Projection of Varieties and Elimination Ideals

Applications: Word-Level Abstraction from Bit-Level Circuits, Combinational Verification, Reverse Engineering Functions from Circuits

Priyank Kalla

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

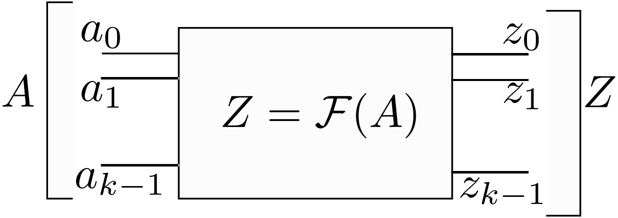
Slides updated Nov 27, 2021

We will employ everything we have learnt so far....

- Hilbert's Nullstellensatz over $\mathbb{F}_q$
- Gröbner basis theory
- Efficient term ordering from circuits
- Canonical representations of circuits $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$ to $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$

And learn a new concept: Elimination ideals

- Apply these techniques to circuit analysis and verification



- Circuit: $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$
- Model it as a polynomial function $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$
- Interpolate a word-level polynomial from the circuit: $Z = \mathcal{F}(A)$
- Obtain $Z = \mathcal{F}(A)$ as a unique, canonical, word-level, polynomial representation from the *bit-level* circuit
- Why do we want to do that?

Hierarchical Abstraction and Verification

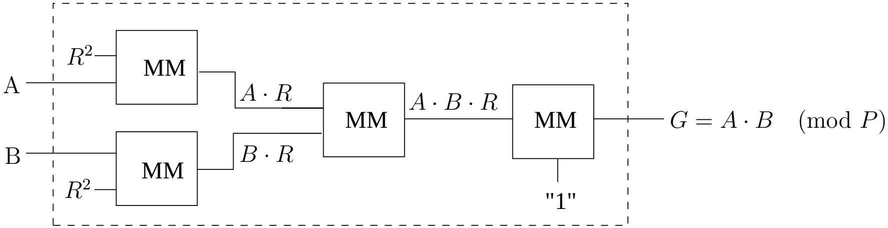
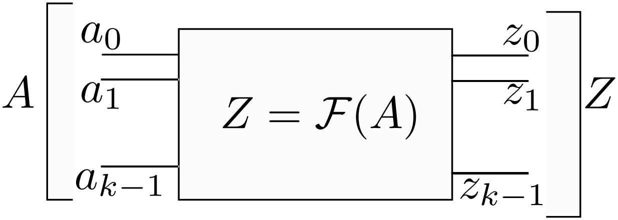


Figure: *Montgomery* multiplier over GF(2^k)

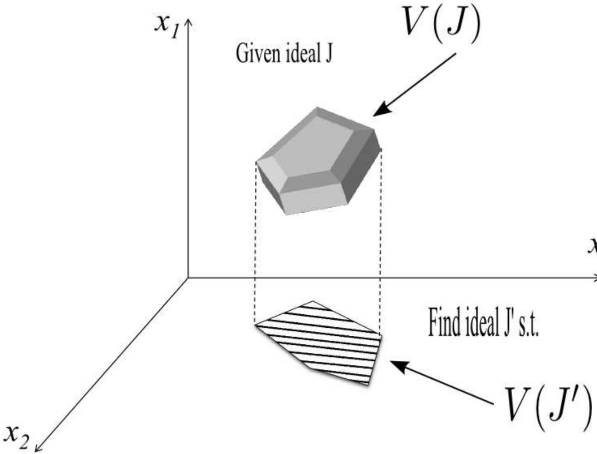
Montgomery Multiply: $F = A \cdot B \cdot R^{-1}$, $R = \alpha^k$

Projection of Variety

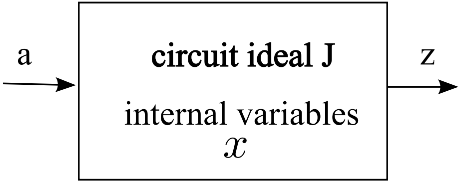


- Represent the polynomials of the circuit as ideal J (or $J + J_0$)
- Consider $V_{\mathbb{F}_q}(J)$
- Let x_i denote the bit-level variables of the circuit: $J \subset \mathbb{F}_q[x_i, Z, A]$
- Project $V_{\mathbb{F}_q}(J)$ on Z, A, denoted by $V_{\mathbb{F}_q}(J)|_{Z,A}$
    - Does this recover the function of the circuit?

Projection of a Variety



Projection on a circuit



$$V(J) = \left\{ \begin{array}{c} (a_0, x_0, z_0) \\ (a_1, x_1, z_1) \\ (a_2, x_2, z_2) \end{array} \right\}$$

Projection of $V(J)$ on (a, z) :

$$\pi_x(V(J)) = V(J)|_{a,z} = \left\{ \begin{array}{c} (a_0, z_0) \\ (a_1, z_1) \\ (a_2, z_2) \end{array} \right\}$$

Projection Map

Definition

Given variety $V = \mathbf{V}(f_1, \dots, f_s) = \mathbf{V}(J) \subset \mathbb{F}_q^n$. The l^{th} projection map $\pi_l : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-l}, \pi_l((c_1, \dots, c_n)) = (c_{l+1}, \dots, c_n)$

- We may also denote π_l by $\text{Proj}[V(J)]_{l+1,\dots,n}$, or by $V(J)|_{l+1,\dots,n}$
- In some sense, we have eliminated the first l variables from the system
- This is related to elimination ideals and variable elimination

Elimination Ideals and Gröbner Bases

Definition (*Elimination Ideal*)

Given $J = \langle f_1, \ldots, f_s \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$, the lth *elimination ideal* J_l is the ideal of $\mathbb{F}_q[x_{l+1}, \ldots, x_n]$ defined by $J_l = J \cap \mathbb{F}_q[x_{l+1}, \ldots, x_n]$.

In other words, the lth elimination ideal does not contain variables $x_1, \ldots, x_l$, nor do the generators of it.

Theorem (*Elimination Theorem*)

Let $J \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be an ideal and let G be a Gröbner basis of J with respect to a lex ordering where $x_1 > x_2 > \cdots > x_n$. Then for every $0 \leq l \leq n$, the set $G_l = G \cap \mathbb{F}_q[x_{l+1}, \ldots, x_n]$ is a Gröbner basis of the lth elimination ideal J_l.

A Gröbner basis example [From Cox/Little/O'Shea]

Solve the system of equations over $\mathbb{C}$:

$$f_1 : x^2 - y - z - 1 = 0$$
$$f_2 : x - y^2 - z - 1 = 0$$
$$f_3 : x - y - z^2 - 1 = 0$$

Gröbner basis G with lex term order $x > y > z$

$$
\begin{aligned}
g_1 &: x - y - z^2 - 1 &= 0\\
g_2 &: y^2 - y - z^2 - z &= 0\\
g_3 &: 2yz^2 - z^4 - z^2 &= 0\\
g_4 &: z^6 - 4z^4 - 4z^3 - z^2 &= 0
\end{aligned}
$$

- $G_1 = G \cap \mathbb{C}[y, z] = \{g_2, g_3, g_4\}$
- $G_2 = G \cap \mathbb{C}[z] = \{g_4\}$
- Is $V(\langle G \rangle) = \emptyset$? No, because $G \neq \{1\}$
- G tells me that $V(\langle G \rangle)$ is finite!
- G is *triangular*: solve g_4 for z, then g_2, g_3 for y, and then g_1 for x

Remember: GB of zero-dimensional ideal?

Theorem

Let $\mathbb{F}$ be any field and $\overline{\mathbb{F}}$ be its closure, and $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis of J. Then:

$$V_{\overline{\mathbb{F}}}(J) = \text{finite} \quad \iff$$

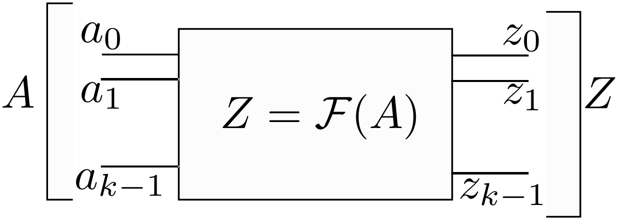
$$\forall x_i \in \{x_1, \ldots, x_n\},\ \exists g_j \in G, s.t. lm(g_j) = x_i^l, \text{for some } \ l \in \mathbb{N}$$

- Also: $J + J_0$ is ZERO dimensional, even though J might not be.

Theorem (Projection & Elimination over $\mathbb{F}_q$)

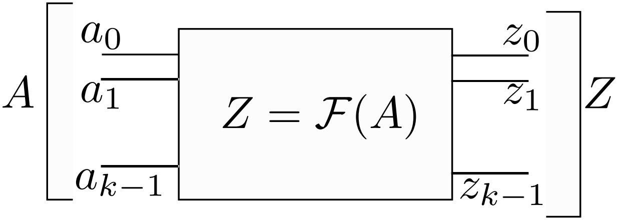
Let $J \in \mathbb{F}_q[x_1, \ldots, x_n]$, $J_0 = \langle x_i^q - x_i : i = 1, \ldots, n \rangle$. Then $Proj(V(J + J_0))|_{x_{l+1}, \ldots, x_n} = V((J + J_0)_l)$.

Abstraction from Circuits

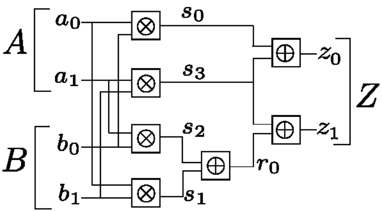


- To obtain, $Z = \mathcal{F}(A)$:
- Denote x_i as bit-level variables, A, Z as word-level variables
- Obtain $J + J_0$ from the circuits
- Compute Gröbner basis G with lex order with $x_i > Z > A$
- G_{x_i} be the elimination ideal that eliminates x_i
- Projection of variety onto Z, A is equal to $V(G_{x_i})$,
- This recovers the function of the circuit $Z = \mathcal{F}(A)$

Abstraction from Circuits



- G is computed with lex $x_i > Z > A$
- There exists a polynomial $A^q - A$ in G
- There exists a polynomial $Z = \mathcal{F}(A)$ in G
  - Why? Can you prove it?
- $Z = \mathcal{F}(A)$ is the unique canonical representation of the circuit. Why?
- The rest is irrelevant for us



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

Add J_0 and compute $GB(J + J_0)$ with $x_i > Z > A > B$, then G :

$g_1 : z_0 + z_1\alpha + Z$; $g_2 : b_0 + b_1\alpha + B$; $g_3 : a_0 + a_1\alpha + A$; $g_4 : s_3 + r_0 + z_1$; $g_5 : s_1 + s_2 + r_0$; $g_6 : s_0 + s_3 + z_0$; $g_7 : Z + AB$; $g_8 : a_1 b_1 + a_1 B + b_1 A + z_1$; $g_9 : r_0 + a_1 b_1 + z_1$; $g_{10} : s_2 + a_1 b_0$

Proof Outline

$Z = \mathcal{F}(A) \in G$ is a canonical representation of the function implemented by the circuit.

- LEX order: $x_i > Z > A$
- Specification polynomial is of the type $f : Z - \mathcal{F}(A)$, i.e. $lm(f) = Z$, and $Z > \mathcal{F}(A)$
- $G = GB(J + J_0) = \{g_1, \ldots, g_t\}$, so $lm(g_i) \mid Z$
- There exists a $g_i = Z + \mathcal{G}(A)$
- Now show that $\mathcal{F}(A) = \mathcal{G}(A) \pmod{A^q - A}$

To Conclude

- Lex orders are elimination orders, but Deglex and DegRevLex are not elimination orders
- Computing GB with Lex orders is hard, gives very large output
- One can use block orders (I will give you a singular file with a block order)
- Projection of varieties can be solved exactly using Elimination ideals over Galois fields, not so over $\mathbb{R}, \mathbb{Q}, \mathbb{C}$