb{Q}[q]$ feltétlenül teljesül. Vagyis tetszőleges $F \subseteq [0,1]$ halmaz elemeit csak akkor lehet egyetlen p valószínűséggel szimulálni, ha $F \setminus \{0,1\}$ minden q, r elemeire $\mathbb{Q}[q] = \mathbb{Q}[r]$. Nem tudjuk azonban, hogy a fenti feltétel elegendő-e. Például azt sem tudjuk, hogy $\frac{1}{\sqrt{2}}$ és $\frac{1}{\sqrt{3}}$, vagy pl. $\frac{1}{e}$ és $\frac{1}{e+1}$ szimulálhatók-e egyszerre.

Mely $F \subseteq [0,1]$ halmazok elemeit lehet egyetlen p valószínűséggel szimulálni? Tételeink erre nem adnak általában teljes választ.

Pontosabban, $\mathbb{R}$ tetszőleges részhalmazaira ugyan nem tudjuk a választ, azonban ha csak racionális számokra szorítkozunk, akkor pontosan le tudjuk írni azon $F \subseteq \mathbb{Q}$ részhalmazokat, melyeket egy (tetszőleges valós) szám szimulál. Eredményünk az alább következő két Tételből fog következni. Mindezekhez két jelölésre lesz szükségünk.

Ha $N \in \mathbb{N}$ tetszőleges természetes szám, akkor jelölje $\mathbb{Q}_N$ azon racionális számok halmazát, melyek nevezői N-nek hatványai, azaz legyen

$$Q_N := \left\{ \frac{j}{N^k} : j, k \in \mathbb{Z} \right\} \qquad (N \in \mathbb{N})$$

Jelölje továbbá $\mathbb{S}_p$ a p által szimulált számok halmazát, azaz legyen

$$S_p := \{q \in [0,1] : p \text{ szimulálja } q - t\} \qquad (p \in [0,1])$$

5. TÉTEL *Legyen $p \in [0,1]$ tetszőleges. Ekkor $S_p \cap \mathbf{Q} \subseteq Q_N$ valamilyen $N \in \mathbf{N}$ számra.*

BIZONYÍTÁS: A bizonyítás alapötlete Martin Goldsterntől származik.

Ha p nem algebrai, akkor, mint már észrevettük, $S_p \cap \mathbf{Q} = \{0,1\}$, vagyis a Tétel állítása nyilvánvalóan teljesül.

Tehát p algebrai. Legyen

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

egy olyan minimális fokú egész együtthatós polinom (nem azonosan nulla), melynek p gyöke, és $a_n > 0$. Megmutatjuk, hogy $S_p \cap \mathbf{Q} \subseteq Q_{an}$.
0 és 1 nyilván elemei Q_{an}-nek. Legyen tehát $q \in S_p \cap \mathbf{Q} \setminus \{0,1\}$. Mivel p szimulálja q-t, ezért $q = g(p)$ valamely

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

egész együtthatós polinomra. Ekkor $g(p) - q = 0$, de mivel $f(x)$ minimális fokú polinom volt, ezért $f(x)$ osztója $g(x) - q$-nak, azaz

$$(*) \qquad g(x) - q = f(x) \cdot h(x),$$

ahol

$$h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$$

egy racionális együtthatós polinom. A (*) egyenlet a polinomok fokszámaira és együtthatóira a következő egyenletrendszert jelenti:

$$\begin{aligned}
m &= n + k \\
b_m &= a_n \cdot c_k \\
b_{m-1} &= a_n \cdot c_{k-1} + a_{n-1} \cdot c_k \\
b_{m-2} &= a_n \cdot c_{k-2} + a_{n-1} \cdot c_{k-1} + a_{n-2} \cdot c_k \\
&\cdots \\
b_1 &= a_1 \cdot c_o + a_o \cdot c_1 \\
b_o - q &= a_o \cdot c_o
\end{aligned}$$

ÁLLÍTÁS: $(a_n)^{i+1} \cdot c_{k-i}$ mindig egész szám, ha $i = 0, 1, \ldots, k$.
BIZONYÍTÁS: i-re vonatkozó indukcióval. Az $i = 0$ esetet a fenti második egyenlőség igazolja. Más i index esetén pedig induljunk ki a

$$b_{m-i} = a_n \cdot c_{k-1} + a_{n-1} \cdot c_{k-i+1} + a_{n-2} \cdot c_{k-1+2} + \cdots$$

egyenlőségből. Mindkét oldalt $(a_n)^i$-vel szorozva kapjuk, hogy

$$(a_n)^i \cdot b_{m-i} = (a_n)^{i+1} \cdot c_{k-i} + (a_n)^i \cdot a_{n-1} \cdot c_{k-i+1} + (a_n)^i \cdot a_{n-2} \cdot c_{k-1+2} + \cdots .$$

Az egyenlőség bal oldala egész szám, és az indukciós feltétel szerint a bal oldal mindegyik tagja is egész, az első kivételével, így az első tag is egész szám. Ez bizonyítja állításunkat.

Az állítás szerint $(i = k)$ $j = (a_n)^{k+1} \cdot c_0$ egész szám, de így a $b_0 - q = a_0 \cdot c_0$ egyenlőség miatt

$$q = b_0 - a_0 \cdot j/(a_n)^{k+1} \in Q_{an},$$

mint állítottuk. ■

6. TÉTEL *Minden $N \in \mathbf{N}$ természetes számhoz van olyan $p \in [0,1]$ valós szám, amelyre $S_p \cap \mathbf{Q} \supseteq Q_N \cap [0,1]$.*

BIZONYÍTÁS: Legyen $N \in \mathbf{N}$ adott. Az 1. Tétel szerint van olyan $p \in [0,1]$, mely szimulálja az $\frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{N}, \frac{2}{N}, \ldots, \frac{N-1}{N}$ számokat. Megmutatjuk, hogy p szimulálja $Q_N \cap [0,1]$ minden elemét, azaz p szimulál minden N^k nevezőjű törtet.

k-ra vonatkozó teljes indukcióval bizonyítunk. A $k = 1$ esetet p választása igazolja. Az indukciós lépéshez legyen k rögzített, és tegyük fel, hogy p szimulál minden N^k nevezőjű törtet, és legyen $j < N^{k+1}$. Megmutatjuk, hogy p szimulálja a j/N^{k+1} törtet is. Osszuk el j-t maradékosan N^k-val, azaz legyen $j = qN^k + r$, $0 \le q < N$ és $0 \le r < N^k$.
Az indukciós feltétel és p választása miatt p szimulálja az $x = \frac{q}{N}$, $\frac{1}{N-q}$ és az $\frac{r}{N^k}$ racionális számokat, és a két utolsó szorzatát, $z = \frac{1}{N-q} \cdot \frac{r}{N^k}$ számot is. Ha $y = 1$, akkor a bevezetőben említett @ tulajdonság miatt p szimulálja a

$$\frac{q}{N} + \left(1 - \frac{q}{N}\right) \cdot \frac{r}{(N-q)N^k} = \frac{q}{N} + \frac{r}{N^{k+1}} \frac{qN^k + r}{N^{k+1}} = \frac{j}{N^{k+1}}$$

számot is, mint állítottuk. ■

A fenti két Tételt összevetve szükséges és elégséges feltételt kapunk arra, hogy racionális számok mely részhalmazai szimulálhatók egyetlen $p \in [0,1]$ valós számmal:

7. KÖVETKEZMÉNY Tetszőleges $F \subseteq \mathbf{Q} \cap [0,1]$ részhalmazhoz pontosan akkor létezik egy $p \in [0,1]$ szám, mely F minden elemét szimulálja, ha

valamilyen $N \in \mathbb{N}$ természetes számra F minden elemének nevezője N-nek hatványa, azaz $F \subseteq Q_N$. ■

Most részletesebben megvizsgáljuk, hogy a bizonyításainkban felhasznált p számok milyen racionális számokat szimulálnak. Legyen $N \geq 4$ pozitív egész, $n = N!/3$ és legyen p az $np(1-p)^{n-1} = \frac{1}{3}$ egyenlet megoldása. Az 1. Tétel bizonyításában láttuk, hogy p szimulálja az összes, N-nél nem nagyobb nevezőjű törtet. (Valójában ez $N = 3$ esetén is igaz, mint cikkünk bevezetőjében írtuk.) A 6. Tétel bizonyításában láttuk, hogy ekkor p $Q_N \cap [0,1]$ elemeit is szimulálja. Sőt, az érvelést továbbfejlesztve az is belátható, hogy $Q_{N!} \cap [0,1]$ elemeit is szimulálja p. Ez következik az alábbi Állításból:

8. ÁLLÍTÁS: Legyenek p és N mint fent, M és k pozitív egészek, $2 \leq k \leq N$, és tegyük fel, hogy p szimulálja az összes j/M alakú törtet, ha $0 < j < M$. Ekkor p a j/Mk alakú törteket is szimulálja minden $0 < j < Mk$ esetén.

BIZONYÍTÁS: Legyen $0 < j < Mk$. Osszuk el j-t maradékosan M-el, azaz legyen $j = Mq + r$, $0 \leq q < k$ és $0 \leq r < M$. A feltétel szerint p szimulálja a $\frac{q}{k}$, $\frac{1}{k-q}$ és az $\frac{r}{M}$ racionális számokat. Mint a 6. Tétel bizonyításában láttuk, p szimulálja a

$$\frac{q}{k} + \left(1 - \frac{q}{k}\right) \cdot \frac{1}{k-q} \cdot \frac{r}{M} = \frac{Mq + r}{Mk} = \frac{j}{Mk}$$

számot is, mint állítottuk. ■

Az 5. Tétel bizonyítását alaposabban megvizsgálva a következőket mondhatjuk: p nyilván algebrai, hiszen a $g(x) = 3nx(1-x)^{n-1} - 1 = N!x(1-x)^{n-1} - 1$ egyenlet gyöke. Legyen $f(x)$ olyan minimális fokú (nem azonosan nulla) egész együtthatós polinom, melynek p gyöke, és legyen f főegyütthatója a. Az 5. Tétel bizonyításakor láttuk, hogy p csak a $Q_a \cap [0,1]$ halmazban levő racionális számokat szimulálja.

Mit tudunk mondani a értékéről?

Egy egész együtthatós polinom együtthatóinak legnagyobb közös osztóját nevezzük a polinom **tartalmának**, és nevezzünk egy polinomot primitívnek, ha tartalma 1. Az ún. *Gauss Lemma* szerint (pl.[Fr] 100. old. 3.39 Tétel) primitív polinomok szorzata is primitív polinom.

$g(x)$ polinomunk nyilván primitív, hiszen konstans tagja -1, és $f(x)$-ről is feltehetjük, hogy primitív. Mivel $f(x)$ minimális fokszámú, ezért $g(x)$-nek osztója, azaz $g(x) = f(x) \cdot h(x)$ valamilyen $h(x)$ racionális együtthatójú polinomra. Hozzuk $h(x)$ együtthatóit közös nevezőre, majd emeljük ki a

számlálók legnagyobb közös osztóját, ekkor $h(x)$-et $\frac{j}{k}h^*(x)$ alakban írhatjuk, ahol $h^*(x)$ primitív egész együtthatós polinom. Ekkor $K \cdot g(x) = j \cdot f(x) \cdot h^*(x)$. A bal oldal tartalma k, a jobb oldalé j a Gauss Lemma alapján, vagyis $j = k$, így $h(x) = h^*(x)$. Ebből következik, hogy $h(x)$ egész együtthatós primitív polinom. Továbbá, $g(x)$ főegyütthatója $\pm N!$, és $g(x) = f(x) \cdot h(x)$, így $a \mid N!$ amiből $Q_a \subseteq Q_{N!}$ következik. Mivel tudjuk, hogy p szimulálja $Q_{N!} \cap [0,1]$ minden elemét, és p csak a $Q_a \cap [0,1]$ halmazban levő racionális számokat szimulálja, ezért

$$S_p \cap \mathbb{Q} = Q_{N!} \cap [0,1]$$

Például, $N = 3$ esetén kapjuk, hogy a bevezetőben említett $p = \frac{3+\sqrt{3}}{6}$ szám által szimulált racionális számok halmaza pontosan $Q_6 \cap [0,1]$.

Az 5. Tételt könnyen általánosíthatjuk $\mathbb{Q}$ helyett $\mathbb{Q}z$-re is, ahol $z \in \mathbb{R}$ tetszőleges valós szám, és

$$\mathbb{Q}z := \{qz \mid q \in \mathbb{Q}\}$$

9. TÉTEL . *Legyenek $z \in \mathbb{R}$ és $p \in [0,1]$ tetszőlegesek, $z \neq 0$. Ekkor van olyan $N \in \mathbb{N}$ természetes szám, amelyre $S_p \cap \mathbb{Q}_N z \subseteq (Q_n z) \cap [0,1]$, ahol $Q_N z = \{qz \mid q \in Q_N\}$.*

BIZONYÍTÁS: (I) Legyen először z transzcendens, azaz nem algebrai. Ha p z-nek egyetlen nemnulla többszörösét sem szimulálja, akkor nincs mit bizonyítanunk. Tegyük fel tehát, hogy p szimulálja z-nek valamely nemnulla többszörösét. Ekkor p algebrai $\mathbb{Q}(z)$ felett ($\mathbb{Q}(z)$-vel jelöljük a $\mathbb{Q}$ számtest z számmal való transzcendens bővítését), ezért van egy minimális fokú $f(x)$ polinom, melynek együtthatói $\mathbb{Q}(z)$-ből valók, és melynek p gyöke. $f(x)$ együtthatói z-nek racionális együtthatós törtfüggvényei[2] de a nevezők közös többszöröseivel bővítve feltehetjük, hogy $f(x)$ egész együtthatójú polinom. Azaz

$$f(x) = a_n(z)x^n + a_{n-1}(z)x^{n-1} + \cdots + a_0(z)$$

ahol $a_i(z)$ egész együtthatós polinomok ha $i = 0, 1, \ldots, n$. Legyen $a_n(z)$ főegyütthatója N, $f(x)$-et esetleg -1-gyel beszorozva feltehetjük, hogy N pozitív. Megmutatjuk, hogy $S_p \cap \mathbb{Q}z \subseteq Q_N z$.

[2] Racionális törtfüggvénynek nevezzük két polinom hányadosát. Tehát $f(x)$ együtthatói racionális együtthatójú polinomok hányadosai.

Legyen tehát $q \in \mathbb{Q}$, $q \neq 0$ olyan, hogy p szimulálja qz-t. Valamely

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + b \cdots + b_1 x + b_0$$

nemnulla egész együtthatós polinomra $qz = g(p)$, azaz $g(p) - qz = 0$. Ekkor $f(x)$ minimális fokszáma miatt $g(x) - qz$ osztható $f(x)$-szel, vagyis

$$g(x) - qz = f(x) \cdot h(x)$$

valamely $h(x)$ polinomra, melynek együtthatói $\mathbf{Q}z$-nek elemei. Azaz $h(x)$ együtthatói z-nek racionális együtthatójú racionális törtfüggvényei, vagyis

$$h(x) = c_n(z)x^n + c_{n-1}(z)x^{n-1} + \cdots + c_0(z)$$

ahol $c_i(z)$ racionális együtthatójú racionális törtfüggvények, $i = 0, 1, \ldots, n$. Az 5. Tétel bizonyításához hasonlóan az alábbi Állítást látjuk be:

9. ÁLLÍTÁS: Minden $i = 0, 1, \ldots, k$ esetén $(a_n(z))^{i+1} \cdot c_{k-i}(z) = d_i(z)$ teljesül valamely egész együtthatós $d_i(x)$ polinomra.

BIZONYÍTÁS: i-re vonatkozó teljes indukcióval. $i = 0$ esetén a $a_n(z)c_k(z) = b_m$, ami egész szám, vagyis $d_0(z) = b_m$ konstans polinom. Az indukciós lépéshez használjuk fel a

$$b_{m-i} = a_n(z) \cdot c_{k-i}(z) + a_{n-1}(z) \cdot c_{k-i+1}(z) + \cdots$$

egyenlőséget. Mindkét oldalt $(a_n(z))^i$-vel szorozva kapjuk:

$$(a_n(z))^i \cdot b_{m-i} = (a_n(z))^{i+1} \cdot c_{k-i}(z) + (a_n(z))^i \cdot a_{n-i}(z) \cdot c_{k-i+1}(z) + \cdots$$

amiből az állítás az indukciós feltétel miatt következik. ■

Mivel $g(x) - qz = f(x) \cdot h(x)$, így $b_0 - qz = a_0(z) \cdot c_0(z)$ Ha mindkét oldalt $(a_n(z))^{k+1}$-vel beszorozzuk, az Állítás $i = k$ esetét alkalmazva kapjuk: $(a_n(z))^{k+1} \cdot (b_0 - qz) = a_0(z) \cdot (a_n(z))^{k+1} \cdot c_0(z) = a_0(z) \cdot d_k(z)$.
Így

$$b_0 \cdot (a_n(z))^{k+1} - qz \cdot (a_n(z))^{k+1} - a_0(z) \cdot d_k(z) = 0$$

De z transzcendens lévén a bal oldali polinom azonosan 0 kell hogy legyen (e ponton használjuk csak fel z transzcendens voltát).
Mivel pedig b_0 egész szám, szintúgy az $a_n(x)$, $a_0(x)$ és a $d_k(x)$ polinomok is egész együtthatósak, ezért a $q \cdot x \cdot (a_n(x))^{k+1}$ polinom együtthatói is szükségképpen egész számok. Speciálisan a főegyüttható, qN^{k+1} is egész szám, vagyis $q \in \mathbb{Q}_N$, ami bizonyítja Tételünket.

(II) Már csak azon eset maradt hátra, mikor z algebrai, de nem racionális (a racionális eset éppen az 5. Tétel). Ez esetben Greg Call segített át minket a holtponton. Legyen tehát

$$j(x) = d_r x^r + d_{r-1}x^{r-1} + \cdots + d_0$$

olyan egész együtthatós nemnulla polinom, melynek z gyöke. Mint az (I) esetben, ha p z-nek egyetlen nemnulla többszörösét sem szimulálja, akkor nincs mit bizonyítanunk. Ha pedig igen,akkor,mint a bevezetőben láttuk, p is algebrai. Legyen tehát

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

p minimálpolinomja, azaz egy olyan minimális fokszámú nemnulla, egész együtthatós polinom, melynek p gyöke. Megmutatjuk, hogy ez esetben $N = d_0 a_n$ igazolja a Tétel állítását ($z \neq 0$ miatt $d_0 \neq 0$). Mint eddig, feltehetjük, hogy d_0 és a_n mindegyike pozitív.

Legyen $q \in \mathbb{Q}$, $q \neq 0$ olyan, hogy p szimulálja qz-t. Ekkor $g(p) = qz$ valamely egész együtthatós nemkonstans $g(x)$ polinomra. Így $z = g(p)/q$, és $j(z) = 0$ miatt kapjuk:

$$0 = q^r \cdot j\left(\frac{g(p)}{q}\right) = d_r \cdot (g(p))^r + q \cdot d_{r-1} \cdot (g(p))^{r-1} + \cdots + q^r \cdot d_0.$$

Legyen most $q = \frac{s}{t}$ ahol s és t relatív prímek. A fenti egyenlőség mindkét oldalát t^{r-1}-el szorozva az alábbit kapjuk:

$$0 = t^r \cdot d_r \cdot (g(p))^r + s \cdot t^{r-1} \cdot d_{r-1} \cdot (g(p))^{r-1} + \cdots + s^r \cdot d_0/t$$

ami azt jelenti, hogy p gyöke valamely egész együtthatós (az utolsó tag kivételével) $u(x)$ polinomnak. Pontosabban:

$$u(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + \frac{s^r d_0}{t}$$

ahol b_i mind egész számok. Mivel $f(x)$ minimális fokszámú polinom, melynek p gyöke, ezért $u(x)$ osztható $f(x)$-el, azaz $u(x) = f(x) \cdot h(x)$ valamely racionális együtthatójú

$$h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_0$$

polinomra. Az 5. Tétel bizonyításában szereplő Állítás most is ugyanúgy igazolható, mint az 5. Tételben. Így találunk olyan e egész számot, amelyre $c_o = e/(a_n)^{k+1}$. Ezért

$$b_0 + \frac{s^r d_o}{t} = a_0 c_0 = \frac{e a_o}{(a_n)^{k+1}}$$

amiből $t(ea_0 - b_0(a)^{k+1}) = s^r d_0 (a_n)^{k+1}$ következik. Így t osztója a baloldali mennyiségnek, de mivel t és s relatív prímek, ezért $t \mid d_0(a_n)^{k+1}$, amiből $t \mid N^{k+1}$ következik, hiszen $N = d_0 a_n$. Így $q = s/t \in Q_N$. ■

Mint említettük, sok megoldatlan kérdésre nem ismerjük a választ, ha irracionális számokat akarunk szimultán szimulálni. Például szimulálható-e két tetszőleges $[0,1]$-beli algebrai szám egyszerre? Még az $1/\sqrt{2}$, $1/\sqrt{3}$ pár esetén sem tudjuk a választ!

Végezetül megemlítjük a probléma általánosítását három- és több- oldalú érmék esetére. Egy k-oldalú érme $p_1, p_2, \ldots, p_k$ valószínűségekkel esik oldalaira, ahol természetesen $0 < p_i < 1$ és $p_1 + p_2 + \cdots + p_k = 1$. Az Olvasóra bízzuk annak definiálását, hogy egy $(p_1, p_2, \ldots, p_k)$-érme mikor szimulál egy $(q_1, q_2, \ldots, q_k)$-érmét. Az 1. Tétel szerint ha a $p_1, p_2, \ldots, p_k$ számok mindegyike racionális, akkor a $(p_1, p_2, \ldots, p_k)$-érme szimulálható egy kétoldalú érmével. A következő feladat megoldását az Olvasóra bízzuk. Nem nehéz belátni, hogy ha p szimulálja $\frac{1}{2}$-et és $\frac{1}{3}$-ot, akkor az $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ háromoldalú érmét is szimulálja. (Pl. a bevezetőben említett $p = \frac{3+\sqrt{3}}{6}$.) Továbbá az is könnyen belátható, hogy ha p szimulálja az $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ háromoldalú érmét, akkor az $\frac{1}{3}$ valószínűséghez tartozó kétoldalú érmét is. A feladat: találjunk olyan $p \in [0,1]$ számot, amelyhez tartozó kétoldalú érme szimulálja az $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ háromoldalú érmét, de nem szimulálja az $\frac{1}{2}$ valószínűséghez tartozó kétoldalú érmét!

A dolgozatunkban tárgyalt problémát már [SzV]-ben is tárgyaltuk, megoldatlan problémáinkat [Sz1]-ben és [Sz2]-ben is terjesztettük. Hasonló érdekes témákról olvashatunk még a [P1], [P2] cikkekben, sőt [CV]-ben kimerítően körüljárják a szerzők a jelen cikkünkben (lényegében) központi szerepet játszó

$$\sum_{i=0}^{n} a_i p^i (1-p)^{n-i},$$

alakú polinomokat. (Sajnos ott sem találnak a szerzők olyan valószínűséget, mely egyszerre szimulálná az $1/\sqrt{2}$ és $1/\sqrt{3}$ számokat!)

Irodalom

[CV] Call, G. S., Velleman, D. J., *Pascal's Matrices*, Amer. Math. Monthly **100** (1193), 217–256.

[Fr] Fried Ervin, *Klasszikus és Lineáris Algebra*, Tankönyvkiadó, Budapest 1977.

[P1] Pinch, R. G. E., *Binomial Equivalence of Algebraic Integers*, J. of the Indian Math. Soc. **58** (1992), 33–38.

[P2] Pinch, R. G. E., *a-Convexity*, Math. Proc. Cambridge Phil. Soc. **97** (1985), 63–68.

[Sz1] Szalkai István, *Probléma*, jelen folyóirat, 1991/4, 18. old.

[Sz2] Szalkai István, *Problem*, in Combinatorics: Paul Erdős is eighty, International Conf. in Keszthely, 1993, Coll. Math. Soc. J. Bolyai, megjelenőben.

[SzV] Szalkai, I., Velleman, D. J., *Versatile Coins*, Amer. Math. Monthly, **100** (1993), 26–33.

VERSATILE COINS

I. SZALKAI and D. VELLEMAN

Imagine a coin which, when flipped, comes up heads with probability $\frac{3+\sqrt{3}}{6}$. Flipping it three times, the probability of getting either three heads or three tails would be $1/2$, while flipping it twice the probability of getting one head and one tail would be exactly $1/3$. We say that this funny coin *simulates* both the coins with probabilities of heads $1/2$ and $1/3$. In general we say that p *simulates* q if there is some positive integer n and positive numbers $0 \le a_i \le \binom{n}{i}$ for $i = 0, \ldots, n$ such that

$$q = \sum_{i=0}^{n} a_i p^i (1-p)^{n-i}.$$

The main results of the present paper are:

THEOREM 1. *Suppose F is a finite set of rational numbers and $F \subseteq [0,1]$. Then ther is a (sungle) number $p \in [0,1]$ such that p simulates every element of F.*

THEOREM 4. *Suppose $F \subseteq [0,1]$, F is finite, and the ratio of any two nonzero elements of F is rational. Then there is a (single) number $p \in [0,1]$ such that p simulates every element of F.*

COROLLARY 7. *Suppose* $F \subseteq \mathbb{Q} \cap [0,1]$. *Then there is a (single) number* $p \in [0,1]$ *such that* p *simulates every element of* F *iff for some positive integer* N, *all the denominatots of the elements of* F *are powers of* N.

There are still many unanswered questions. E.g. *if* q *and* r *are algebraic numbers between 0 and 1, must there be a number* $p \in [0,1]$ *such that* p *simulates both* q *and* r? For example, $1/\sqrt{2}$ and $1/\sqrt{3}$ can be simulated by a single p, or the two numbers $\frac{1}{e}$ and $\frac{1}{e+1}$?