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

Nov 22, 2017 - onwards
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
Polynomial Interpolation from Circuits

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: \( F = A \cdot B \cdot R^{-1}, \quad R = \alpha^k \)
Represent the polynomials of the circuit as ideal $J$ (or $J + J_0$)

Consider $V_{F_q}(J)$

Let $x_i$ denote the bit-level variables of the circuit: $J \subset F_q[x_i, Z, A]$

Project $V_{F_q}(J)$ on $Z, A$, denoted by $V_{F_q}(J)|_{Z,A}$
- Does this recover the function of the circuit?
Projection of a Variety

Given ideal $J$

Find ideal $J'$ s.t.

$V(J)$

$V(J')$
Projection on a circuit

\[ a \longrightarrow \text{circuit ideal } J \longrightarrow z \]

\[ \text{internal variables } x \]

\[ V(J) = \begin{cases} 
(a_0, x_0, z_0) \\
(a_1, x_1, z_1) \\
(a_2, x_2, z_2) 
\end{cases} \]

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

\[ \pi_x(V(J)) = V(J)_{|a,z} = \begin{cases} 
(a_0, z_0) \\
(a_1, z_1) \\
(a_2, z_2) 
\end{cases} \]
Definition

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

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

Given $J = \langle f_1, \ldots, f_s \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$, the $l$th 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 $l$th 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 $l$th 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 $x > y > z$

$$g_1 : x - y - z^2 - 1 = 0$$
$$g_2 : y^2 - y - z^2 - z = 0$$
$$g_3 : 2yz^2 - z^4 - z^2 = 0$$
$$g_4 : z^6 - 4z^4 - 4z^3 - z^2 = 0$$

- $G_1 = G \cap \mathbb{C}[y, z] = \{g_2, g_3, g_4\}$
- $G_2 = G \cap \mathbb{C}[z] = \{g_4\}$
- $G$ is triangular: solve $g_4$ for $z$, then $g_2, g_3$ for $y$, and then $g_1$ for $x$
  - Solutions to $z$ are $0, 1, -1 + \sqrt{2}, -1 - \sqrt{2}$
  - $V(G) = \{(1, 0, 0), (0, 1, 0), (0, 0, 1), (-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}), (-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2})\}$
Projection of Variety and Elimination Ideals

- Using elimination, obtain partial solution to $V(I_l)$, then extend it to $V(I)$, one variable at a time
- However, all partial solutions to $V(I_l)$ may not lift to $V(I)$

Example
Consider $f_1 : xy - 1$, $f_2 : xz - 1$. Eliminate $x$, you get $f_3 : y - z$. All points $(a, a)$ are solutions to $f_3$. All points $(1/a, a, a)$ extend to complete solutions, except $(0, 0)$.

Given $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$, $\pi_l(V(J)) \subset V(J_l)$
In other words, $\text{Proj}[V(J)]_{x_l+1, \ldots, x_n} \subset V(J_l)$

Theorem (Over $\mathbb{F}_q$ Elimination ideals give Projection exactly)

Over Galois fields, $\mathbb{F}_q$, let $J$ be any ideal, and $J_0$ be the ideal of vanishing polynomials. Let $I = J + J_0$. The projection of variety is equal to the variety of the elimination ideal. In other words, $\pi_l(V(I)) = V(I_l)$. 
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 the 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

\[ G \text{ is computed with } \text{lex } x_i > Z > A \]

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

\( g_1 : z_0 + z_1 \alpha + Z; \quad g_2 : b_0 + b_1 \alpha + B; \quad g_3 : a_0 + a_1 \alpha + A; \quad g_4 : s_3 + r_0 + z_1; \quad g_5 : s_1 + s_2 + r_0; \quad g_6 : s_0 + s_3 + z_0; \quad g_7 : Z + AB; \quad g_8 : a_1 b_1 + a_1 B + b_1 A + z_1; \quad g_9 : r_0 + a_1 b_1 + z_1; \quad g_{10} : s_2 + a_1 b_0 \)
$Z = \mathcal{F}(A) \in G$ 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. $\text{lm}(f) = Z$, and $Z > \mathcal{F}(A)$
- $G = GB(J + J_0) = \{g_1, \ldots, g_t\}$, so $\text{lm}(g_i) \mid Z$
- There exists a $g_i = Z + \mathcal{G}(A)$
- Now show that $\mathcal{F}(A) = \mathcal{G}(A) \pmod{A^q - A}$
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 \( \mathbb{R}, \mathbb{Q}, \mathbb{C} \).