CONSTRUCTIONS OF LOCALLY RECOVERABLE CODES WHICH ARE OPTIMAL

GIACOMO MICHELI

Abstract. We provide a Galois theoretical framework which allows to produce good polynomials for the Tamo and Barg construction of optimal locally recoverable codes (LRC). Our approach allows to prove existence results and to construct new good polynomials, which in turn allows to build new LRCs. The existing theory of good polynomials fits in our new framework.

1. Introduction

Let $n, k, r$ be positive integers. A locally recoverable code (LRC) $C$ having parameters $(n, k, r)$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ of dimension $k$ such that, if one deletes one component of any $v \in C$, this can be recovered by accessing at most $r$ other components of $v$. LRC codes are of great interest in the context of distributed and cloud storage systems. One of the most interesting constructions of LRC is due to Tamo and Barg [7] and is realised via constructing polynomials of degree $r + 1$ which are constants on subsets of $\mathbb{F}_q$ of cardinality $r + 1$. These polynomials are called good polynomials. Construction of good polynomials are also provided in [3]. All these constructions are essentially based on algebraic properties of the base field $\mathbb{F}_q$.

In this paper we fit the theory of good polynomials in a Galois theoretical context, showing that finding polynomials that are good can be reduced to solve a Galois theory problem. Moreover, existing constructions of good polynomials fit completely in our context and can be derived by our main theorems in Section 3.

In addition, using the same method we provide existential results in Subsection 3.1 and explicit new constructions in Subsection 3.2. In Section 4 we put the method in practice constructing good polynomials for many different base fields. All the results

2010 Mathematics Subject Classification. 11T06.
Key words and phrases. Chebotarev Density Theorem; optimal locally recoverable codes; Finite fields; Galois Theory.

The author was supported by the Swiss National Science Foundation grant number 171248.
are based on estimates provided by the Chebotarev Density Theorem for global function fields, which are also supported by the tables in Section 4.

We explain now in a nutshell the key idea of our constructions. We are interested in polynomials $f$ of degree $r + 1$ which are constants on disjoint sets $A_i \subset \mathbb{F}_q$ (i.e. $f(A_i) = \{t_i\}$, for some $t_i \in \mathbb{F}_q$) each of cardinality $r + 1$, for $i \in \{1, \ldots, \ell\}$, for some $\ell \in \mathbb{N}$. One of the tasks is to maximise $\ell$, as this will allow to build many LRC codes, as it is explained in Theorem 2.5 (of course, it is trivial to get $\ell = 1$, as it is enough to take a totally split polynomial). The fundamental observation is that $\ell$ is exactly the number of totally split places of degree 1 of the global function field extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$, where $t$ is transcendental over $\mathbb{F}_q$ and $x$ is a zero of $f - t$ over the algebraic closure of $\mathbb{F}_q(t)$. Now, a place is totally split in $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ if and only if it is totally split in $M_f : \mathbb{F}_q(t)$, where $M_f$ is the Galois closure of the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$. Let $G_f$ be the Galois group of $M_f : \mathbb{F}_q(t)$. By the Chebotarev Density Theorem (and under some additional technical requirements), the number of totally split places is roughly of the size of $(q + 1)/\#G_f$. Therefore, the entire task of finding good polynomials relies on finding polynomials $f \in \mathbb{F}_q[X]$ with minimal Galois group $G_f = \text{Gal}(M_f : \mathbb{F}_q(t))$.

The strength of our method relies on the fact that we do not need to base our constructions on algebraic properties of the base field as in [3, 7] but we extract good polynomials with a density argument. Let us now show with a toy example this fact. Suppose that we want to construct via good polynomials a $(n, k, 2)$-LRC code over an alphabet of size $q$, with $q \equiv 2 \mod 3$ using one of the constructions in [3]. One would need a degree 3 polynomial that is totally split at at least some place $t_0 \in \mathbb{F}_q$. But then this cannot be a composition, as its degree is prime and cannot be a linearised polynomial, as its degree is incompatible with the characteristic. Also, it cannot be a power because $x \mapsto x^3$ is a bijection by the congruence class of $q$ modulo 3, so the constructions in [3] do not apply. Of course, one could get an $(n, k, 2)$-LRC code by extending the base field to $\mathbb{F}_{q^2}$ (instead of $\mathbb{F}_q$) and using the good polynomial $x^3$. Our approach does not need field extensions: for example Theorem 3.11 always ensures that the existence (and constructibility) of a good polynomial of degree 3 with predictable $\ell$ without increasing the field size. If $F_1$ and $F_2$ are fields contained in a larger field $L$, we denote by $F_1F_2$ their compositum, i.e. the smallest subfield of $L$ containing $F_1$ and $F_2$.

**Notation.** For us, a $(n, k, r)$-LRC code is a subspace of $\mathbb{F}_q^n$ of dimension $k$ with locality $r$, i.e. if a component of a codeword is lost, then it can be recovered by looking at most at $r$ other components. Let $F, K$ be fields. We denote by $F[X]$ the polynomial ring in
the variable $X$ over the field $F$. A field extension $K \subseteq F$ will be denoted by $F : K$ (and not $F/K$, in order not to overlap with other notation) and its degree by $[F : K]$, i.e. the dimension of $F$ as a $K$-vector space. For any $\alpha \in K$ that is not a square, we denote by $\sqrt{\alpha}$ any zero of $X^2 - \alpha$ over the algebraic closure of $F$. Let $p$ be a prime number, $m$ a positive integer, $q = p^m$ and $\mathbb{F}_q$ be the finite field of order $q$. Let $t$ be transcendental over $\mathbb{F}_q$ and $\mathbb{F}_q(t)$ be the rational function field in the variable $t$ over the base field $\mathbb{F}_q$. In this paper we use the notation and terminology of [6], which we briefly recall here. A global function field over its field of constants $\mathbb{F}_q$ is a field extension $F$ over $\mathbb{F}_q$ that is a finite dimensional extension of $\mathbb{F}_q(t)$. For a place $P$ of $F$, we denote by $\mathcal{O}_P$ its valuation ring and say that $P$ has degree 1 if $[\mathcal{O}_P/P : \mathbb{F}_q] = 1$. We will only deal with global function fields, so the term global will mostly be understood.

For a function field $F$ over $\mathbb{F}_q$, we denote by $\mathcal{P}(F)$ (resp. $\mathcal{P}^1(F)$) the set of places (resp. places of degree 1) of $F$. Let $F : K$ be an extension of function fields. Let $P \subseteq K$ be a place of $K$ and $Q \subseteq F$ be a place of $F$. We say that $P$ lies above $Q$ if $P \subseteq Q$. Moreover we denote by $e(Q | P)$ (resp. $f(Q | P)$) the ramification index (resp. the relative degree) of the extension of places $Q | P$. We say that $f \in \mathbb{F}_q[X]$ is a separable polynomial if $f \not\in \mathbb{F}_q[X^p]$, in such a way that $f - t$ is a separable irreducible polynomial over $\mathbb{F}_q(t)$. We denote by $M_f$ the splitting field of $f - t$ over $\mathbb{F}_q(t)$, i.e. the Galois closure of the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$, where $x$ is any of the roots of $f - t$ over the algebraic closure of $\mathbb{F}_q(t)$. We denote by $k_f$ the field of constants of $M_f$, i.e.

$$k_f = \{u \in M_f : u \text{ is algebraic over } \mathbb{F}_q\}.$$  

Notice that $k_f$ in principle might be non trivial (an example is $k_f$ for $f = x^3$ and $q \equiv 2 \mod 3$; in this case $M_f = k_f(t)[x]/(f - t)$ and $k_f = \mathbb{F}_q^2$). Recall that $\mathbb{F}_q(x) \cong \mathbb{F}_q(t)[x]/(f(x) - t)$. Let $G_f$ be the monodromy group of $f$, i.e. the Galois group of the the field extension $M_f : \mathbb{F}_q(t)$. When we refer to the genus $g_f$ of $M_f$ we consider $M_f$ as a function field over its field of constants $k_f$. In all interesting cases we will have $k_f = \mathbb{F}_q$ so this distinction will not affect us. For an element $g \in G_f$ and a place $P \in \mathcal{P}^1(\mathbb{F}_q(t))$ we say that $g$ is a Frobenius for $P$ if there exists a place $R$ lying above $P$ such that $g(R) = R$ and the map $g_R : \mathcal{O}_R/R \to \mathcal{O}_R/R$ acts as $g(y) = y^q$. In particular, we say that the identity is a Frobenius for $P$ if $\mathcal{O}_R/R \cong \mathcal{O}_P/P \cong \mathbb{F}_q$.

In the rest of the paper we will identify the places of degree 1 of $\mathbb{F}_q(t)$ with $\mathbb{F}_q \cup \{\infty\}$. For a finite set $A$, we denote its cardinality by $\#A$. Let us denote the symmetric group of degree $m$ by $S_m$ and the alternating group by $A_m$. Let us denote the multiplicative group $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^*$. We say that a polynomial $f \in \mathbb{F}_q[X]$ is totally split if it factors as a product of $\deg(f)$ distinct linear factors.
2. Locally Recoverable Codes and Good Polynomials

Let us start with the fundamental definition.

Definition 2.1. Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree $r + 1$ and let $\ell$ be a positive integer. Then $f$ is said to be $(r, \ell)$-good if

- $f$ has degree $r + 1$,
- there exist $A_1, \ldots, A_\ell$ distinct subsets of $\mathbb{F}_q$ such that
  - for any $i \in \{1, \ldots, \ell\}$, $f(A_i) = \{t_i\}$ for some $t_i \in \mathbb{F}_q$, i.e. $f$ is constant on $A_i$,
  - $\#A_i = r + 1$,
  - $A_i \cap A_j = \emptyset$ for any $i \neq j$.

We say that the family $\{A_1, \ldots, A_\ell\}$ is a splitting covering for $f$. We say that a polynomial is $r$-good if it has degree $r + 1$ and it is $(r, \ell)$-good for some $\ell > 0$. For simplicity of notation, we allow $\ell$ to be negative or zero, in which case an $(r, \ell)$-good polynomial is simply a polynomial of degree $r + 1$. A polynomial that is not good is a polynomial such that there is no $t_0 \in \mathbb{F}_q$ such that $f(X) - t_0$ splits completely in $\deg(f)$ distinct linear factors.

Remark 2.2. Observe that if a polynomial of degree $r + 1$ is $(r, \ell)$-good, then $\ell$ is at most $\left\lfloor \frac{q}{r+1} \right\rfloor$.

Remark 2.3. Notice that an $(r, \ell)$-good polynomial is also $(r, t)$-good for any $t \leq \ell$, as one can simply drop some of the $A_i$'s.

Let us recall the definition of optimal LRC codes [7]

Definition 2.4. A $(n, k, r)$-LRC code $C$ is said to be optimal if the minimum distance $d$ of $C$ satisfies

$$d = n - k - \left\lceil \frac{k}{r} \right\rceil + 2.$$

In fact it can be proven that $n - k - \left\lceil \frac{k}{r} \right\rceil + 2$ is the maximum distance achievable by any $(n, k, r)$-LRC code [5].

The following result is [7, Construction 1]. We write it in the format of [3, Theorem 4], which is more convenient for our purposes.

Theorem 2.5. Let $r \geq 1$ be a positive integer and $g$ be an $(r, \ell)$-good polynomial over $\mathbb{F}_q$ for the set $A = \bigcup_{i=1}^{\ell} A_i$. Let $t \leq \ell$, $n = (r + 1)\ell$ and $k = rt$. For $a = (a_{i,j}, i =$
0, . . . , r − 1; j = 0, . . . , t − 1) ∈ \mathbb{F}_q^k$, let

\[ f_a(X) = \sum_{i=0}^{r-1} \sum_{j=0}^{t-1} a_{i,j} g(X)^j x^i. \]

Define

\[ C = \{(f_a(x), x \in A) | a \in \mathbb{F}_q^k\}. \]

Then $C$ is an optimal $(n, k, r, \ell)$-LRC code over $\mathbb{F}_q$.

The following is the key observation.

**Remark 2.6.** Let $L_f = \mathbb{F}_q(x)$, where $x$ is any root of $f - t$ in $M_f$. It is easy to see that each of the $A_i$’s corresponds to a totally split place of degree 1 of the extension $L_f : \mathbb{F}_q(t)$: if $f(A_i) = t_i$ for some $t_i \in \mathbb{F}_q$, then the place corresponding to $t_i$ factors as a product of exactly $r + 1$ places of $L_f$, which themselves correspond to the elements of $A_i$.

Clearly, the correspondence between the $A_i$’s and the totally split places of $\mathbb{F}_q(t)$ is injective and simply given by $A_i \mapsto f(A_i) = \{t_i\}$. In addition, the maximum $\ell$ for which $f$ is $(r, \ell)$-good is the number of totally split places in $\mathbb{F}_q(t)$ of the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$. As Theorem 2.5 shows, a large $\ell$ is desirable as for fixed locality $r$ it allows constructions of optimal codes with parameters $(r + 1, \ell, rt, r)$.

**Remark 2.7.** Notice that it is obvious to construct an $(r, 1)$-good polynomial as it is enough to take a totally split polynomial. That allows to construct only one LRC code with parameters $(r + 1, r, r)$. This is the reason why in this paper we include both $r$ and $\ell$ in the notion of “good” polynomial.

### 3. Galois Theory over Global Function Fields and Good Polynomials

We now briefly explain the essence of the method. We start with a polynomial $f$ and we are interested in the number of $t_0$’s in $\mathbb{F}_q$ such that $f - t_0$ splits completely, by Remark 2.6. Let $t$ be transcendental over $\mathbb{F}_q$ and let us consider the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ where $x$ is a root of $f - t$ over the algebraic closure of $\mathbb{F}_q(t)$. The splitting of the places of degree 1 of the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ correspond to the factorization shapes of $f - t_0$, when $t_0 \in \mathbb{F}_q$ varies in $\mathbb{F}_q$. Unfortunately, the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ is not always Galois, but if we take the Galois closure $M_f$ of such extension, we can still extract information about the splitting of the places in $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ by looking at the disjoint cycle decomposition of the elements of the Galois group (this is a classical fact, but see for example [1, Lemma 1] or [4, Theorem 6]): as we are interested in the totally split places, we take the identity.
as element (which has all fixed points). As long as the field of constants $k_f$ of $M_f$ is simply $\mathbb{F}_q$, Chebotarev Density Theorem for function fields applied on the identity (see for example [2]) ensures that the number of totally split places can be precisely estimated by [2, Corollary 1].

The following proposition summarises all the results we need from algebraic number theory in a compact way. We include the proof for completeness.

**Proposition 3.1.** Let $f \in \mathbb{F}_q[X]$ be a separable polynomial. Let $g_f$ be the genus of $M_f$ and let $x$ be a root of $f(X) - t$ in $M_f$.

(i) If the extension field $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ has a totally split place $P$ of degree 1, then $k_f = \mathbb{F}_q$.

(ii) Suppose that $k_f = \mathbb{F}_q$. Let $T^1_{\text{split}}(f)$ be the set of $t_0 \in \mathbb{F}_q$ such that $f - t_0$ factors in $\deg(f)$ distinct linear factors over $\mathbb{F}_q$. Then

$$\frac{q + 1 - 2g_f\sqrt{q}}{\#G_f} - \frac{\# \text{Ram}^1(M_f : \mathbb{F}_q(t))}{2} \leq \frac{#T^1_{\text{split}}(f)}{\#G_f} \leq \frac{(q + 1) + 2g_f\sqrt{q}}{\#G_f},$$

where $\text{Ram}^1(M_f : \mathbb{F}_q(t))$ is the set of ramified places of degree 1 of the extension $M_f : \mathbb{F}_q(t)$.

(iii) Let $C(f)$ be the smallest integer such that

$$\frac{C(f) + 1 - 2g_f\sqrt{C(f)}}{\#G_f} - \frac{\# \text{Ram}^1(M_f : \mathbb{F}_q(t))}{2} > 0.$$

If $q > C(f)$, and $k_f = \mathbb{F}_q$, then $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ has a totally split place.

**Proof.** Let us prove (i). Since $M_f$ is the Galois closure of $\mathbb{F}_q(x) : \mathbb{F}_q(t)$, by [6, Lemma 3.9.5] $P$ is totally split also in $M_f : \mathbb{F}_q(t)$. Let $R \subseteq M_f$ be a place lying above the totally split place $P \in \mathcal{P}^1(\mathbb{F}_q(t))$. Since $P$ is totally split and of degree 1 we have that $[\mathcal{O}_R/R : \mathcal{O}_P/P] = 1$ and then $\mathcal{O}_R/R \cong \mathbb{F}_q$. By [6, Proposition 1.1.5, (c)] we have that $\mathcal{O}_R/R$ contains the field of constants of $M_f$, and in turn $k_f$ cannot be a proper extension of $\mathbb{F}_q$.

Let us now prove (ii). Let $P$ be a place of $\mathbb{F}_q(t)$. Since $M_f$ is a Galois extension of $\mathbb{F}_q(t)$ all places of $M_f$ lying above $P$ have the same relative degree $f(P)$ and ramification index $e(P)$ by [6, Corollary 3.7.2].

**Claim 1.** A place $P$ in $\mathbb{F}_q(t)$ is totally split in $M_f : \mathbb{F}_q(t)$ if and only if it is unramified and the identity is a Frobenius for $P$. 
Proof of claim 1. A place $P$ is totally split if and only if any place $R \subseteq M_f$ lying over $P$ is unramified and $f(P) = 1$, which happens if and only if $P$ is unramified and the identity of $G_f$ acts as a Frobenius for the (trivial) field extension $O_R/R : O_P/P$.

Claim 2. Let $t_0 \in \mathbb{F}_q$. The polynomial $f(X) - t_0 \in \mathbb{F}_q[X]$ splits into $\deg(f)$ distinct linear factors if and only if the place $P_0$ corresponding to $t_0$ in $\mathbb{F}_q(t)$ is totally split in $M_f : \mathbb{F}_q(t)$.

Proof of claim 2. Recall that $x \in M_f$ is a root of $f(X) - t_0$. First observe that the splitting of degree 1 places in the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$ correspond exactly to the factorization of $f(x) - t_0$, for $t_0 \in \mathbb{F}_q$. Since $M_f$ is the Galois closure of the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$, then [6, Lemma 3.9.5.] ensures that $P_0$ is also totally split in $M_f : \mathbb{F}_q(t)$. Viceversa, since ramification and relative degrees are multiplicative in intermediate extensions, it is easy to see that if $P_0$ is totally split in the extension $M_f : \mathbb{F}_q(t)$, then it is also totally split in $\mathbb{F}_q(x) : \mathbb{F}_q(t)$.

Using the claims above and observing that the place at infinity of $\mathbb{F}_q(t)$ is ramified, we reduced the problem to finding all places $P \subset \mathbb{F}_q(t)$ that are totally split in $M_f : \mathbb{F}_q(t)$.

We want to use [2, Corollary 1]. Since in our case $k_f = \mathbb{F}_q$ the field of constants extension is trivial. In the notation of Koster’s corollary we have that $M = M_f$, $N = G_f$, and $\text{Id} \in \overline{F}$. Moreover, we are interested in $\gamma = \text{Id}$, therefore $(P, M_f)(\text{Id}) = \delta_P/e(P)$, where $\delta_P = 1$ if the identity is a Frobenius at $P$ (i.e. $P$ splits into factors of relative degree 1 and multiplicity $e(P)$), and 0 otherwise. Then we have

$$\left| \sum_{P \in \mathbb{P}^1(\mathbb{F}_q(t)/\mathbb{F}_q)} \frac{\delta_P}{e(P)} - \frac{1}{\#G_f}(q + 1) \right| \leq \frac{2}{\#G_f}g_f \sqrt{q},$$

Splitting the sum for ramified and unramified places we get

$$\left| \sum_{P \in \text{Ram}^1(M_f, \mathbb{F}_q(t)) \atop \text{Id is a Frobenius at } P} \frac{1}{e(P)} + \sum_{\text{unramified } P \in \mathbb{P}^1(\mathbb{F}_q(t)/\mathbb{F}_q) \atop \text{Id is a Frobenius at } P} 1 - \frac{1}{\#G_f}(q + 1) \right| \leq \frac{2}{\#G_f}g_f \sqrt{q}.$$

Observe now that $e(P) \geq 2$, the place at infinity is ramified, and

$$\#T_{\text{split}}^1(f) = \sum_{\text{unramified } P \in \mathbb{P}^1(\mathbb{F}_q(t)/\mathbb{F}_q) \atop \text{Id is a Frobenius at } P} 1,$$

the final claim follows directly.
The statement in (iii) is immediate by observing that the condition on \( q \) ensures the existence of a totally split place by point (ii).

Point (ii) of the proposition above essentially states a very classical fact from algebraic number theory: since the number of ramified places is bounded by an absolute constant (depending only on the degree of \( f \)) the set of totally split places of a Galois extension of global fields has density \( 1/\#G \) where \( G \) is the Galois group of the extension field. When the global fields are actually global function fields (i.e. finite extensions of \( \mathbb{F}_q(t) \)) the number of degree one totally split places can be estimated as in [2, Corollary 1], leading to the estimate in (ii). The estimate is essentially optimal, as the Riemann Hypothesis for curves over finite fields is proved and is equivalent to the Hasse-Weil bound.

We notice now how \( \# \text{Ram}^1(M_f : \mathbb{F}_q(t)) \) and \( g_f \) can be explicitly bounded by a constant depending on the degree of \( f \) and independent of \( q \).

**Remark 3.2.** Proposition 3.1, point (ii) is in the format of an estimate, but whenever \( g_f \) is zero, it can be used to obtain an exact formula, if in the proof one works out exactly what happens at the ramified places for the quantities \( \delta_P/e(P) \).

**Proposition 3.3.** Let \( f \in \mathbb{F}_q[X] \) be a separable polynomial, \( n = \deg(f) \), and \( g_f \) be the genus of the splitting field \( M_f \) of \( f - t \) over \( \mathbb{F}_q \). Let \( \text{Ram}(M_f : \mathbb{F}_q(t)) \) (resp. \( \text{Ram}^1(M_f : \mathbb{F}_q(t)) \)) be the set of ramified places of \( \mathbb{F}_q(t) \) (resp. ramified places of degree 1) in the field extension \( M_f : \mathbb{F}_q(t) \). Then

(i) \( \# \text{Ram}^1(M_f : \mathbb{F}_q(t)) \leq \# \text{Ram}(M_f : \mathbb{F}_q(t)) \leq n \).

(ii) Suppose that \( \text{char}(\mathbb{F}_q) = p \nmid \#G_f \) and \( k_f = \mathbb{F}_q \). Then \( g_f \leq ((n - 2)\#G_f + 2)/2 \).

**Proof.** In (i), the first inequality is obvious by inclusion of sets. Let \( x \) be a root of \( f(X) - t \) in \( M_f \). The second inequality comes from the fact that a place \( P \) of \( \mathbb{F}_q(t) \) is ramified in the extension \( \mathbb{F}_q(x) : \mathbb{F}_q(t) \) if and only if it is ramified in its Galois closure \( M_f : \mathbb{F}_q(t) \). Therefore, it is enough to look at the zeroes of the derivative of \( f(X) \) to find the ramified places at finite, which are at most \( n - 1 \). The place at infinity is always ramified.

To prove (ii) we want to use Hurwitz genus formula in [6, Corollary 3.4.14]. Since the characteristic is coprime with the degree \( [M_f : \mathbb{F}_q(t)] = \#G_f \) of the extension and since \( e(P) \mid \#G_f \) (because \( M_f \) is a Galois extension of \( \mathbb{F}_q(t) \)), we can use Dedekind Different Theorem in the tamely ramified case [6, Theorem 3.5.1, (b)] obtaining

\[
2g - 2 = -2[M_f : \mathbb{F}_q(t)] + \sum_{P \in \mathbb{P}(\mathbb{F}_q(t))} \sum_{P' \mid P} (e(P' \mid P) - 1) \deg(P')
\]
restricting the outer sum to ramified places and using the trivial estimate \( e(P' \mid P) - 1 \leq e(P' \mid P) \) and the fact that \( \deg(P') = f(P' \mid P) \deg(P) \) we have that

\[
2g - 2 = -2[M_f : \mathbb{F}_q(t)] + \sum_{\text{ramified } P \in \mathcal{P}(\mathbb{F}_q(t))} \deg(P) \sum_{P' \mid P} e(P' \mid P) f(P' \mid P).
\]

Using now the fundamental equality [6, Theorem 3.1.11] we get

\[
2g - 2 = -2[M_f : \mathbb{F}_q(t)] + [M_f : \mathbb{F}_q(t)] \cdot \sum_{\text{ramified } P \in \mathcal{P}(\mathbb{F}_q(t))} \deg(P).
\]

Now, the ramified places at finite correspond to the evaluations of \( f(X) \) at the zeroes of \( f'(X) \). Since \( f'(X) \) has degree \( n - 1 \) and the place at infinity is ramified of degree 1, we have that \( \sum_{\text{ramified } P \in \mathcal{P}(\mathbb{F}_q(t))} \deg(P) \leq n \). The final claim follows immediately.

**Remark 3.4.** The condition \( \text{char}(\mathbb{F}_q) = p \nmid \#G_f \) is purely technical and needed to obtain explicit estimates later on.

3.1. **Existence of good polynomials.** In this section we prove some existential results over base fields which are relatively large compared with the locality parameter \( r \).

**Proposition 3.5.** Let \( r \) be a positive integer and \( q \) be a prime power. Then any separable polynomial of degree \( r + 1 \) over \( \mathbb{F}_q \) such that \( k_f = \mathbb{F}_q \) is at least \((r, \ell)\)-good, with \( \ell \) at least

\[
\frac{(q + 1) - 2g_f \sqrt{q}}{(r + 1)!} - \deg(f)/2.
\]

Moreover, if \( k_f \neq \mathbb{F}_q \) then \( f \) is not a good polynomial.

**Proof.** First observe that \( G_f \) can be seen as a subgroup of the symmetric group \( S_{r+1} \), which forces \( \#G_f \leq (r + 1)! \). The statement follows immediately by applying point (ii) of Proposition 3.1 and bounding \( \#\text{Ram}^1(M_f : \mathbb{F}_q(t)) \) with point (i) of Proposition 3.3. If \( k_f \neq \mathbb{F}_q \), then the statement (i) of Proposition 3.1 applies, so \( f \) cannot have a totally split place and therefore it cannot be \((r + 1, \ell)\)-good for any positive integer \( \ell \).

**Remark 3.6.** The condition \( k_f = \mathbb{F}_q \) is generic, let us briefly sketch the reason here. Let \( M_f = \mathbb{F}_q(t, y) \) by the primitive element theorem, with \( y \) satisfying a degree \([M_f : \mathbb{F}_q]\) polynomial \( F \) over \( \mathbb{F}_q(t) \). We have \( k_f = \mathbb{F}_q \) if and only if \( F \) is irreducible [6, Corollary 3.6.8] and the condition of being irreducible for a bivariate polynomial over a finite field is generic.
Proposition 3.7. Let $B \subseteq \mathbb{F}_q$ be a set of size $r + 1$. Let $r$ be a positive integer such that $\gcd(q, (r+1)!) = 1$ and $f = \prod_{b \in B} (x - b)$. Then $f$ is $(r, \ell)$-good, with $\ell$ at least

$$\frac{q + 1}{(r+1)!} - \left( r - 1 + \frac{2}{(r+1)!} \right) \sqrt{q} - \frac{r + 1}{2}.$$ 

Proof. Clearly $f$ is separable because the characteristic does not divide degree of the polynomial. First using (i) of Proposition 3.1 we get that $k_f = \mathbb{F}_q$, as $t = 0$ is a totally split place. Now using Proposition 3.5 we get that $f$ is at least $(r, \frac{(q+1) - 2g_f \sqrt{q}}{(r+1)!} - \deg(f)/2)$-good. Using now the bound on $g_f$ given by (ii) of Proposition 3.3 we get the wanted result. \qed

Remark 3.8. The proposition above implies that forcing just one totally split place immediately gives the existence of many totally split places, which is an interesting fact. It is worth noticing here that the worst case scenario given in Proposition 3.7 is actually the generic case: if one fixes a random polynomial of degree $n$ in $\mathbb{F}_q[\!\! [X] \!\!]$ and considers $G_f$, then most likely $G_f = S_n$, in which case the estimate for the number of totally split places is given by $q/(n!)$. Table 2b shows some instances of this fact for degree 5.

3.2. Selection of very good polynomials. The method provides existential results and fits the existing literature on good polynomials in a Galois theoretical context, but also allows to produce new good polynomials, which is the most important application. We give emphasize here that we want “very good” polynomials, i.e. $(r, \ell)$-good polynomials such that $\ell$ is as large as possible (we already noticed in Remark 2.7 that building an $r$-good polynomial is a trivial task if $\ell$ is not taken into account). Let us start with the two fundamental and well known constructions

Proposition 3.9. The following are $r$-good polynomials

- Let $r + 1 = m$ be a divisor of $q - 1$. The polynomial $x^m$ is $(r, (q - 1)/r)$-good.
- Let $V$ be an additive subgroup of $\mathbb{F}_q$. The polynomial $\prod_{v \in V} (x - v)$ is $(\#V - 1, q/\#V)$-good.

If one combines the construction above via composition, one can get new good polynomials as described in [7, Theorem 3.3] and [3, Section A,B].

Remark 3.10. All the good polynomials above have in common that $k_f = \mathbb{F}_q$ and $g_f = 0$, so thanks to Remarks 3.2 and 2.6, they fit completely in the easy case (the genus zero condition) of our context. In particular, $k_f = \mathbb{F}_q$ (which is a necessary condition
for a polynomial to be good) exactly when \( m \mid q - 1 \) or the linearised polynomial splits completely over \( \mathbb{F}_q \).

Also, the splitting field of their composition inherits nice properties so the results in [7, Theorem 3.3] and [3, Section A,B] can also be derived from our framework.

For the sake of explanation of our method, let us fit for example the case of \( f = X^m \in \mathbb{F}_q[X] \) in our context. For simplicity, let us assume \( m \geq 3 \). First, observe that such example of good polynomial exists only when \( m \mid q - 1 \), which is exactly the condition needed to have \( k_f = \mathbb{F}_q \): in fact, if \( m \mid q - 1 \) then \( \mathbb{F}_q \) contains a primitive \( m \)-th root of unity and therefore we have that \( M_f = \mathbb{F}_q(t)[x]/(f(x) - t) \) as it is enough to add just one root of \( f - t \) to \( \mathbb{F}_q(t) \) to get all the other roots. Now, \( \mathbb{F}_q(x) = \mathbb{F}_q(t)[x]/(f(x) - t) = M_f \) as \( t \) is just another name for \( f(x) \) so the function field \( \mathbb{F}_q(x) \) is still rational, so \( g_f \) is zero. Trivially \( \#G_f = \left[ M_f : \mathbb{F}_q(t) \right] = m \). In addition \( \text{Ram}^1(M_f : \mathbb{F}_q(t)) = \{ \infty, 0 \} \) so we get

\[
\frac{q + 1}{m} - 1 \leq \#T_{\text{split}}^1(f) \leq \frac{q + 1}{m}.
\]

Since \( \#T_{\text{split}}^1(f) \) has to be an integer and \( m \geq 3 \), we obtain directly that \( \ell = \#T_{\text{split}}^1(f) = (q - 1)/m \). In this case the direct proof is actually easier than the one proposed here, on the other hand it only works thanks to the cyclic group structure of \( \mathbb{F}_q^* \) while our approach works in general, as it is based on a density argument.

**The method.** Constructing good polynomials of given degree using Proposition 3.1 is very simple: the number of \( t_0 \)'s such that \( f - t_0 \) splits into distinct \( \deg(f) \) linear factors can be estimated with \( q/\#G_f \) (as long as \( k_f = \mathbb{F}_q \), otherwise it is the empty set) up to an error term depending on the ramified places of degree 1, and \( g_f \). Informally, to construct an \((r, \ell)-good\) polynomial the task becomes the following: find a transitive subgroup \( G \) of \( S_{r+1} \) such that \( q/\ell \) is roughly of the size of \( G \) and realise \( G \) as \( G_f \) for a family of \( f \)'s. Now sieve the family allowing only polynomials with minimal ramification. We give now simple applications of the method in the case \( r = 2 \) with \( \#G_f = 6 \), in the case \( r = 3 \) with \( \#G_f = 8 \), and \( r = 6 \) with \( \#G_f = 12 \). We want to stress here that these constructions hold for almost all \( q \)'s.

**Theorem 3.11.** Let \( q \) be a prime power, \( b \in \mathbb{F}_q \) and \( f = x(x - 1)(x - b) \in \mathbb{F}_q[X] \). Then

(i) if \( q \) is even then \( f \) is \((2, \ell)-good\) with \( \ell \) at least

\[
\left\lceil \frac{q + 1 - 2\sqrt{q}}{6} - 1 \right\rceil,
\]

(ii) if \( q \) is odd then \( f \) is \((2, \ell)-good\) with \( \ell \) at least

\[
\left\lceil \frac{q + 1}{6} - 1 \right\rceil.
\]
(ii) if \( q = 3^m \), then \( f \) is \((2, \ell)\)-good with \( \ell \) at least
\[
\left\lfloor \frac{q + 1 - 2\sqrt{q}}{6} - 1 \right\rfloor,
\]
Moreover, if \( b = -1 \) then \( f \) is \((2, \ell)\)-good with \( \ell \) at least
\[
\left\lfloor \frac{q + 1 - 2\sqrt{q}}{6} - \frac{1}{2} \right\rfloor,
\]
(iii) if \( q \) is odd such that \( q \mod 3 \neq 0 \), and \( 1-b+b^2 \) is not a square in \( \mathbb{F}_q \), then \( f \) is \((2, \ell)\)-good with \( \ell \) at least
\[
\left\lfloor \frac{q + 1 - 2\sqrt{q}}{6} - \frac{1}{2} \right\rfloor.
\]

Proof. Applying (i) of Proposition 3.1 gives that \( k_f = \mathbb{F}_q \) and therefore we can apply (ii). Clearly \( \#G_f \) is at most 6, as it has to be a subgroup of the symmetric group. \( M_f \) is constructed by simply adding two roots \( \{x_1, x_2\} \) of \( f-t \), since the third one can always be obtained from the other two with field operations. Therefore \( M_f = \mathbb{F}_q(t)(x_1, x_2) = \mathbb{F}_q(x_1, x_2) \) (\( t \) can be obtained by evaluating \( f \) at \( x_1 \) for example), and then \( g_f \leq 1 \) by Riemann’s inequality [6, Corollary 3.11.4] (the minimal polynomial of \( x_1 \) over \( \mathbb{F}_q(x_2) \) has degree at most 2 and viceversa). The ramified places at finite of \( M_f \) are in correspondence with the zeroes of the derivative of \( f \). As usual, the place at infinity is always ramified.

- For even \( q = 2^m \), \( f' = x^2 + b = (x + b^{2^{m-1}})^2 \) so that \( \#\text{Ram}^1(M_f : \mathbb{F}_q(t)) = 2 \).
- For \( q = 3^m \), \( f' = -2(b+1)x + b = (b+1)x + b \), which has either no roots \( (b+1 = 0 \) and \( \#\text{Ram}^1(M_f : \mathbb{F}_q(t)) = 1 \) or one root \( (b+1 \neq 0 \) and \( \#\text{Ram}^1(M_f : \mathbb{F}_q(t)) = 2 \).
- For odd \( q \), \( q \mod 3 \neq 0 \) we have \( f' = 3x^2 - 2(b+1)x + b \), which has no roots exactly when \( b^2 - b + 1 \) is not a square.

Using the formula in (ii) of Proposition 3.1 we get the wanted results.

\[\square\]

Remark 3.12. Notice that the construction is not exploiting the multiplicative nor the additive subgroups of \( \mathbb{F}_q \). With this method we are able for example to write a polynomial of fixed degree (see for example the case of Theorem 3.11) in \( \mathbb{Z}[X] \) that is \((r, \ell(q))\)-good at any \( q \), with \( \ell(q) \) being an explicit constant.

Suppose now that we want to construct a \((n, k, 3)\)-code over an alphabet of size \( q \), with \( q \equiv 3 \mod 4 \). For some \( \ell \) we would need an \((3, \ell)\)-good polynomial \( f \). None of the constructions in [3] apply as we now explain. First of all, observe that \( f \) cannot be a
composition of a non-trivial linearised polynomial and a power function, as its degree is 4 and \( q \) is odd. If \( f \) was a power function, then (up to multiplication by a scalar) \( f = x^4 \), but then \( 4 \nmid q - 1 \) and so \( x^4 - t_0 \) is never totally split for any \( t_0 \in \mathbb{F}_q \). The following result provides a \((r, \ell)\)-good polynomial with \( \ell \) roughly of the size of \([ (q - 1)/8 ] \).

**Theorem 3.13.** Let \( q \geq 5 \) be an odd prime power. Let \( a \in \mathbb{F}_q^* \) and \( f = X^4 + aX^2 \in \mathbb{F}_q[X] \). Then \( \# G_f = 8 \) and

- if \(-a/2 \) is not a square in \( \mathbb{F}_q \), the polynomial \( f \) is \((3, \ell)\)-good with \( \ell \) at least \( \left[ \frac{q + 1}{8} - 1 \right] \),
- if \(-a/2 \) is a square, then \( \ell \) is at least \( \left[ \frac{q + 1}{8} - 2 \right] \).

**Proof.** First we compute the splitting field of \( f - t \). It is clear that

\[
M_f = \mathbb{F}_q \left( t, \sqrt{-a + \sqrt{a^2 + 4t}} \right).
\]

Since \( \sqrt{-a + \sqrt{a^2 + 4t}} \sqrt{-a - \sqrt{a^2 + 4t}} = -t \), then we have that

\[
M_f = \mathbb{F}_q \left( t, \sqrt{t}, \sqrt{-a + \sqrt{a^2 + 4t}} \right).
\]

By the tower law we have that \( \# G_f = [M_f : \mathbb{F}_q(t)] \leq 8 \). In order to show that \([M_f : \mathbb{F}_q(t)] = 8 \) it is enough to show that \( \sqrt{-t} \notin \mathbb{F}_q \left( t, \sqrt{-a + \sqrt{a^2 + 4t}} \right) \). This can happen only when \( \mathbb{F}_q \left( t, \sqrt{-a + \sqrt{a^2 + 4t}} \right) \) is Galois over \( \mathbb{F}_q(t) \), and therefore \([M_f : \mathbb{F}_q(t)] = 4 \). Consider the subfields \( F_1 = \mathbb{F}_q(t, \sqrt{a^2 + 4t}) \) and \( F_2 = \mathbb{F}_q(t, \sqrt{-t}) \). \( F_1 \) and \( F_2 \) are distinct and satisfy \([F_1 : \mathbb{F}_q(t)] = [F_2 : \mathbb{F}_q(t)] = 2 \). By contradiction, let us assume \([M_f : \mathbb{F}_q(t)] = 4 \).

One observes that, since \( F_1 \cap F_2 = \mathbb{F}_q(t) \) then \([F_1F_2 : \mathbb{F}_q(t)] = 4 \), and therefore \( M_f \) can be written as a compositum of \( F_1 \) and \( F_2 \), i.e. \( M_f = F_1F_2 = \mathbb{F}_q \left( t, \sqrt{a^2 + 4t}, \sqrt{-t} \right) \). But one can show directly that \( \frac{-a + \sqrt{a^2 + 4t}}{2} \) is not a square in \( F_1F_2 \), so \( F_1F_2 \) does not contain all the roots of \( f - t \) and therefore cannot be its splitting field.

We now compute \( g_f \) and \( k_f \). For simplicity let us denote \( x = \sqrt{-a + \sqrt{a^2 + 4t}} \) and \( y = \sqrt{-a - \sqrt{a^2 + 4t}} \). One can show that \( M_f = \mathbb{F}_q(t, x, y) \). Also, \( \mathbb{F}_q(t, x, y) = \mathbb{F}_q(x, y) \) since
t can be obtained using only $x$ and elementary $\mathbb{F}_q$-operations that do not involve $t$. The elements $x$ and $y$ verify the equation $x^2 + y^2 + a = 0$, which is a conic so its genus is zero. Another way to see the fact that $g_f = 0$ is to use the inequality in [6, Proposition 3.11.5] on the equation $x^2 + y^2 + a = 0$. Moreover by [6, Corollary 3.6.8], $k_f = \mathbb{F}_q$ because $x^2 + y^2 + a$ is absolutely irreducible if $a \neq 0$.

Let us now compute $\#\text{Ram}^1(M_f : \mathbb{F}_q(t))$. Since the ramified places of degree 1 correspond to the zeroes in $\mathbb{F}_q$ of the derivative of $f$ (the place at infinity is always ramified), it is easy to see that $\text{Ram}^1(M_f : \mathbb{F}_q(t)) = \{\infty, 0\}$ if $-a/2$ is not a square in $\mathbb{F}_q$ and $\text{Ram}^1(M_f : \mathbb{F}_q(t)) = \{\infty, 0, b, -b\}$ otherwise, where $b \in \mathbb{F}_q$ is an element such that $b^2 = -a/2$. A direct application of Proposition 3.9 gives now the wanted result.

\[\square\]

Let us finish with an example of a $(5, \ell)$-good polynomial. Again, let us explain why this is a new example of a good polynomial. Fix the size of the base field to be $q$ and assume that one wants to construct an LRC with locality 5. Suppose that $6 \not| q - 1$ and $q = p^n$ is not divisible by 2 or 3. Then one would need a degree 6 polynomial such that $f - t_0$ is totally split for many $t_0$'s in $\mathbb{F}_q$. But then, none of the constructions in Proposition 3.9 will work, nor compositions of those: in fact $f$ cannot be a composition (possibly trivial) of a $p$-linearised polynomial with a power function for degree reasons, and also cannot be power function because $6 \not| q - 1$, and therefore $x^6$ is not a good polynomial over $\mathbb{F}_q$.

**Theorem 3.14.** Let $q$ be an odd prime power such that $q \not\equiv 0 \mod 2, 3$ and $a \in \mathbb{F}_q^\ast$ such that $a$ is not a square. Let $f = (X^3 - aX)^2 \in \mathbb{F}_q[X]$. Then $\#G_f = 12$ and $f$ is a $(5, \ell)$-good polynomial with $\ell$ at least

$$\left\lceil \frac{q + 1 - 2\sqrt{q}}{12} - 2 \right\rceil.$$  

**Proof.** First, we need to compute $M_f$, the splitting field of $f - t$. Observe that $\sqrt{t} \in M_f$ and that adding $\sqrt{t}$ to $\mathbb{F}_q(t)$ allows the splitting

$$f - t = (X^3 - aX - \sqrt{t})(X^3 - aX + \sqrt{t}).$$

Set $H_1 = X^3 - aX - \sqrt{t}$ and $H_2 = X^3 - aX + \sqrt{t}$. We need now to split $H_1$ over $\mathbb{F}_q(\sqrt{t})$, because in that case also $H_2$ splits as $H_2(X) = -H_1(-X)$. Since $H_1(X)$ is irreducible over $\mathbb{F}_q(\sqrt{t})$, then $N = \text{Gal}(M_f : \mathbb{F}_q(\sqrt{t}))$ is equal to $S_3$ or $A_3$. But since one can check directly that the discriminant $\Delta = 4a^3 - 27t$ of $H_1$ over $\mathbb{F}_q(\sqrt{t})$ is not a square in $\mathbb{F}_q(\sqrt{t})$, then $N \neq A_3$, which forces $N = S_3$ and therefore $[M_f : \mathbb{F}_q(\sqrt{t})] = \#N = 6$. By the
tower law we have
\[# G_f = [M_f : \mathbb{F}_q(t)] = [M_f : \mathbb{F}_q(\sqrt{t})] : [\mathbb{F}_q(\sqrt{t}) : \mathbb{F}_q(t)] = 12. \#

We now want to show that \( k_f = \mathbb{F}_q \) so that we can apply point (ii) of Proposition 3.1. But this is completely obvious because one can consider \( \text{Gal}(M_f : k_f(t)) \), as \( k_f(t) \) is clearly a subfield of \( M_f \), and exactly the same arguments as above apply. This shows that
\[ \# \text{Gal}(M_f : k_f(t)) = [M_f : k_f(t)] = [M_f : k_f(\sqrt{t})] : [k_f(\sqrt{t}) : k_f(t)] = 12. \]
Since \( \text{Gal}(M_f : k_f(t)) \subseteq G_f \) we must have equality, and therefore \( k_f(t) = \mathbb{F}_q(t) \), which in turn forces \( k_f = \mathbb{F}_q \).

Let \( y \) and \( z \) be two roots of \( H_1 \). Observe that \( M_f = \mathbb{F}_q(t, \sqrt{t}, y, z) = \mathbb{F}_q(y, z) \) as \( \sqrt{t} \) (and so \( t \)) can be obtained by evaluating \( f \) at \( y \) for example, and adding two roots of \( H_1 \) is enough to obtain the third root using field operations. Then we have \( g_f \leq 1 \) by Riemann’s inequality [6, Corollary 3.11.4] (the minimal polynomial of \( y \) over \( \mathbb{F}_q(z) \) has degree at most 2 and viceversa).

Let us now compute \( \text{Ram}^1(M_f : \mathbb{F}_q(t)) \). As usual, we look at the number of zeroes in \( \mathbb{F}_q \) of the derivative \( f'(X) = 2(X^3 - aX)(3X^2 - a) \). Since \( a \) is not a square, \( f'(X) \) has at most 3 zeroes in \( \mathbb{F}_q \), depending on whether 3 is a square or not in \( \mathbb{F}_q \). Since the place at infinity is always ramified we have that \( \text{Ram}^1(M_f : \mathbb{F}_q(t)) \) consists of at most 4 places.

Plugging everything in the formula off (ii) of Proposition 3.1 we get the wanted result.

\[ \square \]

**Remark 3.15.** To further limit the size of the ramified places, in Theorem 3.14 we could also impose that \( a/3 \) is not a square (but this would restrict the fields where the theorem holds to the ones where 3 is a square).

**Remark 3.16.** Notice that having Galois group of order 12 for a polynomial of degree 6 is highly non-generic, as the Galois group of a random degree 6 polynomial will be \( S_6 \), which has cardinality 720. Moreover, the polynomial \( f - t \) has a small Galois group even among all polynomials which are compositions of degree 3 and degree 2 polynomials: the generic condition is in fact to have a Galois group of size 72. To see this, it is enough to notice that in the proof of Theorem 3.14 when we add all the roots of \( H_1 \), then \( H_2 \) splits because of the particular form of \( f \).
4. Examples

In this section we see how the estimates given in our results agree with the actual number of totally split places. The computations were performed in SAGE [8] and the code is available upon request.

Tables 1a and 1b show the agreement of the estimate in Theorem 3.11 with the actual number of totally split places. Even though this agreement is asymptotic in $q$, it is not completely sharp due to the fact that $g_f = 1$ for the polynomial we looked at. The polynomial lead to LRC optimal codes with locality 2.

Table 1

| $q = 2^{3n}$ | $T_{\text{split}}^1$ | lower bound |
|--------------|----------------------|--------------|
| 8            | 1                    | 0            |
| 64           | 10                   | 8            |
| 512          | 85                   | 77           |
| 4096         | 682                  | 661          |
| 32768        | 5461                 | 5401         |

(a) Let $a \in \mathbb{F}_8$ be a zero of $X^3 + X + 1$. The table compares $T_{\text{split}}^1(X(X + 1)(X + a))$ with the lower bound given by Theorem 3.11 over some base fields.

| $q = 5^n$ | $T_{\text{split}}^1$ | lower bound |
|-----------|----------------------|--------------|
| 5         | 1                    | 0            |
| 25        | 3                    | 2            |
| 125       | 21                   | 17           |
| 625       | 103                  | 95           |
| 3125      | 521                  | 502          |
| 15625     | 2603                 | 2562         |
| 78125     | 13021                | 12927        |

(b) Comparing $T_{\text{split}}^1(X(X + 1)(X + 3))$ with the lower bound given by Theorem 3.11 over many base fields.

Table 2a shows almost a perfect agreement, which comes from the genus zero condition, which makes Chebotarev’s error term a $O(1)$. The polynomial lead to LRC optimal codes with locality 3.

In practice, for a random polynomial having a totally split place, the estimate $q/(r!)$ for the number of totally split places seem to hold most of the time. Table 2b shows the behaviour of a totally split polynomial of degree 5. The polynomial lead to LRC optimal codes with locality 4.
Table 2

| $q$ | $\#T_{\text{split}}^1$ | lower bound |
|-----|----------------|-------------|
| 125 | 15            | 14          |
| 127 | 15            | 14          |
| 131 | 16            | 15          |
| 137 | 16            | 16          |
| 139 | 17            | 16          |
| 149 | 18            | 18          |
| 151 | 18            | 17          |

(a) Comparing $\#T_{\text{split}}^1(X^4 + 7X^2)$ with the prediction given by Theorem 3.13 over some base fields

| $q$ | $\#T_{\text{split}}^1$ | prediction: $\lceil \frac{q+1}{(r+1)!} \rceil$ |
|-----|----------------|----------------------------------|
| 1787 | 17            | 15                              |
| 1789 | 11            | 15                              |
| 1801 | 17            | 16                              |
| 1811 | 15            | 16                              |
| 1823 | 17            | 16                              |
| 1831 | 21            | 16                              |
| 1847 | 17            | 16                              |
| 1849 | 23            | 16                              |
| 1861 | 11            | 16                              |

(b) Comparing $\#T_{\text{split}}^1(X(X - 1)(X - 2)(X - 3)(X - 4))$ with the lower bound given by Theorem 3.7 over some base fields.

Tables 3a and 3b show the agreement between the lower bound of Theorem 3.14 and the actual number of totally split places of $f$.

Table 3

| $q$ | $\#T_{\text{split}}^1$ | lower bound |
|-----|----------------|-------------|
| 241 | 20            | 16          |
| 263 | 22            | 18          |
| 313 | 26            | 22          |
| 347 | 29            | 24          |
| 349 | 29            | 25          |
| 359 | 30            | 25          |
| 397 | 33            | 28          |

(a) Comparing $\#T_{\text{split}}^1((X^3 + 7X^2)^2)$ with the lower bound given by Theorem 3.14 over some prime base fields

| $q$ | $\#T_{\text{split}}^1$ | lower bound |
|-----|----------------|-------------|
| 343 | 28            | 24          |
| 2197 | 182         | 174         |
| 16807 | 1400 | 1378         |

(b) Comparing $\#T_{\text{split}}^1((X^3 + 5X)^2)$ with the lower bound given by Theorem 3.14 over some large non prime base fields
5. Conclusions

In this paper we fitted the theory of good polynomials in a global function field context. The theory includes all the previous constructions and shows that the construction of good polynomials can be reduced to a Galois theoretical problem over global function fields:

**Problem 5.1.** Find polynomials $f \in \mathbb{F}_q[X]$ such that

- The splitting field $M_f$ of $f - t$ over the rational function field $\mathbb{F}_q(t)$ is $\mathbb{F}_q$
- The Galois group of $f - t$ over $\mathbb{F}_q(t)$ is as small as possible when compared with the Galois group of polynomials of the same degree.

We solve some instances of this problem to show how effective and practical the method is, which in turn allows us to build new good polynomials over base fields where the known constructions do not work. Also, the method produces theoretical existential results for any totally split polynomial of fixed degree over a large base field.

6. Acknowledgements

We would like to thank Federico Amadio Guidi and Violetta Weger for checking the preliminary version of this manuscript. The author is thankful to the Swiss National Science Foundation grant number 171248.

References

[1] Andrea Ferraguti and Giacomo Micheli. Complete classification of permutation rational functions of degree three over finite fields. *arXiv preprint arXiv:1805.03097*, 2018.

[2] Michiel Kosters. A short proof of a chebotarev density theorem for function fields. *Mathematical Communications*, 22(2):227–233, 2017.

[3] Jian Liu, Sihem Mesnager, and Lusheng Chen. New constructions of optimal locally recoverable codes via good polynomials. *IEEE Transactions on Information Theory*, 64(2):889–899, 2018.

[4] Giacomo Micheli. On the selection of polynomials for the dlp algorithm. *arXiv preprint arXiv:1706.08447*, 2017.

[5] Dimitris S Papailiopoulos and Alexandros G Dimakis. Locally repairable codes. *IEEE Transactions on Information Theory*, 60(10):5843–5855, 2014.
[6] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[7] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.

[8] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version x.y.z)*, YYYY. http://www.sagemath.org.

Mathematical Institute, University of Oxford, Woodstock Rd, Oxford OX2 6GG, United Kingdom

E-mail address: giacomo.micheli@maths.ox.ac.uk