Ideals, Varieties and Symbolic Computation

Priyank Kalla

Associate Professor
Electrical and Computer Engineering, University of Utah
kalla@ece.utah.edu
http://www.ece.utah.edu/~kalla

Lectures: Sept 25, 2017 onwards
Agenda:

- Wish to build a polynomial algebra model for hardware
- Modulo arithmetic model is versatile: can represent both *bit-level* and *word-level* constraints
- To build the algebraic/modulo arithmetic model:
  - Rings, Fields, Modulo arithmetic
  - Polynomials, Polynomial functions, Polynomial Rings
  - Ideals, Varieties, Symbolic Computing and Gröbner Bases
  - Decision procedures in verification
$R = \text{ring, Ideal } J \subseteq R,$

s.t.:

- $0 \in J$
- $\forall x, y \in J, x + y \in J$
- $\forall x \in J, z \in R, x \cdot z \in J$
Ideals in Rings

$R = \text{ring, Ideal } J \subseteq R,$

s.t.:

- $0 \in J$
- $\forall x, y \in J, x + y \in J$
- $\forall x \in J, z \in R, x \cdot z \in J$

- Examples of Ideals: $R = \mathbb{Z}, J = 2\mathbb{Z}, 3\mathbb{Z}, \ldots, n\mathbb{Z}$
- Ideals versus Subrings: $\mathbb{Z} \subset \mathbb{Q}$, but $\mathbb{Z}$ not an ideal in $\mathbb{Q}$
- $1 \in \text{Ring } R$, but $1$ need not be in ideal $J$
Polynomial Ideals

Definition

**Ideals of Polynomials:** Let $f_1, f_2, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_d]$. Let

$$J = \langle f_1, f_2, \ldots, f_s \rangle = \{ f_1 h_1 + f_2 h_2 + \cdots + f_s h_s : h_1, \ldots, h_s \in R \}$$

$J = \langle f_1, f_2, \ldots, f_s \rangle$ is an ideal generated by $f_1, \ldots, f_s$ and the polynomials are called the generators (basis) of $J$. [Note, $h_i$: arbitrary elements in $R$]
Definition

**Ideals of Polynomials:** Let \( f_1, f_2, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_d] \). Let

\[
J = \langle f_1, f_2, \ldots, f_s \rangle = \{ f_1 h_1 + f_2 h_2 + \cdots + f_s h_s : h_1, \ldots, h_s \in R \}
\]

\( J = \langle f_1, f_2, \ldots, f_s \rangle \) is an ideal generated by \( f_1, \ldots, f_s \) and the polynomials are called the generators (basis) of \( J \). [Note, \( h_i \): arbitrary elements in \( R \)]

Given the above definition, prove that \( J \) is indeed an ideal.
Definition

Ideals of Polynomials: Let $f_1, f_2, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_d]$. Let

$$J = \langle f_1, f_2, \ldots, f_s \rangle = \{f_1 h_1 + f_2 h_2 + \cdots + f_s h_s : h_1, \ldots, h_s \in R\}$$

$J = \langle f_1, f_2, \ldots, f_s \rangle$ is an ideal generated by $f_1, \ldots, f_s$ and the polynomials are called the generators (basis) of $J$. [Note, $h_i$: arbitrary elements in $R$]

Given the above definition, prove that $J$ is indeed an ideal.
Is $0 \in J$?
Polynomial Ideals

**Definition**

**Ideals of Polynomials:** Let $f_1, f_2, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_d]$. Let

$$J = \langle f_1, f_2 \ldots, f_s \rangle = \{f_1 h_1 + f_2 h_2 + \cdots + f_s h_s : h_1, \ldots, h_s \in R\}$$

$J = \langle f_1, f_2 \ldots, f_s \rangle$ is an ideal generated by $f_1, \ldots, f_s$ and the polynomials are called the generators (basis) of $J$. [Note, $h_i$: arbitrary elements in $R$]

Given the above definition, prove that $J$ is indeed an ideal.

Is $0 \in J$? Put $h_i = 0$
**Definition**

**Ideals of Polynomials:** Let $f_1, f_2, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_d]$. Let

$$J = \langle f_1, f_2, \ldots, f_s \rangle = \{ f_1 h_1 + f_2 h_2 + \cdots + f_s h_s : h_1, \ldots, h_s \in R \}$$

$J = \langle f_1, f_2, \ldots, f_s \rangle$ is an ideal generated by $f_1, \ldots, f_s$ and the polynomials are called the generators (basis) of $J$. [Note, $h_i$: arbitrary elements in $R$]

**Given the above definition**, prove that $J$ is indeed an ideal.

Is $0 \in J$?  Put $h_i = 0$

Given $f_i, f_j \in J$ is $f_i + f_j \in J$?
Definition

Ideals of Polynomials: Let $f_1, f_2, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_d]$. Let

$$J = \langle f_1, f_2 \ldots, f_s \rangle = \{ f_1 h_1 + f_2 h_2 + \cdots + f_s h_s : h_1, \ldots, h_s \in R \}$$

$J = \langle f_1, f_2 \ldots, f_s \rangle$ is an ideal generated by $f_1, \ldots, f_s$ and the polynomials are called the generators (basis) of $J$. [Note, $h_i$: arbitrary elements in $R$]

Given the above definition, prove that $J$ is indeed an ideal.

Is $0 \in J$? Put $h_i = 0$

Given $f_i, f_j \in J$ is $f_i + f_j \in J$? Put $h_i, h_j = 1$
Definition

**Ideals of Polynomials:** Let \( f_1, f_2, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_d] \). Let

\[
J = \langle f_1, f_2 \ldots, f_s \rangle = \{ f_1 h_1 + f_2 h_2 + \cdots + f_s h_s : h_1, \ldots, h_s \in R \}
\]

\( J = \langle f_1, f_2 \ldots, f_s \rangle \) is an ideal generated by \( f_1, \ldots, f_s \) and the polynomials are called the generators (basis) of \( J \). [Note, \( h_i \): arbitrary elements in \( R \)]

Given the above definition, prove that \( J \) is indeed an ideal.

Is \( 0 \in J \)? Put \( h_i = 0 \)

Given \( f_i, f_j \in J \) is \( f_i + f_j \in J \)? Put \( h_i, h_j = 1 \)

Given \( f_i \in J, h_i \in R \) is \( f_i \cdot h_i \in J \)?
Generators of Ideals

- An ideal may have many different generators
- It is possible to have:
  \[ J = \langle f_1, \ldots, f_s \rangle = \langle p_1, \ldots, p_l \rangle = \cdots = \langle g_1, \ldots, g_t \rangle \]
- Where \( f_i, p_j, g_k \in \mathbb{F}[x_1, \ldots, x_d] \) and \( J \subseteq \mathbb{F}[x_1, \ldots, x_d] \)
- Does there exist a **Canonical** representation of an ideal?
- A **Gröbner Basis** is a canonical representation of the ideal, with **many nice properties** that allow to solve many polynomial decision questions
- **Buchberger’s Algorithm** allows to compute a Gröbner Basis
  - Given \( F = \{ f_1, \ldots, f_s \} \in \mathbb{R}[x_1, \ldots, x_d] \)
An ideal may have many different generators

It is possible to have:

\[ J = \langle f_1, \ldots, f_s \rangle = \langle p_1, \ldots, p_l \rangle = \cdots = \langle g_1, \ldots, g_t \rangle \]

Where \( f_i, p_j, g_k \in \mathbb{F}[x_1, \ldots, x_d] \) and \( J \subseteq \mathbb{F}[x_1, \ldots, x_d] \)

Does there exist a canonical representation of an ideal?

A Gröbner Basis is a canonical representation of the ideal, with many nice properties that allow to solve many polynomial decision questions

Buchberger’s Algorithm allows to compute a Gröbner Basis

Given \( F = \{ f_1, \ldots, f_s \} \in \mathbb{R}[x_1, \ldots, x_d] \)

It finds \( G = \{ g_1, \ldots, g_t \} \), such that
Generators of Ideals

- An ideal may have many different generators
- It is possible to have:
  \[ J = \langle f_1, \ldots, f_s \rangle = \langle p_1, \ldots, p_l \rangle = \cdots = \langle g_1, \ldots, g_t \rangle \]
- Where \( f_i, p_j, g_k \in \mathbb{F}[x_1, \ldots, x_d] \) and \( J \subseteq \mathbb{F}[x_1, \ldots, x_d] \)
- Does there exist a Canonical representation of an ideal?

A Gröbner Basis is a canonical representation of the ideal, with many nice properties that allow to solve many polynomial decision questions

Buchberger’s Algorithm allows to compute a Gröbner Basis
- Given \( F = \{f_1, \ldots, f_s\} \in \mathbb{R}[x_1, \ldots, x_d] \)
- It finds \( G = \{g_1, \ldots, g_t\} \), such that
- \( J = \langle F \rangle = \langle G \rangle \)
Generators of Ideals

- An ideal may have many different generators
- It is possible to have:
  \[ J = \langle f_1, \ldots, f_s \rangle = \langle p_1, \ldots, p_l \rangle = \cdots = \langle g_1, \ldots, g_t \rangle \]
- Where \( f_i, p_j, g_k \in \mathbb{F}[x_1, \ldots, x_d] \) and \( J \subseteq \mathbb{F}[x_1, \ldots, x_d] \)
- Does there exist a **Canonical** representation of an ideal?
- A **Gröbner Basis** is a canonical representation of the ideal, with many nice properties that allow to solve many polynomial decision questions
- Buchberger’s Algorithm allows to compute a Gröbner Basis
  - Given \( F = \{ f_1, \ldots, f_s \} \in \mathbb{R}[x_1, \ldots, x_d] \)
  - It finds \( G = \{ g_1, \ldots, g_t \} \), such that
  - \( J = \langle F \rangle = \langle G \rangle \)
  - Why is this important? [We’ll see a little later....]
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y]$
Example of Ideal Generators

- \( I_1 = \langle f_1, f_2 \rangle \subset Q[x, y] \)
- \( f_1 = x^2 - 4; \ f_2 = y^2 - 1 \)
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset Q[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $I_2 = \langle g_1, g_2 \rangle \subset Q[x, y]$
Example of Ideal Generators

- \( I_1 = \langle f_1, f_2 \rangle \subset Q[x, y] \)
- \( f_1 = x^2 - 4; \quad f_2 = y^2 - 1 \)
- \( I_2 = \langle g_1, g_2 \rangle \subset Q[x, y] \)
- \( g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3; \)
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset Q[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $I_2 = \langle g_1, g_2 \rangle \subset Q[x, y]$
- $g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3$
- Is $g_1 \in I_1$? Is $g_2 \in I_1$?
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset Q[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $I_2 = \langle g_1, g_2 \rangle \subset Q[x, y]$
- $g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3$
- Is $g_1 \in I_1$? Is $g_2 \in I_1$?
- $g_1 = 2f_1 + 3f_2; \quad g_2 = f_1 - f_2; \quad \Rightarrow \quad g_1, g_2 \in I_1$, so $I_2 \subset I_1$. 
Example of Ideal Generators

- $l_1 = \langle f_1, f_2 \rangle \subset Q[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $l_2 = \langle g_1, g_2 \rangle \subset Q[x, y]$
- $g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3$
- Is $g_1 \in l_1$? Is $g_2 \in l_1$?
- $g_1 = 2f_1 + 3f_2; \quad g_2 = f_1 - f_2; \quad \implies \quad g_1, g_2 \in l_1,$ so $l_2 \subseteq l_1$.
- Similarly, show that $f_1, f_2 \subseteq l_2$
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset Q[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $I_2 = \langle g_1, g_2 \rangle \subset Q[x, y]$
- $g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3$
- Is $g_1 \in I_1$? Is $g_2 \in I_1$?
- $g_1 = 2f_1 + 3f_2; \quad g_2 = f_1 - f_2; \implies g_1, g_2 \in I_1$, so $I_2 \subseteq I_1$.
- Similarly, show that $f_1, f_2 \subseteq I_2$
- If $I_1 \subset I_2$, and $I_2 \subset I_1$ then $I_1 = I_2$
Example of Ideal Generators

- \( I_1 = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y] \)
- \( f_1 = x^2 - 4; \ f_2 = y^2 - 1 \)
- \( I_2 = \langle g_1, g_2 \rangle \subset \mathbb{Q}[x, y] \)
- \( g_1 = 2x^2 + 3y^2 - 11; \ g_2 = x^2 - y^2 - 3; \)
- Is \( g_1 \in I_1? \) Is \( g_2 \in I_1? \)
- \( g_1 = 2f_1 + 3f_2; \ g_2 = f_1 - f_2; \implies g_1, g_2 \in I_1, \) so \( I_2 \subset I_1. \)
- Similarly, show that \( f_1, f_2 \subset I_2 \)
- If \( I_1 \subset I_2, \) and \( I_2 \subset I_1 \) then \( I_1 = I_2 \)
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset Q[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $I_2 = \langle g_1, g_2 \rangle \subset Q[x, y]$
- $g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3$
- Is $g_1 \in I_1$? Is $g_2 \in I_1$?
- $g_1 = 2f_1 + 3f_2; \quad g_2 = f_1 - f_2; \quad \implies g_1, g_2 \in I_1$, so $I_2 \subseteq I_1$.
- Similarly, show that $f_1, f_2 \subseteq I_2$
- If $I_1 \subset I_2$, and $I_2 \subset I_1$ then $I_1 = I_2$

The Ideal Membership Testing Problem

Given $R = \mathbb{F}[x_1, \ldots, x_d], f_1, \ldots, f_s, \quad f \in R$, let $J = \langle f_1, \ldots, f_s \rangle \subseteq R$. Find out whether $f \in J$?
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $I_2 = \langle g_1, g_2 \rangle \subset \mathbb{Q}[x, y]$
- $g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3$
- Is $g_1 \in I_1$? Is $g_2 \in I_1$?
- $g_1 = 2f_1 + 3f_2; \quad g_2 = f_1 - f_2; \implies g_1, g_2 \in I_1$, so $I_2 \subseteq I_1$.
- Similarly, show that $f_1, f_2 \subseteq I_2$
- If $I_1 \subset I_2$, and $I_2 \subset I_1$ then $I_1 = I_2$

The Ideal Membership Testing Problem

Given $R = \mathbb{F}[x_1, \ldots, x_d], f_1, \ldots, f_s, \quad f \in R$, let $J = \langle f_1, \ldots, f_s \rangle \subseteq R$. Find out whether $f \in J$?

$f =$ specification, $J =$ implementation, Do an equivalence check: Is $f \in J$? [Or something like that...]
Given $R = \mathbb{F}[x_1, \ldots, x_d]$, $f_1, \ldots, f_s, \in R$, let $J = \langle f_1, \ldots, f_s \rangle \subseteq R$. The set of all solutions to:

$$f_1 = f_2 = \cdots = f_s = 0$$

is called the variety $V(f_1, \ldots, f_s)$.
Given $R = \mathbb{F}[x_1, \ldots, x_d]$, $f_1, \ldots, f_s \in R$, let $J = \langle f_1, \ldots, f_s \rangle \subseteq R$. The set of all solutions to:

$$f_1 = f_2 = \cdots = f_s = 0$$

is called the variety $V(f_1, \ldots, f_s)$

Variety depends not just on the given set of polynomials $f_1, \ldots, f_s$, but rather on the ideal $J = \langle f_1, \ldots, f_s \rangle$ generated by these polynomials.
Varieties of Ideals

Given $R = \mathbb{F}[x_1, \ldots, x_d], f_1, \ldots, f_s, \in R$, let $J = \langle f_1, \ldots, f_s \rangle \subseteq R$. The set of all solutions to:

$$f_1 = f_2 = \cdots = f_s = 0$$

is called the variety $V(f_1, \ldots, f_s)$

Variety depends not just on the given set of polynomials $f_1, \ldots, f_s$, but rather on the ideal $J = \langle f_1, \ldots, f_s \rangle$ generated by these polynomials.

$J = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$
Prove that Variety depends on the Ideal

Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$
Prove that Variety depends on the Ideal

- Given \( J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d] \)
- Let \( \mathbf{a} = (a_1, \ldots, a_d) \) be a point in \( \mathbb{F}^d \)
Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$

Let $a = (a_1, \ldots, a_d)$ be a point in $\mathbb{F}^d$

Let $a \in V(J)$
Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$

Let $a = (a_1, \ldots, a_d)$ be a point in $\mathbb{F}^d$

Let $a \in V(J)$

Then $f_1(a) = \cdots = f_s(a) = 0$
Prove that Variety depends on the Ideal

- Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$
- Let $a = (a_1, \ldots, a_d)$ be a point in $\mathbb{F}^d$
- Let $a \in V(J)$
- Then $f_1(a) = \cdots = f_s(a) = 0$
- Let $f \in J$
Prove that Variety depends on the Ideal

- Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$
- Let $a = (a_1, \ldots, a_d)$ be a point in $\mathbb{F}^d$
- Let $a \in V(J)$
- Then $f_1(a) = \cdots = f_s(a) = 0$
- Let $f \in J$
- Is $f(a) = 0$?
Prove that Variety depends on the Ideal

- Given \( J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d] \)
- Let \( \mathbf{a} = (a_1, \ldots, a_d) \) be a point in \( \mathbb{F}^d \)
- Let \( \mathbf{a} \in V(J) \)
- Then \( f_1(\mathbf{a}) = \cdots = f_s(\mathbf{a}) = 0 \)
- Let \( f \in J \)
- Is \( f(\mathbf{a}) = 0? \)
- \( f = f_1 h_1 + \cdots + f_s h_s \)
Prove that Variety depends on the Ideal

- Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$
- Let $a = (a_1, \ldots, a_d)$ be a point in $\mathbb{F}^d$
- Let $a \in V(J)$
- Then $f_1(a) = \cdots = f_s(a) = 0$
- Let $f \in J$
- Is $f(a) = 0$?
- $f = f_1 h_1 + \cdots + f_s h_s$
- $f(a) = f_1(a) h_1 + \cdots + f_s(a) h_s = 0$
Prove that Variety depends on the Ideal

- Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_d]$
- Let $a = (a_1, \ldots, a_d)$ be a point in $\mathbb{F}^d$
- Let $a \in V(J)$
- Then $f_1(a) = \cdots = f_s(a) = 0$
- Let $f \in J$
- Is $f(a) = 0$?
  \[ f = f_1 h_1 + \cdots + f_s h_s \]
  \[ f(a) = f_1(a) h_1 + \cdots + f_s(a) h_s = 0 \]
- Extend the argument to all $f \in J$ for all $a \in V(J)$, and you can show that Variety depends on the ideal $J = \langle f_1, \ldots, f_s \rangle$, not just on the set of polynomials $F = \{f_1, \ldots, f_s\}$
Example of Ideal Generators

- $I_1 = \langle f_1, f_2 \rangle \subset Q[x, y]$
- $f_1 = x^2 - 4; \quad f_2 = y^2 - 1$
- $I_2 = \langle g_1, g_2 \rangle \subset Q[x, y]$
- $g_1 = 2x^2 + 3y^2 - 11; \quad g_2 = x^2 - y^2 - 3$
- Is $g_1 \in I_1$? Is $g_2 \in I_1$?
- $g_1 = 2f_1 + 3f_2; \quad g_2 = f_1 - f_2; \quad \Rightarrow \quad g_1, g_2 \in I_1$, so $I_2 \subseteq I_1$.
- Similarly, show that $f_1, f_2 \subseteq I_2$
- If $I_1 \subset I_2$, and $I_2 \subset I_1$ then $I_1 = I_2$

Note $V(I_1) = V(I_2) = \{(\pm 2, \pm 1)\}$