A Gröbner basis approach for counting rational places in algebraic function fields

Kasper Halbak Christensen and Olav Geil
Aalborg University
Denmark

Meeting of the Catalan, Spanish, Swedish Math Societies
(CAT-SP-SW-MATH), Umeå, June 12th–15th, 2017

Function fields and rational places

Function field:
F a finite algebraic extension of $\mathbb{F}_q(X)$.

Valuation ring:
$\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$ where $\forall z \in F$ we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

(Rational) place:
$P = \mathcal{O} \backslash \mathcal{O}^*$ is the unique maximal ideal of $\mathcal{O}$.
P is rational if $\mathcal{O}/P \simeq \mathbb{F}_q$.

Valuation: $\exists t$ such that $P = \langle t \rangle$. $\forall z \in F \backslash \{0\}$ we uniquely can write $z = t^n u$ where $u \in \mathcal{O}^*$.

$$v_P : \begin{cases} F \to \mathbb{Z} \cup \infty \\ v_p(z) = \begin{cases} n & \text{if } z = t^n u \\ \infty & \text{if } z = 0 \end{cases} \end{cases}$$

Function fields and rational places

Function field:
F a finite algebraic extension of $\mathbb{F}_q(X)$.

Valuation ring:
$\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$ where $\forall z \in F$ we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

(Rational) place:
$P = \mathcal{O} \backslash \mathcal{O}^*$ is the unique maximal ideal of $\mathcal{O}$.
P is rational if $\mathcal{O}/P \simeq \mathbb{F}_q$.

Valuation: $\exists t$ such that $P = \langle t \rangle$. $\forall z \in F \backslash \{0\}$ we uniquely can write $z = t^n u$ where $u \in \mathcal{O}^*$.

$$v_P : \begin{cases} F \to \mathbb{Z} \cup \infty \\ v_p(z) = \begin{cases} n & \text{if } z = t^n u \\ \infty & \text{if } z = 0 \end{cases} \end{cases}$$

Function fields and rational places

Function field:
F a finite algebraic extension of $\mathbb{F}_q(X)$.

Valuation ring:
$\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$ where $\forall z \in F$ we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

(Rational) place:
$P = \mathcal{O} \backslash \mathcal{O}^*$ is the unique maximal ideal of $\mathcal{O}$.
P is rational if $\mathcal{O}/P \simeq \mathbb{F}_q$.

Valuation: $\exists t$ such that $P = \langle t \rangle$. $\forall z \in F \backslash \{0\}$ we uniquely can write $z = t^n u$ where $u \in \mathcal{O}^*$.

$$v_P : \begin{cases} F \to \mathbb{Z} \cup \infty \\ v_p(z) = \begin{cases} n & \text{if } z = t^n u \\ \infty & \text{if } z = 0 \end{cases} \end{cases}$$

Weierstrass semigroups

Let P be a rational place.

$\mathcal{L}$-space:
$\mathcal{L}(nP) = \{z \in F \mid v_P(z) \geq -n, \text{ and } v_Q(z) \geq 0, \forall Q \neq P\}$
$\mathcal{L}(\infty P) = \cup_{n \geq 0} \mathcal{L}(nP)$

Weierstrass semigroup:
$\Lambda_P = -v_P(\mathcal{L}(\infty P)) = \langle w_1, \dots, w_m \rangle$.

Genus (an invariant of F):
$g = \#(\mathbb{N}_0 \backslash \Lambda_P)$.

Weierstrass semigroups

Let P be a rational place.

$\mathcal{L}$-space:
$\mathcal{L}(nP) = \{z \in F \mid v_P(z) \geq -n, \text{ and } v_Q(z) \geq 0, \forall Q \neq P\}$
$\mathcal{L}(\infty P) = \cup_{n \geq 0} \mathcal{L}(nP)$

Weierstrass semigroup:
$\Lambda_P = -v_P(\mathcal{L}(\infty P)) = \langle w_1, \ldots, w_m \rangle$.

Genus (an invariant of F):
$g = \#(\mathbb{N}_0 \backslash \Lambda_P)$.

The maximal number of rational places

$N(F) = \#$ rational places in F.

$g(F) =$ the genus of F.

$N_q(g) = \max\{N(F) \mid F$ a function field over $\mathbb{F}_q$ with $g(F) = g\}$.

Application in coding theory. Ensures high information rate while still allowing for error-correction.

The maximal number of rational places

$N(F) = \#$ rational places in F.

$g(F) =$ the genus of F.

$N_q(g) = \max\{N(F) \mid F$ a function field over $\mathbb{F}_q$ with $g(F) = g\}$.

Application in coding theory. Ensures high information rate while still allowing for error-correction.

The maximal number of rational places

$N(F) = \#$ rational places in F.

$g(F) =$ the genus of F.

$N_q(g) = \max\{N(F) \mid F$ a function field over $\mathbb{F}_q$ with $g(F) = g\}$.

Application in coding theory. Ensures high information rate while still allowing for error-correction.

The objective

Data base with known information on $N_q(g)$ at `manypoints.org`

Hasse-Weil bound:
$|N(F) - (q+1)| \leq 2g\sqrt{q}$

But also bounds in **terms of a Weierstrass semigroup of** F rather than genus:
If $\Lambda = \langle w_1, \ldots, w_m \rangle$ then
$N(F) \leq |\Lambda \setminus \cup_{i=1}^{m} (qw_i + \Lambda)| + 1.$

Or bounds using **partial information on semigroup**:
$N(F) \leq qw_1 + 1.$

The objective

Data base with known information on $N_q(g)$ at `manypoints.org`

Hasse-Weil bound:
$|N(F) - (q+1)| \leq 2g\sqrt{q}$

But also bounds in **terms of a Weierstrass semigroup of** F rather than genus:
If $\Lambda = \langle w_1, \ldots, w_m \rangle$ then
$N(F) \leq |\Lambda \setminus \cup_{i=1}^{m} (qw_i + \Lambda)| + 1.$

Or bounds using **partial information on semigroup**:
$N(F) \leq qw_1 + 1.$

The objective

Data base with known information on $N_q(g)$ at `manypoints.org`

Hasse-Weil bound:
$|N(F) - (q+1)| \leq 2g\sqrt{q}$

But also bounds in **terms of a Weierstrass semigroup of** F rather than genus:
If $\Lambda = \langle w_1, \ldots, w_m \rangle$ then
$N(F) \leq |\Lambda \setminus \cup_{i=1}^{m} (qw_i + \Lambda)| + 1.$

Or bounds using **partial information on semigroup**:
$N(F) \leq qw_1 + 1.$

The objective

Data base with known information on $N_q(g)$ at `manypoints.org`

Hasse-Weil bound:
$|N(F) - (q+1)| \leq 2g\sqrt{q}$

But also bounds in **terms of a Weierstrass semigroup of** F rather than genus:
If $\Lambda = \langle w_1, \ldots, w_m \rangle$ then
$N(F) \leq |\Lambda \setminus \cup_{i=1}^{m} (qw_i + \Lambda)| + 1.$

Or bounds using **partial information on semigroup**:
$N(F) \leq qw_1 + 1.$

A particular simple example

Consider $\mathbb{F}_q = \mathbb{F}_{t^2}$ and $g = \frac{t(t-1)}{2}$.

Hasse-Weil says:
$N_q(g) \leq 2\frac{t(t+1)}{2}t + t^2 + 1 = t^3 + 1$.

$\Lambda = \langle t, t+1 \rangle$ has genus $\frac{t(t-1)}{2}$.

Hermitian function field has Λ as Weirstrass semigroup for P where $\mathcal{L}(\infty P) = \mathbb{F}_q[X, Y]/\langle X^{t+1} - Y^t - Y \rangle$.

The affine variety of $\langle X^{t+1} - Y^t - Y, X^q - X, Y^q - Y \rangle$ is of size t^3.

Conclusion: The Hermitian function field has $t^3 + 1$ rational places.

Therefore, $N_q(g) = t^3 + 1$ for $g = \frac{t(t-1)}{2}$.

A particular simple example

Consider $\mathbb{F}_q = \mathbb{F}_{t^2}$ and $g = \frac{t(t-1)}{2}$.

Hasse-Weil says:
$N_q(g) \leq 2\frac{t(t+1)}{2}t + t^2 + 1 = t^3 + 1$.

$\Lambda = \langle t, t+1 \rangle$ has genus $\frac{t(t-1)}{2}$.

Hermitian function field has Λ as Weirstrass semigroup for P where $\mathcal{L}(\infty P) = \mathbb{F}_q[X, Y]/\langle X^{t+1} - Y^t - Y \rangle$.

The affine variety of $\langle X^{t+1} - Y^t - Y, X^q - X, Y^q - Y \rangle$ is of size t^3.

Conclusion: The Hermitian function field has $t^3 + 1$ rational places.

Therefore, $N_q(g) = t^3 + 1$ for $g = \frac{t(t-1)}{2}$.

A particular simple example

Consider $\mathbb{F}_q = \mathbb{F}_{t^2}$ and $g = \frac{t(t-1)}{2}$.

Hasse-Weil says:
$N_q(g) \leq 2\frac{t(t+1)}{2}t + t^2 + 1 = t^3 + 1$.

$\Lambda = \langle t, t+1 \rangle$ has genus $\frac{t(t-1)}{2}$.

Hermitian function field has Λ as Weirstrass semigroup for P where $\mathcal{L}(\infty P) = \mathbb{F}_q[X, Y]/\langle X^{t+1} - Y^t - Y \rangle$.

The affine variety of $\langle X^{t+1} - Y^t - Y, X^q - X, Y^q - Y \rangle$ is of size t^3.

Conclusion: The Hermitian function field has $t^3 + 1$ rational places.

Therefore, $N_q(g) = t^3 + 1$ for $g = \frac{t(t-1)}{2}$.

The general problem of estimating $N_q(g)$

Lower bounds on $N_q(g)$ are established by determining and studying new function fields.

Methods are involved: algebraic geometry and function field theory.

The idea in the present project:
To use insight on simplified description of $\mathcal{L}(\infty Q)$ in combination with computer search to say something about $N_q(\Lambda)$ or $N_q(g)$ when possible.

The general problem of estimating $N_q(g)$

Lower bounds on $N_q(g)$ are established by determining and studying new function fields.

Methods are involved: algebraic geometry and function field theory.

The idea in the present project:
To use insight on simplified description of $\mathcal{L}(\infty Q)$ in combination with computer search to say something about $N_q(\Lambda)$ or $N_q(g)$ when possible.

Background

In coding theory one only uses $R = \mathcal{L}(\infty P)$ (or the generalization to more places), but only seldom the function field $\mathrm{Quot}(R)$.

Høholdt, van Lint, Pellikaan and Miura introduced the concept of order domains to obtain:

- simplified understanding of $\mathcal{L}(\infty P)$ and corresponding codes
- generalizations to structures of higher transcendence degree.

Miura and Pellikaan (and G) showed that finitely generated order domains R (over $\mathbb{F}_q$) are equivalent to:

- quotient rings $\mathbb{F}_q[X_1, \ldots, X_m]/I$ where I satisfies certain Gröbner basis theoretical properties.

Matsumoto showed that for transcendence degree 1 (semigroups being numerical):

- $R \subseteq \mathcal{L}(\infty P)$ with equality if the "curve" is non-singular.
- The number of rational places equals the number of affine roots of I over $\mathbb{F}_q$ plus 1.

Background

In coding theory one only uses $R = \mathcal{L}(\infty P)$ (or the generalization to more places), but only seldom the function field Quot(R).

Høholdt, van Lint, Pellikaan and Miura introduced the concept of order domains to obtain:

- simplified understanding of $\mathcal{L}(\infty P)$ and corresponding codes
- generalizations to structures of higher transcendence degree.

Miura and Pellikaan (and G) showed that finitely generated order domains R (over $\mathbb{F}_q$) are equivalent to:

- quotient rings $\mathbb{F}_q[X_1, \ldots, X_m)/I$ where I satisfies certain Gröbner basis theoretical properties.

Matsumoto showed that for transcendence degree 1 (semigroups being numerical):

- $R \subseteq \mathcal{L}(\infty P)$ with equality if the "curve" is non-singular.
- The number of rational places equals the number of affine roots of I over $\mathbb{F}_q$ plus 1.

Background

In coding theory one only uses $R = \mathcal{L}(\infty P)$ (or the generalization to more places), but only seldom the function field Quot(R).

Høholdt, van Lint, Pellikaan and Miura introduced the concept of order domains to obtain:

- simplified understanding of $\mathcal{L}(\infty P)$ and corresponding codes
- generalizations to structures of higher transcendence degree.

Miura and Pellikaan (and G) showed that finitely generated order domains R (over $\mathbb{F}_q$) are equivalent to:

- quotient rings $\mathbb{F}_q[X_1, \ldots, X_m)/I$ where I satisfies certain Gröbner basis theoretical properties.

Matsumoto showed that for transcendence degree 1 (semigroups being numerical):

- $R \subseteq \mathcal{L}(\infty P)$ with equality if the "curve" is non-singular.
- The number of rational places equals the number of affine roots of I over $\mathbb{F}_q$ plus 1.

Background

In coding theory one only uses $R = \mathcal{L}(\infty P)$ (or the generalization to more places), but only seldom the function field Quot(R).

Høholdt, van Lint, Pellikaan and Miura introduced the concept of order domains to obtain:

- simplified understanding of $\mathcal{L}(\infty P)$ and corresponding codes
- generalizations to structures of higher transcendence degree.

Miura and Pellikaan (and G) showed that finitely generated order domains R (over $\mathbb{F}_q$) are equivalent to:

- quotient rings $\mathbb{F}_q[X_1, \ldots, X_m)/I$ where I satisfies certain Gröbner basis theoretical properties.

Matsumoto showed that for transcendence degree 1 (semigroups being numerical):

- $R \subseteq \mathcal{L}(\infty P)$ with equality if the "curve" is non-singular.
- The number of rational places equals the number of affine roots of I over $\mathbb{F}_q$ plus 1.

The order domain conditions (trdg=1)

Weighted degree ordering $\prec_w$ on monomials in $X_1, \ldots, X_m$:

$X_1^{i_1} \cdots X_m^{i_m} \prec_w X_1^{j_1} \cdots X_m^{j_m}$ if

- either $w_1 i_1 + \cdots + w_m i_m < w_1 j_1 + \cdots + w_m j_m$
- or $w_1 i_1 + \cdots + w_m i_m = w_1 j_1 + \cdots + w_m j_m$, but $X_1^{i_1} \cdots X_m^{i_m} \prec X_1^{j_1} \cdots X_m^{j_m}$, where $\prec$ is a second fixed monomial ordering (for example lexicographic)

An ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ is said to satisfy the order domain conditions if:

- There exists a Gröbner basis $\{F_1, \ldots, F_s\}$ for I with respect to $\prec_w$ such that every F_i possesses (exactly) two monomials of highest weight in its support.
- For the set of monomials which are NOT leading monomials of any polynomial in I, no two have the same weight.

The order domain conditions (trdg=1)

Weighted degree ordering $\prec_w$ on monomials in $X_1, \ldots, X_m$:

$X_1^{i_1} \cdots X_m^{i_m} \prec_w X_1^{j_1} \cdots X_m^{j_m}$ if

- either $w_1 i_1 + \cdots + w_m i_m < w_1 j_1 + \cdots + w_m j_m$
- or $w_1 i_1 + \cdots + w_m i_m = w_1 j_1 + \cdots + w_m j_m$, but $X_1^{i_1} \cdots X_m^{i_m} \prec X_1^{j_1} \cdots X_m^{j_m}$, where $\prec$ is a second fixed monomial ordering (for example lexicographic)

An ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ is said to satisfy the order domain conditions if:

- There exists a Gröbner basis $\{F_1, \ldots, F_s\}$ for I with respect to $\prec_w$ such that every F_i possesses (exactly) two monomials of highest weight in its support.
- For the set of monomials which are NOT leading monomials of any polynomial in I, no two have the same weight.

Our approach

Given $\Lambda = \langle w_1, \dots, w_m \rangle$
We start by establishing a minimal **Gröbner basis for the binomial ideal**

$$I_w = \langle X_1^{i_1} \cdots X_m^{i_m} - X_1^{j_1} \cdots X_m^{j_m} \mid w_1 i_1 + \cdots + w_m i_m = w_1 j_1 + \cdots + w_m j_m \rangle$$

with respect to the weighted degree ordering. Elimination via:

$$\langle T^{w_1} - X_1, T^{w_2} - X_2, \dots, T^{w_m} - X_m \rangle$$

The above description satisfies the order domain conditions...but we only have q affine points ($q+1$ rational places). Hence, the next step is to try to add more terms (of lower weight) in such a way that the polynomials still constitute a Gröbner basis.

For principal ideals, i.e. $\Lambda = \langle w_1, w_2 \rangle$ we can add anything!!!

Our approach

Given $\Lambda = \langle w_1, \ldots, w_m \rangle$
We start by establishing a minimal **Gröbner basis for the binomial ideal**

$$I_w = \langle X_1^{i_1} \cdots X_m^{i_m} - X_1^{j_1} \cdots X_m^{j_m} \mid w_1 i_1 + \cdots + w_m i_m = w_1 j_1 + \cdots + w_m j_m \rangle$$

with respect to the weighted degree ordering. Elimination via:

$$\langle T^{w_1} - X_1, T^{w_2} - X_2, \ldots, T^{w_m} - X_m \rangle$$

The above description satisfies the order domain conditions...but we only have q affine points ($q+1$ rational places). Hence, the next step is to try to add more terms (of lower weight) in such a way that the polynomials still constitute a Gröbner basis.

For principal ideals, i.e. $\Lambda = \langle w_1, w_2 \rangle$ we can add anything!!!

Our approach

Given $\Lambda = \langle w_1, \ldots, w_m \rangle$
We start by establishing a minimal **Gröbner basis for the binomial ideal**

$$I_w = \langle X_1^{i_1} \cdots X_m^{i_m} - X_1^{j_1} \cdots X_m^{j_m} \mid w_1 i_1 + \cdots + w_m i_m = w_1 j_1 + \cdots + w_m j_m \rangle$$

with respect to the weighted degree ordering. Elimination via:

$$\langle T^{w_1} - X_1, T^{w_2} - X_2, \ldots, T^{w_m} - X_m \rangle$$

The above description satisfies the order domain conditions...but we only have q affine points ($q+1$ rational places). Hence, the next step is to try to add more terms (of lower weight) in such a way that the polynomials still constitute a Gröbner basis.

For principal ideals, i.e. $\Lambda = \langle w_1, w_2 \rangle$ we can add anything!!!

Binomial ideals (with Ali Sepas):

Example:
$\Lambda = \langle 3, 5, 7 \rangle$. We investigate weighted degree orderings according to weights $w_1 = 3$, $w_2 = 5$, $w_3 = 7$, with the second ordering being lexicographic.

Both $X \succ_{lex} Y \succ_{lex} Z$ and $X \succ_{lex} Z \succ_{lex} Y$ give GB with 6 polynomials:
$\{Y^7 - Z^5, XZ - Y^2, XY^5 - Z^4, X^2Y^3 - Z^3, X^3Y - Z^2, X^4 - YZ\}$

All other choices of lexicographic part give GB with 4 polynomials. For instance both $Z \succ_{lex} X \succ_{lex} Y$ and $Z \succ_{lex} Y \succ_{lex} X$ give:
$\{X^5 - Y^3, ZY - X^4, ZX - Y^2, Z^2 - X^3Y\}$.

Binomial ideals (with Ali Sepas):

Example:
$\Lambda = \langle 3, 5, 7 \rangle$. We investigate weighted degree orderings according to weights $w_1 = 3$, $w_2 = 5$, $w_3 = 7$, with the second ordering being lexicographic.

Both $X \succ_{lex} Y \succ_{lex} Z$ and $X \succ_{lex} Z \succ_{lex} Y$ give GB with 6 polynomials:
$\{Y^7 - Z^5, XZ - Y^2, XY^5 - Z^4, X^2Y^3 - Z^3, X^3Y - Z^2, X^4 - YZ\}$

All other choices of lexicographic part give GB with 4 polynomials.
For instance both $Z \succ_{lex} X \succ_{lex} Y$ and $Z \succ_{lex} Y \succ_{lex} X$ give:
$\{X^5 - Y^3, ZY - X^4, ZX - Y^2, Z^2 - X^3Y\}$.

From binomial ideal to $\mathcal{L}(\infty P)$

If binomials are successfully modified to other polynomials $\{F_1, \ldots, F_s\}$ satisfying the order domain conditions, then we:

- Check if $1 \in \langle F_i, \frac{\partial F_i}{\partial X_j} \mid 1 \leq i \leq s \text{ and } 1 \leq j \leq m \rangle$ in which case $\mathcal{L}(\infty P) = \mathbb{F}_q[X_1, \ldots, X_m]/\langle F_1, \ldots, F_s \rangle$.
- Determine the number of affine points by establishing a Gröbner basis for $\langle F_1, \ldots, F_s, X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ and by using the footprint bound.

From binomial ideal to $\mathcal{L}(\infty P)$

If binomials are successfully modified to other polynomials $\{F_1, \ldots, F_s\}$ satisfying the order domain conditions, then we:

- Check if $1 \in \langle F_i, \frac{\partial F_i}{\partial X_j} \mid 1 \leq i \leq s \text{ and } 1 \leq j \leq m \rangle$ in which case $\mathcal{L}(\infty P) = \mathbb{F}_q[X_1, \ldots, X_m]/\langle F_1, \ldots, F_s \rangle$.
- Determine the number of affine points by establishing a Gröbner basis for $\langle F_1, \ldots, F_s, X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ and by using the footprint bound.

From binomial ideal to $\mathcal{L}(\infty P)$

If binomials are successfully modified to other polynomials $\{F_1, \ldots, F_s\}$ satisfying the order domain conditions, then we:

- Check if $1 \in \langle F_i, \frac{\partial F_i}{\partial X_j} \mid 1 \leq i \leq s \text{ and } 1 \leq j \leq m \rangle$ in which case $\mathcal{L}(\infty P) = \mathbb{F}_q[X_1, \ldots, X_m]/\langle F_1, \ldots, F_s \rangle$.
- Determine the number of affine points by establishing a Gröbner basis for $\langle F_1, \ldots, F_s, X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ and by using the footprint bound.

The footprint bound

By definition, a **Gröbner basis** for I is a generating set $\{F_1, \ldots, F_s\}$ such that if $F \in I$ then $\mathrm{lm}(F)$ is divisible by some $\mathrm{lm}(F_i)$.

By definition, the **footprint** of an ideal with respect to a monomial ordering is the set of monomials that are not leading monomial of any polynomial in I. Is easily read of from the Gröbner basis.

The footprint bound: If the footprint is finite, then the size of the corresponding affine variety is at most equal to the size of the footprint.

If $\mathbb{F}$ is perfect and I contains a square free univariate polynomial in each variable then equality holds.

Hence, we consider the footprint of $I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

The footprint bound

By definition, a **Gröbner basis** for I is a generating set $\{F_1, \ldots, F_s\}$ such that if $F \in I$ then $\mathrm{lm}(F)$ is divisible by some $\mathrm{lm}(F_i)$.

By definition, the **footprint** of an ideal with respect to a monomial ordering is the set of monomials that are not leading monomial of any polynomial in I. Is easily read of from the Gröbner basis.

The footprint bound: If the footprint is finite, then the size of the corresponding affine variety is at most equal to the size of the footprint.

If $\mathbb{F}$ is perfect and I contains a square free univariate polynomial in each variable then equality holds.

Hence, we consider the footprint of $I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

The footprint bound

By definition, a **Gröbner basis** for I is a generating set $\{F_1, \ldots, F_s\}$ such that if $F \in I$ then $\mathrm{lm}(F)$ is divisible by some $\mathrm{lm}(F_i)$.

By definition, the **footprint** of an ideal with respect to a monomial ordering is the set of monomials that are not leading monomial of any polynomial in I. Is easily read of from the Gröbner basis.

The footprint bound: If the footprint is finite, then the size of the corresponding affine variety is at most equal to the size of the footprint.

If $\mathbb{F}$ is perfect and I contains a square free univariate polynomial in each variable then equality holds.

Hence, we consider the footprint of $I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

The footprint bound

By definition, a **Gröbner basis** for I is a generating set $\{F_1, \ldots, F_s\}$ such that if $F \in I$ then $\mathrm{lm}(F)$ is divisible by some $\mathrm{lm}(F_i)$.

By definition, the **footprint** of an ideal with respect to a monomial ordering is the set of monomials that are not leading monomial of any polynomial in I. Is easily read of from the Gröbner basis.

The footprint bound: If the footprint is finite, then the size of the corresponding affine variety is at most equal to the size of the footprint.

If $\mathbb{F}$ is perfect and I contains a square free univariate polynomial in each variable then equality holds.

Hence, we consider the footprint of $I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

Preliminary results

- The bound $N_q(\langle w_1, w_2 \rangle) \leq \min\{qw_1 + 1, q^2 + 1\}$ is often sharp, but not always.
- New study: Lower bounds on the minimal number of rational places
- For more generators $w_1, \ldots, w_m$ the method needs to be refined to be efficient.
- Maybe one should start with a minimal generating set of polynomials (not GB), add lower terms and first then calculate GB. (For calculation of minimal generating sets see: Chap. 4 of Assi and García-Sánchez, "Numerical Semigroups and Applications," Springer 2016).
- ...or...we have other ideas.

Preliminary results

- The bound $N_q(\langle w_1, w_2 \rangle) \leq \min\{qw_1 + 1, q^2 + 1\}$ is often sharp, but not always.
- New study: Lower bounds on the minimal number of rational places
- For more generators $w_1, \ldots, w_m$ the method needs to be refined to be efficient.
- Maybe one should start with a minimal generating set of polynomials (not GB), add lower terms and first then calculate GB. (For calculation of minimal generating sets see: Chap. 4 of Assi and García-Sánchez, "Numerical Semigroups and Applications," Springer 2016).
- ...or...we have other ideas.

Preliminary results

- The bound $N_q(\langle w_1, w_2 \rangle) \leq \min\{qw_1 + 1, q^2 + 1\}$ is often sharp, but not always.
- New study: Lower bounds on the minimal number of rational places
- For more generators $w_1, \ldots, w_m$ the method needs to be refined to be efficient.
- Maybe one should start with a minimal generating set of polynomials (not GB), add lower terms and first then calculate GB. (For calculation of minimal generating sets see: Chap. 4 of Assi and García-Sánchez, "Numerical Semigroups and Applications," Springer 2016).
- ...or...we have other ideas.

Preliminary results

- The bound $N_q(\langle w_1, w_2 \rangle) \leq \min\{qw_1 + 1, q^2 + 1\}$ is often sharp, but not always.
- New study: Lower bounds on the minimal number of rational places
- For more generators $w_1, \ldots, w_m$ the method needs to be refined to be efficient.
- Maybe one should start with a minimal generating set of polynomials (not GB), add lower terms and first then calculate GB. (For calculation of minimal generating sets see: Chap. 4 of Assi and García-Sánchez, "Numerical Semigroups and Applications," Springer 2016).
- ...or...we have other ideas.

Preliminary results

- The bound $N_q(\langle w_1, w_2 \rangle) \leq \min\{qw_1 + 1, q^2 + 1\}$ is often sharp, but not always.
- New study: Lower bounds on the minimal number of rational places
- For more generators $w_1, \ldots, w_m$ the method needs to be refined to be efficient.
- Maybe one should start with a minimal generating set of polynomials (not GB), add lower terms and first then calculate GB. (For calculation of minimal generating sets see: Chap. 4 of Assi and García-Sánchez, "Numerical Semigroups and Applications," Springer 2016).
- ...or...we have other ideas.

Two generators

Maximal number of rational places (exhaustive search except for $*$)

$\Lambda \backslash q$	2	3	4	8	9
$\langle 2,3 \rangle$	5	7	9	13	16
$\langle 2,5 \rangle$	5	7	9	17	19
$\langle 2,7 \rangle$	5	7	9	17	19
$\langle 3,4 \rangle$	5	10	13	21^*	28
$\langle 2,9 \rangle$	5	7	9	17	19
$\langle 3,5 \rangle$	5	10	13	–	–
$\langle 4,5 \rangle$	5	10	17	–	–

Two generators

Minimal number of rational places (exhaustive search except for $*$)

$\Lambda \backslash q$	2	3	4	8	9	16	27	32
$\langle 2, 3 \rangle$	1	1	1	5	4	9^*	19^*	25^*
$\langle 2, 5 \rangle$	1	1	1	1	1	8^*	19^*	25^*
$\langle 3, 4 \rangle$	1	1	1	2^*	–	–	–	–

- T. Høholdt, J. van Lint and R. Pellikaan, "Algebraic Geometry Codes," Chapter 10 in *Handbook of Coding Thoery*, (V. S. Pless and W. C. Huffman eds), Vol. 1, Elsevier, 1998, pp. 871–961
- S. Miura, "Linear Codes on Affine Algebraic Varieties," *Trans. IEICE*, Vol. J81-A, 1998, pp. 1386-1397 (in Japanese).
- R. Matsumoto, "Miura's Generalization of One-Point AG codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization," *IEICE Trans. Fundamentals,* Vol. E82-A, 1999, pp. 2007-2010
- R. Matsumoto and S. Miura, "On Construction and Generalization of Algebraic Geometry Codes," textitProc. of Algebraic Geometry, Number Thoery, Coding Theory and Cryptography, Univ. of Tokyo, January 19-20, 2000, (Ed. T. Katsura et al.), 2000, pp. 3-15
- R. Pellikaan, "On the existence of order functions," *Journal of Statistical Planning and Inference*, Vol. 94, 2001, pp. 287–301

O. Geil and R. Pellikaan, "On the structure of order domains," *Finite Fields and Appl.*, Vol. 8, 2002, pp. 369–396.