Numerical semigroups and codes

Lecturer: Maria Bras-Amorós

Mon	Numerical Semigroups. The Paradigmatic Example of Weierstrass Semigroups
Tue	Classification, Characterization and Counting of Semigroups
Wed	Semigroup and Alegebraic Geometry Codes
Thu	Semigroup Ideals and Generalized Hamming Weights
Fri	$\mathbb{R}$-molds of Numerical Semigroups with Musical Motivation

References can be found in
`http://crises-deim.urv.cat/~mbras/cimpa2017`

Numerical Semigroups. The Paradigmatic Example of Weierstrass Semigroups

Maria Bras-Amorós

CIMPA Research School
Algebraic Methods in Coding Theory
Ubatuba, July 3-7, 2017

Contents

Algebraic curves

William Fulton.

Algebraic curves.

Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989.

Massimo Giulietti.

Notes on algebraic-geometric codes.

www.math.kth.se/math/forskningsrapporter/Giulietti.pdf.

Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan.

Algebraic Geometry codes, pages 871–961.

North-Holland, Amsterdam, 1998.

Oliver Pretzel.

Codes and algebraic curves, volume 8 of *Oxford Lecture Series in Mathematics and its Applications*.

The Clarendon Press Oxford University Press, New York, 1998.

Henning Stichtenoth.

Algebraic function fields and codes.

Universitext. Springer-Verlag, Berlin, 1993.

Fernando Torres.

Notes on Goppa codes.

www.ime.unicamp.br/~ftorres/RESEARCH/ARTS_PDF/codes.pdf.

Plane curves

Let K be a field with algebraic closure $\bar{K}$.

Let $\mathbb{P}^2(\bar{K})$ be the projective plane over $\bar{K}$:

$$\mathbb{P}^2(\bar{K}) = \{[a:b:c] : (a,b,c) \in \bar{K}^3 \setminus \{(0,0,0)\}\} \Big/ \left([a{:}b{:}c] \sim [a'{:}b'{:}c'] \iff \begin{array}{c} (a,b,c) = \lambda(a',b',c') \\ \text{for some } \lambda \neq 0 \end{array} \right)$$

Plane curves

Let K be a field with algebraic closure $\bar{K}$.

Let $\mathbb{P}^2(\bar{K})$ be the projective plane over $\bar{K}$:

$$\mathbb{P}^2(\bar{K}) = \{[a:b:c] : (a,b,c) \in \bar{K}^3 \setminus \{(0,0,0)\}\} / _{\left([a:b:c]\sim[a':b':c'] \Longleftrightarrow \begin{smallmatrix} (a,b,c) = \lambda(a',b',c') \\ \text{for some } \lambda \neq 0 \end{smallmatrix}\right)}$$

Affine curve

Let $f(x,y) \in K[x,y]$.
The affine curve associated to f is the set of points

$$\{(a,b) \in \bar{K}^2 : f(a,b) = 0\}$$

Plane curves

Projective curve

Let $F(X, Y, Z) \in K[X, Y, Z]$ be a homogeneous polynomial.
The projective curve associated to F is the set of points

$$\mathcal{X}_F = \{(a : b : c) \in \mathbb{P}^2(\bar{K}) : F(a : b : c) = 0\}$$

Homogenization and dehomogenization

Affine to projective

The homogenization of $f \in K[x, y]$ is

$$f^*(X, Y, Z) = Z^{\deg(f)} f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

The points $(a, b) \in \bar{K}^2$ of the affine curve defined by $f(x, y)$ correspond to the points $(a : b : 1) \in \mathbb{P}^2(\bar{K})$ of $\mathcal{X}_{f^*}$.

Homogenization and dehomogenization

Projective to affine

A projective curve defined by a homogeneous polynomial $F(X, Y, Z)$ defines three affine curves with dehomogenized polynomials

$$F(x, y, 1), F(1, u, v), F(w, 1, z).$$

The points $(X : Y : Z)$ with $Z \neq 0$ (resp. $X \neq 0$, $Y \neq 0$) of $\mathcal{X}_F$ correspond to the points of the affine curve defined by $F(x, y, 1)$ (resp. $F(1, u, v)$, $F(w, 1, z)$). The points with $Z = 0$ are said to be at infinity.

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

Exercise

Let $q = 2$, $\mathbb{F}_{q^2} = \mathbb{Z}_2/(x^2 + x + 1)$, α the class of x. Then, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$.

Does $\mathcal{H}_2$ have points at infinity? Find all the points of $\mathcal{H}_2$.

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

Exercise

Let $q = 2$, $\mathbb{F}_{q^2} = \mathbb{Z}_2/(x^2 + x + 1)$, α the class of x. Then, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$.

Does $\mathcal{H}_2$ have points at infinity? Find all the points of $\mathcal{H}_2$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$.

Hermitian example $(X^{q+1} = Y^qZ + YZ^q)$

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

Exercise

Let $q = 2$, $\mathbb{F}_{q^2} = \mathbb{Z}_2/(x^2 + x + 1)$, α the class of x. Then, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$.

Does $\mathcal{H}_2$ have points at infinity? Find all the points of $\mathcal{H}_2$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$. For the remaining points, notice that

$$\begin{array}{cccc} 0^{q+1} = 0 & 1^{q+1} = 1 & \alpha^{q+1} = 1 & (\alpha^2)^{q+1} = 1 \\ 0^q + 0 = 0 & 1^q + 1 = 0 & \alpha^q + \alpha = 1 & (\alpha^2)^q + \alpha^2 = 1 \end{array}$$

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^q Z - Y Z^q = 0.$$

Exercise

Let $q = 2$, $\mathbb{F}_{q^2} = \mathbb{Z}_2/(x^2 + x + 1)$, α the class of x. Then, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$.

Does $\mathcal{H}_2$ have points at infinity? Find all the points of $\mathcal{H}_2$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$. For the remaining points, notice that

$$\begin{array}{cccc} 0^{q+1} = 0 & 1^{q+1} = 1 & \alpha^{q+1} = 1 & (\alpha^2)^{q+1} = 1 \\ 0^q + 0 = 0 & 1^q + 1 = 0 & \alpha^q + \alpha = 1 & (\alpha^2)^q + \alpha^2 = 1 \end{array}$$

Then the points are:
$P_1 = (0 : 0 : 1) \equiv (0, 0)$, $P_2 = (0 : 1 : 1) \equiv (0, 1)$, $P_3 = (1 : \alpha : 1) \equiv (1, \alpha)$, $P_4 = (1 : \alpha^2 : 1) \equiv (1, \alpha^2)$,
$P_5 = (\alpha : \alpha : 1) \equiv (\alpha, \alpha)$, $P_6 = (\alpha : \alpha^2 : 1) \equiv (\alpha, \alpha^2)$, $P_7 = (\alpha^2 : \alpha : 1) \equiv (\alpha^2, \alpha)$, $P_8 = (\alpha^2 : \alpha^2 : 1) \equiv (\alpha^2, \alpha^2)$

Irreducibility

If F can factor in a field extension of K then the curve is a proper union of at least two curves.

Irreducibility

If F can factor in a field extension of K then the curve is a proper union of at least two curves.

Hence, we impose F to be irreducible in any field extension of K.

Irreducibility

If F can factor in a field extension of K then the curve is a proper union of at least two curves.

Hence, we impose F to be irreducible in any field extension of K.

In this case we say that F is absolutely irreducible.

Function field

$$G(X,Y,Z) - H(X,Y,Z) = mF(X,Y,Z) \Longrightarrow G(a,b,c) = H(a,b,c) \text{ for all } (a:b:c) \in \mathcal{X}_F.$$

Function field

$G(X,Y,Z) - H(X,Y,Z) = mF(X,Y,Z) \Longrightarrow G(a,b,c) = H(a,b,c)$ for all $(a:b:c) \in \mathcal{X}_F$.

So, we consider

$$K(X,Y,Z)/(F) = \{G(X,Y,Z) \in K(X,Y,Z)\}/_{(G \sim H \Longleftrightarrow G-H=mF)}$$

Function field

$G(X, Y, Z) - H(X, Y, Z) = mF(X, Y, Z) \Longrightarrow G(a, b, c) = H(a, b, c)$ for all $(a : b : c) \in \mathcal{X}_F$.

So, we consider

$$K(X, Y, Z)/(F) = \{G(X, Y, Z) \in K(X, Y, Z)\}/_{(G \sim H \Longleftrightarrow G - H = mF)}$$

Since F is irreducible, $K(X, Y, Z)/(F)$ is an integral domain and we can construct its field of fractions Q_F.

Function field

$G(X,Y,Z) - H(X,Y,Z) = mF(X,Y,Z) \Longrightarrow G(a,b,c) = H(a,b,c)$ for all $(a:b:c) \in \mathcal{X}_F$.

So, we consider

$$K(X,Y,Z)/(F) = \{G(X,Y,Z) \in K(X,Y,Z)\}/_{(G\sim H \Longleftrightarrow G-H=mF)}$$

Since F is irreducible, $K(X,Y,Z)/(F)$ is an integral domain and we can construct its field of fractions Q_F.

For evaluating one such fraction at a projective point we want the result not to depend on the representative of the projective point. Hence, we require the numerator and the denominator to have one representative each, which is a homogeneous polynomial and both having the same degree.

Function field

$G(X,Y,Z) - H(X,Y,Z) = mF(X,Y,Z) \Longrightarrow G(a,b,c) = H(a,b,c)$ for all $(a:b:c) \in \mathcal{X}_F$.

So, we consider

$$K(X,Y,Z)/(F) = \{G(X,Y,Z) \in K(X,Y,Z)\}/_{(G\sim H \Longleftrightarrow G-H=mF)}$$

Since F is irreducible, $K(X,Y,Z)/(F)$ is an integral domain and we can construct its field of fractions Q_F.

For evaluating one such fraction at a projective point we want the result not to depend on the representative of the projective point. Hence, we require the numerator and the denominator to have one representative each, which is a homogeneous polynomial and both having the same degree.

The function field of $\mathcal{X}_F$, denoted $K(\mathcal{X}_F)$, is the set of elements of Q_F admitting one such representation.

Function field

$G(X,Y,Z) - H(X,Y,Z) = mF(X,Y,Z) \Longrightarrow G(a,b,c) = H(a,b,c)$ for all $(a:b:c) \in \mathcal{X}_F$.

So, we consider

$$K(X,Y,Z)/(F) = \{G(X,Y,Z) \in K(X,Y,Z)\}/_{(G \sim H \Longleftrightarrow G-H=mF)}$$

Since F is irreducible, $K(X,Y,Z)/(F)$ is an integral domain and we can construct its field of fractions Q_F.

For evaluating one such fraction at a projective point we want the result not to depend on the representative of the projective point. Hence, we require the numerator and the denominator to have one representative each, which is a homogeneous polynomial and both having the same degree.

The function field of $\mathcal{X}_F$, denoted $K(\mathcal{X}_F)$, is the set of elements of Q_F admitting one such representation.

Its elements are the rational functions of $\mathcal{X}_F$.

Regular functions

We say that a rational function $f \in K(\mathcal{X}_F)$ is regular in a point P if there exists a representation of it as a fraction $\frac{G(X,Y,Z)}{H(X,Y,Z)}$ with $H(P) \neq 0$.

Regular functions

We say that a rational function $f \in K(\mathcal{X}_F)$ is regular in a point P if there exists a representation of it as a fraction $\frac{G(X,Y,Z)}{H(X,Y,Z)}$ with $H(P) \neq 0$.

In this case we define

$$f(P) = \frac{G(P)}{H(P)}.$$

Regular functions

We say that a rational function $f \in K(\mathcal{X}_F)$ is regular in a point P if there exists a representation of it as a fraction $\frac{G(X,Y,Z)}{H(X,Y,Z)}$ with $H(P) \neq 0$.

In this case we define

$$f(P) = \frac{G(P)}{H(P)}.$$

The ring of all rational functions regular in P is denoted $\mathcal{O}_P$.

Regular functions

We say that a rational function $f \in K(\mathcal{X}_F)$ is regular in a point P if there exists a representation of it as a fraction $\frac{G(X,Y,Z)}{H(X,Y,Z)}$ with $H(P) \neq 0$.

In this case we define

$$f(P) = \frac{G(P)}{H(P)}.$$

The ring of all rational functions regular in P is denoted $\mathcal{O}_P$.

Again it is an integral domain and this time its field of fractions is $K(\mathcal{X}_F)$.

Singularities

Let $P \in \mathcal{X}_F$ be a point. If all the partial derivatives F_X, F_Y, F_Z vanish at P then P is said to be a singular point. Otherwise it is said to be a simple point.

Singularities

Let $P \in \mathcal{X}_F$ be a point. If all the partial derivatives F_X, F_Y, F_Z vanish at P then P is said to be a singular point. Otherwise it is said to be a simple point.

Curves without singular points are called non-singular, regular or smooth curves.

Singularities

Let $P \in \mathcal{X}_F$ be a point. If all the partial derivatives F_X, F_Y, F_Z vanish at P then P is said to be a singular point. Otherwise it is said to be a simple point.

Curves without singular points are called non-singular, regular or smooth curves.

The tangent line at a singular point P of $\mathcal{X}_F$ is defined by the equation

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0.$$

Singularities

Let $P \in \mathcal{X}_F$ be a point. If all the partial derivatives F_X, F_Y, F_Z vanish at P then P is said to be a singular point. Otherwise it is said to be a simple point.

Curves without singular points are called non-singular, regular or smooth curves.

The tangent line at a singular point P of $\mathcal{X}_F$ is defined by the equation

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0.$$

From now on we will assume that F is absolutely irreducible and that $\mathcal{X}_F$ is smooth.

Hermitian example $(X^{q+1} = Y^q Z + Y Z^q)$

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^q Z - Y Z^q = 0.$$

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^q Z - Y Z^q = 0.$$

Exercise

- Find the partial derivatives of $\mathcal{H}_q$
- Are there singular points?
- What is the tangent line at P_∞?

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

Exercise

- Find the partial derivatives of $\mathcal{H}_q$ $F_X = X^q, F_Y = -Z^q, F_Z = -Y^q$
- Are there singular points? No
- What is the tangent line at P_∞?
  $F_X(P_\infty)X + F_Y(P_\infty)Y + F_Z(P_\infty)Z = -Z = 0.$

Genus

The genus of a smooth plane curve $\mathcal{X}_F$ may be defined as

$$g = \frac{(\deg(F) - 1)(\deg(F) - 2)}{2}.$$

Genus

The genus of a smooth plane curve $\mathcal{X}_F$ may be defined as

$$g = \frac{(\deg(F) - 1)(\deg(F) - 2)}{2}.$$

For general curves the genus is defined using differentials on a curve.

Genus

The genus of a smooth plane curve $\mathcal{X}_F$ may be defined as

$$g = \frac{(\deg(F) - 1)(\deg(F) - 2)}{2}.$$

For general curves the genus is defined using differentials on a curve.

Exercise

What is in general the genus of $\mathcal{H}_q$?

Genus

The genus of a smooth plane curve $\mathcal{X}_F$ may be defined as

$$g = \frac{(\deg(F) - 1)(\deg(F) - 2)}{2}.$$

For general curves the genus is defined using differentials on a curve.

Exercise

What is in general the genus of $\mathcal{H}_q$? $\frac{q(q-1)}{2}$

Weierstrass semigroup

Valuation at a point

Theorem

Consider a point P in the projective curve $\mathcal{X}_F$. There exists $t \in \mathcal{O}_P$ such that for any non-zero $f \in K(\mathcal{X}_F)$ there exists a unique integer $v_P(f)$ with

$$f = t^{v_P(f)} u$$

for some $u \in \mathcal{O}_P$ with $u(P) \neq 0$.

Valuation at a point

Theorem

Consider a point P in the projective curve $\mathcal{X}_F$. There exists $t \in \mathcal{O}_P$ such that for any non-zero $f \in K(\mathcal{X}_F)$ there exists a unique integer $v_P(f)$ with

$$f = t^{v_P(f)} u$$

for some $u \in \mathcal{O}_P$ with $u(P) \neq 0$.

The value $v_P(f)$ depends only on $\mathcal{X}_F$, P.

Valuation at a point

Theorem

Consider a point P in the projective curve $\mathcal{X}_F$. There exists $t \in \mathcal{O}_P$ such that for any non-zero $f \in K(\mathcal{X}_F)$ there exists a unique integer $v_P(f)$ with

$$f = t^{v_P(f)} u$$

for some $u \in \mathcal{O}_P$ with $u(P) \neq 0$.

The value $v_P(f)$ depends only on $\mathcal{X}_F$, P.

If $G(X, Y, Z)$ and $H(X, Y, Z)$ are two homogeneous polynomials of degree 1 such that $G(P) = 0$, $H(P) \neq 0$, and G is not a constant multiple of $F_X(P)X + F_Y(P)Y + F_Z(P)Z$, then we can take t to be the class in $\mathcal{O}_P$ of $\frac{G(X,Y,Z)}{H(X,Y,Z)}$.

Valuation at a point

An element such as t is called a local parameter.

Valuation at a point

An element such as t is called a local parameter.

The value $v_P(f)$ is called the valuation of f at P.

Valuation at a point

An element such as t is called a local parameter.

The value $v_P(f)$ is called the valuation of f at P.

The point P is said to be a zero of multiplicity m if $v_P(f) = m > 0$ and a pole of multiplicity $-m$ if $v_P(f) = m < 0$.

Valuation at a point

An element such as t is called a local parameter.

The value $v_P(f)$ is called the valuation of f at P.

The point P is said to be a zero of multiplicity m if $v_P(f) = m > 0$ and a pole of multiplicity $-m$ if $v_P(f) = m < 0$.

The valuation satisfies that $v_P(f) \geqslant 0$ if and only if $f \in \mathcal{O}_P$ and that in this case $v_P(f) > 0$ if and only if $f(P) = 0$.

Valuation at a point

Lemma

1. $v_P(f) = \infty$ *if and only if* $f = 0$
2. $v_P(\lambda f) = v_P(f)$ *for all non-zero* $\lambda \in K$
3. $v_P(fg) = v_P(f) + v_P(g)$
4. $v_P(f+g) \geqslant \min\{v_P(f), v_P(g)\}$ *and equality holds if* $v_P(f) \neq v_P(g)$
5. *If* $v_P(f) = v_P(g) \geqslant 0$ *then there exists* $\lambda \in K$ *such that* $v_P(f - \lambda g) > v_P(f)$.

Valuation at a point

Let $L(mP)$ be the set of rational functions having only poles at P and with pole order at most m.

Valuation at a point

Let $L(mP)$ be the set of rational functions having only poles at P and with pole order at most m.

Let $A = \bigcup_{m \geqslant 0} L(mP)$, that is, A is the ring of rational functions having poles only at P.

Valuation at a point

Let $L(mP)$ be the set of rational functions having only poles at P and with pole order at most m.

Let $A = \bigcup_{m \geqslant 0} L(mP)$, that is, A is the ring of rational functions having poles only at P.

$L(mP)$ is a K-vector space and so we can define $l(mP) = \dim_K(L(mP))$.

Valuation at a point

Let $L(mP)$ be the set of rational functions having only poles at P and with pole order at most m.

Let $A = \bigcup_{m \geqslant 0} L(mP)$, that is, A is the ring of rational functions having poles only at P.

$L(mP)$ is a K-vector space and so we can define $l(mP) = \dim_K(L(mP))$.

One can prove that $l(mP)$ is either $l((m-1)P)$ or $l((m-1)P) + 1$ and

$$l(mP) = l((m-1)P) + 1 \iff \exists f \in A \text{ with } v_P(f) = -m$$

Valuation at a point

Let $L(mP)$ be the set of rational functions having only poles at P and with pole order at most m.

Let $A = \bigcup_{m \geqslant 0} L(mP)$, that is, A is the ring of rational functions having poles only at P.

$L(mP)$ is a K-vector space and so we can define $l(mP) = \dim_K(L(mP))$.

One can prove that $l(mP)$ is either $l((m-1)P)$ or $l((m-1)P)+1$ and

$$l(mP) = l((m-1)P) + 1 \Longleftrightarrow \exists f \in A \text{ with } v_P(f) = -m$$

Define $\Lambda = \{-v_P(f) : f \in A \setminus \{0\}\}$.

Valuation at a point

Let $L(mP)$ be the set of rational functions having only poles at P and with pole order at most m.

Let $A = \bigcup_{m \geqslant 0} L(mP)$, that is, A is the ring of rational functions having poles only at P.

$L(mP)$ is a K-vector space and so we can define $l(mP) = \dim_K(L(mP))$.

One can prove that $l(mP)$ is either $l((m-1)P)$ or $l((m-1)P)+1$ and

$$l(mP) = l((m-1)P) + 1 \iff \exists f \in A \text{ with } v_P(f) = -m$$

Define $\Lambda = \{-v_P(f) : f \in A \setminus \{0\}\}$.

Obviously, $\Lambda \subseteq \mathbb{N}_0$.

Weierstrass semigroup

Lemma

The set $\Lambda \subseteq \mathbb{N}_0$ *satisfies*

1. $0 \in \Lambda$
2. $m + m' \in \Lambda$ *whenever* $m, m' \in \Lambda$
3. $\mathbb{N}_0 \setminus \Lambda$ *has a finite number of elements*

Proof:

1. Constant functions $f = a$ have no poles and satisfy $v_P(a) = 0$ for all $P \in \mathcal{X}_F$. Hence, $0 \in \Lambda$.

$\square$

Weierstrass semigroup

Lemma

The set $\Lambda \subseteq \mathbb{N}_0$ *satisfies*

1. $0 \in \Lambda$
2. $m + m' \in \Lambda$ *whenever* $m, m' \in \Lambda$
3. $\mathbb{N}_0 \setminus \Lambda$ *has a finite number of elements*

Proof:

2. If $m, m' \in \Lambda$ then there exist $f, g \in A$ with $v_P(f) = -m$, $v_P(g) = -m'$.
   $v_P(fg) = -(m + m') \Longrightarrow m + m' \in \Lambda$.

$\square$

Weierstrass semigroup

Lemma

The set $\Lambda \subseteq \mathbb{N}_0$ *satisfies*

1. $0 \in \Lambda$
2. $m + m' \in \Lambda$ *whenever* $m, m' \in \Lambda$
3. $\mathbb{N}_0 \setminus \Lambda$ *has a finite number of elements*

Proof:

3. The well-known Riemann-Roch theorem implies that

$$l(mP) = m + 1 - g$$

if $m \geqslant 2g - 1$.
On one hand this means that $m \in \Lambda$ for all $m \geqslant 2g$, and on the other hand, this means that $l(mP) = l((m-1)P)$ only for g values of m.
$\Longrightarrow \#(\mathbb{N}_0 \setminus \Lambda) = g$.

Weierstrass semigroup

Lemma

The set $\Lambda \subseteq \mathbb{N}_0$ *satisfies*

1. $0 \in \Lambda$
2. $m + m' \in \Lambda$ *whenever* $m, m' \in \Lambda$
3. $\mathbb{N}_0 \setminus \Lambda$ *has a finite number of elements*

The three properties of a subset of $\mathbb{N}_0$ in the lemma constitute the definition of a numerical semigroup.

Weierstrass semigroup

Lemma

The set $\Lambda \subseteq \mathbb{N}_0$ *satisfies*

1. $0 \in \Lambda$
2. $m + m' \in \Lambda$ *whenever* $m, m' \in \Lambda$
3. $\mathbb{N}_0 \setminus \Lambda$ *has a finite number of elements*

The three properties of a subset of $\mathbb{N}_0$ in the lemma constitute the definition of a numerical semigroup.

The particular numerical semigroup of the lemma is called the Weierstrass semigroup at P and the elements in $\mathbb{N}_0 \setminus \Lambda$ are called the Weierstrass gaps.

Numerical semigroups

Example: What amounts can be withdrawn?

Numerical semigroups

Example: What amounts can be withdrawn?

0€, 20€, 40€, 50€, 60€, 70€, 80€, 90€, 100€, . . .

Numerical semigroups

Example: What amounts can be withdrawn?

0€, 20€, 40€, 50€, 60€, 70€, 80€, 90€, 100€, ...

- 0 in the set

Numerical semigroups

Example: What amounts can be withdrawn?

$$0€, 20€, 40€, 50€, 60€, 70€, 80€, 90€, 100€, \ldots$$

- 0 in the set
- s, s' in the set $\Longrightarrow s + s'$ in the set

Numerical semigroups

Example: What amounts can be withdrawn?

$$0€, 20€, 40€, 50€, 60€, 70€, 80€, 90€, 100€, \ldots$$

- 0 in the set
- s, s' in the set $\Longrightarrow s + s'$ in the set

If we just consider multiples of 10 then

Numerical semigroups

Example: What amounts can be withdrawn?

$$0€, 20€, 40€, 50€, 60€, 70€, 80€, 90€, 100€, \ldots$$

- 0 in the set
- s, s' in the set $\Longrightarrow s + s'$ in the set

If we just consider multiples of 10 then

- only 10€, 30€ are **not** in the set $(\#(\mathbb{N}_0 \setminus (S/10)) < \infty)$

Examples

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^q Z - Y Z^q = 0.$$

$F_X = X^q, F_Y = -Z^q, F_Z = -Y^q \Longrightarrow$ no singular points.

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

$F_X = X^q, F_Y = -Z^q, F_Z = -Y^q \Longrightarrow$ no singular points.

$P_\infty = (0 : 1 : 0)$ is the unique point of $\mathcal{H}_q$ at infinity (with $Z = 0$).

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^q Z - Y Z^q = 0.$$

$F_X = X^q, F_Y = -Z^q, F_Z = -Y^q \Longrightarrow$ no singular points.

$P_\infty = (0 : 1 : 0)$ is the unique point of $\mathcal{H}_q$ at infinity (with $Z = 0$).

$t = \frac{X}{Y}$ is a local parameter at P_∞ since $F_X(P_\infty)X + F_Y(P_\infty)Y + F_Z(P_\infty)Z = -Z$.

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

$F_X = X^q, F_Y = -Z^q, F_Z = -Y^q \Longrightarrow$ no singular points.

$P_\infty = (0 : 1 : 0)$ is the unique point of $\mathcal{H}_q$ at infinity (with $Z = 0$).

$t = \frac{X}{Y}$ is a local parameter at P_∞ since $F_X(P_\infty)X + F_Y(P_\infty)Y + F_Z(P_\infty)Z = -Z$.

$\frac{X}{Z}, \frac{Y}{Z}$ are regular everywhere except at P_∞ ($\Rightarrow \frac{X}{Z}, \frac{Y}{Z} \in \cup_{m \geqslant 0}\mathcal{L}(mP_\infty)$).

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^q Z - Y Z^q = 0.$$

$F_X = X^q, F_Y = -Z^q, F_Z = -Y^q \Longrightarrow$ no singular points.

$P_\infty = (0:1:0)$ is the unique point of $\mathcal{H}_q$ at infinity (with $Z = 0$).

$t = \frac{X}{Y}$ is a local parameter at P_∞ since $F_X(P_\infty)X + F_Y(P_\infty)Y + F_Z(P_\infty)Z = -Z$.

$\frac{X}{Z}, \frac{Y}{Z}$ are regular everywhere except at P_∞ ($\Rightarrow \frac{X}{Z}, \frac{Y}{Z} \in \cup_{m \geqslant 0} \mathcal{L}(mP_\infty)$).

To find their valuation...

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

$F_X = X^q, F_Y = -Z^q, F_Z = -Y^q \Longrightarrow$ no singular points.

$P_\infty = (0 : 1 : 0)$ is the unique point of $\mathcal{H}_q$ at infinity (with $Z = 0$).

$t = \frac{X}{Y}$ is a local parameter at P_∞ since $F_X(P_\infty)X + F_Y(P_\infty)Y + F_Z(P_\infty)Z = -Z$.

$\frac{X}{Z}, \frac{Y}{Z}$ are regular everywhere except at P_∞ ($\Rightarrow \frac{X}{Z}, \frac{Y}{Z} \in \cup_{m \geqslant 0}\mathcal{L}(mP_\infty)$).

To find their valuation...

$t^{q+1} = \left(\frac{Z}{Y}\right)^q + \frac{Z}{Y} \Rightarrow v_{P_\infty}(\left(\frac{Z}{Y}\right)^q + \frac{Z}{Y}) = q + 1 \Rightarrow v_{P_\infty}(\frac{Z}{Y}) = q + 1 \Rightarrow$
$v_{P_\infty}(\frac{Y}{Z}) = -(q+1)$.

Hermitian example ($X^{q+1} = Y^qZ + YZ^q$)

Let q be a prime power.

The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by

$$x^{q+1} = y^q + y \text{ and } X^{q+1} - Y^qZ - YZ^q = 0.$$

$F_X = X^q, F_Y = -Z^q, F_Z = -Y^q \Longrightarrow$ no singular points.

$P_\infty = (0:1:0)$ is the unique point of $\mathcal{H}_q$ at infinity (with $Z = 0$).

$t = \frac{X}{Y}$ is a local parameter at P_∞ since $F_X(P_\infty)X + F_Y(P_\infty)Y + F_Z(P_\infty)Z = -Z$.

$\frac{X}{Z}, \frac{Y}{Z}$ are regular everywhere except at P_∞ ($\Rightarrow \frac{X}{Z}, \frac{Y}{Z} \in \cup_{m\geqslant 0}\mathcal{L}(mP_\infty)$).

To find their valuation...

$t^{q+1} = \left(\frac{Z}{Y}\right)^q + \frac{Z}{Y} \Rightarrow v_{P_\infty}(\left(\frac{Z}{Y}\right)^q + \frac{Z}{Y}) = q+1 \Rightarrow v_{P_\infty}(\frac{Z}{Y}) = q+1 \Rightarrow$
$v_{P_\infty}(\frac{Y}{Z}) = -(q+1)$.

$\left(\frac{X}{Z}\right)^{q+1} = \left(\frac{Y}{Z}\right)^q + \frac{Y}{Z} \Rightarrow (q+1)v_{P_\infty}(\frac{X}{Z}) = -q(q+1) \Rightarrow v_{P_\infty}(\frac{X}{Z}) = -q$.

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

$\Rightarrow q, q+1 \in \Lambda.$

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

$\Rightarrow q, q+1 \in \Lambda$.

$\Rightarrow \Lambda$ contains what we will call later the semigroup generated by $q, q+1$.

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

$\Rightarrow q, q+1 \in \Lambda$.

$\Rightarrow \Lambda$ contains what we will call later the semigroup generated by $q, q+1$.

The complement in $\mathbb{N}_0$ of the semigroup generated by $q, q+1$ has $\frac{q(q-1)}{2} = g$ elements.

Exercise

Can you prove that?

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

$\Rightarrow q, q+1 \in \Lambda$.

$\Rightarrow \Lambda$ contains what we will call later the semigroup generated by $q, q+1$.

The complement in $\mathbb{N}_0$ of the semigroup generated by $q, q+1$ has $\frac{q(q-1)}{2} = g$ elements.

Exercise

Can you prove that? The number of gaps is $(q-1) + (q-2) + \cdots + 1 = \frac{q(q-1)}{2}$

Hermitian example ($X^{q+1} = Y^q Z + Y Z^q$)

$\Rightarrow q, q+1 \in \Lambda$.

$\Rightarrow \Lambda$ contains what we will call later the semigroup generated by $q, q+1$.

The complement in $\mathbb{N}_0$ of the semigroup generated by $q, q+1$ has $\frac{q(q-1)}{2} = g$ elements.

Exercise

Can you prove that? The number of gaps is $(q-1) + (q-2) + \cdots + 1 = \frac{q(q-1)}{2}$

Since we know that the complement of Λ in $\mathbb{N}_0$ also has g elements, this means that both semigroups are the same.

Klein example ($X^3Y + Y^3Z + Z^3X = 0$)

The Klein quartic over $\mathbb{F}_q$ is defined by

$$x^3y + y^3 + x = 0 \text{ and } X^3Y + Y^3Z + Z^3X = 0$$

Klein example ($X^3Y + Y^3Z + Z^3X = 0$)

The Klein quartic over $\mathbb{F}_q$ is defined by

$$x^3y + y^3 + x = 0 \text{ and } X^3Y + Y^3Z + Z^3X = 0$$

$F_X = 3X^2Y + Z^3, F_Y = 3Y^2Z + X^3, F_Z = 3Z^2X + Y^3.$

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

The Klein quartic over $\mathbb{F}_q$ is defined by

$$x^3y + y^3 + x = 0 \text{ and } X^3Y + Y^3Z + Z^3X = 0$$

$F_X = 3X^2Y + Z^3, F_Y = 3Y^2Z + X^3, F_Z = 3Z^2X + Y^3.$

If the characteristic of $\mathbb{F}_{q^2}$ is 3 then $F_X = F_Y = F_Z = 0$ implies $X^3 = Y^3 = Z^3 = 0 \Rightarrow X = Y = Z = 0 \Rightarrow \mathcal{K}$ has no singularities.

Klein example ($X^3Y + Y^3Z + Z^3X = 0$)

The Klein quartic over $\mathbb{F}_q$ is defined by

$$x^3y + y^3 + x = 0 \text{ and } X^3Y + Y^3Z + Z^3X = 0$$

$F_X = 3X^2Y + Z^3, F_Y = 3Y^2Z + X^3, F_Z = 3Z^2X + Y^3.$

If the characteristic of $\mathbb{F}_{q^2}$ is 3 then $F_X = F_Y = F_Z = 0$ implies $X^3 = Y^3 = Z^3 = 0 \Rightarrow X = Y = Z = 0 \Rightarrow \mathcal{K}$ has no singularities.

If the characteristic of $\mathbb{F}_{q^2}$ is different than 3 then $F_X = F_Y = F_Z = 0$ implies $X^3Y = -3Y^3Z$ and $Z^3X = -3X^3Y = 9Y^3Z$.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

The Klein quartic over $\mathbb{F}_q$ is defined by

$$x^3y + y^3 + x = 0 \text{ and } X^3Y + Y^3Z + Z^3X = 0$$

$F_X = 3X^2Y + Z^3, F_Y = 3Y^2Z + X^3, F_Z = 3Z^2X + Y^3$.

If the characteristic of $\mathbb{F}_{q^2}$ is 3 then $F_X = F_Y = F_Z = 0$ implies $X^3 = Y^3 = Z^3 = 0 \Rightarrow X = Y = Z = 0 \Rightarrow \mathcal{K}$ has no singularities.

If the characteristic of $\mathbb{F}_{q^2}$ is different than 3 then $F_X = F_Y = F_Z = 0$ implies $X^3Y = -3Y^3Z$ and $Z^3X = -3X^3Y = 9Y^3Z$.

From the equation of the curve $-3Y^3Z + Y^3Z + 9Y^3Z = 7Y^3Z = 0$.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

The Klein quartic over $\mathbb{F}_q$ is defined by

$$x^3y + y^3 + x = 0 \text{ and } X^3Y + Y^3Z + Z^3X = 0$$

$F_X = 3X^2Y + Z^3, F_Y = 3Y^2Z + X^3, F_Z = 3Z^2X + Y^3.$

If the characteristic of $\mathbb{F}_{q^2}$ is 3 then $F_X = F_Y = F_Z = 0$ implies $X^3 = Y^3 = Z^3 = 0 \Rightarrow X = Y = Z = 0 \Rightarrow \mathcal{K}$ has no singularities.

If the characteristic of $\mathbb{F}_{q^2}$ is different than 3 then $F_X = F_Y = F_Z = 0$ implies $X^3Y = -3Y^3Z$ and $Z^3X = -3X^3Y = 9Y^3Z$.

From the equation of the curve $-3Y^3Z + Y^3Z + 9Y^3Z = 7Y^3Z = 0$.
If $\gcd(q, 7) = 1$ then either

$$Y = 0 \Rightarrow \begin{cases} X = 0 & \text{if } F_Y = 0 \\ Z = 0 & \text{if } F_X = 0 \end{cases} \quad \text{or} \quad Z = 0 \Rightarrow \begin{cases} X = 0 & \text{if } F_Y = 0 \\ Y = 0 & \text{if } F_Z = 0 \end{cases}$$

so, there are no singular points.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

$P_0 = (0:0:1) \in \mathcal{K}$.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

$P_0 = (0 : 0 : 1) \in \mathcal{K}$.

$t = \frac{Y}{Z}$ is a local parameter at P_0 since
$F_X(P_0)X + F_Y(P_0)Y + F_Z(P_0)Z = X$.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

$P_0 = (0:0:1) \in \mathcal{K}$.

$t = \frac{Y}{Z}$ is a local parameter at P_0 since
$F_X(P_0)X + F_Y(P_0)Y + F_Z(P_0)Z = X$.

$$\left(\frac{X}{Y}\right)^3 + \frac{Z}{Y} + \left(\frac{Z}{Y}\right)^3 \frac{X}{Y} = 0 \Rightarrow \text{ or } \left\{ \begin{array}{rcl} 3v_{P_0}(\frac{X}{Y}) & = & v_{P_0}(\frac{Z}{Y}) \\ 3v_{P_0}(\frac{X}{Y}) & = & 3v_{P_0}(\frac{Z}{Y}) + v_{P_0}(\frac{X}{Y}) \\ v_{P_0}(\frac{Z}{Y}) & = & 3v_{P_0}(\frac{Z}{Y}) + v_{P_0}(\frac{X}{Y}) \end{array} \right.$$

$$v_{P_0}(\tfrac{Z}{Y}) = -1 \Rightarrow \text{ or } \left\{ \begin{array}{rcl} 3v_{P_0}(\frac{X}{Y}) & = & -1 \\ 3v_{P_0}(\frac{X}{Y}) & = & -3 + v_{P_0}(\frac{X}{Y}) \\ -1 & = & -3 + v_{P_0}(\frac{X}{Y}) \end{array} \right.$$

$$\Rightarrow \text{ or } \left\{ \begin{array}{rcl} v_{P_0}(\frac{X}{Y}) & = & -1/3 \\ v_{P_0}(\frac{X}{Y}) & = & -3/2 \\ v_{P_0}(\frac{X}{Y}) & = & 2 \end{array} \right.$$

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

$P_0 = (0:0:1) \in \mathcal{K}$.

$t = \frac{Y}{Z}$ is a local parameter at P_0 since
$F_X(P_0)X + F_Y(P_0)Y + F_Z(P_0)Z = X$.

$$\left(\frac{X}{Z}\right)^3 \frac{Y}{Z} + \left(\frac{Y}{Z}\right)^3 + \frac{X}{Z} = 0 \Rightarrow \text{ or } \left\{ \begin{array}{rcl} 3v_{P_0}(\frac{X}{Z}) + v_{P_0}(\frac{Y}{Z}) & = & 3v_{P_0}(\frac{Y}{Z}) \\ 3v_{P_0}(\frac{X}{Z}) + v_{P_0}(\frac{Y}{Z}) & = & v_{P_0}(\frac{X}{Z}) \\ 3v_{P_0}(\frac{Y}{Z}) & = & v_{P_0}(\frac{X}{Z}) \end{array} \right.$$

$$v_{P_0}(\tfrac{Y}{Z}) = 1 \Rightarrow \text{ or } \left\{ \begin{array}{rcl} 3v_{P_0}(\frac{X}{Z}) + 1 & = & 3 \\ 3v_{P_0}(\frac{X}{Z}) + 1 & = & v_{P_0}(\frac{X}{Z}) \\ 3 & = & v_{P_0}(\frac{X}{Z}) \end{array} \right.$$

$$\Rightarrow \text{ or } \left\{ \begin{array}{rcl} v_{P_0}(\frac{X}{Z}) & = & 2/3 \\ v_{P_0}(\frac{X}{Z}) & = & -1/2 \\ v_{P_0}(\frac{X}{Z}) & = & 3 \end{array} \right.$$

Klein example ($X^3Y + Y^3Z + Z^3X = 0$)

Now we want to see under which conditions

$$f_{ij} = \frac{Y^i Z^j}{X^{i+j}} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0).$$

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

Now we want to see under which conditions

$$f_{ij} = \frac{Y^i Z^j}{X^{i+j}} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0).$$

We have

$$v_{P_0}(f_{ij}) = -2i - 3j$$

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

Now we want to see under which conditions

$$f_{ij} = \frac{Y^i Z^j}{X^{i+j}} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0).$$

We have

$$v_{P_0}(f_{ij}) = -2i - 3j$$

The poles of f_{ij} have $X = 0 \Rightarrow$ only may be at $P_0 = (0 : 0 : 1)$, $P_1 = (0 : 1 : 0)$.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

Now we want to see under which conditions

$$f_{ij} = \frac{Y^i Z^j}{X^{i+j}} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0).$$

We have

$$v_{P_0}(f_{ij}) = -2i - 3j$$

The poles of f_{ij} have $X = 0 \Rightarrow$ only may be at $P_0 = (0:0:1)$, $P_1 = (0:1:0)$.

Symmetries of $\mathcal{K} \Rightarrow$ $\left.\begin{array}{rcl} v_{P_1}(\frac{Y}{X}) & = & -1 \\ v_{P_1}(\frac{Z}{X}) & = & 2 \end{array}\right\} \Rightarrow v_{P_1}(f_{ij}) = -i + 2j.$

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

Now we want to see under which conditions

$$f_{ij} = \frac{Y^i Z^j}{X^{i+j}} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0).$$

We have

$$v_{P_0}(f_{ij}) = -2i - 3j$$

The poles of f_{ij} have $X = 0 \Rightarrow$ only may be at $P_0 = (0:0:1)$, $P_1 = (0:1:0)$.

Symmetries of $\mathcal{K} \Rightarrow \left.\begin{array}{rcl} v_{P_1}(\frac{Y}{X}) & = & -1 \\ v_{P_1}(\frac{Z}{X}) & = & 2 \end{array}\right\} \Rightarrow v_{P_1}(f_{ij}) = -i + 2j.$

$\Rightarrow f_{ij} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0)$ if and only if $-i + 2j \geqslant 0$.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

Now we want to see under which conditions

$$f_{ij} = \frac{Y^i Z^j}{X^{i+j}} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0).$$

We have

$$v_{P_0}(f_{ij}) = -2i - 3j$$

The poles of f_{ij} have $X = 0 \Rightarrow$ only may be at $P_0 = (0:0:1)$, $P_1 = (0:1:0)$.

Symmetries of $\mathcal{K} \Rightarrow \left.\begin{array}{rcl} v_{P_1}(\frac{Y}{X}) & = & -1 \\ v_{P_1}(\frac{Z}{X}) & = & 2 \end{array}\right\} \Rightarrow v_{P_1}(f_{ij}) = -i + 2j.$

$\Rightarrow f_{ij} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0)$ if and only if $-i + 2j \geqslant 0$.

Then Λ contains $\{2i + 3j : i, j \geqslant 0, 2j \geqslant i\} = \{0, 3, 5, 6, 7, 8, \ldots\}$.

Klein example $(X^3Y + Y^3Z + Z^3X = 0)$

Now we want to see under which conditions

$$f_{ij} = \frac{Y^i Z^j}{X^{i+j}} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0).$$

We have

$$v_{P_0}(f_{ij}) = -2i - 3j$$

The poles of f_{ij} have $X = 0 \Rightarrow$ only may be at $P_0 = (0:0:1)$, $P_1 = (0:1:0)$.

Symmetries of $\mathcal{K} \Rightarrow \left.\begin{array}{rcl} v_{P_1}(\frac{Y}{X}) & = & -1 \\ v_{P_1}(\frac{Z}{X}) & = & 2 \end{array}\right\} \Rightarrow v_{P_1}(f_{ij}) = -i + 2j.$

$\Rightarrow f_{ij} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0)$ if and only if $-i + 2j \geqslant 0$.

Then Λ contains $\{2i + 3j : i, j \geqslant 0, 2j \geqslant i\} = \{0, 3, 5, 6, 7, 8, \ldots\}$.

This has 3 gaps which is exactly the genus of $\mathcal{K}$. So,

$$\Lambda = \{0, 3, 5, 6, 7, 8, 9, 10, \ldots\}.$$

Klein example ($X^3Y + Y^3Z + Z^3X = 0$)

It is left as an exercise to prove that all this can be generalized to the curve $\mathcal{K}_m$ with defining polynomial

$$F = X^m Y + Y^m Z + Z^m X,$$

provided that $\gcd(1, m^2 - m + 1) = 1$. In this case

$$v_{P_0}(f_{ij}) = -(m-1)i - mj$$

and

$$f_{ij} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0) \text{ if and only if } -i + (m-1)j \geqslant 0.$$

Since $(m-1)i + mj = (m-1)i' + mj'$ for some $(i', j') \neq (i, j)$ if and only if $i \geqslant m$ or $j \geqslant m-1$ we deduce that

$$\{-v_{P_0}(f_{ij}) : f_{ij} \in \cup_{m \geqslant 0} \mathcal{L}(mP_0)\} =$$

$$\{(m-1)i + mj : (i, j) \neq (1, 0), (2, 0), \ldots, (m-1, 0)\}.$$

This set has exactly $\frac{m(m-1)}{2}$ gaps which is the genus of $\mathcal{K}_m$. So it is exactly the Weierstrass semigroup at P_0.

Bounding the number of points of a curve

Bounding the number of points of a curve

- Depending on the genus of the curve:
  - Serre-Hasse-Weil bound
    Let $\mathcal{X}$ be a curve of genus g over $\mathbb{F}_q$. Then the number of points with coordinates in $\mathbb{F}_q$ satisfies

$$\#N_q(g) \leqslant q + 1 + g\,[2\sqrt{q}]$$

Bounding the number of points of a curve

- Depending on Weierstrass semigroups:
  1. Geil-Matsumoto:
     $N_q(\Lambda) \leqslant GM_q(\Lambda) = \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1$
  - Pros and cons:
    - + Best known bound related to Weierstrass semigroups (for some values it is better than Serre-Hasse-Weil bound).
    - - not simple.

Example with $q = 3$ and $\Lambda = \langle 5, 7 \rangle$

$$GM_q(\Lambda) = \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1$$

- Λ:
  - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ...

Example with $q = 3$ and $\Lambda = \langle 5, 7 \rangle$

$$GM_q(\Lambda) = \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1$$

- Λ:
  - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ...
- $q5 + \Lambda$:
  - 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 ...

Example with $q = 3$ and $\Lambda = \langle 5, 7 \rangle$

$$GM_q(\Lambda) = \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1$$

- Λ:
  - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ...
- $q5 + \Lambda$:
  - 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 ...
- $q7 + \Lambda$:
  - 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 ...

Example with $q = 3$ and $\Lambda = \langle 5, 7 \rangle$

$$GM_q(\Lambda) = \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1$$

- Λ:
  - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ...
- $q5 + \Lambda$:
  - 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 ...
- $q7 + \Lambda$:
  - 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 ...
- $\Lambda \setminus \{(q5 + \Lambda) \cup (q7 + \Lambda)\}$:
  - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ...

Example with $q = 3$ and $\Lambda = \langle 5, 7 \rangle$

$$GM_q(\Lambda) = \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1$$

- Λ:
  - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ...
- $q5 + \Lambda$:
  - 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 ...
- $q7 + \Lambda$:
  - 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 ...
- $\Lambda \setminus \{(q5 + \Lambda) \cup (q7 + \Lambda)\}$:
  - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 ...
- $GM_q(\Lambda) = \#\{0,5,7,10,12,14,17,19,24\} + 1 = 10$

Bounding the number of points of a curve

- Depending on Weierstrass semigroups:
  2. Lewittes:
     $N_q(\Lambda) \leqslant L_q(\Lambda) = q\lambda_1 + 1$
  - Pros and cons:
    - - Weaker than Geil-Matsumoto.
    - + simpler.

Example with $q = 3$ and $\Lambda = \langle 5, 7 \rangle$

$N_q(\Lambda) \leqslant L_q(\Lambda) = q\lambda_1 + 1$

- $L_q(\Lambda) = 3 \cdot 5 + 1 = 16$

A lot more faster!!

Results obtained using numerical semigroup techniques (in Albert Vico's PhD thesis)

- A closed formula for the Geil-Matsumoto bound for Weierstrass semigroups generated by two integers (i.e. hyperelliptic, Hermitian, Geil's norm-trace, etc.).
- An analysis of the semigroups for which the Geil-Matsumoto bound equals the Lewittes' bound.
- A result that (in some cases) simplifies the computation of the Geil-Matsumoto bound.

1^{st} Result: A closed formula for GM bound for semigroups with two generators

Lemma

The Geil-Matsumoto bound for the semigroup generated by a and b with $a < b$ is:

$$GM_q(\langle a, b\rangle) = 1 + \sum_{n=0}^{a-1} \min\left(q, \left\lceil \frac{q-n}{a} \right\rceil \cdot b\right) =$$

$$\begin{cases} 1 + qa & \text{if } q \leqslant \lfloor \frac{q}{a} \rfloor b \\ 1 + (q \bmod a)q + (a - (q \bmod a))\lfloor \frac{q}{a} \rfloor b & \text{if } \lfloor \frac{q}{a} \rfloor b < q \leqslant \lceil \frac{q}{a} \rceil b \\ 1 + ab\lceil \frac{q}{a} \rceil - (a - (q \bmod a))b & \text{if } q > \lceil \frac{q}{a} \rceil b \end{cases}$$

2^{nd} Result: coincidences of $GM(\Lambda) = L(\Lambda)$

- We proved that:
  $GM_q(\langle a, b\rangle) = L_q(\langle a, b\rangle)$ if and only if $q \leqslant \lfloor \frac{q}{a} \rfloor b$.
- Otherwise the Geil-Matsumoto bound always gives an improvement with respect to the Lewittes's bound.
- We would wish to generalize this to semigroups with any number of generators.

2^{nd} Result: coincidences of $GM(\Lambda) = L(\Lambda)$

Lemma

It holds

$$GM_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = L_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = q\lambda_1 + 1$$

if and only if $q(\lambda_i - \lambda_1) \in \Lambda$ *for all* i *with* $2 \leqslant i \leqslant n$

Lemma

If $q \leqslant \left\lfloor \frac{q}{\lambda_1} \right\rfloor \lambda_2$ *then*

$$GM_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = L_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = q\lambda_1 + 1$$

3^{rd} Result: Simplifying computation of GM bound

Lemma

Let $\Lambda = \langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle$ and let I be and index set included in $\{1, \ldots, n\}$, the next statements are equivalent:

1. $\Lambda \setminus \cup_{i=1}^{n} (q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i \in I} (q\lambda_i + \Lambda)$
2. *For all $i \notin I$ there exists $1 \leqslant j \leqslant n$, $j \in I$ such that $q(\lambda_i - \lambda_j) \in \Lambda$.*

3^{rd} Result: Simplifying computation of GM bound

Lemma

Let $\Lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$ *with* $\lambda_1 < \lambda_2 < \ldots < \lambda_n$ *and* $\lambda_1 < q$.

1. *Let* λ_j *be the maximum generator strictly smaller than* $\frac{q}{\left\lfloor \frac{q}{\lambda_1} \right\rfloor}$ *then* $\Lambda \setminus \cup_{i=1}^{n} (q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i=1}^{j} (q\lambda_i + \Lambda)$.
2. *Let* λ_j *be the maximum generator strictly smaller than* $2\lambda_1 - 1$ *then* $\Lambda \setminus \cup_{i=1}^{n} (q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i=1}^{j} (q\lambda_i + \Lambda)$.