



Debreceni Egyetem
Természettudományi és Technológiai Kar
Matematikai Intézet

Diplomamunka

Diszkrét logaritmus probléma sandpile csoportban

készítette:

Dsupin Krisztián

témavezető: Dr. Tengely Szabolcs

Debrecen, 2020

Tartalomjegyzék

1.	Bevezetés	3
2.	Sandpile modell	4
2.1.	Alapfogalmak	4
2.2.	Monodrómia párosítás	9
2.3.	Diszkrét logaritmus probléma gráfok jacobianján	10
2.4.	Algoritmus	10
3.	Módosított kerékgráf	12
3.1.	$\overline{W}_n$ -beli diszkrét logaritmus probléma megoldása	12
4.	Négyzetes körgráf	18
4.1.	C_n^2 -beli diszkrét logaritmus probléma megoldása	19
5.	Általánosított inverz	26
6.	Függelék	29

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőmnek, Dr. Tengely Szabolcsnak, aki nélkülözhetetlen tanácsaival, szakértelmével és folyamatos segítségével nagyban hozzájárult a diplomamunkám létrejöttéhez. Köszönettel tartozom továbbá családomnak és barátaimnak a támogatásukért, amivel segítették, hogy ez a dolgozat elkészülhessen.

1. Bevezetés

Körülbelül 30 éve, 1987-ben jelent meg Bak, Tang és Wiesenfeld forradalmi cikke, melyben bemutatták a rácsmodellt, amit ők "self-organised criticality" névvel illettek [1]-ben. Megjelenése óta a modell erősen vizsgált témakörre vált mind a matematikai, mind a fizikai irodalomban. A modellben apró hatások komplex rendszerek felbukkanásához vezethetnek, mely a rendszert egy stacionárius állapot felé mozdítja. Számos modellt indított útjának a szerzők cikke, például Olami–Feder–Christensen modell [2], mely földrengések modellezését szolgálja, vagy forest-fire modell [3], amit erdőtüzek szimulálása motivált, azonban járványok vizsgálatakor is hasznosítható [4]. Ezenfelül az agykutatás területén is alkalmazott [5], az agyi aktivitások leírására. A teljesség igénye nélkül alkalmazott továbbá biológiai, társadalmi területeken, és tőzsdei fluktuációk elemzésekor is.

Egy megfelelő reprezentációs csoport keresése a diszkrét logaritmus probléma számára a mai napig egy népszerű problémakör a kriptográfiában. Az elliptikus görbék egyre széleskörűbb használata kitűnő példa arra, hogy a diszkrét logaritmus probléma alkalmas hatékony kriptográfiai protokollok megvalósítására, ugyanis az RSA mellett napjaink egyik legelterjedtebb kriptorendszere, melyet használnak kulcscsere protokollok, digitális aláírások és pszeudorandom számok generálására is.

Általánosan a diszkrét logaritmus probléma az alábbi módon fogalmazható meg. Amennyiben G multiplikatív csoport, $g, h \in G$, keresett olyan x , melyre $g^x = h$. Ha H additív csoport $P, Q \in H$, akkor keresett y , melyre $yP = Q$. A probléma megoldása megfelelő csoportok esetén számításilag nehéz, így alkalmasak kriptográfiai protokollok felhasználására. Whitfield Diffie és Martin Hellman 1976-ban javasolták kulcscsere megvalósítására, majd Taher ElGamal 1985-ben nyilvános kulcsú kriptorendszert mutatott be, melyek mind a diszkrét logaritmus problémán alapulnak. Emellett egyéb érdekesebb nemkommutatív csoportokban is definiáltak diszkrét logaritmus problémát, például [6]-ban. Azonban mindennapi használatban főleg a véges testek feletti elliptikus görbék váltak elterjedté.

A két talán elsőre idegennek tűnő témakört kapcsolta össze Biggs [7]-ben. Kriptográfiai használatra javasolt bizonyos gráf családoknak sandpile modell segítségével értelmezhető csoportját. Azonban egymástól függetlenül [8]-ban és [9]-ben is bemutatták ennek hatékony megoldhatóságát. A diplomamunkámban két gráfcsalád felett értelmezett diszkrét logaritmus probléma kerül bemutatásra, azok megoldhatóságával együtt.

2. Sandpile modell

2.1. Alapfogalmak

2.1. Definíció. Legyen $G = (V, E)$ multigráf, ahol $V = \{v_1, \dots, v_n\}$ a csúcsok halmaza, valamint $e = (u, v) \in E \subseteq V \times V$ az élek halmaza, továbbá, ha $u = v$, ekkor az $e = (u, v)$ élt hurokélnek nevezzük. Ezek megengedettek, de nem tesznek hozzá sokat elméleti szempontból, így feltesszük, hogy G hurokélmentes.

Legyen $w : V \times V \rightarrow N$ egy súlyfüggvény, ahol $w(u, v) > 0$ pontosan akkor, ha $(u, v) \in E$.

Legyen $u, v \in V$, ekkor v -t elérhetőnek nevezzük u -ból, ha létezik éleknek olyan sorozata, amely u -ban kezdődik és v -ben végződik. Egy csúcsot globálisan elérhetőnek vagy nyelőnek nevezünk, ha G minden csúcsából elérhető. A következőkben feltesszük, hogy G -nek létezik legalább egy globálisan elérhető csúcsa.

Egy $v \in V$ csúcs kifoka alatt azt a $d^+(v)$ nemnegatív egészet értjük, ami a v -ből induló élek súlyainak összege, befoka alatt a $d^-(v)$ -vel jelölt nemnegatív egészet, ami a v -be érkező élek súlyainak összege.

2.2. Definíció. A (V, E, s) rendezett hármast sandpile gráfnak nevezzük, ha (V, E) irányított multigráf, $s \in V$ pedig globálisan elérhető csúcs.

Továbbá ha $d^-(s) = 0$, akkor abszolút nyelőnek nevezzük. Jelölje a nemnyelő csúcsokat $\tilde{V} := V \setminus \{s\}$. Egy sandpile gráf nyelő csúcsának abszolút nyelőnek kell lennie, de a témakörben a legtöbb esetben érdemi változás nélkül eltávolíthatjuk a nyelőből kiinduló éleket. Továbbá egy $G = (V, E, s)$ sandpile gráfra gyakran csak (V, E) gráfként hivatkozunk.

2.1. Megjegyzés. Egy sandpile gráfra szemléletesen tekinthetünk úgy, mintha homokszemeket helyeznénk egy gráf csúcsaira. Azt szeretnénk modellezni, hogy hogyan viselkedik a gráf által alkotott rendszer, ha folyamatosan új homokszemeket pakolunk a csúcsaira. Ahogy a homokvárak is, amint túl sok szem kerül egy adott pontra, akkor az ledől, és homokszemek további pontok felé mozdulnak. Egy sandpile gráf esetében annak teherbírását a kifoka határozza meg, a ledőlés utáni homokszemek helyzetét pedig a ledöntött éllel szomszéd csúcsok adják.

2.3. Definíció. Legyen X véges halmaz, ekkor $\mathbb{Z}X = \left\{ \sum_{x \in X} a_x x \mid a_x \in \mathbb{Z}, \forall x \in X \right\}$

egy szabad Abel-csoport X -n. Megszorítva nemnegatív együtthatókra hasonlóan adódik $\mathbb{N}X$.

2.4. Definíció. Legyen G sandpile gráf $v_1, \dots, v_n$ csúcsokkal.

G Laplace-leképezése alatt a $\Delta : \mathbb{Z}V \rightarrow \mathbb{Z}V$ csúcson értelmezett leképezést értjük, ahol:

$$\Delta(v) := d^+(v)v - \sum_{u \in V} w(v, u)u.$$

G redukált Laplace-leképezése alatt $\tilde{\Delta} : \mathbb{Z}\tilde{V} \rightarrow \mathbb{Z}\tilde{V}$ nemnyelő csúcsokon értelmezett leképezést értünk, ahol:

$$\tilde{\Delta}(v) := d^+(v)v - \sum_{u \in \tilde{V}} w(v, u)u.$$

Legyen $D = \text{diag}(d^-(v_1), \dots, d^-(v_n))$ diagonális mátrix, A a G szomszédsági mátrixa, vagyis $A_{ij} = w(v_i, v_j)$. Ekkor G Laplace-mátrixa $L = D - A$.

Továbbá egy G gráf Δ Laplace-leképezése megegyezik L transzponáltjával. A Laplace-leképezés és Laplace-mátrix sok esetben megkönnyíti a számolást a sandpile csoportban, például generátor keresésben vagy rend kiszámolásban.

2.1. Tétel (Kirchoff). Egy G gráf feszítő fájnak száma megegyezik tetszőleges redukált Laplace-mátrixának determinánsával.

2.5. Definíció. Egy G feletti konfiguráció alatt egy $c : V \rightarrow \mathbb{Z}$ függvényt értünk, amire $c(v) \geq 0$ minden $v \in V^*$ esetén, továbbá $c(s) = - \sum_{v \in \tilde{V}} c(v)$.

Jelölésben $c = (c_1, \dots, c_n)$.

2.6. Definíció. Egy c konfigurációt stabilnak nevezünk egy $v \in \tilde{V}$ csúcsban, ha $c(v) \leq d^-(v)$. Ellenkező esetben c instabil.

Egy konfigurációt stabilnak nevezünk, ha minden csúcsban stabil.

2.7. Definíció. Amennyiben c instabil egy v csúcsban, ekkor v ledőlhet, ami egy $\tilde{c}$ konfigurációba jutását jelenti, ahol redukáljuk $c(v)$ értékét $d^-(v)$ -vel, és v minden w szomszédja esetén növeljük $c(w)$ értékét eggyel. Vagyis:

$$\tilde{c}(v) = \begin{cases} c(u) - d^-(u), & \text{ha } u = v, \\ c(u) + 1, & \text{ha } u \text{ és } v \text{ szomszédosak,} \\ c(v), & \text{egyéb esetben.} \end{cases}$$

Ha c instabil v csúcsban, akkor v ledöntését megengedettnek nevezzük.

2.2. Megjegyzés. Egy c konfigurációra alkalmazva egy megengedett ledöntési sorozat eredményeképp létrejövő konfiguráció leírható

$$\tilde{c} = c - d^-(v)v + \sum_{u \in \tilde{V}} w(u, v)u = c - \tilde{\Delta}v.$$

2.8. Definíció. Egy $v_1, \dots, v_k$ nem nyelő csúcsok sorozata megengedett ledöntési sorozat c konfigurációra nézve, amennyiben v_1 megengedett, továbbá $v_1, \dots, v_{i-1}$ ledöntéséből keletkező konfiguráció következtében v_i ledöntése is megengedett.

Egy c konfigurációra alkalmazva egy megengedett ledöntési sorozat eredményeképp létrejövő konfiguráció leírható $\tilde{c} = c - \tilde{\Delta}\sigma$, ahol $\sigma \in \mathbb{Z}\tilde{V}$, σ_v pedig a v csúcs előfordulásának száma a sorozatban. Ez jelölésben $c \xrightarrow{\sigma} c - \tilde{\Delta}\sigma$.

2.2. Tétel. Legyen c egy sandpile konfiguráció.

1. Ekkor létezik $\tilde{c}$ stabil konfiguráció, amire $c \rightarrow \tilde{c}$.
2. Tegyük fel, hogy $c \rightarrow \tilde{c}$ egy σ ledöntési vektorral, és $c \rightarrow \tilde{c}'$ egy σ' . Ha $\tilde{c}$ stabil, akkor $\sigma' \geq \sigma$. Ha $\tilde{c}$ és $\tilde{c}'$ is stabil, akkor $\tilde{c} = \tilde{c}'$.

2.9. Definíció. Legyen c egy G feletti konfiguráció, ekkor c stabilizálása egy egyértelmű $\tilde{c}$ stabil konfiguráció, amelyre $c \rightarrow \tilde{c}$, mely jelölésben c° .

2.10. Definíció. Jelölje $\mathcal{M}$ a nemnegatív, stabil konfigurációkat G felett. Ekkor $\mathcal{M}$ kommutatív monoid a stabilizáló összeadásra nézve, vagyis

$$a \circledast b := (a + b)^\circ.$$

A stabilizáló összeadás $N\tilde{V}$ -beli összeadás, amit stabilizálás követ. Az egység a nulla konfiguráció.

2.11. Definíció. Egy c konfiguráció elérhető, ha minden a konfiguráció esetén létezik b konfiguráció, hogy $a + b \rightarrow c$, továbbá visszatérő, ha nemnegatív, elérhető és stabil.

2.12. Definíció. A G feletti maximálisan stabil konfiguráció alatt az alábbiértjük:

$$c_{\max} = \sum_{v \in \tilde{V}} (d^+(v) - 1)v.$$

2.1. Állítás. Egy c konfiguráció visszatérő pontosan akkor, ha létezik olyan $a \geq 0$ konfiguráció, hogy $c = a \circledast c_{\max}$.

2.3. Tétel. A G feletti visszatérő konfigurációk csoportot alkotnak a stabilizáló összeadásra nézve.

2.13. Definíció. A G feletti visszatérő konfigurációk csoportját sandpile csoportnak nevezzük és jelölése $\mathcal{S}(G)$.

2.3. Megjegyzés. 2.1 miatt egy sandpile csoport elemeit úgy is megkaphatjuk, ha szisztematikusan homokszemeket adunk a $c_{\max}$ konfigurációhoz, majd stabilizálunk.

2.4. Megjegyzés. Szemléletesen egy konfiguráció egy a gráf minden csúcsában adott homokszemek listája. Egy ilyen konfigurációt stabilnak mondunk, ha minden csúcsban a homokszemek száma kevesebb, mint a csúcs teherbírása. Ha instabil konfigurációhoz jutunk, a rendszer stabilizálja önmagát és ledönti az instabil csúcsokat. Egy instabil csúcsból annak stabilizálása során minden szomszédos csúcsba átkerül egy homokszem, így az eredeti csúcsban a kifok mértékével csökken, a szomszédos csúcsokban egyel-egyel nő a homokszemek száma. A rendszer stabilizálása addig tart, ameddig minden csúcs nem stabilizálódik, amely véges sok lépésben megtörténik, mivel létezik nyelő csúcs, ami a rendszerben felhalmozódott instabilitást okozó homokszemeket elnyeli.

2.14. Definíció. Legyen $\mathcal{L} \subset \mathbb{Z}V$ Laplace-rács a Δ képe, $\tilde{\mathcal{L}} \subset \mathbb{Z}\tilde{V}$ redukált Laplace-rács a $\tilde{\Delta}$ képe. Ekkor G kritikus csoportja

$$\mathcal{C}(G) = \mathbb{Z}\tilde{V}/\tilde{\mathcal{L}}.$$

2.4. Tétel. Létezik $\mathcal{S}(G)$ és $\mathcal{C}(G)$ között izomorfizmus az alábbi módon:

$$\begin{aligned} \mathcal{S}(G) &\rightarrow \mathcal{C}(G) \\ c &\mapsto c + \tilde{\mathcal{L}}. \end{aligned}$$

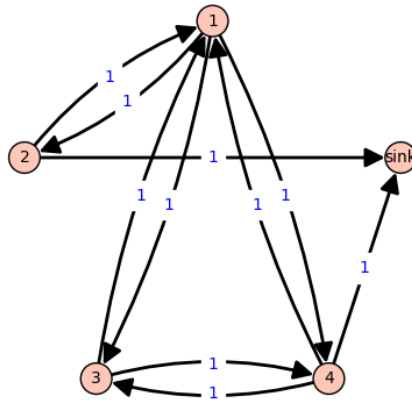
Továbbá az $\mathcal{S}(G)$ sandpile csoport η egységeleme az alábbi módon számolható:

$$\eta = ((c_{\max} - (2c_{\max})^\circ) + c_{\max})^\circ.$$

2.1. Példa. Példaként tekintsük az alábbi G gráfot:

- $V(G) = \{v_1, v_2, v_3, v_4, s\}$
- $E(G) = \{(v_1, v_2, 1), (v_1, v_3, 1), (v_1, v_4, 1), (v_2, s, 1), (v_3, v_4, 1), (v_4, s, 1)\}$

ahol (v_i, v_j, w) jelöli a v_i és v_j közötti w súlyú élt.



Az így adódó gráf nyelő nélküli kifokai rendre $(3, 2, 2, 3)$, amik meghatározzák egy adott konfiguráció stabilitását.

Vegyük például a $c = (4, 0, 1, 0)$ konfigurációt, amely instabil a v_1 csúcsban, mivel a konfiguráció v_1 -re eső eleme nagyobb, mint annak kifoka. Stabilizálásához v_1 csúcsot ledöntve egy-egy homokszem áramlik a szomszédaiba, azaz v_2, v_3, v_4 csúcsokba. Így a $(1, 1, 2, 1)$ konfigurációhoz jutunk. Ekkor azonban v_3 válik instabillá, amit ledöntve a már stabil $(2, 1, 0, 2)$ konfigurációhoz jutunk.

Összefoglalva a stabilizálást: $(4, 0, 1, 0) \rightarrow (1, 1, 2, 1) \rightarrow (2, 1, 0, 2)$.

A konfigurációk között akadnak olyanok, melyek érhetők önmagukból indulva legális operációsorozat végrehajtásával. Ezek a visszatérő konfigurációk, melyek $\mathcal{S}(G)$ csoportot alkotják.

Az $\mathcal{S}(G)$ csoport elemszáma megegyezik a feszítő fájnak számával 2.1 miatt, melyet az $\bar{L}$ redukált Laplace-mátrixának determinánsából kapunk. Az L -ből a nyelő csúcshoz tartozó sort és oszlopot elhagyva kapjuk:

$$\bar{L} = \begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 2 & 0 & 0 \\ -1 & 0 & 2 & -1 \\ -1 & 0 & -1 & 3 \end{pmatrix}.$$

Továbbá ekkor $\det(\bar{L}) = 11$, így a csoport elemszáma is 11.

Mivel $c_{max} = (2, 1, 1, 2)$, így 2.4 felhasználásával a csoport egységeleme a következő:

$$\begin{aligned} \eta &= ((c_{max} - (2c_{max})^\circ) + c_{max})^\circ \\ &= (((2, 1, 1, 2) - (4, 2, 2, 4)^\circ) + (2, 1, 1, 2))^\circ \\ &= (((1, 1, 1, 2) - (1, 1, 1, 2)) + (2, 1, 1, 2))^\circ \\ &= (((1, 1, 1, 2) - (1, 1, 1, 2)) + (2, 1, 1, 2))^\circ \\ &= (((1, 1, 1, 2) - (1, 1, 1, 2)) + (2, 1, 1, 2))^\circ \\ &= ((3, 1, 1, 2))^\circ \\ &= (2, 1, 1, 0) \end{aligned}$$

Továbbá visszatérő konfigurációk az alábbiak:

$c_1 = (2, 1, 1, 2)$	$c_2 = (2, 0, 1, 2)$	$c_3 = (1, 1, 1, 2)$	$c_4 = (1, 0, 1, 2)$
$c_5 = (0, 1, 1, 2)$	$c_6 = (1, 1, 0, 2)$	$c_7 = (2, 0, 0, 2)$	$c_8 = (2, 1, 0, 2)$
$c_9 = (2, 1, 0, 1)$	$c_{10} = (2, 1, 1, 1)$	$c_{11} = (2, 1, 1, 0)$	

$\mathcal{S}(G)$ Cayley-táblázata az alábbi:

	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}
c_1	c_3	c_4	c_5	c_9	c_8	c_{10}	c_{11}	c_6	c_7	c_2	c_1
c_2	c_4	c_5	c_9	c_8	c_7	c_1	c_{10}	c_{11}	c_6	c_3	c_2
c_3	c_5	c_9	c_8	c_7	c_6	c_2	c_1	c_{10}	c_{11}	c_4	c_3
c_4	c_9	c_8	c_7	c_6	c_{11}	c_3	c_2	c_1	c_{10}	c_5	c_4
c_5	c_8	c_7	c_6	c_{11}	c_{10}	c_4	c_3	c_2	c_1	c_9	c_5
c_6	c_{10}	c_1	c_2	c_3	c_4	c_7	c_8	c_9	c_5	c_{11}	c_6
c_7	c_{11}	c_{10}	c_1	c_2	c_3	c_8	c_9	c_5	c_4	c_6	c_7
c_8	c_6	c_{11}	c_{10}	c_1	c_2	c_9	c_5	c_4	c_3	c_7	c_8
c_9	c_7	c_6	c_{11}	c_{10}	c_1	c_5	c_4	c_3	c_2	c_8	c_9
c_{10}	c_2	c_3	c_4	c_5	c_9	c_{11}	c_6	c_7	c_8	c_1	c_{10}
c_{11}	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}

2.2. Monodrómia párosítás

A továbbiakban célunk egy a csoporton értelmezett diszkrét logaritmus problémát megoldó algoritmus bemutatása, melyet Shokrieh [9]-ben mutatott be. A sandpile csoportok megközelíthetők görbeelméleti szemszögből is, melyet a mi esetünkben az elliptikus görbéken ismert MOV támadás alapjául szolgáló bilineáris párosítás motivál.

2.15. Definíció. Egy G gráf divizorán az alábbi $V(G)$ által generált szabad Ábel-csoportot értjük:

$$Div(G) = \left\{ \sum_{v \in V} a_v(v) \mid a_v \in \mathbb{Z} \right\}.$$

G divizorainak elemeire gondolhatunk úgy, mint egyesített lineáris kombináció a gráfok csúcsain. Továbbá $Div(G)$ elemeit divizornak nevezzük. Egy D divizor esetén egy v csúcs együtthatóját jelölje $D(v)$.

Legyen $\mathcal{M}(G) = Hom(V, \mathbb{Z})$ Abel-csoport, mely minden egész értékű függvényt tartalmaz, amik a gráf csúcsain értelmezettek.

Legyen $f \in \mathcal{M}(G)$, valamint jelölje $ord_v(f) = \sum_{u, v \in E} (f(u) - f(v))$, ekkor legyen

$$div(f) = \sum_{v \in V} ord_v(f)v.$$

Tekintsük $deg : Div(G) \rightarrow \mathbb{Z}$ csoport homomorfizmust az alábbiak szerint:

$$deg(D) = \sum_{v \in V} D(v).$$

Definiálj a $Prin(G) = \{div(f) \in Div(G) \mid f \in \mathcal{M}(G)\}$ a fő divizorok csoportját.

Jelölje $Div^0(G)$ a homomorfizmus magját, vagyis ami tartalmazza a nulla fokú divizorokat.

G Jacobianja alatt a következőt értjük:

$$\text{Jac}(G) = Div^0(G) \backslash \text{Prin}(G).$$

2.2. Állítás. Legyenek $D_1, D_2 \in Div^0(G)$, továbbá m_1, m_2 egészek, hogy $m_1 D_1 = \text{div}(f_1)$ és $m_2 D_2 = \text{div}(f_2)$, ekkor megmutatható, hogy

$$\frac{1}{m_2} \sum_{v \in V} D_1(v) f_2(v) = \frac{1}{m_1} \sum_{v \in V} D_2(v) f_1(v).$$

2.16. Definíció. Jelölje $\langle \cdot, \cdot \rangle : Div^0(G) \times Div^0(G) \rightarrow \mathbb{Q}$:

$$\langle D_1, D_2 \rangle = \frac{1}{m_2} \sum_{v \in V} D_1(v) f_2(v).$$

Ekkor a párosítás szimmetrikus és bilineáris.

2.17. Definíció. Legyen A mátrix, ekkor minden P mátrixot, melyre $APA = A$ teljesül, az A mátrix pszeudoinverzének vagy általánosított inverzének nevezzük.

2.2. Példa. Legyen J az $n \times n$ -es csak egyesekből álló mátrix. Ekkor Q mátrix esetén $Q + \frac{1}{n}J$ reguláris, továbbá $Q^+ = (Q + \frac{1}{n}J)^{-1} - \frac{1}{n}J$ mátrix a Q pszeudoinverze. Sőt ezt Q Moore-Penrose pszeudoinverzének is nevezzük, mivel ellenőrizhető, hogy $QQ^+ = Q^+Q = I - \frac{1}{n}J$ és $Q^+QQ^+ = Q^+$ is teljesül.

2.5. Tétel. Legyen P tetszőleges pszeudoinverze L Laplace-mátrixnak, ekkor a monodrómia párosítás a következő módon adott:

$$\langle \overline{D_1}, \overline{D_2} \rangle = [D_1]^T P [D_2] \pmod{\mathbb{Z}}.$$

2.3. Diszkrét logaritmus probléma gráfok jacobianján

Tekintsünk egy G gráfot, ahol $\text{Jac}(G)$ ciklikus csoport, ekkor a csoport felett megadható diszkrét logaritmus problémát szeretnénk megoldani a monodrómia párosítás segítségével. Továbbá tegyük fel, hogy $\text{Jac}(G)$ egy generátora is ismert.

2.4. Algoritmus

Bemenet: $D_1, D_2 \in Div^0(G)$, ahol $\overline{D_2} = x \cdot \overline{D_1}$ teljesül $\text{Jac}(G)$ -ben

Kimenet: $x \pmod{\text{ord}(\overline{D_1})}$

Algoritmus:

1. Számoljuk ki $\langle \overline{D_1}, g \rangle = r_1 + \mathbb{Z}$ és $\langle \overline{D_2}, g \rangle = r_2 + \mathbb{Z}$ a 2.5 formula segítségével.
2. Oldjuk meg a $r_2 = r_1x + y$ diofantikus egyenletet $x \pmod{\text{ord}(\overline{D})}$ érték meghatározásához.

Algoritmus elemzése

Mivel a monodrómia párosítás bilineáris, ezért: $\langle \overline{D_2}, g \rangle = x \langle \overline{D_1}, g \rangle$, vagyis $r_2 = r_1x \pmod{\mathbb{Z}}$ -ben. Ahhoz, hogy belássuk, hogy a diofantikus egyenlet megoldása pont $x \pmod{\text{ord}(\overline{D})}$ értéket adja, tekintsük az alábbi lemmát.

2.1. Lemma. Legyen g generátora $\text{Jac}(G)$ ciklikus csoportban. Legyen h tetszőleges eleme $\text{Jac}(G)$ -nek. Ha $\langle h, g \rangle = \frac{a}{b} + \mathbb{Z}$, ahol $a, b \in \mathbb{Z}, \text{lnko}(a, b) = 1$, ekkor h rendje $\text{Jac}(G)$ -ben b .

Bizonyítás. Legyen h rendje $\text{Jac}(G)$ -ben γ . A monodrómia párosítás bilinearitása miatt:

$$\frac{\gamma a}{b} + \mathbb{Z} = \gamma \langle h, g \rangle = \langle \gamma \cdot h, g \rangle = \langle 0, g \rangle = \mathbb{Z}.$$

Vagyis emiatt $b \mid \gamma$.

A másik oldalról

$$\langle b \cdot h, g \rangle = b \langle h, g \rangle = a + \mathbb{Z} = \mathbb{Z}.$$

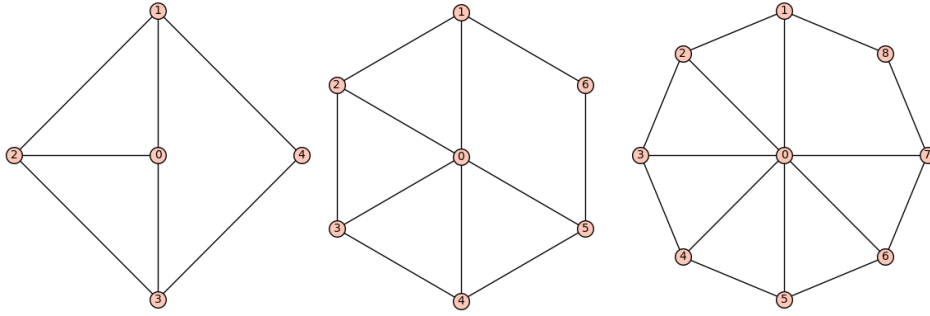
Mivel $\text{Jac}(G)$ ciklikus és a monodrómia párosítás bilineáris, minden $\text{Jac}(G)$ -beli elem triviálisan párosítható $b \cdot h$ -val. A monodrómia párosítás nem-elfajultsága miatt $b \cdot h = 0$, ami miatt $\gamma \mid b$.

Vagyis $\gamma = b$. □

Mivel $\overline{D_2} = x \overline{D_1}$, ezért $\overline{D_2}$ rendje osztja $\overline{D_1}$ rendjét, ami 2.1 miatt $r = \frac{a}{b}$ ($a, b \in \mathbb{Z}, \text{lnko}(a, b) = 1$), b pedig $\overline{D}$ rendje $\text{Jac}(G)$. Ekkor b -vel szorozva $r_2 = r_1x + y$ -ből kapjuk $ax + by = c$ egyenletet valamely c egészre. Ekkor az adott $ax + by = c$ ($\text{lnko}(a, b) = 1$) lineáris diofantikus egyenletnek létezik megoldása, és x meghatározott modulo b .

3. Módosított kerékgráf

Legyen n pozitív egész, W_{2n+1} pedig a $2n+1$ csúcsú kerékgráf, ami áll egy $v_1, \dots, v_{2n+1}$ csúcsokból álló "abroncs", és w "középpont" részéből. Ekkor w szomszédos v_i -vel minden $1 \leq i \leq 2n+1$ esetén. Jelölje $\overline{W}_n$ azt a gráfot, amit a következő módosításokkal kapunk W_{2n+1} -ből: adjunk egy új v_{2n+2} csúcsot a gráfhoz, amiket kössön él v_1 és v_{2n+1} csúcsokhoz, továbbá töröljük a v_1 és v_{2n+1} csúcsokat összekötő élt.



Jelölje $\overline{W}_n$ csúcsainak halmazát V , éleinek halmazát E . Valamint legyen $V^* = V \setminus \{q\}$, ami szemléletesen a módosított kerékgráf abroncsa.

Ekkor a $G = (V, E, w)$ sandpile gráfból keletkezett $\mathcal{S}(G)$ -n definiálható diszkrét logaritmus probléma. Vagyis adott g generátor $\mathcal{S}(G)$ -n, valamint $b, c \in \mathcal{S}(G)$ konfiguráció, ekkor keresett olyan $x \in \mathbb{Z}$, hogy $c_2 = (x \cdot c_1)^\circ$.

3.1. $\overline{W}_n$ -beli diszkrét logaritmus probléma megoldása

Ennek megoldása a 2.4 fejezetben leírt módon történik. A gráf ismeretében, mely csak egy n paramétertől függ. Ekkor kiszámítható az $L = D - A$ Laplace-mátrix, valamint az ahhoz tartozó P pszeudinverz például, 2.2 alapján. Kiszámítható továbbá $\mathcal{S}(G)$ generátor eleme, majd a generátor elemhez tartozó divizor, ami $g = (g_1, \dots, g_{2n+2})$ konfiguráció esetén: $D_g = (-\sum_{i=1}^{2n+2} g_i, g_1, \dots, g_{2n+2})$ vektorral leírható. Hasonlóan kiszámítjuk a c_1 és c_2 konfigurációkhoz tartozó D_{c_1}, D_{c_2} divizorokat is. Majd az algoritmus 1 pontja szerint, felhasználva 2.5 állítást kiszámoljuk $D_{c_1} \cdot P \cdot D_g$ és $D_{c_2} \cdot P \cdot D_g$, amelyekből keletkező diofantikus egyenletet megoldva adódik a megoldás.

3.1. Példa. Tekintsük példaként az 5 csúcsú módosított kerékgrafot. Legyenek $c_1 = (2, 1, 1, 1)$ és $c_2 = (1, 0, 2, 1)$ tetszőlegesen választott konfigurációk.

Ekkor a gráf Laplace-mátrixa:

$$L = D - A = \begin{pmatrix} 3 & -1 & -1 & -1 & 0 \\ -1 & 3 & -1 & 0 & -1 \\ -1 & -1 & 3 & -1 & 0 \\ -1 & 0 & -1 & 3 & -1 \\ 0 & -1 & 0 & -1 & 2 \end{pmatrix}.$$

Pszéudoinverze:

$$P = \begin{pmatrix} \frac{47}{200} & -\frac{1}{25} & -\frac{3}{200} & -\frac{1}{25} & -\frac{7}{50} \\ -\frac{1}{25} & \frac{75}{17} & -\frac{25}{47} & -\frac{75}{17} & -\frac{25}{7} \\ -\frac{3}{200} & -\frac{1}{25} & \frac{200}{47} & -\frac{25}{17} & -\frac{50}{7} \\ -\frac{1}{25} & -\frac{8}{75} & -\frac{1}{25} & \frac{17}{75} & -\frac{1}{9} \\ -\frac{7}{50} & -\frac{1}{25} & -\frac{7}{50} & -\frac{1}{25} & \frac{25}{25} \end{pmatrix}.$$

Tekintve a sandpile csoportot, a generátor elem a $g = (2, 1, 1, 0)$ konfiguráció, amelyből képzett divizor $D_g = (-4, 2, 1, 1, 0)$.

Majd kiszámolva $D_{c_1} = (-5, 2, 1, 1, 1)$, $D_{c_2} = (-4, 1, 0, 2, 1)$ értékek adódnak.

Továbbá tekintsük a

$$D_{c_1} \cdot P \cdot D_g = (-5, 2, 1, 1, 1) \cdot \begin{pmatrix} \frac{47}{200} & -\frac{1}{25} & -\frac{3}{200} & -\frac{1}{25} & -\frac{7}{50} \\ -\frac{1}{25} & \frac{75}{17} & -\frac{25}{47} & -\frac{75}{17} & -\frac{25}{7} \\ -\frac{3}{200} & -\frac{1}{25} & \frac{200}{47} & -\frac{25}{17} & -\frac{50}{7} \\ -\frac{1}{25} & -\frac{8}{75} & -\frac{1}{25} & \frac{17}{75} & -\frac{1}{9} \\ -\frac{7}{50} & -\frac{1}{25} & -\frac{7}{50} & -\frac{1}{25} & \frac{25}{25} \end{pmatrix} \cdot \begin{pmatrix} -4 \\ 2 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{83}{12}$$

$$D_{c_2} \cdot P \cdot D_g = (-4, 1, 0, 2, 1) \cdot \begin{pmatrix} \frac{47}{200} & -\frac{1}{25} & -\frac{3}{200} & -\frac{1}{25} & -\frac{7}{50} \\ -\frac{1}{25} & \frac{75}{17} & -\frac{25}{47} & -\frac{75}{17} & -\frac{25}{7} \\ -\frac{3}{200} & -\frac{1}{25} & \frac{200}{47} & -\frac{25}{17} & -\frac{50}{7} \\ -\frac{1}{25} & -\frac{8}{75} & -\frac{1}{25} & \frac{17}{75} & -\frac{1}{9} \\ -\frac{7}{50} & -\frac{1}{25} & -\frac{7}{50} & -\frac{1}{25} & \frac{25}{25} \end{pmatrix} \cdot \begin{pmatrix} -4 \\ 2 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{16}{3}$$

Így $r = \frac{11}{12}$, $r' = \frac{1}{3}$ adódnak, amiből a $\frac{11}{12}x + y = \frac{1}{3}$ lineáris diofantikus egyenletet megoldva kapjuk az $x = 20$ megoldást.

Példa a diszkrét logaritmus megoldására SageMath programban

Gráf mérete

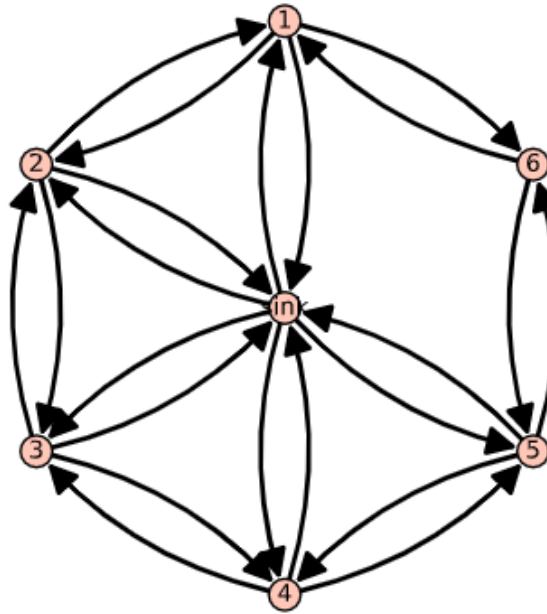


2

Választott konfigurációk

`[(1, 2, 2, 1, 2, 1), (2, 1, 0, 2, 1, 1)] ▼`

Legyenek a választott konfigurációk (1, 2, 2, 1, 2, 1) és (2, 1, 0, 2, 1, 1)



Adott G gráf esetén számítsuk ki Laplace matrixát, majd annak pszeudoinverzét.

Az így kapott $L = D - A$ Laplace mátrix:

$$\begin{pmatrix} 5 & -1 & -1 & -1 & -1 & -1 & 0 \\ -1 & 3 & -1 & 0 & 0 & 0 & -1 \\ -1 & -1 & 3 & -1 & 0 & 0 & 0 \\ -1 & 0 & -1 & 3 & -1 & 0 & 0 \\ -1 & 0 & 0 & -1 & 3 & -1 & 0 \\ -1 & 0 & 0 & 0 & -1 & 3 & -1 \\ 0 & -1 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

L pszeudoinverze:

$$\begin{pmatrix} \frac{86}{539} & -\frac{31}{1078} & -\frac{3}{1078} & \frac{2}{539} & -\frac{3}{1078} & -\frac{31}{1078} & -\frac{54}{539} \\ -\frac{1078}{31} & \frac{8624}{2489} & \frac{8624}{67} & -\frac{1078}{101} & -\frac{8624}{1011} & -\frac{8624}{745} & \frac{539}{16} \\ -\frac{1078}{3} & \frac{8624}{67} & \frac{8624}{2545} & \frac{1078}{25} & -\frac{8624}{689} & -\frac{8624}{1011} & \frac{539}{68} \\ -\frac{1078}{2} & \frac{8624}{101} & \frac{8624}{25} & \frac{1078}{163} & -\frac{8624}{25} & -\frac{8624}{101} & -\frac{539}{89} \\ \frac{539}{3} & -\frac{1078}{1011} & \frac{1078}{689} & \frac{539}{25} & \frac{1078}{2545} & -\frac{1078}{67} & -\frac{539}{68} \\ -\frac{1078}{31} & \frac{8624}{745} & -\frac{8624}{1011} & \frac{1078}{101} & \frac{8624}{67} & \frac{8624}{2489} & -\frac{539}{16} \\ -\frac{1078}{54} & -\frac{8624}{16} & -\frac{8624}{68} & -\frac{1078}{89} & \frac{8624}{68} & \frac{8624}{16} & \frac{539}{247} \end{pmatrix}$$

A $\mathcal{S}(G)$ sandpile csoport generátor eleme:
 $(2, 1, 1, 1, 1, 0)$

A generátor elemből kapott divisor vektor:
 $(-6, 2, 1, 1, 1, 0)$

A választott konfigurációkból kapott divisor vektorok:
 $D_b = (-9, 1, 2, 2, 1, 2, 1)$
 $D_c = (-7, 2, 1, 0, 2, 1, 1)$

Az 1. generátor felhasználásával:

$$D_b \cdot P \cdot D_g = (-9, 1, 2, 2, 1, 2, 1) \cdot \begin{pmatrix} \frac{86}{539} & -\frac{31}{1078} & -\frac{3}{1078} & \frac{2}{539} & -\frac{3}{1078} & -\frac{31}{1078} & -\frac{54}{539} \\ -\frac{1078}{31} & \frac{8624}{245} & \frac{8624}{67} & -\frac{1078}{101} & -\frac{8624}{689} & -\frac{8624}{1011} & -\frac{8624}{539} \\ -\frac{1078}{2} & \frac{8624}{101} & \frac{8624}{25} & \frac{1078}{163} & -\frac{8624}{25} & -\frac{8624}{101} & -\frac{8624}{539} \\ \frac{539}{3} & -\frac{1078}{1011} & -\frac{1078}{689} & \frac{539}{25} & \frac{1078}{245} & -\frac{1078}{67} & -\frac{539}{68} \\ -\frac{1078}{31} & \frac{8624}{145} & \frac{8624}{1011} & \frac{1078}{101} & \frac{8624}{67} & \frac{8624}{245} & -\frac{8624}{539} \\ -\frac{1078}{54} & -\frac{8624}{16} & -\frac{8624}{68} & -\frac{1078}{89} & \frac{8624}{68} & \frac{8624}{16} & \frac{8624}{539} \\ -\frac{539}{539} & \frac{539}{539} & -\frac{539}{539} & -\frac{539}{539} & -\frac{539}{539} & \frac{539}{539} & \frac{539}{539} \end{pmatrix} \cdot \begin{pmatrix} -6 \\ 2 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{945}{88} = 10 + \frac{65}{88}$$

$$D_c \cdot P \cdot D_g = (-7, 2, 1, 0, 2, 1, 1) \cdot \begin{pmatrix} \frac{86}{539} & -\frac{31}{1078} & -\frac{3}{1078} & \frac{2}{539} & -\frac{3}{1078} & -\frac{31}{1078} & -\frac{54}{539} \\ -\frac{1078}{31} & \frac{8624}{245} & \frac{8624}{67} & -\frac{1078}{101} & -\frac{8624}{689} & -\frac{8624}{1011} & -\frac{8624}{539} \\ -\frac{1078}{2} & \frac{8624}{101} & \frac{8624}{25} & \frac{1078}{163} & -\frac{8624}{25} & -\frac{8624}{101} & -\frac{8624}{539} \\ \frac{539}{3} & -\frac{1078}{1011} & -\frac{1078}{689} & \frac{539}{25} & \frac{1078}{245} & -\frac{1078}{67} & -\frac{539}{68} \\ -\frac{1078}{31} & \frac{8624}{145} & \frac{8624}{1011} & \frac{1078}{101} & \frac{8624}{67} & \frac{8624}{245} & -\frac{8624}{539} \\ -\frac{1078}{54} & -\frac{8624}{16} & -\frac{8624}{68} & -\frac{1078}{89} & \frac{8624}{68} & \frac{8624}{16} & \frac{8624}{539} \\ -\frac{539}{539} & \frac{539}{539} & -\frac{539}{539} & -\frac{539}{539} & -\frac{539}{539} & \frac{539}{539} & \frac{539}{539} \end{pmatrix} \cdot \begin{pmatrix} -6 \\ 2 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{775}{88} = 8 + \frac{71}{88}$$

Keressük az alábbi lineáris diofantikus egyenlet megoldását: $\frac{65}{88}x + y = \frac{71}{88}$

A diofantikus egyenlet megoldása:
 $x_1 = 39 \pmod{88}$

A diszkrét logaritmus probléma megoldása az $x = 39$.

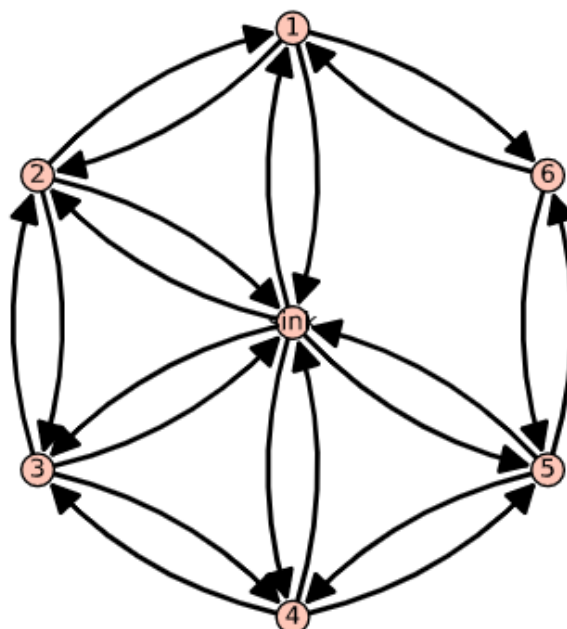
Gráf mérete



2

Választott konfigurációk

Legyenek a választott konfigurációk (1, 1, 2, 1, 2, 1) és (2, 2, 2, 1, 2, 1)

Adott G gráf esetén számítsuk ki Laplace matrixát, majd annak pszeudoinverzét.

Az így kapott $L = D - A$ Laplace mátrix:

$$\begin{pmatrix} 5 & -1 & -1 & -1 & -1 & -1 & 0 \\ -1 & 3 & -1 & 0 & 0 & 0 & -1 \\ -1 & -1 & 3 & -1 & 0 & 0 & 0 \\ -1 & 0 & -1 & 3 & -1 & 0 & 0 \\ -1 & 0 & 0 & -1 & 3 & -1 & 0 \\ -1 & 0 & 0 & 0 & -1 & 3 & -1 \\ 0 & -1 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

L pszeudoinverze:

$$\begin{pmatrix} \frac{86}{539} & -\frac{31}{1078} & -\frac{3}{1078} & \frac{2}{101} & -\frac{3}{1078} & -\frac{31}{1078} & -\frac{54}{539} \\ -\frac{1078}{31} & \frac{8624}{67} & \frac{8624}{2545} & -\frac{1078}{101} & -\frac{8624}{689} & -\frac{8624}{1011} & \frac{539}{16} \\ -\frac{1078}{3} & \frac{8624}{101} & \frac{8624}{25} & \frac{1078}{163} & -\frac{8624}{25} & -\frac{8624}{101} & -\frac{539}{89} \\ \frac{539}{3} & -\frac{1078}{1011} & \frac{1078}{689} & \frac{539}{25} & \frac{1078}{2545} & -\frac{1078}{67} & -\frac{539}{68} \\ -\frac{1078}{31} & -\frac{8624}{745} & -\frac{8624}{1011} & \frac{1078}{101} & \frac{8624}{67} & \frac{8624}{2489} & -\frac{539}{16} \\ -\frac{1078}{54} & -\frac{8624}{16} & -\frac{8624}{68} & -\frac{1078}{89} & \frac{8624}{68} & \frac{8624}{16} & \frac{539}{247} \\ -\frac{54}{539} & \frac{539}{539} & -\frac{539}{539} & -\frac{539}{539} & -\frac{539}{539} & \frac{539}{539} & \frac{539}{539} \end{pmatrix}$$

A $\mathcal{S}(G)$ sandpile csoport generátor eleme:
 $(2, 1, 1, 1, 1, 0)$

A generátor elemből kapott divisor vektor:
 $(-6, 2, 1, 1, 1, 0)$

A választott konfigurációkból kapott divisor vektorok:
 $D_{c_1} = (-8, 1, 1, 2, 1, 2, 1)$
 $D_{c_2} = (-10, 2, 2, 2, 1, 2, 1)$

Az 1. generátor felhasználásával:

$$D_{c_1} \cdot P \cdot D_g = (-8, 1, 1, 2, 1, 2, 1) \cdot \begin{pmatrix} \frac{86}{539} & -\frac{31}{1078} & -\frac{3}{1078} & \frac{2}{101} & -\frac{3}{1078} & -\frac{31}{1078} & -\frac{54}{539} \\ -\frac{31}{1078} & \frac{2489}{8624} & \frac{67}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{1078}{8624} & \frac{67}{8624} & \frac{2489}{8624} & \frac{25}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{3}{1078} & -\frac{1011}{8624} & \frac{1078}{8624} & \frac{163}{25} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{1078}{8624} & -\frac{1011}{8624} & \frac{1078}{8624} & \frac{25}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{31}{1078} & -\frac{1078}{8624} & -\frac{1078}{8624} & \frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & \frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \end{pmatrix} \cdot \begin{pmatrix} -6 \\ 2 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{1679}{176} = 9 + \frac{95}{176}$$

$$D_{c_2} \cdot P \cdot D_g = (-10, 2, 2, 2, 1, 2, 1) \cdot \begin{pmatrix} \frac{86}{539} & -\frac{31}{1078} & -\frac{3}{1078} & \frac{2}{101} & -\frac{3}{1078} & -\frac{31}{1078} & -\frac{54}{539} \\ -\frac{31}{1078} & \frac{2489}{8624} & \frac{67}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{1078}{8624} & \frac{67}{8624} & \frac{2489}{8624} & \frac{25}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{3}{1078} & -\frac{1011}{8624} & \frac{1078}{8624} & \frac{163}{25} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{1078}{8624} & -\frac{1011}{8624} & \frac{1078}{8624} & \frac{25}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{31}{1078} & -\frac{1078}{8624} & -\frac{1078}{8624} & \frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \\ -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & \frac{1078}{8624} & -\frac{1078}{8624} & -\frac{1078}{8624} & -\frac{539}{8624} \end{pmatrix} \cdot \begin{pmatrix} -6 \\ 2 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{2155}{176} = 12 + \frac{43}{176}$$

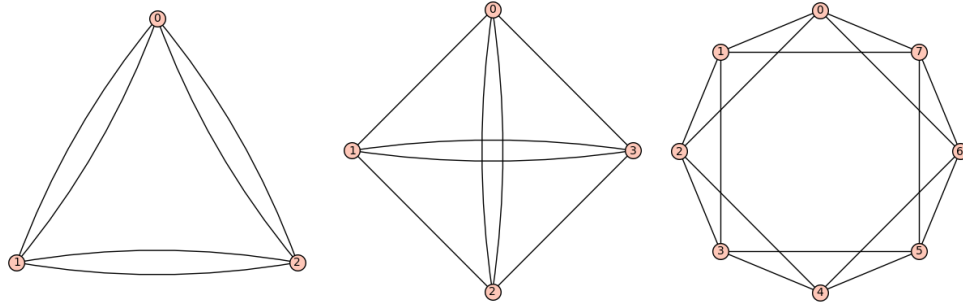
Keressük az alábbi lineáris diofantikus egyenlet megoldását: $\frac{95}{176}x + y = \frac{43}{176}$

A diofantikus egyenlet megoldása:
 $x_1 = 69 \pmod{176}$

4. Négyzetes körgráf

Más sandpile gráfok esetén is felvetődik a kérdés, hogy alkalmasak-e kriptográfiai használatra. Már Shokrieh is felvetette [9]-ben a módszere alkalmazásának lehetőségét nem ciklikus sandpile csoportokban. Az alábbi fejezetben [10] által leírt C_n^2 gráf sandpile csoportján értelmezett diszkrét logaritmus probléma megoldására alkalmazzuk Shokrieh módszerét.

4.1. Definíció. Legyen n pozitív egész, C_n pedig az n csúcsú körgráf $V = \{v_1, \dots, v_n\}$ csúcshalmazzal. Ekkor legyen C_n^2 négyzetes körgráf az alábbi 4-reguláris gráf V csúcshalmazzal, ahol minden i -edik csúcs szomszédos az $i \pm 1 \pmod{n}$ és $i \pm 2 \pmod{n}$ csúcsokkal.



C_3^2, C_4^2 és C_8^2 gráfok

Több tanulmányban is foglalkoznak C_n^2 sandpile csoportjának struktúrájának meghatározásával. A sandpile csoport elemszámának meghatározásában is fontos C_n^2 feszítő fáinak száma $\tau_n^{(2)} = nF_n^2$, ahol F_n az n -edik Fibonacci szám. Ezt eredetileg Bedrosian sejtett meg, majd Kleitman és Golden bizonyított [11]-ben. Továbbá Hou, Woo és Chen [10]-ben megmutatta, hogy C_n^2 sandpile csoportja két vagy három ciklikus csoport direkt szorzata, amik a következők:

$$\mathcal{S}(C_n^2) \cong \mathbb{Z}_{(n, F_n)} \oplus \mathbb{Z}_{F_n} \oplus \mathbb{Z}_{\frac{nF_n}{(n, F_n)}}.$$

A csoport struktúrájának ismeretét és 2.4 részben leírtakat felhasználva oldjuk meg a sandpile csoportban definiált diszkrét logaritmus problémát, mely az előző részhez hasonlóan az alábbi módon adható meg. Legyen $G = C_n^2$ négyzetes körgráf, $\mathcal{S}(G)$ a gráfból keletkező sandpile csoport, továbbá $c_1, c_2 \in \mathcal{S}(G)$ konfigurációk. Keresett olyan $2 \leq x \leq \text{ord}(\mathcal{S}(G))$, hogy $c_2 = (x \cdot c_1)^\circ$. Ekkor n paraméter megválasztásától függően a sandpile csoport két vagy három csoport direkt szorzatára bomlik fel.

4.1. C_n^2 -beli diszkrét logaritmus probléma megoldása

Az alapötlet Shokrieh algoritmusának használata, melyet alkalmazzunk az egyes ciklikus részcsoporthoz, majd részmegoldásokból a kínai maradéktétel alkalmazásával adjuk meg az eredeti probléma megoldását.

A gráf ismeretében kiszámoljuk L Laplace-mátrixát, valamint annak P pszeudoinverzét a korábban ismertetett módon. A problémában adott c_1 és c_2 konfigurációkhoz adott divizorokat jelölje D_{c_1} és D_{c_2} hasonlóan az előző fejezethez, melyek a részcsoporthoz számától függetlenül ugyanazok.

Két generátoros eset

Amennyiben $\text{lnko}(n, F_n) = 1$, ekkor $\mathcal{S}(G) \cong Z_{F_n} \oplus \mathbb{Z}_{\frac{nF_n}{(n, F_n)}}$. Legyenek g_1 és g_2 generátorai az egyes részcsoporthoz. Ekkor minden $c \in \mathcal{S}(G)$ konfiguráció esetén $c = (n_1 \cdot g_1 + n_2 \cdot g_2)^\circ$, ahol $n_i \in \mathbb{N}$ és $0 \leq n_i \leq \text{ord}(g_i)$ $i = 1, 2$. A generátorok ismeretében kiszámolhatóak a generátor konfigurációkhoz tartozó divizorok, melyeket jelölje D_{g_1} és D_{g_2} .

Az egyes generátorok alkotta részcsoporthoz használjuk Shokrieh módszerét. Ismételten a 2.5 állítást felhasználva kiszámoljuk $D_{c_1} \cdot P \cdot D_{g_1}$ és $D_{c_2} \cdot P \cdot D_{g_1}$ értékeket.

Amelyekből adódik egy x_1 , mely a keletkező diofantikus egyenlet megoldását adja modulo $\text{ord}(g_1)$. Hasonlóan $D_{c_1} \cdot P \cdot D_{g_2}$ és $D_{c_1} \cdot P \cdot D_{g_2}$ értékekből is adódik x_2 megoldás modulo $\text{ord}(g_2)$.

Három generátoros eset

Amennyiben $(n, F_n) \neq 1$, ekkor $\mathcal{S}(G) = \mathbb{Z}_{(n, F_n)} \oplus Z_{F_n} \oplus \mathbb{Z}_{\frac{nF_n}{(n, F_n)}}$. Legyenek g_1, g_2 és g_3 generátorai az egyes részcsoporthoz. Ekkor minden $c \in \mathcal{S}(G)$ esetén $c = (n_1 \cdot g_1 + n_2 \cdot g_2 + n_3 \cdot g_3)^\circ$, ahol $n_i \in \mathbb{N}$ és $0 \leq n_i \leq \text{ord}(g_i)$ $i = 1, 2, 3$. A generátorok ismeretében kiszámolhatóak a generátor konfigurációkhoz tartozó divizorok, melyeket jelölje D_{g_1}, D_{g_2} és D_{g_3} .

A két generátoros esetben már megoldott módon megkapjuk x_1 és x_2 megoldásokat a g_1 és g_2 generátorok által generált részcsoporthoz. Hasonlóan g_3 generátort felhasználva $D_{c_1} \cdot P \cdot D_{g_3}$ és $D_{c_1} \cdot P \cdot D_{g_3}$ értékekből keletkező diofantikus egyenletet megoldva adódik x_3 modulo $\text{ord}(g_3)$.

Mindkét esetben hasonlóan eljárva a kapott x_1, x_2 , és esetleges x_3 megoldásokból adódó kongruencia rendszert a kínai maradéktétel segítségével megoldva adódik a diszkrét logaritmus probléma megoldása $\mathcal{S}(C_n^2)$ -ben.

4.1. Példa. Tekintsük példaként a 7 csúcsú négyzetes kerékgérfot. Legyenek $c_1 = (1, 3, 3, 2, 0, 1)$ és $c_2 = (3, 1, 3, 2, 2, 0)$ tetszőlegesen választott konfigurációk.

Ekkor a gráf Laplace-mátrixa:

$$L = \begin{pmatrix} 4 & -1 & -1 & 0 & 0 & -1 & -1 \\ -1 & 4 & -1 & -1 & 0 & 0 & -1 \\ -1 & -1 & 4 & -1 & -1 & 0 & 0 \\ 0 & -1 & -1 & 4 & -1 & -1 & 0 \\ 0 & 0 & -1 & -1 & 4 & -1 & -1 \\ -1 & 0 & 0 & -1 & -1 & 4 & -1 \\ -1 & -1 & 0 & 0 & -1 & -1 & 4 \end{pmatrix}.$$

Pszéudoinverze:

$$P = \begin{pmatrix} \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{6}{91} & -\frac{1}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{6}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} \\ -\frac{1}{91} & -\frac{2}{91} & -\frac{1}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} \end{pmatrix}.$$

Tekintve a sandpile csoportot, mely két részcsoporthoz direkt szorzatára bomlik fel, a generátor konfigurációk a következők:

- $g_1 = (1, 1, 3, 2, 3, 0)$
- $g_2 = (1, 1, 3, 2, 3, 0)$.

Ezekből képzett divizorok:

- $D_{g_1} = (-10, 1, 3, 3, 2, 0, 1)$
- $D_{g_2} = (-11, 3, 1, 3, 2, 2, 0)$.

Továbbá kiszámoljuk $D_{c_1} = (-5, 2, 1, 1, 1)$, $D_{c_2} = (-4, 1, 0, 2, 1)$ divizorokat.

A g_1 generátort felhasználva tekintsük az alábbiakat

$$D_{c_1} \cdot P \cdot D_{g_1} = (-10, 1, 3, 3, 2, 0, 1) \begin{pmatrix} \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{6}{91} & -\frac{1}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{6}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} \\ -\frac{1}{91} & -\frac{2}{91} & -\frac{1}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} \end{pmatrix} \begin{pmatrix} -10 \\ 1 \\ 1 \\ 3 \\ 2 \\ 3 \\ 0 \end{pmatrix} =$$

$$= \frac{381}{13},$$

$$\begin{aligned}
D_{c_2} \cdot P \cdot D_{g_1} &= (-11, 3, 1, 3, 2, 2, 0) \begin{pmatrix} \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} \\ -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} \\ -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} \\ -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} \end{pmatrix} \begin{pmatrix} -10 \\ 1 \\ 1 \\ 3 \\ 2 \\ 3 \\ 0 \end{pmatrix} \\
&= \frac{425}{13},
\end{aligned}$$

Így az algoritmusban használt jelöléseket megtartva $r = \frac{4}{13}, r' = \frac{9}{13}$ adódnak, amiből a $\frac{4}{13}x + y = \frac{9}{13}$ lineáris diofantikus egyenletet megoldva kapjuk az $x_1 = 12$ megoldást modulo 13.

A g_2 generátort felhasználva tekintsük az alábbiakat

$$\begin{aligned}
D_{c_1} \cdot P \cdot D_{g_2} &= (-10, 1, 3, 3, 2, 0, 1) \begin{pmatrix} \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} \\ -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} \\ -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} \\ -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} \end{pmatrix} \begin{pmatrix} -11 \\ 3 \\ 1 \\ 3 \\ 2 \\ 2 \\ 0 \end{pmatrix} = \\
&= \frac{381}{13},
\end{aligned}$$

$$\begin{aligned}
D_{c_2} \cdot P \cdot D_{g_2} &= (-11, 3, 1, 3, 2, 2, 0) \begin{pmatrix} \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} \\ -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} \\ -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} \\ -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} & -\frac{2}{91} \\ -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} & -\frac{1}{91} \\ -\frac{1}{91} & -\frac{2}{91} & -\frac{6}{91} & -\frac{6}{91} & -\frac{2}{91} & -\frac{1}{91} & \frac{18}{91} \end{pmatrix} \begin{pmatrix} -11 \\ 3 \\ 1 \\ 3 \\ 2 \\ 2 \\ 0 \end{pmatrix} \\
&= \frac{425}{13}.
\end{aligned}$$

Így $r = \frac{41}{91}, r' = \frac{89}{91}$ adódnak, amiből a $\frac{41}{91}x + y = \frac{89}{91}$ lineáris diofantikus egyenletet megoldva kapjuk az $x_2 = 51$ megoldást modulo 91.

Végezetül tekintve a diofantikus egyenletek megoldásait, az alábbi kongruencia rendszer adódik:

$$\begin{aligned}
x &= 12 \pmod{13} \\
x &= 51 \pmod{91}
\end{aligned}$$

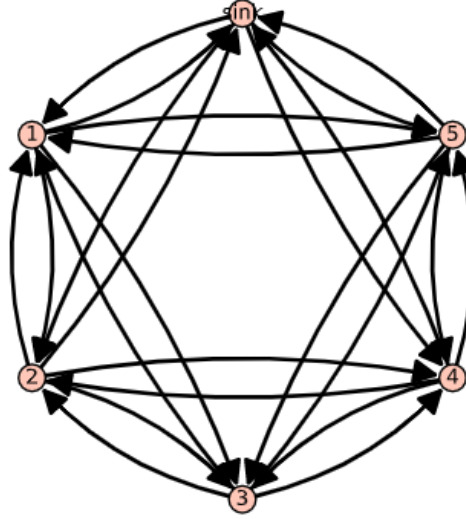
Ezt megoldva adódik a diszkrét logaritmus probléma $x = 51$ megoldása.

Példa a diszkrét logaritmus megoldására SageMath programban

Gráf mérete 6

Választott konfigurációk ▾

Legyenek a választott konfigurációk (1, 3, 3, 3, 3) és (2, 3, 2, 0, 3)



Adott G gráf esetén számítsuk ki Laplace matrixát, majd annak pszeudoinverzét.

Az így kapott $L = D - A$ Laplace mátrix:

$$\begin{pmatrix} 4 & -1 & -1 & 0 & -1 & -1 \\ -1 & 4 & -1 & -1 & 0 & -1 \\ -1 & -1 & 4 & -1 & -1 & 0 \\ 0 & -1 & -1 & 4 & -1 & -1 \\ -1 & 0 & -1 & -1 & 4 & -1 \\ -1 & -1 & 0 & -1 & -1 & 4 \end{pmatrix}$$

L pszeudoinverze:

$$\begin{pmatrix} \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} \\ -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} \end{pmatrix}$$

A $\mathcal{S}(G)$ sandpile csoport generátor eleme:

(1, 1, 3, 3, 3)
(3, 3, 0, 2, 2)
(3, 2, 0, 2, 2)

A generátor elemből kapott divisor vektor:

(-11, 1, 1, 3, 3, 3)
(-10, 3, 3, 0, 2, 2)
(-9, 3, 2, 0, 2, 2)

A választott konfigurációkból kapott divisor vektorok:

$D_{c_1} = (-13, 1, 3, 3, 3, 3)$
 $D_{c_2} = (-10, 2, 3, 2, 0, 3)$

Az 1. generátor felhasználásával:

$$D_{c_1} \cdot P \cdot D_g = (-13, 1, 3, 3, 3, 3) \cdot \begin{pmatrix} \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} \end{pmatrix} \cdot \begin{pmatrix} -11 \\ 1 \\ 1 \\ 3 \\ 3 \\ 3 \end{pmatrix} = \frac{77}{2} = 38 + \frac{1}{2}$$

$$D_{c_2} \cdot P \cdot D_g = (-10, 2, 3, 2, 0, 3) \cdot \begin{pmatrix} \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{72} & -\frac{5}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{72} & -\frac{5}{72} \\ -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} \end{pmatrix} \cdot \begin{pmatrix} -11 \\ 1 \\ 1 \\ 3 \\ 3 \\ 3 \end{pmatrix} = \frac{57}{2} = 28 + \frac{1}{2}$$

Keressük az alábbi lineáris diofantikus egyenlet megoldását: $\frac{1}{2}x + y = \frac{1}{2}$

A diofantikus egyenlet megoldása:

$$x_1 = 1 \pmod{2}$$

Az 2. generátor felhasználásával:

$$D_{c_1} \cdot P \cdot D_g = (-13, 1, 3, 3, 3, 3) \cdot \begin{pmatrix} \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} \\ -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} \end{pmatrix} \cdot \begin{pmatrix} -10 \\ 3 \\ 3 \\ 0 \\ 2 \\ 2 \end{pmatrix} = \frac{129}{4} = 32 + \frac{1}{4}$$

$$D_{c_2} \cdot P \cdot D_g = (-10, 2, 3, 2, 0, 3) \cdot \begin{pmatrix} \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} \\ \frac{1}{72} & \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} \end{pmatrix} \cdot \begin{pmatrix} -10 \\ 3 \\ 3 \\ 0 \\ 2 \\ 2 \end{pmatrix} = \frac{101}{4} = 25 + \frac{1}{4}$$

Keressük az alábbi lineáris diofantikus egyenlet megoldását: $\frac{1}{4}x + y = \frac{1}{4}$

A diofantikus egyenlet megoldása:

$$x_2 = 1 \pmod{4}$$

Az 3. generátor felhasználásával:

$$D_{c_1} \cdot P \cdot D_g = (-13, 1, 3, 3, 3, 3) \cdot \begin{pmatrix} \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} \\ -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{13}{72} \end{pmatrix} \cdot \begin{pmatrix} -9 \\ 3 \\ 2 \\ 0 \\ 2 \\ 2 \end{pmatrix} = \frac{347}{12} = 28 + \frac{11}{12}$$

$$D_{c_2} \cdot P \cdot D_g = (-10, 2, 3, 2, 0, 3) \cdot \begin{pmatrix} \frac{13}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{5}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{72} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} & -\frac{1}{36} \\ -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & -\frac{1}{36} & \frac{1}{72} \end{pmatrix} \cdot \begin{pmatrix} -9 \\ 3 \\ 2 \\ 0 \\ 2 \\ 2 \end{pmatrix} = \frac{271}{12} = 22 + \frac{7}{12}$$

Keressük az alábbi lineáris diofantikus egyenlet megoldását: $\frac{11}{12}x + y = \frac{7}{12}$

A diofantikus egyenlet megoldása:

$$x_3 = 5 \pmod{12}$$

A diofantikus egyenletek megoldásaiból, a Kínai maradéktétel segítségével adódik a probléma megoldása.

A diszkrét logaritmus probléma megoldása az $x = 5$.

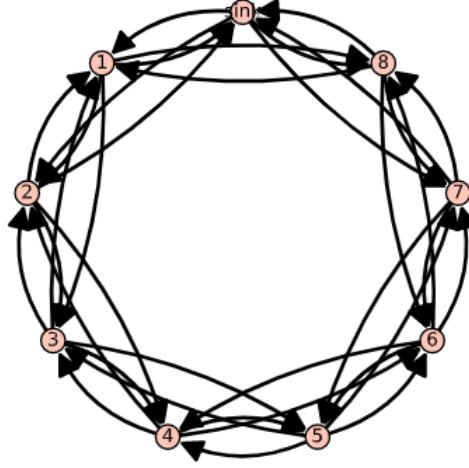
Gráf mérete

9

Választott konfigurációk

[(1, 3, 0, 3, 1, 1, 3, 2), (3, 3, 2, 2, 2, 2, 3, 3)] ▼

Legyenek a választott konfigurációk (1, 3, 0, 3, 1, 1, 3, 2) és (3, 3, 2, 2, 2, 2, 3, 3)

Adott G gráf esetén számítsuk ki Laplace matrixát, majd annak pszeudoinverzét.

Az így kapott $L = D - A$ Laplace mátrix:

$$\begin{pmatrix} 4 & -1 & -1 & 0 & 0 & 0 & 0 & -1 & -1 \\ -1 & 4 & -1 & -1 & 0 & 0 & 0 & 0 & -1 \\ -1 & -1 & 4 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 4 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 4 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 & 4 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & 4 & -1 & -1 \\ -1 & 0 & 0 & 0 & 0 & -1 & -1 & 4 & -1 \\ -1 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & 4 \end{pmatrix}$$

L pszeudoinverze:

$$\begin{pmatrix} \frac{107}{459} & \frac{19}{918} & \frac{1}{918} & -\frac{28}{459} & -\frac{71}{918} & -\frac{71}{918} & -\frac{28}{459} & \frac{1}{918} & \frac{19}{918} \\ \frac{19}{459} & \frac{107}{918} & \frac{1}{918} & -\frac{28}{459} & -\frac{71}{918} & -\frac{71}{918} & -\frac{28}{459} & \frac{1}{918} & \frac{19}{918} \\ \frac{1}{918} & \frac{1}{918} & \frac{107}{918} & -\frac{28}{459} & -\frac{71}{918} & -\frac{71}{918} & -\frac{28}{459} & \frac{1}{918} & \frac{19}{918} \\ -\frac{28}{459} & -\frac{28}{459} & -\frac{28}{459} & \frac{107}{918} & \frac{19}{918} & \frac{19}{918} & \frac{107}{918} & -\frac{28}{459} & -\frac{28}{459} \\ -\frac{71}{918} & -\frac{71}{918} & -\frac{71}{918} & \frac{19}{918} & \frac{107}{918} & \frac{19}{918} & \frac{19}{918} & -\frac{71}{918} & -\frac{71}{918} \\ -\frac{71}{918} & -\frac{71}{918} & -\frac{71}{918} & \frac{19}{918} & \frac{107}{918} & \frac{19}{918} & \frac{19}{918} & -\frac{71}{918} & -\frac{71}{918} \\ -\frac{28}{459} & -\frac{28}{459} & -\frac{28}{459} & \frac{107}{918} & \frac{19}{918} & \frac{19}{918} & \frac{107}{918} & -\frac{28}{459} & -\frac{28}{459} \\ -\frac{1}{918} & -\frac{1}{918} & -\frac{1}{918} & -\frac{28}{459} & -\frac{71}{918} & -\frac{71}{918} & -\frac{28}{459} & \frac{1}{918} & \frac{19}{918} \\ \frac{19}{918} & \frac{19}{918} & \frac{19}{918} & -\frac{28}{459} & -\frac{71}{918} & -\frac{71}{918} & -\frac{28}{459} & \frac{1}{918} & \frac{19}{918} \end{pmatrix}$$

A $\mathcal{S}(G)$ sandpile csoport generátor eleme:

(1, 3, 2, 3, 2, 3, 3, 2)

(1, 3, 3, 1, 1, 3, 3, 0)

A generátor elemből kapott divisor vektor:

(-19, 1, 3, 2, 3, 2, 3, 3, 2)

(-15, 1, 3, 3, 1, 1, 3, 3, 0)

A választott konfigurációkból kapott divisor vektorok:

 $D_{c_1} = (-14, 1, 3, 0, 3, 1, 1, 3, 2)$ $D_{c_2} = (-20, 3, 3, 2, 2, 2, 2, 3, 3)$

Az 1. generátor felhasználásával:

$$D_{c_1} \cdot P \cdot D_g = (-14, 1, 3, 0, 3, 1, 1, 3, 2) \cdot \begin{pmatrix} 107 & 19 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 459 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 1 & 19 & 107 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & 459 & 918 & -459 & -918 & -459 & 918 & 918 \\ -459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ -71 & -28 & 918 & 19 & 107 & 107 & 19 & -28 & 1 \\ -918 & -459 & 918 & 918 & -459 & -918 & -459 & 918 & 918 \\ -71 & -28 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \end{pmatrix} \cdot \begin{pmatrix} -19 \\ 1 \\ 3 \\ 3 \\ 2 \\ 3 \\ 3 \\ 3 \\ 2 \end{pmatrix} = \frac{2657}{34} = 78 + \frac{5}{34}$$

$$D_{c_2} \cdot P \cdot D_g = (-20, 3, 3, 2, 2, 2, 2, 3, 3) \cdot \begin{pmatrix} 107 & 19 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 459 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 1 & 19 & 107 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & 459 & 918 & -459 & -918 & -459 & 918 & 918 \\ -459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ -71 & -28 & 918 & 19 & 107 & 107 & 19 & -28 & 1 \\ -918 & -459 & 918 & 918 & -459 & -918 & -459 & 918 & 918 \\ -71 & -28 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \end{pmatrix} \cdot \begin{pmatrix} -19 \\ 1 \\ 3 \\ 2 \\ 2 \\ 2 \\ 3 \\ 3 \\ 2 \end{pmatrix} = \frac{1869}{17} = 109 + \frac{16}{17}$$

Keressük az alábbi lineáris diofantikus egyenlet megoldását: $\frac{5}{34}x + y = \frac{16}{17}$

A diofantikus egyenlet megoldása:
 $x_1 = 20 \pmod{34}$

Az 2. generátor felhasználásával:

$$D_{c_1} \cdot P \cdot D_g = (-14, 1, 3, 0, 3, 1, 1, 3, 2) \cdot \begin{pmatrix} 107 & 19 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 459 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 1 & 19 & 107 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & 459 & 918 & -459 & -918 & -459 & 918 & 918 \\ -459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ -71 & -28 & 918 & 19 & 107 & 107 & 19 & -28 & 1 \\ -918 & -459 & 918 & 918 & -459 & -918 & -459 & 918 & 918 \\ -71 & -28 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \end{pmatrix} \cdot \begin{pmatrix} -15 \\ 1 \\ 1 \\ 3 \\ 1 \\ 1 \\ 3 \\ 3 \\ 0 \end{pmatrix} = \frac{9341}{153} = 61 + \frac{8}{153}$$

$$D_{c_2} \cdot P \cdot D_g = (-20, 3, 3, 2, 2, 2, 2, 3, 3) \cdot \begin{pmatrix} 107 & 19 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 459 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ 1 & 19 & 107 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & 459 & 918 & -459 & -918 & -459 & 918 & 918 \\ -459 & 918 & 918 & -459 & -918 & -918 & -459 & 918 & 918 \\ -71 & -28 & 918 & 19 & 107 & 107 & 19 & -28 & 1 \\ -918 & -459 & 918 & 918 & -459 & -918 & -459 & 918 & 918 \\ -71 & -28 & 1 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \\ 19 & 107 & 19 & -28 & -71 & -71 & -28 & 1 & 19 \\ 918 & 918 & -459 & -918 & -459 & -918 & -459 & 918 & 918 \end{pmatrix} \cdot \begin{pmatrix} -15 \\ 1 \\ 3 \\ 3 \\ 1 \\ 1 \\ 3 \\ 3 \\ 0 \end{pmatrix} = \frac{1476}{17} = 86 + \frac{14}{17}$$

Keressük az alábbi lineáris diofantikus egyenlet megoldását: $\frac{8}{153}x + y = \frac{14}{17}$

A diofantikus egyenlet megoldása:
 $x_2 = 54 \pmod{153}$

A diofantikus egyenletek megoldásából, a Kínai maradéktétel segítségével adódik a probléma megoldása.
A diszkrét logaritmus probléma megoldása az $x = 54$.

5. Általánosított inverz

A következő fejezetben a C_n^2 gráf sandpile csoportja felett értelmezett diszkrét logaritmus probléma megoldását szeretnénk leegyszerűsíteni, egy általánosan használható parametrizált formula megadásával. Ehhez a gráf Laplace-mátrixának pszeudoinvertét szeretnénk általánosan megadni.

5.1. Definíció. Egy $A = (a_{ij})$ négyzetes mátrixot Toeplitz-mátrixnak nevezünk, ha a főátlóval párhuzamos elemei megegyeznek, azaz az alábbi formájú:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{-2} & a_{-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{-n+1} & a_{-n+2} & a_{-n+3} & \dots & a_0 \end{pmatrix}.$$

A négyzetes körgráf Laplace-mátrixa egy speciális Toeplitz-mátrix, melyet ciklikus mátrixnak is neveznek.

5.2. Definíció. Egy $A = (a_{ij})$ négyzetes mátrixot k -ciklikus mátrixnak nevezünk, melynek sorai ciklikusan ismétlődnek, azaz az alábbi formájú:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ ka_{n-1} & ka_0 & a_1 & \dots & a_{n-2} \\ ka_{n-2} & ka_{n-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ka_1 & ka_2 & ka_3 & \dots & a_0 \end{pmatrix}.$$

Ha $k = 1$ az A mátrixot egyszerűen ciklikusnak nevezzük, ahol $a_{ij} = a_{j-i}$, $q \leq i, j \leq n$. Az ilyen alakú mátrixok struktúrájával Cline, Plemmons és Worm [12] munkájukban foglalkoztak. A mi esetünkben a sandpile csoport jellemzésében eredményeik közül a ciklikus mátrixok pszeudoinverté játszik majd kulcsszerepet.

Ehhez egy általánosabb inverz fogalmat vezetünk be. Az 3 és 4 fejezetekben már előkerült a pszeudoinvert fogalma, azonban ennek általánosításához tekintsük az alábbiakat.

5.3. Definíció. Egy M $n \times m$ mátrix pszeudoinverté alatt egy M' mátrixot értünk, melyre $M = MM'M$ teljesül. Továbbá, amennyiben M' teljesíti az $M' = M'MM'$ feltételt, akkor M és M' egymás fél-inverzai. Azt az egyedi fél-invertet, melyre MM' és $M'M$ hermitikusága is teljesül, Moore-Penrose invertnek nevezik, melynek jelölése M^+ .

Jelölje $\mathcal{C}_n$ az $n \times n$ komplex mátrixok félcsoporthját a szorzásra nézve. Minden $A \in \mathcal{C}_n$ esetén, A -nak valamely hatványa egy H maximális $\mathcal{C}_n$ -beli részcsoporthoz

tartozik. A legkisebb ilyen p pozitív egész számot, melyre $A^p \in H$ azt A indexének nevezzük. Ha A indexe 1, akkor A' , mely A pszeudoinverze H -ban van, melyet A csoport inverzének nevezünk.

Az [13]-ban A -nak olyan A' fél-inverzeit tekintik, melyben a A' nemnulla sajátértékei reciprokai az A nemnulla sajátértékeinek, ezeket spektrál inverznek nevezik. Továbbá Scroggs és Odell megmutatják, hogy egy A nemnulla mátrixnak pontosan akkor létezik spektrál inverze, ha A indexe 1. A spektrál inverz felhasználásával a gráfunk sandpile csoportjának Laplace-mátrixának is megadható spektrál inverze, mely a [12]-ből adódóan megegyezik a Moore-Penrose pszeudoinverzszel.

Jelölje Z az $n \times n$ mátrixokat, melynek sajátértékei különbözőek. Ekkor $\mathcal{C}_Z$ -beli mátrixok zártak a szorzásra nézve és félcsoportot alkotnak.

5.1. Tétel. Minden $A \in \mathcal{C}_Z$ indexe 1, és az egyedüli A^s spektrál inverz az egyetlen pszeudoinverze A -nak. Továbbá ha Z normális, akkor $A^s = A^+$

5.2. Tétel. Legyen A egy $n \times n$ -es k -ciklikus mátrix $a_0, \dots, a_{n-1}$ első sorral és $\mu_0, \dots, \mu_{n-1}$ sajátértékekkel. Legyen ω primitív n -edik egységgyök, és $\lambda^n = k$. Ekkor A^s első sora $b_0, \dots, b_{n-1}$, ahol

$$b_i = \frac{1}{n} \sum_{j=0}^{n-1} \beta_j (\lambda \omega^j)^{-i}, \quad i = 0, 1, \dots, n-1,$$

továbbá

$$\beta_j = \begin{cases} 0 & \text{ha } \mu_j = 0; \\ \frac{1}{\mu_j} & \text{ha } \mu_j \neq 0. \end{cases}$$

5.3. Tétel. Legyen A k -ciklikus és szinguláris, ekkor A^+ is k -ciklikus pontosan akkor, ha k az egységkörön van.

5.1. Következmény. Ha A k -ciklikus valamilyen k esetén, amikor k az egységkörön van, akkor $A^s = A^+$

A C_n^2 gráf esetén alkalmazható a 5.2 tétel $k = 1$ esetén, továbbá a gráf ismeretében Laplace-mátrixa jól leírható. Ezek segítségével a pszeudoinverz paraméteres felírása is megadható.

5.1. Példa. Példaként tekintsük C_4^2 gráfot, mely 4 reguláris és szomszédsági mátrixa segítségével megadható Laplace-mátrixa, mely

$$L = \begin{pmatrix} 4 & -1 & -2 & -1 \\ -1 & 4 & -1 & -2 \\ -2 & -1 & 4 & -1 \\ -1 & -2 & -1 & 4 \end{pmatrix}.$$

Látható, hogy a gráf 1-ciklikus, így $L^s = L^+$. Legyen $\omega = i = \sqrt{-1}$, ekkor REF miatt L sajátértékei megadhatók a következőképpen:

$$\mu_j = 2 + \omega^j - \omega^{2j}, \quad j = 0, 1, 2, 3.$$

Vagyis $\mu_0 = 0, \mu_1 = 6, \mu_2 = 4, \mu_3 = 6$. Továbbá 5.2 alkalmazásával A^+ első sora az alábbi módon adódik:

$$b_i = \frac{1}{4} \left(\frac{1}{2} + \frac{\omega^{-t}}{3+i} + \frac{\omega^{-3t}}{3-i} \right), \quad t = 0, 1, 2, 3.$$

Ebből $b_0 = \frac{7}{48}, b_1 = \frac{1}{16}, b_2 = -\frac{1}{48}, b_3 = \frac{1}{16}$, amely a pszeudoinverz első sorát adja, ami hasonlóan L -hez 1-ciklikus, így

$$L^+ = \begin{pmatrix} \frac{7}{48} & -\frac{1}{16} & -\frac{1}{48} & -\frac{1}{16} \\ -\frac{1}{16} & \frac{7}{48} & -\frac{1}{16} & -\frac{1}{48} \\ -\frac{1}{48} & -\frac{1}{16} & \frac{7}{48} & -\frac{1}{16} \\ -\frac{1}{16} & -\frac{1}{48} & -\frac{1}{16} & \frac{7}{48} \end{pmatrix}.$$

Az alábbi általánosítás segítségével tekintsük C_n^2 sandpile csoportján adott diszkrét logaritmus probléma megoldását. Legyenek $\mathcal{S}(C_n^2)$ Laplace-mátrixa L , pszeudoinverze $P = L^+$, továbbá generátorai n paraméterétől függően $g_i = (g_{i,0}, \dots, g_{i,n-1})$ $i = 1, 2$ vagy $i = 1, 2, 3$. Adott $c_j = (c_{j,0}, \dots, c_{j,n-1})$ $j = 1, 2$ konfigurációk esetén a keresett diszkrét logaritmus probléma $(x \cdot c_1)^\circ = c_2$ esetén x megadása. Ekkor az 2.4 algoritmusbeli $r_{i,j} = c_j \cdot P \cdot g_i$ párosítások értékeinek számítása egyszerűsödik le.

Először tekintsük az alábbi kifejezést:

$$P \cdot g_i = \begin{pmatrix} p_0 & p_1 & \dots & p_{n-1} \\ p_{n-1} & p_0 & \dots & p_{n-2} \\ \vdots & \vdots & & \vdots \\ p_1 & p_2 & \dots & p_0 \end{pmatrix} \cdot \begin{pmatrix} g_{i,0} \\ g_{i,1} \\ \vdots \\ g_{i,n-1} \end{pmatrix} = \begin{pmatrix} v_{i,0} \\ v_{i,1} \\ \vdots \\ v_{i,n-1} \end{pmatrix},$$

ahol

$$v_{i,k} = \begin{cases} \sum_{l=0}^{n-1} p_l \cdot g_l & \text{ha } k = 0; \\ \sum_{l=0}^{n-1} p_{l-k \pmod n} \cdot g_l & \text{ha } k \neq 0. \end{cases} = v_i.$$

Innen

$$c_j \cdot v_i = \sum_{l=0}^{n-1} c_{j,l} \cdot v_{i,l} = c_0 \cdot \sum_{l=0}^{n-1} p_l \cdot g_l + \sum_{k=1}^{n-1} c_k \sum_{l=0}^{n-1} p_{l-k \pmod n} \cdot g_l,$$

ahonnan p_i elemek 5.2 szerint explicit kiszámolhatók.

6. Függetlenség

```
1 def w_graph(n):
2     G=graphs.WheelGraph(2*n+3)
3     V = G.vertices()
4     G.delete_edge(V[0],V[2*n+2])
5
6     return(G)
7
8 def cn2_graph(n):
9     G = graphs.CycleGraph(n)
10    G.allow_multiple_edges(True)
11    for i in range(0, n):
12        G.add_edge(i, (i + 2) % n)
13
14    return(G)
15
16 def config_vector(c):
17    return vector([b for a,b in c.items()])
18
19 def divisor_vector(v):
20    return vector([-1*sum(v)] + list(v))
21
22 def graph_figure(G, sink_vertex):
23    G = G.to_directed()
24    G.allow_multiple_edges(True)
25    G.to_directed()
26    G_edges = list(G.edges())
27
28    for e in G_edges:
29        if e[0] == sink_vertex:
30            list(G.edges()).remove(e)
31
32    ↪ G.relabel(list(range(0,sink_vertex))+['sink']+list(range(sink_vertex+1,order(G)+1)))
33
34    return G
35
36 example_list_wgraph = [
37    [(2, 1, 1, 1), (1, 0, 2, 1)],
38    [(2, 2, 1, 0), (2, 2, 1, 1)],
39    [(2, 1, 2, 1), (2, 2, 2, 0)],
40    [(2, 2, 1, 1), (1, 2, 2, 1)],
41    [(0, 1, 2, 1), (1, 1, 2, 1)],
42
43    [(1, 2, 2, 1, 2, 1), (2, 1, 0, 2, 1, 1)],
44    [(2, 1, 1, 2, 1, 0), (2, 0, 1, 2, 2, 0)],
```

```

45 [(1, 1, 2, 1, 2, 1), (2, 2, 2, 1, 2, 1)],
46 [(2, 2, 2, 1, 0, 1), (2, 0, 2, 0, 1, 1)],
47 [(0, 1, 1, 1, 2, 1), (0, 1, 2, 1, 2, 1)],
48
49 [[(2, 1, 2, 1, 1, 2, 2, 1), (2, 1, 1, 2, 2, 2, 1, 1)],
50 [(2, 1, 0, 1, 2, 2, 2, 0), (2, 2, 0, 2, 0, 2, 1, 1)],
51 [(2, 2, 0, 2, 1, 0, 2, 0), (2, 1, 0, 2, 2, 1, 0, 1)],
52 [(0, 1, 1, 2, 0, 2, 2, 1), (1, 2, 2, 0, 2, 2, 1, 1)],
53 [(1, 1, 0, 2, 2, 1, 2, 1), (2, 2, 0, 1, 1, 2, 1, 0)]]]
54
55 example_list_cn2graph = [
56 [(3, 2, 2, 1, 2), (1, 2, 2, 3, 2)],
57 [(2, 3, 2, 0, 3), (1, 2, 0, 3, 2)],
58 [(1, 3, 3, 3, 3), (2, 3, 2, 0, 3)],
59 [(1, 2, 0, 3, 2), (3, 2, 0, 1, 2)],
60 [(3, 2, 2, 1, 0), (0, 1, 2, 2, 3)],
61
62 [(1, 3, 3, 2, 0, 1), (3, 1, 3, 2, 2, 0)],
63 [(3, 2, 0, 2, 1, 3), (3, 2, 2, 0, 3, 1)],
64 [(2, 3, 2, 0, 2, 1), (2, 3, 2, 2, 0, 3)],
65 [(3, 0, 1, 2, 2, 2), (3, 3, 2, 3, 2, 2)],
66 [(3, 2, 2, 1, 3, 3), (0, 3, 1, 3, 2, 2)],
67
68 [(2, 2, 3, 2, 3, 1, 3), (3, 3, 0, 3, 1, 2, 1)],
69 [(3, 3, 3, 1, 3, 2, 2), (3, 3, 3, 1, 2, 3, 1)],
70 [(3, 3, 3, 2, 3, 3, 2), (3, 3, 3, 2, 0, 3, 3)],
71 [(3, 3, 3, 0, 2, 1, 3), (3, 2, 0, 2, 1, 3, 3)],
72 [(2, 0, 3, 2, 3, 3, 0), (3, 2, 2, 3, 1, 0, 2)],
73
74 [(1, 3, 0, 3, 1, 1, 3, 2), (3, 3, 2, 2, 2, 2, 3, 3)],
75 [(2, 3, 2, 2, 3, 2, 3, 0), (3, 0, 1, 2, 2, 3, 3, 2)],
76 [(3, 2, 3, 0, 1, 3, 3, 0), (3, 2, 3, 1, 2, 3, 2, 2)],
77 [(2, 3, 2, 3, 3, 1, 2, 3), (3, 3, 1, 1, 3, 0, 3, 3)],
78 [(3, 1, 0, 3, 1, 2, 3, 3), (3, 2, 3, 2, 3, 0, 1, 3)],
79
80 [(3, 2, 2, 3, 1, 2, 0, 2, 3), (3, 1, 3, 1, 3, 2, 2, 3, 3)],
81 [(3, 3, 3, 2, 2, 2, 1, 1, 3), (1, 3, 3, 3, 3, 3, 2, 2, 1)],
82 [(0, 3, 1, 3, 3, 2, 3, 1, 2), (2, 3, 2, 2, 1, 2, 1, 2, 2)],
83 [(2, 3, 1, 3, 1, 2, 1, 3, 2), (3, 3, 1, 3, 3, 1, 1, 3, 2)],
84 [(3, 3, 3, 2, 2, 3, 1, 1, 3), (2, 2, 2, 1, 2, 2, 3, 3, 1)]]]
85
86 def dlp_print():
87     pretty_print('Legyenek a választott konfigurációk {0} és
88         ↳ {1}\n'.format(c1_vector, c2_vector))
89
90     G_figure = graph_figure(G, 0)
91     G_figure.show()

```

```

92     pretty_print('Adott  $G$  gráf esetén számítsuk ki Laplace matrixát,
    ↪ majd annak pszeudoinvertét.')
93     print
94     pretty_print('\nAz így kapott  $L = D - A$  Laplace mátrix:',
    ↪ laplacian_matrix)
95     print
96     pretty_print('L pszeudoinverté: \n', pseudo_inverse);
97     print
98
99     pretty_print('A  $\mathcal{S}(G)$  sandpile csoport generátor eleme:')
100    for g in Generator_vector:
101        pretty_print(g)
102    print
103
104    pretty_print("A generátor eleméből kapott divisor vektor:")
105    for g in Generator_divisor:
106        pretty_print(g)
107    print
108
109    pretty_print("A választott konfigurációkból kapott divisor
    ↪ vektorok:")
110    pretty_print("$D_b={0}$".format(c1_divisor))
111    pretty_print("$D_c={0}$".format(c2_divisor))
112    print
113
114    def dlp_objects():
115        global c1_configuration, c2_configuration, c1_divisor, c2_divisor
116        c1_configuration = SandpileConfig(S, list(c1_vector))
117        c2_configuration = SandpileConfig(S, list(c2_vector))
118
119        c1_divisor = divisor_vector(c1_vector)
120        c2_divisor = divisor_vector(c2_vector)
121
122        global group_order
123        group_order = S.group_order()
124
125        global laplacian_matrix, pseudo_inverse
126        laplacian_matrix = S.laplacian_matrix()
127        pseudo_inverse = laplacian_matrix.pseudoinverse()
128
129        global generator_divisor, Generator, Generator_order,
    ↪ Generator_vector, Generator_divisor
130        Generator = S.group_gens()
131        Generator_order = [order(g) for g in Generator]
132        Generator_vector = [config_vector(g) for g in Generator]
133        Generator_divisor = [divisor_vector(g) for g in Generator_vector]
134
135

```

```

136 def dlp_sandpile():
137     Generator_order_temp = copy(Generator_order)
138     Solutions = []
139
140     for i in range(0, len(Generator)):
141         pretty_print('Az {0}. generátor felhasználásával:'.format(i+1))
142         print
143
144         pairing1 = c1_divisor*pseudo_inverse*Generator_divisor[i]
145         pairing2 = c2_divisor*pseudo_inverse*Generator_divisor[i]
146
147         r1 = pairing1 - floor(pairing1)
148         r2 = pairing2 - floor(pairing2)
149
150         divisor_temp = Matrix(len(Generator_divisor[i]), 1,
151                                ↪ Generator_divisor[i])
152         pretty_print('$D_b \cdot P \cdot D_g$', c1_divisor, '$\cdot$',
153                                ↪ pseudo_inverse, '$\cdot$', divisor_temp, '$=$',
154                                pairing1, '$=$', floor(pairing1), '$+$', r1)
155         print
156         pretty_print('$D_c \cdot P \cdot D_g$', c2_divisor, '$\cdot$',
157                                ↪ pseudo_inverse, '$\cdot$', divisor_temp, '$=$',
158                                pairing2, '$=$', floor(pairing2), '$+$', r2)
159         print
160
161         if r1.denominator() != Generator_order[i]:
162             Generator_order_temp[i] = r1.denominator()
163
164         var('x,y')
165         solution_diof_eq = solve_diophantine(r1*x+y==r2)
166
167         pretty_print('Keressük az alábbi lineáris diofantikus egyenlet
168                                ↪ megoldását:', r1, '$x + y =$', r2)
169         print
170
171         if solution_diof_eq != 0:
172             solution = int(mod(int(solution_diof_eq[0](t_0 = 0)),
173                                ↪ Generator_order_temp[i]))
174
175         else:
176             solution = 0
177             Generator_order_temp[i] = 1
178         pretty_print('A diofantikus egyenlet megoldása:')
179         pretty_print('$x_{0} = \{1\} \ ; \ (\text{mod} \ \{2\})$', i+1, solution,
180                                ↪ Generator_order_temp[i]))
181         print
182

```

```

178         Solutions.append(solution)
179
180     dlp_solution = CRT_list(Solutions, Generator_order_temp)
181
182     return(dlp_solution)
183
184     #CODE W
185     @interact(layout=[['n','g']])
186     def _(n = slider([1 .. 3], label = 'Gráf mérete', default = 2)):
187         @interact
188         def _(selected_elements = selector(example_list_wgraph[n-1], label =
189             ↳ 'Választott konfigurációk', default =
190             ↳ example_list_wgraph[n-1][0])):
191             global c1_vector, c2_vector
192             c1_vector = selected_elements[0]
193             c2_vector = selected_elements[1]
194
195             global S, G
196             G = w_graph(n)
197             S = Sandpile(G,0)
198
199             dlp_objects()
200             dlp_print()
201
202             solution = dlp_sandpile()
203
204             pretty_print('A diszkrét logaritmus probléma megoldása az $x =
205             ↳ {0}.$'.format(solution))
206
207     #CODE CN2
208     @interact(layout=[['n','g']])
209     def _(n = slider([6 .. 10], label = 'Gráf mérete', default = 8)):
210         @interact
211         def _(selected_elements = selector(example_list_cn2graph[n-6], label
212             ↳ = 'Választott konfigurációk', default =
213             ↳ example_list_cn2graph[n-6][0])):
214             global c1_vector, c2_vector
215             c1_vector = selected_elements[0]
216             c2_vector = selected_elements[1]
217
218             global S, G
219
220             G = cn2_graph(n)
221             S = Sandpile(G,0)
222
223             dlp_objects()
224             dlp_print()

```

```
221     solution = dlp_sandpile()
222
223     pretty_print('A diofantikus egyenletek megoldásaiból, a Kínai
↪   maradéktétel segítségével adódik a probléma megoldása.')
224     pretty_print('A diszkrét logaritmus probléma megoldása az $x =
↪   {0}.$'.format(solution))
```

Irodalomjegyzék

- [1] Per Bak, Chao Tang, and Kurt Wiesenfeld. Self-organized criticality: An explanation of $1/f$ noise. *Physical Review Letters*, 59:381–384, 08 1987.
- [2] Kim Christensen and Zeev Olami. Variation of the Gutenberg-Richter b values and nontrivial temporal correlations in a Spring-Block Model for earthquakes. *Journal of Geophysical Research*, 97:8729–8735, 06 1992.
- [3] Peter Grassberger. On a self-organized critical forest-fire model. *Journal of Physics A: Mathematical and General*, 26:2081, 01 1999.
- [4] C.J. Rhodes and R.M. Anderson. Forest-fire as a model for the dynamics of disease epidemics. *Journal of the Franklin Institute*, 335(2):199 – 211, 1998. Part Special Issue on Biomathematics.
- [5] John Beggs and Dietmar Plenz. Neuronal Avalanches in Neocortical Circuits. *The Journal of Neuroscience*, 23:11167–11177, 12 2003.
- [6] Ivana Ilic. *The Discrete Logarithm Problem in Non-abelian Groups*. PhD thesis, Boca Raton, FL, USA, 2010.
- [7] Norman Biggs. The critical group from a cryptographic perspective. *Bulletin of the London Mathematical Society*, 39, 08 2007.
- [8] Simon Blackburn. Cryptanalysing the Critical Group: Efficiently Solving Biggs’s Discrete Logarithm Problem. *IACR Cryptology ePrint Archive*, 2008:170, 11 2008.
- [9] Farbod Shokrieh. The monodromy pairing and discrete logarithm on the Jacobian of finite graphs. *Journal of Mathematical Cryptology*, 4, 07 2009.
- [10] Yaoping Hou, Chingwah Woo, and Pingge Chen. On the sandpile group of the square cycle C_n^2 . *Linear Algebra and its Applications*, 418:457–467, 10 2006.
- [11] D. J. Kleitman and B. Golden. Counting Trees in a Certain Class of Graphs. *The American Mathematical Monthly*, 82(1):40–44, 1975.
- [12] R.E. Cline, R.J. Plemmons, and G. Worm. Generalized inverses of certain Toeplitz matrices. *Linear Algebra and its Applications*, 8(1):25 – 33, 1974.

- [13] James E. Scroggs and Patrick L. Odell. An Alternate Definition of a Pseudo-inverse of a Matrix. *SIAM Journal on Applied Mathematics*, 14(4):796–810, 1966.
- [14] David Perkinson, Jacob Perlman, and John Wilmes. Primer for the algebraic geometry of sandpiles. 605, 12 2011.
- [15] Dmitry Zhukov, Valery Kanishchev, and Sergey Lyamin. Application of the Theory of Self-Organized Criticality to the Investigation of Historical Processes. *SAGE Open*, 6:215824401668321, 10 2016.