ON CANONICAL SUBFIELD PRESERVING POLYNOMIALS

GIACOMO MICHELI AND DAVIDE SCHIPANI

Abstract. Explicit monoid structure is provided for the class of canonical subfield preserving polynomials over finite fields. Some classical results and asymptotic estimates will follow as corollaries.

1. Introduction

Let q be a prime power and m a natural number. In [1] the structure of the group consisting of permutation polynomials [3] of $\mathbb{F}_{q^m}$ having coefficients in the base field $\mathbb{F}_q$ was made explicit. We start observing that, if f is a permutation of $\mathbb{F}_{q^m}$ with coefficients in $\mathbb{F}_q$ then

$$f(\mathbb{F}_q) = \mathbb{F}_q \quad \text{and} \quad \forall\, d, s \mid m \qquad f(\mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}) = \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}.$$

Indeed for any integer $s \geq 1$, since f has coefficients in $\mathbb{F}_q$ and $\mathbb{F}_{q^s}$ is a field, we have $f(\mathbb{F}_{q^s}) \subseteq \mathbb{F}_{q^s}$. Being f also a bijection, this is also an equality. The property above follows then directly (see also [1, Lemma 2]).

It is natural now to ask which are the polynomials f, having coefficients in $\mathbb{F}_q$, such that

$$f(\mathbb{F}_q) \subseteq \mathbb{F}_q \quad \text{and} \quad \forall\, d, s \mid m \qquad f(\mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}) \subseteq \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}. \tag{1.1}$$

Let us call T_q^m the set of such polynomials. We remark that this is a monoid under composition and its invertible elements $(T_q^m)^*$ consist of the group of permutation polynomials with coefficients in $\mathbb{F}_q$ mentioned above. In this paper we give the explicit semigroup structure of T_q^m, obtaining the main result of [1] (i.e. the group structure mentioned above) as a corollary. The explicit semigroup structure will allow us to compute the probability that a polynomial chosen uniformly at random having coefficients in $\mathbb{F}_q$ satisfies condition (1.1). This will imply the following remarkable results:

- Given p prime, for q relatively large, the density of T_q^p is approximately zero.
- Given q, for p relatively large prime, the density of T_q^p is approximately one.

2010 *Mathematics Subject Classification.* Primary 11T06,12E05; Secondary 12E20.
Key words and phrases. polynomials, finite fields, subfield preserving, semidirect product, monoid.

- For $q = p$ large prime the density of T_p^p is approximately $1/e$.

Indeed, Theorem 5.3 shows how the asymptotic density intrinsically depends on the ratio between p and q (to be compared with the trivial density in Theorem 5.1 and Corollary 5.2).

2. Preliminary definitions

Definition 2.1. We say $f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ to be *subfield preserving* if

$$f(\mathbb{F}_q) \subseteq \mathbb{F}_q \quad \text{and} \quad \forall\, d, s \mid m \qquad f(\mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}) \subseteq \mathbb{F}_{q^d} \setminus \mathbb{F}_{q^s}. \tag{2.1}$$

Moreover, we will say f to be *q-canonical* if its polynomial representation has coefficients in $\mathbb{F}_q$ (or simply *canonical* when q is understood).

Remark 2.2. One of the reason why we use the term *canonical* to address the property of having coefficients in a subfield is that, under this property, the induced application $\tilde{f}$ of $f(x)$ is always well defined no matter what irreducible polynomial we choose for the representation of the finite field extension $\mathbb{F}_{q^m}$.

Denote by $\mathcal{L}_{\mathbb{F}_{q^m}}$ the set of all subfield preserving polynomials.

Remark 2.3. If we drop the condition on the coefficients, the semigroup structure becomes straightforward:

$$\mathcal{L}_{\mathbb{F}_{q^m}} \cong \bigtimes_{k \mid m} M_{[k\pi(k)]}.$$

with $\pi(k)$ being the number of monic irreducible polynomials of degree k over $\mathbb{F}_q$ and $M_{[n]}$ being the set of all maps from $\{1, \dots, n\}$ to itself.

Remark 2.4. Clearly not all subfield preserving polynomials are canonical, which can also be checked by a cardinality count with the results later in the paper.

In the rest of the paper we will need the following lemma, whose proof can be easily adapted from [1] and [2].

Lemma 2.5. *Let $f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ be a map. Then $f \in \mathbb{F}_q[x]$ if and only if $f \circ \varphi_q = \varphi_q \circ f$ where $\varphi_q(x) = x^q$.*

Indeed the set of functions we are looking at consists of $T_q^m = \mathcal{L}_{\mathbb{F}_{q^m}} \cap \mathcal{C}_{\varphi_q}$ where $\mathcal{C}_{\varphi_q} := \{f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \mid f \circ \varphi_q = \varphi_q \circ f\}$.

3. Combinatorial underpinning

Let S be a finite set and $\psi : S \to S$ a bijection. For any $T \subseteq S$, let

$$\mathcal{K}_\psi(T) := \{f : T \to T \mid \forall x \in T \quad f \circ \psi(x) = \psi \circ f(x)\}.$$

For any partition $\mathcal{P}$ of S into sets P_k, let

$$M_S(\mathcal{P}) := \{f : S \to S \mid \forall\ k \quad f(P_k) \subseteq P_k\}.$$

When $\mathcal{P} = \{S\}$ is the trivial partition, we will denote $M_S(\{S\}) = M_S$ namely the monoid of applications from S to itself.

For any bijection $\phi : S \to S$, define ϕ_k for any k as the composition of the cycles of ϕ of length k, and set $\phi_k = (\emptyset)$ if ϕ has no cycles of length k. Let W denote the set $\{1, \dots, |S|\}$, then $\phi = \prod_{k \in W, \phi_k \neq (\emptyset)} \phi_k$. If $\mathrm{supp}(\phi_k)$ denotes the set of elements moved by ϕ_k, then ϕ induces a partition $\mathcal{P}_\phi$ on $S = \bigcup_{k \in W} S_k$, with $S_k = \mathrm{supp}(\phi_k)$, for $k \geq 2$, and S_1 being the set of fixed points of ϕ.

Lemma 3.1.

$$M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S) \cong \bigtimes_{k \in W, \phi_k \neq (\emptyset)} \mathcal{K}_{\phi_k}(S_k)$$

Proof. Clearly any $f \in \mathcal{K}_{\phi_k}(S_k)$ can be extended to S as the identity and then the extension $\bar{f}$ belongs to $\mathcal{K}_\phi(S) \cap M_S(\mathcal{P}_\phi)$. Indeed we have a natural injection

$$\bigtimes_{k \in W, \phi_k \neq (\emptyset)} \mathcal{K}_{\phi_k}(S_k) \hookrightarrow M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S).$$

This is also a surjection: in fact let $f \in M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S)$ and define

$$f_k(x) := \begin{cases} f(x) & \text{if } x \in S_k, \\ x & \text{otherwise.} \end{cases}$$

Since $M_S(\mathcal{P}_\phi) \cap \mathcal{K}_\phi(S) \subseteq M_S(\mathcal{P}_\phi)$, then $f_k(S_k) \subseteq S_k$ which implies

$$f_k\big|_{S_k} \in \mathcal{K}_{\phi_k}(S_k).$$

As the S_k form a partition, the composition of all the f_k coincides with f. □

Now, for $n, k \in \mathbb{N}$ let U_n^k be a set with kn elements and ψ a bijection of U_n^k having n cycles of length k. Let us put indeces on the elements of the set in the following way: let a_{ij} be the j-th element of the i-th cycle, with $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, k\}$.

Let $[h]$ denote $\{1, \dots, h\}$ for a natural number h. We say $\lambda : [h] \to [h]$ to be a cyclic shift of $[h]$ if $\lambda(j + \ell) = \lambda(j) + \ell$ modulo h for any $j, \ell \in [h]$.

Let $\gamma_1, \dots, \gamma_n$ be cyclic shifts of $[k]$ and $\sigma : [n] \to [n]$ a map. We construct then $f_\sigma^\gamma : U_n^k \to U_n^k$ as follows:

$$f_\sigma^\gamma(a_{ij}) := a_{\sigma(i)\gamma_i(j)}.$$

Theorem 3.2. *$g \in \mathcal{K}_\psi(U_n^k) \iff \exists\ \gamma := (\gamma_1, \dots, \gamma_n)$, γ_i cyclic shifts of $[k]$, and $\exists\ \sigma : [n] \to [n]$ map such that $g = f_\sigma^\gamma$.*

Proof. Suppose first $g \in \mathcal{K}_\psi(U_n^k)$. Then

$$g(a_{ij}) = g(\psi^{j-1}(a_{i1})) = \psi^{j-1}(g(a_{i1})).$$

Define $\sigma(i) := [g(a_{i1})]_1$ and $\gamma_i(j) := [g(a_{ij})]_2$, where the subscripts $[x]_1$ and $[x]_2$ refer to the two indeces of $x \in U_n^k$ in the representation a_{ij} above.

Observe that for all $i \in [n]$, γ_i is a cyclic shift, indeed it holds modulo k:

$$\gamma_i(j+\ell) = [g(a_{i\ j+\ell})]_2 = [g(\psi^\ell(a_{ij}))]_2 =$$

$$[\psi^\ell(g(a_{ij}))]_2 = [g(a_{ij})]_2 + \ell = \gamma_i(j) + \ell.$$

Moreover remark that

$$g(a_{ij}) = g(\psi^{j-1}(a_{i1})) = \psi^{j-1}(g(a_{i1})) = \psi^{j-1}(a_{\sigma(i)\gamma_i(1)}) =$$

$$a_{\sigma(i)\ \gamma_i(1)+j-1} = a_{\sigma(i)\gamma_i(j)} = f_\sigma^\gamma(a_{ij}).$$

Let us prove now the other implication:

$$\psi(f_\sigma^\gamma(a_{ij})) = \psi(a_{\sigma(i)\gamma_i(j)}) = a_{\sigma(i)\ \gamma_i(j)+1} =$$

$$a_{\sigma(i)\gamma_i(j+1)} = f_\sigma^\gamma(a_{i\ j+1}) = f_\sigma^\gamma(\psi(a_{ij}))$$

for all $i \in [n]$ and $j \in [k]$. □

3.1. **Semidirect product of monoids.** We now recall the definition of semidirect product of monoids

Definition 3.3. Let M, N be monoids and let $\Gamma : M \to \mathrm{End}(N)$ with $m \mapsto \Gamma_m$ be an antihomomorphism of monoids (i.e. $\Gamma_{m_1 m_2} = \Gamma_{m_2} \circ \Gamma_{m_1}$). We define $M \ltimes_\Gamma N$ as the monoid having support $M \times N$ and operation $*$ defined by the formula

$$(m_1, n_1) * (m_2, n_2) = (m_1 m_2, \Gamma_{m_2}(n_1)\, n_2)$$

Remark 3.4. It is straightforward to verify that the associative property holds.

We will now prove an easy lemma that will be useful in Section 4. For any monoid H let us denote by H^* the group of invertible elements of H.

Lemma 3.5. *Let $M \ltimes G$ be a semidirect product of monoids where G is a group. Then*

$$(M \ltimes G)^* = M^* \ltimes G$$

Proof. The inclusion $(M \ltimes G)^* \subseteq M^* \ltimes G$ is trivial, since if $(m, g) \in (M \ltimes G)^*$ then there exists (m', g') such that

$$(m, g) * (m', g') = (e_1, e_2)$$

so $mm' = e_1$ identity element of M. Let us now prove $(M \ltimes G)^* \supseteq M^* \ltimes G$. Let $(m, g) \in M^* \ltimes G$, then its inverse is $(m^{-1}, \Gamma_{m^{-1}}(g^{-1}))$. □

We are now ready to prove the main proposition of this section as a corollary of Theorem 3.2.

We first observe that the set of cyclic shifts of $[k]$ is clearly isomorphic to C_k, the cyclic group of order k, and each cyclic shift can be identified by its action on 1.

Corollary 3.6.

$$\mathcal{K}_\psi(U_n^k) \cong M_{[n]} \ltimes_\Gamma C_k^n$$

where Γ si defined by

$$\Gamma(\sigma)(\gamma) := \Gamma_\sigma(\gamma) := \gamma_\sigma := (\gamma_{\sigma(1)}, \ldots, \gamma_{\sigma(n)})$$

for any $\gamma \in C_k^n$.

Proof. The reader should first observe

$$\Gamma_\mu(\gamma_{\sigma(1)}, \ldots, \gamma_{\sigma(n)}) = \big(\gamma_{\sigma(\mu(1))}, \ldots, \gamma_{\sigma(\mu(i))}, \ldots, \gamma_{\sigma(\mu(n))}\big)$$

for any $\sigma, \mu \in M_{[n]}$. This can be easily seen by denoting $\gamma_{\sigma(i)} =: g_i$. Therefore, Γ is an antihomomorphism, as we wanted:

$$\Gamma(\sigma\mu)(\gamma) = \gamma_{\sigma\mu} = \big(\gamma_{\sigma(\mu(1))}, \ldots, \gamma_{\sigma(\mu(i))}, \ldots, \gamma_{\sigma(\mu(n))}\big) =$$
$$\Gamma_\mu(\gamma_{\sigma(1)}, \ldots, \gamma_{\sigma(n)}) = \Gamma_\mu \circ \Gamma_\sigma(\gamma).$$

Let

$$\Delta : M_{[n]} \ltimes C_k^n \longrightarrow \mathcal{K}_\psi(U_n^k)$$
$$(\sigma, \gamma) \mapsto f_\sigma^\gamma.$$

Δ is clearly a bijection by Theorem 3.2. It is also an automorphism since

$$\Delta((\overline{\sigma}, \overline{\gamma}) * (\sigma, \gamma))(a_{i,j}) = \Delta(\overline{\sigma}\sigma, \overline{\gamma}_\sigma \gamma)(a_{i,j}) = f_{\overline{\sigma}\sigma}^{\overline{\gamma}_\sigma \gamma}(a_{i,j}) =$$
$$a_{\overline{\sigma}\sigma(i), \overline{\gamma}_{\sigma(i)}\gamma_i(j)} = f_{\overline{\sigma}}^{\overline{\gamma}}(a_{\sigma(i), \gamma_i(j)}) = f_{\overline{\sigma}}^{\overline{\gamma}} \circ f_\sigma^\gamma(a_{i,j}) =$$
$$\big(\Delta(\overline{\sigma}, \overline{\gamma}) \circ \Delta(\sigma, \gamma)\big)(a_{i,j})$$

for all $i \in [n]$ and all $j \in [k]$. □

4. Semigroup structure of T_q^m

Consider now T_q^m and notice that, since $M_{\mathbb{F}_{q^m}}(\mathcal{P}_{\varphi_q}) = \mathcal{L}_{\mathbb{F}_{q^m}}$ and $\mathcal{K}_{\varphi_q}(\mathbb{F}_{q^m}) = \mathcal{C}_{\varphi_q}$, then we have

$$T_q^m = \mathcal{L}_{\mathbb{F}_{q^m}} \cap \mathcal{C}_{\varphi_q} = M_{\mathbb{F}_{q^m}}(\mathcal{P}_{\varphi_q}) \cap \mathcal{K}_{\varphi_q}(\mathbb{F}_{q^m}). \tag{4.1}$$

Indeed the condition

$$f(S_k) \subseteq S_k$$

for each S_k in the partition induced by φ_q is equivalent to the subfield preserving requirement (2.1), being

$$S_1 = \mathbb{F}_q \quad \text{and} \quad S_k = \bigcap_{a|k,\, a\neq k} \left(\mathbb{F}_{q^k} \setminus \mathbb{F}_{q^a}\right) \quad \text{for } k \geq 2.$$

Any element α in a cycle of length d is associated to the irreducible polynomial $\prod_{i=0}^{d-1} (x - \alpha^{q^i}) \in \mathbb{F}_q[x]$, so there is a bijection between the cycles of φ_q of length d and the monic irreducible polynomials of degree d over $\mathbb{F}_q$, whose cardinality is

$$\pi(d) = \frac{1}{d} \sum_{j\,|d} \mu(d/j) q^j$$

with μ being the Moebius function. Now, write

$$\varphi_q = \prod_{k\,|\,m} \phi_k$$

similarly as above with $\phi = \varphi_q$ and label the elements of the finite field as follow: $a_{i,j}^{(k)}$ is the j-th element living in the i-th k-cycle.

Example 4.1. Let $\mathbb{F}_{2^2} = \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$ consisting of $\{0, 1, \alpha, \alpha + 1\}$. Indeed

$$\varphi_q = \phi_1 \phi_2 = (0)(1)(\alpha, \alpha + 1)$$

and then $a_{1,1}^{(1)} = 0$, $a_{2,1}^{(1)} = 1$, $a_{1,1}^{(2)} = \alpha$ and $a_{1,2}^{(2)} = \alpha + 1$.

Theorem 4.2.

$$T_q^m \cong \bigtimes_{k|m} M_{[\pi(k)]} \ltimes C_k^{\pi(k)} \tag{4.2}$$

Proof. It follows from Lemma 3.1 and Corollary 3.6 using the partition induced by the Frobenius morphism. Indeed, using equation 4.1 and Lemma 3.1 we get

$$T_q^m \cong \bigtimes_{k\in W, \phi_k \neq (\emptyset)} \mathcal{K}_{\phi_k}(S_k).$$

Using now Corollary 3.6 we get

$$T_q^m \cong \bigtimes_{k|m} M_{[\pi(k)]} \ltimes C_k^{\pi(k)}.$$

More explicitely, the action of $t \in \bigtimes_{k|m} M_{[\pi(k)]} \ltimes C_k^{\pi(k)}$ on an element $a_{i,j}^{(k)} \in S_k \subseteq \mathbb{F}_{q^m}$ is given by

$$t(a_{i,j}^{(k)}) = (\sigma^{(k)}, \gamma^{(k)})(a_{i,j}^{(k)}) = f_{\sigma^{(k)}}^{\gamma^{(k)}}(a_{i,j}^{(k)}) = a_{\sigma^{(k)}(i),\gamma_i^{(k)}(j)}^{(k)}$$

where $\gamma^{(k)}$ and $\sigma^{(k)}$ are the components indexed by k. □

Corollary 4.3.

$$(T_q^m)^* \cong \bigtimes_{k|m} \mathcal{S}_{\pi(k)} \ltimes C_k^{\pi(k)}$$

where $\mathcal{S}_{\pi(k)}$ is the permutation group of $\pi(k)$ elements.

Proof. Observe that

$$(T_q^m)^* \cong \bigtimes_{k|m} (M_{[\pi(k)]} \ltimes C_k^{\pi(k)})^*$$

holds trivially. Applying now Lemma 3.5 yields

$$(T_q^m)^* \cong \bigtimes_{k|m} (M_{[\pi(k)]} \ltimes C_k^{\pi(k)})^* \cong \bigtimes_{k|m} \mathcal{S}_{\pi(k)} \ltimes C_k^{\pi(k)}.$$

□

Corollary 4.4.

$$|T_q^m| = \prod_{k\,|m} k^{\pi(k)} \pi(k)^{\pi(k)}$$

$$|(T_q^m)^*| = \prod_{k\,|m} k^{\pi(k)} \pi(k)!$$

Remark 4.5. Corollary 4.3 corresponds to [1, Theorem 2] and Corollary 4.4 generalizes the corollary of [1, Theorem 2].

Remark 4.6. Let us observe that a simpler construction as a direct product for $(T_q^m)^*$ can also be seen as follows:

- First notice that any permutation polynomial over $\mathbb{F}_q$ can be extended to a permutation polynomial over $\mathbb{F}_{q^m}$ with coefficients in $\mathbb{F}_q$ by simply defining it as the identity function on $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$ and Lagrange interpolating over the whole field. The produced permutation polynomial over $\mathbb{F}_{q^m}$ has coefficients in $\mathbb{F}_q$, since it commutes with φ_q, which is easily checked by looking at the base field and the rest separately.
- $(T_q^m)^*$ has then a normal subgroup isomorphic to $\mathcal{S}_q$ consisting of

$$\{s \in (T_q^m)^* \mid s \text{ is the identity on } \mathbb{F}_{q^m} \setminus \mathbb{F}_q\}.$$

- Let
$$H_q^m := \{h \in (T_q^m)^* \mid h \text{ is the identity on } \mathbb{F}_q\}.$$
H_q^m is also normal in $(T_q^m)^*$.
- $\mathcal{S}_q \times H_q^m = (T_q^m)^*$. Indeed note first that $H_q^m \cap \mathcal{S}_q = 1$. Now given $f \in (T_q^m)^*$ we have to prove that it can be written as a composition of an element of H_q^m and an element of $\mathcal{S}_q$. Let $s_2 \in \mathcal{S}_q$ such that s_2 restricted to $\mathbb{F}_q$ is f. Let $s_1 \in \mathcal{S}_q$ such that s_1 restricted to $\mathbb{F}_q$ is the inverse permutation of the restriction of f to $\mathbb{F}_q$. In other words $f \circ s_1$ restricted to $\mathbb{F}_q$ is the identity. Observe then that, since $f \circ s_1$ has also coefficients in $\mathbb{F}_q$, it lives in H_q^m. Verify that $s_2 \circ f \circ s_1 = f$. And so we have written f as a composition of an element of $\mathcal{S}_q$ and an element of H_q^m.

5. Asymptotic density of T_q^m

Let us first compute the asymptotic density of the group of permutation polynomials described in [1] inside the whole group of permutation polynomials, and inside the monoid of the polynomial functions having coefficients in the subfield $\mathbb{F}_q$. We will restrict to the case $\mathbb{F}_{q^p}$, p prime.

Theorem 5.1. *Consider an element of $\mathbb{F}_q[x]/(x^{q^p} - x)$ chosen uniformly at random. The probability that this is a permutation polynomial tends to 0 as p and/or q tends to ∞.*

Proof. Given Corollary 4.4, we need to consider
$$L := \lim_{p \vee q \to \infty} \frac{q!(p)^{\frac{q^p - q}{p}} (\frac{q^p - q}{p})!}{q^{q^p}}.$$
By Stirling approximation this is
$$L = \lim_{p \vee q \to \infty} \frac{q!(p)^{\frac{q^p - q}{p}} (\frac{q^p - q}{pe})^{\frac{q^p - q}{p}} \sqrt{2\pi \frac{q^p - q}{p}}}{q^{q^p}}.$$
Now notice that
$$\lim_{p \vee q \to \infty} \left(\frac{q^p - q}{q^p}\right)^{\frac{q^p - q}{p}} = \lim_{p \vee q \to \infty} \left(1 - \frac{1}{q^{p-1}}\right)^{q^{p-1} \cdot \frac{q - q^{2-p}}{p}}$$
By the continuity of the exponential function, this can be written as
$$\lim_{p \vee q \to \infty} e^{\frac{q - q^{2-p}}{p} \ln\left(1 - \frac{1}{q^{p-1}}\right)^{q^{p-1}}} = e^{-\lim_{p \vee q \to \infty} \frac{q}{p}}$$
so that
$$L = \lim_{p \vee q \to \infty} \frac{q!(q^p)^{\frac{q^p - q}{p}} e^{-\frac{q}{p}} \sqrt{2\pi \frac{q^p - q}{p}}}{q^{q^p} e^{\frac{q^p - q}{p}}}.$$

$$= \lim_{p \vee q \to \infty} \frac{q! e^{-\frac{q}{p}} \sqrt{2\pi \frac{q^p - q}{p}}}{q^q e^{\frac{q^p - q}{p}}} = 0,$$

as one can easily see by exploring the cases $q \to \infty$ with Stirling and q fixed. □

By observing that $q^p! > q^{q^p}$ definitively for large p and/or q, we have also the following:

Corollary 5.2. *Consider a permutation of the set $\mathbb{F}_{q^m}$ chosen uniformly at random. The probability that its associated permutation polynomial has coefficients in the subfield $\mathbb{F}_q$ tends to 0 as p and/or q tends to ∞.*

We are now interested in an asymptotic estimate for the density of T_q^p in $\mathbb{F}_q[x]/(x^{q^p} - x)$ for p prime number. We will show in fact that the monoid of canonical subfield preserving polynomials has nontrivial density inside the monoid of polynomial functions having coefficients in the subfield $\mathbb{F}_q$. Given Corollary 4.4, the probability that an element of $\mathbb{F}_q[x]/(x^{q^p} - x)$ chosen uniformly at random is subfield preserving is

$$\frac{|T_q^p|}{q^{q^p}} = \frac{q^q (q^p - q)^{\frac{q^p - q}{p}}}{q^{q^p}}.$$

Theorem 5.3. *Consider an element of $\mathbb{F}_q[x]/(x^{q^p} - x)$ chosen uniformly at random. The probability that this is subfield preserving tends to $e^{-\lim_{p \vee q \to \infty} \frac{q}{p}}$ as p and/or q tends to ∞.*

Proof. We need to consider

$$\ell := \lim_{p \vee q \to \infty} \frac{q^q (q^p - q)^{\frac{q^p - q}{p}}}{q^{q^p}}.$$

With similar arguments as in Theorem 5.1, this transforms to

$$\ell = \lim_{p \vee q \to \infty} \frac{q^q (q^p)^{\frac{q^p - q}{p}}}{q^{q^p}} e^{-\frac{q}{p}} = e^{-\lim_{p \vee q \to \infty} \frac{q}{p}}$$

□

Corollary 5.4.

- $\lim_{p \to \infty} \frac{|T_q^p|}{q^{q^p}} = 1$, *if q is fixed.*
- $\lim_{q \to \infty} \frac{|T_q^p|}{q^{q^p}} = 0$, *if p is fixed.*

Corollary 5.5. *Let $q = p$.*

$$\lim_{p \to \infty} \frac{|T_p^p|}{p^{p^p}} = 1/e$$

Remark 5.6. Clearly all the limits above are computed for p and q running over the natural numbers, but they hold in particular for the subsequences of increasing primes p and possible orders of finite fields q.

6. Example

Let us consider the structure of T_2^2 as an example. Let α be a root of $x^2+x+1=0$, so that $\mathbb{F}_{2^2}=\mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$. It is easy to check that for each polynomial $f\in L$ with

$$L:=\{0,1,x^2+x,x^2+x+1,x^3,x^3+1,x^3+x^2+x,x^3+x^2+x+1\}$$

we have $f(\alpha)\in\mathbb{F}_2$. We know that T_2^2 contains 8 polynomials, so that

$$T_2^2=\frac{\mathbb{F}_2[x]}{(x^4-x)}\setminus L=$$

$$\{x,x+1,x^2,x^2+1,x^3+x^2+1,x^3+x,x^3+x^2,x^3+x+1\}.$$

The structure is $C_2 \bigtimes M_2$.

Indeed $C_1^2\rtimes M_2=M_2$ and consists of

$$\{x,x^2+1,x^3+x^2,x^3+x+1\}$$

that is those functions which fix $\mathbb{F}_4\setminus\mathbb{F}_2$ and act as M_2 on $\mathbb{F}_2$.

Also $C_2\rtimes M_1=C_2$ and consists of

$$\{x,x^2\}$$

that is those functions which fix $\mathbb{F}_2$ and act as C_2 on $\mathbb{F}_4\setminus\mathbb{F}_2$. This is also H_2^2.

7. Conclusions

The set of canonical subfield preserving polynomials has been studied and a monoid structure has been provided via combinatorial arguments (Section 3 and 4) . The density of this set has been addressed yielding curious results at least for the case of prime degree extension (Section 5). A simple example has also been given (Section 6).

Acknowledgements. The first author was supported in part by Swiss National Science Foundation grant number 149716.

References

[1] L. Carlitz, D.R. Hayes, Permutations with coefficients in a subfield, *Acta Arith.*, 21 (1972), 131–135.

[2] Z. Chen, Permutation-type formulas of Frobenius map and their applications, *Ars Combin.*, 39 (1995), 175–181.

[3] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland,

E-mail address: giacomo.micheli@math.uzh.ch

Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland,

E-mail address: davide.schipani@math.uzh.ch