EÖtvös Loránd Tudományegyetem

Természettudományi Kar

Nagy Ábris

Cayley-gráfok átmérője és expanderek

BSc Szakdolgozat

Témavezető

Somlai Gábor

Algebra És Számelmélet Tanszék

Budapest, 2014

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek Somlai Gábornak, hogy elvállalta a konzulensi teendőket. Köszönöm, hogy mindig rendelkezésemre állt és tanácsaival hozzájárult a szakdolgozat elkészüléséhez.

Valamint köszönöm családomnak és barátaimnak, hogy mindig mellettem álltak és segítették a munkámat.

Tartalomjegyzék

Bevezető

A Cayley-gráfok és az expanderek a modern algebra sokszor alkalmazott definíciói. Cayley-gráfok segítségével, mivel szimmetrikus gráfok, hatékony CPU-hálózatokat lehet tervezni, vagy meg lehet fogalmazni egy nyelvet, ami segíthet kirakni a Rubik-kockát. Expandereket lehet használni pédául hibajavító kódok konstruálására vagy véletlen elemek generálására. A szakdolgozatban az ezekhez szükséges matematikai alapok szerepelnek valamint pár program, példaként a gyakorlati megvalósításra.

A szakdolgozat elején bevezetjük a Cayley-gráfok fogalmát, és megismerkedünk pár alapvető tujadonságukkal. Bemutatjuk mi a kapcsolat egy csoport és Cayley-gráfjai között.

Ezután S_n, A_n, $PSL(2,q)$ és $PSL(n,q)$ csoportokra megadunk olyan S generátorrendszereket, amikre a gráfok átmérője kicsi, és S elemszáma kisebb mint 8. Ezekre a csoportokra a tételt külön bizonyítjuk három teljesen eltérő módon. Egyedül az S_n és A_n esetet lehet együtt kezelni. Azért ezt a tételt emeljük ki, mert a kis átmérőjű Cayley gráfoknak van gyakorlati alkalmazása.

Általában is érdekes a kérdés, hogy mekkora a korábban megadott csoportok összefüggő Cayley gráfjainak az átmérője. A 2.3 fejezetben felső becslést adunk S_n és egyúttal A_n Cayley gráfjainak átmérőjére. Ez a becslés minden olyan generátorrendszer mellett érvényes, ahol a generátorrendszerben van olyan permutáció, ami az elemek legalább 67%-át helyben hagyja. Ehhez véletlen sétákat használunk S_n Cayley-gráfjain. A véletlen sétákról is belátunk pár egyszerű tulajdonságot köztük, hogy egy adott kezdeti eloszlás egy séta során konvergál az egyenletes eloszláshoz. Ezzel egy fontos alkalmazását mutatjuk be a véletlen módszernek.

Kis átmérőjű gráfokat keresve jutunk el az expander gráfok fogalmához. Megadunk 3 egymástól eltérő, algebrai, kombinatorikus és valószínűségszámítási definíciót, majd megmutatjuk, hogy ezek között könnyű kapcsolatot találni. Belátjuk azt is, hogy az expanderek pontosan azok a gráfok amikre a véletlen séta a lehető leggyorsabban konvergál. Ezután explicit konstrukciót adunk expander gráfsorozatokra. A módszer egy gráfok közötti művelet, a cikk-cakk szorzás bevezetése, aminek segítségével rekurzív módon lehet expander sorozatot gyártani. Végül megemlítjük, hogy a véletlen módszer segítségével és Cayley-gráfokkal is belátható olyan gráfok létezése, amik expanderek.

Az utolsó fejezetben a Cayley gráfokra vonatkozó tételek gyakorlati megvaló-

sítása található. Az S_n és $PSL(2,q)$ csoportokra írtunk egy-egy programot ami a csoport egy elemét felbontja a 2.2 fejezetben szereplő elemek szorzatára. Ezenkívül ugyanebben a két csoportban véletlen séták felhasználásával véletlen elemeket generálunk. Ez sok csoportelméleti alkalmazásban felmerülő, fontos alkalmazása kis átmérőjű Cayley gráfoknak.

1. Algebrai alapfogalmak

Mielőtt a szakdolgozat címében említett témákra térnénk, megemlítünk pár alapvető algebrai tételt és fogalmat, amit később használni fogunk. Ezeket bizonyítás és lényegében megjegyzések nélkül, csak felsoroljuk.

1.1. Definíció. (Kronecker-szorzat) *Vagyük az A $n \times m$-es és a B $p \times q$-as mátrixokat. A Kroneker-szorzatukat jeöljük $C = A \otimes B$-vel. Ekkor a C mátrixot úgy kapjuk, hogy az A minden elemét megszorozzuk, B-vel. Így a C egy $mp \times nq$-as mátrix.*

1.2. Tétel. (Frobenius—Perron-tétel [15]) *Legyen $A = [a_{ij}] \in \mathbb{R}^{n \times n}$, minden $a_{ij} \geq 0$. Ekkor van egy $\lambda \geq 0$ valós sajátértéke, amire $|\lambda| \geq |\lambda_i|$ az A mátrix minden λ_i sajátértékére. A λ-hoz tartozó v sajátvektor minden koordinátája nemnegatív valós szám. Továbbá ha A-ban nincs egy $k \times (n-k)$-s csupa 0 részmátrix, (ami nem tartalmazza az átlót,) akkor λ multiplicitása 1, v pedig pozitív.*

1.3. Definíció. (Kettős mellékosztály) *A H, K részcsoport G-ben, akkor a H, K szerinti kettős mellékosztályok a G csoport $\{HxK | x \in G\} \subseteq G$ alakú részhalmazai.*

1.4. Definíció. *Legyen G véges csoport, és a rendjének prímtényezős felbontása $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. A $p_i^{\alpha_i}$ rendű részcsoportokat a G csoport p_i-Sylow részcsoportjainak nevezzük.*

1.5. Tétel. (Sylow-tételek) *Legyen G véges csoport, és p a G rendjének tetszőleges prímosztója. Ekkor igazak az alábbiak:*

1. *Van G-ben p-Sylow részcsoport*
2. *G minden p-hatványrendű részcsoportja része G egy p-Sylow részcsoportjának*
3. *Bármely két p-Sylow részcsoport konjugált G-ben*
4. *Ha q egy G rendjét osztó p-hatvány, akkor a q-rendű G-beli részcsoportok száma kongruens 1-gyel modulo p*
5. *A p-Sylow részcsoportok száma osztója $|G : P|$-nek*

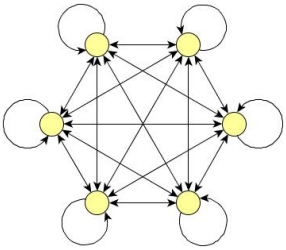
2. Cayley-gráfok

2.1. Bevezető a Cayley-gráfokhoz

2.1. Definíció. *Legyen H egy csoport és S a H elemeinek részhalmaza. A H csoport S által generált* $\mathrm{Cay}(H,S)$ *Cayley-gráfján azt a $G=(V,E)$ gráfot értjük amire $V=H$ és két $g,h\in H$ csúcsra $(g,h)\in E \Leftrightarrow$ létezik $s\in S$ amire $g=sh$. A gráfban az egyes éleket, megfeleltetjük az adott S-beli elemmel való szorzásnak, szokszor így fogunk az élekre hivatkozni. Ha egy G gráfhoz létezik H és S, hogy $G=\mathrm{Cay}(H,S)$, akkor G-t Cayley-gráfnak nevezzük.*

2.2. Megjegyzés. Ha $S=S^{-1}$ akkor a gráfot tekinthetjük irányítatlannak, ugyanis ha $a,b\in G$-re és $s\in S$-re $as=b$, azaz $(a,b)\in \mathrm{Cay}(G,S)$ akkor mivel $s^{-1}\in S$ és $bs^{-1}=a$ ezért $(b,a)\in \mathrm{Cay}(G,S)$ is teljesül.

2.3. Példák. Legyen $G=S_3$ és válasszuk $S=G$-t, generátorhalmaznak. A Cayley-gráf a következő:



1. ábra. $G=S_3$ és $S=S_3$

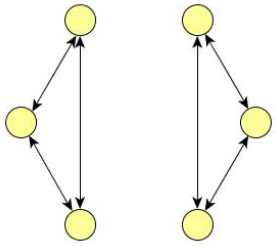
Általában az egységelemet nem szokás bevenni a generálóhalmazba. Így egyszerű gráfokat kapunk, jelen esetben a teljes gráfot kapnánk.

Ha kevesebb elemet választunk be az is előfordulhat, hogy a gráf nem lesz összefüggő. Ez látszik 2.3 ábrán. A gráf pontosan akkor összefüggő, ha S generálja G-t.

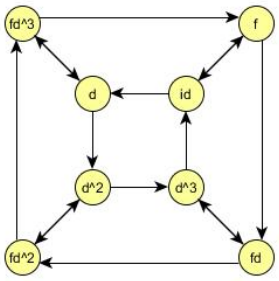
Érdekesebb szerkezetű gráfokat is megkaphatunk, például legyen $G=D_4=\langle d,f\rangle$, ahol $f^2=id$ és $d^4=id$.

Végtelen gráfokat is elő lehet állítani Cayley-gráfként. Legyen például $G=\mathbb{Z}$ a végtelen ciklikus csoport és $S=\{-1,+1\}$

A fenti példákból látszik, hogy ezek a gráfok valamilyen szempontból, nagyon szimmetrikusak, minden pont környezete ugyanúgy néz ki. Ezt az észrevételt a következő definíció teszi formálissá.



2. ábra. $G = S_3$ és $S = A_3 \setminus \{1\}$



3. ábra. $G = D_4$ és $S = \{d, f\}$

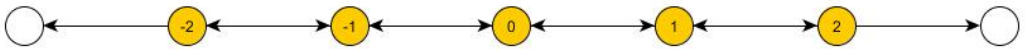
2.4. Definíció. *Egy $G = (V, E)$ gráfot csúcstranzitívnak vagy tranzitívnak nevezünk, ha minden $v_1, v_2 \in V$ létezik egy $f : V \to V$ gráfautomorfizmus, hogy $f(v_1) = v_2$.*

2.5. Definíció. *Legyen G egy permutációcsoport az X halmazon. Tekintsük az $x \in$ elemet helyben hagyó $g \in G$ elemeket. Könnyen ellenőrizhető, hogy ezek részcsoportot alkotnak, amit G_x-el jelölünk, és az x pont stabilizátorának hívunk. $G_x = \{g \in G | x = xg\}$*

2.6. Definíció. *Egy permutációcsoportot t-tranzitívnak nevezünk, ha bármely két különböző elemekből álló $(v_1, v_2, \ldots, v_t)$, $(u_1, u_2, \ldots, u_t)$ rendezett t-esre létezik $\sigma \in G$, hogy $v_i^\sigma = u_i$, minden $1 \leq i \leq n$-re. A csoportot szigorúan t-tranzitívnak nevezünk, ha minden ilyen párhoz pont egy σ tartozik.*

Például triviális, hogy S_n n-tranzitív minden n-re. A következő tétel [12] segítségével, ennél bonyolultabb példákat is megadhatunk:

2.7. Állítás. *[12] Ha a G csoport k-tranzitívan hat a X halmazon, akkor minden $x \in X$ pont stabilizátora $(k-1)$-tranzitívan hat $X \setminus \{x\}$-en. Fordítva, ha G tranzitívan*



4. ábra. $G = \mathbb{Z}$ és $S = \{-1, +1\}$

hat az X-en és egy $x \in X$ pont stabilizátora $(k-1)$-tranzitív az $X \setminus \{x\}$-en, akkor G hatása az Xhalmazon k-tranzitív.

2.8. Megjegyzés. [12] Ha a $G \leq S_X$ csoport szigorúan k-tranzitív, akkor minden $x \in X$ pontra G_x szigorúan $(k-1)$-tranzitív részcsoportja $S_X \setminus \{x\}$-nek. A 2.7 állítás miatt ez a stabilizátor $(k-1)$-tranzitív. Ha lenne két eleme, amely az $x_2, \ldots, x_k \in X \setminus \{x\}$ pontrendszert az $y_2, \ldots, y_k \in X \setminus \{x\}$-ba viszi, akkor ez a két elem az $x, x_2, \ldots, x_k$ pontokat sorra a $x, y_2, \ldots, y_k$ pontokba vinné, ami ellentmond annak, hogy G szigorúan k-tranzitív.

Megfordítva, ha $G \leq S_X$ tranzitív, és van olyan $x \in X$ pont, amelynek a stabilizátora szigorúan $(k-1)$-tranzitív $S_X \setminus \{x\}$-ben, akkor G az S_X-nek szigorúan k-tranzitív részcsoportja a 2.7 állítás miatt. Tegyük föl, hogy g_1 és g_2 is olyan elemek, amelyek x_i-t y_i-be viszik minden $1 \leq i \leq k$-ra. Ekkor $g = g_1 g_2^{-1}$ az összes x_i pontot fixálja. Mivel G tranzitív, van olyan $h \in G$, melyre $h(x_1) = x$, és így hgh^{-1} helyben hagyja az $x = h(x_1), \ldots, h(x_k)$ elemeket. Ezért hgh^{-1} benne van az x pont stabilizátorában, és mivel ez szigorúan $k-1$-tranzitív, $hgh^{-1} = id$, vagyis $g = id$, és így $g_1 = g_2$.

2.9. Következmény. [12] Egy permutációcsoport pontosan akkor szigorúan 1-tranzitív, ha tranzitív és valamelyik pont stabilizátora egyelemű.

Bizonyítás. Az előző megjegyzésből következik $k = 1$ esetén. □

2.10. Megjegyzés. Ha a G csoport tranzitív és $x \in G$-re $|G_x| = 1$ akkor a többi elem stabilizátora is egyelemű. Legyen $y \in G$ ekkor létezik $g \in G$ amire $xg = y$. Egy $h \in G$ elemre $yh = y$ pontosan akkor, ha $xgh = xg$, azaz $xghg^{-1} = x$. Tehát az x-et és az y-t helyben hagyó elemek egymás konjugáltjai.

2.11. Definíció. *Legyen $G \leq S_X$ ekkor azt monjuk, hogy G reguláris ha szigorúan 1-tranzitív, vagy az előző tétel alapján tranzitív és minden pont stabilizátora egyelemű.*

Egy reguláris permutációcsoportra gondolhatunk úgy is, hogy veszünk egy tetszőleges G csoportot és azt az Ω halmazt, ami G elemeiből áll. Ezután minden $g \in G$-re definiáljuk a $\rho_g : x \mapsto xg$ leképezést, ahol $x \in \Omega$. Legyen $G_R = \langle \rho_g | g \in G \rangle$, ekkor $G_R \leq \mathrm{Symm}(\Omega)$. Minden $g \in G$-hez ρ_g-t hozzárendelve látszik az, hogy van reguláris részcsoport. A G_R reguláris, hiszen tranzitív, és minden $x \in \Omega$-ra igaz, hogy csak az identitás hagyja helyben.

Ebből látszik, hogy egy reguláris permutációcsoport megfeleltethető egy Cayley-gráfnak. Ha vesszük az $S \subseteq G$ halmazt, úgy hogy generálja G-t, vesszük a G elemeit mint alaphalmazt és a (g, gs) $g \in G$, s eleme S éleket akkor megkapjuk a $\mathrm{Cay}(G, S)$ Cayley-gráfot.

Ugyanígy egy $\mathrm{Cay}(G, S)$ Cayley-gráf meghatároz egy reguláris permutációcsoportot a csúcsain, és ez részcsoportja a G-nek. Válasszuk a gráf egy tetszőleges csúcsát a csoport egységelemének. Ennek a csúcsnak a szomszédai lesznek S elemei.

2.12. Állítás. *Egy G csoport Cayley-gráfjai pontosan azok, amiknek az automorfizmus csoportjában van reguláris H-val izomorf részcsoport.*

Ebből az is látszik, hogy egy gráfra a csúcstranzitivitás nem elegendő kitétel ahhoz, hogy Cayley-gráf legyen. Erre a legkisebb elemszámú példa a Petersen-gráf.

Érdekes kérdés, hogy mely $S \subset H$ halmazokra teljesül, hogy $\langle S \rangle = H$. Sok esetben erre elég jó válasszal tudunk szolgálni. Például John D. Dixon eredménye [7], hogy majdnem minden permutáció pár generálja S_n-t vagy A_n-t.

2.13. Tétel. (Dixon) *Legyen a (g, h), $g, h \in S_n$ rendezett pár. Legyen ekkor az $A = \{(g, h) \in S_n^2 | \langle (g, h) \rangle = S_n$ vagy $A_n\}$.*

$$\frac{|A|}{|S_n|^2} \geq 1 - \frac{2}{(\log \log n)^2}$$

megfelelően nagy n-re

Mivel $\langle (g, h) \rangle = A_n$ akkor és csak akkor ha g, h páros permutációk. Mivel S_n-ben a permutációknak a fele páros a tételből azonnal következik az alábbi állítás:

2.14. Következmény. Használjuk az előző tétel jelöléseit. Ekkor:

$$\lim_{t \to 0} P(\langle g, h \rangle = A_n) = \frac{1}{4}$$

$$\lim_{t \to 0} P(\langle g, h \rangle = S_n) = \frac{3}{4}$$

A továbbiakban feltételezzük hogy:

- S zárt az inverz képzésre, így csak irányítatlan gráfokkal foglalkozunk
- $H = \langle S \rangle$, tehát a gráf összefüggő
- $1 \notin S$, azaz nincsenek hurokélek

így egy $|S|$-reguláris összefüggő irányítatlan gráfot kapunk. Természetesen felmerül a kérdés, hogy egy adott H csoport mely S részhalmazaira lesznek a Cayley-gráfok izomorfak, illetve milyen csoportoknak vannak olyan részhalmazai amire a gráfok izomorfak. Ezzel a következőkben nem foglalkozunk.

Cayley-gráfok alkalmazásaiban, például CPU hálózatoknál, — ahol szeretnénk hogy az egyes CPU-k, memória modulok ne legyenek túl messze egymástól, — fontos kérdés, hogy két csúcs között mi a lehető legnagyobb távolság. Ugyanez a szám a Rubik-kocka Cayley-gráfjál megadja legfeljebb hány forgatás kell a kocka kirakásához.

2.15. Definíció. *$G = (V, E)$ gráf, legyen g,h $\in$ V-re $d(g, h)$ legyen az őket összekötő legrövidebb út élszáma. Ekkor* $\operatorname{diam}(G) := max_{g,h \in V} d(g, h)$

Even és Goldreich bebizonyították [3], hogy egy Cayley-gáf átmérőjének kiszámítása NP-nehéz, még abban az egyszerű esetben is, ha a csoport kommutatív és minden elemének a rendje kettő. Hasonlóan nehéz feladat egy permutációcsoport irányított Cayley-gáfjában két pont távolségét meghatározni, erről Mark R. Jerrum mutatta meg, hogy PSPACE-teljes [9]. Ezért és mert az alkalmazásokban általában arra van szükség, hogy az átmérő kicsi legyen, a továbbiakban csak azzal foglalkozunk, hogy felső korlátot adjunk az átmérőre.

A probléma, hogy olyan S-t találjunk, amire $\operatorname{diam}(\operatorname{Cay}(H, S))$ kicsi, természetesen csak $|S|$ elemszámának korlátozásával érdekes. Különben tetszőleges csoportra és $S = H$-ra $\operatorname{diam}(\operatorname{Cay}(H, S)) = 1$, azaz a gráf fokszámának növelésével természetesen csökken a gráf átmérője. Ha S speciális tulajdonságú, szintén igaz, hogy a Cayley-gráf átmérője kicsi:

2.16. Állítás. *Ha G csoport és $H < G$ legyen $S := G - H$. Ekkor:*

$$\operatorname{diam}(\operatorname{Cay}(G, S)) = \begin{cases} 1 & ha\ H = \{1\} \\ 2 & ha\ H \neq \{1\} \end{cases}$$

Bizonyítás. Először legyen $H = \{1\}$, ekkor $\mathrm{Cay}(G, S) = K_{|G|}$ teljes gráf, hiszen csak a hurokéleknek megfelelő egységelemet hagytuk el.

Most tekintsük a $H \neq \{1\}$ esetet. Legyen $a, b \in G - H$ két tetszőleges elem. Ekkor mivel a és b is szomszédos 1-gyel a gráfban, tehát $d(a, b) \leq 2$. Ha az egyik elem H-ban van, de a másik H-n kívül, akkor szomszédosak. Mivel $H \neq \{1\}$, $|H| \geq 2$ így tetszőlges $c, d \in H$-ra és $x \in G-H$-ra $x^{-1}c$, $x^{-1}d \in G-H$ így x szomszédos c-vel és d-val a gráfban. Viszont c, d nem szomszédosak egymással mert $c^{-1}d$, $c^{-1}d \in H$, tehát $d(c, d) = 2$. Így $\mathrm{diam}(\mathrm{Cay}(G, G - H) = 2$. □

Mikor az S generáló halmaz elemeit véletlenül választjuk, szintén adhatunk felső becslést az átmérőre:

2.17. Tétel. *[8] Legyen a $G = S_n$ és $S = \{g, h, g^{-1}, h^{-1}\}$, ahol g, h az S_n elemei. A g és h elemeket egyenletes eloszlásból, függetlenül választjuk. Legyen $H = \langle g, h \rangle$, ekkor $1 - \epsilon$ valószínűséggel $\mathrm{Cay}(H, S)$ átmérője $\mathcal{O}(n^2 \log^c n)$-ben van. A c konstans nem függ ϵ-tól.*

2.2. Cayley gráfok optimális átmérője

Ebben a fejezetben azzal foglalkozunk, hogy bizonyos csoportokra olyan generáló részhalmazt adjunk meg amire a kapott Cayley gráf átmérője és $|S|$ is kicsi. Az átmérő helyett egy másik, de azzal ekvivalens tulajdonságot fogunk használni.

2.18. Definíció. *Egy $g \in H$ csoportelem S-hossza legyen az a minimális d szám, amire $g = s_1 s_2 ... s_d$, ahol $s_i \in S$. Az S-beli elemek ilyen szorzatát a következőkben egy S-feletti szónak, vagy csak szónak fogjuk nevezni.* $\mathrm{L}(\mathrm{Cay}(H, S))$ *legyen a legkisebb $l \in \mathbb{N}$, hogy minden $g \in H$ előáll legfeljebb l darab S-beli elem szorzataként. A továbbiakban, ha S egyértlemű akkor S-hossz helyett csak hosszt fogunk használni.*

2.19. Állítás. $\mathrm{L}(\mathrm{Cay}(H, S)) = \mathrm{diam}(\mathrm{Cay}(H, S))$

Bizonyítás. A $g, h \in V$ közötti legrövidebb utat úgy kaphatjuk meg, hogy vesszük, $g^{-1}h$ egy minimális S-hosszú felbontását $g^{-1}h = s_1 s_2 ... s_d$ és g-ből indulva végigmegyünk az $s_1, s_2, ..., s_d$ elemeknek megfelelő éleken. Így egy d-hosszú úton h-ba jutunk. □

A Cayley-gráfok említett két alkalmazásánál nyilván egy ilyen utat is szeretnénk találni két csúcs között. Így tudnánk kirakni a Rubik kockát, vagy így tudna egymással kommunikálni egy számítógép hálózat két eleme. Természetesen szeretnénk,

hogy az algoritmus ami megadja ezt az utat ne legyen túl bonyolult, már csak azért sem mert nem szerencsés, ha például a számítógépünk erőforrásainak nagy részét az veszi el, hogy a hálózat különböző elemei egymással kommunikálnak.

Érdemes megjegyezni, hogy egy számítógép hálózat elrendezésének miért célszerű egy Cayley-gráfot választani. Fontos érv, hogy olyan gráfot szeretnénk ahol a csúcsok távolsága egymástól ne legyen túl nagy, ugyanakkor fokszámuk szintén kicsi maradjon az elrendezés megvalósításának megkönnyítésére. Erről a következőkben megmutatjuk, hogy lehetséges. Ezenfelül a csúcstranzitivitás miatt nem kell foglalkoznunk azzal, hogy a gráf melyik pontjában vagyunk éppen, tehát egyféle útkereső algoritmus elegendő.

Az átmérőre a legegyszerűbb korlátot úgy kapjuk, ha az egységelemből indulva szélességi kereséssel bejárjuk a gráfot és összeszámoljuk, hogy az l-edik szintig hány csúcsot értünk már el: $1+s+s(s+1)+\ldots+s(s+1)^{l-2} = 1+s+\frac{(s-1)^{l-2}}{l-3}$, ahol $s = |S|$. Persze sok csúcsot is többször számolunk, így azt kapjuk, hogy $\mathrm{L}(\mathrm{Cay}(H,S)) \geq \log_{|S|-1}(|G|)$, hiszen minden csúcsból legfeljebb $|S|-1$ új csúcsba juthatunk el.

2.20. Tétel. (L. Babai — W. M. Kantor — A. Lubotsky [4]) *Létezik egy C konstans, hogy minden G nemkommutatív véges egyszerű csoportnak van egy S generátorrendszere, hogy $|S| \leq 7$ és* $\mathrm{diam}(\mathrm{Cay}(G,S)) \leq C \log |G|$

A tételt a $G = S_n$, A_n, $PSL(2,q)$, $PSL(n,q)$ esetekre bizonyítjuk.

2.21. Tétel. *S_n-nek van olyan két elemű S generátorrendszere, amire* $\mathrm{Cay}(S_n, S \cap S^{-1})$ *átmérője $\mathcal{O}(n \cdot \log(n))$.*

A tétel bizonyítása előtt megmutatjuk ugyanezt $|S| = 3$ esetén. $|S| = 2$-re nagyon hasonló lesz a bizonyítás, de három elemre sokkal egyszerűbb és természetesebb.

Legyen X egy n elemű halmaz, $\infty \in X$. Elég találni egy olyan S halmazt amire egy (x, ∞) permutáció hossza $\mathcal{O}(\log(n))$, és $X \setminus \{\infty, x\}$ elemei pedig elérhetőek x-ből $\mathcal{O}(\log(n))$ hosszú, ∞-t helyben hagyó w szavak segítségével.

Ekkor minden (∞, x) transzpozíció $\mathcal{O}(\log(n))$ hosszú, hisz egyszerűen az elemek összeszorzásából látszik, hogy

$$(\infty, x)^w = (\infty, x^w) \tag{1}$$

ha w helyben hagyja ∞-t. Itt a bal oldalon konjugálás szerepel, a jobb oldalon pedig w hat az x-en.

Minden k-hosszú ciklus előáll k darab (∞, x) alakú transzpozíció szorzataként, ha ∞ benne van a ciklusban és $k+1$ szorzataként ha nincs:

$$(a_1, a_2, \ldots, a_k) = (\infty, a_1)(\infty, a_2)\ldots(\infty, a_k)(\infty, a_1),$$

így legfeljebb $\frac{3}{2}n$ transzpozíció szorzataként előáll minden permutáció. Ebből következik, hogy G minden elemének a hossza $\mathcal{O}(n \log n)$.

Először legyen n páros:

X-et azonosítsuk $\mathbb{Z}_{n-1} \cup \{\infty\}$-nel, és vegyük a következő két permutációt $b : x \mapsto 2x$ és $c : x \mapsto 2x+1$. Ezek ∞-t helyben hagyják. Kettes számrendszerben felírva $t \in \mathbb{Z}_{n-1}$-et látható, hogy minden $t \in \mathbb{Z}_{n-1}$ előáll:

$$t = \sum_{i=0}^{m} a_i 2^i = (...(a_m 2 + a_{m-1})2 + ...)2 + a_0 \tag{2}$$

alakban, ahol $a_i \in \{0, 1\}$ és $m = \lceil \log(n) \rceil$. Így $a_0 = b$ és $a_1 = c$ választással tetszőleges $t \in \mathbb{Z}_{n-1}$ felírható $t = 0^w$ alakban, ahol $0 \in X = \mathbb{Z}_{n-1} \cup \{\infty\}$. Itt $w \in \langle b, c \rangle$ és w szó $\{b, c\}$-hossza $m = \mathcal{O}(\log(n))$.

Ha n páratlan, válasszunk ki két (∞, ∞') elemet X-ből és feleltessük meg X-et $\mathbb{Z}_{n-2} \cup \{\infty, \infty'\}$-nek. A két permutáció b és c legyen ugyanaz mint az előbb. A generátorrendszer pedig: $S := \{(\infty, 0), (\infty, \infty')b, c\}$. Mivel b helyben hagyja a 0-t, a ∞-t és a ∞'-t, ezért felcserélhető a (∞, ∞') és $(\infty, 0)$ involúciókkal. Így a $(\infty', 0)$ permutációt megkapjuk a következő alakban:

$$(\infty, 0)^{(\infty,\infty')b} = (\infty, \infty')b(\infty, 0)(\infty, \infty')b^{-1} = (\infty', 0) \tag{3}$$

Hasonlóan $(\infty, \infty') = (\infty, 0)^{(\infty', 0)}$. Mindkettő S-hossza konstans, tehát eltekinthetünk tőle. Ezek után (∞, t) transzpozíciót, ugyanúgy mint az előbb megkaphatjuk a Horner-elrendezés segítségével, minden $t \in \mathbb{Z}_{n-2}$-re. Ezzel beláttuk, hogy minden n-re konstruálható három elemű generátorrendszere S_n-nek, amire $\mathcal{O}(\log(n))$ az átmérője az ehhez tartozó Cayley gráfnak.

2.22. Megjegyzés. Ahhoz hogy áttérjünk 2 generátorra, a következő gondolatmenetet szeretnénk alkalmazni. A korábban definiált b helyben hagyja 0-t és ∞-t. Ebből azt kapjuk, hogy $((\infty, 0)b)^2 = b^2$. Ha b rendje $\mathcal{O}(\log(n))$-es és páros, akkor $(\infty, 0)$ előáll $(\infty, 0)b$ hatványaként. Ekkor $S = \{(\infty, 0)b, c\}$ választásával alkalmazhatnánk az előző módszert. Sajnos b nem teljesíti a fenti két kritériumot, ezért egy kicsit változtatnunk kell a konstrukción.

Bizonyítás. Feltehetjük, hogy $n \geq 2^{11}$. Legyen $l \geq 7$ olyan, hogy $(12, l) = 1$ és $2^{l+10} \geq n \geq 2^{l+4}$. Osszuk fel az n elemű X-et 13 diszjunkt $X_1, X_2, ..., X_{12}, E$ részhalmazra úgy, hogy $|X_i| = 2^l - 1$ minden $1 \leq i \leq 12$ esetén. Ekkor próbálgatással-et úgy választottuk, hogy teljesüljön a következő:

$$100 + \frac{|E|}{100} < |X_2 \cup X_3 \cup \ldots \cup X_{12}| \tag{4}$$

Legyen ∞ az E egy eleme. Feleltessük meg X_1-et $\mathbb{Z}_{2^l-1}$-nek. Legyen $b_1 : x \mapsto 2x$ és $c : x \mapsto 2x + 1$ az X_1-halmazon. Mivel 1 pályája b-vel l-hosszú, és c a b-nek az $x \mapsto x - 1$ -el vett konjugáltja, $(2(x + 1) - 1 = 2x + 1,)$ így $|b|, |c| = l$. Mivel -et úgy válaszotottuk, hogy páratlan legyen és $\log(n)$ nagyságrendű. Legyen $\overline{b}_1$ olyan, hogy $\overline{b}_1^{12} = b_1$ az X_1-en és máshol legyen az identitás. Mivel $l = |b_1|$-re $(l, 12) = 1$, a tizenkettedik hatványra emelés bijekció, így létezik ilyen $\overline{b}_1$ sőt $\overline{b}_1 = b_1^k$ valamilyen k-ra, tehát $|\overline{b}_1| = l$ szintén igaz.

Legyen f olyan diszjunkt 101-hosszú ciklusok szorzata amiknek a tartója $(E \setminus \{\infty\}) \cup X_2 \cup \ldots \cup X_{12}$-ben vannak, és lefedik $E \setminus \{\infty\}$-t. Mivel a 4 Tétel teljesül, f-et megkonstruálhatjuk úgy, hogy kiválasztunk 100 elemet E-ből egyet pedig $X_2 \cup X_3 \cup \ldots \cup X_{12}$-ből, majd ezek elhagyásával ezt ismételjük, amíg E-nek van 100 eleme. Mikor $|E| < 100$ kiválasztjuk az összes elmét a 101-hosszú ciklus többi elemét pedig az $X_2 \cup X_3 \cup \ldots \cup X_{12}$-ből.

A két permutáció a következő:

- $b = (\infty, 0) f \overline{b}_1$
- c egy 12-hosszú ciklus $(X_1, X_2, \ldots, X_1 2)$, $c^{12} = c_1$ az X_1 halmazon és c az identitás E-n

Vegyük észre, hogy $\langle b^{12}, c^{12} \rangle = \langle b_1, c_1 \rangle$ X_1-en ugyanolyan tulajdonságú mint az első konstrukcióban $\langle b, c \rangle$ volt. Legyen tehát $S = \{b, c\}$. Mint az előbb most is elegendő megmutatni, hogy minden (∞, x), $x \in X \setminus \{\infty\}$ transzpozíció S-hossza $\mathcal{O}(\log(n))$.

Először megjegyezzük, hogy $b^{101l} = (\infty, 0)$ mivel $101l$ páratlan, $|\overline{b_1}| = l$ és $|f| = 101$. Így $(\infty, 0)$ hossza $\mathcal{O}(\log(n))$. Mint a három-generátoros esetben minden (∞, x_1), $x_1 \in X_1$ transzpozícióról megkapjuk, hogy $\langle b^{12}, c^{12} \rangle$ beli elemekkel konjugálva, $\mathcal{O}(\log(n))$ hosszú. Ezekután c-vel konjugálva minden (∞, x), $x \in X_2 \cup X_3 \cup \ldots \cup X_{12}$ transzpozícióra kapjuk, hogy $\mathcal{O}(\log(n))$ hosszú, mivel c hossza konstans 12.

Végül b^i-vel konjugálva, ahol $1 \leq i \leq 100$, megkapjuk az összes (∞, e), $e \in E \setminus \{\infty\}$. $\square$

2.23. Tétel. (L. Babai — W. M. Kantor — A. Lubotsky) *Az A_n-nek van olyan kételemű, S generáló részhalmaza, amire* $\mathrm{diam}(\mathrm{Cay}(A_n, S)) \in \mathcal{O}(n \log(n))$

Bizonyítás. Legyenek $l, X_1, X_2, ..., X_{12}, E$ és $\bar{b}_1$ mint az előző bizonyításban. Legyen ∞, ∞' az E két eleme. Legyen f olyan, mit előbb, de most $\mathrm{supp}(f) := (E \setminus \{\infty, \infty'\}) \cup X_2 \cup X_3 \cup \ldots \cup X_{12}$ és fedje $E \setminus \{\infty, \infty'\}$-t. Ekkor $b = (\infty, \infty', 0) f \bar{b}_1$ és c ugyanolyan mint az előbb azzal a különbséggel, hogy felcseréli ∞-t és ∞'-t.

Megjegyezzük, hogy $b, c \in A_n$, mivel $|b|$ páratlan, és c megszorítva $X_1 \cup X_2 \cup \ldots \cup X_{12}$-re páratlan és (∞, ∞') is páratlan permutáció.

Azt állítjuk, hogy ekkor $\mathrm{diam}(\mathrm{Cay}(A_n, \{b, c\})) = \mathcal{O}(n \cdot \log(n))$. Valóban, mert $b^l = (\infty, \infty', 0)^{\pm 1}$, mivel $|f| = 101$, $|\bar{b}_1| = l$ és $3 \nmid 101, l$, így $(\infty, \infty, 0)$ hossza $\mathcal{O}(\log(n))$. Mivel a 3-hosszú ciklusok generálják A_n-t méghozzá $\mathcal{O}(n)$ átmérővel, sőt akkor is ha a ciklus 2 eleme fix, elég ha a $(\infty, \infty 1, z)$, ahol $z \in X \setminus \{\infty, \infty'\}$ permutációkat előállítjuk.

Hasonlóan az előző bizonyításhoz, $(\infty, \infty', 0)$-t b_1, c_1-el megfelelő sorrendben konjugálva, megkapunk minden (∞, ∞', x_1) alakú ciklust, ahol $x_1 \in X_1$. Ezután c-vel konjugálva megkapjuk a (∞, ∞', x) alakúakat, ahol $x \in X_1 \cup X_2 \ldots \cup X_{12}$. Végül b^i-vel konjugálva megkapunk minden (∞, ∞', e) ciklust, ahol $e \in E$. $\square$

Mielőtt belátjuk a tételt $PSL(2, q)$-ra, és $PSL(n, q)$-ra, (ahol q prímhatvány,) bevezetünk pár jelölést, amiket használni fogunk majd a bizonyításokban.

$x(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ ha $t \in \mathbb{F}_q$, $h(b) = \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix}$ ha $b \neq 0$, $r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Ekkor $x(t+u) = x(t)x(u)$, $x(t)^{h(b)} = x(tb^2)$ és $H = \{h(b) | b \neq 0\}$, ami egy ciklikus csoport.

2.24. Tétel. *Legyen $G = PSL(2, q)$, vagy $SL(2, q)$*

(a) Legyen q páratlan prímszám. Ekkor $\mathrm{diam}(\mathrm{Cay}(G, S)) = \mathcal{O} \log(|G|)$*, ahol* $S = \left\{x(1), h(\frac{1}{2})r, x(1)^{-1}, h(\frac{1}{2})r^{-1}\right\}$.

(b) Minden q-ra, ha θ egy primitív eleme az $\mathbb{F}_p \leq \mathbb{F}_q$ bővítésnek, azaz generálja az $\mathbb{F}_q$ multiplikatív csoportját, akkor akkor $\mathrm{diam}(\mathrm{Cay}(G, S)) = \mathcal{O} \log(|G|)$*, ahol $S = \{x(1), h(1/2)r, h(\theta)\}$, ha q páratlan és $S = \{x(1), r, h(\theta)\}$, ha q páros*

Bizonyítás. Ha $ad - bc = 1$ akkor $c \neq 0$ -ra egyszerű számolással kapjuk, hogy

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = x(-c^{-1} + ac^{-1})x(-c)^r x(-c^{-1} + dc^{-1}). \tag{5}$$

Abban az esetben mikor $c = 0$, állítsuk elő rg-t g helyett. Így már elég megmutatnunk, hogy $x(a)$ S-hossza minden $a \in \mathbb{F}_q$ esetén „elég" kicsi. Ha $q = p$ egy páratlan prím legyen $\theta = 2$. Ha pedig $q > p$, akkor θ legyen a $\mathbb{F}_p \leq \mathbb{F}_q$ bővítés egy primitív eleme. Minden $t \in \mathbb{F}_q$ felírható:

$$t = \sum_{i=0}^{m} a_i \theta^{2i} = (...(a_m \theta^2 + a_{m-1})\theta^2 + ...)\theta^2 + a_0 \tag{6}$$

Ha $q = p$, $m + 1 \leq \frac{1}{2}\log(q)_4$, $a_i \in \{0, 1, 2, 3\}$, ha $q \geq p$, $m \leq \log_p(q)$, $a_i \in \mathbb{F}_p$. A $q = p$ eset: Feltehetjük, hogy $p > 2$ ugyanis $p = 2$ esetén $SL(2, 2)$-t generálja $\{x(1), r\}$. Vezessük be a $r' = h(\frac{1}{2})r$ jelölést. A következő egyenlőséget mátrixszorzással kapjuk: $x(1)^{-2}(x(1)^2)^{r'}x(1)(x(1)^{-4})^{r'} = h(2)^{-1}$. Így látható, hogy $h(2)^{-1}$ S-hossza legfeljebb 13. A már említett szorzási szabályokból és a Horner-elrendezésből következik az alábbi:

$$x(t) = (...(x(a_m)^{h(2)}x(a_{m-1}))^{h(2)}...)^{h(2)}x(a_0) \tag{7}$$

Mivel itt minden $0 \leq i \leq m$-re a_i hossza legfeljebb 3 és $h(2)$-é legfeljebb 13, azt kapjuk, hogy $x(t)$ hossza $\mathcal{O}(\log(p))$. Mivel már tetszőleges mátrixot előállítottunk $\mathcal{O}(1)$ darab $x(t)$-ből, készen vagyunk.

Ha $q > p$: Mint az előbb, minden $t \in \mathbb{F}_q$ előáll mint:

$$x(t) = (...(x(a_m)^{h(2)}x(a_{m-1}))^{h(2)}...)^{h(2)}x(a_0)$$

ahol $x(a_i)$-k $a_i \in \mathbb{F}_p$ száma $m + 1$, $h(\theta)$-k és $h(\theta)^{-1}$-k száma pedig összesen $2m$. Már beláttuk, hogy $x(a_i)$-k hossza $\mathcal{O}(\log(n))$, tehát $x(t)$ hossza $m\mathcal{O}(\log(p)) = \mathcal{O}(m \cdot \log(p)) = \mathcal{O}(\log(q)) = \mathcal{O}(\log(|G|))$. Újra a (5) azonosságot alkalmazva a bizonyítás kész. □

2.25. Megjegyzés.

- A konstansok összeszámlálásával kapjuk, hogy az átmérő
  (a)-ban felülről becsülhető $45\log(|G|)$-vel
  (b)-ben $135\log(|G|)$-vel

- A bizonyítás egyben algoritmust is ad $PSL(2,q)$ vagy $SL(2,q)$ elemeinek $\mathcal{O}(\log(|G|))$ felírásában, $S \cup S^{-1}$ elemeiből. Ezt le is programoztam, ennek a dokumentációja a következő fejezetben található.

- M. Kassabov és T. R. Riley [11] belátták a tételt $|S| = 2$ esetén is. Ezt nem bizonyítjuk

2.26. Tétel. *(M. Kassabov — T. R. Riley) Minden $k \geq 2$ és $n \geq 3$ egész számra* $\operatorname{diam}(\operatorname{Cay}(SL_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\})) \leq 3600n^2 \log k$*, ahol*

$$\mathcal{A}_n = \begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \mathcal{B}_n = \begin{pmatrix} 0 & & 1 & & & \\ & & 0 & 1 & & \\ & & & 0 & \ddots & \\ & & & & \ddots & 1 \\ (-1)^{n-1} & & & & & 0 \end{pmatrix}$$

És létezik egy olyan algoritmus, ami egy $SL_n(\mathbb{Z}/k\mathbb{Z})$-beli mátrixot $\{\mathcal{A}_n, \mathcal{B}_n\}$ felett felbont egy $\mathcal{O}(\log|SL_n(\mathbb{Z}/k\mathbb{Z})|)$-hosszú szóra $\mathcal{O}(\log|SL_n(\mathbb{Z}/k\mathbb{Z})|)$-idő alatt.

2.27. Tétel. *$G = PSL(n,q)$ vagy $SL(n,q)$ $n \geq 3$ ekkor létezik olyan 4 elemű generátor rendszere, S amire* $\operatorname{diam}(\operatorname{Cay}(G,S)) = \mathcal{O}(\log(|G|))$

A bizonyítás előtt bevezetünk pár jelölést amit, majd használni fogunk. A köetkezőkben G-t úgy fogjuk elképzelni, hogy az elemei $n \times n$-es mátrixok, tehát a tételt $SL(n,q)$-ra fogjuk bizonyítani. A bizonyítás $PSL(n,q)$-ra annyiban tér el, hogy $SL(n,q)$ elemeit moduló az egység determinánsú skalármátrixok kell tekintani.

Legyen $q \leq i < j \leq n$-re X_{ij} az a csoport aminek az elemei olyan $n \times n$ mátrixok amiknek az átlójában egyesek, az (i,j) elemben az $\mathbb{F}_q$ test egy tetszőleges eleme, máshol pedig 0-k szerepelnek. A mátrixszorzás tulajdonságai miatt X_{ij} izomorf $\mathbb{F}_q$ additív csoportjával, $\mathbb{F}_q^+$-szal. Továbbá $U = \langle X_{ij} | 1 \leq i < j \leq n \rangle$ egy p-Sylow részcsoportja G-nek. Egyrészt felsőháromszög mátrixokból áll, amik szorzata és inverze szintén ilyen alakú másrészt $|U| = q^{\frac{1}{2}n(n-1)}$. Ezenkívül $U = \prod_{1 \leq i < j \leq n} X_{ij}$ a tényezőket teszőleges sorrendben írva, szintén a mátrixszorzás szabályai miatt.

Ha $\mathbb{F}_q^n$-ben a szokásos bázis $e_1, e_2, \ldots, e_n$, akkor r_i $1 \leq i < n$ legyen az következő transzformáció: $e_i \mapsto e_{i+1} \mapsto -e_i$ a bázis többi elemét pedig nem változtatja meg, mátrixszal például:

$$r_1 = \begin{pmatrix} 0 & 1 & & \\ -1 & 0 & & \\ & & \ddots & \end{pmatrix}$$

Legyen $h_i(t) = diag(1, 1, \ldots, t, t^{-1}, \ldots, 1)$, ahol t^{-1} az i-edik elem és $e_1, e_2, \ldots, e_n$. Legyen $H_i = \langle h_i(t) | t \in \mathbb{F}_q^\times \rangle$ minden $1 \leq i \leq n-1$-re akkor $H = \prod_i H_i$ a G beli diagonális mátrixok részcsoportja. Ezenkívül $L_{i,i+1} := \langle X_{i,i+1}, r_i \rangle \cong SL(2,q)$ és $L_{i,i+1} \cap H = H_i$. Ha $B :=$ ⟨felsőháromszög mátrixok részcsoportja, akkor az U csoport korábbi leírásából jól látható, hogy ⟩, akkor $B = UH = HU$. Sőt, $U \lhd B$, ugyanis a felsőháromszög mátrixok főátlóbeli elemeit egymással kell szorozni csak, így egyszerűen adódik, hogy $h(t)^{-1}Uh(t) = U$ minden $h(t) \in H$.

Legyen $N := \langle H, r_i | 1 \leq i < n \rangle$ a G beli monomiális mátrixok csoportja, azaz olyan mátrixok által alkotott csoport, aminek minden sorában és oszlopában egy nem nulla elem áll. Ezeknek a csoportoknak a leírásából az is látszik, hogy $H \lhd N$ mert diagonális mátrixszal ha szorzunk akkor csak a sorok vagy az oszlopok szorzódnak a diagonális mátrix megfelelő elemével mivel $t \neq 0$ elemek nem nullázódnak ki. $N/H \cong S_n$ és itt r_i felel meg az $(i, i+1)$ transzpozíciónak.

2.28. Állítás. (Bruhat-felbontás) *A $G = SL(n,q)$ felírható a következő alakban:*

$$G = BNB = \coprod_{n \in N} BnB$$

ahol B és N a korábban definiált csoportok. Ezt a csoport Bruhat-felbontásának nevezzük.

Ezt az állítást nem bizonyítjuk, és a felbontásban szereplő csoportok tuljadonságaira sem térünk ki, mert nagyon hosszú és bonyolult lenne, viszont a bizonyításban csak a felbontás létezését használjuk majd.

Bizonyítás. S elemei a következőek lesznek: $s \in N$ legyen olyan, hogy az $N/H \cong S_n$ izomorfizmusnál a képe egy n-hosszú ciklus valamint L_{12} () tételben definiált 3 elemű generátorrendszere. Vegyük észre, hogy $r' = h(\frac{1}{2})r_1$ vagy r_1 képe ugyanennél az izomorfizmusnál az $(1,2)$. Mivel úgy választjuk s-et hogy a képe az $(1, 2, \ldots, n)$ ciklus legyen akkor $z := sr'$ képe $(2, 3, \ldots, n)$.

Először megmutatjuk, hogy U minden elemének S-hossza $\mathcal{O}(\log(|G|))$. Rendezzük az X_{ij} csoportokat a következőképpen: $U = \prod_{i=1}^{n} \prod_{k=0}^{n-i-1} X_{i,i+k+1}$. Ekkor $U \subseteq YY^sY^{s^2} \dots Y^{s^{n-1}}$, ahol $Y = X_{1,2}X_{1,2}^zX_{1,2}^{z^2} \dots X_{1,2}^{z^{n-2}}$. $X_{1,2}$ minden eleme $\mathcal{O}(\log(q))$ hosszú az () tétel alapján. Ebből következik, hogy Y elemei $\mathcal{O}(n \cdot \log(q))$, U elemei pedig $\mathcal{O}(n \cdot n \cdot \log(q)) = \mathcal{O}(\log(|G|))$.

Most vizsgáljuk meg a H csoportot. Tudjuk, hogy H Abel-csoport. A H_i csoporok $SL(2,q)$-val izomorfak, így zintén az előző tételből következik, hogy H_1 minden eleme $\mathcal{O}(\log(q))$ hosszú. H_i és s definíciójából következik, hogy $H_i = H_1^{s^i}$, tehát H minden eleme $\mathcal{O}(n \cdot \log(q))$ Ebből következik, hogy $B = UH$ elemeinek hossza is $\mathcal{O}(\log(|G|))$.

Mivel tudjuk, hogy $SL(n,q)$ Bruhat-felbontása $G = BNB$, ahol $B = UH$ miatt $BNB = UHNHU = UNU$ az N definíciója miatt. Mivel r_1 és s generálja S_n-t, $Hr' = Hr_1$ és Hs generálják $N/H \cong S_n$-t. Mivel S_n-nek ez a két elem $\mathcal{O}(n^2)$ átmérőjét adja, minden Hg, $g \in N$ mellékoksztály S-hossza $\mathcal{O}(n^2)$, tehát G minden elemére beláttuk az állítást. □

2.3. Cayley gráfok átmérője tetszőleges generátorhalmaz mellett

Eddig egy $\Gamma = \mathrm{Cay}(G,S)$ gráf átmérőjét a hagyományos, gráf értelemben vizsgáltuk, azaz egy adott S halmazra nézve. Egy másik megközelítés, hogy minden S generátorrendszerre amire Γ összefüggő kiszámoljuk az átmérőt majd vesszük ezeknek a maximumát.

2.29. Definíció. *Egy $\Gamma = \mathrm{Cay}(G,S)$ gráf legrosszabb átmérőjén, az összes generátor halmaz mellett felvett átmérők maximumát értjük. Formálisam megfogalmazva a* $\max_{S \subseteq G}\{\mathrm{diam}(\mathrm{Cay}(G,S))\}$ *számot.*

2.30. Definíció. *Egy $\Gamma = \mathrm{Cay}(G,S)$ gráf egy legrosszabb generátorrendszere az az $S \subseteq$ halmaz amire a* $\mathrm{diam}(\mathrm{Cay}(G,S))$ *érték maximális.*

Ebben a fejezetben azzal foglalkozunk, hogy felső korlátot adjunk az átmérőre tetszőleges generátorrendszer esetén is. Az egyetlen megszorítás amit tenni fogunk, hogy a generátorrendszernek legyen egy olyan eleme ami az alaphalmaz elemeinek legalább 67%-át helyben hagyja.

A bizonyításban véletlen sétákat fogunk használni, valamint egy becslést Markov-láncok elérési idejéről. Először az ezekhez kapcsolódó alapvető, és a következőkben szükséges definíciókat, tételeket fogunk belátni.

2.31. Definíció. *Legyen $G = (V, E)$ összefüggő gráf, $V = \{v_1, v_2, \dots v_n\}$. Jelöljük a $v_i \in V$ csúcs fokszámát $d(v_i)$ − vel. Ekkor az $u_0, u_1, \dots\ u_i \in V$ csúcsok által meghatározott sétát véletlen sétának nevezzük, ha a k-adik lépésben u_{k-1}-ből $\frac{1}{d(u_{k-1})}$ valószínűséggel lépünk u_{k-1} egy szomszédjába. A séta k-adik elemét u^k-val fogjuk jelölni. Legyen σ^0 egy adott kezdeti eloszlás V-n. Ekkor jelöljük u^k eloszlását σ^k-val. A legtöbb esetben a σ^0 eloszlásunk úgy fog kinézni, hogy 1 valószínűséggel vagyunk u^0-ban és 0 valószínűséggel a többi pontban. Az u^0 csúcs a séta kezdőpontja.*

2.32. Definíció. *Markov-láncnak nevezzük $X_1, X_2, \dots$ valószínűségi változók sorozatát, ha a következő teljesül:*

$$P(X_{n+1} = x | X_n = x_n, X_{n-1} = x_{n-1}, \dots, X_1 = x_1) = P(X_{n+1} = x | X_n = x_n)$$

Ez szavakkal megfogalmazva azt jelenti, hogy a sorozat $n+1$-edik eleme csak az n-ediktől függ. Az X_i-k értékkészletének unióját állapothalmaznak nevezzük.

Egy véletlen séta a $G = (V, E)$ gráfon megfeleltethető egy Markov-láncnak, ahol az állapothalmaz elemei a gráf csúcsai, és $P(X_{k+1} = v_i)|X_k = v_k) = \frac{1}{d(v_i)}$, ha $(v_k, v_i) \in E$ és 0 különben.

2.33. Definíció. *Jelöljük p_{ij}-vel a valószínűségét annak, hogy a Markov-lánt v_i-ből a v_j-be lép. Ekkor a $P = \{p_{ij}\}$ mátrixot a Markov-folyamat átmenet mátrixának nevezzük. Itt p_{ii} annak a valószínűségét jelöli, hogy a folyamat a v_i csúcsban marad. A véletlen sétában az előző definíció alapján ez 0.*

Az átmenet mártixot a következőképpen is definiálhatjuk:

$$P = D^{-1}A, \text{ ahol } D = \begin{pmatrix} d(v_1) & 0 & \dots \\ 0 & d(v_2) & \dots \\ 0 & 0 & \ddots \end{pmatrix}$$

A pedig a mátrix adjacencia mátrixa.

2.34. Definíció. *Jelöljük a $G = (V, E)$ gráf adjacencia mátrixát A-val. Legyen a mátrix legnagyobb sajátértéke d, és $D = diag(d, d, \dots, d) \in \mathbb{R}^{n \times n}$. Az $\hat{A} = D^{-1}A$ mátrixot a G normalizált adjacencia mátrixának nevezzük. Reguláris gráfokra ez megegyezik az átmenet mátrixszal.*

2.35. Megjegyzés. Az A mátrixról tudjuk, hogy szimmetrikus, definiáljuk a következő, mátrixot: $N = D^{-1/2}AD^{-1/2}$. Mivel D diagonális, N-is szimmetrikus és $P = D^{-1/2}ND^{1/2}$, tehát P és N sajátértékei megegyeznek. Mivel N szimmetrikus ezek a sajátértékek valósak.

A fenti definíciókból következik, hogy $\sigma^k = \sigma^{k-1}P = \ldots = \sigma^0 P^k$

2.36. Definíció. *A π eloszlást stacionáriusnak nevezzük, ha $\pi = \pi P$. Azaz π a P bal oldali sajátvektora,* 1 *sajátértékkel.*

2.37. Állítás. *Legyen $G = (V, E)$ tetszőleges, $m = |E|$. Ekkor a $\pi(v) = \frac{d(v)}{2m}$ a stacionáris eloszlás G-n.*

Bizonyítás. A 2.33 definíció alapján felírhatjuk a P mátrixot, $P = D^{-1}A$ alakban. Ezután csak összeszorozzuk a mátrixokat, és kihasználjuk, hogy A egy sorában pontosan fokszámnyi egyes van.

$$\pi D^{-1}A = \begin{pmatrix} \frac{d(v_1)}{2m} \\ \vdots \\ \frac{d(v_n)}{2m} \end{pmatrix}^T \begin{pmatrix} \frac{1}{d(v_1)} & & \\ & \ddots & \\ & & \frac{1}{d(v_n)} \end{pmatrix}^T A = \begin{pmatrix} \frac{1}{2m} \\ \ddots \\ \frac{1}{2m} \end{pmatrix} A = \pi$$

□

Érdemes megjegyezni, hogy mi Cayley-gáfokon fogjuk használni a definíciót. Mivel a Cayley-gráfok $|S|$-regulárisak, minden $v_i \in V$-re $\pi(v_i) = \frac{|S|}{|V|}$. Tehát a stacionárius eloszlás megegyezik a V-n vett egyenletes eloszlással.

2.38. Lemma. *Legyenek $1 = \lambda_1, \lambda_2, \ldots, \lambda_n$ a P sajátértékei. Ekkor az 1.2 tételből következik, hogy $\lambda_i < 1$ minden $2 \leq i \leq n$ esetén, ha a gráf amin a véletlen séta átmenetmátrixa P összefüggő.*

2.39. Tétel. *Ha G egy összefüggő és nem páros gráf, akkor $\sigma_k \to \pi$, ha $k \to \infty$ minden σ kezdeti eloszlás esetén.*

Mivel a tétel bizonyításában és általánosan is nem csak a konvergencia ténye, hanem sebessége is fontos a tételt a következő formában fogjuk belátni.

2.40. Tétel. *Legyenek a P egy véletlen séta átmenet mártixa, egy nem páros gráfon. Sajátértékeit jelöljük $\lambda_1, \geq \lambda_2 \geq \ldots \geq \lambda_n$-vel. Legyen $\mu = \max\{|\lambda_2|, |\lambda_n|\}$. Ekkor egy v_i kezdőpontra és tetszőleges $v_j \in V$-re:*

$$|P(u^k = v_j) - \pi(j)| \leq \mu^k \sqrt{\frac{\pi(j)}{\pi(i)}} \tag{8}$$

Bizonyítás. Az N mátrix sajátértékei megegyeznek a P sajátértékeivel. Tudjuk, hogy N szimmetrikus. Ebből következik, hogy van sajátvektorokból álló ortonormált bázisa: $b_1, b_2, \ldots b_n$. Ezért N felírható a következő alakban:

$$N = \sum_{l=1}^{n} \lambda_l b_l b_l^T \tag{9}$$

Mivel π a P sajátvektora választhatjuk úgy a b_i vektorokat, hogy $b_{1,i} = \sqrt{\pi_i}$ teljesüljön.

$$\begin{aligned}
P(u^k = v_j) &= (P^k)_{ij} && P^k\text{-ban ez egy } i \rightsquigarrow j \text{ útnak felel meg} \\
&= e_i^T D^{-1/2} N^k D^{1/2} e_j && N \text{ definíciója szerint} \\
&= \sum_{l=1}^{n} e_i^T D^{-1/2} \lambda_l^k b_l b_l^T D^{1/2} e_j && N\text{-et felbontjuk a (4) képlet szerint} \\
& && \text{használjuk: } b_i \text{ egy hosszú sajátvektorok} \\
&= \sum_{l=1}^{n} \lambda_l^k (e_i^T D^{-1/2} b_l)(e_j^T D^{1/2} b_l) && b_l^T D^{1/2} e_j \text{ egy szám} \\
& && \text{tehát vehetjük a transzponáltját,} \\
&= \sum_{l=1}^{n} \lambda_l^k \frac{1}{\sqrt{\pi(i)}} b_{li} \sqrt{\pi(j)} b_{lj} && D^{1/2}\text{-ben a fokszámok gyökei vannak} \\
&= \pi(j) + \frac{\sqrt{\pi(j)}}{\sqrt{\pi(i)}} \sum_{l=2}^{n} \lambda_l^k b_{li} b_{lj} && b_1\text{-et így választottuk}
\end{aligned}$$

Az összeg első tényezője a határérték, most a szummás tagot fogjuk felülről becsülni.

$$
\begin{aligned}
\left|\sum_{l=2}^{n} \lambda b_{li} b_{lj}\right| &\leq \sum_{l=2}^{n} |\lambda b_{li} b_{lj}| && \text{a háromszögegyenlőtlenség} \\
&\leq \mu^k \sum_{l=2}^{n} |b_{li} b_{lj}| && \text{ebben nem szerepelt } b_1 \\
&\leq \mu^k \sum_{l=1}^{n} |b_{li} b_{lj}| && \text{egy pozitív tagot adtunk hozzá} \\
&\leq \mu^k \left(\sum_{l=1}^{n} b_{li}^2\right)^{1/2} \left(\sum_{l=1}^{n} b_{lj}^2\right)^{1/2} && \text{Cauchy—Schwarz-egyenlőtlenség} \\
&\leq \mu^k && \text{A } b_l\text{-ek normáltak}
\end{aligned}
$$

Ebből következik, hogy:

$$\left|P(u^k = v_j) - \pi(j)\right| \leq \mu^k \sqrt{\frac{\pi(j)}{\pi(i)}}$$

□

A tétel egyik fontos alkalmazása, hogy lehetővé teszi, hogy elemeket válasszunk ki egy hamazból egyenletes eloszlás szerint. Annyit kell tennünk, hogy megkonstruálunk egy gráfot a halmaz elemeiből, majd ezen elindítunk egy véletlen sétát egy tetszőleges pontból. Megfelelő lépésszám után a csúcsok eloszlása tetszőlegesen kövel lesz az egyenletes eloszláshoz.

Elsőre meglepő, hogy szükség van egyáltalán olyan, nem triviális módszerre, amivel egyenletesen választhatunk elemeket egy halmazból, de sokszor előfordul, hogy a halmaz túl nagy ahhoz, hogy ábrázoljuk. Egy jó példa a kártyakeverés, ami a véletlen séták egyik első alkalmazási területe volt. Ezt tekinthetjük úgy, hogy egy 52-elemű halmaz egy permutációját szeretnénk előállítani. Itt tehát a halmaz, amiből egyenletesen szeretnénk választani egy elemet 52! méretű. Sok esetben ez az egyetlen módszer az egyenletes eloszlás megvalósítására.

Az előző bekezdésben említett gráfot létrehozhatjuk, például egy Cayley gráfként. A kártyakeveréses példát megvalósíthatjuk úgy, hogy $S_{52} - t$ generáljuk a 2.21 tételben szereplő kételemű halmazzal.

Eddig a fejezetben az állítások csak akkor teljesültek, ha a gráf nem volt páros. Ez könnyen megmagyarázható, hiszen egy $G = (A, B; E)$ páros gráfban, ha $u^0 \in A$ akkor $u^{2k} \in A$ és $u^{2k+1} \in B$ minden k-ra. Ezt a problémát könnyen meg lehet oldani, ha bevezetünk egy új definíciót ami csak egy kicsit tér el a véletlen sétáétól.

2.41. Definíció. *Lusta véletlen sétának nevezünk egy sétát az adott gáfon, ha minden lépésben $\frac{1}{2}$ valószínűséggel helyben marad, és $\frac{1}{2}$ valószínűséggel úgy viselkedik mint egy véletlen séta, azaz $\frac{1}{2d}$ valószínűséggel megy az egyik szomszédba, ha d a foka a pontnak.*

2.42. Definíció. *Legyenek az M mátrix sajátértékei a következők: $|\lambda_1| \geq |\lambda_2| \geq \ldots \geq |\lambda_n|$. Ekkor a $\gamma := \lambda_1 - \lambda_2$ különbséget az A mátrixra vonatkozó spektrális résnek fogjuk nevezni. Angolul spectral gap, vagy eigenvalue gap. Ez a mennyiség sok következő állításban fel fog tűnni.*

Ha ϵ pontossággal akarjuk közelíteni az egyenletes eloszlást, tudnunk kell, hány lépést kell tennünk, hogy ez megvalósuljon.

2.43. Definíció. *Ha adott egy Markov-lánc aminek a stacionárius eloszlása π, és σ tetszőleges kezdeti eloszlás. Legyen $\frac{1}{2} > \epsilon > 0$ akkor definiáljuk a keverési időt a következőképpen:*

$$t_{mix}(\epsilon) = \max_{\sigma}\{\min_{k}\{\|\pi - \sigma^k\|_{sup} \leq (1 - e^{\epsilon})\pi\}\}$$

Az előző tétel alapján, adott kezdeti eloszlásra elég megtalálnunk a legkisebb t-t, amire $\mu^t \leq \epsilon\sqrt{\pi(i)}$. Írjuk μ-t fel $\mu = 1 - \gamma$ alakba. Mivel tudjuk, hogy $1 - \gamma \leq e^{-\gamma}$ elég ha $e^{-\gamma k} \leq \epsilon\sqrt{\pi(i)}$. Ebből k-t kifejezve kapjuk a következő egyenlőtlenséget, azaz az egyenlőtlenség jobb oldala a keverési idő:

$$k \geq \frac{1}{\gamma}\left(-\log\frac{1}{\epsilon} - \frac{1}{2}\log\frac{1}{\pi(i)}\right). \tag{10}$$

Látszik tehát, hogy a szükséges lépések száma egy logaritmikus nagyságrendű tagtól eltekintve, a spektrális rés reciprokától becsülhető.

A tétel bizonyításakor szükségünk lesz a keverési idő következő becslésére:

2.44. Tétel. *Legyen $G = (V, E)$ egy gráf, $|V| = n$, $diam(G) = d$, és jelöljük Δ-val a maximális fokszámot. Ekkor $t_{mix} = \mathcal{O}(d\Delta n \log(n))$*

2.45. Definíció. *Azoknak a nyelveknek az osztályát amikre létezik olyan randomizált, (véletlent is használó) Turing-gép, ami várhatóan polinomiális időben erősen eldönti ZPP-vel —Zero-error Probabilistic Polynomial— jelöljük. Ez azt jelenti, hogy létezik olyan Turing-gép ami egy adott b bemenetre 1-et ad vissza ha b a nyelvben van és 0-t különben, a futásidő várható értéke pedig polinomiális az input méretében. Egy ilyen algoritmust Las Vegas algoritmusnak nevezünk.*

2.46. Definíció. *Egy permutáció fokszámán a következőkben a tartójának az elemszámát fogjuk érteni.*

2.47. Tétel. *Legyen $\epsilon > 0$ és S egy generátorrendszere S_n-nek vagy A_n-nek. Tegyük fel, hogy létezik az S-nek olyan eleme aminek fokszáma $\leq \frac{n}{3+\epsilon}$. Ekkor a $\mathrm{Cay}(G, S))$ Cayley-gráf átmérője $\mathcal{O}(n^C)$ nagyságrendű, ahol a C egy ϵ-tól független konstans. Továbbá két teszőleges elem között $\mathcal{O}(n^C)$-hosszú út található, Las Vegas algoritmussal.*

A tétel bizonyítása előtt pár lemmát fogunk belátni. Ezek közül, az első csak a módszer bemutatása, amit a másodikban majd alkalmazunk egy egyszerűbb esetben, ezt nem fogjuk használni a bizonyításban.

2.48. Lemma. *Legyen $G = \langle S \rangle$, egy n-ed rendű tranzitív, permutaciócsoport, $\delta > 0$ rögzített, $A \subset [n] = \{1, 2, \ldots, n\}$ és $|A| = k$. Ekkor létezik olyan $\mathcal{O}(n^2|S|\log(n))$-hosszú π szó S felett amire:*

$$|A \cap A^\pi| \leq \frac{k^2}{n}(1 + \delta)$$

Bizonyítás. Legyen Γ egy gráf, aminek pontjai $[n]$ elemei, és két elem között akkor megy él, ha S egy eleme az egyiket átviszi a másikba. Mivel G hatása tranzitív, ezért világos hogy Γ összefüggő és reguláris. Legyen t_{mix} a keverési ideje a Γ-n értelmezett lusta véletlen sétának, tehát minden csúcsot $\frac{1}{n}e^{\pm\epsilon}$ valószínűséggel érintettünk már t_{mix} lépés után. Válasszuk ϵ-t úgy, hogy $\epsilon = \log(1 + \delta)$ teljesüljön. A 2.44 tétel alapján $t_{mix} = \mathcal{O}(n^2|S|\log n)$. Ha π egy t_{mix} hosszú S feletti szó, ami egy lusta véletlen sétából származik, akkor tetszőleges $i \in [n]$-re:

$$P(i^\pi \in A) \leq \frac{k}{n}e^\epsilon = \frac{k}{n}(1 + \delta)$$

Ezeket a valószínűségeket minden $i \in A$-ra összegezve a várható értékre azt kapjuk, hogy:

$$E(A \cap A^\pi) \leq \frac{k^2}{n}(1 + \delta)$$

Válasszuk π-t úgy, hogy $|A \cap A^\pi|$ értéke legfeljebb az átlag legyen. □

2.49. Megjegyzés. Ha π-t egyenletesen választjuk akkor $E(A \cap A^\pi) = \frac{k^2}{n}$, tehát a lemma lényege, hogy majdnem ugyanezt az értéket elérhetjük, úgy is, hogy π rövid legyen S felett. Megfelelő π keresésére így használhatunk egy rövid véletlen sétát.

2.50. Lemma. *Legyen $G = \langle S \rangle$, egy n-ed rendű t-tranzitív, permutációcsoport, $\delta > 0$ rögzített. Legyen $(v_1, v_2, \ldots, v_t)$ és $(u_1, u_2, \ldots, u_t)$ az $[n]$ különböző elemeiből álló rendezett t-esek. Ekkor létezik olyan $\mathcal{O}(n^2|S|\log(n))$-hosszú π szó S felett amire:*

(A) $|A \cap A^\pi| \leq h + (1+\delta)\frac{k^2}{n}$

(B) $v_i^\pi = u_i \quad (1 \leq i \leq t)$

ahol h azon (v_i, u_i) párok száma, amire $v_i, u_i \in A$

Bizonyítás. Legyen $\Gamma = (V, E)$ gráf, ahol $V = \{1, 2, \ldots, n\}^{t+1}$, valamint legyen $((v_1, v_2, \ldots, v_t), (u_1, u_2, \ldots, u_t)) \in E$ akkor és csak akkor, ha létezik $\sigma \in S$, hogy $v_i^\sigma = u_i$ minden $1 \leq i \leq t$ esetén. Ekkor $|V| = \frac{n!}{(n-t-1)!} \leq n^{t+1}$, és Γ egy $2|S|$-reguláris gráf. Mivel G egy t-tranzitív permutációcsoport, Γ összefüggő. Legyen t_{mix} mint a 2.48 lemmában és $\epsilon = \frac{1}{2}\log(1+\delta)$. A 2.44 tétel alapján $t_{mix} = \mathcal{O}(tn^{2(t+1)}|S|\log n)$. Legyen π mit az előző bizonyításban, és jelölje B azt az eseményt, hogy π teljesíti a (B) feltételt.

$$P(B) = \frac{e^{\pm\epsilon}}{n(n-1)\ldots(n-t+1)}$$

tetszőleges $v \notin (v_1, v_2, \ldots, v_t)$-re és $u \notin (u_1, u_2, \ldots, u_t)$-ra:

$$P(B \cap v^\pi = u) = \frac{e^{\pm\epsilon}}{n(n-1)\ldots(n-t)}$$

Ebből a következőt kapjuk a $(v^\pi = u|B)$ esemény valószínűségére:

$$P(v^\pi = u|B) = \frac{e^{\pm\epsilon}}{(n-t)}$$

Ezt az előző lemmához hasonlóan minden $v_i \in A$-ra összegezve:

$$E(|A \cap A^\pi||B) = h + \frac{(k-h)^2 e^{2\epsilon}}{n} = h + \frac{(k-h)^2(1+\delta)}{n}$$

Tehát választhatjuk úgy π-t hogy (A) és (B) is teljesüljenek. □

2.51. Definíció. *Legyen G egy csoport. Két teszőleges g, h elemre a G-ből a $[g, h] = g^{-1}h^{-1}gh$ elemet a g és h kommutátorának nevezzük. Fontos megjegyezni, hogy $[g, h] = 1$ akkor és csak akkor ha g és h felcserélhetőek.*

2.52. Lemma. *Legyen σ, τ két permutáció és $A = \mathrm{supp}(\tau)$. Legyen $x \in A$ és $y = x^\tau$. Ha $x^{\sigma^{-1}} \in A$ és $y^{\sigma^{-1}} \notin A$ akkor τ és τ^σ nem felcserélhető, azaz $[\tau, \tau^\sigma] \neq 1$.*

Bizonyítás. Legyen $\phi = \tau^\sigma$. Mivel $y^{\sigma^{-1}} \notin A$, ezért $y^{\sigma^{-1}\tau} = y^{\sigma^{-1}}$, azaz $y^\phi = y^{\sigma^{-1}\tau\sigma} = y\sigma^{-1}\sigma = y$, azaz $x^\tau = y = y^\phi = x^{\tau\phi}$. Indirekt tegyük fel, hogy τ és ϕ felcserélhetőek. Ebből következik, hogy $y = x^\tau = x^{\tau\phi} = x^{\phi\tau}$. Ez rögtön ellentmondáshoz vezet, ha leellenőrizzük, hogy $x^\phi \neq x$. Mivel $x^{\sigma^{-1}} \in A$, ezért $x^{\sigma^{-1}\tau} \neq x^{\sigma^{-1}}$, és így $x^{\sigma^{-1}\tau\sigma} = x^\phi \neq x$. □

2.53. Lemma. *Legyen τ, π két tetszőleges permutáció ekkor* $\mathrm{supp}(\tau^\pi) = \mathrm{supp}(\tau)^\pi$

Bizonyítás. Legyen $x \notin \mathrm{supp}(\tau)^\pi$. Ezt π^{-1} nem $\mathrm{supp}(\tau)$-ba viszi, hiszen akkor $x \in \mathrm{supp}(\tau)^\pi$ teljesülne. Jelölje $y = x^{\pi^{-1}}$-t. Ezt τ helyben hagyja, π pedig visszaviszi x-be. Ebből következik, hogy $x \notin \mathrm{supp}(\tau^\pi)$.

Hasonlóan, ha $x \in \mathrm{supp}(\tau)^\pi$ akkor a π^{-1}-nél vett képe benne van $\mathrm{supp}(\tau)$-ban. Ekkor $y = x^{\pi^{-1}}$ elmozdul τ hatására, és képe τ-nál szintén $\mathrm{supp}(\tau)$-ban van. Ennek a π-nél vett képe nem mehet vissza x-be, azaz $x \in \mathrm{supp}(\tau^\sigma)$. □

2.54. Lemma. *Legyen τ, π két tetszőleges permutáció, mint az előbb. Azt állítjuk, hogy teljesül a* $|\mathrm{supp}([\tau, \tau^\pi])| \leq 3|\mathrm{supp}(\tau) \cap \mathrm{supp}(\tau^\pi)|$ *egyenlőtlenség.*

Bizonyítás. A bizonyításban az olyan x-eket fogjuk összeszámolni amik elmozdulnak $[\tau, \tau^\pi]$-nél. Ehhez a $\mathrm{supp}(\tau)$ és a $\mathrm{supp}(\tau)^\pi = \mathrm{supp}(\tau^\pi)$ halmazokat elég vizsgálni, hisz ami nincs benne ezekben, az egész biztos nem mozdul el.

Vizsgáljuk először azt az esetet amikor $x \in \mathrm{supp}(\tau) \cap \mathrm{supp}(\tau^\pi)$. Ezek közül azoknak a száma, amik benne vannak $\mathrm{supp}([\tau, \tau^\pi])$-ben világos, hogy felülről becsülhető a metszet elemszámával.

Ha $x \in \mathit{supp}(\tau) \setminus \mathit{supp}(\tau^\pi)$, akkor először tegyük fel, hogy τ^{-1} nem viszi ki ebből a halmazból, vagyis nem viszi bele $\mathrm{supp}(\tau) \cap \mathrm{supp}(\tau^\pi)$-be. Ekkor $(\tau^\pi)^{-1}$ nem mozditja el, majd τ visszaviszi x-be. Innen τ^π megint nem viszi sehova. Ebből következik, hogy csak akkor mozdulhat el ha $x^{\tau^{\pi^{-1}}} \in \mathrm{supp}(\tau) \cap \mathrm{supp}(\tau^\pi)$. Ilyen x-ből legfeljebb pont annyi lehet mint a metszet elemszáma.

Az utolsó eset amikor $x \notin \mathrm{supp}(\tau)$. Ebben az esetben τ^{-1} se mozdítja el x-et, tehát azt kell vizsgálni, hogy $x^{\tau^{\pi^{-1}}\tau\tau^\pi} \neq x$ mikor teljesül. Ahhoz, hogy az egyenlőtlenség teljesüljön szükség van arra, hogy $y = x^{(\tau^\pi)^{-1}}$ benne legyen $\mathit{supp}(\tau)$-ban, de ekkor y megint csak a metszetben lehet. Az ilyen x-ek elemszáma megint a metszet elemszámával becsülhető, hisz $(\tau^\pi)^{-1}$ egy permutáció. □

Bizonyítás. [A 2.47 tételhez] A 2.50 lemmát fogjuk alkalmazni többször egymás után, $A = \mathrm{supp}(\tau)$, $t = 2$, $v_1, u_1 \in A$, $u_2 = u_1^\tau \in A$ és $v_2 \notin A$ választással. Ha a (B)

tulajdonság teljesül akkor a 2.52 lemma miatt τ és π nem felcserélhetőek. Vegyük észre, hogy most $h = 1$.

Kezdetben válasszuk τ-t hogy $|\operatorname{supp}(\tau)| \leq \frac{n}{3+\epsilon}$ teljesüljön. Minden iterációban kicseréljük τ-t a $[\tau, \tau^\pi]$ kommutátorra, ahol π az (A), (B) tulajdonságokat kielégítő permutáció, $A = \operatorname{supp}(\tau)$, V_i, u_i pedig olyan mint az előző bekezdésben. A (B) tulajdonság garantálja, hogy $\tau \neq id$, (A) ból pedig következik, hogy τ fokszáma gyorsan csökken. Legyen $|\operatorname{supp}(\tau)| = k$, $|\operatorname{supp}([\tau, \tau^\pi])| = l$ ekkor a 2.54 lemma miatt

$$\frac{l}{n} \leq \frac{3}{n} + 3\left(\frac{k}{n}\right)^2 (1+\delta)$$

tetszőlegesen kis δ-ra. Létezik c konstans amire:

$$\frac{l}{n} \leq c\left(\frac{k}{n}\right)^2$$

Ebből következik, hogy m iteráció után:

$$\frac{l}{n} \leq c^{2^{m-1}}\left(\frac{k}{n}\right)^{2^m}$$

Tehát $m \in \mathcal{O}(\log\log n)$, azaz $\mathcal{O}(\log\log n)$ lépésben elérjük $k \leq 3$-at. A 3 hosszú permutációk pedig generálják A_n-et, míg az involúciók S_n-et. Ahhoz, hogy a sorozat tényleg konvergáljon c-nek elég kicsinek kell lennie mint $\left(\frac{k}{n}\right)^2$, ezért van szükség a $\frac{k}{n} \leq \frac{1}{3+\epsilon}$ kezdeti feltételre.

A τ hossza minden iterációban a négyszeresére változik, plusz egy $\mathcal{O}(n^6|S|\log n)$ nagyságrendű tagot veszünk hozzá. Mivel $\mathcal{O}(\log\log n)$ iteráció van következik, hogy az utolsó iterációban a kommutátor $n^6|S|\log n^{\mathcal{O}(1)}$ hoszú. $\square$

3. Expanderek

A következőekben tárgyalt gráfok relatíve új fogalmat alkotnak a matematikában, viszont több területen is előfordulnak. Az, hogy milyen természetes ezeknek a gráfoknak a bevezetése, abból is látszik, hogy definiciójuk legalább háromféleképpen is megfogalmazható: algebrai, kombinatorikus, vagy valószínűségszámítási fogalmak segítségével. Algebrailag az expanderek olyan gráfok amiknek a spektrális rése nagy. Kombinatorikus megfogalmazásban az expanderek olyan gráfok amikben minden csúcshalmaz határa nagy, ahol a határon a halmaz és komplementere közötti éleket értjük. Valószínűségszámítási szempontból expanderek az olyan gráfok amiken a véletlen sétára a 2.39 tételbeli konvergencia azaz, hogy tetszőleges kezdeti eloszlás az egyenleteshez konvergál a lehető leggyorsabb. Ezentúl minden gráf amiről beszélünk összefüggő, d-reguláris és irányítatlan. A definíciókat a kombinatirikai megközelítéssel fogjuk kezdeni.

3.1. Definíciók

3.1. Definíció. *Egy $G = (V, E)$ gráfban $S, T \subseteq V$ halmazokra jelöljük a közöttük vezető élek halmazát $E(S,T) := \{(s,t) \in E | s \in S, t \in T\}$-el. Speciálisan $S \subseteq V$ halmazra $E(S, \bar{S}) = \partial S$-t az S részhalmaz határának nevezzük.*

3.2. Definíció. *Bővülési hányadosnak nevezzük a következőt:*

$$h(G) = \min_{S:|S|\leq \frac{n}{2}} \frac{|\partial S|}{|S|}$$

3.3. Definíció. *Egy d-reguláris, növekvő csúcsszámú, $(G_i)_{i\in\mathbb{N}}$ gráfokból álló sorozatot ϵ-expandernek nevezünk, ha létezik $\epsilon > 0$, hogy $h(G_i) \geq \epsilon$ minden i-re.*

Egy gráfról általában eldönteni, hogy expander-e, nem egyszerű feladat, pontosabban $h(G)$ kiszámítása egy adott G gráfra co-NP-nehéz. A következő példákról (3.4, 3.5) sem fogjuk megmutatni, hogy valóban expanderek.

3.4. Példa. Minden m egészre 8-reguláris G_m gráfok sorozata. A csúcshalmaz $V_m = \mathbb{Z}_m \times \mathbb{Z}_m$, ahol az (x, y) csúcs szomszédai az $(x + y, y), (x - y, y), (x, y + x), (x, y - x), (x+y+1, y), (x-y+1, y), (x, y+x+1), (x, y-x+1)$. Minden műveletet moduló m értünk.

Ez volt az első explicit konstrukció amiről G. A. Margulis megmutatta, hogy ezek a gráfok expanderek [10]. Előtte csak valószínűségszámítást használó bizonyítások voltak arra, hogy egy gáf expander. Ez a bizonyítás reprezentációelméletre épül, ami lényegesen meghaladja ennek a dolgozatnak a korlátait. Ez is mutatja milyen nehéz valamiről megmutatni, hogy expander.

3.5. Példa. Minden p prímre egy p-csúcsú 3-reguláris $G_p(V_p, E_p)$ gráf. Ennél $V_p = \mathbb{Z}_p$ és minden x csúcs össze van kötve $x+1$-gyel, $x-1$-gyel és $\frac{1}{x}$-gyel, ahol a 0 képe legyen a 0. Minden műveletet moduló p értünk.

Ezekre a gráfokra a bizonyítás egy nehéz számelméleti tételen, a Selberg 3/16 tételen alapul. Ez megtalálható [10]-ben, a 11.1.2 pontban, itt szintén nem bizonyítjuk.

3.2. Expanderek különböző definicióinak ekvivalenciája

Ebben a fejezetben megmutatjuk, hogy a bevezetőben említett különböző megközelítések, tényleg összefüggnek egymással.

3.6. Tétel. *Legyen G egy d-reguláris gráf, aminek az adjacencia mátrixának a sajátértékei: $d = \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$. Ekkor:*

$$\frac{d-\lambda_2}{2} \leq h(g) \leq \sqrt{2d(d-\lambda_2)}$$

A tétel különböző eseteit Cheeger [6], Buser [5], Alon, és Milman [2] bizonyították. A tételből jól látszik, hogy ha egy gráfsorozatban minden elem spektrális rése nagyobb mint $\epsilon > 0$ akkor ez a sorozat $\frac{\epsilon}{2}$-expander, illetve egy ϵ- expander sorozat minden elemének spektrális rése becsülhető ϵ és fokszám segítségével.

3.7. Tétel. (Expander keverési lemma [10]) *Legyen G egy d-reguláris gráf, a csúcsainak száma n. Jelölje $\mu = \mu(G) = max(|\lambda_2|, |\lambda_n|)$. Minden $S, T \subseteq V$-re:*

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| \leq \mu\sqrt{|S||T|}$$

Itt a bal oldalon $|E(S,T)|$ az élek száma S és T között, míg $d|S||T|/n$ az élek várható értéke S és T között. Ekkor, ha μ értéke kicsi az azt jelenti, hogy a bal oldalon lévő két érték közötti különbség kicsi, vagyis a gráf úgy viselkedik ebből a szempontból, mint egy véletlen gráf.

Ezekből a tételekből látszik, hogy a spektrális rés mérete és az expanzió és bizonyos gráfelméleti tulajdonságok között erős összefüggés van. Most pedig bemutatjuk, hogy véletlen séták konvergenciájára is hasonló a helyzet.

3.8. Tétel. *Legyen G egy (n, d, α) gráf aminek a normalizált adjacencia mátrixa $\hat{A}$. Legyen π a véletlen séta stacionárius eloszlása G-n. Mivel G reguláris ez most az egyenletes eloszlás. Ekkor minden kezdeti σ eloszlásra és minden $t > 0$ egészre:*

$$\|\hat{A}^t p - \pi\|_1 \leq \sqrt{n}\alpha^k$$

Jól látszik, hogy ez a 2.40 tétel analógiája expanderekre.

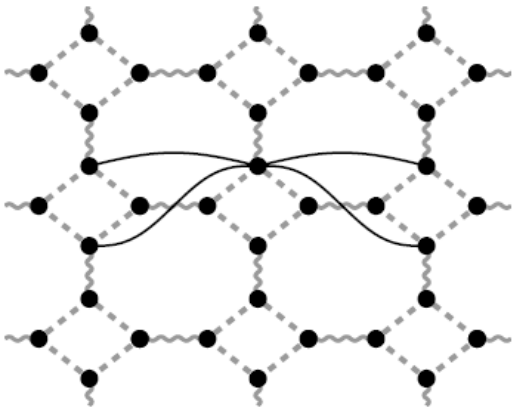
3.3. Cikk-cakk szorzat

Ebben a fejezetben bevezetünk egy új kétváltozós, nem szimmetrikus műveletet gráfokon. Ezután ezt arra fogjuk használni, hogy explicit konstrukciót adjunk expanderekre. A művelet neve cikk-cakk szorzat, angolul zig-zag proguct.

3.9. Definíció. *Egy $G = (V, E)$ gáfra azt mondjuk, hogy (n, m, α)-gráf, ha $|V| = n$, $|E| = m$, és $h(G) = \alpha$.*

Legyen G egy (n, m, α) gráf, H pedig egy (m, d, β). Minden $v \in V(G)$ csúcsra rögzítsük az éleknek egy számozását: $e_v^1, e_v^2, \ldots, e_v^m$, és ezeknek az éleknek csúcspontja. A H csúcsait pedig tekintsük úgy mint a $[m]$ halmaz elemeit. A $G\textcircled{z}H$ csúcshalmaza legyen a $V(G) \times V(H)$ Descartes-szorzat. Érdemes erre a halmazra úgy tekintenünk, hogy minden $v \in G$ csúcsot helyettesítünk $(v, 1), (v, 2), \ldots, (v, m)$ csúcsok egy „felhőjével", minden v-vel szomszédos élhez egy új csúcsot rendelve. Így az eredeti gráf egy éle kétszer jelenik meg az új gráfban, mint csúcs, mindkét végén lévő csúcshoz kapcsolódva. A $G\textcircled{z}H$ gráf éleinek leírásához először egy másik szorzatot fogunk bevezetni.

Legyen a $G\textcircled{r}H$ gráf csúcshalmaza ugyanaz mint $G\textcircled{z}H$-é, az élei pedig a G élei, amik most a felhők között mennek úgy, hogy az ugyannak az régi gráfbeli élnek megfelelő csúcsokat kötjük össze, (a 3.3 ábrán a hullámos élek,) és H éleit n-szer H minden példányában behúzzuk (a szaggatott élek). Ekkor a $G\textcircled{z}H$ élei úgy keletkeznek, hogy veszünk 3-hosszú sétákat $G\textcircled{r}H$-n úgy, hogy először egy felhőn belül lépünk, majd két felhő között, utána az új felhőben, (szaggatott-hullámos-szaggatott), az ábrán ezek a folytonos sötét élek. Formálisan megfogalmazva:



5. ábra. A $\mathbb{Z}^2$ és a 4-hosszú, kör cikk-cakk szorzata

3.10. Definíció. *$G\textcircled{z}H = (V(G) \times [m], E')$ ahol $((v,i),(u,j)) \in E'$ akkor és csak akkor, ha létezik $k,l \in [m]$, hogy $(i,k),(l,j) \in E(H)$ és $e_v^k = e_u^l$*

3.11. Megjegyzés. A fent definiált $\textcircled{r}$ szorzatot a gráfelméletben sok helyen használják mikor H egy kör. Segítségével egy gráf fokszámát lehet csökkenteni úgy, hogy közben az összefüggőség nem változik. Sok még megoldatlan gráfelméleti problémára ennek segítségével mutatták meg, hogy elég lenne 3-reguláris összefüggő gráfokra megoldani.

Ennek segítségével megmutatható például, hogy SL=LSPACE [10]. Itt LSPACE az $\mathcal{O}(\log(n))$ tárral megoldható feladatok osztálya. Az SL ben pedig azok a nyelvek vannak benne, amik logaritmikus tárral visszavezethetőek arra a problémára, hogy létezik-e út egy irányítatlan gráfban két adott pont között.

3.12. Tétel. (Cikk-cakk tétel, Reingold-Vadhan-Wigderson [10]) *Adott G, (n,m,α)-gráf és a H egy (m,d,β) gráf. Ekkor $G\textcircled{z}H$, egy $(nm, d^2, \varphi(\alpha,\beta))$-gráf, ahol φ-re teljesülnek az alábbiak:*

1. *ha $\alpha < 1$ és $\beta < 1$ akkor $\varphi(\alpha,\beta) < 1$*
2. *$\varphi(\alpha,\beta) < \alpha + \beta$*
3. *$\varphi(\alpha,\beta) < 1 - \frac{(1-\beta^2)(1-\alpha)}{2}$*

Bizonyítás. A 2. egyenlőtlenséget csak egy gyengébb felső korlátra bizonyítjuk. Ez a felső korlát $\varphi \leq \alpha+\beta+\beta^2$. A definícióból azonnal látszik, hogy a $G\textcircled{z}H$ egy (mn, d^2) gráf. A spektrális rést egy véletlen sétával fogjuk megbecsülni a $G\textcircled{z}H$ gráfon. Ebben a gráfban minden lépés három részre osztható: (i) egy véletlen lépés egy felhőn belül, (ii) egy determinisztikus lépés két felhő között és (iii) egy véletlen lépés egy másik feldőben. Ez alapján felírhatjuk a véletlen séta átmenet mátrixát, ezt jelöljük Z-vel. Legyen B a H gráf adjacencia mátrixa $\hat{B}$ pedig legyen a véletlen séta átmenet mátrixa H-n. Az (i) és (iii) véletlen lépések a H diszjunkt példányain történnek tehát a hozzájuk tartozó átmenet mátrix $\tilde{B} = \hat{B} \otimes I_n$. A (ii) determinisztikus lépésben a (v, k) csúcsból a (u, j) csúcsba lépünk amire $e_v^k = e_u^l$, így ezt a lépést a következő P mátrixszal valós szorzással azonosíthatjuk:

$$P_{(v,k)(u,l)} = \begin{cases} 1 & \text{ha } e_v^k = e_u^l \\ 0 & \text{különben} \end{cases}$$

után felírhatjuk, hogy $Z = \tilde{B}P\tilde{B}$. Mivel a $G\textcircled{z}H$ gráf reguláris az 1_{nm} vektor sajátvektora Z-nek. Mivel az átmenet mátrix szimmetrikus, így van ortonormált bázis, ami hozzá tartozik. Ezek után az eredeti sajátértékekről szóló állításunk megfogalmazható a következő alakban skaláris szorzattal:

$$\frac{|fZf|}{\|f\|^2} \leq \alpha + \beta + \beta^2$$

minden f-re ami merőleges 1_{mn}-re.

A következő lépés, hogy felbontjuk f-et úgy, hogy tükröződjön a felbontásban, hogy $V(G\textcircled{z}H) = V(G) \times [m]$. Legyen $f^{\|} = \frac{1}{m}\sum_{j\in[m]} f(x, j)$ az átlaga az f-eknek a felhőkön. Definiáljuk $f^{\perp} = f - f^{\|}$-t. Látszik, hogy $f^{\perp}$ minden felhőn 0-ra adódik össze.

$$\begin{aligned} |fZf| &= |f\tilde{B}P\tilde{B}f| \\ &\leq |f^{\|}\tilde{B}P\tilde{B}f^{\|}| + 2|f^{\|}\tilde{B}P\tilde{B}f^{\perp}| + |f^{\perp}\tilde{B}P\tilde{B}f^{\perp}| \end{aligned}$$

Két dolog is következik abból, hogy $\tilde{B}$ n darab $\hat{B}$ direktösszege:

- Mivel $\hat{B}1_m = 1_m$, következik, hogy $\tilde{B}f^{\|} = f^{\|}$
- Feltesszük, hogy $\|\hat{B}\| \leq \beta\|u\|$, ha $u \perp 1_m$ és $f^{\perp}$ összege minden felhőn nulla. Ezért $\|\tilde{B}f^{\perp}\| \leq \beta\|f^{\perp}\|$

definiáljuk a következő valós értékű függvényt $V(G)$-n: legyen $g(v) = \sqrt{m} f^{\|}(v,i)$. Vegyük észte, hogy így $\|f\|^2 = \|g\|^2$. A P definíciójából következik, hogy $f^{\|}Pf^{\|} = g\hat{A}g$, $\hat{A} = \hat{A}_G$ az átmenet mátrixa a véletlen sétának G-n. De mivel $f^{\|} \perp i_{nm}$ így $g \perp 1_n$ és ebből következik, hogy $g\hat{A}g \leq \alpha\|g\|^2$, azaz $|f^{\|}Pf^{\|}| \leq \alpha\|f\|^2$. Mivel P és $\tilde{B}$ is sztohasztikus mátrixok, ezért kontrakciók l_2-ben. Minedezek alapján azt kapjuk, hogy

$$\|fZf\| \leq \alpha\|f\|^2 + 2\beta\|f^{\|}\| \cdot \|f^{\perp}\| + \beta^2\|f^{\perp}\|^2$$

De mivel $\|f^{\|}\|$ és $\|f^{\perp}\|$ merőlegesek, $\|f\|^2 = \|f^{\|}\|^2 + \|f^{\|}\|^2$, tehát ennek a kvadratikus alaknak a maximuma a $\left(\begin{smallmatrix} \alpha & \beta \\ \beta & \beta^2 \end{smallmatrix}\right)$ mátrix nagyobb abszolútértékű sajátértéke. Ezzel a bizonyítás kész. □

3.13. Megjegyzés. Ezek közül az első pont azt fejezi ki, hogy ha G és H is expanderek akkor $G ⓩ H$ is az. A 2. és 3. korlát az alkalmazásokban nagyon fontos. Az előbbi akkor hasznos, mikor α és β kicsik, a második mikor nagyok.

3.4. Expandercsalád konstrukciója a cikk-cakk szorzással

Először definiáljuk gráfoknak a hatványozását. Adott $G = (V, E)$ gráfra a G k-adik hatványát úgy, hogy a $G^k = (V, E')$ gráfban behúzunk egy (u, v) élt minden k-hosszú $u \rightsquigarrow v$ útra G-ben. A G^k adjacencia mátrixa a G adjacencia mátrixának k-adik hatványa, ebből látszik, hogy ha G egy (n, d, α) gráf akkor G^k egy (n, d^k, α^k) gráf.

Legyen a H egy $(d^4, d, \frac{1}{4})$ gráf, adott d konstansra. Bebizonyítható, hogy van ilyen gráf ami expander [10]. A $(G_n)_{n\in\mathbb{N}}$ sorozatot definiáljuk a következőképpen: legyen $G_1 = H^2$ és legyen $G_{n+1} = (G_n)^2 ⓩ H$ minden $n \geq 1$-re. Azt állítjuk, hogy a $(G_n)_{n\in\mathbb{N}}$ sorozat expander család.

3.14. Állítás. *A G_n egy $(d^{4n}, d^2, \frac{1}{2})$ gráf minden n-re*

Bizonyítás. A bizonyítás teljes indukcióval történik. Első lépésben $n = 1$-re a definícióból azonnal következik az állítás. Az indukciós lépéshez először vegyük észre, hogy G_n^2 egy $(d^{4n}, d^4, \frac{1}{4})$ gráf. Mikor vesszük ennek a cikk-cakk szorzatát H-val, (ez a művelet értelmes mert G_n^2 fokszáma megegyezik H elemszámával,) akkor az előző tétel beli második korlát alapján φ-re, a G_{n+1} egy $(d^{4(n+1)}, d^2, \frac{1}{2})$ gráf. □

3.5. Expanderek további konstrukciói, és kapcsolat a Cayley-gráfokkal

A 3.2 fejezetben láttuk, hogy az expandereket valószínűségszámítási módszerekkel is érdemes vizsgálni. Ha a definíciókat meggondoljuk érezzük, hogy van kapcsolat egy gráf bővülésének mértéke, amit a bővülési hányadossal mértünk és az átmérője között. Tehát adja magát a gondolat, hogy az expandereket megpróbáljuk az átmérővel jellemezni. Természetesen lehet olyan Cayley gráfot konstruálni, aminek átmérője $O(log|G|)$ és mégsem expander.

A következő tétel a spektrális rés és az átmérő kapcsolatát adja meg eg Cayley-gráfban.

3.15. Lemma. *Legyen G egy teszőleges véges csoport, $1 \in S \subset G$ és γ a gráf spektrális rése.*

$$\frac{\operatorname{diam}(\operatorname{Cay}(G,S)) - 1}{\log |G|} \leq \frac{1}{\gamma} \leq |S| \operatorname{diam}(\operatorname{Cay}(G,S))^2$$

Ebből az is következik, hogy a 2.2 és a 2.3 fejezetben bizonyított korlátok az átmérőre mind segítséget nyújtanak expanderek keresésében.

A következő tétel megmutatja, hogy egy csoportra, véletlenszerűen választott generátorrendszer mellett a Cayley-gráfja expander. Ezzel egy másik megközeltésre kapunk lehetőséget, az eddigi explicit konstrukciók helyett.

3.16. Tétel. (Alon-Roichmann [10]) *Legyen G egy véges csoport és válasszuk az $S \subset H$ csoportot egyenletesen H-ból úgy, hogy $|S| = 100 \log H$. Ekkor legalább $\frac{1}{2}$ valószínűséggel a $(\operatorname{Cay}(G,S))$ gráf második legnagyob abszolútértékű sajátértéke osztva a fokszámmal kisebb mint $\frac{1}{2}$.*

4. Programok dokumentációja

4.1. Felbontás S_n-ben

A dokumentáció során végig a 2.21 tétel jelöléseit fogjuk használni. Egy S_n-beli π elem felbontásához vegyük a π-t ciklusfelbontását. A ciklusokat külön fogjuk felbontani, majd az így kapott szavakat összeszorozzuk. Minden ciklust felírhatunk transzpozíciók szorzataként a következőképpen:

$$(a_1, a_2, \dots a_n) = (a_1, a_2)(a_1, a_3), \dots (a_1, a_{n-1})(a_1, a_n) \tag{11}$$

Ezután minden tanszpozíciót $(a, b) = (\infty, a)(\infty, b)(\infty, a)$ alakba írunk, ahol ∞ az $\{1, 2, \dots, n\}$ halmaz egy tetszőleges a, b-től különböző eleme. Mivel (∞, a) rendje 2 egyszerűsíthetünk a szorzatban, így kapjuk a következő alakú szorzatot:

$$(\infty, a_1)(\infty, a_2)(\infty, a_3) \dots (\infty, a_n)(\infty, a_1)$$

Most bontsuk fel a $\{1, 2, \dots, n\}$ halmazt a tételben szereplő, $E, X_1, X_2, \dots, X_{12}$ halmazokra. Ezt egyszerűen úgy csináljuk, hogy $E = \{1, 2, \dots, |E|\}$, $X_1 = \{|E| + 1, |E| + 2, \dots, |E| + |X_1|\}$, $\dots$, $X_{12} = \{|E| + 11|X_1| + 1, \dots, n\}$. Ehhez meg kell határozni próbálgatással-et, úgy hogy megfeleljen a 2.21 tétel feltételeinek. Ezt próbálgatással csináljuk $l = 1$-től kezdődően.

Konstruáljuk meg b-t és c-t a következőképpen:

A c minden $X_1 \cup X_2 \cup \dots \cup X_{11}$-beli elemet egyel nagyobb indexű halmazba visz, egy X_{12}-belit pedig X_1-be majd alkalmazza rá az $x \mapsto 2x + 1$ leképezést.

A b függvénybeli $\hat{b}_1$-t a $b_1 : x \mapsto 2x$ függvény hatványozásával kapjuk meg. Mivel b_1 rendje és 12 relatív prímek a tizenkettedik hatványra elemlés bijekció, tehát van elem aminek a 12-dik hatványa is b, fordítva pedig b 12-dik gyöke előáll b egy hatványaként. Az f-et úgy konstruáljuk, meg hogy mindig veszünk 100 elemet E-ből, és hozzá egyet $X_2 \cup X_3 \cup \dots \cup X_{12}$-ből. Az utolsó körnél annyi elemet veszünk az unióból, hogy 101-hosszú legyen a kör.

Ezután az algoritmus háromféleképpen megy attól függően, hogy a (∞, a) permutációban, amit fel akarunk bontani az a elem melyik halmazba esik.

Az első eset amikor $a \in X_1$. Ekkor a (7), és (1) egyenlőségeket alkalmazva (∞, a)-t felbontjuk $\langle b^{12}, c^{12} \rangle$-ben. Itt felhasználjuk azt is, hogy $b^{101l} = (\infty, 0)$.

A következő eset amikor $a \in X_2 \cup X_3 \cup \ldots \cup X_{12}$. Ilyenkor kiszámoljuk hogy $a \in X_i$ melyik $2 \leq i \leq 12$-re teljesül, mad c^{12-i}-t alkalmazzuk a-ra. Erre már teljesül, hogy $x^{c^{12-i}} \in X_1$, tehát alkalmazhatjuk az első esetbeli módszert.

Az utolsó eset amikor $a \in E$. A b konstrukciója alapján kiszámoljuk, hogy a hanyadik elem a 101-hosszú körben, legyen ez i. Ekkor b^i-vel konjugálva a-t egy $X_2 \cup X_3 \cup \ldots \cup X_{12}$-beli elemet kapunk. Erre alkalmazhatjuk az előző esetet.

4.2. Véletlen elem generálása S_n-ben

Mivel az előző részben már megkonstruáltuk a szükséges permutációkat, csak annyi maradt hátra, hogy összeszorozzunk megfelelően sokat b-ből és c-ből. Ehhez szükségünk van a keverési idő egy alsó becslésére. Használjuk a 10 egyenlőtlenséget. Mivel a spektrális rést nem ismerjük, használjuk a 3.15 tételt a becslésére. A kettőt összevetke kapjuk, hogy:

$$t_{mix} \geq |S| \operatorname{diam}(\operatorname{Cay}(G,S))^2 \left(\log \frac{1}{\epsilon} + \frac{1}{2} \log \frac{1}{\pi(i)} \right) \tag{12}$$

Mivel $\operatorname{diam}(\operatorname{Cay}(G,S))^2$-t is csak nagyságrendileg ismerjük ez a konstans is a bemenet része kell, hogy legyen.

Sajnos mivel a 2.21 tétel, csak $n \geq 2^{12}$-re működik, t_{mix} értékére nagyon nagy alsó becslést kapunk. Ha $n = 2^{12}$-re, és $C = 1$-re alkalmazzuk a 2.21 beli becslést a következőt kapjuk:

$$|S| \operatorname{diam}(\operatorname{Cay}(G,S))^2 \approx 2 \cdot \left(2^{11} \log(2^{11})\right)^2 \approx 4,6 \cdot 10^6$$

Ez persze $S_{2^{11}}$ rendjéhez képest kicsi, de ahhoz, hogy a gyakorlatban alkalmazzuk még mindig nagyon sok szorzás elvégzését jelenti. Mindegyik szorzás legalább $\mathcal{O}(n)$ nagyságrendű időt vesz igénybe, mert a permutációkat n-hosszú vektorokban tároltam. Ezért végül ez a feltétel nem mutatja, hogy gyorsan lehet véletlen elemet generálni S_n-ben. Természetesen az átmérő segítségével csak rosszul lehet megbecsülni a spektrális rést, így könnyen lehet, hogy a konstruált gráf mégis jó expanziós tulajdonságokkal rendelkezik, és így az algoritmus mégis használható.

Annyit viszont biztosan állíthatunk, hogy a konstans kisebb mint 3600 a 2.26 tétel alapján. Viszont a gyakorlati alkalmazáshoz ezzel sem kerültünk közelebb.

4.3. Felbontás $PSL(2, \mathbb{Z}_q)$-ban

Az $\mathbb{F}_q$-ban való számolás nehézsége miatt a $\mathbb{Z}_q$ feletti mátrixokra oldottam meg a feladatot. Itt lehet moduló $q = p^n$ számolni viszont p többszöröseinek nincs inverze.

Az algoritmus első lépése, hogy primitív gyököt találjunk q-hoz. Mivel $n \in \mathbb{F}_q^\times$ primitív gyök, akkor és csak akkor, ha $o(n) = \varphi(q)$, ezenkívül minden $n \in \mathbb{F}_q^\times$ $o(n)|\varphi(q)$ ez a következőképpen történik: először kiszámoljuk $\varphi(q)$-t, majd prímtényezőkre bontjuk $p_1, \dots p_k$. Következő lépésként minden $n \in \mathbb{F}_q^\times$-ra és minden i-re kiszámoluk $n^{\frac{\varphi(q)}{p_i}}$. Az az n amire $n^{\frac{\varphi(q)}{p_i}} \neq 1$ minden i-re primitív gyök.

Ennek az elemnek az inverzét is ki kell számolni ahhoz, hogy a $h(\theta)$ mátrixot meghatározzuk, ez a következő tétel és algoritmus segítségével történik.

4.1. Tétel. (Bézout-lemma) *Legyenek a, b egész számok, amik közül legalább az egyik nem 0, d pedig legyen a legnagyobb közös osztójuk. Ekkor létezik x, y egész, hogy $ax + by = d$. Az ilyen x, y párokat Bézout-együtthatóknak fogjuk nevezni.*

Bizonyítás. A tétel bizonyítása lényegében az Euklideszi algoritmusra épül. Legyen a, b adott. Ekkor létezik minimális abszolútértékű $d = as+bt$ az $ax+by$ alakú számok között, ahol x, y egészek. Feltehető, hogy d pozitív.

Ha a-t vagy b-t elosztjuk d-vel a maradék szintén $q = ax + by$ alakú lesz. Mivel $|q| < |d| = d$ a maradékos osztás miatt, és d-t úgy választottuk, hogy minimális abszolútértékő legyen, következik, hogy $c = 0$, tehát $d|a$ és $d|b$.

Tegyük fel, hogy δ, a-nak és b-nek d-től különböző közös osztója. Ekkor osztója $as + bt = d$-nek is. Mivel $\delta|d$ és $\delta \neq d$ következik, hogy $\delta < d$, tehát d a legnagyobb közös osztó. □

A tételből következik, hogy ha $(a, q) = 1$, akkor létezik s, t, hogy $as + qt = 1$. Ezt az egynlőséget moduló q tekintve kapjuk, hogy $as \equiv 1 \pmod{n}$. Azaz s az a multiplikatív inverze.

Ha a fenti tételben szereplő együtthatókat meg tudnánk határozni, akkor készen lennénk mivel $\mathbb{F}_{p^n}$ minden invertálható elemének ki tudnánk számoloni az inverzét. Ezeket az együtthatókat a következő algoritmussal számoljuk ki, ami az euklideszi algoritmus egy bővített változata.

4.2. Állítás. *Az 1. algoritmus meghatározza a és b legnagyobb közös osztóját, valamint egy Bézout-együttható párt.*

Algorithm 1 Euklideszi algoritmus

procedure INVERZ(a, b) ▷ s és t lesznek a szükséges együtthatók
  $s_0 \leftarrow 1$, $s_1 \leftarrow 0$
  $t_0 \leftarrow 0$, $t_1 \leftarrow 1$
  $r_0 \leftarrow a$, $r_1 \leftarrow b$
  while $r_i \neq 0$ **do** ▷ Ha $r = 0$ készen vagyunk
    $q \leftarrow r$ div r' ▷ *div* a maradékos osztás hányadosát határozza meg
    $(r_i, r_{i+1}) := (r_{i+1}, r_i - qr_{i+1})$ ▷ itt a (x, y) jelölés egy
    $(s_i, s_{i+1}) := (s_{i+1}, s_i - qs_{i+1})$ ▷ rendezett párt jelöl
    $(t_i, t_{i+1}) := (t_{i+1}, t_i - qt_{i+1})$
  end while
  return t ▷ Ez lesz a inverze
end procedure

Bizonyítás. Mivel $0 \leq r_{i+1} < r_i$ az r'-k és az r-ek szigorúan csökkenő sorozatot alkotnak, tehát az algoritmus véges sok lépés után megáll.

Mivel $(r_{i-1}, r_i) = (r_i, r_{i+1})$, így $(a, b) = (r_k, r_k + 1)$, $k + 1 = 0$ az index ahol az algorizmus leáll. Ebből következik, hogy $(a, b) = r_k$

Mivel $a = r_0$,$b = r_1$ valamint s_0, s_1 és t_0, t_1 kezdeti definíciójából következik, hogy $as_i + bt_i = r_i$ $i = 0, 1$-re. Mivel t_i, s_i, r_i ugyanazt a rekurziót követi az egyenlőség minden i-re igaz, tehát k-ra is. Azt már beláttunk, hogy $(a, b) = r_k$, tehát s_k, t_k valóban Bézout-együttható pár. □

A következő lépés, hogy a bemeneti mátrixot a (5) formula alapján felbontjuk $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{F}_q$ alakú mátrixok szorzatára.

Ezután egyszerűen maradékos osztással meghatározzuk a Horner elrendezésben szereplő együtthatókat, a fenti felbontásban szereplő mindhárom a-ra, ahol θ az előző bekezdésben meghatározott primitív gyök.

Végül annyi marad hátra, hogy a fenti együtthatóknak megfelelően előállítjuk a (7) képletben szereplő szót.

4.4. A konstans meghatározása $PSL(2, \mathbb{Z}_q)$-ban

A 2.24 tételben azt állítottuk, hogy:

$$\operatorname{diam}(\operatorname{Cay}(PSL(2, \mathbb{Z}_q), S)) \leq Cn^2 \log q \leq C4 \log q \tag{13}$$

a tételben meghatározott S-re. Az alkalmazások szempontjából természetesen felmerül a kérdés, hogy C értéke mennyi.

Ezt megkaphatjuk, ha a tétel bizonyításában mindig számon tartjuk a konstansokat. Ez egy biztos felső korlátot jelent, viszont a gyakorlatban sokkal fontosabb, hogy a mi adott megvalósításunkban mekkora ez a C érték. Ehhez különböző q-kra vettem elég sok véletlen $A \in PSL(2, \mathbb{Z}_q)$ mátrixot, kiszámoltam a felbontásukat és vettem ezek hosszának az átlagát.

A véletlen mátrixokat úgy generáltam, hogy három elemüket a nyelv beépített „rand()” függvényével egyenletesen választottam, a negyediket pedig úgy, hogy a determináns ± 1 legyen. Feltételezem, hogy ez a $PSL(2, \mathbb{Z}_q)$ csoporton is közel van az egyenletes eloszláshoz. Lehetne véletlen elemeket venni a csoportból A 4.2 fejezethez hasonlóan, viszont akkor itt is felmerül a probélma, hogy még nem ismerjük a konstanst a 13 egyenlőtlenségből. A 6 ábra mutatja q értékeit, a felbontások hosszának átlagát egy húsz elemű mintán, és a $4 \log q$ értékeket.

q	átlag	4*log(q)	q	átlag	4*log(q)
3	4.65	4.39445	13	13.45	10.2598
9	11.05	8.7889	169	26.05	20.5196
27	17.6	13.1833	2197	45.25	30.7794
81	24.95	17.5778	28561	62.1	41.0392
5	7.2	6.43775	17	20.1	11.3329
25	17.25	12.8755	289	37.8	22.6657
125	25.85	19.3133	4913	62.6	33.9986
625	35.7	25.751	83521	74.35	45.3314
7	10.65	7.78364	19	14.8	11.7778
49	22.85	15.5673	361	32.35	23.5555
343	40.05	23.3509	6859	56.6	35.3333
2401	57.55	31.1346	130321	74.4	47.111
11	12.4	9.59158	23	36.65	12.542
121	28.5	19.1832	529	75.1	25.084
1331	40.15	28.7747	12167	115.95	37.6259
14641	55.2	38.3663	279841	75.95	50.1679

6. ábra. $G = S_3$ és $S = S_3$

Ebből az látszik, hogy a konstans értéke körülbelül 2 lehet.

4.5. Véletlen elem generálása $PSL(2, \mathbb{Z}_q)$-ben

Az előző fejezetben meghatározott konstans segítségével és a 12 egyenlőtlenség segítségével ugyanúgy mint a 4.2 fejezetben könnyen generálhatunk elemeket az egyenletes eloszlásból $PSL(2, \mathbb{Z}_q)$-n. Mivel itt a tétel tetszőleges q-ra működik a futásidő nem okoz gondot.

Hivatkozások

[1] N. Alon and F. R. K. Chung. Explicit construction of linear sized tolerant networks, Discrete Math., 72:15–19, 1989.

[2] N. Alon and V. D. Milman: $\lambda 1$, isoperimetric inequalities for graphs, and superconcentrators, J. Combin. Theory Ser. B, 38(1)

[3] László Babai, Robert Beals, Ákos Seress: On the diameter of the symmetric group: polynomial bounds, Proc. 15th Ann. Symp. on Discrete Algorithms (SODA'04), ACM–IEEE 2004, pp. 1108–1112

[4] L. Babai, W. M. Kantor and A. Lubotsky: Small diameter Cayley-graphs for finite simple groups, European Journal of Combinatorics, 10, 1989

[5] P. Buser: A note on the isoperimetric constant, Ann. Sci. Ecole Norm. Sup. (4), 15(2):213–230, 1982

[6] J. Cheeger: A lower bound for the smallest eigenvalue of the Laplacian, Problems in analysis, oldalszám: 195–199. Princeton Univ. Press, Princeton, NJ, 1970

[7] J. D. Dixon: The probability of generating the symmetric group. Math. Z. 110, 1969

[8] H. A. Helfgott, Á. Seress, and A. Zuk: Random generators of the symmetric group: diameter, mixing time and spectral gap, arXiv:1311.6742 [math.GR]

[9] M. R. Jerrum: The complexity of finding minimum length generator sequences. Theoretical Computer Science 36, 1985

[10] Shlomo Hoory, Nathan Linial, and Avi Widgerson: Expander graphs and their application, Bulletin of the American Mathematcal Society, 43, 2006

[11] M. Kassabov and T. R. Riley: Diameters of Cayleygraphs of Chevalley groups, European Journal of Combinatorics, 28(3), pages 791–800, 2007

[12] Kiss E: Bevezetés az algebrába, Typotex (2007)

[13] L. Lovász: Eigenvalues of graphs, 2007

[14] Péter Pál Varjú: Random walks in compact groups, Ducumenta Mathematica, 18, 2013

[15] O. Perron: Zur Theorie der Matrices Mathematische Annalen, 64(2), 1907