BOUNDING THE NUMBER OF AFFINE ROOTS

with applications in communication theory

Olav Geil
Aalborg University
Denmark

NORCOM 2019, Schæffergården, Denmark, August 5–7, 2019

Outline

- Part 1: Affine roots counted without multiplicity. The footprint bound mainly applied to Cartesian product point sets
- Part 2: Affine roots from Cartesian product point sets counted with multiplicity
- Part 3: Points on curves. Algebraic geometric codes
- Part 4: Remarks on general linear codes

Part 1:

Affine roots counted without multiplicity. The footprint bound mainly applied to Cartesian product point sets

Why polynomials?

When working over finite fields all functions are polynomials.

Lagrange interpolation:

$F : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^n$ is defined by its q^m values.

Given $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ the polynomial

$$\frac{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (X_i - \beta)}{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (\alpha_i - \beta)}$$

evaluates to 1 in $\vec{\alpha}$ and to 0 every where else.

Take proper "linear" combinations of terms of above type.

Why polynomials?

When working over finite fields all functions are polynomials.

Lagrange interpolation:

$F : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^n$ is defined by its q^m values.

Given $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ the polynomial

$$\frac{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (X_i - \beta)}{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (\alpha_i - \beta)}$$

evaluates to 1 in $\vec{\alpha}$ and to 0 every where else.

Take proper "linear" combinations of terms of above type.

Why polynomials?

When working over finite fields all functions are polynomials.

Lagrange interpolation:

$F : \mathbb{F}_q^m \to \mathbb{F}_q^n$ is defined by its q^m values.

Given $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ the polynomial

$$\frac{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (X_i - \beta)}{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (\alpha_i - \beta)}$$

evaluates to 1 in $\vec{\alpha}$ and to 0 every where else.

Take proper "linear" combinations of terms of above type.

Why polynomials?

When working over finite fields all functions are polynomials.

Lagrange interpolation:

$F : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^n$ is defined by its q^m values.

Given $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ the polynomial

$$\frac{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (X_i - \beta)}{\prod_{i=1}^{m} \prod_{\beta \in \mathbb{F}_q \setminus \{\alpha_i\}} (\alpha_i - \beta)}$$

evaluates to 1 in $\vec{\alpha}$ and to 0 every where else.

Take proper "linear" combinations of terms of above type.

$F : \mathbb{F}_3^2 \to \mathbb{F}_3$ given by

$$\begin{array}{lll} F(0,0)=2 & F(0,1)=1 & F(0,2)=1 \\ F(1,0)=0 & F(1,1)=1 & F(1,2)=0 \\ F(2,0)=1 & F(2,1)=1 & F(2,2)=2 \end{array}$$

As a polynomial:

$F(X,Y) =$

$$\frac{(X-1)(X-2)(Y-1)(Y-2)}{(0-1)(0-2)(0-1)(0-2)}2+\frac{(X-1)(X-2)(Y-0)(Y-2)}{(0-1)(0-2)(1-0)(1-2)}1+\cdots$$

$$+\frac{(X-0)(X-1)(Y-0)(Y-2)}{(2-0)(2-1)(1-0)(1-2)}1+\frac{(X-0)(X-1)(Y-0)(Y-1)}{(2-0)(2-1)(2-0)(2-1)}2$$

$$= 2XY + 2Y^2 + X + 2$$

(In general $2XY + 2Y^2 + X + 2 + A(X,Y)(X^3 - X) + B(X,Y)(Y^3 - Y)$ works)

$F : \mathbb{F}_3^2 \to \mathbb{F}_3$ given by

$$\begin{array}{lll} F(0,0)=2 & F(0,1)=1 & F(0,2)=1 \\ F(1,0)=0 & F(1,1)=1 & F(1,2)=0 \\ F(2,0)=1 & F(2,1)=1 & F(2,2)=2 \end{array}$$

As a polynomial:

$F(X,Y) =$

$$\frac{(X-1)(X-2)(Y-1)(Y-2)}{(0-1)(0-2)(0-1)(0-2)}2+\frac{(X-1)(X-2)(Y-0)(Y-2)}{(0-1)(0-2)(1-0)(1-2)}1+\cdots$$

$$+\frac{(X-0)(X-1)(Y-0)(Y-2)}{(2-0)(2-1)(1-0)(1-2)}1+\frac{(X-0)(X-1)(Y-0)(Y-1)}{(2-0)(2-1)(2-0)(2-1)}2$$

$$= 2XY + 2Y^2 + X + 2$$

(In general
$2XY + 2Y^2 + X + 2 + A(X,Y)(X^3 - X) + B(X,Y)(Y^3 - Y)$
works)

$F : \mathbb{F}_3^2 \rightarrow \mathbb{F}_3$ given by

$$\begin{array}{lll} F(0,0)=2 & F(0,1)=1 & F(0,2)=1 \\ F(1,0)=0 & F(1,1)=1 & F(1,2)=0 \\ F(2,0)=1 & F(2,1)=1 & F(2,2)=2 \end{array}$$

As a polynomial:

$F(X,Y) =$

$$\frac{(X-1)(X-2)(Y-1)(Y-2)}{(0-1)(0-2)(0-1)(0-2)}2+\frac{(X-1)(X-2)(Y-0)(Y-2)}{(0-1)(0-2)(1-0)(1-2)}1+\cdots$$

$$+\frac{(X-0)(X-1)(Y-0)(Y-2)}{(2-0)(2-1)(1-0)(1-2)}1+\frac{(X-0)(X-1)(Y-0)(Y-1)}{(2-0)(2-1)(2-0)(2-1)}2$$

$$= 2XY + 2Y^2 + X + 2$$

(In general
$2XY + 2Y^2 + X + 2 + A(X,Y)(X^3 - X) + B(X,Y)(Y^3 - Y)$
works)

Restricting to powers less than q

$F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ has the same function values (and in particular roots) as

$$F(X_1, \ldots, X_m) + A_1(X_1, \ldots, X_m)(X_1^q - X_1) + \cdots + A_m(X_1, \ldots, X_m)(X_m^q - X_m).$$

Therefore $F(X_1, \ldots, X_m)$ has the same function values as $F(X_1, \ldots, X_m)$ rem $\{X_1^q - X_1, \ldots, X_m^q - X_m\}$.

Hence, as long as we are only interested in roots and do not count multiplicity we may restrict to:

$\deg_{X_i}(F) < q$ for $i = 1, \ldots, m$.

Restricting to powers less than q

$F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ has the same function values (and in particular roots) as

$$F(X_1, \ldots, X_m) + A_1(X_1, \ldots, X_m)(X_1^q - X_1) + \cdots + A_m(X_1, \ldots, X_m)(X_m^q - X_m).$$

Therefore $F(X_1, \ldots, X_m)$ has the same function values as $F(X_1, \ldots, X_m)$ rem $\{X_1^q - X_1, \ldots, X_m^q - X_m\}$.

Hence, as long as we are only interested in roots and do not count multiplicity we may restrict to:

$\deg_{X_i}(F) < q$ for $i = 1, \ldots, m$.

Restricting to powers less than q

$F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ has the same function values (and in particular roots) as

$$F(X_1, \ldots, X_m)+$$
$$A_1(X_1, \ldots, X_m)(X_1^q - X_1) + \cdots + A_m(X_1, \ldots, X_m)(X_m^q - X_m).$$

Therefore $F(X_1, \ldots, X_m)$ has the same function values as $F(X_1, \ldots, X_m)$ rem $\{X_1^q - X_1, \ldots, X_m^q - X_m\}$.

Hence, as long as we are only interested in roots and do not count multiplicity we may restrict to:

$\deg_{X_i}(F) < q$ for $i = 1, \ldots, m$.

From one variable to more

$F(X) \in \mathbb{F}[X]$ has at most $\deg F$ roots over $\mathbb{F}$ (even when counted with multiplicity).

How to generalize to more variables?

$F(X, Y) \in \mathbb{R}[X, Y]$ most probably has infinitely many roots.

Example: $XY + 2$ has the roots $\{(k, -\frac{2}{k}) \mid k \in \mathbb{R} \backslash \{0\}\}$.

But if we are only looking for roots of $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ over finite set $S_1 \times \cdots \times S_m$, $S_i \in \mathbb{F}$ then finitely many roots.

...or if $\mathbb{F} = \mathbb{F}_q$ then again finitely many roots.

From one variable to more

$F(X) \in \mathbb{F}[X]$ has at most $\deg F$ roots over $\mathbb{F}$ (even when counted with multiplicity).

How to generalize to more variables?

$F(X, Y) \in \mathbb{R}[X, Y]$ most probably has infinitely many roots.

Example: $XY + 2$ has the roots $\{(k, -\frac{2}{k}) \mid k \in \mathbb{R} \backslash \{0\}\}$.

But if we are only looking for roots of $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ over finite set $S_1 \times \cdots \times S_m$, $S_i \in \mathbb{F}$ then finitely many roots.

...or if $\mathbb{F} = \mathbb{F}_q$ then again finitely many roots.

From one variable to more

$F(X) \in \mathbb{F}[X]$ has at most $\deg F$ roots over $\mathbb{F}$ (even when counted with multiplicity).

How to generalize to more variables?

$F(X, Y) \in \mathbb{R}[X, Y]$ most probably has infinitely many roots.

Example: $XY + 2$ has the roots $\{(k, -\frac{2}{k}) \mid k \in \mathbb{R}\backslash\{0\}\}$.

But if we are only looking for roots of $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ over finite set $S_1 \times \cdots \times S_m$, $S_i \in \mathbb{F}$ then finitely many roots.

...or if $\mathbb{F} = \mathbb{F}_q$ then again finitely many roots.

Roots over finite sets

$X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$. Hence, to look for roots of $F(X_1, \ldots, X_m)$ over $\mathbb{F}_q$ corresponds to looking for common roots of

$$\{F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m\}$$

If we look for roots over finite set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}$ we look for common roots of

$$\left\{F(X_1, \ldots, X_m), \prod_{\alpha \in S_1}(X_1 - \alpha), \ldots, \prod_{\alpha \in S_m}(X_m - \alpha)\right\}.$$

Roots over finite sets

$X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$. Hence, to look for roots of $F(X_1, \ldots, X_m)$ over $\mathbb{F}_q$ corresponds to looking for common roots of

$$\{F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m\}$$

If we look for roots over finite set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}$ we look for common roots of

$$\left\{F(X_1, \ldots, X_m), \prod_{\alpha \in S_1}(X_1 - \alpha), \ldots, \prod_{\alpha \in S_m}(X_m - \alpha)\right\}.$$

The polynomial $F(X, Y) = X^2Y + Y^2 + 2$ over $\mathbb{F}_5$

To look for roots of $F(X, Y)$ over $\mathbb{F}_5$ corresponds to looking for common roots of $\{F(X, Y), X^5 - X, Y^5 - Y\}$.

Figure: Two choices: $\mathrm{lm}(F) = X^2Y$ or $\mathrm{lm}(F) = Y^2$. Number of roots at most $\min\{13, 10\} = 10$

The polynomial $F(X,Y) = X^2Y + Y^2 + 2$ over $\mathbb{F}_5$

To look for roots of $F(X,Y)$ over $\mathbb{F}_5$ corresponds to looking for common roots of $\{F(X,Y), X^5 - X, Y^5 - Y\}$.

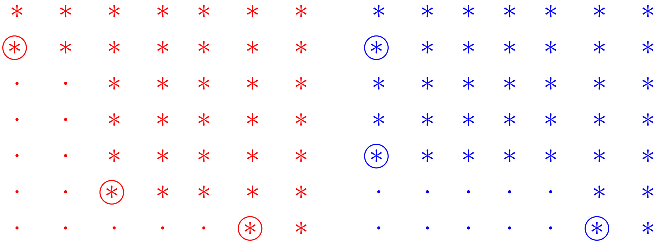


Figure: Two choices: $\mathrm{Im}(F) = X^2Y$ or $\mathrm{Im}(F) = Y^2$. Number of roots at most $\min\{13, 10\} = 10$

Univariate polynomials – revisited

How many roots can $F(X) = X^2 + aX + b$ have over $\mathbb{F}_5$?

In other words what is the maximal number of common roots of of $\{X^2 + aX + b, X^5 - X\}$?.

Figure: An alternative way to "see" the well-known result that a degree d univariate polynomial can have at most d roots

Univariate polynomials – revisited

How many roots can $F(X) = X^2 + aX + b$ have over $\mathbb{F}_5$?

In other words what is the maximal number of common roots of of $\{X^2 + aX + b, X^5 - X\}$?.

$$\cdot \quad \cdot \quad \circledast \quad * \quad * \quad \circledast \quad *$$

Figure: An alternative way to “see” the well-known result that a degree d univariate polynomial can have at most d roots

The footprint

Monomial ordering is a total ordering such that

- 1 is the smallest monomial
- multiplication of monomials respects the ordering.

For two (or more) variables there are infinitely many monomial orderings. For one variable only one.

Given an ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ and a monomial ordering $\prec$ the footprint is

$$\Delta_{\prec}(I) = \{X_1^{i_1} \cdots X_m^{i_m} \mid X_1^{i_1} \cdots X_m^{i_m} \text{ is not a leading monomial of any polynomial in } I\}$$

The footprint

Monomial ordering is a total ordering such that

- 1 is the smallest monomial
- multiplication of monomials respects the ordering.

For two (or more) variables there are infinitely many monomial orderings. For one variable only one.

Given an ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ and a monomial ordering $\prec$ the footprint is

$$\Delta_{\prec}(I) = \{X_1^{i_1} \cdots X_m^{i_m} \mid X_1^{i_1} \cdots X_m^{i_m} \text{ is not a leading monomial of any polynomial in } I\}$$

$F(X,Y) = X^2Y + Y^2 + 2$ over $\mathbb{F}_5$ – revisited

$$I = \langle X^2Y + Y^2 + 2, X^5 - X, Y^5 - Y \rangle = \{K_1(X,Y)(X^2Y+Y^2+2) + K_2(X,Y)(X^5-X) + K_3(X,Y)(Y^5-Y) \mid K_1, K_2, K_3 \in \mathbb{F}_5[X,Y]\}$$

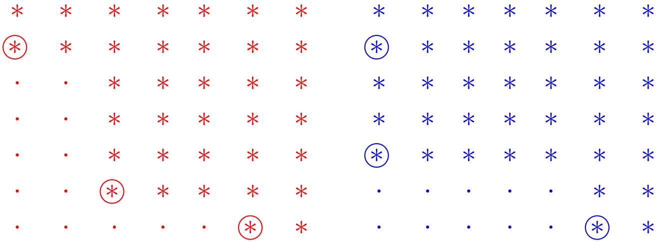


Figure: Two choices: $\mathrm{lm}(F) = X^2Y$ or $\mathrm{lm}(F) = Y^2$. What we estimated is the size of the footprint $\Delta_{\prec}(I)$!!!

The footprint bound

Theorem: Let $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ be an ideal. Then $\{M + I \mid M \in \Delta_{\prec}(I)\}$ constitutes a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$ as a vector space over $\mathbb{F}$

Theorem (footprint bound): The number of roots of a zero-dimensional ideal I is at most equal to the size of the footprint $\Delta_{\prec}(I)$.

Equality holds if the field is perfect and if the ideal contains a univariate square-free polynomial in each variable.

For instance equality holds if the field is $\mathbb{F}_q$ and I contains $X_1^q - X_1, \ldots, X_m^q - X_m$.

We are often only occupied with estimating the size of the footprint, but sometimes we need to actually determine it.

The footprint bound

Theorem: Let $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ be an ideal. Then $\{M + I \mid M \in \Delta_{\prec}(I)\}$ constitutes a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$ as a vector space over $\mathbb{F}$

Theorem (footprint bound): The number of roots of a zero-dimensional ideal I is at most equal to the size of the footprint $\Delta_{\prec}(I)$.

Equality holds if the field is perfect and if the ideal contains a univariate square-free polynomial in each variable.

For instance equality holds if the field is $\mathbb{F}_q$ and I contains $X_1^q - X_1, \ldots, X_m^q - X_m$.

We are often only occupied with estimating the size of the footprint, but sometimes we need to actually determine it.

The footprint bound

Theorem: Let $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ be an ideal. Then $\{M + I \mid M \in \Delta_{\prec}(I)\}$ constitutes a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$ as a vector space over $\mathbb{F}$

Theorem (footprint bound): The number of roots of a zero-dimensional ideal I is at most equal to the size of the footprint $\Delta_{\prec}(I)$.

Equality holds if the field is perfect and if the ideal contains a univariate square-free polynomial in each variable.

For instance equality holds if the field is $\mathbb{F}_q$ and I contains $X_1^q - X_1, \ldots, X_m^q - X_m$.

We are often only occupied with estimating the size of the footprint, but sometimes we need to actually determine it.

The footprint bound

Theorem: Let $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ be an ideal. Then $\{M + I \mid M \in \Delta_{\prec}(I)\}$ constitutes a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$ as a vector space over $\mathbb{F}$

Theorem (footprint bound): The number of roots of a zero-dimensional ideal I is at most equal to the size of the footprint $\Delta_{\prec}(I)$.

Equality holds if the field is perfect and if the ideal contains a univariate square-free polynomial in each variable.

For instance equality holds if the field is $\mathbb{F}_q$ and I contains $X_1^q - X_1, \ldots, X_m^q - X_m$.

We are often only occupied with estimating the size of the footprint, but sometimes we need to actually determine it.

When we only know the leading monomial

Let $\text{lm}(F) = X_1^{i_1} \cdots X_m^{i_m}$ and consider $S = S_1 \times \cdots \times S_m$ with $s_1 = \#S_1, \ldots, s_m = \#S_m$. We may assume $\deg_{X_1} F < s_1, \ldots, \deg_{X_m} F < s_m$.

F has at most $s_1 \cdots s_m - (s_1 - i_1) \cdots (s_m - i_m)$ roots.

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Figure: Maximal number of roots over $\mathbb{F}_5$ of bivariate polynomials

When we only know the leading monomial

Let $\text{lm}(F) = X_1^{i_1} \cdots X_m^{i_m}$ and consider $S = S_1 \times \cdots \times S_m$ with $s_1 = \#S_1, \ldots, s_m = \#S_m$. We may assume $\deg_{X_1} F < s_1, \ldots, \deg_{X_m} F < s_m$.

F has at most $s_1 \cdots s_m - (s_1 - i_1) \cdots (s_m - i_m)$ roots.

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Figure: Maximal number of roots over $\mathbb{F}_5$ of bivariate polynomials

Upper bound is attainable

Consider $S_1 = \{\alpha_1, \ldots, \alpha_{s_1}\}$, $S_2 = \{\beta_1, \ldots, \beta_{s_2}\}$ and $0 \leq i_1 < s_1$, $0 \leq i_2 < s_2$.

The polynomial

$$\left(\prod_{r=1}^{i_1}(X - \alpha_r)\right)\left(\prod_{t=1}^{i_2}(Y - \beta_t)\right)$$

has exactly $(s_1 - i_1)(s_2 - i_2)$ non-roots. Hence, $s_1 s_2 - (s_1 - i_1)(s_2 - i_2)$ roots.

Generalizes to any finite Cartesian product.

Upper bound is attainable

Consider $S_1 = \{\alpha_1, \dots, \alpha_{s_1}\}$, $S_2 = \{\beta_1, \dots, \beta_{s_2}\}$ and $0 \leq i_1 < s_1$, $0 \leq i_2 < s_2$.

The polynomial

$$\left(\prod_{r=1}^{i_1}(X - \alpha_r)\right)\left(\prod_{t=1}^{i_2}(Y - \beta_t)\right)$$

has exactly $(s_1 - i_1)(s_2 - i_2)$ non-roots. Hence, $s_1 s_2 - (s_1 - i_1)(s_2 - i_2)$ roots.

Generalizes to any finite Cartesian product.

Upper bound is attainable

Consider $S_1 = \{\alpha_1, \ldots, \alpha_{s_1}\}$, $S_2 = \{\beta_1, \ldots, \beta_{s_2}\}$ and $0 \leq i_1 < s_1$, $0 \leq i_2 < s_2$.

The polynomial

$$\Big(\prod_{r=1}^{i_1}(X - \alpha_r)\Big)\Big(\prod_{t=1}^{i_2}(Y - \beta_t)\Big)$$

has exactly $(s_1 - i_1)(s_2 - i_2)$ non-roots. Hence, $s_1 s_2 - (s_1 - i_1)(s_2 - i_2)$ roots.

Generalizes to any finite Cartesian product.

Only knowing the total degree

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Figure: Maximal number of roots over $\mathbb{F}_5$ of bivariate polynomials

Worst case is on the border.

Schwartz-Zippel bound

Consider a polynomial $F(X_1, \ldots, X_m)$ over $\mathbb{F}_q$ of total degree d less than q. The number of roots is at most dq^{m-1}.

Remark, that $X_1^q - X_1$ has all elements of $\mathbb{F}_q^m$ as roots.

Only knowing the total degree

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Figure: Maximal number of roots over $\mathbb{F}_5$ of bivariate polynomials

Worst case is on the border.

Schwartz-Zippel bound

Consider a polynomial $F(X_1, \ldots, X_m)$ over $\mathbb{F}_q$ of total degree d less than q. The number of roots is at most dq^{m-1}.

Remark, that $X_1^q - X_1$ has all elements of $\mathbb{F}_q^m$ as roots.

Only knowing the total degree

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Figure: Maximal number of roots over $\mathbb{F}_5$ of bivariate polynomials

Worst case is on the border.

Schwartz-Zippel bound

Consider a polynomial $F(X_1, \ldots, X_m)$ over $\mathbb{F}_q$ of total degree d less than q. The number of roots is at most dq^{m-1}.

Remark, that $X_1^q - X_1$ has all elements of $\mathbb{F}_q^m$ as roots.

Error-correcting codes

Communication through noisy channel over $\mathbb{F}_3$:
$\vec{c} = (2, 0, 1, 2, 1, 1, 0)$ (injected into channel)
$\vec{e} = (1, 2, 0, 0, 0, 0, 0)$ (error)
$\vec{r} = \vec{c} + \vec{e} = (0, 2, 1, 2, 1, 1, 0)$ (output from channel)
Two errors occurred: $w_H(\vec{e}) = 2$

Protection through use of error-correcting code C:
$C \subseteq \mathbb{F}_q^n$ dim $C = k$. Message space $\mathbb{F}_q^k$

Let $\{\vec{g}_1, \ldots, \vec{g}_k\}$ be a basis for C Encoding: $\vec{m} \begin{bmatrix} \vec{g}_1 \\ \vdots \\ \vec{g}_k \end{bmatrix} = \vec{c}$.

$d =$ min dist $= \min\{w_H(\vec{c} \mid \vec{c} \in C \backslash \{\vec{0}\}\}$
Using a minimum distance decoder we can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.

Error-correcting codes

Communication through noisy channel over $\mathbb{F}_3$:
$\vec{c} = (2,0,1,2,1,1,0)$ (injected into channel)
$\vec{e} = (1,2,0,0,0,0,0)$ (error)
$\vec{r} = \vec{c} + \vec{e} = (0,2,1,2,1,1,0)$ (output from channel)
Two errors occurred: $w_H(\vec{e}) = 2$

Protection through use of error-correcting code C:
$C \subseteq \mathbb{F}_q^n$ dim $C = k$. Message space $\mathbb{F}_q^k$

Let $\{\vec{g}_1, \ldots, \vec{g}_k\}$ be a basis for C Encoding: $\vec{m} \begin{bmatrix} \vec{g}_1 \\ \vdots \\ \vec{g}_k \end{bmatrix} = \vec{c}$.

$d =$ min dist $= \min\{w_H(\vec{c} \mid \vec{c} \in C \backslash \{\vec{0}\}\}$
Using a minimum distance decoder we can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.

Reed-Muller codes and hyperbolic codes

Write $\mathbb{F}_q^m = \{P_1, \ldots, P_{n=q^m}\}$.

$\mathrm{RM}_q(s, m) =$
$\{(F(P_1), \ldots, F(P_n)) \mid F \in \mathbb{F}_q[X_1, \ldots, X_m], \deg(F) \leq s\}$

In the above definition we may assume $\deg_{X_i}(F) < q$. The dimension equals the number of such monomials of total degree less than or equal to s.

Hyperbolic codes are improvements where we take full advantage of the footprint bound. This allows us to increase the dimension without lowering the minimum distance.

Reed-Muller codes and hyperbolic codes

Write $\mathbb{F}_q^m = \{P_1, \ldots, P_{n=q^m}\}$.

$\mathrm{RM}_q(s, m) =$
$\{(F(P_1), \ldots, F(P_n)) \mid F \in \mathbb{F}_q[X_1, \ldots, X_m], \deg(F) \leq s\}$

In the above definition we may assume $\deg_{X_i}(F) < q$. The dimension equals the number of such monomials of total degree less than or equal to s.

Hyperbolic codes are improvements where we take full advantage of the footprint bound. This allows us to increase the dimension without lowering the minimum distance.

Reed-Muller codes versus Hyperbolic codes over $\mathbb{F}_7$

$$\mathrm{ev}: \mathbb{F}_7[X, Y] \rightarrow \mathbb{F}_7^{49} \text{ given by } \mathrm{ev}(F) = \big(F(P_1), \ldots, F(P_{49})\big)$$

42	43	44	45	46	47	48
35	37	39	41	43	45	47
28	31	34	37	40	43	46
21	25	29	33	37	41	45
14	19	24	29	34	39	44
7	13	19	25	31	37	43
0	7	14	21	28	35	42

7	6	5	4	3	2	1
(14)	12	10	8	6	4	2
(21)	(18)	[15]	12	9	6	3
(28)	(24)	(20)	[16]	12	8	4
(35)	(30)	(25)	(20)	[15]	10	5
(42)	(36)	(30)	(24)	(18)	12	6
(49)	(42)	(35)	(28)	(21)	(14)	7

Figure: Maximal number of roots and Hamming weight of basis element

$RM_7(5, 2)$ corresponds to ○: $n = 49,\ k = 21,\ d = 14$

$Hyp_7(14, 2)$ corresponds to ○ plus □: $n = 49,\ k = 24,\ d = 14.$

Reed-Muller codes versus Hyperbolic codes over $\mathbb{F}_7$

$\text{ev} : \mathbb{F}_7[X, Y] \to \mathbb{F}_7^{49}$ given by $\text{ev}(F) = \big(F(P_1), \ldots, F(P_{49})\big)$

42	43	44	45	46	47	48
35	37	39	41	43	45	47
28	31	34	37	40	43	46
21	25	29	33	37	41	45
14	19	24	29	34	39	44
7	13	19	25	31	37	43
0	7	14	21	28	35	42

7	6	5	4	3	2	1
○14	12	10	8	6	4	2
○21	○18	□15	12	9	6	3
○28	○24	○20	□16	12	8	4
○35	○30	○25	○20	□15	10	5
○42	○36	○30	○24	○18	12	6
○49	○42	○35	○28	○21	○14	7

Figure: Maximal number of roots and Hamming weight of basis element

$\text{RM}_7(5, 2)$ corresponds to $\circ$: $n = 49,\ k = 21,\ d = 14$

$\text{Hyp}_7(14, 2)$ corresponds to $\circ$ plus $\square$: $n = 49,\ k = 24,\ d = 14.$

Quantum codes from the CSS construction

Given codes $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$ the CSS construction gives us an $[[n, \ell, d_z/d_x]]_q$ quantum code.

That is, a q^ℓ-dimensional subspace of $\mathbb{C}^{q^n}$ which can correct $\lfloor (d_z - 1)/2 \rfloor$ phase-shift errors and $\lfloor (d_x - 1)/2 \rfloor$ qudit-flip errors.

Here,
$\ell = \dim C_1 - \dim C_2$,
$d_z = wt(C_1 \backslash C_2) = \min\{w_H(\vec{c}) \mid \vec{c} \in C_1 \backslash C_2\}$, and
$d_x = wt(C_2^\perp \backslash C_1^\perp)$

Footprint bound / Feng-Rao bound / quantum codes

C_2 is the span of $\circ$.

C_1 is the span of $\circ$ and $\square$.

7	6	5	4	3	2	1
○14	□12	10	8	6	4	2
○21	○18	□15	12	9	6	3
○28	○24	○20	□16	12	8	4
○35	○30	○25	○20	□15	10	5
○42	○36	○30	○24	○18	□12	6
○49	○42	○35	○28	○21	○14	○7

7	14	21	28	35	42	49
○6	□12	18	24	30	36	42
○5	○10	□15	20	25	30	35
○4	○8	○12	□16	20	24	28
○3	○6	○9	○12	□15	18	21
○2	○4	○6	○8	○10	□12	14
○1	○2	○3	○4	○5	○6	○7

Figure: Left-hand side: The footprint numbers tells us that $wt(C_1 \backslash C_2) = \min\{12, 15, 16\} = 12$. Right-hand side: The Feng-Rao numbers tells us that $wt(C_2^{\perp} \backslash C_1^{\perp}) = \min\{12, 15, 16\} = 12$. Hence, we obtain a $[[49, 5, 12/12]]_7$ quantum code.

More polynomials

Common roots of more polynomials. We may assume pairwise different leading monomials.

$\mathrm{lm}(F_1) = X^3Y$, $\mathrm{lm}(F_2) = XY^2$ over $S_1 \times S_2$ with $s_1 = 5$ and $s_2 = 6$.

*	*	*	*	*	*	*
⊛	*	*	*	*	*	*
·	*	*	*	*	*	*
·	*	*	*	*	*	*
·	*	*	*	*	*	*
·	⊛	*	*	*	*	*
·	·	·	⊛	*	*	*
·	·	·	·	·	⊛	*

There do exist such polynomials with 12 common roots (again products of linear factors).

Generalizes to t polynomials and m variables.

More polynomials

Common roots of more polynomials. We may assume pairwise different leading monomials.

$\mathrm{lm}(F_1) = X^3Y$, $\mathrm{lm}(F_2) = XY^2$ over $S_1 \times S_2$ with $s_1 = 5$ and $s_2 = 6$.

$$\begin{array}{ccccccc}
* & * & * & * & * & * & * \\
\circledast & * & * & * & * & * & * \\
\cdot & * & * & * & * & * & * \\
\cdot & * & * & * & * & * & * \\
\cdot & * & * & * & * & * & * \\
\cdot & \circledast & * & * & * & * & * \\
\cdot & \cdot & \cdot & \circledast & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \circledast & *
\end{array}$$

There do exist such polynomials with 12 common roots (again products of linear factors).

Generalizes to t polynomials and m variables.

More polynomials

Common roots of more polynomials. We may assume pairwise different leading monomials.

$\text{lm}(F_1) = X^3Y$, $\text{lm}(F_2) = XY^2$ over $S_1 \times S_2$ with $s_1 = 5$ and $s_2 = 6$.

$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$
$\circledast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$
$\cdot$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$
$\cdot$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$
$\cdot$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$
$\cdot$	$\circledast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$
$\cdot$	$\cdot$	$\cdot$	$\circledast$	$\ast$	$\ast$	$\ast$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\circledast$	$\ast$

There do exist such polynomials with 12 common roots (again products of linear factors).

Generalizes to t polynomials and m variables.

Applications in information theory

The number of common roots of r polynomials gives information on:

- Information leakage in secret sharing.
- Information leakage from wire-tap channels.

Actually again we study $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ and C_1/C_2. We look for minimum support of r linearly independent words in C_1 but not in C_2.

Applications in information theory

The number of common roots of r polynomials gives information on:

- Information leakage in secret sharing.
- Information leakage from wire-tap channels.

Actually again we study $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ and C_1/C_2. We look for minimum support of r linearly independent words in C_1 but not in C_2.

Ramp secret sharing schemes

$C_2 \subset C_1 \subseteq \mathbb{F}_q^n$.

$C_2 = \text{Span}\{\vec{b}_1, \ldots, \vec{b}_{k_2}\} \quad C_1 = \text{Span}\{\vec{b}_1, \ldots, \vec{b}_{k_1}\}$

$\ell = k_1 - k_2$.

Secret message $\vec{s} = (a_{k_2+1}, \ldots, a_{k_1}) \in \mathbb{F}_q^\ell$.

Choose $a_1, \ldots, a_{k_2}$ by random.

Encode $\vec{c} = a_1\vec{b}_1 + \cdots + a_{k_1}\vec{b}_{k_1} = (c_1, \ldots, c_n)$.

Share 1 is c_1,...., Share n is c_n.

Ramp secret sharing schemes

$C_2 \subset C_1 \subseteq \mathbb{F}_q^n$.

$C_2 = \text{Span}\{\vec{b}_1, \ldots, \vec{b}_{k_2}\}$ $\quad C_1 = \text{Span}\{\vec{b}_1, \ldots, \vec{b}_{k_1}\}$

$\ell = k_1 - k_2$.

Secret message $\vec{s} = (a_{k_2+1}, \ldots, a_{k_1}) \in \mathbb{F}_q^{\ell}$.

Choose $a_1, \ldots, a_{k_2}$ by random.

Encode $\vec{c} = a_1\vec{b}_1 + \cdots + a_{k_1}\vec{b}_{k_1} = (c_1, \ldots, c_n)$.

Share 1 is c_1,...., Share n is c_n.

Ramp secret sharing schemes

$C_2 \subset C_1 \subseteq \mathbb{F}_q^n$.

$C_2 = \text{Span}\{\vec{b}_1, \ldots, \vec{b}_{k_2}\} \quad C_1 = \text{Span}\{\vec{b}_1, \ldots, \vec{b}_{k_1}\}$

$\ell = k_1 - k_2$.

Secret message $\vec{s} = (a_{k_2+1}, \ldots, a_{k_1}) \in \mathbb{F}_q^{\ell}$.

Choose $a_1, \ldots, a_{k_2}$ by random.

Encode $\vec{c} = a_1\vec{b}_1 + \cdots + a_{k_1}\vec{b}_{k_1} = (c_1, \ldots, c_n)$.

Share 1 is c_1,...., Share n is c_n.

Privacy and reconstruction

A ramp secret sharing scheme has $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction if

- An adversary cannot obtain m q-bits of information about $\vec{s}$ with t_m shares (but for some $t_m + 1$ shares)
- It is possible to recover m q-bits of information about $\vec{s}$ with any collection of r_m shares (but not for all collections of $r_m - 1$ shares).

Common zeros...

The m-th relative generalized Hamming weight is:

$$M_m(C_1, C_2) = \min\{\#\text{Supp}D \mid D \text{ is a subspace of } C_1, \dim D = m, D \cap C_2 = \{\vec{0}\}\}$$

$$r_m = n - M_{\ell-m+1}(C_1, C_2) + 1$$

$$t_m = M_m(C_2^{\perp}, C_1^{\perp}) - 1$$

Common zeros...

The m-th relative generalized Hamming weight is:

$$M_m(C_1, C_2) = \min\{\#\mathrm{Supp} D \mid D \text{ is a subspace of } C_1, \dim D = m, D \cap C_2 = \{\vec{0}\}\}$$

$r_m = n - M_{\ell-m+1}(C_1, C_2) + 1$

$t_m = M_m(C_2^{\perp}, C_1^{\perp}) - 1$

Gröbner bases

For univariate polynomials $F(X)$ and $G(X)$ we have $\langle F(X), G(X)\rangle = \langle \gcd(F(X), G(X))$. Hence, the footprint is easily calculated.

$\mathbb{F}[X_1, \ldots, X_m]$ is NOT a PID for $m \geq 2$. So we must expect more generators.

Definition: $\{F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m)\}$ is a Gröbner basis for I w.r.t. $\prec$ if

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- For any $F(X_1, \ldots, X_m) \in I$ there exists an $i \in \{1, \ldots, s\}$ such that $\mathrm{lm}(F_i)$ divides $\mathrm{lm}(F)$.

Buchberger's algorithm extends any basis to a Gröbner basis. Complexity in general high. Involves multivariate division algorithm.

Gröbner bases

For univariate polynomials $F(X)$ and $G(X)$ we have $\langle F(X), G(X)\rangle = \langle \gcd(F(X), G(X)\rangle$. Hence, the footprint is easily calculated.

$\mathbb{F}[X_1, \ldots, X_m]$ is NOT a PID for $m \geq 2$. So we must expect more generators.

Definition: $\{F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m)\}$ is a Gröbner basis for I w.r.t. $\prec$ if

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- For any $F(X_1, \ldots, X_m) \in I$ there exists an $i \in \{1, \ldots, s\}$ such that $\mathrm{lm}(F_i)$ divides $\mathrm{lm}(F)$.

Buchberger's algorithm extends any basis to a Gröbner basis. Complexity in general high. Involves multivariate division algorithm.

Gröbner bases

For univariate polynomials $F(X)$ and $G(X)$ we have $\langle F(X), G(X)\rangle = \langle \gcd(F(X), G(X))$. Hence, the footprint is easily calculated.

$\mathbb{F}[X_1, \ldots, X_m]$ is NOT a PID for $m \geq 2$. So we must expect more generators.

Definition: $\{F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m)\}$ is a Gröbner basis for I w.r.t. $\prec$ if

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- For any $F(X_1, \ldots, X_m) \in I$ there exists an $i \in \{1, \ldots, s\}$ such that $\text{lm}(F_i)$ divides $\text{lm}(F)$.

Buchberger's algorithm extends any basis to a Gröbner basis. Complexity in general high. Involves multivariate division algorithm.

Gröbner bases

For univariate polynomials $F(X)$ and $G(X)$ we have $\langle F(X), G(X)\rangle = \langle \gcd(F(X), G(X))$. Hence, the footprint is easily calculated.

$\mathbb{F}[X_1, \ldots, X_m]$ is NOT a PID for $m \geq 2$. So we must expect more generators.

Definition: $\{F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m)\}$ is a Gröbner basis for I w.r.t. $\prec$ if

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- For any $F(X_1, \ldots, X_m) \in I$ there exists an $i \in \{1, \ldots, s\}$ such that $\text{lm}(F_i)$ divides $\text{lm}(F)$.

Buchberger's algorithm extends any basis to a Gröbner basis. Complexity in general high. Involves multivariate division algorithm.

Theoretical application of Buchberger's algorithm

What is the second highest number of roots of a polynomial of given degree?

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Cannot be seen from this figure!!!

...but the value suggested by the figure is right! Proof uses Buchberger's algorithm at theoretical level

Theoretical application of Buchberger's algorithm

What is the second highest number of roots of a polynomial of given degree?

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Cannot be seen from this figure!!!

...but the value suggested by the figure is right! Proof uses Buchberger's algorithm at theoretical level

Theoretical application of Buchberger's algorithm

What is the second highest number of roots of a polynomial of given degree?

20	21	22	23	24
15	17	19	21	23
10	13	16	19	22
5	9	13	17	21
0	5	10	15	20

Cannot be seen from this figure!!!

...but the value suggested by the figure is right! Proof uses Buchberger's algorithm at theoretical level

Part 2:

Affine roots from Cartesian product point sets counted with multiplicity

Multiplicity

Definition: $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ is a root of $F(X_1, \ldots, X_m)$ of multiplicity r if $F(X_1, \ldots, X_m) \in J_r \backslash J_{r+1}$. Here,

$$J_s = \langle (X_1 - \alpha_1)^{p_1} \cdots (X_m - \alpha_m)^{p_m} \mid p_1 + \cdots + p_m = s \rangle.$$

One can reformulate the footprint bound in this setting using the CRT

The bad news: The footprint method can be applied, but is not efficient any more.

Theorem (Schwartz-Zippel bound (Dvir et al)): Let $F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ be of total degree t. Then

$$\sum_{\vec{\alpha} \in \mathbb{F}_q^m} \text{mult}(F, \vec{\alpha}) \leq t q^{m-1}.$$

Multiplicity

Definition: $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ is a root of $F(X_1, \ldots, X_m)$ of multiplicity r if $F(X_1, \ldots, X_m) \in J_r \backslash J_{r+1}$. Here,

$$J_s = \langle (X_1 - \alpha_1)^{p_1} \cdots (X_m - \alpha_m)^{p_m} \mid p_1 + \cdots + p_m = s \rangle.$$

One can reformulate the footprint bound in this setting using the CRT

The bad news: The footprint method can be applied, but is not efficient any more.

Theorem (Schwartz-Zippel bound (Dvir et al)): Let $F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ be of total degree t. Then

$$\sum_{\vec{\alpha} \in \mathbb{F}_q^m} \text{mult}(F, \vec{\alpha}) \leq tq^{m-1}.$$

Multiplicity

Definition: $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ is a root of $F(X_1, \ldots, X_m)$ of multiplicity r if $F(X_1, \ldots, X_m) \in J_r \backslash J_{r+1}$. Here,

$$J_s = \langle (X_1 - \alpha_1)^{p_1} \cdots (X_m - \alpha_m)^{p_m} \mid p_1 + \cdots + p_m = s \rangle.$$

One can reformulate the footprint bound in this setting using the CRT

The bad news: The footprint method can be applied, but is not efficient any more.

Theorem (Schwartz-Zippel bound (Dvir et al)): Let $F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ be of total degree t. Then

$$\sum_{\vec{\alpha} \in \mathbb{F}_q^m} \text{mult}(F, \vec{\alpha}) \leq t q^{m-1}.$$

Multiplicity

Definition: $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ is a root of $F(X_1, \ldots, X_m)$ of multiplicity r if $F(X_1, \ldots, X_m) \in J_r \backslash J_{r+1}$. Here,

$$J_s = \langle (X_1 - \alpha_1)^{p_1} \cdots (X_m - \alpha_m)^{p_m} \mid p_1 + \cdots + p_m = s \}.$$

One can reformulate the footprint bound in this setting using the CRT

The bad news: The footprint method can be applied, but is not efficient any more.

Theorem (Schwartz-Zippel bound (Dvir et al)): Let $F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ be of total degree t. Then

$$\sum_{\vec{\alpha} \in \mathbb{F}_q^m} \text{mult}(F, \vec{\alpha}) \leq tq^{m-1}.$$

Multiplicity – cont.

Theorem: Let $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ be a non-zero polynomial and let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to a lexicographic ordering $\prec_{lex}$. Then for any finite sets $S_1, \ldots, S_m \subseteq \mathbb{F}$

$$\sum_{\vec{a} \in S_1 \times \cdots \times S_m} \mathrm{mult}(F, \vec{a}) \leq i_1 s_2 \cdots s_m + s_1 i_2 s_3 \cdots s_m + \cdots + s_1 \cdots s_{m-1} i_m.$$

Corollary: The number of roots of multiplicity at least r is at most $(i_1 s_2 \cdots s_m + s_1 i_2 s_3 \cdots s_m + \cdots + s_1 \cdots s_{m-1} i_m)/r$

For any $(i_1, \ldots, i_m)$ there exists F with leading monomial $X_1^{i_1} \cdots X_m^{i_m}$ such that the theorem is sharp. But the corollary is only sharp for few $(i_1, \ldots, i_m)$.

Multiplicity – cont.

Theorem: Let $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ be a non-zero polynomial and let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to a lexicographic ordering $\prec_{lex}$. Then for any finite sets $S_1, \ldots, S_m \subseteq \mathbb{F}$

$$\sum_{\vec{a} \in S_1 \times \cdots \times S_m} \mathrm{mult}(F, \vec{a}) \leq i_1 s_2 \cdots s_m + s_1 i_2 s_3 \cdots s_m + \cdots + s_1 \cdots s_{m-1} i_m .$$

Corollary: The number of roots of multiplicity at least r is at most $\left(i_1 s_2 \cdots s_m + s_1 i_2 s_3 \cdots s_m + \cdots + s_1 \cdots s_{m-1} i_m\right)/r$

For any $(i_1, \ldots, i_m)$ there exists F with leading monomial $X_1^{i_1} \cdots X_m^{i_m}$ such that the theorem is sharp. But the corollary is only sharp for few $(i_1, \ldots, i_m)$.

Multiplicity – cont.

Theorem: Let $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ be a non-zero polynomial and let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to a lexicographic ordering $\prec_{lex}$. Then for any finite sets $S_1, \ldots, S_m \subseteq \mathbb{F}$

$$\sum_{\vec{a} \in S_1 \times \cdots \times S_m} \text{mult}(F, \vec{a}) \leq i_1 s_2 \cdots s_m + s_1 i_2 s_3 \cdots s_m + \cdots + s_1 \cdots s_{m-1} i_m.$$

Corollary: The number of roots of multiplicity at least r is at most $\left(i_1 s_2 \cdots s_m + s_1 i_2 s_3 \cdots s_m + \cdots + s_1 \cdots s_{m-1} i_m\right)/r$

For any $(i_1, \ldots, i_m)$ there exists F with leading monomial $X_1^{i_1} \cdots X_m^{i_m}$ such that the theorem is sharp. But the corollary is only sharp for few $(i_1, \ldots, i_m)$.

Number of roots of multiplicity at least r

Definition: Let $r \in \mathbb{N}, i_1, \ldots, i_m \in \mathbb{N}_0$. Define

$$D(i_1, r, s_1) = \min\left\{\left\lfloor \frac{i_1}{r} \right\rfloor, s_1\right\}$$

and for $m \geq 2$

$$D(i_1, \ldots, i_m, r, s_1, \ldots, s_m) =$$

$$\max_{(u_1,\ldots,u_r)\in A(i_m,r,s_m)} \Big\{(s_m - u_1 - \cdots - u_r)D(i_1, \ldots, i_{m-1}, r, s_1, \ldots, s_{m-1})$$
$$+ u_1 D(i_1, \ldots, i_{m-1}, r-1, s_1, \ldots, s_{m-1}) + \cdots$$
$$+ u_{r-1} D(i_1, \ldots, i_{m-1}, 1, s_1, \ldots, s_{m-1}) + u_r s_1 \cdots s_{m-1}\Big\}$$

where

$$A(i_m, r, s_m) =$$
$$\{(u_1, \ldots, u_r) \in \mathbb{N}_0^r \mid u_1 + \cdots + u_r \leq s_m \text{ and } u_1 + 2u_2 + \cdots + ru_r \leq i_m\}.$$

Number of roots of multiplicity at least r – cont.

Theorem: For a polynomial $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to the lexicographic ordering $\prec_{lex}$ with $X_m \prec_{lex} \cdots \prec_{lex} X_1$. Then F has at most $D(i_1, \ldots, i_m, r, s_1, \ldots, s_m)$ roots of multiplicity at least r in $S_1 \times \cdots \times S_m$.

We have closed formula upper bounds on D for two variables (4 special cases).

We have a closed formula upper bound on D for arbitrary many variables, but the leading monomial being "below" a certain threshold.

A lot of open questions!!!

Number of roots of multiplicity at least r – cont.

Theorem: For a polynomial $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to the lexicographic ordering $\prec_{lex}$ with $X_m \prec_{lex} \cdots \prec_{lex} X_1$. Then F has at most $D(i_1, \ldots, i_m, r, s_1, \ldots, s_m)$ roots of multiplicity at least r in $S_1 \times \cdots \times S_m$.

We have closed formula upper bounds on D for two variables (4 special cases).

We have a closed formula upper bound on D for arbitrary many variables, but the leading monomial being "below" a certain threshold.

A lot of open questions!!!

Number of roots of multiplicity at least r – cont.

Theorem: For a polynomial $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to the lexicographic ordering $\prec_{lex}$ with $X_m \prec_{lex} \cdots \prec_{lex} X_1$. Then F has at most $D(i_1, \ldots, i_m, r, s_1, \ldots, s_m)$ roots of multiplicity at least r in $S_1 \times \cdots \times S_m$.

We have closed formula upper bounds on D for two variables (4 special cases).

We have a closed formula upper bound on D for arbitrary many variables, but the leading monomial being "below" a certain threshold.

A lot of open questions!!!

$D(i_1, i_2, 3, 5, 5)$

20	21	22	23	24										
20	20	21	21	23										
20	20	20	21	22										
15	16	17	19	21										
15	15	16	17	20										
15	15	15	17	18	22	23	23	24	24					
10	11	12	15	17	21	22	22	23	23					
10	10	11	13	15	18	20	20	22	22					
10	10	10	13	14	17	19	19	21	21					
5	6	7	11	12	14	17	17	20	20					
5	5	6	9	11	13	16	16	18	19	23	23	24	24	24
5	5	5	9	9	10	14	14	16	18	21	21	23	23	23
0	1	2	7	8	9	13	13	14	17	19	19	22	22	22
0	0	1	5	6	6	11	11	12	16	17	17	21	21	21
0	0	0	5	5	5	10	10	10	15	15	15	20	20	20

Two variables

Proposition: For $k = 1, \ldots, r-1$, $D(i_1, i_2, r, s_1, s_2)$ is upper bounded by

(C.1) $s_2 \frac{i_1}{r} + \frac{i_2}{r} \frac{i_1}{r-k}$
if $(r-k)\frac{r}{r+1}s_1 \leq i_1 < (r-k)s_1$ and $0 \leq i_2 < ks_2$

(C.2) $s_2 \frac{i_1}{r} + ((k+1)s_2 - i_2)(\frac{i_1}{r-k} - \frac{i_1}{r}) + (i_2 - ks_2)(s_1 - \frac{i_1}{r})$
if $(r-k)\frac{r}{r+1}s_1 \leq i_1 < (r-k)s_1$ and $ks_2 \leq i_2 < (k+1)s_2$

(C.3) $s_2 \frac{i_1}{r} + \frac{i_2}{k+1}(s_1 - \frac{i_1}{r})$
if $(r-k-1)s_1 \leq i_1 < (r-k)\frac{r}{r+1}s_1$ and $0 \leq i_2 < (k+1)s_2$.

Finally,

(C.4) $D(i_1, i_2, r, s_1, s_2) = s_2 \lfloor \frac{i_1}{r} \rfloor + i_2(s_1 - \lfloor \frac{i_1}{r} \rfloor)$
if $s_1(r-1) \leq i_1 < s_1 r$ and $0 \leq i_2 < s_2$.

Small degree

Theorem: If $i_m < rs_m$ and if for $t = 1, \ldots, m-1$

$$i_t \leq s_t \min\left\{ \frac{\sqrt[m-1]{r}-1}{\sqrt[m-1]{r}-\frac{1}{r}}, \frac{\sqrt[m-2]{2}-1}{\sqrt[m-2]{2}-\frac{1}{2}} \right\}$$

then $D(i_1, \ldots i_m, r, s_1, \ldots s_m) \leq s_1 \cdots s_m - (s_1 - \frac{i_1}{r}) \cdots (s_m - \frac{i_m}{r})$.

Besides being interesting in itself...

Studying the number of roots with multiplicity is relevant in connection with

- Multiplicity codes (Kopparty et al). These are locally decodable codes
- Kakeya sets over finite fields (Dvir et al)
- List decoding (Guruswami-Sudan)

Besides being interesting in itself...

Studying the number of roots with multiplicity is relevant in connection with

- Multiplicity codes (Kopparty et al). These are locally decodable codes
- Kakeya sets over finite fields (Dvir et al)
- List decoding (Guruswami-Sudan)

Besides being interesting in itself...

Studying the number of roots with multiplicity is relevant in connection with

- Multiplicity codes (Kopparty et al). These are locally decodable codes
- Kakeya sets over finite fields (Dvir et al)
- List decoding (Guruswami-Sudan)

Besides being interesting in itself...

Studying the number of roots with multiplicity is relevant in connection with

- Multiplicity codes (Kopparty et al). These are locally decodable codes
- Kakeya sets over finite fields (Dvir et al)
- List decoding (Guruswami-Sudan)

Minimum distance decoding of Reed-Solomon codes

Consider a Reed-Solomon code over $\mathbb{F}_q = \{P_1, \ldots, P_q\}$:

$\mathrm{RS}_q(k) = \{(F(P_1), \ldots, F(P_q)) \mid \deg(F) < k\}$.

The minimum distance is $d = q - k + 1$. Define $t = \lfloor (d-1)/2 \rfloor = \lfloor (q-k)/2 \rfloor$.

If we receive $\vec{r} = (r_1, \ldots, r_q)$ then we determine a non zero polynomial

$$Q(X,Y) = Q_0(X) + YQ_1(X)$$

that satisfies the following

- $Q(P_1, r_1) = 0,\ Q(P_2, r_2) = 0, \ldots, Q(P_q, r_q) = 0$
- $\deg(Q_0) \leq q - 1 - t = l_0$
- $\deg(Q_1) \leq t = l_1$

Minimum distance decoding of Reed-Solomon codes

Consider a Reed-Solomon code over $\mathbb{F}_q = \{P_1, \ldots, P_q\}$:

$\mathrm{RS}_q(k) = \{(F(P_1), \ldots, F(P_q)) \mid \deg(F) < k\}$.

The minimum distance is $d = q - k + 1$. Define $t = \lfloor (d-1)/2 \rfloor = \lfloor (q-k)/2 \rfloor$.

If we receive $\vec{r} = (r_1, \ldots, r_q)$ then we determine a non zero polynomial

$$Q(X, Y) = Q_0(X) + YQ_1(X)$$

that satisfies the following

- $Q(P_1, r_1) = 0,\ Q(P_2, r_2) = 0, \ldots, Q(P_q, r_q) = 0$
- $\deg(Q_0) \leq q - 1 - t = l_0$
- $\deg(Q_1) \leq t = l_1$

Minimum distance decoding of Reed-Solomon codes

Consider a Reed-Solomon code over $\mathbb{F}_q = \{P_1, \ldots, P_q\}$:

$\mathrm{RS}_q(k) = \{(F(P_1), \ldots, F(P_q)) \mid \deg(F) < k\}$.

The minimum distance is $d = q - k + 1$. Define $t = \lfloor (d-1)/2 \rfloor = \lfloor (q-k)/2 \rfloor$.

If we receive $\vec{r} = (r_1, \ldots, r_q)$ then we determine a non zero polynomial

$$Q(X, Y) = Q_0(X) + YQ_1(X)$$

that satisfies the following

- $Q(P_1, r_1) = 0,\ Q(P_2, r_2) = 0, \ldots, Q(P_q, r_q) = 0$
- $\deg(Q_0) \leq q - 1 - t = l_0$
- $\deg(Q_1) \leq t = l_1$

Decoding of RS-code – cont.

How can we be sure that such a polynomial $Q(X, Y)$ exists?

Let $Q_0(X) = Q_{0,0} + Q_{0,1}X + Q_{0,2}X^2 + \cdots + Q_{0,l_0}X^{l_0}$ and $Q_1(X) = Q_{1,0} + Q_{1,1}X + \cdots + Q_{1,l_1}X^{l_1}$. We get

$$Q(P_1, r_1) = 0$$

$$\Updownarrow$$

$$Q_{0,0} + Q_{0,1}P_1 + Q_{0,2}P_1^2 + \cdots + Q_{0,l_0}P_1^{l_0}$$
$$+Q_{1,0}r_1 + Q_{1,1}r_1P_1 + \cdots + Q_{1,l_1}r_1P_1^{l_1} = 0$$

This is a homogeneous equation with $(l_0 + 1) + (l_1 + 1) = q + 1$ unknown (the $Q_{i,j}$'s).

There are q such equations. A homogeneous system of linear equations with more unknowns than equations possesses a non zero solution.

Decoding of RS-code – cont.

How can we be sure that such a polynomial $Q(X, Y)$ exists?

Let $Q_0(X) = Q_{0,0} + Q_{0,1}X + Q_{0,2}X^2 + \cdots + Q_{0,l_0}X^{l_0}$ and $Q_1(X) = Q_{1,0} + Q_{1,1}X + \cdots + Q_{1,l_1}X^{l_1}$. We get

$$Q(P_1, r_1) = 0$$

$$\Updownarrow$$

$$Q_{0,0} + Q_{0,1}P_1 + Q_{0,2}P_1^2 + \cdots + Q_{0,l_0}P_1^{l_0} + Q_{1,0}r_1 + Q_{1,1}r_1P_1 + \cdots + Q_{1,l_1}r_1P_1^{l_1} = 0$$

This is a homogeneous equation with $(l_0 + 1) + (l_1 + 1) = q + 1$ unknown (the $Q_{i,j}$'s).

There are q such equations. A homogeneous system of linear equations with more unknowns than equations possesses a non zero solution.

Decoding of RS-code – cont.

How can we be sure that such a polynomial $Q(X, Y)$ exists?

Let $Q_0(X) = Q_{0,0} + Q_{0,1}X + Q_{0,2}X^2 + \cdots + Q_{0,l_0}X^{l_0}$ and $Q_1(X) = Q_{1,0} + Q_{1,1}X + \cdots + Q_{1,l_1}X^{l_1}$. We get

$$Q(P_1, r_1) = 0$$

$$\Updownarrow$$

$$Q_{0,0} + Q_{0,1}P_1 + Q_{0,2}P_1^2 + \cdots + Q_{0,l_0}P_1^{l_0} + Q_{1,0}r_1 + Q_{1,1}r_1P_1 + \cdots + Q_{1,l_1}r_1P_1^{l_1} = 0$$

This is a homogeneous equation with $(l_0 + 1) + (l_1 + 1) = q + 1$ unknown (the $Q_{i,j}$'s).

There are q such equations. A homogeneous system of linear equations with more unknowns than equations possesses a non zero solution.

Decoding of RS-code – cont.

In matrix form we have:

$$\begin{bmatrix} 1 & P_1 & P_1^2 & \cdots & P_1^{l_0} & r_1 & r_1 P_1 & \cdots & r_1 P_1^{l_1} \\ 1 & P_2 & P_2^2 & \cdots & P_2^{l_0} & r_2 & r_2 P_2 & \cdots & r_2 P_2^{l_1} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & P_q & P_q^2 & \cdots & P_q^{l_0} & r_q & r_q P_q & \cdots & r_q P_q^{l_1} \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ Q_{0,2} \\ \vdots \\ Q_{0,l_0} \\ Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Decoding of RS-codes – cont.

Assume $\vec{c} = (F(P_1), F(P_2), \ldots, F(P_q))$ was send (it is unknown to us) and assume that at most t errors occurred under transmission.

We have $Q(P_1, r_1) = Q(P_2, r_2) = \cdots = Q(P_q, r_q) = 0$ and as at most t errors occurred at least $q - t$ zeros among

$$Q(P_1, F(P_1)), Q(P_2, F(P_2)), \ldots, Q(P_q, F(P_q))$$

Interpret $Q(X, F(X)) = Q_0 + F(X)Q_1(X)$ as a polynomial in X. It is of degree at most $\max\{q - 1 - t, (k - 1) + t\} = q - 1 - t$. A polynomial of degree at most $q - 1 - t$, that has at least $q - t$ zeros is the zero-polynomial 0. We get

$$Q(X, F(X)) = 0 \Leftrightarrow F(X) = -\frac{Q_0(X)}{Q_1(X)}$$

Decoding of RS-codes – cont.

Assume $\vec{c} = (F(P_1), F(P_2), \ldots, F(P_q))$ was send (it is unknown to us) and assume that at most t errors occurred under transmission.

We have $Q(P_1, r_1) = Q(P_2, r_2) = \cdots = Q(P_q, r_q) = 0$ and as at most t errors occurred at least $q - t$ zeros among

$$Q(P_1, F(P_1)), Q(P_2, F(P_2)), \ldots, Q(P_q, F(P_q))$$

Interpret $Q(X, F(X)) = Q_0 + F(X)Q_1(X)$ as a polynomial in X. It is of degree at most $\max\{q - 1 - t, (k - 1) + t\} = q - 1 - t$. A polynomial of degree at most $q - 1 - t$, that has at least $q - t$ zeros is the zero-polynomial 0. We get

$$Q(X, F(X)) = 0 \Leftrightarrow F(X) = -\frac{Q_0(X)}{Q_1(X)}$$

Decoding of RS-codes – cont.

Assume $\vec{c} = (F(P_1), F(P_2), \ldots, F(P_q))$ was send (it is unknown to us) and assume that at most t errors occurred under transmission.

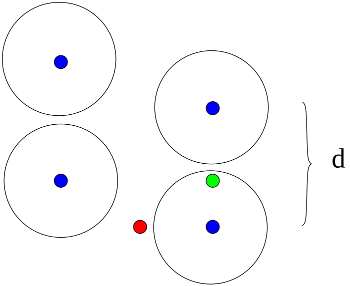
We have $Q(P_1, r_1) = Q(P_2, r_2) = \cdots = Q(P_q, r_q) = 0$ and as at most t errors occurred at least $q - t$ zeros among

$$Q(P_1, F(P_1)), Q(P_2, F(P_2)), \ldots, Q(P_q, F(P_q))$$

Interpret $Q(X, F(X)) = Q_0 + F(X)Q_1(X)$ as a polynomial in X. It is of degree at most $\max\{q - 1 - t, (k-1) + t\} = q - 1 - t$. A polynomial of degree at most $q - 1 - t$, that has at least $q - t$ zeros is the zero-polynomial 0. We get

$$Q(X, F(X)) = 0 \Leftrightarrow F(X) = -\frac{Q_0(X)}{Q_1(X)}$$

List decoding



There does not always exists a codeword within the distance $t = \lfloor (d-1)/2 \rfloor$ from the received word $\vec{r}$. In such a case we would like to investigate greater radii than t. Using such a method we must accept to sometimes find more candidates for the send word.

List decoding

Look for $Q(X, Y) = Q_0(X) + Q_1(X)Y + \cdots + Q_m(X)Y^m$ such that

- $Q(P_i, r_i) = 0$ for $i = 1, \ldots, q$
- Certain degree conditions on the Q_i's must be satisfied

Determine all factors $Y - F(X)$ i $Q(X, Y)$. There can at most be m such factors (in by far most cases only one factor).

The method can be further improved, if zeros are counted with multiplicity.

Above method generalizes to many classes of codes. Improved bounds on zeros of prescribed multiplicity might help further.

List decoding

Look for $Q(X,Y) = Q_0(X) + Q_1(X)Y + \cdots + Q_m(X)Y^m$ such that

- $Q(P_i, r_i) = 0$ for $i = 1, \ldots, q$
- Certain degree conditions on the Q_i's must be satisfied

Determine all factors $Y - F(X)$ i $Q(X,Y)$. There can at most be m such factors (in by far most cases only one factor).

The method can be further improved, if zeros are counted with multiplicity.

Above method generalizes to many classes of codes. Improved bounds on zeros of prescribed multiplicity might help further.

List decoding

Look for $Q(X,Y) = Q_0(X) + Q_1(X)Y + \cdots + Q_m(X)Y^m$ such that

- $Q(P_i, r_i) = 0$ for $i = 1, \ldots, q$
- Certain degree conditions on the Q_i's must be satisfied

Determine all factors $Y - F(X)$ i $Q(X,Y)$. There can at most be m such factors (in by far most cases only one factor).

The method can be further improved, if zeros are counted with multiplicity.

Above method generalizes to many classes of codes. Improved bounds on zeros of prescribed multiplicity might help further.

Part 3:

Points on curves. Algebraic geometric codes

Hermitian curves

$I = \langle X^4 - Y^3 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
Hermitian variety: $\#\mathcal{V}(I_9) = 27$.

Given $F(X, Y) \in \mathbb{F}_9[X, Y]$ how many roots from Hermitian variety? That is we ask for the size of the variety of $\langle F \rangle + I_9$.

$w(X^i Y^j) = 3i + 4j$.
$X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if:

- $w(X^\alpha Y^\beta) < w(X^\gamma Y^\delta)$
- $w(X^\alpha Y^\beta) = w(X^\gamma Y^\delta)$ but $\beta < \delta$

$\{X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\}$ is a Gröbner basis w.r.t. $\prec_w$.

Hermitian curves

$I = \langle X^4 - Y^3 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
Hermitian variety: $\#\mathcal{V}(I_9) = 27$.

Given $F(X, Y) \in \mathbb{F}_9[X, Y]$ how many roots from Hermitian variety? That is we ask for the size of the variety of $\langle F \rangle + I_9$.

$w(X^i Y^j) = 3i + 4j$.
$X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if:

- $w(X^\alpha Y^\beta) < w(X^\gamma Y^\delta)$
- $w(X^\alpha Y^\beta) = w(X^\gamma Y^\delta)$ but $\beta < \delta$

$\{X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\}$ is a Gröbner basis w.r.t. $\prec_w$.

Hermitian curves

$I = \langle X^4 - Y^3 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
Hermitian variety: $\#\mathcal{V}(I_9) = 27$.

Given $F(X, Y) \in \mathbb{F}_9[X, Y]$ how many roots from Hermitian variety? That is we ask for the size of the variety of $\langle F \rangle + I_9$.

$w(X^i Y^j) = 3i + 4j$.
$X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if:

- $w(X^\alpha Y^\beta) < w(X^\gamma Y^\delta)$
- $w(X^\alpha Y^\beta) = w(X^\gamma Y^\delta)$ but $\beta < \delta$

$\{X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\}$ is a Gröbner basis w.r.t. $\prec_w$.

Hermitian curves – cont.

$\{X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\}$ is a Gröbner basis w.r.t. $\prec_w$.

8	11	14	17	20	23	26	29	32	35	38	$\cdots$
4	7	10	13	16	19	22	25	28	31	34	$\cdots$
0	3	6	9	12	15	18	21	24	27	30	$\cdots$

Figure: $w(\Delta(\langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\rangle))$ and $w(\Delta(\langle X^4 - Y^3 - Y\rangle))$

Observe, that all weights are different and $X^4 - Y^3 - Y$ has two monomials of highest weight.

Hence,
$w(X^iY^jF(X,Y)) = w(X^iY^jF(X,Y) \text{ rem } \{X^4 - Y^3 - Y\})$ and the leading monomial of the latter can be identified by its weight.

Hermitian curves – cont.

$\{X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\}$ is a Gröbner basis w.r.t. $\prec_w$.

8	11	14	17	20	23	26	29	32	35	38	$\cdots$
4	7	10	13	16	19	22	25	28	31	34	$\cdots$
0	3	6	9	12	15	18	21	24	27	30	$\cdots$

Figure: $w(\Delta(\langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\rangle))$ and $w(\Delta(\langle X^4 - Y^3 - Y\rangle))$

Observe, that all weights are different and $X^4 - Y^3 - Y$ has two monomials of highest weight.

Hence,
$w(X^iY^jF(X,Y)) = w(X^iY^jF(X,Y) \text{ rem } \{X^4 - Y^3 - Y\})$ and the leading monomial of the latter can be identified by its weight.

Hermitian curves – cont.

8	11	14	(17)	20	23	26	29	32
4	7	10	13	16	19	22	25	28
0	3	6	9	12	15	18	(21)	24

Figure: $\text{lm}(F) = X^3Y^2$

$\text{lm}(F) = X^3Y^2$. This is of weight 17. We have YF rem $\{X^4 - Y^3 - Y\} \in I_9$ and as $w(Y) = 4$ the leading monomial is of weight $17 + 4 = 21$. Hence, it is X^7

The footprint of $\langle F(X,Y), X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\rangle$ is of size at most 17.

Hermitian curves – cont.

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	(28)
0	3	6	9	12	15	18	21	24

Figure: $\mathrm{lm}(F) = X^3Y^2$

General result: $F(X, Y)$ can have at most $w(\mathrm{lm}(F))$ roots on the Hermitian curve.

Not sharp in the upper right corner: $w(\mathrm{lm}(F)) = 28$, but the Hermitian curve has only 27 affine points. From the footprint clear that at most 25 roots. This simple observation has a huge impact. It allows for improved information and improved code constructions.

Generalizes to $X^{q+1} - Y^q - Y \in \mathbb{F}_{q^2}[X, Y]$ ... and as we shall see in a moment to any one-point AG code construction.

Hermitian curves – cont.

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	(28)
0	3	6	9	12	15	18	21	24

Figure: $\text{lm}(F) = X^3Y^2$

General result: $F(X, Y)$ can have at most $w(\text{lm}(F))$ roots on the Hermitian curve.

Not sharp in the upper right corner: $w(\text{lm}(F)) = 28$, but the Hermitian curve has only 27 affine points. From the footprint clear that at most 25 roots. This simple observation has a huge impact. It allows for improved information and improved code constructions.

Generalizes to $X^{q+1} - Y^q - Y \in \mathbb{F}_{q^2}[X, Y]$ ... and as we shall see in a moment to any one-point AG code construction...

Hermitian curves – cont.

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	(28)
0	3	6	9	12	15	18	21	24

Figure: $\text{lm}(F) = X^3Y^2$

General result: $F(X, Y)$ can have at most $w(\text{lm}(F))$ roots on the Hermitian curve.

Not sharp in the upper right corner: $w(\text{lm}(F)) = 28$, but the Hermitian curve has only 27 affine points. From the footprint clear that at most 25 roots. This simple observation has a huge impact. It allows for improved information and improved code constructions.

Generalizes to $X^{q+1} - Y^q - Y \in \mathbb{F}_{q^2}[X, Y]$ ... and as we shall see in a moment to any one-point AG code construction ...

Order domain conditions (for curves)

Let $w_1, \ldots, w_m$ be fixed and define $w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w_1 + \cdots + i_m w_m$. Define weighted degree ordering $\prec_w$ by $N \prec_w M$ if

- $w(N) < w(M)$
- $w(N) = w(M)$ but $N \prec_{lex} M$.

(one may replace $\prec_{lex}$ with any other monomial ordering)
Given an ordering as above we will say that I satisfies the order domain conditions if:

- I possesses a Gröbner basis $\{F_1, \ldots, F_s\}$ w.r.t. $\prec_w$ such that F_i has exactly two monomials of highest weight, $i = 1, \ldots, s$.
- No two different monomials in $\Delta_{\prec_w}(I)$ has the same weight.

Everything we did with the Hermitian curve works in this general set-up!!! (can even be generalized to higher dimensional weights).

Order domain conditions (for curves)

Let $w_1, \ldots, w_m$ be fixed and define $w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w_1 + \cdots + i_m w_m$. Define weighted degree ordering $\prec_w$ by $N \prec_w M$ if

- $w(N) < w(M)$
- $w(N) = w(M)$ but $N \prec_{lex} M$.

(one may replace $\prec_{lex}$ with any other monomial ordering)
Given an ordering as above we will say that I satisfies the order domain conditions if:

- I possesses a Gröbner basis $\{F_1, \ldots, F_s\}$ w.r.t. $\prec_w$ such that F_i has exactly two monomials of highest weight, $i = 1, \ldots, s$.
- No two different monomials in $\Delta_{\prec_w}(I)$ has the same weight.

Everything we did with the Hermitian curve works in this general set-up!!! (can even be generalized to higher dimensional weights).

Order domain conditions (for curves)

Let $w_1, \ldots, w_m$ be fixed and define $w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w_1 + \cdots + i_m w_m$. Define weighted degree ordering $\prec_w$ by $N \prec_w M$ if

- $w(N) < w(M)$
- $w(N) = w(M)$ but $N \prec_{lex} M$.

(one may replace $\prec_{lex}$ with any other monomial ordering)
Given an ordering as above we will say that I satisfies the order domain conditions if:

- I possesses a Gröbner basis $\{F_1, \ldots, F_s\}$ w.r.t. $\prec_w$ such that F_i has exactly two monomials of highest weight, $i = 1, \ldots, s$.
- No two different monomials in $\Delta_{\prec_w}(I)$ has the same weight.

Everything we did with the Hermitian curve works in this general set-up!!! (can even be generalized to higher dimensional weights).

An amazing result due to Miura and Pellikaan

Consider an algebraic function field of transcendence degree 1. Let P be a rational place and ν_P the corresponding valuation. Consider $R = \cup_{m=0}^{\infty} \mathcal{L}(mP)$ with corresponding Weierstrass semigroup $-\nu_P(R) = \langle w_1, \ldots, w_m \rangle$.
Then R can be described as $\mathbb{F}[X_1, \ldots, X_m]/I$ where $\prec_w$ and I satisfy the orderdomain conditions!!!!!

- We can avoid Riemann-Roch and improve upon the Goppa bound (both at a theoretical and practical level)
- All "points" are affine in this model (except the hidden point P)
- Suggests a way to treat higher dimensional objects.

An amazing result due to Miura and Pellikaan

Consider an algebraic function field of transcendence degree 1. Let P be a rational place and ν_P the corresponding valuation. Consider $R = \cup_{m=0}^{\infty} \mathcal{L}(mP)$ with corresponding Weierstrass semigroup $-\nu_P(R) = \langle w_1, \ldots, w_m \rangle$.
Then R can be described as $\mathbb{F}[X_1, \ldots, X_m]/I$ where $\prec_w$ and I satisfy the orderdomain conditions!!!!!

- We can avoid Riemann-Roch and improve upon the Goppa bound (both at a theoretical and practical level)
- All "points" are affine in this model (except the hidden point P)
- Suggests a way to treat higher dimensional objects.

Our application to rational places

As all "points" are affine in this model, from the footprint bound we derive bounds on the number of rational places.

Let $\mathcal{F}$ be an algebraic function field over $\mathbb{F}_q$ of transcendence degree 1. Assume $\mathcal{F}$ possesses a rational place with Weierstrass semigroup $\Lambda = \langle w_1, \ldots, w_m \rangle$.
The number of rational places of $\mathcal{F}$ is at most

$$\#\left(\Lambda \backslash \cup_{i=1}^{m} (qw_i + \Lambda) + 1\right)$$

The genus $g = \#(\mathbb{N}_0 \backslash \Lambda)$ is an invariant.

For small g we can run through all possible semigroups with g gaps and obtain a bound in terms of g and q. Also we can derive some general estimates. Such bounds are sharper than the Serre bound for small fields!!!

Our application to rational places

As all "points" are affine in this model, from the footprint bound we derive bounds on the number of rational places.

Let $\mathcal{F}$ be an algebraic function field over $\mathbb{F}_q$ of transcendence degree 1. Assume $\mathcal{F}$ possesses a rational place with Weierstrass semigroup $\Lambda = \langle w_1, \ldots, w_m \rangle$.
The number of rational places of $\mathcal{F}$ is at most

$$\#\left(\Lambda \backslash \cup_{i=1}^{m} (qw_i + \Lambda) + 1 \right)$$

The genus $g = \#(\mathbb{N}_0 \backslash \Lambda)$ is an invariant.

For small g we can run through all possible semigroups with g gaps and obtain a bound in terms of g and q. Also we can derive some general estimates. Such bounds are sharper than the Serre bound for small fields!!!

Our application to rational places

As all "points" are affine in this model, from the footprint bound we derive bounds on the number of rational places.

Let $\mathcal{F}$ be an algebraic function field over $\mathbb{F}_q$ of transcendence degree 1. Assume $\mathcal{F}$ possesses a rational place with Weierstrass semigroup $\Lambda = \langle w_1, \ldots, w_m \rangle$.
The number of rational places of $\mathcal{F}$ is at most

$$\#\left(\Lambda \backslash \cup_{i=1}^{m} (qw_i + \Lambda) + 1\right)$$

The genus $g = \#(\mathbb{N}_0 \backslash \Lambda)$ is an invariant.

For small g we can run through all possible semigroups with g gaps and obtain a bound in terms of g and q. Also we can derive some general estimates. Such bounds are sharper than the Serre bound for small fields!!!

Part 4:

Remarks on general linear codes

primary versus dual codes

In coding theory we consider both primary (image) and dual (kernel) description of codes.

The footprint method is mostly usefull for primary codes.
The order bound or the original Feng-Rao bound usefull for dual codes.

Both the Feng-Rao bound and the footprint bound can be translated to linear code (linear algebra) level. Here, multiplication is replaced with componentwise inner product!!!

At this level we call the footprint bound for the Feng-Rao bound for primary codes – since one can show that the two Feng-Rao bounds are consequences of each other.

primary versus dual codes

In coding theory we consider both primary (image) and dual (kernel) description of codes.

The footprint method is mostly usefull for primary codes.
The order bound or the original Feng-Rao bound usefull for dual codes.

Both the Feng-Rao bound and the footprint bound can be translated to linear code (linear algebra) level. Here, multiplication is replaced with componentwise inner product!!!

At this level we call the footprint bound for the Feng-Rao bound for primary codes – since one can show that the two Feng-Rao bounds are consequences of each other.

primary versus dual codes

In coding theory we consider both primary (image) and dual (kernel) description of codes.

The footprint method is mostly usefull for primary codes.
The order bound or the original Feng-Rao bound usefull for dual codes.

Both the Feng-Rao bound and the footprint bound can be translated to linear code (linear algebra) level. Here, multiplication is replaced with componentwise inner product!!!

At this level we call the footprint bound for the Feng-Rao bound for primary codes – since one can show that the two Feng-Rao bounds are consequences of each other.