dc_650_12

ALGEBRAI GEOMETRIA ALKALMAZÁSA A KOMBINATORIKÁBAN ÉS A CSOPORTELMÉLETBEN

SZABÓ ENDRE

Doktori Értekezés Tézisei

Bevezető

A Disszertáció három fontos, egymással összefonódó témáról, és az alkalmazásaikról szól. Íme, a három téma (a tételek sorszáma erre a Tézis–füzetre vonatkozik):

1. *Incidencia becslések.*
   Itt az alap–probléma, hogy felső becslést adjunk az illeszkedések számára p pont és q geometriai alakzat között. A Disszertáció fő eredménye ebben a témában a 6. Tétel, ami általánosítja (többek között) a nevezetes Szemerédi–Trotter tételt.
2. *Hogyan találjunk csoportokat?*
   Itt azt vizsgáljuk, hogyan fordulhat elő, hogy háromszor n geometriai alakzat között közel Cn^2-szer fordul elő bizonyos három alakzatból álló geometriai konfiguráció. Tipikusan egy nagy szimmetria–csoport a felelős a túl sok speciális rész–konfigurációért. A Disszertáció fő eredményi ebben a témában a 14. és a 15. Tételeket. Ezek szorosan kötődnek (többek között) Hrushovski [36] Csoport konfigurációs tételéhez, és Terence Tao [56] cikkéhez.
3. *Növekedés csoportokban.*
   Legyen α véges részhalmaz egy csoportban! Azt vizsgáljuk, hogyan nő az α^n hatványok mérete az n függvényében. Különösen az olyan részhalmazok struktúrája érdekel minket, melyekre α^n csak lassan nő. A Disszertáció fő eredményei ebben a témában a 16., 17. és 18. Tételek. Ezek szorosan kapcsolódnak (sok más dolog mellett) a Freiman–Ruzsa tételhez, valamint Helfgott [33], Breuillard–Green–Tao [13] és Bourgain- Gamburd [4] eredményeihez.

Az első két téma kombinatorikus jellegű, a harmadik pedig csoportelméleti. Noha nem jelenik meg önálló fejezetként, mindhárom témában kulcsfontosságú szerepet kap az algebrai geometria.

A Disszertációban sok érdekes alkalmazása van a fenti eredményeknek.

Date: 2013. március 5..

1. *Alkalmazások a kombinatorikában.*
- A 19. Következmény jelentősen megjavítja az legjobb ismert kitevőt Hirzebruch [35] problémájában.
- A 20. Tétel megválaszolja Erdős, Lovász, Vesztergombi [24] kérdését.
- A 24. Következmény megoldja Székely László sejtését (lásd [18, Conjecture 3.41]). Továbbá, a 23. Tétel messzemenőkig általánosítja ezt a sejtést.
- A 26. Tétel egy fontos esetben megoldja az úgynevezett „Orchard problem" (lásd [37, 54]) egy változatát.

2. *Alkalmazások a csoportelméletben.*
- A 27. Következmény korlátos rangú egyszerű csoportokra bebizonyítja Babai [2] sejtését.
- A 29. Tétel korlátos rangú egyszerű csoportokra bebizonyítja Liebeck, Nikolov és Shalev [39] sejtését. A 30. Tétel egy variáció ugyanerre a témára.
- A 33. Tétel kimondja, hogy Weiss [61] sejtése igaz a BCP(r) csoportok osztályában.

A Disszertáció helye a matematikában. A következő néhány bekezdésben megpróbálom elhelyezni ezeket az eredményeket a tágabb matematikai környezetükben.

Első témánk különféle incidencia–számok becslése. Kiindulópontunk Szemerédi–Trotter [55] tétele: a síkban elhelyezett p pont és q egyenes között legfeljebb $\mathcal{O}\left(p^{2/3}q^{2/3} + p + q\right)$ illeszkedés fordulhat elő. Ennek számos általánosítása született, melyek felső becslést adnak p pont és q geometriai alakzat közötti illeszkedések számára. Íme egy kis ízelítő: Pach–Sharir [43] (lásd az 1. Tételt) munkájában az alakzatok síkgörbék, Chazelle–Edelsbrunner–Guibas–Sharir [14] és Solymosi–Tao [53] magasabb dimenziós hipersíkokkal foglalkoznak, Tóth [59] komplex egyenesekkel $\mathbb{C}^2$-ben, Bourgain–Katz–Tao [6] és Bourgain [3] pedig a p elemű test feletti projektív tér egyeneseire, illetve bizonyos hiperboláira vonatkozó becslést bizonyítanak, ahol p tetszőleges prím. A Disszertációban szereplő 6. Tétel egy magasabb dimenziós, tetszőleges valós- illetve komplex varietásokra érvényes általánosítás. Érdekes volna kiterjeszteni véges testekre is, de ez még teljesen nyitott kérdés. A 6. Tétel az egyik legfontosabb összekötő kapocs az első és a második témánk között: a csoportok konstrukciójában a 6. Tétel segítségével tudunk kizárni bizonyos fajta degenerációkat.

Második témánk egy nagyon általános matematikai jelenség: Ha egy geometriai szituációban sok váratlan egybeeséssel találkozunk, akkor arra számíthatunk, hogy a háttérben egy nagy szimmetria–csoport rejtőzik. Erre a témára végtelen sok variáció van, most csak két eredményt említek. Hrushovski Csoport konfigurációs tétele [36] (lásd még [44]-ot is) modell–elméleti

eszközökkel konstruál (nagyon nagy általánosságban) szimmetria csoportokat. Nagy vonalakban a következőről van szó. Tekintsünk egy $\mathcal{T}$ *stabil*[1] matematikai elmélet valamelyik modelljében két, „függvényszerű" kétváltozós relációkból[2] álló *d-dimenziós*[3] *családot*.[4] A két indexhalmaz direkt szorzata $2d$-dimenziós, így arra számítunk, hogy ha a két család relációit páronként *komponáljuk*,[5] eredményül egy $2d$-dimenziós családot kapunk. Ha a kompozíciók ehelyett csak egy d-dimenziós családot alkotnak,[6] akkor a reláció–családok egy csoportból származtathatók az alábbi értelemben: A $\mathcal{T}$ elméletben definiálható egy X halmaz, amin hat egy d-dimenziós G szimmetria–csoport, és mindhárom reláció család „lényegében úgy néz ki", mint az X halmazon az $R_g = \{(x, y) \mid y = gx\}$ (g végigfut G elemein) reláció–család. A Csoport konfigurációs tételnek az a speciális esete, amikor $\mathcal{T}$ az algebrailag zárt testek elmélete, 1.3.6. Lemmaként szerepel a Disszertációban, és fontos szerepet kap a 14. és 15. Tételek bizonyításában.

Míg Hrushovski eredménye inkább „folytonos jellegű", addig a 14. és 15. Tételek egy kombinatorikai szituációban jutnak hasonló következtetésre. E két tétel előzménye Elekes–Rónyai [20] dolgozata (ahol a szimmetria csoport még nem jelenik meg expliciten). Érdekes új fejlemény Tao [56] dolgozata: ő azt a jelenséget vizsgálja, hogy ha A, B „nagyon nagy" részhalmazok egy véges testben, és P egy kétváltozós polinom, akkor a $P(A, B)$ halmaz „tipikusan" betölti majdnem az egész testet. A kivételes polinomok, a 14. és 15. Tételünkhez hasonlóan, vagy az összeadásból, vagy a szorzásból (tehát vagy a test additív-, vagy pedig a multiplikatív csoportjából) származtathatók átparaméterezéssel. Tao meg is említi a blogjában (lásd [57]), hogy az „Elekes–Szabó theory" komoly szerepet kaphat a probléma további vizsgálatában.

Itt érdemes megjegyezni, hogy a 14. és 15. Tételekben szereplő véges pont–konfigurációk megjelennek a kapott csoportban is, és könnyen látható, hogy ott egy *nem–növő* részhalmazt alkotnak: tehát olyan α véges részhalmazt, melynek harmadik *hatványa*[7] legfeljebb $K|\alpha|$ méretű.

Ezzel eljutottunk a harmadik témánkhoz: csoportok nem–növő részhalmazainak vizsgálatához. A téma érdekes mind a kommutatív, mind pedig a nem–kommutatív csoportok világában, és mindkét változatnak sok–sok alkalmazása van a csoportelméleten kívül is (lásd később). Figyelemreméltó

---

[1] A stabilitás lényegében azt jelenti, hogy az elmélet modelljeiben nem fordul elő túl sokféle „típusú" elem.

[2] Ez azt jelenti, hogy majdnem minden x csak korlátos sok y-nal áll relációban.

[3] Modell–elméletben, alkalmas feltételek mellett, definiálható egy nagyon általános, az algebrából ismert Krull–dimenzióra hajazó *dimenzió* fogalom.

[4] Egy *család* tagjait egy indexhalmazzal paraméterezzük. A család dimenziója ennek az indexhalmaznak a dimenziója.

[5] Az R és S relációk *kompozíciója* az $\{(x, z) \mid \exists y : (x, y) \in R \text{ és } (y, z) \in S\}$ reláció.

[6] Tipikusan a kompozíciók mind különbözőek, $2d$-dimenziós családot alkotnak. Néha vannak egybeesések, és kisebb dimenziót kapunk. A mi esetünk a „maximális degeneráció".

[7] α^n jelöli az α elemeiből alkotott n-tényezős szorzatok halmazát.

a kommutatív és a nem–kommutatív világ összefonódása, egymásra hatása: noha látszólag teljesen különböző jelenségeket vizsgálnak, mégis sok–sok ötletet, módszert kölcsönöznek egymástól.

Kezdjünk a kommutatív csoportokkal. Az additív kombinatorika egyik meghatározó eredménye a Freiman–Ruzsa tétel [26] (lásd még Ruzsa [51] bizonyítását): Ha $\alpha \subseteq \mathbb{Z}$ egy véges számhalmaz amelyre $|\alpha + \alpha| \leq K|\alpha|$ teljesül,[8] akkor α lefedhető egy $d(K)$ dimenziós, $f(K)|\alpha|$ méretű általánosított számtani sorozattal. Később Green és Ruzsa [30] általánosították a tételt tetszőleges Abel csoportra: ilyenkor az α halmaz egy általánosított számtani sorozat és egy részcsoport összegével fedhető le. (Az ilyen halmazokat hívjuk *mellékosztály–sorozatnak*). A legfontosabb nyitott kérdés ebben az irányban, hogy létezik-e a nem–növő halmazoknak olyan leírása, melyben a paraméterek (mint $f(K)$ az előbb) a K polinomjai. Például, igaz-e, hogy minden $\alpha \subseteq \mathbb{Z}_2^n$ nem–növő halmaz lefedhető egy legfeljebb $|\alpha|$ méretű részcsoportnak legfeljebb CK^m mellékosztályával (ahol m egy mindentől független állandó)?

A kommutatív kitérő után térjünk vissza a nem–feltétlenül kommutatív csoportokhoz! Legyen α egy nem–növő részhalmaz egy csoportban! Mit mondhatunk az α szerkezetéről? Az első, és egyben legismertebb eredmény Gromov [32] tétele: $|\alpha^n|$ pontosan akkor becsülhető felülről az n egy polinomjával,[9] ha az α által generált részcsoport *virtuálisan nilpotens*.[10] (Itt a polinom függhet a csoporttól.)

Nem–növő halmazok vizsgálatában Helfgott [33] tétele hozta meg a következő áttörést: Legyen α generátor rendszer az $SL(2,p)$ csoportban[11] (p tetszőleges prím). Ekkor vagy α exponenciális ütemben nő, azaz $|\alpha^3| \geq |\alpha|^{1+\varepsilon}$ egy mindentől független ε konstanssal, vagy pedig $\alpha^3 = G$ (tehát nincs is hely további növekedésre).[12] Helfgott egyik fontos motivációja az volt, hogy a tételéből azonnal következik hogy az $SL(2,p)$ csoportokban igaz a Babai sejtés (lásd a 27. Következményt). Később kiderült, hogy Helfgott tétele jelentősen kiterjeszthető: a *Szorzattétel* szerint ugyanez az állítás tetszőleges q prímhatványra érvényes az $SL(n,q)$ csoportban is[13] (lásd a

[8] A Plünecke–Ruzsa becslésekből következik, hogy ilyenkor $|\alpha + \alpha + \alpha| \leq K^2|\alpha|$, tehát α nem–növő. Nem–kommutatív csoportokban ez az érvelés nem működik, ezért kellett α^3 méretét korlátozni. Érdekes, hogy α magasabb hatványainak mérete már nem–kommutatív csoportokban is becsülhető.

[9] Gromov tételében tehát az α halmaz összes hatványát korlátozzuk, nem csak α^3-öt.

[10] Egy csoport *virtuálisan nilpotens*, ha van véges indexű nilpotens részcsoportja.

[11] Egy p prímre $SL(n,p)$ jelöli az olyan 1-determinánsú $n \times n$ méretű mátrixok csoportját (a művelet a mátrixok szorzása), melyeknek elemeit a modulo p maradékosztályokból választjuk. Általánosabban, ha q egy prím hatványa, illetve $\mathbb{F}$ egy tetszőleges test, akkor $SL(n,q)$, illetve $SL(n,\mathbb{F})$ jelöli az olyan 1-determinánsú $n \times n$ méretű mátrixok csoportját, melyeknek elemeit a q elemű végest testből, illetve $\mathbb{F}$-ből választjuk.

[12] Helfgott cikkében még $\alpha^3 = G$ helyett $\alpha^k = G$ szerepel egy alkalmas k kitevővel.

[13] Valójában a Szorzattétel az $SL(n,q)$ minden egyszerű részcsoportjára vonatkozik, tehát az alternáló csoportok kivételével az összes véges egyszerű csoportra. Az ε konstans csak n-től (azaz a csoport rangjától) függ.

16. Tételt). A tétel fontosságát jól mutatja, hogy egymástól függetlenül egyszerre két csapat is bebizonyította: Breuillard–Green–Tao [11] illetve Pyber–Szabó [50].

Az utóbbi néhány évben sok előrelépés történt a nem–növő halmazok struktúrájának minél teljesebb leírására. Ezek közül most csak két cikket szeretnék kiemelni. Breuillard–Green–Tao [13] tetszőleges csoport nem–növő részhalmazaival foglalkoznak. Tételük közös általánosítása Gromov tételének és a Freiman–Ruzsa tételnek: Ha α nem–növő részhalmaz egy csoportban (tehát $\left|\alpha^3\right| \leq K|\alpha|$), akkor található olyan H részcsoport, amelyik teljes egészében benne van az $\alpha^{d(K)}$ hatványban, és a hozzá tartozó faktorcsoportban[14] α képe lefedhető egy alkalmas *nil–sorozat*[15] korlátos sok (mondjuk $f(K)$) eltoltjával. A leírásuk talán egyetlen szépséghibája, hogy a módszerük nem ad becslést $d(K)$ és $f(K)$ nagyságrendjére. A kombinatorikai, illetve számelméleti alkalmazásokhoz viszont fontos lenne, hogy $d(K)$ és $f(K)$ polinomok legyenek, legalább egy szűkebb csoport–osztályban.[16] Ezt a célt (a polinom korlátokat) tűztük ki Pyber Lászlóval a [48] cikkben. Beláttuk (lásd a 18. Tételt), hogy ha α egy *szimmetrikus*[17] nem–növő részhalmaz az $SL(n, \mathbb{F})$ csoportban ($\mathbb{F}$ tetszőleges test), akkor található olyan H részcsoport, amelyik teljes egészében benne van az α^6 hatványban, és a hozzá tartozó faktorcsoportban[14] α képe lefedhető egy feloldható részcsoport $f(K)$ darab eltoltjával, ahol $f(K)$ egy (n-től függő) polinom.

A Szorzattétel eddigi leglátványosabb alkalmazása az úgynevezett „Bourgain–Gamburd expansion machine". A módszert Bourgain és Gamburd fejlesztették ki *expander gráfok*[18] konstrukciójához. (Az expander gráfoknak pedig fontos alkalmazásaik vannak például a számítás–tudományban). A [4] cikkben Bourgain és Gamburd belátta, hogy az $SL(2, p)$ csoport minden olyan *Cayley gráfja*,[19] amelyik nem tartalmaz kis köröket, expander egy közös ε expanziós konstanssal. Amikor [4] készült, még csak Helfgott tétele létezett, ezért kellett az $SL(2, p)$ csoportra szorítkozni. Később ugyanezzel a módszerrel, használva az újabb Szorzattétel teljes erejét, sok–sok új expander családot konstruáltak (lásd például Breuillard–Green–Tao [12] és [9], Varjú [60], Bourgain–Varjú [8]), valamint Golsefidy–Varjú [29] cikkét!) Az expander gráfoknak érdekes számelméleti alkalmazása van az „affin szita"

---

[14] Pontosabban: H normalizátorának H szerinti faktorcsoportjában.

[15] A *nil–sorozatok* az általánosított számtani sorozatok megfelelői nilpotens csoportban. Sokszor elég annyit tudni, hogy α képe a faktorcsoportban lefedhető egy nilpotens részcsoport kevés eltoltjával.

[16] A Szorzattétel is átfogalmazható ilyen formába, és az átfogalmazásban a konstansok polinomiálisan függenek K-tól. Sok (már létező) alkalmazás ezen múlik.

[17] Egy csoport α részhalmaza *szimmetrikus*, ha minden elemével együtt annak inverzét is tartalmazza, azaz $\alpha^{-1} = \alpha$.

[18] Egy n-csúcsú gráf ε-*expander*, ha bármely legfeljebb $\frac{n}{2}$ csúcsból álló X részhalmaza legalább $\varepsilon|X|$ további, X-en kívüli csúccsal szomszédos.

[19] Egy G csoport α generátor–rendszeréhez tartozó *Cayley gráf* csúcsai a G elemei, és két csúcsot, mondjuk x-et és y-t, akkor kötünk össze éllel, ha $xy^{-1} \in \alpha$.

módszerekben (lásd például a Bourgain–Gamburd–Sarnak [5] cikket), tulajdonképpen a szita–módszerek adták az eredeti motivációt a [4] cikkhez.

Az additív kombinatorika fontos fejezetét alkotják az *Összeg–szorzat tétel*[20] (Erdős–Szemerédi [25]), és ennek különféle változatai (lásd például Tao [58] cikkét, és az ottani hivatkozásokat). Összeg–szorzat típusú tételek ugyan nem bukkannak fel a Disszertációban, mégis, több témánkkal is szoros kapcsolatban állnak. Elekes [17] megmutatta, hogy az Összeg–szorzat tétel következik a Szemerédi–Trotter tételből (lásd még Solymosi [52] cikkét). Fordítva, Bourgain–Katz–Tao [7] egy Összeg–szorzat típusú tételből bizonyítanak be egy Szemerédi–Trotter típusú tételt. Helfgott [33] tételét (az $SL(2,p)$ csoportról) eredetileg egy Összeg–szorzat típusú tétel segítségével bizonyította, és még ma is sokan úgy tekintenek a Szorzattételre, mint egyfajta nem–kommutatív Összeg–szorzat tétel. Az általános Szorzattétel bizonyítása már más úton halad, de a nem növő halmazok vizsgálatában továbbra is fontos szerepük van az Összeg–szorzat tételeknek (lásd például Gill–Helfgott [27] cikkét). Ez a kapcsolat fordítva is működik: (kommutatív) Összeg–szorzat típusú tételek bizonyíthatók a (nem–kommutatív) Szorzattétel segítségével (lásd például: Breuillard–Green–Tao [11, 8. fejezet]).

Érdemes megemlíteni még Bourgain [3] friss eredményét, ami szoros kapcsolatban áll a témáinkkal. A korábban emlegetett „expansion–machine" módszereit használva egy véges geometriai, hiperbolákra vonatkozó Szemerédi–Trotter típusú tételt bizonyít.

A Disszertáció felépítése. A Disszertáció hét dolgozatra épül, melyek rendre megfelelnek a Disszertáció egy-egy fejezetének.

- [23] és [22] közös dolgozatok Elekes Györggyel, megfelelnek a Disszertáció 1. illetve 5. fejezetének.
- [21] közös dolgozat Elekes Györggyel és Simonovits Miklóssal, megfelel a Disszertáció 4. fejezetének.
- [50] és [48] közös dolgozatok Pyber Lászlóval, megfelelnek a Disszertáció 2. és 3. fejezetének.
- [45] közös dolgozat Cheryl Praeger–rel, Pyber Lászlóval és Pablo Spiga–val, megfelel a Disszertáció 6. fejezetének.
- [28] közös dolgozat Nick Gill–el, Pyber Lászlóval és Ian Short–tal, megfelel a Disszertáció 7. fejezetének.

A Disszertáció eredményeit a Tézisekben témájuk alapján öt csoportba soroltam:

1. *Incidencia becslések.*
A Disszertáció 1.2. szakasza tartozik ide, ami a [23] dolgozat része. Ebben a témában a dolgozat fő eredménye a 6. Tétel.

2. *Hogyan találjunk csoportokat?*
A Disszertáció 1.1 és 1.4. szakaszai tartoznak ide. Fő eredmények: a 14. és a 15. Tételek.

[20] Ha A egy véges valós számhalmaz, akkor $\max\left(|A+A|, |A\cdot A|\right) \geq c|A|^{1+\varepsilon}$.

3. *Növekedés csoportokban.*
A Disszertáció 2. és 3. fejezete. Fő eredmények: a 16. és a 18. Tételek.

4. *Alkalmazások a kombinatorikában.*
A Disszertáció 5. és 4. fejezetei, és az 1.5. szakasza. Legfontosabb eredmények: a 20., a 23. és a 26. Tételek, valamint a 24. Következmény.

5. *Alkalmazások a csoportelméletben.*
A Disszertáció 7. és 6. fejezete. Legfontosabb eredmények: a 29., a 30. és a 33. Tételek.

1. Incidencia becslések

Illeszkedési–számokra adott korlátok központi szerepet töltenek be a kombinatorikus geometria sok területén, és a geometriai algoritmusok elméletében. (A közelmúltban szerepet kaptak az additív kombinatorikában is, lásd [17, 19, 18].) Az első ilyen típusú eredmény Szemerédi–Trotter [55] tétele, amit később Pach és Sharir kiterjesztettek folytonos síkgörbékre:

1. Tétel (Pach–Sharir [43])**.** *Legyen Γ egyszerű (azaz önmagukat nem metsző) síkgörbék egy olyan családja, melyben bármely két görbének legfeljebb M közös pontja van, és minden ponton keresztül legfeljebb s Γ-beli görbe halad át (azaz Γ-nak s szabadsági foka van). Ekkor p pont és q Γ-beli görbe közti illeszkedések száma legfeljebb:*

$$C\left(p^{s/(2s-1)}q^{(2s-2)/(2s-1)} + p + q\right), \tag{1}$$

ahol a C konstans szorzó csak s-től és M-től függ. Speciális esetben, ha Γ a síkbeli egyenesek családja, akkor $s = 2$, $M = 1$, és visszakapjuk az eredeti Szemerédi–Trotter korlátot.

Szükségünk lesz az alábbi jelölésekre:

2. Definíció. Legyen X egy tetszőleges alaphalmaz (ez lehet például $\mathbb{R}^N$, az N-dimenziós tér), P egy részhalmaz, Q pedig az X részhalmazainak egy rendszere. (Úgy gondolunk Q elemeire, mintha X-beli „geometriai alakzatok" lennének.)

- $I(P, Q)$ jelöli a (P, Q) rendszer *illeszkedéseinek számát*, azaz az olyan $P \times Q$-beli (p, q) párok számát, melyekre a p pont benne van a q alakzatban.
- Tetszőleges $t \in P$ pont esetén $Q_t \subseteq Q$ jelöli az olyan Q-beli alakzatok halmazát, amelyek tartalmazzák a t pontot.

Tekintsük most azt a konfigurációt $\mathbb{R}^3$-ban, amelyik p egy egyenesre eső pontból, és q ezt az egyenest tartalmazó síkból áll. Ebben a konfigurációban az illeszkedések száma pq. Világos, hogy ha egy térbeli alakzatokra vonatkozó, (1)-hez hasonló becslést keresünk, akkor szükségünk lesz valamiféle nem–degeneráltsági feltételre, ami kizárja az ilyen jellegű konfigurációkat. Az alábbi definíció ezt finomítja: megenged ilyen rész–konfigurációkat, de persze nem túl nagyokat. A b paraméter és a k kombinatorikus dimenzió szabályozza, hogy mennyit. Később a becslésekben a konstans szorzók

függhetnek k-tól és b-től is, kitevők azonban csak k-tól függenek majd. (Egy önmagában is érdekes feladat volt találni olyan nem–degeneráltsági feltételt, amelyik eléggé „megengedő" ahhoz, hogy sok érdekes geometriai szituációkban teljesüljön.)

3. Definíció (Kombinatorikus dimenzió rekurzív definíciója)**.** Rögzítünk egy $b > 0$ konstanst. Legyen X egy tetszőleges alaphalmaz, P egy részhalmaz, Q pedig az X részhalmazainak egy rendszere. Azt mondjuk, hogy $\operatorname{cdim}_b(P, Q) = 0$, ha $|Q| \leq b$. Általában, $\operatorname{cdim}_b(P, Q) \leq k$ (ahol $k \geq 1$ egész), ha van olyan $P' \subseteq P$ részhalmaz, amelyre

- $|P \setminus P'| \leq b$, azaz P' „majdnem az egész" P, és
- minden $t \in P'$-re $\operatorname{cdim}_b\big(P \setminus \{t\}, Q_t\big) \leq k - 1$.

4. *Megjegyzés.* Könnyen ellenőrizhetjük, hogy az 1. Tételben szereplő (p pont, q görbe) konfiguráció kombinatorikus dimenziója, alkalmas b választása mellett, legfeljebb 2.

Az, hogy közvetlenül a 3. Definícióból határozzuk meg a kombinatorikus dimenziót, elég reménytelen feladatnak tűnik. A következő lemma mutatja, hogy geometriai szituációkban, elég nagy általánosságban, a kombinatorikus dimenzió megegyezik a geometriai dimenzióval.

5. Lemma. *Legyen A egy k-dimenziós varietás, jelölje $\mathcal{H}$ a legfeljebb d fokú A-beli részvarietások halmazát. Választhatunk olyan csak k-tól és d-től függő b értéket, mellyel igaz a következő állítás: Ha $P \subseteq A$ egy* általános helyzetű[21] *véges részhalmaz, akkor* $\operatorname{cdim}_b(P, \mathcal{H}) \leq k$.

Az alábbi tétel lényegében a Disszertáció 1.2.5. Tételének és a Disszertáció 1.2.6. Tételének az összevonása.

6. Tétel. *Legyen $\mathcal{P}$ egy véges ponthalmaz az N-dimenziós komplex projektív térben, $\mathcal{V}$ pedig algebrai varietások véges kollekciója (ugyanebben a projektív térben). Tegyük fel, hogy a $(\mathcal{P}, \mathcal{V})$ konfiguráció kombinatorikus dimenziója $k = \operatorname{cdim}_b(\mathcal{P}, \mathcal{V}) \geq 2$, és $\mathcal{V}$ minden tagja legfeljebb d fokú. Ekkor léteznek olyan, csak k-tól N-től és d-től függő α, β pozitív konstansok, melyekre*

$$k\alpha + \beta = k$$

és a $(\mathcal{P}, \mathcal{V})$ rendszer illeszkedéseinek száma

$$I(\mathcal{P}, \mathcal{V}) \leq C\Big(|\mathcal{P}|^{\alpha}|\mathcal{V}|^{\beta} + |\mathcal{P}| + |\mathcal{V}| \log(2|\mathcal{P}|)\Big),$$

ahol a C konstans az N, b, k, d paraméterektől függ. Abban a speciális esetben, amikor a kollekció hipersíkokból áll (azaz $d = 1$), választhatjuk az

$$\alpha = \frac{N(k-1)}{Nk-1} - \varepsilon\,, \qquad \beta = \frac{k(N-1)}{Nk-1} + k\varepsilon$$

kitevőket, ahol $0 < \varepsilon < \frac{k-1}{k(Nk-1)}$ tetszőleges.

[21] Itt most *P általános helyzetű*, ha minden legfeljebb d^k fokú részvarietás legfeljebb b pontot tartalmaz P-ből.

7. *Megjegyzés.* A 6. Tételt azért fogalmaztuk meg projektív térben, hogy beszélhessünk az algebrai halmazok fokszámáról. Természetesen analóg tétel érvényes $\mathbb{C}^N$-beli algebrai halmazokra is, de mivel itt nincs standard fokszám–fogalom, azért körülményesebb megfogalmazni, hogy mitől függ a C konstans szorzó.

Érdemes összehasonlítani Pach-Sharir tételét a 6. Tétellel. A disszertációbeli tétel általánosítja a korábbit, amennyiben síkgörbék helyett magasabb dimenziós alakzatokat vizsgál, és komplex geometriában is érvényes. Az általánosságnak azonban ára van: Pach-Sharir tétele megenged tetszőleges folytonos síkgörbéket, és a becslés kitevői pontosak, míg a 6. Tétel csak algebrai varietásokra vonatkozik, a kitevők messze nem optimálisak, és a hibatagban megjelenik egy bosszantó $\log(2|\mathcal{P}|)$ faktor. (A Disszertációban explicit α és β kitevők szerepelnek.)

2. Hogyan találjunk csoportokat?

Ez a rész a Disszertáció 1.1 és 1.4. szakaszairól szól. A hátterében egy nagyon általános elv húzódik: Ha egy geometriai szituációban sok váratlan egybeeséssel találkozunk, akkor arra számíthatunk, hogy egy nagy szimmetria–csoportra bukkanunk. Egyik legismertebb eredmény ebben az irányban Hrushovski [36] Csoport konfigurációs tétele (lásd még: [44]).

Mi most egy geometriai–kombinatorikai szituációval foglalkozunk. Alább definiáljuk, hogy mikor mondunk egy $V \subseteq \mathbb{C}^3$ algebrai felületet *gazdagnak* (azaz mikor van rajta túl sok egybeesés). Néhány egyszerű példa bemutatása után kiderül majd, hogy a gazdag felületeknek nagyon speciális szerkezetük van. Vagy a V felület egy síkgörbére állított henger (lásd a 13. Példát), vagy egy algebrai csoportot találunk a háttérben: V lényegében a csoport szorzás–függvényének a grafikonjából származik (mint a 12. Példában). Abban a speciális esetben, amikor a felület egyenlete $z = f(x, y)$ alakban írható, Elekes György és Rónyai Lajos látták be ezt az állítást a [20] cikkben. A tetszőleges felületekre való kiterjesztést, és a magasabb dimenziós általánosítást pedig (lásd a 14. és a 15. Tételeket) a [23] cikkben bizonyítottuk Elekes Györggyel.

8. Definíció (Gazdagság)**.**

(a) Egy $V \subset \mathbb{C}^3$ algebrai felületre azt mondjuk, hogy *gazdag*, ha végtelen sok n értékre találhatók olyan $X, Y, Z \subset \mathbb{C}$ n-elemű komplex számhalmazok, melyekre

$$\big|V \cap (X \times Y \times Z)\big| \geq \mathcal{C}n^2$$

valamilyen n-től független $\mathcal{C} > 0$ konstanssal.

(b) Legyenek A, B, C m-dimenziós komplex varietások ($m \geq 1$). Egy $V \subset A \times B \times C$ $2m$-dimenziós részvarietás *gazdag*, ha végtelen sok n értékre találhatók olyan $X \subset A$, $Y \subset B$ és $Z \subset C$ „általános helyzetű” (lásd a Disszertáció 1.2.12. Definícióját) n-elemű részhalmazok, melyek

kielégítik ugyanazt a becslést:

$$\big|V \cap (X \times Y \times Z)\big| \geq \mathcal{C}n^2$$

valamilyen n-től független $\mathcal{C} > 0$ konstanssal.

Az *algebrai csoportok* olyan csoportok, melyek alaphalmaza egy varietás, és a csoportművelet egy polinomokkal megadható függvény. Az algebrai csoportokat régóta intenzíven vizsgálják, szerkezetükről nagyon sokat lehet tudni. Lássunk néhány példát:

9. *Példa.* Minden komplex egydimenziós összefüggő algebrai csoport az alábbi három típus valamelyikébe tartozik. Az első két típusba csak egy–egy csoportot sorolunk, a harmadik típusba viszont végtelen sok egymástól különböző csoport tartozik (melyek topologikus csoportként mind izomorfak egymással).

(a) $\mathbb{C}$ — a komplex számok additív csoportja.
(b) $\mathbb{C}^*$ — a nem–nulla komplex számok multiplikatív csoportja. A $z \to e^{2\pi iz}$ leképezés mutatja, hogy $\mathbb{C}^*$ izomorf a $\mathbb{C}/\mathbb{Z}$ faktorcsoporttal.
(c) Elliptikus görbék — ezek az $y^2 = x^3 + ax + b$ egyenletű síkgörbék (kiterjesztve egy végtelen távoli ponttal), ahol $4a^3 + 27b^2 \neq 0$. Az elliptikus görbék felírhatók $\mathbb{C}/\mathbb{L}$ faktorcsoportként is, ahol $\mathbb{C}$ az (a)-beli csoport, $\mathbb{L}$ pedig egy (az origót tartalmazó) parallelogramma rács. (Egymással nem–egybevágó rácsok különböző faktor–csoportokat adnak.)

10. *Példa.* Tekintsük a „négyzetgyök függvényt”! Valójában ez nem is igazi függvény: minden $x_0 \neq 0$ komplex szám körül két „folytonos ága” van. Tovább komplikálja a helyzetet, hogy ha egyszerre tekintjük az összes nem–nulla szám négyzetgyökeit, akkor az ágak „összekeverednek”: ha x folytonosan körbejárja (a komplex síkon) az origót, akkor a két négyzetgyöke is folytonosan változik, de a kör végére éppen felcserélve érkeznek vissza az eredeti pozíciójukba. A négyzetgyökhöz hasonlóan viselkedő „függvényeket” *többértékű algebrai függvényeknek* nevezzük.

11. Definíció. Legyenek A és B halmazok. Egy olyan F függvényt, amelyik A minden eleméhez B egy részhalmazát rendeli, *A-ból B-be vezető többértékű függvénynek* nevezünk.

(a) Az F *grafikonja* az alábbi részhalmaz:

$$\Gamma_F = \Big\{(a,c) \;\Big|\; a \in A,\, c \in F(a)\Big\} \subseteq A \times B\,.$$

(b) Minden $H \subseteq A$ részhalmazra és minden $b \in B$ pontra legyen

$$F(H) = \cup_{h\in H} F(h) \subseteq B\,, \qquad F^{-1}(b) = \big\{a \in A \;\big|\; F(a) \ni b\big\}\,.$$

Világos, hogy F^{-1} egy többértékű függvény B-ből A-ba. Amennyiben $\max_{a\in A}\big|F(a)\big|$ és $\max_{b\in B}\big|F^{-1}(b)\big|$ végesek, akkor legyen $\deg(F)$ a kettő közül a nagyobbik, különben pedig $\deg(F) = \infty$.
(c) Legyenek A és B algebrai görbék. Azt mondjuk, hogy F *algebrai*, ha $\deg(F) < \infty$, és a Γ_F grafikon egy algebrai görbe az $A \times B$ felületen.

(d) Legyenek most A és B m-dimenziós varietások. Azt mondjuk, hogy F *algebrai*, ha $\deg(F) < \infty$, és a Γ_F grafikon lezártja egy m-dimenziós részvarietás a $2m$-dimenziós $A \times B$-ben.

12. *Példa.* Legyen $\mathcal{G}$ egy komplex algebrai csoport. Először az egydimenziós esettel foglalkozunk, a csoportművelet segítségével készítünk gazdag algebrai felületeket $\mathbb{C}^3$-ben. Utána általánosítjuk a konstrukciót magasabb dimenziós csoportokra.

(a) Most még $\mathcal{G}$ tetszőleges. Legyen $n = 2k + 1$ egy páratlan természetes szám. Tekintsük a

$$\mathcal{G}_{sp} := \left\{ (x, y, z) \in \mathcal{G}^3 \;\middle|\; \text{a } \mathcal{G} \text{ csoportban } xyz = 1 \right\},$$

(algebrai) varietást, amit „a $\mathcal{G}^3$-beli speciális részvarietásnak", illetve egydimenziós $\mathcal{G}$ esetén „a $\mathcal{G}^3$ speciális felületének" nevezünk. Válasszunk egy $a \in \mathcal{G}$ végtelen rendű elemet (ilyen mindig van, amennyiben $\dim(\mathcal{G}) \geq 1$), és legyen

$$X = Y = Z := \{a^{-k}, a^{-(k-1)}, \ldots, a^{-1}, 1, a, \ldots, a^{(k-1)}, a^k\} .$$

Könnyű ellenőrizni, hogy $\mathcal{G}_{sp}$ valóban legalább $\lceil k^2/2 \rceil \geq \frac{1}{4}n^2$ pontot tartalmaz $X \times Y \times Z$-ből, tehát gazdag.

(b) Tegyük most fel, hogy $\mathcal{G}$ egydimenziós, és legyenek f, g, h többértékű algebrai függvények $\mathcal{G}$-ből $\mathbb{C}$-be. A direkt szorzatuk, $F = f \times g \times h$, ugyancsak többértékű függvény $\mathcal{G}^3$-ből $\mathbb{C}^3$-be, és $\deg(F) = \deg(f)\deg(g)\deg(h)$. Tekintsük a $\mathcal{G}_{sp}$ speciális felület képét, az $F(\mathcal{G}_{sp}) \subset \mathbb{C}^3$ részhalmazt, ennek lezártja egy $V \subseteq \mathbb{C}^3$ algebrai felület. Világos, hogy a V felület legalább $\lceil \frac{k^2}{2\deg(F)} \rceil = \mathcal{C}n^2$ pontot tartalmaz az $F(X \times Y \times Z) = f(X) \times g(Y) \times h(Z)$ Descartes–szorzatból, tehát gazdag.

(c) A V varietásnak legfeljebb $\deg(V)$ irreducibilis komponense van, tehát van olyan irreducibilis komponens, amelyik gazdag.

(d) Tekintsük most az általános esetet: $\dim(\mathcal{G}) = m \geq 1$ tetszőleges. Legyenek f, g, h többértékű algebrai függvények $\mathcal{G}$-ből három m-dimenziós komplex varietásba: A-ba, B-be illetve C-be. Az előző érvelés szó szerint átvihető erre a szituációra. $F = f \times g \times h$ egy többértékű algebrai függvény $\mathcal{G}^3$-ből $A \times B \times C$-be (mind $\mathcal{G}^3$, mind pedig a szorzat varietás $3m$-dimenziós). Az $F(\mathcal{G}_{sp})$ részhalmaz lezártja egy $2m$-dimenziós V részvarietás $A \times B \times C$-ben, és bizonyos esetekben (például, ha $\mathcal{G}$ Abel csoport) lesznek olyan $V_0 \subseteq V$ irreducibilis komponensek, amelyek gazdagok. Kiderül majd, hogy ők lesznek a gazdag részvarietások „mintapéldányai".

13. *Példa* (Hengerek).

(a) Egy $V_0 \subset \mathbb{C}^3$ algebrai felületet *hengernek* mondunk, ha az egyenlete csak két változótól függ: $F(x, y) = 0$, $F(x, z) = 0$ vagy $F(y, z) = 0$. Tekintsük például az $F(x, y) = 0$ esetet, és válasszunk olyan $X =$

$\{x_1, x_2, \dots, x_n\}$, $Y = \{y_1, y_2, \dots, y_n\}$ komplex számhalmazokat, amelyekre $F(x_i, y_i) = 0$ minden i-re. Világos, hogy tetszőleges n elemű $Z \subset \mathbb{C}$ számhalmazra $\big|V_0 \cap (X \times Y \times Z)\big| \geq n^2$, tehát V gazdag.

(b) Legyenek A, B, C m-dimenziós varietások. Azt mondjuk, hogy egy $V \subset A \times B \times C$ $2m$-dimenziós részvarietás *tartalmaz hengert*, ha vagy a $V \to A \times B$, vagy a $V \to B \times C$, vagy pedig a $V \to A \times C$ vetítések képe nem $2m$-dimenziós (tehát kisebb). Könnyen látható, hogy egy ilyen V tényleg tartalmaz egy hengert.

Az alábbi tétel lényegében a Disszertáció 1.1.3. Tételének leegyszerűsített változata.

14. Tétel (Gazdag felületek $\mathbb{C}^3$-ben)**.** *Legyen $V \subset \mathbb{C}^3$ egy d fokú algebrai felület. Vannak olyan η és n_0 csak d-től függő konstansok, melyekkel a következő tulajdonságok ekvivalensek.*

(a) Legalább egy $n \geq n_0$ értékre vannak olyan $X, Y, Z \subset \mathbb{C}$ n-elemű számhalmazok, melyekre

$$\big|V \cap (X \times Y \times Z)\big| \geq n^{2-\eta}\,.$$

(b) V-nek van olyan V_0 irreducibilis komponense, amelyik vagy egy henger (lásd a 13. Példát), vagy pedig a 12. Példában leírt konstrukcióból származik (valamilyen egydimenziós komplex algebrai csoportból). Utóbbi esetben a konstrukcióban használt többértékű függvények fokszáma d függvényében korlátozható.

(c) Jelölje $\mathbb{D} \subset \mathbb{C}$ az egységkörlemezt. Vagy V tartalmaz egy hengert (lásd a 13. Példát), vagy pedig vannak $f, g, h : \mathbb{D} \to \mathbb{C}$ egy-egy–értelmű analitikus függvények, amelyeknek az inverze is analitikus, és amelyekre

$$V \supseteq \Big\{ \big(f(x), g(y), h(z)\big) \in \mathbb{C}^3 \;\Big|\; x, y, z \in \mathbb{D},\ x + y + z = 0 \Big\}\,.$$

(d) V-nek van olyan V_0 irreducibilis komponense, amelynek minden nyílt részhalmaza gazdag.

Szerepel a tételben egy (kicsi) pozitív η konstans. Nem adunk meg explicit értéket, mert azt gondoljuk, hogy a jelenlegi becsléseink messze nem optimálisak. Valójában még az sem kizárt, hogy a tétel tetszőleges $0 < \eta < 1$ értékkel igaz — lásd a Disszertáció 1.1.4. Problémáját.

Az alábbi tétel a Disszertáció 1.4.2. Tételének leegyszerűsített változata.

15. Tétel (Gazdag részvarietások magasabb dimenzióban)**.** *Tetszőleges m pozitív egészhez található pozitív valós η a következő tulajdonsággal. Legyenek A, B, C m-dimenziós projektív varietások, $V \subset A \times B \times C$ pedig olyan $2m$-dimenziós részvarietás, amelyik nem tartalmaz hengert (lásd a 13. Példát). A következő tulajdonságok ekvivalensek:*

(a) Egy „elég nagy” n értékre vannak olyan $X \subset A$, $Y \subset B$, $Z \subset C$ n-elemű „általános helyzetű” részhalmazok, melyekre

$$\big|V \cap (X \times Y \times Z)\big| \geq n^{2-\eta}\,.$$

(b) V-nek van egy olyan V_0 irreducibilis komponense, amelyik a 12. Példában leírt konstrukcióból származik (valamilyen m-dimenziós komplex algebrai csoportból).

(c) V-nek van olyan V_0 irreducibilis komponense, amelynek minden nyílt részhalmaza gazdag.

Az (a) pontban szereplő „elég nagy" és „általános helyzetű" fogalmak pontos definícióját lásd a Disszertáció 1.4.2. Tételében illetve a Disszertáció 1.2.12. Definíciójában.

3. Növekedés csoportokban

Adott $n \times n$ méretű mátrixok egy véges halmaza, α. Azt vizsgáljuk, hogy mely α halmazokra lesz $\left|\alpha^3\right|$ sokkal nagyobb, mint $|\alpha|$, és mikor lesz nagyjából ugyanakkora.

Mi történik az algebrai csoportokban? A Disszertáció 2. fejezetében az algebrai csoportok szerkezetét vizsgáljuk. Algebrai geometriai, és csoportelméleti módszerek segítségével sikerült két, a nem–növő halmazokra vonatkozó tételt bizonyítani. A további fejezetekben ez a két tétel alapvető fontosságúvá válik a növekedés vizsgálatában.

A Disszertáció 2.1.4. Tétele a véges egyszerű csoportokra vonatkozó Szorzattétel. Fontosságát mutatja, hogy ez egy sok–sok szerzős eredmény: Breuillard–Green–Tao [10], és Pyber–Szabó [49].

16. Tétel (Szorzat-tétel)**.** *Legyen G egy egyszerű részcsoport az $SL(n,q)$ csoportban (q egy prímhatvány),*[22] *α egy generátor–rendszer G-ben. Ekkor vagy $\alpha^3 = G$, vagy pedig*

$$\left|\alpha^3\right| \geq |\alpha|^{1+\varepsilon}$$

ahol ε csak az n-től függő pozitív konstans.

Tetszőleges (nem feltétlenül véges) lineáris csoportokról szól a Disszertáció 2.13.4. Következménye. Íme egy egyszerűsített változat:

17. Tétel. *Legyen $\mathbb{F}$ tetszőleges test, $K \geq 1$ egy konstans, és α egy olyan véges részhalmaz az $SL(n,\mathbb{F})$ csoportban, amelyre*

$$\left|\alpha^3\right| \leq K|\alpha| \,.$$

Ekkor létezik olyan $m = m(n)$ konstans, és olyan Δ virtuálisan feloldható[23] *részcsoport, melyekre α lefedhető legfeljebb K^m darab Δ-mellékosztállyal.*

---

[22] Minden véges egyszerű csoport beágyazható valamelyik $SL(n,q)$ csoportba, ahol n nagyjából a csoport rangja.

[23] Egy csoport *virtuálisan feloldható*, ha van véges indexű feloldható részcsoportja.

Mit ad nekünk a Csoportelmélet? A Disszertáció 3. fejezetében a 17. Tételt csoportelméleti módszerekkel és a 16. Tétellel kombináljuk. Így jóval pontosabb képet kapunk a nem–növő mátrix–halmazok struktúrájáról. Íme, a Disszertáció 3.6.13. Tétele, ami speciális esetként magába foglalja a Szorzattételt is:

18. Tétel. *Legyen $\mathbb{F}$ tetszőleges test, $K \geq 1$ egy konstans, és α egy olyan véges részhalmaz $SL(n,\mathbb{F})$-ben, amely minden elemével együtt tartalmazza annak inverzét is (azaz $\alpha = \alpha^{-1}$), és amelyre*

$$\left|\alpha^3\right| \leq K|\alpha| \,.$$

Ekkor az α által generált részcsoportnak vannak olyan $P \leq \Gamma$ normálosztói, melyekre α^3 tartalmazza P egy mellékosztályát, Γ/P feloldható, és α lefedhető legfeljebb $K^{c(n)}$ Γ-mellékosztállyal, ahol $c(n)$ csak az n-től függ.

4. Alkalmazások a kombinatorikában

Adott a (valós vagy komplex) síkon n nem–degenerált kúpszelet, semelyik három nem érinti egymást ugyanabban a pontban. Hirzebruch [35] kérdezte, hogy van-e $Cn^{2-\varepsilon}$ alakú felső becslés az érintési pontok számára. A kérdést Megyesi Gáborral oldottuk meg a [42] cikkben. A 6. Tétel segítségével a ottani becslés jelentősen javítható: a Disszertáció 1.5.1. Következménye szerint

19. Következmény. *A fenti kúpszelet konfigurációban az érintési pontok száma legfeljebb $Cn^{\frac{139}{79}}$.*

Adott a (valós) síkon három középpont, és körülöttük egy–egy n koncentrikus körből álló körsereg. Egy pontot akkor nevezünk *háromszoros pontnak*, ha átmegy rajta mindhárom körseregnek egy-egy tagja. Erdős, Lovász és Vesztergombi [24] megkérdezték: mely középpont–hármasok esetén lehet végtelen sok n-re úgy választani a köröket, hogy legalább cn^2 háromszoros pont legyen? Elekes György [16] mutatott ilyen példát. Másrészt, a Disszertáció 1.5.3. Tételéből kiderül, hogy a legtöbb pont–hármas körül nincsenek ilyen körseregek:

20. Tétel. *Van egy abszolút konstans $\eta > 0$ és egy $n_1 \in \mathbb{Z}$ korlát a következő tulajdonsággal. Ha $n > n_1$, és a fenti körsereg konfigurációhoz legalább $n^{2-\eta}$ háromszoros pont található, akkor a három középpont egy egyenesre esik.*

Íme, a bizonyítás alapötlete: Először átfogalmazzuk a problémát. Három kör pontosan akkor metszi egymást egy pontban, ha a sugaraik kielégítenek egy bizonyos polinom–egyenletet. Tehát azt kell eldönteni, hogy az egyenlet zérushelye, egy $V \subset \mathbb{R}^3$ felület, gazdag-e. Egy felület pontosan akkor gazdag, ha az egyenlete kielégít egy bizonyos, a 14. Tétel segítségével konstruált parciális differenciálegyenletet. Végül a parciális differenciál egyenlet ellenőrzése egy kis algebrai zsonglőrködés.

Körök helyett vizsgálhatunk általánosabb folytonos görbéket. Az n tagú koncentrikus körseregek helyett n folytonos görbét választunk egy „folytonosan paraméterezett görbeseregből". Az egyszerűség kedvéért most olyan görbeseregekre szorítkozunk, melyek megadhatók egy-egy polinom szintvonalaival — „algebrai görbeseregek" mindig felírhatók ilyenek uniójaként.

21. Definíció. Legyen $G \subseteq \mathbb{R}^2$ egy nyílt halmaz a síkon, $\overline{G}$ a lezártja.

(a) Egy *algebrai görbesereg* $\overline{G}$-ben folytonos síkgörbéknek olyan $\Gamma = \{\gamma^{(t)} \subset \overline{G} \ : \ t \in [0,1]\}$ összessége, mely megadható egy háromváltozós, legfeljebb d fokú p polinommal:

$$\gamma^{(t)} = \left\{(x,y) \in \overline{G} \;\middle|\; p(x,y,t) = 0\right\} .$$

A p polinom többféleképpen is választható.[24] A Γ görbesereg *foka* a lehetséges legkisebb $\deg(p)$ érték.

(b) A Γ görbesereg *expliciten paraméterezett*, ha $\overline{G}$ minden pontján pontosan egy Γ-beli görbe megy át, és a $p\big((x,y,f(x,y)\big) = 0$ egyenlettel definiált implicit függvény analitikus G-ben, és folytonos $\overline{G}$-ben.

(c) Egy $\mathcal{E} \subset \overline{G}$ folytonos görbe a Γ sereg *burkoló görbéje*, ha minden pontjában van érintője, nincs közös rész–íve a Γ sereg egyetlen tagjával sem, és minden $P \in \mathcal{E}$ ponthoz van olyan $\gamma^{(t)} \in \Gamma$, amelyik a P pontban érinti az $\mathcal{E}$ görbét.

Legyenek $\alpha^{(r)}$, $\beta^{(s)}$, $\gamma^{(t)}$ algebrai görbeseregek a síkban. Azon (r_0, s_0, t_0) számhármasok mértani helye, melyekre az $\alpha^{(r_0)}$, $\beta^{(s_0)}$, $\gamma^{(t_0)}$ görbéknek van közös pontja, egy $V \subset \mathbb{R}^3$ algebrai felület.

22. Definíció. Választunk n pontot mindhárom görbecsaládból. Egy P síkbeli pont a konfiguráció *tripla–pontja*, ha mindhárom családban van olyan kiválasztott görbe, amelyik átmegy a P ponton.

Amennyiben a V felület nem gazdag (tipikusan ez a helyzet), akkor a 20. Tétel utáni érvelés mutatja, hogy legfeljebb $n^{2-\eta}$ tripla–pontot. Teljes általánosságban nem tudjuk eldönteni, hogy V gazdag-e, ámde a 14. Tétel segítségével jól használható geometriai kritériumokat kaphatunk. Az alábbi tétel a Disszertáció 4.4.1. Tételének egyszerűsített változata.

23. Tétel. *Legyenek $G \subset H$ nyílt halmazok a síkban, Γ_1, Γ_2 expliciten paraméterezett algebrai görbeseregek $\overline{H}$-ban, Γ_3 pedig egy expliciten paraméterezett algebrai görbesereg $\overline{G}$-ben. Jelölje d a három sereg fokának a maximumát. Tegyük fel, hogy Γ_3-nak van olyan $\mathcal{E}$ burkoló görbéje, amelyik benne van H-ban (tehát nem csak a lezártjában), és $\mathcal{E}$-nek a másik két sereg egyetlen tagjával sincs közös íve. Ha mindhárom görbeseregből kiválasztunk n görbét (n elég nagy), akkor a konfigurációnak legfeljebb $n^{2-\eta(d)}$ tripla–pontja lehet G-ben, ahol $0 < \eta(d)$ egy csak d-től függő állandó.*

Ennek azonnali következménye a Disszertáció 4.5.1. Tétele, amit korábban Székely László sejtett (lásd [18, Conjecture 3.41]):

[24] Például p minden hatványa ugyanazt a Γ görbesereget definiálja.

24. Következmény. *Adott három pont a síkban. Rajzolunk* $3n$ *olyan egységkört, melyekből mindhárom ponton legalább* n *áthalad. Ha* n *elég nagy, akkor a konfigurációnak legfeljebb* $n^{2-\eta}$ *tripla–pontja van. Itt* $\eta > 0$ *egy abszolút konstans.*

Végül meglátogatjuk egy klasszikus probléma (Gyümölcsöskert probléma, angolul Orchard problem, lásd [37], [54]) alábbi változatát:

25. *Probléma.* Rögzítünk egy $C > 0$ konstanst. Határozzuk meg azokat az n-pontú $\mathcal{H}$ halmazokat, melyekre a $\mathcal{H}$-t legalább három pontban metsző egyenesek száma legalább Cn^2.

Az általános filozófiánk most is azt sugallja, hogy a $\mathcal{H}$ halmazt valamiféle „szimmetria csoporttal" kell leírni. Ilyen ilyen általánosságban egyelőre nem tudunk csoportot találni (bár minden ismert konstrukció elmondható „csoport–nyelven" is). A Disszertáció 5.2.2. Tétele egy speciális, algebrai geometriával kezelhető, esetben oldja meg a kérdést.

26. Tétel. *Legyen* $\mathcal{H}$ *egy olyan véges ponthalmaz a síkban, melyhez található legalább* $c|\mathcal{H}|^2$ *olyan egyenes, amelyik áthalad legalább három* $\mathcal{H}$*-beli ponton. Tegyük fel, hogy egy legfeljebb* d *fokú irreducibilis algebrai görbe áthalad* $\mathcal{H}$ *minden pontján. Ha* $|\mathcal{H}|$ *elég nagy (*c *és* d *függvényében), akkor ebből következik, hogy a görbe harmadfokú.*

Itt érdemes megjegyezni, hogy Green–Tao [31] teljes általánosságban érvényes, pontos felső korlátot adtak a $\mathcal{H}$ halmaz méretére.

5. Alkalmazások a csoportelméletben

Babai sejtés. Babai [2] sejtette, hogy minden L nem–kommutatív véges egyszerű csoport minden Cayley–gráfjának az átmérője legfeljebb $C\big(\log|L|\big)^c$, ahol c és C abszolút konstansok. A Szorzattételből (16. Tétel) azonnal következik, hogy Babai sejtése igaz korlátos rangú egyszerű csoportokra:

27. Következmény. *Ha* L *egy korlátos rangú*[25] *nem–Abel véges egyszerű csoport, és* α *egy szimmetrikus generátor–rendszer* L*-ben, akkor a* $\Gamma(L,\alpha)$ *Cayley gráf átmérője legfeljebb* $C\big(\log|L|\big)^c$*, ahol* c *és* C *abszolút konstansok.*

Szorzatfelbontások. Legyen α egy csoport részhalmaza. Az α *konjugáltjai* a

$$g^{-1}\alpha g = \big\{g^{-1}ag \,\big|\, a \in \alpha\big\}$$

alakú részhalmazok, ahol g tetszőleges elem a csoportból. A Disszertáció 7. fejezetének kiindulópontja Liebeck, Nikolov és Shalev [39] következő sejtése:

28. Sejtés. *Legyen* G *egy nem–Abel véges egyszerű csoport,* $\alpha \subseteq G$ *pedig egy legalább kételemű részhalmaz. Ekkor* G *előáll az* α *halmaz legfeljebb* $c\log|G|/\log|\alpha|$ *konjugáltjának szorzataként, ahol* c *egy univerzális konstans.*

[25]Egy G véges egyszerű csoport rangja nagyjából egyenlő a legkisebb n amelyre G részcsoportja lesz az $SL(n,q)$ csoportnak valamilyen q prímhatványra.

Megjegyezzük, hogy a becslés egy konstans szorzó erejéig optimális, hiszen α-beli elemek $\frac{1}{2}\log|G|/\log|\alpha|$-tényezős szorzatainak száma nem lehet több $\sqrt{|G|}$-nél. A 28. Sejtés Liebeck és Shalev egy mély (és hasznos) tételének a kiterjesztése: [40]-ban belátták, hogy a sejtés teljesül abban az esetben, amikor α egy konjugált osztály.

Ha a 28. Sejtésben szereplő G csoport rangját korlátozzuk, akkor a 16. Tétel és egy meglepő kombinatorikus érvelés segítségével tetszőleges α részhalmazt tudunk kezelni. Erről szól a Disszertáció 7.1.3. Tétele:

29. Tétel. *Legyen G egy r rangú[25] nem–Abel véges egyszerű csoport, $\alpha \subseteq G$ pedig egy legalább kételemű részhalmaz. Ekkor G előáll az α halmaz legfeljebb $c(r)\log|G|/\log|\alpha|$ konjugáltjának szorzataként, ahol $c(r)$ egy r-től függő konstans.*

A Disszertáció 7.1.4. Tétele átalakítja ezt az eredményt egy növekedési tétellé:

30. Tétel. *Legyen G egy r rangú[25] nem–Abel véges egyszerű csoport, $\alpha \subseteq G$ pedig egy tetszőleges részhalmaz. Vagy van az α halmaznak egy olyan α' konjugáltja, amelyre $|\alpha\alpha'| \geq |\alpha|^{1+\varepsilon(r)}$, ahol $\varepsilon(r) > 0$ egy r-től függő konstans, vagy pedig $\alpha^3 = G$.*

Ennek analógiájaként érdemes a 28. Sejtést is átalakítani egy növekedési sejtéssé. A Disszertáció 7.6. és 7.4. szakaszában a klasszikus Plünecke–Ruzsa típusú egyenlőtlenségeket általánosítjuk tetszőleges (nem feltétlenül kommutatív) csoportokra, és ezek segítségével belátjuk, hogy az eredeti 28. Sejtésből következik az alábbi, növekedésről szóló változat:

31. Sejtés. *Léteznek $\varepsilon > 0$ valós és $b > 0$ egész konstansok az alábbi tulajdonsággal. Tetszőleges G nem–Abel véges egyszerű csoport minden α részhalmazának vagy van olyan α' konjugáltja, melyre $|\alpha\alpha'| \geq |\alpha|^{1+\varepsilon}$, vagy pedig G egyenlő az α halmaz b konjugáltjának szorzatával.*

Elképzelhető, hogy a 31. Sejtés $b = 3$-mal teljesül, $b = 2$-re viszont vannak ellenpéldák.

Permutáció–csoportok. Egy Γ gráf *G-csúcs–tranzitív*, ha G az $\mathrm{Aut}(\Gamma)$ olyan részcsoportja, amelyik tranzitívan hat Γ csúcshalmazán. Azt mondjuk, hogy egy G-csúcs–tranzitív gráf *lokálisan G-primitív*, ha egy α csúcs G_α stabilizátora primitív permutáció–csoportot indukál az α szomszédainak halmazán. (A tranzitivitás miatt ez vagy minden csúcsra teljesül, vagy egyikre sem). 1978-ban Richard Weiss [61] azt sejtette, hogy egy véges, összefüggő, G-csúcs–tranzitív, lokálisan G-primitív gráf esetében a G_α csúcs–stabilizátor mérete felülről korlátozható az α csúcs fokszámának függvényében. (A tranzitivitás miatt minden csúcs foka ugyanakkora, és a stabilizátorok is mind izomorfak).

A Disszertáció 6. fejezetében a Weiss sejtéssel foglalkozunk. A [47, 46]-beli redukciós tételek mutatják, hogy elég korlátozni bizonyos H-csúcs–tranzitív gráfok stabilizátorának méretét, ahol H a G csoport egy kompozíciófaktora. Mivel H egyszerű csoport, a H-csúcs–tranzitív gráfokat a Szorzattétel (lásd a 16. Tételt) segítségével vizsgálhatjuk. Ezzel a módszerrel belátjuk a Weiss sejtést abban a speciális esetben, ha a G csoport kompozíciófaktorainak rangja korlátos.

32. Definíció. Jelölje $\mathrm{BCP}(r)$ azon véges csoportok osztályát, melyeknek nincs olyan H/K szelése (itt $K < H \leq G$ és K normálosztó H-ban), amelyik izomorf az $\mathrm{Alt}(r+1)$ alternáló csoporttal.[26]

A $\mathrm{BCP}(r)$-csoportok osztályát először Babai, Cameron és Pálfy [1] vizsgálták. Belátták, hogy egy n-ed fokú primitív $\mathrm{BCP}(r)$-csoportnak legfeljebb $n^{f(r)}$ eleme van. Az eredményük fontos építőkő lett számos permutációcsoportos algoritmusban [38]. A $\mathrm{BCP}(r)$-csoportok nagyon fontos szerepet kapnak a részcsoport növekedés vizsgálatában is (lásd [41]).

A Disszertáció 6.1.2. Tétel azt mondja ki, hogy a Weiss sejtés igaz a $\mathrm{BCP}(r)$-csoportok osztályára. A teljes Weiss sejtés tehát azt kérdezi, hogy megválasztható-e az alábbi g függvény úgy, hogy ne függjön r-től.

33. Tétel. *Létezik egy $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ függvény az alábbi tulajdonsággal. Ha G egy $\mathrm{BCP}(r)$-csoport, akkor minden olyan G-csúcs–tranzitív, lokálisan G-primitív gráfban, ahol a csúcsok fokszáma d, a csúcs–stabilizátor mérete legfeljebb $g(d, r)$.*

[26] Könnyen látható, hogy egy $\mathrm{BCP}(r)$-csoport minden kompozíciófaktora vagy egy sporadikus egyszerű csoport, vagy pedig egy legfeljebb r rangú véges egyszerű csoport.

Az eredmények rövid összefoglalása, alkalmazások

Incidencia becslések. Vizsgálatunk kiindulópontja Szemerédi–Trotter [55] tétele, illetve Pach–Sharir [43] tétele volt.

A Disszertációban elért eredmények:

- Bevezettük a kombinatorikus dimenzió fogalmát.
- Általánosítottuk a Szemerédi–Trotter tételt magasabb dimenzióba. Az egyenesek szerepét a hipersíkok veszik át.
- Általánosítottuk a Pach–Sharir tételt magasabb dimenzióba. A síkgörbék szerepét tetszőleges algebrai varietások játsszák.
- Az általánosított incidencia tételeink érvényesek nem csak valós, hanem komplex hipersíkokra, illetve komplex varietásokra is.

Az irodalomban sokan foglalkoznak incidencia tételekkel, jelenleg is igen aktív kutatási terület. Lásd például: Chazelle–Edelsbrunner–Guibas–Sharir [14], Solymosi–Tao [53], Tóth [59], Bourgain–Katz–Tao [6], Bourgain [3].

Mind a Szemerédi–Trotter tételnek, mind pedig a Pach-Sharir tételnek számos alkalmazása van a kombinatorikában Most csak egy témakört említek: az összeg–szorzat tételeket gyakran incidencia–tételek segítségével bizonyítják (lásd például Elekes [17], és Solymosi [52] cikkét). A Disszertáció további részében is nagyon lényeges szerepe van az általánosított incidencia tételnek: ennek segítségével találunk szimmetria csoportokat.

Hogyan találjunk csoportokat? Vizsgálatunk kiindulópontja Elekes–Rónyai [20] tétele a kétváltozós racionális függvényekről.

A Disszertációban elért eredmények:

- Kiterjesztettük az Elekes–Rónyai tételt valós függvényekről komplex függvényekre.
- Észrevettük, hogy az Elekes–Rónyai tételben szereplő speciális alakú függvények valójában az egydimenziós affin algebrai csoportoknak felelnek meg. Ez nyitotta meg az utat a különféle általánosítások felé.
- Vannak olyan egydimenziós algebrai csoportok, amelyek nem szerepelnek az Elekes–Rónyai tételben: az elliptikus görbék. Kerestünk olyan geometriai–kombinatorikai konfigurációkat, melyek éppen ezekkel a csoportokkal hozhatók kapcsolatba.
- Kiterjesztettük a tételt „többértékű függvényekre”, vagy másképpen felületekre. Ez a kiterjesztés már figyelembe veszi az összes egydimenziós algebrai csoportot.
- Kiterjesztettük az Elekes–Rónyai tételt magasabb dimenzióba. Ez a kiterjesztés számot ad a magasabb dimenziós algebrai csoportokról.

A [20] dolgozatban az Elekes–Rónyai tétel segítségével oldották meg a Prudy problémát. A kiterjesztett tételnek még további szép kombinatorikai alkalmazásai szerepelnek a Disszertációban, ezekről a későbbiekben részletesen írok.

Növekedés csoportokban. Munkánk kiinduló pontja Helfgott [33] tétele és annak általánosításai (lásd Dinai [15] és Helfgott [34] cikkét) voltak, de a későbbi fejleményekben nagy szerepe volt Freiman [26] illetve Green–Ruzsa [30] tételének is.

A Disszertációban elért eredmények:

- Kiterjesztettük Helfgott tételét tetszőleges korlátos rangú véges egyszerű csoportra. (Ezt a tételt tőlünk függetlenül Breuillard, Green és Tao [11] is belátták).
- Tetszőleges lineáris csoportok nem–növő halmazait vizsgáltuk. Beláttuk, hogy ezek megértéséhez elegendő a virtuálisan feloldható csoportokkal foglalkozni.
- Részletes leírást adtunk a lineáris csoportok nem–növő halmazainak struktúrájára.

A fenti eredmények közeli rokona Breuillard–Green–Tao [13]. A Szorzattételeknek sok alkalmazása van a csoportelméletben és a számelméletben, lásd például Bourgain–Gamburd [4], Breuillard–Green–Tao [12] és [9], Varjú [60], Bourgain–Varjú [8], Golsefidy, Varjú [29], valamint Bourgain–Gamburd–Sarnak [5]. A Disszertációban szereplő csoportelméleti alkalmazásokról a későbbiekben részletesen írok.

Alkalmazások a kombinatorikában. Első két (kombinatorikai) témánknak számos kombinatorikai alkalmazása szerepel a Disszertációban:

- A korábban ismertnél sokkal pontosabb választ adtunk Hirzebruch [35] kérdésére: maximum hány érintési pont lehet n kúpszelet között?
- Megválaszoltuk Erdős, Lovász és Vesztergombi [24] kérdését: mely középpont–hármasok esetén lehet végtelen sok n-re úgy választani a köröket, hogy legalább cn^2 háromszoros pont legyen?
- A burkológörbék segítségével általános kritériumot adtunk arra, mikor van szub–kvadratikus becslés egy görbe–család háromszoros pontjainak számára.
- Az általános kritérium segítségével megoldottuk Székely egy sejtését (lásd [18, Conjecture 3.41]): három ponton keresztül nem lehet n-n-n egységkört rajzolni úgy, hogy Cn^2 háromszoros pontot kapjunk.
- Megoldottuk a „Gyümölcsöskert probléma” (angolul Orchard problem, lásd [37], [54]) egy változatát.

Alkalmazások a csoportelméletben. A harmadik (csoportelméleti) témánknak több csoportelméleti alkalmazása is bekerült a Disszertációba:

- Beláttuk, hogy korlátos rangú egyszerű csoportokra igaz Babai [2] sejtése.
- Beláttuk, hogy korlátos rangú egyszerű csoportokra igaz Liebeck–Nikolov–Shalev [39] sejtése.
- Megtaláltuk Liebeck–Nikolov–Shalev [39] sejtésének egy új, a Szorzattételre hajazó változatát. Beláttuk, hogy ez a változat is igaz a korlátos rangú egyszerű csoportokban.

- Beláttuk, hogy Weiss [61] sejtése igaz egy fontos csoport–osztályban (a Babai–Cameron–Pálfy [1] cikkben bevezetett BCP(r)-csoportokban).

Hivatkozások

1. L. Babai, P. J. Cameron, and P. P. Pálfy, *On the orders of primitive groups with restricted nonabelian composition factors*, J. Algebra **79** (1982), 161–168.
2. L. Babai and Á. Seress, *On the diameter of permutation groups*, European J. Comb. **13** (1992), 231–243.
3. J. Bourgain, *A modular Szemeredi-Trotter theorem for hyperbolas*, preprint: arXiv:1208.4008, 2012.
4. J. Bourgain and A. Gamburd, *Uniform expansion bounds for Cayley graphs of $SL_2(F_p)$*, Annals of Math. **167** (2008), no. 625–642, 625–642.
5. J. Bourgain, A. Gamburd, and P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** (2010), no. 3, 559–644.
6. J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geometric And Functional Analysis **14** (2004), no. 1, 27–57.
7. ———, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27–57.
8. J. Bourgain and P. P. Varjú, *Expansion in $SL_d(\mathbb{Z}/q\mathbb{Z})$, q arbitrary*, Inventiones **188** (2012), no. 1, 151–173.
9. E. Breuillard, B. Green, R. Guralnick, and T. Tao, *Expansion in finite simple groups of Lie type*, in preparation.
10. E. Breuillard, B. Green, and T. Tao, *Linear approximate groups*, Electronic Research Announcements in Mathematical Sciences **17** (2010), 57–67.
11. ———, *Approximate subgroups of linear groups*, Geometric And Functional Analysis **21** (2011), no. 4, 774–819.
12. ———, *Suzuki groups as expanders*, Groups, Geom. Dyn. **5** (2011), no. 2, 281–299, in volume in honour of Fritz Grunewald.
13. ———, *The structure of approximate groups*, Publ. Math. IHES **116** (2012), no. 1, 115–221, arXiv:1110.5008.
14. B. Chazelle, H. Edelsbrunner, L. Guibas, and M. Sharir, *A singly-exponential stratification scheme for real semi-algebraic varieties and its applications*, Theoretical Computer Science **84** (1991), 77–105.
15. O. Dinai, *Expansion properties of finite simple groups*, Ph.D. thesis, Hebrew University, 2009, arXiv:1001.5069.
16. Gy. Elekes, *Circle grids and bipartite graphs of distances*, Combinatorica **15** (1995), 167–174.
17. ———, *On the number of sums and products*, Acta Arithmetica **LXXXI** (1997), no. 4, 365–367.
18. ———, *Sums versus products in number theory, algebra and Erdős geometry — a survey*, Paul Erdős and his Mathematics II, Bolyai Math. Soc. Stud., vol. 11, Bolyai Math. Soc., Budapest, 2002, pp. 241–290.
19. Gy. Elekes, M. B. Nathanson, and I. Z. Ruzsa, *Convexity and sumsets*, Journal of Number Theory **83** (1999), 194–201.
20. Gy. Elekes and L. Rónyai, *A combinatorial problem on polynomials and rational functions*, Journal of Combinatorial Theory, series A **89** (2000), 1–20.
21. Gy. Elekes, M. Simonovits, and E. Szabó, *A combinatorial distinction between unit circles and straight lines: How many coincidences can they have?*, Combinatorics, Probability and Computing **18** (2009), no. 5, 691–705.
22. Gy. Elekes and E. Szabó, *On triple lines and cubic curves — the orchard problem revisited*, preprint, arXiv:1302.5777.

23. ———, *How to find groups? (and how to use them in Erdős geometry?)*, Combinatorica **32** (2012), no. 5, 537–571.
24. P. Erdős, L. Lovász, and K. Vesztergombi, *On graphs of large distances*, Discrete and Computational Geometry **4** (1989), 541–549.
25. P. Erdős and E. Szemerédi, *On sums and products of integers*, To the memory of Paul Turán (P. Erdős, L. Alpár, and G. Halász, eds.), Studies in Pure Mathematics, Akademiai Kiadó - Birkhauser Verlag, 1983, pp. 213–218.
26. G Freiman, *Groups and the inverse problems of additive number theory (in Russian)*, Number-theoretic studies in the Markov spectrum and in the structural theory of set addition (in Russian), Kalinin. Gos. Univ., Moscow, 1973, pp. 175–183.
27. N. Gill and H. A. Helfgott, *Growth in solvable subgroups of* $GL_r(\mathbb{Z}/p\mathbb{Z})$, preprint, arXiv:1008.5264, 2010.
28. N. Gill, L. Pyber, I. Short, and E. Szabó, *On the product decomposition conjecture for finite simple groups*, accepted in Groups, Geometry, and Dynamics. arXiv:1111.3497, 2012.
29. A. S. Golsefidy and P. P. Varjú, *Expansion in perfect groups*, preprint: arXiv:1108.4900.
30. B. Green and I. Ruzsa, *Freiman's theorem in an arbitrary abelian group*, Jour. London Math. Soc. **75** (2007), no. 1, 163–175.
31. B. Green and T. Tao, *On sets defining few ordinary lines*, preprint: arXiv:1208.4714.
32. M. Gromov, *Groups of polynomial growth and expanding maps*, Publ. Math., Inst. Hautes Étud. Sci. **53** (1981), 53–78.
33. H. A. Helfgott, *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Annals of Math. **167** (2008), 601–623.
34. ———, *Growth in* $SL_3(\mathbb{Z}/p\mathbb{Z})$, J. European Math. Soc. **13** (2011), no. 3, 761–851.
35. F. Hirzebruch, *Singularities of algebraic surfaces and characteristic numbers*, Contemp. Math. **58** (1986), 141–155.
36. E. Hrushovski, *Contributions to stable model theory*, Ph.D. thesis, University of California, Berkeley, 1986.
37. J. Jackson, *Rational amusements for winter evenings*, Longman Hurst Rees Orme and Brown, London, 1821.
38. W. M. Kantor and E. M. Luks, *Computing in quotient groups*, STOC '90 Proceedings of the twenty-second ACM symposium on Theory of computing, 1990, pp. 524–534.
39. M. W. Liebeck, N. Nikolov, and A. Shalev, *Product decompositions in finite simple groups*, Bulletin of the LMS **44** (2012), no. 3, 469–472.
40. M. W. Liebeck and A. Shalev, *Diameters of finite simple groups: sharp bounds and applications*, Ann. of Math. (2) **154** (2001), no. 2, 383–406.
41. A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser, 2003.
42. G. Megyesi and E. Szabó, *On the tacnodes of configurations of conics in the projective plane*, Mathematische Annalen **305** (1996), 693–703.
43. J. Pach and M. Sharir, *On the number of incidences between points and curves*, Combinatorics, Probability and Computing **7** (1998), 121–127.
44. A. Pillay, *Geometric stability theory*, Oxford Logic Guides, vol. 32, Clarendon Press, Oxford, 1996.
45. C. Praeger, L. Pyber, P. Spiga, and E. Szabó, *Graphs with automorphism groups admitting composition factors of bounded rank*, Proc. of the AMS. **140** (2012), no. 7, 2307–2318.
46. C. E. Praeger, *Imprimitive symmetric graphs*, Ars Combinatoria **19A** (1985), 149–163.
47. C. E. Praeger, P. Spiga, and G. Verret, *Bounding the size of the vertex-stabiliser in vertex-transitive graphs*, preprint: arXiv:1102.1543, 2011.
48. L. Pyber and E. Szabó, *Helfgott's conjecture, soluble version*, preprint.
49. ———, *Growth in finite simple groups of Lie type*, announcement, arXiv:1001.4556, 2010.

50. ———, *Growth in finite simple groups of Lie type of bounded rank*, preprint, arXiv:1005.1858, 2010.
51. I. Z. Ruzsa, *Generalized arithmetical progressions and sumsets*, Acta Math. Hung. **65** (1994), no. 4, 379–388.
52. J. Solymosi, *On the number of sums and products*, Bull. London Math. Soc. **37** (2005), no. 4, 491–494.
53. J. Solymosi and T. Tao, *An incidence theorem in higher dimensions*, Discrete & Computational Geometry **48** (2012), no. 2, 255–280.
54. J. J. Sylvester, *Problem 2473*, Math. Questions from the Educational Times **8** (1867), 106–107.
55. E. Szemerédi and W. T. Trotter, Jr., *Extremal problems in discrete geometry*, Combinatorica **3** (1983), no. 3–4, 381–392.
56. T. Tao, *Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets*, preprint: arXiv:1211.2894.
57. ———, *Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets*, blog: http://terrytao.wordpress.com/2012/11/14/expanding-polynomials-over-finite-fields-of-large-characteristic-and-a-regularity-lemma-for-definable-sets.
58. ———, *The sum-product phenomenon in arbitrary rings*, Contrib. Discrete Math. **4** (2009), no. 2, 59–82.
59. D. Cs. Tóth, *The Szemeredi-Trotter theorem in the complex plane*, preprint: arXiv:math/0305283, 2003.
60. P. Varjú, *Expansion in $SL_d(O_K/I)$, I square-free*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 1, 273–305.
61. R. Weiss, *s-transitive graphs*, Colloq. Math. Soc. János Bolyai, vol. 25, Math. Soc. János Bolyai, 1978, pp. 827–847.