Eötvös Loránd Tudományegyetem

Természettudományi Kar

# Algebrai módszerek a kombinatorikában

Szakdolgozat

Varga Bálint

Matematika BSc

Alkalmazott matematikus szakirány

Témavezető: Csikvári Péter

Számítógéptudományi Tanszék

Budapest, 2012

# Tartalomjegyzék

# 1. fejezet

# Bevezetés

Ha az ember meghallja a "Nullstellensatz" kifejezést és utánanéz a fogalomnak, minden bizonnyal először D. Hilbert következő tételére bukkan:

**1. Tétel** (Hilbert)**.** *Legyen $T$ algebrailag zárt test. Legyenek $f, g_1, g_2, \ldots, g_k \in T[x_1, \ldots, x_n]$, továbbá tegyük fel, hogy minden olyan $(c_1, c_2, \ldots, c_n) \in T^n$ vektorra, ahol $\forall i$-re $g_i(c_1, c_2, \ldots, c_n) = 0$, ott $f(c_1, c_2, \ldots, c_n) = 0$ is teljesül. Másképp fogalmazva a $g_1, g_2, \ldots, g_k$ polinomok minden közös zérushelye egyben $f$-nek is gyöke. Ekkor léteznek olyan $h_1, h_2, \ldots, h_k \in T[x_1, x_2, \ldots, x_n]$ polinomok és olyan $m$ természetes szám, hogy*

$$f^m = \sum_{i=1}^{k} h_i g_i.$$

A tétel egy bizonyítása megtalálható [1]-ben. A dolgozatban ennek a tételnek egy speciális változatával foglalkozunk.

Legyen $k{=}n$ és legyen $S_i{\subseteq}T$ nemüres részhalmaz, $i{=}1, \ldots, n$. Válasszuk $g_i$-ket a következőképp:

$$g_i = \prod_{s \in S_i} (x_i - s)$$

Ezen speciális feltételek mellett Hilbert fenti tételénél erősebb állítás is megfogalmazható:

**2. Tétel.** *Legyen $T$ tetszőleges test. Legyen $f{\in}T[x_1, \ldots, x_n]$ és legyenek $S_1, S_2, \ldots, S_n{\subseteq}T$ nemüres részhalmazok. Definiáljuk $g_i$-ket a fenti módon. Ha*

$$f(s_1, s_2, \ldots, s_n) = 0 \ \forall (s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \ldots \times S_n$$

*vektoron, vagyis a $g_1, g_2, \ldots, g_k$ polinomok minden közös zérushelye egyben $f$-nek is gyöke, akkor léteznek olyan $h_1, h_2, \ldots, h_n \in T[x_1, \ldots, x_n]$ polinomok, amelyekre*

$$f = \sum_{i=1}^{n} h_i g_i,$$

*továbbá*

$$\deg(h_i) \leq \deg(f) - \deg(g_i).$$

*Sőt, ha van $R$ részgyűrű $T$-ben, hogy $f, g_1, g_2, \ldots, g_n \in G[x_1, \ldots, x_n]$, akkor $h_1, h_2, \ldots, h_n$ is választhatóak $R[x_1, \ldots, x_n]$-ből.*

Ebből pedig levezethető a következő tétel:

**3. Tétel.** *Legyen $T$ tetszőleges test. Legyen $f \in T[x_1, \ldots, x_n]$, és legyen $\prod_{i=1}^{n} x_i^{t_i}$ $(t_i \in \mathbb{N})$ egy legmagasabb fokú monom $f$-ben, amely együtthatója nem nulla. Ekkor tetszőleges $S_1, \ldots, S_n \subseteq T$ halmazokhoz, amelyekre teljesül, hogy $|S_i| > t_i$, létezik $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ vektor, hogy $f(s_1, \ldots, s_n) \neq 0$.*

Ezen két tételt hívjuk "Kombinatorikus Nullstellensatznak", mert ennek a két polinomokról szóló, tisztán algebrai tételnek meglepően sok alkalmazási lehetősége van a kombinatorikában.

A dolgozat első fejezetében a két fenti tétel bizonyítása szerepel, Noga Alon eredeti [2] cikke alapján.

A technika közel 20 éves története alatt sok általánosítása született az eredeti tételeknek, ezek közül került egy a második fejezetbe.

A harmadik fejezetben bemutatok néhány alkalmazást, elsősorban a számelmélet, a véges geometria és a gráfelmélet területéről.

# 2. fejezet

# Fogalmak, Jelölések

A dolgozat egészében $T$ tetszőleges testet jelent. Ha $f \in T[x_1, x_2, \dots, x_n]$, akkor $f$ egy $n$ változós polinom, amely az $x_1, x_2, \dots, x_n$ változóktól függ és amelynek minden együtthatója a $T$ testből való. Monom alatt az $x_1, x_2, \dots, x_n$ változókból álló $\prod_{i=1}^{n} x_i^{d_i}$ alakú kifejezéseket értek.

**2.1. Definíció.** *Az $\prod_{i=1}^{n} x_i^{d_i}$ monom fokszáma $\sum_{i=1}^{n} d_i$.*

**2.2. Definíció.** *Jelölje $f_{d_1 d_2 \cdots d_n}$ az $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ monom $f$-beli együtthatóját.*

**2.3. Definíció.** *Az $f$ polinom foka*

$$\deg(f) = \max\left\{\sum_{i=1}^{n} d_i \mid f_{d_1 d_2 \dots d_n} \neq 0\right\}$$

**2.4. Definíció.** *Az $f$ polinom főtagjai azok a monomok, amelyekre*

$$\sum_{i=1}^{n} d_i = \deg(f) \text{ és } f_{d_1 d_2 \dots d_n \neq 0}$$

**2.5. Definíció.** *Az $f$ polinom $x_i$-beli foka az $x_i$ változó maximális előfordulása, vagyis*

$$\deg_{x_i}(f) = \max\{d_i | f_{d_1 d_2 \dots d_{i-1} d_i d_{i+1} \dots d_n} \neq 0\}$$

Hivatkozni fogok a következő "jól ismert" tételre:

**2.6. Tétel.** *Legyen $f \in T[x]$, $\deg(f) = n$. Ha $n > 0$, akkor $f$-nek legfeljebb $n$ gyöke van $T$-ben.*

# 3. fejezet

# Kombinatorikus Nullstellensatz

A "Kombinatorikus Nullstellensatz" a következő két tétel:

**3.1. Tétel.** *Legyen $f \in T[x_1, \ldots, x_n]$ és legyenek $S_1, S_2, \ldots, S_n \subseteq T$ nemüres részhalmazok. Definiáljuk $g_i$-ket a következő egyváltozós polinomoknak:*

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

*Ha*

$$f(s_1, s_2, \ldots, s_n) = 0 \ \forall (s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \ldots \times S_n \text{ vektoron,}$$

*vagyis a $g_1, g_2, \ldots, g_k$ polinomok minden közös zérushelye egyben $f$-nek is gyöke, akkor léteznek olyan $h_1, h_2, \ldots, h_n \in T[x_1, \ldots, x_n]$ polinomok, amelyekre*

$$f = \sum_{i=1}^{n} h_i g_i,$$

*továbbá*

$$\deg(h_i) \leq \deg(f) - \deg(g_i).$$

*Sőt, ha van olyan $R$ részgyűrű $T$-ben, hogy $f, g_1, g_2, \ldots, g_n \in R[x_1, \ldots, x_n]$, akkor $h_1, h_2, \ldots, h_n$ is $R[x_1, \ldots, x_n]$-beli.*

**3.2. Tétel.** *Legyen $f \in T[x_1, \ldots, x_n]$, és legyen $\prod_{i=1}^{n} x_i^{t_i}$ $(t_i \in \mathbb{N})$ egy legmagasabb fokú monom $f$-ben, amely együtthatója nem nulla. Ekkor tetszőleges $S_1, \ldots, S_n \subseteq T$ halmazokhoz, amelyekre teljesül, hogy $|S_i| > t_i$, létezik $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ vektor, hogy $f(s_1, \ldots, s_n) \neq 0$.*

Ebben a fejezetben ezen tételek bizonyítása szerepel. Szükségünk lesz hozzá a következő lemmára:

**3.3. Lemma.** *Legyen $p \in T[x_1, x_2, \ldots, x_n]$. Tegyük fel, hogy $p$-ben $x_i$ kitevője legfeljebb $t_i$, $1 \leq i \leq n$. Legyenek $S_1, S_2, \ldots, S_n \subseteq T$ nemüres részhalmazok, melyekre $|S_i| > t_i$. Ha*

$$\forall (s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n\text{-re } p(s_1, s_2, \ldots, s_n) = 0,$$

*akkor $p$ az azonosan $0$ polinom.*

*Bizonyítás.* Alkalmazzunk $n$-szerinti indukciót!

Az $n = 1$ esetben a polinom egyváltozós, egyváltozós polinomokra pedig az állítás ismert.

Tegyük fel, hogy $n-1$ változóra már beláttuk az állítást! Vegyünk $S_i$ halmazokat, $p$ polinomot a feltételek szerint, és írjuk $p$-t az $x_n$ változó hatványai szerint csoportosítva:

$$p(x_1,x_2,\ldots,x_n)=\sum_{j=1}^{t_n} p_j(x_1,x_2,\ldots,x_{n-1})\cdot x_n^j$$

A $p_j$-k $x_n$-től már nem függő $n-1$ változós polinomok, ahol $x_i$ kitevője továbbra is legfeljebb $t_i$, így teljesülnek rájuk az indukciós feltevés feltételei. Tehát ha belátjuk, hogy

$$p_j(s_1,s_2,\ldots,s_{n-1})=0\ \forall(s_1,s_2,\ldots,s_{n-1})\in S_1\times S_2\times\cdots\times S_{n-1} \text{ vektoron,}$$

akkor az indukcióból következik, hogy $p_j\equiv 0$ minden $j$-re, tehát $p$ is azonosan 0.

A Lemma feltételeiből tudjuk, hogy

$$p(s_1,s_2,\ldots,s_n)=0\ \forall(s_1,s_2,\ldots,s_n)\in S_1\times S_2\times\cdots\times S_n \text{ vektoron.}$$

Rögzítsünk egy tetszőleges $(s_1,s_2,\ldots,s_{n-1})\in S_1\times S_2\times\cdots\times S_{n-1}$ vektort, és tekintsük $p$-t $x_n$-től függő egyváltozós polinomnak, az így kapott $p_j(s_1,s_2,\ldots,s_{n-1})$ együtthatókkal!

Ennek a polinomnak a foka legfeljebb $t_n$, és vegyük észre, hogy $S_n$ minden eleme gyöke. Mivel $|S_n|>t_n$, ezért ez a polinom csak az azonosan 0 polinom lehet. Következésképpen

$$p_j(s_1,s_2,\ldots,s_{n-1})=0, \forall j=1,\ldots,n\text{-re.}$$

Mivel $(s_1,s_2,\ldots,s_{n-1})$ tetszőleges volt, készen vagyunk. $\square$

Ezek után rátérhetünk a tételek bizonyítására:

*A* 3.1 *Tétel bizonyítása.* Vezessük be a $t_i:=|S_i|-1$ jelölést, és írjuk fel $g_i(x_i)$-t $x_i$ hatványainak lineáris kombinációjaként, a következő módon:

$$g_i(x_i)=\prod_{s\in S_i}(x_i-s)=x_i^{t_i+1}-\sum_{j=1}^{t_i} g_{ij}\cdot x_i^j.$$

Osszuk el $f$-et maradékosan $x_1^{t_1+1}$-gyel! Kapjuk:

$$f=l_{11}\cdot x_1^{t_1+1}+m_{11},$$

ahol $m_{11}$-ben $x_1$ kitevője legfeljebb $t_1$. Legyen:

$$\tilde{f}_1:=f-l_{11}\cdot g_1=l_{11}\cdot x_1^{t_1+1}+m_{11}-l_{11}\left(x_1^{t_1+1}-\sum_{j=1}^{t_1} g_{1j}\cdot x_1^j\right)=l_{11}\cdot\sum_{j=1}^{t_1} g_{1j}\cdot x_1^j+m_{11}.$$

Ekkor $\tilde{f}_1$-ben $x_1$ kitevője vagy $t_1$, vagy több, attól függően, hogy $l_{11}$ függ-e még $x_1$-től. Ha igen, a kapott $\tilde{f}_1$ polinommal ismételjük a fenti eljárást, amíg a polinomban $x_1$ kitevője $t_1$ nem lesz! Tegyük fel, hogy ehhez $k_1$ lépés kellett. Kapjuk:

$$\tilde{f}_1=f-l_{11}\cdot g_1-\ldots-l_{1k_1}\cdot g_1=f-g_1\cdot\sum_{j=1}^{k_1} l_{1j}$$

A $h_1=\sum_{j=1}^{k_1} l_{1j}$ jelöléssel:

$$\tilde{f}_1=f-g_1h_1$$

Ezt végezzük el a többi változóval is! Legyen $1 < i \le n$. Egy általános lépésben:

$$\tilde{f}_{i-1} = l_{ij} \cdot x_i^{t_i+1} + m_{ij},$$

$$\tilde{f}_i := \tilde{f}_{i-1} - l_{ij} \cdot g_i = l_{ij} \cdot x_i^{t_i+1} + m_{ij} - l_{ij}\left(x_i^{t_i+1} - \sum_{j=1}^{t_i} g_{ij} \cdot x_i^j\right) = l_{ij} \cdot \sum_{j=1}^{t_i} g_{ij} \cdot x_i^j + m_{ij},$$

$$h_i := \sum_{j=1}^{k_i} l_{ij}, \quad \tilde{f}_i = \tilde{f}_{i-1} - h_i g_i.$$

Mivel $\tilde{f}_i$-ben $x_i$ kitevője legfeljebb $t_i$, és ezt későbbi lépésekben sem változtatjuk meg, $\tilde{f}_n$-ben $x_i$ kitevője legfeljebb $t_i$, $i = 1, \ldots, n$. Az egész eljárás összefoglalható a következő formában:

$$\tilde{f}_n = f - h_1 g_1 - h_2 g_2 - \ldots - h_n g_n = f - \sum_{i=1}^{n} h_i g_i.$$

A feltételek miatt tetszőleges $(s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$ vektoron

$$\tilde{f}(s_1, \ldots, s_n) = f(s_1, \ldots, s_n) - \sum_{i=1}^{n} h_i(s_1, \ldots, s_n) g_i(s_i) = 0,$$

így alkalmazva $\tilde{f}_n$-re az előző 3.3 Lemmát, kapjuk, hogy

$$f - \sum_{i=1}^{n} h_i g_i = \tilde{f}_n \equiv 0,$$

azaz

$$f = \sum_{i=1}^{n} h_i g_i.$$

Mivel a fokszám egyik lépésben sem nőtt,

$$\deg(f) \ge \deg(\tilde{f}_{i-1}) = \deg(l_{ij} \cdot x^{t_i+1} + m_{ij}),$$

ahol is $m_{ij}$ választása miatt

$$\deg(l_{ij} \cdot x^{t_i+1} + m_{ij}) \ge \deg(l_{ij} \cdot x^{t_i+1}) = \deg(l_{ij}) + \deg(x^{t_i+1}) = \deg(l_{ij}) + \deg(g_i),$$

tehát

$$\deg(f) - \deg(g_i) \ge \deg(l_{ij}).$$

Hozzávéve, hogy

$$\deg(l_{ij}) \ge \deg\left(\sum_{j=1}^{k_i} l_{ij}\right) = \deg(h_i),$$

kapjuk:

$$\deg(f) - \deg(g_i) \ge \deg(h_i).$$

Végül vegyük észre, hogy $h_i$ bármelyik együtthatója előállítható $f$, $g_1$, $g_2$, $\ldots$, $g_n$ együtthatóiból, összeadás, kivonás és szorzás műveletével, vagyis ha van egy $R$ részgyűrű $T$-ben, hogy $f, g_1, g_2, \ldots, g_n \in R[x_1, x_2, \ldots, x_n]$, akkor ezekkel a műveletekkel nem lépünk ki $R$-ből, tehát $h_i \in$ $\in R[x_1, x_2, \ldots, x_n]$.

$\square$

*A 3.2 Tétel bizonyítása.* Feltehető, hogy $|S_i|=t_i+1$, ugyanis ha $|S_i|\geq t_i+2$, tetszőlegesen dobáljunk ki annyi elemet, hogy éppen $t_i+1$ maradjon. Ha ezekben a szűkebb halmazokban található olyan n-es, amelyre

$$f(s_1,\ldots,s_n)\neq 0,$$

akkor az az eredeti halmazokra is jó.

Indirekt bizonyítunk: tegyük fel, hogy a tétel hamis:

$$\forall(s_1,\ldots,s_n)\in S_1\times\cdots\times S_n\text{-re } f(s_1,\ldots,s_n)=0.$$

Az előző 3.1 Tétel szerint

$$\exists h_1,h_2,\ldots,h_n\in T[x_1,\ldots,x_n],\ \text{hogy } f=\sum_{i=1}^{n}h_ig_i,$$

valamint

$$\deg(h_i)\leq\deg(f)-\deg(g_i)=\sum_{j=1}^{n}t_j-(t_i+1).$$

Feltevésünk szerint a $\prod_{i=1}^{n}x_i^{t_i}$ monom szerepel $f$-ben, tehát az együtthatója nem nulla. Keressük meg ezt a tagot $\sum_{i=1}^{n}h_ig_i$-ban!

Mivel $\deg(h_i)\leq\sum_{j=1}^{n}t_j-(t_i+1)$, $\sum_{i=1}^{n}t_i$ fokú tag csak úgy jöhet létre, ha valamely $h_i$-t $x^{t_i+1}$-nel szorzok. Vagyis ha van $\deg(f)$ fokszámú tag, az osztható $x_i^{t_i+1}$-gyel valamely $i$-re. Ezek szerint $\prod_{i=1}^{n}x_i^{t_i}$ együtthatója csak 0 lehet. Ez ellentmondás.

$\square$

# 4. fejezet

# Egy általánosítás

Ez a fejezet az első fejezet két tételének egy általánosításáról szól, amely M. Lason [3] cikkéből való.

Bizonyos értelemben mind a 3.3 Lemma, mind a 3.2 Tétel egy többváltozós változata annak az algebrai tételnek, miszerint egy polinomnak nem lehet több gyöke, mint a maximális fokszáma, tehát ha ez a maximális fokszám $n$, akkor tetszőleges, legalább $n+1$ elemű halmaz elemeit behelyettesítve nem lehet minden érték 0.
De többváltozós polinomoknál, ha egy pillanatra félretesszük a hivatalos definíciót, a "maximális fokszám"-ra több elképzelésünk is lehet. Például 3.3 Lemmában az egyes változók fokszámainak legnagyobb előfordulását nevezhetjük a változó maximális fokszámának. Az 3.2 Tételben a polinomban szereplő monomok fokszámösszegére keresünk maximálisat, és az egyes változók maximális fokszámán egy ilyen "maximális monom"-beli fokszámot értünk.

A következőkben $f$ monomjaihoz $\mathbb{N}^n$-beli vektorokat rendelünk, majd ezen vektorok halmazán bevezetünk egy részbenrendezést. A 4.4 Tétel szerint elég az ezen rendezésben maximális monomokat néznünk: ha az egyes változókra egy ilyen monomban előforduló fokszámánál nagyobb elemszámú halmazokat írok elő, már ezen halmazokon sem lehet minden érték nulla.

Formálisan:

$f$ monomjait feleltessük meg $\mathbb{N}^n$ vektoroknak a következő módon:

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n} \longleftrightarrow (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

**4.1. Definíció.** *Nevezzük a*

$$Supp(f) := \{\ (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{N}^n \mid f_{\alpha_1 \cdots \alpha_n} \neq 0\ \}$$

*halmazt $f$ tartójának.*

**4.2. Definíció.** *Ha nem okoz félreértést, az $(\alpha_1, \alpha_2 \ldots \alpha_n)$ jelölés helyett az $\underline{\alpha}$ jelölést használom.*

Definháljunk $\mathbb{N}^n$-en egy részbenrendezést:

**4.3. Definíció.** $\underline{\alpha}, \underline{\beta} \in \mathbb{N}^n$*-ra legyen* $\underline{\alpha} \leq \underline{\beta}$*, ha* $1 \leq i \leq n$*-re* $\alpha_i \leq \beta_i$.

Minden készen áll a következő tételhez:

**4.4. Tétel.** *Tegyük fel, hogy $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ egy maximális elem Supp$(f)$-ben. Ekkor tetszőleges $S_1, S_2, \cdots, S_n \subseteq T$, $|S_i| > \alpha_i$ halmazokhoz*

$$\exists (s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n, \text{ hogy } f(s_1, s_2, \ldots, s_n) \neq 0.$$

*Bizonyítás.* A bizonyítás teljes indukció $\alpha_1+\cdots+\alpha_n$ szerint.
Ha $\alpha_1+\cdots+\alpha_n=0$, az csak úgy lehet, ha $\alpha_1=\cdots=\alpha_n=0$, ami a fenti rendezésben mindennel összehasonlítható, vagyis csak úgy lehet maximális, ha $f\equiv c$, és mivel $(\alpha_1,\alpha_2,\ldots,\alpha_n)\in \mathrm{Supp}(f)$, $c\neq 0$.

Ha $\alpha_1+\cdots+\alpha_n>0$, akkor feltehetjük, hogy $\alpha_1>0$. Fixáljunk le egy tetszőleges $s\in S_1$ elemet, és osszuk el maradékosan $f$-et $(x_1-s)$-sel:

$$f=g\cdot(x_1-s)+h,$$

ahol $\deg_{x_1}(h)<1$, vagyis $h$ nem függ $x_1$-től.
Ha van $(s_2,\ldots,s_n)\in S_2\times\cdots\times S_n$, hogy $h(s_1,\ldots,s_n)\neq 0$, akkor

$$f(s,s_2,s_3,\ldots,s_n)=h(s_1,\ldots,s_n)\neq 0,$$

ezzel kész vagyunk.

Most tegyük fel, hogy

$$h(s_2,\ldots,s_n)=0,\ \forall(s_2,\ldots,s_n)\in S_2\times\ldots\times S_n.$$

Vegyük észre, hogy $g$-ben pontosan azon monomok vannak $f$-ből, amelyekben szerepelt $x_1$, és a többi változó kitevőit ez az osztás nem befolyásolja.

$$\mathrm{Supp}(g)\subseteq\{(\beta_1-r,\beta_2,\cdots,\beta_n)\mid(\beta_1,\beta_2,\cdots,\beta_n)\in\mathrm{Supp}(f),\ 1\le r\le\beta_1\},$$

és $(\alpha_1-1,\alpha_2,\cdots,\alpha_n)$-nek benne kell lenni $\mathrm{Supp}(g)$-ben, különben sehogy nem jöhetne létre $(\alpha_1,\alpha_2,\cdots,\alpha_n)$.
Tehát $(\alpha_1-1,\alpha_2,\cdots,\alpha_n)$ maximális $\mathrm{Supp}(g)$-ben. Alkalmazzuk $g$-re és
$(\alpha_1-1,\alpha_2,\ldots,\alpha_n)$-re az indukciós feltételt!

$$\exists(s_1,s_2,\ldots,s_n)\in(S_1/s)\times S_2\times\cdots\times S_n,\ g(s_1,s_2,\cdots,s_n)\neq 0.$$

Így

$$f(s_1,s_2,\cdots,s_n)=g(s_1,s_2,\cdots,s_n)\cdot(s_1-s)\neq 0.$$

□

M. Lason [3] fent említett cikkében található a következő "Együttható-formula"-nak nevezett tétel is. Tulajdonképpen többváltozós polinom-interpolációról lesz szó. Egy többváltozós polinom együtthatóit egy megfelelő méretű halmazon felvett értékeiből állítjuk elő.

**4.5. Definíció.** *Legyenek $S_1,S_2,\cdots,S_n\subseteq T$. Definiáljuk $N(s_1,\ldots,s_n)$-t a következőképp:*

$$N(s_1,\ldots,s_n):=\prod_{i=1}^{n}\prod_{b\in S_i/s_i}(s_i-b)$$

Vegyük észre, hogy ez az $N$ függvény a Lagrange-interpoláció többváltozós megfelelőjénél használt normálótag:

$$L_{s_1,\ldots,s_n}(x_1,\ldots,x_n)=\frac{\prod_{i=1}^{n}\prod_{b\in S_i/s_i}(x_i-b)}{\prod_{i=1}^{n}\prod_{b\in S_i/s_i}(s_i-b)}=\frac{\prod_{i=1}^{n}\prod_{b\in S_i/s_i}(x_i-b)}{N(s_1,\ldots,s_n)}$$

**4.6. Definíció.** *Legyen*

$$\mathit{Cone}(f):=\{\beta\in\mathbb{N}^n|\ \exists\alpha\in \mathit{Supp}(f),\ \mathit{hogy}\ \beta\le\alpha\}$$

A bizonyítás végét megkönnyíti a következő lemma:

**4.7. Lemma.** *Legyen $S$ egy tetszőleges, véges részhalmaza $T$-nek, $|S| \geq 2$. Ekkor*

$$\sum_{s\in S}\prod_{b\in S/s}(s-b)^{-1}=0$$

*Bizonyítás.* Tekintük a következő egyváltozós polinomot:

$$f(x)=\sum_{s\in S}\prod_{b\in S/s}\frac{(x-b)}{(s-b)}$$

Egyrészről ha $f$-et kifejtem $x$ hatványai szerint, kapom, hogy $f$ foka legfeljebb $|S|-1$, valamint $x^{|S|-1}$ együtthatója $\sum_{s\in S}\prod_{b\in S/s}\frac{1}{(s-b)}$.
Másrészről $f(s)=1$ minden $s\in S$-re, tehát $f\equiv 1$. Így

$$\sum_{s\in S}\prod_{b\in S/s}\frac{1}{(s-b)}=0.$$

□

Most már következhet a tétel:

**4.8. Tétel** (Együttható-formula)**.** *Tegyük fel, hogy $(\alpha_1,\alpha_2,\cdots,\alpha_n)$ maximális elem Supp$(f)$-ben. Ekkor tetszőleges $S_1,\cdots,S_n\subseteq T$, $|S_i|=\alpha_i+1$ halmazokra*

$$f_{\alpha_1\cdots\alpha_n}=\sum_{(s_1,\dots,s_n)\in S_1\times\cdots\times S_n}\frac{f(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}$$

*Bizonyítás.* Először is, a formula lineáris:
Ha már tudom, hogy

$$f_{1\alpha_1\cdots\alpha_n}=\sum_{(s_1,\dots,s_n)\in S_1\times\cdots\times S_n}\frac{f_1(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}$$

illetve

$$f_{2\alpha_1\cdots\alpha_n}=\sum_{(s_1,\dots,s_n)\in S_1\times\cdots\times S_n}\frac{f_2(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}$$

akkor tetszőleges $\lambda_1,\lambda_2\in T$, $f=\lambda_1\cdot f_1+\lambda_2\cdot f_2$-re:

$$f_{\alpha_1\cdots\alpha_n}=\lambda_1\cdot f_{1\alpha_1\cdots\alpha_n}+\lambda_2\cdot f_{2\alpha_1\cdots\alpha_n}=$$

$$=\lambda_1\cdot\sum_{(s_1,\dots,s_n)\in S_1\times\cdots\times S_n}\frac{f_1(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}+\lambda_2\cdot\sum_{(s_1,\dots,s_n)\in S_1\times\cdots\times S_n}\frac{f_2(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}=$$

$$=\sum_{(s_1,\dots,s_n)\in S_1\times\cdots\times S_n}\frac{\lambda_1\cdot f_1(s_1,\dots,s_n)+\lambda_2\cdot f_2(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}=$$

$$=\sum_{(s_1,\dots,s_n)\in S_1\times\cdots\times S_n}\frac{f(s_1,\dots,s_n)}{N(s_1,\dots,s_n)},$$

tehár ekkor a formula $f$-re is áll.

Másodszor vegyük észre, hogy tetszőleges $(t_1,\dots,t_n)\in S_1\times\cdots\times S_n$ vektorhoz választott

$$h(x_1,\dots,x_n)=\prod_{i=1}^{n}\prod_{b\in S_i/t_i}(x_i-b)$$

függvényre igaz a tétel.

Valóban, ezen a tetszőlegesen választott $(t_1,\dots,t_n)$ vektoron $h(t_1,\dots,t_n)=N(t_1,\dots,t_n)$, az összes többi $(s_1,\dots,s_n)\in S_1\times\dots\times S_n$ vektoron $h(s_1,\dots,s_n)=0$, tehát

$$1=h_{\alpha_1\cdots\alpha_n}=\frac{h(t_1,\dots,t_n)}{N(t_1,\dots,t_n)}=\sum_{(s_1,\dots,s_n)\in S_1\times\dots\times S_n}\frac{h(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}$$

Ezek után a bizonyítás indukció $|\mathrm{Cone}(f)|$ szerint.

Ha $|\mathrm{Cone}(f)|=0$, akkor $f\equiv 0$, itt az állítás triviálisan teljesül.

Tegyük fel, hogy $|\mathrm{Cone}(f)|$ minden kisebb értékére a tétel már fennáll, és legyen $(\beta_1,\dots,\beta_n)$ maximális elem $\mathrm{Cone}(f)$-ben. Ez maximális $\mathrm{Supp}(f)$-ben is, $\mathrm{Cone}(f)$ definíciója miatt.

Ha $(\beta_1,\dots,\beta_n)=(\alpha_1,\dots,\alpha_n)$, akkor vegyünk tetszőleges $(s_1,\dots,s_n)\in S_1\times\dots\times S_n$ vektort. $h$-t válasszuk $(s_1,\dots,s_n)$-hez és tekintsük a következő polinomot:

$$\tilde{f}(x_1,\dots,x_n)=f(x_1,\dots,x_n)-f_{\alpha_1\cdots\alpha_n}\cdot\prod_{i=1}^{n}\prod_{b\in S_i/s_i}(x_i-b)=f(x_1,\dots,x_n)-f_{\alpha_1\cdots\alpha_n}\cdot h$$

Ebben a polinomban $x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}$ együtthatója 0, valamint

$$\mathrm{Cone}(\tilde{f})\subset\mathrm{Cone}(f)$$

hiszen minden $\gamma\in \mathit{Supp}(h)$-ra $\gamma\leq\alpha$, tehát $\mathit{Cone}(f)$ nem bővült és $\alpha$ már kiesett, tehát

$$|\mathrm{Cone}(\tilde{f})|<|\mathrm{Cone}(f)|$$

így $\tilde{f}$-re az indukciós feltétel szerint teljesül az állítás, és így a formula linearitása alapján $f=\tilde{f}+$ $+f_{\alpha_1\cdots\alpha_n}\cdot h$-ra is teljesül.

Most legyen $(\beta_1,\dots,\beta_n)\neq(\alpha_1,\dots,\alpha_n)$. A feltevések szerint $(\alpha_1,\dots,\alpha_n)$-nél nincs nagyobb elem $\mathrm{Supp}(f)$-ben, tehát $\mathrm{Cone}(f)$-ben sincs, így $\exists\ i$, hogy $\beta_i<\alpha_i$. Feltehetjük, hogy $\beta_1<\alpha_1$. Legyen $B_1\subset S_1$, úgy, hogy $|B_1|=\beta_1$.

Tekintsük a következő polinomot:

$$\tilde{f}=f-f_{\beta_1\ldots\beta_n}\cdot x_2^{\beta_2}x_3^{\beta_3}\cdot\ldots\cdot x_n^{\beta_n}\cdot\prod_{b\in B_1}(x_1-b).$$

Ahogy az előbb, $\mathrm{Cone}(f)$ most sem bővült, $\beta$ kiesett, tehát

$$\mathrm{Cone}(\tilde{f})\subset\mathrm{Cone}(f)$$

így $\tilde{f}$-re áll a tétel.

Ha $x_2^{\beta_2}x_3^{\beta_3}\cdot\ldots\cdot x_n^{\beta_n}\cdot\prod_{b\in B_1}(x_1-b)$-re is igaz, akkor a formula linearitásából már következik a tétel.

Mivel $\beta_1<\alpha_1$, $\left(x_2^{\beta_2}x_3^{\beta_3}\cdot\ldots\cdot x_n^{\beta_n}\cdot\prod_{b\in B_1}(x_1-b)\right)_{\alpha_1\cdots\alpha_n}$ nyilván 0.

Kiírva a formula másik felét:

$$\sum_{(s_1,\dots,s_n)\in S_1\times\dots\times S_n}\frac{s_2^{\beta_2}s_3^{\beta_3}\cdot\ldots\cdot s_n^{\beta_n}\cdot\prod_{b\in B_1}(s_1-b)}{\prod_{i=1}^{n}\prod_{b\in S_i/s_i}(s_i-b)}=$$

$$= \sum_{(s_1,\dots,s_n)\in S_1\times\dots\times S_n} \frac{\prod_{b\in B_1}(s_1-b)}{\prod_{b\in S_1/s_1}(s_1-b)} \cdot \frac{s_2^{\beta_2} s_3^{\beta_3}\cdot\ldots\cdot s_n^{\beta_n}}{\prod_{i=2}^{n}\prod_{b\in S_i/s_i}(s_i-b)} =$$

$$= \sum_{(s_1,\dots,s_n)\in S_1\times\dots\times S_n} \frac{\prod_{b\in B_1}(s_1-b)}{\prod_{b\in S_1/s_1}(s_1-b)} \cdot \prod_{i=2}^{n} \frac{s_i^{\beta_i}}{\prod_{b\in S_i/s_i}(s_i-b)} =$$

$$= \left(\sum_{s_1\in S_1} \frac{\prod_{b\in B_1}(s_1-b)}{\prod_{b\in S_1/s_1}(s_1-b)}\right) \cdot \left(\sum_{(s_2,\dots,s_n)\in S_2\times\dots\times S_n} \prod_{i=2}^{n} \frac{s_i^{\beta_i}}{\prod_{b\in S_i/s_i}(s_i-b)}\right) =$$

$$= \left(\underbrace{\sum_{s_1\in B_1} \frac{\prod_{b\in B_1}(s_1-b)}{\prod_{b\in S_1/s_1}(s_1-b)}}_{=0} + \sum_{s_1\in S_1/B_1} \frac{\prod_{b\in B_1}(s_1-b)}{\prod_{b\in S_1/s_1}(s_1-b)}\right) \cdot \left(\sum_{(s_2,\dots,s_n)\in S_2\times\dots\times S_n} \prod_{i=2}^{n} \frac{s_i^{\beta_i}}{\prod_{b\in S_i/s_i}(s_i-b)}\right) =$$

$$= \left(\sum_{s_1\in S_1/B_1} \prod_{b\in(S_1/B_1)/s_1} (s_1-b)^{-1}\right) \cdot \left(\sum_{(s_2,\dots,s_n)\in S_2\times\dots\times S_n} \prod_{i=2}^{n} \frac{s_i^{\beta_i}}{\prod_{b\in S_i/s_i}(s_i-b)}\right)$$

Mivel $|B_1| = \beta_1 < \alpha_1$ és $|S_1| = \alpha_1 + 1$, $|S_1/B_1| \geq 2$, így alkalmazható a 4.7 Lemma:

$$\sum_{s_1\in S_1/B_1} \prod_{b\in(S_1/B_1)/s_1} (s_1-b)^{-1} = 0.$$

$\square$

A tétel magában is értékes, de a segítségével a 4.4 Tételre is kapunk egy új bizonyítást:

*Bizonyítás.* Tegyük fel, hogy $(\alpha_1, \alpha_2, \dots, \alpha_n)$ maximális elem $\mathrm{Supp}(f)$-ben. Ekkor $f_{\alpha_1\dots\alpha_n} \neq 0$. Az Együttható-formula szerint tetszőleges $S_1, \cdots, S_n \subseteq T$, $|S_i| = \alpha_i + 1$ halmazokra

$$0 \neq f_{\alpha_1\cdots\alpha_n} = \sum_{(s_1,\dots,s_n)\in S_1\times\dots\times S_n} \frac{f(s_1,\dots,s_n)}{N(s_1,\dots,s_n)}$$

tehát nem lehet $f(s_1,\dots,s_n) = 0$ minden $(s_1,\dots,s_n) \in S_1\times\dots\times S_n$-re.

$\square$

# 5. fejezet

# Alkalmazások

Ebben a fejezetben az előző két fejezet tételeinek néhány alkalmazását mutatom be. Először számelméleti és algebrai alkalmazásokról lesz szó [2] és [4], majd gráfelméleti alkalmazásokról [2] és [5] alapján.

## 5.1. Számelméleti, algebrai alkalmazások

**5.1. Tétel** (Cauchy-Davenport)**.** *Legyen $p$ prím, $A, B$ két nemüres részhalmaza $\mathbb{Z}_p$-nek. Ekkor*

$$|A+B| \geq \min\{p, |A|+|B|-1\}$$

*Bizonyítás.* Ha $|A|+|B| > p$, akkor válasszunk egy tetszőleges $z \in \mathbb{Z}_p$-t.

$$p = |\mathbb{Z}_p| \geq |A \cup (z-B)| = |A|+|z-B|-|A \cap (z-B)| = |A|+|B|-|A \cap (z-B)|$$

amiből következik, hogy $|A \cap (z-B)| \geq 1$, tehát a metszetük nem üres. Tehát létezik $a \in A, z-b \in$ $\in (z-B)$, hogy $a = z-b$ tehát $a+b = z$. Mivel $z$ tetszőleges volt, $A+B = \mathbb{Z}_p$.

Legyen $|A|+|B| \leq p$.
Indirekt tegyük fel, hogy $|A+B| \leq |A|+|B|-2$. Vegyünk olyan $C$ részhalmazát $\mathbb{Z}_p$-nek, hogy

$$A+B \subseteq C, \ |C| = |A|+|B|-2$$

Definiáljuk a következő polinomot:

$$P(x,y) = \prod_{c \in C}(x+y-c)$$

Ekkor $P(a,b) = 0$ minden $(a,b) \in A \times B$-re, mert $A+B \subseteq C$. Nézzük meg, mi az együtthatója $x^{|A|-1}y^{|B|-1}$-nek!

A zárójelek felbontásakor $|A|-1$ - szer választok $x$-et, a többire y-t, ezt $\binom{|A|+|B|-2}{|A|-1}$ féleképp tehetem meg. $\binom{|A|+|B|-2}{|A|-1} = \frac{(|A|+|B|-2)!}{(|A|-1)! \cdot (|B|-1)!}$, ahol $|A|+|B|-2, \ |A|-1, \ |B|-1 < p$, tehát

$$\binom{|A|+|B|-2}{|A|-1} \neq 0.$$

Így teljesülnek az 3.2 Tétel feltételei, $\exists \ (a,b) \in A \times B$, hogy $f(a,b) \neq 0$. Ellentmondás. $\square$

A fenti tétel rokona a következő Erdős-Heilbronn tétel:

**5.2. Tétel** (Erdős-Heilbronn)**.** *Legyen p prím, A nemüres részhalmaza* $\mathbb{Z}_p$*-nek. Ekkor*

$$|\{a+a^{'} \mid a, a^{'} \in A, a \neq a^{'}\}| \ \geq \ \min\{p,\ 2|A|-3\}$$

*Bizonyítás.* A $p=2$ eset triviális. Tegyük fel, hogy $p>2$!

Ha $2|A|-3 \geq p$, akkor tetszőleges $g \in \mathbb{Z}_p$-re

$$p = |\mathbb{Z}_p| \geq |A \cup (g-A)| = |A| + |g-A| - |A \cap (g-A)| = 2|A| - |A \cap (g-A)|$$

miatt $|A \cap (g-A)| \geq 3$, tehát létezik $a \in A, g-a^{'} \in (g-A)$, úgy, hogy $a \neq \frac{g}{2}$. Egy ilyen $a$-t választva $a = g-a^{'},\ a \neq a^{'}$, vagyis $g = a+a^{'}$. Mivel $g$ tetszőleges volt,

$$\{a+a^{'} \mid a, a^{'} \in A, a \neq a^{'}\} = \mathbb{Z}_p$$

Másodszor legyen $2|A|-3<p$ és indirekt tegyük fel, hogy a tétel nem igaz. Vegyünk egy $C$ halmazt, hogy

$$\{a+a^{'} \mid a, a^{'} \in A, a \neq a^{'}\} \subseteq C,\ |C| = 2|A|-4$$

Definiáljuk a következő polinomot:

$$P(x,y) = (x-y)\prod_{c \in C}(x+y-c)$$

Vegyük észre, hogy $P(x,y)=0$ minden $(x,y) \in A^2$-ra. Nézzük, mit tudunk $P$ együtthatóiról!

Ha $i+j=|C|+1$, akkor $x^i y^j$ együtthatója $\binom{|C|}{i-1} - \binom{|C|}{i}$, mert minden zárójelből vagy $x$-et vagy $y$-t kell választanom, és hogy egy választás $+1$-gyel vagy $-1$-gyel járul hozzá az együtthatóhoz, csak attól függ, hogy az utolsó zárójelből $x$-et vagy $y$-t választottam.
Átalakítással a következő formába hozhatom:

$$\binom{|C|}{i-1} - \binom{|C|}{i} = \frac{(i-j)|C|}{i!\,j!}$$

Ebből látszik, hogy $x^i y^j$ együtthaója pontosan akkor 0, ha $i=j$, vagyis $i=j=\frac{|C|+1}{2}$ ($\mathbb{Z}_p$-ben). Vagyis $x^{|A|-2}y^{|A|-1}$ és $x^{|A|-1}y^{|A|-2}$ közül legalább az egyik szerepel a polinomban. Tehát az 3.2 Tétel értelmében létezik $(x,y) \in A^2$, ahol $P(x,y) \neq 0$. Ellentmondás.

□

A következőkben az előző két tétel kiterjesztéséről lesz szó. Mindkét összeg leírható a következő általános formában:

**5.3. Definíció.** *Legyen p prím,* $A_1, A_2, \ldots, A_k$ *nemüres részhalmazai* $\mathbb{Z}_p$*-nek. Legyen*

$$h(x_1, x_2, \ldots, x_k) \in \mathbb{Z}_p[x_1, x_2, \ldots, x_k].$$

*Vezessük be az*

$$\oplus_h \sum_{i=1}^{k} A_i = \{a_1+a_2+\cdots+a_k \mid a_i \in A_i,\ h(a_1, a_2, \ldots, a_k) \neq 0\}$$

*jelölést.*

A Cauchy-Davenport tételnél pl. $h \equiv 1$, az Erdős-Heilbronn tételnél $h = x_1 - x_2$ megfelelő.

Adódik a kérdés: mit mondhatunk ezen halmazok elemszámáról?

A témakör egyik általános eredménye a következő:

**5.4. Tétel.** *Legyen p prím, $A_1, A_2, \ldots, A_k$ nemüres részhalmazai $\mathbb{Z}_p$-nek. Legyen $h(x_1, x_2, \ldots, x_k)$ $\mathbb{Z}_p$ feletti polinom. Legyen $|A_i| = c_i + 1$, minden $0 \le i \le k$-ra. Legyen $m = \sum_{i=1}^k c_i - \deg(h)$. Ha a $\prod_{i=1}^k x_i^{c_i}$ monom együtthatója nem nulla az*

$$(x_1 + x_2 + \ldots + x_k)^m \cdot h(x_1, \ldots, x_k)$$

*polinomban (és $\mathbb{Z}_p$ felett), akkor*

$$\left| \oplus_h \sum_{i=1}^k A_i \right| \ge \min\{p,\ m+1\}$$

*Bizonyítás.* Az $m+1 > p$ eset triviális, csak $m < p$-vel foglalkozunk.

Indirekt tegyük fel, hogy a tétel nem igaz és vegyünk egy olyan $E$ halmazát $\mathbb{Z}_p$-nek, melyre

$$\oplus_h \sum_{i=1}^k A_i \subseteq E,\ |E| = m$$

Definiáljuk a következő $P$ polinomot:

$$P(x_1, x_2, \ldots, x_k) = h(x_1, x_2, \ldots, x_k) \cdot \prod_{e \in E} (x_1 + x_2 + \ldots + x_k - e)$$

Vegyük észre, $P(a_1, a_2, \ldots, a_k) = 0$ minden $(a_1, a_2, \ldots, a_k) \in A_1 \times \ldots \times A_k$-ra, ugyanis ha

$$h(a_1, a_2, \ldots, a_k) \ne 0, \text{ akkor } a_1 + a_2 + \ldots + a_k \in \oplus_h \sum_{i=1}^k A_i,$$

tehát

$$\prod_{e \in E} (a_1 + a_2 + \ldots + a_k - e) = 0$$

Vegyük észre azt is, hogy $\deg(P) = m + \deg(h) = \sum_{i=1}^k c_i$, és így a $\prod_{i=1}^k x_i^{c_i}$ monom együtthatója $P$-ben ugyan az, mint $(x_1 + x_2 + \ldots + x_k)^m \cdot h(x_1, \ldots, x_k)$-ban, tehát a feltevések szerint nem nulla.

Így az 3.2 Tétel értelmében létezik $(a_1, a_2, \ldots, a_k) \in A_1 \times A_2 \times \ldots \times A_k$, hogy $P(a_1, a_2, \ldots, a_k) \ne 0$. Ellentmondás.

□

Ebben a tételben az ellentmondást a 3.2 Tétel hozta. Ha a 4.4 Tételt használjuk, a bizonyítás hasonlóan működik, hasonló feltételt is kapunk, amely bonyolultabb, de erősebb.
Először jöjjön egy tétel, amire szükségünk lesz:

**5.5. Tétel** (Multinomiális tétel). *Ha $m < p$, akkor*

$$(x_1 + x_2 + \ldots + x_k)^m = \sum_{\substack{0 \le i_1, i_2, \ldots, i_k \\ i_1 + i_2 + \ldots + i_k = m}} \frac{m!}{i_1!\, i_2! \cdot \ldots \cdot i_k!} x_1^{i_1} x_2^{i_2} \cdot \ldots \cdot x_k^{i_k},$$

$$\mathit{Supp}\left((x_1 + x_2 + \ldots + x_k)^m\right) = \{(i_1, i_2, \ldots, i_k) \mid 0 \ge i_j,\ i_1 + i_2 + \ldots + i_k = m\}$$

*Bizonyítás.* A zárójelek felbontásakor minden lépésben egy változót választok, így nyilvánvaló, hogy minden monomban a fokszámok összege $m$. Vegyünk $0 \le i_1, i_2, \ldots, i_k,\ i_1 + \ldots + i_k = m$ számokat és nézzük, mennyi az együtthatója az $\prod_{j=1}^k x_j^{i_j}$ monomnak!
Megtehetem, hogy először $x_1$-ket választom ki, majd az $x_2$-ket, és így tovább. Így a monom együtthatója

$$\binom{m}{i_1}\binom{m - i_1}{i_2}\binom{m - i_1 - i_2}{i_3} \cdots \binom{m - i_1 - i_2 - \ldots - i_{k-2}}{i_{k-1}}$$

amit átalakítva

$$\frac{m!}{i_1!\,(m-i_1)!}\cdot\frac{(m-1_1)!}{i_2!\,(m-i_1-i_2)!}\cdot\frac{(m-i_1-i_2)!}{i_3!\,(m-i_1-i_2-i_3)!}\cdot\ldots\cdot\frac{(m-i_1-i_2-\ldots-i_{k-2})}{i_{k-1}!\,(m-i_1-i_2-\ldots-i_{k-1})!}$$

A nevező második szorzótényezője épp a következő számláló, tehát kiütik egymást, egészen az utolsó tényezőig, amikor nincs következő nevező. Marad:

$$\frac{m!}{i_1!\,i_2!\cdot\ldots\cdot i_k!}$$

Valamint ezek egyike sem nulla $\mathbb{Z}_p$-ben, mivel $0\le i_1,i_1,\ldots,i_k\le m<p$. □

**5.6. Tétel.** *Legyen p prím, $A_1,A_2,\ldots,A_k$ nemüres részhalmazai $\mathbb{Z}_p$-nek. Legyen $h(x_1,x_2,\ldots,x_k)$ $\mathbb{Z}_p$ feletti polinom. Legyen $|A_i|=c_i+1$, minden $1\le i\le k$-ra. Legyen $m$ olyan szám, amelyre a $\prod_{i=1}^k x_i^{c_i}$ monom maximális elem*

$$\mathit{Supp}\,((x_1+x_2+\ldots+x_k)^m h(x_1,\ldots,x_k))\text{ -}\mathit{ban}.$$

*Ekkor*

$$\left|\oplus_h\sum_{i=1}^k A_i\right| \;\ge\; \min\{p,\ m+1\}$$

*Bizonyítás.* Az $m+1>p$ eset triviális, újfent csak az $m<p$ esettel foglalkozunk.

Indirekt tegyük fel, hogy a tétel nem igaz és vegyünk egy olyan $E$ halmazát $\mathbb{Z}_p$-nek, melyre

$$\oplus_h\sum_{i=1}^k A_i\subseteq E,\ |E|=m$$

Definiáljuk a következő $P$ polinomot:

$$P(x_1,x_2,\ldots,x_k)=h(x_1,x_2,\ldots,x_k)\cdot\prod_{e\in E}(x_1+x_2+\ldots+x_k-e)$$

Vegyük észre, $P(a_1,a_2,\ldots,a_k)=0$ minden $(a_1,a_2,\ldots,a_k)\in A_1\times\ldots\times A_k$-ra, ugyanis ha

$$h(a_1,a_2,\ldots,a_k)\ne 0,\ \text{akkor } a_1+a_2+\ldots+a_k\in\oplus_h\sum_{i=1}^k A_i,$$

tehát

$$\prod_{e\in E}(a_1+a_2+\ldots+a_k-e)=0$$

Vegyük észre azt is, hogy

$$\mathrm{Supp}(P)\subseteq\mathrm{Cone}((x_1+x_2+\ldots+x_k)^m h(x_1,\ldots,x_k)),$$

ugyanis

$$\mathrm{Supp}\left(\prod_{e\in E}(x_1+x_2+\ldots+x_k-e)\right)=\{(i_1,i_2,\ldots,i_k)\mid i_j\ge 0,\ i_1+i_2+\ldots+i_k\le m\},$$

tehát

$$\mathrm{Supp}(P)=\{(\alpha_1+i_1,\alpha_2+i_2,\ldots,\alpha_k+i_k)\mid \underline{\alpha}\in\mathrm{Supp}(h),\ i_j\ge 0,\ i_1+i_2+\ldots+i_k\le m\},$$

valamint az előző lemma miatt

$$\mathrm{Supp}\,(h(x_1,\ldots,x_k)\cdot(x_1+x_2+\ldots+x_k)^m)=$$

$$= \{(\alpha_1+i_1, \alpha_2+i_2, \dots, \alpha_k+i_k) \mid \underline{\alpha} \in \mathrm{Supp}(h),\ 0 \geq i_j,\ i_1+i_2+\ldots+i_k = m\}.$$

Tehát ha a $\prod_{i=1}^k x_i^{c_i}$ monom maximális elem

$$\mathrm{Supp}\left((x_1+x_2+\ldots+x_k)^m h(x_1,\dots,x_k)\right)\text{-ban},$$

akkor $P$-ben is.

Így az 4.4 Tétel értelmében létezik $(a_1, a_2, \dots, a_k) \in A_1 \times A_2 \times \ldots \times A_k$, hogy $P(a_1, a_2, \dots, a_k) \neq 0$. Ellentmondás. □

Ennek a tételnek speciális esete a 5.4 Tétel, mert ha egy $\underline{\alpha} \in \mathrm{Supp}(f)$-re $\sum_{i=1}^k \alpha_i = \deg(f)$, akkor $\underline{\alpha}$ automatikusan maximális elem $\mathrm{Supp}(f)$-ben, hiszen ha lenne olyan $\underline{\beta} \in \mathrm{Supp}(f)$, amire $\underline{\alpha} < \underline{\beta}$, akkor $\deg(f) = \sum_{i=1}^k \alpha_i < \sum_{i=1}^k \beta_i$ teljesülne.

A tétel feltétele egyszerűsíthető: olyan alakra hozható, ahol nem kell elvégezni a polinom-szorzást. Vizsgáljuk meg, hogy mik lesznek a maximális elemei

$$\{(\alpha_1+i_1, \alpha_2+i_2, \dots, \alpha_k+i_k) \mid \underline{\alpha} \in \mathrm{Supp}(h),\ 0 \leq i_j,\ i_1+i_2+\ldots+i_k = m\}\text{-nek!}$$

A következőkben $\underline{i}, \underline{j} \in \mathbb{N}^k$ vektorok, amelyek koordináta-összege $m$, $\underline{i}$ legyen fix. $\underline{\alpha}, \underline{\beta} \in \mathrm{Supp}(h)$, és $\underline{c} = \underline{\alpha} + \underline{i}$.

**5.7. Lemma.** *Létezik $\underline{j}$, hogy $\underline{j} \ \geq \ \underline{c} - \underline{\beta} \iff \sum_{c_i - \beta_i > 0} \ c_i - \beta_i \leq m$.*

*Bizonyítás.*

Ha $\sum_{c_i-\beta_i>0} \ c_i - \beta_i \leq m$, akkor

$$j_i := \begin{cases} 0, \text{ ha } c_i - \beta_i \leq 0 \\ c_i - \beta_i, \text{ egyébként} \end{cases}$$

Ekkor

$$\underline{j} \ \geq \ \underline{c} - \underline{\beta},$$

az egyetlen baj az lehet, ha $\sum_{i=1}^k j_i < m$. Ez esetben növeljük mondjuk a $k$-adik koordinátát.

Ha létezik $\underline{j}$, hogy $\underline{j} \ \geq \ \underline{c} - \underline{\beta}$, akkor

$$\beta_i^{'} := \begin{cases} 0, \text{ ha } c_i - \beta_i \leq 0 \\ c_i - \beta_i, \text{ egyébként} \end{cases}$$

Ekkor

$$\underline{c} - \underline{\beta} \ \leq \ \underline{\beta^{'}} \ \leq \ \underline{j},$$

vagyis

$$\sum_{c_i - \beta_i > 0} c_i - \beta_i \ = \ \sum_{i=1}^k \beta_i^{'} \ \leq \ \sum_{i=1}^k j_i = m$$

□

**5.8. Lemma.** *Az $\prod_{i=1}^k x_i^{c_i}$ monom együtthatója $(x_1+x_2+\ldots+x_k)^m h(x_1,\dots,x_k)$-ban*

$$\sum_{\substack{\underline{\alpha} \in Supp(h),\ \alpha_i \leq c_i, \\ \sum \underline{c} - \sum \underline{\alpha} = m}} \frac{h_{\underline{\alpha}} \cdot m!}{(c_1-\alpha_1)! \cdot (c_2-\alpha_2)! \cdot \ldots \cdot (c_k-\alpha_k)!}$$

*Bizonyítás.* Szorzás közben úgy jöhet létre $\prod_{i=1}^k x_i^{c_i}$ monom, ha

$$\underline{\alpha} \in \mathrm{Supp}(h),\ \ \alpha_i \le c_i,\ \ \sum_{i=1}^k c_i - \alpha_i = m \text{ monomot szorzok } \underline{c} - \underline{\alpha}\text{-val.}$$

Az $\alpha$-nak megfelelő monom együtthatója $h_{\underline{\alpha}}$, $\quad 0 \le \underline{c} - \underline{\alpha},\ \ \sum_{i=1}^k c_i - \alpha_i = m$, tehát

$$\underline{c} - \underline{\alpha} \in \mathrm{Supp}((x_1 + \ldots + x_k)^m),$$

és a 5.5 Lemma után az együtthatója

$$\frac{m!}{(c_1 - \alpha_1)! \cdot (c_2 - \alpha_2)! \cdot \ldots \cdot (c_k - \alpha_k)!}$$

□

Ezek után a 5.6 Tétel a következő alakba írható:

**5.9. Tétel.** *Legyen p prím, $A_1, A_2, \ldots, A_k$ nemüres részhalmazai $\mathbb{Z}_p$-nek. Legyen $h(x_1, x_2, \ldots, x_k)$ $\mathbb{Z}_p$ feletti polinom. Legyen $|A_i| = c_i + 1$, minden $1 \le i \le k$-ra. Legyen $\underline{\alpha} \in$ Supp$(h)$ olyan, amelyre $\underline{\alpha} \ \le\ \underline{c}$,*

$$\min\left\{ \sum_{c_i - \beta_i > 0} c_i - \beta_i \mid \underline{\beta} \in \mathit{Supp}(h),\ \ \underline{\beta} \ne \underline{\alpha} \right\} > \sum_{i=1}^k c_i - \sum_{i=1}^k \alpha_i \quad (1)$$

*és*

$$\sum_{\substack{\underline{\beta} \in \mathit{Supp}(h),\ \underline{\beta}\ \le\ \underline{c} \\ \sum_{i=1}^k \beta_i = \sum_{i=1}^k \alpha_i}} h_{\underline{\beta}} \cdot \frac{\left(\sum_{i=1}^k c_i - \sum_{i=1}^k \alpha_i\right)!}{(c_1 - \beta_1)! \cdot (c_2 - \beta_2)! \cdot \ldots \cdot (c_k - \beta_k)!} \ne 0. \quad (2)$$

*Legyen $m = \sum_{i=1}^k c_i - \sum_{i=1}^k \alpha_i$. Ekkor*

$$\left| \oplus_h \sum_{i=1}^k A_i \right| \ \ge\ \min\{p,\ m+1\}$$

*Bizonyítás.* A 5.8 Lemma szerint (2) azzal ekvivalens, hogy $\underline{c} \in \mathrm{Supp}((x_1{+}x_2{+}\ldots{+}x_k)^m h(x_1, \ldots, x_k))$, a 5.7 Lemma alapján (1) pedig azzal, hogy $\underline{c}$ maximális elem $\mathrm{Supp}((x_1{+}x_2{+}\ldots{+}x_k)^m h(x_1, \ldots, x_k))$-ban. Így teljesülnek a 5.6 Tétel feltételei. □

Jöjjön egy példa, hogy lássuk, tényleg erősebb állítást kaptunk.

Legyen $A_1, A_2, A_3 \subset \mathbb{Z}_{19}$, $|A_1| = 14, |A_2| = 4, |A_3| = 4$. Legyen $h(x_1, x_2, x_3) = x_1^8 x_2 x_3^2 + x_1 x_2^7 x_3^{10}$. $\sum_{i=1}^3 c_i = 19,\ \deg(h) = 18$. Erre a példára a 5.4 Tétel szerint a következő becslést kapjuk:

$$\left| \oplus_h \sum_{i=1}^k A_i \right| \ \ge\ \min\{19, 2\} = 2.$$

Most nézzük, mit kezdhetünk a 5.9 Tétellel!
Legyen $\underline{\alpha} = (8{,}1{,}2)$. Ekkor

$$\sum_{\substack{\underline{\beta} \in \mathrm{Supp}(h),\ \underline{\beta}\ \le\ \underline{c} \\ \sum_{i=1}^k \beta_i = \sum_{i=1}^k \alpha_i}} h_{\underline{\beta}} \cdot \frac{\left(\sum_{i=1}^k c_i - \sum_{i=1}^k \alpha_i\right)!}{(c_1 - \beta_1)! \cdot (c_2 - \beta_2)! \cdot \ldots \cdot (c_k - \beta_k)!} = 1 \cdot \frac{8!}{5! \cdot 2! \cdot 1!} \ne 0,$$

$$\min\left\{\sum_{c_i-\beta_i>0} c_i-\beta_i \mid \underline{\beta}\in \mathrm{Supp}(h),\ \underline{\beta}\neq\underline{\alpha}\right\}=12>8=\sum_{i=1}^{k} c_i-\sum_{i=1}^{k}\alpha_i,$$

vagyis alkalmazható a 5.9 Tétel,

$$\left|\oplus_h \sum_{i=1}^{k} A_i\right| \ \geq\ \min\{19,9\}=9.$$

A következő részben elhagyjuk a témakört és két másik alkalmazást mutatok be.

**5.10. Definíció.** *Legyen* $(a_{i,j})=A\in T^{n\times n}$ *mátrix,* $S(n)$ *az* $1,2,\ldots,n$ *számok permutációinak halmaza. A*

$$Per(A)=\sum_{\sigma\in S(n)}\prod_{i=1}^{n} a_{i,\sigma(i)}$$

*számot az* $A$ *mátrix permanensének nevezzük.*

**5.11. Tétel** (Permanens lemma)**.** *Legyen* $T$ *tetszőleges test,* $A\in T^{n\times n}$*. Tegyük fel, hogy* $Per(A)\neq 0$*. Ekkor tetszőleges* $b=(b_1,b_2,\ldots,b_n)\in T^n$ *vektorhoz és* $S_1,S_2,\ldots,S_n$*,* $|S_i|=2$ *halmazokhoz* $\exists\ x=(x_1,x_2,\ldots,x_n)\in S_1\times\cdots\times S_n$*, hogy*

$$(Ax)_i\neq b_i, \forall 1\leq i\leq n.$$

*Bizonyítás.* Legyen

$$P(x_1,x_2,\ldots,x_n)=\prod_{i=1}^{n}\left[\left(\sum_{j=1}^{n} a_{i,j}x_j\right)-b_i\right]$$

Jobban kiírva:

$$\prod_{i=1}^{n}\left[\left(\sum_{j=1}^{n} a_{i,j}x_j\right)-b_i\right]=\prod_{i=1}^{n}\left[\left(a_{i,1}x_1+a_{i,2}x_2+\ldots+a_{i,n}x_n-b_n\right)\right],$$

Ebből látszik, $\deg(P)=n$. Nézzük a $\prod_{i=1}^{n} x_i$-s tag együtthatóját!

Úgy kapok $\prod_{i=1}^{n} x_i$-t, hogy a szorzás közben minden változót pontosan egyszer választok. Minden választás megfelel az $1,2,\ldots,n$ számok egy $\sigma$ permutációjának:

$$\sigma(i)=\text{ annak a változónak a sorszáma, amelyiket az i-edik zárójelből választok}$$

és természetesen minden permutációnak megfelel egy választás, hasonló módon, tehát $\prod_{i=1}^{n} x_i$ együtthatója

$$\sum_{\sigma\in S(n)}\prod_{i=1}^{n} a_{i,\sigma(i)}=\mathrm{Per}(A),$$

ami a feltevésünk szerint nem nulla.

Teljesülnek az 3.2 Tétel feltételei, vagyis $\exists\ (x_1,\ldots,x_n)\in S_1\times\cdots\times S_n$, hogy $P(x_1,\ldots,x_n)\neq 0$.

Vegyük észre, ez éppen azt jelenti, hogy

$$\forall 1\leq i\leq n \text{ -re } \left(\sum_{j=1}^{n} a_{i,j}x_j\right)-b_i=(Ax)_i-b_i\neq 0,\Longleftrightarrow (Ax)_i\neq b_i.$$

□

A tétel egy érdekes alkalmazása a következő:

**5.12. Tétel** (Erdős - Ginzburg - Ziv)**.** *Legyen p prím.* $\mathbb{Z}_p$ *tetszőleges* $2p-1$ *eleméből kiválasztható* $p$*, hogy azok összege* $0$ *(*$\mathbb{Z}_p$*-ben).*

*Bizonyítás.* Számozzuk meg az elemeket 1-től $2p-1$-ig. Feltehető, hogy növekvő sorban vannak:

$$0 \le a_1 \le a_2 \le \ldots \le a_{2p-1} < p$$

Ha valamely $i$-re $a_i = a_{i+p-1}$, akkor

$$a_i \le a_{i+1} \le \ldots \le a_{i+p-1} = a_i \implies a_i = a_{i+1} = \ldots = a_{i+p-1}$$

tehát

$$a_i + a_{i+1} + \ldots + a_{i+p-1} = p \cdot a_i = 0.$$

Egyébként legyen

$$A = \mathbf{1}^{(p-1)\times(p-1)},$$

legyen

$$S_i = \{a_i, a_{i+p-1}\},$$

és $(b_1, b_2, \ldots, b_{p-1})$ álljon $\mathbb{Z}_p$ elemeiből, kivéve $-a_{2p-1}$-t.

$\mathrm{Per}(A) = (p-1)!$ ami Wilson tétele szerint $(p-1)! \equiv -1$, tehát a 5.12 Tétel szerint tudok úgy választani $s_1 \in S_1, s_2 \in S_2, \ldots s_{p-1} \in S_{p-1}$-t, hogy

$$\sum_{j=1}^{n} s_j \ne b_i, \;\; 1 \le i \le n,$$

tehát

$$\sum_{j=1}^{n} s_j = -a_{2p-1}$$

vagyis

$$\sum_{j=1}^{n} s_j + a_{2p-1} = 0.$$

□

Végül jöjjön egy alkalmazás a "geometria" köréből.

**5.13. Tétel** (Füredi Z. - N. Alon)**.** *Legyenek* $H_1, H_2, \ldots, H_m$ *olyan hipersíkok* $\mathbb{R}^n$ *− ben, hogy pontosan egy kivétellel a* $\{0,1\}^n$ *egységkocka minden csúcsát fedik. Ekkor* $m \ge n$*.*

*Bizonyítás.* Feltehető, hogy a kimaradó csúcs a csupa nulla vektor, mert ha egy másik csúcs maradt ki, pl. az $(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$ pont körüli forgatással az olyan rendszert kaphatunk, ahol az origó marad ki.

Jelöljük $(a, b)$-vel $a, b \in \mathbb{R}^n$ vektorok skaláris szorzatát. Legyen $(a_i, x) = b_i$ a $H_i$ hipersíkot definiáló egyenlet. Vegyük észre, hogy egyik $b_i$ sem lehet nulla, mert különben a nullvektor kielégítené.

Ezek után tegyük fel indirekt, hogy $m < n$ darab hipersíkkal is meg lehet csinálni a kérdéses fedést. Tekintsük a következő $P$ polinomot:

$$P(x) = (-1)^{n+m}\left(\prod_{j=1}^{m} b_j\right)\cdot\left(\prod_{i=1}^{n}(x_i-1)\right)-\prod_{i=1}^{m}[(a_i,x)-b_i].$$

Először vegyük észre, hogy $P$ minden $x \in \{0,1\}^n$ vektoron eltűnik, hiszen ha $x = (0,0,\dots,0)$, akkor

$$P(x) = (-1)^{n+m}\prod_{j=1}^{m} b_j\cdot(-1)^n-(-1)^m\prod_{i=1}^{m} b_i = (-1)^m\prod_{j=1}^{m} b_j-(-1)^m\prod_{i=1}^{m} b_i,$$

Ha pedig $x$ nem a nullavektor, akkor valamely $i$-re $(x_i-1)=0$ és $(a_i,x)-b_i=0$, hiszen az $(a_i,x)$ által definiált hipersík fed egy csúcsot.

Másrészről a fokszámokat vizsgálva

$$\deg\left((-1)^{n+m}\left(\prod_{j=1}^{m} b_j\right)\cdot\left(\prod_{i=1}^{n}(x_i-1)\right)\right)=n,$$

míg

$$\prod_{i=1}^{m}[(a_i,x)-b_i]=m$$

és feltevésünk szerint $m<n$, tehát $\deg(P)=n$. Sőt, $\prod_{i=1}^{n} x_i$ együtthatója $(-1)^{n+m}\prod_{j=1}^{m} b_j$, ami nem 0.

Így teljesülnek az 3.2 Tétel feltételei, tehát $\exists x \in \{0,1\}^n$ vektor, ahol $p(x)\neq 0$. Ellentmondás.

$\square$

## 5.2. Gráfelméleti alkalmazások

A továbbiakban legyen $G=(V,E)$ egy egyszerű, irányítatlan gráf. $V(G)$ jelölje a csúcsok halmazát:

$$V=\{v_1,v_2,\dots v_n\},$$

$E(G)$ pedig az élek halmazát:

$$E(G)\subseteq\{\{v_i,v_j\}\mid v_i,v_j\in V(G)\}$$

$\vec{G}=(V,\vec{E})$ jelölje $G$ egy irányítását. $\vec{E}$ jelölje az irányított élek halmazát:

$$\vec{E}=\{v_iv_j\mid\{v_i,v_j\}\in E(G),\ \text{és az él feje } v_j\}$$

Jelöljük egy $v_i\in V(G)$ csúcs fokát $\deg_G(v_i)$, illetve $\vec{G}$-ben egy $v\in V$ csúcs befokát $\deg^+_{\vec{G}}(v)$-vel, kifokát $\deg^-_{\vec{G}}(v)$-vel. Ha egyértelmű, melyik gráfról van szó, az alsó indexet elhagyom.

A polinomok és gráfok elméletét a következő polinom kapcsolja össze:

**5.14. Definíció.** *Minden $v_i\in V(G)$ csúcsnak feleltessük meg az $x_i$ változót. Az*

$$f_G(x_1,x_2,\cdots,x_n)=\prod_{\{v_i,v_j\}\in E,\ j>i}(x_j-x_i)$$

*polinomot a $G$ gráf polinomjának nevezzük.*

Az első tétel ennek a polinomnak néhány tulajdonságáról szól, de előtte jöjjön még néhány definíció:

**5.15. Definíció.** *Egy $\vec{R}\subseteq\vec{G}$ részgráfot irányított Euler-részgráfnak hívunk, ha*

$$V(\vec{R})=V(\vec{G}),\ \ \vec{E}(\vec{R})\subseteq\vec{E}(\vec{G})$$

*valamint*

$$\forall v\in V\text{-re }\ \deg^+_{\vec{R}}(v)=\deg^-_{\vec{R}}(v).$$

**5.16. Definíció.** *Egy irányított Euler-részgráfot nevezzünk párosnak, ha páros sok élet tartalmaz, páratlannak, ha páratlan sokat.*
*Jelöljük $EE(\vec{G})$-vel a $\vec{G}$-ben levő páros Euler-részgráfok számát, $EO(\vec{G})$-vel pedig a páratlanokét.*

**5.17. Definíció.** *$G$ egy színezésén egy*

$$c:V\to\mathbb{Z}$$

*függvényt értünk. A színezés jó, ha*

$$\forall\ \{v_i,v_j\}\in E(G)\text{-re } c(v_i)\neq c(v_j).$$

**5.18. Definíció.** *$f_G$-vel kapcsolatban a "monom" és a "kifejtési tag" kifejezések alatt mást értek. Mindkettő zárójelfelbontás közben keletkezett szorzat, de mikor "kifejtési tag"-ról beszélek, számít a változók sorrendje is.*
*Pl. $x_1x_2x_1x_3x_2x_1$ és $x_1x_2x_3x_1x_2x_1$ azonos monomok, de különböző kifejtési tagok.*

Most már jöhet a tétel:

**5.19. Tétel.**

*I. Minden $f_G$-beli monomban a fokszámok összege $|E|$.*

*II. $f_G$ kifejtési tagjai kölcsönösen egyértelműen megfeleltethetőek $G$ irányításaival.*

*III. Legyen $\prod_{i=1}^{n} x_i^{c_i}$ $f_G$ egy kifejtési tagja, $\vec{G}$ a neki megfelelő irányítás. Ekkor*

$$|f_{G_{c_1 c_2 \ldots c_n}}| = |EE(\vec{G}) - EO(\vec{G})|$$

*IV. Egy $c$ pontosan akkor jó színezés, ha $f_G(c(v_1), c(v_2), \ldots, c(v_n)) \neq 0$.*

*Bizonyítás.*

I. $f_G$ zárójelei megfelelnek $G$ éleinek, tehát amikor

$$f_G(x_1, x_2, \cdots, x_n) = \prod_{\{v_i, v_j\} \in E} (x_j - x_i)\text{-t}$$

kifejtem, minden kifejtési tagban $|E|$ darab változót választok, minden zárójelből egyet.

II. Megadok egy kölcsönösen egyértelmű megfeleltetést:

$\vec{G}$-nek feleljen meg az a kifejtési tag, amikor minden zárójelből a zárójelnek megfelelő él fejének megfelelő változót választom.

Hasonlóképpen:

Egy kifejtési tagnak feleljen meg az az irányítás, amikor minden élet úgy irányítok, hogy az élnek megfelelő zárójelből választott változónak megfelelő csúcs legyen az él feje.

Ez nyilvánvalóan kölcsönösen egyértelmű.

III. Legyen $\prod_{i=1}^{n} x_i^{c_i}$ $f_G$ egy kifejtési tagja, $\vec{G}$ az előző pontban neki megfeleltetett irányítás. Hogy megtudjam, mennyi $f_{G_{c_1 c_2 \ldots c_n}}$, össze kell számolnom a megfelelő kifejtési tagokat, ezek közül hánynak lesz az együtthatója 1, hánynak $-1$, és kivonni a $-1$-esek számát a 1-esekéből.

Vegyük észre, hogy $c_i = \deg^{+}_{\vec{G}}(v_i)$! Mivel a kifejtési tagok és az irányítások kölcsönösen megfelelnek egymásnak, elég megszámolnom, hogy hány olyan $\vec{G}'$ irányítás van, amelyben

$$\deg^{+}_{\vec{G}}(v_i) = \deg^{+}_{\vec{G}'}(v_i), \;\; 0 \leq i \leq n$$

és ezzel megszámoltam azokat a kifetési tagokat, amelyekben az $x_i$ változó $c_i$-szer szerepel.

Nézzük, milyen összefüggés van közöttük!

Vegyünk a feltételeknek megfelelő különböző $\vec{G}$ és $\vec{G}'$-t. Ekkor van olyan éle $\vec{G}'$-nek, amit $\vec{G}$-től eltérően van irányítva. Fordítsuk meg! Ekkor a két csúcs ki- és befoka, amelyek között fut, eltér $\vec{G}$-től. Tehát a csúcsoknak van egy-egy másik éle, ami $\vec{G}$-től eltérően van irányítva. Valamelyiket megforgatva egy új csúcs kerül ugyan ebbe helyzetbe. Ezt addig tudom folytatni, ameddig visszaérek a kezdeti csúcshoz. Ekkor vagy minden él úgy van irányítva, mint $\vec{G}$-ben, vagy újrakezdhetem az algoritmust, de ekkor az előzőekben megforgatott élekhez már nem kell nyúlnom, azok már $\vec{G}$-vel egyezően vannak irányítva. Miven véges sok él van, eljutok $\vec{G}$-hez.

Vegyük azon élek részgráfját, amelyeket megforgattam!

A fázisok egymástól éldiszjunktak, tehát a kapott gráf az egy-egy fázisból kapott gráfok uniója. Egy fázisban ha egy csúcsra beléptem, onnan ki is léptem, tehát egy fázisban minden csúcs ki- és befoka egyenlő. Ebből az következik, hogy a forgatott élek gráfja $\vec{G}$-nek irányított Euler-részgráfja.

Másrészről nyilvánvaló, hogy ha egy irányított Euler-részgráfon változtatom meg az élek irányát, akkor a ki- és befokok nem változnak. Tehát pontosan annyi megfelelő kifejtési tag van, ahány irányított Euler-részgráfja a hozzá tartozó $\vec{G}$-nek.

Vegyük észre, hogy annyi zárójelből választok másik változót, ahány élnek megfordítottam az irányítását, és minden eltérő választás $-1$-gyel való szorzást von maga után. Tehát nem tudom, hogy a $\vec{G}$-hez tartozó kifejtési tag együtthatója 1 vagy $-1$, de azt tudom, hogy ha egy páros Euler-részgráfon cserélek irányítást, akkor ugyanazt a monomot kapom, ugyanazzal az együtthatóval, ha pedig egy páratlan Euler-részgráfon cserélek, akkor ugyan azt a monomot kapom, $-1$-szeres együtthatóval. Ebből már látszik, hogy

$$|f_{G_{c_1c_2\ldots c_n}}| = |EE(\vec{G}) - EO(\vec{G})|$$

IV. Definíció szerint $c$ pontosan akkor jó színezés, ha szomszédos csúcsokhoz különböző számokat rendel. Ezek szerint $f_G$-ben egyik tényező sem 0, így a szorzatuk sem lehet 0.

□

A Nullstellensatznak sok használati módja van a gráfelméleten belül. Én a színezéssel kapcsolatos eredményekből mutatok néhányat. Azon belül gráfok listaszínezéséről lesz szó elsősorban:

**5.20. Definíció.** *Legyen $f : V(G) \to \mathbb{N}$ függvény. Azt mondjuk, hogy $G$ $f$-listaszínezhető, ha tetszőleges*

$$S(v_i) \subset \mathbb{Z},\ v_i \in V(G),\ |S(v_i)| = f(v_i)$$

*halmazokhoz létezik jó $c$ színezés, hogy*

$$c(v_i) \in S(v_i),\ v_i \in V(G)$$

Szavakra fordítva: tetszőleges $f(v_i)$ elemszámú listát előírva minden $v_i \in V(G)$-re, létezik jó színezés a listáról.

**5.21. Definíció.** *Azt mondjuk, hogy a $G$ gráf $k$-listaszínezhető, ha $f$-listaszínezhető az $f \equiv k$ függvénnyel.*

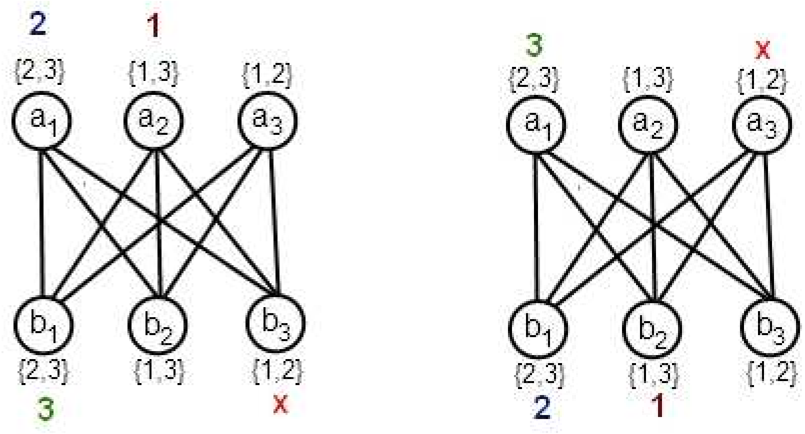
**5.22. Definíció.** *ch(G) az a legkisebb $k$ természetes szám, amelyre $G$ $k$-listaszínezhető.*

A $k$-színnel való színezés felfogható lista-színezésként, ahol minden csúcsra az $S(v_i)$=$\{1,2,\ldots,k\}$ listát írom elő, tehát a színezés speciális esete a lista-színezésnek. Hogy lássuk, a fogalom valóban erősebb, nézzük a következő példát:

Legyen $G = K_{3,3}$, ahol a csúcsokat kivételesen nevezzük $\{a_1, a_2, a_3; b_1, b_2, b_3\}$-nak.
Legyen $S(a_i) = S(b_i) = \{1,2,3\} \setminus \{i\}$. Megmutatjuk, hogy $K_{3,3}$ nem színezhető a megadott listáról.

Ha $a_1$-nek 2-est adok, akkor akkor $b_1$-nek 3-ast kell adnom, akkor $a_2$-nek szükségszerűen 1-es jut és $b_3$-nak nem marad szín.

Hasonlóan, ha $a_1$-nek 3-ast adok, akkor $b_1$-nek 2-est kell adnom $b_2$-nek pedig szükségszerűen 1-es jut és $a_3$-nak nem marad szín.




Tehát összefoglalva:

$$\chi(G) \leq \mathrm{ch}(G)$$

A lista-színezés témakör egyik fő eredménye a Nullstellensatz segítségével a következő:

**5.23. Tétel.** *Legyen $\vec{G}$ egy olyan irányítása $G$-nek, ahol $EE(\vec{G}) \neq EO(\vec{G})$. Ekkor $G$ $f$-színezhető tetszőleges $f(v_i) \geq \deg^+(v_i)+1$ függvénnyel.*

*Bizonyítás.* A 5.16 Tételből tudjuk, hogy minden monom foka

$$\deg(f_G) = |E|, \text{ és hogy a } \prod_{i=1}^{n} x_i^{\deg^+_{\vec{G}}(v_i)}$$

monom együtthatójának abszolútértéke $\left|EE(\vec{G}) - EO(\vec{G})\right|$, ami feltevésünk szerint nem 0. Így tetszőleges $|S_i| \leq \deg^+_{\vec{G}}(v_i)+1$ halmazokkal teljesülnek az 3.2 Tétel feltételei, tehát létezik $(s_1, s_2, \ldots, s_n) \in$ $\in S_1 \times S_2 \times \ldots \times S_n$, hogy $f_G(s_1, s_2, \ldots, s_n) \neq 0$, ami megfelel egy jó színezésnek. □

Ennek a tételnek a segítségével beláthajuk *Brooks* tételének lista-színezésre vonatkozó változatát. A bizonyítás Jan Hladkÿ Daniel Král' és Uwe Schauz [5] eredménye. Először jöjjön pár definíció:

**5.24. Definíció.** *G egy 2-összefüggő, feszített részgráfját blokknak nevezzük.*

**5.25. Definíció.** *Az olyan gráfot, amelynek minden blokkja vagy egy teljes gráf, vagy egy páratlan kör Gallai-fának nevezzük.*

**5.26. Definíció.** *Legyen $G$ összefüggő. Elvágó csúcshalmaznak nevezünk egy olyan $V^{'} \subset V(G)$ halmazt, amelyre $V(G) \setminus V^{'}$ csúcsok által feszített gráf nem összefüggő.*

A következő lemma segít a bizonyításban:

**5.27. Lemma.** *Minden összefüggő gráfnak, ami nem egy Gallai-fa, van olyan feszített részgráfja, ami egy páros kör, legfeljebb egy húrral.*

*Bizonyítás.* Vegyünk egy tetszőleges összefüggő gráfot, ami nem egy *Gallai-fa*. Ekkor van olyan $H$ blokkja, ami se nem páratlan kör, se nem teljes gráf így van benne elvágó csúcshalmaz. (Mivel nem teljes gráf, van benne olyan csúcspár, amit nem köt össze él. Ekkor az összes többi csúcs elvételével a kapott gráf nem összefüggő, tehát elvágó csúcshalmazt alkotnak.) Vegyünk egy minimális elvágó csúcshalmazt, legyen ez $S$! Mivel $H$ 2-összefüggő, $|S| \geq 2$.

Vegyünk két különböző csúcsot $S$-ből, legyenek ezek $u$ és $v$. Legyen $P_u, P_v$ két legrövidebb út, amelyek végpontjai $u$ és $v$, és $G/S$ különböző komponenseiben haladnak. (Biztos, hogy $G/S$ minden összefüggő komponenese össze van kötve $S$ minden pontjával, mert ha van olyan pont, amely nincs összeköttetésben valamelyik komponenssel, akkor azt a csúcsot kihagyva $S$-ből $|S|$-nél kisebb elemszámú elvágó halmazt találtam, ami ellentmond $S$ minimalitásának.) A $V(P_u) \cup V(P_v)$ csúcsok egy kört feszítenek, amelynek legfeljebb egy húrja van, az $\{u, v\}$ él. Legyen ez a kör $C$.

Ha $C$ páros, kész vagyunk.

Ha páratlan, akkor $P_u, P_v$ közül az egyik páros, a másik páratlan.
Ha $\{u, v\} \in E(G)$, akkor az $\{u, v\}$ él és $P_u, P_v$ közül a páratlan hosszú út együtt egy páros kört feszít, húr nélkül.

Ha páratlan, $\{u, v\} \notin E(G)$, de van egy olyan $w \notin C$ csúcs, hogy $w$-nek legalább két szomszédja van $C$-ban, legyenek ezek $c_1, \dots, c_k$ (ebben a sorrendben), akkor ez a $k$ csúcs szétbontja $C$-t $k$ útra. Ha ezek közül egy is páros, akkor $w$ csúccsal együtt ez egy páros kört feszít, húr nélkül.

Ha mind páratlan, akkor például $c_1 - c_2$, $c_2 - c_3$ utak pontjai $w$-vel egy páros kört feszítenek, a $\{w, c_2\}$ húrral, kivéve, ha $k = 3$, és $c_3 - c_1$ egyetlen él, ugyanis ekkor a $\{c_1, c_3\}$ él is bekerül a feszített részgráfba. Ekkor viszont $c_3 - c_1$, $c_1 - c_2$ utak pontjai valamint $w$ feszít egy páros kört a $\{w, c_1\}$ húrral.

Marad az az eset, hogy $C$ páratlan, $\{u, v\} \notin E(G)$ és $\forall w \notin C$-ra $w$-nek legfeljebb egy szomszédja van $C$-ban. Vegyük azon utakat, amelyek mindkét végpontjuk $C$-beli, de ezen kívül nincs közös pontjuk. (Mivel $H$ nem egy páratlan kör, van még csúcsa, és mivel 2-összefüggő, benne van egy útban.) Ezek közül egy legrövidebb legyen $P$. $P$ két végpontja két részre szedi $C$-t, amelyek közül az egyik páros a másik páratlan, így $P$-vel az egyik egy páros kört feszít, ahol nincs húr, mert ha lenne akkor lenne egy $P$-nél rövidebb út. Ezzel kész vagyunk. $\square$

**5.28. Tétel.** *Legyen $G$ összefüggő gráf. Ha $G$ nem egy Gallai-fa, akkor tetszőleges $f(v_i) \geq \deg(v_i)$ függvénnyel $G$ f-színezhető.*

*Bizonyítás.* A 5.23 Tételt fogjuk használni: keresünk egy olyan $\vec{G}$ irányítását $G$-nek, ahol

$$\deg^+(v_i) \leq \deg(v_i) - 1 \ \forall v_i \in V(G) \text{ és } EE(\vec{G}) \neq EO(\vec{G}).$$

A 5.23 Tétel értelmében ekkor $G$ tetszőleges $f(v_i) \geq \deg(v_i) \geq \deg^+(v_i) + 1$ függvénnyel f-színezhető.

A feltétel, hogy $\deg^+(v_i) \leq \deg(v_i) - 1$, azzal ekvivalens, hogy $\deg^-(v_i) \geq 1$. Elegendő hát ilyen irányítást találni.

A 5.27 Lemma szerint $G$-nek van olyan feszített részgráfja, ami egy páros kör, legfeljebb egy húrral. Húzzuk össze ezt a kört egyetlen $w$ ponttá, és tegyük a következőt:

I. Keressünk egy $w$ gyökerű feszítőfát, és indexeljük meg a csúcsokat: $w$ kapja az 1-es indexet, majd rendre a $w$ csúcs ki-szomszédai, az ő ki-szomszédjaik, amíg a csúcsok el nem fogynak.

II. Irányítsuk meg az éleket ezen indexelés szerint! Minden élre az él feje legyen a kisebb indexű csúcs. Ezzel elértük, hogy $w$-n kívül minden csúcs kifoka legalább egy, és az irányítás aciklikus.

III. Tegyük vissza $w$ helyére a kört, és irányítsuk meg ciklikusan, az esetleg benne levő húrt pedig tetszőlegesen. Így minden csúcs kifoka legalább 1. Ezzel megkaptuk $G$ egy $\vec{G}$ irányítását.

Vegyük észre, hogy irányított kör csak a $w$ helyére visszahelyezett körben lehetséges, ott pedig legfeljebb kettő van, egy páros, és esetleg egy páratlan. Ezek plusz az üres gráf alkotják $\vec{G}$ összes Euler-részgráfját. Így

$$|EE(\vec{G}) - EO(\vec{G})| \geq 1$$

□

Most nézzük, hogy milyen becslések ismertek magára $\mathrm{ch}(G)$-re. Először is a fenti tételből tudjuk, hogy ha $G$ nem Gallai-fa, akkor lista-színezhető az $f(v_i) = \deg(v_i)$ függvénnyel, tehát

$$\mathrm{ch}(G) \leq \max_{v_i \in V(G)} \{\deg(v_i)\}$$

A 5.23 Tétel következménye a következő becslés is:

**5.29. Tétel.** *Indexeljük meg $G$ csúcsait egy sorrendben. Legyen $\vec{G}$ az az irányítás, ahol minden él töve a nagyobb indexű csúcs. Ekkor*

$$ch(G) \leq \min\left\{\max_{v_i \in V(G)} \{\deg^+(v_i)\}, \max_{v_i \in V(G)} \{\deg^-(v_i)\}\right\}$$

*Bizonyítás.* Az irányítás aciklikus, tehát az egyetlen Euler-részgráf az üres gráf, így

$$|EE(\vec{G}) - EO(\vec{G})| = 1$$

Tehát a 5.23 Tétel értelmében $G$ lista-színezhető az $f(v_i) = \deg^+(v_i)$ függvénnyel, így

$$\mathrm{ch}(G) \leq \max_{v_i \in V(G)} \{\deg^+(v_i)\}.$$

Ha az irányítást megfordítom, egy új $\vec{G}'$ aciklikus irányítást kapok, ahol $\deg^+_{\vec{G}'}(v_i) = \deg^-_{\vec{G}}(v_i)$, tehát újra a 5.23 Tételt használva

$$\mathrm{ch}(G) \leq \max_{v_i \in V(G)} \{\deg^-(v_i)\}.$$

□

A tételnek az előnye, hogy algoritmikusan gyorsan ellenőrizhető, és gyakran jobb eredményt ad, mint Brooks tétele.

Egy más megközelítésben $f_G$ és $\mathrm{ch}(G)$ viszonyát vizsgálhatjuk.
Szintén a 5.23 Tétel egyszerű következménye a következő:

**5.30. Tétel.**

$$ch(G) \leq \min\left\{\max_{i=1,\ldots,n} \{\alpha_i\} \mid \underline{\alpha} \in Supp(f_G)\right\} + 1$$

*Bizonyítás.* Legyen

$$k = \min\left\{\max_{i=1,\ldots,n} \{\alpha_i\} \mid \underline{\alpha} \in \mathrm{Supp}(f_G)\right\},$$

és legyen $\alpha \in \mathrm{Supp}(f_G)$ az a monom, amelyen ez az érték felvétetik.

A 5.19 Tételből tudjuk, hogy $f_G$-ben minden monom fokszámösszege $|E(G)|$, tehát

$$\sum_{i=1}^{n} \alpha_i = \deg(f_G),$$

így alkalmazható a 3.2 Tétel:
Tetszőleges $|S_i| > \alpha_i$ halmazokhoz létezik

$$(s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \ldots \times S_n, \text{ hogy } f_G(s_1, s_2, \ldots, s_n) \neq 0,$$

ami megfelel egy jó színezésnek az $S_1, S_2, \ldots, S_n$ listákról. Válasszuk úgy $S_i$-ket, hogy $|S_i| = k+1$ teljesüljön. □

Az előző tétel triviális következménye, mégis érdekes lehet a következő:

**5.31. Tétel.** *Ha valamely* $\underline{\alpha}$*-ra*

$$\max_{i=1,\ldots,n}\{\alpha_i\}+1 \ < \ ch(G),$$

*akkor* $f_{\underline{\alpha}} = 0$.

*Bizonyítás.* Indirekt tegyük fel, hogy $f_{\underline{\alpha}} \neq 0$. Ekkor az előző tétel alapján:

$$\mathrm{ch}(G) \leq \min\left\{\max_{i=1,\ldots,n}\{\alpha_i\} \mid \underline{\alpha} \in \mathrm{Supp}(f_G)\right\} + 1 \leq \max_{i=1,\ldots,n}\{\alpha_i\}+1 \ < \ \mathrm{ch}(G)$$

□

Ez adja az ötletet a következő sejtés megfogalmazásához:

**5.32. Sejtés.**

$$ch(G) = \min\left\{\max_{i=1,\ldots,n}\{\alpha_i\} \mid \underline{\alpha} \in Supp(f_G)\right\} + 1$$

Nyilvánvalóan igaz minden fára, körre és teljes gráfra, valamint nem találtam kivételt a legfeljebb 10 élű gráfok között. $f_G$ kiszámítása elég számításigényes feladat, így a nagyobb gráfok közül csupán a Petersen-gráfra ellenőriztem. A következő lépés a $K_{2*r}$ gráfosztály lehet, ahol $K_{2*r}$ jelöli az $r$ osztatú teljes gráfot, ahol minden pontosztályban 2 csúcs van. [6]-ban Erdős, Rubin és Taylor megmutatták, hogy $\mathrm{ch}(K_{2*r}) = r$.

# Köszönetnyilvánítás

Köszönöm szüleimnek, hogy türelemmel neveltek a szépre és jóra. Köszönöm a barátaimnak, hogy elkísértek és terelgettek idáig az utamon. Köszönöm tanáraimnak, hogy kitartóan töltötték fejembe a tudást. S végül de nem utolsó sorban köszönöm Csikvári Péternek, témavezetőmnek hogy felkeltette és fenntartotta érdeklődésemet a témakör iránt és bármikor segítségemre volt, mikor szükségem volt rá.

# Irodalomjegyzék

[1] Daniel R. Grayson, The Hilbert Nullstellensatz, NSF, 2001. http://www.math.uiuc.edu/ dan/ShortProofs/nullstellen.pdf

[2] Noga Alon. Combinatorial Nullstellensatz. Combinatorics, Probability and Computing, 1999. http://www.tau.ac.il/ nogaa/PDFS/null2.pdf.

[3] Michał Lasoń. A generalization of Combinatorial Nullstellensatz. The Electronic Journal of Combi- natorics, 17, 2010. http://www.combinatorics.org/Volume_17/PDF/v17i1n32.pdf.

[4] Mateusz Michałek. A short proof of Combinatorial Nullstellensatz. American Mathematical Monthly, 2010. http://arxiv.org/pdf/0904.4573v1.

[5] Jan Hladký Daniel Král', and Uwe Schauz. Brooks' theorem via the Alon-Tarsi theorem. Discrete Mathematics, 310(23):3426–3428, (2010)

[6] P. Erdős, A. L. Rubin and H. Taylor, Choosability in graphs, Proc. West Coast Conf. on Combinatorics, Graph Theory and Computing, Congressus Numerantium XXVI, 1979, 125-157.