Understanding Polynomial Maps over Finite Fields

Giacomo Micheli
University of South Florida

Polynomial maps in Cryptography and Coding Theory

- S-boxes
- Hidden Field Equation cryptosystem
- Reed-Solomon Codes
- Constructions of Locally Recoverable Codes (connections with PIR)
- ...

Polynomial maps over finite fields

Let q be a prime power and $\mathbb{F}_q$ be the finite field of order q. Any map from $\mathbb{F}_q$ to $\mathbb{F}_q$ is actually a polynomial map by Lagrange interpolation:

$$f(x) = \sum_{a \in \mathbb{F}_q} \frac{\prod_{b \in \mathbb{F}_q, b \neq a}(x-b)}{\prod_{b \in \mathbb{F}_q, b \neq a}(a-b)} f(a)$$

So, why do I care about saying "polynomial maps"?

We just saw that restricting to polynomials is no restriction, every map is a polynomial.

So, why do I care about saying “polynomial maps”?

We just saw that restricting to polynomials is no restriction, every map is a polynomial. **In this framework it makes no sense to ask how does a polynomial over a finite field behaves as a map.**

Action of polynomial maps over large finite fields

Let $f \in \mathbb{F}_q[x]$ and consider f as a map over $\mathbb{F}_q$. We want to understand what is the behaviour of f in the regime $q >> \deg(f)$ (for example when looking at a large extension field of $\mathbb{F}_q$).

Action of polynomial maps over large finite fields

Let $f \in \mathbb{F}_q[x]$ and consider f as a map over $\mathbb{F}_q$. We want to understand what is the behaviour of f in the regime $q >> \deg(f)$ (for example when looking at a large extension field of $\mathbb{F}_q$).
For example, you might want to understand when f is a permutation and what is its non-linearity (S-boxes) or you might want to estimate the number of subsets $A \subseteq \mathbb{F}_{q^n}$ such that $|A| = \deg(f)$ and f is constant on A (constructions of locally recoverable codes).

The method

Let $\mathbb{F}_q(t)$ be the field of rational functions over $\mathbb{F}_q$ in the variable t. Let M be the splitting field of $f(X) - t$ over $\mathbb{F}_q(t)$.

The method

Let $\mathbb{F}_q(t)$ be the field of rational functions over $\mathbb{F}_q$ in the variable t. Let M be the splitting field of $f(X) - t$ over $\mathbb{F}_q(t)$. Suppose that M has field of constants $\mathbb{F}_q$.

The method

Let $\mathbb{F}_q(t)$ be the field of rational functions over $\mathbb{F}_q$ in the variable t. Let M be the splitting field of $f(X) - t$ over $\mathbb{F}_q(t)$. Suppose that M has field of constants $\mathbb{F}_q$.
Let G be the Galois group of $f(X) - t$, i.e. $G = \mathrm{Aut}(M/\mathbb{F}_q(t))$.
Notice that G acts on the roots $\{z_1, \dots z_{\deg(f)}\} \subseteq M$ of $f(X) - t$.
Fact: the number of $t_0 \in \mathbb{F}_q$ such that $f(X) - t_0 = \prod_{i=1}^{\ell} p_i(x)$ is "roughly" $(|S|/|G|)q$ where S is the subset of elements of G that have cycle decomposition

$$\underbrace{(- - \cdots -)}_{\deg(p_1(x))}\underbrace{(- - \cdots -)}_{\deg(p_2(x))}\cdots\underbrace{(- - \cdots -)}_{\deg(p_\ell(x))}$$

An example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of t_0's in $\mathbb{F}_q$ for which $f(X)$ has exactly four preimages.

An example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of elements of $\mathbb{F}_q$ for which $f(X)$ has exactly four preimages.

An example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of elements of $\mathbb{F}_q$ for which $f(X)$ has exactly four preimages. Notice that this is the same as the number T of elements $t_0 \in \mathbb{F}_q$ such that $f(X) - t_0$ has four zeroes.

An example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of elements of $\mathbb{F}_q$ for which $f(X)$ has exactly four preimages. Notice that this is the same as the number T of elements $t_0 \in \mathbb{F}_q$ such that $f(X) - t_0$ has four zeroes.

- The first step is to compute $G = \mathrm{Gal}(f(X) - t \mid \mathbb{F}_q(t))$ and verify that the splitting field of $f(X) - t$ has the correct field of constants (this is an easy to address technicality, a generalization of the method works for any field of constants extension). For the sake of simplicity of notation (and also because it is the generic case) we assume $G = S_4$.

An example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of elements of $\mathbb{F}_q$ for which $f(X)$ has exactly four preimages. Notice that this is the same as the number T of elements $t_0 \in \mathbb{F}_q$ such that $f(X) - t_0$ has four zeroes.

- The first step is to compute $G = \mathrm{Gal}(f(X) - t \mid \mathbb{F}_q(t))$ and verify that the splitting field of $f(X) - t$ has the correct field of constants (this is an easy to address technicality, a generalization of the method works for any field of constants extension). For the sake of simplicity of notation (and also because it is the generic case) we assume $G = S_4$.
- It is immediate to see that the number T is the same as the number of t_0's such that $f(X) - t_0 = (X - a)(X - b)(X - c)(X - d)$.

An example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of elements of $\mathbb{F}_q$ for which $f(X)$ has exactly four preimages. Notice that this is the same as the number T of elements $t_0 \in \mathbb{F}_q$ such that $f(X) - t_0$ has four zeroes.

- The first step is to compute $G = \mathrm{Gal}(f(X) - t \mid \mathbb{F}_q(t))$ and verify that the splitting field of $f(X) - t$ has the correct field of constants (this is an easy to address technicality, a generalization of the method works for any field of constants extension). For the sake of simplicity of notation (and also because it is the generic case) we assume $G = S_4$.
- It is immediate to see that the number T is the same as the number of t_0's such that $f(X) - t_0 = (X - a)(X - b)(X - c)(X - d)$.
- The only element of S_4 having 4 fixed points is obviously the identity, so that $|S| = 1$, and therefore the number T of t_0's having 4 preimages is roughly $100003/24 \sim 4166$

Another example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of t_0's in $\mathbb{F}_q$ for which $f(X) - t_0$ has exactly two zeroes.

Another example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of t_0's in $\mathbb{F}_q$ for which $f(X) - t_0$ has exactly two zeroes.

- The first step is to compute $G = \mathrm{Gal}(f(X) - t \mid \mathbb{F}_q(t))$ and verify that the splitting field of $f(X) - t$ has the correct field of constants. We assume $G = S_4$.

Another example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of t_0's in $\mathbb{F}_q$ for which $f(X) - t_0$ has exactly two zeroes.

- The first step is to compute $G = \mathrm{Gal}(f(X) - t \mid \mathbb{F}_q(t))$ and verify that the splitting field of $f(X) - t$ has the correct field of constants. We assume $G = S_4$.
- It is immediate to see that the number T is the same as the number of t_0's such that $f(X) - t_0 = (X - a)(X - b)g(X)$.

Another example

Let $q = 100003$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree 4. For example, we might be interested to understand the number T of t_0's in $\mathbb{F}_q$ for which $f(X) - t_0$ has exactly two zeroes.

- The first step is to compute $G = \mathrm{Gal}(f(X) - t \mid \mathbb{F}_q(t))$ and verify that the splitting field of $f(X) - t$ has the correct field of constants. We assume $G = S_4$.
- It is immediate to see that the number T is the same as the number of t_0's such that $f(X) - t_0 = (X - a)(X - b)g(X)$.
- The elements of S_4 having exactly 2 fixed points are

$$\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$$

so that $|S| = 7$, and therefore the number T of t_0's having exactly 2 preimages is roughly $100003/6 \sim 16667$

An algebraic number theoretical lemma

Lemma

Let $L : K$ be a finite separable extension of function fields, let M be its Galois closure and $G := \mathrm{Gal}(M : K)$ be its Galois group. Let P be a place of K and $\mathcal{Q}$ be the set of places of L lying above P. Let R be a place of M lying above P. Then we have the following:

1. *There is a natural bijection between $\mathcal{Q}$ and the set of orbits of $H := \mathrm{Hom}_K(L, M)$ under the action of the decomposition group $D(R|P) = \{g \in G \mid g(R) = R\}$.*
2. *Let $Q \in \mathcal{Q}$ and let H_Q be the orbit of $D(R|P)$ corresponding to Q. Then $|H_Q| = e(Q|P)f(Q|P)$ where $e(Q|P)$ and $f(Q|P)$ are ramification index and relative degree, respectively.*
3. *The orbit H_Q partitions further under the action of the inertia group $I(R|P)$ into $f(Q|P)$ orbits of size $e(Q|P)$.*

References

- Andrea Ferraguti and Giacomo Micheli. Exceptional Scatteredness in Prime Degree *Journal of Algebra*, 2020.
- Andrea Ferraguti, and Giacomo Micheli. "Full classification of permutation rational functions and complete rational functions of degree three over finite fields." *Designs, Codes and Cryptography* 2020.
- Giacomo Micheli. Constructions of locally recoverable codes which are optimal. *IEEE Transactions on Information Theory*, 2019.
- Giacomo Micheli. On the selection of polynomials for the DLP quasi-polynomial time algorithm for finite fields of small characteristic. *SIAM J. Appl. Algebra Geom.*, 2019.

Thank you!