Complement set for varieties of ideals with single generator

Xiaojun Sun   Priyank Kalla
Department of Electrical & Computer Engineering
University of Utah, Salt Lake City
{xiaojuns,kalla}@ece.utah.edu

Last Update: Feb 3, 2014

1 Problem description

In our approach, finding the complement set for varieties of ideals is necessary. On polynomial ring $F_q[x]$, ideal J_0 is generated by vanishing polynomial: $J_0 = \langle f_{vanish} \rangle = \langle x^q - x \rangle$, then we call its variety over F_q: $V_{F_q}(J_0)$ the **universal set** because it contains all elements in F_q. Assume we have another ideal $J = \langle g \rangle$ with only 1 generator, the question is, is there any method to find an ideal J' such that

$$V_{F_q}(J') = V_{F_q}(J_0) \setminus V_{F_q}(J) = \overline{V_{F_q}(J)}$$

Example: consider polynomial ring $F_4[x]$, where $\{0, 1, \alpha, 1+\alpha\}$ are all elements in F_4. Consider a set of 2 elements $\{1, \alpha\}$ as the variety of ideal J over F_4: $V_{F_4}(J) = \{1, \alpha\}$, where $J = \langle x^2 + (1+\alpha)x + \alpha \rangle$. J_0 is the ideal generated by vanishing polynomial $J_0 = \langle x^4 - x \rangle$, then its variety over F_4 covers all elements in F_4:

$$V_{F_4}(J_0) = V_{\overline{F_4}}(J_0) = \{0, 1, \alpha, 1+\alpha\}$$

As the definition, the complement set of $V_{F_4}(J)$ is $\overline{V_{F_4}(J)} = \{0, 1+\alpha\}$.
Problem 1: How to find ideal J' such that $V_{F_4}(J') = \overline{V_{F_4}(J)}$?
Problem 2: If $J = \langle f \rangle$ has only one generator (f is univariate polynomial),

does J' also has only one generator? In above example, $J = \langle x^2+(1+\alpha)x+\alpha\rangle$, then $J' = \langle x^2 + (1 + \alpha)x\rangle$.
Problem 3: Please check out our conjecture in following part.

2 A conjecture on ideal quotient

First thing is to define **ideal quotient**.

(**Quotient of Ideals**) If I and J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is the set

$$\{f \in k[x_1, \ldots, x_n] : fg \in I,\ \forall g \in J\}$$

and is called the **ideal quotient** of I by J.

Our conjecture is:
Conjecture If J_0, J are ideals with only one univariate generator polynomial from $F_q[x]$, and $J_0 = \langle x^q - x\rangle$, their varieties over F_q satisfy

$$V_{F_q}(J_0 : J) = V_{F_q}(J_0) \setminus V_{F_q}(J)$$

Our conjecture needs a proof. One guess may help the proof is:
Assume desired ideal $J' = \langle h\rangle$, vanishing polynomial is f (such that $J_0 = \langle f\rangle$), original ideal is $J = \langle g\rangle$. The variety of J' must vanish h, and simultaneously satisfies "vanish J_0 (which means it falls into F_q)" and "NOT vanish J (means disjoint with J)".
From these constrains we guess that

$$h = \frac{f}{g}$$

when $h = 0$, it means $f = 0$ and $g \neq 0$. Furthermore, apply this to example on page 1:

$$h = \frac{f}{g} = \frac{x^4 - x}{x^2 + (1 + \alpha)x + \alpha} = x^2 + (1 + \alpha)x$$

and $V_{F_4}(\langle h\rangle) = \{0, 1 + \alpha\}$ is the complement set of $V_{F_4}(J)$.