fizikai szemle

AZ EÖTVÖS LORÁND FIZIKAI TÁRSULAT LAPJA

Alapította Eötvös Loránd 1891-ben Mathematikai és Physikai Lapok néven

XX. évfolyam 6. szám 1970. június

NAPLÓ AZ INFORMÁCIÓELMÉLETRŐL

Rényi Alfréd

Pár évvel ezelőtt, nem sokkal az államvizsgák után, postámban egy vastag iratcsomagot találtam, amelyhez egy levél volt mellékelve; írója egy volt hallgatóm, aki abban az évben államvizsgázott. A levél a következőképpen hangzott:

„Kedves Professzor Úr, a mellékelt kézirat elküldésével ígéretemet teljesítem, amelyet az államvizsgám után folytatott beszélgetésünk során tettem. Engedje meg, hogy röviden emlékeztessem e beszélgetésre, mivel én arra a dolog természeténél fogva, lévén az számomra igen nagy jelentőségű, egész pontosan emlékszem, míg egyáltalán nem csodálkoznék, ha Professzor Úr sok elfoglaltsága miatt nem emlékezne beszélgetésünk részleteire.

Szakdolgozatom címe „Az információ matematikai fogalma" volt, Professzor Úr arra biztatott a szakdolgozat sikeres megvédése után, hogy dolgozatomat jelentessem meg. Erre én azt válaszoltam, hogy

RÉNYI ALFRÉD
1921—1970

Minden páros szám felírható két prímszám összegeként. Ez a Goldbach-sejtés mintaszerűen mutatja a tiszta matematikai tételek ideális tulajdonságait: nagyon egyszerű állítás, és még a modern matematika teljes kelléktárával is nagyon nehéz, elvégezetlenül nehéz a bizonyítása.

Innen, a legtisztább számelmélettől indult el Riesz Frigyes tanítványaként Rényi Alfréd. Őneki sikerült igazolnia egy olyan n szám létezését, hogy minden egész szám felírható egy prímszámnak és egy legfeljebb n prímszám szorzatából adódó számnak az összegeként. De egészen fiatalon megtanulta azt is, hogy a matematika belső tiszta ragyogásával egyenrangúan szép, ahogy a matematika a való világban megnyilvánul.

A Szovjetunióban végzett aspirantúrája után már a matematika alkalmazásainak legkiválóbb magyar szakembereként tartjuk számon. Ő az Alkalmazott Matematikai Intézet megteremtője és első igazgatója. (Az is maradt: haláláig vezette a Matematikai Kutatóintézetet.) Legkedvesebb munkaterületei a valószínűségszámítás, matematikai statisztika, információelmélet. Ezek minden területén egyénit és értékeset alkotott: a matematikai axiomatikától a gyári minőségellenőrzésig.

Rényi érdeklődését nem öncélú gondolati konstrukciók foglalták le, hanem az eleven világ. Természetes tehát, hogy feszült figyelemmel fordult a fizikának azon területei felé, ahol a valószínűség nem ismereteink fogyatékossága miatt bukkan fel, hanem a természet alapvető sajátságaként nyilvánul meg. Izgatta a kvantummechanika és a statisztikus mechanika. Tudományos dolgozatokat írt végtelen anyagi rendszerek entrópiájáról. Elgondolkozott azon, hogy a valószínűségi törvények talán mindenütt a legalapvetőbbek.

„A napokban könyveimet rendezgetve belelapoztam Marcus Aurelius meditációiba. Éppen ott nyitottam fel, ahol arról ír, hogy két eset lehetséges: a világ vagy egy nagy véletlen összevisszaság, vagy pedig rend és törvény uralkodik benne, azonban bármelyik is igaz e két ellentétes lehetőség közül, a gondolkodó ember ugyanazt a következtetést kell, hogy levonja: úgy álljon szilárdan ott, ahová a sors vagy a véletlen helyezte, mint a szikla amelyen megtörnek a tenger vad, sós hullámai. Bár sokszor olvastam e sorokat, most először gondolkoztam el azon, hogy Marcus Aurelius tulajdonképpen miért is tekinti magától értetődőnek, hogy a világban vagy a véletlen uralkodik, vagy pedig rend és törvény? Miért hiszi, hogy e két lehetőség egymást kizárja? Én azt hiszem, hogy valójában e két állítás nem ellentétes, hanem mindkettő egyszerre igaz: a világban a véletlen uralkodik, és éppen ezért van benne rend és törvény, ami a véletlenek tömegéből a valószínűségeknek megfelelően bontakozik ki. Ezért tartom a valószínűség fogalmának tisztázását annyira fontosnak, és ezért foglalkoztatnak e kérdések szüntelenül."

Rényi Alfréd nem csupán egyik izgalmas dialógusában szólaltatta meg Galileit. Ő is szeretett fizikusokkal beszélgetni a természetről és törvényeiről. Több írását közölte a Fizikai Szemle, a fenti sorok is itt jelentek meg először. Azon a februári napon, amikor Bubát utoljára kísértük el, sokan voltunk a Farkasréti temetőben emlékezve és búcsúzva, barátai és tanítványai.

Marx György

a legnagyobb örömmel vállalkozom erre, annál is inkább, mert szakdolgozatom úgy készült, hogy az információelméleti tanulmányaim során naplót vezettem, amelyben a kérdésre vonatkozó gondolataimat magam számára feljegyeztem, és ezt a naplót írtam át a szakdolgozatok szokásos nyelvére. Megjegyeztem, hogy bár nyilván naplóm sem alkalmas átdolgozás nélkül az említett célra, de annak hangja sokkal közvetlenebb, és ezért azt hiszem, az átdolgozásnál célszerűbb lenne a naplóból kiindulni. Professzor Úr erre azt mondta, hogy nagyon örülne, ha ezt a naplót láthatná, — feltéve, hogy abban nincsenek olyan bizalmas feljegyzések, amelyeket nem akarok másnak megmutatni. Ezek után ígértem meg, hogy a naplót eljuttatom Professzor Úrnak.

Őszinte tisztelettel
Donát Bonifác".

Átolvasva Donát Bonifác naplóját, arra a meggyőződésre jutottam, hogy azt minden változtatás, átdolgozás vagy kihagyás nélkül közzéteszem. A napló sok valóban eredeti, önálló és újszerűen megfogalmazott gondolatot tartalmaz, amelyek igenis Donát Bonifác szellemi tulajdonának tekintendők. Ami pedig Donát az egyetemi oktatásra tett kritikai megjegyzéseit illeti, ezek — ha nem is kiforrottak —, akkor is megfontolandók, hiszen céljuk az egyetemi oktatás eredményesebbé tétele. Végeredményben az oktatás van a hallgatókért és nem megfordítva, így a hallgatóknak joguk van ahhoz, hogy önálló véleményt formáljanak arról, ahogyan őket tanítják és ha e kérdésről komolyan gondolkoznak, ezért nekik senki sem tehet szemrehányást, még akkor sem, ha elgondolásaikkal nem ért egyet. Remélem, hogy Donát naplója sok gondolkodó embert fog hozzásegíteni ahhoz, hogy az információ fogalmával kapcsolatos jelentős, de bonyolult elvi kérdésekben tájékozódjon és — úgy, mint Donát tette — a tények és érvek alapos mérlegelése alapján önálló véleményt alakítson ki. A Fizikai Szemle a Napló első részét közli. A lényegesen nagyobb, teljes szöveg a Magvető Könyvkiadónál megjelenő könyvemben („Ars Mathematica") lesz olvasható.

R. A.

Mottó: Hat hűséges barát kísér
Tanítva engemet
Nevük: Hogyan, mitől, miért
Mikor, hol és minek.
(Kipling)

Az 1. előadás

— Ma volt az első előadás információelméletről. Az előadó nagyon jó fejnek látszik; azzal kezdte, hogy a matematikának egy olyan új ágával fog ez az előadás foglalkozni, amely még nincs is 20 éves: amikor mi (mármint a teremben ülő hallgatók) születtünk, még nem létezett információelmélet. Lehet, hogy ez gyerekes dolog, de ez valahogy megfogta a fantáziámat, és már ekkor — még mielőtt az információelméletről bármi kézzelfoghatót hallottam volna — elhatároztam, hogy ezzel a tárggyal komolyan fogok foglalkozni. Rögtön el is határoztam, hogy e tárgyról nem jegyzetet írok, hanem naplót: nemcsak az előadáson hallottakat rögzítem, hanem saját gondolataimat is feljegyzem: azokat a kérdéseket, amelyeket önmagamnak felteszek, és persze a válaszokat is, ha tudok rájuk válaszolni. Ezért választottam mottóul Kipling egy versét (saját nem túl sikerült fordításomban).

Az előadás során ez az elhatározásom még megerősödött. Nagyon tetszett ugyanis az előadó kijelentése, hogy ő az előadást szemináriumszerűen fogja tartani, és azt akarja, hogy minél aktívabban résztvegyünk az órán; időnként kérdéseket fog feltenni nekünk, és minket is biztatott, hogy ha bármi nem világos, amit ő mond, szakítsuk nyugodtan félbe és tegyünk fel neki kérdéseket. Ez a módszer nekem sokkal szimpatikusabb, mint ha egy előadó kinyilatkoztatásszerűen szónokol és elvárja, hogy némán hallgassuk őt. Az, hogy egy előadó megengedi, hogy belekérdezzünk az előadásába, azt mutatja, hogy az előadó biztos a dolgában, és nem fél attól, hogy olyat találunk kérdezni, amire nem tud válaszolni. Persze, tulajdonképpen ostobaság, ha az előadó ettől fél: mi nem várjuk el a tanártól, hogy mindentudó legyen. Az a tanár, aki valóban ért a szakmájához, nem is jön ilyenkor zavarba. Például tavaly a professzor előadása után az egyik évfolyamtársam feltett neki egy kérdést: a professzor azt válaszolta, hogy ez egy nagyon érdekes és újszerű kérdés, tudomása szerint ezzel eddig senki nem foglalkozott; megígérte, hogy majd gondolkodik a problémán. A következő óra után azután közölte, hogy gondolkodott a problémán és megtalálta a megoldást, amely valóban nem volt ismeretes előzőleg; közölte, hogy egy most sajtó alatt levő feladatgyűjteménybe bele fogja venni a problémát és annak megoldását, megemlítve, hogy a kérdést az évfolyamtársam vetette fel. Sajnos vannak tanárok, akik másként reagálnak a kérdéseinkre. Még másodéves korunkban az egyik előadó előadásában egy tételre hibás bizonyítást mondott el. Amikor többen szóltunk, hogy a bizonyítás egy pontját (azt, amelyik hibás volt) nem értjük és kértük, hogy azt magyarázza meg részletesebben, ezt fölényesen elutasította azzal, hogy máskor figyeljünk jobban. Persze, ezek után nem túl nagy lelkesedéssel jártunk az óráira, ő meg a kollokviumon ütött vissza — no de hagyjuk, ez a botrány eléggé közismert, úgyhogy inkább visszatérek az információelméletre.

Az előadó először néhány szót szólt az információ-fogalom alapvető jelentőségéről. Azt mondta, hogy biztos benne, hogy e kérdésről mindannyian kellően informálva vagyunk, ezért csak röviden beszél erről. Rámutatott, hogy minden élő szervezetben állandóan áramlik az információ: például az emberi szervezetben az érzékszervek információt gyűjtenek a külvilágból, ezt az idegrendszer továbbítja az agyba, az agy az így kapott információt feldolgozza és ennek alapján utasítást — ami szintén információ — ad az izmoknak, amelyet szintén az idegsejtek továbbítanak, s. i. t. Hasonlóképpen egy üzemben vagy bármilyen más szervezetben, amelyben sok ember működik együtt, is állandóan áramlik az információ, jelentések, utasítások, kérdések formájában, enélkül kollektív munka nem volna lehetséges. Rámutatott, hogy a modern technika minden nagy vívmányával kapcsolatban központi szerepet játszik az információtovábbítás, -feldolgozás, -tárolás, így például az űrhajózás egyik fő problémája az űrhajó és a földi irányító központ közötti információátvitel; az elektronikus számológépek lényege éppen abban áll, hogy e gépek nagymennyiségű információt dolgoznak fel nagy sebességgel megadott program (vagyis információ) alapján; az automatizálás egyik fő problémája éppen az automatikus berendezés egyes részei közötti információcsere; a visszacsatolás pl. azt jelenti, hogy az irányító központ információt kap arról, hogy utasításait a berendezés hogyan hajtja végre és ennek alapján az utasításait menetközben a szükségesnek megfelelően módosítja stb.

Azt mondotta, hogy az információ matematikai elmélete annak felismerése által vált lehetségessé, hogy az információ mennyiségét számmal lehet jellemezni, — hasonlóan ahhoz, ahogyan számmal lehet kifejezni a távolságot, az időt, a tömeget, a hőmennyiséget stb.

Az előadó azt, hogy az információ mennyisége mérhető, számmal kifejezhető, a Bar-Kochba játék segítségével magyarázta meg. Az, hogy mennyi információra van szükség ahhoz, hogy kitaláljuk, amit feladtak a többiek, azzal mérhető, hogy a legcélravezetőbb kérdezés mellett hány kérdés kell a kitaláláshoz. ,,Kérdés" alatt persze, a Bar-Kochba játék szabályainak megfelelően, olyan kérdés értendő, amely igennel vagy nemmel megválaszolható. A kapott válaszokat leírva, és ,,igen" helyett 1-est, ,,nem" helyett 0-t írva, a kapott válaszsorozat (amely tehát azt, amit ki kellett találni, egyértelműen jellemzi) helyettesíthető egy 0 és 1 jegyekből álló számsorozattal. Ezt az eljárást *kódolás*nak hívják, magát a 0 és 1 jegyekből álló számsorozatot *kódszó*nak. Az, hogy minden természetes szám egyesekkel és nullákkal kifejezhető, jól ismert, hiszen ehhez elegendő a számot felírni a 2-es számrendszerben. De az is nyilvánvaló, hogy minden magyar (vagy más) nyelvű szöveg is kifejezhető, kódolható a 0 és 1 számjegyekből álló számsorozattal. Például ezt elérhetjük úgy, hogy az abc betűihez hozzárendelünk a 0 és 1 számjegyekből álló sorozatokat és betűnként írjuk át a szöveget. Ha például az alábbi 30 betűből álló abc-t vesszük alapul,

a á b c d e é f g h i j k l m n o ö p q r s t u ü v w x y z

továbbá a pontnak és a szóköznek is megfeleltetünk egy-egy 0-ból és 1-ből álló jelsorozatot, akkor tehát 32 ilyen sorozatra van szükség és 5 darab 0-ból és 1-ből álló jelsorozat éppen 32 van, tehát minden betűhöz, továbbá a ponthoz és a szóközhöz egy 5-jegyű nullákból és egyesekből álló sorozatot rendelhetünk hozzá. Így a szöveg éppen 5-ször annyi jelből fog állni, mint betűkkel leírva. Hasonlóképpen minden információ kifejezhető 0 és 1 jelek elég hosszú sorozatával. Ennek nagy gyakorlati jelentősége van, hiszen az elektronikus számológép programozásánál, mivel a gépnek a 2-es számrendszer az ,,anyanyelve", a géppel nemcsak a program során feldolgozandó számadatokat kell a kettes számrendszerbe átírva közölni, hanem mindenfajta utasítást is 0 és 1 jelekből álló sorozat formájában kell kódolni és a gépbe betáplálni. Az információmennyiség definícióját ezek után úgy is megfogalmazhatjuk, hogy egy tetszőleges információ mennyiségét úgy mérjük meg, hogy a szóbanforgó információt átírjuk, azaz kódoljuk 0 és 1 jegyekből álló sorozattá, a lehető legcélszerűbb módon (vagyis úgy, hogy a lehető legrövidebb jelsorozatot kapjuk) és az így kapott jelsorozat (kódszó) hosszával (számjegyei számával) mérjük az információ mennyiségét. Az előadó hangsúlyozta, hogy ez persze nem szabatos matematikai definíció, ezt majd később fogja megadni, hanem ez csak szemléletes kifejezése annak, hogy mit értünk információmennyiségen; ez csak arra szolgál, hogy legyen valamilyen elképzelésünk erről a fogalomról; amit mondott, tekintsük azt első lépésnek az információmennyiség fogalmának megközelítésében. Azt is hangsúlyozta, hogy amikor az információ mennyiségét akarjuk mérni, számmal kifejezni, akkor szándékosan és tudatosan figyelmen kívül hagyjuk az információ tartalmának és jelentőségének kérdését.

Nagy sikere volt (főleg a lányoknál) annak a példájának, hogy a válasz arra a kérdésre, hogy ,,Kisasszony, szereti a sajtot?" — akár igen, akár nem a válasz —, ugyanúgy 1 egységnyi információt tartalmaz, mint a válasz arra a kérdésre, hogy ,,Kisasszony, akar a feleségem lenni?", pedig a két válasz tartalma és jelentősége nyilvánvalóan egészen más. Ezzel kapcsolatban rámutatott, hogy az elmondottak szerint az információ egysége egyetlen egy, igennel vagy nemmel megválaszolható, egyébként tetszőleges kérdésre adott válaszban foglalt információ mennyisége.

Másként kifejezve: az információ egysége egyetlen egy 0 vagy 1 jellel kifejezhető (kódolható) információ mennyisége. Így például egy a 2-alapú számrendszerben felírt szám minden egyes számjegye 1 egységnyi információt tartalmaz. Ezzel függ össze az információ egységének elnevezése: az információ egységét bit-nek nevezik, ami a *bi*nary digi*t* (angolul: kettes számrendszerbeli számjegy) rövidítése. Ebben az elnevezésben még egy szójáték is el van rejtve, hiszen ,,bit" angolul azt jelenti, hogy valaminek egy kis darabkája, morzsája, tehát a bit: *egy morzsányi információ.*

A kódolással kapcsolatban arról is szó volt, hogy általában az információ továbbítása céljából kell az információt a továbbítás módjának megfelelően kódolni. Így például a távirat továbbítása céljából az üzenetet a Morse-abc jeleivel (hosszú és rövid jelekkel) kell kódolni. A TV-adó a képet úgy kódolja, hogy azt kis pontokra bontja és annak megfelelően, hogy a pontok sötétek vagy világosak, ad le jeleket, amelyeket elektromágneses hullámok továbbítanak a TV vevőkészülékhez, amely azokat visszaalakítja képpé — más szóval dekódolja. De ennél sokkal egyszerűbb példát is lehet adni a kódolás fogalmára, amelyet tulajdonképpen mindenki jól ismer, még ha nem is nevezi így: kódolás tulajdonképpen maga az írás is, amely hangoknak betűket feleltet meg; ebben az esetben az olvasás a dekódolás. Az agyunk is valahogy kódolja az információt, amelyet emlékezetünkben elraktároz, csak ma még nem tudjuk pontosan, hogy milyen eljárással történik az agyban a kódolás és a dekódolás. Kódolás az is, amikor valaki csomót köt a zsebkendőjére, hogy erről valami eszébe jusson. Az előadó említette, hogy egyes indián törzsek ezt a fajta kódolást magas színvonalra fejlesztették: kötélre kötött csomók segítségével küldtek üzeneteket. Kódolás az is, amikor fényjeleket adnak egymásnak a hajók, vagy az Alpokban balesetet szenvedett turisták síppal adnak SOS jelet. Mindenféle titkosírás is persze kódolás — innen származik maga a ,,kódolás" szó. A gramofonlemezen, a magnószalagon is kódolva van a zene vagy a beszéd stb. Egyikünk megjegyezte, hogy úgy látszik, a kódolással tehát úgy vagyunk, mint Moliere darabjának szereplője, aki nem tudta, hogy ő egész életében prózában beszélt: mi sem tudtuk, hogy szinte minden tevékenységünk során információt kódolunk és dekódolunk.

Az előadáson éppen 32-en voltunk jelen hallgatók. Az előadó feltette a kérdést, hogy ha ő valamelyikünkre gondol, hány kérdéssel tudnánk kitalálni, hogy melyikünkre gondolt. Rögtön rávágtam, hogy 5 kérdéssel, persze az előadó megkérdezte, hogy hogyan kérdeznék. Azt válaszoltam, hogy a neveket abc-sorrendben felírnám, azután első kérdésként azt kérdezném, hogy az első 16 név között van-e a gondolt név. Akár ,,igen", akár ,,nem" a válasz, a megmaradó lehetőségek száma a felére, azaz 16-ra csökkent. Hasonlóképpen a második kérdéssel 8-ra, a harmadikkal 4-re, a negyedikkel 2-re csökkenthető a még fennmaradó lehetőségek száma és így az ötödik kérdéssel biztosan ki tudom találni, hogy a 32 hallgató közül kire gondolt. Ezek után az előadó azt kérdezte, hogy ha az 5 kérdést egyszerre kell feltennem, tehát az egyes kérdések megválasztásánál nem állnak rendelkezésemre az előző kérdésekre kapott válaszok, akkor is elég-e 5 kérdés? Erre azt válaszoltam, hogy ezt nem tudom, mivel a Bar-Kochba játéknál az ember mindig az előző kérdésekre kapott válaszok alapján választja meg a következő kérdését, de azt hiszem, hogy ha egyszerre kell a kérdéseket feltenni, akkor 5-nél több kérdésre van szükség. Ebben viszont tévedtem. Az előadó megmutatta, hogyan lehet 5 olyan kérdést egyszerre feltenni, hogy az 5 válaszból egyértelműen megállapítható, hogy a 32 hallagató közül kire gondolt. A hallgatókat meg kell számozni 0-tól 31-ig, a sorszámokat felírni a 2-es számrendszerbe, így mind a 32 névhez tartozik egy 5 jegyű, nullákból álló kettes számrendszerbeli szám (az 5-nél kevesebb jegyű számokat 5 jegyűvé tesszük azzal, hogy 0-kat írunk az elejére, pl. a 0 sorszámnak a 00000, az 1 sorszámnak a 00001 felel meg); én a 14-ik vagyok a névsorban,* tehát az én nevemnek a 01110 szám felel meg. Ezek után az öt kérdés a következő: a gondolt hallgató nevének sorszámát a 2-es számrendszerben felírva az első, második, a harmadik, a negyedik, az ötödik jegy egyes-e? Ha például erre az öt kérdésre rendre a ,,nem, igen, igen, igen, nem" válaszokat kapjuk, akkor rám gondolt az előadó. Ez nagyon meglepett, hiszen a Bar-Kochba játékban nagy gyakorlatom van, a kollégiumban sokszor játsszuk es én vagyok elismerten a legjobb Bar-Kochbázó (nemrégiben azzal arattam sikert, hogy kitaláltam a következőt: ,,kukac által rágott lyuk abban az almában, amely Newton fejére esett".), de arra még soha nem gondoltam, hogy a kérdéseket ne egymásután, hanem egyszerre tegyem fel.

Ezek után az előadó néhány további példát mondott, pl. ,,hány bit információt tartalmaz a személyi igazolvány sorszáma?" Azt mondta, hogy Magyarországon kereken 7,5 millió felnőtt állampolgarnak van személyi igazolványa. Így tehát arról van szó, hogy ha ő egy tetszőleges felnőtt magyar állampolgárra gondol, hány kérdéssel tudjuk kibarkochbázni, hogy kire gondolt. Erre persze könnyen tudtunk válaszolni. Mivel $2^{22} = 4194304$ és $2^{23} = 8388608$, tehát ehhez 23 kérdés szükséges. Ezek után azt kérdezte, hogy helyes-e azt mondani, hogy a személyi igazolvány sorszáma pontosan 23 bit információt tartalmaz. Többen is azt válaszoltuk, hogy ez akkor lesz csak pontosan igaz, ha a személyi igazolványok száma eléri a 8388608-at, tehát azt a számot amelynek a 2-alapú logaritmusa pontosan 23. Ha jelenleg csak 7 és fél millió a személyi igazolványok száma, úgy a személyi igazolványok számában foglalt információ valamivel kevesebb, mint 23 bit, de 22 bitnél persze több. Így közösen eljutottunk a következő eredményre: ha a Bar-Kochba játékban a szabályokat úgy módosítjuk, hogy pontosan N különböző dolog (személy, tárgy stb.) valamelyikére szabad csak gondolni, akkor a gondolt dolog kitalálásához $\log_2 N$ bit információra van szükség. Ezek után azt mondta az előadó, hogy próbáljuk a kapott eredményt megfogalmazni a Bar-Kochba játék nélkül. Némi próbálgatás után ez is sikerült, a következőképpen: *Ha egy adott, N elemű H halmaz egy ismeretlen x elemét megadjuk, amelyről eleve semmi mást nem tudtunk, mint hogy a H halmazhoz tartozik, az így kapott információ mennyisége $\log_2 N$ bit.* Ezt a képletet nevezik *Hartley-féle képlet*nek. Ezután az előadó az *információ additivitásának törvényét* ismertette. Legegyszerűbben ezt is a Bar-Kochba játékon keresztül lehet megérteni. Ha egyszerre két dolgot kell kitalálnunk, mondjuk x_1-et és x_2-t, mégpedig x_1-ről csak azt tudjuk, hogy az N_1 elemű H_1 halmaz eleme, x_2-ről pedig csak azt, hogy az N_2 elemű H_2 halmaz eleme, akkor ezt úgy is felfoghatjuk, hogy az (x_1, x_2) párt kell ki-

* Donát Bonifác persze a valódi nevére gondol — ő nem is tudja, hogy milyen álnevet adtam neki. R. A.

találnunk, amely eleme az összes (x_1, x_2) párok H halmazának, ahol x_1 a H_1 halmaz tetszőleges eleme és x_2 a H_2 halmaz tetszőleges eleme, függetlenül attól, hogy mi x_1 értéke. Nyilvánvaló, hogy a H halmaznak N_1N_2 eleme van és így az (x_1, x_2) pár kitalálásához szükséges kérdések száma (vagyis az (x_1, x_2) pár meghatározásában foglalt információ mennyisége) a Hartley-képlet szerint $\log_2 N_1N_2$. Másrészt azonban x_1 és x_2 kitalálását végezhetjük külön-külön, így x_1 kitalálásához $\log_2 N_1$ kérdésre, x_2 kitalálásához $\log_2 N_2$ kérdésre, összesen x_1 és x_2 együtt való kitalálásához $\log_2 N_1 + \log_2 N_2$ kérdésre van szükség, vagyis x_1 és x_2 meghatározásához szükséges információmennyiség összesen $\log_2 N_1 + \log_2 N_2$ bit. Ezen információ mennyiségre tehát látszólag két kifejezést kaptunk, de persze a kettő egyenlő egymással, a logaritmusfüggvény jólismert tulajdonsága miatt (szorzat logaritmusa egyenlő a tényezők logaritmusainak összegével):

$$\log_2 N_1N_2 = \log_2 N_1 + \log_2 N_2.$$

Így tehát eljutottunk az *információ additivitásának törvényéhez.*

Befejezésül még az információ fogalmáról beszélgettünk. Az előadó figyelmeztetett, hogy most, hogy már az információ mennyiségét számszerűleg mérni tudjuk, az „információ" szót tulajdonképpen kétféle — konkrét és absztrakt, illetve kvalitatív és kvantitatív — értelemben használjuk. Információ alatt értjük egyrészt magát a konkrét információt (értesülést), másrészt ennek számszerű mértékét, vagyis a konkrét információban foglalt absztrakt információmennyiség mértékszámát, bitben kifejezve. Célszerű csak a konkrét információt nevezni „információ"-nak, míg a konkrét információ számszerű információ-tartalmát „információmennyiség"-nek nevezni. Félreértés elkerülése végett az „információ" szó helyett időnként az „értesülés" szót fogjuk használni. Azt is mondta, hogy érdemes tisztázni, hogy az információ szón (a konkrét, kvalitatív értelemben) ugyanazt értjük-e. Azt kérte, hogy mindenki írjon fel egy papírra tíz olyan magyar szót, amelynek jelentése többé-kevésbé rokon az „információ" szó jelentésével. Én a következő tíz szót írtam fel:

1. értesülés	6. tájékoztatás
2. hír	7. felvilágosítás
3. közlés	8. tudás
4. újság	9. jellemzés
5. adat	10. bejelentés

A többiek céduláin előfordultak még e szavak következő variánsai is: ismeret, híradás, közlemény, adatszolgáltatás, tudatás, megmondás, bemondás, megadás, leírás, kijelentés.

Azzal váltunk el, hogy igen nehéz volna az „információ" szemléletes fogalmát formálisan definiálni, de ez nem is szükséges, mert amikor e szót használjuk, mindannyian lényegében ugyanarra gondolunk és a továbbiakban az információ matematikai fogalmát úgyis szabatosan definiálni fogjuk; nyomatékosan hangsúlyozta az előadó, hogy e fogalomhoz még nem jutottunk el, csak az első lépést tettük meg ebbe az irányba, azt a lépést, amit elsőnek Hartley tett meg 1928-ban.

Végül néhány feladatot oldottunk meg, amelyek segítettek a Hartley-formula értelmét megérteni. Például a következő kérdést vizsgáltuk, amely, mint az előadó mondotta, az információelmélet egy fontos fejezetéhez, a *kereséselmélet*hez tartozik: 27 aranyérménk van, amelyek közül 26 valódi, egy azonban hamis, ugyanis más fémből van, csak be van aranyozva és így szemre nem különböztethető meg a többitől; tudjuk, hogy a hamis érme könnyebb, mint a valódiak. A hamis pénz megtalálására rendelkezésünkre áll egy kétkarú mérleg, amellyel csak azt lehet eldönteni, hogy a két serpenyő tartalma egyforma nehéz-e és ha nem, melyik a nehezebb. Kérdés: hány mérés szükséges a hamis pénz megtalálásához? Mielőtt a feladatot megoldottuk volna, először a szóbanforgó információmennyiségek kiszámítása útján a következőképpen kaptunk egy alsó becslést a szükséges mérések számára: a hamis pénz bármelyik lehet a 27 közül, tehát a hiányzó információ a Hartley-formula szerint $\log_2 27$.

Mármost minden mérésnek csak 3 eredménye lehetséges (a bal oldali serpenyő nehezebb, a jobb oldali serpenyő nehezebb, ill. a kettő egyenlő súlyú) és így egy-egy mérés $\log_2 3$ információt adhat csak. Ha tehát x mérést végzünk, úgy kell, hogy $x \log_2 3 > \log_2 27$ legyen. Mivel $\log_2 27 = 3 \log_2 3$, ebből következik, hogy $x \geq 3$, vagyis legalább 3 mérés szükséges. 3 méréssel viszont valóban meg lehet találni a hamis pénzt: először a mérleg mindkét serpenyőjébe 9 – 9 érmét teszünk. Ha az egyik serpenyő felszáll, az abban levő 9 érme közt van a hamis; ha egyensúlyban van, akkor a maradék 9 között van a hamis érme. Így egy méréssel a lehetőségek számát 9-re csökkentettük. Másodszorra ebből a 9-ből teszünk hármathármat a mérleg két serpenyőjébe és így a következő mérés után már csak három érme van, amelyik számításba jön. Harmadszorra e 3 érme közül teszünk egyet-egyet a mérleg két serpenyőjébe és így akármi is a mérés eredménye, megtaláljuk a hamis pénzt.

*

Az előadás végén az volt az érzésem, hogy amit hallottam, teljesen értem. Most, hogy átgondoltam az egészet, látom, hogy egy sereg kérdés nyitva maradt.

Az világos, hogy egy igennel vagy nemmel megválaszolható kérdésre adott válasz egy egységnyi, azaz egy bit információt tartalmaz; igen ám, de mi van, ha a Bar-Kochba játékban ügyetlenül kérdezek és azt, amit 5 kérdéssel ki lehetett volna találni, az ötödik kérdés után még nem tudom kitalálni: hogyan lehetséges ez, hiszen ügyetlen kérdezésnél is 5 kérdésre 5 választ és így 5 bit információt kapok? Itt látszólag valami ellentmondás van: van, amikor elég 5 bit egy 32 elemű halmaz egy elemének kitalálásához, máskor pedig nem elég? Az információ mennyisége nem függhet attól, hogy én jól kérdezek-e. Másként kifejezve: nyilván, ha ügyetlenül kérdezek, akkor 5 kérdésre kapott válaszból 5 bitnél kevesebb információt kapok — mondjuk, csak 3 bitet. De hiszen az egyes kérdésekre adott válaszok külön-külön ekkor is egy-egy bitet tartalmaznak. Hová veszett e hát 2 bit? E kérdés első pillanatban rejtélyesnek látszott, de azután eszembe jutott, hogy mi történt legutóbb, amikor Bar-Kochbát játszottunk, és ez segített megoldani a rejtélyt. Az történt ugyanis, hogy aznap este fáradt és szórakozott voltam és ez lehetett az oka, hogy feltettem a kérdezés során olyan kérdést, amelyet már egy perccel előbb megkérdeztem és megválaszoltak. „De hisz ezt már kérdezted" — mondták a többiek kórusban és azt ajánlották, hogy ha fáradt vagyok, hagyjuk abba — és ez is történt. Kissé bosszantott az eset akkor, de most jól jött. Rájöttem ugyanis, hogy az ügyetlen kérdezés legegyszerűbb módja az, ha a második alkalommal a kérdező egyszerűen megismétli az első kérdést. Ez esetben persze továbbra is igaz, hogy mind az első kérdésére, mind a második (az elsővel azonos) kérdésére kapott válasz egy-egy bit információt tartalmaz, de a második bit nem új információ, hanem ugyanaz, amit már az első válaszban megkapott a kérdező; így tehát az ügyetlen kérdező két azonos kérdésre adott két azonos válasz együttvéve nem két, hanem csak egy bit információt tartalmaz. Lényegében ez a helyzet akkor is, ha nem ennyire durva hibát követ el valaki, csak éppen nem a legcélszerűbb módon kérdez. Ez esetben persze nem pontosan ugyanazt az információt kapja meg kétszer, hanem a másodszorra kapott egy bit információnak csak egy része új, egy része olyan információ, amely az első kérdésre kapott válaszban már benne volt, vagyis a két bit részben átfedi egymást. Ha pl. a két bitnek a fele közös, akkor a két válaszból együttvéve nem 2, hanem csak $1\frac{1}{2}$ bit információt kaptunk. Ha például az első 8 szám egyikét kell kitalálnom és először azt kérdezem, hogy a gondolt szám az 1, 2, 3, 4 számok egyike-e és függetlenül a választól másodszorra megkérdezem, hogy a gondolt szám az 1, 5, 6, 7 számok egyike-e, akkor a kérdésre adott válasz nyújt ugyan némi új információt, de ez kevesebb, mint egy teljes bit és éppen ezért ennél az ügyetlen kérdezésnél előfordulhat, hogy összesen 3 helyett 4 kérdésre van szükség, míg ha másodszorra azt kérdezem, hogy a gondolt szám az 1, 2 és 5, 6 számok valamelyike-e, akkor a harmadik kérdésre biztosan ki tudom találni a gondolt számot. Igaz viszont, hogy az említett rossz kérdezés esetében előfordulhat, hogy már a második kérdésre kapott válasz után ki tudom találni a gondolt számot, míg a jó kérdezés mellett ez nem fordulhat elő: annál mindig szükség van a harmadik kérdésre! Így tehát a rossz kérdezés tulajdonképpen hazárdjátékot jelent. Az az érzésem, hogy ennél a hazárdjátéknál az ember átlagban veszít; ezt majd egyszer később még végig akarom gondolni. Most előbb egy másik problémát akarok jól átgondolni: az a benyomásom, hogy ennek tisztázása szükséges az előbbi probléma megértéséhez is. Arról van szó, hogy mit jelent a nem egész értékű információ? Az az állítás, hogy valamely N elemű H halmaz egy ismeretlen elemének kitalálásához $\log_2 N$ bitnyi információra van szükség, teljesen világos, ha $\log_2 N$ egész szám, vagyis ha $N = 2^k$, ahol k pozitív egész szám, mert ez esetben valóban pontosan k kérdéssel ki lehet találni az ismeretlen elemet, kevesebb kérdéssel viszont nem. De mit jelent tulajdonképpen az, hogy valamit $\log_2 N$ kérdéssel ki lehet találni, ha $\log_2 N$ nem egész szám? Ezen a kérdésen az előadó valahogy átsiklott; persze lehet, hogy legközelebb akar erre visszatérni, engem azonban most izgat a kérdés.

Ezen a kérdésen sokat gondolkoztam, amíg rájöttem a megoldásra. A következő meggondolás vezetett célhoz: egy 7 elemű halmaz egy elemének kitalálásához 4 kérdésre van szükség, míg a Hartley-formula szerint egy 7, ill. 9 elemű halmaz egy elemének megadásához $\log_2 7 = 2{,}80735\ldots$, illetve $\log_2 9 = 3{,}16993\ldots$ bit információ szükséges. Ha azonban a hét elemű H_1 halmaz egy x_1 elemét x (pl. a hét egy napját) és a 9 elemű H_2 halmaz egy x_2 elemét (pl. a nap 9 bolygója egyikét) egyszerre akarom kitalálni, ehhez nem $3 + 4 = 7$, hanem csak 6 kérdésre van szükségem, hiszen összesen $7 \cdot 9 = 63$ lehetőség közül kell egyet megtalálni és $63 < 64 = 2^6$ (illetve $\log_2 63 = \log_2 7 + \log_2 9 = 5{,}97728 < 6$). Ezek után már könnyen meg tudtam magamnak válaszolni a kérdést teljes általánosságban, hogy milyen értelemben igaz tetszőleges N számra, amely nem 2 hatványa, hogy egy N elemű halmaz egy ismeretlen elemének kitalálásához $\log_2 N$ kérdésre van szükség (ahol tehát $\log_2 N$ nem egész szám!). Ez a következőt jelenti. Ha nekem az N elemű halmaz egy ismeretlen elemét nem egyszer kell kitalálnom, hanem sokszor, mondjuk k-szor, például úgy, hogy k másik játékossal játszom Bar-Kochbát és ezek mindegyike egymástól függetlenül gondol az N elemű halmaz egy-egy elemére és nekem ezt a k elemet egyszerre kell kitalálnom, akkor ezt tehetem úgy, hogy nem egyenként kérdezek a k dologra, hanem a k ismeretlen dologból álló $(x_1, x_2, \ldots, x_k)$ k-ast igyekszem kitalálni. Mivel ez N^k különböző értéket vehet fel, az ehhez szükséges kérdések számát úgy kapom meg, hogy veszem N^k 2 alapú logaritmusát és ezt felkerekítem egész számmá: ha ez a kérdésszám S_k, akkor tehát

$$\log_2 N^k \leq S_k \leq \log_2 N^k + 1.$$

Mivel

$$\log_2 N^k = k \log_2 N,$$

így tehát

$$\log_2 N \leq \frac{S_k}{k} \leq \log_2 N + \frac{1}{k}.$$

Mivel S_k azt jelenti, hogy az N elemű halmaz k elemének kitalálásához hány kérdésre van szükség, $\frac{S_k}{k}$ azt jelenti, hogy az N elemű halmaz egy elemének kitalálásához *átlagban* hány kérdésre van szükség. Mivel $1/k$ tetszőleges kicsinnyé tehető azáltal, hogy k értékét elég nagynak választjuk, a kapott eredmény azt jelenti, hogy ha N nem 2 hatvány, akkor ha elég sokszor kell egy N elemű halmaz egy ismeretlen elemét kitalálni, akkor az ehhez *átlagban* szükséges kérdések száma tetszőleges kevéssel lesz csak nagyobb $\log_2 N$-nél. Ebben az értelemben igaz tehát, hogy pl. egy 7 elemű halmaz egy ismeretlen elemének kitalálásához 2,80735. . . kérdésre van szükség. Például az $N = 7$ esetben, mivel $7^6 = 117649 < 2^{17}$, tehát ha egy 7 elemű halmaz hat elemét egyszerre akarom kitalálni, ehhez 17 kérdés elég és így a halmaz egy elemének kitalálásához átlagban $\frac{17}{6} = 2{,}833\ldots$ kérdés elégséges.

A Bar-Kochba játékkal kapcsolatban utánanéztem hogy tulajdonképpen ki volt Bar-Kochba és miért róla nevezték el ezt a játékot. Amikor i. sz. 135-ben a zsidók szabadságharcot indítottak a római elnyomás ellen, Bar-Kochba volt a vezérük. (A Bar-Kochba név azt jelenti, hogy „A csillag fia".) A túlerőben levő római hadsereg ostrom alá vette a várat, melyet Bar-Kochba vezetésével egy kislétszámú, de elszánt helyőrség hősiesen védett. Ezek történeti tények. Mármost a Bar-Kochba játék nevét állítólag onnan kapta, hogy Bar-Kochba kiküldött egy felderítőt, hogy kikémlelje a rómaiak táborát; a felderítő azonban a rómaiak elfogták és kegyetlenül megkínozták, többek között kivágták a nyelvét. A felderítő megszökött a római fogságból és jelentkezett Bar-Kochbánál, beszélni azonban nem tudott és így szavakban nem tudta elmondani, hogy mit látott. Bar-Kochba erre igennel és nemmel megválaszolható kérdéseket tett fel neki, amelyekre a megkínzott katona fejbólintással, ill. fejrázással válaszolt. Így Bar-Kochba mindent megtudott a néma felderítőtől a római seregről, amire a vár védelméhez szüksége volt.

A baj csak az, hogy e meggyőzően hangzó történetről a forrásmunkák nem tudnak. Valószínűleg ezt a legendát az költötte, aki a Bar-Kochba játékot kitalálta és Bar-Kochbáról elnevezte, de hogy ez ki volt, azt nem sikerült eddig kideríteni. Úgy látszik, hogy a játék Budapesten keletkezett a század elején. A játék Budapesten a XX. század elején mindenesetre igen népszerű volt, főleg az írók körében; Karinthy és Kosztolányi írásaiban többször is említésre kerül a játék, ők, továbbá Szomaházy István nagy mesterei voltak a Bar-Kochba játéknak.

Elgondolkoztam azon, hogy ha igaz volna a Bar-Kochbaról szóló történet, akkor ő tulajdonképpen az információelmélet előfutára lett volna. A Bar-Kochba-legendának azonban úgy látszik, nincsen semmi történeti alapja. Érdekes volna viszont megállapítani, mióta ismeretes, hogy igennem válaszokkal, tehát két jelből álló jelsorozatokkal minden információ kifejezhető (kódolható); úgy látszik, ezt a tényt régóta ismerik — erre vall mindenesetre egy régi indiai monda. Így hát az információelmélet előzményei mindenképpen nagyon messzire nyúlnak vissza, annak ellenére, hogy igen fiatal tudomány. Újabb példa ez arra az igazságra, amivel Thomas Mann Jákobja kezdődik: „Mélységes mély a múltnak kútja. . ."

2. előadás

Valóban, az előadó éppen azzal kezdte, amire én is rájöttem: Megmagyarázta, hogy mit jelent a Hartley-formula, ha $\log_2 N$ nem egész szám. Ezek után arról beszélt, hogy amikor eddig azt mondtuk, hogy egy N elemű halmaz egy ismeretlen elemét kell kitalálni, tulajdonképpen hallgatólagosan feltettük, hogy ez az elem egyformán valószínű. A valóságban azonban ez csak ritkán teljesül. Amikor arról beszélünk, hogy ξ a $H = \{x_1, x_2, \ldots, x_N\}$ halmaz egy ismeretlen eleme, ez tulajdonképpen azt jelenti, hogy ξ egy olyan *valószínűségi változó*, amelynek lehetséges értékei $x_1, x_2, \ldots, x_N$. Mármost jelölje p_k annak a valószínűségét, hogy ξ az x_k értéket veszi fel ($k = 1, 2, \ldots, N$), akkor az általános esetben $p_1, p_2, \ldots, p_N$ tetszőleges pozitív számok, amelyeknek az összege 1. Amikor megtudjuk, hogy az adott esetben ξ melyik lehetséges értéket vette fel, vagyis ha *megfigyeljük* a ξ valószínűségi változót, ez a megfigyelés bizonyos mennyiségű információt tartalmaz, amelyet $H(\xi)$-vel jelölünk. Ennek a $H(\xi)$ információmennyiségnek a meghatározásával foglalkoztunk mostanáig is, csak eddig arra az esetre szorítkoztunk, amikor ξ lehetséges értékeit, tehát az $x_1, x_2, \ldots, x_N$ értékeket ugyanazzal a valószínűséggel, vagyis $\frac{1}{N}$ valószínűséggel veszi fel, tehát amikor $p_1 = p_2 = \ldots = p_N = \frac{1}{N}$.

Ebben a speciális esetben érvényes az

$$H(\xi) = \log_2 N$$

Hartley-féle formula. Az általános esetre a $H(\xi)$ információmennyiséget a

$$H(\xi) = p_1 \log \frac{1}{p_1} + p_2 \log \frac{1}{p_2} + \ldots + p_N \log \frac{1}{p_N}$$

ún. *Shannon-féle formula* adja meg. $H(\xi)$ szemléletes jelentése az általános esetben lényegében ugyanaz, mint az egyenlő valószínűségek esetében, egy egész csekély módosítással. A Bar-Kochba játék nyelvén kifejezve $H(\xi)$ értelmezése a következő: ha ξ jelöli azt, amit a Bar-Kochba játékban ki kell találni, tehát a másik játékos p_1 valószínűséggel gondol x_1-re, p_2 valószínűséggel x_2-re, s. i. t., . . ., p_N valószínűséggel x_N-re, akkor ezt a játékot elég sokszor játszva és a legcélszerűbb kérdezési módszert alkalmazva a gondolt dolog kitalálásához átlagban, 1-hez tetszőleges közeli valószínűséggel, tetszőleges kevéssel több, mint $H(\xi)$ kérdésre van szükség. Az eltérés a Hartley-féle speciális esettel szemben abban áll, hogy itt hozzá kell tennünk azt a megszorítást, hogy „1-hez tetszőleges közeli valószínűséggel", amire a szimmetrikus esetben nem volt szükség.

A Bar-Kochba játék nyelve helyett a kódolás fogalmával kifejezve $H(\xi)$ definíciója a következőképpen fogalmazható meg: ξ jelentsen egy valószínűségi változót, amely az $x_1, x_2, \ldots, x_N$ értékeket rendre $p_1, p_2, \ldots, p_N$ valószínűséggel veszi fel. Végezzünk ξ értékére vonatkozólag egymásután független megfigyeléseket, akkor e megfigyeléseket $0-1$ sorozatokkal kódolva elérhető, hogy egy megfigyelés kódolásához átlagban 1-hez tetszőleges közeli valószínűséggel, $H(\xi) = p_1 \log \frac{1}{p_1} + p_2 \log \frac{1}{p_2} + \ldots + p_N \log \frac{1}{p_N}$-nél tetszőleges kevéssel több 0 vagy 1 jel kerüljön felhasználásra.

A fenti állítás helyességét először a következő példán ellenőrizzük: Két pénzdarabbal dobjunk és ξ jelentse, hogy az érmék közül hány mutat fejet. Így tehát ξ a 0, 1 és 2 értékeket veszi fel, rendre $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$ valószínűségekkel. Ennélfogva e példában azt kell megmutatnunk, hogy ξ értékét sok egymásutáni dobásnál megfigyelve, az eredménysorozatot lehet úgy $0-1$ sorozat formájában kódolni, hogy 1-hez tetszőlegesen közeli valószínűséggel átlagban egy dobás kódolásához tetszőleges kevéssel több, mint

$$\frac{1}{4}\log_2 \frac{1}{\left(\frac{1}{4}\right)} + \frac{1}{2}\log_2 \frac{1}{\left(\frac{1}{2}\right)} + \frac{1}{4}\log_2 \frac{1}{\left(\frac{1}{4}\right)} = 1{,}5$$

számjegyre legyen csak szükség. Könnyen belátható, hogy a célszerű eljárás a következő: ha egy dobásnál 1 fejet dobtunk, azaz $\xi = 1$, akkor ezt az eredményt egy 1-es számjegy leírásával kódoljuk; ha $\xi = 0$ (vagyis ha mindkét érme írást mutat), akkor ezt az eredményt a 00 jelsorozattal kódoljuk, végül, ha $\xi = 2$ (vagyis ha mindkét érme fejet mutat), akkor ezt az eredményt a 01 jelsorozattal kódoljuk.

Ilyen módon egy-egy dobás eredményét vagy egy vagy két számjeggyel kódoljuk aszerint, hogy az eredmény $\xi = 1$ vagy más; mivel ξ az 1 értéket $\frac{1}{2}$ valószínűséggel veszi fel, tehát egy dobásnak megfelelő kódszó hossza olyan η valószínűségi változó, amelynek értéke $\frac{1}{2}$ valószínűséggel 1 és $\frac{1}{2}$ valószínűséggel 2, tehát a kódszó hosszának várható értéke $1{,}5 = \frac{1}{2} 1 + \frac{1}{2} \cdot 2 = 1{,}5$. Ennélfogva a nagy számok törvénye szerint, ha elég sok dobást végzünk, akkor az egyes dobásoknak megfelelő kódszavak átlagos hossza 1-hez tetszőleges közeli valószínűséggel $1{,}5 + \varepsilon$-nál kisebb lesz, akármilyen kis pozitív szám is ε.

A kódolási eljárás, amit e példában alkalmaztunk, a Bar-Kochba játék nyelvére lefordítva azt jelenti, hogy ha ki kell találnunk, hogy a másik játékos két érmével hány fejet dobott, először azt kell kérdeznünk, hogy egy fejet dobott-e? Ha a válasz igen, akkor egy kérdéssel kitaláltuk, amit kell, míg ha a válasz nem, másodszorra azt kérdezzük, hogy a fejek száma 2-e? Akár „igen", akár „nem" a válasz, tudni fogjuk, hogy mennyi a fej-dobások száma, ti. az első esetben 2, a másodikban 0. Ha jól meggondoljuk, hogy miért ez a legjobb kérdezési mód, rájövünk, hogy arról van szó, hogy ha lehetséges, mindig olyan kérdést kell feltenni, amelyre az „igen" és a „nem" válasz valószínűségei pontosan egyenlők; ha ez nem lehetséges, olyan kérdést kell feltenni, hogy az „igen" és „nem" valószínűsége olyan közel legyenek egymáshoz, amennyire ez lehetséges. Ezen a módon be lehet látni a Shannon-féle formula helyességét az általános esetre nézve is. Az órán még egy konkrét példát vizsgáltunk meg, amikor egy pénzdarabbal addig dobunk amíg először jön ki második alkalommal ugyanaz az eredmény, tehát másodszorra fej, vagy másodszorra írás és ξ magát az egész dobássorozatot jelenti. Könnyen belátható, hogy a kívánt helyzet már a második dobásra bekövetkezik, ha az első két dobás eredménye azonos, míg, ha az első két dobás eredménye különböző, akkor a harmadik dobásnál következik be, hiszen utóbbi esetben a harmadik dobás szükségképpen megegyezik vagy az első vagy a második dobás eredményével. Így tehát ξ értékei az FF, II, FIF, FII, IFF, IFI dobássorozatok (ahol F fej-dobást, I írás-dobást jelöl) és ezek valószínűségei $\frac{1}{4}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}$, ennélfogva

$$H(\xi) = 2 \cdot \frac{1}{4} \log_2 4 + 4 \cdot \frac{1}{8} 8 \log_2 8 = 2{,}5.$$

A célszerű kódolás e példákban egyszerűen abban áll, hogy F helyett zérust, I helyett egyest írunk és így a ξ fent felsorolt értékeinek megfelelő kódszavak (a sorrendet megtartva) 00, 11, 010, 011, 100, 101 lesznek és ezért a kódszó várható hossza $\frac{1}{2} \cdot 2 + \frac{1}{2}\, 3 = 2{,}5$ lesz; így megint csak a nagy számok törvényéből következik, hogy ξ értékét igen sokszor megfigyelve és az eredményt a megadott módon kódolva, 1-hez tetszőleges közeli valószínűséggel az egy megfigyelésre eső $0-1$ jelek átlagos száma kisebb lesz, mint $2{,}5 + \varepsilon$, akármilyen kis pozitív szám is ε.

A tárgyalt két példában azért volt olyan egyszerű megtalálni a legcélszerűbb kódolást, mert a $p_1, p_2, \ldots, p_N$ számok mind $\frac{1}{2}$ hatványaival voltak egyenlők és így minden lépésben lehetséges volt a még ki nem zárt lehetőségeket úgy két osztályra bontani, hogy azok valószínűsége pontosan egyenlő legyen. Az általános esetben ez nem lehetséges és ezért a Shannon-formula helyességének igazolása valamivel bonyolultabb, bár a lényeg ugyanaz, mert végeredményben a nagy számok törvényén múlik a dolog.

Az általános esetben a Shannon-formula igazolásának bizonyítását az előadó csak vázolta, hogy a gondolatmenet világos legyen, a részletek kidolgozását ránk bízta. A bizonyítás menete a következő: Ha a ξ valószínűségi változó az $x_1, x_2, \ldots, x_N$ értékeket rendre $p_1, p_2, \ldots, p_N$ valószínűséggel veszi fel és ξ értékét igen sokszor — mondjuk n esetben — megfigyeljük, úgy, hogy a megfigyelések függetlenek, akkor a valószínűségszámításból jólismert szabály szerint (független események együttes bekövetkezésének valószínűsége egyenlő az egyes események valószínűségeinek szorzatával), egy olyan eredménysorozat valószínűsége, amelyben n_1-szer fordul elő az x_1 érték, n_2-ször az x_2 érték, ..., n_N-szer az x_N érték, $p_1^{n_1} p_2^{n_2} \ldots p_N^{n_N}$ lesz. Mármost a nagy számok törvénye szerint, ha δ és ε tetszőleges kis pozitív számok, ha n elég nagy, akkor legalább $1-\delta$ valószínűséggel

$\frac{n_1}{n}$ ε-nál kevesebbel fog különbözni p_1-től, ...,

$\frac{n_2}{n}$ ε-nál kevesebbel fog különbözni p_2-től, s. i. t. ..

$\frac{n_N}{n}$ ε-nál kevesebbel fog különbözni p_N-től, és így

az előbb felírt valószínűség közelítőleg a $q = (p_1^{p_1} p_2^{p_2} \ldots p_N^{p_N})^n$ számmal lesz egyenlő. Mivel az összes lehetséges eredménysorozatok valószínűségeinek összege 1, tehát ξ megfigyelt értékei sorozata δ-nál kisebb összvalószínűségű szabálytalan esetektől eltekintve közelítőleg $\frac{1}{q}$ számú sorozat valamelyikével lesz egyenlő; ezen sorozatok 0 és 1 jelekkel való kódolásához körülbelül $\log_2 \frac{1}{q}$ számú ilyen jegyre van szükség. Mivel

$$\log_2 \frac{1}{q} = n \log_2 \cdot (p_1^{-p_1} p_2^{-p_2} \ldots p_N^{-p_N}) =$$

$$= n \left(p_1 \log_2 \frac{1}{p_1} + \ldots + p_N \log_2 \frac{1}{p_N} \right),$$

tehát ezzel bebizonyítottuk, hogy ξ egy értékének 0 és 1 jelekkel való kódolásához 1-hez tetszőlegesen közeli valószínűséggel átlagban körülbelül $H(\xi)$ hosszúságú jelsorozat szükséges. Ezzel teljes általánosságban igazoltuk a Shannon-féle formula helyességét. Nyilvánvaló, hogy a Shannon-formula speciális esetként tartalmazza a Hartley-formulát, ha ugyanis

$$p_1 = p_2 = \ldots = p_N = \frac{1}{N},$$

akkor

$$p_1 \log_2 \frac{1}{p_1} + p_2 \log_2 \frac{1}{p_2} + \ldots + p_N \log_2 \frac{1}{p_N} =$$

$$= N \left(\frac{1}{N} \log_2 \frac{1}{\left(\frac{1}{N} \right)} \right) = \log_2 N.$$

Azt is bebizonyítottuk, hogy ha N értékét rögzítjük, akkor a $p_1 \log_2 \frac{1}{p_1} + \ldots + p_N \log_2 \frac{1}{p_N}$ kifejezés minden, az egyenletes eloszlástól különböző $(p_1, \ldots, p_N)$ eloszlásra kisebb lesz, mint $\log_2 N$. Ez azt jelenti, hogy ha egy ξ valószínűségi változóról tudjuk, hogy csak N különböző értéket vehet fel, úgy e változó egy értéke akkor fogja a legtöbb információt tartalmazni, ha ξ lehetséges értékeit ugyanazzal a valószínűséggel veszi fel.

A bizonyítás a következő: az $y = \log_2 \frac{1}{x}$ függvényt ábrázoló görbe, mint jól tudjuk, konvex. Ha e görbén N tetszőleges pontot veszünk fel és azokba tetszőleges pozitív tömegeket helyezünk, akkor tehát e tömegpontok tömegközéppontja mindig a görbe fölött lesz: ez azonban azt jelenti, hogy

$$p_1 \log_2 \frac{1}{p_1} + p_2 \log_2 \frac{1}{p_2} + \ldots + p_N \log_2 \frac{1}{p_N} \leq$$

$$\leq \log_2 \left(p_1 \frac{1}{p_1} + \ldots + p_N \frac{1}{p_N} \right) = \log_2 N.$$

Az óra végén még arról beszélt az előadó, hogy a

$$H(\xi) = p_1 \log_2 \frac{1}{p_1} + p_2 \log_2 \frac{1}{p_2} + \ldots + p_N \log_2 \frac{1}{p_N}$$

képletet *Shannon* és *Wiener* egymástól függetlenül állították fel 1948-ban. A képlet azonban már a múlt században szerepelt Boltzmann munkáiban, ezért a Shannon-formulát szokták *Boltzmann—Shannon formulá*nak is nevezni. Boltzmann e képletre egészen más problémával kapcsolatban jutott, mégpedig statisztikus mechanikai vizsgálatai során az *entrópiára* adta meg e képletet, több, mint fél évszázaddal Shannon előtt. Ő azt mutatta meg, hogy ha egy nagy számú molekulából álló gázban az egyes molekulák lehetséges állapotainak valószínűségei $p_1, p_2, \ldots, p_N$, akkor a rendszer entrópiája

$$H = c \left(p_1 \log \frac{1}{p_1} + p_2 \log \frac{1}{p_2} + \ldots + p_N \log \frac{1}{p_N} \right),$$

ahol c egy állandó. (A statisztikus mechanikában a természetes logaritmust használják, nem a 2-alapú logaritmust, de ez mindegy, hiszen a kettő csak egy állandó szorzóban különbözik egymástól.) Egy fizikai rendszer entrópiája, mint ismeretes, a rendszer rendezetlenségének mértéke. Ezt úgy is fel lehet fogni, hogy a rendszer entrópiája a molekulái állapotára vonatkozó *bizonytalanság* mértékszáma.

Ezen interpretáción keresztül igen egyszerűen beláthatjuk, hogy miért kapta Boltzmann ugyanazt a képletet az entrópiára, mint Shannon és Wiener az információra. Ha ugyanis jól meggondoljuk, a bizonytalanság nem más, mint információ-hiány, vagyis negatív információ, vagy másként kifejezve: az információ nem más, mint a bizonytalanság csökkenése. Mielőtt megfigyelnénk egy ξ valószínűségi változó értékét, bizonytalanságban vagyunk arra nézve, hogy ξ lehetséges értékei közül melyiket fogja felvenni. Amikor ξ értékét megfigyeljük, ez a bizonytalanság megszünik. Mármost ez a megfigyelés, mint látjuk, $H(\xi)$ bit információt tartalmaz: mivel ez az információ megszüntette a ξ értékére vonatkozólag a megfigyelés előtt fennálló bizonytalanságot, kézenfekvő e bizonytalanság mértékszámául is a $H(\xi)$ számot választani. $H(\xi)$ tehát tekinthető a ξ értékére vonatkozólag, annak megfigyelése előtt, fennálló bizonytalanság mértékszámának is. A bizonytalanság mértékszámát nevezzük entrópiának. Így tehát a Shannon-formula úgy is értelmezhető, hogy ha egy ξ valószínűségi változó az $x_1, x_2, \ldots, x_N$ értékeket rendre $p_1, \ldots, p_N$ valószínűséggel veszi fel, akkor ξ entrópiáját (tehát a ξ értékere annak megfigyelése előtt fennálló bizonytalanság mértékszámát) amelyet $H(\xi)$-vel jelölünk, a $H(\xi) = \sum p_k \log_2 \frac{1}{p_k}$ képlet alapján számíthatjuk ki.

Megkérdeztük, hogy miért jelölik az entrópiát, illetve információt a H betűvel. Az előadó azt válaszolta, hogy ezt a jelölést még Boltzmann vezette be és az ő hatására vált hagyományossá. Az előadó rámutatott, hogy egy ξ valószínűségi változó $H(\xi)$ entrópiája (ill. ami ugyanaz, a ξ valószínűségi változó megfigyelésében foglalt információ mennyisége) nem függ ξ értékeitől, vagyis az $x_1, x_2, \ldots, x_N$ számoktól (amelyekről elegendő annyit tudnunk, hogy ezek egymástól különböző számok), hanem csak azoktól a $p_1, p_2, \ldots, p_N$ valószínűségektől, amellyel ξ ezen értékeket felveszi. Ha tehát $f(x)$ egy olyan függvény, amely az $x_1, x_2, \ldots, x_N$ helyeken csupa különböző értéket vesz fel, akkor az $f(\xi)$ valószínűségi változó entrópiája ugyanakkora, mint ξ entrópiája, tehát $H[f(\xi)] = H(\xi)$. Beláttuk azt is — az $x \log_2 x$ függvény konvexitása alapján —, hogy ha $f(x)$ az $x_1, x_2, \ldots, x_N$ helyeken nem csupa különböző értéket vesz fel, akkor $H[f(\xi)] < H(\xi)$, vagyis ez esetben értéke kevésbé bizonytalan, mint ξ értéke. Az információ additivitásának törvényét, amelyet még a Hartley-formula kapcsán ismertünk fel, kiterjesztettük az általános esetre. Ez a törvény általános alakban a következőképpen szól: ha ξ és η független valószínűségi változók, akkor ξ és η együttes megfigyelésében foglalt információ mennyisége — amelyet $H((\xi, \eta))$-val jelölünk — egyenlő a ξ és η külön-külön való megfigyelésében foglalt információmennyiségek összegével, vagyis $H((\xi,\eta)) = H(\xi) + H(\eta)$. Ez az összefüggés a logaritmus függvény alaptulajdonságából következik. Ha ugyanis ξ az x_k értéket ($k = 1, 2, \ldots, N$) p_k valószínűséggel veszi fel és η az y_j értékeket ($j = 1, 2, \ldots, M$) q_j valószínűséggel veszi fel, akkor a (ξ, η) változópár az (x_k, y_j) értékpárt $p_k q_j$ valószínűséggel veszi fel, tehát (felhasználva, hogy $\sum p_k = \sum q_j = 1$) azt kapjuk, hogy

$$H((\xi, \eta)) = \sum_{k=1}^{N} \sum_{j=1}^{M} p_k q_j \log_2 \frac{1}{p_k q_j} =$$

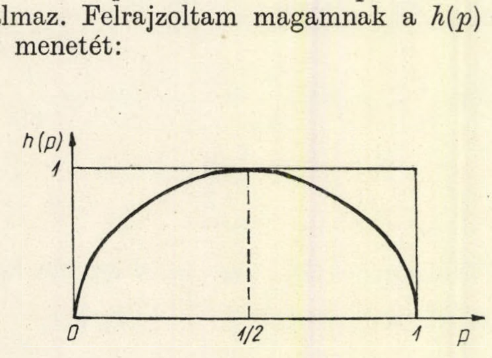
$$= \sum_{k=1}^{N} \sum_{j=1}^{M} p_k q_j \left(\log_2 \frac{1}{p_k} + \log_2 \frac{1}{q_j} \right) =$$

$$= \left(\sum_{j=1}^{M} q_j \right) \left(\sum_{k=1}^{N} p_k \log_2 \frac{1}{p_k} \right) + \left(\sum_{k=1}^{N} p_k \right) \left(\sum_{j=1}^{M} q_j \log_2 \frac{1}{q_j} \right) =$$

$$= H(\xi) + H(\eta).$$

*

Ha rosszmájú akarnék lenni, azt mondanám, hogy a második órán azt tanultuk, hogy amit az első órán tanultunk, abból tulajdonképpen semmi nem igaz. De persze ez nem így van, csak arról van szó, hogy amit az első órán még pontatlanul fogalmaztunk meg, azt most szabatosabbá tettük. Úgy látom, az előadó módszere abban áll, hogy bonyolult fogalmakat több lépésben magyaráz meg. Első közelítésben bizonyos másodrendű jelentőségű dolgokat elhanyagol, azért, hogy a lényeget jobban kidomborítsa; miután a fogalommal már megbarátkoztunk, pótlólag helyreigazítja azt, ami az első közelítésben pontatlan volt. A fogalmak kialakításának ez a módszere hasonlít ahhoz, ahogy egy szobrász kifarag egy darab márványból vagy fából egy szobrot. Először csak a fő körvonalakat alakítja ki és csak azután tér át a részletek pontos kifaragására. Ennek a módszernek — bár számomra szokatlan — kétségtelenül vannak előnyei, főleg az, hogy szinte rászorít az önálló, kritikus gondolkodásra. Persze, a szokásos jegyzetelés ilyen tanítás mellett nem megy, hiszen a későbbi előadások alapján tulajdonképpen az előző előadáson hallottakat korrigálni kell a jegyzetben is. Ha a szokásos módon írnék jegyzetet (csak definíciókat, tételeket és bizonyításokat jegyezve fel), akkor ez nehézséget okozna nekem, de az én napló-módszerem mellett ez nem okoz zavart. Ezért is örülök, hogy elhatároztam magam a naplóvezetésre. Nézzük meg hát közelebbről, hogy az első előadásban hallottakból mi szorul korrekcióra. Elsősorban nyilván korrekcióra szorul az a megállapítás, hogy egy igen vagy nem válasz (vagy egy jel, amely csak két értéket, pl. a 0 és 1 értékeket veheti fel), mindig 1 bit információt tartalmaz. A második órán a hallottakat az $N = 2$ esetre specializálva ezt az állítást, úgy kell módosítani, hogy egy ilyen jel akkor tartalmaz 1 bit információt, ha a jel két értéke eleve egyenlő valószínűségű — azaz mindkettő $\frac{1}{2}$ valószínűségű —; minden más esetben a jelben foglalt információ mennyisége 1 bitnél kisebb. Pontosabban: ha pl. a Bar-Kochba játéknál felteszünk egy kérdést, amelynél az „igen" válasz valószínűsége p és így a „nem" válasz valószínűsége $1-p$, akkor e kérdésre a válasz a Shannon-féle formula szerint $h(p) = p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p}$ bit információt tartalmaz. Felrajzoltam magamnak a $h(p)$ függvény menetét:



1. ábra.

A görbe a $p = \frac{1}{2}$ pontban (és csak ott) eléri az 1 értéket, másutt 1-nél kisebb; a görbe a $p = \frac{1}{2}$ ponton át húzott függőleges egyenesre szimmetrikus, hiszen $h(p)$ képletéből látható, hogy $h(p) = h(1-p)$ és így $h\left(\frac{1}{2}+x\right) = h\left(\frac{1}{2}-x\right)$, ha $0 \leq x \leq \frac{1}{2}$. Ez persze így is kell, hogy legyen, hiszen a válaszban foglalt információ mennyisége szempontjából nyilván mellékes, hogy az „igen" válasz valószínűsége egyenlő-e p-vel, vagy a „nem" válasz valószínűsége egyenlő p-vel, mely esetben az „igen" valószínűsége $1-p$. Például, ha valaki egy kockával dob és én azt kérdezem tőle, hogy „hatost dobtál?", akkor, mivel e kérdésre az „igen" válasz valószínűsége $\frac{1}{6}$, a kérdésemre adott válasz

$$h\left(\frac{1}{6}\right) = \frac{1}{6}\log_2 6 + \frac{5}{6}\log_2\frac{6}{5} = 0{,}65$$

bit információt tartalmaz csak, nem egy teljes bitet.

Vagy visszatérve az előadó tréfájára, ha megkérdezem egy lánytól, hogy akar-e a feleségem lenni, a válasz információtartalma attól függ, hogy mekkora a valószínűsége, hogy igennel fog válaszolni. Ha e valószínűség igen kicsi, vagy ha közel van egyhez, akkor a válasz igen kevés információt fog tartalmazni, hiszen szinte biztosan azt a választ kapom, amire számítok. Amikor idáig eljutottam, egyszerre világossá vált előttem az előadónak az a megjegyzése, hogy ha a ξ valószínűségi változó a lehetséges értékeit különböző valószínűséggel veszi fel, akkor ξ értékének kitalálásánál úgy kell mindig a kérdéseket feltenni, hogy az igen válasz valószínűsége olyan közel legyen $\frac{1}{2}$-hez, amennyire ez lehetséges: ez azért van így, mert így kapjuk a válaszból a lehető legtöbb információt. Ezt persze az előadó is megmondhatta volna, de talán jobbnak látta, hogy mi jőjjünk erre rá. Most már azt is ki tudom számítani, hogy ügyetlen kérdezésnél a Bar-Kochba játéknál mennyi információt kapok. Ha például az első 8 szám egyikét kell kitalálnom és a 8 lehetőség mindegyike eleve ugyanolyan valószínűséggel bír, vagyis mindegyik valószínűsége $\frac{1}{8}$, és első kérdésként azt kérdezem, hogy a gondolt szám az 1, 2, 3, 4 számok egyike-e, akkor, mivel e kérdésre az „igen" válasz valószínűsége $\frac{1}{2}$, pontosan 1 bit információt kapok. Ha most második kérdésként azt teszem fel, hogy a gondolt szám az 1, 5, 6, 7 számok egyike-e, akkor abban az esetben, ha az első kérdésre igen volt a válasz, a második kérdésre nyilván $\frac{1}{4}$ (feltételes) valószínűséggel kapok igenlő választ, míg ha az első kérdésre nemleges volt a válasz, a második kérdésre $\frac{3}{4}$ (feltételes) valószínűséggel kapok igenlő választ; így mindkét esetben a második kérdésre kapott válasz csak $h\left(\frac{1}{4}\right) = 0{,}83653$ bit új információt tartalmaz, vagyis a második válaszban foglalt 1 bit információból csak 0,83653 bit új információ, a többi 0,16347 bit olyan információ, amit már tudtam.

A most tanultak alapján újból végiggondoltam a hamis-pénz problémát is. Rájöttem, hogy csak azért lehetséges valóban 3 méréssel megtalálni, hogy a 27 érme közül melyik könnyebb a többinél, mert lehet a méréseket úgy választani, hogy a 3 lehetséges mérési eredmény egyenlő valószínűségű legyen, egyébként ugyanis hiába van a mérésnek 3 lehetséges kimenetele, egy mérés $\log_2 3$-nél kevesebb információt adna. Ha például nem 27, hanem 35 érme között kell megtalálnom a hamisat, és a mérleg két serpenyőjébe 8—8 érmét teszek, akkor a három mérési eredmény valószínűsége $\frac{8}{25}, \frac{8}{25}, \frac{9}{25}$ és így ez a mérés a Shannon-formula szerint nem $\log_2 3 = 1{,}58496$ bit információt, hanem csak ennél valamivel kevesebbet,

$$2 \cdot \frac{8}{25}\log_2\frac{25}{8} + \frac{9}{25}\log_2\frac{25}{9} = 1{,}58269$$

bit információt ad.

Sokat gondolkoztam azon is, hogy mit is jelent, hogy az információ úgy is értelmezhető, mint a bizonytalanság csökkenése. Valóban, amikor elkezdődik a Bar-Kochba játék, teljes bizonytalanságban vagyok arra vonatkozólag, amit feladtak. A kérdéseimre adott válaszokból kapott információ következtében ez a bizonytalanság a játék folyamán egyre csökken és amikor kitaláltam, amit feladtak, teljesen megszűnik. Ha a bizonytalanság eredetileg B bit volt, miután x bit információhoz jutottam, definíció szerint még $B-x$ bit bizonytalanság áll fenn.

Így tehát a játék során bármely időpontban a gondolt dologra vonatkozóan még fennálló bizonytalanság és az addig gyűjtött információ összege állandó, hiszen $x + (B-x) = B$. Ez az összefüggés nagyon ismerősnek tűnt nekem, tudtam, hogy valami hasonló összefüggéssel már találkoztam: némi gondolkodás után rájöttem, hogy a helyzet nagyon hasonlít a potenciális és kinetikus energia összegének állandóságára az esés folyamán. Amikor egy tégla a háztetőn nyugszik, csak potenciális energiája van, kinetikus energiája nincs. Amikor a tégla esni kezd, egyre nő a kinetikus energiája úgy, hogy a kettő összege az esés során állandó. Ez a hasonlat egy izgalmas problémát vet fel: *úgy látszik, van bizonyos hasonlóság, analógia, az információ és az energia fogalmai között!* Úgy tűnik továbbá, hogy létezik egy olyan törvény, amelyet az információ megmaradási törvényének lehet nevezni. Az előbb észrevett összefüggés ugyanis úgy is kimondható, hogy a Bar-Kochba játék során a már megkapott és a még hiányzó információ összege állandó. Elhatároztam, hogy a következő órán megkérdezem az előadót, hogy jól látom-e, hogy az információ és az energia fogalmai között lehet bizonyos párhuzamot vonni.

Még egy ponton látok hasonlóságot: az energiaátalakítás (pl. elektromos energiának mechanikai energiává való alakítása stb.) és az információ kódolása között érzek bizonyos analógiát. Amikor például egy képben foglalt információt a TV adó kódolja elektromágneses hullámokban foglalt információvá és ezt az információt a TV vevőkészülék visszaalakítja képpé, ez nagyon emlékeztet a mechanikai energia elektromos energiává való alakítására a dinamóban és távvezetéken való átvitel után mechanikai energiává való visszaalakítására az elektromotorban. Az az érzésem, hogy valóban valami alapvető rokonság van az energia és az információ fogalma között: nagyon várom a következő órát, hogy ezt a kérdést tisztázzuk.

NAGY TISZTASÁGÚ ALKALIHALOGENID EGYKRISTÁLYOK NÖVESZTÉSE ZÓNAOLVASZTÁSSAL

Voszka Rudolf
BOTE Biofizikai Intézet
(MTA Kristályfizikai Tanszéki Kutató Csoport)

Extrém tisztaságú egykristályok előállítása mind az alapkutatás, mind az alkalmazások szempontjából alapvető fontosságú. Az alkalihalogenidekkel kapcsolatban hosszú ideig az volt a vélemény, hogy a viszonylag könnyen és jól tisztítható anyagok közé tartoznak. Az utóbbi 10 évben azonban, főként az ionizáló sugárzás által kiváltott folyamatok tanulmányozása révén kiderült, hogy ez a vélemény téves és számos eredmény, amelyet kizárólag az alaprácsnak tulajdonítottak, szennyezésekkel kapcsolatos. Intézetünkben 1964, óta foglalkozunk nagy tisztaságú alkalihalogenid egykristályok előállításával és a következőkben összefoglaljuk lényegesebb eredményeinket.

Alkalihalogenidek vonatkozásában a következő problémával állunk szemben. Az alkalihalogenidek többé-kevésbé higroszkóposak, sőt a kereskedelemben kapható, vízből kristályosított p. a. alapanyagok vízzárványokat is tartalmazhatnak. Az ilyen alapanyag megolvasztásakor még a leggondosabb vákuumszárítás mellett is hidrolizál, és az olvadékból nőtt kristály nagy koncentrációban tartalmaz OH^- ionokat, amelyek szubsztitúciósan helyezkednek el a rácsban. A p. a. anyagok 10^{-5} mol/mol nagyságrendben más, főleg két vegyértékű fémionokat (M^{2+}) is tartalmaznak, amelyek szintén szubsztitúciósan épülnek be a rácsba. Ezek beépülésekor az elektromos semlegesség azáltal valósul meg, hogy a rácsban megfelelő számú kationvakancia is létrejön. Vegyük tekintetbe azt is, hogy az OH^- és az M^{2+} ionok egymással reakcióba léphetnek és a rácsban $M(OH)_2$ molekulák képződhetnek.

Egyes szerzők tisztítás céljából *kémiai eljárásokkal* kísérleteztek [1—2]. Magunk is alkalmaztunk kémiai módszereket [3], tapasztalataink szerint azonban 10^{-7} mol/mol-nál nagyobb tisztaság a szokásos laboratóriumi körülmények között nem érhető el.

Másokhoz hasonlóan [4—5], a *vákuumdesztillálást* is felhasználtuk tisztítás céljából, de ez a módszer sem hozta meg a remélt eredményt [6]. Mindkét eljárás a p. a. anyagnál tisztábbat nyújt, de egyik sem oldja meg az olvasztásnál fellépő hidrolízis problémáját.

A szerzők legtöbbje a *zónatisztítást* alkalmazza. A hidrolízistermékek kiküszöbölésére, ill. a további hidrolízis megakadályozására különböző atmoszférákat vesznek igénybe: halogénhidrogén gáz- [7], halogéngáz atmoszférát [8—10], halogénezett szénhidrogének (széntetraklorid, kloroform stb.) gőzeit [11]. A zónázásnál alkalmazott tégelyanyag lehet kvarc [3, 7, 9] grafit [8, 12] vagy platina [13]. Tégelymentes zónázással is kísérleteztek [14], ez azonban a viszonylag kis felületi feszültség miatt csak 6 mm átmérőig járt sikerrel.

Az intézetünkben alkalmazott és ezideig legeredményesebb eljárás három lépésből áll:

Az oxigéntartalmú szennyezések eltávolítása az olvadék halogénezett szénhidrogénekkel való kezelésével;

többszöri függőleges zónázás kvarccsőben kb. 60 mm/ó sebességgel;

egykristály megnövesztése ugyanabban a berendezésben, kb. 2 mm/ó sebességgel.

a) *Az oxigéntartalmú szennyezések eltávolítása* érdekében kloridoknál széntetrakloriddal (CCl_4), bromidoknál bromoformmal ($CHBr_3$) kezeltük az olvadékot. A kínálkozó lehetőségek közül ui. az említett módszer a leghatásosabb, ami pl. kloridok esetében az alábbi meggondolás alapján látható be. Vegyük számba a következő reakciókat:

1. $OH^- + HCl = Cl^- + H_2O$

2. $OH^- + Cl_2 = Cl^- + HCl + \frac{1}{2}O_2$

3. $2OH^- + CCl_4 = 2Cl^- + 2HCl + CO_2$

Sósavgázzal való kezeléskor víz képződik, amely újra hidrolízishez, tehát OH^- ionok keletkezéséhez vezethet. Klórgáz esetében oxigén képződik, amely ugyancsak reakcióba léphet az olvadékkal. Széntetraklorid alkalmazásakor viszont széndioxid jön létre, amely nem reagál az olvadékkal, hanem a gázárammal távozik. A széntetrakloridos kezelés során természetesen nemcsak az OH^- ionok, hanem más oxigéntartalmú anionok is, mint O_2^-, CO_3^- stb. kicserélődnek Cl^- ionokra.

Ha az anionszennyezők eltűntek az olvadékból, az olvadék telítődik klórgázzal s felületi feszült-