Computation with Gröbner bases over finite fields

Elisa Gorla

Université de Neuchâtel, Switzerland

First European training school in Network Coding
Universitat Autonoma de Barcelona, February 6, 2013

Outline

When does a system have solutions?

Question

Given $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$, when does the following system have solutions in $\mathbb{F}^n$?

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

When does a system have solutions?

Question

Given $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$, when does the following system have solutions in $\mathbb{F}^n$?

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

- If $f_1, \ldots, f_s$ have degree 1, we can decide if there are solutions and solve the system by Gaussian elimination.

When does a system have solutions?

Question

Given $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$, when does the following system have solutions in $\mathbb{F}^n$?

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

- If $f_1, \ldots, f_s$ have degree 1, we can decide if there are solutions and solve the system by Gaussian elimination.
- If $n = 1$, compute $f = \gcd(f_1, \ldots, f_s)$. The solutions of the system are exactly the solutions of $f = 0$. They are at most $\deg f$.

Polynomial ideals and solutions over the algebraic closure

Write $\mathcal{Z}_{\mathbb{F}}(f_1, \ldots, f_s)$ for the set of solutions of $f_1 = \ldots = f_s = 0$.

Example

$f = x^2 + 1$ has $\mathcal{Z}_{\mathbb{R}}(f) = \emptyset$ but $\mathcal{Z}_{\mathbb{C}}(f) = \{\pm i\}$.

It is often easier to describe the set of solutions in $\overline{\mathbb{F}}^n$, where $\overline{\mathbb{F}}$ is the algebraic closure of $\overline{\mathbb{F}}$.

Polynomial ideals and solutions over the algebraic closure

Write $\mathcal{Z}_{\mathbb{F}}(f_1, \ldots, f_s)$ for the set of solutions of $f_1 = \ldots = f_s = 0$.

Example

$f = x^2 + 1$ has $\mathcal{Z}_{\mathbb{R}}(f) = \emptyset$ but $\mathcal{Z}_{\mathbb{C}}(f) = \{\pm i\}$.

It is often easier to describe the set of solutions in $\overline{\mathbb{F}}^n$, where $\overline{\mathbb{F}}$ is the algebraic closure of $\overline{\mathbb{F}}$.

Solving the system $f_1 = \ldots = f_s = 0$ is the same as computing the set of zeros of the ideal $I = (f_1, \ldots, f_s) = \{\sum_{i=1}^{s} g_i f_i \mid g_i \in \mathbb{F}[x_1, \ldots, x_n]\}$:

$$\mathcal{Z}(f_1, \ldots, f_s) = \mathcal{Z}(I).$$

Polynomial ideals and solutions over the algebraic closure

Write $\mathcal{Z}_{\mathbb{F}}(f_1, \ldots, f_s)$ for the set of solutions of $f_1 = \ldots = f_s = 0$.

Example

$f = x^2 + 1$ has $\mathcal{Z}_{\mathbb{R}}(f) = \emptyset$ but $\mathcal{Z}_{\mathbb{C}}(f) = \{\pm i\}$.

It is often easier to describe the set of solutions in $\overline{\mathbb{F}}^n$, where $\overline{\mathbb{F}}$ is the algebraic closure of $\overline{\mathbb{F}}$.

Solving the system $f_1 = \ldots = f_s = 0$ is the same as computing the set of zeros of the ideal $I = (f_1, \ldots, f_s) = \{\sum_{i=1}^{s} g_i f_i \mid g_i \in \mathbb{F}[x_1, \ldots, x_n]\}$:

$$\mathcal{Z}(f_1, \ldots, f_s) = \mathcal{Z}(I).$$

Theorem (Hilbert's Nullstellensatz)

$I = (f_1, \ldots, f_s) \subseteq \mathbb{F}[x_1, \ldots, x_n]$. $\mathcal{Z}_{\overline{\mathbb{F}}}(f_1, \ldots, f_s) = \emptyset$ *iff* $I = (1)$.

When does a system have finitely many solutions?

Let $\mathcal{S}$ denote the system $f_1 = \ldots = f_s = 0$ and $I = (f_1, \ldots, f_s) \subset \mathbb{F}[x_1, \ldots, x_n] = P$.

Theorem (Finiteness Criterion)

The following are equivalent:

1. *$\mathcal{S}$ has finitely many solutions in $\overline{\mathbb{F}}^n$.*
2. *The set of solutions $\mathcal{Z}(I)$ is zero-dimensional, i.e., $\dim(P/I) = 0$.*
3. *For $i = 1, \ldots, n$ we have $I \cap \mathbb{F}[x_i] = (g_i) \neq (0)$.*

Remark

- 1.-3. imply that $\mathcal{S}$ has finitely many solutions over $\mathbb{F}$.
- The number of solutions of $\mathcal{S}$ is at most $\deg(g_1) \cdots \deg(g_n)$.

How many solutions does a system have?

Example

Let $f_1 = x_1^2 + x_2 + x_3 - 1$, $f_2 = x_1 + x_2^2 + x_3 - 1$, $f_3 = x_1 + x_2 + x_3^2 - 1$, $I = (f_1, f_2, f_3) \subseteq P = \mathbb{F}_{23}[x_1, x_2, x_3]$.

For all $i = 1, 2, 3$ we have

$$I \cap \mathbb{F}_{23}[x_i] = 6x_i^6 - x_i^4 + x_i^3 - 6x_i^2 =: g(x_i).$$

$g(x) = 0$ has solutions $x = 0, 1, 4, 17$.

By substituting into the original system, we see that of the 64 possible combinations, only the following 5 are solutions:

$$(1, 0, 0), (0, 1, 0), (0, 0, 1), (4, 4, 4), (17, 17, 17).$$

Exact number of solutions

If a polynomial f vanishes on a point then also sqfree(f) vanishes on that point. Hence $\mathcal{Z}(I)$ stays the same if we add the the squarefree parts of some polynomials in I.

Definition

$\mathbb{F}$ a finite field. The radical of I is $\sqrt{I} = I + (\text{sqfree}(g_1), \ldots, \text{sqfree}(g_n))$.

Exact number of solutions

If a polynomial f vanishes on a point then also sqfree(f) vanishes on that point. Hence $\mathcal{Z}(I)$ stays the same if we add the the squarefree parts of some polynomials in I.

Definition

$\mathbb{F}$ a finite field. The radical of I is $\sqrt{I} = I + (\text{sqfree}(g_1), \ldots, \text{sqfree}(g_n))$.

Example

Let $f_1 = x_1^2 + x_2 + x_3 - 1$, $f_2 = x_1 + x_2^2 + x_3 - 1$, $f_3 = x_1 + x_2 + x_3^2 - 1$, $I = (f_1, f_2, f_3) \subseteq P = \mathbb{F}_{23}[x_1, x_2, x_3]$. Since $g_i = 6x_i^2(x_i - 1)^2(x_i - 4)(x_i + 6)$ for all i, $\text{sqfree}(g_i) = x_i(x_i - 1)(x_i - 4)(x_i + 6)$ and $\sqrt{I} = (f_1, g_1, g_2, g_3)$.

Exact number of solutions

If a polynomial f vanishes on a point then also sqfree(f) vanishes on that point. Hence $\mathcal{Z}(I)$ stays the same if we add the the squarefree parts of some polynomials in I.

Definition

$\mathbb{F}$ a finite field. The radical of I is $\sqrt{I} = I + (\text{sqfree}(g_1), \ldots, \text{sqfree}(g_n))$.

Example

Let $f_1 = x_1^2 + x_2 + x_3 - 1$, $f_2 = x_1 + x_2^2 + x_3 - 1$, $f_3 = x_1 + x_2 + x_3^2 - 1$, $I = (f_1, f_2, f_3) \subseteq P = \mathbb{F}_{23}[x_1, x_2, x_3]$. Since $g_i = 6x_i^2(x_i - 1)^2(x_i - 4)(x_i + 6)$ for all i, $\text{sqfree}(g_i) = x_i(x_i - 1)(x_i - 4)(x_i + 6)$ and $\sqrt{I} = (f_1, g_1, g_2, g_3)$.

Theorem (Exact number of solutions)

Let $\mathbb{F}$ a finite field, let I be a zero-dimensional ideal. The number of solutions $\mathcal{Z}_{\overline{\mathbb{F}}}(I)$ is equal to $\dim_{\mathbb{F}}(P/\sqrt{I})$.

Normal position

The Lex method extends the Gaussian elimination method.

In order to solve a system $f_1 = \ldots = f_s = 0$, we compute

$$(g_i) = I \cap \mathbb{F}[x_i]$$

for $i = 1, \ldots, n$, then

$$\sqrt{I} = I + (\text{sqfree}(g_1), \ldots, \text{sqfree}(g_n)).$$

Definition

$\sqrt{I}$ is in normal x_n-position if any two zeroes $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n) \in \mathcal{Z}(\sqrt{I})$ have $a_n \neq b_n$.

If $\mathbb{F}$ has enough elements, a linear transformation can be found which puts $\sqrt{I}$ in normal x_n-position.

Solutions of the polynomial system

Theorem (The Shape Lemma)

Let $\mathbb{F}$ be a finite field, let $\sqrt{I}$ be a zero-dimensional ideal in normal x_n-position, let $h_n = \mathrm{sqfree}(g_n) \in \mathbb{F}[x_n]$ be monic, $(h_n) = \sqrt{I} \cap \mathbb{F}[x_n]$, let $d = \deg(h_n)$.

1. *The reduced Lex Gröbner basis of the ideal $\sqrt{I}$ is of the form*

$$\{x_1 - h_1, \ldots, x_{n-1} - h_{n-1}, h_n\},$$

   where $h_1, \ldots, h_{n-1} \in \mathbb{F}[x_n]$.

2. *h_n has d distinct zeros $\alpha_1, \ldots, \alpha_d \in \overline{\mathbb{F}}$, and the set of zeros of I is $\mathcal{Z}(I) = \{(h_1(\alpha_i), \ldots, h_{n-1}(\alpha_i), \alpha_i) \mid i = 1, \ldots, d\}$.*

Gröbner bases

Choose an ordering on the set of monomials of $\mathbb{F}[x_1, \ldots, x_n]$, e.g., the Lex order is given by

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n} \Leftrightarrow (a_1 - b_1, \ldots, a_n - b_n) >_{Lex} (0, \ldots, 0).$$

Definition

The set $G = \{k_1, \ldots, k_t\}$ is a Gröbner basis of $I = (f_1, \ldots, f_s)$ if division of any polynomial $f \in I$ by G gives remainder 0.

Gröbner bases

Choose an ordering on the set of monomials of $\mathbb{F}[x_1, \ldots, x_n]$, e.g., the Lex order is given by

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n} \Leftrightarrow (a_1 - b_1, \ldots, a_n - b_n) >_{Lex} (0, \ldots, 0).$$

Definition

The set $G = \{k_1, \ldots, k_t\}$ is a Gröbner basis of $I = (f_1, \ldots, f_s)$ if division of any polynomial $f \in I$ by G gives remainder 0.

Example

$P = \mathbb{Z}_3[x_1, x_2]$, $f_1 = x_1 x_2^2 - x_2^3$, $f_2 = x_1^2 + x_2^2$,
$I = (f_1, f_2) \ni f = x_2^2 f_2 - (x_1 + x_2) f_1 = 2x_2^4$.

Gröbner bases

Choose an ordering on the set of monomials of $\mathbb{F}[x_1, \ldots, x_n]$, e.g., the Lex order is given by

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n} \Leftrightarrow (a_1 - b_1, \ldots, a_n - b_n) >_{Lex} (0, \ldots, 0).$$

Definition

The set $G = \{k_1, \ldots, k_t\}$ is a Gröbner basis of $I = (f_1, \ldots, f_s)$ if division of any polynomial $f \in I$ by G gives remainder 0.

Example

$P = \mathbb{Z}_3[x_1, x_2]$, $f_1 = x_1 x_2^2 - x_2^3$, $f_2 = x_1^2 + x_2^2$,
$I = (f_1, f_2) \ni f = x_2^2 f_2 - (x_1 + x_2) f_1 = 2x_2^4$.

$\{f_1, f_2\}$ is not a Gröbner basis, since f is not divisible by f_1 nor f_2.

Gröbner bases

Choose an ordering on the set of monomials of $\mathbb{F}[x_1, \ldots, x_n]$, e.g., the Lex order is given by

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n} \Leftrightarrow (a_1 - b_1, \ldots, a_n - b_n) >_{Lex} (0, \ldots, 0).$$

Definition

The set $G = \{k_1, \ldots, k_t\}$ is a Gröbner basis of $I = (f_1, \ldots, f_s)$ if division of any polynomial $f \in I$ by G gives remainder 0.

Example

$P = \mathbb{Z}_3[x_1, x_2]$, $f_1 = x_1 x_2^2 - x_2^3$, $f_2 = x_1^2 + x_2^2$,
$I = (f_1, f_2) \ni f = x_2^2 f_2 - (x_1 + x_2) f_1 = 2x_2^4$.

$\{f_1, f_2\}$ is not a Gröbner basis, since f is not divisible by f_1 nor f_2.

Gröbner bases can be computed via Buchberger's algorithm.