Számítógépek és híradástechnika: az emberiség új kommunikációs korszaka
II. Rész: Matematikai háttér

3. Matematikai feladatok

Első matematikai feladatként nézzük a lehetséges üzenetek és a lehetséges csatornajel-sorozatok közötti megfeleltetés problémáját a Shannon modellben. Az alapfeladat egyszerűen megfogalmazható: különböző üzenetnek különböző jelsorozatot kell megfeleltetni. A skatulyaelv azt mondja ki, hogy ha kevesebb skatulya van, mint golyó, akkor van olyan skatulya, amelyben egynél több golyó van. Ezért tehát legalább annyi csatornajel-sorozat szükséges, mint amennyi üzenet lehetséges.

Kezdjük a csatorna mennyiségi jellemzésével.

A csatorna *C* kapacitását a *T* időhosszúságú (megkülönböztethető) jelsorozatok számának, *N(T)*-nek segítségével definiáljuk:

$$C = \lim_{T\to\infty} \frac{\log_2 N(T)}{T} \quad .$$

Ha két csatornára *N(T)* megegyezik, akkor a két csatorna helyettesíthető egymással, ekvivalensek. A legegyszerűbb csatorna a szimmetrikus bináris csatorna. Két jel vihető át, mondjuk 0 és 1, és minden jel ugyanolyan hosszú (időben). A csatorna kapacitás, C, erre a csatornára pontosan azt jelenti, hogy egységnyi idő alatt C jel, vagyis C bit vihető át. Ez magyarázza, hogy a kapacitás mérőszámának dimenziója bit/sec.

Nehezebb kérdés matematikailag a forrás választási lehetőségeinek számát meghatározni. A Shannon entrópia nem is ezt méri közvetlenül, hanem a választás bizonytalanságát, vagyis, hogy a lehetséges üzenetekből milyen bizonytalansággal történik a választás. A választás véletlenségét valószínűség-eloszlással jellemezzük, ami matematikai modellel való közelítés. A bizonytalanság mérőszámát megadó függvény természetes elvárásokat kielégítően került meghatározásra. A folytonosságra, az egyenletes eloszlásokon való monotonitásra és a megfigyelés lépcsőzésére tett feltevések alapján felírt függvényegyenlet megoldásaként adódik a Shannon entrópiaformula:

$\mathrm{A}\{p_1, p_2, ..., p_n\}$ valószínűségeloszlás entrópiája

$$\mathrm{H}(p_1, p_2, ..., p_n) = -\sum_{i=1}^{n} p_i \log_2 p_i \, .$$

A forrás entrópiáját úgy határozzuk meg, hogy igen hosszú üzeneteket tekintünk. A hosszú üzenet választásának eloszlására meghatározzuk az entrópiát, és osztjuk az üzenet hosszával. Általános estben az üzenet hosszával végtelenhez tartva határértékként kapjuk az üzenet elemi részeire, szimbólumaira az átlagos entrópiát, *H*-t. Az *L* hosszú, *L* szimbólumból álló üzenet entrópiája ekkor $L(H\pm\gamma)$ lesz. Amennyiben a forrás működésének sebessége *V* szimbólum/sec, akkor *T* idő alatt a forráshoz $TV(H\pm\gamma)$ entrópia rendelhető.

Az előkészítés után nézzük a skatulyák és golyók számát. A formulákban a görög betűk az idő igen nagynak választásával tetszőlegesen kicsivé tehető mennyiségek.

A *C* kapacitású csatorna *T* idő alatt

$$2^{T(C-\delta)} \le N(T) \le 2^{T(C+\delta)}$$

számú különböző jelsorozatot képes átvinni, ennyi a dobozok száma.

Hogyan lehet az entrópiából a választható üzenetek számára következtetni? Az igen hosszú véletlen jelenségekre igen általános feltevés (ergodikusság) mellett az jellemző, hogy közel 1 valószínűséggel egy tipikus halmazba esik a jelenség előfordulása. A tipikus halmaz elemeinek valószínűségére valószínűség-számítási törvények alapján alsó és felső becslés adható, és az bizonyítható, hogy közel egyenletesen oszlanak el a választási lehetőségek a tipikus halmazon. A tipikus halmaz, vagyis a meghatározó többség *M(VT)* számosságára *V* sebesség és *T* idő esetén a valószínűségekre kapott becslés reciprokjaként a

$$2^{TV(H-\lambda)} \le M(VT) \le 2^{TV(H+\lambda)}$$

egyenlőtlenség teljesül. Így kaptuk meg tehát a golyók számát.

A skatulyaelvből kapjuk a csatorna alaptételét, amely szerint tetszőleges
ε > 0 **választáshoz** ***V < C/H − ε***
sebesség esetében lehetséges miden különböző T idejű tipikus üzenetet különböző T hosszú jelsorozattal kódolni, azaz lehetséges az adást veszteségmentesen működtetni. Nem lehet azonban *V>C/H* sebesség esetén veszteségmentesen továbbítani minden üzenetet.

A kommunikáció fenti alapvető matematikai törvényszerűsége megadja adott csatorna esetében a kommunikáció lehetőségeit és korlátjait, de nem ad közvetlen segítséget a megoldáshoz. Az entrópia-formula független az eloszlás permutációjától, és nem függ az üzenet szimbólumkészletétől sem. Konkrét forrás kódolása esetében mindkét információnak rendelkezésre kell állnia mind a forrás kódoló-adó oldalán, mind a rendeltetési hely vevő-dekódoló oldalán. Adattárolási és számítási kapacitás nélkül (kivéve az analóg esetet) az új típusú csatornák nem lennének használhatók.

A vázolt blokkséma csatornadoboza a jel tér- és időbeli terjedését jelentő közeget ábrázolja, és magában foglalja a terjedés közben bekövetkező torzulásokat, a zajt is.

A matematikai elmélet egyik fontos összetevője a forrás bizonytalanságának mérőszámaként bevezetett entrópia, ami egyben az optimális kód hosszának várható értékére ad alsó korlátot. Ugyanez a mérőszám alkalmas a zaj, és a titkosítás kérdéseinek vizsgálatára is.

Shannon [1] alapművében nem különbözteti meg élesen a kódoló-adó és a vevő-dekódoló kettős funkcióját. A digitális adatátvitelben ezek már élesebben szétválnak, a kódolás és dekódolás algoritmikus feladata önállósulhat. Az információelmélet központi feladata pedig a véletlen jellegű zaj kezelésére, az adás és a vétel együttesen hatékony megoldására, a nagy csatornakapacitás, vagy más jellemzővel, a nagy sávszélesség elérésére irányul. A forrás jó kódolása nem a csatorna kapacitásának biztosítása, hanem jó kihasználása szempontjából fontos. Elméletben függetlenné tehető a két feladat. A forrást kódolhatjuk a lehető legtömörebben bináris jelsorozattá, és a csatornajeleket elegendő ez után csak a független, azonos eloszlású, két egyforma valószínűségű lehetőségből álló forráshoz (szimmetrikus Bernoulli eloszlás) illeszteni.

A vázolt gondolatmenet alapján látható, hogy a csatorna jó kihasználásához a forrás üzenetét hosszú időszakaszonként blokkolva kellene továbbítani, ami jelentős késleltetést okozhat. A nagy teljesítményű csatornák messze meghaladják az emberi üzenet-kibocsátás által igényelt teljesítményt. Az időbeli összegyűjtés és blokk-kódolás helyett a hasonló hatást biztosító térbeli összegyűjtést, azaz több forrás üzenetének párhuzamos továbbítását lehet alkalmazni.

A közeli jövő lehetőségeinek érzékeltetésére próbáljuk elképzelni, mit jelent a 2008-ra jósolt 1Terabit/sec, azaz 10^{12} bit/sec kapacitású Ethernet csatorna. A Föld akkori lakosságát

10 milliárd, azaz 10^{10} embernek véve, 128 billentyűs klaviatúrát használva másodpercenként mindenki írhatna folyamatosan 14 leütésből álló szöveget, és ez egyszerre átvihető lenne ezen a csatornán.

A forrás (jövőbeli) véletlenségét matematikai idealizált modellel közelítjük. A valós szituációt egy bizonytalanabb, nagyobb entrópiájú matematikai jelenséggel, sztochasztikus folyamattal helyettesítjük. A valós forrás tipikus kimenetei ezért részhalmazát képezik a matematikai modelljében kapott tipikus véletlen halmaznak, amennyiben jól modelleztük a forrást.

A Shannon modell leegyszerűsített, elemi bemutatása után térjünk át múlt megértésével, jellemzésével összefüggő kérdéskörre, ami a felhalmozott adat- és ismeretkészlet elemzéséhez ad matematikai hátteret.

A nagyon hosszú vagy kiterjedt, konkrétan előforduló folyamatot (realizációt) önmagában is nézhetjük, eloszlás nélkül, tömöríthetőség szempontjából.

Ez átvezet az algoritmikus jellemzés világába, a nagy adatállományok tömörítésének kérdéseihez, ami a második matematikai feladatköre a dolgozatnak.

A Kolmogorov bonyolultság elméletköre a 60-as évek elején fejlődött ki elsősorban Kolmogorov iskolájában, de attól függetlenül és szinte egyidőben R. Solomonoff és Chaitin munkássága alapján. A kiindulási kérdések sorában a véletlenszám-generátorok jóságának ellenőrzése, a véletlen jelenségek algoritmikus jellemzése, az univerzális számítógépi tanulási algoritmus a leglényegesebbek. Kolmogorov az elmélet indulását jelentő [2] dolgozatában a következő kérdést tette fel: milyen rövid kód lenne elegendő ahhoz, hogy a „Háború és béke" teljes szövegét abból egy számítógép előállítsa? Mondhatná valaki, hogy tud definiálni olyan függvényt, amely a 0 kódhoz a „Háború és béke" teljes szövegét rendeli. Ekkor azonban a vevő oldalra ennek a függvénynek egy programkódját át kell küldenie, s a program kódja valószínűleg adatként tartalmazná a regény valamennyire tömörített szövegét. Az is igaz, hogy ha már egyszer ott van a rendeltetési hely vevőjében ez a programkód, akkor elég a 0 üzenet és a program azonosítójának küldése a regény helyett. (Gondoljunk vissza az I. részből a 7. ábra adattároló elemeire.)

Alapvető feltétele egy kód használatának, hogy ismerjük és ki tudjuk számítani azt a függvényt, amivel a dekódolást elvégezhetjük. Azt is mondhatjuk, hogy a kód és a dekódoló program kódjának ismerete kell együttesen a dekódoláshoz. A két kód együttes hosszának minimuma jelenti a tömöríthetőség alsó határát. Ez az intuitív alapja a Kolmogorov bonyolultságnak, amit a következőkben vázlatosan ismertetünk.

Először egy tetszőleges kiszámítható (parciális rekurzív, Turing kiszámítható) függvény szerint definiáljuk egy nem negatív egész szám, vagy egy véges bináris szó bonyolultságát. (A nem negatív egész számok és a véges bináris szavak közötti kölcsönösen egyértelmű megfeleltetést használva egy egész számot és a neki megfeleltetett véges bináris szót azonosnak tekintjük. A kiszámítható függvények többsége parciális függvény, ami azt jelenti, hogy bizonyos helyeken nincsenek meghatározva, mert ott a kiszámításuk végtelen ciklusba esik.)

Definíció. Az x nem negatív egész számnak az $f(p)$ kiszámítható függvény szerinti bonyolultságán a

$$C_f(x) = \min\langle l(p) \,|\, f(p) = x \rangle,$$

értéket értjük, amennyiben létezik x-nek ilyen f szerinti p kódja, és végtelen a bonyolultság, ha ilyen kód nem létezik. Az $l(p)$ függvény a p kód hosszát adja.■

Az elmélet alaptétele, amelyet a három említett matematikus egymástól függetlenül, szinte egy időben talált meg, optimális kódoló létezését mondja ki:

Tétel: Létezik olyan optimális kiszámítható függvény, $f_0(p)$, hogy bármely $f(p)$ kiszámítható függvényre és x egész számra

$$C_{f_0}(x) \le C_f(x) + k_f \ ,$$

ahol k_f csak f-től függő konstans. ■

(A bizonyítás az univerzális kétváltozós függvény létezésére alapul. Létezik olyan *U(n,p)* kiszámítható függvény, amelyre minden f*(p)* kiszámítható függvényhez létezik n_f, hogy $U(n_f,p)=f(p)$. Az (n_f,p) rendezett pár alkalmas kódjából és az univerzális függvényből tudjuk az optimális kódoló függvényt megkonstruálni. Az optimális kódoló a dekódoló program és a hozzátartozó kód együttes hosszára adja a minimumot.)

Definíció. Látható, hogy az optimális függvények szerinti bonyolultság csak konstanssal tér el egymástól, ezért tetszőlegesen rögzíthetjük, mondjuk az f_0, optimális függvényt, és segítségével definiáljuk az

$$I(x) = C_{f_0}(x)$$

Kolmogorov bonyolultságot. ■

Az *I(x)* függvény azonban csak elméleti objektív felső határ a tömöríthetőségre, mert nem kiszámítható függvény. Ennek ellenére két alapvető tulajdonsága alapján lehet vele számolni:

1. Felülről becsülhető a tétel alapján bármilyen konkrét függvény szerinti bonyolultsággal.
2. Az $I(x)=k$ érték mögött egy konkrét k hosszú p kód áll, amire $f_0(p)=x$.

A Kolmogorov bonyolultság sok szempontból jobban használható változata, az úgynevezett prefix Kolmogorov bonyolultság, csak olyan kódoló függvényeket enged meg, ahol a lehetséges kódok halmaza prefixmentes, azaz egyik kód sem folytatása egy másiknak. Ebben az esetben is létezik optimális g_0 prefixmentes kódoló, és definiálható segítségével a

$$K(x) = C_{g_0}(x)$$

prefix Kolmogorov bonyolultság.

Hasonló úton jutunk a feltételes Kolmogorov bonyolultsághoz, ami azt fejezi ki, mennyit segít egy x szám kiszámításában egy másik y szám ismerete.

Definíció. Az x szám y szerinti feltételes közönséges, illetve prefix Kolmogorov bonyolultságán, *I(x|y)*-en, illetve *K(x|y)*-en a

$$I(x \mid y) = C_{f_0}(x \mid y) = \min(l(p) \mid f_0(p,y) = x)$$

illetve

$$K(x \mid y) = C_{g_0}(x \mid y) = \min(l(p) \mid g_0(p,y) = x)$$

értékeket értjük, ahol $f_0(p,y)$ és $g_0(p,y)$ kétváltozós optimális kódoló függvények. ■

Mindkét függvény tulajdonságai megegyeznek a feltétel nélküli esetre mutatott tulajdonságokkal.

A feltételes bonyolultság alkalmas arra, hogy egy véges halmaz elemeinek a halmaz szerinti feltételes bonyolultságát elemezhessük. Ehhez még arra van szükség, hogy magát a halmazt kóddal jellemezhessük, azaz a halmaz kódjából elő tudjuk állítani program segítségével a halmaz elemeit.

Legyen $\mathcal{A}$ véges elemű halmaz, kódja legyen a, és elemeinek száma legyen m. Nézhetjük $x \in \mathcal{A}$ esetén az $I(x|\mathcal{A}) = I(x|a)$ és $K(x|\mathcal{A}) = K(x|a)$ feltételes Kolmogorov bonyolultságokat. A Kolmogorov bonyolultság 2. tulajdonsága alapján megint a skatulya elv szerint látható, hogy $\mathcal{A}$ elemeinek többségére az $\mathcal{A}$ szerinti feltételes bonyolultság nem lehet érdemben kisebb,

mint $\log_2 m$. Ugyanis a $\log_2 m$-nél Δ-val rövidebb kódok száma, amit f_0, illetve g_0 használhat, legfeljebb $m2^{-\Delta}$.

Amennyiben az a kód úgy viselkedik, mint egy felsorolható halmazsereg paramétere, és a alapján az m_a elemű $\mathcal{A}_\alpha$ halmaz elemeit algoritmikusan fel tudjuk sorolni, akkor a

$K(x|a) \le \log_2 m_a + c$

is teljesül valamilyen c konstanssal, amely a halmazsereg felsoroló függvényétől függ csupán.

Speciálisan, ha $\mathcal{A}$ az a hosszú szavak halmaza, azt kapjuk, hogy a szavak döntő többsége még a hosszának ismeretében is legalább olyan bonyolult, mint amilyen (hosszú), de nem is bonyolultabb a hosszánál. (Ebben az esetben ugyanis $m=2^a$.**)**

Az algoritmusokkal kezelt jelek világának egy másik fontos törvényére mutat rá a feltételes Kolmogorov bonyolultság, amit az **információ-nemnövekedés törvényének** nevezhetünk. Szemléletesen úgy vethető fel a kérdés, hogy mennyi információt nyerhetünk ki az adatbázisokból? Mit jelent az például, hogy az apa – fiú kapcsolatokat tároló adatbázisból a nagyapa – unoka kapcsolatokat ki tudjuk nyerni? A kérdés az, hogy valóban nyerünk-e információt? A válasz: a kinyert információ nem lehet több annál, mint amennyit bevittünk.

A pontos matematikai megfogalmazáshoz jelölje x az adatbázis tartalmát, q a kérdésadatot, v pedig a q kérdésre adott választ. Minthogy a válasz x-ből és q-ból kiszámítható, valamilyen kétváltozós f kiszámítható függvényre $f(q,x)=v$. A feltételes Kolmogorov bonyolultságot definiáló optimális függvény 1. tulajdonsága szerint

$$K(v \mid x) = C_{g_0}(v \mid x) \le C_f(v \mid x) + n_f \le l(q) + n_f \ .$$

A fenti egyenlőtlenség azt fejezi ki, hogy az adatbázis tartalmának ismeretében a válasz feltételes Kolmogorov bonyolultsága, azaz információmennyisége nem lehet nagyobb a kérdés hosszánál. (Finomabb becsléssel az is megmutatható, hogy a kérdés prefix Kolmogorov bonyolultságánál nem nagyobb a válasz feltételes információmennyisége. Ezen felül még az is teljesül az adatbázis tartalmára, x-re, hogy a válaszfüggvény valamilyen végrehajtható programkódját is tartalmazza.)

Ennek a törvénynek finomabb elemzésekor azt is figyelembe kell venni, hogy a választ megkapó személy – aki lehet a kérdező is- általában kevesebb információval rendelkezik, mint amit a teljes adatbázis tartalmaz. Ehhez az információhoz viszonyítva a válasz feltételes információmennyisége lehet nagyobb is, mint a kérdés információmennyisége. Ez azt jelenti, hogy a választ megkapó saját tudása és a kérdés ismeretében nem tudná a választ előállítani további kívülről kapott információ nélkül, illetve a kérdés, a válasz és a saját ismerete nem lenne elég ahhoz, hogy megértse a választ. Az adatbázis nem az egyén, hanem az információs rendszer kollektívájának együttes ismeretét tükrözi. Az egyén így tud többet kapni a közösből annál, mint amit ő adott hozzá.

Természetszerűen vetődik fel a kérdés, hogy a két információmennyiség, a Shannon entrópia és a Kolmogorov bonyolultság, vagy másik nevén Kolmogorov entrópia között van-e kapcsolat. Általánosságban azt lehet mondani, hogy minél nagyobb jelenségről van szó, annál szorosabb a két mennyiség kapcsolata.

Az igen hosszú véletlen jelenségekről, mint amilyen egy igen hosszú üzenet, már említettük, hogy úgy viselkednek, mint egy lényeges halmazra koncentrálódó egyenletes eloszlású jelenség. Egy L hosszú tipikus $X=x_1x_2 \ldots x_L$ üzenet $p(X)$ valószínűsége a

$$2^{-L(H+\varepsilon)} \le p(X) \le 2^{-L(H-\varepsilon)}$$

egyenlőtlenségnek tesz eleget. Jelöljük ezt a tipikus halmazt $\mathcal{A}$-val, és elemeinek számát m-mel. Tekintettel arra, hogy a *p(X)* valószínűségek összege az $\mathcal{A}$ halmazon legfeljebb 1, és tetszőlegesen közel lesz 1-hez, ha *L*-et elég nagynak választjuk, ezért *m*-re az alábbi becslést kapjuk:

$$(1-\delta)2^{L(H-\varepsilon)} \le m \le 2^{L(H+\varepsilon)} .$$

Amennyiben az $\mathcal{A}$ halmazt algoritmikusan jól tudjuk jellemezni, ami a gyakorlatban tipikusan statisztikai jellemzőkre tett egyenlőtlenségekkel történik, akkor használhatjuk a $K(X|\mathcal{A})$ feltételes Kolmogorov bonyolultságot, és m becsléséből az

$$L(H-\varepsilon') \le K(X \mid \mathcal{A}) \le L(H+\varepsilon')$$

becslés adódik, ahol ε' tetszőlegesen kicsi választásához valamilyen alkalmasan nagy L_0-nál nagyobb *L*-re teljesül az egyenlőtlenség.

Azt kaptuk tehát, hogy a Shannon entrópia szerint az egy szimbólumra jutó entrópia a tipikus halmaz elemein megegyezik a feltételes Kolmogorov entrópia - azaz az elméletileg legrövidebb kód hosszának- egy szimbólumra jutó részével.

Összegezve, mindkét esetben arra jutottunk, hogy meg kell találni a jelenség szempontjából lehető legkisebb, és minden lényeges lehetőséget tartalmazó halmazt, amit hatékonyan jellemezni tudunk, és ezen a halmazon az egyenletes kódhossz választásánál nem érdemes jobb kódolási módszert keresni. Ezzel kaptuk meg mindkét úton a kódolás univerzális lehetőségeit és korlátjait.

(Pontosan ezt fejezi ki a Kolmogorov féle struktúrafüggvény: adott *x*-hez keressük azt az *x*-et tartalmazó véges $A(x,\alpha)$ halmazt, amelynek prefix Kolmogorov bonyolultsága legfeljebb α, és elemszáma, m_α minimális. Az *x* struktúrafüggvénye $\mathrm{str}_x(\alpha)=\alpha+\log_2 m_\alpha$. Az $A(x,\alpha)$ halmaz az *x*-hez hasonló elemek halmazának tekinthető.)

A fentiekből érezhető, hogy a véletlenség és az algoritmusok között valamilyen kapcsolat van. Paradox módon végtelen sorozatok véletlenségét algoritmikusan lehet jellemezni. Kolmogorov utolsó [3] dolgozata, amelyet Uszpenszkij-jel közösen írt, igen részletes áttekintést ad a véletlenség és az algoritmusok összefüggéséről. Adott eloszlás szerinti végtelen véletlen sorozatok halmazának komplementere algoritmikusan jellemezhető, és úgy nevezett effektíven null-mértékű halmazt jelent az adott eloszlás szerint.

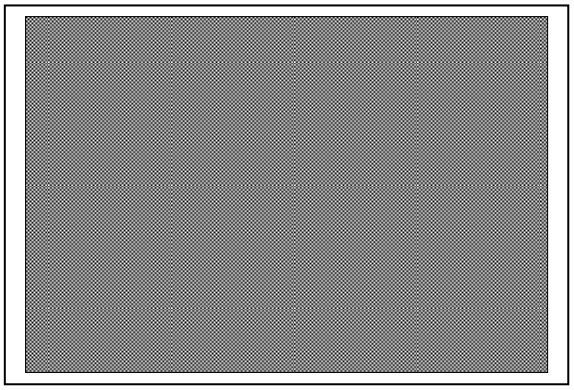
Véges esetben minden más. Képzeljünk el 1000 pénzfeldobással létrehozott nulla-egy sorozatot, és egy csupa nullából álló 1000 hosszú sorozatot. Nyilván az elsőt véletlennek tekintjük, a másodikat nem. Kezdjük el a második sorozatot bitenként összevissza sorrendben átírni az első sorozattá. Meg tudjuk-e mondani, hol történt a váltás a nem véletlen és a véletlen eset között?

(A múlt megvalósult véletlensége is egészen más, mint a jövő lehetséges véletlensége. Vegyük például a 10 pénzérme feldobási kísérletet. Ennek eloszlása egyszerű, mind az $1024=2^{10}$ eset azonos valószínűségű. Végeztessük el a kísérletet 10240 személlyel. Igen nagy a valószínűsége, $1-e^{-10}$, hogy lesz közöttük olyan, aki csupa fejet dobott. Véletlennek fogjuk-e tekinteni ezt az eredményt? Nem jó a kérdés, az eredmény már nem véletlen, csak véletlenül ez adódott.)

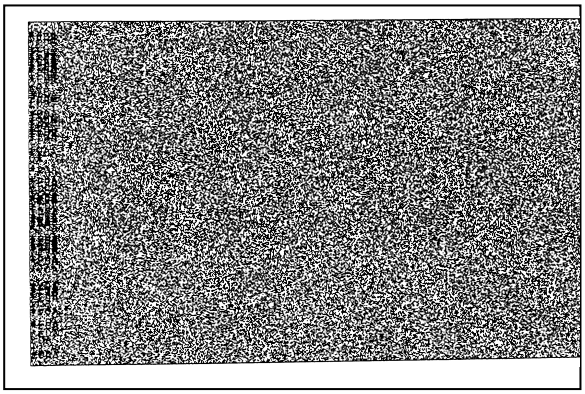
Véges sorozatokra a véletlen nem definiálható, csak az, hogy mennyire tekinthető véletlennek. Egy véges halmaz elemét akkor tekintjük a halmazban véletlenszerűnek, ha a halmaz szerinti feltételes Kolmogorov entrópiája nem sokkal kisebb a halmaz elemszámának

logaritmusánál. Egy elem annál véletlenszerűbb, minél közelebb van feltételes Kolmogorov entrópiája a halmaz elemszámának logaritmusához.

Egy véletlen jelenségből származó nagyon hosszú előfordulások egyre nagyobb hányada viselkedik a fenti értelemben erősen véletlenszerűen. Az algoritmikus tanulás lényege: kiszűrjük a jellemző szabályosságokat, s a megmaradó egyedi tulajdonságokat tömörítetlen adatként adjuk meg. A jellemző sajátosságokkal megadott halmazon a vehetjük lehető legvéletlenebb egyenletes eloszlást, és így kapjuk meg a jelenséghez hasonló lehetőségek halmazát.



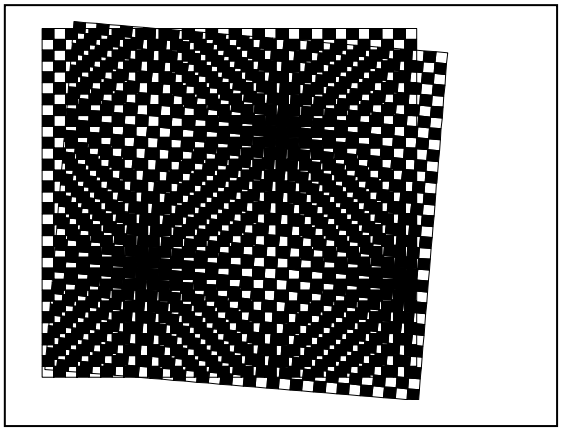
10. ábra



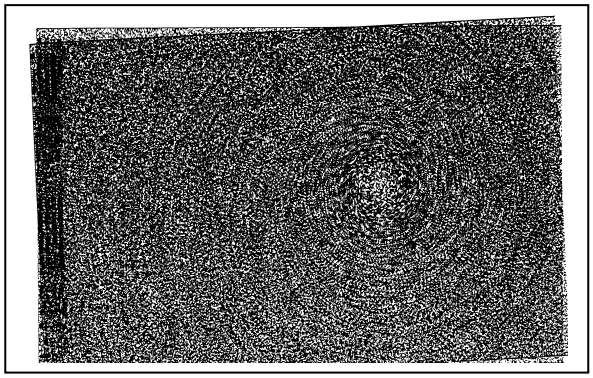
11. ábra

Nézzünk erre egy érdekes vizuális példát. Vegyük az ½ szürkeségű színezéseket, vagyis ahol a képpontok (képcellák) fele fekete, fele fehér. Az I. rész ábráinak sorszámozását folytatva, a 10. és 11. ábrák két eltérő színezést mutatnak. A 10. ábra sakktábla-színezés, elég annyi adat róla, hogy bal felső cella színe milyen, és a teljes színezést elő tudjuk állítani. A 11. Ábra véletlenszám-generátorral készült, megfelel egy tipikus színezésnek. (Az ábra 1990-ben készült, s e baloldalon látható sötét sáv a lézernyomtató hibaüzenete volt.) Aki nem ismeri a generátort, gyakorlatilag nem tudja tömöríteni a kép kódját.

Véletlennek köszönhetően a két ábra igen érdekes vizuális tulajdonságát észleltem egy előadásom [4] előkészítése során. Írásvetítő fóliát készítettem az ábrákról, és a fólia az eredeti ábrára helyezve interferencia képeket mutatott. A 10. ábra sakktábla színezése négyzetrácsos szimmetriájú sötétedéseket mutat. Ez egyszerűen következik a sakktáblaszínezésből, nagyítva látható egy részlet a 12. Ábrán. (Ilyen elven viselkednek a Moiré alakzatok is.)



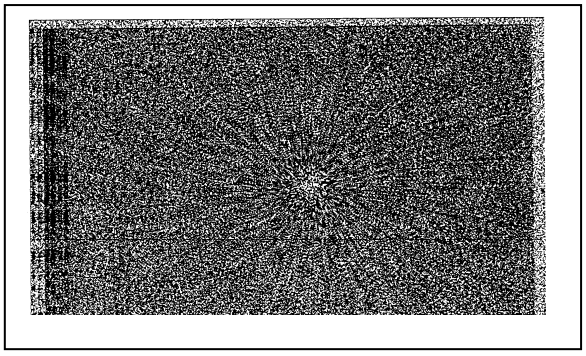
12. ábra



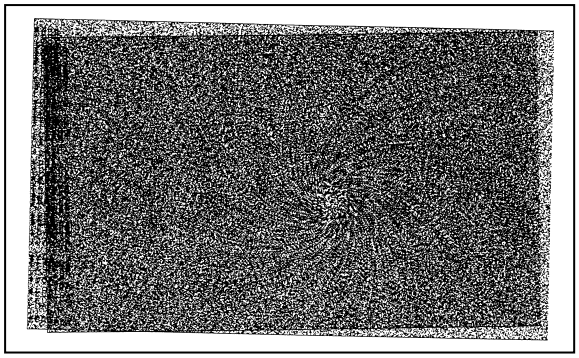
13. ábra

Meglepő a 11. ábra színezésének viselkedése volt. Koncentrikus körök jelentek meg rajta. A fólia mozgatásával a körök középpontja fehér foltként vándorolt, a forgatás hatására a körök összehúzódtak, vagy tágultak. A 13. ábra a két színezés elforgatásos öninterferenciájáról egy álló képet mutat, mozgásban a jelenség még érdekesebb.

Kicsinyítve kis mértékben a fóliát, más típusú interferencia jelenik meg: egy pontba futó sugárnyaláb, vagy egy pontba futó spirálkarok (14. és 15. Ábra.) Mozgatás közben a középpont fehér foltként vándorol, további forgatás hatására a spirálok erősebben csavarodnak, közben beszűkülnek. (Komplementer színezéssel is megnéztem a jelenséget, minden hasonlóan viselkedik, csak a középpont lesz sötét folt.)



14.ábra



15. ábra

A jelenség mögött a véletlen tömegjelenségek alapvető tulajdonsága húzódik: egy véletlen fekete-fehér színezésben miden kis alakzat valószínűségének megfelelő gyakorisággal fordul elő. Amikor az eredeti képre ráhelyezzük a róla készült fóliát, egy sík-transzformációt végzünk. A transzformáció sajátgörbéire illeszkedő hosszabb fekete alakzatok rajta maradnak a görbén, és egymást fedve megnyúlnak. Ezek a megnyúló alakzatok rajzolják ki az egybevágóság forgatásos esetében a köröket, centrális kicsinyítés esetében a sugárnyalábot, forgatásos kicsinyítés esetében a spirálokat. A vizuális magyarázat mellet más magyarázata is van a jelenségnek: a sajátgörbék mentén az egymásra helyezett ábrák fekete pontjainak száma adott hosszúságú kis szakaszon nagyobb szórású, mint más görbék mentén. Ez a nagyobb szórás válik láthatóvá. A jelenséget Julesz Béla: „Dialógusok az észlelésről” c. könyvében a randompont-kinematogramok monokuláris mozgásészlelése tárgyalásánál Glass hatás és Glass mintázatok néven említi. (Glass, 1969)

Visszatérve az algoritmikus tanulás kérdéskörére, a Kolmogorov bonyolultság ezen a téren szintén fontos elvi szerepet játszik, segítségével univerzális tanuló algoritmusok adhatók, amelyek azonban nem kiszámíthatóak.

A Shannon entrópiaformula a p valószínűséghez a $-log_2 p$ információmennyiséget rendeli. Ennek megfordításaként a prefix Kolmogorov entrópiával a

$$\pi(x) = 2^{-K(x)} \text{ eloszlást, amelyre } \sum_{x=1}^{\infty} \pi(x) < 1 \ ,$$

kapjuk a nem negatív egészek felett a Kraft egyenlőtlenséget is felhasználva. A kiszámítható eloszlások között ez a legnagyobb bizonytalanságnak megfelelő eloszlás, amelyet a Levin féle apriori eloszlásként emlegetnek. Erre épül az univerzális tanuló eljárás a statisztika klasszikus Bayes módszere szerint. A Bayes módszer, mint a statisztikai tanulás alapmegoldása, a megfigyelt jelenség eloszlásának paraméterét adó paramétertéren a megfigyelés előtti apriori eloszlásból és a megfigyelésből a Bayes tétel szerint számítja ki a paramétertéren a

megfigyelés utáni eloszlást. A Bayes elv szerint, amennyiben az apriori eloszlás ismeretlen, véges paramétertér esetén a legbizonytalanabbat, az egyenletes eloszlást kell választani. Végtelen paramétertérre ez nem használható, s ha a kiszámítható eloszlások világában vagyunk, akkor a nem negatív számok halmazát véve paramétertérnek, a Levin féle apriori eloszlás választása a legjobb megoldás. Ez az alapja az univerzális tanuló algoritmusnak. Minthogy $\pi(x)$ nem kiszámítható, kiszámítható közelítései adják a megvalósítható tanuló algoritmusokat. (Lásd M. Li és P. M. B. Vitányi [5], és a The Computer Journal [6] speciális kiadását Kolmogorov Complexity címmel. Az információelmélet témakör legfrissebb hazai szakirodalma Györfi László, Győri Sándor és Vajda István [7] tankönyve.)

A véges világban - tehát a digitalizált világban is- a matematika végtelen ideális konstrukciói – végtelen kicsi és nagy, a folytonosság, univerzális algoritmusok, véletlen - csak segítenek, végtelennel közelítik a véges modellt, amit utána vissza kell véges közelítésbe hozni.

Ezzel a gondolatsorral lépjünk át a számítógépes információs rendszerek új világába.

4.Összefoglalás

Attól kezdve, hogy egy üzenet, vagy instrumentális felvétel következtében egy jel bejutott a hálóba, minden a processzorok működése szerint történik vele. A processzorokon programok futnak, amelyek megint csak valamilyen üzenetek eredményeként jöttek létre, és jel alakban is léteznek.

Az adattároló, a processzor, az adó, a vevő, a csatorna, az interakciós berendezések mind műszaki alkotások, sokszor igen finom fizikai jelenségekre épülve. Ettől még a processzorokon futó programok készítéséhez nem csak műszaki, hanem a felhasználási területre vonatkozó ismeretek is szükségesek. Láthatóan a jelek világában mindent áthat a programozás, a szoftverkészítés feladata. Legmeghatározóbb komponensként a programozható számítógépek – domináló módon a Neumann-elvű számítógépek – biztosítják a teljes világháló működtetését. Az 1945-ben lefektetett architektúra még nincs 60 éves, a köré épülő újabb és újabb technológiák még mindig megjósolhatatlan lehetőségeket hoznak felszínre. A legutóbbi 10 év dominálóvá váló legfontosabb technológiái időrendben: személyi számítógépek, Internet, World Wide Web, mobil kommunikációs eszközök, Gbit Ethernet, HTML és XML, multimédia berendezések, e-kereskedelem, GPS és térinformatika, hálózati számítás, Web Service, mobil érzékelők (beépített rendszerek + mobil kapcsolat), átható számítás (pervaisive computing). Mindez a sok pozitív lehetőség mellett negatív jelenségeket előidéz. A számítógépes bűnözés, az információ-szennyezés és a „Nagy Testvér” mindenre kiterjedő megfigyelési lehetősége talán a legfontosabb negatív hatások.

A 3. szakaszban felvázolt matematikai modellek lehetőségeket és korlátokat mutatnak az új, digitalizált, mesterséges világot létrehozó kommunikációs technológiák számára. Ezek a törvényszerűségek tipikusan csak határértékben érvényesek, és mint sok más eszmei fogalma a matematikának, mint a végtelen nagy és kicsi, a folytonosság, valószínűség, univerzális algoritmusok, a véges rendszereket felülről közelítik a végtelenből. Az információs technológiák a felhasználható egyre kisebb téridő-granulátumú jelek segítségével egyre nagyobb méretű véges feladatok megoldását teszik lehetővé. Egyre nagyobb mennyiségben, finomsággal, felbontással képesek a múlt üzeneteit, észleléseit feldolgozható módon megőrizni. Az információ mérőszámaira épülő matematikai törvények egyre erősebben érvényesülnek, de nem adnak megoldást feladatainkra, keresnünk kell a jó közelítő, kompromisszumos, véges megoldásokat.

Fontos felhívni a figyelmet arra, hogy miután egy üzenet, vagy észlelés jelekké kódolódott, többé már egyáltalán nem véletlen; a múltban, a kiválasztás, megfigyelés előtt volt véletlen. A

múltra vonatkozó rögzült észleléseink, feljegyzéseink, ítéleteink lehetnek hiányosak, pontatlanok, homályosak, de már nem véletlenek abban az értelemben, hogy valami eloszlás jellemezné őket. Amennyiben tudnánk, hogy a múlt milyen valószínűség-eloszlásból származik, a hiányzó, homályos részeket ki tudnánk egészíteni az eloszlásra jellemző tipikus jelenségekkel, szimulálhatnánk a hiányzó részeket. Amennyiben a jövő jelenségei is ebből az eloszlásból fognak bekövetkezni, a múlthoz ebben az értelemben hasonló jelenségekre számíthatunk a jövőben.

Ami továbbra is véletlen a világhálón lévő jelek gyűjteményében, az a rárakódó zaj. Paradox módon a programok jelentik a legnehezebben kezelhető, és elkerülhetetlen zajforrást, ami téves üzenetek vételét eredményezi. Az informatikus szakemberek képzésében ez a meghatározó feladat: olyan szakemberek legyenek, akik képesek ennek a zajnak csökkentésére.

Dolgozatomban, egyáltalán nem véletlenül, központi szerepet játszik a véletlen. A kommunikációnak kizárólag véletlen szituációk között van szerepe. Bízhatunk benne, hogy a természet és az élet lényege a véletlen, a kiszámíthatatlanság, ezért az emberi kommunikáció mégis csak az emberek között fog fennmaradni.

Kolmogorov a véletlen problémáját így foglalta össze:

„A mindennapi beszédben véletlennek hívjuk azokat a jelenségeket, amelyekben nem tudunk olyan szabályosságokat találni, amelyek lehetővé tennék, hogy pontosan előre jelezzük jövőbeli bekövetkezésüket. Általában véve, nincs alapunk abban hinni, hogy egy véletlen jelenségnek bármilyen meghatározott valószínűséggel kellene rendelkeznie. Különbséget kell tenni ezért a valódi véletlen (mint a szabályosság teljes hiánya) és a sztochasztikus véletlen (ami a valószínűség-elmélet tárgya) között. Ez felveti annak kérdését, hogy magyarázatot keressünk arra, hogyan alkalmazható a véletlen matematikai elmélete a valós világra."

A válasz valahol a múlt és a jövő viszonyában kereshető. A két entrópia-fogalom közötti átjárás is erre a kapcsolatra mutat lehetőségeket. A tudományok fejlődésében ennek kihasználásában az információs technológiák fejlődése új korszakot nyitott. A múlt megfigyeléséből a jövő lehetőségeinek eloszlására következtethetünk, s beavatkozási lehetőségeinkkel a kedvezőbb irányba alakíthatjuk az eloszlást. Az emberiség kommunikációjának ez lehet a legbelső célja.

Irodalomjegyzék

[1] Claude E. Shannon – Warren Waever, A kommunikáció matematikai elmélete (az információelmélet születése és távlatai), OMIKK, Budapest, 1986.

[2] Kolmogorov, A.N. Three approaches to the quantitative definition of information. Problems of Information Transmission **1** (1) 1965. 1-7.

[3] Kolmogorov. A.N. – Uspenskii V.A., Algorithms and randomness. SIAM J. Theory of Probability and Applications, 32 (1987) 389-412.

[4] Benczúr András, An attempt to the algorithmic definition of fuzziness. Annales Univ. Sci. Budapest., Sect. Comp. (1991) 19-33.

[5] Ming Li, - Paul Vitanyi, An Introduction to Kolmogorov Complexity and its Applications. Second Edition, Springer Verlag 1997.

[6] Kolmogorov Complexity, Special Issue, eds. Alexander Gammerman and Vladimir Vovk, The Computer Journal, Vol. 42, No. 4, 1999.

[7] Györfi László – Győri Sándor – Vajda István, Információ- és kódelmélet, Budapest, Typotex Kiadó, 2000.