Bounding the number of affine roots

with applications in reliable and secure communication

Olav Geil

Inaugural Lecture, Aalborg University,
August 11110, 11111100000

Bounding the number of affine roots – with applications in reliable and secure communication

Polynomials: $F(X) = 2X^2 - 6X + 4$ and $G(X, Y) = 3X^3Y + 5XY^5 - 9XY - 148$.

Roots: $F(2) = 2 \cdot 2^2 - 6 \cdot 2 + 4 = 8 - 12 + 4 = 0$ and $G\big((1, 2)\big) = 3 \cdot 1^3 \cdot 2 + 5 \cdot 1 \cdot 2^5 - 9 \cdot 1 \cdot 2 - 138 = 6 + 160 - 18 - 148 = 0$

Affine: Means do not worry (actually means not projective)

Field: A nice system of mathematical objects with addition, subtraction, multiplication and division. Examples: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$.

Coding theory: Reliable communication in noisy environment

Secret sharing: Share information among participants so that only specified groups can recover the secret

Bounding the number of affine roots – with applications in reliable and secure communication

Polynomials: $F(X) = 2X^2 - 6X + 4$ and
$G(X, Y) = 3X^3Y + 5XY^5 - 9XY - 148.$

Roots: $F(2) = 2 \cdot 2^2 - 6 \cdot 2 + 4 = 8 - 12 + 4 = 0$ and
$G\big((1, 2)\big) = 3 \cdot 1^3 \cdot 2 + 5 \cdot 1 \cdot 2^5 - 9 \cdot 1 \cdot 2 - 138 = 6 + 160 - 18 - 148 = 0$

Affine: Means do not worry (actually means not projective)

Field: A nice system of mathematical objects with addition, subtraction, multiplication and division. Examples: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$.

Coding theory: Reliable communication in noisy environment

Secret sharing: Share information among participants so that only specified groups can recover the secret

From the foreword of *Finite Fields* by Rudolf Lidl and Harald Niederreiter, 1996:

> **The theory of finite fields is a branch of modern algebra that has come to the fore in the last 50 years because of its diverse applications in combinatorics, coding theory, and the mathematical study of switching circuits, among others.** The origins of the subject reach back into the 17th and 18th century...Fermat...Euler...Lagrange...Legendre contributing to the structure theory of special finite fields—namely, the so-called finite prime fields. The general theory of finite fields may be said to begin with the work of...Gauss...Galois, **but it only became of interest for applied mathematicians in recent decades with the emergence of discrete mathematics as a serious discipline.**

Prime fields

$\mathbb{F}_2 = \{0, 1\}$. Rule: $2 = 0$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$1 + 1 = 2 = 0$

Hence, $-1 = 1$ and $\frac{1}{1} = 1$

Prime fields

$\mathbb{F}_2 = \{0, 1\}$. Rule: $2 = 0$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$1 + 1 = 2 = 0$

Hence, $-1 = 1$ and $\frac{1}{1} = 1$

Prime fields – cont.

$\mathbb{F}_3 = \{0, 1, 2\}$. Rule: $3 = 0$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$2 \cdot 2 = 4 = 1$

Hence, $-1 = 2$, $-2 = 1$, $\frac{1}{1} = 1$, and $\frac{1}{2} = 2$.

Prime fields – cont.

$\mathbb{F}_3 = \{0, 1, 2\}$. Rule: $3 = 0$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$2 \cdot 2 = 4 = 1$

Hence, $-1 = 2$, $-2 = 1$, $\frac{1}{1} = 1$, and $\frac{1}{2} = 2$.

...ups

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Rule: $4 = 0$

$2 \cdot 0 = 0$, $2 \cdot 1 = 2$, $2 \cdot 2 = 4 = 0$, and $2 \cdot 3 = 6 = 2$. Hence, we cannot divide by 2!!!

Field extensions

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. Rules: $2 = 0$ and $\alpha^2 = \alpha + 1$

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$(\alpha + 1) \cdot \alpha = \alpha^2 + \alpha = \alpha + 1 + \alpha = 2\alpha + 1 = 1$

Hence, $-1 = 1$, $-\alpha = \alpha$, $-(\alpha + 1) = \alpha + 1$, $\dfrac{1}{1} = 1$, $\dfrac{1}{\alpha} = \alpha + 1$ and $\dfrac{1}{\alpha + 1} = \alpha$.

Field extensions

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. Rules: $2 = 0$ and $\alpha^2 = \alpha + 1$

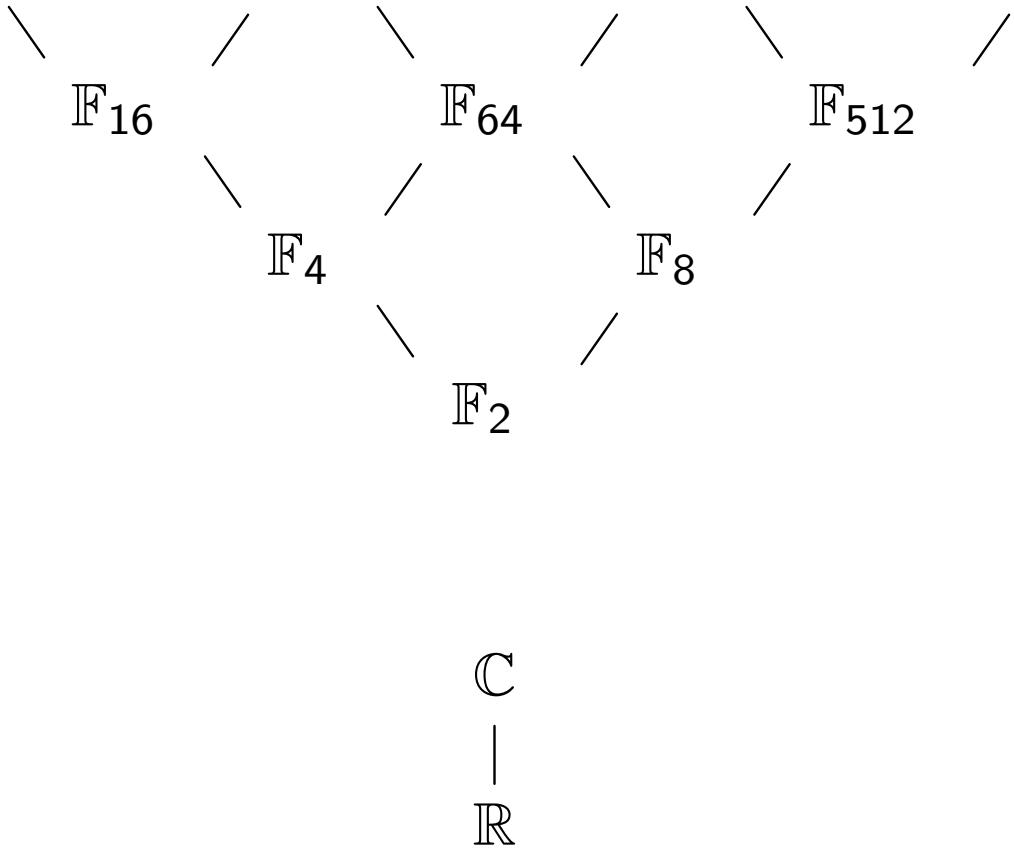
$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

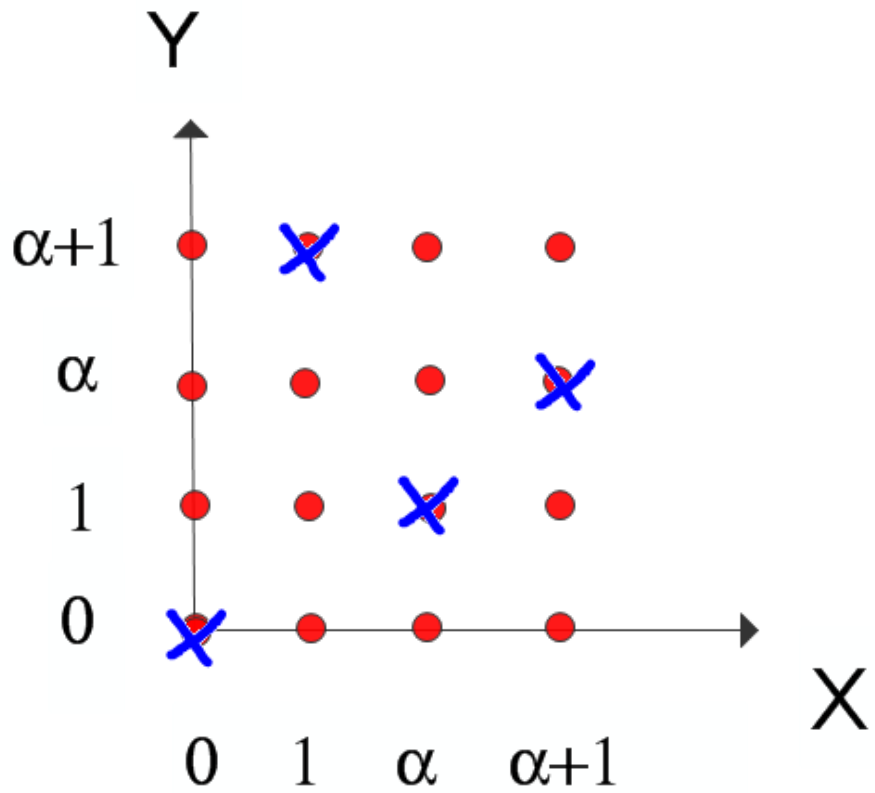
$(\alpha + 1) \cdot \alpha = \alpha^2 + \alpha = \alpha + 1 + \alpha = 2\alpha + 1 = 1$

Hence, $-1 = 1$, $-\alpha = \alpha$, $-(\alpha + 1) = \alpha + 1$, $\frac{1}{1} = 1$, $\frac{1}{\alpha} = \alpha + 1$ and $\frac{1}{\alpha + 1} = \alpha$.

Field extensions – cont.



The line $Y = (\alpha + 1)X$ over $\mathbb{F}_4$



Even more weird

$(1, 0, 1, 0)$ is orthogonal to itself!!! (over $\mathbb{F}_2$ or $\mathbb{F}_4$ or...) as

$$1 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 = 2 = 0.$$

...but we **can** (and do) apply most of the usual linear algebra machinery anyway

Communication over noisy channels

Until 1948: "Nothing better than repetition codes exists"

Rather than transmitting 0, send 000.
Rather than transmitting 1, send 111.

If 010 is received, then decode to 0
If 110 is received, then decode to 1...

Shannon, 1948:
It is possible to communicate reliable with any rate up till the capacity of a given channel. Use long enough codes (random codes work!!!)

...however, to prove that a code is actually good and to decode we do need (algebraic) structure!!!

Communication over noisy channels

Until 1948: "Nothing better than repetition codes exists"

Rather than transmitting 0, send 000.
Rather than transmitting 1, send 111.

If 010 is received, then decode to 0
If 110 is received, then decode to 1...

Shannon, 1948:
It is possible to communicate reliable with any rate up till the capacity of a given channel. Use long enough codes (random codes work!!!)

...however, to prove that a code is actually good and to decode we do need (algebraic) structure!!!

Linear 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 linear 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: $\vec{m} \begin{bmatrix} \vec{g}_1 \\ \vdots \\ \vec{g}_k \end{bmatrix} = \vec{c}$.

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

Linear 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 linear 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: $\vec{m} \begin{bmatrix} \vec{g}_1 \\ \vdots \\ \vec{g}_k \end{bmatrix} = \vec{c}$.

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

Reed-Solomon codes

Example: The Reed-Solomon code of dimension 3 over $\mathbb{F}_7$ is denoted $\mathrm{RS}_7(3)$.

$\mathbb{F}_7 = \{0, 1, 2, \ldots, 6\}$. Rule: $7 = 0$.

$\vec{m} = (2, 1, 3)$ is encoded as follows:

$F(X) = 2 + X + 3X^2$

$\vec{c} = (F(0), F(1), F(2), \ldots, F(6)) = (2, 6, 2, 4, 5, 5, 4)$

Reed-Solomon codes – cont.

$\mathrm{RS}_q(k)$, $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$, $(k \leq q = n)$

$\vec{m} = (f_0, f_1, \ldots, f_{k-1})$

$F(X) = f_0 + f_1 X + \cdots + f_{k-1} X^{k-1}$

$\vec{c} = (F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_q))$

Codewords are of length $n = q$. The dimension is k. The minimum distance is $n - k + 1$ as a polynomial of degree at most $k - 1$ can have at most $k - 1$ zeros.

Reed-Solomon codes – cont.

$\mathrm{RS}_q(k)$, $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$, $(k \leq q = n)$

$\vec{m} = (f_0, f_1, \ldots, f_{k-1})$

$F(X) = f_0 + f_1 X + \cdots + f_{k-1} X^{k-1}$

$\vec{c} = (F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_q))$

Codewords are of length $n = q$. The dimension is k. The minimum distance is $n - k + 1$ as a polynomial of degree at most $k - 1$ can have at most $k - 1$ zeros.

Why polynomials?

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

$$F(X,Y) =$$

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

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

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

Why polynomials?

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

$F(X,Y) =$

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

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

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

From one variable to more

$F(X) \in \mathbb{F}[X]$ has at most $\deg F$ zeros 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 zeros of $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ over finite set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}$ then finitely many zeros.

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

From one variable to more

$F(X) \in \mathbb{F}[X]$ has at most $\deg F$ zeros 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 zeros of $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ over finite set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}$ then finitely many zeros.

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

From one variable to more

$F(X) \in \mathbb{F}[X]$ has at most $\deg F$ zeros 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 zeros of $F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ over finite set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}$ then finitely many zeros.

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

Zeros over finite sets

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

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

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

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

Zeros over finite sets

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

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

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

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

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

To specify that we are looking for roots over $\mathbb{F}_5$ we include the polynomials $X^5 - X, Y^5 - Y$.

Hence, we consider the common roots of $X^2Y + Y^2 + 2, X^5 - X, Y^5 - Y$.

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

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

To specify that we are looking for roots over $\mathbb{F}_5$ we include the polynomials $X^5 - X, Y^5 - Y$.

Hence, we consider the common roots of $X^2Y + Y^2 + 2, X^5 - X, Y^5 - Y$.

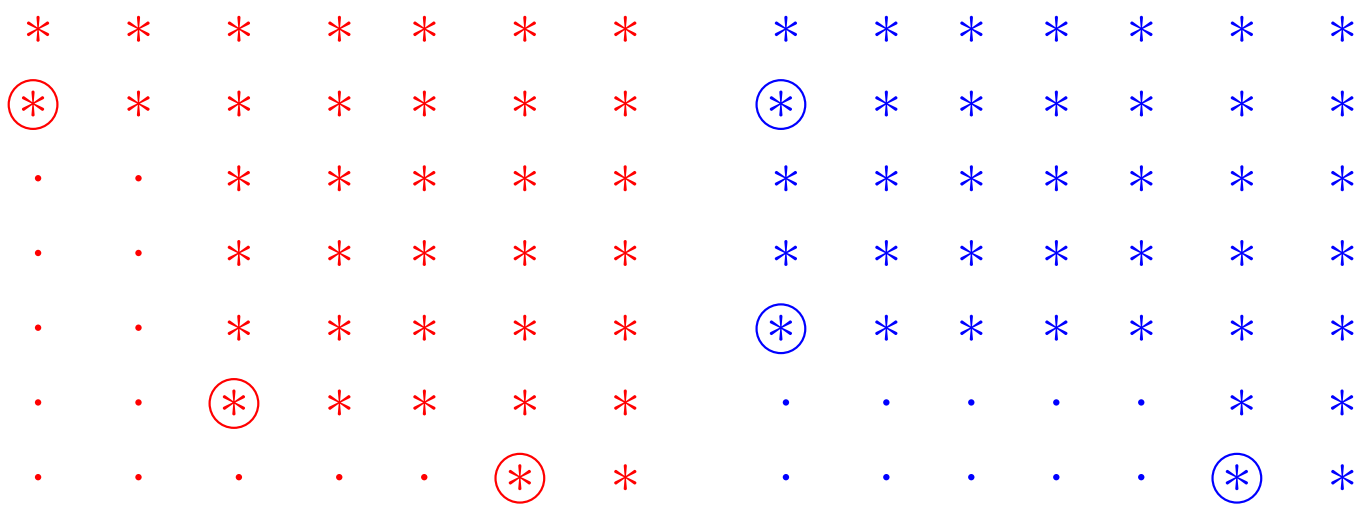


Figure: Two choices: $\mathrm{Im}(F) = X^2Y$ or $\mathrm{Im}(F) = Y^2$. Number of zeros at most $\min\{13, 10\} = 10$

Univariate polynomials – revisited

$F(X) = X^2 + 2X + 4$ over $\mathbb{F}_5$

Hence, we consider the number of common zeros of $F(X), X^5 - X$.

Figure: An alternative way to see the well-known result

Univariate polynomials – revisited

$F(X) = X^2 + 2X + 4$ over $\mathbb{F}_5$

Hence, we consider the number of common zeros of $F(X), X^5 - X$.

Figure: An alternative way to see the well-known result

When we only know the leading monomial

Let $\mathrm{lm}(F) = X_1^{i_1} \cdots X_m^{i_m}$ 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 $s_1 \cdots s_m - (s_1 - i_1) \cdots (s_m - i_m)$ zeros.

Y^4	XY^4	X^2Y^4	X^3Y^4	X^4Y^4
Y^3	XY^3	X^2Y^3	X^3Y^3	X^4Y^3
Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2
Y	XY	X^2Y	X^3Y	X^4Y
1	X	X^2	X^3	X^4

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 zeros over $\mathbb{F}_5$ of bivariate polynomials

When we only know the leading monomial

Let $\mathrm{lm}(F) = X_1^{i_1} \cdots X_m^{i_m}$ 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 $s_1 \cdots s_m - (s_1 - i_1) \cdots (s_m - i_m)$ zeros.

Y^4	XY^4	X^2Y^4	X^3Y^4	X^4Y^4	20	21	22	23	24
Y^3	XY^3	X^2Y^3	X^3Y^3	X^4Y^3	15	17	19	21	23
Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	10	13	16	19	22
Y	XY	X^2Y	X^3Y	X^4Y	5	9	13	17	21
1	X	X^2	X^3	X^4	0	5	10	15	20

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

Only knowing the leading monomial – cont.

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-zeros. Hence, $s_1 s_2 - (s_1 - i_1)(s_2 - i_2)$ roots.

Generalizes to any finite Cartesian product.

Only knowing the leading monomial – cont.

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-zeros. Hence, $s_1 s_2 - (s_1 - i_1)(s_2 - i_2)$ roots.

Generalizes to any finite Cartesian product.

Only knowing the leading monomial – cont.

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-zeros. 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 zeros 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 zeros is at most dq^{m-1}.

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

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 zeros 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 zeros is at most dq^{m-1}.

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

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 zeros 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 zeros is at most dq^{m-1}.

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

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

$\mathrm{ev} : \mathbb{F}_7[X, Y] \to \mathbb{F}_7^{49}$ 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 zeros and Hamming weight of basis element

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

$\mathrm{Hyp}_7(14, 2)$ 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 zeros and Hamming weight of basis element

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

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

More polynomials

Common zeros 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 zeros 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 zeros 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.

Gaussian elimination

$$\begin{bmatrix} 1 & 1 & 2 & 1 & 1 \\ 2 & 4 & 2 & 4 & 1 \\ 3 & 3 & 6 & 6 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 2 & 1 & 1 \\ 0 & 1 & -1 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & -\frac{2}{3} \end{bmatrix}$$

corresponding to

$$\begin{cases} X_1 + X_2 + 2X_3 + X_4 + 1 \\ 2X_1 + 4X_2 + 2X_3 + 4X_4 + 1 \\ 3X_1 + 3X_2 + 6X_3 + 6X_4 + 1 \end{cases}$$

$$\Updownarrow$$

$$\begin{cases} X_1 + X_2 + 2X_3 + X_4 + 1 \\ X_2 - X_3 + X_4 - \frac{1}{2} \\ X_4 - \frac{2}{3} \end{cases}$$

Gröbner bases – an example

Consider the polynomials $X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y$.

Let the field be $\bar{\mathbb{F}}_2$

For some monomial orderings: $Y^4 + X^5 + Y, X^{16} + X$

For some other monomial orderings:
$X^5 + Y^4 + Y, XY^{12} + XY^9 + XY^6 + XY^3 + X, Y^{16} + Y$

Example cont. – first case

$Y^4 + X^5 + Y, X^{16} + X$

Figure: X on the first axis, Y on the second. Leading monomials X^{16} and Y^4

Number of common roots is $4 \cdot 16 = 64$.

Example cont. – second case

$$X^5 + Y^4 + Y, XY^{12} + XY^9 + XY^6 + XY^3 + X, Y^{16} + Y$$

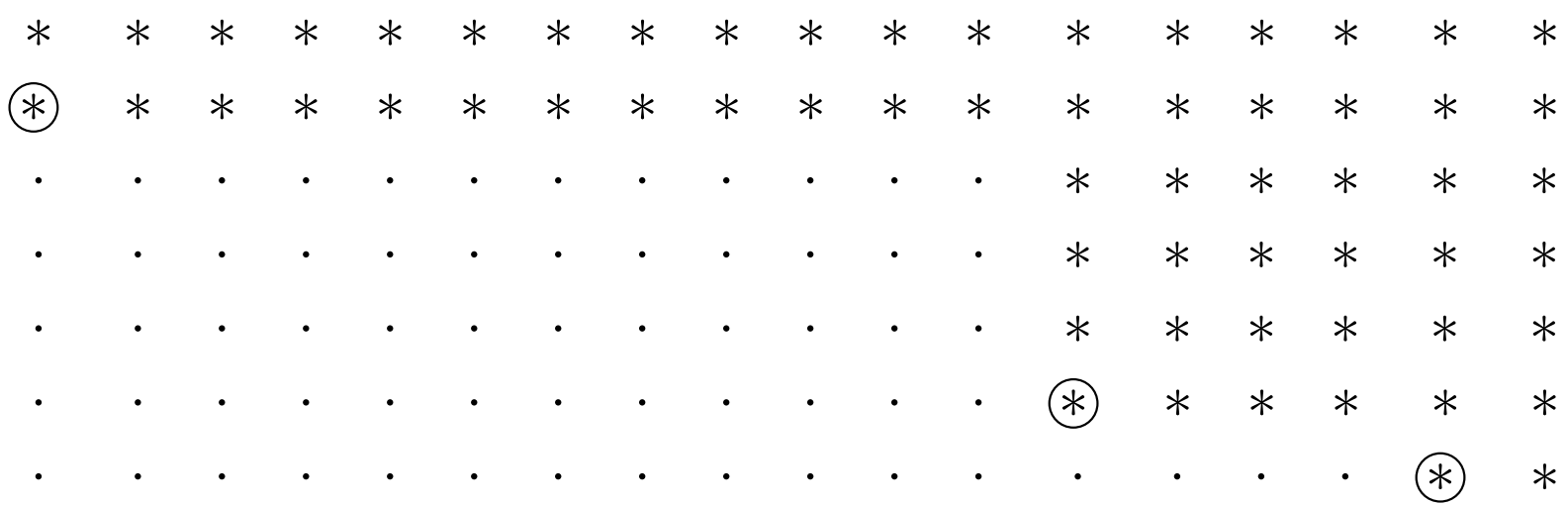


Figure: Y on the first axis, X on the second. Leading monomials X^5, XY^{12} and Y^{16}

Number of common roots is $5 \cdot 12 + 4 = 64$.

Ideals

$$
\begin{aligned}
I &= \langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle \\
&= \Big\{ K_1(X,Y)(X^5 + Y^4 + Y) + K_2(X,Y)(X^{16} + X) \\
&\qquad + K_3(X,Y)(Y^{16} + Y) \mid K_1, K_2, K_3 \in \bar{\mathbb{F}}_2[X,Y] \Big\}
\end{aligned}
$$

"Happens" to be equal to both $\langle Y^4 + X^5 + Y, X^{16} + X \rangle$ and $\langle X^5 + Y^4 + Y, XY^{12} + XY^9 + XY^6 + XY^3 + X, Y^{16} + Y \rangle$.

Ideals

$$
\begin{aligned}
I &= \langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle \\
&= \Big\{ K_1(X,Y)(X^5 + Y^4 + Y) + K_2(X,Y)(X^{16} + X) \\
&\qquad + K_3(X,Y)(Y^{16} + Y) \mid K_1, K_2, K_3 \in \bar{\mathbb{F}}_2[X,Y] \Big\}
\end{aligned}
$$

"Happens" to be equal to both $\langle Y^4 + X^5 + Y, X^{16} + X \rangle$ and $\langle X^5 + Y^4 + Y, XY^{12} + XY^9 + XY^6 + XY^3 + X, Y^{16} + Y \rangle$.

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

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

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

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

The footprint bound

Theorem (footprint bound): The number of zeros 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 $X_1^q - X_1, \ldots, X_m^q - X_m$.

The footprint bound

Theorem (footprint bound): The number of zeros 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 $X_1^q - X_1, \ldots, X_m^q - X_m$.

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

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- The leading monomial of any polynomial in I is divisible by some $\mathrm{lm}(F_1), \ldots, \mathrm{lm}(F_s)$

Buchberger's algorithm extends any basis to a Gröbner basis. 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

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- The leading monomial of any polynomial in I is divisible by some $\mathrm{lm}(F_1), \ldots, \mathrm{lm}(F_s)$

Buchberger's algorithm extends any basis to a Gröbner basis. 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

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- The leading monomial of any polynomial in I is divisible by some $\mathrm{lm}(F_1), \ldots, \mathrm{lm}(F_s)$

Buchberger's algorithm extends any basis to a Gröbner basis. 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

- $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \in I$
- The leading monomial of any polynomial in I is divisible by some $\mathrm{lm}(F_1), \ldots, \mathrm{lm}(F_s)$

Buchberger's algorithm extends any basis to a Gröbner basis. Involves multivariate division algorithm.

Theoretical application of Buchberger's algorithm

What is the second highest number of zeros 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 zeros 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 zeros 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

Point-set = points on a curve

How many roots does a polynomial $F(X_1, \ldots, X_m)$ have among the points on the curve?

Corresponds to asking for the number of common roots of the polynomials defining the curve and $F(X_1, \ldots, X_m)$.

The curves that we are interested in have particular nice properties that we can employ.

Example: Hermitian curve over $\mathbb{F}_9$ = the roots of $X^4 - Y^3 - Y$.

$I = \langle X^4 - Y^3 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.

The latter is a Gröbner basis when Y^3 is leading. Hence, 27 points.

Point-set = points on a curve

How many roots does a polynomial $F(X_1, \ldots, X_m)$ have among the points on the curve?

Corresponds to asking for the number of common roots of the polynomials defining the curve and $F(X_1, \ldots, X_m)$.

The curves that we are interested in have particular nice properties that we can employ.

Example: Hermitian curve over $\mathbb{F}_9$ = the roots of $X^4 - Y^3 - Y$.

$I = \langle X^4 - Y^3 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.

The latter is a Gröbner basis when Y^3 is leading. Hence, 27 points.

Point-set = points on a curve

How many roots does a polynomial $F(X_1, \ldots, X_m)$ have among the points on the curve?

Corresponds to asking for the number of common roots of the polynomials defining the curve and $F(X_1, \ldots, X_m)$.

The curves that we are interested in have particular nice properties that we can employ.

Example: Hermitian curve over $\mathbb{F}_9$ = the roots of $X^4 - Y^3 - Y$.

$I = \langle X^4 - Y^3 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.
$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.

The latter is a Gröbner basis when Y^3 is leading. Hence, 27 points.

Hermitian curve

Given $F(X,Y) \in \mathbb{F}_9[X,Y]$ how many roots does it have on the Hermitian curve? That is, we ask what is the number of common roots of $F(X,Y), X^4 - Y^3 - Y, X^9 - X, Y^9 - Y$.

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

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

Hermitian curve

Given $F(X,Y) \in \mathbb{F}_9[X,Y]$ how many roots does it have on the Hermitian curve? That is, we ask what is the number of common roots of $F(X,Y), X^4 - Y^3 - Y, X^9 - X, Y^9 - Y$.

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

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

Hermitian curve – cont.

$\{X^4 - Y^3 - Y\}$ is a Gröbner basis for I w.r.t. $\prec_w$.
$\{X^4 - Y^3 - Y, X^9 - X\}$ is a Gröbner basis for I_9 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: $w(\Delta_{\prec_w}(I_9))$ and $w(\Delta_{\prec_w}(I))$

Observe, that all weights are different and $X^4 - Y^3 - Y$ has two monomials of highest weight.
We can w.l.o.g. assume that $F(X, Y)$ is a linear combination of monomials in $\Delta_{\prec_w}(I_9)$.

Crucial observation: Hence,
$w\left(X^i Y^j F(X, Y)\right) = w\left(X^i Y^j F(X, Y) \text{ rem } \{X^4 - Y^3 - Y\}\right)$ and the leading monomial of the latter can be identified by its weight.

Hermitian curve – cont.

$\{X^4 - Y^3 - Y\}$ is a Gröbner basis for I w.r.t. $\prec_w$.
$\{X^4 - Y^3 - Y, X^9 - X\}$ is a Gröbner basis for I_9 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: $w(\Delta_{\prec_w}(I_9))$ and $w(\Delta_{\prec_w}(I))$

Observe, that all weights are different and $X^4 - Y^3 - Y$ has two monomials of highest weight.
We can w.l.o.g. assume that $F(X, Y)$ is a linear combination of monomials in $\Delta_{\prec_w}(I_9)$.

Crucial observation: Hence,

$$w\left(X^i Y^j F(X,Y)\right) = w\left(X^i Y^j F(X,Y) \text{ rem } \{X^4 - Y^3 - Y\}\right)$$ and the leading monomial of the latter can be identified by its weight.

Hermitian curve – cont.

$\{X^4 - Y^3 - Y\}$ is a Gröbner basis for I w.r.t. $\prec_w$.
$\{X^4 - Y^3 - Y, X^9 - X\}$ is a Gröbner basis for I_9 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: $w(\Delta_{\prec_w}(I_9))$ and $w(\Delta_{\prec_w}(I))$

Observe, that all weights are different and $X^4 - Y^3 - Y$ has two monomials of highest weight.
We can w.l.o.g. assume that $F(X, Y)$ is a linear combination of monomials in $\Delta_{\prec_w}(I_9)$.

Crucial observation: Hence,
$w\big(X^i Y^j F(X, Y)\big) = w\Big(X^i Y^j F(X, Y) \text{ rem } \{X^4 - Y^3 - Y\}\Big)$ 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: $\mathrm{Im}(F) = X^3Y^2$

$$
\begin{aligned}
F(X,Y) &= X^3Y^2 + \text{ lower terms} \\
&\to YF(X,Y) = X^3Y^3 + \text{ lower terms} \\
&\to X^3Y^3 + \text{ lower terms } + X^3(X^4 - Y^3 - Y) \\
&= X^7 + \text{ lower terms } \in \langle F(X,Y), X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle
\end{aligned}
$$

The simple version: $17 + 4 = 21$.

Amazing result: Estimate on size of footprint equals $17 = w(X^3Y^2)$

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

$$
\begin{aligned}
F(X,Y) &= X^3Y^2 + \text{ lower terms} \\
&\to YF(X,Y) = X^3Y^3 + \text{ lower terms} \\
&\to X^3Y^3 + \text{ lower terms } + X^3(X^4 - Y^3 - Y) \\
&= X^7 + \text{ lower terms } \in \langle F(X,Y), X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle
\end{aligned}
$$

The simple version: $17 + 4 = 21$.

Amazing result: Estimate on size of footprint equals $17 = w(X^3Y^2)$

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: $\mathrm{Im}(F) = X^8 Y$

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

Not sharp in the upper right corner: $w(\mathrm{Im}(F)) = 28$, but the Hermitian curve has only 27 affine points. From the footprint clear that at most 25 roots.

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: $\mathrm{Im}(F) = X^8 Y$

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

Not sharp in the upper right corner: $w(\mathrm{Im}(F)) = 28$, but the Hermitian curve has only 27 affine points. From the footprint clear that at most 25 roots.

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 $N \prec_{lex} M$.

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 $\Delta_{\prec_w}(I)$ have the same weight.

Everything we did with the Hermitian curve works in this general set-up!!!

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 $N \prec_{lex} M$.

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 $\Delta_{\prec_w}(I)$ have the same weight.

Everything we did with the Hermitian curve works in this general set-up!!!

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 $N \prec_{lex} M$.

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 $\Delta_{\prec_w}(I)$ have the same weight.

Everything we did with the Hermitian curve works in this general set-up!!!

Impli/appli–cations

- Gives a simple way of treating general one-point algebraic geometric codes at a theoretical level.
- Gives tools for actual construction of one-point algebraic geometric codes.
- Allows for generalization to higher dimensional objects.
- Derived results in algebraic function field theory.
- Various new constructions by relaxing the order domain conditions.
- And so on and so forth...

A surprising implication in algebraic function field theory

K a field. $K(x)$ the field of fractions of $K[x]$.

If F is a finite algebraic extension of $K(x)$ then F/K is called an algebraic function field of one variable.

A ring $\mathcal{O}$, $K \subsetneq \mathcal{O} \subsetneq F$ is called a valuation ring if for any $z \in F$ we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

$\mathcal{O}$ has a unique maximal ideal (called a place). We have $P = \mathcal{O} \backslash \mathcal{O}^* = t\mathcal{O}$.
Any $0 \neq z \in F$ can be uniquely written $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}^*$ in which case we write $\nu_P(z) = n$. We define $\nu_P(0) = \infty$.

If $K = \mathcal{O}_P/P$ then P is called a rational place.

A surprising implication in algebraic function field theory

K a field. $K(x)$ the field of fractions of $K[x]$.

If F is a finite algebraic extension of $K(x)$ then F/K is called an algebraic function field of one variable.

A ring $\mathcal{O}$, $K \subsetneq \mathcal{O} \subsetneq F$ is called a valuation ring if for any $z \in F$ we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

$\mathcal{O}$ has a unique maximal ideal (called a place). We have $P = \mathcal{O} \backslash \mathcal{O}^* = t\mathcal{O}$.
Any $0 \neq z \in F$ can be uniquely written $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}^*$ in which case we write $\nu_P(z) = n$. We define $\nu_P(0) = \infty$.

If $K = \mathcal{O}_P/P$ then P is called a rational place.

Surprising implication – cont.

Let P be a rational place, then the Weierstrass semigroup related to P is

$$\begin{aligned} \Lambda_P &= \{-\nu_P(x) \in \mathbb{N}_0 \mid x \in F, \nu_Q(x) \geq 0 \text{ for all } Q \neq P\} \\ &= \mathbb{N}_0 \backslash \{i_1, \ldots, i_g\}. \end{aligned}$$

The number g is an invariant of the function field called the genus.

Research area (for function fields over $\mathbb{F}_q$): Bound the number of rational places in terms of g and q.

Surprising implication – cont.

Let P be a rational place, then the Weierstrass semigroup related to P is

$$\begin{aligned} \Lambda_P &= \{-\nu_P(x) \in \mathbb{N}_0 \mid x \in F, \nu_Q(x) \geq 0 \text{ for all } Q \neq P\} \\ &= \mathbb{N}_0 \backslash \{i_1, \ldots, i_g\}. \end{aligned}$$

The number g is an invariant of the function field called the genus.

Research area (for function fields over $\mathbb{F}_q$): Bound the number of rational places in terms of g and q.

Surprising consequence of the footprint bound

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

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

For small g (genus) 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!!!

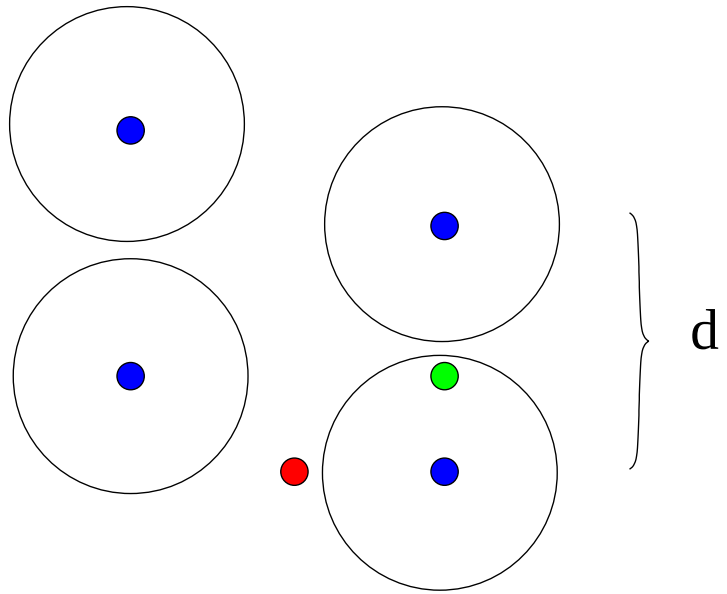
Surprising consequence of the footprint bound

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

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

For small g (genus) 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!!!

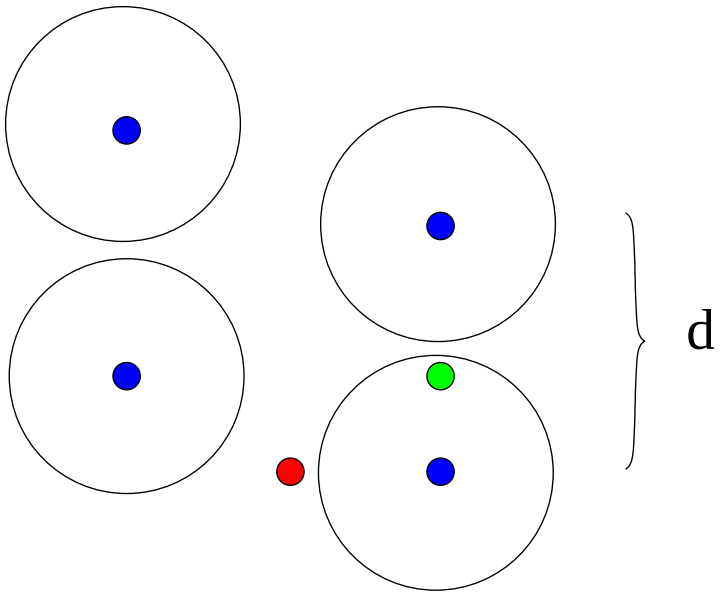
List decoding



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.

An important ingredient is zeros of multiplicity more than one.

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.

An important ingredient is zeros of multiplicity more than one.

Multiplicity

Definition: $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ is a zero 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,

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

Example: The number of zeros of $F(X, Y)$ of multiplicity at least 2 over $\mathbb{F}_q$ is related to

$$\langle F(X, Y), (X^q - X)^2, (X^q - X)(Y^q - Y), (Y^q - Y)^2 \rangle.$$

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

Theorem: (The Schwartz-Zippel bound) 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 zero 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,

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

Example: The number of zeros of $F(X, Y)$ of multiplicity at least 2 over $\mathbb{F}_q$ is related to

$$\langle F(X, Y), (X^q - X)^2, (X^q - X)(Y^q - Y), (Y^q - Y)^2 \rangle.$$

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

Theorem: (The Schwartz-Zippel bound) 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 zero 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,

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

Example: The number of zeros of $F(X, Y)$ of multiplicity at least 2 over $\mathbb{F}_q$ is related to

$$\langle F(X, Y), (X^q - X)^2, (X^q - X)(Y^q - Y), (Y^q - Y)^2 \rangle.$$

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

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

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

Multiplicity

Definition: $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ is a zero 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,

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

Example: The number of zeros of $F(X, Y)$ of multiplicity at least 2 over $\mathbb{F}_q$ is related to

$$\langle F(X, Y), (X^q - X)^2, (X^q - X)(Y^q - Y), (Y^q - Y)^2 \rangle.$$

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

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

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

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 $S_1, \ldots, S_m \subseteq \mathbb{F}$

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

Corollary: The number of zeros 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 zeros 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 zeros 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 zeros 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 zeros 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 $D(i_1, \ldots, i_m, r, s_1, \ldots, s_m)$ zeros of multiplicity at least r in $S_1 \times \cdots \times S_m$.

Research problem: Estimate the value of D for different families of cases.

Some results...but a lot of open questions!!!

Number of zeros 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 $D(i_1, \ldots, i_m, r, s_1, \ldots, s_m)$ zeros of multiplicity at least r in $S_1 \times \cdots \times S_m$.

Research problem: Estimate the value of D for different families of cases.

Some results...but a lot of open questions!!!

Number of zeros 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 $D(i_1, \ldots, i_m, r, s_1, \ldots, s_m)$ zeros of multiplicity at least r in $S_1 \times \cdots \times S_m$.

Research problem: Estimate the value of D for different families of cases.

Some results...but a lot of open questions!!!

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

Shamir's secret sharing scheme

Share a secret s in $\mathbb{F}_q$ among $q-1$ participants such that any group of t participants can recover the secret, but no group of size $t-1$ can.

Set $f_0 = s$ and choose $f_1, \ldots, f_{t-1} \in \mathbb{F}_q$ by random.

$$F(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_{t-1} X^{t-1}$$

Shares are $F(\alpha_2), F(\alpha_3), \ldots, F(\alpha_q)$ where $\mathbb{F}_q = \{0, \alpha_2, \alpha_3, \ldots, \alpha_q\}$

- t participants can recover due to Lagrange interpolation giving the unique answer
- $t-1$ participants cannot recover due to adding the secret (the hidden share) we get a group of size t. For this group Lagrange interpolation would give the unique answer.

Shamir's secret sharing scheme

Share a secret s in $\mathbb{F}_q$ among $q-1$ participants such that any group of t participants can recover the secret, but no group of size $t-1$ can.

Set $f_0 = s$ and choose $f_1, \ldots, f_{t-1} \in \mathbb{F}_q$ by random.

$$F(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_{t-1} X^{t-1}$$

Shares are $F(\alpha_2), F(\alpha_3), \ldots, F(\alpha_q)$ where $\mathbb{F}_q = \{0, \alpha_2, \alpha_3, \ldots, \alpha_q\}$

- t participants can recover due to Lagrange interpolation giving the unique answer
- $t-1$ participants cannot recover due to adding the secret (the hidden share) we get a group of size t. For this group Lagrange interpolation would give the unique answer.

Shamir's secret sharing – cont.

$\mathbb{F}_q = 7$ and $t = 3$. Assume $F(2) = 3$ and $F(3) = 5$ are known. We cannot predict $f_0 = F(0) = s$

$F(0)$	$F(x)$
0	$6X^2$
1	$5X^2 + 5X + 1$
2	$4X^2 + 3X + 2$
3	$3X^2 + X + 3$
4	$2X^2 + 6X + 4$
5	$X^2 + 4X + 5$
6	$2X + 6$

Ramp secret sharing schemes

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

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

$\ell = k_1 - k_2$.

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

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

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

$\ell = k_1 - k_2$.

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

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

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

$\ell = k_1 - k_2$.

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.

Leakage versus recovery

Information leakage and recovery are precisely characterized by the relative generalized Hamming weights.

For polynomial codes $C_2 \subseteq C_1$, the rth generalized Hamming weight equals:

n minus maximal number of common roots among r polynomials which are used in the construction of C_1, but NOT in the construction of C_2

...the same parameters by the way can be used to characterize the error-correcting capability of codes for asymmetric quantum channels...

Leakage versus recovery

Information leakage and recovery are precisely characterized by the relative generalized Hamming weights.

For polynomial codes $C_2 \subseteq C_1$, the rth generalized Hamming weight equals:

n minus maximal number of common roots among r polynomials which are used in the construction of C_1, but NOT in the construction of C_2

...the same parameters by the way can be used to characterize the error-correcting capability of codes for asymmetric quantum channels...

Leakage versus recovery

Information leakage and recovery are precisely characterized by the relative generalized Hamming weights.

For polynomial codes $C_2 \subseteq C_1$, the rth generalized Hamming weight equals:

n minus maximal number of common roots among r polynomials which are used in the construction of C_1, but NOT in the construction of C_2

...the same parameters by the way can be used to characterize the error-correcting capability of codes for asymmetric quantum channels...