Universiteit Utrecht

Faculteit Bètawetenschappen

Het tellen van irreducibele en singuliere polynomen in eindige lichamen

Bachelor Scriptie

Arja Blok

Wiskunde

Begeleider:

prof. dr. F. Beukers
Mathematisch Instituut

14 juni 2018

Abstract

Het aantal polynomen van een bepaalde graad over een eindig lichaam is eindig, het aantal met de speciale eigenschappen irreducibele en singulariteit worden gegeven voor één en twee variabelen. Voor irreducibele in één variabele worden twee bewijzen gegeven voor de gevonden explicite uitdrukking, in twee variabelen is er een benadering. De uitdrukkingen voor singuliere polynomen worden onderverdeelt in een explicite wanneer de totale graad groot genoeg is en een afschatting voor kleinere graad. Voor polynomen tot graad twee volgt een geometrische uitleg voor het exacte aantal.

Contents

1 Inleiding

Er zijn maar een eindig aantal polynomen van een bepaalde graad over een eindig lichaam. Het aantal daar van is vrij eenvoudig te tellen, voor elke coëfficient zijn er zo veel opties als er elementen in het lichaam zijn. Omdat het aantal polynomen eindig is zijn ook het aantal polynomen met speciale eigenschappen zoals irreducibiliet of singuliriteit eindig, echter hoeveel zijn dit er nu precies? In dit stuk zullen we de voornamelijk de rationale gevallen bekijken.
Irreducibiliteit van een polynoom in een polynoomring is zoals het priem zijn van een getal in de natuurlijke getallen. Het tellen van deze laatste is nog een open probleem maar het tellen van irreducibele polynomen in een variabele is al een tijdje opgelost. De beroemde wiskundige Gauß wijde al in 1798 in zijn omvangrijke werk 'Disquisitiones Arithmeticae' hier een stuk aan.[7]
Singulariteit is een belangrijke eigenschap in de algebraïsche meetkunde. En heeft daarmee ook toepassingen in meer bekende wiskundige vakgebieden zoals complexe analyse, topologie en getaltheorie. De stellingen die we hier bekijken zijn relatief jong, de exacte grens voor stelling 5.1 komt uit 2003.
Voor irreducibele polynomen bekijken we eerst het geval met een variabele. Daarna zullen we het aantal op twee manieren berekenen: met behulp van het inclusie-exclusie principe en met genererende functies. Deze laatste methode kunnen we ook gebruiken om iets te zeggen over het aantal irreducibele polynomen in meerdere variabelen.
Daarna bekijken we de verhouding van het aantal singuliere polynomen in twee variabelen. Als de graad van het polynoom voldoende groot is kunnen we hier een exacte verhouding vinden. Voor een kleinere graad kunnen we een afschatting doen door een onder en bovengrens te vinden. Tenslotte berekenen we het exacte aantal singuliere polynomen van graad twee door te kijken naar alle verschilende vormen van deze polynomen.

2 Achtergrond van de stof

Polynomen over een eindig lichaam zijn net zoals polynomen over de reeële getallen, maar nu met coëfficienten in het eindige lichaam. Een eindig lichaam is een wiskundige structuur waarin optelling, vermenigvuldiging en deling mogelijk zijn met eindig veel elementen, het volgt dat dit alleen een priemmacht aantal kan zijn. Irreducibel wil zeggen dat een polynoom niet te schrijven is als het product van twee niet constante polynomen. Dit is zoals priemgetallen over de gehele getallen. Singulier voor een polynoom in twee variabelen betekend dat er een punt is zodat zowel het polynoom zelf, de afgeleide naar de eerste en tweede variabele nul is.

We zullen eerst iets uitleggen over eindige lichamen en polynomen daarin. Hierin noemen we een aantal begrippen zoals die in het tweede jaars cursus 'Ringen en Galoistheorie' aanbod komen. We geven dook e Möbius inversie en een bewijs hiervoor zodat we deze kunnen gebruiken bij het tellen van irreducibele polynomen.

2.1 Eindige lichamen

Een lichaam is een wiskundige structuur waarin optellen en vermenigvuldigen mogelijk zijn.[5, p. 6] Om precies te zijn een lichaam $\mathbb{F}$ is een verzameling inclusief de elementen 1 en 0 en twee opperaties $+$ en $\cdot$ zodat $(\mathbb{F}, +, 0)$ een abelse groep is en daarnaast aan de volgede axioma's is voldaan voor alle $a, b, c \in \mathbb{F}$:

Identiteit Er is een element $1 \neq 0$ zodat geldt $1 \cdot a = a = a \cdot 1$.

Commutativiteit $ab = ba$.

Associativiteit $(ab)c = a(bc)$.

Distributiviteit $a(b + c) = ab + ac$ en $(a + b)c = ac + bc$.

Inverse Er is voor elke a een a^{-1} zodat $aa^{-1} = 1 = a^{-1}a$.

Eindige lichamen, ook wel 'Galois field' in het Engels, hebben een eindig aantal elementen.

Stelling 2.1. *Een lichaam heeft karakteristiek* 0 *respectievelijk* p *priem als het kleinste deellichaam isomorf is met* $\mathbb{Q}$ *of* $\mathbb{Z}/p\mathbb{Z}$. *[5, p.66]*

Het is evident dat een eindige verzameling niet $\mathbb{Q}$ kan bevatten, dus een eindig lichaam heeft karakteristiek p. Dus $\mathbb{F}$ is een eindig dimensionale uitbreiding, zeg n, van $\mathbb{Z}/p\mathbb{Z}$ en hieruit volgt dan het aantal elementen in $\mathbb{F} = p^n$ en het lichaam dat hierbij hoort bestaat altijd en is uniek op isomorfie na.
Een klein voorbeeld is $\mathbb{F}_3$, we hebben dan de elementen $0, 1$ en 2. Er geldt $1 + 2 = 3 \mod (3) = 0$ dus 2 is de inverse van 1 onder optelling. Ook $2 \cdot 2 = 4 \mod (3) = 1$, dus 2 is de inverse van 2 onder vermenigvuldiging.

2.2 Polynomen

De polynomen in eindige lichamen werken hetzelfde als polynomen in andere lichamen als $\mathbb{Q}$ of $\mathbb{R}$. De coëfficienten van het polynoom zijn nu elemnenten van $\mathbb{F}_q$, de verzameling van al deze polynomen noteren we met $\mathbb{F}_q[X]$.

De algemene form van een polynoom in één variabele is

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

of voor een polynoom in twee variabelen

$$f(x, y) = a_{n,0}x^n + a_{n-1,1}x^{n-1}y + \ldots$$

waarbij a_i of $a_{i,j}$ coëfficiënten in het eindige lichaam zijn.

De graad van een polynoom is de hoogst voorkomende macht. Voor polynomen in meerdere variabelen bedoelen we met de graad de totale graad, dat is de hoogste som van alle machten in een term.

2.3 Möbius inversie

In de bewijzen voor het aantal irreducibele polynomen gebruiken we enkele keren de Möbius inversie. Dit is een stelling die ons een voorschrift voor $f(n)$ geeft als we weten dat $F(n) = \sum_{d|n} f(d)$, waarbij f en F bekende functies zijn met als domein de gehele getallen.
Er wordt dan gebruik gemaakt van de Möbius functie die we noteren als $\mu(n)$. Deze is als volgt gedefinieerd: $\mu(1) = 1, \mu(a) = 0$ als a deelbaar is door een kwadraat groter dan 1 en voor $p_1, ..., p_m$ verschillende priemgetallen geldt $\mu(p_1 \cdots p_m) = (-1)^m$. Verder is de functie multiplicatief, dus $\mu(ab) = \mu(a)\mu(b)$ als a, b copriem zijn.[6, p.18]

Stelling 2.2 (Möbius inversie)**.** *Zij* f *een arithmetic functie en* F *gedefinieerd door*

$$F(n) = \sum_{d|n} f(d).$$

Dan geldt voor elke $n \in \mathbb{N}$,

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d}).$$

Bewijs Allereerst merken we op dat $\sum_{d|n} \mu(d) = 1$ als $n = 1$ en $\sum_{d|n} \mu(d) = 0$ als $n > 1$. Het eerste geval is eenvoudig, de enige delers van 1 is 1 zelf en $\mu(1) = 1$. Als $n > 1$ dan laat $p_1, \ldots, p_k$ de priemfactoren van n zijn. Merk op dat als er een priemfactor twee maal voorkomt de Möbius functie voor deze deler nul is. Er volgt

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \ldots \mu(p_k) + \mu(p_1p_2) + \ldots + \mu(p_1 \cdots p_k) \\ &= 1 - \binom{k}{1} + \binom{k}{2} + \ldots + (-1)^k \binom{k}{k}\end{aligned}$$

Dit is de binomiaal ontwikkeling van $(1-1)^k = 0$ omdat $k \geq 1$
Nu laat $d' = \frac{n}{d}$ dan

$$\begin{aligned}\sum_{d|n} F(d)\mu(\frac{n}{d}) &= \sum_{d|n} F(\frac{n}{d})\mu(d) \\ &= \sum_{d|n}\sum_{i|d'} f(i)\mu(d) \\ &= \sum_{d,\ i;\ di|n} \mu(d)f(i) \\ &= \sum_{i|n}\sum_{d|\frac{n}{i}} \mu(d)f(i).\end{aligned}$$

Dan $\sum_{d|\frac{n}{i}} \mu(d) = 0$ tenzij $\frac{n}{i} = 1$, dus $i = n$ hieruit volgt dat

$$\sum_{d|n} F(d)\mu(\frac{n}{d}) = f(n).$$

3 Irreducibele polynomen in een variabele

Een polynoom noemen we irreducibel als deze niet te ontbinden is in twee niet constante polynomen.
Laat $\mathcal{I}_n$ de verzameling van alle irreducibele monische polynomen van graad n in een variabele zijn en $I_n = |\mathcal{I}_n|$.

Stelling 3.1. *Er geldt met boven staande notatie* $I_n = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d$.

Hierin is μ de Möbius functie.
We zullen twee bewijzen geven hiervoor, een met behulp van het inclusie en exclusie principe zoals ook in [1] en een met genererende functies zoals in [3].

3.1 Inclusie-exclusie principe

Voor polynomen met graad één is de uitspraak eenvoudig; alle polynomen van graad een zijn irreducibel en dus zijn er q, dit zijn alle opties voor de constante. Dit komt overeen met wat we vinden voor $n = 1$ in formule 3.1. Het is dus genoeg om te kijken naar de verzameling $\mathcal{R}_n$ van alle nulpunten van alle irreducibele polynomen van graad $n > 1$.
We doen eerste de volgende uitspraken over polynomen in eindige lichamen:

Claim 1. De nulpunten van een irreducibel polynoom zijn altijd verschillend

Zij $\alpha_1, \ldots, \alpha_n$ de nulpunten van een irreducibel polynoom f van graad n en K het uitbreidingslichaam dat al deze nulpunten bevat. Dan is f te schrijven als product van lineaire factoren over K en dus is de uitbreiding van K over $\mathbb{F}_q$ Galois. En dus bevat K n verschillende nulpunten van f.

Claim 2. Twee verschillende monisch irreducibele polynomen hebben geen gemeenschappelijke nulpunt.

De Galoisgroepen van de uitbreidingslichamen permuteren de alle nulpunten van de irreducibele polynomen. Als de polynomen een gemeenschappelijk nulpunt hebben dus volgt uit het permuteren van de nulpunten dat alle nulpunten een gemeenschappelijk nulpunt zijn. Maar een polynoom is op een constante factor na eenduidig vast gelegd door zijn nulpunten. Hieruit volgt dat twee irreducibele polynomen een gemeenschappelijk nulpunt hebben dan en slechts dan als gelijk zijn modulo $\mathbb{F}_q^*$.

Hieruit volgt $\mathcal{I}_n = \frac{1}{n}\mathcal{R}_n$. Nu zijn de elementen in $\mathcal{R}_n$ precies die elementen in $\mathbb{F}_{q^n}$ maar niet in een deellichaam van $\mathbb{F}_{q^n}$ zijn bevat, ofwel

$$\mathcal{R}_n = \{\alpha \in \mathbb{F}_{q^n} |\ [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n\},$$
$$\mathcal{R}_n = \{\alpha \in \mathbb{F}_{q^n} |\ \alpha \text{ niet in een echt deellichaam van } \mathbb{F}_{q^n}\}$$

Stel dat de priemontbinding van $n = u_1^{k_1}u_2^{k_2}u_3^{k_3}\cdots u_r^{k_r}$, met r verschillende priem getallen. Een lichaam $\mathbb{F}_{q^m}$ is een deellichaam van $\mathbb{F}_{q^n}$ als m deelt n. Zie ook afbeelding 1.
Dus de maximale deellichamen zijn van de vorm $\mathbb{F}_{q^{\frac{n}{u}}}$ met $u = u_1, u_2, \ldots, u_r$. Hier uit volgt dat

$$\mathcal{R}_n = \mathbb{F}_{q^n} / \cup_{i=1}^{r} \mathbb{F}_{q^{\frac{n}{u_i}}}.$$

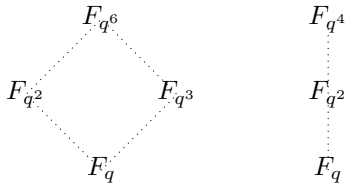


Figure 1: Twee verschillende manieren om $\mathbb{F}_q$ uit te breiden.

We kunnen nu met het inclusie-exclusie principe het aantal elementen van $\mathcal{R}_n$ berekenen.

$$\begin{aligned}|\mathcal{R}_n| &= |\mathbb{F}_{q^n}| - (\sum_{i=1}^{r} |\mathbb{F}_{q^{\frac{n}{u_i}}}|) + \sum_{i,j=1,i\neq j}^{r} |\mathbb{F}_{q^{\frac{n}{u_i}}} \cap \mathbb{F}_{q^{\frac{n}{u_j}}}| - \ldots (-1)^r |\mathbb{F}_{q^{\frac{n}{u_1 \cdot u_2 \cdots u_r}}}| \\ &= q^n - (\sum_{i=1}^{r} q^{\frac{n}{u_i}}) + \sum_{i,j=1,i\neq j}^{r} q^{\frac{n}{u_i \cdot u_j}} - \ldots + (-1)^r q^{\frac{n}{u_1 \cdot u_2 \cdots u_r}} \\ &= \sum_{d|n} \mu(\frac{n}{d}) q^d.\end{aligned}$$

3.2 Genererende functies

Laat z een formele variabele, dat wil zeggen, we gebruiken z als een boekhoudkundig hulpmiddel.
Als $\mathcal{N}$ de verzameling is met alle monische polynomen dan is elk element in deze verzameling uniek te schrijven als het product van monische irreducibele polynomen in $\mathcal{I}$.
We definiëren de volgende generende functies:

$$\begin{aligned}N(z) &= \sum_{f\in\mathcal{N}} z^{\deg f} = \sum_{n\geq 1} \mathcal{N}_n z^n, \\ I(z) &= \sum_{f\in\mathcal{I}} z^{\deg f} = \sum_{n\geq 1} \mathcal{I}_n z^n.\end{aligned}$$

Merk op dat er maar één monisch polynoom van graad nul is, namelijk het constante polynoom 1. Elk polynoom f kan geschreven worden als product van irreducibele polynomen. Stel nu dat $g_1, g_2, \ldots$ alle irreducibele polynomen zijn, dan volgt

$$\begin{aligned}1 + N(z) &= 1 + \sum_{f\in\mathcal{N}} z^{\deg f} \\ &= \sum_{m_1,m_2,\ldots\geq 0} z^{\deg(g_1^{m_1} g_2^{m_2} \ldots)} = \sum_{m_1,m_2,\ldots\geq 0} z^{\deg(g_1^{m_1}) + \deg(g_2^{m_2}) \ldots} \\ &= \left(\sum_{m_1\geq 0} z^{\deg\,(g_1^{m_1})}\right)\left(\sum_{m_2\geq 0} z^{\deg\,(g_2^{m_2})}\right)\ldots \\ &= \prod_{g\in\mathcal{I}} \sum_{m\geq 0} z^{\deg\, g^m} = \prod_{g\in\mathcal{I}} \sum_{m\geq 0} z^{m \deg\, g} = \prod_{g\in\mathcal{I}} \sum_{m\geq 0} \left(z^{\deg\, g}\right)^m \\ &= \prod_{g\in\mathcal{I}} \frac{1}{1 - z^{\deg\, g}}.\end{aligned}$$

Nu voor elke $n \geq 1$ geldt dat $\frac{1}{1-z^{\deg\, g}}$ zo vaak voorkomt als het aantal $g \in \mathcal{I}_n$, en merkt op dat z een formele variabele is, dus

$$1 + N(z) = \prod_{n\geq 1} \left(\prod_{g\in\mathcal{I}_n} \frac{1}{1 - z^n}\right) = \prod_{n\geq 1} \frac{1}{(1 - z^n)^{\mathcal{I}_n}}.$$

Door de logaritme te nemen vinden we:

$$\log(1 + N(z)) = \sum_{n\geq 1} -I_n \log(1 - z^n).$$

Omdat $N_n = q^n$ geldt $1 + N(z) = 1 + \sum_{n\geq 1} q^n z^n = \frac{1}{1-qz}$. Dus met het voorgaande en de reeksontwikkeling

van $\log 1 + x = \sum_{m\geq 1} \frac{(-1)^{m-1}}{m}(x)^m$ volgt

$$\log \frac{1}{1-qz} = \sum_{n\geq 1} -I_n \log(1-z^n)$$
$$-\log(1-qz) = \sum_{n\geq 1} -I_n \left(\sum_{m\geq 1} \frac{(-1)^{m-1}}{m}(-z^n)^m \right)$$
$$-\sum_{m\geq 1} \frac{(-1)^{m-1}}{m}(-qz)^m = \sum_{n\geq 1}\sum_{m\geq 1} -I_n \frac{(-1)^{m-1}}{m}((-z^n)^m),$$

de min tekens aanbeide zijde vallen tegen elkaar weg en we nemen nu aanbeide zijde de coëficiënt van$n[z^k,]$

$$\frac{1}{k}(q)^k = \sum_{m|k} I_{k/m}\frac{1}{m}$$
$$q^k = \sum_{d|k} I_d d$$
$$I_n = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})q^d.$$

Dan kunnen we de Möbius inversie toepassen en vinden we $I_n = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})q^d$ zoals we wilden.

3.3 Verhouding

De verhouding tussen alle polynomen en de irreducibele van graad n is

Stelling 3.2. $\frac{I_n}{N_n} \sim \frac{1}{n}$

Bewijs De formule 3.1 is ook te schrijven als $\mathcal{I}_n = \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{n/2}}{n}\right)$. Voor grote n is $q^{n/2}$ veel kleiner dan q^n. Dus $\frac{I_n}{N_n} = \frac{I_n}{q^n} \sim \frac{1}{n}$.

We merken op dat het aantal irreducibele polynomen steeds schaarser wordt als de graad hoger wordt.

4 Irreducibele polynomen in meerdere variabelen

Voor polynomen in meer variabelen is het lastiger iets te zeggen over het totale aantal irreducibele polynomen. Von zur Gathen geeft de uitdrukkingen voor het aantal reducibele polynomen tot graad 6,[2, p.948] deze zijn lang en hebben geen gemakkelijke uitdrukking. Maar we kunnen het probleem op de zelfde manier benaderen als in 3.2 met generende functies benaderen. We kijken in het bijzonder naar polynomen in twee variabelen maar merken op dat het bewijs voor hogere aantallen op de zelfde manier te vinden is.
Allereerst moeten we bepalen wat een monisch polynoom in meerdere variabelen is. De hoogste macht is niet eenduidig. Daarom kijken we naar de polynomen modulo $\mathbb{F}^*$, dit zijn alle eenheden in $\mathbb{F}$ en omdat we met een lichaam te maken hebben, heeft zijn dit alle elementen ongelijk aan 0. Dan geldt dat net als met polynomen in een variabel dat de vermenigvuldiging van twee polynomen opnieuw monisch is. Verder bedoelen we met de graad van een polynoom met de meerdere variabelen de totale graad, dat is het hoogste totaal van exponenten.
Het aantal polynomen in twee variabelen van graad ten hoogste n is q^{b_n} waarin $b_n = \binom{2+n}{2} = \frac{(n+2)(n+1)}{2}$. Namelijk het polynoom heeft de vorm $f(x,y) = \sum_{u+v\leq n} ax^u y^v$, dus voor iedere combinatie van u en v die voldoen is er opnieuw een a te kiezen uit F_q. Dit zijn $\binom{2+n}{n}$. Het aantal de monische polynomen van precies graad n zijn dan

$$N_n = \frac{q^{b_n} - q^{b_{n-1}}}{q-1}.$$

We defineren opnieuw de generende functies

$$N(z) = \sum_{n\geq 1} N_n z^n, \quad I(z) = \sum_{n\geq 1} I_n z^n.$$

Er geldt opnieuw

$$1 + N(z) = \prod_{n\geq 1} \frac{1}{(1-z^n)^{I_n}},$$

omdat we nog steeds naar alle machten van irreducibele polynomen kunnen kijken.
Laat nu op de zelfde wijze als in 3.2

$$L(z) = \log(1+N(z)) = \sum_{n\geq 1} -I_n \log(1-z^n) = \sum_{n\geq 1} \frac{I(z^n)}{n}.$$

Allereerst kijken we naar de cofficinten van z^m, we schrijven $[z^n]L(z)$ voor de cofficint van z^n in $L(z)$. Merk op dat

$$L(z) = \sum_{n\geq 1} \frac{I(z^n)}{n} = \sum_{n\geq 1} \frac{1}{n} \sum_{i\geq 1} I_i (z^n)^i = \sum_{n\geq 1} \sum_{i\geq 1} \frac{I_i}{n} z^{ni}.$$

We nemen aan beide zijde de coëfficient van z^m, rechts moeten we dus alle combinaties van n en i nemen zodat $n \cdot i = m$. Laat $n \to m/i$,

$$[z^m]L(z) = \sum_{i|m} i\frac{I_i}{m}$$
$$m[z^m]L(z) = \sum_{d|m} dI_d.$$

De möbius inversie hierop toegepast geeft

$$nI_n = \sum_{d|n} d[z^d]\mu(\frac{n}{d}).$$

Dus $I_n = \sum_{d|n} \frac{d}{n}[z^d]\mu(\frac{n}{d}) = \sum_{i|n} i[z^{n/i}]\mu(i)$.
Om nu iets over I_n te kunnen zeggen in absolute waarden merken we op dat

$$[z^n]L(z) = [z^n]\log(1+N(z)),$$

door deze te ontwikkelen vinden we

$$[z^n]L(z) = [z^n](N(z) - \frac{1}{2}N(z)^2 + \frac{1}{3}N(z)^3 - \ldots).$$

De eerste is eenvoudig, $[z^n]N(z)$ is precies N_n.
Voor een benadering van $N(z)^2$ vinden we

$$\begin{aligned}[z^n]N(z)^2 = [z^n](N_1z + N_2z^2 + \ldots)^2 = [z^n]\sum_{k\geq 1}\left(N_k^2 z^{2k} + \sum_{i+j=k, i\neq j} N_iN_jz^k\right)\\ = N_1N_{n-1} + N_2N_{n-2} + N_3N_{n-3} + \ldots.\end{aligned}$$

De term N_1N_{n-1} is $\left(\frac{q^{b_n}-q^{b_{n-1}}}{q-1}\right)\left(\frac{q^{b_n}-b_0}{q-1}\right)$ en deze is dus van orde $q^{b_{n-1}+b_1-2} = q^{(n+1)n/2+1}$.
Voor de tweede term vinden we op gelijke wijze $N_2N_{n-2} = \frac{(q^{b_2}-q^{b_1})(q^{b_{n-2}}-q^{b_{n-3}})}{(q-1)^2}$ en deze is dus van de orde $\frac{q^{b_2+b_{n-2}}}{q^2} = q^{b_2+b_{n-2}-2}$.
Voor een willekeurige term $N_{n-i}N_i$ kunnen we dus de orde uitdrukken als $q^{b_{n-i}+b_i+2}$. We kunnen deze macht uitwerken en opzoek gaan naar het maximum:

$$\begin{aligned}b_{n-i} + b_i + 2 &= (n-i+2)(n-i+1)/2 + (i+2)(i+1)/2 - 2\\ &= i^2 - ni + \frac{1}{2}n(n+3).\end{aligned}$$

Dit is een kwadratische functie in i met een minimum in $i = \frac{1}{2}n$. De grootse waardes zijn dus voor i of $n-i$ klein, verder is de functie strikt dalend bij $i < n/2$ en strikt stijgend bij $i > n/2$, dus als i kleiner is dan de helft van de graad dan is de term $N_{n-(i-1)}N_{i-1}$ van strikt grotere orde dan $N_{n-i}N_i$. Merk verder op dat de term $N_{n-2}N_2$ pas verschillend is van de eerste vanaf graad 4, dus voor $n \geq 4$ geldt:

$$[z^n]N(z)^2 = \frac{1}{2}(2N_1N_{n-1} + \mathcal{O}(q^{b_{n-2}+b_2-2})).$$

Voor de term van $[z^n]N(z)^3$ merken we op dat $N_iN_jN_{n-i-j}$ van de orde $q^{b_i+b_j+b_{n-i-j}-3}$ is. We vinden dan

$$\begin{aligned}b_i + b_j + b_{n-i-j} - 3 &= \frac{(i+2)(i+1)}{2} + \frac{j+2)(j+1)}{2} + \frac{(n-i-j+2)(n-i-j+1)}{2} - 3\\ &= \frac{1}{2}((3-2n)i + (3-2n)j + 2ij + n^2 + 3).\end{aligned}$$

Alleen als $n \geq 3$ is, is het nodig deze term te bekijken. Als dus $n \geq 3$ dan volgt dat voor groter wordende i de som kleiner wordt en het zelfde voor groter wordende j want $2ij \leq 2((n-1)/2)^2$.

En dus vinden we

$$\begin{aligned}[z^n]L(z) &= N_n - \frac{1}{2}(2N_1N_{n-1} + \mathcal{O}(q^{b_{n-2}+b_2-2})) + \mathcal{O}(q^{b_{n-2}+b_2-2})\\ &= N_n - N_1N_{n-1} + \mathcal{O}(q^{b_{n-2}+b_2-2}).\end{aligned}$$

Samen met de uitdrukking voor I_n geeft dit:

$$\begin{aligned}I_n &= \sum_{i|n}\mu(i)\,[z^{n/i}]L(z)\\ &= \mu(1)\,[z^n]L(z) + \sum_{i|n, i\neq 1}\mu(i)\,[z^{n/i}]L(z)\\ &= N_n - N_1N_{n-1} + \mathcal{O}(q^{b_{n-2}+b_2-2}) + \mathcal{O}(q^{b_{n-2}})\\ &= N_n - N_1N_{n-1} + \mathcal{O}(q^{b_{n-2}+b_2-2}).\end{aligned}$$

We hebben nu de volgende gelijkheiden aangetoond:

Stelling 4.1. $I_n = \sum_{k|n}\frac{\mu(k)}{k}\log(1+N(z))$,
$\mathcal{I}_n = \mathcal{N}_n - N_1 \cdot N_{n-1} + O(q^{b_{n-2}+b_2-2})$.

4.1 Verhouding

Met de laatste vergelijking kunnen we de verhouding van de irreducibele polynomen van graad n afschatten. Namelijk voor n relatief veel groter dan q geldt:

$$\frac{I_n}{N_n} \sim \frac{N_n - N_1 N_{n-1}}{N_n} = 1 - \frac{N_1 N_{n-1}}{N_n}.$$

Nu N_1 is een constante voor elke q, namelijk $N_1 = \frac{q(q^2-1)}{(q-1)} = q^2 + q$. En

$$N_{n-1}/N_n = \frac{q^{b_{n-1}-b_{n-2}}}{q^{b_n-b_{n-1}}} \sim \frac{q^{b_{n-1}}}{q^{b_n}} = \frac{q^{(n+1)n}}{q^{(n+2)(n+1)}} = q^{-n-1}.$$

Dus de orde van $\frac{I_n}{N_n} \sim 1-q(1-n)$, de verhouding irreducibele polynomen nadert 1. Dit is het tegenovergesteld als we voor polynomen in één variabele vonden.

Veder merken we op dat het aantal reducibele polynomen voornamelijk polynomen zijn die een lineaire factor hebben. Want in de tweede gelijkheid van stelling 4.1 in de bijdrage van functie in de form $f = g \cdot h$ met $g \in \mathcal{N}_1$ en $h \in \mathcal{N}_{n-1}$ van de hoogste orde.

4.2 Absoluut en rationele irreduciblititeit

Er zijn twee soorten irriducibiliet te onderscheiden: rationaal en absoluut. Een polynoom f is rationaal irreducibel als en geen $g,\ h \in \mathbb{F}_q[X]_{n\geq 1}$ bestaan zodat $f = g \cdot h$. We noemen f absoluut irreducibel als er ook geen zulke $g,\ h$ bestaan over een uitbreidingslichaam. Dus de absolute reducibele polynomen bevatten ook de rationale. Een voorbeeld in $\mathbb{F}_3$ is bijvoorbeeld $f = x^2 + 1$, dit polynoom heeft geen nulpunten in $\mathbb{F}_3$ en is dus irreducibel in dit lichaam. Maar het is wel reducibel in $\mathbb{F}_3(\sqrt{2})$, want dan $f = (x-\sqrt{2})(x+\sqrt{2})$.

Polynomen in één variabele zijn nooit absoluut irreducibel als de graad van het polynoom groter of gelijk is aan twee. In dat geval is er namelijk een nulpunt α in een uitbreidingslichaam en kunnen we $x - \alpha$ uit het polynoom factoriseren.

Absoluut irreducibiliteit voor meerdere variabelen is lastiger te bepalen. We verwijzen hier voor naar een artikel van Fredman [4] waarin hij een stelling bewijs over het aantal absoluut irreducibele polynomen in twee variabelen ten opzichte van het aantal rationeel irreducibele en het totaal aantal polynomen.

5 Singuliere polynomen

Een polynoom $f(x,y)$ heeft een een singulier punt $P=(\tilde{x},\tilde{y})$ als geldt:

$$\begin{aligned} f(\tilde{x},\tilde{y}) &= 0,\\ f_x(\tilde{x},\tilde{y}) &= 0,\\ f_y(\tilde{x},\tilde{y}) &= 0. \end{aligned}$$

Met f_x, f_y de afgeleiden naar respectievelijk de eerste en tweede variabele. Een polynoom is singulier als het een singulier punt heeft. Hoewel de differentiaal voor continue functies is gedefinieerd, kunnen we in eindige lichamen ook kijken naar de afbeelding die dezelfde eigenschappen heeft als de differentiaal afbeelding. Dus voor een polynoom $f(x,y)=\sum_{n>1,\ m>1} a_{nm}x^n y^m$ is $\partial f/\partial x = \sum_{n>1,\ m>1} a_{nm} n x^{n-1} y^m$.

Wanneer de graad relatief groot is ten opzichte van de grote van het lichaam is het mogelijk een precieze uitdrukking te geven voor het aantal rationaal singuliere polynomen. We zullen zien dat de grens waarbij deze uitdrukking geldt $n=3q-2$ is. Vervolgens bekijken we een algemene afschatting voor polynomen vanaf graad 3. Tenslotte bekijken we de polynomen met graad kleiner dan 3 en we merken op dat we in dit geval ook iets kunnen zeggen over het aantal absoluut singuliere polynomen.
We noteren $\mathcal{S}_n$ voor de verzameling van alle rationale singuliere polynomen van graad kleiner dan n en $S_n = |\mathcal{S}_n|$.

5.1 Graad groter dan $3q-2$

Stelling 5.1 (Lenstra, 2006)**.** *Voor polynomen van twee variabelen in $\mathbb{F}_q$ is de verhouding singuliere polynomen*

$$\frac{S_n}{N_n} = 1-(1-q^{-3})^{q^2}$$

dan en slechts dan als $n \geq 3q-2$.

Merk op dat deze verhouding niet afhankelijk is van n, dus voor n groot genoeg veranderd de verhouding singuliere polynomen niet meer.

Bewijs. Laat $P=(u,v)\in\mathbb{F}_q^2$, dan is het ideaal $m_p=(x-u,y-v)\subseteq \mathbb{F}_[x,y]$ het maximale ideaal van P. En $s_P = m_P^2 = (x-u,y-v)^2 \subseteq \mathbb{F}_[x,y]$ het singulariteitsideaal. Deze bevat precies de polynomen die singulier zijn in P. De factor ring $\mathbb{F}_q[x,y]/s_P = \mathbb{F}+(x-u)\mathbb{F}+(y-v)\mathbb{F}$ is een driedimensionale vectorruimte over $\mathbb{F}$.

Voor twee verschillende punten P en Q in $\mathbb{F}_q^2$ zijn de maximale idealen m_P en m_Q comaximaal, dat wil zeggen $m_P+m_Q=\mathbb{F}_q[x,y]$. Voor twee $P=(u,v)\neq Q=(u',v')$ in $\mathbb{F}_q^2$ geldt dat of wel $u\neq u'$ of $v\neq v'$. Stel dan $u\neq u'$, dan geldt $(u-u')^{-1}((x-u)-(x-u')) = (u-u')^{-1}(u-u') = 1$ en dus is het ideaal m_P+m_Q de gehele polynoomring. Als $u=u'$ dan kunnen we dit argument geven voor $(y-v)-(y-v')$.
Ook s_P en s_Q zijn comaximaal, want voor $u\neq u'$ bekijk

$$\begin{aligned} ((x-u)-(x-u'))^3 &= (u-u')^3 \in \mathbb{F}_q^*\\ &= (x-u)^3-(x-u)^2(x-u')+(x-u)(x-u')^2-(x-u')^3. \end{aligned}$$

De eerste twee termen van de som zitten in s_P, de andere twee in $s_{P'}$. Zonder verlies van algemeenheid kunnen we dit ook voor $v\neq v'$doen, dus $s_P+s_{P'}$ bevat een eenheid en daarmee zijn de idealen comaximaal. Uit de Chinese reststelling volgt

$$\mathbb{F}_q[x,y]/\prod_{P\in\mathbb{F}_q^2} s_P \cong \prod_{P\in\mathbb{F}_q^2} \mathbb{F}_q[x,y]/s_P.$$

Laat

$$\phi : \mathbb{F}_q[x,y] \to \prod_{P\in\mathbb{F}_q^2} \mathbb{F}_q[x,y]/s_P$$

$$\phi(f) \mapsto (f + s_{P_1}, \ldots, f + s_{P_i})$$

het product van canonieke ringhomomorfismes. Dan geldt f is singulier is in P dan en slechts dan als $f \in s_P$, en dus $(\phi(f))_n = 0$ want dan $(f + s_P)_n = 0$. En omgekeerd is f niet singulier als $(\phi(f)) \neq 0$ voor alle $P \in \mathbb{F}_q^2$. Met ϕ_n noteren de de restrictie van ϕ op polynomen van graad n of lager. Dan is de verzameling van alle niet singuliere polynomen $\mathbb{N}_n \backslash \mathbb{S}_n$ gelijk aan het inverse beeld van ϕ zonder 0, dus

$$\mathcal{N}_n \backslash \mathcal{S}_n = \phi^{-1} \left(\prod_{P \in \mathbb{F}_q^2} \mathbb{F}_q[x,y]/s_P \backslash 0 \right).$$

Voor elke P is $|\mathbb{F}_q[x,y]/s_P| = q^3$, want dit was een driedimensionale vectorruimte over $\mathbb{F}_q$. Dus

$$| \prod_{P \in \mathbb{F}_q^2} \mathbb{F}_q[x,y]/s_P \backslash 0| = (q^3 - 1)^{q^2}.$$

Merk op dat ϕ_n een lineaire afbeelding is van vectorruimtes over $\mathbb{F}_q$. Als de functie ϕ_n surjectief is dan volgt dat voor het teruggehaalde beeld van $\phi_n(f)$ geldt $|\{g \in (F)_n[x,y] \mid \phi(g) = \phi(f)\}| = q^{b_n - 3q^2}$. Want $\phi_n(g) = \phi_n(f)$ als beide functies gelijk zijn modulo elke s_P. Er geldt $|\prod_{P \in \mathbb{F}_q^2} \mathbb{F}_q[x,y]/s_P| = (q^3)^{q^2}$ en het totale aantal polynomen was q^{b_n} en nu $|\phi_n^{-1}(f)| = q^{b_n}/(q^{3q^2})$.
Dan is $|\mathcal{N}_n \backslash \mathcal{S}_n| = q^{b_n - 3q^2} \cdot (q^3 - 1)^{q^2}$, het product van het aantal punten maal het aantal elementen van deze inverse beelden.[8]
Er volgt $\mathcal{S}_n$ zijn de alle polynomen zonder de niet singuliere polynomen dus

$$\begin{aligned}
\frac{S_n}{N_n} &= \frac{|\mathcal{N}_n - (\mathcal{N}_n \backslash \mathcal{S}_n)|}{N_n} = 1 - \frac{|\mathcal{N}_n \backslash \mathcal{S}_n|}{N_n} \\
&= 1 - (q^{b_n - 3q^2}(q^3 - 1)^{q^2})(q^{b_n})^{-1} \\
&= 1 - (q^{-3q^2}(q^3 - 1)^{q^2}) \\
&= 1 - (q^{-3}(q^3 - 1))^{q^2} \\
&= 1 - (1 - q^3)^{q^2}.
\end{aligned}$$

Aan de andere kant, stel dat 5.1 geldt, dus er is een exacte verhouding tussen S_n en N_n met de waarde gegeven door 5.1. Deze verhouding is rationaal, met

$$1 - (1 - q^3)^{q^2} = \frac{q^{3q^2} - (q^3 - 1)^{q^2}}{q^{3q^2}} = \frac{S_n}{N_n}.$$

Deze breuk is volledig vereenvoudigd, want de noemer heeft als enige factor q, terwijl in de teller een veelvoud van q plus 1 staat. Hieruit volgt dat q^{3q^2} een deler is van N_n.
We merken op dat het beeld van $\phi_n(\mathcal{N}_n)$ alle polynomen zijn, bekeken modulo alle s_P. Even zo is het beeld van $\phi_n(\mathcal{S}_n)$ alle singuliere polynomen modulo alle s_P. Dus

$$\frac{|\mathcal{S}_n|}{|\mathcal{N}_n|} = \frac{|\phi_n(\mathcal{S}_n)|}{|\phi_n(\mathcal{N}_n)|},$$

en dan is q^{3q^2} ook een deler van $|\phi_n(\mathcal{N}_n)|$. Maar ook $|\prod_{P \in \mathbb{F}_q^2} \mathbb{F}_q[x,y]/s_P| = (q^3)^{q^2}$ en het beeld van ϕ_n is zeker bevat in zijn codomein, dus ϕ_n is surjectief.
Er rest ons dus te bewijzen wanneer de functie ϕ_n surjectief is.

De twee idealen $(x^q - x, y^q - y)$ en $\prod_{P \in \mathbb{F}_q^2} m_P$ zijn gelijk omdat de eerste in de tweede bevat is en de codimenties gelijk zijn.[2, p.966][1]

[1] We hebben geen sluitende redenering voor deze uitspraak maar hebben het vermoeden dat we op het linker ideaal Fermats kleine stelling kunnen toepassen.

We defineren het ideaal I door

$$I = \prod_{P\in\mathbb{F}_q^2} s_P = \prod_{P\in\mathbb{F}_q^2} m_P^2 = \left(\prod_{P\in\mathbb{F}_q^2} m_P\right)^2 = (x^q - x, y^q - y)^2.$$

We kunnen $\mathbb{F}_q[x, y]$ beschouwen als een vectorruimte over $\mathbb{F}_q$ door elke $x^i y^j$ als een basisvector te beschouwen, we noemen deze ruimte W. Laat W_n de vectorruimte van alle polynomen met graad lager dan n, W_n heeft dan een basis gegeven door

$$\mathcal{B} = \{x^i y^j |\ i + j \leq n\}.$$

Deze basis heeft $\frac{(n+1)(n+2)}{2}$ vectoren.
We kunnen ook $\mathbb{F}_q[x, y]/I$ bekijken als een vectorruimte over $\mathbb{F}_q$, we noteren deze met V_I. Een basis voor deze ruimte is

$$\mathcal{B}_I = \{x^i y^j |\ (0 \leq i \leq 2q \text{ en } 0 \leq j \leq q) \text{ of } (0 \leq i \leq q \text{ en } 0 \leq j \leq 2q)\}.$$

Het aantal elementen in deze basis is $3q^3$.

Stel voor een polynoom in $x^k y^l \in \mathbb{F}_q[x, y]$ geldt dat als $k \geq 2q$, dan kunnen we een factor $(x^q - x)^2 = x^{2q} - 2x^{q+1} + x^2$ weg delen door

$$x^k y^l = x^{k-2q} y^l (x^q - x)^2 + 2x^{q+1} y^l - x^2 y^l.$$

Voor $l \geq 2q$ kunnen we al vergelijkbare wijze en factor $(y^2 q - x)^2$ weg delen. Als $k \geq q$ en $l \geq q$ kunnen we een factor $(x^q - x)(y^q - q)$weg delen door

$$x^k y^l = (x^{k-q} y^{l-q} (x^q y^q - x^q y - x y^q + xy)) + x^k y^{l-q+1} + x^{k-q+1} y^l - x^{k-q+1} y^{l-q+1}.$$

Op deze manier kunnen we dus een willekeurig polynoom $f = \sum_{i+j\leq n} a_{ij} x^i y^j$ schrijven als een polynoom in $\mathbb{F}_q[x, y]/I$.

Er geldt nu im $(\phi_n) = V_I \cap W_n$. Want zeker voor een willekeurige $f = x^i y^j \in V_I \cap W_n$ geldt $f \in V_I$, dus niet singulier en dus $f = \phi_n(f) \in$ im (ϕ_n). Zij $f = x^i y^j \in W_n$ met $i \geq 2q$, dan kunnen we met het reductieproces zoals we hierboven beschreven hebben concluderen dat f congruent is aan een lineaire combinatie van polynomen in V_I. Hieruit volgt dat dim im $\phi_n =$ dim $V_I \cap W_n$ en omdat deze beide eindig zijn volgt im $(\phi_n) = V_I \cap W_n$.
We wisten al dat wanneer ϕ_n surjectief is dat dan im (ϕ_n) een vectorruimte van dimensie $3q^2$ opspant. Dus moet ook gelden dim $V_I = 3q^2 =$ dim V_I, en dus $W_n \subseteq V_I$. Uit dit laatste volgt $n \geq 3q + 2$, hetgene wat we wilden bewijzen.
Om de laatste equivalentie inzichtelijk te maken verwijzen we naar afbeelding **??**. Op de horizontale as staan de exponenten van x en op de verticale as die van y. Het grijze gebied zijn de basis factoren die V_I opspannen. De lijn van $(0, n)$ tot $(n, 0)$ geeft de exponenten die W_n opspannen. Als $V_I \subseteq W_n$ dan moest dus gelden $(2q - 1) + (q - 1) = 3q - 2 \leq n$.

5.2 Benadering voor kleine graad

Als $n < 3q-2$ kunnen we geen eenvoudige algemene uitdrukking vinden voor het aantal singuliere polynomen. We kunnen wel een afschatting vinden, gegeven door:

Stelling 5.2. *Voor $n \geq 3$ geldt*

$$\frac{1}{q} - \frac{1}{2q^2} \leq \frac{S_n}{N_n} \leq \frac{1}{q}.$$

We gebruiken dezelfde notatie als boven. Zeker geldt dat het totale aantal singuliere polynomen kleiner is dan de som van alle singuliere polynomen van elk punt. Het aantal singuliere polynomen in een wilekeurig punt P in $\mathbb{F}_q^2$ is $|\mathcal{N}_n \cap s_P| = q^{b_n - 3}$. Want s_P was een driedimensionale vectorruimte over $\mathbb{F}_q$. Hieruit volgt dat het aantal singuliere polynomen kleiner is dan $q^2 \cdot q^{b_n - 3} = q^{-1} q^{b_n} = \frac{1}{q}|\mathcal{N}_n|$.

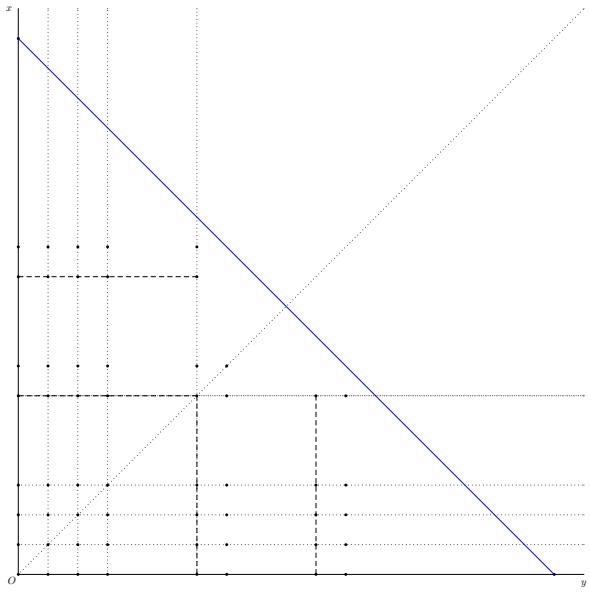


Figure 2: Een visualisatie van de basissen van de vectorruimtes V_I, ruimte binnen de onderbroken lijn, en W_n de ruimte binnen de blauwe lijn. De punten staan voor de basisvector $x^i y^j$, met op de verticale as de macht van de x component en op de horizontale as de y component. De onderbroken lijnen staan op de plaatsen waar de machten van gelijk zijn aan $q-1$ en $2q-1$.

Verder is het aantal singuliere polynomen groter dan het aantal polynomen met precies één singulier punt, dat zijn alle singuliere polynomen zonder de polynomen met meer dan één singulierpunt, oftewel:

$$\sum_{P\in\mathbb{F}_q^2} |\mathcal{N}_n \cap s_P| - \sum_{\substack{P,P'\in\mathbb{F}_q^2,\\ P\neq P'}} |\mathcal{N}_n \cap s_P \cap s_{P'}|.$$

De eis dat een polynoom singulier is in twee verschillende punten komt over een met een stelsel van 6 lineaire vergelijkingen, welke opgelost moet worden voor de coëfficienten van het polynoom. De maximale oplossingsruimte heeft dan dimensie 6. We wisten al dat de polynomen met een singulierpunt in s_P een driedimensionale ruimte opspannen, ofwel de eerste en laatste drie vergelijkingen zijn onderling lineair onafhankelijk. Het rest ons dus te kijken of de eerste en laatste drie onderling onafhankelijk zijn.

Stel nu $P=(u,v)\neq P'=(u',v')$, $n\geq 3$, $a_{ij}\in\mathbb{F}_q$ en laat $f=\sum_{2\leq i+j\leq n} a_{ij}(x-u)^i(y-v)^j$. Dan is de graad van f ten hoogste n en $f\in s_P$.
Om voor f nu singulier te zijn in s_P en $s_{P'}$ moet gelden

$$\begin{aligned} f(u',v') = 0 &= \sum_{2\leq i+j\leq n} a_{ij}(u'-u)^i(v'-v)^j,\\ \frac{\partial}{\partial x}f(u',v') = 0 &= \sum_{2\leq i+j\leq n} a_{ij}i(u'-u)^{i-1}(v'-v)^j,\\ \frac{\partial}{\partial y}f(u',v') = 0 &= \sum_{2\leq i+j\leq n} a_{ij}j(u'-u)^i(v'-v)^{j-1}. \end{aligned}$$

Als we nu alleen kijken naar de coëficienten $a_{11},\ a_{20},\ a_{30}$ dan kunnen we de volgende matrix opstellen:

$$\begin{pmatrix} (u-u')(v-v') & (u-u')^2 & (u-u')^3\\ (v-v') & 2(u-u') & 3(u-u')^2\\ (u-u') & 0 & 0 \end{pmatrix}.$$

Door te ontwikkelen naar de onderste rij vinden we dat de determinant gelijk is aan $-(u-u')^5$. Als $u \neq u'$ dan is de determinant van deze matrix niet nul, dus de codimensie van de vectorruimte $\mathbb{F}_q[x,y] \cap s_P \cap s_{P'}$ in de vectorruimte $\mathbb{F}_q[x,y] \cap s_P$ is de rang van de matrix, dus 3.
Als $u = u'$ dat kunnen we zonder verlies van algemeenheid dit argument ook geven voor $v \neq v'$.

Hieruit volgt dat de vergelijkingen allemaal lineair onafhankelijk zijn en dus dat de codimensie van $\mathbb{F}_q[x,y] \cap s_P \cap s_{P'}$ over $\mathbb{F}_q[x,y]_{\leq n}$ gelijk is aan 6. Voor de punten P en P' zijn er $\binom{q^2}{2} = \frac{q^2(q^2-1)}{2}$ keuzes. Daarmee is het aantal polynomen dat maar één singulierpunt heeft $\frac{q^4-q^2}{2} \cdot q^{b_n-6}$. En dus is de verhouding van het aantal singuliere polynomen

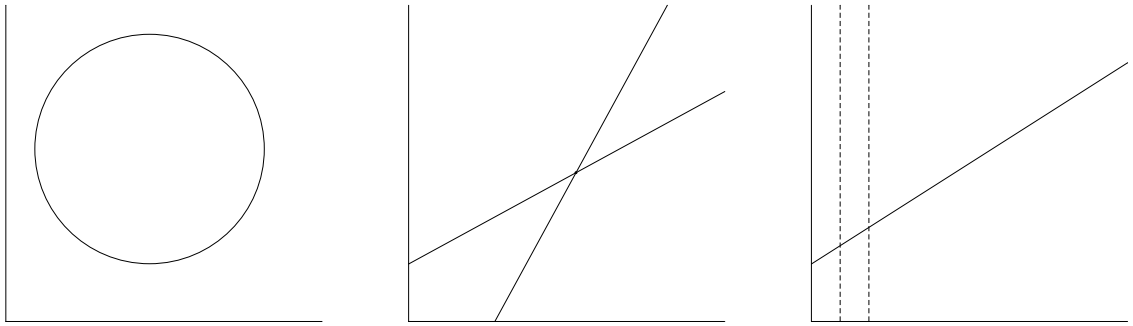
$$\frac{S_n}{N_n} \geq q^{-b_n}|\{\text{polynomen met tenminste één singulierpunt}\}| - |\{\text{polynomen met tenminste twee singulierepunten}\}|$$
$$= q^{-b_n}(q^2 q^{b_n-3} - \frac{q^4-q^2}{2} \cdot q^{b_n-6}) = \frac{1}{q} - \frac{1}{2q^2} + q^{-4}/2 \geq \frac{1}{q} - \frac{1}{2q^2}.$$

5.3 Graad kleiner dan 3

Voor polynomen met graad nul, de constante polynomen, is het enige singuliere polynoom het nulpolynoom. Want dan heeft de vergelijking $f(P) = 0$ een oplossing, namelijk alle P en dus zijn er q^2 singuliere punten. In de andere gevallen $f(P) \neq 0$ voor alle P. Er is dus één singulier polynoom onder de constante polynomen, zowel rationaal als absoluut.

Voor polynomen met graad één zijn er geen singuliere polynomen. In dit geval zijn er geen oplossingen voor $\frac{\partial f}{\partial x}(P) = a_{10} = 0$ of $\frac{\partial f}{\partial y}(P) = a_{01} = 0$ als a_{10} en a_{01} niet nul zijn, als beide wel nul zijn is het geen eerste graad polynoom. Dit geldt voor zowel rationaal als absoluut.

Voor polynomen van graad 2 bekijken we de drie gevallen waaruit zo een polynoom kan bestaan. Namelijk dat het glad is, het ontbind in twee lineaire vergelijkingen over het lichaam of het ontbindt over een uitbreidingslichaam. Wanneer een polynoom ontbindt in twee lineaire polynomen kunnen we daar de gevallen onderscheiden dat deze twee dezelfde zijn of niet, oftewel, het polynoom is een kwadraat of niet. In figuur 3 staan deze gevallen.



(a) Een glad polynoom.

(b) Een polynoom dat in twee lineaire factoren ontbind.

(c) Een polyoom dat is twee gelijke lijnen ontbind.

Figure 3: De verschillende gevallen van kwadratische polynomen in twee variabelen over $\mathbb{F}_q$.

Figuur 3 is een visualisatie van de gevallen die kunnen voorkomen door de polynomen in de projectieve ruimte te bekijken. Hierin identificeren we de eindpunten van het assenstelsel met elkaar, dus het punt $(u,q) = (u,0)$ en $(q,v) = (0,v)$. Dit figuur hebben we op de horizontale as de x-coördinaat, de verticale as de y-coördinaat. In het eindige lichaam bestaan alleen punten, maar om de polynomen inzichtelijk te maken hebben we de

punten verbonden met lijnen.

Polynomen die een singulierpunt hebben, hebben een nulpunt en zijn dus te ontbinden in $\mathbb{F}_q$. Dit is het geval van figuur 3a, het polynoom is glad en er is geen punt waarop zowel de x als y-richting horizontaal is, en dus de afgeleide naar x en y gelijkertijd = nul is.

Voor een polynoom dat ontbindt in twee lineaire polynomen geldt dat als het een singulier punt heeft ook de twee polynomen waarin het ontbindt op dat punt een nulpunt hebben. Stel namelijk van niet en laat $f = gh \neq 0$ een polynoom met g, h twee lineaire polynomen en P een singulier punt van f. Dan uit $f(P) = 0 = g(P)h(P)$ volgt dat of $g(P) = 0$ of $h(P) = 0$. Laat zonder verlies van algemeenheid $h(P) = 0$ en $g(P) \neq 0$. Uit dit samen met

$$\frac{\partial f}{\partial x}(P) = \frac{\partial g}{\partial x}(P)h(P) + \frac{\partial h}{\partial x}(P)g(P) = 0$$

volgt dan $g(P) = 0$ of $\frac{\partial h}{\partial x}(P) = 0$. We hadden aangenomen dat $g(P) \neq 0$ dus de afgeleide van h in P moet dan nul zijn. Op vergelijkbare wijze volgt uit

$$\frac{\partial f}{\partial y}(P) = \frac{\partial g}{\partial y}(P)h(P) + \frac{\partial h}{\partial y}(P)g(P) = 0$$

dat $g(P) = 0$ of $\frac{\partial h}{\partial y}(P) = 0$. Als nu $g(P) \neq 0$ volgt dat het punt P een singulier punt van h is, maar h was een lineair polynoom. Deze heeft geen singulier punt tenzij dit het nulpolynoom is. Maar dan zou ook f gelijk zijn aan nul en dit geeft een tegenspraak. Dus $g(P) = h(P) = 0$ voor een singulier punt van f.

We bekijken nu alle combinaties van waarop een polynoom in twee lineaire factoren kan worden ontbonden. Allereerst de polynomen die in twee gelijke lijnen ontbinden. We kunnen deze beschrijven door de punten waar hij twee verticale lijnen snijdt, bijvoorbeeld de lijnen $x = 0$ en $x = 1$. Er zijn q mogelijkheden om de eerste lijn te snijden en nog een q om de tweede te snijden, dit geeft ons q^2 mogelijkheden. Daar moeten we nog de verticale lijnen bij optellen, dit zijn er q. Al deze polynomen kunnen we nu vermenigvuldigen met een constante in $\mathbb{F}_q^*$ en dit geeft een nieuw polynoom. Dus voor dit geval zijn er in totaal $(q-1)(q^2+q) = q^3 - q$ polynomen en elk heeft q singuliere punten.

Voor het geval waar f in twee niet gelijke lijnen ontbindt over $\mathbb{F}_q$ merken we op dat er q^2 mogelijkheden zijn voor het singuliere punt en dus ook voor het snijpunt van deze lijnen. Zie ook afbeelding 3b. In het snijpunt zijn beide polynomen gelijk en uit de redenatie boven volgt dat het singuliere punt op dit snijpunt moet liggen. Deze lijnen hebben ook niet meer dan één snijpunt, dus hebben de bijbehorende polynomen één singulier punt.
Voor elke lijn zijn er $q+1$ richtingen, net als bij het geval van dubbele lijnen zijn er q punten voor de volgende x-coördinaat en de verticale lijn. Het totale aantal combinaties zijn in dit geval $q^2\binom{p+1}{2}$. Bij elke combinatie horen opnieuw $q-1$ polynomen. Het totale aantal is dus $q^2\frac{(p+1)q}{2}(p-1) = \frac{1}{2}(q^5 - q^3)$.

Het totale aantal rationaal singuliere polynomen tot en met graad 2 is dus $S_2 = \frac{1}{2}q^5 + \frac{1}{2}q^3 - q + 1$. Dit komt inderdaad niet overeen met 5.1. Maar ook

$$S_2/N_2 = \frac{\frac{1}{2}q^5 + \frac{1}{2}q^3 - q + 1}{q^6} \geq \frac{1}{2q},$$

dus ook stelling 5.2 geldt hier niet. Maar dan wel zeker

$$S_2/N_2 \leq \frac{1}{q}.$$

De ondergrens van 5.2 geldt dus voor alle $n \geq 2$.

5.4 Absoluut singuliere polynomen

Net als bij irreducibiliteit kunnen we twee soorten singulariteiten onderscheiden, namelijk rationaal en absoluut. In het geval dat een polynoom rationaal singulier is heeft het een singulierpunt in $\mathbb{F}_q^2$. In het absolute

geval ligt tenminste één coördinaat van het punt in een uitbreidingslichaam van $\mathbb{F}_q$. Eenvoudig te zien is dat een rationaal singulier polynoom ook zeker absoluut singulier is.

Net als bij irreducibiliteit merken we op dat voor constante en lineaire polynomen geen verschil is tussen beide varianten. In dit geval omdat een punt uit een uitbreidingslichaam geen nulpunt kan zijn van een lineair polynoom en voor een constant polynoom is nog steeds het nul polynoom het enige singuliere polynoom.

Het aantal absoluut singuliere polynomen van graad twee zijn de polynomen die ontbinden over een uitbreidingslichaam van $\mathbb{F}_q$. In dit geval is het kwadratische lichaam $\mathbb{F}_{q^2}$ het enige lichaam dat we moeten bekijken. Als f een singulierpunt P heeft in het uitbreidingslichaam dan volgt uit Galois theorie dat de lijn geconjugeerde $\hat{P}$ ook een singulierpunt is. We hebben dus te maken met een situatie zoals in figuur 3b maar waarbij het snijpunt in $\mathbb{F}_q^2$ ligt. We merken wel opdat als we alle punten tellen we de singuliere polynomen dubbel tellen opdam elk polynoom twee singuliere punten heeft, we delen de uitkomst dus door drie.
Er zijn voor de lijnen in het uitbreidingslichaam q mogelijkheden als richtingcoëfficiënt en dus vinden we in totaal $q^2\frac{q(q-1)}{2}(q-1) = \frac{1}{2}(q^5 - 2q^4 + q^3)$ absoluut singuliere polynomen zijn die niet rationeel zijn.

Dit geeft dat het totaal aantal singuliere polynomen van graad twee of lager gelijk is aan

$$q^5 - q^4 + q^3 - q + 1.$$

Voor graad drie en groter is het lastiger om iets te zeggen over het aantal singuliere polynomen. Von zur Gathen geeft afhankelijk van de graad en de grote van het grondlichaam verschillende afschatting van het aantal polynomen met een singulier punt in een bepaald uitbreidingslichaam.[2, p.972-977]

6 Conclusie

We hebben in dit onderzoek gezocht naar kwantitatieve antwoorden op de vraag hoeveel irreducibele en singuliere polynomen er zijn over een eindig lichaam. Voor polynomen in één variabele was dit mogelijk en dit hebben we met twee verschillende bewijzen ondersteund. Voor polynomen in meerdere variabelen was er geen algemene formule te vinden maar hebben we wel iets kunnen zeggen over de verhouding irreducibele polynomen. Namelijk dat het grooste deel van de polynomen irreducibel is als de graad relatief veel groter is dan de grote van het lichaam. Dit is het tegenovergestelde van het een variabele geval.

Ook voor singuliere polynomen waren er condities wanneer we iets konden zeggen over exacte aantallen. Dit kon als de functie die we geconstrueerd hadden en welke het coördinaat nul was als het polynoom een singulierpunt had, surjectief was. Hiervoor moest gelden dan de vectorruimte van alle polynomen kleiner of gelijk aan de graad n bevat is in de vectorruimte van alle polynomen modulo het product van alle singulariteit idealen. Opvallend was dat voor voldoende grote graad de verhouding niet meer van graad maar alleen nog van de grote van het lichaam afhankelijk was.

We hebben ook een ondergrens gevonden voor het aantal singuliere polynomen wanneer de graad groter was dan twee. En een bovengrens als de graad groter was dan drie.
Voor alle polynomen tot en met graad twee hebben we door middel van geometrische eigenschappen het exacte aantal singuliere polynomen bepaald. Voor graad drie of groter hebben we een boven en ondergrens kunnen vinden, waarna bleek dat de ondergrens ook voor graad twee valide is.

We hebben de volgende waardes gevonden:

- Voor polynomen in een variabele : $I_n = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d$.
- Voor meerdere variabelen : $I_n = N_n - N_1 \cdot N_{n-1} + O(q^{b_{n-2}+b_2-2})$.
- Voor $n \geq 3q-2$ geldt $\frac{S_n}{N_n} = 1-(1-q^{-3})^{q^2}$.
- Voor $n \geq 3$ geldt $\frac{1}{q} - \frac{1}{2q^2} \leq \frac{S_n}{N_n} \leq \frac{1}{q}$.
- En $S_0 + S_1 + S_2 = \frac{1}{2}q^5 + \frac{1}{2}q^3 - q + 1$.
- Aantal absolute singuliere kwadratische polynomen zijn $q^5 - q^4 + q^3 - q$.

We hebben in dit onderzoek de alleen naar de rationele irreducibele polynomen gekeken en niet naar de absolute. Voor graad één en twee is dit het zelfde maar voor hogere graad niet meer. Een vervolg onderzoek zou dit en de samenhang hier tussen kunnen bekijken. Dit zelfde geldt voor absoluut singuliere polynomen met graad groter dan twee.
We hebben ook geprobeerd het totale aantal singuliere polynomen voor graad drie op een zelfde manier te vinden als we dat voor graad twee hebben gedaan maar het classificeren van alle verschillende polynomen is een stuk ingewikkelder.

References

[1] S. K. Chebolu and J. Mináč, *Counting irreducible polynomials over finite fields using the inclusion-exclusion principle*, Mathematics Magazine **84**, p. 369-371 (december 2011).

[2] J. von zur Gathen,*Counting reducible and singular bivariate polynomials*, Finite Fields and Their Applications **14**, p. 944-978 (2008)

[3] A. Bodin, *Number of Irreducible Polynomials in Several Variables over Finite Fields*, The American Mathematical Monthly **115**, p. 653-660 (2008), Mathematical Association of America, ISSN 00029890, 19300972.

[4] M. L. Fredman, *The Disribution of Absolutely Irreducible Polynomials in Serveral Indeterminates*, Proceedings ot the American Mathematical Society **31**, 387-390 (februari 1972)

[5] F. Beukers,*Rings and Galois theory*, Utrecht University, Department of Mathematics (2017)

[6] F. Beukers,*Elementary Number Theory*, Utrecht University, Department of Mathematics (2012)

[7] C. F. Gauss, *Untersuchungen Über Höhere Arithmetik*,(Chelsea Publishing Company, New York, 1981), 2de ed., ISBN 0-8284-0191-8, Vertaald door: H. Maser

[8] E. W. Weisstein,"Fiber." van MathWorld–A Wolfram Web Resource.,`http://mathworld.wolfram.com/Fiber.html`, bekeken op 1-6-2018.