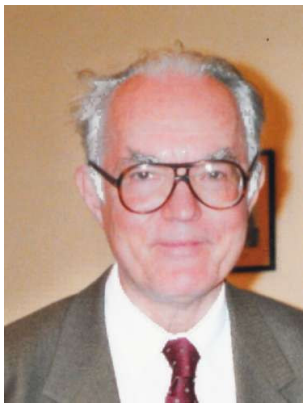
ÉLET és TUDOMÁNY

A hét kutatója Matematika

Világhírközlés – Interjú Csiszár Imrével

2015.06.02.

Az információelmélettel a terület korai időszakában ismerkedett meg Csiszár Imre matematikus, akadémikus, aki júniusban az életműdíjnak tekinthető Hamming-medált veheti át, melyet az elektromérnökök nemzetközi egyesülete (Institute of Electrical and Electronics Engineers) évente ítél oda egy kiemelkedő kutatónak vagy legfeljebb háromtagú kutatócsoportnak. Csiszár Imre az információ matematikai és hírközlési sajátosságait vizsgáló területet Rényi Alfréd vezetésével térképezhette fel, majd később a hazai információelmélet-kutatás vezető alakjává vált.



– Mi az oka annak, hogy csak 1948-ban indult ez a terület? Hiszen a valószínűségszámítási háttér jóval korábban adott volt.

– Hogy egyáltalán 1948-ban elkezdődhetett, az is Claude Shannon géniuszának volt köszönhető, akinek ekkor jelent meg cikke a témában. Ha ő nincs, akkor legalább tíz évig nem lett volna információelmélet. Ő ismerte fel, hogy a hírközlési problémákra alkalmazhatók digitális modellek. Akkor még digitális hírközlés nem létezett, teljesen analóg volt. Valahogy Shannon kitalálta – égből pottyant volt e gondolat – hogy úgy kell tekinteni az információt, mint diszkrét jelek sorozatát, és ennek matematikai tulajdonságait kell vizsgálni, és ebből mély következtetéseket lehet levonni. A digitális hírközlés csak húsz évvel később, a hetvenes évekre született meg. A digitális számítógép már létezett, tehát valahonnan lehetett venni az ötletet, de hírközlésben – telefóniában, rádióban – addig nem volt jelen. Ez egészen különleges, hiszen legtöbbször úgy születik egy tudományág, hogy sok ember munkájából jön össze. A Shannon által kitűzött alapproblémákon vagy húsz évig dolgoztak a matematikusok – ő volt ennek az elsőszámú tudósa, az ő eredményeit fejlesztették tovább általában.

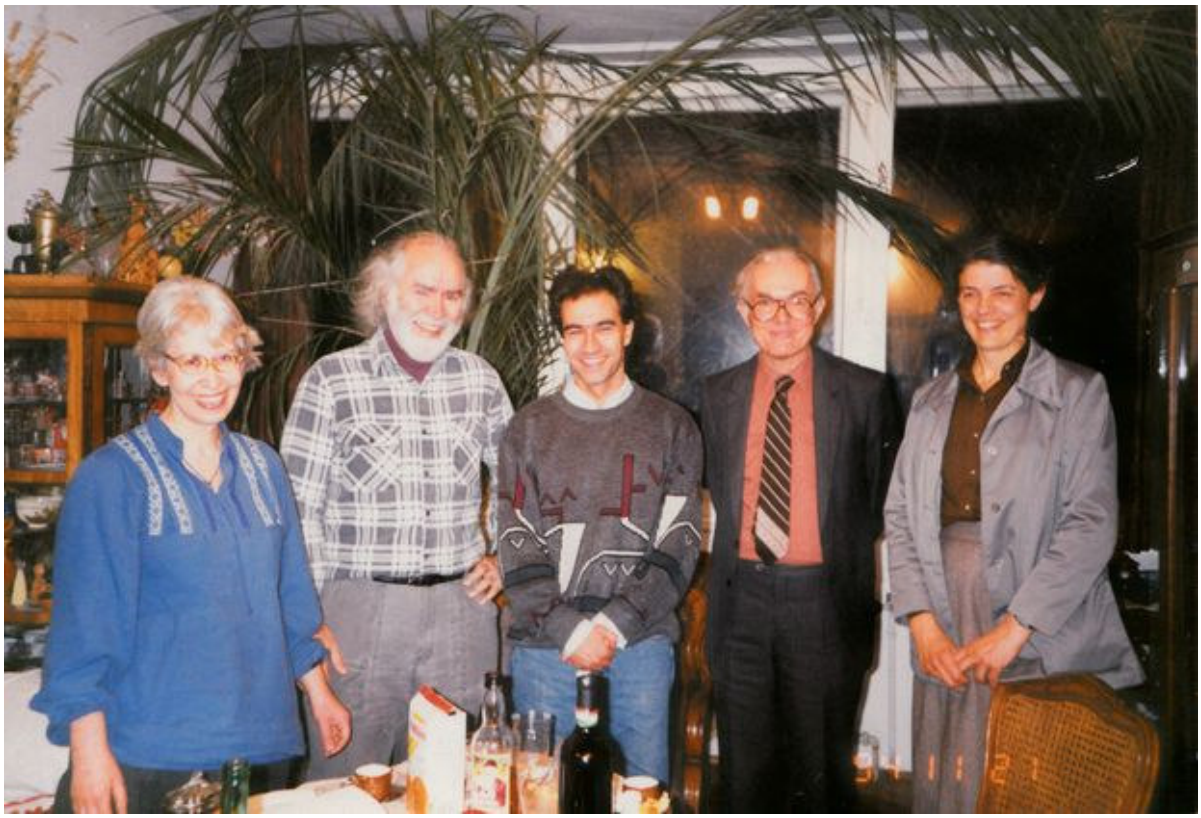
– Rényi mely kérdéseken dolgozott?

– Nem igazán szerette a fősodor problémáit, mindig valami újat akart kitalálni. Shannon egyik fő felfedezése az volt, hogy az információ mennyiségét mérni lehet, ez volt a Shannon-féle entrópia. Rényi gondolata az volt, hogy miért ne lehetne más mértékszám is. Így kitalálta a Rényi-féle entrópiát.

Bizonyos helyzetekben csak ezt tudjuk használni. És felismerte azt is, hogy az eredetileg hírközlésre alkalmazott gondolatkört nemcsak arra, hanem számos más problémára lehet használni: információszerzésre, kereséselméletre – manapság is használják a Rényi-féle entrópiát például a statisztikus fizikában és a keresési problémák egy részében.

– Gondolom nem véletlen, hogy a fősodorral inkább a nagyhatalmaknál foglalkoztak.

– Az USA-ban állt olyan szinten a technika, hogy gyakorlatban is lehetett alkalmazni. Amit mi csináltunk, az elmélet volt, nem alkalmaztuk, s tudomásom szerint a szovjet vezető kutatók sem foglalkoztak konkrét alkalmazásokkal, de ők egy óriási intézményben dolgoztak – lényegében a SZTAK volt nagyban –, így ott a mérnökmunkatársak áttehették a gyakorlatba. Előfordult, hogy konkrét gyakorlati problémák vezettek matematikai kérdésekhez. Például a számítógép-memóriák kezdetben a Szovjetunióban nem voltak túl megbízhatók, arra dolgoztak ki módszereket, hogy ha a memóriák meghibásodnak, akkor az egyes cellák meghibásodása esetén is jól működjenek – ez volt a tetszőlegesen változó csatornák elméletének az egyik kiindulópontja, ezzel magam is sokat foglalkoztam. Hollandiában, Németországban, Csehszlovákiában, Japánban, Izraelben is voltak és vannak erős kutatók – közülük sokan itt vannak a falamon a közös fényképeinken. A hetvenes évekre mi a legjobbak közé kerültünk Körner János és Marton Katalin kollégáimmal, azóta mindhárman Shannon-díjat kaptunk. Később felbomlott ez a csapat: Körner elment Olaszországba, inkább kombinatorikai irányban kutat, Marton Katalin pedig a matematika rokonágához pártolt. Ám ezeken a területeken mindketten továbbra is eredményesen alkalmaznak információelméleti módszereket.



Marton Katalin, Paul Shields (USA), Simonyi Gábor (Renyi Int. Inf.elm. Oszt. kutatója), Csiszár Imre és Shields élettársa (balról jobbra)

– Hogyan kezdődött ez a virágkor a hetvenes években?

– A hetvenes évek elején többször jártam Amerikában, a többiek is voltak külföldön, ott ismertük meg a modern főirányt, a többfelhasználós információelméletet. Ekkor kezdtek el ezzel a témával intenzíven foglalkozni, úgyhogy rögtön a kályhánál kezdtük a dolgot. 1981-ben jelent meg a könyvünk Körnerrel, néhány évig még ezután is folyt a közös kutatás.

– A több felhasználó miatt jelent meg a gráfelmélet az információelméletben?

– Nem igazán. Persze ma már a hálózatelmélet esetén a gráfelméleti tulajdonságok tényleg fontos szerepet játszanak, de mivel mi akkor csak néhány felhasználóból álló hálózatokkal foglalkoztunk, így bonyolultabb gráfelméleti meggondolásokra nem volt szükség. Shannon egyik kérdése hozta be: arra volt kíváncsi, hogyan lehet az információt biztosan helyesen eljuttatni a fogadó félnek.

– És ebben hol van a gráfelmélet?

– Ahhoz, hogy egy üzenetet nulla hibával lehessen dekódolni, az szükséges, hogy más üzenet leadása ne vezethessen ugyanahhoz a kimenethez. Tehát a lehetséges üzeneteket és lehetséges kimeneteket összekötjük, így egy gráf keletkezik. Ez egy páros gráf lesz, az lesz az érdekes, amikor nem egy üzenetet adunk le, hanem egymás után sokat, az ekkor fellépő gráfszorzatokkal és gráfszínezéssel kapcsolatos problémák hamar bonyolulttá válnak.

– Az üzenet helyes átvitelén kívül a titkosítás is örök kérdés.

– Az utóbbi húsz évben intenzívebben foglalkoztam a titkossággal. Kétféle titkosság van: a számítási komplexitáson alapuló, amit a gyakorlatban használnak kiterjedt módon. Ekkor azért nem lehet megfejteni egy kódot, mert igaz, hogy elvileg tudnánk, de gyakorlatban irtózatos mennyiségű számolásra lenne szükség, amire még a mai számítógépek se képesek. Ez most még jól működik, de sokan gondolkodnak azon, hogy információelméleti titkosság, tehát elvi megfejthetetlenség kellene.

– És az hogyan lehetséges?

– Ehhez az kell, hogy az adó és a vevő között legyen valami véletlen folyamat által meghatározott titkos kulcs. Az ősidőkben is tudták, hogy ha egy véletlen 0-1 sorozat rendelkezésre áll az adónak és a vevőnek is, akkor azzal biztosan megfejthetetlenül lehet kódolni egy ugyanolyan hosszúságú üzenetet. A legmagasabb katonai és diplomáciai csatornákon használták, de mivel ugyanazt a kulcsot nem szabad többször használni, ráadásul ugyanolyan hosszúnak kell lennie a kulcsnak, mint a szövegnek, még a mai technikai fejlettség mellett sem kivitelezhető olyan mennyiségű kulcsot letárolni, hogy azzal nagy mennyiségű hírközlést lehessen kódolni. Azt találták ki, hogy magában a csatornában keletkező véletlen zaj az, amit erre a célra fel lehet használni – az a feltevés, hogy van egy legitim felhasználó, és van egy ellenség. Normális esetben a legitim felhasználó csatornája jobb, ezt a különbséget használnák: lehetne olyan kód, amit a legitim felhasználó még tud dekódolni, a lehallgató már nem. Viszont ugyanolyan minőségű csatorna esetén ez megbukhat. Vannak olyan változatok, amikor az adó és a vevő valamilyen természeti jelenséget tud megfigyelni, úgy hoz létre korrelált véletlent. A neten például fellépnek olyan véletlen jelenségek, amelyeket az adó és a vevő megfigyelhet, amely zajjal torzított, ebből tud létrehozni egy kulcsot, amit a lehallgató nem tud.

 Muriel Medard, az IEEE Information Theory Society elnöke 2012-ben Budapesten Csiszár Imrével

– Ennek Ön milyen matematikai vonatkozásait vizsgálta?

– Arra voltam kíváncsi, hogy ha az ember ismeri a csatornát – a zaj sztochasztikus természetét –, akkor milyen sebességgel lehet úgy információt átvinni, hogy a legitim vevő tudja dekódolni, az ellenség viszont ne tudjon meg semmit. Egy analóg probléma, hogy ha olyan lehetősége van a két felhasználónak, hogy korrelált információforrásnak a két kimenetét figyelje meg, akkor abból milyen mennyiségű titkos kulcsot tud létrehozni. Ennek érdekében a felhasználók kommunikálhatnak egymással, de úgy, hogy az ellenség a titkos kulcsról akkor se tudjon meg semmit, ha ezt a kommunikációt lehallgatja. Hasonló problémákat többfelhasználós modellekre is vizsgáltam. Számtalan matematikailag izgalmas kérdést lehet felvetni. Sokan úgy gondolják, hogy ez lesz a jövő, több helyen már használják is.

MÉCS ANNA