Galois Fields and Hardware Design

Construction of Galois Fields, Basic Properties, Uniqueness, Containment, Closure, Polynomial Functions over Galois Fields

Priyank Kalla

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

Lectures conducted Sept 23, 2019 onwards

Agenda

- Introduction to Field Construction
- Constructing $\mathbb{F}_{2^k}$ and its elements
- Addition, multiplication and inverses over GFs
- Conjugates and their minimal polynomials
- GF containment and algebraic closure
- Hardware design over GFs

Definition

An integral domain R is a set with two operations $(+, \cdot)$ such that:

1. The elements of R form an abelian group under $+$ with additive identity 0.
2. The multiplication is associative and commutative, with multiplicative identity 1.
3. The distributive law holds: $a(b+c) = ab + ac$.
4. The cancellation law holds: if $ab = ac$ and $a \neq 0$, then $b = c$.

Examples: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p, \mathbb{F}[x], \mathbb{F}[x, y]$. Finite rings $\mathbb{Z}_n, n \neq p$ are not integral domains.

Definition

A Euclidean domain $\mathbb{D}$ is an integral domain where:

1. associated with each non-zero element $a \in \mathbb{D}$ is a non-negative integer $f(a)$ s.t. $f(a) \leq f(ab)$ if $b \neq 0$; and
2. $\forall a, b \ (b \neq 0), \exists (q, r)$ s.t. $a = qb + r$, where either $r = 0$ or $f(r) < f(b)$.

- Can apply the Euclid's algorithm to compute $g = GCD(g_1, \dots, g_t)$
- $GCD(a, b, c) = GCD(GCD(a, b), c)$
- Then $g = \sum_i u_i g_i$, i.e. GCD can be represented as a linear combination of the elements

Euclid's Algorithm

Inputs: Elements $a, b \in \mathbb{D}$, a Euclidean domain
Outputs: $g = GCD(a, b)$

```
Assume a > b, otherwise swap a, b  {/* GCD(a, 0) = a */}
while  b ≠ 0  do
    t := b
    b := a (mod b)
    a := t
end while
return  g := a
```

Algorithm 1: Euclid's Algorithm

GCD(84, 54) = 6

$$84 = 1 \cdot 54 + 30$$
$$54 = 1 \cdot 30 + 24$$
$$30 = 1 \cdot 24 + \underline{6}$$
$$24 = 4 \cdot \underline{6} + 0$$

Lemma

If $g = gcd(a, b)$ then $\exists s, t$ such that $s \cdot a + t \cdot b = g$.

Unroll Euclid's algorithm to find s, t. A HW assignment!

Euclidean Domains

- $\mathbb{D} = \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$
- The ring $\mathbb{F}[x]$ is a Euclidean domain where $\mathbb{F}$ is any field
- The ring $R = \mathbb{F}[x, y]$ is NOT a Euclidean domain where $\mathbb{F}$ is any field
    - For $x, y \in R$, $GCD(x, y) = 1$, but cannot write $1 = f_1(x, y) \cdot x + f_2(x, y)y$
- $\mathbb{Z}_{2^k}$ is neither and integral domain not a Euclidean domain

Fields

Definition

Let $\mathbb{D}$ be a Euclidean domain, and $p \in \mathbb{D}$ be a prime element. Then $\mathbb{D} \pmod{p}$ is a field.

- That is why $\mathbb{Z} \pmod{p}$ is a field
- In $\mathbb{R}[x], x^2 + 1$ is a prime — actually called an irreducible polynomial
- So $\mathbb{R}[x] \pmod{x^2 + 1}$ is a field and is the field of complex numbers $\mathbb{C}$
- $\mathbb{R}[x] \pmod{p} = \{f(x) \mid \forall g(x) \in \mathbb{R}[x], f(x) = g(x) \pmod{p}\}$

$\mathbb{R}[x] \pmod{x^2+1} = \mathbb{C}$

- Let $f, g \in \mathbb{R}[x] \pmod{x^2+1}$
- $f =$ remainder of division by x^2+1, it is linear
- Let $f = ax + b, \;\; g = cx + d$

$$
\begin{aligned}
f \cdot g &= (ax+b)(cx+d) \pmod{x^2+1} \\
&= acx^2 + (ad+bc)x + bd \pmod{x^2+1} \\
&= (ad+bc)x + (bd - ac) \;\text{ after reducing by }\; x^2 = -1
\end{aligned}
$$

- Replace x with $i = \sqrt{-1}$, and we get $\mathbb{C}$
- $\mathbb{C}$ is a 2 (=degree(x^2+1)) dimensional extension of $\mathbb{R}$
- Intuitively, that is why $\mathbb{C} \supset \mathbb{R}$ (containment and closure)

Recall from my previous slides:

From Rings to Fields

Rings $\supset$ Integral Domains $\supset$ Unique Factorization Domains $\supset$ Euclidean Domains $\supset$ Fields

Now you know the reason for this containment

Construct Galois Extension Fields

- $\mathbb{F}_p[x]$ is a Euclidean domain, let $P(x)$ be irreducible over $\mathbb{F}_p$, and let degree of $P(x) = k$
- $\mathbb{F}_p[x] \pmod{P(x)} = \mathbb{F}_{p^k}$, a finite field of p^k elements
- Denote GFs as $\mathbb{F}_q$, $q = p^k$ for prime p and $k \geq 1$
- $\mathbb{F}_{p^k}$ is a k-dimensional **extension** of $\mathbb{F}_p$, so $\mathbb{F}_p \subset \mathbb{F}_{p^k}$
- Our interest $\mathbb{F}_{2^k} = \mathbb{F}_2[x] \pmod{P(x)}$ where $P(x) \in \mathbb{F}_2[x]$ is a degree-k irreducible polynomial

- Irreducible polynomials of any degree k always exist over $\mathbb{F}_2$, so $\mathbb{F}_{2^k}$ can be constructed for arbitrary $k \geq 1$

Table: Some irreducible polynomials in $\mathbb{F}_2[x]$.

Degree	Irreducible Polynomials
1	$x; x+1$
2	x^2+x+1
3	$x^3+x+1; x^3+x^2+1$
4	$x^4+x+1; x^4+x^3+1; x^4+x^3+x^2+x+1$

- $\mathbb{F}_{2^k} = \mathbb{F}_2[x] \pmod{P(x)}$, let α be a root of $P(x)$, i.e. $P(\alpha) = 0$
- $P(x)$ has no roots in $\mathbb{F}_2$ (irreducible); root lies in its algebraic extension $\mathbb{F}_{2^k}$
- Any element $A \in \mathbb{F}_{2^k}$:
  $A = \sum_{i=0}^{k-1}(a_i \cdot \alpha^i) = a_0 + a_1 \cdot \alpha + \cdots + a_{k-1} \cdot \alpha^{k-1}$ where $a_i \in \mathbb{F}_2$
- The "degree" of $A < k$
- Think of $A = \{a_{k-1}, \ldots, a_0\}$ as a bit-vector

Example of $\mathbb{F}_{16}$

- $\mathbb{F}_{2^4}$ as $\mathbb{F}_2[x] \pmod{P(x)}$, where $P(x) = x^4 + x^3 + 1$, $P(\alpha) = 0$
- Any element $A \in \mathbb{F}_{16} = a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ (degree < 4)

Table: Bit-vector, Exponential and Polynomial representation of elements in $\mathbb{F}_{2^4} = \mathbb{F}_2[x] \pmod{x^4 + x^3 + 1}$

$a_3a_2a_1a_0$	Expo	Poly	$a_3a_2a_1a_0$	Expo	Poly
0000	0	0	1000	α^3	α^3
0001	1	1	1001	α^4	α^3+1
0010	α	α	1010	α^{10}	$\alpha^3+\alpha$
0011	α^{12}	$\alpha+1$	1011	α^5	$\alpha^3+\alpha+1$
0100	α^2	α^2	1100	α^{14}	$\alpha^3+\alpha^2$
0101	α^9	α^2+1	1101	α^{11}	$\alpha^3+\alpha^2+1$
0110	α^{13}	$\alpha^2+\alpha$	1110	α^8	$\alpha^3+\alpha^2+\alpha$
0111	α^7	$\alpha^2+\alpha+1$	1111	α^6	$\alpha^3+\alpha^2+\alpha+1$

Definition

The characteristic of a finite field $\mathbb{F}_q$ with unity element 1 is the smallest integer n such that $1 + \cdots + 1$ (n times) $= 0$.

Definition

The characteristic of a finite field $\mathbb{F}_q$ with unity element 1 is the smallest integer n such that $1 + \cdots + 1$ (n times) $= 0$.

- What is the characteristic of $\mathbb{F}_{2^k}$? Of $\mathbb{F}_{p^k}$?

Definition

The characteristic of a finite field $\mathbb{F}_q$ with unity element 1 is the smallest integer n such that $1 + \cdots + 1$ (n times) $= 0$.

- What is the characteristic of $\mathbb{F}_{2^k}$? Of $\mathbb{F}_{p^k}$?
- Characteristic $= 2$ and p, respectively, of course!

Add, Mult in $\mathbb{F}_{2^k}$

Definition

The characteristic of a finite field $\mathbb{F}_q$ with unity element 1 is the smallest integer n such that $1 + \cdots + 1$ (n times) $= 0$.

- What is the characteristic of $\mathbb{F}_{2^k}$? Of $\mathbb{F}_{p^k}$?
- Characteristic $= 2$ and p, respectively, of course!
- In $\mathbb{F}_{2^k}$ coefficients reduced modulo 2

Add, Mult in $\mathbb{F}_{2^k}$

Definition

The characteristic of a finite field $\mathbb{F}_q$ with unity element 1 is the smallest integer n such that $1 + \cdots + 1$ (n times) $= 0$.

- What is the characteristic of $\mathbb{F}_{2^k}$? Of $\mathbb{F}_{p^k}$?
- Characteristic $= 2$ and p, respectively, of course!
- In $\mathbb{F}_{2^k}$ coefficients reduced modulo 2

Add, Mult in $\mathbb{F}_{2^k}$

Definition

The characteristic of a finite field $\mathbb{F}_q$ with unity element 1 is the smallest integer n such that $1 + \cdots + 1$ (n times) $= 0$.

- What is the characteristic of $\mathbb{F}_{2^k}$? Of $\mathbb{F}_{p^k}$?
- Characteristic $= 2$ and p, respectively, of course!
- In $\mathbb{F}_{2^k}$ coefficients reduced modulo 2

$$\begin{aligned}
\alpha^5 + \alpha^{11} &= \alpha^3 + \alpha + 1 + \alpha^3 + \alpha^2 + 1 \\
&= 2 \cdot \alpha^3 + \alpha^2 + \alpha + 2 \\
&= \alpha^2 + \alpha \quad (\text{as characteristic of } \mathbb{F}_{2^k} = 2) \\
&= \alpha^{13}
\end{aligned}$$

Definition

The characteristic of a finite field $\mathbb{F}_q$ with unity element 1 is the smallest integer n such that $1 + \cdots + 1$ (n times) $= 0$.

- What is the characteristic of $\mathbb{F}_{2^k}$? Of $\mathbb{F}_{p^k}$?
- Characteristic $= 2$ and p, respectively, of course!
- In $\mathbb{F}_{2^k}$ coefficients reduced modulo 2

$$
\begin{aligned}
\alpha^5 + \alpha^{11} &= \alpha^3 + \alpha + 1 + \alpha^3 + \alpha^2 + 1 \\
&= 2 \cdot \alpha^3 + \alpha^2 + \alpha + 2 \\
&= \alpha^2 + \alpha \quad (\text{as characteristic of } \mathbb{F}_{2^k} = 2) \\
&= \alpha^{13}
\end{aligned}
$$

Addition in $\mathbb{F}_{2^k}$ is Bit-vector XOR operation

Add, Mult in $\mathbb{F}_{2^k}$

$$
\begin{aligned}
\alpha^4 \cdot \alpha^{10} &= (\alpha^3 + 1)(\alpha^3 + \alpha) \\
&= \alpha^6 + \alpha^4 + \alpha^3 + \alpha \\
&= \alpha^4 \cdot \alpha^2 + (\alpha^4 + \alpha^3) + \alpha \\
&= (\alpha^3 + 1) \cdot \alpha^2 + (1) + \alpha \quad (\text{as } \ \alpha^4 = \alpha^3 + 1) \\
&= \alpha^5 + \alpha^2 + \alpha + 1 \\
&= \alpha^4 \cdot \alpha + \alpha^2 + \alpha + 1 \\
&= (\alpha^3 + 1) \cdot \alpha + \alpha^2 + \alpha + 1 \\
&= \alpha^4 + \alpha^2 + 1 \\
&= \alpha^3 + \alpha^2
\end{aligned}
$$

Reduce everything $\pmod{P(x) = x^4 + x^3 + 1}$, and $-1 = +1$ in $\mathbb{F}_{2^k}$

Every non-zero element has an inverse

- How to find the inverse of α?
- HW for you: think Euclidean algorithm!
- What is the inverse of α in our $\mathbb{F}_{16}$ example?

Vanishing Polynomials of $\mathbb{F}_q$

Lemma

Let A be any non-zero element in $\mathbb{F}_q$, then $A^{q-1} = 1$.

Theorem

[Generalized Fermat's Little Theorem] Given a finite field $\mathbb{F}_q$, each element $A \in \mathbb{F}_q$ satisfies: $A^q \equiv A$ or $A^q - A \equiv 0$

Example

Given $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha + 1\}$ with $P(x) = x^2 + x + 1$, where $P(\alpha) = 0$.

$$0^{2^2} = 0; \quad 1^{2^2} = 1; \quad \alpha^{2^2} = \alpha \pmod{\alpha^2 + \alpha + 1}$$

and

$$(\alpha + 1)^{2^2} = \alpha + 1 \pmod{\alpha^2 + \alpha + 1}$$

- An irreducible poly $P(x)$ is primitive if its root α can generate all non-zero elements of the field.
- $\mathbb{F}_q = \{0, 1 = \alpha^{q-1}, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q-2}\}$
- $x^4 + x^3 + 1$ is primitive but $x^4 + x^3 + x^2 + x + 1$ is not

$$
\begin{aligned}
\alpha^4 &= \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^5 &= \alpha^4 \cdot \alpha \\
&= (\alpha^3 + \alpha^2 + \alpha + 1)(\alpha) \\
&= (\alpha^4) + \alpha^3 + \alpha^2 + \alpha \\
&= (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) \\
&= 1
\end{aligned}
$$

Theorem

Let $f(x) \in \mathbb{F}_2[x]$ be an arbitrary polynomial, and let β be an element in $\mathbb{F}_{2^k}$ for any $k > 1$. If β is a root of $f(x)$, then for any $l \geq 0, \beta^{2^l}$ is also a root of $f(x)$. Elements β^{2^l} are conjugates of each other.

Example

Let $\mathbb{F}_{16} = \mathbb{F}_2[x] \pmod{P(x) = x^4 + x^3 + 1}$. Let $P(\alpha) = 0$. Let us find conjugates of α as α^{2^l}.

$$
\begin{aligned}
l &= 1 : \alpha^2 \\
l &= 2 : \alpha^4 = \alpha^3 + 1 \\
l &= 3 : \alpha^8 = \alpha^3 + \alpha^2 + \alpha \\
l &= 4 : \alpha^{16} = \alpha \quad \text{(conjugates start to repeat)}
\end{aligned}
$$

So $\alpha, \alpha^2, \alpha^3 + 1, \alpha^3 + \alpha^2 + \alpha$ are conjugates of each other.

Get the irreducible polynomial back from conjugates

Example

Over $\mathbb{F}_{16} = \mathbb{F}_2[x] \pmod{x^4 + x^3 + 1}$, conjugate elements:

- $\alpha, \alpha^2, \alpha^4, \alpha^8$
- $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}$
- $\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}$
- α^5, α^{10}

Minimal Polynomial of an element β

Let e be the smallest integer such that $\beta^{2^e} = \beta$. Construct the polynomial $f(x) = \prod_{i=0}^{e-1}(x + \beta^{2^i})$. Then $f(x)$ is an irreducible polynomial, and it is also called the irreducible polynomial of β.

Get the irreducible polynomial back from conjugates

Minimal polynomial of any element β is: $f(x) = \prod_{i=0}^{e-1}(x + \beta^{2^i})$

Example

Over $\mathbb{F}_{16} = \mathbb{F}_2[x] \pmod{x^4 + x^3 + 1}$, conjugate elements and their minimal polynomials are:

- $\alpha, \alpha^2, \alpha^4, \alpha^8: \; f_1(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8) = x^4 + x^3 + 1$
- $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}: \; f_2(x) = x^4 + x^3 + x^2 + x + 1$
- $\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}: \; f_3(x) = x^4 + x + 1$
- $\alpha^5, \alpha^{10}: \; f_4(x) = x^2 + x + 1$

Some observations....

Note that $f_4 = x^2 + x + 1$ is the polynomial used to construct $\mathbb{F}_4$. Also notice that associated with every element in $\mathbb{F}_{2^k}$ is a minimal polynomial and its roots (conjugates), that demonstrate the containment of fields and also the uniqueness of the fields upto the labeling of the elements.

Containment of fields and elements

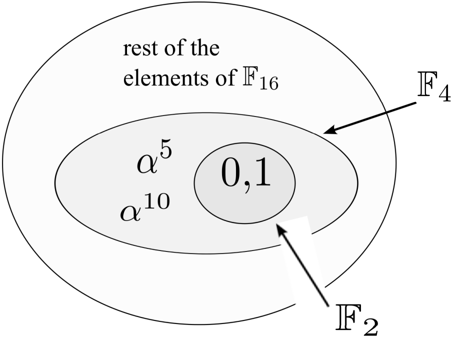


Figure: Containment of fields: $\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$

Additive & Multiplicative closure: $\alpha^5 + \alpha^{10} = 1, \quad \alpha^5 \cdot \alpha^{10} = 1.$

Containment and Closure

Theorem

$\mathbb{F}_{2^n} \subset \mathbb{F}_{2^m}$ if n divides m.

Example: $\mathbb{F}_2 \subset F_{2^2} \subset \mathbb{F}_{2^4} \subset \mathbb{F}_{2^8} \subset \ldots$
$\mathbb{F}_2 \subset \mathbb{F}_{2^3} \subset \mathbb{F}_{2^6} \subset \ldots$
$\mathbb{F}_2 \subset \mathbb{F}_{2^5} \subset \mathbb{F}_{2^{10}} \subset \ldots$
$\mathbb{F}_2 \subset \mathbb{F}_{2^7} \subset \mathbb{F}_{2^{14}} \subset \ldots$ and so on

Algebraic Closure of $\mathbb{F}_q$

The algebraic closure of $\mathbb{F}_{2^k}$ is the union of ALL such fields $\mathbb{F}_{2^n}$ where $k \mid n$.

Polynomial Functions over $\mathbb{F}_q$

- Any combinational circuit with k-bit inputs and k-bit output
  - Implements a function $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$
  - Can be viewed as a function $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$ or $f : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_{2^k}$
  - Need symbolic representations: view them as polynomial functions
- Treat the circuit $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$ as a polynomial function
- Please see the last section in my book chapter

Polynomial Functions $f : \mathbb{F}_q \to \mathbb{F}_q$

- Every function is a polynomial function over $\mathbb{F}_q$
- Consider 1-bit right-shift operation $Z[2:0] = A[2:0] >> 1$

$\{a_2a_1a_0\}$	A	$\to$	$\{z_2z_1z_0\}$	Z
000	0	$\to$	000	0
001	1	$\to$	000	0
010	α	$\to$	001	1
011	$\alpha+1$	$\to$	001	1
100	α^2	$\to$	010	α
101	α^2+1	$\to$	010	α
110	$\alpha^2+\alpha$	$\to$	011	$\alpha+1$
111	$\alpha^2+\alpha+1$	$\to$	011	$\alpha+1$

Polynomial Functions $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$

- Every function is a polynomial function over $\mathbb{F}_q$
- Consider 1-bit right-shift operation $Z[2:0] = A[2:0] >> 1$

$\{a_2 a_1 a_0\}$	A	$\rightarrow$	$\{z_2 z_1 z_0\}$	Z
000	0	$\rightarrow$	000	0
001	1	$\rightarrow$	000	0
010	α	$\rightarrow$	001	1
011	$\alpha + 1$	$\rightarrow$	001	1
100	α^2	$\rightarrow$	010	α
101	$\alpha^2 + 1$	$\rightarrow$	010	α
110	$\alpha^2 + \alpha$	$\rightarrow$	011	$\alpha + 1$
111	$\alpha^2 + \alpha + 1$	$\rightarrow$	011	$\alpha + 1$

$$Z = (\alpha^2 + 1)A^4 + (\alpha^2 + 1)A^2 \text{ over } \mathbb{F}_{2^3} \text{ where } \alpha^3 + \alpha + 1 = 0$$

Polynomial Functions $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$

Theorem

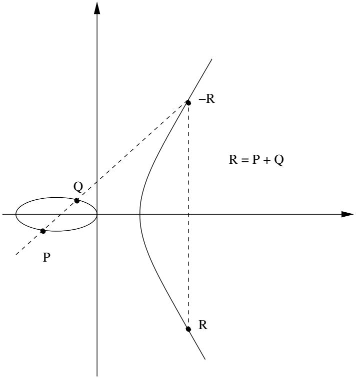
(From [1]) Any function $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ is a polynomial function over $\mathbb{F}_q$, that is there exists a polynomial $\mathcal{F} \in \mathbb{F}_q[x]$ such that $f(a) = \mathcal{F}(a)$, for all $a \in \mathbb{F}_q$.

Analyze f over each of the q points, apply **Lagrange's interpolation formula**

$$\mathcal{F}(x) = \sum_{n=1}^{q} \frac{\prod_{i \neq n}(x - x_i)}{\prod_{i \neq n}(x_n - x_i)} \cdot f(x_n), \tag{1}$$

Elliptic Curve Cryptography

$$y^2 + xy = x^3 + ax^2 + b \text{ over } \mathrm{GF}(2^k)$$



Compute Slope: $\dfrac{y_2 - y_1}{x_2 - x_1}$

Computation of inverses over $\mathbb{F}_{2^k}$ is expensive

Point addition using Projective Co-ordinates

- Curve: $Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4$ over $\mathbb{F}_{2^k}$
- Let $(X_3,\ Y_3,\ Z_3) = (X_1,\ Y_1,\ Z_1) + (X_2,\ Y_2,\ 1)$

$$
\begin{aligned}
A &= Y_2 \cdot Z_1^2 + Y_1 & \qquad E &= A \cdot C \\
B &= X_2 \cdot Z_1 + X_1 & \qquad X_3 &= A^2 + D + E \\
C &= Z_1 \cdot B & \qquad F &= X_3 + X_2 \cdot Z_3 \\
D &= B^2 \cdot (C + aZ_1^2) & \qquad G &= X_3 + Y_2 \cdot Z_3 \\
Z_3 &= C^2 & \qquad Y_3 &= E \cdot F + Z_3 \cdot G
\end{aligned}
$$

No inverses, just addition and multiplication

Multiplication in GF(2^4)

Input:
$A = (a_3 a_2 a_1 a_0)$
$B = (b_3 b_2 b_1 b_0)$
$A = a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + a_3 \cdot \alpha^3$
$B = b_0 + b_1 \cdot \alpha + b_2 \cdot \alpha^2 + b_3 \cdot \alpha^3$

Irreducible Polynomial:
$P = (11001)$
$P(x) = x^4 + x^3 + 1, \quad P(\alpha) = 0$

Result:
Output $G = A \times B \pmod{P(x)}$

Multiplication over GF(2^4)

			a_3	a_2	a_1	a_0
$\times$			b_3	b_2	b_1	b_0
			$a_3 \cdot b_0$	$a_2 \cdot b_0$	$a_1 \cdot b_0$	$a_0 \cdot b_0$
		$a_3 \cdot b_1$	$a_2 \cdot b_1$	$a_1 \cdot b_1$	$a_0 \cdot b_1$	
	$a_3 \cdot b_2$	$a_2 \cdot b_2$	$a_1 \cdot b_2$	$a_0 \cdot b_2$		
$a_3 \cdot b_3$	$a_2 \cdot b_3$	$a_1 \cdot b_3$	$a_0 \cdot b_3$			
s_6	s_5	s_4	s_3	s_2	s_1	s_0

In polynomial expression:
$S = s_0 + s_1 \cdot \alpha + s_2 \cdot \alpha^2 + s_3 \cdot \alpha^3 + s_4 \cdot \alpha^4 + s_5 \cdot \alpha^5 + s_6 \cdot \alpha^6$

S should be further reduced $\pmod{P(x)}$

Multiplication over GF(2^4)

$$
\begin{array}{ccc|cccc|cl}
s_6 & s_5 & s_4 & s_3 & s_2 & s_1 & s_0 & & \\
\hline
 & & & s_4 & 0 & 0 & s_4 & \Leftarrow & s_4 \cdot \alpha^4 \pmod{P(\alpha)} \\
 & & & s_5 & 0 & s_5 & s_5 & \Leftarrow & s_5 \cdot \alpha^5 \pmod{P(\alpha)} \\
 & & + & s_6 & s_6 & s_6 & s_6 & \Leftarrow & s_6 \cdot \alpha^6 \pmod{P(\alpha)} \\
\hline
 & & & g_3 & g_2 & g_1 & g_0 & &
\end{array}
$$

$$
\begin{aligned}
s_4 \cdot \alpha^4 \pmod{\alpha^4 + \alpha^3 + 1} &= s_4(\alpha^3 + 1) = s_4 \cdot \alpha^3 + s_4 \\
s_5 \cdot \alpha^5 \pmod{\alpha^4 + \alpha^3 + 1} &= s_5(\alpha^3 + \alpha + 1) = s_5 \cdot \alpha^3 + s_5 \cdot \alpha + s_5 \\
s_6 \cdot \alpha^6 \pmod{\alpha^4 + \alpha^3 + 1} &= s_6(\alpha^3 + \alpha^2 + \alpha + 1) \\
&= s_6 \cdot \alpha^3 + s_6 \cdot \alpha^2 + s_6 \cdot \alpha + s_6
\end{aligned}
$$

$$G = g_0 + g_1 \cdot \alpha + g_2 \cdot \alpha^2 + g_3 \cdot \alpha^3$$

Montgomery Architecture

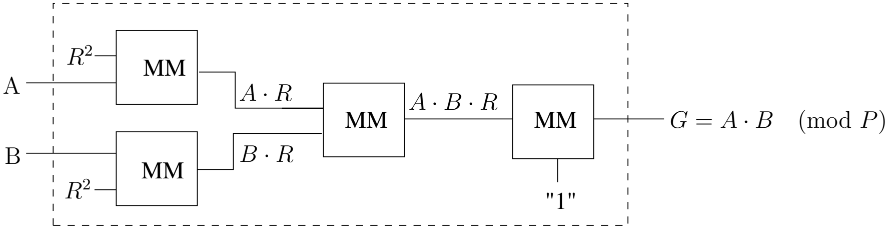


Figure: *Montgomery* multiplier over GF(2^k)

Montgomery Multiply: $F = A \cdot B \cdot R^{-1}$, $R = \alpha^k$

- Barrett architectures do not require precomputed R^{-1}
- We can verify 163-bit circuits, and also catch bugs!
- Conventional techniques fail beyond 16-bit circuits

Let us take verification of GF multipliers as an example:

- Given specification polynomial: $f : Z = A \cdot B \pmod{P(x)}$ over $\mathbb{F}_{2^k}$, for given k, and given $P(x)$, s.t. $P(\alpha) = 0$
- Given circuit implementation C
  - Primary inputs: $A = \{a_0, \dots, a_{k-1}\}, B = \{b_0, \dots, b_{k-1}\}$
  - Primary Output $Z = \{z_0, \dots, z_{k-1}\}$
  - $A = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{k-1}\alpha^{k-1}$
  - $B = b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1}, \ Z = z_0 + z_1\alpha + \cdots + z_{k-1}\alpha^{k-1}$
- Does the circuit C correctly compute specification f?

Mathematically:

- Construct a miter between the spec f and implementation C
- Model the circuit (gates) as polynomials $\{f_1, \dots, f_s\} \in \mathbb{F}_{2^k}[x_1, \dots, x_d]$
- Apply Weak Nullstellensatz

Equivalence Checking over $\mathbb{F}_{2^k}$

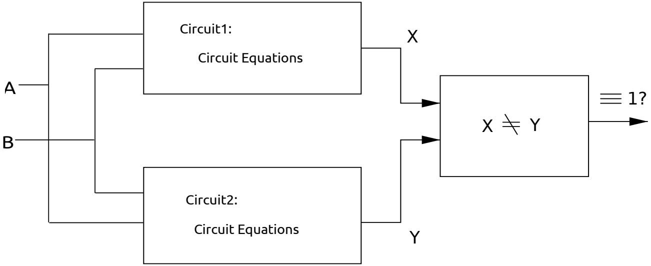


Figure: The equivalence checking setup: miter.

Spec can be a polynomial f, or a circuit implementation C

Model the miter gate as: $t(X - Y) = 1$, where t is a free variable

Verify a polynomial spec against circuit C

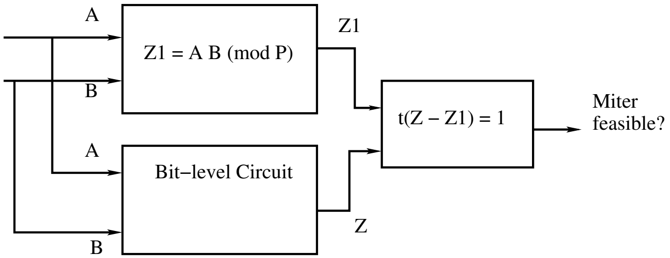


Figure: The equivalence checking setup: miter.

- When $Z = Z_1$, $t(Z - Z_1) = 1$ has no solution: infeasible miter
- When $Z \neq Z_1$: let $t^{-1} = (Z - Z_1)$. Then $t \cdot (t^{-1}) = 1$ always has a solution!
- Apply Nullstellensatz over $\mathbb{F}_{2^k}$

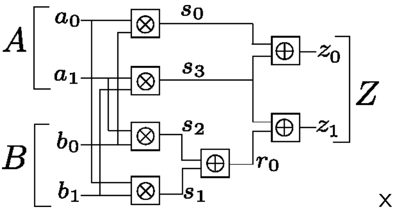


Figure: A 2-bit Multiplier

- Write $A = a_0 + a_1\alpha$ as a polynomial $f_A : A + a_0 + a_1\alpha$
- Polynomials modeling the entire circuit: ideal $J = \langle f_1, \dots, f_{10} \rangle$

$f_1 : z_0 + z_1\alpha + Z$; $f_2 : b_0 + b_1\alpha + B$; $f_3 : a_0 + a_1\alpha + A$; $f_4 :$ $s_0 + a_0 \cdot b_0$; $f_5 : s_1 + a_0 \cdot b_1$; $f_6 : s_2 + a_1 \cdot b_0$; $f_7 : s_3 + a_1 \cdot b_1$; $f_8 :$ $r_0 + s_1 + s_2$; $f_9 : z_0 + s_0 + s_3$; $f_{10} : z_1 + r_0 + s_3$

Continue with multiplier verification

- So far, ideal $J = \langle f_1, \ldots, f_{10} \rangle$ models the implementation
- Let polynomial $f : Z - A \cdot B$ denote the spec
- Miter polynomial $f_m : t \cdot (Z - Z_1) - 1$
- Update the ideal representation of the miter: $J = J + \langle f, f_m \rangle$
- Finally: ideal $J = \langle f_1, \ldots, f_{10},\ f,\ f_m \rangle$ represents the miter circuit
- $J \subseteq \mathbb{F}_{2^k}[A, B, Z, Z_1, a_0, a_1, b_0, b_1, r_0, s_0, \ldots, s_3, t]$
- Verification problem: is the variety $V_{\mathbb{F}_4}(J) = \emptyset$?
- How will we solve this problem?

Theorem (Weak Nullstellensatz over $\mathbb{F}_{2^k}$)

Let ideal $J = \langle f_1, \dots, f_s \rangle \subset \mathbb{F}_{2^k}[x_1, \dots, x_n]$ *be an ideal. Let* $J_0 = \langle x_1^{2^k} - x_1, \dots, x_n^{2^k} - x_n \rangle$ *be the ideal of all vanishing polynomials. Then:*

$$V_{\mathbb{F}_{2^k}}(J) = \emptyset \iff V_{\overline{\mathbb{F}_{2^k}}}(J + J_0) = \emptyset \iff \mathit{reducedGB}(J + J_0) = \{1\}$$

Proof:

$$\begin{aligned} V_{\mathbb{F}_{2^k}}(J) &= V_{\overline{\mathbb{F}_{2^k}}}(J) \cap \mathbb{F}_{2^k} \\ &= V_{\overline{\mathbb{F}_{2^k}}}(J) \cap V_{\mathbb{F}_{2^k}}(J_0) = V_{\overline{\mathbb{F}_{2^k}}}(J) \cap V_{\overline{\mathbb{F}_{2^k}}}(J_0) \\ &= V_{\overline{\mathbb{F}_{2^k}}}(J + J_0) \end{aligned}$$

Remember: $V_{\mathbb{F}_q}(J_0) = V_{\overline{\mathbb{F}_q}}(J_0)$. The variety of J_0 does not change over the field or the closure!

Apply Weak Nullstellesatz to the Miter

- Note: Word-level polynomials $f_A : A + a_0 + a_1\alpha \in \mathbb{F}_{2^k}$
- Gate level polynomials $f_4 : s_0 + a_0 \cdot b_0 \in \mathbb{F}_2$
- Since $\mathbb{F}_2 \subset \mathbb{F}_{2^k}$, we can treat ALL polynomials of the miter, collectively, over the larger field $\mathbb{F}_{2^k}$, so $J \subseteq \mathbb{F}_{2^k}[A, B, Z, Z_1, a_0, a_1, \ldots, z_0, z_1]$
- Consider word-level vanishing polynomials: $A^{2^2} - A$
- What about bit-level vanishing polynomials: $a_0^2 - a_0$
- So, $J_0 = \langle W^{2^k} - W, B^2 - B \rangle$, where W are all the word-level variables, and B are all the bit-level variables
- Now compute $G = GB(J + J_0)$. If $G = \{1\}$, the circuit is correct. Otherwise there is definitely a BUG within the field $\mathbb{F}_{2^k}$

[1] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, 1997.