Kolegij *Studentska natjecanja*, ak. god. 2023./2024.
http://web.math.pmf.unizg.hr/nastava/studnatj/

Tema br. 2:

Polinomijalna metoda u kombinatorici

Aleksandar Bulj, 15. 3. 2024.

Prepoznavanje algebarske strukture u kombinatornom problemu vrlo je važna strategija rješavanja problema budući da omogućava korištenje algebarskih rezultata u problemu koji naizgled nema strukturu kojom možemo baratati. Jedan od najvažnijih alata u tome je korištenje polinoma.

Glavnina rezultata preuzeta je iz knjige [Gut16], a bilješke s kolegija koji je Larry Gutha držao na istu temu 2012. godine dostupne su na linku [Gut12].

1 Polinomi (u više varijabli)

Definirajmo najprije osnovne pojmove koje ćemo koristiti.

U nastavku ćemo sa $\mathbb{F}$ označavati polje, sa $\mathbb{F}_p$ označavat ćemo konačno polje sa p elemenata i podrazumijevati da je p prost, tj. možemo pretpostaviti da je $\mathbb{F}_p$ baš skup $\{0, 1, 2, \ldots, p-1\}$ uz zbrajanje i množenje modulo p. Poznati je rezultat da konačno polje sa p elemenata postoji ako i samo ako je p potencija nekog prostog broja i većina rezultata koje ćemo obraditi jednostavno se generalizira na takva polja, ali kako se takvom generalizacijom ne dobiva ništa esencijalno novo, nećemo ulaziti u nepotrebna poopćenja.

Za proizvoljan skup S sa $|S|$ označavat ćemo broj elemenata skupa S.

Definicija 1. *Neka je R prsten, neka su $d_1, \ldots, d_n \in \mathbb{N}_0$ i $x_1, \ldots, x_n$ varijable. Izraz $x_1^{d_1} \cdots x_n^{d_n}$ nazivamo* ***monomom*** *u n varijabli stupnja $d_1 + \cdots + d_n$. Konačnu linearnu kombinaciju monoma sa koeficijentima iz R nazivamo* ***polinomom*** *u n varijabli nad prstenom R. Skup svih polinoma uz prirodno definirano zbrajanje i množenje čini prsten i označavamo ga sa $R[x_1, \ldots, x_n]$.* ***Stupanj polinoma*** *definira se kao najveći stupanj monoma sa nenul koeficijentom.*

Ukoliko pokušamo sažeto zapisati polinome u n varijabli, vidjet ćemo da je poželjno uvesti sljedeće oznake.

Definicija 2. *Za $x = (x_1, \ldots, x_n)$ i $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ definiramo:*

$$x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n} \quad i \quad |\alpha| := \alpha_1 + \cdots + \alpha_n.$$

Neka je $\mathbb{F}$ polje. Polinome u n varijabli stupnja manjeg ili jednakog d označavamo sa $\mathrm{Poly}_d(\mathbb{F}^n)$ i možemo zapisati kao:

$$P(x) = \sum_{|\alpha|} c_\alpha x^\alpha.$$

Prirodno pitanje je kolika je uopće dimenzija vektorskog prostora $\mathrm{Poly}_d(\mathbb{F}^n)$, tj. koliko ima monoma stupnja najviše d. Odgovor je dan u sljedećoj lemi.

Lema 1. *Dimenzija prostora* $\mathrm{Poly}_d(\mathbb{F}^n)$ *jednaka je*

$$\dim(\mathrm{Poly}_d(\mathbb{F}^n)) = \binom{d+n}{n}$$

Dokaz. Kao što smo već spomenuli, zbog toga što se polinom definira kao konačna linearna kombinacija monoma, dimenzija vektorskog prostora $\mathrm{Poly}_d(\mathbb{F}^n)$ jednaka je broju monoma oblika $x_1^{d_1} \cdots x_n^{d_n}$ za koje vrijedi $d_1 + \cdots + d_n \leq d$. Definiramo li: $d_0 = d - (d_1 + \ldots d_n)$, problem je ekvivalentan brojanju rješenja jednadžbe $d_0 + d_1 + \cdots + d_n = d$, gdje su $d_0, \ldots d_n, \in \mathbb{N}_0$. Za brojanje rješenja koristimo poznati trik "kuglica i štapića". Precizno, svakoj uređenoj $n+1$-torci $(d_0, \ldots, d_n)$ možemo na jedinstven način pridružiti niz od d kuglica i n štapića raspoređenih na $d+n$ mjesta. Broj kuglica do prvog štapića predstavlja d_0, broj kuglica do drugog štapića d_1 itd. Ukupan broj rasporeda kuglica i štapića dobijemo tako da odredimo n mjesta na koje ćemo staviti štapiće, a na ostala mjesta stavimo kuglice. To možemo napraviti na ukupno $\binom{d+n}{n}$ načina i time je tvrdnja dokazana. □

Sljedeća lema osnovni je alat koji ćemo koristiti za traženje polinoma malog stupnja koji se poništava na traženom skupu u problemu.

Lema 2. *Neka su* $S \subset \mathbb{F}^n$ *i* $d \in \mathbb{N}$ *takvi da je* $|S| < \binom{d+n}{n}$. *Tada postoji* ***nenul*** *polinom* $P \in \mathrm{Poly}_d(\mathbb{F}^n)$ *koji je jednak* 0 *na* S.

Posljedično, za svaki konačan skup $S \subset \mathbb{F}^n$ *postoji* ***nenul*** *polinom* P *stupnja najviše* $n|S|^{\frac{1}{n}}$ *koji se poništava na* S.

Dokaz. Dokažimo najprije prvi dio leme.

Označimo li točke iz S sa $s_1, \ldots, s_k$, problem odgovara traženju koeficijenata $c_\alpha \in \mathbb{F}$ u polinomu $P(x) = \sum_{|\alpha| \leq d} c_\alpha x^\alpha$ tako da vrijedi: $P(s_1) = \cdots = P(s_k) = 0$. Zapišemo li to kao sustav jednadžbi s nepoznanicama c_α, potrebno je odrediti rješenje linearnog sustava oblika $Ac = 0$ sa $k < \binom{d+n}{n}$ jednadžbi i $\binom{d+n}{n}$ varijabli. Po teoremu o rangu i defektu (odnosno Gaussovim eliminacijama) znamo da prostor rješenja takvog sustava čini vektorski prostor dimenzije barem jedan pa odabirom nekog nenul vektora dobivamo koeficijente c_α i time nenul polinom koji se poništava na S.

Za drugu tvrdnju dovoljno je primijetiti da za $d := \lfloor n|S|^{\frac{1}{n}} \rfloor$, vrijedi:

$$\binom{d+n}{n} = \frac{(d+n)\cdots(d+1)}{n!} > \frac{(n|S|^{\frac{1}{n}})^n}{n!} \geq |S|$$

pa tvrdnja slijedi iz prvog dijela zadatka. □

Pitanje "geometrije" skupa nultočaka polinoma jedne varijable je nezanimljivo. Naime, skup nultočaka polinoma stupnja d jednak je uniji najviše d točaka iz $\mathbb{F}$. S druge strane, pitanje "geometrije" skupa nultočaka polinoma u više varijabli neusporedivo je kompleksnije. Na

primjer, već skup realnih nultočaka polinoma u 2 varijable stupnja 2 može biti bilo koja konika. Široko područje matematike, algebarska geometrija, bavi se upravo pitanjem proučavanja skupa nultočaka polinoma više varijabli.

Kako smo vidjeli da su nultočke polinoma jedne varijable dobro klasificirane, povežimo polinome u više varijabli sa polinomima jedne varijable.

Početna važna opservacija je da svaki polinom iz $R[x_1, \ldots, x_n]$ možemo shvatiti kao polinom jedne varijable u proizvoljnoj varijabli, npr. x_n, sa koeficijentima iz prstena $R[x_1, \ldots, x_{n-1}]$. Na primjer, polinom $P(x, y) = x^3 - 3x^2y^2 + 2x^2y + xy + x + y + 1$ možemo zapisati kao: $P(x, y) = x^3 + (-3y^2 + 2)x^2 + (y + 1)x + (y + 1)$, shvatiti ga kao polinom u x sa koeficijentima iz $R[y]$ i zatim koristiti sve teoreme za polinome jedne varijable nad prstenom.

Napomena. Posebno važna ideja u algebarskoj geometriji je ulaganje prstena $R[y]$ u polje racionalnih funkcija u varijabli y jer tada možemo koristiti i sve rezultate za polinome kod koji je važno da su definirani nad poljem (kao npr. algoritam za dijeljenje polinoma), ali navedeno izlazi van plana ovog kratkog predavanja i zainteresiranog čitatelja upućujemo na klasičnu literaturu iz algebarske geometrije.

Preformulirajmo spomenutu tvrdnju o nultočkama polinoma u oblik koji ćemo koristiti u ovom predavanju.

Lema 3. *Ako polinom $P \in \mathbb{F}[x]$ stupnja $\leq d$ iščezava u $d + 1$ točaka, tada je P nulpolinom.*

Dokaz. Iz jednostavne opservacije $x^k - a^k = (x - a) \sum_{j=0}^{k-1} x^j a^{k-1-j}$ slijedi $P(x) - P(a) = (x - a)Q(x)$, gdje je $Q \in \mathbb{F}[x]$. Dakle, ako je a nultočka od P, tada $x - a | P(x)$. Kada bi P imao $d + 1$ različitih nultočaka, on bi morao biti djeljiv polinomom $Q(x) = \prod_{j=0}^{d+1}(x - a_j)$ stupnja $d + 1$, što je zbog jednakosti stupnjeva moguće samo ako je $P = Q \cdot 0$ i tvrdnja slijedi. □

Sljedeća lema jednostavna je posljedica prethodne, ali bit će korištena puno puta pa je posebno izdvajamo.

Lema 4. *Ako polinom $P \in \mathrm{Poly}_d(\mathbb{F}^n)$ iščezava u $d+1$ točki pravca l tada P iščezava u svakoj točki tog pravca.*

Dokaz. Neka je pravac l parametarski zadan s $\gamma(t) = at + b$ za neke $a, b \in \mathbb{F}^n$ i neka je $Q(t) := P(at + b)$. Zbog toga što je P polinom u n varijabli stupnja najviše d, uvrštavanjem izraza slijedi da je Q polinom jedne varijable stupnja najviše d koji se poništava u $d+1$ točaka od $\mathbb{F}$. Tada je $Q = 0$, odnosno $P = 0$ na l. □

Induktivno dobivamo sljedeći rezultat o nultočkama polinoma n varijabli.

Lema 5. *Neka je $P \in \mathbb{F}[x_1, \ldots, x_n]$ stupnja najviše d_i u varijabli x_i, za sve $i = 1, 2, \ldots, n$. Ako su skupovi $A_1, \ldots, A_n \subset \mathbb{F}$ takvi da je $|A_i| \geq d_i + 1$ i P iščezava na skupu $A_1 \times \cdots \times A_n$, tada je $P = 0$.*

Ekvivalentno, za netrivijalni polinom $P \in \mathbb{F}[x_1, \ldots, x_n]$ stupnja najviše d_i u varijabli x_i, za sve $i = 1, 2, \ldots, n$ i proizvoljne skupove $A_i \subset \mathbb{F}$ koji zadovoljavaju $|A_i| \geq d_i + 1$, $i = 1, 2, \ldots, n$ vrijedi da postoji točka $(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$ takva da je $P(a_1, \ldots, a_n) \neq 0$.

Dokaz. Dokaz provodimo indukcijom po n. U slučaju $n = 1$ tvrdnja slijedi iz prethodne leme pa uzmimo $n \in \mathbb{N}$ proizvoljan i pretpostavimo da tvrdnja vrijedi za sve polinome sa manje od n varijabli. Neka su $a_i \in A_i$, $i = 1, 2, \ldots, n-1$ proizvoljni, ali fiksni. Zapišemo li polinom P u obliku $P(x_1, \ldots, x_n) = Q_{d_n}(x_1, \ldots x_{n-1})x_n^{d_n} + \ldots Q_0(x_1, \ldots, x_{n-1})$, tada je polinom $P_{a_1,\ldots,a_{n-1}}(x_n) := P(a_1, \ldots, a_{n-1}, x_n)$ polinom jedne varijable stupnja d_n koji se poništava u $d_n + 1$ točaka pa je nulpolinom po prethodnoj lemi. To znači da je $Q_j(a_1, \ldots, a_{n-1}) = 0$ za sve $j = 1, \ldots, d_n$. Kako su a_i-jevi bili proizvoljni elementi od A_i, slijedi da se svaki od polinoma Q_j, koji ima $n-1$ varijabli poništava na $A_1 \times \cdots \times A_{n-1}$ pa po pretpostavci indukcije slijedi da je $Q_j = 0$ za sve $j = 1, \ldots, d_n$, a odatle slijedi i da je $P = 0$. □

Prirodno pitanje koje se postavlja je možemo li za neki manji skup i za neki netrivijalan polinom tvrditi da ne može biti jednak 0 na cijelom skupu. Odgovor je potvrdan u slučaju da znamo nešto o obliku polinoma P i o tome govori sljedeći netrivijalan rezultat preuzet iz [Alo99], a kratki dokaz koji navodimo preuzet je iz [Mic10].

Teorem 6 ("Combinatorial nullstellensatz")**.** *Neka su $d_1, \ldots, d_n \in \mathbb{N}_0$, $d := d_1 + \cdots + d_n$ i neka je $P \in \mathrm{Poly}_d(\mathbb{F}^n)$ takav da je koeficijent uz $x_1^{d_1} \cdots x_n^{d_n}$ različit od 0.*

Ako su $A_1, \ldots, A_n \subset \mathbb{F}$ proizvoljni skupovi takvi da je $|A_i| \geq d_i + 1$ za sve $i = 1, 2, \ldots, n$, tada postoji točka $(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$, takva je $P(a_1, \ldots, a_n) \neq 0$.

Napomena. Primjer slučaja u kojem prethodni rezultat daje značajno jaču ocjenu je sljedeći. Polinom oblika $P(x, y) = ax^4 + by^4 + x^2y^2$ je stupnja 4 po obje varijable pa da bismo dokazali da postoji točka $(x_0, y_0) \in \mathbb{R}^2$ za koju je $P(x_0, y_0) \neq 0$, koristeći lemu 5 možemo je naći u proizvoljnom produktu skupova od 5 elemenata. Međutim, koristeći prethodni teorem, zbog toga što je koeficijent u x^2y^2 različit od 0, vidimo da točku u kojoj se polinom ne poništava možemo naći i na produktu skupova s 3 elementa. Međutim, važno je primijetiti da je stupanj monoma uz koji promatramo nenul koeficijent mora biti jednak stupnju polinoma.

Dokaz. Dokaz provodimo indukcijom po d. U slučaju $d = 0$, tvrdnja je očita jer uvjet implicira da je P jednak konstanti različitoj od 0.

Neka je sad $d > 1$ proizvoljan. Pretpostavimo da tvrdnja vrijedi za sve polinome stupnja manjeg ili jednakog $d-1$ i dokažimo da vrijedi za d. Pretpostavimo suprotno, tj. da postoji polinom P stupnja d koji ima nenul koeficijent uz monom $x_1^{d_1} \cdots x_n^{d_n}$ stupnja d i da je $P(x) = 0$ za sve $x \in A_1 \times \cdots \times A_n$. Odaberimo proizvoljan $a \in A_1$. Shvatimo li P kao polinom u x_1 sa koeficijentima iz prstena $\mathbb{F}[x_2, \ldots x_n]$, tada po algoritmu za dijeljenje polinoma (koji možemo provesti i nad prstenom kad je vodeći koeficijent u polinomu kojim dijelimo jednak 1) postoje polinomi $Q, R \in \mathbb{F}[x_1, \ldots, x_n]$ takvi da je $P = (x_1 - a)Q + R$, za koje vrijedi $\deg_{x_1}(Q) = d - 1 = (d_1 - 1) + d_2 + \cdots + d_n$ i $\deg_{x_1}(R) = 0$, tj. polinom R ne ovisi o x_1. Po uvjetu zadatka i algoritmu za dijeljenje polinoma slijedi da je koeficijent uz $x_1^{d_1-1}x_2^{d_2} \ldots x_n^{d_n}$ u polinomu Q različit od 0. Nadalje, za svaki $x \in A_1 \times \cdots \times A_n$, zbog toga što što R ne ovisi o x_1, vrijedi:

$$R(x) = R(a, x_2, \ldots, x_n) = P(a, x_2, \ldots, x_n) - (a - a)Q(a, x_2, \ldots, x_n) = 0$$

pa posebno za $x \in (A_1 \setminus \{a\}) \times A_2 \times \dots A_n$ vrijedi

$$(x_1 - a)Q(x) = P(x) - R(x) = 0.$$

Zbog toga što je $x_1 \neq a$ na navedenom skupu, slijedi $Q(x) = 0$ na $(A_1 \setminus \{a\}) \times A_2 \times \cdots \times A_n$. Međutim, to je kontradikcija sa pretpostavkom indukcije primijenjenom na polinom Q. □

2 Primjene u kombinatorici

Još jednom napominjemo da sa $\mathbb{F}_p$ označavamo konačno polje sa p elemenata i implicitno pretpostavljamo da je p prost.

2.1 Problem sumseta

Neka je $(G, +)$ proizvoljna abelova grupa i neka su $A, B \subset G$ proizvoljni. Definirajmo

$$A + B := \{a + b : a \in A, b \in B\}.$$

Skupovi oblika $S = A_1 + \cdots + A_n$ nazivaju se sumseti. Prirodno pitanje je koliko velik (ili mali) može biti skup $A + B$ u ovisnosti o tome što je grupa G. U slučaju kad je $G = \mathbb{R}$, odgovor je elementaran i iskazan je u sljedećoj lemi.

Lema 7. *Neka su $A, B \subset \mathbb{R}$. Tada vrijedi:*

$$|A| + |B| - 1 \leq |A + B| \leq |A||B|$$

i jednakost u obje nejednakosti se može postići.

Dokaz. Dokažimo najprije gornju ocjenu. Zbog toga što postoji točno $|A||B|$ odabira parova (a, b) takvih da je $a \in A$ i $b \in B$, slijedi da je $|A + B| \leq |A||B|$ i jednakost se može postići odabirom $A = \{0, 1, 2, \dots, m - 1\}$, i $B = \{0, m, 2m, \dots (n - 1)m\}$ jer je tada $A + B = \{0, 1, \dots, mn - 1\}$.

Za donju ocjenu primijetimo sljedeće. Označimo li sa $a_1 < \cdots < a_m$ elemente skupa A i sa $b_1 < \cdots < b_n$ elemente skupa B, tada iz uređaja na brojevima slijedi:

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_m + b_1 < a_m + b_2 < a_m + b_3 < \cdots < a_m + b_n.$$

Time smo dobili barem $m+n-1$ različitih brojeva u skupu $A+B$ pa je $|A+B| \geq |A|+|B|-1$. Jednakost se može postići odabirom $A = \{0, 1, 2, \dots, m-1\}$ i $B = \{0, 1, \dots, n-1\}$ jer je tad $A + B = \{0, 1, \dots m + n - 2\}$. □

Ako su sada $A, B \subset \mathbb{F}_p$, što sad možemo reći o veličini skupa $A + B$? Kako $\mathbb{F}_p$ ima p elemenata, tada je $|A + B| \leq p$, a istim argumentom kao i ranije slijedi $|A + B| \leq |A||B|$ pa zaključujemo da vrijedi $|A + B| \leq \min(p, |A||B|)$ pa pitanje gornje ocjene nije posebno zanimljivo. Međutim, za donju ocjenu argument uređaja više nije dobar budući da zbrajanje modulo p ne čuva uređaj i ta ocjena postaje puno teža. Zanimljivo je da je ipak analogna tvrdnja, uz modifikaciju zbog ograničenosti veličine svakog skupa s p, i dalje istinita.

Teorem 8 (Cauchy - Davenport)**.** *Neka su $A, B \subset \mathbb{F}_p$ proizvoljni. Tada vrijedi:*

$$|A + B| \geq \min(|A| + |B| - 1, p).$$

Dokaz. Slučaj $|A| + |B| \geq p + 1$ slijedi iz Dirichletovog principa i ostavljamo ga za zadaću.

Dokazujemo sada da u slučaju $|A|+|B| \leq p$ vrijedi $|A+B| \geq |A|+|B|-1$. Pretpostavimo da tvrdnja ne vrijedi, tj. da je postoje A, B takvi da je $|A + B| \leq |A| + |B| - 2$. Neka je $C \supset A + B$ proizvoljan, takav da je $|C| = |A| + |B| - 2$ i promotrimo polinom:

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

Zbog toga što za svaki $x \in A$ i $y \in B$ postoji $c \in A + B \subset C$ takav da je $c = x + y$, slijedi da se P poništava na $A \times B$. Nadalje, stupanj polinoma je jednak $|A| + |B| - 2 \leq p - 2$ pa promotrimo koeficijent uz $x^{|A|-1}y^{|B|-1}$ u polinomu P. Zbog toga što mora biti maksimalnog stupnja, iz svake zagrade moramo uzeti x ili y pa je koeficijent jednak $\binom{|A|+|B|-2}{|A|-1}$. Zbog toga što je $|A| + |B| - 2 < p$, taj binomni koeficijent nije djeljiv s p pa je različit od 0 u $\mathbb{F}_p$. Međutim, time smo dobili kontradikciju sa teoremom 6, po kojem bi trebala postojati točka $(a, b) \in A \times B$ za koju je $P(a, b) \neq 0$. Dakle, pretpostavka je bila pogrešna pa tvrdnja teorema vrijedi. □

Sljedeće pitanje sličnog tipa je što možemo reći o veličini sumseta ukoliko uvedemo neku restrikciju na elemente koje biramo. Uvedimo novu oznaku radi kraćeg zapisa.

Neka je $(G, +)$ abelova grupa s obzirom na zbrajanje i neka su $A, B \subset G$. Definirajmo

$$A\dot{+}B := \{a + b : a \in A, b \in B, a \neq b\}$$

i takav skup nazivamo restringirani sumset.

Pitamo se opet koliko velik može biti skup $A\dot{+}B$. U slučaju kad je $G = \mathbb{R}$, sličnim argumentom kao i bez restrikcije dobivamo ocjenu:

$$|A| + |B| - 3 \leq |A\dot{+}B| \leq |A||B|,$$

a dokaz ostavljamo za zadaću.

Analogno pitanje u polju $\mathbb{F}_p$ naziva se Erdös - Heilbronnova hipoteza koja je postavljena 1964. godine, a tek 1994. su je riješili Dias da Silva i Hamidoune. Zbog toga što je 30 godina bila neriješena, i dalje se naziva Erdös -Heilbronnova hipoteza iako je to danas teorem čiji dokaz navodimo u nastavku.

Teorem 9 (Erdös -Heilbronnova "hipoteza")**.** *Za $A \subset \mathbb{F}_p$ vrijedi*

$$|A\dot{+}A| \geq \min(2|A| - 3, p).$$

Dokaz. Slučaj $p = 2$ je trivijalan pa pretpostavimo bez smanjenja općenitosti da je $p > 2$.

Slučaj kad je $2|A|-3 \geq p$ slijedi slično kao i Cauchy - Davenportov teorem iz Dirichletovog teorema pa ga ostavljamo za zadaću.

Dokažimo sada tvrdnju u slučaju $2|A| \leq p+2$. Pretpostavimo da tvrdnja ne vrijedi, tj. da postoji $A \subset \mathbb{F}_p$ takav da je $|A\dot{+}A| \leq 2|A|-4$. Neka je $C \supset A\dot{+}A$ proizvoljan takav da je $|C| = 2|A|-4$ i promotrimo polinom:

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

Zbog toga što za sve $x, y \in A$ takve da je $x \neq y$ postoji $c \in A\dot{+}A \subset C$ takav da je $x+y=c$ i zbog toga što je $P(x,x)=0$, slijedi da se polinom P poništava na $A\times A$. Stupanj polinoma jednak je $2|A|-3$ pa promotrimo koeficijent uz $x^{|A|-1}y^{|A|-2}$. Navedenu potenciju možemo dobiti na način da iz prve zagrade "uzmemo" x, a iz produkta $|A|-2$ x-eva i $|A|-2$ y-a ili tako da iz prve zagrade "uzmemo" $-y$, a iz produkta $|A|-1$ x-eva i $|A|-3$ y-a pa je jednak:

$$\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-3} = \left(\frac{|A|-3}{|A|-1} - 1\right)\binom{2|A|-4}{|A|-3},$$

što zbog $2|A|-4 < p$ nije djeljivo s p pa je različito od 0 u $\mathbb{F}_p$. Međutim, time opet dobivamo kontradikciju sa teoremom 6 budući da on povlači da postoji točka $(a,b) \in A\times A$ takva da je $P(a,b) \neq 0$. □

2.2 Nikodymov i Kakeyain skup nad konačnim poljima

U ovom odjeljku dokazat ćemo dva srodna rezultata koji su diskretni analogoni dvaju poznatih i važnih otvorenih problema u $\mathbb{R}^n$.

2.2.1 Kakeya skup

U $\mathbb{R}^n$ Kakeya skup je skup koji sadrži jediničnu dužinu u svakom smjeru. Jedan Kakeya skup u $\mathbb{R}^2$ očito je krug promjera 1. Pitanje je postoje li skupovi manje mjere koji zadovoljavaju isto svojstvo. Besicovitch je 1917. dokazao vrlo neintuitivan rezultat - za proizvoljan $\varepsilon > 0$ postoji Kakeya skup mjere manje od ε. Međutim, modifikacijom Besicovitcheve konstrukcije može se pokazati da postoje Kakeya skupovi mjere 0!

Definiramo li preciznije "mjeru" popunjavanja prostora u koju nećemo ulaziti u ovom predavanju, pitanje je je li Kakeya skup u $\mathbb{R}^n$ Hausdorffove dimenzije n. Odgovor na to pitanje poznat je samo u dimenziji $n=2$, dok je za $n \geq 3$ to važna otvorena slutnja. Iako na prvi pogled nije očito kako, pitanja o veličinama Kakeya skupova usko su povezana sa mnogim problemima u Harmonijskoj analizi i vrlo su aktivno područje istraživanja. Zbog toga su postavljena pitanja koja se zovu "toy problemi" u kojima pokušavaju riješiti sličan ili analogan problem u nekim jednostavnijim modelima. Primjer toga je ocjena veličine Kakeya skupova u vektorskom prostoru $\mathbb{F}_p^n$ umjesto $\mathbb{R}^n$. Uvedimo definiciju.

Definicija 3. *Skup $K \subset \mathbb{F}_p^n$ naziva se Kakeya skup ako sadrži pravac u svakom smjeru, tj. za proizvoljan $a \in \mathbb{F}_p^n$ postoji $b \in \mathbb{F}_p^n$ takav da je pravac $l = \{at+b : t \in \mathbb{F}\}$ sadržan u K.*

Jedan očit Kakeya skup je $K = \mathbb{F}_p^n$, ali pitanje je postoji li manji Kakeya skup i mora li uvijek sadržavati neki pozitivan udio svih točaka. Navedeni problem smatrao se jednako teškim kao i u $\mathbb{R}^n$ i sljedeći teorem kojeg je dokazao Dvir 2009. koristeći polinomijalnu metodu predstavljao je veliko iznenađenje u matematici.

Teorem 10 (Finite field Kakeya)**.** *Svaki Kakeya skup u $\mathbb{F}_p^n$ sadrži barem $c_n p^n$ elemenata. Možemo uzeti $c_n = (10n)^{-n}$.*

Dokaz. Pretpostavimo suprotno, tj. da postoji $K \subset \mathbb{F}_p^n$ Kakeya skup takav da je $|K| < (10n)^{-n}p^n$. Tada po lemi 1 postoji nenul polinom P stupnja d, gdje je $d \leq n|K|^{\frac{1}{n}} = \frac{p}{10} < p$. Ako je $P(x) = \sum_{|\alpha|\leq d} c_\alpha x^\alpha$ raspis polinoma P, definirajmo $P_d(x) := \sum_{|\alpha|=d} c_\alpha x^\alpha$ i $Q = P - P_d$, tj. P_d homogeni polinom maksimalnog stupnja u raspisu od P, Q suma monoma manjeg stupnja. Neka je $a \in \mathbb{F}_p^n \setminus \{0\}$ proizvoljan. Odaberimo $b \in \mathbb{F}_p^n$ takav da je pravac $l = \{at + b : t \in \mathbb{F}\}$ sadržan u K. Polinom $R(t) := P(at + b)$ stupnja je $d < p$ i iščezava u svakoj točki $t \in \mathbb{F}$ pa je identički jednak 0. Međutim, koeficijent uz t^d u polinomu R iznosi: $\sum_{|\alpha|=d} c_\alpha a^\alpha = P_d(a)$. Prema tome, za svaki $a \in \mathbb{F}_p^n \setminus \{0\}$ vrijedi $P_d(a) = 0$, ali kako je P_d homogen polinom stupnja $d \geq 1$, vrijedi i $P_d(0) = 0$ pa zaključujemo da P_d iščezava u svim točkama od $\mathbb{F}_p^n$, a odatle koristeći lemu 5 slijedi da je $P_d = 0$, što je kontradikcija s pretpostavkom da je P nenul polinom. □

2.2.2 Nikodymov skup

Za skup $N \subset [0,1]^2$ kažemo da je Nykodimov ukoliko za svaku točku $x \in [0,1]^2$ postoji pravac l kroz točku x takav da je $l \setminus \{x\} \subset N$. Trivijalni primjer Nikodymovog skupa je cijeli kvadrat $[0,1]^2$, ali opet je pitanje može li takav skup biti manji. Opet je rezultat pomalo neočekivan - postoji Nikodymov skup mjere 0!

Promotrimo sada varijantu Nikodymovog skupa nad konačnim poljima.

Definicija 4. *Za skup $N \subset \mathbb{F}_p^n$ kažemo da je Nikodymov ako za svaki $x \in \mathbb{F}_p^n$ postoji pravac $l(x)$ koji sadrži x takav da je $l \setminus \{x\} \subset N$.*

Pitanje je slično kao kod Kakeya skupa - koliko mali može biti Nikodymov skup.

Teorem 11 (Finite field Nikodym)**.** *Svaki Nikodymov skup u $\mathbb{F}_p^n$ sadrži barem $c_n p^n$ elemenata. Možemo uzeti $c_n = (10n)^{-n}$.*

Dokaz. Pretpostavimo da postoji skup N koji zadovoljava $|N| < (10n)^{-n}p^n$. Tada po lemi 1 postoji nenul polinom P stupnja najviše $\deg P \leq n|N|^{\frac{1}{n}} = \frac{p}{10} < p - 1$ koji se poništava na N. Po uvjetu zadatka vrijedi da za proizvoljnu točku $x \in \mathbb{F}_p^n$ postoji pravac $l = \{x + yt, t \in \mathbb{F}_p\}$, za neki $y \in \mathbb{F}_p^n$ na kojem se P poništava u barem $p - 1$ točaka $t = 1, 2, \ldots, p - 1$ (tu je važno da je p prost da bi točke $x + yt$ bile različite za različite t-ove). Kako je $\deg P < p - 1$, tada je po lemi 4 polinom P je jednak 0 na cijelom pravcu, pa posebno i u točki x. Međutim to znači da se P poništava u svim točkama od $\mathbb{F}_p^n$, što po lemi 5 povlači da je $P = 0$ čime smo dobili kontradikciju. □

2.3 Berlekamp - Welchov teorem

Teorija kodiranja matematičko je područje koje se bavi pitanjima prijenosa podataka uz određene zahtjeve zbog kojih taj problem postaje netrivijalan. Različiti zahtjevi su, na primjer, kompresija podataka, čuvanje tajnosti podataka ili otpornost na greške. U ovom poglavlju pokazat ćemo primjenu polinomijalne tehnike na efikasno rješenje problema otpornosti na velik broj pogrešaka.

Prilikom kopiranja ili slanja podataka događaju se fizičke pogreške zbog kojih se promijeni određen broj bitova. Pretpostavimo da nekome želimo poslati n brojeva nekim šumovitim kanalom, ali možemo biti sigurni samo da će 51% poslanih brojeva biti točno i primljeno. Dodatno, primatelj ne zna koji su točni, a koji krivi brojevi. Je li uopće moguće ostvariti komunikaciju navedenim kanalom tako da se poslana poruka sigurno može i dešifrirati? Nadalje, očito je potrebno poslati više od n brojeva primatelju, ali koliko više? Možemo li to napraviti sa $O(n)$ brojeva ili je potrebno slati značajno više? Konačno, postoji li algoritam kojim primatelj može dešifrirati podatke u polinomijalnom vremenu?

Vrlo zadovoljavajuć odgovor na gornji problem daje klasa kodiranja, takozvani *Reed - Solomonovo* kodiranje, koji se koriste u zapisu na CD-e i DVD-e i daju rješenje prethodnog problema u kojem se šalje $O(n)$ brojeva, uz algoritam za dekodiranje složenosti najviše $O(n^3)$.

Ideja algoritma je slati informacije ukodirane u koeficijente polinoma. Neka je $\mathbb{F}_p$ konačno polje i neka je $Q \in \mathbb{F}_p[x]$ polinom takav da je $\deg Q \leq \delta p$ za neki $\delta > 0$ (npr. za naše prvo pitanje možemo uzeti $\delta = \frac{1}{100}$). U polinom Q ukodiramo podatke tako da je svaki njegov koeficijent jedan broj iz $\mathbb{F}_p$ koji želimo poslati primatelju, a poruka koju šaljemo je niz $(Q(1), \ldots, Q(p))$. Primatelj umjesto niza vrijednosti $(Q(1), \ldots, Q(p))$, dobije vrijednosti $(F(1), \ldots, F(p))$ i pitanje je može li iz F "dešifrirati" što je bio polinom Q.

Osnovna opservacija je sljedeća. Ako znamo da imamo barem $(\frac{1}{2}+\delta)p$ ispravnih vrijednosti, moguće je jedinstveno dešifrirati poruku.

Lema 12. *Postoji najviše jedan polinom Q stupnja najviše δp takav da je $Q(x) = F(x)$ za barem $(\frac{1}{2} + \delta)p$ vrijednosti iz $\mathbb{F}_p$.*

Dokaz. Pretpostavimo da postoje dva takva polinoma, Q_i, $i = 1, 2$ takva da je $Q_i(x) = F(x)$ na $A_i \subset \mathbb{F}_p$, $|A_i| > (\frac{1}{2} + \delta)p$. Tada je $Q_1 - Q_2$ polinom stupnja najviše δp koji se poništava na skupu $A_1 \cap A_2$ veličine barem $|A_1 \cap A_2| \geq |A_1| + |A_2| - |A_1 \cup A_2| \geq |A_1| + |A_2| - p \geq 2\delta p$. Lema 4 implicira da je $Q_1 - Q_2 = 0$ i time je tvrdnja dokazana. □

Dakle, znamo da postoji najviše jedan takav polinom, ali pitanje je kako otkriti koji je to polinom. Promotrimo složenost jednog naivnog pokušaja traženja takvog polinoma. Prođemo po svim podksupovima $I \subset \mathbb{F}_p$ veličine barem $(\frac{1}{2} + \delta)p$, interpolacijom provučemo kroz njih polinom koji se podudara sa F na I i onda iskoristimo dokazanu tvrdnju da postoji najviše jedan takav skup na kojem dani polinom ima stupanj manji od δp. Međutim, takvih podskupova ima $\binom{p}{(\frac{1}{2} + \delta)p}$, odakle korištenjem Stirlingove aproksimacije dobijemo

$$\binom{p}{(\frac{1}{2} + \delta)p} \sim C_0(\delta) p^{-\frac{1}{2}} e^{C_1(\delta)p}, \quad p \to \infty,$$

gdje je $C_0(\delta) = (2\pi(\frac{1}{4} - \delta^2))^{-\frac{1}{2}}$ i $C_1(\delta) = -(\frac{1}{2} - \delta)\log(\frac{1}{2} - \delta) - (\frac{1}{2} + \delta)\log(\frac{1}{2} + \delta) > 0$, što je uz složenost interpolacije polinomom eksponencijalna složenost.

Prema tome, trebamo pametniji algoritam za dekodiranje. To je sadržaj sljedećeg teorema.

Teorem 13 (Berlekamp - Welch)**.** *Neka je $\delta \in (0,1)$, neka je $P(x)$ polinom u $\mathbb{F}_p[x]$ stupnja manjeg od δp i neka je $F : \mathbb{F}_p \to \mathbb{F}_p$ funkcija takva da je $F(x) = P(x)$ za za barem $(\frac{1}{2} + \delta)p$ vrijednosti $x \in \mathbb{F}_p$. Tada postoji algoritam koji u polinomijalnom vremenu može rekonstruirati P iz F.*

Dokaz. Grafom od F nazivamo skup $\{(x, y) \in \mathbb{F}_p^2 : y = F(x)\}$ i cilj nam je otkriti algebarsku strukturu grafa od F. Pokušajmo naći polinom malog stupnja u dvije varijable koji se poništava na grafu od F. Neka je $W(d)$ vektorski prostor polinoma oblika

$$R(x, y) = R_0(x) + R_1(x)y, \quad R_0, R_1 \in \mathrm{Poly}_d(\mathbb{F}).$$

Dimenzija tog vektorskog prostora je $2d + 2$ (zašto?). Graf od F ima ukupno p elemenata pa čim je $2d + 2 > p$, postoji polinom iz $W(d)$ koji se poništava na F. Posebno, stupanj takvog polinoma je manji od $\frac{p}{2}$ i nalaženje takvog polinoma je rješavanje linearnog sustava pa ga možemo naći u složenosti najviše $O(p^3)$ već Gaussovim eliminacijama. Označimo dobiveni polinom sa $R(x, y)$. Kako se R poništava na grafu od F i graf od F se podudara sa grafom od P u barem $(\frac{1}{2} + \delta)p$ točaka, to znači da se polinom $Q(x) = R(x, P(x))$ poništava u barem $(\frac{1}{2} + \delta)p$ vrijednosti x. Međutim, kako je $\deg Q \leq d + \deg P < (\frac{1}{2} + \delta)p$, po lemi 4 slijedi da je $Q = 0$, tj. zaključujemo da za svaki $x \in \mathbb{F}_p$ vrijedi $R(x, P(x)) = 0$.

Iz oblika polinoma R slijedi: $R_0(x) + P(x)R_1(x) = 0$ pa je $P = -R_0/R_1$, što možemo izračunati klasičnim algoritmom za dijeljenje polinoma u najviše $O(p^3)$ koraka čak i bez ubrzanja množenja polinoma. □

2.4 "Problem sa zglobovima"

Nastavljamo sa još jednim teškim problemom postavljenim u 1990-ih. Započnimo definicijom zgloba.

Neka je $\mathcal{L}$ skup pravaca u $\mathbb{R}^3$. Točku $x \in \mathbb{R}^3$ nazivamo zglob ako se u njoj sijeku 3 nekomplanarna pravca iz $\mathcal{L}$.

Opet se pitamo koliko može velik biti skup zglobova. On očito može biti jednak nuli ako se pravci ne sijeku pa je zanimljivo samo pitanje koliko najviše može biti zglobova za dani skup koji sadrži L pravaca. Kako se zglob mora nalaziti na presjeku barem 2 pravca, takvih presjeka ima najviše $\binom{L}{2}$, očito ne može postojati više od $\binom{L}{2}$ zglobova, ali pitanje je možemo li postići i taj broj.

Promotrimo prvi primjer - kocku $\{0, 1, \ldots, n-1\}^3$ i skup pravaca iz cjelobrojne mreže od $\mathbb{Z}^3$ koji prolaze kroz tu kocku. Svaki od tih pravaca siječe neku koordinatnu ravninu u nekoj od n^2 cjelobrojnih točaka na stranici pa imamo ukupno $L := 3n^2$ pravaca koji određuju ukupno $n^3 = (\frac{L}{3})^{\frac{3}{2}}$ zglobova.

Pokušajmo naći primjer sa više zglobova. Promotrimo n ravnina u općem položaju (što to znači i zašto to možemo naći za svaki n?). Svake dvije ravnine određuju pravac pa je

određeno ukupno $L := \binom{n}{2}$ pravaca. Nadalje, presjek svake 3 ravnine postoji i time je određeno $\binom{n}{3} = L \cdot \frac{n-2}{3} \geq L(\frac{\sqrt{2}}{3}L - \frac{1}{2})$ točaka. Time smo dobili opet $O(L^{\frac{3}{2}})$ točaka, uz malo bolju konstantu.

Dakle, postavlja se pitanje postoji li bolja ograda od $O(L^2)$ ili su nam samo primjeri loši. Odgovor je dan u sljedećem toeremu.

Teorem 14. *Proizvoljnih L pravaca u $\mathbb{R}^3$ određuje najviše $10L^{\frac{3}{2}}$ zglobova.*

Dokaz. Pokušajmo vidjeti što možemo zaključiti traženjem polinoma malog stupnja koji se poništava na skupu zglobova. To je sadržaj sljedeće leme.

Lema 15. *Ako nekih L pravaca određuje J zglobova, postoji pravac koji sadrži najviše $3J^{\frac{1}{3}}$ zglobova.*

Dokaz. Po lemi 1 postoji nenul polinom stupnja najviše $3J^{\frac{1}{3}}$ koji se poništava na svim zglobovima i neka je P polinom **najmanjeg stupnja** sa tim svojstvom.

Kad bi se P poništavao na svim pravcima, tada bi u svakom zglobu postojala 3 linearno nezavisna smjera u kojima P ne mijenja vrijednost, tj. u svakom zglobu x postojala bi 3 linearno nezavisna vektora - v_1, v_2, v_3 takva da je $\nabla P(x)v_i = 0$. Međutim, to povlači $\nabla P(x) = 0$ u svakom zglobu i to posebno znači da se polinom $\partial_x P$ poništava u svim zglobovima, a kako je $\deg \partial_x P < \deg P$, dobivamo kontradikciju sa pretpostavkom o minimalnosti stupnja P sa danim svojstvom. Prema tome, postoji pravac na kojem se P ne poništava. Kako je stupanj polinoma P najviše $3J^{\frac{1}{3}}$ i znamo da se poništava u zglobovima, to znači da na tom pravcu ne smije biti više od $3J^{\frac{1}{3}}$ zglobova (u suprotnom bi se po lemi 4 polinom P poništavao na cijelom pravcu) i time je tvrdnja dokazana. □

Dovršimo sada dokaz teorema. Za proizvoljan n označimo sa $J(n)$ maksimalni broj zglobova koji nekih n pravaca može činiti.

Neka je n proizvoljan i promotrimo familiju pravaca koja čini maksimalnih $J(n)$ zglobova. Po dokazanoj lemi postoji pravac koji sadrži najviše $3J(n)^{\frac{1}{3}}$ zglobova, pa kako ostalih $n-1$ pravaca čini najviše $J(n-1)$ zglobova, vrijedi rekurzivna relacija

$$J(n) \leq J(n-1) + 3J(n)^{\frac{1}{3}}.$$

Sumiranjem ocjene od $k = 1$ do L te korištenjem trivijalne opservacije $J(n) \leq J(n+1)$ (ako postoji skup od n pravaca koji čine $J(n)$ zglobova, dodavanjem pravca ne možemo smanjiti taj broj) slijedi

$$J(L) \leq L(0) + \sum_{n=1}^{L} 3J(n)^{\frac{1}{3}} \leq L \cdot 3J(L)^{\frac{1}{3}}.$$

Konačno, iz posljednje nejednakosti slijedi $J(L) \leq 3^{\frac{3}{2}}L$ i time je tvrdnja dokazana.

□

2.5 Zadaci s natjecanja

Konačno, pokažimo kako iskoristiti navedene rezultate na dva teška natjecateljska problema.

Primjer 1 (IMO 2007, problem 6)**.** *Neka je $n \in \mathbb{N}$, $n > 1$. neka je*

$$S = \{(x, y, z) : x, y, z \in \{0, 1, \ldots, n\}, x + y + z > 0\}$$

skup od $(n+1)^3-1$ točaka u $\mathbb{R}^3$. Odredite najmanji broj ravnina čija unija sadrži sve elemente od S, ali ne sadrži točku $(0, 0, 0)$.

Rješenje. Primijetimo da unija $3n$ ravnina $\{(x, y, z) : x = i\}$, $\{(x, y, z) : y = i\}$, $\{(x, y, z) : z = i\}$, $i = 1, 2, \ldots, n$ zadovoljava tvrdnju. Pokažimo da je nemoguće zadovoljiti tvrdnju zadatka sa manje od $3n$ ravnina. Dokazat ćemo to na 2 načina.

1. način. Svaku ravninu koja ne prolazi točkom $(0, 0, 0)$ možemo zapisati u obliku $ax + by + cz + 1 = 0$. Pretpostavimo da je moguće pokriti sve točke u S sa $m < 3n$ ravnina, $a_i x + b_i y + c_i + 1 = 0$, $i = 1, 2, \ldots, m$ i definirajmo

$$P(x, y, z) = \prod_{i=1}^{m} (a_i x + b_i y + c_i z + 1).$$

Dodatno, definirajmo polinom stupnja $3n$ koji se poništava na ravninama kojima smo pokrili S i izbjegli $(0, 0, 0)$:

$$Q(x, y, z) := \prod_{i=1}^{n} [(x - i)(y - i)(z - i)].$$

Tada je polinom $R(x, y, z) := P(x, y, z) - \frac{Q(x,y,z)}{Q(0,0,0)}$ stupnja $3n$, poništava se na $\{0, 1, \ldots, n+1\}^3$ i koeficijent uz $x^n y^n z^n$ mu je jednak $\frac{1}{Q(0,0,0)} \neq 0$. Međutim, to je kontradikcija sa teoremom 6 koji kaže da bi za takav polinom morala postojati točka u $\{0, 1, \ldots, n+1\}^3$ u kojoj je različit od 0.

2. način. Pretpostavimo, kao i u prethodnom načinu, da je moguće zadovoljiti tvrdnju zadatka sa $m < 3n$ ravnina i definirajmo polinom $P(x, y, z)$ kao i ranije. Taj polinom ima svojstva $P(0, 0, 0) = 1 \neq 0$, P se poništava na $\{0, 1, \ldots, n\}^3 \setminus \{(0, 0, 0)\}$ i $\deg P = m < 3n$. Dokazat ćemo da polinom s takvim svojstvima stupnja manjeg od $3n$ može postojati samo ako je nulpolinom. Naime, definirajmo operator (negativne) konačne diferencije u smjeru $e_1 = (1, 0, 0)$ kao $\Delta^{(1)} f(x, y, z) := f(x, y, z) - f(x + 1, y, z)$ te analogno za e_2 i e_3. Primijetimo da djelovanje takvog operatora na polinom snižava stupanj polinoma barem za 1. Zbog uvjeta poništavanja polinoma p slijedi da se polinom $\Delta^{(1)} p$ poništava na $(\{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n\}^2) \setminus \{(0, 0, 0)\}$ i vrijedi $\Delta^{(1)} p(0, 0, 0) = 1$. Induktivno zaključujemo sad da se $(\Delta^{(1)})^n p$ poništava na $\{0\} \times \{0, 1, \ldots, n\}^2 \setminus \{(0, 0, 0)\}$ i vrijedi $(\Delta^{(1)})^n p(0, 0, 0) = 1$. Ponovimo li sad isto za smjerove e_2 i e_3, dobivamo da je $(\Delta^{(1)})^n (\Delta^{(2)})^n (\Delta^{(3)})^n p(0, 0, 0) = 1$. Međutim, zbog toga što je stupanj polinoma p jednak $m < 3n$, tada je polinom $(\Delta^{(1)})^n (\Delta^{(2)})^n (\Delta^{(3)})^n p$ nulpolinom pa mu vrijednost u $(0, 0, 0)$ ne može biti različita od 0 i time smo dobili kontradikciju. □

Primjer 2 (IMC 2007, problem 5)**.** *Neka su $a_1, \ldots, a_n \in \mathbb{Z}$ proizvoljni i neka je $f : \mathbb{Z} \to \mathbb{R}$ funkcija koja zadovoljava da je $\sum_{j=1}^{n} f(k+a_j l) =$ za sve $k, l \in \mathbb{Z}$, $l \neq 0$. Dokažite da je $f = 0$.*

Rješenje. Neka su $a_1 \leq \cdots \leq a_n$. Uvrštavanjem $k = k' - a_1 l$ i definiranjem $a'_j = a_j - a_1$, $j = 1, 2, \ldots, n$ vrijedi $a_1 = 0$, $a'_j \geq 0$ za $j \geq 2$ i uvjet je ekvivalentan s $\sum_{j=1}^{n} f(k' + a'_j l) = 0$. Dakle možemo bez smanjenja općenitosti pretpostaviti da je $0 = a_1 \leq \cdots \leq a_n$.

Kako je teško sistematično pratiti sve izraze koje možemo dobiti uvrštavajući razne k-ove i l-ove, ideja je povezati izraze s polinomima, s kojima jednostavno računamo. Uvrštavamo li u uvjet zadatka sada samo $k, l \geq 0$, $l \neq 0$ i promotrimo li linearne kombinacije takvih uvjeta, dobivamo izraze oblika:

$$\sum_{i=1}^{s} \alpha_i \left(\sum_{j=1}^{n} f(k_i + a_j l_i) \right) = 0. \tag{1}$$

Izlučimo li vrijednosti funkcija u istim točkama, dobivamo neke izraze oblika

$$\sum_{j=1}^{m} c_j f(t_j) = 0, \quad c_j \in \mathbb{R}, t_j \in \mathbb{N}_0.$$

Pridružimo sada svakom izrazu gornjeg oblika polinom $P \in \mathbb{R}[x]$ definiran s:

$$P(x) := \sum_{j=1}^{m} c_j x^{t_j}$$

te sa $I \subset \mathbb{R}[x]$ označimo skup svih polinoma koji se mogu dobiti kao linearna kombinacija izraza dobivenih uvrštavanjem svih $k \geq 0$ i $l > 0$. Tvrdimo da je sada dovoljno dokazati da je $I = \mathbb{R}[x]$. Naime, tada je $x^t \in I$ za sve $t \geq 0$, a to je na strani uvjeta ekvivalentno sa uvjetom $f(t) = 0$ za sve $t \in \mathbb{N}_0$. Za proizvoljan $t < 0$ uvrštavanjem $k = t$ i l dovoljno velikog, tako da je $la_2 + t > 0$ u početnu jednakost dobijemo i da je $f(t) = 0$ za sve $t \in \mathbb{Z}$ i time je tvrdnja zadatka dokazana.

Dokažimo sada da je $I = \mathbb{R}[x]$. Neka je $\sum_{j=1}^{m} c_j f(t_j) = 0$ proizvoljan izraz dobiven kao linearna kombinacija uvjeta kao u (1). Uvrštavanjem $k'_i = k_i + 1$ u (1) slijedi $\sum_{j=1}^{m} c_j f(t_j + 1) = 0$ pa je na polinomijalnoj strani taj je uvjet ekvivalentan sa tvrdnjom da je skup I zatvoren na množenje sa x, tj. $P(x) \in I \implies xP(x) \in I$. Međutim, korištenjem te tvrdnje više puta, slijedi da je I zatvoren na množenje proizvoljnim polinomom. čitatelj upoznat sa osnovnim algebarskim strukturama prepoznat će da je I je zapravo ideal u prstenu polinoma $\mathbb{R}[x]$, ali to nije nužno za nastavak rješenja.

Bezoutova lema za polinome, kaže da ako su $A, B \in \mathbb{R}[x]$ polinomi koji su relativno prosti (nemaju zajedničku nultočku), tada postoje polinomi $P, Q \in \mathbb{R}[x]$ takvi da je $AP + BQ = 1$. Dakle, dovoljno je pokazati da u I postoje dva polinoma koja nemaju zajednički faktor jer tada zaključujemo da je $1 \in I$ pa množenjem sa proizvoljnim polinomom $P \in \mathbb{R}[x]$ zaključujemo da je i $P = P \cdot 1 \in I$.

Uvrštavanjem $k = 0$ i $l \in \mathbb{N}$ u uvjet zadatka, slijedi da su polinomi $P_l(x) = \sum_{j=1}^{n} x^{la_j} \in I$. Tvrdimo da postoji l takav da su $P_1(x)$ i $P_l(x) = P_1(x^l)$ relativno prosti, odnosno ako označimo sa S skup nultočaka od P_1, da postoji $l \in \mathbb{N}$ takav da za sve $z \in S$ vrijedi $z^l \notin S$.

Ako je $|z| \neq 1$, onda $|z|^l \to 0$ ili $|z|^l \to \infty$ pa kako je S konačan, postoji l_0 takav da su svi $l > l_0$ dobar izbor pa preostaje provjeriti z takve da je $|z| = 1$. Ukoliko je $z = e^{2\pi i\alpha}$ za $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, tada zbog konačnosti skupa S opet postoji l_1 takav da su svi $l > l_1$ dobri. Konačno, u slučaju da je $z = e^{2\pi i\frac{p}{q}}$ za neke $p, q \in \mathbb{N}$, tada je svaki višekratnik od q dobar jer $1 \notin S$. Dakle, svaki $l > \max(l_0, l_1)$, koji je i višekratnih svih $q \in \mathbb{N}$ za koje postoji q-ti korijen iz jedinice u skupu nultočaka od P_1 je dobar. □

3 Zadaci za zadaću

Svaki zadatak nosi jedan bod, a ukoliko zadatak ima dva dijela, svaki dio nosi 0.5 bodova. Za uspješno polaganje zadaće potrebno je skupiti barem 5 bodova.

1. Dokažite da za $A, B \subset \mathbb{R}$ vrijedi ocjena $|A|+|B|-3 \leq |A\dot{+}B| \leq |A||B|$ i nađite skupove za koje se postiže jednakost.

2. (a) Nadopunite dokaz teorema 8, tj. dokažite da za p prost i $A, B \subset \mathbb{F}_p$, takve da je $|A| + |B| \geq p + 1$ vrijedi $|A + B| \geq p$.

   (b) Nadopunite dokaz teorema 9, tj. dokažite da za $p > 2$ prost i $A \subset \mathbb{F}_p$ takav da je $2|A| - 3 \geq p$ vrijedi tvrdnja teorema.

   Uputa. Iskoristite Dirichletov princip.

3. Cilj zadatka je osmisliti sustav za osiguranje aktiviranja nuklearnog oružja koji je otporan na urote manje grupe pojedinaca. Za aktivaciju nuklearnog oružja potrebno je upisati neki aktivacijski broj. Za $n \in \mathbb{N}$, osmislite način za podijeliti informacije o aktivacijskoj šifri grupi generala tako da bilo kojih n generala može aktivirati nuklearnu bombu, ali nikojih $n - 1$ nema dovoljno informacija da bi to moglo.

4. Pokazali smo kod dokaza "problema sa zglobovima" da za n točaka u $\mathbb{R}^3$ postoji netrivijalan polinom stupnja najviše $3n^{\frac{1}{3}}$ koji se poništava na njima. Dokažite da za n pravaca u $\mathbb{R}^3$ postoji neki $C > 0$ i polinom stupnja najviše $Cn^{\frac{1}{2}}$ koji se poništava na svim pravcima.

5. U svakom vrhu pravilnog mnogokuta sa 100 vrhova upisana su 2 realna broja. Dokažite da je moguće obrisati iz svakog vrha po jedan tako da među preostalim brojevima svaka dva u susjednim vrhovima budu različita.

   Uputa. Iskoristite teorem 6.

6. Dokažite sljedeće poopćenje Erdos - Heilbronnove slutnje. Ako su $A, B \subset \mathbb{F}_p$, tada vrijedi $|A\dot{+}B| \geq \min(|A| + |B| - 3, p)$.

   Uputa. Imitirajte dokaz Erdos - Heilbronnove slutnje.

7. Dano je n obojanih točaka u $\mathbb{R}^3$ i u svakom koraku dopušteno je napraviti sljedeće. Ako postoji pravac na kojem su obojane 3 točke, možemo obojati bilo koju četvrtu točku na pravcu.

(a) Dokažite da je moguće odabrati $\binom{6}{3} = 20$ točaka tako da se proizvoljna točka u $\mathbb{R}^3$ može dopuštenim postupkom obojati u konačno mnogo koraka.

(b) Pokažite da za bilo koji $n < \binom{6}{3} = 20$ postoji točka u prostoru koju nije moguće obojati opisanim postupkom.

Uputa. Za drugi dio pronađite polinom malog stupnja tako da opisanim postupkom ne možemo izaći iz skupa njegovih nultočaka.

8. Za skup $S \subset \mathbb{R}^n$ kažemo da je *k-terostruko zanimljiv* ako je skup udaljenosti između svake dvije različite točke skupa S skup veličine k.

(a) Dokažite da jednostruko zanimljiv skup u $\mathbb{R}^n$ može imati najviše $n + 1$ točaka i nađite primjer takvog skupa.

(b) Dokažite da dvostruko zanimljiv skup u $\mathbb{R}^n$ ne može imati više od $\frac{(n+1)(n+4)}{2}$ točaka. Primjer nije potrebno naći jer se ne zna postoji li.

Uputa. U prvom dijelu zadatka pretpostavite da je jedna točka jednaka 0 i promotrite Gramovu matricu ostalih točaka. U drugom dijelu zadatka pronađite n linearno nezavisnih polinoma $P_1, \ldots, P_n$ stupnja 4 pridruženih točkama skupa i zatim iz specifičnog oblika dokažite da se nalaze u nekom vektorskom prostoru dimenzije najviše $\frac{(n+1)(n+4)}{2}$.

Literatura

[Alo99] Noga Alon. "Combinatorial Nullstellensatz". Sv. 8. 1-2. Recent trends in combinatorics (Mátraháza, 1995). 1999., str. 7–29. DOI: 10.1017/S0963548398003411. URL: https://doi.org/10.1017/S0963548398003411.

[Mic10] Mateusz Michałek. "A short proof of combinatorial Nullstellensatz". *Amer. Math. Monthly* 117.9 (2010.), str. 821–823. ISSN: 0002-9890. DOI: 10.4169/000298910X521689. URL: https://doi.org/10.4169/000298910X521689.

[Gut12] Larry Guth. *The polynomial method course*. 2012. URL: https://math.mit.edu/~lguth/PolynomialMethod.html.

[Gut16] Larry Guth. *Polynomial methods in combinatorics*. Sv. 64. University Lecture Series. American Mathematical Society, Providence, RI, 2016., str. ix+273. ISBN: 978-1-4704-2890-7. DOI: 10.1090/ulect/064. URL: https://doi.org/10.1090/ulect/064.