CONJECTURE 7.1

FLORIAN ENESCU, IRINA ILIOAEA

For a field K and a subset V of K^n, let $\mathcal{I}_K = \{f \in K[x_1, \ldots, x_n] : f(\underline{x}) = 0, \text{ for all } \underline{x} \in V\}$, called the vanishing ideal of V.

If K_i are subfields in K, for $i = 1, \ldots, n$, let $L = \prod_{i=1}^n K_i \subseteq K^n$ and define $V_L(I) = \{\underline{x} \in L : f(\underline{x}) = 0 \text{ for all } f \in I\}$, for I ideal in $K[x_1, \ldots, x_n]$. Below we will use $K_i = \mathbb{F}_2$, $i = 1, \ldots, n$ and abbreviate the notation to $V_{\mathbb{F}_2}(-)$.

Proposition 0.1. *Let $J \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ an ideal and $J_0 = (x_1^2 - x_1, \ldots, x_n^2 - x_n)$ the vanishing ideal. Let $V = V_{\mathbb{F}_q}(J + J_0)$. Then, $\mathcal{I}_{\mathbb{F}_q}(V) = J + J_0$.*

Proof. Note $V_{\mathbb{F}_q}(J + J_0) = V_{\mathbb{F}_2}(J + J_0)$.

Using Theorem 1.7.10 in [1], we have that

$$\mathcal{I}_{\mathbb{F}_q}(V_{\mathbb{F}_q}(J + J_0)) = \mathcal{I}_{\mathbb{F}_q}(V_{\mathbb{F}_2}(J + J_0)) = J + J_0.$$

Therefore, $\mathcal{I}_{\mathbb{F}_q}(V) = J + J_0$. □

Proposition 0.2. *Let V be a variety in $\mathbb{F}_2^n$. Then $\mathcal{I}_{\mathbb{F}_q}(V) = I \cdot \mathbb{F}_q[x_1, \ldots, x_n]$, where $I \subseteq \mathbb{F}_2[x_1, \ldots, x_n]$. Specifically, we have that $I = \bigcap_{a \in V} m_a$, where $m_a = (x_1 - a_1, \ldots, x_n - a_n) \leq \mathbb{F}_2[x_1, \ldots, x_n]$ and $a = (a_1, \ldots, a_n) \in V \subseteq \mathbb{F}_2^n$. Moreover, this ideal I is unique.*

Proof. Since

$$m_a \mathbb{F}_q[x_1, \ldots, x_n] \subseteq \mathcal{I}_{\mathbb{F}_q}(\{a\}),$$

we must have equality because $m_a \mathbb{F}_q[x_1, \ldots, x_n]$ is a maximal ideal.

$$\mathcal{I}_{\mathbb{F}_q}(V) = \bigcap_{a \in V} \mathcal{I}_{\mathbb{F}_q}(\{a\}) = \bigcap_{a \in V} m_a \mathbb{F}_q[x_1, \ldots, x_n] = (\bigcap_{a \in V} m_a)\mathbb{F}_q[x_1, \ldots, x_n],$$

where the last equality from the flatness of $\mathbb{F}_2[x_1, \ldots, x_n] \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$. Hence, $I = \bigcap_{a \in V} m_a \subseteq \mathbb{F}_2[x_1, \ldots, x_n]$.

For the uniqueness, if $I \cdot \mathbb{F}_q[x_1, \ldots, x_n] = I' \cdot \mathbb{F}_q[x_1, \ldots, x_n]$ then $I \cdot \mathbb{F}_q[x_1, \ldots, x_n] \cap \mathbb{F}_2[x_1, \ldots, x_n] = I' \cdot \mathbb{F}_q[x_1, \ldots, x_n] \cap \mathbb{F}_2[x_1, \ldots, x_n]$, where the last equality also follows from the freeness of the extension $\mathbb{F}_2[x_1, \ldots, x_n] \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$.

□

Remark 0.3. If $E_L = I \cdot \mathbb{F}_q[x_1, \ldots, x_n]$, then by Proposition 0.2 we have that

$$I = \bigcap_{a \in V} m_a.$$

In practice, for presenting E_L as coming from the intersection of ideals m_a, one needs to compute the set V. This can be done by solving the polynomial equations generating E_L. The solution set is V.

This remark is useful in understanding Example V.1 from the paper, specifically the part on page 7. In that example, E_L does not appear in an obvious form that matches the form in this remark. However, one can check that the ideal in the paper and the form produced by this remark coincide.

Remark 0.4. Say we have a ring extension $R \subseteq S$ and I_1, I_2 are ideals in R.

It is obvious that $(I_1 \cap I_2)S \subseteq I_1S \cap I_2S$, but when do we have equality? One condition that ensure this is having S flat over R (and equality holds for finitely many ideals, not just two ideals). This happens when S is R-free as a module.

The extension $\mathbb{F}_2[x_1, \ldots, x_n] \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ is such a ring extension.

References

[1] Preslicka, Anthony J., *The Topology and Algebraic Functions on Affine Algebraic Sets Over an Arbitrary Field*, MS Thesis, Georgia State University, 2012, *https* : *//scholarworks.gsu.edu/math_theses/*121