Intro to Rings, Fields, Polynomials: Hardware Modeling by Modulo Arithmetic

Priyank Kalla

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

Lectures: Sept. 11, 2017 onwards

Agenda for Today

- 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
  - Finite fields $\mathbb{F}_p$, $\mathbb{F}_{p^k}$ and $\mathbb{F}_{2^k}$
- Later on, we will study
  - Ideals, Varieties, and Gröbner Bases
  - Decision procedures in verification

Motivation for Algebraic Computation

- Modeling for bit-precise algebraic computation
  - Arithmetic RTLs: functions over k-bit-vectors
  - k-bit-vector $\mapsto$ integers $\pmod{2^k} = \mathbb{Z}_{2^k}$
  - k-bit-vector $\mapsto$ Galois (Finite) field $\mathbb{F}_{2^k}$
- For many of these applications SAT/SMT fail miserably!
- Computer Algebra and Algebraic Geometry + SAT/SMT
  - Model: Circuits as polynomial functions $f : \mathbb{Z}_{2^k} \to \mathbb{Z}_{2^k}$, $f : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$

Ring algebra

All we need is an algebraic object where we can ADD, MULTIPLY, DIVIDE.
These objects are Rings and Fields.

An **Abelian group** is a set G and a binary operation "$+$" satisfying:

- *Closure:* For every $a, b \in G, a + b \in G$.
- *Associativity:* For every $a, b, c \in G, a + (b + c) = (a + b) + c$.
- *Commutativity:* For every $a, b \in G, a + b = b + a$.
- *Identity:* There is an identity element $0 \in G$ such that for all $a \in G; a + 0 = a$.
- *Inverse:* If $a \in G$, then there is an element $a^{-1} \in G$ such that $a + a^{-1} = 0$.

Example: The set of Integers $\mathbb{Z}$ or $\mathbb{Z}_n$ with $+$ operation.

A **Commutative ring with unity** is a set R and two binary operations "$+$" and "$\cdot$", as well as two distinguished elements $0, 1 \in R$ such that, R is an Abelian group with respect to addition with additive identity element 0, and the following properties are satisfied:

- *Multiplicative Closure:* For every $a, b \in$ R, $a \cdot b \in$ R.
- *Multiplicative Associativity:* For every $a, b, c \in$ R, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- *Multiplicative Commutativity:* For every $a, b \in$ R, $a \cdot b = b \cdot a$.
- *Multiplicative Identity:* There is an identity element $1 \in$ R such that for all $a \in$ R, $a \cdot 1 = a$.
- *Distributivity:* For every $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ holds for all $a, b, c \in R$.

Example: The set of Integers $\mathbb{Z}$ or $\mathbb{Z}_n$ with $+, \cdot$ operations.

Rings

- Examples of rings: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}$
- $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ where $+, \cdot$ computed $+, \cdot \pmod{n}$
- Modulo arithmetic:
  - $(a + b) \pmod{n} = (a \pmod{n} + b \pmod{n}) \pmod{n}$
  - $(a \cdot b) \pmod{n} = (a \pmod{n} \cdot b \pmod{n}) \pmod{n}$
  - $-a \pmod{n} = (n - a) \pmod{n}$
- Arithmetic k-bit vectors $\mapsto$ arithmetic over $\mathbb{Z}_{2^k}$
- For $k = 1$, $\mathbb{Z}_2 \equiv \mathbb{B}$

Rings

- Examples of rings: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}$
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ where $+, \cdot$ computed $+, \cdot \pmod{n}$
- Modulo arithmetic:
  - $(a+b) \pmod{n} = (a \pmod{n} + b \pmod{n}) \pmod{n}$
  - $(a \cdot b) \pmod{n} = (a \pmod{n} \cdot b \pmod{n}) \pmod{n}$
  - $-a \pmod{n} = (n-a) \pmod{n}$
- Arithmetic k-bit vectors $\mapsto$ arithmetic over $\mathbb{Z}_{2^k}$
- For $k = 1$, $\mathbb{Z}_2 \equiv \mathbb{B}$

But, what about division?

How to define division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?

How to define division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?

How to define division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?
- Over $\mathbb{Z}$, can you divide $\frac{3}{4}$?

How to define division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?
- Over $\mathbb{Z}$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 8$, can you divide $\frac{3}{4}$?

How to define division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?
- Over $\mathbb{Z}$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 8$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 7$, can you divide $\frac{3}{4}$?

How to define division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?
- Over $\mathbb{Z}$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 8$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 7$, can you divide $\frac{3}{4}$?

How to define division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?
- Over $\mathbb{Z}$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 8$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 7$, can you divide $\frac{3}{4}$?

Division is multiplication by a (multiplicative) inverse!

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?
- Over $\mathbb{Z}$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 8$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 7$, can you divide $\frac{3}{4}$?

Division is multiplication by a (multiplicative) inverse!

Division

For an element a in a ring R, $\frac{a}{b} = a \times b^{-1}$. Here, $b^{-1} \in R$ s.t. $b \cdot b^{-1} = 1$.

Multiplicative Inverses

- Over $\mathbb{Q}$: if $b = \frac{2}{3}$, $b^{-1} = \frac{3}{2}$?

Multiplicative Inverses

- Over $\mathbb{Q}$: if $b = \frac{2}{3}$, $b^{-1} = \frac{3}{2}$?
- Over $\mathbb{Z}$: if $b = 4$, $b^{-1} = ?$

Multiplicative Inverses

- Over $\mathbb{Q}$: if $b = \frac{2}{3}$, $b^{-1} = \frac{3}{2}$?
- Over $\mathbb{Z}$: if $b = 4$, $b^{-1} =$?
- Over rings: inverses may not exist

Multiplicative Inverses

- Over $\mathbb{Q}$: if $b = \frac{2}{3}$, $b^{-1} = \frac{3}{2}$?
- Over $\mathbb{Z}$: if $b = 4$, $b^{-1} =?$
- Over rings: inverses may not exist
- Over $\mathbb{Z}_8$: if $b = 3, b^{-1} =?$

Multiplicative Inverses

- Over $\mathbb{Q}$: if $b = \frac{2}{3}$, $b^{-1} = \frac{3}{2}$?
- Over $\mathbb{Z}$: if $b = 4$, $b^{-1} =$?
- Over rings: inverses may not exist
- Over $\mathbb{Z}_8$: if $b = 3, b^{-1} =$?
- Over $\mathbb{Z}_8$: if $b = 6, b^{-1} =$?

Multiplicative Inverses

- Over $\mathbb{Q}$: if $b = \frac{2}{3}$, $b^{-1} = \frac{3}{2}$?
- Over $\mathbb{Z}$: if $b = 4$, $b^{-1} = ?$
- Over rings: inverses may not exist
- Over $\mathbb{Z}_8$: if $b = 3, b^{-1} = ?$
- Over $\mathbb{Z}_8$: if $b = 6, b^{-1} = ?$
- Over $\mathbb{Z}_7$: if $b = 6, b^{-1} = ?$

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

Fields

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

The set $\mathbb{Z}_p = \mathbb{Z} \pmod{p} = \{0, 1, \ldots, p-1\}$ is a finite field, when p is a prime integer.

Fields

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

The set $\mathbb{Z}_p = \mathbb{Z} \pmod{p} = \{0, 1, \ldots, p-1\}$ is a finite field, when p is a prime integer.

$\mathbb{Z}_n, n \neq p$ is a ring but not a field. So, $\mathbb{Z}_{2^k}$ is not a field, as even numbers in $\mathbb{Z}_{2^k}$ have no inverses.

Fields

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

The set $\mathbb{Z}_p = \mathbb{Z} \pmod{p} = \{0, 1, \ldots, p-1\}$ is a finite field, when p is a prime integer.

$\mathbb{Z}_n, n \neq p$ is a ring but not a field. So, $\mathbb{Z}_{2^k}$ is not a field, as even numbers in $\mathbb{Z}_{2^k}$ have no inverses.
$\mathbb{Z}_2 \equiv \mathbb{F}_2 \equiv \mathbb{B} \equiv \{0, 1\}$

$\mathbb{B}$ is arithmetic (mod 2)

- Boolean AND-OR-NOT can be mapped to $+, \cdot \pmod 2$

$\mathbb{B}$ is arithmetic $\pmod 2$

- Boolean AND-OR-NOT can be mapped to $+, \cdot \pmod 2$

$\mathbb{B} \rightarrow \mathbb{F}_2$:

$$\begin{aligned} \neg a &\rightarrow a + 1 \pmod 2 \\ a \vee b &\rightarrow a + b + a \cdot b \pmod 2 \\ a \wedge b &\rightarrow a \cdot b \pmod 2 \\ a \oplus b &\rightarrow a + b \pmod 2 \end{aligned} \tag{1}$$

where $a, b \in \mathbb{F}_2 = \{0, 1\}$.

$\mathbb{B}$ is arithmetic $\pmod 2$

- Boolean AND-OR-NOT can be mapped to $+, \cdot \pmod 2$

$\mathbb{B} \rightarrow \mathbb{F}_2$:

$$\begin{aligned} \neg a &\rightarrow a + 1 \pmod 2 \\ a \vee b &\rightarrow a + b + a \cdot b \pmod 2 \\ a \wedge b &\rightarrow a \cdot b \pmod 2 \\ a \oplus b &\rightarrow a + b \pmod 2 \end{aligned} \tag{1}$$

where $a, b \in \mathbb{F}_2 = \{0, 1\}$.

In $\mathbb{Z}_2 \equiv \mathbb{F}_2, -1 = +1 \pmod 2$

Hardware Model in $\mathbb{Z}_2$

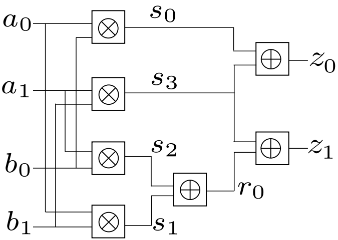

Figure: $\otimes$ = AND, $\oplus$ = XOR.

$$f_1 : s_0 + a_0 \cdot b_0; \quad f_2 : s_1 + a_0 \cdot b_1,$$
$$f_3 : s_2 + a_1 \cdot b_0; \quad f_4 : s_3 + a_1 \cdot b_1,$$
$$f_5 : r_0 + s_1 + s_2; \quad f_6 : z_0 + s_0 + s_3,$$

$$f_7 : z_1 + r_0 + s_3$$

- $\mathbb{Z}_p$: field of p elements, p $= 2, 3, 5, 7, \ldots, 163, \ldots$

Finite Fields

- $\mathbb{Z}_p$: field of p elements, p $=$ 2, 3, 5, 7, $\ldots$, 163, $\ldots$
- Is there a field of 4 elements $\mathbb{F}_4$?

Finite Fields

- $\mathbb{Z}_p$: field of p elements, p $= 2, 3, 5, 7, \ldots, 163, \ldots$
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$

Finite Fields

- $\mathbb{Z}_p$: field of p elements, p $= 2, 3, 5, 7, \ldots, 163, \ldots$
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$
- These are called extension fields, we will study them later

Finite Fields

- $\mathbb{Z}_p$: field of p elements, p $= 2, 3, 5, 7, \ldots, 163, \ldots$
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$
- These are called extension fields, we will study them later
- In fact, we are interested in $\mathbb{F}_{2^k}$ (k-bit vector arithmetic)

Finite Fields

- $\mathbb{Z}_p$: field of p elements, p $=$ 2, 3, 5, 7, ..., 163, ...
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$
- These are called extension fields, we will study them later
- In fact, we are interested in $\mathbb{F}_{2^k}$ (k-bit vector arithmetic)
- Fields are unique factorization domains (UFDs)

Finite Fields

- $\mathbb{Z}_p$: field of p elements, p $= 2, 3, 5, 7, \ldots, 163, \ldots$
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$
- These are called extension fields, we will study them later
- In fact, we are interested in $\mathbb{F}_{2^k}$ (k-bit vector arithmetic)
- Fields are unique factorization domains (UFDs)

- $\mathbb{Z}_p$: field of p elements, p = 2, 3, 5, 7, . . . , 163, . . .
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$
- These are called extension fields, we will study them later
- In fact, we are interested in $\mathbb{F}_{2^k}$ (k-bit vector arithmetic)
- Fields are unique factorization domains (UFDs)

Fermat's Little Theorem

$$\forall x \in \mathbb{F}_p,\ x^p - x = 0$$

Zero Divisors

Zero Divisors (ZD)

For $a, b \in R$, $a, b \neq 0$, $a \cdot b = 0$. Then a, b are zero divisors of each other. $\mathbb{Z}_n, n \neq p$ has zero divisors. What about $\mathbb{Z}_p$?

Integral Domains

Any set (ring) with no zero divisors: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p, \mathbb{F}_{2^k}$. What about $\mathbb{Z}_{2^k}$?

Relationships

Commutative Rings $\supset$ Integral Domains (no ZD) $\supset$ Unique Factorization Domains $\supset$ Fields

For Hardware: Our interests – non-UFD Rings ($\mathbb{Z}_{2^k}$) and Fields $\mathbb{F}_{2^k}$

- In 3-bit arithmetic $\mathbb{Z}_8$: $(x^2 + 6x) \pmod 8$

Verification Problems and UFDs

- In 3-bit arithmetic $\mathbb{Z}_8$: $(x^2 + 6x) \pmod 8$
- Factorize according to its roots: $x(x + 6)$

- In 3-bit arithmetic $\mathbb{Z}_8$: $(x^2 + 6x) \pmod 8$
- Factorize according to its roots: $x(x + 6)$
- What about $(x + 2)(x + 4)$?

Verification Problems and UFDs

- In 3-bit arithmetic $\mathbb{Z}_8$: $(x^2 + 6x) \pmod 8$
- Factorize according to its roots: $x(x + 6)$
- What about $(x + 2)(x + 4)$?
- Degree 2 polynomial has more roots than the degree? Roots $x = 0, 2, 4, 6$?

Verification Problems and UFDs

- In 3-bit arithmetic $\mathbb{Z}_8$: $(x^2 + 6x) \pmod 8$
- Factorize according to its roots: $x(x + 6)$
- What about $(x + 2)(x + 4)$?
- Degree 2 polynomial has more roots than the degree? Roots $x = 0, 2, 4, 6$?
- $\mathbb{Z}_8$ = non-UFD

Verification Problems and UFDs

- In 3-bit arithmetic $\mathbb{Z}_8$: $(x^2 + 6x) \pmod 8$
- Factorize according to its roots: $x(x + 6)$
- What about $(x + 2)(x + 4)$?
- Degree 2 polynomial has more roots than the degree? Roots $x = 0, 2, 4, 6$?
- $\mathbb{Z}_8$ = non-UFD
- Cannot use factorization to prove equivalence over non-UFDs.

Consolidating the results so far...

- Over fields $\mathbb{Z}_p, \mathbb{F}_{2^k}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$
  - We can ADD, MULTIPLY, DIVIDE
  - No zero-divisors, can uniquely factorize a polynomial according to its roots
- Rings $\mathbb{Z}$: integral domains, unique factorization, but no inverses
- Over Rings $\mathbb{Z}_n, n \neq p$; e.g. $n = 2^k$
  - Presence of zero divisors
  - non-UFDs, polynomial can have more zeros than its degree
  - Cannot perform division

Polynomials

- Let $x_1, \ldots, x_d$ be variables
- Monomial is a power product: $X = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_d^{\alpha_d}, \ \alpha_i \in \mathbb{Z}_{\geq 0}$
- Polynomial: finite sum of terms $f = c_1 X_1 + c_2 X_2 + \cdots + c_t X_t$, where X_i are monomials and c_i are coefficients
- $f = x^{-55}$ not a polynomial!
- The terms of f have to be ordered: $X_1 > X_2 > \cdots > X_t$
- Term ordering for univariate polynomials is based on the degree: e.g. $f = 3x^{53} + 99x^3 + 4$
- Multi-variate term-ordering is a lot more involved – and we'll study it shortly

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on
  - Is $\mathbb{F}[x]$ really a ring or a field?

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on
  - Is $\mathbb{F}[x]$ really a ring or a field?
  - Does every non-zero element in $\mathbb{F}[x]$ have an inverse?

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on
  - Is $\mathbb{F}[x]$ really a ring or a field?
  - Does every non-zero element in $\mathbb{F}[x]$ have an inverse?
  - Let $f = \frac{3}{2}(x^2) \in \mathbb{Q}[x]$, What is f^{-1}?

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on
  - Is $\mathbb{F}[x]$ really a ring or a field?
  - Does every non-zero element in $\mathbb{F}[x]$ have an inverse?
  - Let $f = \frac{3}{2}(x^2) \in \mathbb{Q}[x]$, What is f^{-1}?
- $\mathbb{F}[x_1, x_2, \dots, x_d]$ denotes the set (ring) of all multi-variate polynomials in $x_1, \dots, x_d$

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on
  - Is $\mathbb{F}[x]$ really a ring or a field?
  - Does every non-zero element in $\mathbb{F}[x]$ have an inverse?
  - Let $f = \frac{3}{2}(x^2) \in \mathbb{Q}[x]$, What is f^{-1}?
- $\mathbb{F}[x_1, x_2, \ldots, x_d]$ denotes the set (ring) of all multi-variate polynomials in $x_1, \ldots, x_d$
- R need not have coefficients over a field. E.g., $\mathbb{Z}_{2^k}[x_1, \ldots, x_d]$: polynomial ring with coefficients in $\mathbb{Z}_{2^k}$

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on
  - Is $\mathbb{F}[x]$ really a ring or a field?
  - Does every non-zero element in $\mathbb{F}[x]$ have an inverse?
  - Let $f = \frac{3}{2}(x^2) \in \mathbb{Q}[x]$, What is f^{-1}?
- $\mathbb{F}[x_1, x_2, \ldots, x_d]$ denotes the set (ring) of all multi-variate polynomials in $x_1, \ldots, x_d$
- R need not have coefficients over a field. E.g., $\mathbb{Z}_{2^k}[x_1, \ldots, x_d]$: polynomial ring with coefficients in $\mathbb{Z}_{2^k}$
- $\mathbb{R}[x_1, \ldots, x_d]$ is a finite or infinite set?

For symbolic computation: Polynomial Rings

- Let $\mathbb{F}$ be a field (any field: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$)
- Then, $R = \mathbb{F}[x]$ denotes the set (ring) of all univariate polynomials in x (including constants), with coefficients in $\mathbb{F}$
- Examples: Let $R = \mathbb{Q}[x]$, then $x \in R, (x^{99} + \frac{2}{3}x^{57}) \in R$ and so on
  - Is $\mathbb{F}[x]$ really a ring or a field?
  - Does every non-zero element in $\mathbb{F}[x]$ have an inverse?
  - Let $f = \frac{3}{2}(x^2) \in \mathbb{Q}[x]$, What is f^{-1}?
- $\mathbb{F}[x_1, x_2, \ldots, x_d]$ denotes the set (ring) of all multi-variate polynomials in $x_1, \ldots, x_d$
- R need not have coefficients over a field. E.g., $\mathbb{Z}_{2^k}[x_1, \ldots, x_d]$: polynomial ring with coefficients in $\mathbb{Z}_{2^k}$
- $\mathbb{R}[x_1, \ldots, x_d]$ is a finite or infinite set?
- $\mathbb{Z}_{2^k}[x_1, \ldots, x_d]$ is a finite or infinite set? (It's a loaded question)

- ADD, MULT polynomials, just like you did in high-school
- Reduce coefficients modulo the coefficient field/ring
- Consider: $f_1, f_2 \in \mathbb{Z}_4[x, y]$
    - $f_1 = 3x + 2y; \quad f_2 = 2x + 2y$
    - $f_1 + f_2 = x; \quad f_1 \cdot f_2 = 2x^2 + 2xy$
    - Reduce coefficients in $\mathbb{Z}_4$, i.e. (mod 4)
- Solve $f_1 = f_2 = 0$, Solutions (x, y) should be in $\mathbb{Z}_4$

- ADD, MULT polynomials, just like you did in high-school
- Reduce coefficients modulo the coefficient field/ring
- Consider: $f_1, f_2 \in \mathbb{Z}_4[x, y]$
  - $f_1 = 3x + 2y; \quad f_2 = 2x + 2y$
  - $f_1 + f_2 = x; \quad f_1 \cdot f_2 = 2x^2 + 2xy$
  - Reduce coefficients in $\mathbb{Z}_4$, i.e. (mod 4)
- Solve $f_1 = f_2 = 0$, Solutions (x, y) should be in $\mathbb{Z}_4$
- Solutions $(x, y) = \{(0, 0), (0, 2)\} \in \mathbb{Z}_4 \times \mathbb{Z}_4$

- ADD, MULT polynomials, just like you did in high-school
- Reduce coefficients modulo the coefficient field/ring
- Consider: $f_1, f_2 \in \mathbb{Z}_4[x, y]$
  - $f_1 = 3x + 2y; \quad f_2 = 2x + 2y$
  - $f_1 + f_2 = x; \quad f_1 \cdot f_2 = 2x^2 + 2xy$
  - Reduce coefficients in $\mathbb{Z}_4$, i.e. $\pmod 4$
- Solve $f_1 = f_2 = 0$, Solutions (x, y) should be in $\mathbb{Z}_4$
- Solutions $(x, y) = \{(0, 0), (0, 2)\} \in \mathbb{Z}_4 \times \mathbb{Z}_4$
- Finding solutions to a system of polynomial equations is not easy, solutions also have be found within the ring or field, e.g. $\mathbb{Z}_4$ in our case. That's why we use symbolic reasoning instead of numeric computation

Polynomial Functions (Polyfunctions)

- A function is a map $f : A \to B$; where A, B are the domain and co-domain, respectively.
- Ex: $f : \mathbb{R} \to \mathbb{R}$ is a function over Reals; and $f : \mathbb{Z}_{2^k} \to \mathbb{Z}_{2^k}$ is a function over the finite integer ring $\mathbb{Z}_{2^k}$

PolyFunction

Given a function $f : A \to B$, does there exist a (canonical) polynomial F that describes f? If so, f is a polynomial function.

- Over finite fields every function $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ is a polynomial function. It is possible to interpolate a polynomial F from f.
- Not every $f : \mathbb{Z}_n \to \mathbb{Z}_n, n \neq p$, is a polynomial function.
  - Example1: $f : \mathbb{Z}_4 \to \mathbb{Z}_4, f(0) = 0; f(1) = 1; f(2) = 0; f(3) = 1$; then $F = x^2 \pmod 4$
  - Example2: $f : \mathbb{Z}_4 \to \mathbb{Z}_4, f(0) = 0; f(1) = 0; f(2) = 1; f(3) = 1$; No polynomial $F \pmod 4$ represents f

Zero Polynomials and Zero Functions

- Over $\mathbb{Z}_4[x]$, $F_1 = 2x^2, F_2 = 2x$
- $F_1 - F_2 = 2x^2 - 2x = 0 \ \ (\forall x \in \mathbb{Z}_4)$
- $F_1 \equiv F_2$ and $F_1 - F_2 \equiv 0$ (zero function)
- Need a unique, canonical representation of F over $\mathbb{Z}_{2^k}, \mathbb{F}_{2^k}$
- Equivalently, need a unique, canonical representation of the zero function
- Over $\mathbb{Z}_{2^k}[x]$, we'll study canonical representations of zero functions later in the course
- Over Galois fields $\mathbb{Z}_p : x^p = x \pmod p$ or $x^p - x = 0 \pmod p$

Zero functions in $\mathbb{Z}_p[x]$

A polynomial $F \in \mathbb{Z}_p[x]$ represents the zero function $\iff$ $F \pmod{x^p - x} = 0$, i.e. $x^p - x$ divides F.

- In $\mathbb{Z}_p[x]$, to prove $F_1 \equiv F_2 \iff (F_1 - F_2) \pmod{x^p - x} = 0$.

Zero Functions over Infinite Fields

- Over infinite fields, life is much easier:

Let $\mathbb{F}$ be an infinite field, and $F \in \mathbb{F}[x_1, \ldots, x_d]$. Then:
$F = 0 \iff f : \mathbb{F}^n \to \mathbb{F}$ is the zero function

Circuits are functions over $\mathbb{Z}_{2^k}, \mathbb{F}_{2^k}$. Need algorithms to test if multi-variate polynomials $F(x_1, \ldots, x_d) \in \mathbb{Z}_{2^k}[x_1, \ldots, x_d]$ or in $\mathbb{F}_{2^k}[x_1, \ldots, x_d]$ are zero functions. Hardware verification is a hard problem!