Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Ivan Novak

Računanje drugog momenta familija eliptičkih krivulja

Zagreb, 2021.

Ovaj rad izrađen je na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta pod vodstvom izv. prof. dr. sc. Matije Kazalickog i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2020./2021.

Sadržaj

1 Uvod

Promotrimo familiju eliptičkih krivulja parametriziranu parametrom k,

$$\mathcal{F}_k : y^2 = P(x)k + Q(x),$$

gdje su $P, Q \in \mathbb{Z}[x]$ polinomi stupnja manjeg ili jednakog 3, te je barem jedan od ta dva polinoma stupnja 3. Također, pretpostavljamo da polinomi P i Q nemaju zajedničkih nultočaka. Za prost broj p, definiramo drugi moment te familije s

$$M_{2,p}(\mathcal{F}_k) = \sum_{k \in \mathbb{F}_p} a_{k,p}^2,$$

gdje je $a_{k,p} = p - \#\{(x, y) \in \mathbb{F}_p^2 \mid y^2 = P(x)k + Q(x)\}$.

Cilj nam je izračunati drugi moment $M_{2,p}(\mathcal{F}_k)$. Drugi moment familije krivulja može se, kao što je objašnjeno u uvodu [5], zapisati kao zbroj članova reda $p^{i/2}$ za $i \in \{0, 1, 2, 3, 4\}$, tj. kao izraz oblika

$$M_{2,p}(\mathcal{F}_k) = f_4(p) + f_3(p) + f_2(p) + f_1(p) + f_0(p), \tag{1}$$

gdje je $|f_i(p)| \leq C p^{i/2}$ za neku konstantu C koja ne ovisi o p nego samo o familiji $(\mathcal{F}_k)_k$. Naravno, ovakav zapis nije jedinstven, ali moguće je definirati kanonski izbor gornjih koeficijenata koji je onda jedinstven. Točnije, možemo proširiti definiciju drugog momenta i na polja $\mathbb{F}_{p^i}$ za $i > 1$. Dakle, definiramo drugi moment

$$M_{2,p^i}(\mathcal{F}_k) = \sum_{k \in \mathbb{F}_{p^i}} (p^i + 1 - \#\mathcal{F}_k(\mathbb{F}_{p^i}))^2.$$

Tada možemo promatrati zeta funkciju niza $(M_{2,p^i}(\mathcal{F}_k))_i$,

$$Z((M_{2,p^i}(\mathcal{F}_k))_i, T) := \exp\left(\sum_{i=1}^{\infty} \frac{M_{2,p^i}(\mathcal{F}_k)}{i} T^i\right).$$

Može se pokazati, kao u Teoremu 1.3 iz [5], da je ovo racionalna funkcija, odnosno element skupa $\mathbb{Q}(T)$. Naime, suma $M_{2,p^i}(\mathcal{F}_k)$ može se interpretirati kao linearna kombinacija broja točaka nad $\mathbb{F}_{p^i}$ na nekim afinim mnogostrukostima. Tada iz Dworkovog teorema slijedi da je $Z((M_{2,p^i}(\mathcal{F}_k))_i, T)$ također racionalna funkcija, odnosno element skupa $\mathbb{Q}(T)$. Točnije, možemo ju napisati kao

$$\frac{P_1(T)P_3(T)}{P_0(T)P_2(T)P_4(T)},$$

gdje su $P_i(T) \in \mathbb{Q}[x]$. Nadalje, iz Riemannove hipoteze za konačna polja, jedne od Weilovih slutnji, slijedi da sve nultočke polinoma P_i imaju apsolutnu vrijednost $p^{-i/2}$. Iz toga se može

pokazati da postoje algebarski brojevi $(\alpha_{i,j}^{(p)})_{i,j}$ takvi da za svaki $l \geq 1$ vrijedi

$$M_{2,p^l}(\mathcal{F}_k) = \sum_{i=0}^{4} \sum_{j} (\alpha_{i,j}^{(p)})^l,$$

te vrijedi $|\alpha_{i,j}^{(p)}| = p^{i/2}$. Onda možemo definirati $f_i(p)$ kao $\sum_j \alpha_{i,j}^{(p)}$. Rastav (1) ćemo zvati kanonski rastav drugog momenta od $\mathcal{F}_k$. Više o Weilovim slutnjama može se naći u [14].

Neka je $(a_p)_p$ neki niz indeksiran skupom prostih brojeva. Neka je S skup svih realnih brojeva β takvih da postoji $A > 0$ takav da je $|a_p| \leq Ap^\beta$ za svaki prost broj p. Pretpostavimo da S ima minimum α. Tada definiramo prosjek niza $(a_p)_p$, u oznaci $\mu((a_p)_p)$, kao

$$\lim_{n\to\infty} \frac{1}{\pi(n)} \sum_{p\leq n} \frac{a_p}{p^\alpha}.$$

Onda ima smisla promatrati prosjeke nizova $(f_i(p))_p$. Michel [7] je dokazao sljedeći teorem za prosjek niza $(f_4(p))_p$.

Teorem 1.1. *Ako je $\mathcal{F}_k$ familija eliptičkih krivulja sa nekonstantnom j-invarijantom onda postoji $\mu((a_p)_p)$ i pozitivan je.*

Nas zanimaju prosjeci članova nižeg reda. Formalno, imamo sljedeću slutnju.

Slutnja (Bias Conjecture)**.** *Neka je $\mathcal{G}_k$ jednoparametarska familija eliptičkih krivulja nad $\mathbb{Q}$, te neka je $M_{2,p} = \sum_{i=0}^{4} f_i(p)$ kanonski rastav drugog momenta od $\mathcal{G}_k$. Tada za najveći $i \in \{0,1,2,3\}$ za koji $\mu((f_i(p))_p)$ nije jednak 0 vrijedi da je $\mu((f_i(p))_p)$ negativan.*

U skladu s ovom slutnjom, definiramo bias (pristranost) familije $\mathcal{G}_k$ kao $\mu((f_i(p))_p)$, za najveći i za koji taj limes nije jednak 0. Ekvivalentna formulacija slutnje je da je bias familije $\mathcal{G}_k$ negativan.

Motivacija za proučavanje drugog momenta dolazi iz činjenice da prvi momenti imaju veze s rangom familija eliptičkih krivulja, pa je prirodno postaviti pitanje za momente višeg reda. Proučavanje drugog momenta prvi je započeo Miller u [8].

Kazalicki i Naskrecki su u [5] dokazali slutnju za $\mathcal{F}_k$ za generički izbor polinoma P i Q, uz pretpostavku Sato-Tateov slutnje za krivulje genusa 2. Ovaj rad je dopuna tog članka, te je cilj proučavati rubne slučajeve koji nisu potpuno pokriveni tim člankom. Za slučajeve koje ćemo promatrati ćemo koristiti Sato-Tateovu slutnju za krivulje genusa 1, koja je dokazana.

Za afinu algebarsku mnogostrukost $T \subset \mathbb{A}^d$ definiranu nad $\mathbb{F}_p$ za neki prost broj p i prirodan broj d, sa $\#T(\mathbb{F}_p)$ označavati ćemo broj d-torki $(x_1, \ldots, x_d) \in \mathbb{F}_p^d$ koje se nalaze u T. Ako je p jasan iz konteksta, pisat ćemo $\#T$. Polinome poistovjećujemo sa skupovima njihovih nultočaka, pa oznaka $\#T(\mathbb{F}_p)$ ima smisla i ako je $T \in \mathbb{Q}[x_1, \ldots, x_d]$ i ako nazivnici koeficijenata od T nisu djeljivi s p (točnije, onda umjesto T promatramo redukciju od T modulo p i broj nultočaka redukcije).

Sada ćemo uvesti krivulje koje će nam biti važne. Definiramo $\Delta(x_1, x_2) \in \mathbb{Q}[x_1, x_2]$ kao

$$P(x_1)Q(x_2) - Q(x_1)P(x_2),$$

te $M_\infty(x_1, x_2, y) \in \mathbb{Q}[x_1, x_2, y]$ kao

$$P(x_1)P(x_2) - y^2.$$

Nadalje, lako se vidi da je Δ djeljiv polinomom $x_2 - x_1$, pa definiramo

$$\tilde{\Delta}(x_1, x_2) := \frac{\Delta(x_1, x_2)}{x_2 - x_1}.$$

Definiramo i polinom $S(x) \in \mathbb{Q}[x]$ kao $\tilde{\Delta}(x, x)$. Lako se vidi da vrijedi $S(x) = P(x)Q'(x) - Q(x)P'(x)$.

Također, definiramo algebarske krivulje C i $\tilde{C}$ kao presjeke ploha M_∞ sa $\pi^{-1}(\Delta)$ i $\pi^{-1}(\tilde{\Delta})$ gdje je $\pi : \mathbb{A}^3 \to \mathbb{A}^2$ projekcija na prve dvije koordinate, odnosno $\pi(x_1, x_2, y) = (x_1, x_2)$.

Također, koristit ćemo oznake $P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ te $Q(x) = b_3x^3 + b_2x^2 + b_1x + b_0$. Nadalje, za matricu $\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$, njene 2×2 minore označavat ćemo sa $\mu_{i,j}$, gdje su $0 \leq i \leq j \leq 3$. Drugim riječima, definiramo $\mu_{i,j} = a_ib_j - a_jb_i$.

Nadalje, definiramo još dva izraza koji će nam biti važni:

$$\begin{aligned} \mu &:= \mu_{1,3}^2 - 4\mu_{0,3}\mu_{2,3} \\ s &:= \mu_{1,2}^3 + 27\mu_{0,1}\mu_{1,3}^2 + 27\left(\mu_{0,2}^2 - \mu_{0,1}\mu_{1,2}\right)\mu_{2,3} - 9\mu_{0,3}\left(\mu_{1,2}^2 + 9\mu_{0,1}\mu_{2,3}\right). \end{aligned}$$

Pokazuje se prirodnim razdvajati računanje drugog momenta na slučajeve u ovisnosti o tome koji od brojeva $\mu_{2,3}, \mu, s$ su jednaki 0. Razlog za to je što upravo ti brojevi utječu na to koliko krivulje koje ćemo promatrati imaju singulariteta, i kakvi su ti singulariteti. Kazalicki i Neskracki su se primarno bavili generičkim slučajem, tj. slučajem u kojem niti jedan od tih brojeva nije jednak 0. Mi ćemo se fokusirati na neke od preostalih slučajeva. Konkretnije, potpuno ćemo riješiti slučaj kad je $\mu = 0$. U Tablici 1 navedeni su svi slučajevi. Kazalicki i Naskrecki su riješili slučaj 1. U

	$\mu_{23} = 0$	$\mu = 0$	$s = 0$
1	NE	NE	NE
2	NE	NE	DA
3	NE	DA	NE
4	NE	DA	DA
5	DA	NE	NE
6	DA	NE	DA
7	DA	DA	NE
8	DA	DA	DA

Tablica 1: Popis slučajeva ovisno o parametrima $\mu_{2,3}, \mu, s$

ovom članku smo, u odjeljku 4, riješili slučajeve 3,4,7 i 8. U Teoremu 4.4 riješeni su slučajevi 3 i 4, a u Teoremu 4.8 slučajevi 7 i 8. U sva četiri slučaja koje smo riješili vrijedi da je polinom Q u kvocijentnom prstenu $\mathbb{Q}[x]/(P)$ jednak umnošku konstante i kvadrata. Drugim riječima, dokazali smo slutnju za parove polinoma (P, Q) za koje vrijedi $Q(x) = AP(x) + BT(x)^2$ za neke racionalne brojeve A, B te neki polinom $T \in \mathbb{Q}[x]$.

U slučajevima 5, 6, 7, 8 je ostatak pri dijeljenju polinoma Q pri dijeljenju s P stupnja manjeg ili

jednakog od 1, tj. Q je linearan ili konstantan polinom u $\mathbb{Q}[x]/(P)$.

U slučajevima 2, 4, 6, 8 vrijedi da krivulja $\tilde{\Delta}$ ima jedan ili dva afina singulariteta. U Primjeru 3.7 smo dali parametrizaciju polinoma P i Q za koje je $s = 0$.

U pododjeljku 2.1 navedene su neke pomoćne tvrdnje koje ćemo koristiti u radu. U pododjeljku 2.2 iskazani su rezultati iz [5] koji vrijede neovisno o izboru polinoma P i Q. U nastavku odjeljka 2 definirani su još neki pojmovi bitni za ovaj rad, prvenstveno iz algebarske geometrije. U pododjeljku 2.4 opisan je blowing-up kao metoda razrješenja singulariteta. U pododjeljku 2.5 ukratko je definiran pojam genusa. Pododjeljak 2.6 se bavi Sato-Tateovom slutnjom odnosno teoremom.

U odjeljku 3 se bavimo krivuljom

$$\tilde{\Delta}(x_1, x_2) := \frac{P(x_1)Q(x_2) - Q(x_1)P(x_2)}{x_2 - x_1}.$$

Cilj odjeljka je povezati broj $\mathbb{F}_p$- racionalnih točaka na krivulji $\tilde{\Delta}$ s brojem $\mathbb{F}_p$-racionalnih točaka na nekoj nesingularnoj projektivnoj krivulji. Za to je potrebno analizirati singularitete te ih razriješiti koristeći blowing-up. Iz pododjeljka 2.2 vidi se koja je važnost krivulje $\tilde{\Delta}$ za početni problem i zašto je potrebno analizirati tu krivulju.

Navedimo još eksplicitne formule za $\tilde{\Delta}$ i S, koristeći koeficijente $(\mu_{i,j})_{i,j}$:

$$\begin{aligned}\tilde{\Delta}(x_1, x_2) &= \mu_{2,3}x_1^2x_2^2 + \mu_{1,3}(x_1x_2^2 + x_1^2x_2) + \mu_{0,3}(x_1^2 + x_1x_2 + x_2^2) + \mu_{1,2}x_1x_2 + \mu_{0,2}(x_1 + x_2) + \mu_{0,1},\\ S(x) &= \mu_{2,3}x^4 + 2\mu_{1,3}x^3 + (3\mu_{0,3} + \mu_{1,2})x^2 + 2\mu_{0,2}x + \mu_{0,1}.\end{aligned}$$

2 Matematička pozadina i prijašnji rezultati

2.1 Neke pomoćne tvrdnje

Lema 2.1. *Za prost broj p i cijele brojeve a, b i c, gdje je $a \not\equiv 0 \pmod p$ i ϕ_p Legendrov simbol modulo p vrijedi:*

$$\sum_{t\in\mathbb{F}_p} \phi_p(at^2+bt+c) = \begin{cases} -\phi_p(a) & \text{ako je } b^2-4ac \not\equiv 0 \pmod p \\ (p-1)\phi_p(a) & \text{ako je } b^2-4ac \equiv 0 \pmod p. \end{cases} \tag{2}$$

Dokaz: Ako je $b^2-4ac=0$, onda je $at^2+bt+c = a(t-d)^2$ za neki $d\in\mathbb{F}_p$, pa se kao pribrojnik s lijeve strane za $t\neq d$ pojavljuje $\phi_p(a)$, a za $t=d$ dobiva se 0, pa tvrdnja slijedi.

Ako je pak $D := b^2-4ac \neq 0$, onda se suma može zapisati kao $\phi_p(a)\sum_{t\in\mathbb{F}_p}\phi_p(t^2-D)$. Sada treba prebrojati za koliko vrijednosti t je t^2-D kvadrat u $\mathbb{F}_p$, koliko puta je jednako nuli i koliko puta nije kvadrat. Ako je $t^2-D=x^2\neq 0$, onda je $(t-x)(t+x)=D$, odnosno postoji $A\in\mathbb{F}_p^\times$ za koji je $t-x=A$, $t+x=DA^{-1}$, odnosno $t=\dfrac{A+DA^{-1}}{2}$. Nadalje, $A+DA^{-1}=B+DB^{-1}$ ako i samo ako je $A=B$ ili $AB=D$.

Dakle, broj različitih vrijednosti t za koje je t^2-D kvadrat različit od nule je $\dfrac{p-1}{2}$ ako D nije kvadrat u $\mathbb{F}_p$, te $\dfrac{p-3}{2}$ ako D jest kvadrat.
Broj vrijednosti t za koje je $t^2-D=0$ je 0 ako D nije kvadrat te 2 ako D jest kvadrat. U oba slučaja, dobijemo da je ukupna suma jednaka $-\phi_p(a)$. □

Lema 2.2. *Ako polinomi s racionalnim koeficijentima A i B nemaju zajedničkih nultočaka, onda za svaki osim konačno mnogo prostih brojeva p njihove redukcije modulo p nemaju zajedničkih nultočaka.*

Dokaz: Kako su A i B relativno prosti, vrijedi da postoje polinomi $C, D\in\mathbb{Q}[x]$ takvi da je $A(x)D(x)-B(x)C(x)=1$. Kad reduciramo cijeli izraz modulo p za neki prost broj koji ne dijeli ni jedan od nazivnika koeficijenata ovih polinoma, ako bi vrijedilo $A(t)=B(t)=0$ u $\mathbb{F}_p$ za neki $t\in\mathbb{F}_p$, onda bismo imali da je $0=1$ u $\mathbb{F}_p$, kontradikcija. □

Dokaz sljedeće leme može se pronaći u [5] (Proposition 4.1.), a koristi Galoisovu teoriju i teoriju reprezentacija. Koristit ćemo ju samo da bismo točno odredili čemu je bias jednak. Za $x>0$, označimo sa $\pi(x)$ broj prostih brojeva manjih ili jednakih x.

Lema 2.3. *Neka je $T(x)\in\mathbb{Q}[x]$ ireducibilan polinom. Tada vrijedi*

$$\lim_{x\to+\infty}\frac{\sum_{p\leq x}\#T(\mathbb{F}_p)}{\pi(x)} = 1.$$

2.2 Rezultati neovisni o izboru P i Q

U ovom ćemo pododjeljku izvesti formulu za drugi moment koja će vrijediti za svaki par polinoma P, Q stupnja manjeg ili jednakog 3. Kao prvo, prirodno je (zbog ljepših krajnjih rezultata) u izraz za $M_{2,p}$ dodati član $a_{\infty,p} = p - \#\{(x,y) \in \mathbb{F}_p^2 \mid P(x) = y^2\}$, pa je onda familija $\mathcal{F}_k$ zapravo parametrizirana sa $\mathbb{P}^1(\mathbb{F}_p)$. Zapravo ćemo onda računati $\tilde{M}_{2,p} := M_{2,p} + a_{\infty,p}^2$.

Početna ideja u [5] je bila uvesti sljedeće mnogostrukosti u redom $\mathbb{A}^4$ te $\mathbb{A}^3$:

$$M_{aff} : = (P(x_1)k + Q(x_1))(P(x_2)k + Q(x_2)) - y^2,$$
$$M_{\infty} : = P(x_1)P(x_2) - y^2.$$

Njihovim 'ljepljenjem' dobivamo mnogostrukost M koja se nalazi u prostoru $\mathbb{A} \times \mathbb{A} \times \mathbb{P} \times \mathbb{A}$. Formalno, poistovjetimo točke $(x_1, x_2, k, y) \in M_{aff}$ sa točkama $(x_1, x_2, (k : 1), y)$ i točke $(x_1, x_2, y) \in M_{\infty}$ sa $(x_1, x_2, (1 : 0), y)$, te definiramo M kao uniju tih dvaju skupova.
Trodimenzionalna mnogostrukost M nam je važna zbog sljedećeg rezultata, čiji dokaz se može naći u [5] (Theorem 2.2).

Teorem 2.4. *Za svaku potenciju prostog broja q vrijedi $\tilde{M}_{2,q}(\mathcal{F}_k) = q^3 + q^2 + \#M(\mathbb{F}_q)$.*

Ovime smo prebacili problem određivanja drugog momenta na problem brojanja točaka na geometrijskom objektu M. Nadalje, polinom koji definira M je stupnja 2 po k. Tada, za fiksne x_1 i x_2, broj točaka oblika $(x_1, x_2, (k : 1), y) \in M$ možemo prebrojati koristeći Lemu 2.1. Korijen diskriminante tog kvadratnog polinoma je upravo $P(x_1)Q(x_2) - Q(x_1)P(x_2) = \Delta(x_1, x_2)$, i to objašnjava važnost krivulje Δ. Pažljivijim prebrojavanjem dobiva se sljedeći rezultat (Theorem 2.3. iz [5]).

Lema 2.5. *Neka je q potencija prostog broja različitog od 2. Tada vrijedi*

$$\#M(\mathbb{F}_q) = q^3 + q^2 + q\left(\#C(\mathbb{F}_q) - \#\Delta(\mathbb{F}_q)\right) + q\Big(\sum_{\substack{x \in \mathbb{F}_q \\ P(x) \equiv 0}} \phi_q(Q(x))\Big)^2,$$

odnosno

$$\tilde{M}_{2,q}(\mathcal{F}_k) = q\left(\#C(\mathbb{F}_q) - \#\Delta(\mathbb{F}_q) + \Big(\sum_{\substack{x \in \mathbb{F}_p \\ P(x) \equiv 0}} \phi_p(Q(x))\Big)^2\right),$$

gdje su C i Δ krivulje definirane u odjeljku 1.

Primijetimo da Δ i C obje sadrže pravac $x_1 = x_2$, odnosno reducibilne su. Zato nećemo proučavati njih već mnogostrukosti $\tilde{\Delta}(x_1, x_2) = \dfrac{\Delta(x_1, x_2)}{x_2 - x_1}$ i $\tilde{C} = M_{\infty} \cap \pi^{-1}(\tilde{\Delta})$, gdje je $\pi : \mathbb{A}^3 \to \mathbb{A}^2$ definirana s $\pi(x_1, x_2, y) = (x_1, x_2)$. Također definiramo polinom $S(x) := \tilde{\Delta}(x, x)$. Imamo sljedeći rezultat koji će nam biti početna točka analize posebnih slučajeva.

Lema 2.6. *Za neparan prost broj p vrijedi*

$$\tilde{M}_{2,p}(\mathcal{F}_k) = p\left(\#\tilde{C}(\mathbb{F}_p) - \#\tilde{\Delta}(\mathbb{F}_p) + p - \#P(\mathbb{F}_q) - \#S(\mathbb{F}_p) + \#P \cap S(\mathbb{F}_p) + \Big(\sum_{\substack{x \in \mathbb{F}_p \\ P(x) \equiv 0}} \phi_p(Q(x))\Big)^2\right).$$

Dokaz: Fiksirajmo prost broj p. Za mnogostrukost T, pisati ćemo $\#T$ umjesto $\#T(\mathbb{F}_p)$. Vrijedi

$$\#\tilde{\Delta} = \#\{(x_1, x_2) \in \Delta(\mathbb{F}_p) \wedge x_1 \neq x_2\} + \#S = \#\Delta - p + \#S,$$

gdje druga jednakost slijedi jer je svih p točaka oblika (x, x) za $x \in \mathbb{F}_p$ na krivulji Δ, a prva slijedi iz definicije krivulje $\tilde{\Delta}$. Nadalje, vrijedi

$$\#\tilde{C} = \#(\pi^{-1}(\tilde{\Delta}) \cap M_\infty) = \#C - \#(\pi^{-1}(\Delta \setminus \tilde{\Delta}) \cap M_\infty).$$

Ako je točka $(x_1, x_2) \in \Delta \setminus \tilde{\Delta}$, onda je $x_1 = x_2$. Broj točaka oblika $(x_1, x_1, y) \in \pi^{-1}(\Delta \setminus \tilde{\Delta}) \cap M_\infty$ je jednak 1 ako je x_1 nultočka od P i nije nultočka od S, jednak 2 ako x_1 nije nultočka od P niti od S, te jednak 0 ako je x_1 nultočka od S. Dakle, vrijedi

$$\#\tilde{C} = \#C - \#P + \#(P \cap S) - 2(p - \#P - \#S + \#(P \cap S) = \#C - 2p + \#P + 2\#S - \#(P \cap S).$$

Oduzimanjem dobivenih izraza za $\#\tilde{C}$ i $\#\tilde{\Delta}$ i korištenjem Leme 2.5 slijedi tvrdnja. □

2.3 Algebarska geometrija

U odjeljku 3 bavimo se analizom singulariteta krivulje $\tilde{\Delta}$. Razlog je što u krajnjoj formuli želimo dobiti broj točaka na glatkoj projektivnoj krivulji genusa manjeg ili jednakog 1, na koju onda možemo primijeniti Sato-Tateov teorem.

Cilj ovog pododjeljka je definirati pojmove koji se koriste u tom poglavlju i iskazati neke rezultate koji opravdavaju zaključke. Konceptualno zahtjevniji dokazi su izostavljeni, isto kao i neki tehnički detalji. Za potpuniji i detaljniji tretman upućujemo na [4]. Ovaj pododjeljak većinom prati pristup iz [10].

Neka je k algebarski zatvoreno polje. Za prirodan broj n, definiramo afinu n-dimenzionalnu ravninu $\mathbb{A}^n_k$ kao k^n, odnosno kao skup n-torki elemenata iz k. Razlog za drugačiju oznaku je što ćemo $\mathbb{A}^n_k$ snabdjeti topologijom koju ćemo uskoro opisati. Ubuduće ćemo pisati samo $\mathbb{A}^n$ umjesto $\mathbb{A}^n_k$ kad god će iz konteksta biti jasno što je k.

Za skup polinoma $I \subseteq k[x_1, \ldots, x_n]$, definiramo

$$\mathcal{Z}(I) := \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid f(x_1, \ldots, x_n) = 0 \ \forall f \in I\}.$$

Analogno, za skup točaka $S \subset \mathbb{A}^n$, definiramo

$$\mathcal{I}(S) := \{f \in k[x_1, \ldots, x_n] \mid f(x_1, \ldots, x_n) = 0 \ \forall (x_1, \ldots, x_n) \in S\}.$$

Primijetimo da vrijedi $\mathbb{Z}(I) = \mathbb{Z}(\langle I \rangle)$, gdje je $\langle I \rangle$ najmanji ideal u $k[x_1, \ldots, x_n]$ koji je nadskup od I. Primijetimo da za ideale I i J vrijedi $\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(I \cap J)$. Za proizvoljnu familiju ideala $(I_\alpha)_\alpha$ vrijedi

$$\cap_\alpha \mathcal{Z}(I_\alpha) = Z(\cup_\alpha I_\alpha).$$

Također, $\mathcal{Z}((0)) = \mathbb{A}^n$ i $\mathcal{Z}(k[x_1, \ldots, x_n]) = \emptyset$. Iz ovih svojstava slijedi da je familija svih komplemenata skupova oblika $\mathcal{Z}(I)$ za neki ideal I topologija na $\mathbb{A}^n$. Ovu topologiju zovemo *topologija Zariskog*. Nadalje će riječi 'zatvoren' i 'otvoren' označavati te pojmove u topologiji Zariskog.

Operacije $\mathcal{Z}$ i $\mathcal{I}$ su naizgled obrnute. Ima smisla pitati se jesu li međusobno inverzne. To ipak ne vrijedi u potpunosti, jer na primjer za ideale (x) i (x^2) u $k[x, y]$ vrijedi $\mathcal{Z}((x)) = \mathcal{Z}((x^2)) = \{(0, y) \mid y \in k\}$, pa $\mathcal{Z}$ nije injekcija.

S druge strane, iz definicija jednostavno slijedi $\mathcal{Z}(\mathcal{I}(S)) = \overline{S}$ za svaki $S \in k[x_1, \ldots, x_n]$ gdje je $\overline{S}$ najmanji zatvoren skup koji sadrži S.

Definicija 2.7. Za ideal $I \subset k[x_1, \ldots, x_n]$, definiramo *radikal* od I kao

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid f^m \in I \text{ za neki } m \in \mathbb{N}\}.$$

Za ideal kažemo da je radikal ako je jednak svom radikalu.

Primijetimo da za svaki $S \subset \mathbb{A}^n$ zapravo vrijedi da je $\mathcal{I}(S)$ radikal, pa je sljedeći teorem u nekom smislu najviše čemu se možemo nadati da vrijedi.

Teorem 2.8 (Hilbertov teorem o nulama)**.** *Za svaki ideal $I \subset k[x_1, \ldots, x_n]$ vrijedi*

$$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}.$$

Dokaz ovog teorema može se naći u [1]. Zanimljivo, ovaj teorem ima primjene i u nekim drugim granama matematike. Primjena u teoriji grafova može se naći u članku [3].

Sada je cilj definirati afinu mnogostrukost. Za to nam prvo treba par topoloških definicija.

Definicija 2.9. Neka je X topološki prostor. Za X kažemo da je reducibilan ako je prazan ili ako postoje zatvoreni neprazni pravi podskupovi U i V od X takvi da je $U \cup V = X$. Inače kažemo da je X ireducibilan. Za podskup Y topološkog prostora X kažemo da je ireducibilan ako je Y ireducibilan topološki prostor u odnosu na relativnu topologiju u odnosu na X.

Sljedeći kriterij služi za određivanje koji od Zariski zatvorenih skupova su ireducibilni.

Propozicija 2.10. *Zatvoren skup $Y \subset \mathbb{A}^n$ je zatvoren ako i samo ako je ideal $\mathcal{I}(Y)$ prost.*

Dokaz: Ako $\mathcal{I}(Y)$ nije prost, onda postoje f i g koji nisu elementi $\mathcal{I}(Y)$ takvi da je $fg \in \mathcal{I}(Y)$. Međutim, onda je $\mathcal{Z}((f)) \cup \mathcal{Z}((g)) = \mathcal{Z}((fg)) \supset Y$, pa su $\mathcal{Z}((f)) \cap Y$ i $\mathcal{Z}((g)) \cap Y$ pravi zatvoreni podskupovi od Y čija unija je Y, pa je Y reducibilan.

Ako je Y reducibilan, onda je $Y = \mathcal{Z}(I) \cup \mathcal{Z}(J)$ za neke ideale I i J takve da su $\mathcal{Z}(I)$ i $\mathcal{Z}(J)$ pravi neprazni podskupovi od Y. Zbog Hilbertovog teorema o nulama, bez smanjenja općenitosti možemo pretpostaviti da su I i J radikali. Ako bi bilo $I \subset J$, onda bi vrijedilo $Y = \mathcal{Z}(I)$, što je kontradikcija. Analogno, $J \not\subset I$.

Uzmimo $f \in I \setminus J$ te $g \in J \setminus I$, te promotrimo fg. Vrijedi $fg \in \mathcal{I}(Y)$. Međutim, $f \notin \mathcal{I}(Y)$. Naime, u suprotnom bi se f poništavao na skupu $\mathcal{Z}(J)$, iz čega bi slijedilo $f \in J$, što je kontradikcija. Analogno, $g \notin \mathcal{I}(Y)$. Dakle, $\mathcal{I}(Y)$ nije prost. □

Definicija 2.11. Topološki prostor X je Noetherin ako se svaki rastući niz $(X_n)_{n\in\mathbb{N}}$ zatvorenih podskupova od X stabilizira, odnosno ako postoji M takav da je $X_n = X_M$ za svaki $n > M$.

Napomena: Topološki prostor $\mathbb{A}^n$ je Noetherin. Naime, ako je

$$\mathcal{Z}(I_1) \subset \mathcal{Z}(I_2) \subset \dots$$

rastući niz zatvorenih skupova, onda je

$$I_1 \supset I_2 \supset \dots$$

padajući niz ideala u $k[x_1, \dots, x_n]$. Kako je, po Hilbertovom teoremu u bazi, $k[x_1, \dots, x_n]$ Noetherin prsten, zaključujemo da se niz $(I_k)_k$ stabilizira, pa se i niz $(\mathcal{Z}(I_k))_k$ stabilizira.

Propozicija 2.12. *Neka je Y neprazan i zatvoren podskup Noetherinog topološkog prostora X. Tada se Y može napisati kao konačna unija zatvorenih ireducibilnih podskupova $Z_1, \dots, Z_m$ tako da je $Z_i \not\subset Z_j$ za $i \neq j$. Skup $\{Z_1, \dots, Z_m\}$ je jedinstveno određen s Y.*

Dokaz: Neka je U skup svih Y za koje ne vrijedi da ih je moguće zapisati kao konačnu uniju ireducibilnih zatvorenih skupova. Ako je U neprazan. onda zbog Noetherinosti U sadrži minimalni element, označimo ga s Y.

Ako je Y ireducibilan, dobili smo kontradikciju odmah. Ako je Y reducibilan, onda je $Y = Y' \cup Y''$ za neke njegove prave zatvorene neprazne podskupove. Međutim, onda se Y' i Y'' može, zbog minimalnosti Y, zapisati kao uniju konačno mnogo zatvorenih ireducibilnih skupova, pa se isto može napraviti i s Y, što je kontradikcija. Dakle, za svaki Y postoji zapis. Uvjet da nikoja dva člana iz zapisa nisu podskupovi jedan drugog možemo lako zadovoljiti tako što izbacimo sve elemente zapisa koji su podskup nekog drugog. Preostaje dokazati jedinstvenost.

Neka su

$$Z_1 \cup Z_2 \cup \dots \cup Z_r = W_1 \cup W_2 \cup \dots \cup W_m$$

dva zapisa od Y kao unije ireducibilnih zatvorenih skupova. Tada je svaki Z_i podskup nekog $W_{p(i)}$, te je svaki W_j podskup nekog $Z_{q(j)}$. Međutim, tada je $Z_i \subset Z_{q(p(i))}$ iz čega slijedi $i = q(p(i))$. Zaključujemo da su p i q međusobno inverzne bijekcije i vrijedi $Z_i = W_{p(i)}$, iz čega slijedi tvrdnja. □

Definicija 2.13. *Afina mnogostrukost* je zatvoren ireducibilan podskup od $\mathbb{A}^n$ za neki $n \geq 0$. *Kvazi-afina mnogostrukost* je neprazan skup koji je skupovna razlika dvije afine mnogostrukosti.

Napomena: Iz Propozicije 2.12 slijedi da se svaki zatvoren podskup od $\mathbb{A}^n$ može zapisati kao unija konačno mnogo afinih mnogostrukosti.

Definicija 2.14. Neka je Y afina mnogostrukost. Tada prsten

$$A(Y) := k[x_1, \ldots, x_n]/\mathcal{I}(Y)$$

zovemo koordinatni prsten od Y.

Sada ćemo definirati projektivnu ravninu i projektivne analogone ovih pojmova.

Definicija 2.15. Neka je $n \geq 0$ i k algebarski zatvoreno polje. Definirajmo na $k^{n+1} \setminus \{(0, \ldots, 0)\}$ relaciju ekvivalencije $\sim$ na sljedeći način:

$$P \sim Q : \Longleftrightarrow \quad \text{postoji } c \in k \text{ takav da je } P = c \cdot Q.$$

Definiramo projektivnu n-dimenzionalnu ravninu $\mathbb{P}_k^n$ kao skup svih klasa ekvivalencije po relaciji $\sim$.

U nastavku ćemo pisati $\mathbb{P}^n$ umjesto $\mathbb{P}_k^n$. Klasu ekvivalencije točke $(x_0, x_1, \ldots, x_n)$ označavat ćemo s $(x_0 : x_1 : \ldots : x_n)$. Ovom oznakom zapravo naglašavamo da su nam bitni samo omjeri između pojedinih koordinata da bismo odredili o kojoj se točki radi.

Za polinom $f \in k[x_0, \ldots, x_n]$ kažemo da je homogen ako je jednak k-linearnoj kombinaciji nekoliko monoma istog stupnja. Za ideal $I \subset k[x_0, \ldots, x_n]$ kažemo da je homogen ako je generiran homogenim polinomima.

Definicija 2.16. Ako je S skup homogenih polinoma u $k[x_0, \ldots, x_n]$, definiramo njegov zero set (prijevod!)

$$\mathcal{Z}(S) := \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ za svaki } F \in S\}.$$

Ako je I homogeni ideal od $k[x_0, \ldots, x_n]$, definiramo $\mathcal{Z}(I)$ kao zero set (prijevod!) skupa svih homogenih polinoma iz I.

Sada definiramo topologiju Zariskog na $\mathbb{P}^n$ kao topologiju čiji zatvoreni skupovi su skupovi oblika $\mathcal{Z}(I)$ za neki homogeni ideal $I \subset k[x_0, \ldots, x_n]$.

Promotrimo otvorene skupove $U_i \subset \mathbb{P}^n$, za $i \in \{0, \ldots, n\}$, definirane kao

$$U_i = \{(a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n \mid a_i \neq 0\}.$$

Vrijedi $U_0 \cup U_1 \cup \ldots \cup U_n = \mathbb{P}^n$. Nadalje, svaku točku $P \in U_i$ možemo zapisati kao

$$P = (a_0 : \ldots : a_{i-1} : 1 : a_{i+1} \ldots : a_n)$$

za jedinstveno određene $a_0, \ldots a_{i-1}, a_{i+1}, \ldots, a_n$.

Dakle, imamo bijekcije $\psi_i : \mathbb{A}^n \to U_i$ dane s

$$(b_1, \ldots, b_n) \mapsto (b_1 : \ldots : b_i : 1 : b_{i+1} : \ldots : b_n),$$

čiji inverzi ψ_i^{-1} su dani s

$$(a_0 : a_1 : \ldots : a_n) \mapsto \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right).$$

Promotrimo homogeni polinom $F \in k[x_0, \ldots, x_n]$ stupnja d. Tada definiramo njegovu dehomogenizaciju po i-toj komponenti kao polinom $f \in k[x_1, \ldots, x_n]$ definiran s

$$f(x_1, \ldots, x_n) = F(x_1, \ldots, x_i, 1, x_{i+1}, \ldots, x_n).$$

Primijetimo da je stupanj polinoma f manji ili jednak d. Obratno, ako imamo polinom $f \in k[x_1, \ldots, x_n]$ stupnja d, definiramo njegovu homogenizaciju po i-toj komponenti kao homogeni polinom $F \in k[x_0, x_1, \ldots, x_n]$ stupnja d definiran s

$$F(x_0, x_1, \ldots, x_n) = x_i^d f(x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i).$$

Analogno kao u afinom slučaju, imamo sljedeću definiciju.

Definicija 2.17. *Projektivna mnogostrukost* je zatvoren ireducibilan podskup od $\mathbb{P}^n$ za neki $n \geq 0$. *Kvazi-projektivna mnogostrukost* je podskup od $\mathbb{P}^n$ koji je skupovna razlika neke dvije projektivne mnogostrukosti.

Sada želimo promatrati funkcije na mnogostrukostima.

Definicija 2.18. Neka je $Y \subset \mathbb{A}^n$ kvazi-afina mnogostrukost. Za funkciju $f : Y \to k$ kažemo da je *regularna* u točki $P \in Y$ ako postoji otvoreni podskup $U \subset Y$ koji sadrži P i polinomi $g, h \in k[x_1, \ldots, x_n]$ takvi da je $h \neq 0$ na U i da je restrikcija od f na U jednaka restrikciji funkcije g/h na U. Kažemo da je f regularna ako je regularna u svakoj točki skupa Y. Ako je $U \subset Y$ otvoren, tada s $\mathcal{O}_Y(U)$ označavamo prsten svih regularnih funkcija na U. Umjesto $\mathcal{O}_Y(Y)$ pišemo samo $\mathcal{O}(Y)$.

Intuitivno, regularne funkcije su racionalne funkcije na 'većini' mnogostrukosti Y. Napomenimo da je svaki neprazan otvoren podskup neke mnogostrukosti Y gust (u topološkom smislu) u Y, pa intuitivno svaki otvoreni podskup čini velik udio skupa Y.

Definicija analognog pojma za projektivne mnogostrukosti se svodi na definiciju u afinom slučaju.

Definicija 2.19. Neka je $Y \subset \mathbb{P}^n$ kvazi-projektivna mnogostrukost. Neka je $P \in Y$ i neka je i indeks takav da je $P \subset U_i$ (drugim riječima, i-ta komponenta točke P nije 0). Tada kažemo da je $f : Y \to k$ regularna ako je, uz identifikaciju skupova U_i i $\mathbb{A}^n$, funkcija $f : Y \cap U_i \to k$ regularna u P. Kažemo da je f regularna ako je regularna u svakoj točki skupa Y. Ako je $U \subset Y$ otvoren, tada s $\mathcal{O}_Y(U)$ označavamo prsten svih regularnih funkcija na U. Umjesto $\mathcal{O}_Y(Y)$ pišemo samo $\mathcal{O}(Y)$.

Sada definiramo morfizme između mnogostrukosti.

Definicija 2.20. Neka su X i Y kvazi-afine ili kvazi-projektivne mnogostrukosti (dozvoljavamo da je jedno kvazi-afina, a drugo kvazi-projektivna mnogostrukost). Definiramo *morfizam* između X i

Y kao neprekidnu (u topologijama Zariskog) funkciju $\phi : X \to Y$ takvu da za svaki otvoren skup $U \subset Y$ i svaku regularnu funkciju $f \in \mathcal{O}_Y(U)$ vrijedi da je funkcija $f \circ \phi : \phi^{-1}(U) \to k$ element skupa $\mathcal{O}_X(\phi^{-1}(U))$.

Ova definicija je možda malo neintuitivna. Sljedeća karakterizacija pojašnjava što je zapravo morfizam za afine mnogostrukosti.

Propozicija 2.21. *Neka je $Y \subset \mathbb{A}^n$ kvazi-afina mnogostrukost. Ako je X kvazi-afina mnogostrukost i $\phi : X \to Y$ funkcija, onda je ϕ morfizam ako i samo ako su $\pi_i \circ \phi$ regularne funkcije na X, gdje su $\pi_i : \mathbb{A}^n \to k$ projekcije na i-tu koordinatu za $i \in \{1, \ldots, n\}$.*

Definicija 2.22. Neka je X Noetherin topološki prostor. Definiramo dimenziju od X, u oznaci $\dim X$, kao najveći nenegativan cijeli broj r takav da postoje zatvoreni ireducibilni podskupovi $Z_0, Z_1, \ldots, Z_r$ od X takvi da je Z_i pravi podskup od Z_{i+1} za svaki $i \in \{0, \ldots, r-1\}$.

Jasno, jedini nama relevantni X iz prethodne definicije su prostori $\mathbb{A}^n$ odnosno $\mathbb{P}^n$. Sada konačno možemo reći što je krivulja.

Definicija 2.23. Neka je $n \geq 1$. Krivulja u $\mathbb{A}^n$ ili $\mathbb{P}^n$ je mnogostrukost dimenzije 1.

Imamo paralelnu definiciju dimenzije za prstenove.

Definicija 2.24. Neka je R komutativni prsten. Tada definiramo *Krullovu dimenziju* od R, u oznaci $\mathrm{Kdim}(R)$, kao najveći nenegativan cijeli broj r takav da postoje prosti ideali $I_0, I_1, \ldots, I_r$ od R takvi da je I_i pravi podskup od I_{i+1} za svaki $i \in \{0, \ldots, r-1\}$, ako najveći takav r postoji. Ako najveći takav r ne postoji, definiramo $\mathrm{Kdim}(R) = \infty$.

Sada je cilj definirati singularitete mnogostrukosti. Prvo trebamo definiciju funkcijskog polja mnogostrukosti i lokalnog prstena u točki mnogostrukosti.

Može se pokazati da su sve regularne funkcije neprekidne. Nadalje, ako imamo kvazi-afinu ili kvazi-projektivnu mnogostrukost Y, te funkcije $f_1, f_2 : Y \to k$ koje su regularne i čije restrikcije na neki otvoren podskup U od Y su jednake, tada su f_1 i f_2 jednake na Y.

Promotrimo sada skup svih parova (U, f), gdje je $U \subset Y$ otvoren i neprazan, a $f \in \mathcal{O}_Y(U)$. Kažemo da su dva takva para (U_1, f_1) i (U_2, f_2) ekvivalentna ako su restrikcije od f_1 i f_2 na $U_1 \cap U_2$ jednake. Označimo sa $[U, f]$ klasu ekvivalencije od (U, f). Označimo skup svih klasa s $k(Y)$. Tada možemo definirati zbrajanje i množenje na $k(Y)$ na sljedeći način:

$$[U_1, f_1] + [U_2, f_2] := [U_1 \cap U_2, f_1 + f_2],$$
$$[U_1, f_1] \cdot [U_2, f_2] := [U_1 \cap U_2, f_1 f_2].$$

Jednostavno se provjeri dobra definiranost ovih operacija. Nadalje, $k(Y)$ snabdjeven ovim operacijama čini polje, s aditivnim neutralnim elementom $[Y, 0]$ i multiplikativnim neutralnim elementom $[Y, 1]$. Najmanje očita tvrdnja je da svaki element osim $[Y, 0]$ ima multiplikativni inverz. Naime,

skup nultočaka na U neke funkcije f definirane na Y regularne na U je zatvoren podskup od U. Označimo s N taj skup. Tada je $[U \setminus N, 1/f]$ dobro definiran element od $k(Y)$, i vrijedi

$$[U, f] \cdot [U \setminus N, 1/f] = [U \setminus N, 1] = [Y, 1].$$

Definicija 2.25. Gore opisano polje $k(Y)$ zovemo *funkcijsko polje* od Y.

Definicija 2.26. Neka je Y kvazi-afina ili kvazi-projektivna mnogostrukost i neka je $P \in Y$. Definiramo *lokalni prsten od Y u P*, u oznaci $\mathcal{O}_{Y,P}$, kao potprsten od $k(Y)$ koji se sastoji od klasa ekvivalencija $[U, f]$, gdje je U otvorena okolina od P i f regularna funkcija na U.

Sljedeća lema nam treba za definiciju tangecijalnog prostora.

Lema 2.27. *Neka je Y kvazi-afina ili kvazi-projektivna mnogostrukost i $P \in Y$. Neka je $\mathfrak{m}_P \subset \mathcal{O}_{Y,P}$ ideal svih elemenata $[U, f]$ takvih da je $f(P) = 0$. Tada je $\mathfrak{m}_P$ jedinstveni maksimalni ideal od $\mathcal{O}_{Y,P}$.*

Dokaz: Kao prvo, $\mathfrak{m}_P$ je jezgra epimorfizma $\varphi : \mathcal{O}_{Y,P} \to k$ definiranog sa $\varphi([U, f]) = f(P)$, pa je $\mathcal{O}_{Y,P}/\mathfrak{m}_P$ polje, što dokazuje da je $\mathfrak{m}_P$ maksimalan.

Nadalje, elementi $[U, f]$ iz $\mathcal{O}_{Y,P}$ za koje je $f(P) \neq 0$ su invertibilni u $\mathcal{O}_{Y,P}$, pa $\mathfrak{m}_P$ sadrži sve neinvertibilne elemente od $\mathcal{O}_{Y,P}$, pa onda i sve netrivijalne ideale. Slijedi da je to jedinstveni maksimalni ideal. □

Sada možemo definirati tangencijalni prostor mnogostrukosti u točki.

Definicija 2.28. Neka je X afina ili projektivna mnogostrukost, te neka je $P \in X$. Tada definiramo tangencijalni prostor od X u točki P, u oznaci $T_{X,P}$, kao vektorski prostor nad k dualan vektorskom prostoru $\mathfrak{m}_P/\mathfrak{m}_P^2$, gdje je $\mathfrak{m}_P$ jedinstveni maksimalni ideal od $\mathcal{O}_{Y,P}$.

Primjer 2.29. Promotrimo tangencijalni prostor od $\mathbb{A}^n$ u točki $P = (a_1, \ldots, a_n)$. Lokalni prsten od $\mathbb{A}^n$ u P je izomorfan sa skupom svih racionalnih funkcija čiji nazivnici nemaju nultočku P. Maksimalni ideal $\mathfrak{m}$ tog prstena je $(x_1 - a_1, \ldots, x_n - a_n)$. Tada je $\mathfrak{m}/\mathfrak{m}^2$, kao vektorski prostor, generiran elementima $x_1 - a_1 \pmod{\mathfrak{m}^2}, \ldots, x_n - a_n \pmod{\mathfrak{m}^2}$, odnosno ima dimenziju n. Označavat ćemo s $\{\mathfrak{e}_1, \ldots, \mathfrak{e}_n\}$ bazu dualnu toj bazi, koja je onda po definiciji baza tangencijalnog prostora.

Sljedeća propozicija objašnjava poveznicu s parcijalnim derivacijama.

Propozicija 2.30. *Neka je $X \subset \mathbb{A}^n$ afina mnogostrukost definirana idealom $\mathcal{I}(X) = (f_1, \ldots, f_r)$. Neka je $i : X \to \mathbb{A}^n$ ulaganje. Neka je $P \in X$, i neka je $\{f_1, \ldots, f_n\}$ baza za $T_{\mathbb{A}^n,P}$. Tada je $T_{X,P}$ izomorfan s potprostorom od $T_{\mathbb{A}^n,P}$ koji je zadan sljedećim jednadžbama:*

$$\frac{\partial f_i(P)}{\partial e_1} \cdot \mathfrak{e}_1 + \ldots + \frac{\partial f_i(P)}{\partial e_n} \cdot \mathfrak{e}_n = 0,$$

za $i \in \{1, \ldots, r\}$.

Napomena: Dokaz se ugrubo temelji na činjenici da je svaki od polinoma f_i kongruentan s

$$\frac{\partial f_i(P)}{\partial e_1} \cdot (x - a_1) + \ldots + \frac{\partial f_i(P)}{\partial e_n} \cdot (x - a_n)$$

modulo $\mathfrak{m}_P^2$, što se vidi iz Taylorovog zapisa polinoma oko P. Ovdje je m_P maksimalni ideal $(x_1 - a_1, \ldots, x_n - a_n)$ u $k[x_1, \ldots, x_n]$.
Sljedeća propozicija govori o dimenziji tangencijalnog prostora mnogostrukosti.

Propozicija 2.31. *Neka je $X \subset \mathbb{A}^n$ afina ili projektivna mnogostrukost. Tada je dimenzija prostora $T_{X,P}$ veća ili jednaka dimenziji od X.*

Sada konačno možemo definirati singularitete.

Definicija 2.32. Neka je X afina ili projektivna mnogostrukost. Točka $P \in X$ je *regularna* ako je $\dim_k(T_{X,P}) = \dim X$. Ako je $\dim(T_{X,P}) > \dim X$, onda je P *singularna*. Mnogostrukost X je glatka ili regularna ili nesingularna ako su joj sve točke regularne.

Napomena: Neka je X afina mnogostrukost te neka je $\mathcal{I}(X) = (f_1, \ldots, f_r)$. Ako je $\dim X = n - s$, onda je po Propoziciji 2.30 točka $P \in X$ singularna ako i samo ako matrica

$$\begin{pmatrix} \frac{\partial f_1(P)}{\partial e_1} & \frac{\partial f_1(P)}{\partial e_2} & \cdots & \frac{\partial f_1(P)}{\partial e_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_r(P)}{\partial e_1} & \frac{\partial f_r(P)}{\partial e_2} & \cdots & \frac{\partial f_r(P)}{\partial e_n} \end{pmatrix}$$

ima rang manji od s.

Nadalje, kako matrica ima rang manji od s ako i samo ako sve $s \times s$ minore imaju determinantu 0, pronašli smo skup polinomnih jednadžbi koje singularna točka zadovoljava, pa zaključujemo da je skup singularnih točaka od X zatvoren. Nadalje, može se pokazati da taj skup nikad nije jednak X, odnosno uvijek je pravi zatvoreni podskup od X.

2.4 Blowing-up

U prethodnom odjeljku smo definirali afine i projektivne mnogostrukosti te singularitete. Sada želimo objasniti što to znači razriješiti singularitet, i opisujemo metodu blowing-up, koju ćemo koristiti za razrješenje singulariteta.

Definicija 2.33. *Blowing-up* od $\mathbb{A}^n$ u ishodištu $O = (0, \ldots, 0)$ je zatvorena podmnogostrukost $B \subset \mathbb{A}^n \times \mathbb{P}^{n-1}$ dana s

$$B = \{((a_1, \ldots, a_n), (b_1 : \ldots : b_n)) \in \mathbb{A}^n \times \mathbb{P}^{n-1} \mid a_i b_j = a_j b_i \text{ za sve } i, j\}.$$

Ako interpretiramo $\mathbb{P}^{n-1}$ kao skup pravaca kroz ishodište u $\mathbb{A}^n$, tada je B skup svih parova (P, L), gdje je P točka iz $\mathbb{A}^n$, a $L \in \mathbb{P}^{n-1}$ pravac kroz P.

Označimo s π projekciju sa B na $\mathbb{A}^n$, odnosno $\pi(P, L) := P$. Tada je $\pi^{-1}\{O\} = \{O\} \times \mathbb{P}^{n-1}$.

Definicija 2.34. Neka je $X \subset \mathbb{A}^n$ zatvorena podmnogostrukost takva da je $O \in X$, i neka je B blowing-up od $\mathbb{A}^n$ u O. Tada je blowing-up od X u O podmnogostrukost $\tilde{X} \subset B$ definirana kao zatvarač skupa $\pi^{-1}(X \setminus \{O\})$ u B.

Napomena: Primijetimo da je π izomorfizam između $\pi^{-1}(X \setminus \{O\})$ i $X \setminus \{O\}$. Drugim riječima, blowing-up $\tilde{X}$ je dobiven iz X samo nekim promjenama u ishodištu.
Razlog zašto je blowing-up bitan je taj što blowing-up neke mnogostrukosti u pravilu ima manje singularita nego početna mnogostrukost. Promotrimo jedan primjer.

Primjer 2.35. Promotrimo krivulju $D \subset \mathbb{A}^2$ definiranu jednadžbom

$$y^2 = x^3 + x^2.$$

Krivulja ima singularnu točku $(0, 0)$. Izračunajmo blowing-up $\tilde{D}$ od D. Po definiciji, to je zatvarač skupa

$$S := \{((x, y), (s : t)) \in \mathbb{A}^2 \cdot \mathbb{P}^1 \mid y^2 = x^3 + x^2 \ \wedge \ xt = ys \ \wedge (x, y) \neq (0, 0)\}.$$

Zapravo ćemo odrediti zatvarače presjeka od S sa afinim kartama $\{s \neq 0\}$ i $\{t \neq 0\}$. Tada će zatvarač od S biti dobiven ljepljenjem tih dvaju presjeka.

Promotrimo prvo presjek sa $\{s \neq 0\}$. Tada možemo staviti $s = 1$, i zapravo određujemo zatvarač skupa

$$S_1 := \{(x, y, t) \in \mathbb{A}^3 \mid y^2 = x^3 + x^2 \ \wedge \ xt = y \ \wedge \ x \neq 0\}.$$

Ako uvažimo $y = xt$, imamo da za točke iz S_1 vrijedi $x^2t^2 = x^3 + x^2$ i $x \neq 0$, odnosno $t^2 = x + 1$. Zatvarač od S_1 dobije se tako što se makne uvjet $x = 0$, odnosno $\overline{S_1} = \{(x, y, t) \in \mathbb{A}^3 \mid t^2 = x + 1 \ \wedge \ y = tx\}$. Primijetimo da je $\overline{S_1}$ nesingularna krivulja.

Sada, promotrimo presjek sa $\{t \neq 0\}$. Tada možemo staviti $t = 1$, i zapravo određujemo zatvarač skupa

$$S_2 := \{(x, y, s) \in \mathbb{A}^3 \mid ys = x \ \wedge \ y \neq 0 \ \wedge \ y^2 = x^3 + x^2\}.$$

Ako uvažimo $x = ys$, dobijemo $y^2 = y^2(ys^3 + s^2)$ i $y \neq 0$, odnosno $s^2(ys + 1) = 1$ i $y \neq 0$. Ponovno, da bi dobili zatvarač samo maknemo uvjet $y \neq 0$, i imamo

$$\overline{S_2} = \{(x, y, s) \in \mathbb{A}^3 \mid x = ys \ \wedge \ s^2(ys + 1) = 1\}.$$

Vidimo da je i ovo nesingularna krivulja, pa je i $\overline{S}$ dobiven ljepljenjem $\overline{S_1}$ i $\overline{S_2}$ također nesingularna krivulja.

U prethodnom primjeru vidjeli smo kako blowing-up možemo koristiti da bismo razriješili singularitete. Možemo i precizno definirati pojam razrješenja singulariteta.

Definicija 2.36. Neka je X mnogostrukost čiji skup singularnih točaka je S. Tada je *razrješenje singulariteta* od X mnogostrukost X' zajedno sa surjektivnim morfizmom $\pi : X' \to X$ tako da je X' nesingularna i π je izomorfizam nad $X \setminus S$.

Još primjera blowing-upa može se pronaći u [11].

2.5 Kratko o genusu

Za račun biasa potreban nam je pojam genusa krivulje. Postoji nekoliko različitih definicija genusa, i niti jedna od njih nije jednostavna. Mi ćemo ga definirati samo za ravninske krivulje, preko stupanj-genus formule. To nije standardan pristup, ali nama je najpogodniji. Alternativni pristup koji se bazira na Riemann-Rochovom teoremu može se naći u [12] u poglavlju 6.3. Više o Riemann-Rochovom teoremu može se naći u [15]. U poglavlju 1 od [9] dana je definicija genusa preko topološke klasifikacije ploha.

Definicija 2.37. Neka je k algebarski zatvoreno polje. Ravninska krivulja u $\mathbb{A}^2$ je mnogostrukost u $\mathbb{A}^2$ zadana kao skup nultočaka jednog nenul polinoma $f(x, y) \in k[x, y]$. Ravninska krivulja u $\mathbb{P}^2$ je mnogostrukost u $\mathbb{P}^2$ zadana kao skup nultočaka jednog nenul homogenog polinoma $F(x, y, z) \in k[x, y, z]$.

Podsjetimo se, singularna točka ravninske krivulje zadane sa polinomom f je točka na toj krivulji u kojoj obje parcijalne derivacije od f isčezavaju. Međutim, za definiciju genusa trebamo biti nešto precizniji, i definirati kratnost singulariteta. Definicija je preuzeta iz [2].

Definicija 2.38. Neka je $C \subset \mathbb{A}^2$ ravninska krivulja zadana polinomom $f(x, y) \in k[x, y]$. Tada definiramo kratnost točke $P \in C$, u oznaci $\nu_P(C)$ kao najmanji $r \geq 1$ takav da neka r-ta parcijalna derivacija od $f(x, y)$ u točki P nije jednaka 0.

Regularne točke na krivulji onda imaju kratnost 1, a singularne točke kratnost veću od 1. Definicija je analogna za $\mathbb{P}^2$ umjesto $\mathbb{A}^2$, samo što je f iz iskaza tada homogeni polinom u tri varijable.

Definicija 2.39 (Stupanj-genus formula)**.** Neka je $C \subset \mathbb{P}^2$ ravninska krivulja zadana ireducibilnim homogenim polinomom iz $k[x, y, z]$ stupnja d. Genus g krivulje C definiramo sa

$$g := \frac{(d-1)(d-2)}{2} - \sum_{P \in C} \frac{\nu_P(C) \cdot (\nu_P(C) - 1)}{2}.$$

Važno svojstvo genusa je da je invarijantan na biracionalna preslikavanja. Da bismo to precizinije iskazali trebaju nam neke definicije.

Definicija 2.40. Neka su X i Y afine ili algebarske mnogostrukosti. Definiramo *racionalno preslikavanje* iz X u Y kao morfizam iz nekog otvorenog podskupa od X u Y.

Napomena: Racionalno preslikavanje je, prema alternativnoj karakterizaciji morfizma (2.21), preslikavanje u kojem se koordinatne funkcije preslikavanja mogu zapisati kao racionalne funkcije. Važno je napomenuti da racionalno preslikavanje nije funkcija, nego može biti nedefinirano u nekim točkama iz X.

Definicija 2.41. Neka su f i g racionalna preslikavanja redom iz X u Y te iz Y u X. Kažemo da je g inverzno racionalno preslikavanje od f ako je $(g \circ f)(x) = x$ za sve $x \in X$ za koje je kompozicija dobro definirana.

Definicija 2.42. Neka su X i Y afine ili projektivne mnogostrukosti. Definiramo *biracionalno preslikavanje* između X i Y kao racionalno preslikavanje iz X u Y za koje postoji inverzno racionalno preslikavanje iz Y u X. Ako između X i Y postoji biracionalno preslikavanje, kažemo da su X i Y biracionalno ekvivalentne.

Vrijedi sljedeći, već spomenuti teorem.

Teorem 2.43 (Riemann)**.** *Ako su dvije afine ili projektivne mnogostrukosti biracionalno ekvivalentne, onda imaju isti genus.*

Nama važna biracionalna ekvivalencija je ona između mnogostrukosti i njenog blowing-upa. Naime, projekcija π iz Definicije definicija 2.34 je biracionalno preslikavanje iz mnogostrukosti u njen blowing-up.

Također, razrješenje singulariteta bilo koje mnogostrukosti X je biracionalno ekvivalentno s X, jer je π iz Definicije definicija 2.36 biracionalno preslikavanje.

2.6 Sato-Tateova slutnja

Ovdje je dan jako kratak uvod u problematiku Sato-Tateovih slutnji. Za detaljniju ekspoziciju upućujemo na [6] ili [13]. U računanju drugog momenta familije $\mathcal{F}_k$, doći ćemo do situacije gdje nam je bitan prosječan broj točaka na nekoj glatkoj projektivnoj krivulji genusa 1(takve krivulje, ako sadrže barem jednu točku nad poljem nad kojim su definirane, zovemo *eliptičke krivulje*).

Konkretno, u slučaju kad je $\mu = 0$ te $\mu_{2,3} \neq 0$, dokazat ćemo da za sve osim konačno mnogo prostih brojeva p vrijedi sljedeća formula:

$$\tilde{M}_{2,p}(\mathcal{F}_k) = p(\#\overline{\Delta}(\mathbb{F}_p) + p - \#S(\mathbb{F}_p) - 2).$$

Ovdje je $\overline{\Delta}$ eliptička krivulja, te nam je od interesa koliko prosječno točaka nad $\mathbb{F}_p$ se nalazi na toj krivulji. Vrijedi sljedeći poznati rezultat.

Teorem 2.44 (Hasse)**.** *Neka je p prost broj i D eliptička krivulja definirana nad $\mathbb{F}_p$. Tada vrijedi*

$$|p + 1 - \#D(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

Sljedeće pitanje koje se prirodno postavlja je kako je distribuirana greška.Uvedimo oznaku $A_p = p + 1 - \#\overline{\Delta}(\mathbb{F}_p)$. Vrijedi nejednakost

$$|A_p| \leq 2\sqrt{p},$$

pa se postavlja pitanje kako su brojevi $\dfrac{A_p}{\sqrt{p}}$ distribuirani u $[-2, 2]$.

Sato-Tateova slutnja govori upravo o tome. Prije iskaza slutnje treba nam jedna analitička definicija.

Definicija 2.45. Za niz realnih brojeva $(x_n)_n$ kažemo da je *ekvidistribuiran* u odnosu na mjeru μ

ako za svaku neprekidnu funkciju $f : \mathbb{R} \to \mathbb{R}$ vrijedi

$$\int f d\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i).$$

Teorem 2.46 (Sato-Tateova slutnja)**.** *Ako eliptička krivulja D nema kompleksno množenje, tada je njoj pridružen niz* $\left(\frac{A_p}{\sqrt{p}}\right)_p$ *ekvidistribuiran u odnosu na mjeru*

$$\mu := 1_{[-2,2]}(z) \cdot \frac{1}{2\pi} \sqrt{4 - z^2} dz,$$

gdje je dz Lebesgueova mjera.

Postoje i generalizacije ove slutnje za krivulje koje imaju genus veći od 1, ali u slučajevima kojima ćemo se baviti se neće spominjati takve krivulje u formuli za drugi moment, pa nam to nije relevantno. Sato-Tateova slutnja je dokazana u iskazanom obliku. Dakle, iako pišemo 'slutnja', zapravo se radi o teoremu.

Vratimo se na formulu za drugi moment. Tada je u kanonskom rastavu drugog momenta upravo pA_p pribrojnik reda $p^{3/2}$. Želimo dokazati da je prosjek tih pribrojnika po svim prostim brojevima jednak 0, odnosno da vrijedi

$$\lim_{n\to\infty} \frac{1}{\pi(n)} \sum_{p\leq n} \frac{A_p}{\sqrt{p}} = 0.$$

Međutim, to je sada trivijalna posljedica simetričnosti oko ishodišta mjere μ iz Sato-Tateove slutnje, jer je integral identitete u odnosu na tu mjeru jednak 0.

Napomena: Ako krivulja ima kompleksno množenje, tada je mjera u odnosu na koju je niz $(A_p)_p$ ekvidistribuiran drugačija, ali i dalje vrijedi da je ta mjera simetrična oko ishodišta, pa analogni argument da je prosjek jednak 0 prolazi. Točnije, mjera u odnosu na koju je niz ekvidistribuiran je

$$1_{[-2,2]}(z) \cdot \frac{1}{2\pi} \left(\frac{dz}{\sqrt{4 - z^2}} + \delta_0 \right),$$

gdje je δ_0 Diracova delta mjera oko točke 0. Napomenimo da je u ovom slučaju dokaz dosta jednostavniji.

3 Analiza krivulje $\tilde{\Delta}$

U ovom poglavlju ćemo analizirati singularitete krivulje $\tilde{\Delta}$ te njenog projektivnog zatvorenja. Također, provest ćemo blowup za razrješenje singulariteta, pa ćemo u formuli za drugi moment imati samo pribrojnike koji dolaze od broja točaka na glatkim projektivnim mnogostrukostima. Za računanje prosjeka tih pribrojnika onda možemo iskoristiti Sato-Tateovu slutnju.

3.1 Određivanje singulariteta

Lema 3.1. *Neka je $p > 3$ prost broj. Točka $(x_1, x_2) \in \tilde{\Delta}(\overline{\mathbb{F}_p})$ je singularna točka od $\tilde{\Delta}$ ako i samo ako je $x_1 = x_2$ te je x_1 dvostruka nultočka redukcije polinoma S modulo p.*

Dokaz: Odredimo prvo parcijalne derivacije od $\tilde{\Delta}$. Vrijedi:

$$\frac{\partial\tilde{\Delta}}{\partial e_1}(x_1, x_2) = \frac{Q(x_2)(P(x_1) + P'(x_1)(x_2 - x_1)) - P(x_2)(Q(x_1) + Q'(x_1)(x_2 - x_1))}{(x_2 - x_1)^2} \tag{3}$$

$$= \frac{1}{2}(P(x_2)Q''(x_1) - Q(x_2)P''(x_1)) + \frac{(x_2 - x_1)}{6}(P(x_2)Q'''(x_1) - Q(x_2)P'''(x_1)), \tag{4}$$

te analogno za $\dfrac{\partial\tilde{\Delta}}{\partial e_2}(x_1, x_2)$.

Analizirajmo prvo singularitete oblika (x_1, x_2) za koje je $x_1 \neq x_2$. Tada je, zbog (3) i zbog činjenice da je $(x_1, x_2) \in \tilde{\Delta}(\overline{\mathbb{F}_p})$, točka (x_1, x_2) singularitet ako i samo ako vrijede sljedeće tri jednakosti:

$$P(x_1)Q(x_2) = Q(x_1)P(x_2),$$
$$P(x_1)Q'(x_2) = Q(x_1)P'(x_2),$$
$$P'(x_1)Q(x_2) = Q'(x_1)P(x_2).$$

Prva jednakost je zapravo $\Delta(x_1, x_2) = 0$, i ona slijedi iz činjenice da je $\tilde{\Delta}(x_1, x_2) = 0$, odnosno da se promatrana točka nalazi na krivulji. Posljednje dvije jednakosti slijede iz eq. (1) te činjenice da je $x_1 \neq x_2$ i $\Delta(x_1, x_2) = 0$.

Promotrimo matricu

$$\begin{pmatrix} P(x_1) & P'(x_1) & P(x_2) & P'(x_2) \\ Q(x_1) & Q'(x_1) & Q(x_2) & Q'(x_2) \end{pmatrix}.$$

Tada iz gornjih jednakosti slijedi da je prvi stupac proporcionalan sa trećim i četvrtim te je treći stupac proporcionalan sa prvim i drugim. Kako su prvi i treći stupac oba različita od $(0, 0)$ zbog pretpostavke da P i Q nemaju zajedničkih nultočaka, zaključujemo da je svaki stupac proporcionalan s prvim. Dakle, rang matrice je jednak 1, pa postoji $\alpha \in \mathbb{F}_p$ takav da je

$$P(x_1) - \alpha Q(x_1) = P'(x_1) - \alpha Q'(x_1) = P(x_2) - \alpha Q(x_2) = P'(x_2) - \alpha Q'(x_2) = 0.$$

Međutim, tada polinom $P - \alpha Q$, koji je stupnja najviše 3, ima dvije dvostruke nultočke, pa mora biti nul polinom. Međutim, tada su P i Q isti do na množenje konstantom, što je kontradikcija jer

smo pretpostavili da P i Q nisu proporcionalni. Dakle, točka (x_1, x_2) nije singularitet kad god je $x_1 \neq x_2$.

Promotrimo sada slučaj kada je $(x_1, x_2) = (x, x)$ za neki $x \in \overline{\mathbb{F}_p}$. Ako uvrstimo (x, x) umjesto (x_1, x_2) u (4), dobijemo $\dfrac{\partial\tilde{\Delta}}{\partial e_1}(x, x) = \dfrac{1}{2}(P(x)Q''(x) - Q(x)P''(x))$. S druge strane, kako je $S(x) = P(x)Q'(x) - Q(x)P'(x)$, lako se vidi da je

$$S'(x) = P(x)Q''(x) - Q(x)P''(x),$$

pa vrijedi $S'(x) = 2 \cdot \dfrac{\partial\tilde{\Delta}}{\partial e_1}(x, x) = -2 \cdot \dfrac{\partial\tilde{\Delta}}{\partial e_2}(x, x)$. Iz toga slijedi da je x dvostruka nultočka od S ako i samo ako je (x, x) singularna točka od $\tilde{\Delta}$. □

Definiramo projektivnu krivulju $\overline{\Delta} \subset \mathbb{P}^2(\mathbb{F}_p)$ kao projektivno zatvorenje krivulje $\tilde{\Delta}$, odnosno kao skup točaka $(x_1 : x_2 : z) \in \mathbb{P}^2(\mathbb{F}_p)$ za koje je

$$\overline{\Delta}(x_1, x_2, z) := z^{\deg(\tilde{\Delta})}\tilde{\Delta}(x_1/z, x_2/z) = 0.$$

Sa $\#\overline{\Delta}(\mathbb{F}_p)$ označavati ćemo broj točaka $(x_1 : x_2 : z) \in \mathbb{P}^2(\mathbb{F}_p)$ koje se nalaze na $\overline{\Delta}$.
Pomoću sljedeće jednostavne leme ćemo se s analize krivulje $\tilde{\Delta}$ prebaciti na analizu krivulje $\overline{\Delta}$.

Lema 3.2. *Neka je p prost broj. Ako je $\mu_{2,3} \neq 0$ u $\mathbb{F}_p$, tada vrijedi $\#\overline{\Delta}(\mathbb{F}_p) = \#\tilde{\Delta}(\mathbb{F}_p) + 2$. Ako je $\mu_{2,3} = 0$ i $\mu \neq 0$ u $\mathbb{F}_p$, onda vrijedi $\#\overline{\Delta}(\mathbb{F}_p) = \#\tilde{\Delta}(\mathbb{F}_p) + 3$.*

Dokaz: Razlika između broja točaka je jednaka broju točaka na $\overline{\Delta}$ oblika $(x_1 : x_2 : 0)$. Sada koristimo eksplicitnu formulu za $\tilde{\Delta}$. Vrijedi

$$\tilde{\Delta}(x_1, x_2) = \mu_{2,3}x_1^2x_2^2 + \mu_{1,3}(x_1x_2^2 + x_1^2x_2) + \mu_{0,3}(x_1^2 + x_1x_2 + x_2^2) + \mu_{1,2}x_1x_2 + \mu_{0,2}(x_1 + x_2) + \mu_{0,1}.$$

Ako je $\mu_{2,3} = 0$ i $\mu \neq 0$, onda je $\mu_{1,3} \neq 0$, pa je $\deg\tilde{\Delta} = 3$. Homogenizacijom i uvrštavanjem $z = 0$ dobivamo

$$\mu_{1,3}(x_1^2x_2 + x_2^2x_1) = 0.$$

Za $x_1 = 0$, imamo točku $(0 : 1 : 0)$, za $x_2 = 0$ točku $(1 : 0 : 0)$, a za $x_1 = 1, x_2 \neq 0$ točku $(1 : -1 : 0)$, što su ukupno tri točke, i sve su definirane nad $\mathbb{F}_p$.

Ako je $\mu_{2,3} \neq 0$, onda je $\deg\tilde{\Delta} = 4$, pa homogenizacijom i uvrštavanjem $z = 0$ dobivamo $\mu_{2,3}x_1^2x_2^2$. Jedine točke koje zadovoljavaju ovaj uvjet su $(1 : 0 : 0)$ i $(0 : 1 : 0)$. □

Primijetimo da u uvjetima prethodne leme pretpostavljamo da nisu istovremeno $\mu_{2,3}$ i μ jednaki nuli. Razlog za to je što je slučaj u kojem su oba ta parametra jednaka 0 posebno jednostavan i elementaran, pa analiza singulariteta nije potrebna.

Lema 3.3. *Pretpostavimo da je $p \neq 2$, te da vrijedi $\mu_{2,3} \neq 0$ ili $\mu \neq 0$. Skup singularnih točaka od $\overline{\Delta}$ nad $\overline{\mathbb{F}_p}$ jednak je uniji skupa točaka oblika $(x_1 : x_2 : 1)$, gdje je (x_1, x_2) singularna točka od $\tilde{\Delta}$ i*

skupa T, definiranog na sljedeći način: ako je $\mu_{2,3} \neq 0$, onda je $T = \{(1:0:0),(0:1:0)\}$, a ako je je $\mu_{2,3} = 0$ i $\mu \neq 0$, onda je $T = \emptyset$.

Dokaz: Očito je da su točke oblika $(x_1 : x_2 : 1)$ singularne za projektivno zatvorenje neke afine krivulje ako i samo ako je (x_1, x_2) singularna točka te afine krivulje. Preostaje odrediti singularitete oblika $(x_1 : x_2 : 0)$.

Za to koristimo eksplicitne formule za $\overline{\Delta}$ i njene parcijalne derivacije. Označimo s D_1, D_2 i D_3 parcijalne derivacije po svakoj od tri varijable redom. Promotrimo prvo slučaj $\mu_{2,3} \neq 0$. Imamo

$$\begin{aligned}
D_1 &= 2\mu_{2,3}x_1x_2^2 + \mu_{1,3}x_2^2z + 2\mu_{1,3}x_1x_2z + 2\mu_{0,3}x_1z^2 + \mu_{0,3}x_2z^2 + \mu_{1,2}x_2z^2 + \mu_{0,2}z^3,\\
D_2 &= 2\mu_{2,3}x_2x_1^2 + \mu_{1,3}x_1^2z + 2\mu_{1,3}x_2x_1z + 2\mu_{0,3}x_2z^2 + \mu_{0,3}x_1z^2 + \mu_{1,2}x_1z^2 + \mu_{0,2}z^3,\\
D_3 &= \mu_{1,3}x_1x_2(x_1 + x_2) + 2\mu_{0,3}(x_1^2 + x_1x_2 + x_2^2)z + 2\mu_{1,2}x_1x_2z + 3\mu_{0,2}(x_1 + x_2)z^2 + 4\mu_{0,1}z^3.
\end{aligned}$$

Sada uvrstimo $z = 0$ u sve tri jednakosti i izjednačimo ih s 0. Dobivamo da je nužno i dovoljno da vrijedi $x_1x_2 = 0$, odnosno točke $(0 : 1 : 0)$ i $(1 : 0 : 0)$ su singulariteti.

Ako je pak $\mu_{2,3} = 0$ te $\mu \neq 0$, imamo sljedeće formule:

$$\begin{aligned}
D_1 &= \mu_{1,3}x_2^2 + 2\mu_{1,3}x_1x_2 + 2\mu_{0,3}x_1z + \mu_{0,3}x_2z + \mu_{1,2}x_2z + \mu_{0,2}z^2,\\
D_2 &= \mu_{1,3}x_1^2 + 2\mu_{1,3}x_2x_1 + 2\mu_{0,3}x_2z + \mu_{0,3}x_1z + \mu_{1,2}x_1z + \mu_{0,2}z^2,\\
D_3 &= \mu_{0,3}(x_1^2 + x_1x_2 + x_2^2) + \mu_{1,2}x_1x_2 + 2\mu_{0,2}(x_1 + x_2)z + 3\mu_{0,1}z^2.
\end{aligned}$$

Međutim, sada samo trebamo provjeriti za tri točke oblika $(x_1 : x_2 : 0)$ jesu li singulariteti. To su točke $(1 : 0 : 0)$, $(0 : 1 : 0)$ i $(1 : -1 : 0)$. Uvrštavanjem prve točke u izraz za D_1, druge točke u izraz za D_2 i treće točke u izraz za D_1 dobivamo da nijedna od točaka nije singularna za $\overline{\Delta}$. □

Preostaje okarakterizirati singularitete od $\tilde{\Delta}$.

Lema 3.4. *Pretpostavimo da vrijedi $\mu_{2,3} \neq 0$ ili $\mu \neq 0$ u $\mathbb{F}_p$. Tada vrijedi da $\tilde{\Delta}$ ima barem jednu singularnu točku nad $\overline{\mathbb{F}_p}$ ako i samo ako vrijedi*

$$s = \mu_{1,2}^3 + 27\mu_{0,1}\mu_{1,3}^2 + 27\left(\mu_{0,2}^2 - \mu_{0,1}\mu_{1,2}\right)\mu_{2,3} - 9\mu_{0,3}\left(\mu_{1,2}^2 + 9\mu_{0,1}\mu_{2,3}\right) = 0.$$

Dokaz: Točke oblika (x, x) su, prema Lemi 3.1, singularne ako i samo ako je x nultočka polinoma $S(t) = P(t)Q'(t) - Q(t)P'(t)$ i polinoma $S'(t) = P(t)Q''(t) - Q(t)P''(t)$. Promotrimo matricu

$$\begin{pmatrix} P(x) & P'(x) & P''(x) \\ Q(x) & Q'(x) & Q''(x) \end{pmatrix}.$$

Primijetimo da prvi stupac nikad nije jednak $(0, 0)$. Također, treći stupac nije jednak $(0, 0)$, jer su P'' i Q'' linearni polinomi koji imaju zajedničku nultočku ako i samo ako je $\mu_{2,3} = 0$ (ova

tvrdnja slijedi direktno iz raspisa koeficijenata). Nadalje, (x, x) je singularna točka ako i samo ako su prvi i drugi te prvi i treći stupac proporcionalni, što je ekvivalentno s time da su prvi i treći te drugi i treći stupac proporcionalni. To vrijedi ako i samo ako polinomi $P(x)Q''(x) - Q(x)P''(x)$ i $P'(x)Q''(x) - Q'(x)P''(x)$ imaju zajedničku nultočku. Ti polinomi imaju zajedničku nultočku ako i samo ako je njihova rezultanta jednaka 0. Ako pretpostavimo $\mu_{2,3} \neq 0$ i iskoristimo eksplicitne formule za te polinome, uz korištenje Mathematice može se izračunati da je njihova rezultanta jednaka $\mu_{2,3}^2 \cdot s$.

Ako je $s = 0$, onda postoji još jedan singularitet jer je tada rezultanta jednaka 0. Ako je $s \neq 0$, onda nema singulariteta. Dakle, lema je dokazana uz pretpostavku $\mu_{2,3} \neq 0$.

Pretpostavimo sada da je $\mu_{2,3} = 0$ te $\mu \neq 0$. Primijetimo da ako zamijenimo polinom $Q(x)$ sa $b_3P(x) - a_3Q(x) = \mu_{2,3}x^2 + \mu_{1,3}x + \mu_{0,3}$ dobivamo da se S i $\tilde{\Delta}$ ne mijenjaju osim množenja konstantom. Ako onda uvažimo $\mu_{2,3} = 0$ dobivamo sljedeće nužne uvjete za to da je točka (x, x) singularitet:

$$\begin{aligned} \mu_{1,3}P(x) &= (\mu_{1,3}x + \mu_{0,3})P'(x), \\ 0 &= (\mu_{1,3}x + \mu_{0,3})P''(x). \end{aligned}$$

Ako bi bilo $P\left(\frac{-\mu_{0,3}}{\mu_{1,3}}\right) = 0$, dobili bismo i $Q\left(\frac{-\mu_{0,3}}{\mu_{1,3}}\right) = 0$, ali P i Q nemaju zajedničkih nultočaka. Dakle, mora vrijediti $P''(x) = 0$, a jedina nultočka od P'' je $\frac{-a_2}{3a_3} = \frac{-b_2}{3b_3} = \frac{-\mu_{1,2}}{3\mu_{1,3}}$, pa je to jedini kandidat za singularnu točku. To će biti singularna točka ako i samo ako je nultočka od S i od S'. Kako znamo da je to nultočka od S', dovoljno je odrediti kad je to također nultočka od S. Direktnim uvrštavanjem dobivamo da je to ekvivalentno sa $s = 0$. □

Sljedeću lemu ćemo koristiti samo na jednom mjestu, ali sama po sebi je korisna za razumijevanje ponašanja polinoma S.

Lema 3.5. *Polinom S nema trostrukih nultočaka.*

Dokaz: Pretpostavimo da je w trostruka nultočka od S. Tada je

$$P(w)Q^{(j)}(w) - Q(w)P^{(j)}(w) = 0$$

za $j \in \{1, 2, 3\}$, gdje $f^{(j)}$ označava j-tu derivaciju od f. Tada su vektori

$$(P(w), P'(w), P''(w), P'''(w)) \text{ i } (Q(w), Q'(w), Q''(w), Q'''(w))$$

proporcionalni. Međutim, iz Taylorovog razvoja polinoma P i Q oko w tada slijedi da su polinomi P i Q proporcionalni, što je u kontradikciji s pretpostavkom da nemaju zajedničkih nultočaka. □

Primjer 3.6. Okarakterizirajmo sve parove polinoma za koje $S(x)$ ima dvije dvostruke nultočke. Tada i krivulja $\tilde{\Delta}$ ima dva singulariteta. Pronaći ćemo sve takve polinome oblika $P(x) = a+bx+x^2$,

$Q(x) = c + dx + x^3$ gdje su $a, b, c, d \in \mathbb{Q}$. Preostale polinome možemo dobiti uzimanjem linearnih kombinacija polinoma ovakvog oblika koje dobijemo, jer se uzimanjem linearnih kombinacija S i $\tilde{\Delta}$ ne mijenjaju do na množenje konstantom.

Vrijedi da $S(x)$ ima dvije dvostruke nultočke ako i samo ako postoje algebarski cijeli brojevi α i β stupnja manjeg ili jednakog 2 takvi da je $S(x) = (x+\alpha)^2(x+\beta)^2$, tj. ako vrijedi

$$x^4 + 2bx^3 + (3a - d)x^2 - 2cx + ad - bc = (x+\alpha)^2(x+\beta)^2.$$

Izjednačavanjem koeficijenata dobivamo sustav

$$\begin{aligned} \alpha + \beta &= b, \\ (\alpha+\beta)^2 + 2\alpha\beta &= 3a - d, \\ (\alpha+\beta)\alpha\beta &= -c, \\ (\alpha\beta)^2 &= ad - bc. \end{aligned}$$

Stavimo $\alpha + \beta = N$ i $\alpha\beta = M$. Tada sustav postaje

$$\begin{aligned} b &= N, \\ 3a - d &= N^2 + 2M, \\ c &= -MN, \\ ad - bc &= M^2. \end{aligned}$$

Sada ako umjesto b uvrstimo N i umjesto c uvrstimo $-MN$, preostaje nam sustav dvije jednadžbe s dvije nepoznanice po a i d:

$$\begin{aligned} ad &= M^2 - MN^2, \\ 3a - d &= N^2 + 2M. \end{aligned}$$

Iz tih jednadžbi dobivamo jednadžbu

$$d^2 + (N^2 + 2M)d - 3(M^2 - MN^2) = 0.$$

Rješavanjem jednadžbe po d, i onda uvrštavanjem nazad da dobijemo a, dobivamo dvije klase rješenja za (a, b, c, d):

$$\begin{aligned} &\{(M, N, -MN, M - N^2) \mid M, N \in \mathbb{Q}\} \\ &\{(N^2 - M)/3, N, -MN, -3M) \mid M, N \in \mathbb{Q}\} \end{aligned}$$

Primjer 3.7. Sada ćemo, ponovno preko koeficijenata polinoma, odrediti sve parove polinoma (P, Q) za koje je $s = 0$ i za koje još vrijedi $a_3 = b_0 = 0$. Preostali polinomi za koje je $s = 0$ mogu se dobiti linearnim kombinacijama ovakvih polinoma.

Imamo da je

$$s = \mu_{1,2}^3 + 27\mu_{0,1}\mu_{1,3}^2 + 27\left(\mu_{0,2}^2 - \mu_{0,1}\mu_{1,2}\right)\mu_{2,3} - 9\mu_{0,3}\left(\mu_{1,2}^2 + 9\mu_{0,1}\mu_{2,3}\right)$$

kvadratni polinom po b_3, pa je b_3 racionalan ako i samo ako je diskriminanta od s po b_3 kvadrat racionalnog broja. Diskriminanta je jednaka

$$27a_0(a_1a_2b_1 - a_1^2b_2 + 3a_0a_2b_2)^2(4a_2b_1^2 - 4a_1b_1b_2 + 3a_0b_2^2).$$

To je potpun kvadrat ako i samo ako je

$$3a_0(4a_2b_1^2 - 4a_1b_1b_2 + 3a_0b_2^2) = u^2$$

za neki racionalan broj u. Primijetimo da je taj izraz linearan po a_1, pa možemo a_1 izraziti preko u, i dobiti

$$a_1 = \frac{12a_0a_2b_1^2 + 9a_0^2b_2^2 - u^2}{12a_0b_1b_2}.$$

Sada možemo riješiti jednadžbu $s = 0$ po b_3 i dobiti

$$b_3 = \frac{b_2(3a_0b_2 - u)^3}{18a_0b_1(-12a_0a_2b_1^2 + 9a_0^2b_2^2 - 6a_0b_2u + u^2)},$$

pod uvjetom da su svi nazivnici različiti od 0.

Primjer 3.8. Neka je $P(x) = x^3 - 3x^2 - 1$, $Q(x) = -x$. Tada je $\frac{-\mu_{1,2}}{3\mu_{1,3}} = 1$. Nadalje, $S(x) = 2x^3 - 3x^2 + 1$, te $S'(x) = 6x^2 - 6x$, pa je 1 dvostruka nultočka, a $(1, 1)$ singularna za $\tilde{\Delta}$.

Primjer 3.9. Neka je $t \neq 0$ racionalan broj. Promotrimo polinome $P(x) = 1 + 3tx + 3t^2x^2$, $Q(x) = x^3$. Tada je $\mu_{2,3} = 3t^2$, $\mu_{1,3} = 3t$, $\mu_{0,3} = 1$, $\mu_{0,1} = \mu_{1,2} = \mu_{0,2} = 0$, te je $S(x) = 3t^2x^2\left(x + \frac{1}{t}\right)^2$, te su točke $(0, 0)$ i $\left(\frac{-1}{t}, \frac{-1}{t}\right)$ singulariteti od $\tilde{\Delta}$.

Primjer 3.10. Neka je $t \neq 0$ racionalan broj i neka je $P(x) = 1 + 27t^2x^2$, $Q(x) = x + 3t^2x^3$. Tada je $S(x) = 81t^4x^4 - 18t^2x^2 + 1 = (3tx - 1)^2(3tx + 1)^2$, pa su točke $\left(\pm\frac{1}{3t}, \pm\frac{1}{3t}\right)$ singularne za $\tilde{\Delta}$.

3.2 Razrješenje singulariteta

Sada ćemo korištenjem blowing-upa razriješiti singularitete $(1 : 0 : 0)$ i $(0 : 1 : 0)$ od $\overline{\Delta}$ uz pretpostavku $\mu_{2,3} \neq 0$.

Lema 3.11. *Pretpostavimo da je $\mu_{2,3} \neq 0$. Tada za svaki od singulariteta $(1 : 0 : 0)$, $(0 : 1 : 0)$ vrijedi da je u blowing-upu od $\overline{\Delta}$ u odnosu na te singularitete broj točaka iznad tih singulariteta koje su definirane nad $\mathbb{F}_p$ jednak $1 + \phi_p(\mu)$. Posebno, za $\mu = 0$, blowing-up od $\overline{\Delta}$ u odnosu na te singularitete ima jednako mnogo točaka nad $\mathbb{F}_p$ kao i $\overline{\Delta}$. Nadalje, te točke su nesingularne za blowing-up od $\overline{\Delta}$.*

Dokaz: Dokazat ćemo tvrdnju za singularitet $(1 : 0 : 0)$. Dokaz za $(0 : 1 : 0)$ je analogan, samo preimenujemo varijable x_1 i x_2. Zbog toga što je blowing-up lokalna operacija, dovoljno je napraviti blowing-up presjeka od $\overline{\Delta}$ i afine karte $\{x_1 \neq 0\}$. Tada možemo staviti $x_1 = 1$.

Dakle, određujemo zatvarač skupa

$$\{(x_2, z) \in \bar{\mathbb{F}}_p^2, (s : t) \in \mathbb{P}^1 \mid (x_2, z) \neq (0, 0) \wedge x_2 t = zs \wedge z^4 \tilde{\Delta}(1/z, x_2/z)\}.$$

Kad to presiječemo s afinom kartom za koju je $s \neq 0$, dobijemo da tražimo zatvarač skupa

$$\{(x_2, z) \in \bar{\mathbb{F}}_p^2, s \in \bar{\mathbb{F}}_p \mid z \neq 0 \wedge x_2 = zs \wedge z^4 \tilde{\Delta}(1/z, s) = 0\}.$$

Za nenul polinom $L(x)$, definiramo $\tilde{L}(x)$ kao $x^{\deg L} L(1/x)$. Tada dobivamo da je zadnji uvjet iz zagrade ekvivalentan s

$$z^2 \cdot \frac{\tilde{P}(z)Q(s) - \tilde{Q}(z)P(s)}{1 - zs} = 0.$$

Kako je $z \neq 0$, to je ekvivalentno s

$$\frac{\tilde{P}(z)Q(s) - \tilde{Q}(z)P(s)}{1 - zs} = 0.$$

Da bismo dobili zatvarač, dovoljno je maknuti uvjet $z = 0$. Drugim riječima, zatvarač je jednak

$$\{(x_2, z) \in \bar{\mathbb{F}}_p^2, s \in \bar{\mathbb{F}}_p \mid x_2 = zs \wedge \frac{\tilde{P}(z)Q(s) - \tilde{Q}(z)P(s)}{1 - zs} = 0\}.$$

Sada treba odrediti koliko točaka nad $\mathbb{F}_p$ ima iznad točke $(1 : 0 : 0)$, tj. određujemo točke za koje je $z = 0$. Drugim riječima, tražimo za koliko vrijednosti $s \in \mathbb{F}_p$ je $a_3 Q(s) - b_3 P(s) = 0$.

Kako je $a_3 Q(s) - b_3 P(s)$ kvadratni polinom u s sa diskriminantom jednakom $\mu = \mu_{1,3}^2 - 4\mu_{0,3}\mu_{2,3}$, tvrdnja o broju točaka slijedi. Neka su s_1 i s_2 nultočke polinoma $a_3 Q(s) - b_3 P(s)$.

Da bismo dokazali da su te točke regularne, dovoljno je dokazati da parcijalne derivacije polinoma

$$\frac{\tilde{P}(z)Q(s) - \tilde{Q}(z)P(s)}{1 - zs}$$

ne iščezavaju obje u točkama $(0, s_1)$ i $(0, s_2)$. Kad deriviramo taj polinom po varijabli z, dobivamo

$$\frac{(\tilde{P}'(z)Q(s) - \tilde{Q}'(z)P(s))(1 - zs) + s(\tilde{P}(z)Q(s) - \tilde{Q}(z)P(s)}{(1 - zs)^2}.$$

Uvrštavanjem $z = 0$ i $s = s_i$ u dobiveni izraz dobivamo

$$a_2 Q(s_i) - b_2 P(s_i) + s(a_3 Q(s_i) - b_3 P(s_i)).$$

Drugi probrojnik je jednak 0, a ako bi vrijedilo $a_2 Q(s_i) - b_2 P(s_i) = 0$, onda bi bilo i $a_2 b_3 - a_3 b_2 = 0$, što je kontradikcija. Zaključujemo da su točke $(0, s_i)$ regularne, kao što je i trebalo pokazati. □

Lema 3.12. *Neka je (w, w) singularna točka od $\tilde{\Delta}$ i neka je B blowing-up od $\tilde{\Delta}$ u točki (w, w), te*

neka je π projekcija s B na $\tilde{\Delta}$. Tada se u $\pi^{-1}\{(w,w)\}$ nalaze dvije točke, (w,w,ω) i $(w,w,\overline{\omega})$, gdje su ω i $\overline{\omega}$ nultočke polinoma t^2+t+1. Nadalje, te dvije točke su nesingularne za B.

Dokaz: Potrebno je odrediti zatvarač skupa

$$\{(x_1,x_2)\in\mathbb{A}^2,(t:s)\in\mathbb{P}^1 \mid (x_1,x_2)\neq(w,w) \ \wedge \ (x_1-w)t=(x_2-w)s \ \wedge \ \tilde{\Delta}(x_1,x_2)=0\}.$$

Kad to presiječemo s afinom kartom za koju je $s\neq 0$, dobijemo da tražimo zatvarač od

$$\{(x_1,x_2,t)\in\mathbb{A}^3 \mid x_1\neq w \ \wedge \ x_2=t(x_1-w)+w \ \wedge \ \tilde{\Delta}(x_1,t(x_1-w)+w)\}.$$

Posljednji uvjet možemo zapisati kao

$$\frac{P(x_1)Q(t(x_1-w)+w)-Q(x_1)P(t(x_1-w)+w)}{(1-t)(x_1-w)}=0.$$

Ako raspišemo brojnik tako što zapišemo polinome P i Q preko Taylorovog razvoja u točki w, te iskoristimo činjenicu da su $(P(w),P'(w),P''(w))$ i $(Q(w),Q'(w),Q''(w))$ proporcionalni, što slijedi iz činjenice da je w dvostruka nultočka od S, dobijemo da je brojnik jednak

$$(x_1-w)^3(a_3(Q(w+t(x_1-w))-t^3Q(x_1))-b_3(P(w+t(x_1-w))-t^3P(x_1))).$$

Kako je $x_1\neq w$, možemo podijeliti s $(x_1-w)^2$, pa uvjet glasi

$$\frac{a_3(Q(w+t(x_1-w))-t^3Q(x_1))-b_3(P(w+t(x_1-w))-t^3P(x_1))}{1-t}=0.$$

Primijetimo da je ovo stvarno polinom jer je za $t=1$ brojnik jednak 0. Nadalje, za $x_1=w$ dobije se $(a_3Q(w)-b_3P(w))(1+t+t^2)$, što nije nul-polinom po t, jer bi u suprotnom polinom S imao trostruku nultočku w.

Da bismo dobili zatvarač dovoljno je maknuti uvjet $x_1\neq w$.

Sada vidimo da se u praslici točke (w,w) nalaze točke oblika (w,w,ω), gdje je $\omega^2+\omega+1=0$, iz čega slijedi prva tvrdnja.

Sada treba provjeriti da je mnogostrukost u $\mathbb{A}^3$ zadana uvjetima

$$\begin{aligned}&\frac{a_3(Q(x_2)-b_3(P(x_2)-t^3P(x_1))}{1-t}=0,\\&x_2-w-t(x_1-w)=0\end{aligned}$$

nesingularna u točkama (w,w,ω) i $(w,w,\overline{\omega})$. Promotrimo matricu parcijalnih derivacija:

$$\begin{bmatrix}\frac{t^3(b_3P'(x_1)-a_3Q'(x_1))}{1-t} & -t\\ \frac{a_3Q'(x_2)-b_3P'(x_2)}{1-t} & 1\\ \frac{a_3Q(x_2)-b_3P(x_2)-(a_3Q(x_1)-b_3P(x_1))(3t^2-2t^3)}{(1-t)^2} & -x_1\end{bmatrix}$$

Kad uvrstimo (w, w, ω) umjesto (x_1, x_2, t) i promotrimo prva dva retka, vrijedi da su proporcionalni ako i samo ako je $\omega = -1$, što nije slučaj, ili ako je $a_3 Q'(w) = b_3 P'(w)$.

Da bi prva dva stupca bila proporcionalna, onda mora biti i zadnji element prvog stupca jednak 0, odnosno mora vrijediti

$$(2\omega^3 - 3\omega^2 + 1)(a_3 Q(w) - b_3 P(w)) = 0.$$

Međutim, drugi faktor nije 0 jer S nema trostrukih nultočaka, a prvi faktor je jednak $3(1 - \omega^2)$, što također nije jednako 0 kad je karakteristika različita od 3. Dakle, (w, w, ω) je nesingularna za B. Analogno zaključujemo za $(w, w, \overline{\omega})$. □

4 Dokaz Bias Conjecture uz pretpostavku $\mu = 0$

U ovom ćemo poglavlju razmatrati slučaj u kojem je $\mu = 0$. U sljedećoj je lemi dana operativnija karakterizacija tog uvjeta.

Lema 4.1. *Ako je $\mu = 0$, onda postoje $c \in \mathbb{Q}$ i polinom s racionalnim koeficijentima $T(x)$ takvi da je $b_3P(x) - a_3Q(x) = c \cdot T(x)^2$. Ako je $\mu_{2,3} = 0$, tada je $T(x) = 1$ i $c = \mu_{0,3}$. Ako je $\mu_{2,3} \neq 0$, tada je $c = \mu_{2,3}$ i $T(x) = \left(x - \frac{\mu_{1,3}}{\mu_{2,3}}\right)$.*

Dokaz: Vrijedi

$$b_3P(x) - a_3Q(x) = \mu_{2,3}x^2 + \mu_{1,3}x + \mu_{0,3}.$$

Ako je $\mu_{2,3} = 0$, onda je i $\mu_{1,3} = 0$ jer je $\mu = \mu_{1,3}^2 - 4\mu_{0,3}\mu_{2,3}$, pa je $b_3P(x) - a_3Q(x)$ konstantan polinom koji nije jednak nulpolinomu zbog pretpostavke da P i Q nemaju zajedničkih nultočaka.

Ako je $\mu_{2,3} \neq 0$, tada je

$$b_3P(x) - a_3Q(x) = \mu_{2,3} \cdot \left(x - \frac{\mu_{1,3}}{\mu_{2,3}}\right)^2.$$

□

Napomena: Razlog zašto ova lema vrijedi je taj što je μ jednak diskriminanti polinoma dobivenog reduciranjem polinoma Q modulo P. Uvjet $\mu = 0$ kaže da je polinom $\mu_{2,3} \cdot Q$ kvadrat u prstenu $\mathbb{Q}[x] \,/\, (P)$. Oznaku $T(x)$ iz prethodne leme ćemo koristiti u nastavku ovog poglavlja.

Sada ćemo eliminirati krivulju $\tilde{C}$ iz formule za drugi moment.

Lema 4.2. *Ako je $\mu = 0$, onda za sve osim konačno mnogo prostih brojeva p vrijedi*

$$\#\tilde{C}(\mathbb{F}_p) = 2\#\tilde{\Delta}(\mathbb{F}_p) - (\#P(\mathbb{F}_p))^2 + \#P(\mathbb{F}_p) - \#(P \cap S)(\mathbb{F}_p).$$

Dokaz: Neka je p prost broj takav da P i Q nemaju zajedničkih nultočaka u $\mathbb{F}_p$. Promotrimo točku $(x_1, x_2) \in \tilde{\Delta}(\mathbb{F}_p)$.

Znamo da vrijedi $P(x_1)Q(x_2) = Q(x_1)P(x_2)$. Dokažimo da je izraz $P(x_1)P(x_2)$ kvadrat (ili nula) u $\mathbb{F}_p$.

Naime, iz $P(x_1)Q(x_2) = Q(x_1)P(x_2)$ slijedi

$$P(x_1)T(x_2)^2 = T(x_1)^2P(x_2).$$

Ako je $T(x_1)$ ili $T(x_2)$ različito od nule (u $\mathbb{F}_p$), onda množenjem izraza s $P(x_1)$ ili $P(x_2)$ slijedi tvrdnja. Ako je pak $T(x_1) = T(x_2) = 0$, onda je nužno $x_1 = x_2$ jer je T linearan ili konstantan, pa je $P(x_1)P(x_2)$ svakako kvadrat.

Iz netom dokazanog slijedi da je broj točaka na $\tilde{C}(\mathbb{F}_p)$ jednak dvostrukom broju točaka na $\tilde{\Delta}(\mathbb{F}_p)$ umanjenom za broj točaka (x_1, x_2) na $\tilde{\Delta}(\mathbb{F}_p)$ za koje je $P(x_1)P(x_2) = 0$. Naime, za svaku točku (x_1, x_2) s $\tilde{\Delta}$ takvu da nije $P(x_1)P(x_2) = 0$ postoje dvije vrijednosti $y \in \mathbb{F}_p$ takve da je $P(x_1)P(x_2) = y^2$.

Iznad točaka (x_1, x_2) s $\tilde{\Delta}$ za koje je $P(x_1)P(x_2) = 0$ nalazi se samo jedna točka s $\tilde{C}$, ta točka je $(x_1, x_2, 0)$. Takve točke (x_1, x_2) za koje je $x_1 \neq x_2$ su točno parovi različitih nultočaka od P, i ima ih $(\#P)^2 - \#P$. S druge strane, takve točke za koje je $x_1 = x_2$ su upravo one za koje je x_1 nultočka i od P i od S, a njih ima $\#P \cap S$. Zbrajanjem svih zaključaka slijedi tvrdnja leme. □

Direktnom kombinacijom Lema 4.2 i 2.6 dobivamo sljedeću formulu za drugi moment.

Korolar 4.3. *Ako je $\mu = 0$, tada za sve osim konačno mnogo prostih brojeva vrijedi*

$$\tilde{M}_{2,p}(\mathcal{F}_k) = p(\#\tilde{\Delta}(\mathbb{F}_p) + p - \#S(\mathbb{F}_p)).$$

4.1 Podslučaj $\mu = 0$, $\mu_{2,3} \neq 0$

Teorem 4.4. *Ako vrijedi $\mu = 0$ te $\mu_{2,3} \neq 0$, onda je bias jednak $-1 - t$, gdje je t broj međusobno relativno prostih ireducibilnih faktora (nad $\mathbb{Q}[x]$) polinoma S.*

Dokaz: Prvo možemo pomoću Leme 3.2 zamijeniti $\#\tilde{\Delta}$ sa $\#\overline{\Delta} - 2$. Tada iz Korolara 4.3 imamo

$$\tilde{M}_{2,p}(\mathcal{F}_k) = p(\#\overline{\Delta} + p - \#S - 2).$$

Nadalje, označimo sa $p+1-A_p$ broj točaka nad $\mathbb{F}_p$ blowupa krivulje $\overline{\Delta}$. U ovom slučaju, zbog Leme 3.11, nad $\overline{\Delta}$ ima jednako točaka definiranih nad $\mathbb{F}_p$ kao nad njenim razrješenjem singulariteta, pa je $p + 1 - A_p = \#\overline{\Delta}$. Dakle, vrijedi sljedeća jednakost:

$$\tilde{M}_{2,p}(\mathcal{F}_k) = p(2p - A_p - 1 - \#S).$$

Krivulja $\overline{\Delta}$ je stupnja 3 ili 4, te ima barem 2 singularne točke. Prema stupanj-genus formuli, njen genus g je

$$g = \frac{3 \cdot 2}{2} - \sum_{P \in \overline{\Delta}} \frac{\nu_P(\overline{\Delta})(\nu_P(\overline{\Delta}) - 1)}{2}.$$

Svaka singularna točka je kratnosti barem 2 (po definiciji singularne točke), a $\overline{\Delta}$ ima dvije ili tri singularne točke, ovisno o tome je li $s = 0$ ili $s \neq 0$. Zaključujemo $g \leq 3 - 2 \cdot \frac{2 \cdot 1}{2} = 1$.

Ako je genus jednak 0, onda je A_p jednak 0 za sve osim konačno p.

Ako je genus jednak 1, na brojeve $(A_p)_{p \text{ prost}}$ možemo primijeniti Sato-Tateovu slutnju, iz koje slijedi da je prosjek brojeva $\left(\frac{A_p}{\sqrt{p}}\right)_p$ jednak 0.

Dakle, u oba slučaja brojevi $\left(\frac{A_p}{\sqrt{p}}\right)_p$ imaju prosjek 0, pa je pribrojnik najvećeg reda u kanonskom rastavu momenta čiji prosjek nije jednak 0 onaj uz p. Taj pribrojnik je $p(-1-\#S)$. Koristeći Lemu 2.3 dobivamo da im je prosjek jednak $-1 - t$, gdje je t broj ireducibilnih faktora polinoma S koji su međusobno relativno prosti. □

Napomena: Polinom S će u ovom slučaju uvijek imati racionalnu nultočku. Razlog za to je što je $S(x) = P(x)Q'(x) - Q(x)P'(x) = T(x)(2P(x)T'(x) - T(x)P'(x))$, a T je linearan polinom s nultočkom $\frac{\mu_{1,3}}{\mu_{2,3}}$. Dakle, S uvijek ima barem dva ireducibilna faktora i oni su relativno prosti jer nultočka od $T(x)$ nikad nije nultočka od $P(x)$ jer bi onda $P(x)$ i $Q(x)$ imali zajedničku nultočku. Zaključujemo da je bias u ovom slučaju manji ili jednak -3.

Nadalje, ako P još ima dvostruku racionalnu nultočku, tada je broj komponenti od S jednak barem 3, pa je bias tada manji ili jednak -4.

Primjer 4.5. Primjer polinoma P i Q koji zadovoljavaju uvjete ovog teorema je $P(x) = x^3 + 3x^2 + x + 2$, $Q(x) = x^3 + 2x^2 - x + 1$. Za njih je $S(x) = x^4 + 4x^3 + 8x^2 + 2x - 3 = (x+1)(x^3 + 3x^2 + 5x - 3)$. Drugi faktor je ireducibilan, pa je bias jednak -3.

Primjer 4.6. Neka je $P(x) = x^2(x + 1)$ te $Q(x) = (5x - 1)^2$. Tada vrijedi $S(x) = x(5x - 1)(x - 1)(5x - 2)$. Dakle, S ima četiri ireducibilne međusobno relativno proste komponente, pa je bias u ovom slučaju jednak -5.

4.2 Podslučaj $\mu = 0$, $\mu_{2,3} = 0$

Ovaj podslučaj je jednostavan jer je u ovom slučaju ostatak pri dijeljenju polinoma Q polinomom P jednak nekoj konstanti različitoj od nule. Onda je $\tilde{\Delta}(x_1, x_2) = 0$ ako i samo ako je $a_3(x_1^2 + x_1x_2 + x_2^2) + a_2(x_1 + x_2) + a_1 = 0$. Stavimo $c_2 = a_2/a_3$ te $c_1 = a_1/a_3$. Tada je dovoljno odrediti broj nultočaka nad $\mathbb{F}_p$ polinoma

$$x_1^2 + x_1x_2 + x_2^2 + c_2(x_1 + x_2) + c_1.$$

Neka je $D(x)$ diskriminanta tog polinoma po varijabli x_1, tj.

$$D(x) = -3x^2 - 2c_2x + c_2^2 - 4c_1.$$

Uz uvedene oznake, vrijede sljedeći rezultati.

Lema 4.7. *Ako je $c_2^2 \neq 3c_1$ ili, ekvivalentno, $a_2^2 \neq 3a_1a_3$, onda za sve osim konačno prostih brojeva p vrijedi $\#\tilde{\Delta}(\mathbb{F}_p) = p - \phi_p(-3)$. Ako je $c_2^2 = 3c_1$, onda za sve osim konačno prostih brojeva p vrijedi $\#\tilde{\Delta}(\mathbb{F}_p) = p + (p-1)\phi_p(-3)$.*

Dokaz: Ako je $\phi_p(D(x)) = j$ za neki x, tada (po formuli za rješenja kvadratne jednadžbe) postoji točno $j + 1$ točaka oblika (w, x) na $\tilde{\Delta}$. Dakle, broj točaka na $\tilde{\Delta}$ jednak je

$$\sum_{x \in \mathbb{F}_p} (1 + \phi_p(D(x)) = p + \sum_{x \in \mathbb{F}_p} \phi_p(-3x^2 - 2c_2x + c_2^2 - 4c_1).$$

Sada tvrdnja slijedi iz Leme 2.1 primijenjene na $D(x)$. Drugi pribrojnik je jednak $-\phi_p(-3)$ ako je $(2c_2)^2 - 4 \cdot (-3) \cdot (c_2^2 - 4c_1) = 0$ u $\mathbb{F}_p$, što je ekvivalentno s $c_2^2 = 3c_1$ kad god je $p > 3$. Ako je $c_2^2 \neq 3c_1$, onda je drugi pribrojnik jednak $(p-1)\phi_p(-3)$. □

Primijetimo još da u slučaju kad je $c_2^2 = 3c_1$ vrijedi da je $S(x)$ umnožak konstante i kvadrata linearnog polinoma, pa se na S u tom slučaju nalazi točno jedna točka. Iz prethodne leme i ovog opažanja dobivamo preciznije formule.

Teorem 4.8. *Pretpostavimo da je $\mu = 0$ te $\mu_{2,3} = 0$. Tada za sve osim konačno mnogo prostih brojeva p vrijedi*

- *Ako je $a_2^2 \neq 3a_1a_3$, onda $\tilde{M}_{2,p}(\mathcal{F}_k) = p(2p - \phi_p(-3) - \#S(\mathbb{F}_p))$, te je bias jednak -2 ako je $a_2^2 - 3a_1a_3$ kvadrat racionalnog broja, a inače je jednak -1;*
- *Ako je $a_2^2 = 3a_1a_3$, onda $\tilde{M}_{2,p}(\mathcal{F}_k) = p(2p + (p-1)\phi_p(-3) - 1)$, te je bias jednak -1.*

Dokaz: Formule za moment su već dokazane. Kako je prosjek brojeva $(\phi_p(-3))_{p \text{ prost}}$ jednak 0 po Lemi 2.3 primijenjenoj na polinom $x^2 + 3$, te su koeficijenti uz p u formuli za drugi moment u oba slučaja jednaki $-\phi_p(-3) - \#S(\mathbb{F}_p)$, po Lemi 2.3 primijenjenoj na S je bias jednak $-t$, gdje je t broj međusobno relativno prostih ireducibilnih komponenti od S.

Vrijedi da je S do na množenje konstantom jednak $3a_3x^2 + 2a_2x + a_1$. Ako diskriminanta od S nije kvadrat racionalnog broja, tada je S ireducibilan i bias je jednak -1. Ako je diskriminanta potpun kvadrat racionalnog broja različitog od nule, tada S ima dvije različite linearne komponente i bias je jednak -2. Ako je diskriminanta jednaka 0, tada je S kvadrat linearnog polinoma i bias je jednak -1. □

Primjer 4.9. Promotrimo konkretne parove polinoma koji zadovoljavaju uvjete Teorema 4.8.

Neka je $P(x) = x^3 + 3x^2 + 3x$, te $Q(x) = P(x) + 1$. Tada je $\mu = \mu_{2,3} = 0$ i $a_2^2 - 3a_1a_3 = 0$, pa je $\tilde{M}_{2,p}(\mathcal{F}_k) = p(2p + (p-1)\phi_p(-3) - 1)$. U ovom slučaju bias je jednak -1.

Neka je $P(x) = x^3 + 3x^2 + 2x$, te $Q(x) = P(x) + 1$. Tada je $\mu = \mu_{2,3} = 0$ i $a_2^2 - 3a_1a_3 = 3$, pa je bias također jednak -1.

Neka je $P(x) = x^3 + 3x^2 + 4x$, te $Q(x) = P(x) + 1$. Tada je $\mu = \mu_{2,3} = 0$ i $a_2^2 - 3a_1a_3 = 1$, pa je bias jednak -2.

Literatura

[1] D. Allcock. *Hilbert's Nullstellensatz*. Expository notes. 2005. URL: https://web.ma.utexas.edu/users/allcock/expos/nullstellensatz3.pdf.

[2] Y. Bokor. *Resolving Singularities of Plane Algebraic Curves*. Honours Thesis, University of Sydney. 2019. URL: https://www.maths.usyd.edu.au/u/yossi/writings/HonoursThesis.pdf.

[3] Je-Ok Choi. *Hilbert's Nullstellensatz and its application in graph theory*. 2009. URL: https://www.math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Choi.pdf.

[4] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, 1977.

[5] Matija Kazalicki i Bartosz Naskrecki. *Second moments and the bias conjecture for the family of cubic pencils*. Preprint. 2020. arXiv: 2012.11306 [math.NT].

[6] Barry Mazur. „Finding meaning in error terms". *Bulletin of the American Mathematical Society* 45.02 (2008.), str. 185–228. DOI: 10.1090/s0273-0979-08-01207-x.

[7] Philippe Michel. „Rang moyen de familles de courbes elliptiques et lois de Sato-Tate." fre. *Monatshefte für Mathematik* 120.2 (1995.), str. 127–136. URL: http://eudml.org/doc/178698.

[8] Steven J. Miller. „One- and two-level densities for rational families of elliptic curves: evidence for the underlying group symmetries". *Compositio Mathematica* 140.04 (srpanj 2004.), str. 952–992. ISSN: 1570-5846. DOI: 10.1112/s0010437x04000582. URL: http://dx.doi.org/10.1112/S0010437X04000582.

[9] Rick Miranda. *Algebraic curves and Riemann surfaces*. English. Sv. 5. Providence, RI: AMS, American Mathematical Society, 1995., str. xxi + 390. ISBN: 0-8218-0268-2.

[10] B. Moonen. *Introduction to Algebraic Geometry*. Course notes. 2015. URL: https://www.math.ru.nl/~bmoonen/Lecturenotes/alggeom.pdf.

[11] S. Peacock. Lecture notes. URL: https://www.peacock.onl/teaching/Lecture12.pdf.

[12] I. Shafarevich. *Basic algebraic geometry 1*. 3rd ed. Springer, 2013.

[13] Andrew Sutherland. „Sato-Tate distributions". *Contemporary Mathematics* (2019.), str. 197–248. ISSN: 1098-3627. DOI: 10.1090/conm/740/14904. URL: http://dx.doi.org/10.1090/conm/740/14904.

[14] T. Szamuely. *A course on the Weil conjectures*. Lecture notes. 2019. URL: http://pagine.dm.unipi.it/tamas/Weil.pdf.

[15] V. Talovikova. *Riemann-Roch Theorem*. 2009. URL: https://www.math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Talovikova.pdf.

Sažetak

Ivan Novak:

Računanje drugog momenta familija eliptičkih krivulja

Ovaj rad je dopuna članka ([5]) Matije Kazalickog i Bartosza Naskreckog o računanju drugog momenta familija eliptičkih krivulja. U spomenutom članku Bias Conjecture je dokazana u generičkom slučaju, a u ovom radu su dokazani neki od preostalih slučajeva.

Na samom početku rada iskazani su prethodni rezultati. Zatim su definirani potrebni osnovni pojmovi iz algebarske geometrije, ukratko je definiran genus krivulje te je iskazana Sato-Tate slutnja. Također je opisan blowing-up kao jedna od metoda za razrješenje singulariteta algebarskih mnogostrukosti.

U trećem poglavlju su detaljno analizirani singulariteti krivulje nad kojom je potrebno odrediti broj točaka da bi se provjerila Bias Conjecture. Pristup analizi singulariteta je bio nešto elementarniji i detaljniji nego u članku [5], te je za razrješenje singulariteta korištena metoda blowing-up.

U četvrtom poglavlju, koje je najoriginalniji dio rada, su dokazani neki slučajevi Bias Conjecture, korištenjem rezultata iz trećeg poglavlja i Sato-Tate slutnje.

Ključne riječi: *drugi moment, Bias Conjecture, algebarska geometrija, blowing-up*

Summary

Ivan Novak:

Second moments of families of elliptic curves

This paper is a supplement of the paper on second moments of families of elliptic curves and Bias Conjecture ([5]) by Matija Kazalicki and Bartosz Naskrecki. In the mentioned article, Bias Conjecture is proven in the generic case, and this paper covers some of the remaining cases.

In the beginning of the paper, some previous results are listed. After that, the basics of algebraic geometry are covered, a brief definition of genus of a curve is given, and the Sato-Tate conjecture is stated. Also, the method of blowing-up is described as a method to resolve singularities of an algebraic variety.

In the third chapter, we analyse the singularities of a curve whose number of $\mathbb{F}_p$-rational points is critical for proving the Bias Conjecture. The approach towards the analysis of singularities was a bit more thorough and elementary than in [5], and blowing-up was used to resolve the singularities.

In the fourth chapter, which is the most original part of the paper, we prove some cases of the Bias Conjecture, using the results from the third chapter along with Sato-Tate Conjecture.

Keywords: *second moments, Bias Conjecture, algebraic geometry, blowing-up*