Gröbner Basis Structure and the GWW Algorithm

Nate Black

Clemson University

MthSc 985 Symbolic Computation Project

December 11, 2009

Part I: Gröbner Basis Structure

Gröbner Basis Structure of Finite Sets of Points

Definitions

- def. Let $\mathbf{I}$ be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$, then the variety associated with $\mathbf{I}$ is the set of common zeros for the polynomials in $\mathbf{I}$.

$$V(\mathbf{I}) = \left\{ P \in \overline{\mathbb{F}}^n : f(P) = 0, \forall f \in \mathbf{I} \right\}$$

- def. An ideal $\mathbf{I}$ is a zero-dimensional ideal if the associated variety $V(\mathbf{I})$ is a finite set.
- def. The radical of an ideal $\mathbf{I} \subseteq R$ is the set

$$Rad(\mathbf{I}) = \{ r \in R : r^n \in \mathbf{I} \text{ for some positive integer } n \}$$

Definitions

- def. Let $\mathbf{I}$ be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$, then the variety associated with $\mathbf{I}$ is the set of common zeros for the polynomials in $\mathbf{I}$.

$$V(\mathbf{I}) = \left\{ P \in \overline{\mathbb{F}}^n : f(P) = 0, \forall f \in \mathbf{I} \right\}$$

- def. An ideal $\mathbf{I}$ is a zero-dimensional ideal if the associated variety $V(\mathbf{I})$ is a finite set.
- def. The radical of an ideal $\mathbf{I} \subseteq R$ is the set

$$Rad(\mathbf{I}) = \{ r \in R : r^n \in \mathbf{I} \text{ for some positive integer } n \}$$

Definitions

- def. Let $\mathbf{I}$ be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$, then the variety associated with $\mathbf{I}$ is the set of common zeros for the polynomials in $\mathbf{I}$.

$$V(\mathbf{I}) = \left\{ P \in \overline{\mathbb{F}}^n : f(P) = 0, \forall f \in \mathbf{I} \right\}$$

- def. An ideal $\mathbf{I}$ is a zero-dimensional ideal if the associated variety $V(\mathbf{I})$ is a finite set.
- def. The radical of an ideal $\mathbf{I} \subseteq R$ is the set

$$Rad(\mathbf{I}) = \{r \in R : r^n \in \mathbf{I} \text{ for some positive integer } n\}$$

Definitions

Big Idea: If the Gröbner Basis for an ideal $\mathbf{I}$ has some "nice" structure to it, then we can uncover information about $V(\mathbf{I})$ and vice versa. The structure that we seek is the ability to project down a dimension on one of the coordinates.

- Let $\mathcal{P}$ be the set of common zeros of $\mathbf{I}$. (i.e. $\mathcal{P} = V(\mathbf{I})$)
- Let $\pi : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^{n-1}$ be the projection map such that

$$\pi(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1})$$

- Let $\mathcal{S} = \pi(\mathcal{P})$ denote the projection of $\mathcal{P}$.
- def. The fibre of π in $\mathcal{P}$ at a point $s \in \mathcal{S}$ is $\pi^{-1}(s)$, the set of points in $\mathcal{P}$ that project to s. This set is called the fibre of s.
- def. The size of a fibre is its cardinality, and the fibre size of s is the size of its fibre.

Definitions

Big Idea: If the Gröbner Basis for an ideal $\mathbf{I}$ has some "nice" structure to it, then we can uncover information about $V(\mathbf{I})$ and vice versa. The structure that we seek is the ability to project down a dimension on one of the coordinates.

- Let $\mathcal{P}$ be the set of common zeros of $\mathbf{I}$. (i.e. $\mathcal{P} = V(\mathbf{I})$)
- Let $\pi : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^{n-1}$ be the projection map such that

$$\pi(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1})$$

- Let $\mathcal{S} = \pi(\mathcal{P})$ denote the projection of $\mathcal{P}$.
- def. The fibre of π in $\mathcal{P}$ at a point $s \in \mathcal{S}$ is $\pi^{-1}(s)$, the set of points in $\mathcal{P}$ that project to s. This set is called the fibre of s.
- def. The size of a fibre is its cardinality, and the fibre size of s is the size of its fibre.

Definitions

Big Idea: If the Gröbner Basis for an ideal $\mathbf{I}$ has some "nice" structure to it, then we can uncover information about $V(\mathbf{I})$ and vice versa. The structure that we seek is the ability to project down a dimension on one of the coordinates.

- Let $\mathcal{P}$ be the set of common zeros of $\mathbf{I}$. (i.e. $\mathcal{P} = V(\mathbf{I})$)
- Let $\pi : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^{n-1}$ be the projection map such that

$$\pi(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1})$$

- Let $\mathcal{S} = \pi(\mathcal{P})$ denote the projection of $\mathcal{P}$.
- def. The fibre of π in $\mathcal{P}$ at a point $s \in \mathcal{S}$ is $\pi^{-1}(s)$, the set of points in $\mathcal{P}$ that project to s. This set is called the fibre of s.
- def. The size of a fibre is its cardinality, and the fibre size of s is the size of its fibre.

Definitions

Big Idea: If the Gröbner Basis for an ideal $\mathbf{I}$ has some "nice" structure to it, then we can uncover information about $V(\mathbf{I})$ and vice versa. The structure that we seek is the ability to project down a dimension on one of the coordinates.

- Let $\mathcal{P}$ be the set of common zeros of $\mathbf{I}$. (i.e. $\mathcal{P} = V(\mathbf{I})$)
- Let $\pi : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^{n-1}$ be the projection map such that

$$\pi(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1})$$

- Let $\mathcal{S} = \pi(\mathcal{P})$ denote the projection of $\mathcal{P}$.
- def. The fibre of π in $\mathcal{P}$ at a point $s \in \mathcal{S}$ is $\pi^{-1}(s)$, the set of points in $\mathcal{P}$ that project to s. This set is called the fibre of s.
- def. The size of a fibre is its cardinality, and the fibre size of s is the size of its fibre.

Definitions

Big Idea: If the Gröbner Basis for an ideal $\mathbf{I}$ has some "nice" structure to it, then we can uncover information about $V(\mathbf{I})$ and vice versa. The structure that we seek is the ability to project down a dimension on one of the coordinates.

- Let $\mathcal{P}$ be the set of common zeros of $\mathbf{I}$. (i.e. $\mathcal{P} = V(\mathbf{I})$)
- Let $\pi : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^{n-1}$ be the projection map such that

$$\pi(a_1, \dots, a_{n-1}, a_n) = (a_1, \dots, a_{n-1})$$

- Let $\mathcal{S} = \pi(\mathcal{P})$ denote the projection of $\mathcal{P}$.
- def. The fibre of π in $\mathcal{P}$ at a point $s \in \mathcal{S}$ is $\pi^{-1}(s)$, the set of points in $\mathcal{P}$ that project to s. This set is called the fibre of s.
- def. The size of a fibre is its cardinality, and the fibre size of s is the size of its fibre.

Definitions

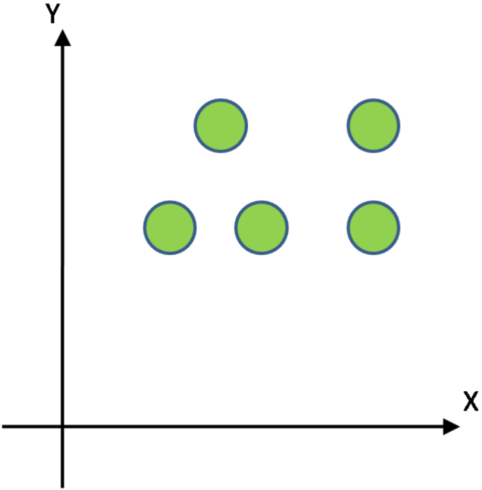
Big Idea: If the Gröbner Basis for an ideal $\mathbf{I}$ has some "nice" structure to it, then we can uncover information about $V(\mathbf{I})$ and vice versa. The structure that we seek is the ability to project down a dimension on one of the coordinates.

- Let $\mathcal{P}$ be the set of common zeros of $\mathbf{I}$. (i.e. $\mathcal{P} = V(\mathbf{I})$)
- Let $\pi : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^{n-1}$ be the projection map such that

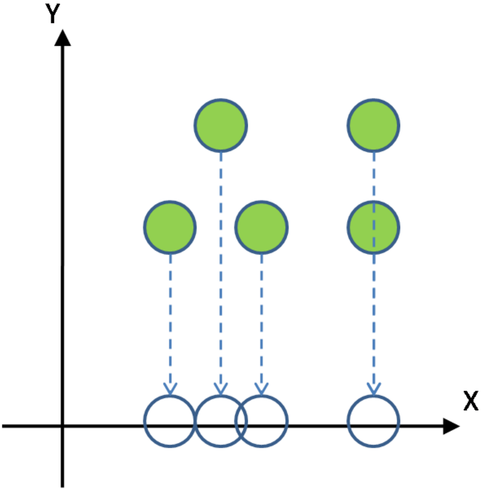
$$\pi(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1})$$

- Let $\mathcal{S} = \pi(\mathcal{P})$ denote the projection of $\mathcal{P}$.
- def. The fibre of π in $\mathcal{P}$ at a point $s \in \mathcal{S}$ is $\pi^{-1}(s)$, the set of points in $\mathcal{P}$ that project to s. This set is called the fibre of s.
- def. The size of a fibre is its cardinality, and the fibre size of s is the size of its fibre.

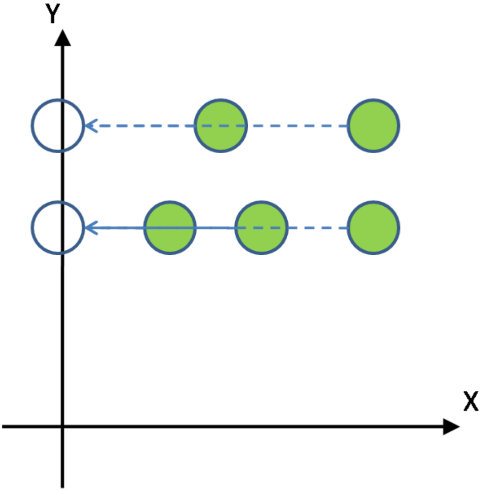
Pictures



Pictures



Pictures



How does the special structure help?

- Does a Gröbner Basis for **I** tell the sizes of the fibres in $\mathcal{P}$?
- If I know a Gröbner Basis for **I**, can I easily find a Gröbner Basis for subsets of $\mathcal{S}$ that are projections of different fibre sizes?

How does the special structure help?

- Does a Gröbner Basis for $\mathbf{I}$ tell the sizes of the fibres in $\mathcal{P}$?
- If I know a Gröbner Basis for $\mathbf{I}$, can I easily find a Gröbner Basis for subsets of $\mathcal{S}$ that are projections of different fibre sizes?

Main Theorem

Let $\mathbb{F}$ be a perfect field, $\mathbf{I}$ be a zero-dimensional radical ideal in $\mathbb{F}[x_1, \ldots, x_n]$, and $\mathcal{P}$ be the set of zeros of $\mathbf{I}$ in $\overline{\mathbb{F}}^n$. Assume the fibre sizes in $\mathcal{P}$ are $m_1 > \ldots > m_r > 0$. Let G be any minimal Gröbner Basis for $\mathbf{I}$ under an elimination order for x_n. View the elements of G as polynomials in x_n with coefficients in $\mathbb{F}[x_1, \ldots, x_{n-1}]$. Then the following statements will hold:

- The x_n-degrees of the polynomials in G are exactly the fibre sizes in $\mathcal{P}$.
- For $1 \leq i \leq r$ let G_i denote the set of leading coefficients of the polynomials in G whose x_n-degrees are $< m_i$. Also, let $\mathcal{S}_{\leq i}$ denote the set of points in $\mathcal{S} = \pi(\mathcal{P})$ that are projections of fibres of size $\geq m_i$. Then each G_i is a Gröbner Basis for $\mathcal{S}_{\leq i}$.

Main Theorem

Let $\mathbb{F}$ be a perfect field, $\mathbf{I}$ be a zero-dimensional radical ideal in $\mathbb{F}[x_1, \ldots, x_n]$, and $\mathcal{P}$ be the set of zeros of $\mathbf{I}$ in $\overline{\mathbb{F}}^n$. Assume the fibre sizes in $\mathcal{P}$ are $m_1 > \ldots > m_r > 0$. Let G be any minimal Gröbner Basis for $\mathbf{I}$ under an elimination order for x_n. View the elements of G as polynomials in x_n with coefficients in $\mathbb{F}[x_1, \ldots, x_{n-1}]$. Then the following statements will hold:

- The x_n-degrees of the polynomials in G are exactly the fibre sizes in $\mathcal{P}$.
- For $1 \leq i \leq r$ let G_i denote the set of leading coefficients of the polynomials in G whose x_n-degrees are $< m_i$. Also, let $\mathcal{S}_{\leq i}$ denote the set of points in $\mathcal{S} = \pi(\mathcal{P})$ that are projections of fibres of size $\geq m_i$. Then each G_i is a Gröbner Basis for $\mathcal{S}_{\leq i}$.

Main Theorem

Let $\mathbb{F}$ be a perfect field, $\mathbf{I}$ be a zero-dimensional radical ideal in $\mathbb{F}[x_1, \ldots, x_n]$, and $\mathcal{P}$ be the set of zeros of $\mathbf{I}$ in $\overline{\mathbb{F}}^n$. Assume the fibre sizes in $\mathcal{P}$ are $m_1 > \ldots > m_r > 0$. Let G be any minimal Gröbner Basis for $\mathbf{I}$ under an elimination order for x_n. View the elements of G as polynomials in x_n with coefficients in $\mathbb{F}[x_1, \ldots, x_{n-1}]$. Then the following statements will hold:

- The x_n-degrees of the polynomials in G are exactly the fibre sizes in $\mathcal{P}$.
- For $1 \leq i \leq r$ let G_i denote the set of leading coefficients of the polynomials in G whose x_n-degrees are $< m_i$. Also, let $\mathcal{S}_{\leq i}$ denote the set of points in $\mathcal{S} = \pi(\mathcal{P})$ that are projections of fibres of size $\geq m_i$. Then each G_i is a Gröbner Basis for $\mathcal{S}_{\leq i}$.

Example

- Let $G = \{z^2 - z, zy - z, x, y^2 - y\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

Example

- Let $G = \{z^2 - z, zy - z, x, y^2 - y\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

Example

- Let $G = \{z^2 - z, zy - z, x, y^2 - y\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

Example

- Let $G = \{z^2 - z, zy - z, x, y^2 - y\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

Example

- Let $G = \{z^2 - z, zy - z, x, y^2 - y\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

Example

- Let $G = \{z^2 - z, zy - z, x, y^2 - y\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

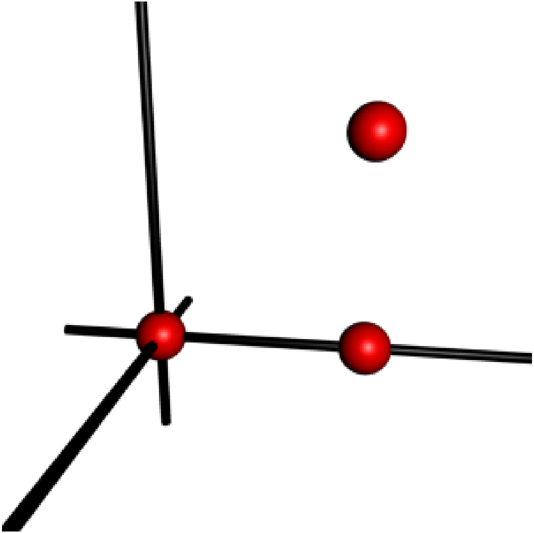
Example

- Let $G = \{z^2 - z, zy - z, x, y^2 - y\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

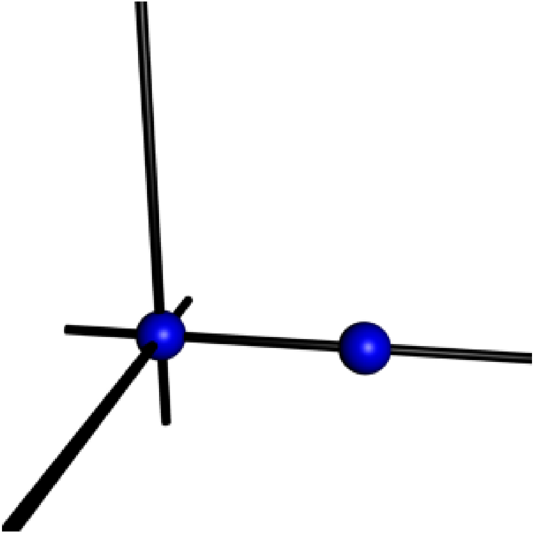
Example

- Let $G = \left\{z^2 - z, zy - z, x, y^2 - y\right\}$ be a Gröbner Basis
- Note that the z-degrees of each polynomial are $2, 1, 0, 0$ respectively
- Thus if we project on the z-coordinate, the fibre sizes will be $2 > 1 > 0$
- Looking at the first element in G we see that $z^2 - z = 0$ has only two solutions: $z = 0, 1$
- First, let $z = 0$ and project on the z-coordinate $G_1 = \{x, y^2 - y\}$
- Second, let $z = 1$ and project on the z-coordinate $G_2 = \{y - 1, x, y^2 - y\}$
- In either case $x = 0$, then for G_1, $y^2 - y = 0$ has two solutions: $y = 0, 1$, while for G_2, $y - 1 = 0$ forces $y = 1$.
- We now have 3 solutions: $\{(0, 0, 0), (0, 1, 0), (0, 1, 1)\}$

Pictures



Pictures



Part II: The GWW Algorithm

Primary Decomposition of Zero-Dimensional Ideals
Over Finite Fields

Definitions

- def. An ideal $\mathbf{I} \subseteq R$ is called primary if whenever $xy \in \mathbf{I}$ then either x or y^n is in $\mathbf{I}$ for some positive integer n.
- def. The nth-Frobenius map sends every element x to x^n. For finite fields of order q the qth-Frobenius map fixes every element in the field.
- def. A primary decomposition of an ideal, $\mathbf{I}$, is a set of ideals, $\{Q_i\}$, such that each Q_i is primary and

  $$\mathbf{I} = Q_1 \cap Q_2 \cap \ldots \cap Q_r$$

  In general this decomposition is not unique, but the number of elements, r, is.

Definitions

- def. An ideal $\mathbf{I} \subseteq R$ is called primary if whenever $xy \in \mathbf{I}$ then either x or y^n is in $\mathbf{I}$ for some positive integer n.
- def. The nth-Frobenius map sends every element x to x^n. For finite fields of order q the qth-Frobenius map fixes every element in the field.
- def. A primary decomposition of an ideal, $\mathbf{I}$, is a set of ideals, $\{Q_i\}$, such that each Q_i is primary and

$$\mathbf{I} = Q_1 \cap Q_2 \cap \ldots \cap Q_r$$

In general this decomposition is not unique, but the number of elements, r, is.

Definitions

- def. An ideal $\mathbf{I} \subseteq R$ is called primary if whenever $xy \in \mathbf{I}$ then either x or y^n is in $\mathbf{I}$ for some positive integer n.
- def. The nth-Frobenius map sends every element x to x^n. For finite fields of order q the qth-Frobenius map fixes every element in the field.
- def. A primary decomposition of an ideal, $\mathbf{I}$, is a set of ideals, $\{Q_i\}$, such that each Q_i is primary and

$$\mathbf{I} = Q_1 \cap Q_2 \cap \ldots \cap Q_r$$

  In general this decomposition is not unique, but the number of elements, r, is.

Outline

- Let $\mathbf{I} \subseteq k[x_1, x_2, \ldots, x_n]$ be the ideal under consideration with k containing $\mathbb{F}_q$ as a subfield.
- Let $R = k[x_1, x_2, \ldots, x_n]/\mathbf{I}$ and $G = \{g \in R : g \equiv g^q (mod \mathbf{I})\}$.
- Then G is an $\mathbb{F}_q$ linear subspace of R. (By the theorem proved in the paper, the dimension will actually be r, where r is the number of ideals in the primary decomposition.)
- Let B be any linear basis for G over $\mathbb{F}_q$.
- Let C be the matrix that represents the qth-Frobenius map acting on B. Then $B^q = B \cdot C$.
- If we represent $g \in R$ as $B(a_1, \ldots, a_d)^T$, then $g^q \equiv g(mod \mathbf{I})$ iff

$$(C - I)(a_1, \ldots, a_d)^T = 0$$

Outline

- Let $\mathbf{I} \subseteq k[x_1, x_2, \ldots, x_n]$ be the ideal under consideration with k containing $\mathbb{F}_q$ as a subfield.
- Let $R = k[x_1, x_2, \ldots, x_n]/\mathbf{I}$ and $G = \{g \in R : g \equiv g^q (mod \mathbf{I})\}$.
- Then G is an $\mathbb{F}_q$ linear subspace of R. (By the theorem proved in the paper, the dimension will actually be r, where r is the number of ideals in the primary decomposition.)
- Let B be any linear basis for G over $\mathbb{F}_q$.
- Let C be the matrix that represents the qth-Frobenius map acting on B. Then $B^q = B \cdot C$.
- If we represent $g \in R$ as $B(a_1, \ldots, a_d)^T$, then $g^q \equiv g (mod \mathbf{I})$ iff

$$(C - I)(a_1, \ldots, a_d)^T = 0$$

Outline

- Let $\mathbf{I} \subseteq k[x_1, x_2, \ldots, x_n]$ be the ideal under consideration with k containing $\mathbb{F}_q$ as a subfield.
- Let $R = k[x_1, x_2, \ldots, x_n]/\mathbf{I}$ and $G = \{g \in R : g \equiv g^q (mod \mathbf{I})\}$.
- Then G is an $\mathbb{F}_q$ linear subspace of R. (By the theorem proved in the paper, the dimension will actually be r, where r is the number of ideals in the primary decomposition.)
- Let B be any linear basis for G over $\mathbb{F}_q$.
- Let C be the matrix that represents the qth-Frobenius map acting on B. Then $B^q = B \cdot C$.
- If we represent $g \in R$ as $B(a_1, \ldots, a_d)^T$, then $g^q \equiv g(mod \mathbf{I})$ iff

$$(C - I)(a_1, \ldots, a_d)^T = 0$$

Outline

- Let $\mathbf{I} \subseteq k[x_1, x_2, \ldots, x_n]$ be the ideal under consideration with k containing $\mathbb{F}_q$ as a subfield.
- Let $R = k[x_1, x_2, \ldots, x_n]/\mathbf{I}$ and $G = \{g \in R : g \equiv g^q (mod \mathbf{I})\}$.
- Then G is an $\mathbb{F}_q$ linear subspace of R. (By the theorem proved in the paper, the dimension will actually be r, where r is the number of ideals in the primary decomposition.)
- Let B be any linear basis for G over $\mathbb{F}_q$.
- Let C be the matrix that represents the qth-Frobenius map acting on B. Then $B^q = B \cdot C$.
- If we represent $g \in R$ as $B(a_1, \ldots, a_d)^T$, then $g^q \equiv g(mod \mathbf{I})$ iff

$$(C - I)(a_1, \ldots, a_d)^T = 0$$

Outline

- Let $\mathbf{I} \subseteq k[x_1, x_2, \ldots, x_n]$ be the ideal under consideration with k containing $\mathbb{F}_q$ as a subfield.
- Let $R = k[x_1, x_2, \ldots, x_n]/\mathbf{I}$ and $G = \{g \in R : g \equiv g^q (mod \mathbf{I})\}$.
- Then G is an $\mathbb{F}_q$ linear subspace of R. (By the theorem proved in the paper, the dimension will actually be r, where r is the number of ideals in the primary decomposition.)
- Let B be any linear basis for G over $\mathbb{F}_q$.
- Let C be the matrix that represents the qth-Frobenius map acting on B. Then $B^q = B \cdot C$.
- If we represent $g \in R$ as $B(a_1, \ldots, a_d)^T$, then $g^q \equiv g(mod \mathbf{I})$ iff

$$(C - I)(a_1, \ldots, a_d)^T = 0$$

Outline

- Let $\mathbf{I} \subseteq k[x_1, x_2, \ldots, x_n]$ be the ideal under consideration with k containing $\mathbb{F}_q$ as a subfield.
- Let $R = k[x_1, x_2, \ldots, x_n]/\mathbf{I}$ and $G = \{g \in R : g \equiv g^q (mod \mathbf{I})\}$.
- Then G is an $\mathbb{F}_q$ linear subspace of R. (By the theorem proved in the paper, the dimension will actually be r, where r is the number of ideals in the primary decomposition.)
- Let B be any linear basis for G over $\mathbb{F}_q$.
- Let C be the matrix that represents the qth-Frobenius map acting on B. Then $B^q = B \cdot C$.
- If we represent $g \in R$ as $B(a_1, \ldots, a_d)^T$, then $g^q \equiv g(mod \mathbf{I})$ iff

$$(C - I)(a_1, \ldots, a_d)^T = 0$$

Example

- Let $\mathbf{I} = \langle y^2 - xz, z^2 - x^2y, x + y + z - 1\rangle \subset \mathbb{F}_5[x, y, z]$
- Using lex order with $x > y > z$, $\mathbf{I}$ has a Gröbner Basis $G = [x + y + z - 1, y^2 + 3y - 2z^4 + z^3 + 2z^2 + z, yz + 2y + 2z^4 - z^3 - z^2 - 2z, z^5 - z^4 + 3z^3 - z^2 + 2z]$
- $R = \mathbb{F}_5[x, y, z]/\mathbf{I}$ has a basis: $B = (z^4, z^3, z^2, z, y, 1)$

Example

- Let $\mathbf{I} = \langle y^2 - xz, z^2 - x^2y, x + y + z - 1 \rangle \subset \mathbb{F}_5[x, y, z]$
- Using lex order with $x > y > z$, $\mathbf{I}$ has a Gröbner Basis $G = [x + y + z - 1, y^2 + 3y - 2z^4 + z^3 + 2z^2 + z, yz + 2y + 2z^4 - z^3 - z^2 - 2z, z^5 - z^4 + 3z^3 - z^2 + 2z]$
- $R = \mathbb{F}_5[x, y, z]/\mathbf{I}$ has a basis: $B = \left(z^4, z^3, z^2, z, y, 1\right)$

Example

- Let $\mathbf{I} = \langle y^2 - xz, z^2 - x^2y, x + y + z - 1\rangle \subset \mathbb{F}_5[x, y, z]$
- Using lex order with $x > y > z$, $\mathbf{I}$ has a Gröbner Basis $G = [x + y + z - 1, y^2 + 3y - 2z^4 + z^3 + 2z^2 + z, yz + 2y + 2z^4 - z^3 - z^2 - 2z, z^5 - z^4 + 3z^3 - z^2 + 2z]$
- $R = \mathbb{F}_5[x, y, z]/\mathbf{I}$ has a basis: $B = \left(z^4, z^3, z^2, z, y, 1\right)$

Example

- $C = \begin{bmatrix} -2 & -1 & 1 & 1 & 1 & 0 \\ -1 & -1 & 2 & 2 & 0 & 0 \\ 2 & -1 & 2 & 1 & 0 & 0 \\ -1 & -2 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$
- The solution space of $C - I$ is given by:

$$\begin{aligned} (0,0,0,0,0,1) &\leftrightarrow g_1 = 1, \\ (0,0,-1,1,0,0) &\leftrightarrow g_2 = z - z^2, \\ (0,1,1,0,0,) &\leftrightarrow g_3 = z^2 + z^3, \\ (-2,1,0,0,0,0) &\leftrightarrow g_4 = z^3 - 2z^4, \end{aligned}$$

Example

- $C = \begin{bmatrix} -2 & -1 & 1 & 1 & 1 & 0 \\ -1 & -1 & 2 & 2 & 0 & 0 \\ 2 & -1 & 2 & 1 & 0 & 0 \\ -1 & -2 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$
- The solution space of $C - I$ is given by:

$$\begin{aligned} (0,0,0,0,0,1) &\quad \leftrightarrow \quad g_1 = 1, \\ (0,0,-1,1,0,0) &\quad \leftrightarrow \quad g_2 = z - z^2, \\ (0,1,1,0,0,) &\quad \leftrightarrow \quad g_3 = z^2 + z^3, \\ (-2,1,0,0,0,0) &\quad \leftrightarrow \quad g_4 = z^3 - 2z^4, \end{aligned}$$

Example

- For g_2 construct the ideal $\mathbf{J} = \langle \mathbf{I}, w - g_2 \rangle \subseteq \mathbb{F}_q[x, y, z, w]$
- Using lex order with $x > y > z > w$, $\mathbf{J}$ has a Gröbner Basis $w^4 + w^3 + w^2 + w,\ (w-2)z + 2w^3 + w^2,\ z^2 - z + w,$ $(w+1)y + zw - z - w,\ yz - 2yw - 2z^2w - 2z^2 + 2zw + 2z,$ $y^2 + yz + z^2 - z,\ x + y + z - 1$
- Note that $h = w^4 + w^3 + w^2 + w$ has 4 roots: $w = 0, -1, -2, 2,$ and the dimension of the solution space was 4.
- Let $w = 0$ then we obtain: $G_0 = \{-2z, z^2 - z, y - z, yz + 3z^2 + 2z,$ $y^2 + yz + z^2 - z, x + y + z - 1\}$ $Q_1 = \langle G_0 \rangle = \langle -2z, y - z, x + y + z - 1 \rangle = \langle z, y, x - 1 \rangle$

Example

- For g_2 construct the ideal $\mathbf{J} = \langle \mathbf{I}, w - g_2 \rangle \subseteq \mathbb{F}_q[x, y, z, w]$
- Using lex order with $x > y > z > w$, $\mathbf{J}$ has a Gröbner Basis $w^4 + w^3 + w^2 + w,\ (w-2)z + 2w^3 + w^2,\ z^2 - z + w,$ $(w+1)y + zw - z - w,\ yz - 2yw - 2z^2w - 2z^2 + 2zw + 2z,$ $y^2 + yz + z^2 - z,\ x + y + z - 1$
- Note that $h = w^4 + w^3 + w^2 + w$ has 4 roots: $w = 0, -1, -2, 2,$ and the dimension of the solution space was 4.
- Let $w = 0$ then we obtain: $G_0 = \{-2z, z^2 - z, y - z, yz + 3z^2 + 2z,$ $y^2 + yz + z^2 - z, x + y + z - 1\}$ $Q_1 = \langle G_0 \rangle = \langle -2z, y - z, x + y + z - 1 \rangle = \langle z, y, x - 1 \rangle$

Example

- For g_2 construct the ideal $\mathbf{J} = \langle \mathbf{I}, w - g_2 \rangle \subseteq \mathbb{F}_q[x, y, z, w]$
- Using lex order with $x > y > z > w$, $\mathbf{J}$ has a Gröbner Basis $w^4 + w^3 + w^2 + w,\ (w-2)z + 2w^3 + w^2,\ z^2 - z + w,$ $(w+1)y + zw - z - w,\ yz - 2yw - 2z^2w - 2z^2 + 2zw + 2z,$ $y^2 + yz + z^2 - z,\ x + y + z - 1$
- Note that $h = w^4 + w^3 + w^2 + w$ has 4 roots: $w = 0, -1, -2, 2,$ and the dimension of the solution space was 4.
- Let $w = 0$ then we obtain: $G_0 = \{-2z, z^2 - z, y - z, yz + 3z^2 + 2z,$ $y^2 + yz + z^2 - z, x + y + z - 1\}$ $Q_1 = \langle G_0 \rangle = \langle -2z, y - z, x + y + z - 1 \rangle = \langle z, y, x - 1 \rangle$

Example

- For g_2 construct the ideal $\mathbf{J} = \langle \mathbf{I}, w - g_2 \rangle \subseteq \mathbb{F}_q[x, y, z, w]$
- Using lex order with $x > y > z > w$, $\mathbf{J}$ has a Gröbner Basis $w^4 + w^3 + w^2 + w,\ (w-2)z + 2w^3 + w^2,\ z^2 - z + w,$ $(w+1)y + zw - z - w,\ yz - 2yw - 2z^2w - 2z^2 + 2zw + 2z,$ $y^2 + yz + z^2 - z,\ x + y + z - 1$
- Note that $h = w^4 + w^3 + w^2 + w$ has 4 roots: $w = 0, -1, -2, 2,$ and the dimension of the solution space was 4.
- Let $w = 0$ then we obtain:
  $G_0 = \{-2z, z^2 - z, y - z, yz + 3z^2 + 2z,$
  $y^2 + yz + z^2 - z, x + y + z - 1\}$
  $Q_1 = \langle G_0 \rangle = \langle -2z, y - z, x + y + z - 1 \rangle = \langle z, y, x - 1 \rangle$

Example

- Similarly we obtain:
  $Q_2 = \langle z+2, y^2-2y+1, x+y+2\rangle$
  $Q_3 = \langle z-2, y-1, x+2\rangle$
  $Q_4 = \langle z^2-z+2, y+z+2z+1, x-z+3\rangle$
- Each Q_i is primary and
  $I = Q_1 \cap Q_2 \cap Q_3 \cap Q_4$
- Thus we have our primary decomposition.

Example

- Similarly we obtain:
  $Q_2 = \langle z+2, y^2-2y+1, x+y+2\rangle$
  $Q_3 = \langle z-2, y-1, x+2\rangle$
  $Q_4 = \langle z^2-z+2, y+z+2z+1, x-z+3\rangle$
- Each Q_i is primary and
  $\mathbf{I} = Q_1 \cap Q_2 \cap Q_3 \cap Q_4$
- Thus we have our primary decomposition.

Example

- Similarly we obtain:
  $Q_2 = \langle z + 2, y^2 - 2y + 1, x + y + 2\rangle$
  $Q_3 = \langle z - 2, y - 1, x + 2\rangle$
  $Q_4 = \langle z^2 - z + 2, y + z + 2z + 1, x - z + 3\rangle$
- Each Q_i is primary and
  $\mathbf{I} = Q_1 \cap Q_2 \cap Q_3 \cap Q_4$
- Thus we have our primary decomposition.

Example

Note that we used $g_2 = z - z^2$ which had a component in its basis with 4 roots. Such a g is called separable.
If we had picked another of the g functions we might not have been so lucky. In that case, some of the Q_i's will be primary and some will not. The ones that are not primary can be reduced and have this procedure applied to them again.

References

- Shuhong Gao, Daqing Wan and Mingsheng Wang, **Primary decomposition of zero-dimensional ideals over finite fields**, *Mathematics of Computation*, 78 (2009), 509–521.
- Shuhong Gao, Virginia M. Rodrigues and Jeffrey Stroomer, **Grobner basis structure of finite sets of points**, preprint, 2003.