NSERC USRA Report
Summer 2017

Generators of Étale Algebras

Student: Santiago Salazar (santiago.salazar@zoho.com)
Supervisor: Zinovy Reichstein (reichst@math.ubc.ca)

1. Problem

It is known by the primitive element theorem that a separable field extension of finite degree can be generated by a single element. This summer we looked at generating étale algebras over finite fields. Recall that an étale algebra E over a field F is an algebra such that $E = K_1 \times \cdots \times K_r$ where K_i is a separable field extension of F. It is still possible to generate E with a single element when F is an infinite field[1]. Otherwise when F is finite let $F := \mathbb{F}_q$ where q is a prime power and $\mathbb{F}_q$ is the field with q elements. We consider algebras of the form

$$E = \mathbb{F}_{q^{n_1}} \times \mathbb{F}_{q^{n_2}} \times \cdots \mathbb{F}_{q^{n_r}}.$$

It is not true in general that E can be generated by a single element. Thus the question we are interested in is *what is the minimum number of elements that generate E?* After an initial reduction, we are able to provide an explicit answer to this question.

2. Results

Throughout, q is a prime power, $\mathbb{F}_{q^n}$ denotes the field extension with q^n elements of $F = \mathbb{F}_q$, and $(\mathbb{F}_{q^n})^r$ denotes the r-fold Cartesian product of $\mathbb{F}_{q^n}$. Operations in the product are performed component-wise. We first obtain a reduction to the pure case where $E = (\mathbb{F}_{q^n})^r$. The reduction will allow us to factor an algebra in to pure algebras and then solve for the number of generators of each pure algebra independently.

Theorem 2.1. *Suppose $E = E_1 \times \cdots \times E_t$, where each factor is a pure étale $\mathbb{F}_q$-algebra, $E_i = (\mathbb{F}_{q^{n_i}})^{r_i}$, and assume further that $n_1, \ldots, n_t$ are distinct. Then*

$$gen(E) = \max\{gen(E_1), \ldots, gen(E_t)\}$$

.

From here on R_m denotes the ring $\mathbb{F}_q[x_1, \ldots, x_m]$. The following condition comes from the fact that if there exists r coprime ideals $I_i \subset R_m$ satisfying $R_m/I_i \cong \mathbb{F}_{q^n}$, then $(\mathbb{F}_{q^n})^r$ can be generated by m elements.

Theorem 2.2. *Let $E = \mathbb{F}_{q^n} \times \cdots \times \mathbb{F}_{q^n}$ (r times). Then gen(E) is the minimal non-negative integer g such that*

$$r \leqslant \frac{1}{n} \sum_{d|n} \mu(n) q^{\frac{gn}{d}} \ .$$

Here, $\mu(n)$ is the Möbius function.

Theorem 2.2 exactly identifies $\text{gen}(E)$, however it has certain computational drawbacks. One may need to try several values for g and for each attempt it is required to compute a sum over divisors of n. These computations are non-trivial for large n. Theorem 2.3 narrows the search for g to two explicit values.

Theorem 2.3. *Let $E = \mathbb{F}_{q^n} \times \cdots \times \mathbb{F}_{q^n}$ (r times). Then*

$$\lceil \tfrac{1}{n} \log_q(nr) \rceil \leqslant gen(E) \leqslant \lceil \tfrac{1}{n} \log_q(nr) \rceil + 1 \ .$$

We note that both bounds may occur. In particular when $n = 1$ we have that $\text{gen}(E) = \lceil \frac{1}{n} \log_q(nr) \rceil$.

3. Further Comments

Proofs of the theorems have been omitted from this report for brevity. The project was a joint effort between Uriya First, Zinovy Reichstein, and Santiago Salazar. The student would like to thank NSERC for supporting the project as well as Zinovy Reichstein and Uriya First for their mentoring throughout the project.

References

[1] Uriya A. First and Zinovy Reichstein. On the number of generators of an algebra. *Comptes Rendus Mathematique*, 355(1):5–9, 2017;2016;.