EKAIA (2024), artikulua prentsan/article in press
https://doi.org/10.1387/ekaia.24890
Behin-behineko bertsioa (euskara-orrazketaren faltan).

ekaia
ZIENTZIA eta TEKNOLOGIA ALDIZKARIA

ISSN: 0214-9001
e-ISSN: 2444-3255

Probabilitatea eta taldeak: azpitaldeen hazkundetik zeta-funtzioetara

(Probability and Groups: from subgroup growth to zeta functions)

*Matteo Vannacci**
Matematika saila UPV/EHU

LABURPENA: Probabilitatea eta taldeak uztartzen dituzten hainbat emaitza emango dira, talde profinituetako Haar probabilitate neurria erabiliz. Emaitza klasikoetatik hasita, gaur egungo ikerkuntzaren emaitzak ere emango dira. Bereziki, gorputz finituen gaineko errepresentazio-hazkuntza zenbait gairi lotuko diegu.
HITZ GAKOAK: Talde teoria, probabilitatea, errepresentazio teoria, azpitaldeen hazkuntza.

ABSTRACT: *Many results connecting groups to probability will be given, using the Haar measure of profinite groups. Starting from classic results, we will introduce recent reseach results. In particular, we will see many connections of representation growth over finite fields to other topics.*
KEYWORDS: Group Theory, Probability, Representation Theory, Subgroup Growth

***Harremanetan jartzeko/Corresponding author:** Matematika saila UPV/EHU, Sarriena auzoa z/g, 48091 Leioa, Espainia.
https://orcid.org/xxxx-xxxxxxxx, vannacci.m@gmail.com

Nola aipatu/How to cite: Vannacci; Matteo (2024). «Probabilitatea eta taldeak», Ekaia, DOI: https://doi.org/10.1387/ekaia.24890

Jasoa: ekainak 8, 2023; Onartua: urtarrilak 2, 2024
ISSN 0214-9001-eISSN 2444-3225 / ©2020 UPV/EHU

EKAIA (2024), artikulua prentsan/article in press
https://doi.org/10.1387/ekaia.24890
Behin-behineko bertsioa (euskara-orrazketaren faltan).

1. Atarikoa

Talde teoriaren aztergai nagusiak taldeak dira. Hainbat propietate defini ditzakegu taldeak sailkatzeko; adibidez, abeldartasuna, ebazgarritasuna, finituki sortua izatea, eta abar. Hala ere, mundu fisikoan gertatzen den bezala, batzuetan talde bati buruzko informazio partziala soilik izaten dugu eta ea informazio horretatik gure taldearen ezaugarriren bat ondoriozta dezakegun jakin nahiko genuke.

Orain da probabilitate teoria jokoan sartzen den momentua. Talde finitu guztietan P probabilitate neurri bat defini dezakegu eta, probabilite horri esker, kuantifikatu dezakegu propietate bakoitza ≪zenbat≫ betetzen den.

Artikulu honetan probabilitatearen eta talde teoriaren elkarrekintza batzuk aurkeztuko ditugu. Emaitza klasikoetatik hasita, gaur egungo ikerkuntzaren emaitzak ere emango dira. Laburpen gisa, artikuluan zehar ematen ditugun enuntziatu nagusiak zerrendatuko ditugu orain.

1.1. Emaitza klasiko nagusiak

Beharbada probabilitea talde teoriari lotzen dion lehen emaitza Gustafsonen Teorema da. Teorema hori $5/8$-*ko Teorema* moduan ere ezagutzen da. Izan bedi G talde finitua, orduan G-ren bi elementu elkarrekin trukatzeko probabilitatea honela defini dezakegu:

$$P_{\mathrm{c}}(G) = \frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2}. \tag{1}$$

A Teorema (Gustafson)**.** *Izan bedi G talde finitua. Orduan, G abeldarra ez bada, $P_{\mathrm{c}}(G) \leq 5/8$.*

A Teoremak esaten digu G abeldarra dela, G taldearen elementu ≪gehiegi≫ trukatzen badira. Gainera, A Teorema talde finituetan betetzen da, eta talde infinituetan, aldiz, badirudi ez dagoela probabilitatea definitzeko modurik. Harrigarriro, talde infinitu batzuetan ere definitu dezakegu probabilitatea, *Haar neurria* deitzen dena eta μ_G ikurraz adieraziko duguna (ikusi 3.2. atala). Haar neurria erabiliz eta (1) ekuazioan egin dugun bezala, G talde topologiko Hausdorff eta trinkoa bada, G-ren bi elementuk elkar trukatzeko probabilitatea honako modu honetan definitu dezakegu:

$$P_{\mathrm{c}}(G) = \mu\left(\{(x,y) \in G \times G \mid xy = yx\}\right)$$

eta honako hau frogatu dezakegu.

B Teorema (Gustafson)**.** *Izan bedi G talde topologiko Hausdorff eta trinko ez-abeldarra. Orduan, $P_{\mathrm{c}}(G) \leq 5/8$.*

Haar neurria eskuragai daukagunez, hori erabiliz talde infinituak aztertzen jarraituko dugu. Beste emaitza klasikoa Mann-Shaleven Teorema da. Teorema horrek talde bat finituki sortua izatea azpitaldeen hazkundeari lotzen dio eta mota horretako lehenengo emaitzako bat izan zen. Hitz batez, G talde profinitua izanik, G taldea sortzea ≪zaila≫ da, baldin eta soilik baldin G-k azpitalde maximal ≪gehiegi≫ baditu (definizioak 4. atalean aurki daitezke).

C Teorema (Mann-Shalev)**.** *Izan bedi G talde profinitua. Orduan, G positiboki finituki sortua (PFG laburtuta) da baldin eta soilik baldin G-k azpitalde maximaletako hazkunde polinomiala (G-k PMSG duela laburtuta) badauka.*

1.2. Hesiaren gainetiko begirada bat

Azkenean, Mann-Shaleven Teorematik abiatuta, antzeko ideiez zenbait emaitza interesgarri frogatu ditzakegu. Lehenik, finituki sortzearen ordez ≪finituki aurkeztua izatea≫ propietatea iker

dezakegu. Kontua da, lehenago finituki sortzea azpitalde maximalei lotuta zegoen bezala, finituki aurkeztea oso propietate esanguratsuari lotuta dagoela: UBERG propietateari. Hemen bakarrik esango dugu G taldeak UBERG propietatea duela, G taldeak gorputz finituen gaineko errepresentazio $\ll$gutxi$\gg$ baditu (ikusi 5. atala).

UBERG propietatea definitu ondoren, propietate hori talde baten $\zeta_G(s)$ zeta-funtzioa definitzeko erabil dezakegu. Horrelako zeta-funtzioak jada sarritan agertu dira talde teorian eta Matematikako beste hainbat adarretan. Hala ere, nahiz eta adibide erraz batzuk baino kalkulatzeko gai izango ez garen, badirudi gure zeta-funtzioek probabilitatearekin zerikusi sakona daukatela (xehetasunak 5. atalean aurki daitezke).

2. Oinarrizko nozioak

Atal honetan artikuluan zehar erabiltzen ditugun oinarrizko emaitzak bilduko ditugu.

2.1. Talde teoria

2.1. definizioa. Izan bitez G taldea eta $x \in G$. Orduan, G-ko x-ren *zentralizatzailea*, $C_G(x)$ ikurraren bidez adierazten duguna, honela definitzen dugu:

$$C_G(x) = \{y \in G \mid x^y = x\}.$$

Aurki lagungarria izango denez gero, G-ren x, y bi elementutarako $x^y = x$ betetzen dela baldin eta soilik baldin $xy = yx$ bada azpimarratzen dugu.

2.2. lema. *Izan bitez G taldea eta G-ren x eta g elementuak. Orduan,*

$$C_G(x^g) = C_G(x)^g.$$

Aurreko lemaren frogapen erraza talde teoriako edozein liburutan aurki dezake irakurleak, adibidez [10, Theorem. 1.4A]. Bestalde, honako oinarrizko definizio hau erabiliko dugu.

2.3. definizioa. Izan bitez G, A eta B taldeak. Orduan, G taldea *A taldearen hedadura B taldeaz* dela esango da, $N \lhd G$ azpitalde normala existitzen bada, non $A \cong N$ eta $B \cong G/N$ diren.

2.2. Talde profinituak

Artikuluaren definiziorik garrantzitsuenetako batekin hasiko gara.

2.4. definizioa. *Talde profinitua* talde topologiko Hausdorff eta trinkoa da, non azpitalde irekien ebakidura tribiala den.

Bestela esanda, G talde topologiko Hausdorff eta trinkoa talde profinitua da baldin eta soilik baldin

$$\bigcap_{N \lhd_o G} N = \{1\}$$

bada. Esan gabe doa $\ll$irekia$\gg$ topologiari dagokiola eta $\ll$normala$\gg$, ordea, talde egiturari. Irakurlea talde profinituetara ohitu dadin, azpitalde irekiek indize finitua daukatela frogatuko dugu orain.

2.5. proposizioa. *Izan bitez G talde profinitua eta $H \leq G$ azpitalde irekia. Orduan, $|G : H|$ finitua da.*

Frogapena. Argi dago G taldeko H azpitaldearen ezker koklaseek G taldearen estalki irekia osatzen dutela. Ondorioz, G talde trinkoa izanik, azpiestalki finitua atera dezakegu, eta, koklase desberdinen kopurua indizearekin bat datorrenez, H azpitaldeak indize finitua dauka. □

Honako hau talde profinituen ezaugarririk garrantzitsuenetako bat da.

2.6. lema. *Izan bitez G talde profinitua eta $H <_{\mathrm{c}} G$. Orduan, $M \leq_{\mathrm{o}} G$ azpitalde maximala existitzen da, non $H \leq M$ den.*

Frogapena. Lehenik, ohartu $H = \bigcap_{N \lhd_o G} HN$ dela (adibidez, ikusi [18, Proposition 0.3.3]). Ondorioz, $H < G$ izanik, $L \lhd_{\mathrm{o}} G$ existitzen da, non $H \leq HL < G$ den.

Beraz, $|G : HL| < \infty$ denez, indize minimoko $HL \leq M <_o G$ azpitaldea aurkitu dezakegu eta argi dago M G-ko azpitalde maximala dela. □

Notazioa. *Talde profinituekin lan egitean ohitura den bezala, talde profinituetan aipatzen ditugun azpitalde guztiak topologiarekiko itxiak eta homomorfismo guztiak jarraituak izango dira.*

2.3. Probabilitate teoria

Lehenik, iruzkin txikia azpimarratuko dugu: Ω multzo finitu bakoitzaren gainean probabilitatea defini dezakegu; hau da, Ω-ren *zenbatzeko probabilitatea* (edo *zenbatzeko neurria*), $S \subseteq \Omega$ azpimultzo bakoitzari

$$P(S) = \frac{|S|}{|\Omega|}$$

balorea esleitzen diona.

Gainera, gogora ezazu A, B bi azpimultzori *askeak* direla esaten diegula $\mu(A \cap B) = \mu(A)\mu(B)$ bada.

2.4. Talde errepresentazioak

Hemen talde errepresentazioei buruzko oroigarri txikia emango dugu.

2.7. definizioa. Izan bitez G taldea eta R eraztuna. Orduan, $\rho : G \to \mathrm{GL}_n(R)$ homomorfismoa n *dimentsioko G taldearen errepresentazioa* dela esango da.

2.8. definizioa. Izan bitez $\mathbb{F}$ gorputza, G taldea eta $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ errepresentazioa.

- Orduan, $W \leq \mathbb{F}^n$ azpiespazioa *ρ-inbariantea* dela esango dugu, $\rho(g)(W) \subseteq W$ bada $g \in G$ guztietarako.
- Bestalde, ρ errepresentazioa *irreduziblea* dela esango dugu, $\mathbb{F}^n$-ko azpiespazio inbarianterik existitzen ez bada, $\{0\}$ eta $\mathbb{F}^n$ kenduta.

Hala ere, nahiz eta ρ errepresentazioa F gorputzaren gainean irreduziblea izan, F-ren hedadura batera pasatu eta gero ρ reduziblea bihurtu daiteke, $\mathbb{F}$ gorputza ≪txikiegia≫ izan delako.

2.9. adibidea. *Izan bedi $G = C_4 = \langle \sigma \rangle$ talde ziklikoa. Orduan, C_4 taldeak honako 2 dimentsioko errepresentazio irreduzible hau du $\mathbb{R}$ gorputzaren gainean:*

$$\rho : C_4 \to \mathrm{GL}_2(\mathbb{R}),\ \rho(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Dena den, gorputza $\mathbb{C}$-raino handituz gero, ρ errepresentazioa irreduziblea ez dela dakusagu: esaterako, $\mathbb{C}$-ren gainean $\rho(\sigma)$ matrizeak i eta $-i$ balio propioak ditu, $\langle (i,1)^T \rangle$ eta $\langle (1,i)^T \rangle$ azpiespazio propioekin, hurrenez hurren.

Aurreko adibidearen arazo motak saihesteko, honako definizio hau jokoan sartzen da.

2.10. definizioa. Izan bedi $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ errepresentazioa. Orduan, ρ errepresentazioa *absolutuki irreduziblea* dela esango dugu, ρ errepresentazioa $\mathbb{F}$-ren $\bar{\mathbb{F}}$ itxitura aljebraikoan irreduziblea bada.

Azpiatal hau errepresentazio absolutuki irreduzibleen karakterizazioa ematen bukatuko dugu. Horregatik, honako emaitza hau aipatu behar dugu: $\mathrm{Gal}(\bar{\mathbb{F}}|\mathbb{F})$ Galoisen taldeak $\mathbb{F}$ gorputzaren gaineko errepresentazio balio propioetan eragiten du.

Izan bedi $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ talde-errepresentazio absolutuki irreduziblea. Orduan, [2, 1.16] emaitzaren ondorioz, $g \in G$ guztietarako $\rho(g)$ matrizearen balio propio guztiek $\mathrm{Gal}(\bar{\mathbb{F}}|\mathbb{F})$ taldearen orbita bakarra osatu behar dute. Hori azken atalean erabiliko dugu, zeta-funtzio batzuk kalkulatu ahal izateko.

2.5. Talde profinituen talde eraztunak

Izan bitez G talde finitua eta R eraztuna. Orduan, *R-rekiko G-ren talde eraztuna* honako multzo hau da:

$$R[G] = \left\{ \sum_{i=1}^{n} \lambda_i g_i \mid \lambda_i \in R,\ g_i \in G,\ i = 1, \dots, n \right\}.$$

Batuketa linealki eta biderketa G taldearen biderketa erabiliz defini ditzakegu. Gainera, R-ren elementuez biderketa eskalarra defini dezakegu. Horrela, $R[G]$ multzoari R-aljebraren egitura esleitzen diogu. Emaitza klasikoa da $R[G]$-gaineko modulu bakoitzak R-gaineko G-ren errepresentazioa ematen duela, eta alderantziz.

Bestalde, $R[G]^d$ aljebra $R[G]$-modulu librea da. Hau da, d sortzaile dituen M multzoak $R[G]$-moduluaren egitura badu, orduan $R[G]^d \twoheadrightarrow M$ homomorfismoa existitzen da.

Talde profinituen kasuan, talde profinitua ≪handiegia≫ denez (esaterako, ikusi 3.5. proposizioa), topologia kontuan hartu behar dugu talde eraztuna definitzeko. Gure lana errazteko, artikulu honetan bakarrik $\widehat{\mathbb{Z}}$-moduluak aintzat hartuko ditugu.

2.11. definizioa. Izan bedi G talde profinitua. Orduan, *$\widehat{\mathbb{Z}}$-rekiko G-ren talde eraztun osatua*, $\widehat{\mathbb{Z}}[\![G]\!]$ ikurraz adieraziko duguna, honako talde eraztun finituen alderantzizko limite hau da:

$$\widehat{\mathbb{Z}}[\![G]\!] = \varprojlim_{n \in \mathbb{N}} \varprojlim_{N \lhd_o G} (\mathbb{Z}/n\mathbb{Z})\,[G/N].$$

Talde eraztun osatua alderantzizko limitearen bitartez definitu dugunez, talde eraztun finituen ezaugarri batzuk automatikoki kasu horretara pasatzen dira; adibidez, $\widehat{\mathbb{Z}}[\![G]\!]$-gaineko modulu bakoitzak $\widehat{\mathbb{Z}}$-gaineko G-ren errepresentazioa ematen du eta $\widehat{\mathbb{Z}}[\![G]\!]$ eraztun osatua $\widehat{\mathbb{Z}}[\![G]\!]$-modulu librea da.

3. Gustafsonen teoremak

3.1. Talde finituak

3.1. definizioa. Izan bedi G talde finitua. Orduan, G-ren bi elementu elkarrekin trukatzeko probabilitatea, $P_{\mathrm{c}}(G)$ ikurraz adieraziko duguna, honela definitzen dugu:

$$P_{\mathrm{c}}(G) = \frac{|\{(x, y) \in G \times G \mid xy = yx\}|}{|G|^2}.$$

Argi dago, G abeldarra ez bada, $P_{\mathrm{c}}(G) < 1$ dela. Gustafson matematikariak 1973. urtean aurreko emaitza hobetzen duen honako teorema hau frogatu zuen.

3.2. teorema (Gustafson)**.** *Izan bedi G talde finitua. Orduan, G abeldarra ez bada, $P_{\mathrm{c}}(G) \leq 5/8$.*

Frogapena. Demagun G taldea n ordenakoa eta ez-abeldarra dela. Jarri $C = \{(x, y) \in G \times G \mid xy = yx\}$ eta definizioz,

$$P_{\mathrm{c}}(G) = \frac{|C|}{n^2} \quad \text{da.}$$

Helburua C-ren kardinala zenbatzea izanik, $x \in G$ finkatu eta gero ikus dezakegu $(x, y) \in C$ dela, baldin eta soilik baldin $y \in C_G(x)$ bada. Horregatik, $|C| = \sum_{x \in G} |C_G(x)|$ izango da. Bestalde, $x \in G$ guztietarako x-ren konjugatuen kopurua $|G : C_G(x)|$-ren berdina da, ≪Orbit-Stabilizer≫ teoremaren arabera (adibidez, ikusi [16, 1.6.1]).

Ondorioz, G-ren $x_1, \ldots, x_k$ elementuak konjugazio klaseen ordezkari gisa hartuz, 2.2. lematik honako hau ondoriozta dezakegu:

$$|C| = \sum_{i=1}^{k} |G : C_G(x_i)| \cdot |C_G(x_i)| = \sum_{i=1}^{k} n = k \cdot n.$$

Gainera, $P_{\mathrm{c}}(G) = k/n$ izango da. Hortaz, $k/n \leq 5/8$ dela frogatzea baino ez zaigu geratzen.

Taldea ez-abeldarra dela gogoratuz eta (behar izanez gero) ordezkariak berrantolatuz, $t < k$ existitzen da, non $x_1, \ldots, x_t$ taldearen zentroan ez dauden ordezkariak diren. Horrenbestez, $x_{t+1}, \ldots, x_k$ zentroko elementu ez-tribialak dira eta $k = t + |Z(G)|$ da. Klase-ekuazioaren arabera, honako ekuazio hau beteko da:

$$n = |G| = |Z(G)| + \sum_{i=1}^{t} |G : C_G(x_i)|.$$

Hipotesia erabiliz, $|G : C_G(x_i)| \geq 2$ dela ondoriozta dezakegu $i = 1, \ldots, t$ guztietarako. Ondorioz, $(n - |Z(G)|)/2 \geq t$ izango da. Hortaz, $k = t + |Z(G)| \leq (n + |Z(G)|)/2$ dela ondoriozta dezakegu. Berriro, G ez-abeldarra dela kontuan hartuz, $n/|Z(G)| \geq 4$ izango da; hain zuzen ere, $n/|Z(G)| < 4$ izango balitz, $G/Z(G)$ ziklikoa eta G abeldarra izango lirateke, kontraesana batera iritziz. Hortaz, $|Z(G)| \leq n/4$ izateak $k \leq (n + |Z(G)|)/2 \leq (n + n/4)/2 = 5/8 \cdot n$ dela dakar berarekin. Horrela, $P_{\mathrm{c}}(G) = k/n \leq 5/8 \cdot n/n = 5/8$ dela frogatu dugu, nahi genuen moduan. □

Ez da zailegia frogatzea aurreko teoremaren bornea hobeezina dela.

3.3. adibidea. *Har dezagun D_8 taldea, 8 ordenako talde dihedrikoa dena, honako aurkezpen honen bitartez idatzita:*

$$D_8 = \langle x, y \mid x^2 = y^4 = 1,\ x^{-1}yx = y^{-1} \rangle.$$

Erraz kalkula daiteke, D_8-k honako 5 konjugazio klase hauek dituela: $\{1\}$, $\{y^2\}$, $\{y, y^3\}$, $\{x, xy^2\}$, $\{xy, xy^3\}$. *Aurreko teoremaren frogapenetik $P_{\mathrm{c}}(D_8) = 5/8$ dela ondoriozta dezakegu.*

3.2. Talde infinituak

Talde finituen kasua ikusita, irakurle erneak galde lezake ea talde infinituetarako antzeko teoremak froga ote genitzakeen. Aurrerago 3.2. teoremaren orokorpena frogatuko dugu, baina lehendabizi konzeptu batzuk sartu behar ditugu.

Lehenengo arazoa da probabilitatea nola definitu. Talde finituetan probabilitea jada definituta dugunez, talde infinituak beraien zati finituen bitartez ikertzen saia gintezke. Hain zuzen ere, G talde infinitua bada eta $N \lhd G$ indize finituko azpitalde normala bada, orduan G/N zatidurak bere zenbatzeko probabilitate neurria darama, multzo finitua delako (cfr. 2.3. atala). Orain, ea probabilitate horiek guztiak elkartzea litekeena den galde daiteke. Erantzuna baikorra den arren, artikulu honetan ezin izango ditugu horri buruzko xehetasun guztiak eman; eta oinarrizko definizioak ematearekin konformatuko gara.

3.4. definizioa. Izan bedi G talde topologiko Hausdorff eta trinkoa. Orduan, G-ren gainean μ probabilitate neurri ez-tribial boreldarra existitzen da, *Haar neurria* deitzen dena, non honako ezaugarri hauek betetzen baititu:

1. **Ezkerretik translazio-inbariantea**: $g \in G$ eta $S \subseteq G$ azpimultzo boreldar guztietarako $\mu(gS) = \mu(S)$.
2. **Zenbakigarriki batukorra**: $\{A_n\}_{n\in\mathbb{N}}$ gertakizun disjuntuen multzo zenbakigarri guztietarako
$$\mu\left(\bigsqcup_{n\in\mathbb{N}} A_n\right) = \sum_{n\in\mathbb{N}} \mu(A_n).$$
3. **Kanpotik erregularra**: $S \subseteq G$ azpimultzo trinko guztietarako
$$\mu(S) = \inf\{\mu(U) \mid S \subseteq U,\ U \text{ irekia}\}.$$
4. **Barnetik erregularra**: $U \subseteq G$ azpimultzo ireki guztietarako
$$\mu(U) = \sup\{\mu(K) \mid K \subseteq U,\ K \text{ trinkoa}\}.$$

Azken bi propietateek μ neurri erregularra dela esaten dute, baina, artikulu honen gainerakoan, ez ditugu propietate horiek gehiago erabiliko. Aldiz, (1) propietatea erabilgarria da aurreko kapituloarekiko lotura egiteko: laster frogatuko dugu G-ren G/N zatidura finituetan μ neurria G/N-ren zenbatzeko neurriarekin bat datorrela.

Izan bitez G talde topologiko Hausdorff eta trinkoa, $H \leq G$ indize finituko azpitaldea eta $N \lhd G$ indize finituko azpitalde normala, non $N \leq H$ den. Demagun $\widetilde{\mu}$ neurria G/N-ren zenbatzeko probabilitatea dela. Zenbatekoa da $\mu(H)$ neurria? Lehenik, μ probabilitatea izanik, $\mu(G) = 1$ da. Bestalde, H indize finitukoa izanik, G-n H-ren koklaseen $g_1, \ldots, g_n$ ordezkariak finka ditzakegu; beraz, honako hau izango dugu:

$$1 = \mu(G) = \mu\left(\bigcup_{i=1}^{n} g_i H\right) = \sum_{i=1}^{n} \mu(g_i H) = n \cdot \mu(H). \tag{2}$$

Ohar bedi 1. eta 2. propietateak erabili ditugula. Ondorioz, $\mu(H) = 1/|G : H|$ dela dugu. Azkenik,

$$\widetilde{\mu}(H/N) = \frac{|H/N|}{|G/N|} = \frac{1}{|G : H|} = \mu(H)$$

dela dakusagu; hau da, μ neurriak $\widetilde{\mu}$ probabilitatea induzitzen du G/N zatidura taldean.

Haar neurria definitu ondoren, oso ondorio interesgarri batzuk atera ditzakegu talde profinituei buruz; horien artean dago honako proposizio hau.

3.5. proposizioa. *Izan bedi G talde profinitua. Orduan, G infinitua bada, G ez-zenbakigarria izango da.*

Frogapena. Demagun G zenbakigarria dela. Haar neurria edukirik,

$$1 = \mu(G) = \mu\left(\bigsqcup_{g\in G} \{g\}\right) = \sum_{g\in G} \mu(\{g\}) = \sum_{g\in G} \mu(\{1\}) =$$
$$= \begin{cases} 0 & \mu(\{1\}) = 0 \text{ bada} \\ \infty & \mu(\{1\}) > 0 \text{ bada} \end{cases} \quad \text{dela dugu,}$$

eta bi kasuetan hipotesiak kontraesan batera garamatza. □

Irakurleari komenigarria izango litzaioke aurreko frogapenean Haar neurriaren (1) eta (2) propietateak non erabili ditugun pentsatzea.

Orain, 3.2. teoremaren orokorpena ikusteko prest gaude. Argi dago, G talde trinkoa bada, $G \times G$ talde trinkoa ere badela, $G \times G$ taldearen gainean biderkadura topologia jarriz, eta frogatu daiteke $G \times G$-ren Haar neurria $\mu \times \mu$ biderkadura neurria dela.

Lehenago egin dugun bezala, honako modu honetan defini dezakegu $G \times G$-ko elkarrekin trukatzen diren elementuen azpimultzoa:

$$C = \{(x, y) \in G \times G \mid xy = yx\}.$$

Haar neurria eskura izanik, C neurtzea gustatuko litzaiguke. Hori dela eta, C neurgarria dela erakutsi behar dugu; hain zuzen, C itxia dela frogatuko dugu. Ohartu $f : G \times G \to G$ funtzioa, $(x, y) \mapsto xyx^{-1}y^{-1}$, jarraitua dela, eta, ondorioz, $C = f^{-1}(1)$ itxia eta neurgarria dela. Esandakoa kontuan hartuz, G talde trinko guztietarako P_c probabilitatea honako modu honetan defini dezakegu:

$$P_{\mathrm{c}}(G) = (\mu \times \mu)(C).$$

Beste alde batetik, G-ko azpitalde ≪natural≫ gehienak neurgarriak dira. Esaterako: erraz frogatu daiteke $Z(G) = \bigcap_{g \in G} C_G(x)$ dela, eta $C_G(x)$ azpitalde itxiak direnez, $Z(G)$ itxia eta neurgarria dela.

3.6. oharra. Hurrengo frogapenean taldeen gaineko integralak agertuko dira. Irakurlea ez litzateke izutu beharko, honako bi konzeptu erraz hauek baino ez baititugu erabilko.

(a) **Fubiniren teorema.** Ziur aski, irakurleak teorema honen adibide bat ikusi zuen analisi matematiko kurtsoan. Hemen hori erabiliko dugu soilik integrazio-eremua banatzeko:

$$\int_{A \times B} f \, \mathrm{d}(\mu \times \mu) = \int_A \left(\int_B f \, \mathrm{d}\mu \right) \mathrm{d}\mu.$$

Ikusi, adibidez, [17].

(b) **Funtzio adierazlearen integrala.** Izan bitez G talde trinkoa, $A \subset G$ eta χ_A A-ren funtzio adierazlea. Hots, $x \in A$ bada, $\chi_A(x) = 1$ izango da, eta, bestela, $\chi_A(x) = 0$. Orduan, χ_A-ren integrala A-ren neurria da. Hau da,

$$\int_G \chi_A \, \mathrm{d}\mu = \mu(A).$$

3.7. teorema (Gustafson)**.** *Izan bedi G talde topologiko Hausdorff eta trinko ez-abeldarra. Orduan, $P_{\mathrm{c}}(G) \leq 5/8$ da.*

Frogapena. Lehenik eta behin, ohartu honako hau idatz dezakegula:

$$P_{\mathrm{c}}(G) = (\mu \times \mu)(C) = \int_{G \times G} \chi_C(x, y) \, \mathrm{d}(\mu \times \mu)(x, y),$$

non $\chi_C : G \times G \to \{0, 1\}$ C multzoaren funtzio adierazlea den. Bigarrenik, oharra erabiliz, integrala honako modu honetan idatz dezakegu:

$$(\mu \times \mu)(C) = \int_G \left(\int_G \chi_C(x, y) \, \mathrm{d}\mu(y) \right) \mathrm{d}\mu(x).$$

Orain barruko integrala aztertuko dugu: hots,

$$\int_G \chi_C(x, y) \, \mathrm{d}\mu(y) = \mu(C_G(x)) \quad x \in G \text{ guztietarako.}$$

Lehenik, 3.2. teoremaren frogapenean egin dugun bezala, $|G : Z(G)| \geq 4$ dela erakuts dezakegu; bestela, G abeldarra izango litzatekeelako. Orduan, G taldea $Z(G)$ zentroaren koklaseen bildura disjuntua denez, $\mu(Z(G)) \leq 1/4$ izango da.

Ildo beretik jarraituz, $x \in Z(G)$ bada, $\mu(C_G(x)) = 1$ izango da; aitzitik, $x \in G \setminus Z(G)$ bada, $C_G(x)$ azpitalde propioa izango da eta $|G : C_G(x)| \geq 2$ dela izango dugu. Beraz, $\mu(C_G(x)) \leq 1/2$ dela dugu.

Azkenik, frogatu ditugunak erabiliz,

$$\begin{aligned} P_{\mathrm{c}}(G) = (\mu \times \mu)(C) &= \int_G \mu(C_G(x))\, \mathrm{d}\mu(x) = \\ &= \int_{Z(G)} \mu(C_G(x))\, \mathrm{d}\mu(x) + \int_{G \setminus Z(G)} \mu(C_G(x))\, \mathrm{d}\mu(x) \leq \\ &\leq \mu(Z(G)) \cdot 1 + \mu(G \setminus Z(G)) \cdot \frac{1}{2} = \mu(Z(G)) + \frac{1}{2}\left(1 - \mu(Z(G))\right) = \\ &= \frac{1}{2} + \frac{1}{2}\mu\left(Z(G)\right) \leq \frac{1}{2} + \frac{1}{4} = \frac{5}{8} \end{aligned}$$

dela ondoriozta dezakegu, frogatu nahi genuen bezala. □

Kontuan hartu 3.3. adibideak berak bornea hobeezina dela frogatzen duela. Hain zuzen ere, talde finitu guztiak talde topologiko Hausdorff eta trinkoak dira, topologia diskretuarekiko.

4. PFG taldeak: Mann-Shaleven teorema

Aurreko atalean bi elementu elkarrekin trukatzeko probabilitatea ikertu dugu. Dena den, zenbait talde teoriako propietate azter ditzakegu probabilitatearen bidez; horietako bat *positiboki sortua izatea* da. Hori egiteko, G talde profinitua bada, honako hau idatziko dugu:

$$X(G,k) := \{(x_1, \ldots, x_k) \in G^k \mid \overline{\langle x_1, \ldots, x_k \rangle} = G\}; \tag{3}$$

hots, G (topologikoki) sortzen duten k-koteen multzoa.

4.1. definizioa. Izan bedi G talde topologiko Hausdorff eta trinkoa. Orduan, G *positiboki finituki sortutako taldea* dela esaten da, *PFG*[1] laburtuta, $k \in \mathbb{N}$ existitzen bada, non

$$P(G,k) := \mu_{G^k}(X(G,k)) > 0 \quad \text{den.}$$

Beste era batean esanda, G PFG da, baldin eta soilik baldin k zenbaki arrunta existitzen bada, non ausaz hautatutako G-ren k elementuk G topologikoki sortzeko probabilitatea positiboa den.

Lehenik eta behin, definizioa zentzuduna izan dezan, $X(G,k)$ neurgarria dela ikusi behar dugu, $k \in \mathbb{N}$ guztietarako.

Demagun $H = \overline{\langle x_1, \ldots, x_k \rangle} \lneq G$ dela. Beraz, 2.6. lemaren ondorioz, $H \leq M \leq_o G$ azpitalde maximala existitzen da. Beste aldetik, $\overline{\langle x_1, \ldots, x_k \rangle} \leq M <_o$ azpitalde maximal baterako, argi dago $H \lneq G$ dela. Hori dela eta, G-ko $x_1, \ldots, x_k$ elementuek ez dute G sortzen baldin eta soilik baldin $x_1, \ldots, x_k$ azpitalde maximal eta irekian badaude.

Horrenbestez, G^k-n $X(G,k)$-ren osagarria

$$\bigcup_{M \in \mathcal{M}} M^k$$

da, non $\mathcal{M}$ multzoa G-ko azpimultzo ireki eta maximalen multzoa den. Orduan, $X(G,k)$-ren osagarria azpitalde irekien bildura izanik, $X(G,k)$ itxia da, eta, beraz, neurgarria.

[1] Hori ingelesetik dator; ingelesez ≪positively finitely generated≫ esaten diegulako talde horiei.

Bestalde, Haar neurriaren definiziotik, $k \in \mathbb{N}$ guztietarako

$$P(G,k) = \inf_{N \lhd_{\mathrm{o}} G} P(G/N,k) \tag{4}$$

dela ondoriozta dezakegu.

4.2. adibidea. *Argi dago talde finitu guztiak PFG direla. Esaterako, talde finitu guztietarako G osoa G-ren sistema sortzaile finitua da; hori dela eta, $n = |G|$ jarrita,*

$$P(G,n) \geq \frac{1}{n^n} > 0.$$

4.3. adibidea. *Adibide honetan $P(\widehat{\mathbb{Z}},1) = 0$ eta $P(\widehat{\mathbb{Z}},2) = \frac{6}{\pi^2}$ direla erakutsiko dugu. Gogora bedi $\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ dela; ondorioz,* (4) *ekuaziotik,*

$$P(\widehat{\mathbb{Z}},1) = \inf_{n\in\mathbb{N}} P(\mathbb{Z}/n\mathbb{Z},1) = \inf_{n\in\mathbb{N}} \frac{\varphi(n)}{n} = 0.$$

Azken berdintza balioztatzeko ikusi, adibidez, [12, Thm. 7].

Beste aldetik, $\widehat{\mathbb{Z}}$ pro-ziklikoa izanik, bere azpitalde itxi guztiak $\widehat{\mathbb{Z}}$ beraren isomorfoak dira; orduan, $P(\widehat{\mathbb{Z}},k) = P(H,k)$, $k \in \mathbb{N}$ guztietarako. Gainera, (2) *ekuazioaren ondorioz, $H \leq_{\mathrm{c}} \widehat{\mathbb{Z}}$ azpitalde itxi eta indize infinituko guztietarako $\mu_{\widehat{\mathbb{Z}}}(H) = 0$. Horregatik, $p = P(\widehat{\mathbb{Z}},2)$ eta $\mu = \mu_{\widehat{\mathbb{Z}}^2}$ jarrita,*

$$1 = \mu(\widehat{\mathbb{Z}}^2) = \mu\left(\bigcup_{H\leq_{\mathrm{c}}\widehat{\mathbb{Z}}} \left\{(g,h) \in \widehat{\mathbb{Z}}^2 \mid \overline{\langle g,h\rangle} = H\right\}\right) =$$

$$= \sum_{H\leq_{\mathrm{o}}\widehat{\mathbb{Z}}} P(H,2)\cdot\mu(H^2) = p\cdot\sum_{n\in\mathbb{N}} \frac{1}{n^2} = p\cdot\frac{\pi^2}{6}$$

dela ondoriozta dezakegu. Ohartu $\widehat{\mathbb{Z}}$ taldearen azpitalde itxi guztiak irekiak eta $n\widehat{\mathbb{Z}}$ motakoak direla erabili dugula frogapenean. Bestalde, hirugarren berdintza egia da, parentesien artean dauden gertakizunak disjuntuak baitira.

Interesgarria da $\zeta(2) = \frac{\pi^2}{6}$ dela ohartzea, non $\zeta(s)$ Riemann zeta funtzioa den, aurki zeta-funtzioekiko beste lotura batzuk adieraziko baititugu.

Aurreko adibidearen antzeko moduan $\widehat{\mathbb{Z}}^d$ taldeetarako probabilitateak kalkula daitezke.

4.4. proposizioa. *Izan bitez $k,d \in \mathbb{N}$. Orduan, $k > d$ guztietarako,*

$$P(\widehat{\mathbb{Z}}^d,k) = \zeta(k)^{-1}\zeta(k-1)^{-1}\cdots\zeta(k-d+1)^{-1}.$$

Beste muturrean, talde batek azpitalde maximal ≪gehiegi≫ badauzka, orduan talde hori sortzeko probabilitatea ezin da positiboa izan. ≪Gehiegi≫ hori zehazteko, $m_n(G)$ ikurraz G-ren n-indizeko azpitalde maximal kopurua idatziko dugu. Ikurren bidez berridatzita:

$$m_n(G) := |\{M \leq_{\mathrm{o}} G \mid M \text{ maximala eta } |G:M| = n\}|.$$

Izan ere, laster F_d talde askeak PFG ez direla adieraziko dugu, eta, kasu honetan, $m_n(F_d) \sim n^n$ betetzen dela ikusi (cfr. [14] edo 4.14. proposizioa). Are txarrago $m_n(G)$ zenbakiak infinitu izan daitezke. Hala ere, G taldea finituki sortua bada, $m_n(G) < \infty$ n guztietarako dela frogatu daiteke.

4.5. definizioa. Izan bedi G talde profinitua. Orduan, G taldeak *azpitalde maximaletako hazkunde polinomiala* (*PMSG*[2] laburtuta) daukala esango dugu, $c \in \mathbb{R}$ konstante positiboa existitzen bada, non $n \in \mathbb{N}$ handi samar guztietarako $m_n(G) \leq n^c$ den.

Argi dago $\widehat{\mathbb{Z}}$ talde profinituak PMSG daukala; n zenbaki lehena bada, $m_n(\widehat{\mathbb{Z}}) = 1$ delako, eta, bestela, $m_n(\widehat{\mathbb{Z}}) = 0$ delako. Hori dela eta, $m_n(\widehat{\mathbb{Z}}) \leq n^0 = 1$ dela dugu, $n \in \mathbb{N}$ guztietarako.

Mann-Shaleven teoremaren lehen erdia frogatzeko prest gaude.

4.6. teorema (Mann-Shalev)**.** *Izan bedi G talde profinitua. G taldeak PMSG badauka, orduan G PFG da.*

Frogapena. Lehendabizi, aurrekoan bezala, gogoratu $\mathcal{M}$ ikurraz G-ren azpitalde maximal eta irekien multzoa adierazten dugula. Beraz, $\mathcal{M}$ zenbakigarria da, hipotesiak $m_n(G)$ finitua dela inplikatzen baitu $n \in \mathbb{N}$ guztietarako eta

$$\mathcal{M} = \bigcup_{n\in\mathbb{N}} \{M \leq_{\mathrm{o}} G \mid M \text{ maximala eta } |G : M| = n\} \quad \text{baita.}$$

Probabilitate teorian maiz gertatzen den modura, $1 - P(G, k)$ probabilitatea aztertzea errazagoa da. Hori egiteko, gogoratu $g_1, \ldots, g_k \in G$ elementuek ez dutela G sortzen, baldin eta soilik baldin $M \leq_{\mathrm{o}} G$ azpitalde maximala existitzen bada, non $\overline{\langle g_1, \ldots, g_k \rangle} \leq M$ den.

Ondorioz, $\mu = \mu_{G^k}$ jarrita,

$$1 - P(G, k) = \mu\left(\bigcup_{M\in\mathcal{M}} M^k\right)$$

dela frogatu dugu. Nahiz eta G-ren azpitaldeak disjuntuak ez izan, azpitalde maximalen multzoa zenbakigarria izanik, probabilitatea goitik muga dezakegu; hau da:

$$\mu\left(\bigcup_{M\in\mathcal{M}} M^k\right) \leq \sum_{M\in\mathcal{M}} \mu\left(M^k\right).$$

Aurrekoaz gain, badakigu $\mu(M^k) = 1/|G : M|^k$ dela, eta, gainera, n-indizeko azpitalde maximal eta ireki guztiek $1/n$ neurria daukatela. Batukariaren gaiak berrantolatuz,

$$\sum_{M\in\mathcal{M}} \mu(M^k) = \sum_{n\geq 2} \frac{m_n(G)}{n^k}$$

dela ondorioztatzen dugu. Hipotesia erabiliz, $c > 0$ existitzen da, non $m_n(G) \leq n^c$ den $n \geq 1$ guztietarako. Aurreko esaldian c behar bezala handituz gero $n \geq 1$ baldintza lor dezakegula antzematen dugu. Hortaz,

$$\sum_{n\geq 2} \frac{m_n(G)}{n^k} \leq \sum_{n\geq 2} \frac{1}{n^{k-c}} \leq \sum_{n\geq 2} \frac{1}{n^2} = \frac{\pi^2}{6} - 1 < 1 \qquad \text{da,}$$

non azken-aurreko inekuazioa egia den $k \geq c+2$ gertatzean. Hori dela eta, $k \geq c+2$ guztietarako $1 - P(G, k) < 1$ da. Beraz, $P(G, k) > 0$ da, teoremaren frogapena amaituz. □

Aurreko teorema ikuspegi desberdinetatik garrantzitsua da. Batetik, Matematikako bi adar desberdin lotzen ditu, probabilitatea eta talde teoria, alegia. Beste alde batetik, ezusteko ondorioak dakartza.

[2] Berriro ingelesezko ≪polynomial maximal subgroup growth≫ izenetik hartuta.

4.7. proposizioa. *Izan bedi G talde profinitua. Orduan, G taldeak PMSG badu, G finituki sortua da.*

Frogapena. 4.6. teorematik G PFG dela $k \in \mathbb{N}$ baterako ondoriozta daiteke. Noski, $X(G,k)$ multzoak neurri positiboa izateak $X(G,k)$ ez-hutsa dela dakar berarekin. □

4.6. teorema frogatu aurretik ez zegoen argi azpitalde maximal ≪gutxi≫ daukan talde bat finituki sortua zergatik izango litzatekeen. Bestalde, 4.7. proposizioaren beste frogapenik ez da ezagutzen, probabilitatea erabili gabe.

Talde profinituen teoriaren teoremarik garrantzitsuenetako bat Mann-Shaleven Teoremaren aurkako inplikazioa da.

4.8. teorema (Mann-Shalev)**.** *Izan bedi G talde profinitua. Orduan, G taldea PFG da, baldin eta soilik baldin G-k PMSG badauka.*

Artikulu xume honetan ezin izango dugu aurreko teorema osoa frogatu. Alabaina, frogapenean erabiltzen diren emaitzak emango ditugu, zati guztiak azaltzen.

Lehen osagaia probabilitatekoa da.

4.9. lema. *Izan bitez G talde profinitua, μ bere Haar neurria eta $(X_i)_{i\in I}$ G-ren azpimultzo neurgarrien segida. Idatzi honako gertaera hau:*

$$X = \bigcap_{n=1}^{\infty} \left(\bigcup_{i=n}^{\infty} X_i \right).$$

(*i*) *Demagun* $\sum_{i=1}^{\infty} \mu(X_i)$ *konbergentea dela. Orduan,* $\mu(X) = 0$ *da.*

(*ii*) *Demagun X_i multzoak binaka askeak direla eta $\sum_{n=1}^{\infty} \mu(X_i)$ konbergitzen ez dela. Orduan,* $\mu(X) = 1$ *da.*

Frogapena. Lemaren frogapena probabilitate teoriako edozein liburutan aurki daiteke. Bakarrik lehen partea frogatuko dugu hemen. Suposatu $\sum_{n=1}^{\infty} \mu(X_i)$ dela. Orduan, $\varepsilon > 0$ guztietarako $N \in \mathbb{N}$ existitzen da, non $\sum_{n=N}^{\infty} \mu(X_i) < \varepsilon$. Beraz,

$$0 \leq \mu(X) \leq \mu\left(\bigcup_{n=N}^{\infty} X_i \right) \leq \sum_{n=1}^{\infty} \mu(X_i) < \varepsilon$$

eta $\mu(X) = 0$ izango dugu. □

Aztertzen ari garen kasuan, erabiliko dugun propietatea bigarrena da. Horregatik, bi azpitalde askeak noiz diren aztertu behar dugu. Hurrengo leman honako definizio hau erabiliko dugu: izan bedi $H \leq G$, orduan *H-ren G-ko muina*, $\mathrm{core}_G(H)$ ikurraz adieraziko duguna, H-ren G-ko konjugatu guztien ebakidura da; ikurrez:

$$\mathrm{core}_G(H) = \bigcap_{g\in G} H^g.$$

Argi dago $\mathrm{core}_G(H)$ dela H-ren barruan dagoen G-ren azpitalde normalik handiena.

4.10. lema. *Izan bitez G talde profinitua eta A, B maximalak eta irekiak diren G-ren azpitalde normalak, non A-k eta B-k muin desberdinak dauzkaten. Orduan, A^k eta B^k askeak dira G^k taldean $k \in \mathbb{N}$ guztietarako.*

Frogapena. Idatzi $A_0 = \mathrm{core}_G(A)$ eta $B_0 = \mathrm{core}_G(B)$. Hasteko, $A_0 \leq B$ bada, $A_0 \leq B_0$ dela ondoriozta daiteke. Baina, A_0 eta B_0 ezberdinak direnez, $B_0 \not\leq A$ dela ondoriozta dezakegu. Beraz, orokortasunik galdu gabe, A_0 ez dagoela B-ren barruan suposatu dezakegu. Horrenbestez, B maximala denez, $A_0B = G$ izan behar dugu eta $AB = G$ da. Gure azpimultzoen indizeak idatziz, $|G : A \cap B| = |G : A| \cdot |G : B|$ dela izango dugu. Azkenik,

$$\mu(A^k \cap B^k) = |G : A \cap B|^{-k} = |G : A|^{-k}|G : B|^{-k} = \mu(A^k)\mu(B^k),$$

frogapena amaitzen duena. □

Mann-Shaleven Teorema frogatzeko azken osagaia talde finituei buruzkoa da. Izan ere, hurrengo emaitza Talde Finitu Bakunen Sailkapenean (CFSG laburtuta[3]) datza eta talde finituen egituraren ezaugarri sakon bat azaltzen du. Beste definizio bat behar dugu: G taldearen H azpitaldea *muin-librea* dela esango dugu $\mathrm{core}_G(H) = 1$ bada.

4.11. teorema ([15, Cororollary 2])**.** *Izan bedi G talde finitua, d sortzaile libre dauzkana. Orduan, G-ren n-indizeko azpitalde maximal eta muin-libreen kopurua $2n^{2d}$ baino txikiagoa da.*

Aurreko emaitzaren frogapena CFSG-n datza; hau da, lehenengo CFSG erabiliz talde bakunetarako klasez klase frogatzen da eta, gero, talde orotarako egiaztatzen da teorema. Gainera, aurreko teoremaren orokorpen ugari daude, bai teorema talde gehiagotarako frogatzen dutenak, baita konstanteak hobetzen dituztenak ere. Hala ere, artikulu honetan ez ditugu horiek erabiliko, Mann-Shaleven teorema frogatzeko tresna guztiak baitauzkagu.

Mann-Shaleven teoremaren frogapena. Demagun $P(G, k) > 0$ dela. Orduan, $\mathrm{d}(G) \leq k$ da, eta G-ren indize finituko azpitalde maximal eta irekien $\mathcal{M}$ multzoa zenbakigarria da, multzo finituen bildura zenbakigarria baita. Ohartu finituki sortutako talde batek, n baikoitzeko, n indizeko azpitalde irekien kopuru finitua duela erabili dugula ([11]).

Orain, G-ren azpitalde maximalen gaineko baliokidetasun erlazioa definituko dugu orain: G taldearen M_1, M_2 bi azpitalde maximal *baliokideak* direla esango dugu, $\mathrm{core}_G(M_1) = \mathrm{core}_G(M_2)$ bada. Aukeratu baliokidetasun klase bakoitzean G-n indize txikiena duen M_i ordezkaria eta adierazi $\{M_i\}_{i\in I}$ bidez ordezkari horiek. Definitu honako zenbaki hau:

$$q_n = |\{i \in I \mid |G : M_i| = n\}|.$$

Izan bedi $M \leq G$ azpitalde maximala eta irekia. Beraz, $i \in I$ existitzen da, non $\mathrm{core}_G(M) = \mathrm{core}_G(M_i) = N_i$ eta $|G : M_i| \leq n$ den. Hau da, M bezalako azpitaldeen kopurua (hau da $m_n(G)$) honako biderketa hau baino txikiagoa da:

$$|\{i \in I \mid |G : M_i| \leq n\}| \cdot |\{M \in \mathcal{M} \mid \mathrm{core}_G(M) = N_i\}| = \alpha_n \cdot \beta_n.$$

Lehenik, 4.11. teorema G/N_i talde finituari aplikatuz, $\beta_n \leq 2n^{2k}$ dela ondorioztatu dezakegu.

Beste aldetik, argi dago $\alpha_n \leq q_2 + \ldots + q_n$ dela. Orain, Borel-Cantelliren lema erabiliko dugu $q_n = o(n^k)$ dela frogatzeko. Har dezagun honako serie hau:

$$\sum_{i=1}^{\infty} \mu\left(M_i^k\right) = \sum_{i=1}^{\infty} |G : M_i|^{-k} = \sum_{n=2}^{\infty} q_n n^{-k}.$$

Serie hori konbergentea dela ikusiko dugu, kontraesanera iritziz. Demagun ez dela konbergentea. Seriearen gaiak binaka askeak direnez (cfr. 4.10. lema), 4.9.(ii) lemak esaten du X multzoak 1eko neurria duela, non

$$X = \left\{\boldsymbol{x} \in G^k \mid \boldsymbol{x} \in M_i^k,\ i \text{ indizeen kopuru infiniturako}\right\} \quad \text{den.}$$

[3] Berriro ingelesetik dator, ≪Classification of Finite Simple Groups≫.

Hala ere, $\boldsymbol{x} \in X(G,k)$ bada (ikusi (3) ekuazioa), $\boldsymbol{x}$ ezin da M_i^k batean ere egon, M_i maximalak eta irekiak baitira. Beraz, aurreko seriea konbergentea izan behar da. Hots, $q_n = o(n^k)$ dela frogatu dugu.

Azkenik, M-ren ordezkarirako aukerak $\sum_{i=2}^{n} q_i$ baino gutxiago dira (gogoratu M azpitaldea M_i baten baliokidea dela eta i indizeko M_j kopurua q_i dela), eta batura horren hazkundea mugatu dezakegu:

$$\sum_{i=2}^{n} q_i = \sum_{i=2}^{n} o(i^k) = o(n^{k+1}).$$

Horrenbestez, n behar bezain handia hartuz, honako ezberdintza hauek izango ditugu:

$$m_n(G) \leq o(n^{k+1}) \cdot 2n^{2k+2} \leq 2n^{3k+3}.$$

Beraz, G taldeak PMSG du, frogatu nahi genuen bezala. □

4.1. PFG taldeen propietate gehiago

Atal honetan 4.8. teorema talde teoria probabilistikoaren beste gai bati lotuko diogu. Paul Erdős matematikaria talde teoria probabilistikoaren sortzailea izan zen, eta, batik bat, permutazio taldeez arduratu zen. Hori dela eta, talde teoria probabilistikoaren lehen emaitzak talde simetriko eta alternatuei buruzkoak dira.

4.12. definizioa. Izan bedi $G \leq \mathrm{Sym}(\Omega)$ permutazio taldea[4]. Orduan, G *primitiboa* dela esango dugu, G trantsitiboa bada eta G taldeak ez badu Ω-ren partizio bat ere finkatzen.

4.13. teorema ([1])**.** *Izan bedi $n \in \mathbb{N}$. Orduan, S_n-ren bi ausazko permutaziok S_n ala A_n sortzeko probabilitatea* 1*era doa, n infiniturantz badoa.*

Beraz, n infiniturantz doanean, ausazko edozein bi permutazio edo gehiagok sortutako azpitaldea primitiboa izateko probabilitatea 1era doa, A_n eta S_n primitiboak direla-eta. Aurreko teorema gure gaiarekin zuzenki lotuta ez dagoela badirudi ere, azpitalde hazkuntzari lotuta dago, hurrengo proposizioan adieraziko dugun moduan. Horren aurretik, honako notazio hau finkatuko dugu: $\varphi : G \to S_n$ homomorfismoa eta $i \in \{1, \ldots, n\}$ badira, $\mathrm{Stab}_{G,\varphi}(i) = \{g \in G \mid \varphi(g)(i) = i\}$ idatziko dugu.

4.14. proposizioa. *Izan bedi d sortzaile libre dituen $F = F_d$ talde profinitu librea, . Orduan, F taldeak ez du PMSG; hain zuzen ere, $m_n(F) \sim n(n!)^{d-1}$.*

Frogapena. Lehenbizi,

$$m_n(F) = \frac{p_n(F)}{(n-1)!} \tag{5}$$

dela erakutsiko dugu, non $p_n(F) = \{\varphi : F \to S_n \mid \varphi(F)$ primitiboa da$\}$ den. Demagun $M \leq F$ azpitalde maximala dela. Orduan, F-k M-ren eskuin koklaseen gainean eragiten du eskuin biderketaz. Beraz, M-ren koklase ez-tribialak $M_2, \ldots, M_n$ (nahi dugun ordenean) eta M koklase tribiala M_1 izendatuz, $\varphi : F \to S_n$ homomorfismoa zehaztuko dugu, non $\varphi(i) = j$ funtzioa $M_i \cdot g = M_j$ ekuazioaren bitartez definitua den. Homomorfismoa horrela definitu ondoren, argi dago:

(a) $\varphi(F)$ primitiboa dela[5] eta

(b) $M = \mathrm{Stab}_{F,\varphi}(1)$ dela.

[4]Hau da, G taldea da, Ω-ren gainean eragiketa fidela dagokiona.

[5]Demagun M-ren koklaseen $\mathcal{P}$ partiketa ez-tribiala dugula eta $M \in P \in \mathcal{P}$ dela. Orduan, $M < \mathrm{Stab}_{F,\varphi}(P) < G$ dela dugu, kontraesana dena.

Bestalde, koklase ez-tribialen izenak aldatzeak (a) eta (b) propietateak betetzen dituzten beste $(n-1)!$ homomorfismo ezberdin ematen ditu. Alderantziz, $\varphi : F \to S_n$ homomorfismo bakoitzak, $\varphi(F)$ primitiboa dela betetzen duenak, $\mathrm{Stab}_{F,\varphi}(1)$ azpitalde maximala ematen du. Horrela (5) frogatu dugu.

Azkenik, $h_n(F) = |\mathrm{Hom}(F, S_n)| = (n!)^d$ idatzita, $p_n(F)/h_n(F) \to 1$ dela frogatuko dugu n infiniturantz doanean. Hori egingo bagenu,

$$m_n(F) \sim \frac{(n!)^d}{(n-1)!} = n \cdot (n!)^{d-1}$$

izango litzatekeela ondorioztatuko genuke, frogapena amaituko lukeena. Orain, 4.13. teorema erabiliz,

$$1 \geq \frac{p_n(F)}{h_n(F)} \geq P(\langle g_1, \ldots, g_d \rangle \text{ primitiboa da} \mid g_1, \ldots, g_d \in S_n) \geq$$
$$P(\langle g_1, \ldots, g_d \rangle = S_n \text{ ala } A_n \mid g_1, \ldots, g_d \in S_n) \to 1,$$

n infiniturantz badoa. □

Mann-Shaleven teoremaren ondorioz, F_d talde profinitu askeak PFG ez direla dakusagu. Ildo beretik jarraituz, talde bat talde libre bat ≪baino txikiagoa≫ izango balitz, taldea PFG izatea pentsa liteke. Edozein d elementuz sortutako talde finitua F_d taldearen zatidura taldea dela gogoratuz, honako definizio hau emango dugu.

4.15. definizioa. Izan bitez G talde profinitua eta A talde finitua. Orduan, A ez dagoela G taldean *sartuta* esango dugu, A ezin badaiteke G-ren koziente finitu eta jarraitu baten azpitalde bezala adierazi.

Ohar bedi, A talde finitua existitzen bada, non A taldea G taldean sartuta ez dagoen, G ezin daitekeela librea izan.

4.16. teorema ([3, Theorem 1.1])**.** *Izan bedi G talde profinitu finituki sortua. Demagun G taldean sartuta ez dagoen A talde finitua existitzen dela. Orduan, G taldea PFG da.*

Emaitza horren frogapena ez dugu emango eta Teorema horren aplikazio batzuk ematearekin konformatuko gara.

4.17. adibidea. *Talde pro-ebazgarri finituki sortuetan ezin da talde bakun finiturik sartuta egon; esaterako, A_5 talde alternatua. Beraz, finituki sortutako talde pro-ebazgarri guztiak PFG dira. Alabaina, PFG talde profinituak existitzen dira, non talde finitu guztiak sartuta baitaude; adibidez, $G = \prod_{n\in\mathbb{N}} A_n$ (edo ikusi [4]).*

Atal hau azken probabilitatearen aplikazio harrigarri bat emanez bukatuko dugu.

4.18. proposizioa. *Izan bitez G talde profinitua eta $N \lhd G$ azpitalde normala eta itxia. Demagun N eta G/N taldeek PMSG dutela. Orduan, G taldeak PMSG du.*

Aurrekoaren frogapena 4.8. teoremaren ondorio erraza baino ez bada ere, harrigarria da: prinzipioz, ez dago talde hedadura baten azpimultzo maximalak faktoreetako azpitalde maximalei lotuta egoteko arrazoirik. Izan ere, ezagutzen den 4.18. proposizioaren frogapen bakarra 4.8. teoremaren menpe dago, 4.7. proposizioarekin gertatu den bezala.

5. PFR taldeak eta UBERG propietatea

Aurreko atalean ezberdinak iruditu daitezkeen bi propietate lotu ditugu: PFG eta PMSG. Orain, PFG propietatea finituki sortua izateari lotuta dagoen moduan, *finituki aurkeztua izatea*ri lotutako propietatea definitzen saiatu gintezke. Lehenbizi, talde profinituetan finituki aurkeztua izatea zer den gogoratu beharko genuke. Izan bedi G talde profinitua. Orduan, G-ren $\mathcal{S}$ *aurkezpena* honelako segida laburra da:

$$(\mathcal{S}): \quad 1 \to R \to F \to G \to 1, \tag{6}$$

non F talde profinitu librea eta geziak homomorfismoak diren. Bestalde, $\mathcal{S}$ *aurkezpen finitua* dela esango dugu, F finituki sortua eta R azpitaldea F talde librean normalki finituki sortua badira[6]. Azkenean, G taldea *finituki aurkeztua* dela esango dugu, G-ri aurkezpen finitu bat badagokio.

Finituki sortuak diren taldeekin egin dugun modura, probabilitatearekin jolas gaitezke. Izan bedi (6) moduko $\mathcal{S}$ segida zehatza. Orduan, G-ren erlazioak R-ren k elementu ausazkoz sortzeko $P(\mathcal{S}, k)$ probabilitatea honako modu honetan definituko dugu:

$$P(\mathcal{S}, k) = \mu\left(\{(r_1, \dots, r_k) \in R^k \mid \overline{\langle r_1, \dots, r_k\rangle^F} = R\}\right) \tag{7}$$

eta G taldea *positiboki finituki aurkeztua* (***PFR*** laburtuta[7]) dela esango dugu, $\mathcal{S}$ aurkezpen guztietarako k existitzen bada, non $P(\mathcal{S}, k) > 0$ den.

Aurrekoan geneukan lotura PFG eta PMSG propietateen artekoa zen. Orain, azpitalde maximalek ez digute balio, normalki sortutako azpitaldeez arduratzen ari baikara. Dena den, lehen bezala, R-ren $r_1, \dots, r_k$ elementuek ez dute R normalki sortzen baldin eta soilik baldin ***F* taldeko** $M \leq R$ azpitalde normala existitzen bada, non $\overline{\langle r_1, \dots, r_k\rangle^F} < M$ den. Hori dela eta, honako definizio hau emango dugu.

5.1. definizioa. Izan bedi G talde profinitua, (6) moduko segida batean agertzen dena. Orduan, R azpitaldea F *taldean azpitalde maximal eta normaletako hazkunde polinomiala* (PM$_{\lhd F}$SG laburtuta) duela esango dugu, $c > 0$ konstantea existitzen bada, non

$$m_n^F(R) := \left|\left\{M \leq F \;\middle|\; \begin{array}{c} M <_{\mathrm{o}} R,\ M \lhd F \text{ propietateekiko maximala,} \\ |R : M| = n \text{ izanik} \end{array}\right\}\right| \leq n^c$$

den n zenbaki handi samar guztietarako.

Aurreko definizioa emanda, 4.6. eta 4.8. teoremen urratsak errepikatuz, honako teorema hau arin frogatu dezakegu.

5.2. teorema (Kionke-Vannacci, [13])**.** *Izan bedi G talde profinitua. G taldeak PM$_{\lhd F}$SG du baldin eta soilik G PFR bada.*

Izan ere, aurreko teoremaren ezkerreranzko inplikazioan ez dugu CFSG erabili behar: $M_1, M_2 \lhd F$ bi azpitalde normal eta desberdin badira, R-ren barne daudenak eta horrekiko maximalak direnak, orduan $M_1 M_2$ azpitaldea F taldean normala dela eta $M_1 M_2 = R$ dela argi dago eta 4.10. lemaren emaitza erabil daiteke; hau da, kasu horretan ez dago 4.8. teoreman adierazi diren $\{M_i\}_{i \in I}$ ordezkariak definitzeko beharrik.

PFG taldeak aztertu ditugunean, istorioa hemen bukatzen da. Haatik, PFR taldeentzat istorioa hastear dago. Ohartu, (6) moduko segida badaukagu, $M \lhd F$ eta $M \leq R$ guztietarako segida berria defini dezakegula, M bidezko zatidura taldeak hartuz:

$$1 \to R/M \to F/M \to G \to 1. \tag{8}$$

[6]Gogorapena: izan bitez G talde profinitua eta $N \lhd G$, orduan N azpitaldea G *taldean normalki finituki sortua* dela esaten dugu, $n_1, \dots, n_r \in N$ existitzen badira, non $N = \overline{\langle n_1, \dots, n_r\rangle^G}$ den; hots, N-ren elementu kopuru finitu bat existitzen da, non elementu horiek sortutako azpitalde normala N den.

[7]Positively Finitely Related.

Bestalde, $M \lhd F$ eta $M \leq_{\mathrm{o}} R$ propietateekiko maximala dela suposatuz gero, F/M taldea G-ren R/M-z hedadura da, eta R/M talde bakuna eta finitua da. Beraz, F taldean normalak diren eta R-ren barruan dauden n indizeko azpitaldeak zenbatu ordez, n kardinaleko G-ren hedadurak zenbatu ditzakegu.

Hala eta guztiz ere, bi talde bakunetako mota dauzkagu: abeldarrak eta ez-abeldarrak. Talde bakun ez-abeldarrak jada aipatu genituen artikulu honetan, CFSG-ren protagonistak dira-eta. CFSG-k emandako ondorioen artean honako hau daukagu.

5.3. teorema ([5]). *Gehienez bi kardinal bereko talde bakun existitzen dira.*

Aurreko teoremak esaten digu G taldeak talde bakun ez-abeldarrez egindako hedadura ≪gutxi≫ izan ditzakeela. Hala ere, artikulu honetan ez gara talde bakunez gehiago arduratuko. Orduan, geratzen zaizkigun hedadurak abeldarrak dira. Baina $1 \to R/M \to F/M \to G \to 1$ (8) bezalako hedadura bada, R/M nukleo abeldarra duena, G-k R/M-n konjugazioz eragiten du. Gainera, M azpitaldearen propietateengatik, $R/M = \mathbb{F}_q^n$ abeldar elementala da, non q zenbaki lehena den. Horrela, G-ren $\rho : G \to \mathrm{GL}_n(\mathbb{F}_q)$ errepresentazioa eraiki dugu.

Beraz, nahiz eta hedaduretatik abiatu, gorputz finituen gaineko errepresentazioak zenbatzea da egitekoa. Esan gabe doa, n dimentsioa eta $\mathbb{F}$ gorputz finitua finkatuta, G talde profinituaren $\mathbb{F}$-ren gainean n-dimentsioko errepresentazioen kopurua finitua dela, G topologikoki finituki sortua bada. Bereziki, $\mathrm{d}(G) = d$ bada, orduan $|\mathbb{F}|^{dn^2}$ baino txikiagoa da. Izan ere, $\varphi : G \to \mathrm{GL}_n(\mathbb{F})$ homomorfismoen kopurua $(|\mathbb{F}|^{n^2})^d$ baino txikiagoa da. Horrenbestez, borne hori hobetu beharko genuke propietate ez-tribiala idatzi nahiko bagenu.

Lehenik, honako notazio hau finkatuko dugu. Izan bitez G talde profinitua, $\mathbb{F}$ gorputz finitua eta $n \in \mathbb{N}$. Orduan, $r(G, \mathbb{F}, n)$ ikurrak $\mathbb{F}$-ren gaineko eta n-dimentsioko G-ren errepresentazio irreduzible guztien kopurua adieraziko du.

5.4. definizioa. Izan bedi G talde profinitua. Orduan, G-k *(gorputz finituen gaineko) hazkuntza exponentzial uniformea* (*UBERG* laburtuta[8]) duela esango da, $c > 0$ konstantea existitzen bada, non $\mathbb{F}$ gorputz finitu eta $n \in \mathbb{N}$ guztietarako honako inekuazio hau betetzen den:

$$r(G, \mathbb{F}, n) \leq |\mathbb{F}|^{cn}.$$

Definizio hori emanda, [13, Theorem A] artikuluaren emaitza nagusia eman dezakegu.

5.5. teorema (Kionke-Vannacci). *Izan bedi G talde profinitua, finituki aurkeztua dena. Orduan G PRF da, baldin eta soilik baldin G taldeak UBERG badu.*

Alabaina, ez dugu hori frogatzeko tresna nahikorik eta frogapena [13] artikuluan aurki daiteke. Aitzitik, atal hau beste lotura interesgarri bat ematen bukatuko dugu.

Izan bedi n-dimentsioko eta $\mathbb{F}_q$ gorputzaren gaineko G talde profinituaren $\rho : G \to \mathrm{GL}_n(\mathbb{F}_q)$ errepresentazioa. Adierazpen hori erabiliz, $V = {\mathbb{F}_q}^n$ espazio bektorialari G-moduluaren egitura eslei diezaiokegu; $g.v = \rho(g)(v)$ erregelaren bidez. Horregatik, errepresentazio bakoitzak $\widehat{\mathbb{Z}}[\![G]\!]$-modulu bat ematen digu eta honelako modulu bakoitzak, gainera, $\widehat{\mathbb{Z}}[\![G]\!]$-ren I ideal bat, $\widehat{\mathbb{Z}}[\![G]\!]$ bere buruarekiko modulu librea delako (ikusi 2.5. atala). Dena den, $V = \widehat{\mathbb{Z}}[\![G]\!]/I$ modulua $\widehat{\mathbb{Z}}[\![G]\!]$-modulua da baldin eta soilik baldin I ideala V-ko bektore baten anulatzailea bada. Hau gerta dadin, $|V| = q^n$ aukera dauzkagu; beraz, honako inekuazio hauek betetzen dira:

$$r(G, \mathbb{F}_q, n) \leq m_{q^n}^{\lhd}(\widehat{\mathbb{Z}}[\![G]\!]) \leq q^n \cdot r(G, \mathbb{F}_q, n),$$

$m_{q^n}^{\lhd}(\widehat{\mathbb{Z}}[\![G]\!])$ zenbakia $\widehat{\mathbb{Z}}[\![G]\!]$ eraztunaren q^n-indizeko *ideal* maximal eta irekien kopurua izanik. Azkenik, $\widehat{\mathbb{Z}}[\![G]\!]$ talde eraztunak *PMIG*[9] duela esango dugu, $\gamma > 0$ existitzen bada, non

$$m_n^{\lhd}(\widehat{\mathbb{Z}}[\![G]\!]) \leq n^{\gamma} \text{ den } n \text{ handi samar guztietarako.}$$

[8] Uniformly Bounded Exponential Representation Growth (over finite fields).
[9] Polynomial Maximal Ideal Growth.

Esandakoa laburtzeko, $\widehat{\mathbb{Z}}[\![G]\!]$ eraztunak PMIG daukala frogatu dugu, baldin eta soilik baldin G taldeak UBERG badauka.

Beste alde batetik, errepresentazio irreduzibleak zenbatzea zaila izan daiteke, gorputza aldatzearekin irreduzibilitate kontzeptua ere alda daitekeelako. Hori konpontzeko, adibideekin jolasten garenean, komenigarria da *absolutuki irreduzibleak* diren errepresentazioak kontuan hartzea. Gogoratu $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ errepresentazioari esaten zaiola *absolutuki irreduziblea* dela, ρ errepresentazioa $\mathbb{F}$-ren itxitura aljebraikoan irreduziblea bada. Gainera, talde baterako UBERG propietatea egiaztatzean, errepresentazio absolutuki irreduzibleak zenbatzea nahikoa dela laster frogatuko dugu. Lehenago egin dugun moduan, $r^*(G, \mathbb{F}, n)$ ikurraz $\mathbb{F}$-ren gaineko eta n-dimentsioko G-ren errepresentazio *absolutuki* irreduzible guztien kopurua adieraziko dugu.

5.6. teorema (Kionke-Vannacci, [13, Lemma 6.8])**.** *Izan bedi G talde profinitua. Orduan, G taldeak UBERG du baldin eta soilik baldin $b > 0$ existitzen bada, non*

$$r^*(G, \mathbb{F}, n) \leq |\mathbb{F}|^{bn}$$

den $\mathbb{F}$ gorputz finitu eta $n \in \mathbb{N}$ guztietarako.

UBERG propietatea, aski naturala izan arren, oso misteriotsua da. Gainerakoan, UBERG aztertzeko bi metodo adieraziko ditugu: PFP_n propietateak definitzea eta errepresentazio zeta-funtzioak elkartzea.

6. PFP_n propietateak

Taldeak ikertzen ditugunean, ea talde bat ≪polita≫ den jakitea interesatuko litzaiguke eta, askotan, polita izatea egitura geometriko baten gaineko eragiketa edukitzea da. Halaber, egitura geometriko motarik politenenetako bat CW-konplexua da; horiek dimentsio ezberdineko $\mathbb{R}^n$-etako zatiak elkarrekin itsatsiz defini daitezke. Taldeak $\mathcal{F}_n$ *propietatea* duela esango dugu, taldea CW-konplexu baten oinarrizko taldea bada, non CW-konplexu horren n dimentsioko zatien kopurua finitua den. Hala eta guztiz ere, mota horretako espazioak aurkitzea oso zaila da eta errazago baliozta ditzakegun propietateak edukitzea gustatuko litzaiguke. Gainera, talde profinituen munduan ez dago CW-konplexuaren konzeptu argirik. Hori dela eta, honako definizio hau normalean erabiltzen da talde bat ≪polita≫ dela esateko.

6.1. definizioa. Izan bedi G talde profinitua. Orduan, G taldeak $\mathcal{FP}_n$ *propietatea* duela esaten dugu, honako mota honetako ebazpen zehatza[10] existitzen bada:

$$\ldots \to P_n \to \ldots \to P_2 \to P_1 \to \widehat{\mathbb{Z}} \to 0, \tag{9}$$

non P_n finituki sortutako $\widehat{\mathbb{Z}}[\![G]\!]$-modulu proiektibo profinituak diren.

Bereziki, G talde abstraktuak $\mathcal{F}_n$ propietatea badu, G taldeak $\mathcal{FP}_n$ propietatea duela frogatu daiteke. Zoritxarrez, talde profinituetan, $\mathcal{FP}_n$ propietatea ez da ondo portatzen; adibidez, talde abstraktuetarako $\mathcal{FP}_1$ propietatea finituki sortzearekin bat dator, baina G talde profinitu finituki ez-sortuak eta $\mathcal{FP}_1$ propietatea betetzen dutenak existitzen dira (ikusi [6]). Horregatik, $\mathcal{FP}_n$ baldintza indartzea komeni zaigu, probabilitatea erabiliz.

6.2. definizioa. Izan bedi G talde profinitua. Orduan, G taldeak PFP_n *propietatea* duela esango dugu, (9) motako ebazpen zehatza existitzen bada, non P_n modulu proiektiboak **PFG** diren.

[10]Gogora bedi $(\varphi_i : M_i \to M_{i-1})$ homomorfismo segida *zehatza* dela esaten dugula, baldin eta $\ker \varphi_i = \mathrm{im}\varphi_{i+1}$ betetzen bada i guztietarako.

Pentsa dezakegu, PFG propietatea finituki sortua izatearen eta PFR finituki aurkeztua izatearen sendotzeak direnez, PFP_n propietateak FP_n propietateen sendotze probabilistikoak direla. Dena dela, ez dago argi ea propietate horien guztien arteko erlazioa zein den. Irakurleak ideia izan dezan, propietateen arteko erlazioen irudia [7, 3. or.] artikuluan agertzen da.

Gauzarik garrantzitsuenak bakarrik laburbiltzeko, orokorrean PFG, UBERG eta PFP_1 propietateak ez datoz bat, baina talde pronilpotenteetan gauza bera dira eta gainera finituki sortua izatearekin bat datoz.

Nahiz eta PFP_n propietateak misteriotsu geratu, Mann-Shaleven teoremaren orokorpen batzuk frogatu ditzakegu. Adieraz beza $\mathcal{S}_k(\widehat{\mathbb{Z}}[\![G]\!])$ ikurrak k-kardinaleko $\widehat{\mathbb{Z}}[\![G]\!]$-modulu irreduzibleen multzoa.

6.3. teorema (Corob Cook-Vannacci, [9, Thm. C])**.** *Izan bedi G talde profinitua. Orduan, G taldeak PFP_n propietatea du, baldin eta soilik baldin honako funtzio hauek hazkuntza polinomiala badute $m \leq n$ guztietarako:*

$$f_m(k) := \sum_{S \in \mathcal{S}_k(\widehat{\mathbb{Z}}[\![G]\!])} (|H^m_{\widehat{\mathbb{Z}}}(G, S)| - 1).$$

Gogoratu $\dim H^1(G, S)$ dimentsioa G-ren sortzaileen kopuruarekin lotuta dagoela, eta $\dim H^2(G, S)$ dimentsioa, aldiz, G-ren erlazioen kopuruarekin.

7. Gorputz finituen gaineko errepresentazio zeta-funtzioak

Talde teorian, eta Matematikako beste hainbat gaitan, talde batekin lotutako segida bat izango bagenu, segidaren propietate asintotikoak taldearen egiturari lotu nahiko genizkioke. Hori egiteko, komenigarria izango litzateke propietate guzti horiek kodifikatzen dituen objektu matematiko bat izango bagenu. Sarritan erabilitzen den objektua zeta-funtzioa da (adibidez, ikusi [14]). Guri dagokigunez, UBERG propietatea daukan G taldea badaukagu, honako funtzio hau idazteak zentzua du: $\mathbb{P}$ zenbaki lehen multzoa izanda,

$$\zeta_G(s) = \exp\left(\sum_{p \in \mathbb{P}} \sum_{n=1}^{\infty} \sum_{j=1}^{\infty} \frac{r^*(G, \mathbb{F}_{p^j}, n)}{j} p^{-snj} |\mathbb{P}^{n-1}(\mathbb{F}_{p^j})|\right), \ s \in \mathbb{C}. \tag{10}$$

Ohartu $\zeta_G(s)$ funtzioan errepresentazio absolutuki irreduzibleak zenbatzen ditugula. Izan ere, 5.6. teoremaren arabera, G taldeak UBERG badu, errepresentazio absolutuki irreduzibleen kopurua ere polinomialki hazten da. Gainera, $\zeta_G(s) = \prod_{p \in \mathbb{P}} \zeta_{G,p}(s)$ idatz daitekeenez, $\zeta_{G,p}(s)$ funtzioari *p-ko faktore lokala* deituko diogu.

7.1. lema. *Izan bedi G talde profinitua eta demagun G taldeak UBERG duela. Orduan, $\sigma_0 \in \mathbb{R}_{>1}$ existitzen da, non $\zeta_G(s)$ absolutuki konbergitzen den $\sigma > \sigma_0$ betetzen duten $s = \sigma + i\tau$ zenbaki konplexu guztietarako.*

Frogapena. Badakigu c konstantea existitzen dela, non $r^*(G, \mathbb{F}_q, n) \leq q^{cn}$ den q zenbaki lehen baten berretura eta $n \in \mathbb{N}$ guztietarako. Beraz, $\sigma > c + 2$ guztietarako:

$$\sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty}\sum_{j=1}^{\infty}\left|\frac{r^*(G,\mathbb{F}_{p^j},n)}{j}p^{-snj}|\mathbb{P}^{n-1}(\mathbb{F}_{p^j})|\right|$$
$$\leq \sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty}\sum_{j=1}^{\infty}\frac{p^{jnc}}{j}p^{-\sigma nj}p^{nj} \leq \sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty}\sum_{j=1}^{\infty}p^{jn(c-\sigma+1)}$$
$$= \sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty}\frac{p^{n(c-\sigma+1)}}{1-p^{n(c-\sigma+1)}} \leq \sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty}2p^{n(c-\sigma+1)}$$
$$\leq 2\sum_{p\in\mathbb{P}}\frac{p^{c-\sigma+1}}{1-p^{c-\sigma+1}} \leq 4\sum_{p\in\mathbb{P}}p^{c-\sigma+1} < \infty.$$

□

7.2. definizioa. Izan bedi G talde profinitua, UBERG duena. Honako zenbaki honi G-ren zeta-funtzioaren *konbegentzia abzisa* dela esango zaio:

$$\sigma_0(G) = \inf\{\sigma \in \mathbb{R} \mid \zeta_G(\sigma) \text{ konbergentea da}\}.$$

Gerta al daiteke konbergentzia abzisak taldeari buruzko zerbait esatea? Uste dugu baietz, baina orain arte ez gara lotura zuzena aurkitzeko gai izan. Alabaina, frogatu ditzakegun emaitzen artean hurrengo teorema dago.

7.3. teorema ([8, Theorem E])**.**

1. *Izan bedi G talde finitua. Orduan, $\sigma_0(G) = 1$ da.*
2. *$\alpha \in \mathbb{R}_{\geq 1}$ guztietarako G_α talde profinitu bat existitzen da, non $\sigma_0(G_\alpha) = \alpha$ den.*

Edonola ere, adibide batzuk kalkulatzen segi dezakegu.

7.4. adibidea. *Izan bitez $G = \{1\}$ taldea eta $\mathbb{F}$ gorputz finitua. Orduan, G taldeak errepresentazio bakarra du $\mathbb{F}$ bakoitzeko. Orduan,*

$$\zeta_{\{1\}}(s) = \exp\left(\sum_{p\in\mathbb{P}}\sum_{j=1}^{\infty}\frac{1}{j}p^{-sj}\right) = \prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)^{-1} = \zeta(s)$$

Riemann zeta-funtzioa da. Aurreko ekuazioan log *seriea erabili dugu; hau da,*

$$-\log(1-x) = \sum_{n=1}^{\infty}\frac{x^n}{n}.$$

7.5. adibidea. *Izan bitez $G = \widehat{\mathbb{Z}}$ taldea eta $\mathbb{F} = \mathbb{F}_q$ gorputz finitua. Orduan, G abeldarra denez, $r^*(G,\mathbb{F},n) = 0$ izango da $n \geq 2$ guztietarako. Aitzitik, $r^*(\widehat{\mathbb{Z}},\mathbb{F},1)$ zenbakia $\widehat{\mathbb{Z}}$-tik $\mathbb{F}^\times$-rako homomorfismoen kopurua da, eta hori $q-1$ da. Zeta-funtzioan jarriz eta logaritmoaren seriea erabiliz,*

$$\zeta_{\widehat{\mathbb{Z}}}(s) = \prod_{p\in\mathbb{P}}\exp\left(\sum_{j=1}^{\infty}\frac{p^j-1}{j}p^{-js}\right) = \prod_{p\in\mathbb{P}}\exp\left(-\log(1-p^{1-s})+\log(1-p^{-s})\right) =$$
$$= \prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^{s-1}}\right)^{-1}\cdot\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right) = \frac{\zeta(s-1)}{\zeta(s)}$$

Aipatutako ezaugarriez gain, zeta-funtzioak aztergai diren bakoitzean beste ezaugarri batzuen bila gabiltza matematikariok, *Riemann hipotesia* betetzea espero dugulako. Ez ditugu hemen baldintza guztiak berridatziko, eta bakarrik aipatuko dugu horien artean ≪arrazionalitatea≫ zegoela. Horrek esan nahi du $\zeta_{G,p}(s)$ faktore lokal guztiak q^{-s} aldagaiarekiko funtzio arrazionalak izatea espero dugula. Biziki interesgarria iruditzen zaigu gure zeta-funtzioak baldintza bera betetzen duela dirudiela, honako adibide honek azalduko digun bezala.

7.6. adibidea. *Izan bedi* $G = \widehat{\mathbb{Z}}^2 \rtimes C_2$, *honako aurkezpen profinitu hau duen taldea:*

$$\langle a_1, a_2, \sigma \mid \sigma^2 = 1,\ [a_1, a_2] = 1,\ a_1^\sigma = a_2 \rangle.$$

Erraz ikusten da $G^{\mathrm{ab}} \cong C_2 \times \widehat{\mathbb{Z}}$ *dela. Orduan,* $2 \nmid q$ *bada,* $r^*(G, \mathbb{F}_q, 1) = 2(q-1)$ *da, eta* $2 \mid q$ *bada,* $r^*(G, \mathbb{F}_q, 1) = q - 1$ *da. Bigarren graduko errepresentazioetarako, demagun* $\widehat{\mathbb{Z}}$*-ren* χ_1, χ_2 *bi karakter irreduzible ezberdin direla, orduan* G*-ren* $\chi_1 \otimes \chi_2 + \chi_2 \otimes \chi_1$ *errepresentazioa irreduziblea da eta mota horretako errepresentazioen kopurua* $\frac{1}{2}(q-1)(q-2)$ *da.*

Hala eta guztiz ere, errepresentazio absolutuki irreduzibleez hitz egiten dugunez, beste errepresentazio batzuen definizio-gorputza espero baino txikiagoa izatea gerta liteke. Hots, $\rho : G \to \mathrm{GL}_2(\mathbb{F}_q)$ *existi daiteke, non* ρ *errepresentazioa* $\mathbb{F}_{q^2}$*-ren gainean diagonalgarria den. Horiek zenbatu ahal izateko, honako emaitza hau erabiliko dugu: errepresentazio absolutuki irreduzibleak Galoisen automorfismoarekiko inbarianteak dira (ikusi 2.4. atala). Aurreko emaitza erabiliz,* a_1 *elementuaren irudiaren balore propioek* $\mathrm{Gal}(\mathbb{F}_{q^2}|\mathbb{F}_q)$ *Galoisen taldearen orbita berean egon behar direla ondoriozta dezakegu (ohar bedi aurreko paragrafoan agertu diren errepresentazioek ere betetzen dutela gauza bera). Horrenbestez, bigarren mota horretako errepresentazioen kopurua* $\frac{1}{2}(q^2 - q)$ *da.*

Beraz, honako hau dugu:

$$r^*(G, \mathbb{F}_q, 2) = \frac{1}{2}(q-1)(q-2) + \frac{1}{2}(q^2 - q) = q^2 - 2q + 1.$$

Azkenik, kalkulatu $\zeta_G(s)$ *zeta-funtzioa:*

$$\exp\left(\sum_{p\neq 2}\left(\sum_{j=1}^{\infty}\frac{2(p^j-1)}{j}p^{-sj} + \sum_{j=1}^{\infty}\frac{p^{2j}-2p^j+1}{j}p^{-2sj}(p^j+1)\right)\right)\cdot$$
$$\exp\left(\sum_{j=1}^{\infty}\frac{2^j-1}{j}p^{-sj} + \sum_{j=1}^{\infty}\frac{2^{2j}-2\cdot 2^j+1)}{j}p^{-2sj}(2^j+1)\right) = \dots$$
$$= \left(1-\frac{1}{2^{s-1}}\right)\left(1-\frac{1}{2^s}\right)^{-1}\frac{\zeta(s-1)^2}{\zeta(s)^2}\cdot\frac{\zeta(2s)\zeta(2s-3)}{\zeta(2s-1)\zeta(2s-2)}.$$

Ohartu $\frac{1}{2}$ *faktorea desagertzen dela, magia bailitzan.*

Aurreko adibidean, errepresentazio absolutuki irreduzibleen ordez errepresentazio irreduzibleak erabiltzea burura dakiguke. Hori egingo bagenu, kalkulu batzuen ondoren lortzen dugun $Z_G(s)$ zeta-funtzioa honako modu honetakoa izango litzateke:

$$Z_G(s) = \frac{\zeta(s-1)^2}{\zeta(s)^2}\cdot\frac{\zeta(2s)}{\zeta(2s-2)}\sqrt{\frac{\zeta(2s-3)}{\zeta(2s-1)}}.$$

Dakusagunez, erro karratua agertu da, eta funtzio hau ez da arrazionala! Horrenbestez, nahiz eta $Z_G(s)$ ezaugarri interesgarriak eduki, zergatik erabaki dugu gure zeta-funtzioa errepresentazio absolutuki irreduzibleen bitartez definitzea? Hurrengo teoremak emandako $\zeta_G(s)$ funtzioa naturalagoa dela adieraziko digu, probabilitatearekiko beste ezusteko lotura bat azalduz.

Teorema eman aurretik, azken teoria zatia behar dugu. Izan bedi R eraztun profinitua. Orduan, R gehiketarekiko talde profinitu abeldarra denez, R eraztunari μ Haar neurria dagokio. Hori dela eta, ausaz hautatutako R-ren k elementuk R osoa sortzeko probabilitatea honako modu honetan defini dezakegu:

$$P_R(R,k) = \mu\left(\left\{(x_1,\dots,x_k) \in R^k \mid \overline{\langle x_1,\dots,x_k\rangle_R} = R\right\}\right).$$

Ohar bedi aurreko definizioan ausazko elementuek R-modulu egiturarekiko R eraztuna sortzen dutela. Bereziki, G talde profinitua bada, aurrekoa G-ren $\widehat{\mathbb{Z}}$-rekiko talde eraztunaren kasuan egin daiteke.

7.7. teorema ([8]). *Izan bedi G talde profinitua. Orduan, k zenbaki arrunt handi samar guztietarako honako hau betetzen da:*

$$\zeta_G(k) = P_{\widehat{\mathbb{Z}}[\![G]\!]}(\widehat{\mathbb{Z}}[\![G]\!], k)^{-1}.$$

Horrenbestez, gure zeta-funtzioak talde eraztuna sortzeko probabilitateak kodifikatzen ditu. Beste alde batetik, analisi konplexu pixka bat erabiliz, probabilitatearen balore horiek zeta-funtzioa guztiz zehazten dutela frogatu daiteke. Izan ere, *serieen bidez* definitutako f eta g bi funtzio konplexu badira, non zenbaki arrunt guztietan balore berdina duten, orduan $f = g$ da. Emaitza hori analisi konplexuko edozein liburutan aurki daiteke.

Bukatzeko, badirudi arestian definitu dugun zeta-funtzioak oso ezaugarri interesgarriak dituela eta uste dugu funtzio horiek aztertzeak lagundu diezagukeela gorputz finituen gaineko errepresentazioak ulertzen.

Erreferentziak

[1] Babai, Lászó. *The probability of generating the symmetric group*. J. Combin. Theory Ser. A 52 (1989), no. 1, 148–153.

[2] Blackburn, N.; Huppert, B. *Finite groups. II*. Grundlehren der Mathematischen Wissenschaften, 242. Springer-Verlag, 1982.

[3] Borovik, A. V.; Pyber, L.; Shalev, A. *Maximal subgroups in finite and profinite groups*. Trans. Amer. Math. Soc. 348 (1996), no. 9, 3745–3761.

[4] Bhattacharjee, M. *The probability of generating certain profinite groups by two elements*. Israel J. Math. 86 (1994), no. 1-3, 311–329.

[5] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. *ATLAS of finite groups. Maximal subgroups and ordinary characters for simple groups*. Oxford University Press, Eynsham, 1985.

[6] Corob Cook, G. *On profinite groups of type* FP_∞. Adv. Math. 294 (2016), 216–255.

[7] Corob Cook, G.; Kionke, S.; Vannacci, M. *Counting irreducible modules for profinite groups*. Rev. Mat. Iberoam. 39 (2023), no. 4, 1519–1566.

[8] Corob Cook, G.; Kionke, S.; Vannacci, M. *Weil zeta functions of group representations over finite fields.* Preprint *arXiv:2212.03748*.

[9] Corob Cook, G.; Vannacci, M. *Probabilistic finiteness properties for profinite groups*. J. Algebra 574 (2021), 584–616.

[10] Dixon, J. D.; Mortimer, B.; *Permutation groups*. Graduate Texts in Mathematics, 163. Springer-Verlag, 1996.

[11] Hall, M. Jr. *Subgroups of finite index in free groups*. Can. J. Math. 1 (1949).

[12] Hardy, G. H.; Wright, E. M. *An introduction to the theory of numbers*. Oxford University Press, Oxford, 2008.

[13] Kionke, S.; Vannacci, M. *Positively finitely related profinite groups*. Israel J. Math. 225 (2018), no. 2, 743–770.

[14] Lubotzky, A.; Segal, D. *Subgroup growth*. Progress in Mathematics, 212. Birkhäuser Verlag, Basel, 2003.

[15] Mann, A.; Shalev, A. *Simple groups, maximal subgroups, and probabilistic aspects of profinite groups*. Israel J. Math. 96 (1996), part B, 449–468.

[16] Robinson, Derek J. S. *A course in the theory of groups*. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[17] Tao, T. *Analysis. I*. Texts and Readings in Mathematics, 37.6 Springer, Singapore, 2016.

[18] Wilson, J. S. *Profinite groups*. London Mathematical Society Monographs. New Series, 19. The Clarendon Press, Oxford University Press, New York, 1998.