Verification of Galois Field Multipliers

A Gröbner Bases + Nullstellensatz Approach

Priyank Kalla

Department of Electrical and Computer Engineering
University of Utah, Salt Lake City
Introduction

- Elliptic Curve Cryptography (ECC) requires multiplication and exponentiation.
- Operations performed over finite (Galois) fields, $GF(2^k)$.
- Hardware VLSI implementations of multipliers and their optimization.
- Mastrovito Multiplication, Galois Field Decomposition $GF(2^k) \equiv GF((2^m)^n)$, Montgomery multiplication, etc.
- So we have a Verification Problem: Spec $\equiv$ implementation?
- Problem is hard: $m = 256$ bits, can be more.
- BDD/SAT/SMT are infeasible, so we explore Computer Algebra!
Galois Fields

A Galois Field is a set $F_q$, satisfying all the following properties:

- **Abelian Group**: w.r.t. addition “+”, and 0 element
- **Commutative ring with unity**: $(+, \times, 1, 0)$
- **Associativity, Commutativity, Distributivity**
- **Inverse**: $\forall a \in F_q - \{0\}, \exists a^{-1} \in F_q$ such that $a \cdot a^{-1} = 1$.
- $q = p^m$, where $p$ is prime. In our case, $p = 2$.
- **Multiplicative cyclic group structure**: $a^q = a$.

$\left( \mathbb{Z} \pmod{p} \right)$, where $p = \text{prime}$ is a field.
Extension Fields

If $D$ is a Euclidean domain, and $p$ is a prime in $D$, then $D \pmod{p}$ is a field.

- $(\mathbb{Z} \pmod{p})$, where $p$ = prime is a field. We call it $\mathbb{Z}_p \equiv F_p \equiv GF(p)$.
- $D = \mathbb{R}[x], p = x^2 + 1$, we have $\mathbb{R}[x] \pmod{x^2 + 1} = \mathbb{C}$, the field of complex numbers.
- $D = \mathbb{Z}_p$ and we take an irreducible polynomial $f(x)$ of degree $m$, irreducible in $\mathbb{Z}_p$, then $\mathbb{Z}_p \pmod{f(x)} = F_{p^m}$ or $GF(p^m)$.
- Consider $GF(p^m)$ as an $m$-dimensional vector space over $GF(p)$.
- Example: $GF(2) \pmod{x^3 + x + 1}$ is $GF(2^3)$.
- Galois Fields are unique up to the labeling of elements.
Field Elements

Consider: $GF(2^3)$ with irreducible polynomial $p(x) = x^3 + x + 1$. Let $A \in F_2[x]$ and compute $A \pmod{p(x)} = a_2x^2 + a_1x + a_0$, where $a_2, a_1, a_0 \in \{0, 1\}$. Let $p(\alpha) = 0$:

- $\langle a_2, a_1, a_0 \rangle = \langle 0, 0, 0 \rangle = 0$
- $\langle a_2, a_1, a_0 \rangle = \langle 0, 0, 1 \rangle = 1$
- $\langle a_2, a_1, a_0 \rangle = \langle 0, 1, 0 \rangle = \alpha$
- $\langle a_2, a_1, a_0 \rangle = \langle 0, 1, 1 \rangle = \alpha + 1$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 0, 0 \rangle = \alpha^2$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 0, 1 \rangle = \alpha^2 + 1$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 1, 0 \rangle = \alpha^2 + \alpha$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 1, 1 \rangle = \alpha^2 + \alpha + 1$
Multiply two elements: \((\alpha^2 + 1)(\alpha^2 + \alpha)\) modulo \(p(x) = \alpha^3 + \alpha + 1\):

\[
(\alpha^2 + 1)(\alpha^2 + \alpha) \\
= \alpha^4 + \alpha^3 + \alpha^2 + \alpha \\
= \alpha(\alpha^3) + \alpha^3 + \alpha^2 + \alpha \\
= \alpha(\alpha + 1) + (\alpha + 1) + \alpha^2 + \alpha \\
= \alpha^2 + \alpha + \alpha + 1 + \alpha^2 + \alpha \\
= \alpha + 1
\]
Mastrovito Multiplier in GF($2^4$)

Input:

\[ A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + a_3 \cdot x^3 \]
\[ B(x) = b_0 + b_1 \cdot x + b_2 \cdot x^2 + b_3 \cdot x^3 \]

Irreducible Polynomial:

\[ P(x) = x^4 + x^3 + 1 \]

Result:

\[ A(x) \times B(x) \pmod{P(x)} \]
Mastrovito Multiplier over GF($2^4$)

<table>
<thead>
<tr>
<th>$\times$</th>
<th>$a_3$</th>
<th>$a_2$</th>
<th>$a_1$</th>
<th>$a_0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b_3$</td>
<td>$a_3 \cdot b_0$</td>
<td>$a_2 \cdot b_0$</td>
<td>$a_1 \cdot b_0$</td>
<td>$a_0 \cdot b_0$</td>
</tr>
<tr>
<td>$b_2$</td>
<td>$a_3 \cdot b_1$</td>
<td>$a_2 \cdot b_1$</td>
<td>$a_1 \cdot b_1$</td>
<td>$a_0 \cdot b_1$</td>
</tr>
<tr>
<td>$b_1$</td>
<td>$a_3 \cdot b_2$</td>
<td>$a_2 \cdot b_2$</td>
<td>$a_1 \cdot b_2$</td>
<td>$a_0 \cdot b_2$</td>
</tr>
<tr>
<td>$b_0$</td>
<td>$a_3 \cdot b_3$</td>
<td>$a_2 \cdot b_3$</td>
<td>$a_1 \cdot b_3$</td>
<td>$a_0 \cdot b_3$</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>$s_6$</td>
<td>$s_5$</td>
<td>$s_4$</td>
<td>$s_3$</td>
<td>$s_2$</td>
</tr>
</tbody>
</table>

In polynomial expression:

$$s_0 + s_1 \cdot x + s_2 \cdot x^2 + s_3 \cdot x^3 + s_4 \cdot x^4 + s_5 \cdot x^5 + s_6 \cdot x^6$$
Mastrovito Multiplier over GF(2^4)

<table>
<thead>
<tr>
<th>s_6</th>
<th>s_5</th>
<th>s_4</th>
<th>s_4</th>
<th>s_3</th>
<th>s_2</th>
<th>s_1</th>
<th>s_0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>s_4</td>
<td>0</td>
<td>0</td>
<td>s_4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>s_5</td>
<td></td>
<td></td>
<td>0</td>
<td>s_5</td>
<td>s_5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>s_6</td>
<td>s_6</td>
<td>s_6</td>
<td>s_6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>r_3</td>
<td>r_2</td>
<td>r_1</td>
<td>r_0</td>
<td></td>
</tr>
</tbody>
</table>

Verification Problem is to check if:

\[ A(x) \times B(x) \equiv r_3 x^3 + r_2 x^2 + r_1 x + r_0 \pmod{P(x)} \]?
**Verification Setup**

To model $F \neq G$ as a polynomial over $GF(2^m)$:

$$t(F - G) = 1,$$

where $t$ is a new variable in $GF(2^m)$.

- When $F = G$, $(F - G) = 0$, so $t \cdot 0 = 1$ has no solutions.
- When $F \neq G$, $(F - G) = t^{-1} \neq 0$, $t \cdot t^{-1} = 1$. 
SAT/SMT or Computer Algebra?

Our Problem: Given a set of polynomial equations, do they have a solution?

- If solutions exists: BUG! Otherwise, equivalence is proven.
- SAT/SMT solvers: Search for a solution, solve systems of equations.
- In ECC, $GF(2^m)$, $m = 256$ word-length of operands.
- SAT/SMT is infeasible.
- Our experience: SAT fairs better than SMT for this problem. Can solve $m = 16$ but not $m = 32$.

Use symbolic computer algebra and algebraic geometry to reason whether a given system of polynomials has a solution or not?
Terminology

Let \( k = F_q = GF(q = 2^m) \):

- \( k[x_1, \ldots, x_n] \) denotes the ring of all polynomials with coefficients in \( k \).
- Given a set of polynomial equations:
  - \( f_1, f_2, \ldots, f_s \in k[x_1, \ldots, x_n] \)
  - Find solutions to \( f_1 = f_2 = \cdots = f_s = 0 \)

Variety: Set of ALL solutions to a given system of polynomial equations: \( V(f_1, \ldots, f_s) \)

- In general, variety can be infinite, or finite non-empty set, or empty.
- Is the variety empty, i.e. is \( V(f_1, \ldots, f_s) = \emptyset \)?
Given a field $k$ and $n \in \mathbb{Z}^+$, we define $n$-dimensional affine space over $k$ to be the set:

$$k^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\}$$

In case $k^2 = \mathbb{R}^2$, we get our affine plane.

Let $k$ be a field, and $f_1, \ldots, f_s$ are polynomials in $k[x_1, \ldots, x_n]$. Then we set:

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0, 1 \leq i \leq s\}$$

We call $V(f_1, \ldots, f_s)$ the affine variety defined by the polynomials.

Variety = Set of all solutions to a given set of polynomial equations!
Consider the points \( \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\} \) in \( F_q^n \):

- Any single point is a variety of some polynomial system

- \((a_1, \ldots, a_n)\) is a variety of \(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n\)

- **Finite unions and intersections** of varieties is a variety

  - Let \( V = V(f_1, \ldots, f_s) \) and \( W = V(g_1, \ldots, g_t) \)
  
  - \( V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_t) \)
  
  - \( V \cup W = V(f_ig_j : 1 \leq i \leq s, 1 \leq j \leq t) \)

- \( F_q^n \) is a finite \( n \)-dimensional affine space, so it is also a variety

Variety depends not just on the given system of polynomial equations, but rather on the **ideal** generated by the polynomials.
Ideals

Definition 1 A subset $I \subset R = k[x_1, \ldots, x_n]$ is an ideal if:

- $0 \in I$
- If $f, g \in I$, then $f + g \in I$
- If $f \in I$ and $h \in R$ then $f \cdot h \in I$

Definition 2 Let $f_1, f_2, \ldots, f_s \in k[x_1, \ldots, x_n]$. Let

$$\langle f_1, f_2 \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} f_i h_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}$$

(1)

$$\langle f_1, f_2 \ldots, f_s \rangle = f_1 h_1 + f_2 h_2 + \cdots + f_s h_s$$

(2)

$I = \langle f_1, f_2 \ldots, f_s \rangle$ is an ideal generated by $f_1, \ldots, f_s$ and the polynomials are called the generators.
Variety depends on the Ideal

Let $V(f_1, \ldots, f_s) = (a_1, \ldots, a_n) \in F_q^n$. Consider the ideal $\langle f_1, f_2 \ldots, f_s \rangle$ evaluated at $(a_1, \ldots, a_n)$:

$$\langle f_1, f_2 \ldots, f_s \rangle$$

$$= \left\{ \sum_{i=1}^{s} f_i h_i : h_1, \ldots h_s \in k[x_1, \ldots, x_n] \right\}$$

$$= f_1 h_1 + f_2 h_2 + \cdots + f_s h_s$$

$$= f_1(a_1, \ldots, a_n)h_1 + \cdots + f_s(a_1, \ldots, a_n)h_s$$

$$= 0$$

Any polynomial in the ideal, vanishes at its variety!
Ideals and their Generators

Consider ideal $I \subset F_q[x_1, \ldots, x_n]$:

- Every ideal in $F_q[x_1, \ldots, x_n]$ is finitely generated
- Also true for $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}$, $\mathbb{Z}_p$: Noetherian rings
- An ideal $I$ has many different bases: $I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$
  - Variety depends on the ideal:
    - $V(I) = V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$
  - Remember Gaussian elimination?
- Some generators (basis) are “better” than others: nice properties, easy to solve, easy to reason whether variety is finite, infinite or empty
- Gröbner basis is one such “nice basis”, which helps to reason about varieties!
Ideal-Variety Examples

- \( I_1 = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y] \)
- \( f_1 = x^2 - 4; \ f_2 = y^2 - 1 \)
- \( I_2 = \langle g_1, g_2 \rangle \subset \mathbb{Q}[x, y] \)
- \( g_1 = 2x^2 + 3y^2 - 11; \ g_2 = x^2 - y^2 - 3; \)
- \( g_1 = 2f_1 + 3f_2; \ g_2 = f_1 - f_2; \implies g_1, g_2 \in I_1, \text{ so } I_2 \subseteq I_1. \)
- Similarly, show that \( f_1, f_2 \subseteq I_2 \)
- If \( I_1 \subset I_2, \text{ and } I_2 \subset I_1 \text{ then } I_1 = I_2 \)
- Note \( V(I_1) = V(I_2) = \{(\pm 2, \pm 1)\} \)
Ideal Membership Testing

Definition 3  Let $f, f_1, f_2, \ldots, f_s \in k[x_1, \ldots, x_n]$. Let $I = \langle f_1, f_2, \ldots, f_s \rangle$. If we have:

$$f = \sum_{i=1}^{s} f_i h_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$$

(3)

then we say that $f \in I$ and we can then write $f = f_1 h_1 + \cdots + f_s h_s$. IOW, we ask: Is $f$ a member of the ideal generated by $f_1, \ldots, f_s$? This is ideal membership testing!

- If $f = f_1 h_1 + \cdots + f_s h_s$ then $f \in I$

- Intuitively, this is like dividing $f$ by $f_1, \ldots, f_s$, getting quotients $h_1, \ldots, h_s$ and zero remainder.

- But what if we cannot find such $h_i$ and zero remainder via division? Does that mean $f \notin I$? Not really, as the following example shows...
Ideal Membership Testing

- Example: \( f = x; \ f_1 = x^2; \ f_2 = x^2 - x; \ f = f_1 - f_2 \), so we have \( f \in I = \langle f_1, f_2 \rangle \). However, both \( f_1, f_2 \) cannot divide \( f \), as \( f \) has smaller degree than both \( f_1, f_2 \).

- The above case depicts one of the problems with the given “generators” \( f_1, f_2 \) of \( I \) – i.e. they are not a “good” generating set. Gröbner basis of \( I = \langle f_1, f_2 \rangle = \langle x \rangle \) and \( x \) generates the same ideal and also allows to decide whether or not \( f \) is in \( I \)?

- For univariate polynomial rings: \( I = \langle f_1, \ldots, f_s \rangle = \text{GCD}(f_1, \ldots, f_s) \). Then \( f \in I \iff f = h \cdot \text{GCD}(f_1, \ldots, f_s) \).

- For multivariate polynomials, this is much harder!
Monomial Ordering

In multivariate polynomials, we need to order the monomial terms in some specific order $x^\alpha = (x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n})$:

- **Total order**: One and only one of the following should be true: $x^\alpha > x^\beta$ or $x^\alpha = x^\beta$ or $x^\alpha < x^\beta$.

- $1 < x^\alpha$, $\forall x^\alpha$ ($x^\alpha \neq 1$)

- $x^\alpha < x^\beta \implies x^\alpha \cdot x^\gamma < x^\beta \cdot x^\gamma$.

**Definition 4** Lexicographic order: Let $x_1 > x_2 > \cdots > x_n$ lexicographically. Also let $\alpha = (\alpha_1, \ldots, \alpha_n)$; $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. Then we have:

$$x^\alpha < x^\beta \iff \begin{cases} \text{Starting from the left, the first co-ordinates of } \alpha_i, \beta_i \text{ that are different satisfy } \alpha_i < \beta_i \end{cases}$$

(4)
Ordering Examples

Let $f = 2x^2yz + 3xy^3 - 2x^3$

- **LEX** $x > y > z$: $f = -2x^3 + 2x^2yz + 3xy^3$
- **DEGLEX** $x > y > z$: $f = 2x^2yz + 3xy^3 - 2x^3$
- **DEGREVLEX** $x > y > z$: $f = 3xy^3 + 2x^2yz - 2x^3$

In singular: we declare ordering as:

```
ring r = 0, (x, y, z), lp; //LEX x > y > z
ring r = 0, (x, z, y), Dp; //DEGLEX x > z > y
ring r = 0, (y, z, x), dp; //DEGREVLEX y > z > x
```
Multivariate Division

\[ \frac{-3x + y^2}{x + 2y + 1} \]

\[ -3x^2 + y^2 \ x + 4xy \]

\[ -3x^2 + 3x - 6xy \]

\[ y^2x + 10xy - 3x \]

\[ \ldots \]

\[ \ldots \]

\[ 2y^3 - 19y^2 - 4y + 3 \]

- To divide \( f \) by \( g \), we denote it as \( f \xrightarrow{g} h \).

- where \( h = f - \frac{\text{lt}(f)}{\text{lt}(g)}g \).
**Multivariate Division**

**Definition 5** Let \( f, f_1, \ldots, f_s, h \in k[x_1, \ldots, x_n], f_i \neq 0; \) \( F = \{ f_1, \ldots, f_s \} \).
Then \( f \) reduces to \( h \) modulo \( F \):

\[
f \xrightarrow{F} h
\]

if and only if there exists a sequence of indices \( i_1, i_2, \ldots, i_t \in \{1, \ldots, s\} \)
and a sequence of polynomials \( h_1, \ldots, h_{t-1} \in k[x_1, \ldots, x_n] \) such that

\[
f \xrightarrow{fi_1} h_1 \xrightarrow{fi_2} h_2 \xrightarrow{fi_3} \cdots \xrightarrow{fi_{t-1}} h_{t-1} \xrightarrow{fi_t} h
\]

**Definition 6** If \( f \xrightarrow{F} r \), then no term in \( r \) is divisible by \( LT(f_i), \forall f_i \in F \).
Then \( r \) is reduced w.r.t. \( F \) as is called the remainder.
Definition 7  Let 
\( f, f_1, \ldots, f_s, r \in k[x_1, \ldots, x_n], f_i \neq 0; \quad F = \{f_1, \ldots, f_s\} \). Then \( f \) reduces to \( r \) modulo \( F \):

\[
\begin{align*}
 f & \xrightarrow{F} r \\
 f & = u_1 f_1 + \cdots + u_s f_s + r 
\end{align*}
\]

then we have

- \( r \) is reduced w.r.t. \( F \)
- \( u_1, \ldots, u_s \in k[x_1, \ldots, x_n] \)
- \( \text{LP}(f) = \text{MAX} (\text{LP}(f_1) \text{LP}(u_1), \ldots, \text{LP}(f_s) \text{LP}(u_s), r) \)
Subtleties of the Division Process

Suppose we have: \( f \xrightarrow{F} r \). If \( r = 0 \) then \( f \in I = \langle F \rangle \). But, if \( r \neq 0 \) then we cannot decide ideal membership unequivocally. That’s why we need Groebner Bases.

Let \( f = xy^2 - x; \ f_1 = xy + 1; \ f_2 = y^2 - 1 \). Note that \( f \in I = \langle f_1, f_2 \rangle \) as \( f = xf_2 \).

\[
\begin{align*}
  f \xrightarrow{f_1,f_2} & : f = y \cdot f_1 + 0 \cdot f_2 + (-x - y) \\
  f \xrightarrow{f_2,f_1} & : f = x \cdot f_2 + 0 \cdot f_1 + 0
\end{align*}
\]

Moral of the Story If we change the order in which we divide by \( f_1, \ldots, f_s \), we obtain different quotients and different remainders.
Motivating Gröbner Bases

Let $F = \{f_1, \ldots, f_s\}$; $I = \langle f_1, \ldots, f_s \rangle$ and let $f \in I$. Then we should be able to represent $f = u_1 f_1 + \cdots + u_s f_s + r$ where $r = 0$. If we were to divide $f$ by $F = \{f_1, \ldots, f_s\}$, then we will obtain an intermediate remainder (say, $h$) after every one-step reduction. The leading term of every such remainder ($\text{LT}(h)$) should be divisible by the leading term of at least one of the polynomials in $F$. Only then we will have $r = 0$.

**Definition 8** Let $F = \{f_1, \ldots, f_s\}$; $G = \{g_1, \ldots, g_t\}$; $I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. Then $G$ is a Gröbner Basis of $I$ if

$$\forall f \in I \ (f \neq 0), \ \exists i : \text{LP}(g_i) \mid \text{LP}(f)$$
Gröbner Bases

A set of non-zero polynomials $G = \{g_1, \ldots, g_t\}$ contained in an ideal $I$, is called a Gröbner basis for $I$ if and only if for all $f \in I$ such that $f \neq 0$, there exists $i \in \{1, \ldots, t\}$ such that $lp(g_i)$ divides $lp(f)$.

$$G = \text{GröbnerBasis}(I)$$

$$\iff \forall f \in I : f \neq 0, \exists g_i \in G : lp(g_i) \mid lp(f)$$

- $f \in I \iff f \xrightarrow{G}+ 0$
- $f \in I \iff f = \sum_{i=1}^{t} h_i g_i$, with $lp(f) = \max (lp(h_i)lp(f_i))$
- If $G = \{g_1, \ldots, g_t\} \subseteq I$ is a Gröbner Basis for $I$, then $I = \langle g_1, \ldots, g_t \rangle$
Questions on the Existence of G.B.

- Does a G.B. always exist for any \( I \subset k[x_1, \ldots, x_n] \)?

- Can it always be computed? Uniquely (up to ordering)?

- What about minimality of the G.B.?

- Study properties of a G.B., and derive algorithms to compute it.
S-Polynomials: Motivation

\[ I = < f_1, f_2 >, \ f = h_1 f_1 + h_2 f_2. \]

- If \( \text{LT}(f) \in < \text{LT}(f_1), \text{LT}(f_2) > \), then some \( \text{LP}(f_i) | \text{LP}(f) \)

- But what if \( \text{LT}(f) \notin < \text{LT}(f_1), \text{LT}(f_2) > \)?

\[ S(f, g) = \frac{L}{\text{lt}(f)} \cdot f - \frac{L}{\text{lt}(g)} \cdot g \]

- \( L = \text{LCM} (\text{lp}(f), \text{lp}(g)) \)
Buchberger’s Theorem

Let \( G = \{g_1, \ldots, g_t\} \) be a set of non-zero polynomials in \( k[x_1, \ldots, x_n] \). Then \( G \) is a Grobner basis for the ideal \( I = \langle g_1, \ldots, g_t \rangle \) if and only if for all \( i \neq j \)

\[
S(g_i, g_j) \xrightarrow{G} + 0
\]

The \( S \)-polynomials account for all missing \( \text{LT}(g_i) \)'s for the Grobner basis computation.

Example:

- \( I = \langle yx - y, y^2 - x \rangle \)
- \( GB(I) = \langle yx - y, y^2 - x, x^2 - x \rangle \)
We are given \( I \subset F_1[x_1, \ldots, x_n] \), \( I = \langle f_1, \ldots, f_s \rangle \). We need to find whether or not \( V(I) = \emptyset \)?

- Consider Ideal generated by constant polynomial \( f = 1 \), i.e. \( I = \langle 1 \rangle \).

- \( V(I) = V(f) = V(1) \). Notice \( 1 = 0 \) have no solution, so \( V(I) = \emptyset \)

- Given polynomial system: \( f_1 = f_2 = \cdots = f_s = 0 \)

- Do they have a common zero?

- No common zero \( (V(f_1, \ldots, f_s) = \emptyset) \iff 1 \in \text{G.B.} \)

- But this is true only over algebraically closed fields!
What if $k$ isn’t closed?

- Let $\overline{k}$ be the algebraic closure of $k$.

- Every field $k$ is contained in $\overline{k}$, which is algebraically closed. Every element of $\overline{k}$ is the root of a non-zero $f \in k[x]$.

- Let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$. Denote variety over extension field $V_{\overline{k}}(I) = \{(a_1, \ldots, a_n) \in \overline{k}^n \mid f_i(a_1, \ldots, a_n) = 0\}$.

- Note: Ideal in $k$ and variety in $\overline{k}$.

("Weak" Nullstellensatz) Let $I$ be an ideal in $k[x_1, \ldots, x_n]$. Then $V_{\overline{k}}(I) = \emptyset \iff I = k[x_1, \ldots, x_n] \iff 1 \in GB(I)$. 

- p.33/37
Algebraic Closure over $GF(2^m)$

- Field containment: $GF(2^n) \subset GF(2^m)$ if $n$ divides $m$.
- $GF(2^2) \subset GF(2^4) \subset GF(2^8) \subset \ldots$
- Algebraic closure of $GF(2^m)$ is an infinite field that is the union of all such fields!
- But, we are looking for solutions in $F_q$ not in $\overline{F_q}$!
Solution in $GF(2^m)$

Algebraic Closure of $GF(q)$

Don’t care!

Solution here?
Vanishing Polynomials in GF($q$)

In $F_q[x_1, \ldots, x_n]$:

- $x_i^q = x_i$ in any $GF(q)$.
- $x_i^q - x_i = 0$ in any $GF(q)$.
- $V(x_1^q - x_1, \ldots, x_n^q - x_n) = F_q^n$ the entire affine space!
- $V_{F_q}(I) = V_{F_q}(I) \cap F_q$
- $V_{F_q}(I) = V_{F_q}(I) \cap V(x_1^q - x_1, \ldots, x_n^q - x_n)$

Given ideal $I = \langle f_1, \ldots, f_s \rangle \subset F_q[x_1, \ldots, x_n]$, and $J = \langle x_i^q - x_i \rangle$, $V_{F_q}(I) = \emptyset \iff 1 \in GB(I, J)$.

Problem: When $q = 2^{256}$, we cannot even declare $x^q - x$ as a polynomial.
Our Experience So Far

- When Spec = Implementation, $V_{F_q}(I) = \emptyset$

- When we insert a bug in the design, Gröbner basis computation doesn’t terminate

- Behaviour is complementary to SAT:
  - SAT is harder for “No solution” instance; G.B. is easier
  - SAT can find a solution quickly, if one exists, whereas GB computation takes time

- Use a hybrid SAT/GB approach