Математичка гимназија

МАТУРСКИ РАД

- из математике -

Комбинаторна алгебарска геометрија

Ученица:
Јелена Иванчић IVд

Ментор:
Лука Милићевић

Београд, јун 2020.

Садржај

1 Увод **1**

2 Рад Елекеша и Шарира **3**

3 Више о праволинијским површима **9**

4 Подели па владај **19**

5 Закључак **31**

А Шта је то регулус **33**

Б Безуова теорема **35**
Б.1 Иредуцибилни полиноми и јединственост факторизације 35
Б.2 Резултанта два полинома 37
Б.3 Безу 40

Ц Доказ оцена за квадрат $\sqrt{N} \times \sqrt{N}$ **43**

Литература **45**

1

Увод

У [Е], Ердош је поставио питање: колики је најмањи број различитих растојања између N тачака у равни? Проверио је да је за квадратну решетку $\sqrt{N} \times \sqrt{N}$ одговор $\sim \frac{N}{\sqrt{\log N}}$, па је предложио доњу оцену $\gtrsim \frac{N}{\sqrt{\log N}}$ (где $A \gtrsim B$ значи да постоји универзална константа $C > 0$ таква да $A > CB$ независно од променљивих у функцијама A и B).

Прве оцене које су добијене биле су облика $\gtrsim N^{1-c}$, са почетном оценом $\gtrsim N^{2/3}$ из 1952. године, па све до оцене $\gtrsim N^{0.8641}$ Каца и Тардоша из 2004. године. Онда су у [ГК] Гут и Кац направили огроман помак ка Ердошевој хипотези и доказали:

Теорема 1. Број различитих растојања између N тачака у равни је $\gtrsim \frac{N}{\log N}$.

Ми ћемо у овом раду приказати њихов доказ Теореме 1. У првом делу рада осврнућемо се на идеју Елекеша и Шарира која повезује почетни проблем са следећом теоремом геометрије инциденција:

Теорема 2. Нека је $\mathcal{L}$ скуп од N^2 правих из $\mathbb{R}^3$ таквих да највише cN њих лежи у равни, односно регулусу, за неку константу $c > 0$. Ако је $2 \leq k \leq N$, онда је број тачака која леже на бар k правих из $\mathcal{L}$ највише $\lesssim_c N^3 k^{-2}$.

(Регулус је површ одређена са два скупа мимоилазних правих за које важи да свака права из једног сече сваку праву из другог и унија правих из једног скупа је једнака унији правих из другог скупа. Нотација $\lesssim_c$ значи да наша скривена константа зависи од c.)

У скорије време је дошло до нових идеја у геометрији инциденција које у сржи имају алгебарске методе. Тако је у [Д], на пример, Двир доказао хипотезу Какеје за коначна поља тако што је направио полином довољно малог степена који се анулира на великом броју правих које је посматрао. Занимљиво је то што се овај проблем сматрао доста тешким, а онда је нађено решење које стаје на једну страну користећи овакав приступ. Из таквог разлога се сматра да је то

решење било "намењено" за тај проблем. Касније су откривена решења разних познатих проблема геометрије инциденција која су такође била заснована на алгебарским методама. Рад Гута и Каца је један такав прелеп спој алгебре и геометрије.

У другом делу рада доказаћемо Теорему 2 за $k = 2$. Биће нам битан појам *праволинијских* површи и веза између њих и полинома. Напоменимо да је у овом случају битно ограничење да $\lesssim N$ правих лежи у регулусу, јер уколико то не би важило, имајући у виду претходну дефиницију регулуса, можемо да направимо да су $N^2/2$ њих у једном, а $N^2/2$ у другом скупу мимоилазних правих, што би дало $\sim N^4$ инциденција. Ово, међутим, не важи за $k \geq 3$.

У трећем делу се бавимо доказом Теореме 2 за $k \geq 3$. Кључна идеја која је довела до оцене је дељење простора на ћелије у којима су "равномерно" распоређене тачке које посматрамо. Поред тога, уводимо појмове критичних и равних тачака и продубљујемо везу између алгебре и геометрије.

На крају, у додатку ћемо јасно дефинисати регулус, доказати Безуову теорему која је од суштинске важности и видети да је оцена из Теореме 2 оштра за случај квадратне решетке $\sqrt{N} \times \sqrt{N}$, односно за праве додељене њој по принципу другог поглавља.

2

Рад Елекеша и Шарира

У овом поглављу ћемо видети како се Ердошев проблем различитих растојања своди на геометријски проблем инциденција у 3 димензије.

Нека је $P \subset \mathbb{R}^2$ скуп од N тачака у равни. Означимо са $d(P)$ скуп различитих растојања између тачака у P. Ми желимо да докажемо да је $|d(P)| \gtrsim \frac{N}{\log N}$. Идеја је да, уколико је $|d(P)|$ мало, онда посматрајући геометријске структуре које чине подскупови скупа тачака P, уочавамо много њих које су изометријски исте. Другим речима, имало би смисла гледати шта се дешава са нашим скупом P када на њега применимо неку изометријску трансформацију g.

Нека је $Q(P)$ скуп четворки тачака $(p_1, p_2, p_3, p_4) \in P^4$ које задовољавају $d(p_1, p_2) = d(p_3, p_4) \neq 0$. Важи следеће тврђење:

Лема 3. Сваки скуп $P \subset \mathbb{R}^2$ са N тачака задовољава

$$|d(P)| \geq \frac{(N^2 - N)^2}{|Q(P)|}.$$

Доказ. Нека су $d_1, d_2, .., d_m$ сва могућа различита растојања међу тачкама у P, где је $m = |d(P)|$, и нека је n_i број парова $(p_j, p_k) \in P^2$ тако да је $d(p_j, p_k) = d_i$, за $i \in 1, 2, .., m$. Тада је очигледно да $\sum_{i=1}^{m} n_i = N^2 - N$ и $|Q(P)| = \sum_{i=1}^{m} n_i^2$, па на основу неједнакости Коши-Шварца добијамо:

$$|Q(P)| \cdot m = \Big(\sum_{i=1}^{m} n_i^2\Big) \cdot \Big(\sum_{i=1}^{m} 1\Big) \geqslant \Big(\sum_{i=1}^{m} n_i\Big)^2 = \Big(N^2 - N\Big)^2$$

тј.

$$|d(P)| \geqslant \frac{(N^2 - N)^2}{|Q(P)|},$$

што је и требало доказати. □

Дакле, да бисмо доказали Теорему 1, довољно је доказати:

Тврђење 4. За сваки скуп $P \subset \mathbb{R}^2$ са N тачака, $|Q(P)| \lesssim N^3 \cdot \log N$.

Посматрајмо сада групу G свих изометријских трансформација добијеним слагањем транслације и ротације. Тада за сваку четворку $(p_1, p_2, p_3, p_4) \in Q(P)$ постоји јединствена трансформација $g \in G$ тако да $g(p_1) = p_3$ и $g(p_2) = p_4$ (ако запишемо g у односу на p_1 као $R \cdot (x - p_1) + t$, где је R матрица ротације, а t вектор транслације, онда из $g(p_1) = p_3$ добијамо $t = p_3 - p_1$, а из $g(p_2) = p_4$ јединствено одређујемо R).

Овиме смо добро дефинисали пресликавање $E : Q(P) \to G$. Сада нам је циљ да ограничимо одоздо $Q(P)$ помоћу E. Иако ово пресликавање не мора бити инјективно, приметимо да постоји јасна веза између $P \cap gP$ и $E^{-1}(g)$. Наиме, важи следеће:

Лема 5. Нека је $g \in G$ и $|P \cap gP| = k$. Тада је $|E^{-1}(g)| = 2 \cdot \binom{k}{2}$.

Доказ. Нека је $P \cap gP = \{q_1, q_2, .., q_k\}$. Из $q_i \in gP$ следи да постоји $p_i \in P$ тако да $g(p_i) = q_i$, при чему важи $p_i \neq p_j$ за $i \neq j$. За свако $1 \leq i, j \leq k, i \neq j$, важи да $(p_i, p_j, q_i, q_j) \in Q(P)$ и $E((p_i, p_j, q_i, q_j)) = g$ тј. $(p_i, p_j, q_i, q_j) \in E^{-1}(g)$, одакле добијамо $|E^{-1}(g)| \geq 2 \cdot \binom{k}{2}$. Такође, ако је $(r_1, r_2, r_3, r_4) \in Q(P)$ такво да $E((r_1, r_2, r_3, r_4)) = g$ онда $r_3 = g(r_1) = q_i$ и $r_4 = g(r_2) = q_j$ за неко $i, j \in [k]$, $i \neq j$. Дакле, $|E^{-1}(g)| = 2 \cdot \binom{k}{2}$. □

Означимо са $G_{=k}(P) \subset G$ скуп свих $g \in G$ за које важи $|P \cap gP| = k$. На основу претходне леме закључујемо:

$$|Q(P)| = \sum_{i=2}^{N} 2 \cdot \binom{i}{2} \cdot |G_{=i}(P)|.$$

Дефинишимо $G_k(P) \subset G$ као скуп свих $g \in G$ за које важи $|P \cap gP| \geq k$. Користећи $|G_{=k}(P)| = |G_k(P)| - |G_{k+1}(P)|$ и претходну једначину добијамо:

$$|Q(P)| = \sum_{k=2}^{N} 2 \cdot \binom{k}{2} \cdot (|G_k(P)| - |G_{k+1}(P)|) = \sum_{k=2}^{N} 2 \cdot (k-1) \cdot |G_k(P)|.$$

Сада да бисмо доказали Тврђење 4 довољно је доказати

$$|G_k(P)| \lesssim N^3 \cdot k^{-2}, \tag{2.1}$$

за $k \in \{2, 3, .., N\}$.

Означимо са $G_k^{trans}(P) = \{g \in G_k(P) \mid g \text{ је транслација}\}$, а са $G_k'(P) = G_k(P) \setminus G_k^{trans}(P)$. Докажимо (2.1) прво за $G_k^{trans}(P)$.

Доказ (2.1) за G_k^{trans}. Нека је $g \in G_k^{trans}(P)$ и $(p_1, p_2, p_3, p_4) \in Q(P)$ таква да је $g(p_1) = p_3$ и $g(p_2) = p_4$ (односно $E((p_1, p_2, p_3, p_4)) = g$). Како је g транслација, из претходног следи да је $p_3 - p_1 = p_4 - p_2$ тј. $p_4 = p_3 + p_2 - p_1$, што значи да постоји највише N^3 четворки у $Q(P) \cap E^{-1}(G_k^{trans}(P))$. На основу Леме 5, $E^{-1}(g) \geq k(k-1)$ за свако $g \in G_k^{trans}$, одакле закључујемо да је $G_k^{trans} \lesssim N^3 k^{-2}$. □

Фокусирајмо се на $G_k'(P)$ сада. Природно је посматрати скупове $S_p(q) = \{g \in G' \mid g(p) = q\}$, за свако $p, q \in P$, где је $G' = \{g \in G \mid g \text{ није транслација}\}$, јер на основну њих можемо да дефинишемо све $g \in G_k'(P)$. Наиме, то су све оне трансформације које се налазе у пресеку неких k скупова облика $S_p(q)$. Главна идеја Елекеша и Шарира је да сада ове скупове $S_p(q)$ претворимо у криве из $\mathbb{R}^3$. Гут и Кац су искористили ову идеју и додатно је унапредили у свом раду, гарантујући да ће те криве бити заправо праве, чиме су избегли техничке непогодности.

Посматрајмо произвољну трансформацију $g \in S_p(q)$: она има јединствену фиксну тачку (x, y) која лежи на симетрали странице pq и око које се одвија ротација за неки угао $0 < \phi < 2\pi$. Лако се добија да је растојање тачке (x, y) од тачке $\frac{p+q}{2}$ функција од p, q и $ctg\frac{\phi}{2}$, па има смисла да посматрамо 1-1 пресликавање $F : G' \to \mathbb{R}^3$ тако да је $F(g) = (x, y, ctg(\frac{\phi}{2}))$, где су x, y, ϕ изабрани као малочас. Може се лако доказати да је, за тачке $p = (p_x, p_y)$ и $q = (q_x, q_y)$ у $\mathbb{R}^2$, $F(S_p(q)) = L_p(q)$ права у $\mathbb{R}^3$ параметризована са:

$$\Big(\frac{p_x + q_x}{2}, \frac{p_y + q_y}{2}, 0\Big) + t\Big(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1\Big). \tag{2.2}$$

Приметимо да се на основну претходне параметризације следи да

$$(p, q) \neq (r, s) \implies L_p(q) \neq L_r(s) \ (*).$$

Онда, $g \in G_k'(P)$ акко $F(g)$ лежи у пресеку бар k права облика $L_p(q)$, где $p, q \in P$. Значи, желимо да докажемо да је број тачака које се налазе у пресеку бар k датих правих $\lesssim N^3 \cdot k^{-2}$, што је скоро па Теорема 2, само нам још фали услов за број правих које леже у истој равни, односно регулусу. Нека је $p \in P$. Дефинишимо $\mathcal{L}_p$ као скуп свих правих $L_p(q)$ за све $q \in P$, и $\mathcal{L}_p'$ као скуп свих правих $L_p(q)$ за све $q \in \mathbb{R}^2$. Нека је $\mathcal{L} = \bigcup_{p \in P} \mathcal{L}_p$. Да бисмо свели почетни проблем на Теорему 2 остаје још да покажемо:

Тврђење 6. Број правих из $\mathcal{L}$ које леже у истој равни, односно регулусу, је $\lesssim N$.

Приметимо да због (2.2) важи да су било које две различите праве у $\mathcal{L}_p$ мимоилазне (због $(*)$ важи $|\mathcal{L}_p| = |P| = N$ и $|\mathcal{L}| = N^2$), стога ниједна раван не може да садржи више од N правих из $\mathcal{L}$. Што се тиче регулуса, поменимо

његову дефиницију још једном: то је површ која се састоји из два скупа мимоилазних правих R_1 и R_2, таква да свака права из првог скупа сече сваку праву из другог, и за сваку тачку у регулусу постоје праве $p_1 \in R_1$ и $p_2 \in R_2$ које пролазе кроз њу. Ова два скупа мимоилазних правих ћемо звати *покривачима* у регулусу. Регулус се такође може дефинисати као скуп свих правих које секу одређене 3 мимоилазне праве. У додатку А стоји скица доказа да из претходне дефиниције следи да је регулус иредуцибилна алгебарска површ степена 2, тј. да је то површ дефинисана са $P(x, y, z) = 0$, где је P иредуцибалан полином степена 2 по три променљиве.

Да бисмо доказали Тврђење 6, довољно је доказати следећу лему:

Лема 7. Нека је R произвољан регулус у $\mathbb{R}^3$. Ако R садржи више од 8 правих из $\mathcal{L}_p$, за неко $p \in P$, онда цео један покривач регулуса лежи у $\mathcal{L}'_p$.

Наиме, из ове леме, и на основу кратког доказа из додатка А да регулус не може имати 3 различита покривача, можемо закључити да постоје највише два различита $p \in P$ таква да је $|R \cap \mathcal{L}_p| \geq 9$ што би значило да је $|R \cap \mathcal{L}| = \sum_{p \in P} |R \cap \mathcal{L}_p| \leq 8 \cdot (|P| - 2) + 2 \cdot N \lesssim N$, чиме бисмо завршили доказ Тврђења 6.

Доказ леме 7. Нека је R дефинисан преко иредуцибилног полинома P другог степена. Посматрајмо неку праву кроз тачку $x = (x, y, z)$ са правцем $v = (v_x, v_y, v_z)$ која лежи у R. Онда, за свако $t \in \mathbb{R}$ важи да је $P(x + t \cdot v) = 0$. Ако то посматрамо као полином по t, како је он нула за свако $t \in \mathbb{R}$, онда коефицијенти тог полинома морају да буду нула, па добијамо 3 (у општем случају $\deg P + 1$) једначина по x, y, z, v_x, v_y, v_z:

1. $P(x, y, z) = 0$
2. $Q(x, y, z, v_x, v_y, v_z) = \frac{\partial P}{\partial x} \cdot v_x + \frac{\partial P}{\partial y} \cdot v_y + \frac{\partial P}{\partial z} \cdot v_z = 0$
3. $T(x, y, z, v_x, v_y, v_z) = \sum_{cyc} (\frac{\partial^2 P}{\partial x^2} \cdot \frac{v_x^2}{2} + \frac{\partial^2 P}{\partial x \partial y} \cdot v_x \cdot v_y) = 0$, циклична сума по x, y, z.

Сада је идеја да конструишемо полиноме малог степена (прецизније другог степена) V_x, V_y, V_z такве да за било коју тачку $x \in \mathbb{R}^3$, $(V_x(x), V_y(x), V_z(x))$ представља правац праве из $\mathcal{L}'_p$ која пролази кроз њу (доказаћемо мало касније да таква права заиста постоји). За тренутак претпоставимо да постоје такви полиноми V_x, V_y, V_z. Посматрајмо праву из $\mathcal{L}_p$ која лежи у R и тачку $\mathbf{x} = (x, y, z)$ на њој. Онда је $P(\mathbf{x}) = 0$, $Q(x, y, z, V_x(\mathbf{x}), V_y(\mathbf{x}), V_z(\mathbf{x})) = Q'(\mathbf{x}) = 0$, и $T(x, y, z, V_x(\mathbf{x}), V_y(\mathbf{x}), V_z(\mathbf{x})) = T'(\mathbf{x}) = 0$, где су Q', T' добијени полиноми по x, y, z трећег и четвртог степена, редом. Значи, за сваку праву из $\mathcal{L}_p$ на којој се P анулира, на њој се анулирају и Q' и T'. Како је број таквих правих

$|R \cap \mathcal{L}_p| \geq 9 = 2 \cdot 4 + 1$, на основу Безуове теореме (детаљније у трећој глави и у додатку Б), P и Q', односно P и T', морају да имају заједничког делиоца. Како је P иредуцибилан полином, добијамо да P дели Q' и T', односно да за сваку тачку $\mathbf{x} \in R$ важи $Q'(\mathbf{x}) = T'(\mathbf{x}) = 0$. То значи да су за сваку тачку $\mathbf{x} \in R$ задовољене једначине $1, 2$, и 3 за правац $(V_x(\mathbf{x}), V_y(\mathbf{x}), V_z(\mathbf{x}))$, одакле следи да права кроз $\mathbf{x}$ са тим правцем лежи у регулусу. Међутим, она по дефиницији V_x, V_y, V_z лежи и у $\mathcal{L}'_p$, одакле закључујемо да постоји покривач регулуса који је сасвим у $\mathcal{L}'_p$.

Конструишимо сада полиноме V_x, V_y, V_z. Посматрајмо произвољну тачку $(x, y, z) \in \mathbb{R}^3$, желимо да нађемо праву $L_p(q)$ у $\mathcal{L}'_p$ која пролази кроз њу. Из (2.2) треба да решимо по q_x, q_y, t следећу једначину:

$$\Big(\frac{p_x + q_x}{2}, \frac{p_y + q_y}{2}, 0\Big) + t\Big(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1\Big) = (x, y, z)$$

Одавде се лако добија $t = z$, $zq_y + q_x = 2x + zp_y - p_x$ и $q_y - zq_x = 2y - p_y - zp_x$ односно:

$$(z^2 + 1)q_y = 2xz + z^2 p_y - zp_x + 2y - p_y - zp_x$$

и

$$(z^2 + 1)q_x = 2x + zp_y - p_x - 2yz + zp_y + z^2 p_x$$

па су онда $(V_x(x, y, z), V_y(x, y, z), V_z(x, y, z)) = (z^2 + 1) \cdot (\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1)$ очигледно полиноми другог степена који задовољавају тражени услов, чиме смо завршили доказ. □

Дакле, остаје нам да докажемо:

Теорема 8. Дато је N^2 правих у $\mathbb{R}^3$ за које $\leq cN$ њих леже у истој равни, односно регулусу, за неку константу $c > 0$. Нека је $2 \leq k \leq N$. Тада је број тачака које се налазе у пресеку бар k датих правих $\lesssim_c N^3 \cdot k^{-2}$.

Нотација $\lesssim_c$ значи да наша скривена константа зависи од c. Као што смо рекли у уводу, раздвајамо случај $k = 2$ и $k \geq 3$. У следећем поглављу ћемо доказати:

Теорема 9. Нека је $\mathcal{L}$ скуп N^2 правих у $\mathbb{R}^3$ за које $\leq cN$ њих леже у истој равни, односно регулусу, за неку константу $c > 0$. Број тачака које се налазе у пресеку бар две праве из $\mathcal{L}$ је $\lesssim_c N^3$.

3

Више о праволинијским површима

Да би доказали Теорему 9 конструисаћемо полином p довољно малог степена који ће се анулирати на великом броју правих које ћемо посматрати. Идеја је да, ако постоји неки други полином q малог степена као p такав да је и он нула на датим правама, онда можемо да искористимо варијанту Безуове теореме у три димезије (детаљније у додатку Б):

Лема 10 (Безу)**.** Нека су $p(x, y, z)$ и $q(x, y, z)$ полиноми у $\mathbb{R}[x, y, z]$ степена m и n редом. Ако се p и q анулирају у више од $mn + 1$ различитих правих, онда p и q имају заједнички фактор.

Очигледно је да ова теорема од посебне користи ако је један од полинома p, q иредуцибилан. Зато су нам од великог значаја површи (ми ћемо се бавити само онима које су описане као нуле неког полинома) које имају доста правих у себи.

Дефиниција 11. Површ $\mathcal{S}$ се назива *праволинијска* површ ако за сваку тачку $x \in \mathcal{S}$ постоји права која пролази кроз њу и лежи у $\mathcal{S}$.

Дводимензиона диференцијабилна вишеструкост је праволинијска површ ако се може представити у облику:

$$x(t, v) = \alpha(t) + v \cdot w(t), v \in \mathbb{R},$$

где су α, w диференцијабилне функције из $I = (0, 1)$ у $\mathbb{R}^3$ при чему важи $w(t) \neq 0$ за $t \in I$. За фиксирано $t \in I$, права кроз $\alpha(t)$ са правцем $w(t)$ се назива *генератор* праволинијске површи. За нас је важно то што генератори формирају "непрекдину" фамилију правих чија унија чини целу површ.

Сада би било добро да видимо када важи да је површ $\mathcal{S}$ праволинијска. Нека је p полином чији скуп нула представља $\mathcal{S}$ и нека је $\mathbf{x} = (x, y, z)$ произвољна тачка у $\mathcal{S}$. Налик доказу леме 7, приметимо да постоји права која пролази кроз $\mathbf{x}$ и лежи у $\mathcal{S}$ акко постоји $\mathbf{v} = (v_x, v_y, v_z) \in \mathbb{R}^3 \setminus \{0\}$ тако да је $p(\mathbf{x} + t \cdot \mathbf{v}) = 0$ за свако $t \in \mathbb{R}$, што посматрајући као полином по t, важи акко су задовољене одређене $\deg(p) + 1$ полиномске једначине по x, y, z, v_x, v_y, v_z. Испоставља се да је довољно гледати само прве четири дате једначине (под претпоставком $\deg(p) \geq 3$):

$$p(x, y, z) = 0; \qquad \nabla_{\mathbf{v}} p(x, y, z) = 0; \qquad \nabla^2_{\mathbf{v}} p(x, y, z) = 0; \qquad \nabla^3_{\mathbf{v}} p(x, y, z) = 0 \quad (3.1)$$

где $\nabla^i_{\mathbf{v}} p(x, y, z) = 0$ представља полином по x, y, z, v_x, v_y, v_z који се налази уз t^i у $p(\mathbf{x} + t \cdot \mathbf{v}) = 0$. Последње три једначине су хомогене једначине првог, другог и трећег степена редом по v_x, v_y, v_z, па их можемо свести на једну полиномску једначину[1]

$$Fl(p)(x, y, z) = 0$$

при чему важи $\deg(Fl(p)) \leq 11 \deg(p) - 24$ (детаљи су концептуално јасни, али је доказ мало дужи, па дајемо само скицу). Овај полином се назива *превојни* полином полинома p, тачка $\mathbf{x}$ за коју је испуњено (3.1) за неко $\mathbf{v} \in \mathbb{R}^3 \setminus \{0\}$ се назива *превојном* тачком, а за праву кроз $\mathbf{x}$ са правцем $\mathbf{v}$ кажемо да додирује $\mathcal{S}$ до степена 3.
Очигледно је да ако је $\mathcal{S}$ праволинијска онда $Fl(p) = 0$ на $\mathcal{S}$. Испоставља се да важи и обратно:

Теорема 12 (Кејли-Салмон)**.** Површ $p = 0$ је праволинијска ако и само ако се $Fl(p)$ анулира на њој.

Доказ ове теореме је захтевнији, може се наћи у [Салм] и [К]. Нама је важнија следећа последица:

[1] На пример:

1. Поделимо све три једначине редом са v_x, v_x^2 и v_x^3; тиме смо добили 3 једначине са две непознате;
2. Како је једна од тих једначина првог степена, можемо да изразимо једну од променљивих преко друге, чиме добијамо два полинома по једној променљивој, рецимо t, са коефицијентима x, y, z;
3. Знамо да постоји v_x, v_y, v_z, са $v_x \neq 0$ које задовољава (3.1) акко ова два добијена полинома имају заједничку нулу што се, користећи резултате из додатка Б, дешава акко је њихова резултанта - полином по x, y, z - нула у $\mathbf{x}$;
4. Наш полином је производ те 3 добијене резултанте (када елиминишемо v_x, v_y, односно v_z, прво).

Последица 13. Нека је $p \in \mathbb{R}[x,y,z]$ полином степена d. Ако се p анулира на више од $11d^2 - 24d$ правих, онда постоји иредуцибилан фактор q полинома p такав да је површ $q = 0$ праволинијска.

Доказ. Нека је $p = q_1 \cdot q_2 \cdot ... \cdot q_k$ факторизација полинома p на иредуцибилне факторе. Ако је $\mathbf{s}$ права која лежи у $p = 0$, за бар једно од $i \in \{1,2,...,k\}$ важи да је $q_i(x) = 0$ за бар $\deg(q_i) + 1$ тачака $x \in \mathbf{s}$ (јер $p(x) = q_1(x) \cdot q_2(x) \cdot ... \cdot q_k(x) = 0$, $x \in \mathbf{s}$). Нека је v правац $\mathbf{s}$ и $x \in \mathbf{s}$ произвољна тачка на правој. Полином $q_i(x + tv)$ је нула у бар $\deg(q_i) + 1$ различитих реалних вредности t, па је он идентички једнак нули, одакле следи да права $\mathbf{s}$ лежи у $q_i = 0$. Стога, свака праву која лежи у $p = 0$, лежи и у неком $q_i = 0$, за $i \in \{1,2,...,k\}$. Како је $\sum_{i=1}^{k} \deg(q_i) = \deg(p) = d$ и више од $11d^2 - 24d$ правих лежи у $p = 0$, мора постојати $i \in \{1,2,...,k\}$ за које више од $11\deg(q_i)^2 - 24\deg(q_i)$ правих лежи у $q_i = 0$. Како свака права која лежи у $q_i = 0$ лежи и у $Fl(q_i) = 0$, из Безуове леме (Лема 10) добијамо да постоји нетривијални заједнички делилац q_i и $Fl(q_i)$. Пошто је q_i иредуцибилан, следи да q_i дели $Fl(q_i)$, па на основу Теореме 12, закључујемо да је $q_i = 0$ праволинијска површ. □

Вратимо се сада на почетну идеју. Посматрајмо неки полином p степена мањег од N (то се испоставља да је довољно мало) и површ

$$p(x,y,z) = 0.$$

Полином p се може јединствено факторизовати на иредуцибилне полиноме:

$$p = p_1 p_2 ... p_m$$

и кажемо да је површ $p = 0$ *без равни и регулуса* уколико ниједан $p_i = 0$ није раван нити регулус, $0 < i \leq m$. Следећа лема је кључна у доказивању Теореме 9.

Лема 14. Нека је p полином степена мањег од N и $\mathcal{S} = \{(x,y,z) |\ p(x,y,z) = 0\}$ праволинијска површ без равни и регулуса. Нека је $\mathcal{L}_1$ скуп правих које леже у $\mathcal{S}$ за који важи $|\mathcal{L}_1| \leq N^2$, и нека је Q_1 скуп тачака које леже на две или више правих из $\mathcal{L}_1$. Тада је

$$|Q_1| \lesssim N^3$$

Пре него што докажемо ову лему, позабавимо се још мало са праволинијским површима. Сада већ примећујемо да што више правих једна површ има у себи, то лакше радимо са њом. Праволинијске површи за које важи

да кроз сваку њихову тачку пролазе бар две праве које леже у њима називамо *двоструко-праволинијске* површи (у супротном се називају *једноструко-праволинијске* површи). Видећемо ускоро да су једине двоструко-праволинијске површи описане иредуцибилним полиномом заправо раван и регулус.

Нека је $p(x, y, z)$ иредуцибилан полином и S површ описана њиме (односно $p = 0$ површ) која није раван или регулус. За тачку $(x, y, z) \in S$ кажемо да је *сјајна тачка* ако лежи на бесконачно много правих у S. За праву l у S кажемо да је *сјајна права* ако постоји бесконачно много правих у S које секу l у не-сјајним тачкама. Важи следећа лема:

Лема 15. 1. Нека је (x_0, y_0, z_0) сјајна тачка у S. Онда, за сваку тачку (x, y, z) у S, права l која пролази кроз (x, y, z) и (x_0, y_0, z_0) лежи у S.

2. Нека је l сјајна права у S. Постоји алгебарска крива C таква да за сваку тачку из $S \setminus C$ постоји права која пролази кроз њу, лежи у S и сече l.

Доказ. 1. Користећи одговарајућу промену координата, без умањења општости, можемо да претпоставимо да је (x_0, y_0, z_0) координатни почетак. За тачку $(x_1, y_1, z_1) \in S \setminus \{(0, 0, 0)\}$, права која пролази кроз њу и координатни почетак лежи у S ако и само ако $p(tx_1, ty_1, tz_1) = \sum_{i=0}^{\deg(p)} t^i \cdot q_i(x_1, y_1, z_1) = 0$ за свако реално t. То је еквивалентно са тиме да се одређених $\deg(p) + 1$ полинома (наиме $q_i, i \in \{0, .., \deg(p)\}$) по променљивама x, y, z анулира у тачки (x_1, y_1, z_1). Значи, да би доказали први део леме, треба да докажемо да се тих $\deg(p) + 1$ полинома анулира на целом S. Међутим, ми знамо да је $(0, 0, 0)$ сјајна тачка у S, односно да кроз координатни почетак пролази бесконачно много правих у S и у њима се наших $\deg(p) + 1$ полинома тривијално анулирају. На основну Безуове леме (Лема 10) можемо да закључимо да p са сваким од $\deg(p) + 1$ одговарајућих полинома има нетривијални заједнички делилац. Како је p иредуцибилан, добијамо да p дели сваки од датих полинома, односно они се анулирају на целом S, чиме смо доказали први део.

2. Слично као у доказу за први део, променимо координате тако да се l поклапа са x правом ($y = 0$ и $z = 0$). За разлику од првог дела, овде неће све тачке у S имати одговарајуће својство. Нека је $(x, y, z) \in S$ тачка за коју важи $v(x, y, z) = (\frac{\partial p}{\partial x}(x, y, z), \frac{\partial p}{\partial y}(x, y, z), \frac{\partial p}{\partial z}(x, y, z)) \neq (0, 0, 0)$. Посматрамо раван која пролази кроз (x, y, z) и нормална је на вектор $v(x, y, z)$ центриран у (x, y, z) (такозвана *тангентна* раван). Поучени идејама из претходних доказа, лако следи да свака права која лежи у S и пролази кроз (x, y, z) мора припадати и тој тангентној равни. Сада нам је јасно да су тачке $(x, y, z) \in S$ које вероватно немају одговарајуће својство заправо оне чија је тангентна раван (уколико постоји) паралелна са $l = x$ правом,

односно оне за које важи $\frac{\partial p}{\partial x}(x,y,z)=0$. Зато, дефинишимо C као део у S где се и p и $\frac{\partial p}{\partial x}$ анулирају. Посматрајмо све тачке $(x,y,z)\in S\setminus C$ и нека је $(x',0,0)$ јединствена тачка пресека тангентне равни у (x,y,z) и праве $l=x$. Доказаћемо да за њих важи други део леме. Како $(x',0,0)$ лежи у тангентној равни знамо да је вектор $(x-x',y,z)$ нормалан на $v(x,y,z)$ односно

$$(x-x')\cdot\frac{\partial p}{\partial x}(x,y,z)+y\cdot\frac{\partial p}{\partial y}(x,y,z)+z\cdot\frac{\partial p}{\partial z}(x,y,z)=0$$

тј. x' се може изразити као $q(x,y,z)/\frac{\partial p}{\partial x}(x,y,z)$, за фиксан полином q одређен полиномом p. Треба да докажемо да права кроз $(x',0,0)$ и (x,y,z) лежи у S. Као и у првом делу, добићемо да одговарајућих $\deg(p)+1$ рационалних функција облика $r_i(x,y,z)/\frac{\partial p}{\partial x}(x,y,z)^{k_i}$, $i\in\{0,...,\deg(p)\}$, треба да се анулирају у тачки (x,y,z). Према томе, треба доказати се сви r_i анулирају у тачкама за које важи $\frac{\partial p}{\partial x}(x,y,z)\neq 0$. Како је $l=x$ сјајна права у S важи да постоји бесконачно много правих које леже у S и секу $l=x$ и за њих тривијално важи да су r_i нула на њима (сем у коначно много где је $\frac{\partial p}{\partial x}=0$). На основу Безуове леме, слично као у првом делу, закључујемо да p дели свако r_i, чиме смо добили оно што смо хтели. Остаје да докажемо да $C\neq S$. Претпоставимо супротно. Како је C део где се анулирају p и $\frac{\partial p}{\partial x}$ и како је p иредуцибилан, а $\frac{\partial p}{\partial x}$ полином мањег степена, због Безуове леме мора важити да је $\frac{\partial p}{\partial x}$ константан полином, односно да је $p(x,y,z)$ облика $ax+q(y,z)$. Како $l=x$ припада S, добијамо да је $a=0$. Такође, пошто је $l=x$ сјајна права, постоји права l' у S која сече l. Како p не зависи од x, сваки транслат праве l' у x смеру мора лежати у S, па добијамо да цела једна раван лежи у S, што није могуће (може се опет искористити Безуова лема и добити да једначина те равни дели p, али p је иредуцибилан полином и S није раван).

□

На основу претходног доказа можемо да закључимо две ствари. Прво, приметимо да у првом делу леме услов да постоји бесконачно много правих које пролазе кроз координатни почетак може бити замењен условом који треба да буде испуњен да бисмо могли да искористимо Безуову лему.

Последица 16. Произвољна тачка $(x,y,z)\in S$ је сјајна тачка уколико она лежи на бар $\deg(p)^2+1$ правих које леже у S.

Слично можемо да ослабимо услов за сјајне праве у S. Наиме, постоји фиксан полином f са целобројним коефицијентима, добијен из услова који мора бити задовољен да бисмо могли да применимо Безуову лему, независно од нашег

полинома p, за који важи следеће (нећемо се трудити да тачно одредимо f, нама је битно само да постоји):

Последица 17. Произвољна права $l \subset S$ је сјајна права уколико постоји бесконачно много правих које леже у S и бар $f(\deg(p)) + 1$ правих у S секу праву l у не-сјајној тачки.

Искоментаришимо још услов да постоји бесконачно много правих у S. Тиме одмах гарантујемо да ће бити бар једна права различита од l која ће скоро цела (сем у коначно много тачака) лежати у $S \setminus C$, па на њеним тачкама можемо да искористимо оно што смо закључили на основу Безуа и тиме добити да l јесте сјајна права (овде изозастављамо чињеницу да ће те нове праве сећи l у не-сјајним тачкама, јер ће то бити јасно из следеће леме).

Остало нам је још да видимо колико сјајних тачака и сјајних правих може да постоји у једној површи одређеној иредуцибилним полиномом, уколико она није права нити регулус.

Лема 18. Ако је p иредуцибилан полином и $\mathcal{S}$ површ одређена њиме која није раван нити регулус онда $\mathcal{S}$ садржи највише једну сјајну тачку и највише две сјајне праве.

Доказ. Претпоставимо да постоје две различите сјајне тачке x_1 и x_2 и нека је l произвољна права у $\mathcal{S}$ која пролази кроз x_1 али не и кроз x_2. Тада, на основу Леме 15, за сваку тачку $y \in l$ права кроз x_2 и y лежи у $\mathcal{S}$. Дакле, раван одређена са правом l и тачком x_2 мора да лежи у $\mathcal{S}$, али то није могуће.

Сада претпоставимо да постоје бар три сјајне праве l_1, l_2 и l_3. За сјајну праву l, означимо са $\mathcal{C}_l$ одговарајућу алгебарску криву из Леме 15. Посматрајмо неки бесконачни скуп правих L_1 које секу l_1. Постоји бесконачни подскуп $L_2 \subset L_1$ такав да свака права у L_2 лежи скоро цела у $\mathcal{S} \setminus \mathcal{C}_{l_2}$ (из доказа Леме 15, $\mathcal{C}_l$ може да има највише $\deg(p)(\deg(p) - 1)$ правих у себи због услова Безуове леме). Аналогно, постоји бесконачни подскуп $L_3 \subset L_2$ такав да свака права у L_3 лежи скоро цела у $\mathcal{S} \setminus \mathcal{C}_{l_3}$. Нека је l произвољна права у L_3. Посматрајмо све сем коначно много тачака на l које леже у $\mathcal{S} \setminus (\mathcal{C}_{l_2} \bigcup \mathcal{C}_{l_3})$. Ако би постојала тачка међу њима која лежи на само једној правој у S (односно само на l) тада би због Леме 15 права l, поред праве l_1, морала да сече и l_2 и l_3. Претпоставимо да постоји бесконачно много правих l које секу све три сјајне праве. Ако су неке две од њих копланарне, онда би све праве које их секу лежале у тој равни, што је немогуће. Следи да су l_1, l_2, l_3 три међусобно мимоилазне праве, па оне формирају регулус $\mathcal{R}$. За сваку праву l која их сече мора важити да припада $\mathcal{R}$, из чега следи да је $\mathcal{S} = \mathcal{R}$, што је контрадикција.

Значи, постоји бесконачан подскуп правих $L_3' \subset L_3$ које не секу све три сјајне праве l_1, l_2 и l_3. Ако је $l \in L_3'$, онда, као што смо показали, све тачке $x \in l$ које

припадају $\mathcal{S} \setminus (\mathcal{C}_{l_2} \bigcup \mathcal{C}_{l_3})$ морају да леже на бар две праве у $\mathcal{S}$. На основу првог дела доказа да постоји највише једна сјајна тачка, закључујемо да је свака права у L_3' сјајна. Подсетимо се да за сваку сјајну праву l постоји највише $\deg(p) \cdot (\deg(p) - 1)$ правих које леже у $\mathcal{C}_l$. То значи да можемо конструисати бесконачни низ правих $k_i \in L_3'$, $i \in \mathbb{N}$, такав да k_j скоро цела лежи у $\mathcal{S} \setminus \mathcal{C}_{k_i}$, за свако $0 < i < j$. Нека је $N = \deg(p)^2$ и $M = 1000N^4$. Постоје три не-сјајне тачке x_1, x_2 и x_3 које леже на k_M и у свим $\mathcal{S} \setminus \mathcal{C}_{k_i}$, за $0 < i < M$. Како је x_1 не-сјајна тачка, на основу Последице 16 она лежи на највише N правих. За сваку праву k_i, $0 < i < M$, постоји права која је сече и пролази кроз x_1. Дакле, постоји бар $(M-1)/N$ правих k_i које секу неку праву r_1 која пролази кроз x_1. Аналогно добијамо да постоје бар $(M-1)/N^3 > 500\deg(p)^2$ правих k_i које секу праве r_1, r_2, r_3 које пролазе кроз x_1, x_2 и x_3. Посматрајући регулус, односно раван, коју сачињавају r_1, r_2 и r_3 и користећи Безуову лему као раније добијамо жељену контрадикцију. □

Једноставна последица претходне леме је да су раван и регулус једине двоструко-праволинијске иредуцибилне површи. Другим речима, ако праволинијска иредуциблна површ није раван нити регулус, онда је она једноструко-праволинијска. Сада можемо да започнемо доказ Леме 14.

Доказ Леме 14. Нека је $p = p_1 p_2 ... p_m$, где су p_i иредуцибилни полиноми. Кажемо да је тачка (x, y, z) сјајна у $\mathcal{S}$ уколико је сјајна у $p_i = 0$, за неко i. Аналогно дефинишемо сјајне праве у $\mathcal{S}$. Користећи Лему 18 добијамо да има највише N сјајних тачака и највише $2N$ сјајних правих (јер је $\mathcal{S}$ без равни и регулуса). Према томе, број тачкака у Q_1 које су сјајне или леже на сјајним правама је највише $N + 2N \cdot |\mathcal{L}_1| \lesssim N^3$, па можемо да се фокусирамо само на оне које нису сјајне и не леже ни на једној сјајној правој.

Посматрајмо произвољну праву l у $\mathcal{S}$ која није сјајна. Како за сваку праволинијску површ постоји "непрекидна фамилија" генератора која је сачињава (са почетка поглавља, одређена са $\alpha(t)$ и $\omega(t)$), свака права која не припада тој фамилији и лежи у $\mathcal{S}$ мора бити сјајна права (кроз сваку тачку површи пролази неки генератор). Према томе, наша права l је генератор. Доказаћемо да је број не-сјајних тачака у којима друге не-сјајне праве секу l (не-сјајни пресеци) највише $N - 1$, одакле ће следити да је број преосталих тачака у Q_1 највише $(N-1) \cdot |\mathcal{L}_1| \leq N^3$, чиме бисмо завршили доказ.
Нека је π произвољна раван која садржи l, али ниједну не-сјајну праву која сече l (оваква раван постоји јер је таквих правих коначно много). Раван π сече $\mathcal{S}$ по кривој θ (одређеној са две променљиве, на пример x и y) степена N. Како l припада тој кривој, на основу Безуове теореме за две променљиве (доказ у додатку Б) добијамо да l (односно полином степена 1 по две променљиве који је дефинише у π) мора да дели θ. Дакле, $\theta = l^k \cdot c$, где је c компонента која

није дељива са l. Како је степен c највише $N-1$, следи да се c и l секу у највише $\deg(c)\cdot 1 \leq N-1$ тачака због услова Безуове теореме. Докажимо да су сви не-сјајни пресеци на l управо те тачке. Посматрајмо неку не-сјајну праву l' која сече l у не-сјајној тачки q. Хоћемо да докажемо да $q \in c$. Како је l' генератор који сече θ, постоји низ генератора који тежи l' за који ће сви (сем првих коначно много) генератора сећи θ, односно l или c. Приметимо да ће само коначно њих сећи l у q јер је q не-сјајна тачка. Како је l не-сјајна права (и у том низу генератора не може да постоји бесконачно њих који секу l у истој тачки различитој од q), сви сем коначно много генератора у том низу секу c. Другим речима, постоји подниз тог низа генератора који тежи l' такав да сваки генератор у њему сече c. Ако посматрамо тачке у којима генератори из тог подниза секу π, оне ће тежити $\{q\} = \pi \cap l$, и пошто је c затворена област (дефинисана је полиномом) следи да је $q \in c$, чиме је доказ готов. □

Сада смо спремни да докажемо Теорему 9. Претпоставимо да имамо скуп $\mathcal{L}$ од највише N^2 правих тако да никојих cN не лежи у равни или регулусу (c је произвољна константа за коју желимо да докажемо Теорему 9). Претпоставимо такође да, за довољно велико Q, наш скуп $\mathcal{L}$ има више од QN^3 пресечних тачака и б.у.о. нека је N најмањи број, не нужно цео, за који постоји такав скуп правих $\mathcal{L}$ (односно, за свако $M < N$, не постоји скуп $\mathcal{L}$ од највише M^2 правих са никојих cM у равни или регулусу који има више од QM^3 пресечних тачака).

Нека је $\mathcal{L}'$ скуп свих правих у $\mathcal{L}$ које секу $\mathcal{L}$ у бар $\frac{QN}{10}$ различитих тачака. Праве које нису у $\mathcal{L}'$ учествују у највише $\frac{QN^3}{10}$ пресека, па је број тачака у пресеку правих из $\mathcal{L}'$ бар $\frac{9QN^3}{10}$. Нека је $0 < \alpha \leq 1$ такав да $|\mathcal{L}'| = \alpha N^2$.

Изаберимо праве из $\mathcal{L}$ са вероватноћом $p = \frac{100}{Q}$. Хоћемо да докажемо да постоји скуп $\mathcal{L}''$ такав да има највише $\frac{200N^2}{Q}$ правих у себи и да важи да свака права из $\mathcal{L}'$ има бар N различитих тачака пресека са правама из тог скупа (мотивација за ово је идеја прављења полинома одговорајуће малог степена који ће се анулирати на свим правама из $\mathcal{L}'$). Нека је X случајна променљива која броји број изабраних правих. Онда је $\mathbb{E}[X] \leq \frac{100N^2}{Q}$, па важи $P(X > \frac{200N^2}{Q}) < \frac{1}{2}$. Означимо са $A_{l'}$ догађај да права l' из $\mathcal{L}'$ сече наш случајно изабран скуп у мање од N различитих тачака. Да би доказали да постоји онакав скуп $\mathcal{L}''$, довољно је утврдити да важи $\sum_{l'\in\mathcal{L}'} P(A_{l'}) < \frac{1}{2}$, односно довољно је доказати $P(A_{l'}) < \frac{1}{2\alpha N^2}$, за свако $l' \in \mathcal{L}'$. Посматрајмо сада произвољну праву $l \in \mathcal{L}'$ и $r \geq \frac{QN}{10}$ тачака на њој у којима их праве из $\mathcal{L}$ секу. Тривијално важи:

$$P(A_l) \leq \sum_{i=0}^{N-1} \binom{r}{i} \cdot p^i(1-p)^{r-i} < N \cdot \binom{r}{N-1} \cdot p^{N-1}(1-p)^{r-N+1} = N \cdot b_{N-1}$$

где је $b_i = \binom{r}{i} \cdot p^i(1-p)^{r-i}$. Онда, за $i < 5N$:

$$\frac{b_{i+1}}{b_i} = \frac{(r-i)\cdot p}{(i+1)\cdot(1-p)} \geq \frac{(\frac{QN}{10} - 5N)\cdot 100}{5N\cdot(Q-100)} > 2$$

Из $\sum_{i=0}^{r} b_i = 1$ добијамо $b_{N-1}\cdot(1+2+...+2^{4N}) \leq 1$, па тривијално важи $P(A_l) < \frac{1}{2\alpha N^2}$ (за довољно велико Q, биће довољно велико N).

Изаберимо са сваке праве из $\mathcal{L}''$ по $\frac{RN}{\sqrt{Q}}$ тачака, где је R довољно велика, али универзална константа (не зависи од Q, N). Дакле, изабрали смо највише $\frac{RN}{\sqrt{Q}}\cdot|\mathcal{L}'| = O(\frac{RN^3}{Q^{\frac{3}{2}}})$ тачака, па из једноставне линеарне алгебре (ову идеју ћемо видети и у следећем поглављу) можемо конструисати полином $p \in \mathbb{R}[x,y,z]$ степена $O(\frac{R^{\frac{1}{3}}N}{Q^{\frac{1}{2}}})$ (односно степена највише $C\frac{R^{\frac{1}{3}}N}{Q^{\frac{1}{2}}}$, за фиксно C) који се анулира у изабраним тачкама. Како смо изабрали R да буде довољно велико (треба нам да важи $\frac{RN}{\sqrt{Q}} > \deg(p)+1$, за шта је довољно $\frac{RN}{\sqrt{Q}} \geq C\frac{R^{\frac{1}{3}}N}{Q^{\frac{1}{2}}}$), следи да се p анулира на свим правама из $\mathcal{L}''$, а како оне секу праве из $\mathcal{L}'$ у бар N различитих тачака (овде и $N > C\frac{R^{\frac{1}{3}}N}{Q^{\frac{1}{2}}}$, за велико N), добијамо да се p анулира на целом скупу $\mathcal{L}'$.

Факторишимо полином $p = p_1p_2$ где је p_1 производ свих иредуцибилних праволинијских фактора који деле p, а p_2 преостали не-праволинијски део, оба степена $O(\frac{R^{\frac{1}{3}}N}{Q^{\frac{1}{2}}}) = O(\frac{N}{Q^{\frac{1}{2}}})$. Нека су $\mathcal{L}_1$ и $\mathcal{L}_2$ скупови правих из $\mathcal{L}'$ које леже редом у $p_1 = 0$ односно $p_2 = 0$ (очигледно $\mathcal{L}_1 \bigcup \mathcal{L}_2 = \mathcal{L}'$). Како права $l_1 \in \mathcal{L}_1 \setminus \mathcal{L}_2$ може да сече $p_2 = 0$ (па самим тим и праве $l_2 \in \mathcal{L}_2 \setminus \mathcal{L}_1$) у највише $\deg(p_2) = O(\frac{N}{Q^{\frac{1}{2}}})$ тачака, добијамо да је пресек правих између $\mathcal{L}_1 \setminus \mathcal{L}_2$ и $\mathcal{L}_2 \setminus \mathcal{L}_1$ највише $O(N^3)$. Дакле, у бар једном од $\mathcal{L}_1$, $\mathcal{L}_2$ мора да буде више од $\frac{3QN^3}{10}$ пресека.

Претпоставимо да у $\mathcal{L}_1$ имамо више од $\frac{3QN^3}{10}$ тачака пресека. Нека је $p_1 = p_3p_4$, где је $p_3 = 0$ без равни и регулуса, а p_4 производ равни и регулуса који деле p_1. Поделимо $\mathcal{L}_1$ на $\mathcal{L}_3$ и $\mathcal{L}_4$ слично као пре, истим аргументом добијамо да је број тачака у пресеку правих из $\mathcal{L}_3 \setminus \mathcal{L}_4$ и $\mathcal{L}_4 \setminus \mathcal{L}_3$ највише $O(N^3)$. На основу Леме 14 знамо да је број пресека међу правама из $\mathcal{L}_3$ исто $O(N^3)$. Дакле, праве из $\mathcal{L}_4$ се секу у бар $\frac{QN^3}{10}$ различитих тачака. Међутим, праве из $\mathcal{L}_4$ леже у највише N равних/регулуса од којих свака/и садржи највише по cN правих. Дакле, број пресека између правих у истој равни/регулусу је $O(N^3)$. Како свака права може да сече раван, односно регулус, којој не припада у највише једној, односно две, тачке, то значи да је преосталих тачака у пресеку правих из $\mathcal{L}_4$ највише $O(N^3)$, контрадикција.

Дакле, мора да важи да се праве из $\mathcal{L}_2$ секу у бар $\frac{3QN^3}{10}$ тачака. Како је $p_2 = 0$ тотално не-праволинијска површ, из Последице 13 закључујемо да не може имати више од $O(\deg(p_2)^2)$ тј. $O(\frac{N^2}{Q})$ правих у себи, одакле следи да $|\mathcal{L}_2| \leq \beta N^2$ где је $\beta = O(\frac{1}{Q})$. Сада желимо да постигнемо контрадикцију са

претпоставком са почетка о избору броја N. Међутим, ми за праве из $\mathcal{L}_2$ можемо да гарантујемо да никојих cN не лежи у равни односно регулусу, а не никојих $c\sqrt{\beta}N$. Дефинишимо скуп $\mathcal{L}_5$ на следећи начин: све док постоји раван/регулус која садржи више од $c\sqrt{\beta}N$ правих, пребацимо све праве које леже у њој/њему у $\mathcal{L}_5$ и обришимо их из $\mathcal{L}_2$. На тај начин, обележимо преостали скуп са $\mathcal{L}_6$. Приметимо како смо овако "оштетили" највише $O(N)$ равни и регулуса па, као и у претходном случају, закључујемо да има највисе $O(N^3)$ пресека између правих у $\mathcal{L}_5$. Такође, постоји највише $O(N^3)$ тачака пресека правих из $\mathcal{L}_5$ и $\mathcal{L}_6$, пошто свака права из другог скупа може сећи сваку раван/регулус из првог у највише једној, односно две, тачке. Међутим, због претпоставке о избору броја N, међу правама у $\mathcal{L}_6$ не може бити више од $Q \cdot (\sqrt{\beta}N)^3$ односно $O(\frac{N^3}{Q^{\frac{1}{2}}})$ тачака, чиме добијамо жељену контрадикцију.

4

Подели па владај

У овом поглављу се бавимо доказом Теореме 8 за $k \geq 3$. Као што назив поглавља сугерише, главна идеја ће нам бити да изделимо простор на ћелије оивичене нулама неког полинома довољно малог степена за које ће важити да су тачке из скупа који посматрамо некако равномерно распоређене по тим ћелијама. Тако ћемо моћи да бројимо инциденције нашег скупа правих у свакој ћелији понаособ, а прелазак праве из једне у другу ћелију ће значити да та права мора да пресече површ задату нашим полиномом, што, као што смо видели у претходном поглављу, не може много пута да се деси. У овом поглављу ћемо видети још важних улога тачака и правих у површи одређеној полиномом.

Теорема 19. Нека је $\mathfrak{S}$ скуп од S тачака у $\mathbb{R}^n$ и J природан број. Постоји полином p степена $d \lesssim 2^{J/n}$ за који важи да је $\mathbb{R}^n \setminus \{p = 0\}$ унија 2^J дисјунктних отворених скупова O_i, од којих сваки садржи $\leq 2^{-J}S$ тачака из $\mathfrak{S}$.

Овде $\{p = 0\} = \{(x, y, z) \in \mathbb{R}^3 \mid p(x, y, z) = 0\}$, и аналогно дефинишемо области $\{p < 0\}$ и $\{p > 0\}$. Да би доказали претходну теорему, ослонићемо се на доказ познате теореме, њој донекле сличне по тврђењу:

Теорема 20 (Теорема о шунки и сендвичу [1])**.** Нека су $U_1, ..., U_n \in \mathbb{R}^n$ отворени скупови коначне запремине, онда постоји хипераван која сваки од њих дели на пола.

Главна идеја у доказу теореме јесте теорема Борсук-Улама, односно:

Теорема 21 (Борсук-Улам)**.** Ако је $f : S^n \to \mathbb{R}^n$ непрекидна непарна функција, онда постоји $x \in S^n$ за које $f(x) = 0$.

Како нас занимају само скупови са коначним бројем тачака, докажимо следећу полиномску верзију Теореме 20:

[1] Ham sandwich theorem

Теорема 22. Нека су $S_1, S_2, ..., S_M$ коначни скупови тачака у $\mathbb{R}^n$, где је $M = \binom{n+d}{n} - 1$. Онда постоји полином $p \in \mathbb{R}[x_1, ..., x_n]$ степена највише d који полови сваки од S_i ($|S_i \cap \{p > 0\}| = |S_i \cap \{p < 0\}|$).

Доказ. Нека је $\delta > 0$ и $U_{i,\delta}$ унија δ-лопти описаних око тачака у S_i, $1 \leq i \leq M$. Докажимо прво да постоји полином p_δ степена највише d који полови сваки од $U_{i,\delta}$ (овде $Vol(U_{i,\delta} \cap \{p < 0\}) = Vol(U_{i,\delta} \cap \{p > 0\})$). Посматрајмо све полиноме из $\mathbb{R}[x_1, .., x_n]$ степена највише d; они се могу записати као $\sum c_{d_1,...,d_n} x_1^{d_1} ... x_n^{d_n}$, где су $d_i \geq 0$ цели бројеви такви да је $d_1 + ... + d_n \leq d$. Таквих $d_1, ..., d_n$ има $\binom{n+d}{n}$, па постоји непрекидна бијекција g полинома из $\mathbb{R}[x_1, ..., x_n]$ степена највише d и $\mathbb{R}^{\binom{n+d}{n}}$ (поређамо коефицијенте произвољно и сваком полиному доделимо тачку са координатама одређеним његовим коефицијентима). Ми ћемо се ограничити на $S^{\binom{n+d}{n}-1}$, односно на полиноме за које важи $\sum c^2_{d_1,..,d_n} = 1$. Посматрајмо непрекидну функцију $f : S^{\binom{n+d}{n}-1} \to \mathbb{R}^{\binom{n+d}{n}-1}$ дефинисана као:

$$f(c) = \begin{pmatrix} Vol(U_{1,\delta} \cap \{g^{-1}(c) < 0\}) - Vol(U_{1,\delta} \cap \{g^{-1}(c) > 0\}) \\ Vol(U_{2,\delta} \cap \{g^{-1}(c) < 0\}) - Vol(U_{2,\delta} \cap \{g^{-1}(c) > 0\}) \\ ... \\ Vol(U_{M,\delta} \cap \{g^{-1}(c) < 0\}) - Vol(U_{M,\delta} \cap \{g^{-1}(c) > 0\}) \end{pmatrix}$$

Како за сваки пар $(c, -c)$ антиподалних тачака на $S^{\binom{n+d}{n}-1}$ важи $f(c) = -f(-c)$ јер $g^{-1}(c) = -g^{-1}(-c)$, применом теореме Борсук-Улама добијамо да постоји c за које $f(c) = 0$. Полином $p_\delta := g^{-1}(c)$ је очигледно тражени полином.

Нека је $\delta_m > 0$, $m \in \mathbb{N}$, произвољан опадајући низ који тежи нули и p_{δ_m} одговарајући полиноми. У низу тачака $g(p_{\delta_m}) \in S^{\binom{n+d}{n}-1}$ постоји конвергентан подниз (само га формирамо по координатама редом, јер оне припадају у $[-1, 1]$, па за њих понаособ постоји, на пример), односно постоји растући подниз m_i, $i \in \mathbb{N}$, за који $\lim_{i\to\infty} g(p_{\delta_{m_i}}) = c$, за неко c које очигледно мора лежати у $S^{\binom{n+d}{n}-1}$. Докажимо да је $p := g^{-1}(c)$ тражени полином.

Претпоставимо да за неко $1 \leq i \leq M$ важи $|S_i \cap \{p > 0\}| \neq |S_i \cap \{p < 0\}|$. Означимо са S_i^+ леву и S_i^- десну страну, и нека је б.у.о. $|S_i^+| > |S_i^-|$. За довољно мало ϵ, $p > 0$ у свим ϵ-лоптама око тачака у S_i^+. Како $\lim_{i\to\infty} p_{\delta_{m_i}} = p$, за свако $i > D$, за неку фиксно D, важиће $p_{\delta_{m_i}} > 0$ на свим ϵ-лоптама у S_i^+. Међутим, како $\lim_{i\to\infty} \delta_{m_i} = 0$, за довољно велико i важи $\delta_{m_i} < \epsilon$, што, заједно са претходним, значи да је $p_{\delta_{m_i}} > 0$ у свим δ_{m_i} лоптама око тачака у S_i^+, контрадикција. □

Сада смо спремни да докажемо Теорему 19.

Доказ Теореме 19. Конструисаћемо тражени полином у J корака. Почнимо са линеарним полиномом p_1 који полови $\mathfrak{S}$ на $\mathfrak{S}^+$ и $\mathfrak{S}^-$. Затим, користећи Теорему

22, изаберимо полином p_2 који бисектује $\mathfrak{S}^+$ и $\mathfrak{S}^-$, и тако даље. Генерално, полином p_j бирамо на основу Теореме 22 тако да дели 2^{j-1} скупа на које је издељена раван полиномом $p_1..p_{j-1}$. На крају када завршимо наш алгоритам, имаћемо полиноме $p_1, p_2, .., p_J$, за које ће $p_1p_2...p_J$ делити раван на 2^J отворена скупа (одређена избором знака + или − за сваки од p_i) који сви садрже $\leq 2^{-J}S$ тачака из $\mathfrak{S}$. Остало је још да видимо колики је степен $p_1p_2...p_J$. По конструкцији, p_j дели 2^{j-1} скупова на пола, па је на основу Теореме 22 његов степен $\lesssim 2^{j/n}$ (n је фиксно, па се то тривијално изводи). Дакле, степен полинома $p_1p_2...p_J$ је $\lesssim \sum_{j=1}^{J} 2^{j/n} \lesssim 2^{J/n}$. □

Сада смо спремни за главну теорему овог поглавља:

Теорема 23. Нека је $k \geq 3$ и $\mathcal{L}$ скуп са L правих у $\mathbb{R}^3$ где највише B правих лежи у истој равни. Нека је $\mathfrak{S}$ скуп тачака у $\mathbb{R}^3$ које леже на бар k правих из $\mathcal{L}$, онда:

$$|\mathfrak{S}| = O(L^{\frac{3}{2}}k^{-2} + LBk^{-3} + Lk^{-1}).$$

Пре него што се упустимо у доказ теореме, прокоментаришимо сваки члан који доприноси десној страни неједнакости.

Пример 24. Посматрајмо неких L/k тачака и по k правих кроз сваку од њих. Очигледно за скуп одређен тим правама $\mathcal{L}$ важи $|\mathfrak{S}| = Lk^{-1}$.

Пример 25. Посматрајмо неких L/B равни и B правих у свакој од њих. Докажимо да је могуће распоредити B правих у свакој од равни тако да је број тачака које леже на бар k њих $\sim B^2k^{-3}$. Ради једноставности, претпоставимо да је $B = 2N^3$ и $k = N$, за неко $N \in \mathbb{N}$. Посматрајмо скуп тачака S облика $(a, b) \in \mathbb{Z}^2$ за које $1 \leq a \leq N$ и $1 \leq b \leq 2N^2$ ($|S| = 2N^3$) и скуп правих L' облика $(x, mx + b)$ за природне бројеве $m \leq N$ и $b \leq N^2$. Тада $|L'| = N^3 \sim B^2k^{-3}$ и свака права из L' пролази кроз тачно $k = N$ тачака из S. Ако сада доделимо свакој тачки $(a, b) \in S$ дуалну праву $(x, ax+b)$, свака права из L ће се сликати у тачку пресека правих додељеним тачкама из S које леже на њој, чиме добијамо конфигурацију од $B = |S| = 2N^3$ правих и $N^3 \sim B^2k^{-3}$ тачака које леже на тачно $k = N$ њих. Дакле, $|\mathfrak{S}| \approx LBk^{-3}$.

Пример 26. Нека је S_0 скуп тачака $(a, b, 0)$, а S_1 скуп тачака $(a, b, 1)$ за природне бројеве $1 \leq a, b \leq L^{\frac{1}{4}}$ и $\mathcal{L}$ скуп правих које спајају све тачке из S_0 са свим тачкама из S_1. Свака раван садржи по највише $L^{\frac{1}{4}}$ тачака из S_0, S_1, па $B \leq L^{\frac{1}{2}}$. Доказаћемо у додатку Ц да $\sim L^{\frac{3}{2}}k^{-2}$ тачака лежи на бар k правих у $\mathcal{L}$ за свако $2 \leq k \leq L^{\frac{1}{2}}/400$.

Веза између Теореме 23 и Семереди-Тротера је јасно видљива, и како ће и она играти улогу у доказу, наведимо је овде (ова формулација директно следи из планарне, пројектовањем на произвољну раван):

Теорема 27 (Семереди-Тротер)**.** Нека је $\mathcal{L}$ скуп са L правих у $\mathbb{R}^n$ и $\mathfrak{S}$ скуп тачака које леже на бар k правих у $\mathcal{L}$. Тада:

$$|\mathfrak{S}| = O(L^2k^{-3} + Lk^{-1}).$$

Прво ћемо доказати Теорему 23 са одређеним претпоставкама:

Тврђење 28. Нека је $k \geq 3$ и $\mathcal{L}$ скуп од L правих у $\mathbb{R}^3$ таквих да не више од B лежи у истој равни. Нека је $\mathfrak{S}$ скуп од S тачака у $\mathbb{R}^3$ таквих да свака лежи на бар k, али највише $2k$, правих у $\mathcal{L}$. Такође, нека је број правих у $\mathcal{L}$ које садрже бар $\frac{1}{100}SkL^{-1}$ тачака из $\mathfrak{S}$ бар $\frac{1}{100}L$. Тада:

$$S \leq C[L^{\frac{3}{2}}k^{-2} + LBk^{-3} + Lk^{-1}].$$

Приметимо да је број инциденција између $\mathfrak{S}$ и $\mathcal{L} \sim Sk$, што значи да нам претпоставке заправо кажу да имамо $\sim L$ просечних правих у $\mathcal{L}$ (са $\sim SkL^{-1}$ тачака из $\mathfrak{S}$).

Доказ Тврђења 28. Претпоставимо да је за довољно велико A:

$$S \geq A[L^{\frac{3}{2}}k^{-2} + Lk^{-1}] \tag{4.1}$$

Наша стратегија је следећа: желимо да покажемо да ће $\gtrsim SL^{-1}k^3$ правих из $\mathcal{L}$ лежати у једној равни, одакле бисмо добили $S \lesssim BLk^{-3}$. То ћемо урадити у два корака. Први је да нађемо полином степена $d \lesssim L^2S^{-1}k^{-3}$ који ће се анулирати на довољној количини наших правих. Други корак је да докажемо да ће се површ одређена тим полиномом састојати из равни које ће, опет, садржати довољну количину правих из $\mathcal{L}$. Онда, како има највише d равни сачињавају ту површ, једна од њих ће имати $\gtrsim L/d$ правих у себи. Како $d \lesssim L^2S^{-1}k^{-3}$, добијамо $B \gtrsim SL^{-1}k^3$, што смо и желели.
(Гут и Кац су прво покушали да нађу тражени полином користећи алгебарске методе из трећег поглавља, али полином који су направили је имао степен $\lesssim L^2S^{-1}k^{-2}$. Идеја о дељењу простора на ћелије је одиграла кључну улогу у смањењу степена.)

Прво ћемо конструисати полином p такав да област Z одређена њиме садржи велики број тачака из $\mathfrak{S}$.

Лема 29. Ако је константа A у неједнакост (4.1) довољно велика, онда постоји алгебарска површ Z степена $\lesssim L^2S^{-1}k^{-3}$ која садржи бар $(1-10^{-8})S$ тачака из $\mathfrak{S}$.

Доказ. Нека је θ довољно велики фиксан број (видећемо колико касније) и d цео део од $\theta L^2 S^{-1} k^{-3}$. Прво, проверимо да је $d \geq 1$. На основу Семереди-Тротера, $S \lesssim L^2 k^{-3} + Lk^{-1}$, па због (4.1) закључујемо $S \lesssim L^2 k^{-3}$. Дакле, $d \geq 1$. На основу Теореме 19, можемо да конструишемо полином степена d такав да његова површ Z дели простор на $\sim d^3$ ћелија O_i од којих свака садржи $\lesssim Sd^{-3}$ тачака из $\mathfrak{S}$.

Претпоставимо да Z садржи мање од $(1 - 10^{-8})S$ тачака у $\mathfrak{S}$, онда наше ћелије O_i садрже бар $10^{-8}S$ тачака из $\mathfrak{S}$. Како их има $\sim d^3$ и свака садржи $\lesssim Sd^{-3}$ њих у себи, постојаће $\gtrsim d^3$ ћелија које ће садржати $\gtrsim Sd^{-3}$ тачака из $\mathfrak{S}$. Назовимо такве ћелије *пуне*. Нека је $\mathcal{L}(O_i)$ скуп правих из $\mathcal{L}$ које секу O_i. Међу пуним ћелијама, посматрајмо ону са минималним $|\mathcal{L}(O_i)|$ и означимо тај број са L_{cell}. Применом Семереди-Тротера на ту ћелију добијамо:

$$Sd^{-3} \lesssim L_{cell}^2 k^{-3} + L_{cell} k^{-1}$$

Како свака права која не припада Z може да пресече Z у највише d тачака, а при сваком преласку праве из O_i у O_j она мора пресећи Z, закључујемо да је број пресека правих које не припадају Z и Z, односно број пресека правих из $\mathcal{L}$ и наших ћелија, највише Ld. Следи да је $L_{cell} \lesssim Ld^{-2}$, одакле

$$S \lesssim L^2 d^{-1} k^{-3} + Ldk^{-1} \implies S \leq C(\theta^{-1} S + \theta L^3 S^{-1} k^{-4})$$

где је C константа независна од θ (добили бисмо је кад бисмо урачунали константе из Семереди-Тротера и Теореме 19). Одавде можемо да претпоставимо да је θ довољно велика константа да важи $C\theta^{-1} < \frac{1}{2}$ одакле добијамо да $S \lesssim \theta L^3 S^{-1} k^{-4}$, односно $S \lesssim L^{\frac{3}{2}} k^{-2}$, што је у контрадикција са тим да је A довољно велико.
Значи, Z је тражена алгебарска површ степена $d \lesssim L^2 S^{-1} k^{-3}$. □

Означимо са $\mathfrak{S}_Z$ скуп свих тачака из $\mathfrak{S}$ које леже у Z (на основну претходне леме $|\mathfrak{S} \setminus \mathfrak{S}_Z| \leq 10^{-8} S$). Наш следећи циљ је да покажемо да доста правих из $\mathcal{L}$ леже у Z. Присетимо се да просечна права из $\mathcal{L}$ садржи $\gtrsim SkL^{-1}$ тачака из $\mathfrak{S}$. Дакле, први корак нам је да ограничимо d са SkL^{-1}.

Лема 30. Ако је A довољно велико, онда

$$d < 10^{-8} SkL^{-1}$$

Доказ. На основу неједнакости (4.1) важи:

$$1 \leq A^{-1} S L^{-\frac{3}{2}} k^2$$

Одакле, кад квадрирамо и помножимо са d, добијамо:

$$d \leq A^{-2} d S^2 L^{-3} k^4 \lesssim A^{-2} SkL^{-1}$$

За A довољно велико тривијално следи лема. □

Из претходне леме следи да, ако права из $\mathcal{L}$ пролази кроз бар $10^{-8}SkL^{-1}$ тачака из $\mathfrak{S}_Z$, онда она лежи у Z. Означимо са $\mathcal{L}_Z$ скуп правих из $\mathcal{L}$ које леже у Z. Докажимо следећу лему:

Лема 31. Скуп $\mathcal{L}_Z$ садржи бар $(1/200)L$ правих.

Доказ. Претпоставили смо да постоји $\geq (1/100)L$ правих из $\mathcal{L}$ које садрже $\geq (1/100)SkL^{-1}$ тачака из $\mathfrak{S}$. Нека је $\mathcal{L}_0 \subset \mathcal{L}$ скуп тих правих. Доказаћемо да већина правих у том скупу припада $\mathcal{L}_Z$. Права из $\mathcal{L}_0$ која не припада Z може садржати највише $10^{-8}SkL^{-1}$ тачака из $\mathfrak{S}_Z$, одакле мора садржати бар $(1/200)SkL^{-1}$ тачака из $\mathfrak{S} \setminus \mathfrak{S}_Z$. Дакле, ако са $I(A, B)$ означимо број инциденција између скупова A и B, онда:

$$\frac{1}{200}SkL^{-1} \cdot |\mathcal{L}_0 \setminus \mathcal{L}_Z| \leq I(\mathcal{L}_0 \setminus \mathcal{L}_Z, \mathfrak{S} \setminus \mathfrak{S}_Z) \leq 2k \cdot |\mathfrak{S} \setminus \mathfrak{S}_Z| \leq 2 \cdot 10^{-8}Sk$$

тј.

$$|\mathcal{L}_0 \setminus \mathcal{L}_Z| \leq 4 \cdot 10^{-6}L$$

одакле следи $|\mathcal{L}_Z| \geq (1/200)L$. □

Овиме смо завршили први корак у нашој стратегији: направили смо алгебарску површ Z степена $\lesssim L^2S^{-1}k^{-3}$ која садржи велику количину правих из $\mathcal{L}$.

На реду је други део доказа, тј. да покажемо да Z садржи раван којој ће припадати велика количина правих из $\mathcal{L}_Z$. Да би то урадили, биће нам потребно још мало знања из алгебарске геометрије, односно треба да видимо на који начин нам праве и тачке у алгебарској површи говоре о томе да ли она садржи раван или не. Ми ћемо овде укратко нешто рећи о тој теми, детаљнији увод се налази у [ЕКШ].

Површ Z је одређена неким полиномом p који се факторише на иредуцибилне полиноме $p = p_1p_2....$ Можемо да претпоставимо да $p_i \neq p_j$ пошто се уклањањем било ког од та два површ Z не мења. Тачка $x \in Z$ се зове *критична тачка* ако $\nabla p(x) = 0$, односно ако су парцијални изводи по свакој променљиви у тој тачки једнаки 0. Ако $x \in Z$ није критична тачка, онда се она назива *регуларном тачком*. Регуларне тачке, као што смо видели у претходном поглављу, имају добро дефинисану тангенту раван на Z (раван нормална на вектор ∇p у тој тачки). Регуларну тачку називамо *равном* уколико кроз њу пролазе бар 3 праве које леже у Z.

Посматрајмо једну равну тачку a у Z. За праву произвољног правца v кроз њу, полином $p(a + tv)$ можемо посматрати као полином по t, v, као што смо

чинили у претходном поглављу. То нас наводи да дефинишемо полином q као

$$q(u) = p(a) + (u-a)\cdot\nabla p(a) + \frac{1}{2}(u-a)^T H_p(a)(u-a)$$

где је $\cdot$ скаларни производ и

$$H_p = \begin{pmatrix} p_{xx} & p_{xy} & p_{xz} \\ p_{yx} & p_{yy} & p_{yz} \\ p_{zx} & p_{zy} & p_{zz} \end{pmatrix}$$

Хесијан полинома p. Полином q је заправо оно што се добије кад распишемо $p(a+(u-a))$ до другог степена по $u-a$, односно апроксимација полинома до трећег степена када је u јако близу a. Посматрајмо три праве l_1, l_2 и l_3 што пролазе кроз a и леже у Z; q се анулира на свакој од њих, што значи да се анулира у три тачке у којима произвољна права $l \subset \pi_a$ (у тангентој равни у a) сече l_1, l_2 и l_3. Пошто је q другог степена, то значи да се q анулира на целој l, односно на целој π_a. Сличним резоновањем добијамо да је услов $q = 0$ на π_a еквивалентан са тиме да се q анулира у произвољне три тачке за које никоје две нису колинеарне са a. Заиста, за тачку $u \in \pi_a$ важи $(u-a)\cdot\nabla p(a) = 0$ па је $q(u) = 0$ еквивалентно са $(u-a)^T H_p(a)(u-a) = 0$, па како за тачку u' колинеарну са u и a важи да је $(u'-a)^T H_p(a)(u'-a) = 0$ акко $(u-a)^T H_p(a)(u-a)$, онда $q(u) = 0$ повлачи да је $q = 0$ на правој кроз u и a. Овиме закључујемо да услов да је тачка a равна повлачи слабији услов да се q анулира у произвољне 3 тачке у π_a, где никоје две нису колинеарне са a. Било би згодно да представимо координате такве три тачке преко полинома у a. То може да се уради на следећи начин: изаберимо координатни систем такав да се ниједан од праваца e_i не поклапа са $\nabla p(a)$ (односно за све тачке које посматрамо). Наше три тачке су:

$$u_i = a + \nabla p(a) \times e_i.$$

Дакле, услов да је a равна тачка повлачи:

$$\Pi_i(p)(a) = (\nabla p(a) \times e_i)^T H_p(a)(\nabla p(a) \times e_i) = 0, \text{ за } i = 1,2,3. \tag{4.2}$$

За регуларну тачку a за коју важи (4.2) кажемо да је *квадратно равна*.[2] За полиноме $\Pi_i(p)$ важи да су степена највише $(d-1)+(d-2)+(d-1) = 3d-4$.

За праву $l \subset Z$ кажемо да је *критична* уколико су све њене тачке критичне (односно, из претходних дискусија знамо да је довољно је да је d тачака на њој критично). Аналогно за праву $l \subset Z$ кажемо да је *равна* уколико није критична и све тачке на њој, сем коначно много, су квадратно равне (опет, довољно је да их је бар $3d-3$). Сада долазимо до кључних лема за наш наставак са доказом.

[2]Иначе, услов (4.2) је еквивалентан са тим да је друга фундаментална форма Z у тачки a нула, али нећемо залазити у то јер је изван нашег домашаја.

Лема 32. Површ одређена бесквадратним полиномом p степена d садржи највише $d(d-1)$ критичних правих у себи.

Доказ. Уколико је p иредуцибилан полином, лема следи тривијално из Безуа. У наставку ћемо се ослањати на индукцију по степену полинома. Зато, претпоставимо да се p растаљва на $p = fg$, где су f и g узајамно прости полиноми (овде користимо то што је p бесквадратни полином) степена d_f и d_g, $d_f + d_g = d$. Како $\partial p = \partial fg + \partial gf$, за сваку критичну праву l важи бар једно:

1. $f = 0$ на l и l је критична у површи дефинисаној са f
2. $g = 0$ на l и l је критична у површи дефинисаној са g
3. $f = 0$ и $g = 0$ на l

Међутим, трећи случај може десити за највише $d_f d_g$ правих, а први и други због индукције за највише $d_f(d_f - 1)$ и $d_g(d_g - 1)$ правих, па добијамо да је број критичних правих $\leq d_f(d_f - 1) + d_f d_g + d_g(d_g - 1) \leq d(d-1)$. □

Следећа лема повезује постојање равни у алгебарској површи и број равних правих (оно што нам треба).

Лема 33. Ако је Z алгебарска површ степена d (односно, дефинисана је неким бесквадратним полиномом степена d) без планарних компоненти, онда она садржи највише $3d^2 - 4d$ равних правих.

Да би доказали ову лему, било би нам потребно нешто знања из диференцијалне геометрије, па нећемо наводити доказ овде, он се може наћи у [ЕКШ] (укратко, суштина доказа је да за иредуцибилне Z, ако друга фундаментална форма Z нестаје у свакој регуларној тачки Z, онда се око регуларних тачака наша површ понаша као раван, одакле би следило да је Z заправо раван; у супротном примењујемо индуктивну хипотезу слично као малопре).

Наставимо сада са нашим доказом. Сетимо се да свака тачка у $\mathfrak{S}_Z$ лежи на бар k правих из $\mathcal{L}$, али не нужно на ијединој из $\mathcal{L}_Z$. Стога, нека је $\mathfrak{S}'_Z$ скуп тачака из $\mathfrak{S}_Z$ које леже на бар 3 праве у $\mathcal{L}_Z$ (јасно зашто бирамо 3 на основу претходне дискусије). Дакле, свака тачка у $\mathfrak{S}'_Z$ је или критична или квадратно равна. Докажимо да $\mathfrak{S}'_Z$ садржи довољну количину тачака.

Лема 34. Скуп $\mathfrak{S} \setminus \mathfrak{S}'_Z$ садржи највише $10^{-7}S$ тачака.

Доказ. Према Леми 29 $|\mathfrak{S} \setminus \mathfrak{S}_Z| \leq 10^{-8}S$.
Нека је $x \in \mathfrak{S}_Z \setminus \mathfrak{S}'_Z$. Она лежи на бар k правих из $\mathcal{L}$, али највише 2 из $\mathcal{L}_Z$, односно лежи на бар $k-2$ праве из $\mathcal{L} \setminus \mathcal{L}_Z$, одакле добијамо:

$$(k-2) \cdot |\mathfrak{S}_Z \setminus \mathfrak{S}'_Z| \leq I(\mathfrak{S}_Z \setminus \mathfrak{S}'_Z, \mathcal{L} \setminus \mathcal{L}_Z).$$

Са друге стране, према Леми 30 знамо да свака права из $\mathcal{L}\setminus\mathcal{L}_Z$ садржи највише $10^{-8}SkL^{-1}$ тачака из $\mathfrak{S}_Z$ одакле:

$$I(\mathfrak{S}_Z\setminus\mathfrak{S}'_Z,\mathcal{L}\setminus\mathcal{L}_Z)\leq I(\mathfrak{S}_Z,\mathcal{L}\setminus\mathcal{L}_Z)\leq 10^{-8}SkL^{-1}\cdot L=10^{-8}Sk,$$

односно:

$$|\mathfrak{S}_Z\setminus\mathfrak{S}'_Z|\leq 10^{-8}\cdot\frac{k}{k-2}S\leq 3\cdot 10^{-8}S$$

па, комбиновањем са почетном неједнакости, добијамо жељену оцену. □

Нека је $\mathfrak{S}'_{Z\,crit}$ скуп свих критичних тачака, а $\mathfrak{S}'_{Z\,flat}$ скуп свих квадратно равних тачака у $\mathfrak{S}'_Z$. На основу претходне дискусије знамо за праву l да је критична уколико садржи више од d критичних тачака на њој, а ако их садржи коначно много и такође садржи више од $3d-3$ квадратно равних тачака, онда је равна. Дакле, ако је $\mathcal{L}'_Z$ скуп правих из $\mathcal{L}_Z$ које пролазе кроз више од $(1/200)SkL^{-1}$ тачака из $\mathfrak{S}'_Z$, можемо закључити да:

Лема 35. Свака права из $\mathcal{L}'_Z$ је или критична или равна.

Доказ. Лема следи на основу претходног разматрања и Леме 30 одакле знамо да је $d<10^{-8}SkL^{-1}$. □

Сада нам треба да $\mathcal{L}'_Z$ садржи довољан број правих.

Лема 36. Број правих из $\mathcal{L}'_Z$ је $\geq(1/200)L$.

Доказ. Подсетимо се наше претпоставке да постоји бар $(1/100)L$ правих из $\mathcal{L}$ које садрже више од $(1/100)SkL^{-1}$ тачака из $\mathfrak{S}$. Означимо тај скуп са $\mathcal{L}_0$. Нека је $l\in\mathcal{L}_0\setminus\mathcal{L}'_Z$. На основу дефиниција $\mathcal{L}_0$ и $\mathcal{L}'_Z$ закључујемо да l садржи бар $(1/200)SkL^{-1}$ правих из $\mathfrak{S}\setminus\mathfrak{S}'_Z$. Дакле:

$$\frac{1}{200}SkL^{-1}\cdot|\mathcal{L}_0\setminus\mathcal{L}'_Z|\leq I(\mathfrak{S}\setminus\mathfrak{S}'_Z,\mathcal{L}_0\setminus\mathcal{L}'_Z)\leq 2k\cdot|\mathfrak{S}\setminus\mathfrak{S}'_Z|$$

Међутим, према Леми 34, $|\mathfrak{S}\setminus\mathfrak{S}'_Z|<10^{-7}S$ одакле следи $|\mathcal{L}_0\setminus\mathcal{L}'_Z|\leq 4\cdot 10^{-5}L$, чиме добијамо тражену неједнакост. □

Лема 32 нам каже да Z, односно $\mathcal{L}'_Z$ садржи највише $d(d-1)<d^2$ критичних правих. Како желимо да имамо што више равних правих у $\mathcal{L}'_Z$ (јер нам то говори о томе да ли постоји раван у Z), докажимо следећу оцену за d:

Лема 37. За довољно велико A важи $d\leq 10^{-4}L^{\frac{1}{2}}$.

Доказ. На основу (4.1) имамо $1 \leq A^{-1}SL^{-\frac{3}{2}}k^2$, па:

$$d \leq dA^{-1}SL^{-\frac{3}{2}}k^2 \lesssim A^{-1}L^{\frac{1}{2}}k^{-1}$$

одакле, за довољно велико A, следи жељена оцена. □

Дакле, $\mathcal{L}'_Z$ садржи највише $d^2 \leq 10^{-8}L$ критичних правих, па на основу Леме 4.8, садржи више од $(1/300)L$ равних правих.

Нека је $Z = Z_{pl} \bigcup Z'$, где је Z_{pl} унија свих равни које леже у Z, а Z' површ одређена остатком фактора. Полиномски посматрано, Z_{pl} је област дефинисана производом иредуцибилних фактора полинома p (који дефинише Z) чији скуп нула представља раван, а Z' део дефинисан преосталим факторима, односно полиномом p'. Како за праву која лежи у пресеку та два дела знамо да је критична, добијамо да равне праве припадају или у Z_{pl} или у Z'. Како равна права из Z која лежи у Z' је равна и у Z' (лако се изводи из $p = p_{pl} \cdot p'$, детаљније у [ЕКШ]), на основу Леме 33 закључујемо да Z' садржи највише $3d^2 - 4d \leq 3 \cdot 10^{-8}L$ равних правих из $\mathcal{L}'_Z$. Дакле, бар $(1/400)L$ правих из $\mathcal{L}'_Z$ леже у Z_{pl}. Како је број равни у Z_{pl} највише d, добијамо да бар једна раван саржи више од $(1/400)Ld^{-1} \gtrsim SL^{-1}k^3$ правих из $\mathcal{L}'_Z$, односно из $\mathcal{L}$. Дакле, $S \lesssim BLk^{-3}$, чиме је готов доказ Тврђења 28. □

Сада ћемо свести главни проблем на Тврђење 28. Прво, уклонимо претпоставку да постоји довољна количина просечних правих (са $\sim SkL^{-1}$ тачака из S у себи):

Тврђење 38. Нека је $k \geq 3$ и $\mathcal{L}$ скуп са L правих у $\mathbb{R}^3$ од којих највише B леже у истој равни. Нека је $\mathfrak{S}$ скуп од S тачака из $\mathbb{R}^3$ које леже на бар k, а највише $2k$, правих у $\mathcal{L}$. Онда

$$S \leq C[L^{\frac{3}{2}}k^{-2} + BLk^{-3} + Lk^{-1}].$$

Доказ. Нека је $\mathcal{L}_1$ скуп правих из $\mathcal{L}$ које садрже бар $(1/100)SkL^{-1}$ тачака из $\mathfrak{S}$. Ако је $|\mathcal{L}_1| \geq (1/100)L$ онда смо завршили на основу Тврђења 28, зато претпоставимо да је $|\mathcal{L}_1| < (1/100)L$. Радићемо индукцију по L.
Приметимо да је:

$$I(\mathfrak{S}, \mathcal{L} \setminus \mathcal{L}_1) \leq \frac{1}{100}SkL^{-1} \cdot L = \frac{1}{100}Sk,$$

односно скуп $\mathcal{L}_1$ доприноси највише инциденција, што је и очекивано. Нека је $\mathfrak{S}' \subset \mathfrak{S}$ скуп свих тачака које леже на бар $(9/10)k$ правих из $\mathcal{L}_1$. Онда:

$$\frac{1}{10}k \cdot |\mathfrak{S} \setminus \mathfrak{S}'| \leq I(\mathfrak{S} \setminus \mathfrak{S}', \mathcal{L} \setminus \mathcal{L}_1) \leq \frac{1}{100}Sk$$

одакле $|\mathfrak{S} \setminus \mathfrak{S}'| \leq (1/10)S \implies |\mathfrak{S}'| \geq (9/10)S$. Сада, за тачку $x \in \mathfrak{S}'$ знамо да припада на бар $(9/10)k$, а највише $2k$, правих из $\mathcal{L}_1$, што је превелики интервал за индукцију. Зато, нека је $\mathfrak{S}' = \mathfrak{S}'_+ \bigcup \mathfrak{S}'_-$, где је $\mathfrak{S}'_+$ скуп свих тачака које припадају на бар k, а $\mathfrak{S}'_-$ скуп свих тачака које припадају на највише k правих из $\mathcal{L}_1$. Бар један од та два скупа има кардиналност S_1 већу од $(9/20)S$. У случају да је то први скуп, $k_1 = k$, а у супротном k_1 је најмањи цео број већи од $(9/10)k$. У оба случаја можемо применити Тврђење 38 на тај скуп тачака и праве из $\mathcal{L}_1$ (користећи индукцију по броју правих јер $L_1 = |\mathcal{L}_1| < (1/100)L$), па добијамо следећу неједнакост:

$$S_1 \leq C[L_1^{\frac{3}{2}} k_1^{-2} + BL_1 k^{-3} + L_1 k_1^{-1}]$$

одакле, користећи да је $S \leq (20/9)S_1$, $L_1 < (1/100)L$ и $k_1^{-1} \leq (10/9)k^{-1}$, следи:

$$S \leq \frac{20}{9} S_1 \leq \left(\frac{20}{9} \cdot \frac{1}{100} \cdot (\frac{10}{9})^3\right) \cdot C[L^{\frac{3}{2}} k^{-2} + BLk^{-3} + Lk^{-1}].$$

Како је израз у заградама < 1, добијамо тражену неједнакост за S. □

Докажимо сада Теорему 23.

Доказ Теореме 23. Нека је $k \geq 3$, $\mathcal{L}$ је скуп од L правих таквих да највише B леже у истој равни и $\mathfrak{S}$ скуп тачака које припадају на бар k правих из $\mathcal{L}$. Нека је $\mathfrak{S} = \bigcup_{j=0}^{\infty} \mathfrak{S}_j$, где је $\mathfrak{S}_j$ скуп тачака које леже на бар $2^j k$, али највише на $2^{j+1}k$, правих из $\mathcal{L}$. Означимо са $k_j = 2^j k$. Применом Тврђења 38 на $(\mathcal{L}, \mathfrak{S}_j, k_j, B)$ добијамо:

$$|\mathfrak{S}_j| \leq C[L^{\frac{3}{2}} k_j^{-2} + BLk_j^{-3} + Lk_j^{-1}] \leq 2^{-j} \cdot C[L^{\frac{3}{2}} k^{-2} + BLk^{-3} + Lk^{-1}]$$

па је $S \leq \sum_{j=0}^{\infty} |\mathfrak{S}_j| \leq 2C[L^{\frac{3}{2}} k_j^{-2} + BLk_j^{-3} + Lk_j^{-1}]$. □

Приметимо да Теорема 23 за $B = N$ и $L = N^2$ имплицира Теорему 8 за случај $k \geq 3$. Дакле, за $k \geq 3$ нам није била битна претпоставка о броју правих у регулусу. Овим поглављем је комплетиран доказ да је број различитих растојања у Ердошевом проблему $\gtrsim \frac{N}{\log N}$.

5

Закључак

У првом делу рада смо прешли из комбинаторног проблема у две на геометријски проблем три димензије. Већ у том делу смо видели назнаке полинома кроз Безуову теорему и кроз посебан геометријски објекат (регулус) који игра важну улогу у једном од случајева.

У другом делу смо видели како да контролишемо површи дефинисане полиномом користећи Безуову теорему. Јако значајне за нас су биле оне које имају много правих у себи, односно *праволинијске* површи. Упознали смо се са њиховом карактеризацијом преко *генератора* и *превојних* полинома, што нам је омогућило да докажемо Теорему 9 свођењем на индукцију, односно случај праволинијских површи, који смо са претходним алатима знали да решимо.

У трећем делу, да бисмо доказали Теорему 8 за $k \geq 3$, била нам је потребна идеја о дељењу равни на ћелије. Видели смо да нас то не кошта много по питању степена полинома са којим је делимо, па смо могли у доказу главне теореме да се служимо њоме. То нам је омогућило да лако ограничимо број инциденција посматраних тачака и прави, и да потом, добијемо да довољна количина правих лежи у површи дефинисаној пређашњим полиномом. Онда смо видели још један пример тога како нам тачке и праве једне површи говоре много о њој.

На крају, у додатку стоји формална дефиниција регулуса, доказ прекопотребне Безуове теореме и занимљив пример $\sqrt{N} \times \sqrt{N}$ квадрата у којем се постиже оцена Теореме 8.

Желела бих да се захвалим свом ментору, Луки Милићевићу, на свим његовим предавањима и курсевима који су увек били пуни дивних идеја које повезују разне области математике, међу којима су и оне најбитније из овог рада. Хвала што сам имала прилику да сазнам за њих још као ученица средње школе.

Такође бих желела да се захвалим свим професорима који су ми предавали математику у Математичкој гимназији, јер су непрестано продубљивали моју

заинтересованост за њу чиме су ме подстицали да напредујем све више.

Додатак А

Шта је то регулус

Као што смо већ видели у претходним поглављима, постоје две дефиниције регулуса:

Дефиниција 39. Регулус је површ одређена свим правама које секу дате 3 међусобно мимоилазне праве.

Дефиниција 40. Регулус је површ одређена са два *покривача* (скупа међусобно мимоилазних правих), таква да свака права једног сече сваку праву другог и кроз сваку тачку регулуса пролази по бар једна права из оба скупа.

Ми ћемо почети са дефиницијом 39. Докажимо следеће тврђење које нам је било од кључног значаја у претходним поглављима:

Тврђење 41. Постоји иредуцибилни полином другог степена за који важи да је свака тачка регулуса R, дефинисног са правама l_1, l_2 и l_3, нула тог полинома.

Доказ. Да бисмо доказали да постоји тражени полином, ради лакшег рачуна нећемо гледати на проблем из перспективе $\mathbb{R}^3$, већ из перспективе $\mathbb{RP}^3$ (сликамо (x, y, z) у $(x, y, z, 1)$). При томе поистовећујемо све тачке $x, y \in \mathbb{PR}^3$ за које важи $x = \lambda y$, за $\lambda \in \mathbb{R} \setminus \{0\}$. На овај начин, свакој тачки из $\mathbb{R}^3$ је додељена права из $\mathbb{PR}^3$ која спаја њу и координатни почетак, свакој правој из $\mathbb{R}^3$ је додељена раван из $\mathbb{PR}^3$ одређена њоме и координатним почетком итд. Означимо са L_1, L_2 и L_3 равни које су додељене нашим мимоилазним правама. Можемо, без умањења општости, да претпоставимо (због примене одговарајуће пројективне трансформације) да важи:

$$L_1 = [X, Y, 0, 0] \text{ и } L_2 = [0, 0, Z, W].$$

Раван L_3 може да буде било шта, али ми ћемо ради једноставности да претпоставимо да је $L_3 = [X, Y, -X, -Y]$. Посматрајмо сада тачку $p = (a, b, c, d)$ за

коју постоји права која сече наше три мимоилазне праве. Дакле, раван L доделјена тој правој сече L_1 и L_2 у неким тачкама $(x, y, 0, 0)$ и $(0, 0, z, w)$. Међутим, знамо да је $t \cdot (x, y, 0, 0) + s \cdot (a, b, c, d) = (0, 0, z, w)$, за неко $s, t \in \mathbb{R}$, где $st \neq 0$. Одавде закључујемо да $tx + sa = 0 = ty + sb$, односно $xb = ya$, и $z = sc$, $w = sd$. Дакле, $(a, b, 0, 0)$ и $(0, 0, c, d)$ припадају L, одакле следи да је L дефинисана са:

$$bX = aY \text{ и } dZ = cW$$

Нека је $(X, Y, -X, -Y)$ једна тачка пресеке L и L_3. Из претходних једначина за L закључујемо:

$$bX = aY \text{ и } -dX = -cY \implies ad - bc = 0$$

Посматрајмо сада неку тачку (x, y, z) из $\mathbb{R}^3$ за коју постоји права која пролази кроз њу и сече наше три мимоилазне праве. Првобитно смо (x, y, z) сликали у $(x, y, z, 1)$, али с обзиром на потенцијалну примену пројективне трансформације, она се слика у неко (a, b, c, d) за које знамо од малочас да важи $ad - bc = 0$. Како је свака пројективна трансформација у $\mathbb{PR}^3$ линеарна, закључујемо да је $ad - bc$ управо полином другог степена по x, y, z, што смо и хтели. □

Сада када имамо ово тврђење остало је још да докажемо да су дефиниције 39 и 40 еквивалентне. Претпоставимо да је регулус R дефинисан са дефиницијом 39, тј. као унија правих које секу три међусобно мимоилазне l_1, l_2 и l_3; тај скуп правих L_1 ће бити један од покривача. Приметимо да за тачку x у простору може да постоји највише једна права која сече све l_1, l_2, l_3. Нека су l_1', l_2', l_3' произвољне три праве покривача L_1; оне су, на основу претходног, међусобно мимоилазне. Посматрајмо регулус R' дефинисан над њима, и нека су p и p' полиноми другог степена који одређују R и R'. Знамо да $R \cap R'$ садржи $l_1, l_2, l_3, l_1', l_2', l_3'$, па на основу Безуове леме p и p' имају заједничког делиоца. Међутим, они су иредуцибилни, па следи $R = R'$. Нека је други покривач L_2 скуп свих правих које секу l_1', l_2', l_3'. За тачку $x \in R$ важи да постоји права из L_1 која пролази кроз њу. Како та тачка x припада и R', важи да постоји права из L_2 која пролази кроз њу. Остало је још да видимо да свака права првог сече сваку праву другог покривача. Претпоставимо да постоје l', l из првог, односно другог, покривача које се не секу. Ако посматрамо регулус R_1 над l', l_1', l_2' на пример, онда опет добијамо $R_1 = R$, па за тачку $x \in l$ знамо да $x \in R_1$, односно постоји јединствена права кроз њу која сече l', l_1', l_2'. Међутим, права l пролази кроз x и сече l_1' и l_2', што је у контрадикцији са тиме да су те две праве мимоилазне.

Јасно је да се аналогно може добити да из дефиниције 40 следи дефиниција 39. Исто тако, ослањајући се на Безуа, лако се добија да регулус не може имати 3 различита покривача (што нам је било битно у другом поглављу), чиме смо употпунили нашу дискусију о регулусу.

Додатак Б

Безуова теорема

Пре него што почнемо са доказивањем Безуове теореме, требаће нам пар основних ствари за полиноме из $k[x_1, x_2, ..., x_n]$, где је k поље (у нашем случају $\mathbb{R}$ или $\mathbb{C}$). Кључна ствар која важи за $k[x]$, када је k поље, јесте Еуклидов алгоритам.

Б.1 Иредуцибилни полиноми и јединственост факторизације

Почнимо са врло познатим стварима да би склопили цео формалан доказ тврђења која следе.

Дефиниција 42. Полином $p \in k[x_1, x_2, .., x_n]$ је *иредуцибилан над* k уколико није константан и не постоје неконстантни полиноми $f, g \in k[x_1, x_2, ..., x_n]$ за које $p = fg$.

Из претходне дефиниције одмах закључујемо следећу чињеницу:

Став 43. Сваки неконстантни полином $f \in k[x_1, x_2, ..., x_n]$ се раставља на иредуцибилне полиноме над k.

Теорема 44. Нека су $f, g, h \in k[x_1, x_2, ..., x_n]$ такви да је f иредуцибилан полином и $f \mid gh$. Онда $f \mid g$ или $f \mid h$.

Доказ. Користимо индукцију по n. Знамо да базни случај $n = 1$ следи из Еуклидовог алгоритма, зато претпоставимо $n > 1$. За почетак докажимо да ако је u иредуцибилан полином из $k[x_1, x_2, ..., x_n]$ такав да не зависи од x_1 (односно $u \in k[x_2, ..., x_n]$), онда за полиноме $g, h \in k[x_1, x_2, ..., x_n]$:

$$u \mid gh \implies u \mid g \ \vee \ u \mid h \tag{Б.1}$$

Наиме, нека је $g = \sum_{i=0}^{m} a_i x_1^i$ и $h = \sum_{i=0}^{l} b_i x_1^i$, где су $a_i, b_i \in k[x_1, x_2, ..., x_n]$, онда $u|g$ акко $u|a_i$ за свако $i = 0, .., m$ и аналогно за полином h. Дакле, претпоставимо да постоји i, j такви да $u \nmid a_i$ и $u \nmid b_j$ и узмимо најмањи такав пар, по обе компоненте. У полиному gh коефицијент уз x_1^{i+j} је једнак:

$$c_{i+j} = (a_0 b_{i+j} + .. + a_{i-1} bj + 1) + a_i b_j + (a_{i+1} b_{j-1} + ... + a_{i+j} b_0),$$

па како је (i, j) најмањи онакав пар закључујемо да $u \nmid c_{i+j}$, што је у контрадикцији са $u \mid gh$.

Вратимо се сада на наш иредуцибилан полином $f \in k[x_1, x_2, ..., x_n]$; како није константан полином, нека без умањења општости по x_1 има позитиван степен. Посматрајмо f, g, h у $k(x_2, .., x_n)[x_1]$, где је $k(x_2, ..., x_n)$ *поље рационалних функција* по промењивама $x_2, .., x_n$. Докажимо прво да је f иредуцибилан над $k(x_2, .., x_n)$. Претпоставимо да постоје неконстантни $g_1, h_1 \in k(x_2, ..., x_n)[x_1]$ такви да:

$$f = g_1 h_1.$$

Постоји $d \in k[x_2, ..., x_n]$ такво да $g' = dg_1$ и $h' = dh_1$ припадају $k[x_1, x_2, .., x_n]$ (они ће имати позитиван степен по x_1 зато сто су g_1, h_1 неконстантни). Тада:

$$d^2 f = g' h'.$$

Како $d^2 \in k[x_2, .., x_n]$, када га раставимо на иредуцибилне факторе, на основу (Б.1), они морају да деле g' или h', па можемо да их пократимо. Приметимо да оно што остаје од g' и h' морају бити неконстантни полиноми (јер ће имати позитиван степен по x_1), што је у контрадикцији са тиме да је f иредуцибилан.

Дакле, f је иредуцибилан у $k(x_2, ..., x_n)[x_1]$, па можемо да применимо индукцију и добијемо, без умањења општости, да $f \mid g$ у $k(x_2, ..., x_n)[x_1]$, односно:

$$g = f h_1, \text{ за } h_1 \in k(x_2, ..., x_n)[x_1].$$

Знамо да постоји $d \in k[x_2, ..., x_n]$ такво да $h' = dh_1 \in k[x_1, x_2, ..., x_n]$. Онда:

$$dg = f h',$$

па, слично као малочас, на основу (Б.1) закључујемо да иредуцибилни делиоци полинома d морају да деле f или h'. Међутим, како је f иредуцибилан у $k[x_1, x_2, ..., x_n]$ и има позитиван степен по x_1, први случај није могућ. Дакле $h'/d \in k[x_1, x_2, ..., x_n]$, чиме смо завршили доказ. □

Једна битнија последица претходне теореме је:

Последица 45. Нека су f и g полиноми из $k[x_1, x_2, ..., x_n]$, онда они имају заједничког делиоца у $k[x_1, x_2, .., x_n]$ са позитивним степеном по x_1 ако и само ако имају заједничког делиоца у $k(x_2, ..., x_n)[x_1]$.

Доказ. Ако f и g имају заједничког делиоца у $k[x_1, x_2, ..., x_n]$ са позитивним степеном по x_1 онда тривијално имају и у $k(x_2, ..., x_n)[x_1]$. Докажимо сада супротни смер. Претпоставимо да

$$f = hf' \text{ и } g = hg',$$

за неке $h, f', g' \in k(x_2, ..., x_n)[x_1]$, где h није константан полином, односно има позитиван степен по x_1. Тада постоји $d \in k[x_2, ..., x_n]$ такво да $h_1 = h'd$, $f_1 = f'd$ и $g_1 = g'd$ припадају $k[x_1, x_2, ..., x_n]$, па:

$$d^2 f = h_1 f_1 \text{ и } d^2 g = h_1 g_1.$$

Када факторишемо полином d^2 на иредуцибилне факторе, на основу претходне теореме закључујемо да они морају да деле h_1 или f_1, односно h_1 или g_1, па можемо да пократимо те факторе са обе стране. Посматрајмо један иредуцибилни фактор h_2 полинома h_1 који има позитиван степен по x_1 (такав мора да постоји јер полином h_1 задовољава то својство). Како је $d^2 \in k[x_2, ..., x_n]$, h_2 је морао остати после скраћивања, па добијамо да $h_2 \mid f$ и $h_2 \mid g$, чиме смо доказали други смер. □

Ради комплетности, наведимо следећу теорему чији доказ нећемо изводити, јер је поприлично једноставан након целог увода.

Теорема 46 (Јединственост факторизације)**.** Нека је $f \in k[x_1, x_2, ..., x_n]$ полином и нека је $f = g_1 g_2 ... g_s$ једна његова факторизација на иредуцибилне факторе. Ако је $f = h_1 h_2 ... h_r$ друга факторизација полинома f на иредуцибилне факторе, онда важи $r = s$ и полиноми g_i се могу пермутовати тако да је сваки f_i једнак константа пута g_i.

Б.2 Резултанта два полинома

Посматрајмо два полинома $f, g \in k[x]$, где је k поље; желимо да нађемо услов када та два полинома морају да имају заједнички делилац. Ту нам је од великог значаја следеће једноставна лема:

Лема 47. Нека су $f, g \in k[x]$ два полинома степена l и m, редом. Онда f и g имају заједничког делиоца ако и само ако постоје полиноми $A, B \in k[x]$ такви да:

1. A и B нису оба нула полином
2. A и B су степена највише $m-1$ и $l-1$, редом
3. $Af + Bg = 0$

Доказ. Оба смера су тривијална, али наведимо онај тежи ради формалности. Претпоставимо да постоје такви A, B и претпоставимо супротно, да су f и g узајмно прости. Онда постоје $A', B' \in k[x]$ такви да $A'f + B'g = 1$ на основу Еуклидовог алгоритма, па ако је $B \neq 0$, без умањења општости, онда:

$$B = (A'f + B'g)B = A'Bf + B'(Bg) = f(A'B - AB') \neq 0.$$

Ово, међутим, није могуће, јер је десна страна степена бар l, док је лева највише $l-1$. □

Сада ако распишемо $f(x) = \sum_{i=0}^{l} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, $A(x) = \sum_{i=0}^{m-1} c_i x^i$ и $B(x) = \sum_{i=0}^{l-1} d_i x^i$, онда тривијално следи (када изједначимо по коефицијентима) да f и g имају заједничког делиоца акко је детерминанта следеће матрице једнака нули:

$$\mathrm{Syl}(f,g,x) = \begin{bmatrix} a_0 & 0 & \cdots & 0 & b_0 & \cdots & 0 \\ a_1 & a_0 & \cdots & & b_1 & \ddots & \vdots \\ a_2 & a_1 & \ddots & \vdots & \vdots & \vdots & b_0 \\ \vdots & \vdots & \cdots & a_0 & \vdots & \ddots & \vdots \\ \vdots & \vdots & \cdots & \vdots & b_m & \vdots & \vdots \\ a_l & a_{l-1} & \cdots & \vdots & 0 & \vdots & \vdots \\ 0 & a_l & \cdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_l & 0 & \cdots & b_m \end{bmatrix}_{(l+m)\times(l+m)}.$$

Матрица $\mathrm{Syl}(f,g,x)$ се иначе назива *Силвестерова матрица*, а њена детерминанта *резултанта* полинома f и g:

$$\mathrm{Res}(f,g,x) = \det(\mathrm{Syl}(f,g,x)).$$

Последица 48. Нека су f и g полиноми из $k[x]$. Резултанта $\mathrm{Res}(f,g,x)$ је полином са целобројним коефицијентима по a_i, b_j и важи:

$$(f,g) \neq 1 \iff \mathrm{Res}(f,g,x) = 0.$$

Приметимо следеће: ако су f и g два узајмно проста полинома степена l и m, онда на основу Еуклидовог алгоритма постоје полиноми $A', B' \in k[x]$ степена највише $m-1$, односно $l-1$, за које важи $A'f + B'g = 1$. Ако их запишемо као $A'(x) = \sum_{i=0}^{m-1} c_i x^i$ и $Bl(x) = \sum_{i=0}^{l-1} d_i x^i$, онда:

$$\mathrm{Syl}(f,g,x) \cdot \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{l-1} \\ d_0 \\ d_1 \\ \vdots \\ d_{m-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{Б.2}$$

Тврђење 49. Нека су f, g полиноми из $k[x]$, онда постоје полиноми $A, B \in k[x]$ такви да:

$$Af + Bg = Res(f,g,x)$$

и коефицијенти полинома A и B се могу изразити као целобројни полиноми по коефицијентима полинома f и g.

Доказ. Ако је $(f,g) \neq 1$ онда на основу Последице 48 можемо да узмемо само $A = B = 0$. Претпоставимо онда да $(f,g) = 1$; као што смо малопре видели, постоје A', B' који задовољавају $A'f + B'g = 1$ и (Б.2). На основу Крамеровог закона, можемо изразити коефицијенте полинома A и B као (дајемо за пример формулу за c_0, остали се аналогно изражавају):

$$c_0 = \frac{1}{\mathrm{Res}(f,g,x)} \cdot \det \begin{bmatrix} 1 & 0 & \cdots & 0 & b_0 & \cdots & 0 \\ 0 & a_0 & \cdots & & b_1 & \ddots & \vdots \\ 0 & a_1 & \ddots & \vdots & \vdots & \vdots & b_0 \\ \vdots & \vdots & \cdots & a_0 & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ldots & \vdots & b_m & \vdots & \vdots \\ 0 & a_{l-1} & \cdots & \vdots & 0 & \vdots & \vdots \\ 0 & a_l & \cdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_l & 0 & \cdots & b_m \end{bmatrix}.$$

Дакле, $A = \mathrm{Res}(f,g,x) \cdot A'$ и $B = \mathrm{Res}(f,g,x) \cdot B'$ су очигледно тражени полиноми. □

Сада смо спремни да докажемо главно тврђење које ћемо користити у доказу Безуове теореме.

Тврђење 50. Нека су $f, g \in k[x_1, x_2, ..., x_n]$ полиноми са позивитним степеном по x_1. Онда:

1. $\text{Res}(f, g, x_1)$ припада $\langle f, g\rangle \cap k[x_2, ..., x_n]$.

2. $\text{Res}(f, g, x_1) = 0$ ако и само ако f и g имају заједничког делиоца у $k[x_1, x_2, ..., x_n]$ позитивног степена по x_1.

(овде је $\text{Res}(f, g, x_1)$ дефинисана као резултанта за случај једне променљиве када се гледају f, g као полиноми по x_1 са коефицијентима из $k[x_2, ..., x_n]$).

Доказ. Први део Тврђења 50 следи тривијално из Тврђења 49. Што се тиче другог дела, посматрајмо полиноме f, g у $k(x_2, ..., x_n)[x_1]$, где је $k(x_2, ..., x_n)$ поље рационалних функција по променљивама $x_2, .., x_n$. Знамо онда да је:

$$\text{Res}(f, g, x_1) = 0 \iff f \text{ и } g \text{ имају заједничког делиоца у } k(x_2, ..., x_n)[x_1].$$

Међутим, на основу Последице 48 добијамо 2. део тврђења. □

Б.3 Безу

Почнимо са Безуовом теоремом за полиноме са две променљиве.

Теорема 51 (Безуова теорема)**.** Нека су f и g два полинома из $\mathbb{R}[x, y]$ (односно $\mathbb{C}[x, y]$) степена m и n редом. Ако постоји више од mn различитих тачака (x, y) у којима се f и g анулирају, онда f и g имају заједничког делиоца у $\mathbb{R}[x, y]$ (односно у $\mathbb{C}[x, y]$).

Доказ. Можемо, без умањења општости, да претпоставимо да су f и g позитивног степена по x (иначе можемо да променимо координатни систем да то важи). Слично, претпоставимо да међу наших $mn + 1$ тачака у којима се анулирају f и g не постоје две са истом y координатом. Докажимо да је $\text{Res}(f, g, x) \in \mathbb{R}[y]$ полином степена највише mn, чиме бисмо добили да је $\text{Res}(f, g, x) = 0$, одакле би, на основу Тврђења 50, следило $(f, g) \neq 1$. Наиме, $f = a_m x^m + ... + a_0$ и $g = b_n x^n + ... + b_0$, где су a_i, b_j полиноми из $\mathbb{R}[y]$ степена највише $m-i$ и $n-j$, редом (можемо да претпоставимо да су тачно тог степена, пошто то само доприноси у $\text{Res}(f, g, x)$). Како је:

$$\mathrm{Res}(f,g,x)=\det\begin{bmatrix} a_0 & 0 & \cdots & 0 & b_0 & \cdots & 0 \\ a_1 & a_0 & \cdots & & b_1 & \ddots & \vdots \\ a_2 & a_1 & \ddots & \vdots & \vdots & \vdots & b_0 \\ \vdots & \vdots & \cdots & a_0 & \vdots & \ddots & \vdots \\ \vdots & \vdots & \cdots & \vdots & b_n & \vdots & \vdots \\ a_m & a_{m-1} & \cdots & \vdots & 0 & \vdots & \vdots \\ 0 & a_m & \cdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_m & 0 & \cdots & b_n \end{bmatrix}_{(m+n)\times(m+n)}$$

и

$$\mathrm{Res}(f,g,x)=\sum_{\sigma\in S_m+n}\mathrm{sgn}(\sigma)\cdot c_{\sigma(1)1}...c_{\sigma(m+n)(m+n)},$$

онда, за пермутацију σ која доприноси $\mathrm{Res}(f,g,x)$, $c_{\sigma(1)1}$ је степена $m+1-\sigma(1)$ ($\sigma(1)\leq m+1$ иначе је $c_{\sigma(1)1}=0$), $c_{\sigma(2)2}$ је степена $m+2-\sigma(2)$,..., $c_{\sigma(n)n}$ је степена $m+n-\sigma(n)$, $c_{\sigma(n+1)(n+1)}$ је степена $n+1-\sigma(n+1)$,..., $c_{\sigma(m+n)(m+n)}$ је степена $m+n-\sigma(m+n)$. Дакле, $c_{\sigma(1)1}...c_{\sigma(m+n)(m+n)}$ је степена $(m+1)...+(m+n)+(n+1)+...+(m+n)-\sum_{i=1}^{m+n}\sigma(i)=2mn+\frac{n(n+1)}{2}+\frac{m(m+1)}{2}-\frac{(m+n)(m+n+1)}{2}=mn$. Одавде добијамо да је $\mathrm{Res}(f,g,x)$ степена највише mn чиме смо завршили доказ. □

На реду је разлог овог додатка - Безуова лема за полиноме по три променљиве:

Последица 52 (Безуова лема за три променљиве)**.** Нека су $f,g\in\mathbb{R}[x,y,z]$ полиноми степена m и n редом. Ако се f и g анулирају на више од mn различитих правих, онда они имају заједничког делиоца у $\mathbb{R}[x,y,z]$. (Аналогно за $\mathbb{C}[x,y,z]$.)

Доказ. Добрим избором координатног система, можемо да претпоставимо да оба f и g имају позитиван степен по x и да постоји $mn+1$ правих у којима се анулирају које нису паралелне са $z=0$ равни (односно секу је у $mn+1$ тачака). Ако посматрамо $\mathrm{Res}(f,g,x)\in\mathbb{R}[y,z]$, за произвољно z (сем за коначно много могућих лоших z) важи да је $\mathrm{Res}(f,g,x)(y,z)=\mathrm{Res}(f_z,g_z,x)$, где су $f_z(x,y)=f(x,y,z)$ и $g_z(x,y)=g(x,y,z)$. Међутим, f_z и g_z се анулирају у бар $mn+1$ тачака, па на основу Безуове теореме $\mathrm{Res}(f_z,g_z,x)=0$. Дакле, за све сем коначно много (y,z) важи $\mathrm{Res}(f,g,x)(y,z)=0$. Ово повлачи $\mathrm{Res}(f,g,x)=0$ за све $y,z\in\mathbb{R}$, па на основу Тврђена 50 закључујемо да f и g имају заједничког делиоца. □

Додатак Ц

Доказ оцена за квадрат $\sqrt{N} \times \sqrt{N}$

У овом делу додатка доказаћемо да се за тачке квадратне решетке $\sqrt{N} \times \sqrt{N}$ постижу оцене $Q(P) \gtrsim N^3 \log N$ и $G_k(P) \gtrsim N^3 k^{-2}$ за $2 \leq k \leq N/100000$ из другог поглавља. Проучаваћемо скуп $\mathcal{L}$ дефинисаних правих из другог поглавља за P и видећемо да се део њих подудара са примером 3 за Теорему 4.5 у четвртом поглављу.

Нека је $S \geq 1$ цео број. Нека је P скуп тачака (x, y) таквих да $|x|, |y| \leq 2S$ - тада је $N = |P| = (4S+1)^2$. Нека је $\mathcal{L}$ скуп правих из $\mathbb{R}^3$ асоцираних са P као у поглављу 2.

Лема 53. Ако су a, b, c, d цели бројеви са апсолутним вредностима $\leq S$, онда права која спаја $(a, b, 0)$ и $(c, d, 1)$ лежи у $\mathcal{L}$.

Доказ. Подсетимо се да су праве из $\mathcal{L}$ параметризоване са:

$$(\frac{p_x + q_x}{2}, \frac{p_y + q_y}{2}, 0) + t(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1)$$

Значи, довољно је доказати да за неко $(p_x, p_y), (q_x, q_y) \in P$ важи:

$$\frac{p_x + q_x}{2} = a,\ \frac{p_y + q_y}{2} = b,\ \frac{q_y - p_y}{2} = c - a,\ \frac{p_x - q_x}{2} = d - b,$$

одакле:

$$p_x = a + d - b,\ q_x = a + b - d,\ p_y = b + a - c,\ q_y = b + c - a.$$

Како $|a|, |b|, |c|, |d| \leq S \implies |p_x|, |p_y|, |q_x|, |q_y| \leq 2S$, добијамо $(p_x, p_y), (q_x, q_y) \in P$ чиме је доказ готов. □

Нека је $\mathcal{L}_0 \subset \mathcal{L}$ скуп правих које спајају $(a, b, 0)$ и $(c, d, 1)$ за природне бројеве $a, b, c, d \leq S$. Тада је $|\mathcal{L}_0| = S^4$. Сада ћемо да проучимо инциденције између тих правих.

Лема 54. Нека је $\mathfrak{S}_k$ скуп тачака из $\mathbb{R}^3$ таквих да леже на бар k правих из $\mathcal{L}_0$. За свако $2 \leq k \leq (1/400)S^2$ важи:

$$|\mathfrak{S}_k| \gtrsim S^6 k^{-2}.$$

Доказ. Посматрајмо тачку $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ за коју $0 < x_3 < 1$. Дефинишимо функцију $F_x : \mathbb{R}^2 \mapsto \mathbb{R}^2$ за коју $F_x(a, b) = (c, d)$ уколико права кроз $(a, b, 0)$ и $(c, d, 1)$ пролази кроз x. Означимо са G скуп $(a, b) \in \mathbb{N}^2$ таквих да је $a, b \leq S$. Број правих из $\mathcal{L}_0$ које пролазе кроз x је тачно $F_x(G) \cap G$. Како се две праве из $\mathcal{L}_0$ секу у рационалној тачки, можемо да претпоставимо да су координате x рационалне и да је $x_3 = p/q$ у сређеном облику (односно $(p, q) = 1$).

Из сличности троуглова добијамо да је $F_x(G)$ квадратна решетка са растојањем $\frac{q-p}{p}$. Како је $(p, q) = 1$, $F_x(G) \cap G$ ће бити правоугаона решетка са растојањем $q - p$. Странице те решетке ће свакако бити $\leq S$, одакле је број тачака у $F_x(G) \cap G$ највише $S^2(q-p)^{-2}$. Међутим, опет из сличности троуглова добијамо да је страница решетке $F_x(G)$ једнака $S \cdot \frac{q-p}{p}$ одакле је највише толико страница решетке $F_x(G) \cap G$ па је број тачака у њој највише $S^2 p^{-2}$. Из те две неједнакости закључујемо да је $|F_x(G) \cap G| \leq 4S^2 q^{-2}$.

Дефинишимо $G_{sred} \subset G$ као скуп свих тачака $(a, b) \in \mathbb{N}^2$ за које $(1/4)S \leq a, b \leq (3/4)S$. Докажимо да ако $|F_x(G_{sred}) \cap G| > 0$ онда је број тачака у $F_x(G) \cap G$ реда величине горње оцене. Наиме, знамо да тачки $y \in G_{sred}$ одговара $F_x(y)$ која је у "средини" квадратне решетке $F_x(G)$, односно на растојању бар $(1/4)S \cdot \frac{q-p}{p}$ од страница те решетке. Такође за неку тачку $y \in G_{sred}$, $F_x(y) \in G$ па се тачка $F_x(y)$ налази на растојању бар $S/2$ од једне вертикалне и једне хоризонталне странице. Одавде добијамо да су странице правоугаоне решетке $F_x(G) \cap G$ бар $\min(\frac{1}{2}S, S \cdot \frac{q-p}{4p})$, одакле тривијално следи $|F_x(G) \cap G| \geq (1/100)S^2 q^{-2}$.

Дефинишимо $X(p, q)$ као скуп свих тачака $x = (x_1, x_2, p/q)$ таквих да $F_x(G_{sred}) \cap G$ није празан скуп. Тада скуп $X(p, q)$ лежи у $\mathfrak{S}_k$ кад год k није веће од $(1/100)S^2 q^{-2}$, односно $q \leq (1/10)Sk^{-\frac{1}{2}}$.

За било које $(a_1, b_1) \in G_{sred}$ и $(a_2, b_2) \in G$ (таквих парова има $\gtrsim S^4$) постоји јединствена тачка $x \in X(p, q)$ која лежи на правој кроз $(a_1, b_1, 0)$ и $(a_2, b_2, 1)$. Свака таква тачка се налази на највише $4S^2 q^{-2}$ правих из $\mathcal{L}_0$. одакле следи да је $|X(p, q)| \gtrsim S^2 q^2$.

Сада фиксирајмо $k \leq (1/400)S^2$. Тада за природан број $(1/20)Sk^{-\frac{1}{2}} \leq q \leq (1/10)Sk^{-\frac{1}{2}}$ (k је довољно мало да постоји такав) и за свако $p \in \mathbb{N}$ такво да $p < q$ и $(p, q) = 1$ важи $X(p, q) \subset \mathfrak{S}_k$. Скупови $X(p, q)$ су очигледно дисјунктни, па добијамо:

$$|\mathfrak{S}_k| \gtrsim \sum_{q=(1/20)Sk^{-\frac{1}{2}}}^{(1/10)Sk^{-\frac{1}{2}}} \sum_{0<p<q,\ (p,q)=1} |X(p, q)| \gtrsim \sum_{q=(1/20)Sk^{-\frac{1}{2}}}^{(1/10)Sk^{-\frac{1}{2}}} \phi(q) S^2 q^2.$$

Суме Ојлерове функције $\phi(n)$ су доста проучаване. Теорема 3.7 у [A] даје оцену $\sum_{q=1}^{x}\phi(q)=\frac{3}{\pi^2}x^2+O(x\log x)$. Дакле, $\sum_{q=x}^{2x}\phi(q)\sim x^2$, па:

$$|\mathfrak{S}_k|\gtrsim(Sk^{-\frac{1}{2}})^2S^2q^2\gtrsim S^6k^{-2}.$$

□

Сада $|G_k(P)|\geq|\mathfrak{S}_k|\gtrsim S^6k^{-2}\gtrsim N^3k^{-2}$ за $2\leq k\leq(1/400)S^2$ односно за $2\leq k\leq(1/100000)N$. На основу другог поглавља имамо:

$$|Q(P)|=\sum_{k=2}^{N}2(k-1)\cdot|G_k(P)|\gtrsim\sum_{k=2}^{N/100000}N^3k^{-1}\gtrsim N^3\log N.$$

За скуп $\mathcal{L}_0\subset\mathcal{L}$ важи да $\lesssim S^2\lesssim N$ правих лежи у истој равни или регулусу на основу Тврђења 6, па добијамо да је оцена из Теореме 8 оштра до на константу.

Ако се вратимо сада на Пример 26 за Теорему 23, добијамо оштру оцену под претпоставком да је $B\gtrsim L^{\frac{1}{2}}$. За мање B не знамо шта се дешава. На пример, претпоставимо да имамо скуп $\mathcal{L}$ правих из $\mathbb{R}^3$ тако да никоје 100 не леже у равни. Колико тачака може лежати на бар 3 праве из датог скупа? Претпоставимо да никојих 100 не лежи ни у регулусу. Колико се онда тачака налази у пресеку правих из датог скупа? Питања овог типа су и даље отворена. Са обзиром на то колико су идеје из алгебре допринеле решавању Ердошевог проблема различитих растојања и њему сличних, одговор на оваква питања би, без икакве сумње, додатно продубио наше схватање повезаности ове две области.

Литература

[A] T. Apostol, *Introduction to Analytic Number Theory*, Springer (1976).

[ГК] L.Guth, N.H.Katz, *On the Erdős distinct distance problem in plane*, Annals of Mathematics 181 (2015), 155-190.

[ГК1] L.Guth, N.H.Katz, *Algebraic methods in discrete analogs of the Kakeya problem*, Advances in Mathematics 225 (2010), 2828–2839.

[Д] Z.Dvir, *On the size of Kakeya sets in finite fields*, Journal of the American Mathematical Society 22 (2009),1093-1097.

[E] P.Erdős, *On sets of distances of n points*, American Mathematical Monthly 53 (1946), 248-250.

[ЕКШ] Gy. Elekes, H. Kaplan, M.Sharir, *On lines, joints, and incidences in three dimensions*, Journal of Combinatorial Theory, Series A 118 (2011) , 962-977.

[K] N.H.Katz, *The flecnode polynomial: a central object in incidence geometry*, arXiv:1404.3412 (2014).

[КЛО] D.Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer (2006), 150-159.

[Салм] G. Salmon, *A Treatise on the Analytic Geometry of Three Dimensions*, Vol.2 5th edition Hodges, Figgis And Co. Ltd. (1915).