NYILATKOZAT

Név: Miklósi Roland Botond

ELTE Természettudományi Kar, szak: Matematika MSc

NEPTUN azonosító: I9K63K

Szakdolgozat címe: Cayley-gráfok és átmérőjük

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2023.06.06

a hallgató aláírása

Cayley-gráfok és átmérőjük

Diplomamunka

Matematikus Msc

Szerző: Miklósi Roland Botond

Témavezető: Dr. Halasi Zoltán

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Matematika Intézet

Budapest, 2023

Tartalomjegyzék

Bevezetés

Talán mindenki számára ismert hungarikum Rubik Ernő játéka, a Rubik-kocka. Ezen kirakós első ránézésre nagyon egyszerűnek tűnhet, legalábbis ez lehet az ember első benyomása róla, azonban hamar kiderül, hogy valójában ez az egyszerű szabályok által vezérelt játék megoldása egy meglehetősen nehéz feladat, és bárki számára tartogat kihívásokat. Értem ezalatt azt, hogy míg egy kezdő játékosnak óriási élményt jelenthet a kocka kirakása, addig egy profi versenyzőnek másodpercek töredékeival való előrelépés is nagy fejlődésnek számít. Tehát van egy egyszerűnek tűnő játékunk, ami valójában roppant nehéz és összetett. Ezt a nehézséget a Rubik-kocka matematikai leírása is jól szemlélteti.

A csoportelmélet jó eszköztárat biztosít a Rubik-kocka struktúrájának alapos matematikai vizsgálatára. Legyen G_R a kocka szimmetriacsoportja és $S_R = \{U, D, L, R, F, B\}$ az a generátorrendszer, amelyben a megfelelő betű a megfelelő lap óramutató járásával megegyező 90°-os forgatását jelöli (például $U =$"up" azaz a felső lap stb.), vagyis minden csoportelem egy forgatássorozat, ami a kocka egy adott pozícióját reprezentálja. Ezen csoport alternáló és ciklikus csoportok direkt és szemidirekt szorzataiként előálló szörnyeteg, nevezetesen

$$G_R \cong \left(C_3^7 \times C_2^{11}\right) \rtimes \left((A_8 \times A_{12}) \rtimes C_2\right),$$

amely alapján a G_R rendje

$$\begin{aligned} |G_R| &= \left(3^7 \cdot 2^{11}\right) \cdot \left(\left(\frac{8! \cdot 12!}{4}\right) \cdot 2\right) \\ &= 43\,252\,003\,274\,489\,856\,000. \end{aligned}$$

A sok különböző lehetőség ellenére a kocka kirakása nagyon jól algoritmizálható, így az évek során számtalan megoldási módszert fejlesztettek ki a Rubik-kocka szerelmesei (pl. Friedrich metódus, Roux metódus stb.).

Láthatjuk tehát, hogy a Rubik-kocka nagyon gazdag matematikai struktúrával rendelkezik, ami összhangban van azzal a tapasztalati ténnyel, hogy a kirakása nagyon nehéz. Mindezek ellenére ez a bonyolult struktúra tartalmaz magában egy meglepően egyszerű és hihetetlennek hangzó információt. Szinte azonnal feltevődik a kérdés, hogy egy teljesen általános pozíciót kézhez kapva legfennebb mennyi forgatás szükséges ahhoz, hogy a kocka kirakott állapotba kerüljön. Erre vonatkozó kutatásokat és kísérleteket már 1981 óta végeznek, végül 2014-ben Rockiki és Davidson bizonyították, hogy ez a szám 26, vagyis a

kocka tetszőleges pozícióból legfennebb 26 forgatással kirakható, ami meghökkentő ahhoz mérten, hogy a kocka csoportja milyen nagy. A Rubik-kockával foglalkozó kutatók és versenyzők körében ezt a számot Isten számának nevezik. Megjegyzendő, hogy ha egy lap 180°-os forgatását csak egy forgatásnak tekintjük (ez az ún. *half turn metric*), akkor ez a szám 20.

Ez a nem kissé meglepő eredmény más megfogalmazásban azt jelenti, hogy a (G_R, S_R) páros hoz tartozó *Cayley-gráf* átmérője pontosan 26, amely azt jelenti, hogy bármely csoportbeli elem felírható legfennebb 26 generátorelemmel és azok inverzeivel. A Cayley-gráf bármely csoport és hozzá tartozó generátorrendszer esetén definiálható (lásd a későbbi fejezetben) és fontos információt tárol a csoport struktúráját illetően. Cayley-gráfok átmérőjére a $\frac{\log|G|}{\log(2|S|)}$ általános alsó korlátot ad, viszont ha G kommutatív, akkor a Cayley-gráf átmérője ennél az értéknél jóval nagyobb lehet. Babai László, neves magyar matematikus, a nem kommutatív véges egyszerű csoportok Cayley-gráfjának átmérőjével kapcsolatosan fogalmazott meg egy nagyon erős sejtést, miszerint a G csoporttól függetlenül létezik olyan $c > 0$ konstans, hogy

$$\operatorname{diam}(\operatorname{Cay}(G, S)) < (\log |G|)^c,$$

ahol S tetszőleges generátorrendszere G-nek. Ez azt jelenti, hogy nem kommutatív véges egyszerű csoportok esetén az általános felső korlát nem sokkal nagyobb, mint a $\frac{\log|G|}{\log(2|S|)}$ alsó korlát. Részeredményeket sikerült elérni, viszont teljes egészében a probléma a mai napig megoldatlan.

Ezen szakdolgozat nem tartalmaz egyéni eredményt, célja a Cayley-gráfokkal való ismerkedés és azok átmérőjével kapcsolatos néhány fontos eredmény ismertetése. Ennek szellemében a szakdolgozat a következőképpen épül fel:

- az *első fejezet*ben a Cayley-gráfokkal kapcsolatos alapvető definíciókat és tulajdonságokat mutatjuk be (mint például a csúcstranzitivitás és regularitás, Sabidussi híres karakterizációs tételei stb.), néhány standard példával szemléltetve az elméletet;

- a *második fejezet* a Cayley-gráfok átmérőjéről szól, néhány alapvető eredmény ismertetése után belátjuk Babai és Seress 1987-es tételét, amely felső korlátot ad a szimemtrikus és alternáló csoportok átmérőjére, majd kitérünk a Babai-sejtéssel kapcsolatos jelenleg ismert eredményekre;

- a *harmadik fejezet* Cayley-gráfokkal kapcsolatos alkalmazásokat tartalmaz: bizonyítjuk a Nielsen-Schreier-tételt Cayley-gráfok segítségével, megvizsgáljuk a legrövidebb utak problémáját Cayley-gráfokban, végül a 2-rangú szabad csoport Cayley-gráfján adunk egy paradox felbontást a Banach-Tarski paradoxon bizonyításához.

Köszönetnyilvánítás

Ezúton szeretném köszönetemet kifejezni mindazoknak, akik nélkül ez a dolgozat nem készülhetett volna el.

Köszönöm Halasi Zoltán tanár úrnak, hogy felkeltette az érdeklődésemet a téma iránt, és mély szakértelemmel és türelemmel vezetett a dolgozat megírása közben. Köszönöm a konzultációkat, a sok hasznos tanácsot és segítséget, amiknek hála jobban megérthettem a fogalmakat és az azok közötti kapcsolatokat.

Továbbá köszönöm minden kedves tanáromnak, hogy betekintést nyújtottak a matematika egy-egy nagyobb szeletébe, ami által egy nagyon színes, szerteágazó mégis mélyen összefüggő világot ismerhettem meg. Az előadások hallgatása, a gyakorlatokra való készülés és az eszmecserék nagyon inspirálóak és motiválóak voltak számomra, így az évek során kíváncsibbá és lelkesebbé váltam a matematika műveléséhez.

Hálával tartozok a családomnak, akik lelki és anyagi támogatása nélkül nem tarthatnék most ott, ahol vagyok. Külön köszönöm a húgomnak, a kedvesemnek és a barátaimnak, hogy mindvégig hittek bennem és a nehezebb időszakokban is türelemmel és biztatással fordultak felém.

Végezetül köszönöm a Márton Áron Szakkollégiumnak a tanulmányaim során nyújtott anyagi támogatást, a műhelygyűlések és a szakkollégiumi konferenciák nagyon tanulságosak voltak, sokat tudtam belőlük meríteni úgy szakmailag, mint emberileg is.

1 Cayley-gráfok

Ehhez az fejezethez többnyire a [LaSe16], [Me08], [GoRo13], [Sa58], [Sa64], [Lö15] és a [Zh21] cikkekből és jegyzetekből inspirálódtunk.

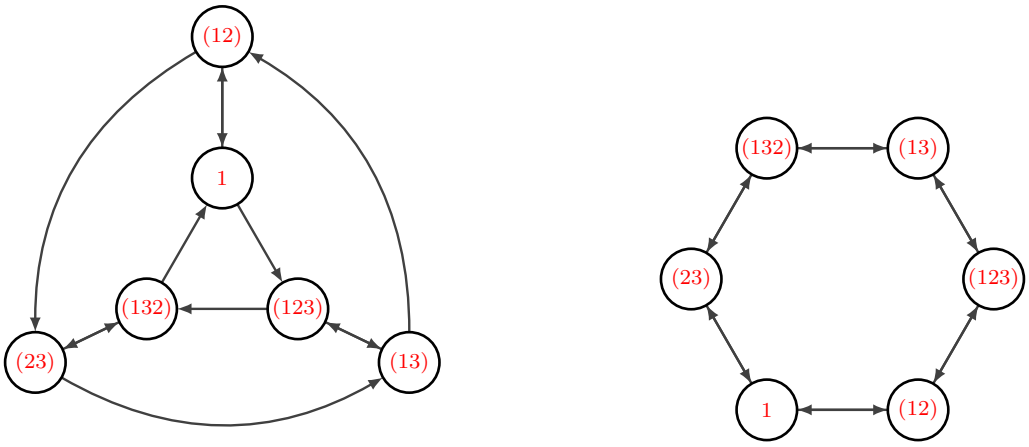
Ahogyan azt a bevezető rész végén is írtuk, ez a fejezet Cayley-gráfokkal kapcsolatos alapvető definíciókat, tulajdonságokat és példákat tartalmaz. Csoportelméleti tanulmányaink egyik nagyon fontos tétele a *Cayley-tétel*, amely kimondja, hogy minden csoportra tekinthetünk permutációcsoportként, pontosabban minden G csoport izomorf a $\mathrm{Sym}(G)$ szimmetrikus csoport egy részcsoportjával. Egy hasonló, szintén Cayley nevéhez fűződő tételből juthatunk el a Cayley-gráf definíciójához.

1.1. Tétel. *Minden végesen generált csoport hűen reprezentálható egy összefüggő, irányított, lokálisan véges gráf automorfizmuscsoportjának egy részcsoportjaként.*

Egy irányított gráfot akkor nevezünk *lokálisan végesnek*, ha bármely v csúcs esetén a bemenő élek száma (v *be-foka*), illetve a kimenő élek száma (v *ki-foka*) véges.

Bizonyítás. Legyen G egy végesen generált csoport és $S = \{s_1, ..., s_n\}$ véges generátorrendszere G-nek. Legyen $\Gamma := \vec{\mathrm{Cay}}\,(G, S)$ az az irányított gráf melynek csúcsait a G elemei alkotják és minden $g \in G$ és $s \in S$ elemekhez rendeljük hozzá a $g \to gs$ irányított élt. Ezt nevezzük a G csoporthoz és S generátorrendszerhez tartozó *irányított Cayley-gráf*nak (röviden *Cayley-digráf*). Mivel G végesen generált ezért Γ lokálisan véges lesz, hiszen ha kijelölünk egy tetszőleges g csúcsot a gráfon, akkor az csak véges sokféleképpen állhat elő hs alakban, hiszen S véges. Mivel S generátorrendszer, ezért bármely $v, w \in G$ elem esetén a $v^{-1}w$ felírható a $S \cup S^{-1}$-beli elemek szorzataként, ami a Γ Cayley-gráfban éppen egy (nem feltétlen irányított) utat jelent v-ből w-be. Ebből adódik, hogy Γ összefüggő. A G csoport hatása a Γ gráfon baloldali eltolással adódik, speciálisan legyen $g \in G$ tetszőleges elem, amely a h-val jelölt csúcsot a gh csúcsba képezi, ami a csúcshalmaz egy permutációját eredményezi. Azt, hogy ily módon egy $g \in G$ elem gráfhomomorfizmusként hat a gráfon, a későbbiekben fogjuk belátni. Ezzel bizonyítottuk, hogy G része a Γ automorfizmuscsoportjának. □

Megjegyzendő, hogy a fenti tételben adott konstrukció erősen függ az S generátorrendszer választásától. Ez az S_3 szimmetrikus csoporton keresztül egyszerűen szemléltethető. Legyenek $S = \{(1,2), (1,2,3)\}$ és $S' = \{(1,2), (2,3)\}$ generátorrendszerek. Ekkor a következő két digráfhoz jutunk:



1.1. ábra. $\overrightarrow{\mathrm{Cay}}\,(S_3, S)$ és $\overrightarrow{\mathrm{Cay}}\,(S_3, S')$

Az 1.1-es Tétel jó lehetőséget ad arra, hogy egy adott csoport tulajdonságait gráfelméleti szempontból vizsgáljuk. Valójában a tétel kimondható irányítatlan gráfokkal is, a konstrukció annyiban módosul, hogy az élekre irányítatlan élekként gondolunk. Így jutunk el az *irányítatlan Cayley-gráf* (röviden *Cayley-gráf*) fogalmához.

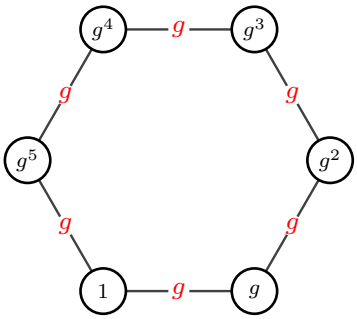
1.2. Definíció. Legyen G egy tetszőleges végesen generált csoport, $S \subset G$ tetszőleges véges generátorrendszerrel. A $\mathrm{Cay}\,(G, S)$ *Cayley-gráf* az a gráf, melynek csúcsait a G csoport elemei adják és két $g, h \in G$ csúcs között pontosan akkor halad él, ha létezik olyan $s \in S$ elem, melyre $h = gs$ vagy $g = hs$.

A hurokélek elkerülése érdekében mindig fel fogjuk tenni, hogy S olyan generátorrendszer, ami nem tartalmazza az egységelemet. A definíciókból könnyen adódik, hogy a Cayley-gráf egyszerűen úgy keletkezik, hogy vesszük a Cayley-digráfot és elhagyjuk az élek irányítását. Általánosabban azt is megtehetjük, hogy magáról az S-ről nem követeljük meg, hogy generátorrendszer legyen. Ekkor viszont a Cayley-gráf nem lesz összefüggő. Továbbá ha S zárt az inverzképzésre, akkor a Cayley-gráf azonosítható a Cayley-digráffal. Valóban, ha g és h között halad irányított él, akkor $h = gs$, ugyanakkor $g = hs^{-1}$ is teljesül, ami azt jelenti, hogy a h és g között is halad irányított él.

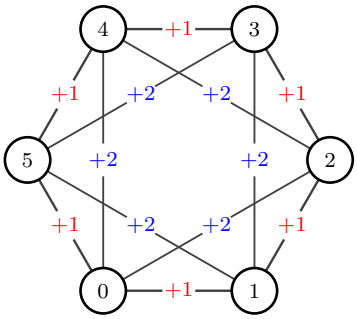
A következő néhány fontosabb példán keresztül szemléltetjük a definíciót, további példák és azok részletesebb tárgyalása olvasható a [LaSe16] jegyzetből.

1.3. Példa. Kezdjük a legegyszerűbb példával. Ha $G = (\mathbb{Z}, +)$ végtelen ciklikus csoport és $S = \{1\}$, akkor a Cayley-gráf egy végtelen lánc lesz.

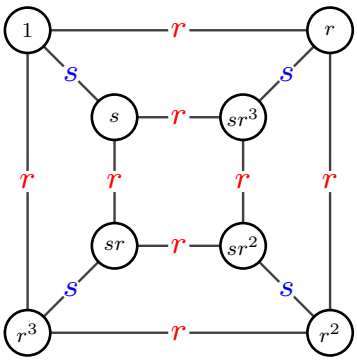
1.4. Példa. Legyen $C_n = \{g\}$ az n-elemű ciklikus csoport g generátorral. Ekkor a hozzá tartozó $\mathrm{Cay}\,(\mathrm{C}_n, g)$ Cayley-gráf egy n csúcsú körgráf. Ez az $n = 6$ esetén a következőképpen néz ki:



1.5. Példa. Az előző példát tovább tarkíthatjuk. Legyen $n = 6$, vegyük a $(C_6, \cdot) \cong (\mathbb{Z}_6, +)$ azonosítást és tekintsük az $S = \{1, 2\}$ generátorrendszert. Ekkor a Cayley-gráf az előző példához hasonlóan egy szabályos hatszög lesz, mely (az extra generátorelem következtében) kiegészül kettő darab 3 hosszúságú körrel, mint ahogyan azt a következő ábra is mutatja:



1.6. Példa. Tekintsük a szabályos négyoldalú sokszög szimmetriacsoportját, vagyis a D_4 diédercsoportot és legyen $S = \{r, s\}$, ahol r egy forgatás, s pedig egy tükrözés. Ekkor a Cay (D_4, S) Cayley-gráf a következő:

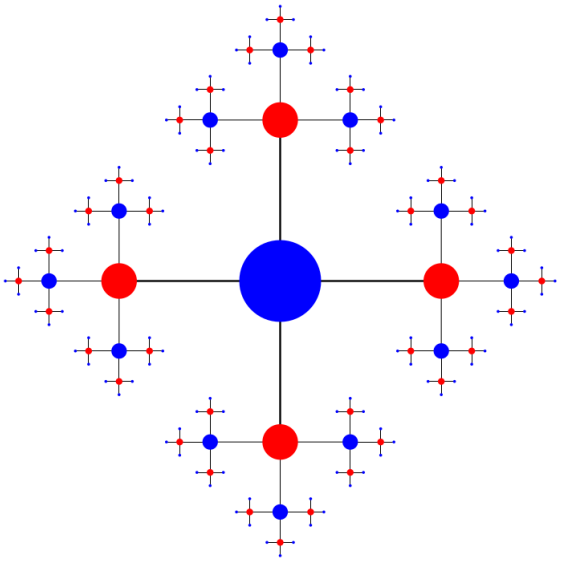


Vegyük észre, hogy a Cayley-gráfban megjelenő körök tulajdonképpen a csoportbeli relációknak felelnek meg.

A következő példához röviden felelevenítjük a szabad csoport definícióját. Legyen S egy tetszőleges halmaz. Az $s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}$ $(n \geq 0, s_i \in S, \epsilon_i \in \{-1, +1\})$ alakú sorozatokat szavaknak nevezzük. Ha egy adott szóban megjelenik egy s és az s^{-1} betű egymás mellett,

akkor velük egyszerűsíthetünk. Hasonlóan, egy szóban bármely két egymást követő elem közé beszúrhatjuk az ss^{-1} vagy az $s^{-1}s$ szavakat. Az ilyen egyszerűsítéseket és bővítéseket elemi átalakításoknak nevezzük. Két szót ekvivalensnek nevezünk, ha elemi átalakítások véges sorozatából megkaphatók egymásból. Az S, mint szabad generátorrendszer által generált szabad csoport elemei a szavak (ezen reláció szerinti) ekvivalenciaosztályai, míg a csoport műveletet konkatenáció (egymás mellé írás) segítségével definiáljuk, az egységelemet az üres szó osztálya képezi. Ezt a csoportot $F(S)$-el jelöljük, és S elemszámát a szabad csoport rangjának nevezzük. Ha $|S| = n$ véges szám, akkor szokásos az F_n jelölés is. A szabad csoportok teljesítik a következő univerzális tulajdonságot: ha G egy tetszőleges csoport és $\varphi : S \to G$ tetszőleges leképezés, akkor egyértelműen létezik egy $\overline{\varphi} : F(S) \to G$ csoporthomomorfizmus úgy, hogy $\overline{\varphi} \circ \iota = \varphi$, ahol ι az S kanonikus beágyazása $F(S)$-be. Ezzel a definícióval nagyon sok helyzetben könnyebb dolgozni.

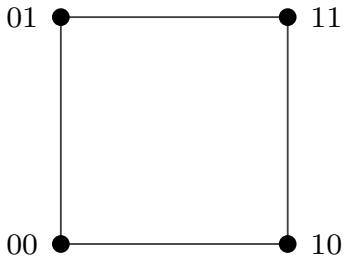
1.7. Példa. A következő, hópehelyre emlékeztető, ábra sokak számára ismerős lehet. Ez az $F_2 = \langle x, y \,|\, \rangle$ 2-rangú szabad csoport Cayley-gráfja. Itt a kék színű csúcsok olyan $x^{\alpha_1}y^{\beta_1}\cdots x^{\alpha_n}y^{\beta_n}$ alakú elemek, melyekre $\alpha_1 + ... + \alpha_n + \beta_1 + ... + \beta_n$ páros, míg a piros csúcsok esetén (kizáró) vagy az $\alpha_1 + ... + \alpha_n$ vagy a $\beta_1 + ... + \beta_n$ páratlan. A kék színű csúcsok halmaza egy 2-indexű részcsoportot alkot F_2-ben, ennek a komplementere (a piros csúcsok halmaza) pedig ezen részcsoport mellékosztálya.



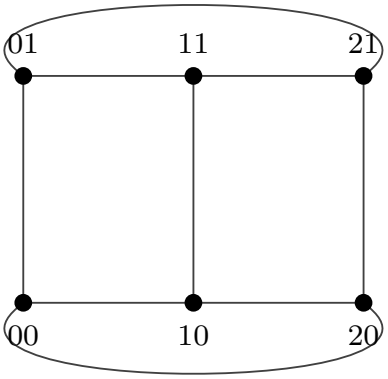
1.2. ábra. Az F_2 Cayley-gráfja

1.8. Példa. Legyen $G = \mathbb{Z}_n \times \mathbb{Z}_m$ ciklikus csoportok direkt szorzata és legyen $S = \{(1,0), (-1,0), (0,1), (0,-1)\}$ generátorrendszere G-nek. Az egyszerűség kedvéért az (i,j) párt, ahol $0 \leq i < n$ és $0 \leq j < m$, jelöljük ij-vel. Mivel S elemszáma 4, ezért minden ij csúcsnak 4 szomszéda lesz abban az esetben, amikor $m, n > 2$. Az így kapott Cayley-gráfot $(n \times m)$-es *tórikus rácsgráf*nak nevezzük. Ezek a gráfok, ahogyan a nevük

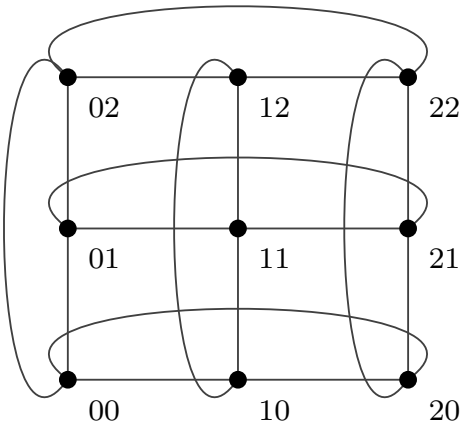
is jelzi, a 2-dimenziós tórusz felületére rajzolhatók. Ez azt jelenti, hogy a gráf csúcsait a tórusz pontjainak feleltetjük meg, az éleket pedig $[0,1]$ intervallumok homeomorf képeivel azonosítjuk a tóruszon oly módon, hogy egy e élnek megfelelő ív végpontjai pontosan az e csúcsainak felelnek meg a gráfban, az e-nek megfelelő ív más csúcsot nem tartalmaz, valamint két ív sosem metszi egymást belső pontban. Az 1.3-as, 1.4-es és 1.5-ös ábrákon az egyszerűbb 2-dimenziós tórikus rácsgráfokat szemléltettük, valamint a 1.6-os ábrán a kvaterniócsoport Cayley-gráfja látható a tóruszra rajzolva.



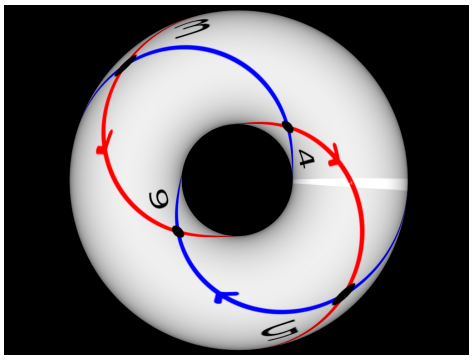
1.3. ábra. (2×2)-es tórikus rácsgráf



1.4. ábra. (3×2)-es tórikus rácsgráf



1.5. ábra. (3×3)-as tórikus rácsgráf

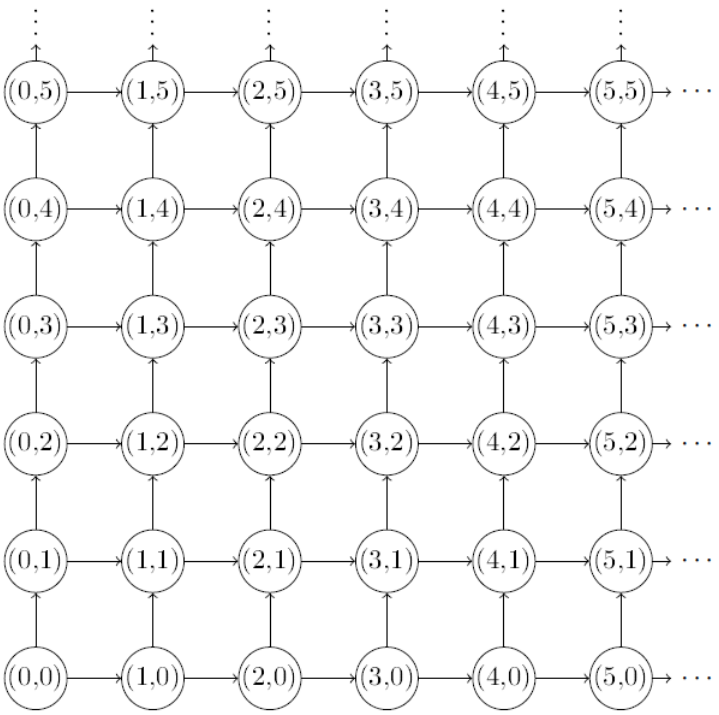


1.6. ábra. Kvaterniócsoport Cayley-gráfja a tóruszon

Ez a konstrukció tetszőleges d dimenzióban általánosítható. Egyszerűen legyen $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_d}$ és $S = \{(\pm 1, 0, ..., 0), (0, \pm 1, ..., 0), ..., (0, ..., \pm 1)\}$. Például a párhuzamos szuperszámítógépekkel kapcsolatos *Cray-kutatás* egy 3-dimenziós tórikus hálózatot vesz alapul.

1.9. Példa. A példák sorát egy némileg általánosabb konstrukcióval zárjuk. Vegyük észre,

hogy a Cayley-gráf definíciójában sehol sem használtuk a csoportnak azt a tulajdonságát, hogy van egységeleme és minden eleme invertálható, tehát egy félcsoport esetén is értelmes definícióhoz jutunk. Vegyük az $(\mathbb{N}^2, +)$ félcsoportot, ahol a „+” a pontonkénti összeadás, és tekintsük az $S = \{(1,0), (0,1)\}$ generátorrendszert. Ekkor a Cayley-digráf egy végtelen háló lesz:

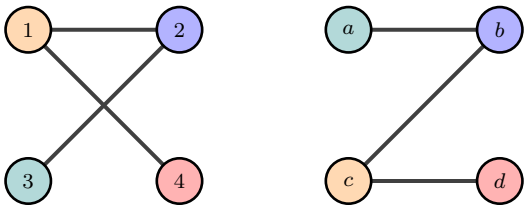


A továbbiakban a Cayley-gráfok néhány alapvető tulajdonságát vizsgáljuk meg, amihez előbb gráfelméleti fogalmakat elevenítünk fel. A következőkben minden gráfra a standard $\Gamma = (V, E)$ gráfelméleti jelölést fogjuk használni, ami alatt azt kell érteni, hogy a Γ gráfot a V csúcshalmaz és az E élhalmaz segítségével adtunk meg. Az általános matematikai filozófiát követve definiáljuk a gráfok közötti homomorfizmus fogalmát. Ha a v,$w \in V$ csúcsok között halad él, akkor ezt az egyszerűség kedvéért jelöljük a $v \sim w$ relációval, illetve a köztük haladó élt $\{v, w\} \in E$ módon jelöljük.

1.10. Definíció. Legyen $\Gamma_1 = (V_1, E_1)$ és $\Gamma_2 = (V_2, E_2)$ két tetszőleges gráf. Egy $\varphi : V_1 \to V_2$ leképezést Γ_1-ből Γ_2-be menő *gráfhomomorfizmus*nak nevezünk, ha minden $v, w \in V_1$ csúcs esetén, melyekre $v \sim w$ következik, hogy $\varphi(v) \sim \varphi(w)$, tehát az élek is élekbe képződnek a φ által. Ha φ bijektív és az inverze is gráfhomomorfizmus, akkor φ-t *gráfizomorfizmus*nak nevezzük. A $\Gamma \to \Gamma$ gráfizomorfizmusokat *gráfautomorfizmus*oknak nevezzük. A Γ összes automorfizmusa a függvénykompozícióval ellátva csoportot alkot, és ezt nevezzük a Γ gráf *automorfizmuscsoportjá*nak. Jelöljük ezt a csoportot $\mathrm{Aut}(\Gamma)$-val.

A következő ábrán két egymással izomorf gráf látható, ahol az izomorfizmust az $1 \to c$, $2 \to b$, $3 \to a$ és $4 \to d$ hozzárendelés definiálja. Megemlítendő, hogy nem izomorf cso-

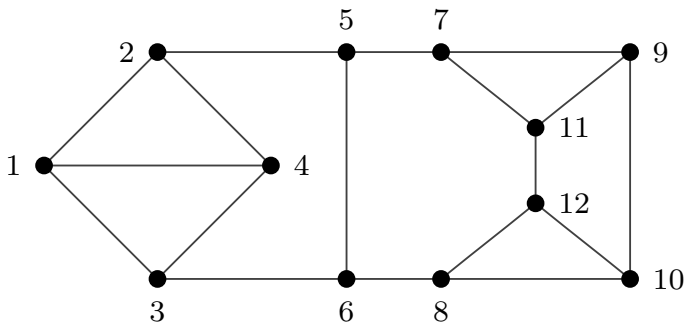
portoknak lehet izomorf Cayley-gráfjuk. Például a $\mathrm{Cay}(S_3, \{(1,2), (2,3)\})$ és $\mathrm{Cay}(C_6, \{g\})$ gráfok izomorfak, de az S_3 nem izomorf a C_6-al.



Az $\mathrm{Aut}(\Gamma)$ csoport nem más, mint egy, a V csúcshalmazon ható permutációcsoport.

1.11. Definíció. Azt mondjuk, hogy a $\Gamma = (V, E)$ gráf *csúcstranzitív*, ha az automorfizmuscsoportja tranzitívan hat a csúcsok halmazán, vagyis bármely $v, w \in V$ csúcs esetén létezik olyan $\varphi \in \mathrm{Aut}(\Gamma)$ gráfautomorfizmus, melyre $w = \varphi(v)$. Egy csúcs foka (jelöljük $\deg(v)$-vel) nem más, mint a rá illeszkedő élek száma, ahol a hurokéleket kétszer számoljuk. Egyszerű gráfban ez pontosan az adott csúcs szomszédainak a száma. A Γ gráfot *reguláris*nak nevezzük, ha minden csúcsnak azonos foka van.

Csúcstranzitív gráfok intuitíven olyan gráfok, amelyek bármely csúcsból szemlélve ugyanolyannak látszanak. Mivel a gráfautomorfizmusok megtartják a fokszámot, ezért minden csúcstranzitív gráf egyben reguláris is. A fordított állítás általában nem igaz. Egy ilyen gráfra példa a 1.7-es ábrán látható. Ha csúcstranzitív lenne, akkor például az 1-es csúcsot az 5-ös csúcsba tudnánk képezni gráfautomorfizmussal, de a gráfautomorfizmusok háromszöget háromszögbe képeznek, viszont az 1-es csúcs része egy háromszögnek, de az 5-ös csúcs nem része egyetlen háromszögnek sem. A következőkben belátjuk, hogy minden Cayley-gráf csúcstranzitív és így reguláris is (ahogyan azt a példák is sejtetik), illetve egy ellenpéldával bizonyítjuk, hogy nem minden csúcstranzitív gráf áll elő valamilyen csoport Cayley-gráfjaként.



1.7. ábra. Reguláris, de nem csúcstranzitív gráf

A csúcstranzitivitás bizonyításához legyen v és w a Cayley-gráfunk két tetszőleges csúcsa.

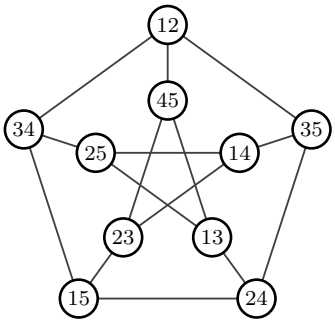
Az $L_a : G \to G$, $g \to ag$ baleltolás a G csúcshalmaz egy bijekciója, melynek inverze $L_{a^{-1}}$. Egyszerű számolás mutatja, hogy L_a gráfhomomorfizmus. Ugyanis ha $x \sim y$, akkor definíció szerint létezik $g \in S$ úgy, hogy $y = xg$, de ekkor

$$a\,(xg) = ay,$$

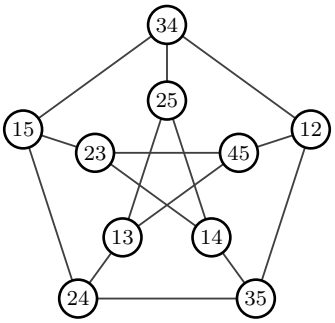
ahonnan az asszociativitás alapján adódik az $(ax)\,g = ay$ egyenlőség. Tehát azt kaptuk, hogy $ax \sim ay$, ami azt jelenti, hogy L_a gráfhomomorfizmus. Ez minden $a \in G$-re igaz, speciálisan $a^{-1} \in G$ elemre is, így az $L_a^{-1} = L_{a^{-1}}$ is gráfhomomorfizmus. Ezzel beláttuk, hogy L_a gráfizomorfizmus.

Az $a = wv^{-1}$ választás révén $L_a\,(v) = av = (wv^{-1})\,v = w$ adódik, és ezzel a készen vagyunk a bizonyítással.

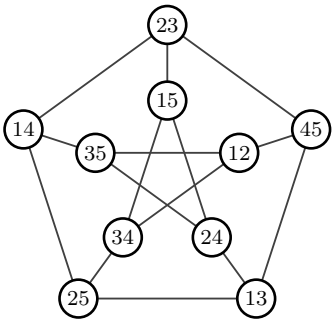
Mivel az 1.7-es ábrán szereplő gráf nem csúcstranzitív ezért Cayley-gráf sem lehet, következésképp nem minden reguláris gráf áll elő Cayley-gráfként. A következőkben arra a kérdésre fogunk választ adni, hogy vajon a csúcstranzitív gráfok Cayley-gráfok-e. Intuitíven persze érezhető, hogy a Cayley-gráfok valamivel „merevebbek”, mint a csúcstranzitív gráfok. Tekintsük az 1.8-as ábrán látható *Petersen-gráfot*.



1.8. ábra. Petersen-gráf



1.9. ábra. $(1, 4, 5, 2, 3)$ hatása



1.10. ábra. $(1, 4, 3, 2)$ hatása

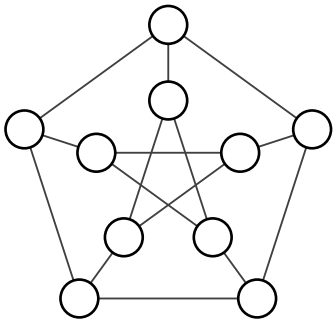
Ez a gráf csúcstranzitív. Ehhez tekintsük az 1.8-as ábrán látható cimkézését. A csúcsokat az $\{1, 2, 3, 4, 5\}$ kételemű részhalmazaival cimkézzük, és két csúcs között pontosan akkor halad él, ha diszjunkt részhalmazokkal vannak cimkézve (például az $\{1, 2\}$ és $\{3, 4\}$ csúcsok között halad él). Röviden egy $\{a, b\}$ részhalmazhoz tartozó csúcsot ab-vel fogunk jelölni. A belső (külső) körben lévő csúcsokat belső (külső) körben lévő csúcsokba könnyedén eljuttathatjuk, ha az $(1, 4, 5, 2, 3)$ permutációt egymás után alkalmazzuk, hiszen ez a belső (külső) csúcsok forgatását eredményezi (lásd az 1.9-es ábrát). Ha tetszőleges belső csúcsot szeretnénk külső csúcsba vinni (vagy fordítva), akkor azt például az $(1, 4, 3, 2)$ permutációval tudjuk elérni (1.10-es ábra). Persze ezzel még nem biztos, hogy a választott csúcsot oda képeztük, ahova szerettük volna, ezért még az $(1, 4, 5, 2, 3)$ permutáció megfelelő hatványát alkalmaznunk kell. Ezek a permutációk gráfautomorfizmusok, ezzel

tehát a Petersen-gráf csúcstranzitivitását beláttuk.

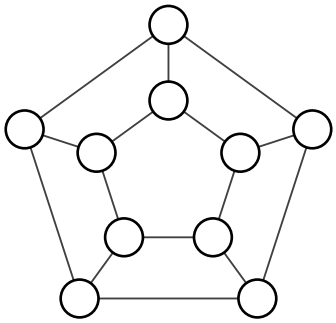
Most megmutatjuk, hogy a Petersen-gráf nem állhat elő Cayley-gráfként. Ha Cayley-gráf lenne, akkor egy tízelemű csoportból származna, tehát vagy a C_{10} ciklikus csoport, vagy a D_{10} diédercsoport és azok valamely generátorrendszere definiálná. Tételezzük fel, hogy a generátorrendszer elemei az $s_1, ..., s_k$ elemek. Ekkor a Cayley-gráfban az e szomszédai az $s_1, ..., s_k, s_1^{-1}, ..., s_k^{-1}$ elemek lesznek. Mivel a Petersen-gráf 3-reguláris, ezért szükséges, hogy a Cayley-gráfban az 1-nek három szomszédja legyen, ez pedig azt jelenti, hogy csak olyan generátorrendszerek jöhetnek szóba, amelyek vagy három másodrendű elemet, vagy egy másodrendű és egy nem másodrendű elemet tartalmaznak.

Ha $D_{10} = \langle r, s \rangle$, ahol $o(r) = 5$ (forgatás) és $o(s) = 2$ (tükrözés), akkor $1 = srsr$, ami egy 4 hosszúságú körnek felel meg a Cayley-gráfban, viszont ilyen kör a Petersen-gráfban nincs, tehát nem lehetnek izomorf gráfok (vö. az 1.11-es és 1.12-es ábrákat). Ha $D_{10} = \langle a, b, c \rangle$, ahol a, b és c három különböző tükrözés és $c = aba$ vagy $c = bab$, akkor az $1 = caba$ vagy az $1 = cbab$ 4 hosszú kört kapjuk. Ha c nem egyezik meg az a, b, aba és bab tükrözések egyikével sem, akkor c-re már csak egy lehetőség maradt, hiszen összesen öt tükrözése van a szabályos ötszögnek. Ekkor a cac tükrözés nem lehet c, a és bab sem, mert az azt implikálná, hogy $c = a$ vagy $c = b$. Ha $cac = aba$, akkor $cbc = bab$, mert a c-vel való konjugálás úgy hat a másik négy tükrözésen, hogy két kettes ciklust valósít meg. Viszont ebből azt kapnánk, hogy $c(ab)c = (cac)(cbc) = ababab = (ab)^3$, ami nem lehetséges, hiszen ab egy forgatás, amit ha egy tükrözéssel konjugálunk, akkor az inverzét kell kapnunk, ami $(ab)^4$. Tehát $cac = b$ egyenlőség kell, hogy igaz legyen, ami az $1 = cacb$ azonossághoz vezet. Tehát ebben az esetben sem lehet a Cayley-gráf izomorf a Petersen-gráffal.

A C_{10} ciklikus csoport esetén ha $C_{10} = \langle g^k, g^5 \rangle$, ahol $o(g) = 10$ és $k \in \mathbb{Z}_+$, akkor az $1 = g^k g^5 g^{-k} g^5$ reláció egy 4 hosszúságú kört jelent a Cayley-gráfban, tehát ekkor sem kapunk a Petersen-gráffal izomorf gráfot.

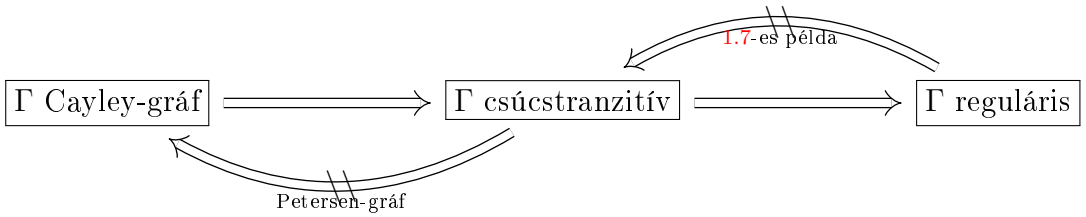


1.11. ábra. Petersen-gráf



1.12. ábra. A D_{10} egy Cayley-gráfja

A következő diagramban összefoglaltuk a fent ismertetett implikációkat.



Legyen $\Gamma = (V, E)$ egy tetszőleges gráf és G a csúcsok egy permutációcsoportja. Tetszőleges $v \in V$ csúcs esetén legyen

$$G_v := \{g \in G : g(v) = v\}$$

a v csúcs *stabilizátora, és*

$$hG_v := \{hg : g \in G_v\}$$

jelölje G_v egy (bal oldali) *mellékosztályát* tetszőleges $h \in G$-re.

1.12. Segédtétel. *Legyen G a V csúcshalmaz egy tranzitív permutációcsoportja és $v \in V$ tetszőleges csúcs. Ekkor a*

$$w \to \{h \in G : h(v) = w\}$$

hozzárendelés bijekció a V és G_v mellékosztályai között.

Fejezetünket Sabidussi két tételével zárjuk: az első a csúcstranzitív gráfokat jellemzi a Cayley-gráfokon keresztül, míg a második a Cayley-gráfokat karakterizálja.

Legyen $\tilde{\Gamma} = \left(\tilde{V}, \tilde{E}\right)$ a $\Gamma = (V, E)$ gráf egy részgráfja, ahol $\tilde{V} \subset V$ és $\tilde{E} \subset E$. Azt mondjuk, hogy a $\tilde{\Gamma}$ a Γ *retraktuma*, ha van olyan $f : \Gamma \to \tilde{\Gamma}$ gráfhomomorfizmus, melynek a $\tilde{\Gamma}$-ra vett megszorítása bijektív. Ekvivalens definícióhoz jutunk, ha a $\tilde{\Gamma}$-ra vett megszorításról azt követeljük meg, hogy az identitás legyen. A $v, w \in V$ csúcsok távolságán a közöttük haladó legrövidebb út hosszát értjük, amit $d(v, w)$-vel jelölünk.

1.13. Tétel. *(Sabidussi, 1964) Minden összefüggő csúcstranzitív gráf egy Cayley-gráf retraktuma.*

Bizonyítás. Legyen $\tilde{\Gamma} = \left(\tilde{V}, \tilde{E}\right)$ összefüggő csúcstranzitív gráf, $v \in \tilde{V}$ egy rögzített csúcs és tekintsük az

$$S := \left\{g \in \mathrm{Aut}\left(\tilde{\Gamma}\right) : v \sim g(v)\right\}$$

halmazt. Legyen G az S által generált részcsoport $\mathrm{Aut}\left(\tilde{\Gamma}\right)$-ban. Ekkor G tranzitívan hat a $\tilde{\Gamma}$ gráfon. Ehhez elegendő belátni, hogy bármely $w \in \tilde{V}$ csúcshoz létezik G-beli elem, ami a v-t a w-be képezi. A bizonyítás $d(v, w)$ szerinti indukcióval történik. Ha $d(v, w) = 1$, akkor a $\tilde{\Gamma}$ csúcstranzitivitása miatt létezik olyan $h \in \mathrm{Aut}\left(\tilde{\Gamma}\right)$ gráfautomorfizmus, amelyre $w = h(v)$ és definíció szerint $h \in S$, tehát $h \in G$. Tegyük fel, hogy $d(v, w) \leq k$-ra igaz az állítás. Ha $d(v, w) = k + 1$, akkor létezik a v-t a w-vel összekötő legrövidebb

úton egy $z \in \tilde{V}$ csúcs, ami szomszédja a w-nek és $d(v,z) \leq k$, így indukciós feltevés alapján létezik olyan $g \in G$ elem, amire $g(v) = z$. A $\tilde{\Gamma}$ csúcstranzitív, ezért van olyan $h \in \mathrm{Aut}\left(\tilde{\Gamma}\right)$ automorfizmus, amelyre $h(z) = w$. Ekkor $hg(v) = w$. Mivel a z és w csúcsok szomszédosak, ezért a $g^{-1}(z)$ és $g^{-1}(w)$ csúcsok is szomszédosak lesznek, tehát $v = g^{-1}(z) \sim g^{-1}(w) = g^{-1}(hg(v))$. Ebből adódik, hogy $g^{-1}hg \in S \subset G$, így $hg = g(g^{-1}hg) \in G$, amit bizonyítani kellett.

Vegyük a $\Gamma = \mathrm{Cay}(G,S)$ Cayley-gráfot. Belátjuk, hogy $\tilde{\Gamma}$ izomorf a Γ egy retraktumával. A 1.12-as Segédtétel alapján az $S_w := \{g \in G : g(v) = w\}$ a G_v stabilizátor egy mellékosztálya, valamint az S előáll úgy, mint $S = \bigcup_{w \sim v} S_w$. Jelöljük $A_1, A_2, ..., A_k$-val a G_v szerinti mellékosztályokat és vegyünk egy-egy $a_i \in A_i$ reprezentánst minden $i = 1, ..., k$-ra. Belátjuk, hogy az $\{a_1, ..., a_k\}$ csúcsok által feszített részgráf[1] izomorf a $\tilde{\Gamma}$-val és retraktuma a Γ-nak. Jelöljük a feszített részgráfot $\Gamma[a_1, ..., a_k]$-val.

Megmutatjuk, hogy $S = G_v S G_v$-vel. Az $S \subseteq G_v S G_v$ irány triviálisan teljesül. Vegyük a $h, h' \in G_v$ és $g \in S$ elemeket. Ekkor definíció szerint $v \sim g(v)$, ahonnan a $v = h(v) \sim g(h(v)) = gh(v)$ adódik és így a $v = h'(v) \sim h'(gh(v)) = h'gh(v)$ is teljesül, tehát $h'gh \in S$.

Most azt látjuk be, hogy minden A_i mellékosztályon belül a Γ-ban nem haladnak élek, valamint két különböző A_i, A_j mellékosztály között vagy nem halad él, vagy az általuk feszített részgráf a $K(A_i, A_j)$[2] teljes páros gráf. Ehhez vegyünk egy $a_i g \in A_i$ és egy $a_j h \in A_j$ $(g, h \in G_v)$ reprezentánst. Az S definíciójából azonnal adódik, hogy $S = S^{-1}$. Ekkor a Cayley-gráf definíciója alapján $a_i g \sim a_j h$ pontosan akkor, ha $(a_i g)^{-1} a_j h \in S$ vagyis $g^{-1} a_i^{-1} a_j h \in S$, ahonnan az $a_i^{-1} a_j \in gSh^{-1} \in G_v S G_v = S$ adódik. Ez azt jelenti, hogy a különböző mellékosztályok elemei közötti szomszédság független a reprezentánsoktól, ez pedig pontosan azt jelenti, hogy két mellékosztályból vagy teljes páros gráfot kapunk, vagy egyáltalán nem haladnak élek az elemek között. Mivel $\tilde{\Gamma}$-ban nincsenek hurokélek ezért $1 \notin S$, tehát $1 = a_i^{-1} a_i \notin S$ és így bármely $g, h \in G_v$ esetén $a_i g \nsim a_i h$.

Definiáljuk a $\varphi : \tilde{\Gamma} \to \Gamma[a_1, ..., a_k]$ leképezést a

$$w \longrightarrow a_i \in S_w$$

hozzárendeléssel. Legyen $x, y \in \tilde{V}$ két tetszőleges csúcs. Mivel G tranzitívan hat $\tilde{\Gamma}$-n, ezért léteznek olyan $g, h \in G$ elemek, melyekre $g(v) = x$ és $h(v) = y$. Ekkor az $x \sim y$ pontosan akkor, ha $g(v) \sim h(v)$. Tehát azt kaptuk, hogy $v \sim g^{-1}h(v)$ vagyis $g^{-1}h \in S$. Másrészt az előzőek alapján $\varphi(x) \sim \varphi(y)$ pontosan akkor, ha $\varphi(x)^{-1} \varphi(y) \in S$. A $g(v) = x$ és

[1] Egy Γ gráf *feszített részgráf*ján egy olyan gráfot értünk, melynek csúcsai az Γ gráf csúcsainak egy S részhalmaza, élei pedig a részhalmazban szereplő csúcsokat összekötő élek. Jelölése: $\Gamma[S]$.

[2] Egy Γ gráfot *páros gráf*nak nevezünk, ha a csúcshalmaz felbontható diszjunk módon A és B részhalmazok uniójára úgy, hogy minden Γ-beli él egyik végponja A-ban, a másik végpontja pedig B-ben van. Jelölés: $\Gamma = (A, B)$.

A $K(A,B)$ *teljes* páros gráf az az (A,B) páros gráf, melynek két osztályának bármely két csúcsa között halad él.

$h(v) = y$ alapján g és h azokat a mellékosztályokat reprezentálják, ahová a $\varphi(x)$ és $\varphi(y)$ tartozik, így feltehetjük, hogy $g = \varphi(x)$ és $h = \varphi(y)$. Ekkor $\varphi(x) \sim \varphi(y)$ pontosan akkor, ha $g^{-1}h \in S$, tehát φ megőrzi az éleket. A φ injektivitása az S_w mellékosztályok diszjunktsága miatt azonnali, míg a szürjektivitás a definíció szerint nyilvánvaló. Ezzel beláttuk, hogy $\tilde{\Gamma}$ izomorf a $\Gamma[a_1, ..., a_k]$ gráffal.

Végül megmutatjuk, hogy $\Gamma[a_1, ..., a_k]$ a Γ retraktuma. Ehhez tekintsük a $\rho : \Gamma \to \Gamma[a_1, ..., a_k]$

$$g \longrightarrow a_i,\ g \in A_i$$

leképezést. Az előző számolás mutatja, hogy ez valóban egy gráfhomomorfizmus és szürjektív, továbbá az is nyilvánvaló, hogy a $\Gamma[a_1, ..., a_k]$-ra vett megszorítás az identitás. □

Végezetül belátjuk Sabidussi karakterizációs tételét [Sa58, Lemma 4].

1.14. Tétel. *(Sabidussi, 1958) Egy $\Gamma = (V, E)$ összefüggő gráf pontosan akkor Cayley-gráfja egy G csoportnak és valamilyen $S \subset G$ generátorrendszernek, ha Γ automorfizmuscsoportja tartalmaz egy olyan $G_0 \leq Aut(\Gamma)$ részcsoportot, ami regulárisan hat a Γ csúcsain.*

Bizonyítás. Előbb tegyük fel, hogy a Γ valamilyen G csoport Cayley-gráfja. Tekintsük a $L : G \to \mathrm{Aut}(\Gamma)$, $g \longrightarrow \left(h \xrightarrow{L_g} gh\right)$ baleltolásokkal vett hatást, ami nyilván reguláris. Az L értelemszerűen injektív, így $G \cong \mathrm{Im}(L) \leq \mathrm{Aut}(\Gamma)$ tehát a $G_0 := \mathrm{Im}(L)$ jó lesz.

Most tételezzük fel, hogy a Γ öszefüggő gráf automorfizmuscsoportja tartalmaz egy G_0 részcsoportot, amely a csúcsokon reguláris. Legyen $v_0, v \in V$ két tetszőleges csúcs. Ekkor a regularitás miatt egyértelműen létezik egy $\phi_v \in G_0$, amelyre $\phi_v(v_0) = v$. Legyenek a v_0 szomszédai $v_1, ..., v_n$, és tekintsük az $S = \{\phi_{v_1}, ..., \phi_{v_n}\} \subset G_0$ részhalmazt. A priori nem tudjuk, hogy az S generátorrendszere lenne a G_0-nak, de ez most nem fontos, a bizonyítás későbbi szakaszából automatikusan fog következni. Tekintsük a $\Gamma_0 = \mathrm{Cay}(G_0, S)$ Cayley-gráfot és defininiáljuk a

$$\Gamma_0 \xrightarrow{\epsilon} \Gamma$$
$$\phi_v \xrightarrow{\epsilon} v$$

leképezést. Belátjuk, hogy ϵ gráfizomorfizmus. Jelölje E_0 a Γ_0 élhalmazát.

Bijekció: a bijekció a hatás regularitásából adódik.

Gráfhomomorfizmus: legyen $\{\phi_v, \phi_v\phi_{v_i}\} \in E_0$ tetszőleges él, ahol $\phi_v \in G_0$ és $\phi_{v_i} \in S$. Ekkor $\epsilon(\{\phi_v, \phi_v\phi_{v_i}\}) = \{\phi_v(v_0), \phi_v(v_i)\} \in E$, hiszen $\{v_0, v_i\} \in E$ és $\phi_v \in \mathrm{Aut}(\Gamma)$, tehát ϵ gráfhomomorfizmus. Az ϵ^{-1} is gráfhomomorfizmus: ha $\{v, w\} \in E$ tetszőleges él, akkor $\phi_v^{-1}(\{v, w\}) = \{v_0, \phi_v^{-1}(w)\} \in E$, tehát $\phi_v^{-1}(w) = v_i = \phi_{v_i}(v_0)$ valamely $1 \leq i \leq n$ esetén. Következésképpen $\epsilon^{-1}(\{v, w\}) = \{\phi_v, \phi_v\phi_{v_i}\} \in E_0$.

Ezzel tehát beláttuk, hogy Γ izomorf a Γ_0 Cayley-gráffal, ahonnan az is következik, hogy Γ_0 összefüggő, vagyis S generátorrendszere a G_0 csoportnak. □

2 Cayley-gráfok átmérője és a Babai-sejtés

Az eddigiek alapján láttuk, hogy a Cayley-gráfok nagyon erős szimmetriatulajdonságokkal rendelkeznek. Most „metrikus” szempontból szeretnénk ezeket a gráfokat, és ennek megfelelően a csoport struktúráját vizsgálni, amit az átmérő fogalmán keresztül fogunk megtenni. Ahogyan azt a bevezetőben is említettük, a Rubik-kocka bármilyen pozícióból legfennebb 26 forgatással kirakható, ami éppen a Rubik-kocka csoportjához tartozó Cayley-gráf átmérője. CPU hálózatok tervezéséhez is központi szerepet töltenek be a Cayley-gráfok, ahol fontos, hogy az egyes CPU-k ne legyenek túl távol egymástól, vagyis bármely két számítógép közötti információcsere során csak kevés közbülső számítógépen kelljen áthaladnia az információnak, tehát lényeges, hogy a választott Cayley-gráf átmérője kicsi legyen.

Ezen fejezetben a Cayley-gráfok átmérőjével kapcsolatos eredményeket mutatunk be. Bizonyítjuk Babai és Seress 1987-ben publikált eredményét (lásd [BaSe87]), ami felső korlátot ad az S_n szimmetrikus- és A_n alternáló csoportok átmérőjére. Kitérünk a Babai-sejtésre és bizonyítás nélkül ismertetjük a sejtéshez kapcsolódó jelenleg ismert legjobb felső korlátokat.

2.1. Cayley-gráfok átmérője

A továbbiakban feltesszük, hogy G véges csoport. Előbb bevezetjük az átmérő fogalmát tetszőleges gráf esetén.

2.1. Definíció. Legyen $\Gamma = (V, E)$ egy tetszőleges gráf. Jelöljük a $v, w \in V$ csúcsok távolságát $d(v, w)$-vel. Ekkor a Γ gráf *átmérője* a csúcsok távolságainak maximuma, vagyis

$$\operatorname{diam}(\Gamma) := \max_{v,w \in V} d(v, w).$$

Hasonló módon definiálható az átmérő digráfok esetén is.

2.2. Példa. Könnyen látható, hogy az n csúcsú körgráf átmérője $\left\lfloor \frac{n}{2} \right\rfloor$, az n csúcsú teljes gráf átmérője 1, illetve a Petersen-gráf átmérője 2.

Ha $\Gamma = \mathrm{Cay}(G, S)$ egy Cayley-gráf, akkor értelemszerűen az átmérő függ az S generátorrendszertől. Például míg a $G = S_3$ és $S = \{(1,2), (1,2,3)\}$ esetén 2 az átmérő, addig az $S' = \{(1,2), (2,3)\}$ generátorrendszer esetén az átmérő 3 lesz (lásd az 1.1-es ábrát).

Ahogyan azt a Rubik-kocka példája is sejteti, az átmérő szoros kapcsolatban áll a csoport struktúrájával. Hogy ezt precízen megfogalmazhassuk, szükségünk lesz a következő két definícióra.

2.3. Definíció. Legyen G egy csoport és S egy generátorrendszer. A $g \in G$ elem S szerinti *hossza* az a legkisebb d pozitív egész szám, amelyre g előáll d darab $S \cup S^{-1}$-beli elemek szorzataként. Jelöljük ezt a számot $\mathrm{length}(g, S)$-el.

2.4. Definíció. Legyen G egy csoport és S egy generátorrendszer. A G csoport S szerinti *átmérője* a csoportelemek S szerinti hosszainak a maximuma, azaz

$$\mathrm{diam}(G, S) = \max_{g \in G} \mathrm{length}(g, S)$$

Az alábbi egyszerű állítás teremt kapcsolatot a két átmérő között.

2.5. Állítás. *Legyen G egy csoport S generátorrendszerrel, és legyen $\Gamma = Cay(G, S)$ a megfelelő Cayley-gráf. Ekkor $diam(\Gamma) = diam(G, S)$, vagyis a Cayley-gráf átmérője az a legkisebb k pozitív egész szám, amelyre minden csoportbeli elem előáll legfennebb k darab $S \cup S^{-1}$-beli elem szorzataként.*

Bizonyítás. A definíciókból könnyen adódik, hogy az $S \cup S^{-1}$-feletti szavak a Cayley-gráfban utaknak felelnek meg és fordítva, ahol a szó hossza az út hosszával egyezik meg. Ez alapján, ha g és h két tetszőleges elem, akkor

$$d(g, h) = \mathrm{length}\left(g^{-1}h, S\right),$$

ahonnan a

$$\mathrm{diam}(\Gamma) = \max_{g,h \in G} d(g, h) = \max_{l \in G} \mathrm{length}(l, S) = \mathrm{diam}(G, S)$$

egyenlőség adódi, ahol $l = g^{-1}h$. □

Hasonlóan egy $T \subset G$ részhalmaz S-feletti hossza is definiálható, nevezetesen legyen

$$\mathrm{length}(T, S) = \max_{g \in T} \mathrm{length}(g, S).$$

A $d(g, h) = \mathrm{length}(g^{-1}h, S)$ egyenlőségből, és a gráfelméleti háromszög-egyenlőtlenségből[1] egy nagyon hasznos egyenlőtlenség következik, amit többször is használni fogunk, neve-

[1] Gráfelméleti háromszög-egyenlőtlenség: ha x, y, z tetszőleges csúcsok egy Γ gráfban, akkor $d(x, z) \leq d(x, y) + d(y, z)$.

zetesen ha $g, h \in G$, akkor

$$\text{length}(gh, S) \leq \text{length}(g, S) + \text{length}(h, S)\,.$$

Az is könnyen adódik, hogy ha S és T két különböző generátorrendszere a G csoportnak, akkor

$$\text{diam}\,(G, S) \leq \text{diam}\,(G, T) \cdot \text{length}\,(T, S)\,.$$

Egy csoport *átmérője* legyen a $\text{diam}(G, S)$ S-feletti átmérők maximuma, amikor S végigfutja a generátorrendszerek halmazát, és jelöljük ezt $\text{diam}(G)$-vel. Természetesen tevődik fel a kérdés, hogy mennyire nehéz egy Cayley-gráf átmérőjének a meghatározása. Even és Goldreich 1981-es publikációjukban (lásd [EvGo81]) belátták, hogy egy Cayley-gráf átmérőjének kiszámítása NP-nehéz probléma, ezért általában nem a tényleges átmérő meghatározása lesz a cél, hanem annak a vizsgálata, hogy milyen alsó, és felső korlátok adhatók, illetve ezek mennyire esnek távol egymástól. Továbbá az is érdekes kérdés, hogy adott típusú csoportok (lásd később a Babai-sejtést) átmérőjére adható-e valamilyen „egységes” felső korlát?

Triviális felső korlátot ad az átmérőre a csoport elemszáma. Mostantól log az e-alapú logaritmust jelöli. Egy lehetséges alsó korlát csoporttól és generátorrendszertől függetlenül $\frac{\log|G|}{\log(2|S|)}$ nagyságrendű. Legyen ugyanis $\Gamma = \text{Cay}(G, S)$ Cayley-gráf és tételezzük fel, hogy $\text{diam}(\Gamma) = d$, valamint legyen $t := 2\,|S|$. Jelöljük $B\,(e, r)$-el az e körüli r sugarú gömböt, vagyis azon csúcsok halmazát, amelyek legfennebb r távolságra vannak az egységelemtől (másképp: legfennebb r darab $S \cup S^{-1}$-beli elem szorzataként állnak elő). Ekkor könnyen adódik, hogy

$$\begin{aligned}
|B\,(e, 1)| &\leq t + 1 \\
|B\,(e, 2)| &\leq t^2 + t + 1 \\
&\vdots \\
|B\,(e, r)| &\leq t^r + t^{r-1} + \ldots + 1.
\end{aligned}$$

A $|B\,(e, r)|$-et tovább becsülhetjük, nevezetesen

$$\begin{aligned}
|B\,(e, r)| &\leq t^r + t^{r-1} + \ldots + 1 \\
&= t^r + \frac{t^r - 1}{t - 1} \\
&\leq t^r + t^r - 1 \\
&< 2t^r.
\end{aligned}$$

Mivel a gráf átmérője d, ezért szükségképpen $|G| = |B\,(e, d)| < 2t^d$, ahonnan logaritmálással adódik a kívánt alsó korlát d-re.

A következő állításban megmutatjuk, hogy ha S speciális tulajdonságú, akkor a Cayley-gráf átmérője kicsi.

2.6. Állítás. *Ha H valódi részcsoport G-ben és $S := G \setminus H$, akkor*

$$diam(\Gamma) = \begin{cases} 1 & ha\ H = \{1\} \\ 2 & ha\ H \neq \{1\} \end{cases}.$$

Bizonyítás. Ha $H = \{1\}$, akkor a Γ Cayley-gráf nem más, mint a $K_{|G|}$ teljes gráf, aminek nyilván 1 az átmérője.

Tegyük fel, hogy $H \neq \{1\}$ és vegyünk két tetszőleges $g_1, g_2 \in G \setminus H$ elemet. Mivel az 1 egységelem szomszédai éppen az $S \cup S^{-1}$ elemek, ezért az g_1 és g_2 is szomszédos 1-el, tehát $d(g_1, g_2) \leq 2$. Ha $g_1 \in H$ és $g_2 \notin H$, akkor szomszédosak a Cayley-gráfban, hiszen $g_2^{-1} g_1 \in G \setminus H$, és így $g_1 = g_2 g_2^{-1} g_1$, tehát $d(g_1, g_2) = 1$. Végül ha $g_1, g_2 \in H$ (ez lehetséges, mivel feltétel szerint $|H| \geq 2$) és $s \in G \setminus H$, akkor $s^{-1} g_1, s^{-1} g_2 \in G \setminus H$, ahonnan következik, hogy s szomszédos g_1-el és g_2-vel is (hiszen $g_{1,2} = s s^{-1} g_{1,2}$). Továbbá g_1 és g_2 nem szomszédosak egymással, mert $g_1^{-1} g_2$ és $g_2^{-1} g_1$ H-beli elemek, tehát $d(g_1, g_2) = 2$. Ezzel beláttuk, hogy a Cayley-gráf átmérője 2. □

2.2. Példa számolások az S_n és A_n csoportok esetén

Mielőtt rátérnénk Babai és Seress eredményére, az S_n szimmetrikus-, illetve az A_n alternáló csoportokon mutatunk be különböző technikákat az átmérő számolására, becslésére. A permutációk szorzása konvenció szerint jobbról balra történik.

2.7. Állítás. *Tekintsük S_n-nek az $S = \{(1,2), (1,2,...,n)\}$ generátorrendszerét. Ekkor*

$$diam(S_n, S) = O\left(n^2\right).$$

Bizonyítás. Legyen (a, b) egy tetszőleges transzpozíció, ahol $a < b$, és legyen $\pi = (1,2)$ valamint $\sigma = (1,2,...,n)$. Mivel $a < b$, ezért $b = a + k$, valamilyen k pozitív egészre. Konjugáljuk meg π-t $\sigma^{a-1}(\pi\sigma)^{k-1}$-el, jelöljük ezt $\pi^{\sigma^{a-1}(\pi\sigma)^{k-1}}$-el. Ekkor

$$1 \xrightarrow{(\pi\sigma)^{k-1}} 1 \xrightarrow{\sigma^{a-1}} a$$
$$2 \xrightarrow{(\pi\sigma)^{k-1}} k+1 \xrightarrow{\sigma^{a-1}} a+k = b.$$

Továbbá tudjuk, hogy a konjugálás megőrzi a ciklusstruktúrát, tehát a $\pi^{\sigma^{a-1}(\pi\sigma)^{k-1}}$ is egy transzpozíció kell legyen. A számolás mutatja, hogy $\pi^{\sigma^{a-1}(\pi\sigma)^{k-1}} = (ab)$. Ezzel egy becslés

adható tetszőleges transzpozíció S-fölötti hosszára, ugyanis

$$\begin{aligned}\text{length}\left(\pi^{\sigma^{a-1}(\pi\sigma)^{k-1}}, S\right) &\leq 2 \cdot \text{length}\left(\sigma^{a-1}(\pi\sigma)^{k-1}, S\right) + \text{length}(\pi, S)\\ &\leq 2 \cdot (a - 1 + 2(k-1)) + 1\\ &\leq 2 \cdot (2n + n) + 1\\ &= 6n + 1.\end{aligned}$$

Legyen most $\rho \in S_n$ tetszőleges permutáció. Mivel ρ felírható maximum $n-1$ transzpozíció szorzataként, ezért

$$\text{length}(\rho, S) \leq (n-1) \cdot (6n+1) = O\left(n^2\right),$$

ahonnan adódik, hogy $\text{diam}(S_n, S) = O(n^2)$. □

A következő állítást kétféleképpen fogjuk bizonyítani.

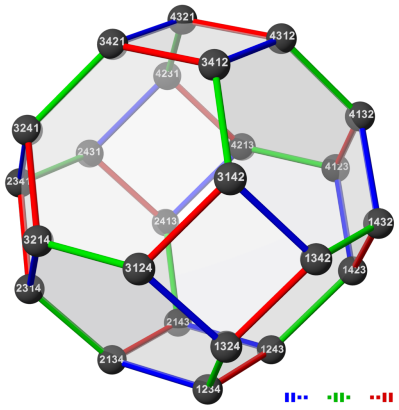
2.8. Állítás. *Tekintsük S_n-nek az $S = \{(1,2), (2,3), ..., (n-1,n)\}$ generátorrendszerét. Ekkor*

$$diam(\Gamma) = \binom{n}{2}.$$

Bizonyítás. 1. Az első bizonyítás tisztán az S_n csoport tulajdonságait használja. Legyen $\sigma \in S_n$ tetszőleges permutáció. Jelöljük az inverziók számát[2] $\lambda(\sigma)$-val. Az egyszerűség kedvéért az $(i, i+1)$ transzpozíciót jelöljük s_i-vel. Vegyük észre, hogy a $\lambda(\sigma)$ éppen a σ S-fölötti hossza. Valóban, ha σ nem az egységelem, akkor van olyan i, hogy $\sigma(i+1) < \sigma(i)$ és az s_i elemmel való szorzás 1-el csökkenti a $\lambda(\sigma)$-t. Folytatva ezt az eljárást σ-ból előáll az egységelem $\lambda(\sigma)$ darab szorzás után. Ebből adódik az állítás, hiszen egy tetszőleges permutációban maximum $\binom{n}{2}$ inverzió lehet.

A $\text{Cay}(S_n, S)$ gráf egy szép, szimmetrikus politóp 1-vaza, amit *n-edfokú permutaéder*nek is szokás nevezni. Ez lényegében azon n-dimenziós pontok konvex burka, amelyek koordinátái az $\{1, 2, ..., n\}$ halmaz permutációival egyeznek meg. Innen azonnal adódik, hogy a permutaéder az n-dimenziós térbe beágyazott $(n-1)$-dimenziós politóp, ugyanis a koordináták összege minden csúcs esetében $1 + 2 + ... + n = \frac{n(n+1)}{2}$, vagyis minden csúcs benne van az $x_1 + x_2 + ... + x_n = \frac{n(n+1)}{2}$ egyenletű hipersíkban. Két csúcs között pontosan akkor halad él, ha azok koordinátasora két szomszédos koordináta felcserélésében különbözik ($n = 4$-re ez a politóp a 2.1-es ábrán látható). A bizonyított állítás geometriailag azt jelenti, hogy ha a permutaéderben az élek mentén akarunk eljutni az egyik csúcsból a másikba, akkor azt legfeljebb $\frac{n(n-1)}{2}$ élen keresztül megtehetjük.

[2] Azon (i, j) párok száma, amelyekre $i < j$ és $\sigma(i) > \sigma(j)$.



2.1. ábra. Negyedfokú permutaéder

2. A második bizonyítás a Lie-algebrák elméletében felbukkanó Weyl-csoportok segítségével történik. Az elmélet részletes leírása nem célja ezen szakdolgozatnak, a fogalmak és eredmények részletes leírása megtalálható például James E. Humphreys *Introduction to Lie Algebras and Representations Theory* című könyvében [Hu72].

Gyökrendszer: legyen E egy valós euklideszi tér, $(\cdot,\cdot)$ skaláris szorzattal. Az $\alpha \in E$ nemnulla vektorra merőleges P_α hipersíkra való tükrözést jelöljük w_α-val. Ez tetszőleges α-ra merőleges β vektorhoz a β-t rendeli, míg az α-t a $-\alpha$-ba küldi. Nem nehéz belátni, hogy

$$w_\alpha(\beta) = \beta - \frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha, \quad \text{minden } \beta \in E\text{-re.}$$

Legyen $\Phi \subset E$ véges részhalmaz. Φ-t *gyökrendszer*nek nevezzük, ha teljesíti az alábbi feltételeket:

- Φ generálja E-t, $0 \notin \Phi$ és ha $\alpha \in \Phi$, akkor $c\alpha \in \Phi$ pontosan akkor, ha $\alpha = \pm 1$;
- ha $\alpha \in \Phi$, akkor a w_α tükrözés Φ-t saját magába viszi;
- $\frac{2(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$ minden $\alpha, \beta \in \Phi$-re.

A $\Phi \subset E$ gyökrendszerhez tartozó *Weyl-csoport* a w_α, $\alpha \in \Phi$ tükrözések által generált részcsoport az E általános lineáris csoportjában, vagyis

$$W = W(\Phi) := \langle w_\alpha : \alpha \in \Phi \rangle \leq GL(E).$$

Bizonyítható, hogy W véges csoport. Azt mondjuk, hogy $\prod \subset \Phi$ *fundamentális gyökrendszer*e Φ-nek, ha $\prod$ bázisa E-nek és minden $\beta \in \Phi$ gyökre

$$\beta = \sum_{\alpha \in \prod} k_\alpha \cdot \alpha,$$

ahol $k_\alpha \in \mathbb{Z}$ és vagy minden $k_\alpha \geq 0$, vagy minden $k_\alpha \leq 0$. Minden $\Phi \subset E$ gyökrendszer tartalmaz fundamentális rendszert, és egy fundamentális rendszer megad egy $\Phi = \Phi^+ \cup$

Φ^{-1} felbontást, ahol

$$\Phi^+ = \left\{ \beta = \sum_{\alpha \in \prod} k_\alpha \cdot \alpha : k_\alpha \geq 0, \text{ minden } \alpha \in \prod \right\},$$
$$\Phi^- = \left\{ \beta = \sum_{\alpha \in \prod} k_\alpha \cdot \alpha : k_\alpha \leq 0, \text{ minden } \alpha \in \prod \right\}.$$

A Φ^+ elemeit *pozitív gyökök*nek, míg a Φ^- elemeit *negatív gyökök*nek nevezzük. Nyilvánvaló, hogy $-\Phi^+ = \Phi^-$, tehát a negatív és pozitív gyökök száma megegyezik. A Φ-hez tartozó Weyl-csoportot már az ún. *fundamentális tükrözés*ek is generálják, vagyis azok a w_α elemek, amelyekre $\alpha \in \prod$. Tetszőleges $g \in W$ Weyl-csoportbeli elem előáll $g = w_{\alpha_1} w_{\alpha_2} \cdots w_{\alpha_t}$ alakban, ahol $\alpha_1, ..., \alpha_t$ fundamentális gyökök. A g *hossza* $l(g) = t$, ha t a legkisebb olyan pozitív egész, melyre g előáll $g = w_{\alpha_1} w_{\alpha_2} \cdots w_{\alpha_t}$ alakban, ahol $\alpha_1, ..., \alpha_t$ fundamentális gyökök. Egy $g \in W$-re legyen $n(g) := |\Phi^+ \cap g^{-1}(\Phi^-)|$, azaz $n(g)$ azon pozitív gyökök száma, melyeket g negatív gyökbe képez. Belátható, hogy minden $g \in W$-re $l(g) = n(g)$.

Legyen $E = \{(a_1, ..., a_{n+1}) \in \mathbb{R}^{n+1} : \sum_i a_i = 0\} \leq \mathbb{R}^{n+1}$ egy n dimenziós euklideszi tér, ahol a skaláris szorzatot az $\mathbb{R}^{n+1}$-en vett természetes skaláris szorzás megszorításával nyerjük. Minden $1 \leq i \neq j \leq n+1$-re vegyük az $\alpha_{ij} = e_i - e_j = \left(0, ..., 0, \underset{i}{1}, 0, ..., 0, \underset{j}{-1}, 0, ..., 0\right)$ vektort és legyen $\Phi = \{\alpha_{ij} : i \neq j\} \subset E$, ami gyökrendszer E-ben és elemszáma $n(n+1)$. Egy α_{ij} esetén $P_{\alpha_{ij}} = \{(a_1, ..., a_{n+1}) : a_i = a_j\}$ és $w_{\alpha_{ij}}$ az i és j koordináták felcserélését eredményezi és az általuk generált Weyl-csoport S_{n+1}-el izomorf. Egy lehetséges fundamentális rendszere Φ-nek a $\prod = \{e_1 - e_2, e_2 - e_3, ..., e_n - e_{n+1}\}$ és ezekhez a vektorokhoz tartozó fundamentális tükrözések éppen azoknak a transzpozícióknak felelnek meg, amelyek a feltételben szerepelnek. Tehát az a $g \in W$ elem lesz a leghosszabb, amelyik az összes pozitív gyököt a negatívakba viszi, és a pozitív gyökök száma $\frac{n(n+1)}{2}$. Megismételve a gonolatmenetet $n+1$ helyett n-re adódik az állítás. □

Ismert, hogy az A_n alternáló csoportot generálják a 3-ciklusok. A megfelelő Cayley-gráf átmérőjére a következő felső becslés adható.

2.9. Állítás. *Legyen $S \subset A_n$ a 3-ciklusok halmaza. Ekkor $diam(A_n, S) \leq n$.*

Bizonyítás. Legyen $\pi \in A_n$ tetszőleges permutáció. Legyen $c = (i_1, ..., i_k)$ egy k-ciklus a π ciklusfelbontásában. Nyilván $c = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$. Ez alapján, ha k páros, akkor c páratlan számú transzpozíció szorzata, illetve páratlan k esetén c páros számú transzpozíció szorzataként áll elő.

Ha c foka páratlan, azaz $k = 2m+1$ alakú, akkor $c = \underbrace{(i_1 i_2 i_3)(i_3 i_4 i_5) \cdots (i_{k-4} i_{k-3} i_{k-2})(i_{k-2} i_{k-1} i_k)}_{m}$

alakban írható fel, amiből a

$$\text{length}\,(c,S) \leq m \leq \deg(c)$$

egyenlőtlenség adódik.

Ha c foka páros, vagyis $k = 2m$ alakú, akkor mivel π páros permutáció, szükséges, hogy páros sok páros fokú ciklust tartalmazzon a ciklusfelbontása, következésképpen c-hez választhatunk egy $c' = (j_1, ..., j_l)$ páros fokú ($l = 2q$) ciklust a π ciklusfelbontásából. Ekkor a cc' felírható $(j_1, i_k, j_2, ..., j_l)\,(i_1, ..., i_{k-1}, j_1, i_k)$ alakban, ahol a ciklusok fokai rendre $2m+1$ és $2q+1$. Innen a

$$\text{length}\,(cc', S) \leq m + q \leq \deg(c) + \deg(c')$$

becsléshez jutunk.

Tekintsük a $\pi = c_1 c_2 \cdots c_r$ ciklusfelbontást. Ekkor

$$\begin{aligned}\text{length}\,(\pi, S) &\leq \sum_{c,c' \text{ ps. hosszú ciklusok}} \text{length}\,(cc', S) + \sum_{c \text{ ptl. hosszú ciklus}} \text{length}\,(c, S) \\ &\leq \sum_{i=1}^{r} \deg(c_i, S) \leq n.\end{aligned}$$

□

2.3. Babai és Seress tételének bizonyítása

A továbbiakban olyan eredményeket fogunk bemutatni, amelyek mind a szimmetrikus-, mind pedig az alternáló csoport esetén érvényesek lesznek, ezért mostantól G jelölje az A_n vagy S_n csoportot.

Célunk a következő tétel bizonyítása, melyben a [Tan] cikkben bemutatott gondolatmenetet visszük végig.

2.10. Tétel. *(Babai-Seress, 1987) Legyen G az S_n vagy A_n csoportok valamelyike. Ekkor*

$$diam(G) \leq \exp\left(\sqrt{n \log n}\,(1 + o(1))\right).$$

Jelöljük a π permutáció *tartóját* $\text{supp}\,(\pi)$-vel, vagyis azon elemek halmazát, amelyeket a π mozgat. A π *foka* definíció szerint a tartójának az elemszáma, amit $\deg(\pi)$-vel jelölünk.

A bizonyításhoz előbb néhány segédtételt fogunk igazolni.

2.11. Definíció. A $T \subset G$ részhalmazt *k-tranzitív*nak $(1 \leq k \leq n)$ nevezzük, ha minden $(x_1, ..., x_k)$ és $(y_1, ..., y_k)$ (ahol $x_i \neq x_j$ és $y_i \neq y_j$ ha $i \neq j$) pár esetén létezik $\pi \in T$ permutáció, melyre $\pi(x_i) = y_i$.

Első segédtételünk a k-tranzitív részhalmazok S-feletti hosszára ad n-ben polinomiális felső korlátot.

2.12. Segédtétel. *Bármely $S \subset G$ generátorrendszerhez és tetszőleges $1 \leq k \leq n-2$ számhoz létezik egy $R_k \subset G$ k-tranzitív részhalmaz, melynek S-feletti hosszára teljesül a*

$$\mathit{length}\,(R_k, S) \leq n^k.$$

Bizonyítás. Jelöljük Ω_k-val az $\{1, 2, ..., n\}$ halmaz elemeiből alkotott összes k-hosszú vektort. Az S természetes módon hat az Ω_k elemein, mégpedig egy vektort koordinátánként permutál. Tekintsük azt a Γ gráfot, aminek a V csúcshalmaza az Ω_k-val egyezik meg, és két vektor között pontosan akkor halad és, ha van olyan S-beli elem, ami az egyik vektort a másik vektorba képezi. Mivel S generálja G-t és G tranzitívan hat az Ω_k-n, ezért Γ összefüggő és bármely két csúcs távolsága maximum $|V|$ lehet. Továbbá

$$|V| = \frac{n!}{(n-k)!} = n\,(n-1)\cdots(n-k+1) \leq n^k,$$

amit bizonyítani kellett. □

A 2.12-es Segédtétel következménye, hogy a $\mathrm{diam}\,(G, S)$ átmérőre 3-ciklusok segítségével tudunk felső korlátot adni.

2.13. Segédtétel. *Legyen $S \subset G$ generátorrendszer és $\gamma \in G$ egy 3-ciklus. Ekkor*

$$\mathit{diam}\,(G, S) \leq 1 + 2n^4 + n \cdot \mathit{length}\,(\gamma, S)\,.$$

Bizonyítás. Bármely 3-ciklus előállítható a γ-ból konjugálással: vegyünk egy R_3 3-tranzitív részhalmazt, és az elemeivel konjugáljuk a γ-t. Ha $\pi \in A_n$ tetszőleges páros permutáció, akkor π legfeljebb n darab 3-ciklus szorzataként áll elő, tehát

$$\begin{aligned}\mathrm{length}\,(\pi, S) &\leq n \cdot (\mathrm{length}\,(R_3, S) + \mathrm{length}\,(\gamma, S) + \mathrm{length}\,(R_3, S)) \\ &\leq 2n^4 + n \cdot \mathrm{length}\,(\gamma, S)\,,\end{aligned}$$

ahol felhasználtuk a 2.12-es Segédtételt.

Legyen $\pi \in S_n$ páratlan permutáció. Mivel S generálja S_n-t, szükséges, hogy S tartalmazzon egy σ páratlan permutációt. Ekkor $\sigma^{-1}\pi$ páros permutáció, tehát a

$$\begin{aligned}\mathrm{length}\,(\pi, S) &= \mathrm{length}\left(\sigma\sigma^{-1}\pi, S\right) \\ &\leq \mathrm{length}\,(\sigma, S) + \mathrm{length}\left(\sigma^{-1}\pi, S\right) \\ &\leq 1 + 2n^4 + n \cdot \mathrm{length}\,(\gamma, S)\end{aligned}$$

egyenlőtlenség adódik. □

2.14. Segédtétel. *Legyenek σ és π olyan permutációk, melyekre $|supp(\sigma) \cap supp(\pi)| = 1$. Ekkor a $[\sigma, \pi] = \sigma\pi\sigma^{-1}\pi^{-1}$ kommutátor egy 3-ciklus.*

Bizonyítás. Legyen $x \in \operatorname{supp}(\sigma) \cap \operatorname{supp}(\pi)$. Ekkor a

$$x \xrightarrow{\pi^{-1}} \pi^{-1}(x) \xrightarrow{\sigma^{-1}} \pi^{-1}(x) \xrightarrow{\pi} x \xrightarrow{\sigma} \sigma(x)$$
$$\sigma(x) \xrightarrow{\pi^{-1}} \sigma(x) \xrightarrow{\sigma^{-1}} x \xrightarrow{\pi} \pi(x) \xrightarrow{\sigma} \pi(x)$$
$$\pi(x) \xrightarrow{\pi^{-1}} x \xrightarrow{\sigma^{-1}} \sigma^{-1}(x) \xrightarrow{\pi} \sigma^{-1}(x) \xrightarrow{\sigma} x$$

számolásból és abból, hogy a kommutátor az $x, \sigma(x)$ és $\pi(x)$ elemeken kívül minden mást helyben hagy, következik, hogy $[\sigma, \pi] = (x, \sigma(x), \pi(x))$. □

Egy $x \in \operatorname{supp}(\pi)$ elem π *szerinti periódusá*nak nevezzük azt a legkisebb pozitív egész m számot, melyre $\pi^m(x) = x$. Jelöljük a periódust $\operatorname{period}(x)$-szel. Vezessük be az $\{1, 2, ..., n\} =: [n]$ jelölést.

A következő két segédtétel fogja képezni a 2.10-es Tétel bizonyításának alapját.

2.15. Segédtétel. *Legyen π egy olyan permutáció, hogy a $p_1, ..., p_k$ páronként különböző prímek osztják a π rendjét és $\prod_{i=1}^{k} p_i \geq n^s$, valamilyen s pozitív egész számra. Ekkor létezik egy m pozitív egész, melyre $2 \leq \deg(\pi^m) \leq \frac{n}{s}$.*

Bizonyítás. Tekintsük az $\operatorname{ord}(\pi) = \prod_{i=1}^{k} p_i^{r_i} \cdot L$ felírást, ahol $\gcd(L, p_i) = 1$, továbbá definiáljuk minden p_i prímhez az $l_i = \frac{\operatorname{ord}(\pi)}{p_i^{r_i}}$ számot. Megmutatjuk, hogy az m valamelyik l_i-vel egyezik meg.

Mivel minden permutáció diszjunkt ciklusok szorzatára bontható, ezért könnyen látható, hogy tetszőleges $x \in [n]$ elem periódusa éppen π azon ciklusának a hossza, amelyik az x-et mozgatja. Legyen $A(x) = \{i : p_i \mid \operatorname{period}(x)\}$. Az $A(x)$-ben szereplő indexekhez tartozó prímek osztják az x-et mozgató ciklus hosszát, és mivel a ciklus hossza maximum n lehet, a

$$\prod_{i \in A(x)} p_i \leq n$$

egyenlőtlenség adódik, minden $x \in [n]$-re.

Ha $\pi^{l_i}(x) = x$, akkor $\operatorname{period}(x) \mid l_i$, így $p_i \nmid \operatorname{period}(x)$, tehát $i \notin A(x)$. Továbbá a $\deg(\pi^{l_i})$ definíció szerint a π^{l_i} által mozgatott elemek számával egyezik meg, ami az előző következtetés alapján azon $x \in [n]$ elemek számával egyenlő, amikre $i \in A(x)$. Legyen ez a szám N_i.

Legyen $R(i, x)$ az „$i \in A(x)$” reláció indikátorfüggvénye. Ezen jelölés alapján

$$\sum_{x \in [n]} R(i, x) = N_i.$$

A $\prod_{i\in A(x)} p_i \leq n$ egyenlőtlenséget logaritmálva a

$$\sum_{i\in[k]} R(i,x)\log p_i = \sum_{i\in A(x)} \log p_i \leq \log n$$

egyenlőtlenséghez jutunk. Emlékezzünk, hogy feltettük, hogy $\prod_{i=1}^{k} p_i \geq n^s$, vagyis

$$\sum_{i=1}^{k} \log p_i \geq s\log n.$$

Az N_i értékek $\log p_i$ súlyokkal vett súlyozott átlagára a következő felső becslés adható:

$$\begin{aligned}\frac{\sum_{i=1}^{k} N_i \log p_i}{\sum_{i=1}^{k}\log p_i} &= \frac{\sum_{i=1}^{k}\sum_{x\in[n]} R(i,x)\log p_i}{\sum_{i=1}^{k}\log p_i}\\ &= \frac{\sum_{x\in[n]}\left(\sum_{i=1}^{k} R(i,x)\log p_i\right)}{\sum_{i=1}^{k}\log p_i}\\ &\leq \frac{\sum_{x\in[n]}\log n}{s\log n}\\ &= \frac{n\log n}{s\log n} = \frac{n}{s}.\end{aligned}$$

Innen következik, hogy létezik olyan N_i, ami kisebb vagy egyenlő, mint $\frac{n}{s}$. □

2.16. Segédtétel. *Legyen $S \subset G$ generátorrendszer és $\pi \in G$ egy tetszőleges permutáció, melyre $\deg(\pi) = k \geq 2$. Legyen $d \in \mathbb{N}$ olyan, hogy $d \leq \frac{k}{3}$ és $d = d_1 + ... + d_r$, ahol $d_i \in \mathbb{N}$. Ekkor létezik $\lambda \in G$ permutáció, melyre*

1. $\deg(\lambda) \leq 2k$;
2. *λ tartalmaz $d_1, ..., d_r$ hosszú ciklusokat;*
3. *$length(\lambda, S) \leq 2 \cdot length(\pi, S) + 2 \cdot length(R_{2d}, S)$, ahol $R_{2d} \subset G$ egy $2d$-tranzitív részhalmaz.*

Bizonyítás. Legyen $B \subset \mathrm{supp}(\pi)$ olyan részhalmaz, melynek elemszáma d és $B \cap \pi(B) = \emptyset$ (ilyen B nyilván választható). Mivel R_{2d} $2d$-tranzitív részhalmaz, ezért választható olyan $\sigma \in R_{2d}$ permutáció, amelyre $\sigma|_B$ d_i hosszú ciklusok szorzata, és σ fixen hagyja a $\pi(B)$ elemeit.

Legyen $\lambda = \sigma^{-1}\pi^{-1}\sigma\pi$. Nyilvánvaló, hogy két permutáció szorzatának a foka maximum a szorzatban szereplő permutációk fokának az összege lehet. Továbbá $\sigma^{-1}\pi^{-1}\sigma$ foka megegyezik a π fokával, hiszen konjugáltak, tehát ugyanolyan típusú ciklusfelbontásuk van. Ekkor

$$\deg(\lambda) \leq \deg\left(\sigma^{-1}\pi^{-1}\sigma\right) + \deg(\pi) = 2k.$$

A 2-es és 3-as tulajdonságok nyilvánvalóak, mivel $\lambda|_B = \sigma^{-1}|_B$. □

Az $f, g : \mathbb{N} \to \mathbb{R}$ függvények esetén bevezetjük az $f \sim g$ jelölést, amely alatt az értendő, hogy $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$. A definícióból egyszerűen adódik, hogy ha $f(n) \sim g(n)$, akkor $f(n) = g(n)(1 + o(1))$. Ha $f(n) \leq g(n) \sim h(n)$, akkor azt $f(n) \lesssim h(n)$ módon fogjuk jelölni.

Most már minden kellék a rendelkezésünkre áll a 2.10-es Tétel bizonyításához.

A 2.10-es Tétel bizonyítása. Legyen $S \subset G$ tetszőleges véges generátorrendszer. Definiáljuk a

$$\phi(n,s) = \min\left\{k : \prod_{i=1}^{k} p_i > n^s\right\},$$
$$\psi(n,s) = \sum_{i=1}^{\phi(n,s)} p_i,$$

ahol p_i az i-edik prímet jelöli. Legyen $s = \log n$. Ekkor $\phi(n, 2s) \sim \frac{(\log n)^2}{\log\log n}$ a prímszámtétel[3] alapján, és $\psi(n, 2s) \sim \frac{2(\log n)^4}{\log\log n}$, amely Riemann-Stieltjes integrálással számolható ki. Legyen $t = 3 \cdot \psi(n, 2s)$. Tetszőleges t-edfokú $\sigma \in G$ permutációhoz létezik olyan $\rho \in R_t$ t-tranzitív permutáció, melyre $|\mathrm{supp}(\sigma) \cap \mathrm{supp}(\rho)| = 1$. A 2.14-es Segédtétel alapján a $[\sigma, \rho]$ kommutátor egy 3-ciklus, tehát

$$\begin{aligned}\mathrm{length}([\sigma,\rho], S) &\leq 2 \cdot \mathrm{length}(\sigma, S) + 2 \cdot \mathrm{length}(R_t, S)\\ &\leq 3 \cdot \mathrm{length}(\sigma, S) \cdot \mathrm{length}(R_t, S)\\ &\leq 3n^t \cdot \mathrm{length}(\sigma, S),\end{aligned}$$

ahol az utolsó becslésnél a 2.12-es Segédtételt használtuk fel.

Induljunk ki egy tetszőleges $\pi \in G$ permutációból. Alkalmazzuk π-re a 2.15-ös és 2.16-os Segédtételeket, és tegyük fel, hogy a j-edik lépésben a $\pi_j \in G$ permutációt állítottuk elő, amelynek foka $m > t$. π_j-re alkalmazva a 2.16-os Segédtételt $d = \psi(n, 2s)$ és $d_i = p_i$-re, egy olyan $\pi'_j \in G$ elemhez jutunk, aminek a foka legfeljebb $2m$. π'_j-re alkalmazható a 2.15-ös Segédtétel, ami egy $\pi_{j+1} \in G$ elemet eredményez $\deg(\pi_{j+1}) < \frac{2m}{2s} = \frac{m}{s}$ fokkal. A 2.12-es és 2.16-os Segédtételek alapján

$$\begin{aligned}\mathrm{length}(\pi'_j, S) &\leq 2 \cdot (\mathrm{length}(\pi_j, S) + \mathrm{length}(R_{2d}, S))\\ &\leq 2 \cdot \mathrm{length}(\pi_j, S) + 2n^{2d}\\ &\leq 2n^t \cdot \mathrm{length}(\pi_j, S).\end{aligned}$$

[3] Jelölje $\pi(x)$ az x-nél kisebb prímszámok számát. A prímszámtétel szerint $\pi(x) \sim \frac{x}{\log x}$.

Legyen $g : \mathbb{N} \to \mathbb{N}$ az ún. *Landau-függvény*, amely minden $n \in \mathbb{N}$-hez hozzárendeli az S_n legnagyobb rendű elemét. Landu bizonyította [La09]-ben, hogy

$$g(n) \sim e^{\sqrt{n \log n}(1+o(1))}.$$

Ennek segítségével becsülni tudjuk a π_{j+1} S-feletti hosszát:

$$\begin{aligned} \operatorname{length}(\pi_{j+1}, S) &\leq \operatorname{length}\left(\pi_{j+1}, \pi_j'\right) \cdot \operatorname{length}\left(\pi_j', S\right) \\ &\leq g(m) \cdot 2n^t \cdot \operatorname{length}(\pi_j, S) \end{aligned}$$

Tegyük fel, hogy a fenti eljárásban l lépés után jutunk el egy legfennebb t-edfokú permutációhoz. Mivel minden lépésben $s = \log n$-ed részére csökken a permutáció foka, ezért a

$$\begin{aligned} \frac{n}{(\log n)^l} \leq t \sim \frac{6(\log n)^4}{\log\log n} &\iff \\ (\log n)^l \gtrsim \frac{n \log\log n}{6(\log n)^4} &\iff \\ l \gtrsim \log\left(\frac{n\log\log n}{6(\log n)^4}\right) \cdot \frac{1}{\log\log n} & \\ = (\log n + \log\log\log n - \log 6 - 4\log\log n - \log\log n) \cdot \frac{1}{\log\log n} & \\ \sim \frac{\log n}{\log\log n} & \end{aligned}$$

becslés adható l-re. Legyen tehát $l \sim \log n$. Ekkor

$$\begin{aligned} \operatorname{length}(\pi_l, S) &\leq g(n)\, g\left(\frac{n}{s}\right) \cdots g\left(\frac{n}{s^l}\right) \cdot \left(2n^t\right)^l \\ &= \left(\prod_{i=0}^{l} e^{\sqrt{\frac{n}{(\log n)^i} \cdot \log\left(\frac{n}{(\log n)^i}\right)}(1+o(1))}\right) \cdot \left(2n^t\right)^l, \end{aligned}$$

amelyet ha logaritmálunk, akkor a

$$\begin{aligned}\log \operatorname{length}(\pi_l, S) &\lesssim \sum_{i=0}^{\log n} \sqrt{\frac{n}{(\log n)^i} \cdot \log\left(\frac{n}{(\log n)^i}\right)} + \log 2 \log n + \frac{6(\log n)^6}{\log\log n} \\ &\sim \sum_{i=0}^{\log n} \sqrt{\frac{n}{(\log n)^i} \cdot \log\left(\frac{n}{(\log n)^i}\right)} \\ &\leq \sqrt{n \log n} + \sqrt{\frac{n}{\log n} \log\left(\frac{n}{\log n}\right)} + \sqrt{\frac{n}{(\log n)^2} \log\left(\frac{n}{(\log n)^2}\right)} \\ &+ \log n \cdot \sqrt{\frac{n}{(\log n)^3} \log\left(\frac{n}{(\log n)^3}\right)} \\ &\sim \sqrt{n \log n}\end{aligned}$$

becsléshez jutunk, ahonnan a

$$\operatorname{length}(\pi_l, S) \leq e^{\sqrt{n \log n}(1+o(1))}$$

egyenlőtlenség következik. Végül a 2.13-as és 2.14-es Segédtételekből következik a

$$\operatorname{diam}(G, S) \leq e^{\sqrt{n \log n}(1+o(1))}$$

becslés. □

2.4. A Babai-sejtés

A sejtést Babai és Seress (lásd a [BaSe87]-es cikket) fogalmazták meg 1987-ben, mely szerint minden nemkommutatív véges egyszerű G csoport esetén létezik olyan abszolút $c > 0$ konstans, melyre

$$\operatorname{diam}(G) < (\log |G|)^c,$$

vagyis a csoport átmérőjére $\log |G|$-ben polinomiális felső korlát adható. Ekvivalens módon

$$\operatorname{diam}(\operatorname{Cay}(G, S)) < (\log |G|)^c,$$

minden $S \subset G$ generátorrendszerre. Megyjegyzendő, hogy ha a sejtés igaz Cayley-gráfokra, akkor igaz a Cayley-digráfokra is (más c konstanssal), hiszen Babai bizonyította a [Ba06]-ban, hogy

$$\operatorname{diam}\left(\vec{\operatorname{Cay}}(G, S)\right) \leq O\left(\operatorname{diam}(\operatorname{Cay}(G, S))^2 (\log |G|)^3\right),$$

ahol $\vec{\operatorname{Cay}}(G, S)$ a Cayley-digráfot jelöli.

Emlékezzünk vissza, hogy minden G csoport és S generátorrendszer esetén a $\frac{\log|G|}{\log(2|S|)}$ alsó korlátot adott. A sejtés lényegében azt mondja ki, hogy a nemkommutatív véges egyszerű csoportok esetén a felső korlát nagyságrendileg nem sokkal nagyobb, mint a $\frac{\log|G|}{\log(2|S|)}$ alsó korlát (mindkettő $\log|G|$-ben polinomiális). Kommutatív csoportok esetén a felső korlát nagyságrendekkel nagyobb lehet, mint $(\log|G|)^c$, nevezetesen ha $|G| = n$, $|S| = s$ és $\Gamma = \mathrm{Cay}(G, S)$ akkor

$$\mathrm{diam}(\Gamma) > \frac{s}{2e} n^{1/s} - s,$$

ahol e az Euler-féle szám. Valóban, ha a Γ átmérője d és $S = \{x_1, ..., x_s\}$, akkor a G minden eleme felírható $x_1^{k_1} \cdots x_s^{k_s}$ alakban, ahol $\sum_i |k_i| \leq d$, következésképpen

$$2^s \binom{d+s}{s} \geq n.$$

Továbbá

$$\begin{aligned} 2^s \binom{d+s}{s} &= 2^s \frac{(d+s)!}{s!d!} \\ &= 2^s \frac{(d+s)(d+s-1)\cdots(d+s-(s-1))\,d!}{s!d!} \\ &= 2^s \frac{(d+s)(d+s-1)\cdots(d+s-(s-1))}{s!} \\ &< 2^s \frac{(d+s)^s}{s!} < \left(\frac{2e(d+s)}{s}\right)^s, \end{aligned}$$

ahonnan átrendezéssel adódik az egyenlőtlenség.

A Babai-sejtés a mai napig egy nyitott kérdés, viszont számos részeredmény ismert a témában. Például Babai, Kantor és Lubotzky 1989-ben közölt cikkükben [BaKaLu89] belátták, hogy létezik olyan $c > 0$ konstans, mely esetén minden G nemkommutatív véges egyszerű csoportnak van olyan legfennebb hételemű S generátorrendszere, amire $\mathrm{Cay}(G, S)$ átmérője kisebb, mint $c \log|G|$.

A továbbiakban áttekintjük a témában elért eddigi eredményeket. A véges egyszerű csoportok klasszifikációja alapján az alternáló, a Lie-típusú véges egyszerű és a sporadikus csoportok tartoznak a sejtés körébe.

A sporadikus csoportok esete

Sporadikus csoportok esetén a sejtés triviálisan teljesül. Mivel csak véges sok sporadikus csoport van, szám szerint 27 (vagy 26 és a Tits-csoport) ezért van egy korlát a méretükre. De ekkor

$$\mathrm{diam}(G) < |G| < (\log|G|)^c,$$

alkalmasan választott $c > 0$ konstanssal. Így mindegyik sporadikus csoporthoz nyerünk egy konstanst, és ezeknek a maximuma megfelelő lesz.

Az alternáló csoport esete

Vegyük észre, hogy a sejtés egy jobb felső korlátot feltételez az alternáló csoport átmérőjére, mint amit a 2.10-es Tételben bizonyítottunk. Nevezetesen a sejtés teljesülése az A_n alternáló csoport esetén a

$$\operatorname{diam}(A_n) < n^c,$$

felső becslést jelentené, ahol $c > 0$ abszolút konstans.

Az A_n alternáló csoport átmérőjére a jelenleg ismert legjobb felső korlát $\log n$-ben kvázi-polinomiális[4], amelyet Helfgott és Seress bizonyítottak 2014-ben [HeSe14], nevezetesen ha $G = S_n$ vagy A_n, akkor

$$\operatorname{diam}(G) \leq \exp\left(O\left((\log n)^4 \log\log n\right)\right).$$

Babai és Seress a [BaSe92] cikkükben hasonló kvázi-polinomiális felső korlátot sejtettek tranzitív permutációcsoportokra, mégpedig ha G egy n-edfokú tranzitív permutációcsoport, akkor

$$\operatorname{diam}(G) \leq \exp\left((\log n)^c\right).$$

Ugyanebben a cikkben azt is belátták, hogy ha G egy n-edfokú tranzitív permutációcsoport, akkor

$$\operatorname{diam}(G) \leq \exp\left(O\left(\log^3 n\right)\right) \operatorname{diam}(A_k),$$

ahol A_k a legnagyobb alternáló csoport a G kompozícióláncában. Ebből és a Helfgott-Seress korlátból következik a tranzitív permutációcsoportokra sejtett felső korlát.

Valószínűségelméleti eszközök segítségével is adható felső korlát az átmérőre, nevezetesen ha $G = S_n$ vagy A_n és a $g, h \in G$ elemeket egyenletes eloszlással, függetlenül választjuk, akkor nagy valószínűséggel generálni fogják a G-t, amikor $n \to \infty$, és ebben az esetben a megfelelő Cayley-gráf átmérője nagy valószínűséggel kisebb lesz, mint $n^2 (\log n)^c$. Ezt Helfgott, Seress és Zuk bizonyították a [HeSeZu15] cikkben.

A Lie-típusú véges egyszerű csoportok esete

Az $SL_2(p)$ (ahol p tetszőleges prím) csoport esetén a sejtést Helfgott bizonyította a 2008-as [He08] cikkében a következő állítás alapján.

Állítás. *Legyen p egy prím és legyen A egy generátorrendszere az $SL_2(p)$ csoportnak..*

[4] Azt mondjuk, hogy $f(n)$ *kvázi-polinomiális*, ha $\log f(n)$ polinomiális $\log n$-ben.

1. *Tegyük fel, hogy* $|A| < p^{3-\delta}$ *valamilyen rögzített pozitív* δ*-ra. Ekkor*

$$\left|A^3\right| > c\,|A|^{1+\epsilon},$$

ahol $c > 0$ *és* $\epsilon > 0$ *csak a* δ*-tól függenek.*

2. *Tegyük fel, hogy* $|A| > p^{\delta}$ *valamilyen rögzített* $\delta > 0$*-ra. Ekkor létezik olyan* δ*-tól függő pozitív egész szám, melyre az* $SL_2(p)$ *minden eleme felírható legfennebb* k *darab* $A \cup A^{-1}$*-beli elem szorzataként.*

2011-ben az eredményt kiterjesztette az $SL_3(p)$ csoportra a [He11] cikkben. Pyber és Szabó [PySza16], illetve tőlük függetlenül Breuillard, Green és Tao [BrGrTa11] bizonyították a következő szorzattételt, melyből következik a Babai-sejtés minden véges rangú Lie-típusú véges egyszerű csoport esetén. Ez tulajdonképpen a fenti állítás általánosítása.

Tétel. *Bármely pozitív egész* r *számhoz létezik egy* $\epsilon = \epsilon(r) > 0$ *úgy, hogy ha* G *tetszőleges* r*-rangú Lie-típusú véges egyszerű csoport* S *generátorrendszerrel, akkor vagy* $|S^3| > |S|^{1+\epsilon}$ *vagy* $S^3 = G$*.*

Következmény. *Ha* G *egy* r*-rangú Lie-típusú véges egyszerű csoport, akkor bármely* S *generátorrendszer esetén*

$$diam(Cay(G,S)) = O\left(\frac{\log|G|}{\log|S|}\right)^c,$$

ahol c *csak az* r*-től függ.*

Bizonyítás. Legyen $\epsilon = \epsilon(r)$ az előző Tétel alapján, valamint legyen k a legkisebb egész szám, amelyre $|S|^{(1+\epsilon)^k} > |G|$. Tételezzük fel, hogy $S^{\left(3^k\right)} \neq G$. Az előző tétel többszöri alkalmazásából adódik, hogy

$$\left|S^{\left(3^k\right)}\right| > |S|^{(1+\epsilon)^k} > |G|,$$

ami ellentmondás. Tehát

$$\operatorname{diam}(\operatorname{Cay}(G,S)) \leq 3^k.$$

Legyen $c = \log_{1+\epsilon} 3$, ekkor

$$|S|^{(1+\epsilon)^k} > |G| \Longleftrightarrow (1+\epsilon)^k > \frac{\log|G|}{\log|S|} \Longleftrightarrow 3^k > \left(\frac{\log|G|}{\log|S|}\right)^c,$$

ahonnan adódik, hogy

$$\operatorname{diam}(\operatorname{Cay}(G,S)) \leq 3^k \leq 3\left(\frac{\log|G|}{\log|S|}\right)^c.$$

□

Megjegyzendő, hogy ha az S mérete nagy, akkor ez egy jobb becslés, mint ami a Babai-sejtésben megjelenik.

Szintén korlátos rang esetén, fontos megemlíteni Breuillard, Green, Guralnick és Tao eredményét (lásd [BrGrGuTa15, Theorem 1.2]), amely szerint egy véletlen Cayley-gráf majdnem biztosan $(1 - o(1)$ valószínűséggel) expander gráf, amiből az átmérőre adódik az $O(\log |G|)$ felső korlát. Az expander gráfok nagyon fontos elemét képezik a gráfelméletnek, és rengeteg elméleti és gyakorlati hasznuk van, például nagy hálózatok tervezésénél, algebrai kódelméletben, számelméletben és geometriában. Ezen gráfok részletes elméleti leírása megtalálható például a [HoLiWi06] jegyzetben.

Nemkorlátos rang esetén a kérdés nyitott. Halasi, Maróti, Pyber és Qiao (lásd [HaMaPyQi19]) belátták, hogy ha G nemkorlátos rangú Lie-típusú véges egyszerű csoport, akkor

$$\operatorname{diam}(G) \leq q^{O(n \log n)^2},$$

ahol a csoportot az $\mathbb{F}_q$ prímhatvány elemszámú véges test fölött értelmeztük.

Klasszikus csoportok esetén Garonzi, Halasi és Somlai a következőt bizonyították be.

Tétel. *(Garonzi-Halasi-Somlai, [GaHaSo22]) Legyen V egy n-dimenziós vektortér az $\mathbb{F}_q$ véges test fölött, ahol q páratlan prímhatvány és G legyen az $SL(V)$, $Sp(V)$ vagy $SU(V)$ csoportok bármelyike. Legyen S egy olyan generátorrendszere G-nek, ami tartalmaz nyírást*[5]*. Ekkor*

$$diam(Cay(G, S)) = (n \log q)^c,$$

valamilyen $c > 0$ konstansra, feltéve, hogy

- *$q \neq 9$, ha $G = Sp(V)$;*
- *$q \neq 81$, ha $G = SU(V)$;*
- *$q \neq 9$ és $q \neq 81$, ha $G = SL(V)$.*

Véletlen generátorrendszereket vizsgálva Eberhard és Jezernik bizonyították (lásd [EbJe22, Corollary 1.5]), hogy az $SL_n(p)$ csoportra teljesül a Babai-sejtés, feltéve, hogy p korlátos prím és a csoportnak legalább 3 véletlen generátorát tekintjük. Ez az eredmény továbbfejleszthető, vagyis $SL_n(p)$ helyett minden olyan esetben igaz, amikor a Garonzi-Halasi-Somlai eredmény teljesül.

[5] A V vektortér egy $1 + \nu$ alakú lineáris transzformációját *nyírás*nak nevezzük, ha az $\mathrm{Im}\nu$ képtér egydimenziós és $\mathrm{Im}\nu \subseteq \mathrm{Ker}\nu$.

3 Alkalmazások

Ebben a fejezetben alkalmazásokon keresztül mutatjuk meg, hogy miként használhatók a Cayley-gráfok a matematika különböző területén. Fő forrásaink a [Lö15], [LaSe16], [Se80] és [PPP] jegyzetek.

3.1. Nielsen-Schreier-tétel

Az alkalmazások sorát a Nielsen-Schreier-tétel bizonyításával kezdjük. Legyen S tetszőleges halmaz és $F(S)$ az S által generált szabad csoport.

3.1. Tétel. *(Nielsen-Schreier) Szabad csoport minden részcsoportja szabad csoport. Ha H egy véges indexű részcsoport $F(S)$-ben, akkor H rangja*

$$|F(S) : H|(|S| - 1) + 1.$$

A részletes algebrai bizonyítás Pálfy Péter Pál *Csoportok és reprezentációik* c. [PPP] egyetemi jegyzetéből olvasható. Mi most a Cayley-gráfok segítségével történő bizonyítást mutatunk be, amihez Clara Löh *Geometric group theory, an introduction* c. könyvét használtuk forrásul [Lö15].

3.2. Definíció. Legyen G tetszőleges csoport és $\Gamma = (V, E)$ tetszőleges gráf, valamint vegyük G-nek egy $\varphi : G \to \mathrm{Aut}(\Gamma)$ hatását a Γ gráfon. Azt mondjuk, hogy a φ hatás *szabad*, ha szabad a csúcsokon és az éleken egyaránt, vagyis bármely $g \in G \setminus \{1\}$ elemre

$$\varphi(g)(v) \neq v, \text{ minden } v \in V\text{-re és}$$
$$\{\varphi(g)(v), \varphi(g)(v')\} \neq \{v, v'\}, \text{ minden } \{v, v'\} \in E \text{ esetén.}$$

Vizsgáljuk meg egy kicsit részletesebben ezt a definíciót. Egyik feltétel sem implikálja a másikat. Képzeljük el, hogy egy $\varphi(g) \in \mathrm{Aut}(\Gamma)$ automorfizmus egyetlen csúcsot sem hagy helyben. Ez nem zárja ki azt, hogy egy él fixen maradjon, például ha $\{v_1, v_2\} \in E$ és $\varphi(g)(v_1) = v_2$, $\varphi(g)(v_2) = v_1$, hiszen irányítatlan gráfban a $\{v_1, v_2\}$ és $\{v_2, v_1\}$ ugyanazt az élt reprezentálják, tehát szabad hatás esetén a $\varphi(g)$ automorfizmus egy adott él két csúcspontját nem cserélheti fel egymással. Fordítva, ha minden él elmozdul egy tőle különböző élbe, akkor az úgy is történhet, hogy például $\{v_1, v_2\}$-ben v_1 fixen marad és v_2 a v_1 egy másik szomszédjába képződik.

A Nielsen-Schreier-tétel bizonyítása a következő tételen fog múlni.

3.3. Tétel. *Egy G csoport pontosan akkor szabad csoport, ha létezik olyan fa, amin G szabadon hat.*

Ennek bizonyításához további algebrai gráfelméleti fogalmakra és lemmákra lesz szükségesünk.

Láttuk, hogy a baleltolás a Cayley-gráfon egy hatást ad meg. A következő lemmában szükséges és elégséges feltételt adunk arra vonatkozóan, hogy ez a hatás milyen esetben lesz szabad.

3.4. Segédtétel. *Legyen G egy csoport S generátorrendszerrel. A baleltolás pontosan akkor fog szabadon hatni a $\Gamma = Cay(G, S)$ Cayley-gráfon, ha S nem tartalmaz másodrendű elemet.*

Bizonyítás. Mivel G regulárisan hat saját magán baleltolással, ezért a Γ csúcsain a hatás szabad. Vizsgáljuk meg, hogy milyen feltételek mellett lesz ez a hatás szabad az éleken.

Ha $s \in S$ másodrendű elem, akkor s helyben hagyja az $\{1, s\} = \{s^2, s\}$ élt, következésképpen a hatás nem lesz szabad az éleken.

Tételezzük fel, hogy a baleltolás nem szabad a Γ élein. Legyen $g \in G$ olyan elem, amely a $\{v, v'\} \in E$ élt helyben hagyja, vagyis $\{v, v'\} = g \cdot \{v, v'\} = \{g \cdot v, g \cdot v'\}$. A Cayley-gráf definíciója alapján az, hogy a v és v' csúcsok között halad él azzal ekvivalens, hogy létezik $s \in S$ úgy, hogy $v' = v \cdot s$. Két lehetőség állhat fenn aszerint, hogy a g a v-t és a v'-t helyben hagyja, vagy megcseréli őket.

- ha $g \cdot v = v$ és $g \cdot v' = v'$, akkor következik, hogy $g = e$, hiszen a hatás szabad a csúcsokon;
- ha $g \cdot v = v'$ és $g \cdot v' = v$, akkor

$$v = g \cdot v' = g \cdot (v \cdot s) = (g \cdot v) \cdot s = v' \cdot s = (v \cdot s) \cdot s = v \cdot s^2,$$

  tehát $s^2 = 1$ kell legyen, hiszen a jobbeltolás is szabad a csúcsokon, de $s \neq 1$ így az S tartalmaz másodrendű elemet.

□

3.5. Segédtétel. *Legyen $F := F(S)$ az S által generált szabad csoport. Ekkor a $\Gamma = Cay(F, S)$ Cayley-gráf egy fa.*

3.6. *Észrevétel.* Vegyük észre, hogy a fordított állítás nem igaz. Egy egyszerű ellenpélda a $\mathbb{Z}_2$ kételemű csoport az $S = \{1\}$ generátorrendszerrel, hiszen ebben az esetben a Cayley-gráf egy kétcsúcsú gráf egy éllel, ami nyilván fa, de $\mathbb{Z}_2$ nem szabad csoport.

Bizonyítás. Definíció szerint a szabad csoport elemei szavak ekvivalenciaosztályai. Könnyen belátható (lásd például a [Lö15] jegyzetben a 3.3.5-ös Állítást és a 3.3.6-os Következményt), hogy minden ekvivalenciaosztály pontosan egy *egyszerűsíthetetlen szó*t tartalmaz. Ezek olyan szavak, amelyekben nem szerepel s és s^{-1} egymás mellett. A továbbiakban tehát egy szabad csoport elemeire egyszerűsíthetetlen szavakként gondolunk.

Két dolgot kell megmutatnunk. Egyrészt azt, hogy Γ összefüggő másrészt, hogy Γ-ban nincs kör. Az összefüggőség nyilvánvaló, hiszen ez éppen azzal ekvivalens, hogy S generátorrendszer.

Tegyük fel indirekten, hogy Γ tartalmaz egy $g_0, ..., g_{n-1}$, $n \geq 3$ kört. Ez azt jelenti, hogy minden $i \in \{0, ..., n-2\}$ index esetén

$$g_{i+1} = g_i \cdot s_{i+1}, \text{ ahol } s_{i+1} \in S \cup S^{-1},$$

és

$$s_n = g_{n-1}^{-1} \cdot g_0.$$

Ekkor teljesül az

$$s_1 s_2 \cdots s_{n-1} s_n = g_0^{-1} \cdot g_1 \cdot g_1^{-1} \cdot g_2 \cdots g_{n-2}^{-1} \cdot g_{n-1} \cdot g_{n-1}^{-1} \cdot g_0 = 1$$

egyenlőség, ami lehetetlen, ugyanis a $g_0, ..., g_{n-1}$ csúcsok mind különböznek, tehát az $s_1 \cdots s_{n-1}$ szó egyszerűsíthetetlen kell hogy legyen. Tehát Γ körmentes, így valóban egy fa. □

A 3.5-ös Segédtétel megfordítható, ha S-re egy extra feltételt tűzünk ki.

3.7. Segédtétel. *Legyen G egy csoport és $S \subset G$ olyan generátorrendszer, amely teljesíti azt, hogy bármely $s, t \in S$ esetén $s \cdot t \neq 1$. Ekkor ha a $\Gamma = Cay(G, S)$ Cayley-gráf egy fa, akkor S szabad generátorrendszere G-nek.*

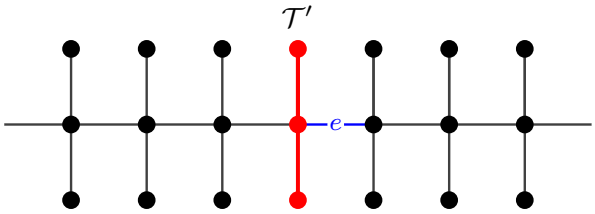
Bizonyítás. Belátjuk, hogy az $F := F(S)$ szabad csoport izomorf a G-vel. A szabad csoportok univerzális tulajdonsága alapján a $\mathrm{id}_S : S \to G$, $s \xrightarrow{\mathrm{id}_S} s$ identikus leképezés kiterjed egyértelműen egy $\varphi : F(S) \to G$ csoporthomomorfizmussá, ami az S-en identikus. Mivel S generálja a G-t, ezért a φ szürjektív, tehát csak azt kell belátnunk, hogy φ injektív. Tételezzük fel, hogy φ nem injektív és legyen $s_1 \cdots s_n \in F$ az a minimális hosszúságú nemüres egyszerűsíthetetlen szó, ami a G egységelemébe képződik. Mivel $\varphi|_S = \mathrm{id}_S$ injektív adódik, hogy $n \geq 2$. Ha $n = 2$, akkor

$$e = \varphi(s_1 \cdot s_2) = \varphi(s_1) \cdot \varphi(s_2) = s_1 \cdot s_2,$$

ami ellentmond az S-re kitűzött tulajdonságnak. Tegyük fel, hogy $n \geq 3$ és vegyük a $g_0 := 1$ és $g_{i+1} := g_i \cdot \varphi(s_{i+1}) = g_i \cdot s_{i+1}$ elemeket minden $i \in \{0, ..., n-2\}$-re. Mivel az $s_1 \cdots s_n$

minimális hosszúságú szó, ami az e-be képződik, következik, hogy a $g_0, ..., g_{n-1}$ elemek mind különbözőek, ráadásul definíció szerint ezek a Γ-ban egy kört képeznek, hiszen a $\{g_0, g_1\}, ..., \{g_{n-2}, , g_{n-1}\}$ és $\{g_{n-1}, g_0\} = \{s_1 \cdots s_{n-1}, 1\} = \{s_1 \cdots s_{n-1}, s_1 \cdots s_n\}$ mind élei a Γ gráfnak, ami ellentmond annak, hogy Γ fa. Tehát φ injektív, következésképpen F izomorf G-vel. □

Legyen G egy tetszőleges csoport és tekintsük a hatását egy Γ összefüggő gráfon. A hatás *feszítőfájá*nak nevezzük azt a Γ-beli részgráfot, ami fa és minden orbitból pontosan egy csúcsot tartalmaz. Tekintsük például a 3.1-es ábrán látható gráfot, és vegyük azt a $\mathbb{Z}$-vel való hatást, ami a csúcsokat vízszintes irányba mozgatja. A hatás egy feszítőfáját piros színnel jelöltük.



3.1. ábra. $\mathbb{Z}$-hatás egy feszítőfája

3.2. ábra. A $\mathcal{T}'$ és eltoltjainak összeomlasztása egy ponttá

Gráfelméletből ismert tétel, hogy minden összefüggő gráfon vett csoporthatásnak van feszítőfája (lásd például [Lö15, Theorem 4.2.4]). Most már minden kellék a rendelkezésünkre áll, hogy rátérjünk a 3.3-as Tétel bizonyítására.

Bizonyítás. Tételezzük fel, hogy G szabad csoport S szabad generátorrendszerrel. Ekkor a 3.5-ös Segédtétel alapján a $\Gamma = \mathrm{Cay}(G, S)$ egy fa. Hasson a G baleltolásokkal a Γ Cayley-gráfon. A szabad csoport univerzális tulajdonságát alkalmazva az $S \to \mathbb{Z}$ leképezésre adódik, hogy S nem tartalmazhat másodrendű elemet. Ekkor a 3.4-es Segédtétel alapján a baleltolás szabadon hat a Γ-n.

Most tegyük fel, hogy a G szabadon hat egy $\mathcal{T}$ fán. Ekkor létezik a hatáshoz $\mathcal{T}' \subset \mathcal{T}$ feszítőfa. A szabad hatásból és a feszítőfa definíciójából adódik, hogy $g \cdot \mathcal{T}'$ diszjunkt $\mathcal{T}'$-től, minden $g \neq 1$-re. Nevezzünk egy $\mathcal{T}$-beli élt *lényeges*nek[1] akkor, ha nem $\mathcal{T}'$-beli él de az egyik végpontja $\mathcal{T}'$-ben van (lásd a 3.1-es ábrán a kék élt). Megszerkesztjük G egy szabad generátorrendszerét.

Legyen $e = \{u, v\}$ egy lényeges él $u \in \mathcal{T}'$ és $v \notin \mathcal{T}'$ csúcsokkal. Mivel $\mathcal{T}'$ a szóban forgó hatás feszítőfája, ezért $\mathcal{T}'$ a v csúcs orbitjából pontosan egy csúcsot fog tartalmazni, azaz egyértelműen létezik egy $g_e \in G$ csoportelem úgy, hogy $g_e^{-1} \cdot v$ a $\mathcal{T}'$ csúcsa, így v a $g_e \cdot \mathcal{T}'$

[1] Képzeljük el azt a gráfot, amit a $\mathcal{T}$-ből kapunk oly módon, hogy a $\mathcal{T}'$ és annak minden $g \cdot \mathcal{T}'$ eltolt példányát összeomlasztunk egyetlen ponttá (ezt szemlélteti a 3.2-es ábra). Ekkor az eredeti $\mathcal{T}'$ gráfbeli lényeges élek ebben a gráfban is élek lesznek. Innen ered a megnevezés.

csúcsa. Legyen $\tilde{S}$ az

$$\tilde{S} := \{g_e \in G : e \text{ lényeges él } \mathcal{T}\text{-ben}\} \subset G$$

részhalmaz. Mivel v nincs $\mathcal{T}'$-ben így 1 sem lehet benne az $\tilde{S}$-ban. Ha e és e' két olyan lényeges él, melyekre $g_e = g_{e'}$, akkor $e = e'$, mivel $\mathcal{T}$ fa, így $\mathcal{T}'$ és $g_e \cdot \mathcal{T}' = g_{e'} \cdot \mathcal{T}'$ összefüggő részgráfokat nem kötheti össze két különböző él, hiszen akkor lenne $\mathcal{T}$-ben egy kör. Továbbá ha $g \in \tilde{S}$, vagyis $g = g_e$ valamilyen e lényeges élre, akkor $g^{-1} = g_{g^{-1}\cdot e} \in \tilde{S}$. Ez abból adódik, hogy ha $e = \{u, v\}$, ahol $u \in \mathcal{T}'$ és $v \notin \mathcal{T}'$, akkor $g^{-1} \cdot e = \{g^{-1} \cdot u, g^{-1} \cdot v\}$, és a $g \in G$ elem definíciója szerint $g^{-1} \cdot v$ már $\mathcal{T}'$-ben van, viszont $g^{-1} \cdot u \in g^{-1} \cdot \mathcal{T}' \neq \mathcal{T}'$, tehát $g^{-1} \cdot e$ is lényeges él. Az a csoportelem, melynek az inverze a $g^{-1} \cdot u$ csúcsot $\mathcal{T}'$-be képezi éppen a $g = (g^{-1})^{-1}$, vagyis $g^{-1} = g_{g^{-1}\cdot e}$. Végül $\tilde{S}$ nem tartalmazhat másodrendű elemet, hiszen ha $g_e \in \tilde{S}$ másodrendű elem lenne, akkor $g_e = g_e^{-1} = g_{g_e^{-1}\cdot e}$ egyenlőségből az adódna, hogy $e = g_e^{-1} \cdot e$, ami lehetetlen, hiszen G szabadon hat a $\mathcal{T}$-n. $\tilde{S}$ minden eleme és annak inverze közül pontosan az egyiket kiválasztva kapunk egy $S \subset \tilde{S}$ részhalmazt, melyre $S \cap S^{-1} = \emptyset$ és $S \cup S^{-1} = \tilde{S}$.

Belátjuk, hogy $\tilde{S}$ generálja a G-t, amiből következik, hogy S is generátorrendszer G-ben. Legyen $g \in G$ tetszőleges elem és válasszunk egy tetszőleges $v \in \mathcal{T}'$ csúcsot. Mivel $\mathcal{T}$ összefüggő, ezért létezik út a v és a $g \cdot v$ között. Ez az út a $\mathcal{T}'$ néhány eltoltján halad át, legyenek ezek sorrendben a $g_0 \cdot \mathcal{T}', g_1 \cdot \mathcal{T}', \ldots, g_n \cdot \mathcal{T}'$ részgráfok, ahol $g_0 = 1, g_n = g$ és minden $i \in \{0, ..., n-1\}$ indexre $g_{i+1} \neq g_i$. A $g_i \cdot \mathcal{T}'$ és $g_{i+1} \cdot \mathcal{T}'$ részgráfokat összeköti egy e_i él. Ekkor a $g_i^{-1} \cdot e_i$ lényeges él, és a neki megfelelő csoportelem az $s_i := g_i^{-1} \cdot g_{i+1}$ lesz. Ekkor a

$$\begin{aligned} g = g_n &= g_0^{-1} \cdot g_n \\ &= g_0^{-1} \cdot g_1 \cdot g_1^{-1} \cdots g_{n-1}^{-1} \cdot g_n \\ &= s_0 \cdots s_{n-1} \end{aligned}$$

előállítást kapjuk, tehát $\tilde{S}$ (és így S is) generátorrendszer. A $\mathrm{Cay}\left(G, \tilde{S}\right)$ tulajdonképpen a $\mathcal{T}$-ből keletkezik úgy, hogy a $\mathcal{T}'$ és annak eltoltjait összeomlasztjuk egy ponttá. Ezt jól szemlélteti a 3.2-es ábra a $\mathbb{Z}$ 1-rangú szabad csoport esetén.

Már csak azt kell bizonyítani, hogy S szabad generátorrendszer. Mivel $S \cap S^{-1} = \emptyset$ teljesül, ezért a 3.7-es Segédtétel alapján elegendő megmutatni, hogy a $\mathrm{Cay}(G, S)$ Cayley-gráf körmentes. Tegyük fel indirekte, hogy a $\mathrm{Cay}\,(G, S) = \mathrm{Cay}\left(G, \tilde{S}\right)$ gráf tartalmaz egy $g_0, ..., g_{n-1}$ kört, ahol $g_{i+1} = g_i \cdot s_{i+1}$ minden $i \in \{0, ..., n-2\}$ esetén és $g_0 = g_{n-1} \cdot s_n$. Legyen $e_i = \{u_i, v_i\}$ a $\mathcal{T}'$ és $s_{i+1} \cdot \mathcal{T}'$ részgráfokat összekötő lényeges él minden $i \in \{0, ..., n-1\}$-re. Tekintsük a $g_0 \cdot e_0 = \{g_0 \cdot u_0, g_0 \cdot v_0\}$ és $g_1 \cdot e_1 = \{g_1 \cdot u_1, g_1 \cdot v_1\}$ éleket. Előbbi a $g_0 \cdot \mathcal{T}'$ és $g_0 \cdot s_1 \cdot \mathcal{T}' = g_1 \cdot \mathcal{T}'$ részgráfok között, míg utóbbi a $g_1 \cdot \mathcal{T}'$ és $g_1 \cdot s_2 \cdot \mathcal{T}' = g_2 \cdot \mathcal{T}'$ részgráfok között halad. Mivel a $\mathcal{T}'$ és annak eltoltjai mind összefüggő gráfok, ezért a $g_0 \cdot v_0$

és $g_1 \cdot u_1$ csúcsok között van egy út $g_1 \cdot \mathcal{T}'$-ben. Ezt az eljárást folytatva és kihasználva, hogy a $g_0, ..., g_{n-1}$ elemek kört definiálnak a Cay $\left(G, \tilde{S}\right)$ Cayley-gráfban egy $\mathcal{T}$-beli körhöz jutunk, ami ellentmondás. □

A Nielsen-Schreier-tétel a következőképpen bizonyítható.

Bizonyítás. Ha $G := F(S)$ szabad csoport, akkor a $\mathcal{T} := \mathrm{Cay}(G, S)$ Cayley-gráf egy fa és a 3.3-as Tétel szerint G szabadon hat rajta baleltolásokkal. Ekkor ha H egy részcsoport G-ben, akkor H is szabadon hat ezen a fán baleltolásokkal, tehát a 3.3-as Tétel alapján H is szabad csoport kell legyen.

Legyen $\mathcal{T}' = (V', E')$ a H-nak $\mathcal{T}$-n vett hatásának egy feszítőfája, legyen G rangja n és H indexe k. A 3.3-as Tétel bizonyításából kiderül, hogy a H rangja éppen a lényeges élek számának a fele. Jelöljük a lényeges élek számát l-el. A H orbitjai éppen a H szerinti jobboldali mellékosztályok, és $\mathcal{T}'$ ezek mindegyikéből pontosan egyet tartalmaz, így $|\mathcal{T}'| = |G : H| = k$. Mivel $\mathcal{T}$ reguláris fa, ezért minden csúcsnak a foka $2 \cdot |S| = 2 \cdot n$, így ha összegezzük a $\mathcal{T}'$-beli csúcsok fokait a

$$2 \cdot n \cdot k = \sum_{v \in V'} \deg(v)$$

egyenlőséghez jutunk. Továbbá $\mathcal{T}'$ k-csúcsú fa, így éleinek száma $k - 1$. Ekkor a

$$\sum_{v \in V'} \deg(v) = 2 \cdot (k - 1) + l$$

összefüggés adódik, hiszen a szummában $\mathcal{T}'$ minden élét kétszer számoljuk meg. Végül a

$$2 \cdot n \cdot k = 2 \cdot (k - 1) + l$$

egyenletből kifejezve az l-et, megkapjuk, hogy H rangja

$$\frac{l}{2} = k \cdot (n - 1) + 1.$$

□

Térjünk vissza egy pillanatra a 2-rangú szabad csoport esetére. A 1.2-es ábrán lévő kék csúcsok 3-rangú szabad csoportot alkotnak a Nielsen-Schreier-tétel szerint, hiszen ezek egy 2-indexű részcsoportot képeznek F_2-ben. Könnyen látható, hogy H-t szabadon generálja az $S = \{x^2, xy, xy^{-1}\}$ halmaz.

3.2. Legrövidebb utak problémája Cayley-gráfokban

Cayley-gráfok esetében az ún. *legrövidebb utak problémája* kisebb komplexitású, mint általános gráfokban.

Legyen G egy n-elemű véges csoport S generátorrendszerrel, és Γ a hozzájuk rendelt Cayley-gráf. Továbbá legyen $g, h \in G$ két tetszőleges csúcs és $k = d(g,h)$,ahol $1 \leq k \leq D$, D pedig a Cayley-gráf átmérőjét jelöli. Mivel a g és h csúcsok közötti legrövidebb út hossza k, ezért léteznek az $s_{i_1}, s_{i_2}, ..., s_{i_k} \in S$ generátorelemek, amelyek ezt az utat adják, vagyis

$$g = g_0 \xrightarrow{s_{i_1}} g_1 \xrightarrow{s_{i_2}} g_2 \longrightarrow \cdots \xrightarrow{s_{i_{k-1}}} g_{k-1} \xrightarrow{s_{i_k}} g_k = h,$$

ahol

$$g_j = g_0 \cdot s_{i_1} \cdot s_{i_2} \cdots s_{i_j},$$

minden $1 \leq j \leq k$ esetén. Innen azt kapjuk, hogy a

$$h = g \cdot s_{i_1} \cdot s_{i_2} \cdots s_{i_k}$$

alakban áll elő, ahonnan

$$g^{-1}h = 1 \cdot s_{i_1} \cdot s_{i_2} \cdots s_{i_k}.$$

Ez tulajdonképpen azt jelenti, hogy ha a g és h csúcsok közötti legrövidebb utat az $s_{i_1}, s_{i_2}, ..., s_{i_k}$ generátorokon keresztül értük el, akkor az e identitás és a $g^{-1}h$ elemek között is megkapjuk a legrövidebb utat az $s_{i_1}, s_{i_2}, ..., s_{i_k}$ elemeken keresztül és fordítva. Mivel a $\{g^{-1}h : g, h \in G\}$ a teljes G csoporttal egyezik meg, ezért a legrövidebb út megtalálásához nem szükséges az összes $\frac{n(n-1)}{2}$ darab csúcspár esetén megtalálni a legrövidebb utakat, elegendő az e identitás és az összes többi $n-1$ darab csúcs közötti legrövidebb utakat megkeresni. Ez tehát azt jelenti, hogy Cayley-gráfokban a legrövidebb utak problémája $O(n)$ komplexitású $O(n^2)$ helyett.

3.3. Cayley-gráfok és a Banach-Tarski paradoxon

A Banach-Tarski paradoxon a halmazelméleti geometria nagyon híres paradoxona, amelyet S. Banach és A. Tarski bizonyítottak be 1924-ben annak szemléltetésére, hogy a kiválasztási axióma helytelen. A paradoxon a következőt állítja: a háromdimenziós tömör gömböt a kiválasztási axióma felhasználásával fel lehet bontani véges sok, (nem mérhető) részhalmaz diszjunkt uniójára, amelyek térben történő mozgatásával két, az eredeti gömbbel megegyező méretű tömör gömböt lehet összerakni. A paradoxon abban rejlik, hogy a fizikai valóságból kiindúlva két gömb térfogata kétszer akkora, mint egy gömb térfogata, az átdarabolás pedig térfogattartó. De akkor viszonylag könnyen meg tudna bárki gazdagodni: csak egy aranygömbre van szükségünk, amit a tétel szerint átdarabolunk két aranygömbé és így tovább. A „csalás" ott történik, hogy nem mérhető darabokat feltételez a tétel, persze a fizikai valóságban ez lehetetlen, ott csak mérhető darabokat tudunk létrehozni. Az állítást ma már matematikailag helyesnek fogadjuk el, és nem a kiválasztási axióma helytelenségét, hanem az intuíciók tévedhetőségét szemlélteti. A Banach-Tarski paradoxon bizonyítása 4 lépésből áll:

1. Megadjuk a 2-rangú szabad csoport paradox felbontását.
2. Keresünk a háromdimenziós térhez egy olyan forgáscsoportot, ami izomorf a 2-rangú szabad csoporttal.
3. Az első lépésben megadott felbontást és a kiválasztási axiómát használva megadjuk az egységgömbfelület egy paradox felbontását.
4. Kiterjesztjük a felbontást a háromdimenziós tömör gömbre.

Ebben a részben csak az első lépését szeretnénk bemutatni, ugyanis ez a lépés jól szemléltehető egy bizonyos Cayley-gráfon.

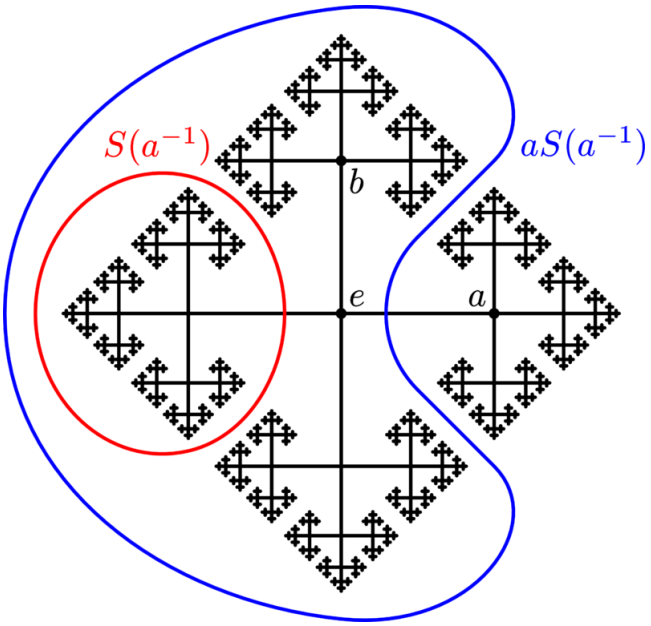
Az F_2 szabad csoport a következőképpen bontható fel: jelöljük $S(a)$-val az a-val kezdődő redukált szavak halmazát, hasonló módon tekintsük az $S(a^{-1})$, $S(b)$ és $S(b^{-1})$ diszjunkt halmazokat. Nem nehéz látni, hogy

$$F_2 = 1 \cup S(a) \cup S\left(a^{-1}\right) \cup S(b) \cup S\left(b^{-1}\right).$$

Célunk az, hogy az F_2-t ezekből a darabokból kétféleképpen hozzuk létre diszjunkt részhalmazok uniójaként, hiszen pontosan ezt szeretnénk elérni a tömör gömb esetén is. A fenti felbontásban lévő $S(a^{-1})$ és $S(b^{-1})$ részhalmazokat toljuk el rendre a-val és b-vel. Ezzel két különböző felbontást kaptunk, hiszen

$$F_2 = S(a) \cup aS\left(a^{-1}\right),$$
$$F_2 = S(b) \cup bS\left(b^{-1}\right).$$

A felbontás szépen szemléltethető az F_2 Cayley-gráfján:



Irodalomjegyzék

[Ba06] L. Babai, *On the diameter of Eulerian orientations of graphs*, in: Proc. 17th Ann. Symp. on Discrete Algorithms (SODA'06), ACM–SIAM, 2006, pp.822–831.

[BaSe92] L. Babai, Á. Seress, *On the diameter of permutation groups,* European J. Combin. 13 (1992), 231-243.

[BaKaLu89] L. Babai, W. M. Kantor, A. Lubotzky, *Small diameter Cayley-graphs for finite simple groups*, European Journal of Combinatorics, 10, 1989.

[BaSe87] L. Babai, Á. Seress, *On the Diameter of Cayley Graphs of the Symmetric Group*, The American Mathematical Monthly, Vol. 94, No. 6 (Jun. - Jul., 1987), 497-506.

[BiYa17] A. Biswas, Y. Yang, *A diameter bound for finite simple groups of large rank*, J. Lond. Math. Soc. (2) 95 (2017), 455-474.

[BrGrGuTa15] E. Breuillard, B. Green, R. Guralnick, T. Tao, *Expansion in finite simple groups of Lie type*, J. Eur. Math. Soc. 17(6), 1367-1434 (2015).

[BrGrTa11] E. Breuillard, B. Green, T. Tao, *Approximate subgroups of linear groups*, Geom. Funct.Anal. 21 (2011) 774-819.

[EbJe22] S. Eberhard, U. Jezernik, *Babai's conjecture for high-rank classical groups with random generators*, Invent. Math. 227 (2022), 149-210.

[EvGo81] S. Even, O. Goldreich, *The minimum-length generator sequence problem is NP-hard*, J. Algorithms 2, 311-313 (1981).

[GaHaSo22] M. Garonzi, Z. Halasi, G. Somlai, *On the Diameter of Cayley Graphs of Classical Groups With Generating Sets Containing a Transvection*, 2022, arXiv:2203.03323.

[GoRo13] C. Godsil, G. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, Springer New York, 2013.

[HaMaPyQi19] Z. Halasi, A. Maroti, L. Pyber, Y. Qiao, *An improved diameter bound for finite simple groups of Lie type*, Bull. Lond. Math. Soc. 51 (2019), 645-657.

[HeSeZu15] H. A. Helfgott, Á. Seress, A. Zuk, *Random generators of the symmetric group: diameter, mixing time and spectral gap*, Journal of Algebra, Vol. 421 (2015), 249-368.

[HeSe14] H. A. Helfgott, Á. Seress, *On the diameter of permutation groups*, Ann. Math. (2) 179 (2014) 611–658.

[He11] H. A. Helfgott, *Growth in* $SL_3(\mathbb{Z}/p\mathbb{Z})$, Journal of the European Mathematical Society, Vol. 13, Issue 3 (2011), 761-851.

[He08] H. A. Helfgott, *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Ann. Math. (2) 167 (2008) 601–623.

[HoLiWi06] S. Hoory, N. Linial, A. Widgerson, *Expander Graphs and Their Applications*, Bulletin (New Series) of the American Mathematical Society, Vol. 43, Num. 4, 439-561, 2006.

[Hu72] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1972.

[LaSe16] Lakshmivarahan, S. & Selvaganesh, Lavanya & Dhall, S.K.. (2016). *Cayley graphs*.

[La09] E. Landau, *Handbuch der Lehre von der Verteilunk der Primzahlen*, Bd. I, Teubner, Leipzig, 1909.

[Lö15] C. Löh, *Geometric group theory, an introduction*, Lecture notes, Regensburg, 2015.

[McKaPr94] B. D. McKay, C. E. Praeger, *Vertex-transitive graphs which are not cayley graphs*, i. Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics, 56(1):5363, 1994.

[Me08] J. Meier, *Groups Graphs and Trees: An introduction to the Geometry of infinite groups*, Cambridge, 2008.

[PPP] P. P. Pálfy, Csopo*rtok és reprezentációik*, Egyetemi jegyzet, Budapest, 2020.

[PySza16] L. Pyber, E. Szabo, *Growth in finite simple groups of Lie type*, J. Amer. Math. Soc. 29 (2016), 95-146.

[Sa64] G. Sabidussi, *Vertex-transitive graphs,* Monatsh. Math, 68:426-438, 1964.

[Sa58] G. Sabidussi, *On a class of fixed-point-free graphs*, Proceedings of the American Mathematical Society, 9(5):800804, 1958.

[Se80] J. - P. Serre, *Trees*, Springer-Verlag, 1980.

[Tan] Y. Sh. Tan, *On the Diameter of Cayley Graphs of Finite Groups*, 2011.

[Zh21] F. Zhou, *CO:444: Algebraic Graph Theory*, Lecture notes, Waterloo, 2021.