



**Nagy számításigényű
csoportalgebrai sejtés
megfogalmazásának elősegítése
párhuzamos programozási
eszközökkel**

Készítette

Lezsák Benjámín Tamás

Programtervező Informatika Bsc.

Témavezető

Troll Ede

tanársegéd

EGER, 2024

Tartalomjegyzék

Bevezetés	3
1. Nem kommutatív csoport feloldható hossza	4
1.1. Csoportalgebrai alapfogalmak	4
1.2. Diédercsoportok feloldható hossza	4
1.2.1. Diédercsoport	5
1.2.2. Feloldás	5
1.2.3. Összeadás és $F_2D_{2^n}$ csoport	6
2. Számítógéppel segített számítás	7
2.1. Megoldási tervek	7
2.1.1. 3 elemű részcsoporthok	7
2.1.2. 2^{m-1} elemű részcsoporthok	7
2.2. Párhozamosítás, elosztott rendszerek	8
2.3. Szuperszámítógépek alkalmazása	8
3. Nem kommutatív csoport feloldható hosszának kiszámítására implementált algoritmusok	10
3.1. Diédercsoport megvalósítása	10
3.2. $F_2D_{2^n}$ csoport megvalósítása	10
3.3. Futási eredmények	10
3.4. Futási idő kiszámítása	11
3.5. Hátralévő kísérletek	12
Összegzés	14
Irodalomjegyzék	15

Bevezetés

A matematika ma már sokszor az informatika eszközeit veszi igénybe a számításokhoz, mivel a számítógépek sokkal gyorsabban képesek kiszámítani az eredményeket, főleg akkor, ha csoportalgebráról van szó. Ám az elmúlt években voltak problémák, amit az eddig használt szoftver, a GAP (Groups, Algorithms, Programming) már nem tudott minden problémára eredményeket szolgáltatni, még szuperszámítógép használata mellett sem. Ezért mi az egyik ilyen problémára csináltunk egy specializált szoftvert, mely képes kiszámítani a 1024-ed rendű Diédercsoportból alkotott félcsoporthoz tartozó egységcsoporjának feloldási hosszát, és akár képes lehet ennél magasabb rendű csoportoknál is.

1. fejezet

Nem kommutatív csoport feloldható hossza

1.1. Csoportalgebrai alapfogalmak

A következőkben bemutatjuk azokat az alapvető csoportalgebrai fogalmakat, melyek a feladat megértéséhez és implementációjához szükségünk van.

1.1. Definíció. Félcsoport: az olyan $(G; \cdot)$ egyműveletes algebrai struktúrákat, ahol G tetszőleges nemüres halmaz, $\cdot$ pedig egy asszociatív művelet, félcsoportnak nevezzük.

Példa: Természetes számok halmaza az összeadásra vagy a szorzásra

1.2. Definíció. Csoport: A $(G; \cdot)$ egyműveletes algebrai struktúra, ahol a $\cdot$ művelet asszociatív, a G halmazon belül van neutrális elem, illetve minden G halmazon belüli elemnek van $\cdot$ műveletre értelmezett inverze, csoportnak nevezzük. Ha a művelet ezek mellett kommutatív is, akkor a csoportot Ábel-csoportokhoz soroljuk.

Példa: Egész számok halmaza az összeadásra

1.3. Definíció. Gyűrű: A $(R; +, \cdot)$ kétváltozós algebrai struktúra, ahol $(R; +)$ Ábel-csoport, $(R; \cdot)$ pedig félcsoport, és a két művelet egymásra disztributív, gyűrűnek nevezzük.

Példa: Egész számok halmaza az összeadásra és szorzásra nézve

1.4. Definíció. Test: A $(R; +, \cdot)$ kétváltozós algebrai struktúra, ahol $(R; +)$ és $(R; \cdot)$ Ábel-csoportok, emellett a két művelet egymásra disztributív, testnek nevezzük.

Valós számok halmaza majdnem teljesen megfelel ennek, de 0-val nem lehet osztani.

1.2. Diédercsoportok feloldható hossza

Ebben a részben megismerkedünk a Diédercsoport és a feloldás fogalmával



1.1. ábra. D_{16} vizuális reprezentációja

1.2.1. Diédercsoport

Egy csoportot Diédercsoportnak nevezünk, ha az egy szabályos sokszög önmagába képező egybevágóságai alkotnak. Az n -oldalú szabályos sokszöghöz tartozó Diédercsoportot D_{2n} -nel jelöljük. Ebben a csoportban a -val jelöljük a $\frac{2\pi}{n}$ szöggel való forgatást, és b -vel a tengelyes tükrözést. Minket ezekből a csoportokból azok érdekelnek, ahol 2^n darab elem van.

Példa: Tekintsük a $D_8 = \langle a, b : a^4 = 1, b^2 = 1, ba = a^3b \rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ 8-adrendű diédercsoportot. Ha a fenti elemek közül bármely két elemet összeszorozzuk, akkor az eredmény szintén a fenti halmaz eleme lesz. $Pl : ab \cdot a^3b = abaaab = aa^3baab = aa^3a^3bab = aa^3a^3abb = a^{10}b^2 = a^2$

1.2.2. Feloldás

Legyen G csoport a szorzásra nem-kommutatívan értelmezve, ekkor kiszámítható a kommutátor, amit $(a, b) := a^{-1}b^{-1}ab$ -vel jelölünk, ahol $a, b \in G$. A G csoport kommutátoraiból képezett $G' = \langle (a, b) : a, b \in G \rangle$ csoportot a G kommutátor-részcsoporthjának nevezzük. Hasonló módon rekurzívan definiálhatók a $G'', G^{(3)}, \dots$ csoportok, melyek egymás részcsoporthjai. A G csoport feloldható, ha létezik olyan $n \in \mathbb{N}$, melyre $G^{(n)} = \{1\}$. Ekkor a legkisebb ilyen n -et a G csoport feloldható hosszának nevezzük, jele: $dl(G)$.

Vizsgáljuk meg a D_8 diédercsoport kommutátorát: $(a, b) = a^{-1}b^{-1}ab = a^3bab = aaaaaabb = a^2$. Ha ezt minden kombinációra megcsináljuk, akkor megkapjuk, hogy $D'_8 = 1, a^2$, és $D''_8 = 1$, vagyis $dl(D_8) = 2$

A D_{2^n} diédercsoportot az alábbiak szerint definiáljuk:

$$D_{2^n} = \langle a, b : a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1}b \rangle = \{1, a, a^2, \dots, a^{2^{n-1}-1}, b, ab, a^2b, \dots, a^{2^{n-1}-1}b\}$$

Az első kommutátor-részcsoporthja:

$$D'_{2^n} = \{1, a^2, a^4, \dots, a^{2^n-2}, a^{2^n-1}\}$$

A második kommutátor-részcsoporthja: $D''_{2^n} = \{1\}$

Ezek alapján D_{2^n} feloldható, és $dl(D_{2^n}) = 2$.

1.2.3. Összeadás és $F_2D_{2^n}$ csoport

Tekintsük a $F_2 = (\{0,1\}; +, \cdot)$ kételemű testet, amit összevonnunk a D_{2^n} csoporttal, majd az így létrejött groupid-nak vesszük a szorzás műveletre vett egységcsoportját, vagyis az összes diédercsoport összeg-kombinációit tartalmazó félcsoportot, amiből azokat az elemeket tartjuk meg, amiknek van inverze a szorzás műveletre. Az így létrejött csoportot $F_2D_{2^n}$ -nel jelöljük. Ennek a feloldási hosszát a korábban említett GAP $n \leq 9$ -ig számította ki, ám az F_2D_{1024} csoportnak már nem tudta megállapítani.

Ezzel ugyan még nem lenne probléma, a egy sorozatot követne a feloldási hossz, viszont nem az, mivel $dl(F_2D_{32}) = dl(F_2D_{64}) = 4$, míg a többinél az előzőhöz képest 1-gyel növekedett. Azóta meg lett állapítva, hogy maximum 1-gyel növekedhet, és emellett nem lehet kevesebb, mint az előző.

2. fejezet

Számítógéppel segített számítás

A számítógépek megkönnyítik a számítást már a holdraszállás óta, mivel sokkal gyorsabban tudnak számolni, mint az emberek, és sokkal pontosabban is. Mint korábban említettem, a GAP is erre szolgál, viszont már egyes részei nem tökéletesek. Sejtéseink szerint az F_2D_{1024} -es csoportnak a feloldási hosszát amiatt nem tudja kiszámítani, mert túl sok adatot akar eltárolni (2^{1024} darab eleme van a csoportnak), és ezekből akarja kiszámolni a teljes csoport feloldási hosszát. A mi ötletünk az, hogy mi csak részcsoporthoz számoljuk ki a feloldási hosszát, mivel a csoport feloldási hossza nem lehet kisebb, mint bármely részcsoporthoz a feloldási hossza.

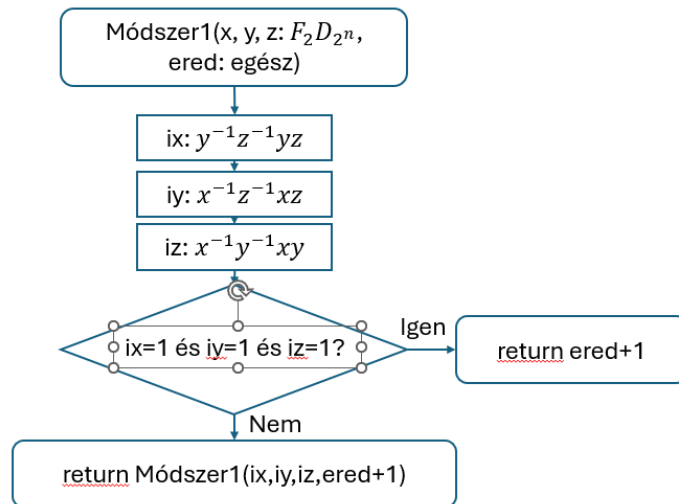
2.1. Megoldási tervek

2.1.1. 3 elemű részcsoporthoz

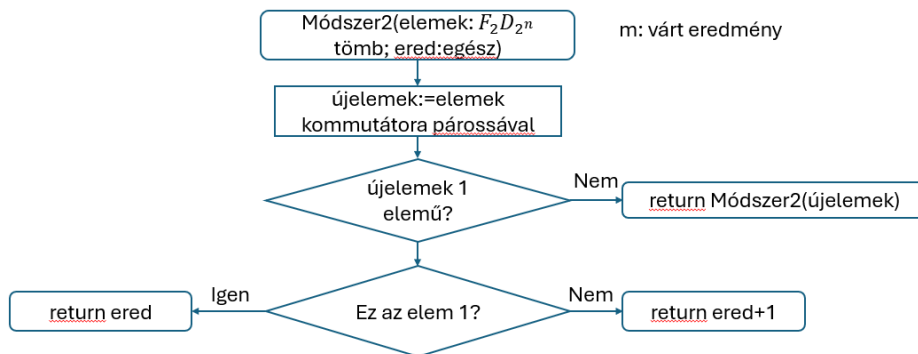
Vesszünk 3 elemet, párossával vesszük a kommutátorokat, majd azokat is ugyanígy vizsgáljuk. Ezt addig folytatjuk, amíg mindhárom elem nem lesz az egységelem, vagyis 1. Ezt kétféleképpen csináljuk, az elemek sorrendben való vizsgálásával és random elemek kiválasztásával. Ennek a módszernek a folyamatábrája a 2.1.-es ábrán látható.

2.1.2. 2^{m-1} elemű részcsoporthoz

$m :=$ várható feloldási hossz (előzőhöz képest $+1$). Ennél párossával kiszámoljuk a kommutátorokat, majd azoknak is, amíg 1 elem nem marad. Ekkor ezt az elemet megvizsgáljuk, és ha ez 1, akkor a feloldási hossz ezen részcsoporthoz $m-1$, ha nem az, hanem a csoport egy eleme, akkor m , és ekkor a programmal meg is találtuk, mi a feloldási hossz. Ennek a módszernek a folyamatábrája a 2.2.-es ábrán látható.



2.1. 3bra.



2.2. 3bra.

2.2. P3rhzamos3t3s, elosztott rendszerek

A p3rhzamos3t3s az a folyamat, amikor egy feladatot t3bb munkav3gz3 is megoszt, 3s ez nincs is m3shogy a programokn3l se. A programokat k3t szinten lehet p3rhzamos3tani, az egyik a processzoron bel3li, amikor a processzor magjai k3z3tt osztjuk meg, a m3sik hogy a processzor 3s a vide3k3rtya k3z3tt osztjuk meg, ut3bbi eset az3rt el3ny3s, mert a vide3k3rtya sz3m3t3k3pess3ge sokkal nagyobb, mint a processzor3. Ezeken bel3l m3g a program feloszt3s3nak m3lys3g3t is tekintj3k, ez lehet bitszint3, utas3t3sszint3, adat- 3s feladatp3rhzamos3t3s. Mi ezek k3z3l jelenleg a processzoron bel3li, adat- 3s feladatp3rhzamos3t3st alkalmazzuk programunkban, de tervek szerint ez tov3bb fejleszthet3

2.3. Szupersz3m3t3g3pek alkalmaz3sa

A szupersz3m3t3g3peket sokszor haszn3lj3k sz3m3t3sok elv3gz3s3re, ugyan ma m3r inkább fizikai 3s biol3gi3i kutat3sokn3l k3rik a seg3ts3g3t, de ezen esetekben is mate-

matikai számításokra használják elsősorban. Ezen eszközök a személyi számítógépek számítási igényének sokszorosát tudják megvalósítani, ezzel jelentősen rövidebb idő alatt képes elvégezni ugyanazokat a számításokat, ami a mi esetünkben kell is, mivel ahhoz, hogy csak kis részét a számításoknak elvégezzük (1000 eset) minimum egy hónap kéne, de a Komondor szuperszámítógépen, amit tervezünk használni, kevesebb mint 0,1 másodperc kell. Később ezt meg is mutatom, hogyan jött ki ez az időigény. Korábban a GAP szoftvert is futtaták ugyanerre a kérdéskörre egy szuperszámítógépen, ám nem adott ki eredményt ennél a csoportnál. Sejtéseink szerint a teljes F_2D_{1024} csoportot akarta betölteni, ami túl sok adatnak bizonyult ($2^{2^{1023}}$ elem), ám a mi programuk futás közben generálja az elemeket, és törli azokat, amiket már nem használ

3. fejezet

Nem kommutatív csoport feloldható hosszának kiszámítására implementált algoritmusok

Megismerkedünk a program azon részeivel, melyek elvégzik számunkra a feladatot

3.1. Diédercsoport megvalósítása

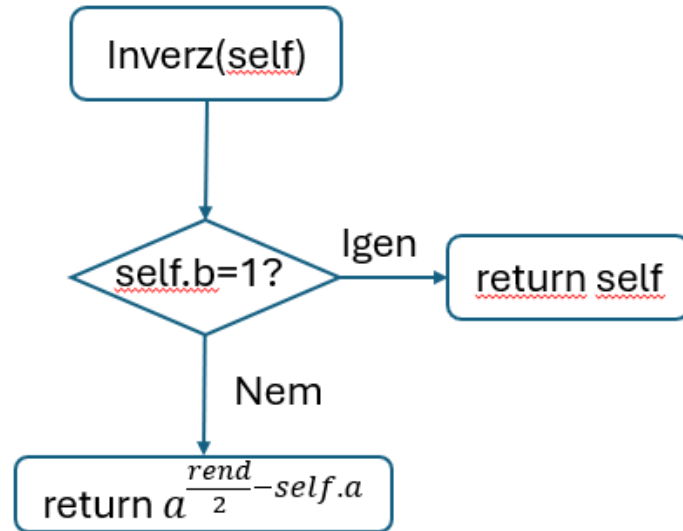
A csoport tagjait mint osztályt hoztuk létre, ezek két mezővel rendelkeznek, a -val és b -vel, a korábban említett forgatás és tükrözés jelölésére. Az osztályon belül még definiálunk 2 műveletet, az inverzet (3.1. ábra) és a szorzást (3.2. ábra). Ezen kívül létrehoztunk egy konténerosztályt, ami csak arra van, hogy egy diédercsoport összes elemét tárolja. Mivel a csoportok, amivel még jelenleg dolgozunk, nem túl nagyok, ezért ezek tárolása minimális tárhelyet vesz igénybe.

3.2. $F_2D_{2^n}$ csoport megvalósítása

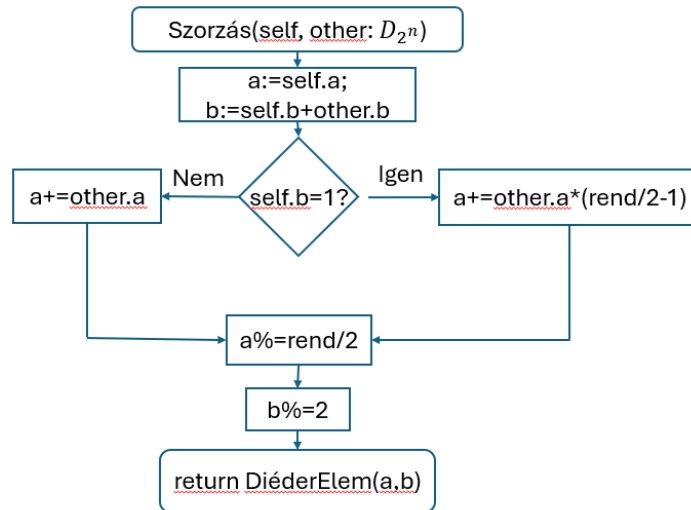
Ennél a csoportnál egy lista tartalmazza az adott elem diédercsoportbeli elemeit, és egy elem ezen elemek összege. Itt is az inverzet (3.3. ábra) és a szorzást, előbbi az általános csoportalgebrai inverzszámítás szabályait követi, míg utóbbi megszorozza minden elemét a másik minden elemével, és azoknak az összegét adja eredményül.

3.3. Futási eredmények

Az eddigi futásoknál, ahol nem túl sok esetet vizsgáltunk (körülbelül 40 esetet) maximum 7-et adott ki eredményül a feloldási hosszra az adott részcsoporthoz.



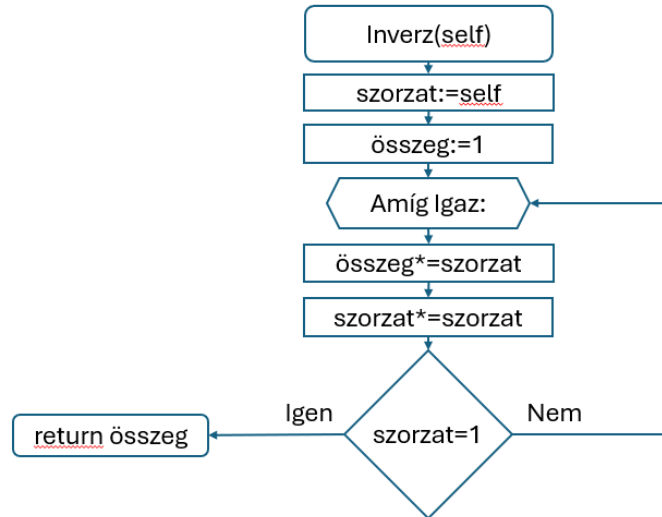
3.1. ábra.



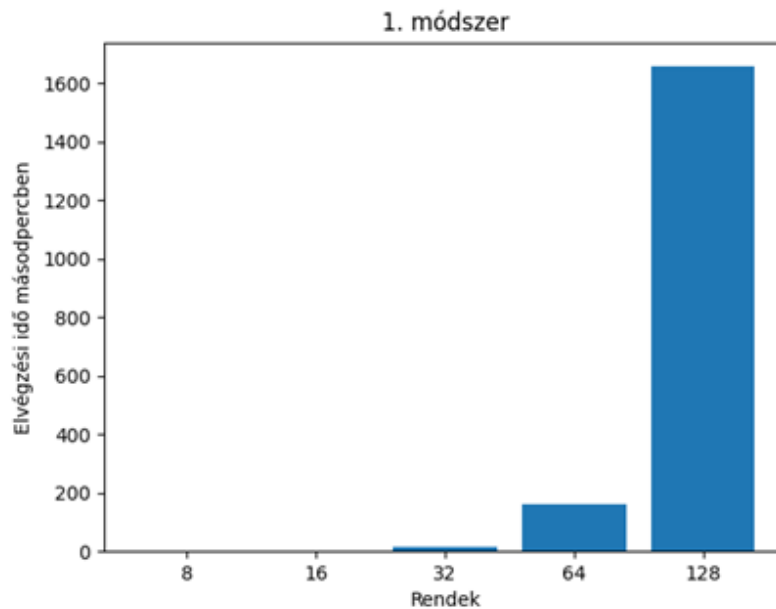
3.2. ábra.

3.4. Futási idő kiszámítása

Langrange interpoláció segítségével egy közelítő ívet tudunk kapni az időkre. Mivel ugyanúgy 1000 esetet vizsgáltunk a lentebbi ábrákon (3.4. ábra és 3.5. ábra), az idő és a diédercsoport rendjének függvényében kiszámítható, hogy ugyanennyi eset kiszámítására a laptopon, amin a program futott, körülbelül mennyi idő kéne nagyobb csoportok esetén, és így jött ki a fentebb említett 32 nap az első módszernél, és 722 nap a második módszernél. Ezeket az időket utána megszorozzuk a laptopom és a Komondor szuperszámítógép számítási erejének arányával, így jöttek ki a várható idők, ami az első módszernél 0,1 másodperc, a másodiknál pedig 2,1 másodperc



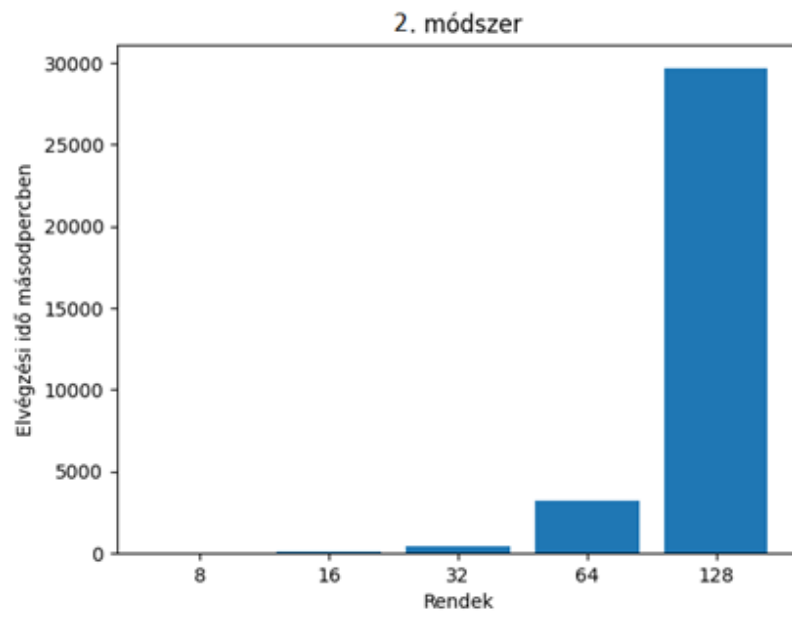
3.3. ábra.



3.4. ábra.

3.5. Hátralévő kísérletek

Ugyan a program kész van, de még a futtatások a fentebb említett hosszú számítási idő miatt nem végezhetőek el teljesen. Egyik opciónk a már említett szuperszámítógép használata, ám előre sejthető, hogy azon is sokáig futna a program, ezért van még egy lehetőségünk, miszerint egy magasabb rendű, mi esetünkben az F_2D_{2048} -as csoporton is megnézni néhány esetre a feloldás hosszát. Ez utóbbi azért működhet, mert ha be tudjuk bizonyítani, hogy ennél a magasabb elemszámú csoportnál 9 a feloldás hossza, akkor tudjuk azt is, hogy az általunk vizsgált csoportnál 8-nak kell lennie, mivel mindig legfeljebb 1-gyel lehet magasabb a feloldási hossz az előzőnél a 2^n elemű Diédercsoport-



3.5. ábra.

toknál.

Összegzés

A Diédercsoport egy egyszerűen megfogható, ám algebrailag annál bonyolultabb csoport, ahol mi az egyik ebből alkotott egységcsoportot vizsgáltuk, és kerestük az eddig ismeretlen feloldási hosszát, párhuzamosítást alkalmazva a programunkban. A programot az elejétől építettük fel, a korábbi módszerek és diédercsoport-megvalósítások kódjainak felhasználása nélkül, és egy, bármely $F_2D_{2^n}$ típusú csoportra használható programot hoztunk létre, új és kipróbált módszerek keverékével. Ezt a programot párhuzamosítottuk, így a módszerek egymás mellett többször is lefutnak. A közeljövőben lefutatjuk szuperszámítógépen is, és ha ez nem jön össze, akkor az F_2D_{2048} -as csoportnak nézzük meg a lehetséges feloldási hosszát.

Link a kódhoz (nem kerül módosításra a dolgozat leadása után): <https://github.com/Downbag/DiederCsoportFeloldas>

Irodalomjegyzék

- [1] FIGULA, Á., JUHÁSZ, T.: *On the derived length of the unit group of group algebras of groups with cyclic commutator subgroup*, Commun. Alg. 51, No. 2, 633-647 (2023)
- [2] JUHÁSZ, T.: *On the derived length of Lie solvable group algebras*, Publ. Math. Debrecen, 68, No. 1-2, 243-256, (2006)
- [3] KONOVALOV, A.: *Wreath products in the unit group of modular group algebras of 2-groups of maximal class*, PhD Thesis, Mathematical Institute, Ukrainian National Academy of Sciences, Kiev, 1995.
- [4] : SEHGAL, S.K.: *Topics in group rings*, Marcel Dekker, New York, 1978.
- [5] *The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.6; 2016*