Operations on Radical Ideals

November 6, 2017

1 preliminaries

Let $\overline{\mathbb{F}_q}$ be the algebraic closure of $\mathbb{F}_q[x_1, ..x_n]$. Let's consider $J_0 = \langle x_1^q - x_1 .. x_n^q - x_n \rangle$ as the set of all vanishing polynomials over this closure. Any arbitrary ideals $J_1 = \langle f_1, ..., f_s \rangle$ *and* $J_2 = \langle h_1, ..., h_r \rangle$ when coupled with the vanishing polynomials, restrict the solutions to finite fields. The ideals, $J_1 + J_0$ and $J_2 + J_0$ then become radical -

$$J_1 + J_0 = \sqrt{J_1 + J_0}$$
$$J_2 + J_0 = \sqrt{J_2 + J_0}$$

2 Intersection of Radical Ideals

Definition 8 and proposition 9 from Chapter 4 [1] gives us the understanding of ideals with respect to intersection operation for finite fields.

Theorem 2.1. *If J_1 and J_2 are any given ideals in $\mathbb{F}_q[x_1, ..., x_n]$, then $J_1 \cap J_2$ is also an ideal which is defined as the set of polynomials which belong to both J_1 and J_2.*

$$J_1 \cap J_2 = \{g : g \in J_1 \text{ and } g \in J_2\} \tag{1}$$

For any two Radical ideals $J_1 + J_0$ and $J_2 + J_0$, intersection operation is defined as

$$(J_1 + J_0) \cap (J_2 + J_0) = (J_1 \cap J_2) + J_0 \tag{2}$$

Proof. We will prove this theorem by proving the inclusion in both the directions. Let f be any arbitrary polynomial such that

$$f \in (J_1 + J_0) \cap (J_2 + J_0) \tag{3}$$

from (1),

$$f \in J_1 + J_0 \text{ and } f \in J_2 + J_0$$

Let t be an extra variable added to the ring $\mathbb{F}_q[x_1, ..x_n]$ -

$$t.f \in t(J_1 + J_0)\ and\ (1-t)f \in (1-t)(J_2 + J_0)$$
$$f = tf + (1-t)f \in t(J_1 + J_0) + (1-t)(J_2 + J_0)$$
$$f = tf + (1-t)f \in t(J_1) + t(J_0) + J_2 + J_0 - t(J_2) - t(J_0)$$

$$f = tf + (1-t)f \in t(J_1) + (1-t)(J_2) + J_0 \tag{4}$$

From chapter 4, Theorem 11[1], for any two given ideals J_1 and J_2 in $\mathbb{F}_q[x_1, ...x_n]$ -

$$J_1 \cap J_2 = (tJ_1 + (1-t)J_2) \cap \mathbb{F}_q[x_1, ..., x_n] \tag{5}$$

Adding field intersection to equation (4) -

$$f \in ((t(J_1) + (1-t)(J_2)) \cap \mathbb{F}_q[x_1, ..., x_n]) + (J_0 \cap \mathbb{F}_q[x_1, ..., x_n]) \tag{6}$$

From equations (5) and (6) -

$$f \in (J_1 \cap J_2) + J_0 \tag{7}$$

To prove the inclusion in other direction, let's take f to be any arbitrary polynomial such that

$$f \in (J_1 \cap J_2) + J_0 \tag{8}$$

from equations (5) and (6)

$$f \in ((tJ_1 + (1-t)J_2) \cap \mathbb{F}_q[x_1, ..., x_n]) + (J_0 \cap \mathbb{F}_q[x_1, ..., x_n])$$
$$f \in ((tJ_1 + (1-t)J_2) \cap \mathbb{F}_q[x_1, ..., x_n]) + J_0$$

assigning $t = 0$

$$f \in ((0 * J_1 + (1-0)J_2) \cap \mathbb{F}_q[x_1, ..., x_n]) + J_0$$
$$f \in (J_2 \cap \mathbb{F}_q[x_1, ..., x_n]) + J_0$$

From chapter 4, Lemma 10[1] -

$$f \in (J_2 + J_0) \tag{9}$$

assigning $t = 1$

$$f \in ((1 * J_1 + (1-1)J_2) \cap \mathbb{F}_q[x_1, ..., x_n]) + J_0$$
$$f \in (J_1 \cap \mathbb{F}_q[x_1, ..., x_n]) + J_0$$

$$f \in (J_1 + J_0) \tag{10}$$

From theorem 1.1, and using equations (9) and (10)

$$f \in (J_1 + J_0) \cap (J_2 + J_0)$$

□

3 Product of Radical Ideals

Theorem 3.1. *If $J_1 = \langle f_1, ..., f_s \rangle$ and $J_2 = \langle h_1, ..., h_r \rangle$ are any given ideals in $\mathbb{F}_q[x_1, ..., x_n]$, then their product denoted $J_1.J_2$, is defined to be the ideal generated by all polynomials $f.g$ where $f \in J_1$ and $g \in J_2$.*

$$J_1.J_2 = \{f_1h_1 + .. + f_sh_r : f_i \in J_1 \text{ and } h_i \in J_2\}$$

The generators of which are given as

$$J_1.J_2 = \langle f_ih_j : 1 \leq i \leq s, 1 \leq j \leq r \rangle \tag{11}$$

For any two product ideals J_1 and J_2 coupled with vanishing polynomials(radical), the product intersection relation is defined as

$$(J_1.J_2) + J_0 = (J_1 \cap J_2) + J_0$$

Proof. We know that for any two arbitrary ideals J_1 and J_2 -

$$\sqrt{J_1.J_2} = \sqrt{J_1 \cap J_2} \tag{12}$$

To prove the equality, we shall prove the inclusion in both directions. Let f be any arbitrary polynomial such that

$$f \in \sqrt{(J_1.J_2)}$$

Given the generators of f from (11), we can easily see that it is composed of generator sets from both J_1 and J_2, hence

$$f \in \sqrt{J_1} \text{ and } f \in \sqrt{J_2}$$

From the definition of radical ideal, there exists some power of q such that

$$\begin{aligned} f^q \in J_1 \text{ and } f^q &\in J_2 \\ f^q &\in J_1 \cap J_2 \\ f &\in \sqrt{J_1 \cap J_2} \end{aligned}$$

To prove the inclusion in other direction, let's take f to be any arbitrary polynomial such that

$$\begin{aligned} f &\in J_1 \cap J_2 \\ f^q &\in \sqrt{J_1 \cap J_2} \\ f^q \in \sqrt{J_1} \text{ and } f^q &\in \sqrt{J_2} \\ f^{2q} &\in J_1.J_2 \\ f &\in \sqrt{J_1.J_2} \end{aligned}$$

Now over finite fields, equation (12) can be written as -

$$(J_1.J_2) + J_0 = (J_1 \cap J_2) + J_0 \tag{13}$$

Since adding the vanishing polynomials make it radical.

□

References

[1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, 2007.