A STATISZTIKUS CSOPORTELMÉLET EGYES PROBLÉMÁIRÓL*

Írta: ERDŐS PÁL és TURÁN PÁL

Századunk matematikája gazdag jellemző új vonásokban. Az első mindjárt a század legelején jelentkezett a valós függvénytanban BOREL és LEBESGUE azon észrevételével, hogy számos tétel sokkal elegánsabban és áttetszőbben mondható ki, ha egy „kis" halmazt figyelmen kívül hagyunk. A nyert tételek frappáns volta a matematika majdnem minden területén hatott és ez alól az algebra sem volt kivétel; elég VAN DER WAERDEN azon tételére gondolnunk, mely szerint fix n-re egy jól meghatározott értelemben majdnem minden racionális egész együtthatós n-edfokú algebrai egyenlet *Galois*-csoportja az S_n n-edfokú szimmetrikus csoport. A strukturális algebra rohamos fejlődése a húszas években azonban ezen statisztikus algebrának nevezhető irányzatot teljesen háttérbe szorította. Ennek kifejlesztése azonban véleményünk szerint még a strukturális algebra számára is bírhat jelentőséggel. G. CANTORnak a transzcendens számok létezésére vonatkozó bizonyításának gondolatát általánosítva tekintsünk olyan A struktúrákat, melyek reprezentálhatók egy oly R térben, melyben pl. valamilyen értelemben mérték bevezethető. Olyasszerű kérdések, melyek bizonyos E tulajdonságú A struktúrák létezését kérdezik, eldönthetők lehetnek kimutatván azt, hogy azon A-k, melyek E-tulajdonsággal *nem* bírnak, R-ben „kis" halmazt alkotnak, szemben azzal, hogy jelenleg ilyen esetekben direkt konstrukciókkal kell kísérleteznünk, ami sok tapasztalat szerint mindig jóval nehezebb. Így pl. a strukturális algebrához közel álló kombinatorikus gráfelméletben ERDŐS kimutatta oly n-szögpontú G gráfok *létezését*, hogy sem G, sem $\bar{G}$ nem tartalmaz $[4 \log n]$-szögpontú teljes részgráfot; ilyen tulajdonságú *explicite megadott* gráfok megadása sokak próbálkozása dacára mindmáig nem sikerült. L. BERS egy erevani előadásában múlt szeptemberben általa kleinszerűnek (kleinian) nevezett csoportok létezését mutatta ki így, anélkül, hogy egyetlen ilyen csoportot explicite meg tudott volna adni. Nem lehetetlen, hogy ily módon a végesen generálható csoportokra vonatkozó Burnside-probléma is az ismertnél jóval egyszerűbben oldható meg.

Jelen előadásban véges csoportok statisztikus elméletével foglalkozunk. Ez esetben, ha a csoport rendje $\leqq n$, R-tér gyanánt S_n választható, a tér elemei az n-elemű P permutációk és egy R-beli halmaz mértéke a benne foglalt P-k száma. Így tehát eredményeink egyben az S_n, a legklasszikusabbnak nevezhető véges csoport, elméletében is új eredmények. A legelső kérdés, mellyel foglalkoztunk, a P-k csoportelméleti rendjének, $O(P)$-nek statisztikus vizsgálata, melyre vonatkozólag D. H. LEHMER még 1963-ban közölte velünk azon tapasztalatot, hogy

* Elhangzott a *MTA III. Osztály*ának 1966. május 18-i ülésén.

vaktában kivett P-re $O(P)$ „kicsi". Hogy $O(P)$ „nagyon nagy" sohasem lehet, azt már LANDAU kimutatta, megmutatván, hogy ha

$$\max_{P \in S_n} O(P) = g(n),$$

akkor

$$\lim_{n \to \infty} \frac{\log g(n)}{\sqrt{n \log n}} = 1. \tag{1}$$

Tehát $O(P)$ az a priori lehetséges $n!$-hoz képest *mindig* kicsi. Mármost azt találtuk, hogy tetszőleges kis $\varepsilon > 0$-nál $k_\varepsilon(n)$-el jelölve azon P-k számát, melyekre

$$\frac{1}{2} - \varepsilon < \frac{\log O(P)}{\log^2 n} < \frac{1}{2} + \varepsilon, \tag{2}$$

fennáll, hogy

$$\lim_{n \to \infty} \frac{k_\varepsilon(n)}{n!} = 1. \tag{3}$$

Tehát az (1)-nél jóval többet mondó (2) reláció „majdnem mindegyik" S_n-beli P-re igaz. Sőt, (3) fennáll azon P-k számára is, melyekre (2) helyett a jóval erősebb

$$\left| \log O(P) - \frac{1}{2} \log^2 n \right| \leqq \omega(n) \log^{3/2} n \tag{4}$$

egyenlőtlenség teljesül, hacsak

$$\lim_{n \to \infty} \omega(n) = +\infty \tag{5}$$

tetszőleges lassan.

Orientációképp jegyezzük meg, hogy azon P-k rendje, melyek kanonikus ciklus-előállítása egyetlen n-hosszúságú ciklusból áll,

$$n = e^{\log n}$$

tehát „elég messze" $e^{\frac{1}{2}\log^2 n}$-tól és számuk mégis

$$(n-1)! = \frac{1}{n} \cdot n!,$$

ami „aránylag nagy". Ez is arra mutat, hogy a statisztikus maximum „nem nagyon éles"; tehát, hogy mégis *van*, azt mutatja, hogy a tétel nem lehet felszínen mozgó. A bizonyítás változatos segédeszközöket használ fel az analízisből, számelméletből, valószínűségszámításból és algebrából; ezek különböző arányú részvételének szükségessége ezen elméletre karakterisztikusnak látszik. A bizonyítás részleteibe itt belemenni már csak azért sem érdemes, mert az kevéssel ezelőtt a *Zeitschrift für Wahrscheinlichkeitstheorie*ban megjelent;[1] ez kiadja azt is, hogy ha P kanonikus ciklus-előállításában fellépő *különböző* ciklushosszak

$$n_1 < n_2 < \ldots < n_k,$$

[1] Bd. 4 (1965) p. 175—186.

akkor „majdnem mindegyik" P-re

$$e^{-\log n(\log\log n)^4} \leqq \frac{O(P)}{n_1 n_2 \dots n_k} \leqq 1. \tag{6}$$

Ennek birtokában elérhetőnek látszik annak igazolása, hogy az $O(P)$ csoportelemrend „logaritmikusan Gauss-eloszlású", azaz tetszőleges valós c-re azon P-k számát $G_c(n)$-el jelölve, melyekre

$$\log O(P) \leqq \frac{1}{2}\log^2 n + c\log^{3/2} n, \tag{7}$$

fennáll a

$$\lim_{n\to\infty} \frac{G_c(n)}{n!} = \sqrt{\frac{3}{2\pi}} \int_{-\infty}^{c} e^{-\frac{3\lambda^2}{2}} d\lambda$$

reláció[2]. Megjegyezzük, hogy a bizonyítások minden nehézség nélkül kidolgozhatók lettek volna, úgy, hogy limeszreláció helyett minden egyes véges n-re fennálló egyenlőtlenségeket adjanak ki.

Ezen eredmények más alakban is kifejezhetők. Jelentős szerepet játszanak a matrixelméletben az $n\times n$-es permutációmatrixok melyek minden sora csupa 0-ból és egyetlen 1-esből áll és az egyes 1-esek oszlopindexei az $1, 2, \dots, n$ elemek egy P permutációját alkotják. Ezen matrixok, mint könnyen látható, a matrixszorzásra nézve csoportot alkotnak, mely izomorf a P-k alkotta permutációcsoporttal. Tehát az összes tételek, melyeket S_n-re mondottunk vagy ki fogunk mondani, állanának az $n\times n$-es permutációmatrixok multiplikatív csoportjára is.

A kimondott tétel, bár egyszerű törvényszerűséget ad meg $O(P)$-re majdnem mindegyik P-re, távolról sem világít meg egy csomó egyéb kérdést, az $O(P)$ rend eloszlási kérdéseit „távol" az $e^{\frac{1}{2}\log^2 n}$ értéktől (persze a *Landau*-féle

$$1 \leqq O(P) \leqq e^{(1+\varepsilon)\sqrt{n\log n}}$$

közben). Ilyen felvilágosítások lennének nyerhetők az $O(P)$ különböző momentumainak ismeretéből, ami rögtön felszínre hozza az $O(P)$ rend

$$M_1 = \frac{1}{n!}\sum_P O(P)$$

várható értékének kérdését. Erre vonatkozólag azt találtuk, hogy alkalmas pozitív numerikus c_1-el

$$M_1 < e^{c_1\sqrt{\frac{n}{\log n}}}; \tag{8}$$

valószínű, hogy

$$\lim_{n\to\infty} \frac{\log M_1}{\sqrt{\frac{n}{\log n}}}$$

létezik és véges.

[2] Ezt azóta be is bizonyítottuk; e bizonyítás a tárgya sorozatunk III. dolgozatának.

A csoportelmélet sok kérdésében nem annyira az $O(P)$-rend értéke, mint inkább aritmetikai struktúrája fontos. Ennek illusztrálására elég megemlíteni FROBENIUS következő tételét, melyből pár sorban nyerte, hogy négyzetmentes rendű csoport mindig feloldható; e tétel szerint, ha m négyzetmentes és

$$m = kl,$$

ahol l minden prímfaktora nagyobb k minden prímfaktoránál, akkor minden m-rendű csoportban éppen l olyan elem van, melyek rendje l osztója.[3] Egy varsói előadás után A. SCHINZEL azt a kérdést vetette fel, hogy vajon igaz-e, hogy majdnem minden P-re $O(P)$ páros. Kimutattuk, hogy ez igaz, sőt sokkal több is; majdnem minden P-re $O(P)$ osztható *minden* p^α prímhatvánnyal, mely

$$\leqq \frac{\log n}{\log\log n}\left\{1+3\frac{\log\log\log n}{\log\log n}-\frac{\omega(n)}{\log\log n}\right\}, \tag{9}$$

hacsak $\omega(n)\to\infty$ tetszőleges lassan. Azon további kérdésre, vajon e tétel mennyire javítható, a felelet az, hogy lényegileg nem, amennyiben kimutattuk, hogy majdnem minden P-re $O(P)$ *nem* osztható legalább egy oly p prímszámnak már első hatványával sem, mely

$$\leqq \frac{\log n}{\log\log n}\left\{1+3\frac{\log\log\log n}{\log\log n}+\frac{\omega(n)}{\log\log n}\right\} \tag{10}$$

hacsak $\omega(n)\to\infty$. Igen valószínű, hogy tetszőleges valós c mellett azon P-k száma, melyekre $O(P)$ legalább egy, a

$$\frac{\log n}{\log\log n}\left\{1+3\frac{\log\log\log n}{\log\log n}+\frac{c}{\log\log n}\right\} \tag{11}$$

mennyiséget meg nem haladó p prímszámmal nem osztható, $n!$-al osztva $n\to\infty$-re egy $\psi_1(c)$ határfüggvényhez tart.

E tételek két elegáns konzekvenciája külön említést érdemel. Először is, ha b tetszőleges pozitív egész szám, úgy majdnem mindegyik P rendje osztható b-vel. Másodszor, majdnem mindegyik P rendje *nem* négyzetmentes.

Eddig az $O(P)$-rend „kis" prímfaktorainak statisztikus vizsgálatával foglalkoztunk. Milyen statisztikus tételek állíthatók az $O(P)$-rend „nagy" prímfaktorairól? Ha $f(P)$ jelenti az $O(P)$ maximális prímfaktorát, akkor azt találtuk, hogy majdnem minden P-re (a triviális $f(P)\leqq n$-en túlmenőleg)

$$f(P) \leqq n e^{-\frac{1}{\omega(n)}\sqrt{\log n}} \tag{12}$$

hacsak $n\to\infty$. Tehát majdnem mindegyik P olyan, hogy $O(P)$-nek nincs „túl nagy" prímfaktora. Hogy e tétel is csak keveset javítható, azt azon további eredményünk mutatja, hogy majdnem minden P-re

$$f(P) \geqq n e^{-\omega(n)\sqrt{\log n}}. \tag{13}$$

Ez érdekes kontrasztban áll a racionális egészeknél fennálló tényállással; míg

[3] „Über auflösbare Gruppen I, II". Sitzungsber. der Berliner Akademie 1893.

(12)—(13)-ból következőleg majdnem mindegyik P-re (azaz legfeljebb $o(n!)$ kivétellel) $O(P)$ olyan, hogy maximális prímfaktora

$$ne^{-\omega(n)\sqrt{\log n}} \quad \text{és} \quad ne^{-\frac{1}{\omega(n)}\sqrt{\log n}}$$

között van, addig az n-et meg nem haladó egészek maximális prímfaktorára ilyen éles tétel nincs; így azon egészek sűrűsége, melyek maximális prímfaktora n^α és n^β közé esik ($\frac{1}{2} < \alpha < \beta < 1$), könnyen láthatólag

$$= \sum_{n^\alpha \leqq p \leqq n^\beta} \frac{1}{p} \to \log \frac{\beta}{\alpha}, \quad \text{ha} \quad n \to \infty,$$

tehát pozitív. Valószínű, hogy itt tetszőleges *pozitív* c mellett azon P-k száma, melyekre $O(P)$ maximális prímfaktora

$$< ne^{-c\sqrt{\log n}},$$

$n!$-al osztva itt is egy $\psi_2(c)$ határeloszláshoz tart.

A (9) tétel mellékesen azt is kiadja, hogy majdnem minden P-re $O(P)$ „eléggé összetett", legalább

$$(1-\varepsilon)\frac{\log n}{(\log\log n)^2} \qquad n > n_0(\varepsilon) \tag{14}$$

különböző prímfaktora van. Ez felveti azon kérdést, vajon fennáll-e pontosabb statisztikus törvényszerűség $U(P)$-re, az $O(P)$ rend különböző prímfaktorainak *teljes* számára is. Azt találtuk, hogy majdnem mindegyik P-re

$$U(P) = (1 + o(1)) \log n \log\log n \tag{15}$$

és ugyanez áll $V(P)$-re is, az $O(P)$-ben fellépő *összes* prímfaktorok számára is (azokat multiplicitás szerint véve). Tehát a (14) alatti prímfaktorok az összeseknek csak kis részét adják majdnem mindegyik P-re. A (15) alatti tétel analógiában áll a racionális egészeknél fennálló tényállással, amennyiben HARDY—RAMANUJAN tétele szerint az m egészre a különböző prímfaktorok számát $U(m)$-mel jelölve majdnem minden $m \leqq n$-re

$$U(m) = (1 + o(1)) \log\log n \tag{16}$$

és analóg a multiplicitása szerint vett prímfaktorszámra, $V(m)$-re is.

A (9) és utána említett tételek bizonyításába akár csak vázlatosan belebocsátkozni nincs idő; ezek azon gondolat megfelelő adaptációján alapulnak, mellyel egyikünk disszertációjában, 32 évvel ezelőtt, a (16) alatti HARDY—RAMANUJAN tételt igazolta. Ez a gondolat, a valószínűségszámításból régen ismert *Csebisev*-egyenlőtlenség alkalmazása egy akkor teljesen távolinak tartott területen, ma már a számelméleti folklore-hoz tartozik, azaz idézés nélkül használják, pedig sokat lehetne beszélni arról, hogy *akkor* milyen váratlanul hatott és *azóta* milyen fejlődést indított meg. E bizonyítások az „On some problems of a statistical group-theory" c. sorozatunk második közleményeképp az *Acta Math. Hung.*-ban fognak megjelenni.

További természetes kérdés S_n különböző tulajdonságú részcsoportjainak statisztikus viselkedése. Mivel minden P elem rendje egyben az általa generált

ciklikus részcsoport rendje is, előbbi tételeink eziránban is megfogalmazhatók lennének. Újabb kérdés eziránban az, hogy S_n-nek hány, *páronként nem-izomorf* ciklikus részcsoportja van és vajon *ezen* részcsoportok rendjére fennáll-e statisztikus jellegű tétel. Ez másképp azt jelenti, hogy az $O(P)$-rend hány *különböző* értéket vehet fel a (7)-ben adott közön belül és ezek eloszlásáról mi mondható ki. Erre vonatkozólag először is azt találtuk, hogy $O(P)$ *különböző* értékeinek számát $W(n)$-el jelölve $n \to \infty$-re

$$W(n) = e^{(1+o(1))\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}}},$$

ami a (7) alatti köz hosszával összehasonlítva rendkívül kicsi! Ezen felül meg tudjuk mutatni, hogy a különböző $O(P)$-értékek legfeljebb $o(W(n))$ számú kivételével egy

$$e^{(c_2+o(1))\sqrt{n}\log^{c_3} n} \leqq O(P) \leqq e^{(c_2+o(1))\sqrt{n}\log^{c_3} n}$$

alakú egyenlőtlenségnek tesznek eleget. Itt c_2 és c_3 pozitív numerikus állandók, ahol $0 \leqq c_3 \leqq \frac{1}{2}$; értékük meghatározása inkább technikai nehézségű feladatnak látszik. Egyáltalán nem lehetetlen, hogy $c_3 = \frac{1}{2}$. Ez azt jelentené, hogy a lehetséges $O(P)$-értékek „javarésze" lényegileg olyan nagy, amilyen nagy csak lehet; hogy mégis a P-k javarészére $O(P) \sim e^{\frac{1}{2}\log^2 n}$, csak azt jelenti, hogy a legtöbb P preferálja a kevés „közepes nagy" lehetséges rend-értéket a sok „naggyal" szemben.

Azzal kapcsolatban, hogy minden G csoport, melynek rendje $\leqq n$, beágyazható S_n-be, régóta felvetődött természetes kérdés, azon legkisebb m vizsgálata egy adott G-re, hogy G beágyazható már S_m-be is. Áttetsző válasz itt is csak statisztikus értelemben várható. Itt legfeljebb n-edrendű *kommutatív* csoportok esetére megmutattuk, hogy ezek majdnem mindegyike beágyazható S_N-be, ahol

$$N = \left[\frac{n}{\psi(n)}\right]$$

hacsak

$$\lim_{x\to\infty} \frac{\log \psi(x)}{\log x} = 0.$$

E tétel sem javítható lényegesen, amennyiben kimutattuk, hogy tetszőleges kis $\varepsilon > 0$-nál már azon legfeljebb n-edrendű kommutatív csoportok száma, melyek $S_{[n^{1-\varepsilon}]}$-ba már *nem* ágyazhatók be, az összesekének már pozitív százaléka.

Megjegyezhető, hogy az említett tételek legnagyobb része automatikusan teljesül S_n helyett A_n-re, az n-edfokú alternáló csoportra is.

Ezen utóbbi tételek bizonyításai az említett sorozatunk IV. dolgozatában fognak szerepelni együtt S_n konjugált osztályaira és elemeinek centralizátoraira vonatkozó statisztikus tételekkel és így ezek bizonyításairól sem szólunk most. Lényegesebbnek tartjuk azon közvetlen feladatok megjelölését, melyek az előbb említett tételek természetes kiegészítései ill. folytatásai és az említett dolgozatokban jórészt nem szerepelnek.

1. $O(P)$ más régiókban való értékeloszlása.
2. $O(P)$ várható értékének aszimptotikus meghatározása (logaritmikusan).
3. $\psi_1(c)$ eloszlásfüggvény meghatározása és létezése.

4. A $\psi_2(c)$ eloszlásfüggvény létezése és meghatározása.

5. FROBENIUS problémája, az $x^m = e$ megoldásszáma S_n-ben. Ez csak $m = p$-re van elintézve, p fix, $n \to \infty$. A nehéz éppen az az eset, mikor m is függ n-től. (L. MOSER—M. WYMAN)[4].

6. Ha $f_n(k)$ jelenti S_n-ben azon P-k számát, melyekre $O(P) = k$, akkor mely k-kra lesz $f_n(k)$ maximális?

7. L. MOSERnek BERCOVVal[5] sikerült S_n-ben meghatározni a kommutatív részcsoportok maximális rendjét. Ez

$$\begin{array}{ll} 3^m, & \text{ha } n = 3m \\ 4 \cdot 3^{m-1}, & \text{ha } n = 3m+1 \\ 2 \cdot 3^m, & \text{ha } n = 3m+2. \end{array}$$

Az egyenlőség nyilván mindegyik esetben elérhető. Érdekes volna S_n a) összes, b) páronként nem-izomorf kommutatív részcsoportjai számának meghatározása és statisztikus tétel ezek rendjének eloszlására.

8. A. SCHINZEL sejtése. S_n majdnem mindegyik részcsoportja feloldható. Ennek igazolására elég lenne nem túl gyenge alsó becslés S_n összes részcsoportjainak számára és egy nem túl durva felső becslés a nem feloldható részcsoportokéra.

9. S_n összes részcsoportjai számának meghatározása legalább aszimptotikusan. Van-e ezek rendjére statisztikus tétel?

10. A legfeljebb n-edrendű csoportok minimális m-indexű S_m-be való beágyazhatóságának statisztikus vizsgálata.

11. S_n részcsoportjai rendje aritmetikai struktúrájának statisztikus vizsgálata.

12. Igaz-e, hogy ha $A \subset B \subset S_n$ és A és B az S_n részcsoportjai, úgy O annak a valószínűsége, hogy A a B-ben invariáns részcsoport?

13. Analóg vizsgálatok A_n helyett S_n más „nagy" részcsoportjaira.

14. Más algebrai struktúrák statisztikus vizsgálata reprezentációs terükben.

ON SOME PROBLEMS OF A STATISTICAL GROUPTHEORY

By P. ERDŐS and P. TURÁN

Summary

After a general motivation (indicating even the necessity of a statistical algebra) several simple laws are given among others for the distribution of values resp. for the arithmetical structure of the (grouptheoretical) order $O(P)$ of the elements P of S_n, the symmetric group with n letters. A list of some further problems is added.

[4] „On the solutions of $x^n = 1$ in symmetric groups" *Can. J. Math.* 7 (1955) p. 159—188.

[5] *On Abelian Permutation Groups.* (Sajtó alatt)