Истраживачка станица Петница

Пројекат
Семинар математике

Експериментална класификација кубних форми над коначним пољима

Полазници
Данило Ранђеловић
Марко Лазић

Ментори
Душан Драгутиновић
Димитрије Глукчевић

Београд, *датум када предате рад*

Садржај

1

Увод

2

Основни појмови

Дефиниција 2.1. Прстен свих мултиваријабилних полинома над n променљивих, над пољем $\mathbb{F}$, означаваћемо са $\mathbb{F}[X_1, X_2, \ldots, X_n]$.

Дефиниција 2.2. Хомогени полином P степена d над пољем F у n променљивих дефинишемо као

$$P(x_1, x_2, \ldots, x_n) = \sum_{i_1+i_2+\ldots+i_n=d} c_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

где су сви коефицијенти c_i у пољу $\mathbb{F}$.

Дефиниција 2.3. Прстен свих хомогених мултиваријабилних полинома степена d над n променљивих у пољу $\mathbb{F}$ означаваћемо са $\mathbb{F}[X_1, X_2, \ldots, X_n]_d$.

У наставку рада, подразумеваћемо да радимо у пољу $\mathbb{F}_p$, коначном пољу просте карактеристике p. Даље, прстен из претходне дефиниције означаваћемо са $\mathbb{F}_p[X]_d^n$, а његове елементе називаћемо *формама*.

Дефиниција 2.4. *Општу линеарну групу* димензије n над пољем $\mathbb{F}$ дефинишемо као

$$GL_n(\mathbb{F}) \coloneqq \{g \in \mathbb{M}_{n\times n}(\mathbb{F}) \mid \det(g) \neq 0\}$$

заједно са операцијом множења матрица.

Другим речима, ово је група свих линеарних аутоморфизама векторског простора димензије n.

Дефиниција 2.5. *Простор променљивих* $\mathbb{V}_n$ је скуп свих n-торки са елементима из поља $\mathbb{F}_p$.

Скуп $\mathbb{V}_n$ можемо еквивалентно посматрати као векторски простор матрица димензија $1 \times n$ над пољем $\mathbb{F}_p$, односно као скуп $\mathbb{M}_{1\times n}(\mathbb{F}_p)$.

Дефиниција 2.6. Нека је $x = [x_1, x_2, \ldots, x_n] \in \mathbb{V}_n$. Тада за $g \in GL_n(\mathbb{F}_p)$ дефинишемо функцију $\circ : GL_n(\mathbb{F}_p) \times \mathbb{V}_n \longrightarrow \mathbb{V}_n$ са

$$\circ(g, x) \coloneqq [x_1, x_2, \ldots, x_n]g^T.$$

Тврдња 2.1. Функција $\circ$ представља дејство групе $GL_n(\mathbb{F}_p)$ на скуп $\mathbb{V}_n$.

Доказ. Довољно је проверити аксиоме дејства:

- $\circ(e, x) = xe^T = xe = x$.
- $\circ(g, \circ(h, x)) = \circ(g, xh^T) = xh^T g^T = x(gh)^T = \circ(gh, x)$.

□

Имајући ово у виду, дејство линеарног пресликавања $g \in GL_n(\mathbb{F}_p)$ на елемент $x \in \mathbb{V}_n$ означаваћемо са gx. Приметимо да ово дејство представља инвертибилну линеарну смену промењљивих.

Дефиниција 2.7. Релацију $\sim$ на скупу $\mathbb{F}_p[X]_d^n$ дефинишемо на следећи начин:

$$q_1 \sim q_2 \Leftrightarrow (\exists g \in GL_n(\mathbb{F}_p))\ (\forall x \in \mathbb{V}_n)\ q_1(x) = q_2(gx).$$

Тврдња 2.2. Релација $\sim$ је релација еквиваленције.

Доказ. Доказујемо редом рефлексивност, симетричност и транзитивност ове релације:

- Одабиром $g = e$ добијамо $q \sim q$.
- Из $q_1(x) = q_2(gx)$ следи и $q_2(x) = q_1(g^{-1}x)$.
- Из $q_1(x) = q_2(gx)$ и $q_2(x) = q_3(hx)$ следи и $q_1(x) = q_3(hgx)$.

□

Кажемо да су форме q_1 и q_2 *еквивалентне* ако и само ако $q_1 \sim q_2$, и тада g називамо *надређеним аутоморфизмом*.

Са $\mathcal{A}(n, d, p)$ означавамо скуп класа еквиваленције ове релације. За фиксне тројке (n, d, p), $n \geq 2$, оценићемо $|\mathcal{A}|$ поступком који се може генерализовати на форме вишег степена, не ослањајући се на познате резултате добијене карактеризацијом квадратних форми.

3

Особине форми

Тројку (n, d, p) сматрамо унапред фиксираном. Подразумевамо да ознаке користе ову одређену тројку уколико није другачије речено. Такође, подразумевамо да форме припадају управо прстену $\mathbb{F}_p[X]_d^n$.

3.1 Идентификатор

Дефиниција 3.1. Нека је q форма. За $k = 0, 1, \ldots, p-1$ дефинишемо *класе остатка* k

$$\mathcal{C}_k(q) \coloneqq \{x \in \mathbb{V}_n \mid q(x) = k\}.$$

Приметимо да важи $\bigsqcup_{i=0}^{p-1} \mathcal{C}_i(q) = \mathbb{V}_n$. Другим речима, скуп $\{\mathcal{C}_i(q)\}_{i=0}^{p-1}$ представља *разбијање* скупа $\mathbb{V}_n$.

Дефиниција 3.2. Нека је q форма. *Идентификатор* форме q је скуп

$$\mathbb{I}_q \coloneqq \{(k, |\mathcal{C}_k(q)|) \mid k = 0, 1, 2, \ldots, p-1\}.$$

Јасно је да свака форма индукује једно разбијање скупа $\mathbb{V}_n$. Поставља се следеће питање:

Да ли можемо класификовати форме на основу разбијања које индукују?

Другим речима, можемо ли искористити изглед разбијања да опишемо дејство произвољног елемента $GL_n(\mathbb{F}_p)$ на посматрану форму? Делимичан одговор нам даје следећа теорема.

Теорема 3.1. Нека су a и b две еквивалентне форме. Тада

$$\mathbb{I}_a = \mathbb{I}_b.$$

Доказ. Нека је $g \in GL_n(\mathbb{F}_p)$ један надређени аутоморфизам ове две форме. Нека је $k \in \{0, 1, 2, \ldots, p-1\}$ произвољно. Доказаћемо да је функција $f_k : \mathcal{C}_k(a) \longrightarrow \mathcal{C}_k(b)$ дефинисана са

$$f_k(x) = gx$$

добро дефинисана бијекција. Заиста, нека је $x \in \mathcal{C}_k(a)$ произвољно. Приметимо

$$b(f_k(x)) = b(gx) = a(x) = k$$

одакле $f_k(x) \in \mathcal{C}_k(b)$, па је f_k заиста добро дефинисана. Имајући у виду да је g аутоморфизам простора $\mathbb{V}_n$, функција f_k је рестрикција дејства елемента g на скуп $\mathcal{C}_k(a)$, па самим тим мора важити

$$|\mathcal{C}_k(a)| \leq |\mathcal{C}_k(b)|.$$

Слично, g^{-1} је надређени аутоморфизам између b и a, па можемо закључити да у претходној неједнакости важи једнакост, одакле следи тврђење. □

Често ћемо се служити контрапозицијом ове теореме.

Лема 3.1. Нека су a и b две форме са различитим идентификаторима. Тада a и b нису еквивалентне.

Приметимо да смо у доказу теореме 3.1 доказали нешто јаче од њене почетне тврдње; не само да постојање аутоморфизма g гарантује да су скупови $\mathcal{C}_k(a)$ и $\mathcal{C}_k(b)$ исте кардиналности, већ је ово фиксно g изоморфизам између поменутих скупова *за свако* $k \in \{0, 1, 2, \ldots, p-1\}$.

Знајући да је g линеарна трансформација, закључујемо да је структура $\mathbb{V}_n$ одржана не само унутар класа истог остатка, већ и између елемената класа различитих остатака.

3.2 Карактеристика

Констатујмо сада два позната тврђења алгебре.

Тврдња 3.1. Свако поље $\mathbb{F}$ је домен јединствене факторизације.

Лема 3.2. Уколико је K домен јединствене факторизације, тада је и прстен полинома $K[X]$ домен јединствене факторизације.

Узастопним примењивањем леме 3.2 можемо закључити и да је прстен $\mathbb{F}_p[X]_d^n$ такође домен јединствене факторизације. Мотивисани овим, доказујемо лему која следи.

Лема 3.3. Нека је q иредуцибилна форма. Тада је свака њој еквивалентна форма такође иредуцибилна.

Доказ. Претпоставимо супротно; нека је q_1 произвољна редуцибилна форма која је еквивалентна форми q. Тада, за неко g, можемо написати

$$q(x) = q_1(gx) = a(gx)b(gx)$$

за две неконстантне (ненула) форме a и b. Ово очито контрадиктује иредуцибилност форме q. □

Сада смо спремни да уведемо још једну особину форми која је заједничка свим формама унутар исте класе еквиваленције релације $\sim$.

Дефиниција 3.3. Нека је q форма. За $i = 1, 2, \ldots, d$ дефинишемо $c_i(q)$ као број иредуцибилних форми степена i које улазе у факторизацију форме q.

Дефиниција 3.4. Нека је q форма. *Карактеристика* форме q је скуп

$$\mathcal{K}_q \coloneqq \{(i, c_i(q)) \mid i = 1, 2, \ldots, d\}.$$

Теорема 3.2. Нека су a и b две еквивалентне форме. Тада

$$\mathcal{K}_a = \mathcal{K}_b.$$

Доказ. По леми 3.3, надређени аутоморфизам форми a и b одржава иредуцибилност сваке форме која улази у факторизацију форме a. Дакле, трансформацијом тих иредуцибилних форми добијамо факторизацију форме b, одакле следи тврђење. □

Поново, наводимо контрапозицију ове теореме.

Лема 3.4. Нека су a и b две форме са различитим карактеристикама. Тада a и b нису еквивалентне.

Следећа теорема, у комбинацији са лемом 3.4, нам дозвољава да конструишемо међусобно нееквивалентне форме.

Теорема 3.3. Нека је A произвољан скуп облика

$$A = \{(i, b_i) \mid (\forall i \in \{1, 2, \ldots, d\})\ b_i \in \mathbb{N}_0\}.$$

Тада важи еквиваленција

$$(\exists q)\ \mathcal{K}_q = A \iff \sum_{i=1}^{d} i b_i = d.$$

Доказ. Доказујемо оба смера еквиваленције одвојено.
($\Rightarrow$) Лева страна једнакости представља допринос сваке иредуцибилне форме степену форме q, који износи d.
($\Leftarrow$) За свако $i \in \{1, 2, \ldots, d\}$, одаберимо по b_i иредуцибилних форми степена i. Њихов производ је управо форма степена d. □

У наставку се бавимо конкретним тројкама (n, d, p), где ћемо форме најпре класификовати по њиховој карактеристици, а затим и по идентификатору.

4

Класификација малих форми

Број различитих моничних монома степена d у n променљивих износи $\binom{n+d-1}{d}$. Свака оваква t-торка једнозначно кореспондира хомогеном полиному из $\mathbb{F}_p[X]_d^n$. Лако се проверава да је пресликавање задато са

$$(c_1, c_2, ..., c_t) \in \mathbb{F}_p^t \quad \longleftrightarrow \sum_{i_1+i_2+...+i_n=d} c_{i_1,i_2,...,i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$$

добро дефинисана бијекција, уколико кажемо да c_k представља коефицијент уз k-ти по реду лексикографски најмањи моном. Надаље, ова t-торка је *придружена* одговарајућој форми.

Тврдња 4.1. Елементе прстена $\mathbb{F}_p[X]_d^n$ можемо посматрати као векторски простор димензије $t = \binom{n+d-1}{d}$, над пољем скалара $\mathbb{F}_p$.

Овај векторски простор надаље означавамо са $\mathbb{V}_t$. Појам линеарне зависности (и независности) форми дефинишемо као и у сваком другом векторском простору.

4.1 Квадратне форме у пољу карактеристике два

Теорема 4.1. Нека је $q \in \mathbb{F}_2[X]_2^n$ произвољна форма. Тада је она или иредуцибилна, или је еквивалентна некој од следећих форми:

- $a(x) \equiv 0$ (a је *нула*-форма)
- $a(x) = x_1 x_2$.
- $a(x) = x_1^2$.

Притом, наведене форме *никада* нису међусобно еквивалентне.

Доказ. У случају када је q иредуцибилна или *нула*-форма, тврђење следи. Нека је даље $q(x) = b(x)c(x)$, где су b и c линеарне форме. Разликујемо два случаја:

- Форме b и c су линеарно независне.
  Нека је g надређени аутоморфизам форми x_1 и b, као и форми x_2 и c (посматрајући их као елементе векторског простора $\mathbb{V}_n$). Овакво g постоји, зато што линеарна независност b и c не нарушава инвертибилност трансформације. Приметимо

  $$x_1 x_2 = b(gx)c(gx) = q(gx)$$

  одакле следи тврђење.

- Форме b и c су линеарно зависне.
  С обзиром на то да радимо у пољу карактеристике два, мора важити $b(x) = c(x)$. Нека је g надређени аутоморфизам форми x_1 и b. Уочимо

  $$x_1^2 = b(gx)^2 = q(gx)$$

  одакле следи тврђење.

Остаје да докажемо да поменуте форме никада нису међусобно еквивалентне; међутим, ово следи директно из леме 3.4. □

Све иредуцибилне форме имају исту карактеристику. Ради њихове даље класификације, служићемо се њиховим идентификаторима у једном од следећих поглавља.

4.2 Квадратне форме у пољу карактеристике већем од два

Коначна поља карактеристике веће од два захтевају посебан коментар због појаве квадратних неостатака.

Теорема 4.2. Нека је $q \in \mathbb{F}_p[X]_2^n$ произвољна форма. Тада је она или иредуцибилна, или је еквивалентна некој од следећих форми:

- $a(x) \equiv 0$
- $a(x) = x_1 x_2$

- $a(x) = x_1^2$
- $a(x) = \omega x_1^2$, где је ω примитивни корен по модулу p.

Притом, наведене форме никада нису међусобно еквивалентне.

Доказ. Случај када је q иредуцибилна, *нула*-форма или производ две линеарно независне форме, спроводимо као у доказу теореме 4.1. Нека је сада $q(x) = b(x)c(x)$, где су b и c две линеарно зависне форме. Разликујемо два случаја:

- $b(x) = kc(x)$, где је k квадратни остатак по модулу p.
  Нека је $j \in \mathbb{F}_p$ такво да $k = j^2$. Сада је очито

  $$q(x) = (jc(x))^2$$

  па можемо поступити слично доказу теореме 4.1. Оваква форма је еквивалентна форми x_1^2.

- $b(x) = lc(x)$, где је l квадратни неостатак по модулу p.
  Може се доказати да је $l = \omega j^2$ за неко $j \in \mathbb{F}_p$. Сада је

  $$q(x) = \omega(jc(x))^2$$

  одакле сличним поступком из доказа теореме 4.1 закључујемо да је оваква форма еквивалентна форми ωx_1^2.

Иако форме x_1^2 и ωx_1^2 имају исту карактеристику, њихови идентификатори нису исти. Наиме, примећујемо

$$|\mathcal{C}_1(x_1^2)| \geq 1 > 0 = |\mathcal{C}_1(\omega x_1^2)|$$

па су ове форме заиста нееквивалентне. □

5

Репрезентација

Дефиниција 5.1. Репрезентација групе G над векторским простором $\mathbb{F}^n$ представља хомоморфизам $\rho : G \longrightarrow GL_n(\mathbb{F})$

Дефиниција 5.2. Дефинишемо репрезентацију $\varphi : GL_n(\mathbb{F}_p) \longrightarrow GL_t(\mathbb{F}_p)$ на следећи начин. За свако $g \in GL_n(\mathbb{F}_p)$, $\varphi(g)$ је елемент $GL_t(\mathbb{F}_p)$ такав да је за сваки полином $f(x) \in \mathbb{F}[X]_d^n$, $x \in \mathbb{V}_n$ и њему придружен $f_t \in \mathbb{F}^t$ важи

$$f(gx) = \varphi(g) f_t$$

Имплементација алгоритма који мора да рачуна дејство групе над полиномима која представља хомогене полиноме као елементе $\mathbb{F}^t$ а дејство као множење матрицом избегава репетитивну употребу симболичких калкулација, што знатно смањује време извршавања алгоритма. Дејство елемената $\varphi(g)$ над $\mathbb{F}^t$ је управо множење вектора матрицом. Калкулација $\varphi(g)$ је тривијална.