Ph.D. Tézisfüzet

Leszámlálási és extremális problémák az aritmetikai kombinatorikában

Palincza Richárd

Témavezető: Dr. Pach Péter Pál

Számítástudományi és Információelméleti Tanszék
Budapesti Műszaki és Gazdaságtudományi Egyetem

2023

Bevezető

A kombinatorika területén számos extremális probléma vált népszerű kérdéssé az elmúlt pár évtizedben. Ezen problémák jó része bár könnyen megfogalmazható, roppant nehéznek bizonyult, például számos Ramsey-típusú probléma is ilyen. A Ramsey-tétel állítása szerint minden c és k számra létezik olyan véges n, melyre, ha kiszínezzük K_n (azaz n csúcsú teljes gráf) éleit c színnel, biztosan találunk legalább egy egyszínű K_k részgráfot. Habár ezt a tételt alapképzésen is tanítják (sőt, egyes középiskolákban is), a pontos határ máig ismeretlen már olyan kis értékekre is, mint $k = 5$ és $c = 2$.

Egy szorosan kapcsolódó eredmény – ha gráfok helyett egész számokat színezünk – van der Waerden tétele [52]. Ez azt állítja, hogy bárhogy színezzük ki a pozitív egész számokat véges sok szín felhasználásával, mindig található közöttük tetszőleges (véges) hosszú egyszínű számtani sorozat. Habár ez már 1927 óta ismert, a kvantitatív változata máig nyitott: a legjobb alsó és felső becslések a pontos határokra általában nagyon távol vannak egymástól. Ezen felül az általános esetben csak csillagászati léptékű felső becslések ismeretesek.

Egy másik gyakran vizsgált kérdéskör a leszámlálási problémák köre. Ezen kérdések során célunk, hogy meghatározzuk egy halmaz bizonyos tulajdonságokkal rendelkező részhalmazainak számát. Ilyen problémák között is számos nehezet találunk, akár már kis esetekre is. Például megszámolni egy gráf adott tulajdonságú részgráfjait már annyira nehéz, hogy azt is NP-teljes eldönteni, hogy egy adott gráfnak egyáltalán van-e *legalább egy* Hamilton-köre [33].

Komoly matematikai bizonyítások során számítógépes segítséget először a Négyszín-tétel igazolására használtak 1976-ban. (Azaz annak igazolásához, hogy tetszőleges síkbarajzolható gráf csúcsai kiszínezhetőek négy szín felhasználásával.) Akkoriban ezt sokan lenézően kezelték és kritizálták, mondván, hogy ez nem egy „igazi” bizonyítás, ha nem lehet (belátható időn belül) kézzel ellenőrizni [47]. Azóta a számítógépes segítség igénybevétele bevett szokás

lett, mind computer algebra rendszerek terén, mind esetek szisztematikus végignézésére és más egyéb alkalmazásokhoz is.

Konkrét példaként számos extremális eredményt is jelentős számítógépes segítséggel értek el. A számtani sorozatot nem tartalmazó halmazok esetén nem csak a kis esetek esetén pontos válaszok, de az aszimptotikusan legjobb konstrukciókat is számítógépes segítséggel találták.

Ezen disszertációban vizsgálunk leszámlálási és extremális problémákat is. A bizonyításainkban egy közös elem a számítógépes segítség használata.

A disszertáció felépítése a tézisek szerint

A disszertáció bevezetés utáni első három fejezete az úgy nevezett *primitív* halmazokkal, és ezek általánosításával kapcsolatos problémákkal foglalkozik. Egész számok egy halmazát akkor nevezünk *primitív*nek, ha nincs két eleme, amik közül egyik osztja a másikat. A továbbiak során jelölje $[n]$ az $\{1, 2, 3, \ldots, n\}$ halmazt.

2. Fejezet

A fejezet főbb eredményei a folyóiratcikkünkön [2] alapulnak. Néhány eredmény szerepelt már a korábbi konferenciacikkünkben[1] is.

Az $[n]$ halmaz primitív részhalmazainak számával először Cameron és Erdős [15] foglalkozott 1938-ban. Jelöljük $g(n)$-nel $[n]$ halmaz primitív részhalmazainak számát. Erdősék belátták, hogy elég nagy n értékekre $1{,}55967^n \leq g(n) \leq 1{,}6^n$ igaz, s sejtették, hogy a $g(n)^{1/n}$ kifejezés határértéke létezik. Habár 2018-ban Angelo [7] belátta ezt a sejtést, nem tudott az ismerteknél jobb becsléseket adni a határértékre. A 2. fejezetben egy, az övétől különböző bizonyítást adunk a sejtésre, megmutatva, hogy az $[n]$ primitív halmazainak száma $(\beta + o(1))^n$ alkalmas β-ra. Ezen felül adunk egy algoritmust, ami – elméletben tetszőlegesen – közelíteni tudja $\beta \approx 1.57$ értékét.

Egy ehhez kapcsolódó probléma meghatározni a $[2n]$ halmaz *maximális méretű* primitív részhalmazainak számát. Ezt a változatot Bishnoi vetette fel az „On a famous pigeonhole problem” [13] című blogbejegyzésében. Megjegyzendő, hogy $[2n]$ egy maximális méretű primitív halmaza pontosan n méretű. Ugyanis, ha $[2n]$ elemeit n csoportba osztjuk a legnagyobb páratlan osztójuk szerint, akkor egy primitív halmaz minden csoportból csak legfeljebb egy-egy elemet tartalmazhat. Másrészről pedig például az $\{n+1, \ldots, 2n\}$ halmaz n

elemű és primitív. Jelölje $f(n)$ a $[2n]$ halmaz n elemű primitív részhalmazainak számát. Vijay [51] belátta, hogy elég nagy n-re $1{,}303^n \leq f(n) \leq 1{,}408^n$ teljesül, ellenben nyitott kérdés maradt, hogy az $f(n)^{1/n}$ határérték létezik-e. A 2. fejezetben a kérdést megválaszoljuk: megmutatjuk, hogy $f(n)^{1/n}$ valóban tart egy α számhoz, mely körülbelül 1,318. Egy algoritmust is adunk, ami képes α értékét tetszőlegesen megközelíteni. Gyakorlati szempontból (rendelkezésre álló számítási kapacitás és futási idő alatt) kiszámítottuk, hogy $1{,}3183 \leq \alpha \leq 1{,}31843$ és $1{,}571068 \leq \beta \leq 1{,}574445$. Utánunk még ugyanabban az évben McNew [36] egyéb módszerekkel javított kicsit a numerikus alsó becsléseinken, ellenben a felső becsléseinken nem tudtak javítani.

A 2. fejezet főbb eredményei a következő tézisek:

2.1. Tétel (Liu, Pach, Palincza [2]). A $[2n]$ halmaz n elemű primitív részhalmazainak száma $f(n) = (\alpha + o(1))^n$. Ezen felül, tetszőleges $\varepsilon > 0$ értékhez létezik olyan $N(\varepsilon)$, hogy α approximálható $1+\varepsilon$ mértékű multiplikatív hibával $N(\varepsilon)$ lépés alatt.

Numerikus eredmények. Az algoritmusunk alsó ($\approx 1{,}3184$) és felső ($\approx 1{,}3183$) becslést ad α-ra, melyek aránya 1,0001 alatti.

A fő ötlet ezen eredmények eléréséhez az volt, hogy számoljuk meg, hányféle módon választhatunk antiláncokat különböző méretű oszthatósági hálókból. A numerikus eredmények számítógépes segítséggel jöttek ki, ügyes algoritmustervezési trükköket is használva a számítások felgyorsítására. Az algoritmusok elméleti háttere a 2.2. alfejezetben olvasható. Az algoritmus tervezésének részleteit bővebben a 2.5. alfejezetben fejtjük ki.

Numerikus eredmények. Az algoritmusunk módosítható úgy, hogy közelítse a $g(n)^{1/n}$ határértéket is, olyan felső ($\approx 1{,}5745$) és alsó ($\approx 1{,}571$) becsléseket ad β értékére, melyek aránya kisebb, mint 1,0022.

Ezen eredmények eléréséhez érdekes megfigyelésekre volt szükség kétdimenziós hálókról, főleg arról, hogy hogyan számoljunk meg *nem* maximális méretű részhalmazokat.

3. Fejezet

A 3. fejezet is egy közös cikkünkön [3] alapul. A fejezet témája egy előbbiekhez kapcsolódó témakör: a h-primitív halmazok.

Azt mondjuk, hogy egy $A \subseteq \mathbb{N}$ halmaz h-primitív, ha nincsenek olyan különböző $a_0, a_1, \ldots, a_h \in A$ elemei, amikre a_0 osztja az $a_1 a_2 \ldots a_h$ szorzatot. Egy S halmaz h-primitív részhalmazainak halmazát jelöljük $\mathcal{P}_h(S)$-sel.

A h-primitív halmazokat először Erdős [25] vizsgálta még 1938-ban („$\mathcal{P}_h$ tulajdonságú halmazok"-ként hivatkozik rájuk), cikkében az $[n]$ halmaz maximális méretű 2-primitív részhalmazaival foglalkozott. A 3. fejezetben a h-primitív halmazok leszámlálásával foglalkozunk. Megjegyezzük, hogy a $h = 1$ eset éppen a primitív halmazok esete, amit az előző fejezetben vizsgáltunk, azonban a $h > 1$ eset más módszereket igényel. A fejezetben igazoljuk, hogy az $[n]]$ halmaz 2-primitív részhalmazainak száma $T(n) \cdot e^{\Theta(n^{2/3}/\log n)}$, ahol $T(n) \approx (3{,}517\ldots)^{\pi(n)}$. Ezen felül $h > 2$ esetén a h-primitív részhalmazok száma $T(n) \cdot e^{\sqrt{n}(1+o(1))}$. Érdekesség, hogy a kitevőben a fő tag mellett a hibatag is pontos konstans szorzó erejéig.

A felső becslést (mind a $h = 2$, mind a $h > 2$ esetben) h-adrendű multiplikatív bázisok segítségével kaptuk meg. Egy $B \subseteq \mathbb{Z}^+$ halmaz akkor alkot *h-adrendű multiplikatív bázist* az S halmazban, ha S minden $s \in S$ elemét ki tudjuk fejezni h darab B-beli elem szorzataként. Például B akkor h-adrendű multiplikatív bázisa $[n]$-nek, ha $[n] \subseteq B^h$, azaz minden n-nél nem nagyobb pozitív egész kifejezhető, mint h darab (nem feltétlen különböző) B-beli elem szorzata. A fő ötletünk az volt, hogy egy adott (h-adrendű) multiplikatív B bázisra és adott h-primitív A halmazra mindig létezik egy $\varphi : A \to B$ injektív leképezés úgy, hogy tetszőleges $\varphi(a) = b$ esetén $b \mid a$ teljesül. Meg tudjuk határozni, hogy mely elemek képződnek prímekre, és mely elemek képződnek B-beli nem-prím elemekre (amik *kevesen* vannak). A lehetséges leképezéseket megszámlálva kapjuk a felső becslést a h-primitív halmazok számára. A h-primitív halmazok és multiplikatív bázisok méretét és kapcsolatát részletesen tárgyalja [40] cikk.

Legyen $H_h(n)$ az $[n]$ halmaz h-primitív részhalmazainak száma, továbbá $T(n)$ legyen az alábbi függvény:

$$T(n) := \prod_{\substack{\sqrt{n} < p \le n, \\ p \text{ prím}}} ([n/p] + 1).$$

A főbb tézisek a 3. fejezetben az alábbiak:

3.1. Tétel (Pach, Palincza [3]). Léteznek olyan c_1 és c_2 pozitív konstansok, hogy az $[n]$ halmaz 2-primitív részhalmazainak számára teljesül az alábbi:

$$T(n) \cdot e^{c_1 n^{2/3}/\log n} \le H_2(n) \le T(n) \cdot e^{c_2 n^{2/3}/\log n},$$

ha n elég nagy.

Ezzel analóg állítás igazolunk $h \geq 3$ esetén is:

3.2. Tétel (Pach, Palincza [3]). Legyen $h \geq 3$ tetszőleges egész. Elég nagy n esetén az $[n]$ halmaz h-primitív részhalmazainak számára teljesül a következő:

$$T(n) \cdot e^{\sqrt{n}} e^{-11\sqrt{n}\log\log n/\log n} \leq H_h(n) \leq T(n) \cdot e^{\sqrt{n}} e^{4\sqrt{n}\log\log n/\log n}.$$

4. Fejezet

Ez a fejezet egy konferenciacikkemen [5] alapul.

A fejezet a korábbi fejezetekből megismert h-primitív halmazokkal és multiplikatív bázisokkal foglalkozik, azonban leszámlálásuk helyett a felismerésük – számításelméleti értelemben vett – bonyolultságával.

Adott h értékre annak eldöntése, hogy egy halmaz h-primitív-e, illetve, hogy (h-adrendű) multiplikatív bázis-e, megtehető polinomiális időben, az összes megfelelő részhalmaz naiv végignézésével. Ezzel szemben, ha a h értéke is a bemenet részét képzi, megmutatjuk, hogy a h-primitívség eldöntése coNP-teljes feladat, továbbá, hogy egy B halmaz h-adrendű multiplikatív bázisa-e egy bemenetként megadott S halmaznak, pedig NP-teljes probléma.

A főbb téziseim a 4. fejezetben az alábbiak:

Megjegyzés. Annak kérdése, hogy adott h-ra egy halmaz h-primitív-e, eldönthető $O(h \cdot n^{h+1})$ aritmetikai művelettel, ahol n a halmaz mérete.

Habár egy adott h-ra ez polinomiális az input méretében, az általános esetről az derül ki, hogy az bonyolult:

4.1. Tétel (Palincza [5]). A következő eldöntési probléma coNP-teljes: „Adottak $a_1, \ldots, a_k$ és h pozitív egészek; döntsük el, hogy az $\{a_1, a_2, \ldots, a_k\}$ halmaz h-primitív-e.”

A tétel bizonyításához a coNP-beliségének megmutatása mellett a *Minimális lefogó ponthalmaz* problémát vezetjük vissza ezen probléma komplementére. A visszavezetés általános bemutatása után egy konkrét példán is szemléltetjük.

A multiplikatív bázisok esetében az alábbiakat mutatjuk meg:

Megjegyzés. Vegyük azt a kérdést, hogy egy halmaz h-adrendű multiplikatív bázis-e az $[n]$ alaphalmazban (ahol h is lehet az input része). Ezt meg lehet válaszolni $O(nh|B|)$ időben. Erről az derül ki, hogy polinomiális a bemenet méretében, mivel, ha a bemenet egy multiplikatív bázis, akkor nem lehet túl kicsi n és h méretéhez képest.

Ezzel szemben, ha tetszőleges alaphalmaz esetén vizsgáljuk a kérdést (nem csak $[n]$-ben), a következő eredményt kapjuk:

4.2. Tétel (Palincza [5]). Ha h is a bemenet része és tetszőleges alaphalmazt tekintünk (nem csak $[n]$ alakúakat), annak eldöntése, hogy egy halmaz h-adrendű multiplikatív bázis-e, NP-teljes problémává válik. Megjegyzendő, hogy már akkor is NP-teljes a probléma, ha az alaphalmazunk 1 elemű (ami annak eldöntése, hogy egy adott szám előáll-e legfeljebb h báziselem szorzataként).

A bemutatott bizonyítás alapötlete az X3C (pontos fedés 3 méretű halmazokkal) probléma visszavezetése a vizsgált problémára.

5. Fejezet

Ezen fejezet is egy folyóiratcikkünkön [4] alapul.

Az előző fejezetekben bizonyos *multiplikatív* tiltott struktúrát elkerülő halmazokkal foglalkoztunk, például azt írtuk elő, hogy a halmaz elemei ne osszák egymást. Ezzel szemben az 5. fejezetben bizonyos *additív* tiltott struktúrákat vizsgálunk, elsősorban azt, amikor a halmazunk nem tartalmaz adott hosszúságú *számtani sorozatot.*

Egy másik különbség a korábbi fejezetekhez képest, hogy ahelyett, hogy leszámlálnánk a megfelelő halmazokat, itt azt vizsgáljunk, hogy mekkora lehet a maximális méretük.

Az elmúlt időben nagy érdeklődés övezte a $\mathbb{Z}_m^n := (\mathbb{Z}/(m\mathbb{Z}))^n$ csoportokban maximális méretű számtanisorozat-mentes halmazok méretének becslését, kiváltképp az $m = 3$ és $m = 4$ esetében. Jelölje $r_k(\mathbb{Z}_m^n)$ a $\mathbb{Z}_m^n$ csoport maximális méretű olyan részhalmazának méretét, ami nem tartalmaz k elemből álló számtani sorozatot. A továbbiakban, ha k elemű számtani sorozatra hivatkozunk, ez alatt mindig nem elfajulót értünk, ahol mind a k tag különböző. Megjegyezzük, hogy az $m = 3, 4, 5$ esetben a „nincs 3 elemű számtani sorozat” és a „nincs három pont egy egyenesen” állítások ekvivalensek, az

utóbbi feltételnek eleget tevő halmazokat a véges geometriában „cap”-nek nevezik.

Az alábbiak ismertek [18, 22–24, 31, 50] a $k = 3$ és $m \in \{3, 4\}$ esetekben:

$$2{,}218021\ldots^n \leq r_3(\mathbb{Z}_3^n) \leq 2{,}755\ldots^n/\sqrt{n},$$

$$3^n/\sqrt{n} \ll r_3(\mathbb{Z}_4^n) \leq 3{,}61\ldots^n,$$

és általában is, bármely $p \geq 3$ prímhez van $\delta_p > 0$ konstans úgy, hogy a következő becslés teljesül:

$$r_3(\mathbb{Z}_p^n) \leq (p - \delta_p)^n.$$

(Megjegyezzük, hogy az $r_3(\mathbb{Z}_3^n)$ alsó becslése csak elég nagy n-ekre érvényes, ellenben a felső becslések minden n-re.) Pontosabban, a módszert erre az esetre alkalmazva [14] azt kapjuk, hogy

$$r_3(\mathbb{Z}_p^n) \leq (J(p)p)^n,$$

ahol

$$J(p) = \frac{1}{p} \min_{0<t<1} \frac{1 - t^p}{(1-t)\, t^{(p-1)/3}}. \tag{1}$$

Mivel $J(p)$ monoton csökkenő és $J(3) \leq 0{,}9184$, ezért ebből következik, hogy minden $m \geq 3$ esetén: (lsd. pl. [14] és [42]):

$$r_3(\mathbb{Z}_m^n) \leq (0{,}9184m)^n. \tag{2}$$

A fejezetben főleg a $r_k(\mathbb{Z}_6^n)$ esettel foglalkozunk. A csoport méretéhez képest exponenciálisan kicsi felső becslést adunk $r_6(\mathbb{Z}_6^n)$-re. Továbbá vizsgáljuk a problémát alacsony dimenziókra, pontos választ adunk $n = 2$-re és nemtriviális alsó és felső becsléseket $n = 3$ esetén. Az utóbbiakat IP solverek segítségével kaptuk, a fejezet arról szól, hogyan használtuk kreatívan ezeket az eszközöket, hogy élesebb eredményeket érjünk el.

A fejezet főbb tézisei az alábbiak:
Kis esetekben pár konkrét érték meghatározása és becslése:

5.1. Tétel (Pach, Palincza [4]). Olyan halmazok esetén, amelyek nem tartalmaznak 6 hosszú számtani sorozatot, a következő korlátok igazak alacsony dimenzió esetén:

$$r_6(\mathbb{Z}_6^1) = 5, \quad r_6(\mathbb{Z}_6^2) = 25, \quad 117 \leq r_6(\mathbb{Z}_6^3) \leq 124.$$

Az $r_6(\mathbb{Z}_6^3) \leq 124$ becslés különösen érdekes az alábbi észrevétel miatt.

Megjegyzés. Habár az

$$r_k(\mathbb{Z}_m^{a+b}) \geq r_k(\mathbb{Z}_m^a) \cdot r_k(\mathbb{Z}_m^b)$$

egyenlőtlenség fennáll minden k, a, b pozitív egész és minden m prímszám esetén a szorzat-konstrukció alapján, itt (mivel a 6 nem prím) nem csak, hogy a szorzat-konstrukció nem működik, hanem $r_6(\mathbb{Z}_6^3) < r_6(\mathbb{Z}_6^2) \cdot r_6(\mathbb{Z}_6^1)$.

Nagy n értékekre a következő aszimptotikus eredményeket kaptuk:

5.2. Tétel (Pach, Palincza [4]). Olyan halmazok esetén, amelyekben nincs 6 hosszú számtani sorozat, a következők igazak:

$$4{,}436^n \leq 2^n r_3(\mathbb{Z}_3^n) \leq r_6(\mathbb{Z}_6^n) \leq 5{,}709^n,$$

feltéve, hogy n elég nagy.

Ezen felül adunk $r_3(\mathbb{Z}_3^n)$ értékétől függő aszimptotikus felső becslést is:

5.4. Tétel (Pach, Palincza [4]). Olyan halmazokra, amelyek nem tartalmaznak 6 hosszú számtani sorozatot, teljesül az alábbi egyenlőtlenség:

$$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}.$$

Rövidebb számtani sorozatok esetén alacsony dimenziós esetben az alábbiakat kaptuk:

Megjegyzés. Olyan halmazokra, amelyekben nincs 4, illetve 5 hosszú számtani sorozat: $r_4(\mathbb{Z}_6^3) \geq 81$, and $r_5(\mathbb{Z}_6^3) \geq 82$.

Ez utóbbi megjegyzésben érdekes, hogy jobb korlátokat kaptunk ügyes konstrukciókkal, mint ha csak naivan futtattuk volna az IP solvereket.

Alkalmazások

Ez a disszertáció elsősorban elméleti eredményekkel foglalkozik, amik önmagukban is érdekesek. További motivációként néhány nem szigorúan matematikai alkalmazását is vázoljuk a témáknak.

A SET játék

Az extremális eredményeknek egy érdekes valóéletbeli alkalmazása a SET nevű kártyajátékhoz [19] kapcsolódik. A játék különböző kártyákból áll, mindnek négy-négy tulajdonsága van. Minden kártyán található egy, kettő vagy három szimbólum, három szín egyikében, három különböző forma, illetve három különböző telítettség egyikében. Minden szín-darabszám-forma-telítettség kombináció pontosan egy kártyán fordul elő a pakliban, tehát összesen $3^4 = 81$ kártyából áll a pakli. A játék során néhány kártyát osztunk képpel felfele az asztal közepére, s a játék célja, hogy *SET*-eket találjunk benne. Egy *SET* három olyan kártya összessége, amik minden tulajdonságukban vagy egyformák, vagy páronként különbözőek. Amikor egy játékos talál egy *SET*-et, elveszi az asztalról, és 3 új kártyát oszt a pakliból. A játék célja általában az, hogy több *SET*-et gyűjtsünk, mint bármely ellenfelünk.

Egy érdekes kérdés annak meghatározása, hogy legalább hány kártyát kell osztanunk, hogy garantáltan létezzen *SET* a kiosztott kártyák között. A játék azt ajánlja, hogy osszunk 12 kártyát, s ha senki nem talált *SET*-et belátható időn belül, osszunk még 3 darabot. Megfigyelhetjük, hogy a játékban egy *SET* megtalálása ekvivalens azzal a feladattal, mintha egyeneseket keresnénk a $\mathbb{Z}_3^4$ affin síkon. Ez pedig azzal is egyenértékű, mintha 3 hosszú számtani sorozatokat keresnénk $\mathbb{Z}_3^4$-ben. Ennélfogva annak a kérdésnek az eldöntése, hogy hány kártyát tudunk kirakni úgy, hogy ne legyen köztük *SET*, ugyanaz, mint $r_3(\mathbb{Z}_3^4)$ meghatározása – aminek értéke 20. (Ez az eredmény már korábban is ismert volt, mi főleg IP solverek összehasonlítására használtuk, lsd. 5.4. alfejezet)

Az előbbi probléma általánosítása több tulajdonságra $r_3(\mathbb{Z}_3^n)$ becslésének kérdéséhez vezet, egészen 2016-ig ismeretlen volt, hogy a pontos érték exponenciálisan kisebb-e a pakli méreténél (3^n) vagy nem, tehát $(3 - o(1))^n$ méretű. Ekkor jött az áttörés a témában, Croot–Lev–Pach és Ellenberg–Gijswijt [18, 23] cikkekben kidolgozott módszer, illetve eredmény szerint exponenciálisan kisebb 3^n-nél. Ennek ellenére még mindig távol van egymástól a legjobb ismert alsó és felső korlát, de az alsó korlát várhatóan javulni fog jobb konstrukciók felfedezésével.

Titokmegosztás

A h-primitív halmazok egy lehetséges alkalmazása egy titokmegosztási protokoll naiv modellje. Vegyünk egy céget (pl. titkosügynökség), aminek vannak

ügynökei és vállalati titkai, ez utóbbiakat különböző prímszámoknak feleltetjük meg. Minden ügynök ismeri ezen titkok egy részhalmazát. Ezt az alábbi módon reprezentáljuk: minden ügynökhöz hozzárendelünk egy egész számot: az általa ismert titkok (reprezentáló prímszámainak) szorzatát. Az egyszerűség kedvéért feltehetjük, hogy a prímfelbontást is tudják, nem csak a számot.

A cég szeretné, hogy egyik ügynökét se lehessen teljes mértékben „helyettesíteni" egyetlen másik ügynökkel sem, tehát semelyik ügynök titkainak halmaza se legyen részhalmaza egy másik ügynök titkainak. Ez a követelmény pont azt jelenti, hogy az ügynökökhöz rendelt számok egy primitív halmazt alkotnak.

Ha a cégünk azt is szeretné, hogy ezen felül h darab összebeszélő ügynök se tudjon helyettesíteni egyetlenegy másik ügynököt sem, akkor pontosan a h-primitívséget kell megkövetelnünk a halmazról.

Ehhez hasonló titokmegosztási protokollokat alkalmaznak is a gyakorlatban, ha szeretnék egy számítógépes rendszertől, hogy hibatűrő (nem mindent csak egy helyen tárolnak), de egyúttal biztonságos is legyen (egy hálózati csomópont feltörésével ne lehessen az összes információhoz hozzájutni).

Publikációs lista

Kapcsolódó Publikációk

[1] H. Liu, P. P. Pach, R. Palincza: *The number of maximum primitive sets of integers* (Conference version), Proceedings of the 11th Hungarian-Japanese Symposium on Discrete Mathematics and Its Applications, (2019), 348–352.

[2] H. Liu, P. P. Pach, R. Palincza: *The number of maximum primitive sets of integers*, Combinatorics, Probability and Computing **30 (5)**, (2021), 781–795.

[3] P. P. Pach, R. Palincza: *The counting version of a problem of Erdős*, European Journal of Combinatorics **90**, (2020), 103187.

[4] P. P. Pach, R. Palincza: *Sets Avoiding Six-Term Arithmetic Progressions in $\mathbb{Z}_6^n$ are Exponentially Small*, SIAM J. Discret. Math. **36**, (2020), 1135–1142.

[5] R. Palincza: *The computational complexity of recognizing some number theoretic properties*, Conference on Developments in Computer Science, (2021), 31–34.

Egyéb Publikáció

[6] P. Biró, T. Fleiner, R. Palincza: *Designing Chess Pairing Mechanisms*, Proceedings of the 10th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, (2017), 77–86.

Hivatkozások

[7] R. Angelo: *A Cameron and Erdős conjecture on counting primitive sets*, Integers **18** (2018), A25, 4pp.

[8] J. Balogh, H. Liu, S. Petříčková, M. Sharifzadeh: *The typical structure of maximal triangle-free graphs*, Forum of Mathematics, Sigma **3**, (2015), 19pp.

[9] J. Balogh, H. Liu, M. Sharifzadeh, A. Treglown: *The number of maximal sum-free subsets of integers*, Proc. Amer. Math. Soc. **143**, (2015), 4713–4721.

[10] J. Balogh, H. Liu, M. Sharifzadeh: *The number of subsets of integers with no k-term arithmetic progression*, Int. Math. Res. Not. **20**, (2017), 6168–6186.

[11] J. Balogh, H. Liu, M. Sharifzadeh, A. Treglown: *Sharp bound on the number of maximal sum-free subsets of integers*, J. Euro. Math. Soc. **20 (8)**, (2018), 1885–1911.

[12] J. Balogh, R. Morris, W. Samotij: *Independent sets in hypergraphs*, J. Amer. Math. Soc. **28**, (2015), 669–709.

[13] A. Bishnoi: `https://anuragbishnoi.wordpress.com/2017/11/02/on-a-famous-pigeonhole-problem`.

[14] J. Blasiak, T. Church, H. Cohn, J. Grochow, E. Naslund, W. Sawin, C. Umans: *On cap sets and the group-theoretic approach to matrix multiplication*, Discrete Anal. **Paper No. 3**, (2017), 27pp.

[15] P. J. Cameron, P. Erdős: *On the number of sets of integers with various properties*, Number Theory (Banff, AB, 1988), de Gruyter, Berlin, (1990), 61–79.

[16] T. H. Chan: *On sets of integers, none of which divides the product of k others*, European J. Comb. **32**, (2011), 443–447.

[17] T. H. Chan, E. Győri, A. Sárközy: *On a problem of Erdős on integers, none of which divides the product of k others*, European J. Comb. **31**, (2010), 260–269.

[18] E. Croot, V. F. Lev, P. P. Pach: *Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small*, Ann. of Math. (2) **185**, (2017), no. 1, 331–337.

[19] B. L. Davis, D. Maclagan: *The card game set*, The Mathematical Intelligencer **25**, (2003), 33–40.

[20] D. Dellamonica, Y. Kohayakawa, S. J. Lee, V. Rödl, W. Samotij: *On the number of B_h-sets*, Combinatorics, Probability and Computing **25**, (2016), 108–127.

[21] D. Dellamonica, Y. Kohayakawa, S. J. Lee, V. Rödl, W. Samotij: *On the number of B_h-sets*, Proceedings of the London Mathematical Society **116 (3)**, (2018), 629–669.

[22] Y. Edel: *Extensions of generalized product caps*, Des. Codes Cryptography **31**, (2004), 5–14.

[23] J. S. Ellenberg, D. Gijswijt: *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Ann. of Math. (2) **185**, (2017) no. 1, 339–343.

[24] C. Elsholtz, P. P. Pach: *Caps and progression-free sets in $\mathbb{Z}_m^n$*, Des. Codes Cryptography (2020) **88**, (2020), 2133–2170.

[25] P. Erdős: *On sequences of integers no one of which divides the product of two others and on some related problems*, Tomsk. Gos. Univ. Uchen. Zap **2**, (1938), 74–82.

[26] J. Fox, L. M. Lovász: *A tight bound for Green's arithmetic triangle removal lemma in vector spaces*, Advances **321**, (2017), 287–297.

[27] B. Green: *The Cameron-Erdős conjecture*, Bull. London Math. Soc. **36**, (2004), 769–778.

[28] Gurobi Optimization, LLC: Gurobi Optimizer Reference Manual, (2023) `https://www.gurobi.com`.

[29] R. Hancock, K. Staden, A. Treglown: *Independent sets in hypergraphs and Ramsey properties of graphs and the integers*, SIAM J. Discret. Math. **33**, (2019), 153–188.

[30] IBM ILOG CPLEX Optimization Studio v. 22.1.1 (2023) `https://www.ibm.com/products/ilog-cplex-optimization-studio`

[31] Z. Jiang: *Improved explicit upper bounds for the Cap Set Problem*, arXiv: 2103.06481.

[32] N. Karmarkar: *A new polynomial-time algorithm for linear programming*, Combinatorica **4**, (1984), 373–395.

[33] R. Karp: *Reducibility among combinatorial problems*, Complexity of Computer Computations, Plenum Press, (1972), 85–103.

[34] Y. Kohayakawa, S. J. Lee, V. Rödl, W. Samotij: *The number of Sidon sets and the maximum size of Sidon sets contained in a sparse random set of integers*, Random Structures & Algorithms **46**, (2015), 1–25.

[35] H. Liu, P. P. Pach: *The number of multiplicative Sidon sets of integers*, Journal of Combinatorial Theory, Series A **165**, (2019), 152–175.

[36] N. McNew: *Counting primitive subsets and other statistics of the divisor graph of $\{1, 2, \dots n\}$*, European J. Comb. **92**, (2021), 103237.

[37] The On-line Encyclopedia of Integer Sequences: `https://oeis.org/A174094`.

[38] The On-line Encyclopedia of Integer Sequences: `https://oeis.org/A051026`.

[39] P. P. Pach: Bounds on the size of Progression-Free Sets in $\mathbb{Z}_m^n$, Uniform Distribution Theory **17**, (2022), 1–10.

[40] P. P. Pach, Cs. Sándor: *Multiplicative bases and an Erdős problem*, Combinatorica **38 (5)**, (2018), 1175–1203.

[41] F. Petrov: *Combinatorial results implied by many zero divisors in a group ring*, arXiv: 1606.03256.

[42] F. Petrov, C. Pohoata: *Improved Bounds for Progression-Free Sets in* C_8^n, Israel J. Math. **236**, (2020), no. 1, 34—363.

[43] C. Pohoata, O. Roche-Newton: *Four-term progression free sets with three-term progressions in all large subsets*, Random Struct. Algorithms. **60**, (2022), 749–770.

[44] Python PuLP 2.7.0 `https://pypi.org/project/PuLP/`

[45] A. A. Sapozhenko: *The Cameron-Erdős conjecture*, (Russian) Dokl. Akad. Nauk. **393**, (2003), 749–752.

[46] D. Saxton, A. Thomason: *Hypergraph container*, Invent. Math. **201**, (2015), 925–992.

[47] A. Soifer: *The Four-Color Theorem*, The Mathematical Coloring Book. Springer, New York, NY., (2019), `https://doi.org/10.1007/978-0-387-74642-5_21`

[48] D. Speyer: `https://sbseminar.wordpress.com/2016/07/08/bounds-for-sum-free-sets-inprime-power-cyclic-groups-three-ways/`

[49] T. Tran: *On the structure of large sum-free sets of integers*, Israel J. Math. **228**, (2018), 249–292.

[50] F. Tyrrell: *New lower bounds for cap sets*, arXiv: 2209.10045.

[51] S. Vijay: *On large primitive subsets of* $\{1, 2, \ldots, 2n\}$, arXiv:1804.01740.

[52] B. L. van der Waerden: *Beweis einer Baudet'schen Vermutung*, Nieuw Arch. Wiskde. (2) **15**, (1928), 212–216.

[53] R. M. Wilson: *Non-isomorphic Steiner triple systems*, Math. Z. **135**, (1974), 303–313.