New identities relating wild Goppa codes

Alain Couvreur, Ayoub Otmani, Jean-Pierre Tillich

New Identities Relating Wild Goppa Codes

Alain Couvreur,* Ayoub Otmani† and Jean–Pierre Tillich‡

November 7, 2013

Abstract

For a given support $L \in \mathbb{F}_{q^m}^n$ and a polynomial $g \in \mathbb{F}_{q^m}[x]$ with no roots in $\mathbb{F}_{q^m}$, we prove equality between the q–ary Goppa codes $\Gamma_q(L, N(g)) = \Gamma_q(L, N(g)/g)$ where $N(g)$ denotes the *norm* of g, that is $g^{q^{m-1}+\cdots+q+1}$. In particular, for $m = 2$, that is, for a quadratic extension, we get $\Gamma_q(L, g^q) = \Gamma_q(L, g^{q+1})$. If g has roots in $\mathbb{F}_{q^m}$, then we do not necessarily have equality and we prove that the difference of the dimensions of the two codes is bounded above by the number of distinct roots of g in $\mathbb{F}_{q^m}$. These identities provide numerous code equivalences and improved designed parameters for some families of classical Goppa codes.

Introduction

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be an extension of finite fields. Given an ordered n–tuple $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$ and a polynomial $G \in \mathbb{F}_{q^m}[x]$ with no roots among the entries of L, the *classical Goppa code* over $\mathbb{F}_q$ denoted by $\Gamma_q(L, G)$ is defined as

$$\Gamma_q(L, G) \stackrel{\text{def}}{=} \left\{ (c_1, \ldots, c_n) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \mod G(x) \right\}.$$

Since their introduction by V. D. Goppa in 1970 [9], classical Goppa codes are subject to intense study and many questions remain open. For instance, even if the existence of asymptotic families of Goppa codes reaching the Gilbert–Varshamov bound is known for a long time, no explicit construction of such a family is known. More generally, the exact computation of the dimension and the minimum distance of a given Goppa code remain an open problem.

Besides, Goppa codes are particularly appealing for cryptographic applications. Indeed, since the introduction of code–based cryptography by McEliece in 1978 [18], Goppa codes still remain among the few families of algebraic codes which resist to any structural attack. This is one of the reasons why every improvement of our knowledge of these codes is of particular interest.

Goppa codes form a subfamily of *alternant codes*, that is subfield subcodes of *Generalised Reed–Solomon codes*. As alternant codes, the classical results on the parameters of subfield subcodes provide lower bounds for their dimension and minimum distance. However, these bounds can be improved for some specific Goppa codes and for a relevant choice of the Goppa polynomial G. A major improvement of these parameters has been obtained in 1976 by Sugiyama *et al.* [20] who proved that if $g \in \mathbb{F}_{q^m}[x]$ is squarefree, then, $\Gamma_q(L, g^{q-1}) = \Gamma_q(L, g^q)$. This equality can easily be generalised as $\Gamma_q(L, g^{sq-1}) = \Gamma_q(L, g^{sq})$ for any positive integer s. This identity relating the subfield subcodes of two Generalised Reed–Solomon codes with distinct parameters allows to take the best from each one. Namely, the dimension of such a code is at least the designed dimension of $\Gamma_q(L, g^{q-1})$ which is $n - m\deg(g)(q-1)$ and the minimum distance is at least the designed distance of $\Gamma_q(L, g^q)$ which equals $\deg(g)q+1$. In the binary case, this identity provides a lower bound for the minimum distance of $\Gamma_2(L, g)$ which is almost twice the designed distance for alternant codes. Some extensions of Sugiyama *et al.*'s result to algebraic geometry codes are presented in [8, 13, 26]. The particular subclass of Goppa codes of the form $\Gamma_q(L, g^{q-1})$ for a squarefree Goppa polynomial g has been called *wild Goppa codes* by Bernstein *et al.* [1, 2]

*GRACE Project — INRIA Saclay & LIX, CNRS UMR 7161 — École Polytechnique, 91120 Palaiseau Cedex, France. alain.couvreur@lix.polytechnique.fr

†Normandie Univ, France; UR, LITIS, F-76821 Mont-Saint-Aignan, France. ayoub.otmani@univ-rouen.fr

‡SECRET Project — INRIA Rocquencourt, 78153 Le Chesnay Cedex, France. jean-pierre.tillich@inria.fr

who proposed them for McEliece's encryption scheme since their improved designed parameters allowed to reduce the size of the public and secret keys for a fixed security level.
Beside Sugiyama *et al.*'s results, many improved lower bounds and exact computations of the true parameters — in particular the dimension — of some particular Goppa codes appear in the literature. For instance (and the list is far from being exhaustive), the authors of [16] propose a new lower bound for the minimum distance using the discrete Fourier transform. Improved lower bounds or exact values of the dimension of Goppa codes for specific families of Goppa polynomials are proved in [3, 19, 21, 23, 24, 25]. Many code equivalences and inclusions relating some particular binary Goppa codes are proved in [4, 5]. Most of these results concern Goppa codes whose Goppa polynomial or one of its divisors sends every entry of the support $L \in \mathbb{F}_{q^m}^n$ into a proper subfield of $\mathbb{F}_{q^m}$. Such a feature induces in general the apparition of linear relations between the parity checks of the code when passing from the Generalised Reed–Solomon code to its subfield subcode, which guarantees a larger dimension compared to the generic estimate for subfield subcodes. Among the previously cited works we should point out Véron's examples [23], who studied Goppa codes whose Goppa polynomial is a *trace polynomial, i.e.* a polynomial $G \in \mathbb{F}_{q^m}[x]$ of the form $G = g + g^q + \cdots + g^{q^{m-1}}$ with $g \in \mathbb{F}_{q^m}[x]$. Roughly speaking, the present article, deals with norms instead of traces. Namely, we consider Goppa polynomials of the form $g^{q^{m-1}+\cdots+q+1}$ and prove a very surprising equality: for $g \in \mathbb{F}_{q^m}[x]$ with no roots in $\mathbb{F}_{q^m}$, we have:

$$\Gamma_q\left(L, g^{q^{m-1}+\cdots+q}\right) = \Gamma_q\left(L, g^{q^{m-1}+\cdots+q+1}\right).$$

To the best of our knowledge, this article provides the first new general identity relating Goppa codes since Sugiyama *et al.*'s article.

Results of the present article

Consider an extension of finite fields $\mathbb{F}_{q^m}/\mathbb{F}_q$ with $m \geqslant 2$. Let n be a positive integer and $L = (\alpha_1, \ldots, \alpha_n)$ be an ordered n–tuple of pairwise distinct elements of $\mathbb{F}_{q^m}$ and $G \in \mathbb{F}_{q^m}[x]$ be a polynomial with no roots among the entries of L, then the classical Goppa code associated to L and G over the subfield $\mathbb{F}_q$ is defined as:

$$\Gamma_q(L, G) \stackrel{\text{def}}{=} \left\{ (c_1, \ldots, c_n) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \mod G(x) \right\}.$$

The n–tuple L is called the *support* of the code. If L contains every element of $\mathbb{F}_{q^m}$, *i.e.* if $n = q^m$, then the corresponding codes are said to have a *full support*. The polynomial G is called the *Goppa polynomial*. As an alternant code a Goppa code has a *designed dimension* $n - m\deg(G)$ and a *designed minimum distance* $\deg(G) + 1$ (see [22, Theorem 9.2.7]). Here we state Theorems 1 and 4 which are the main results of the present article. Their proofs are given in Section 3.

Theorem 1. *Let $g \in \mathbb{F}_{q^m}[x]$ be a polynomial with no roots in $\mathbb{F}_{q^m}$ and L be an ordered n–tuple of pairwise distinct elements of $\mathbb{F}_{q^m}$. Then,*

$$\Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q}\right) = \Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q+1}\right). \tag{1}$$

This result can be combined with Sugyiama *et al.* [20] and gives the following corollary.

Corollary 2. *Let L, g be as in Theorem 1 and assume in addition that g is squarefree, then*

$$\Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q-1}\right) = \Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q}\right) = \Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q+1}\right). \tag{2}$$

In addition, Theorem 1 provides improved designed parameters for the involved codes, namely, they can easily be proved to have parameters of the form:

$$[n,\ \geqslant n - mt(q^{m-1} + \cdots + q - 1),\ \geqslant t(q^{m-1} + \cdots + q + 1) + 1],$$

where t denotes the degree of g. Actually, the dimension is far larger than this bound. Indeed, the polynomial $g^{q^{m-1}+\cdots+q+1}$ sends every element $\alpha \in \mathbb{F}_{q^m}$ on an element of $\mathbb{F}_q$, namely the norm of $g(\alpha)$. In [12], the authors prove that such alternant codes are equivalent to a subfield subcode of a Reed–Solomon code, that is extended or shortened BCH codes. Furthermore, it is well–known that subfield subcodes of Reed–Solomon codes have

a large dimension compared to subfield subcodes of random codes [6, 11, 12, 14]. For instance when $m = 2$, the codes $\Gamma_q\left(L, g^q\right)$ and $\Gamma_q\left(L, g^{q+1}\right)$ are equal and have parameters of the form:

$$[n, \geqslant n - 2t(q-1) + t(t-2), \geqslant t(q+1) + 1].$$

Third, we point out that compared to Sugyiama et. al.'s result [20], our identity (1) does not require the polynomial g to be squarefree. This has the following interesting consequence.

Corollary 3. *Let h be a polynomial in $\mathbb{F}_{q^m}[x]$ with no roots in $\mathbb{F}_{q^m}$ and L be a support. Then, for all integer $s > 0$, we have*

$$\Gamma_q\left(L, h^{s(q^{m-1}+q^{m-2}+\cdots+q)}\right) = \Gamma_q\left(L, h^{s(q^{m-1}+q^{m-2}+\cdots+q+1)}\right)$$

and all the intermediary codes $\Gamma_q\left(L, h^{s(q^{m-1}+q^{m-2}+\cdots+q)+i}\right)$ for $0 < i < s$ are also equal to the above codes.

This corollary can be also combined with Sugyiama *et al.*'s result assuming that the polynomial h is squarefree, which will extend the equality as:

$$\Gamma_q\left(L, h^{s(q^{m-1}+q^{m-2}+\cdots+q)-1}\right) = \cdots = \Gamma_q\left(L, h^{s(q^{m-1}+q^{m-2}+\cdots+q+1)}\right)$$

Finally, it is worth noting that, even if the code has not a full support, Theorem 1 holds true only if g has no roots in $\mathbb{F}_{q^m}$. In particular, this result is not usable when the degree of g is 1. Nevertheless, in the general case one still has the following statement.

Theorem 4. *Let L be a support and $g \in \mathbb{F}_{q^m}[x]$ be a polynomial with no roots in L. Let r be the number of distinct roots of g (i.e. not counted with multiplicity) in $\mathbb{F}_{q^m}$. Then we have:*

$$\dim_{\mathbb{F}_q} \Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q}\right) - \dim_{\mathbb{F}_q} \Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q+1}\right) \leqslant r.$$

Notice that in general the difference between the dimensions of $\Gamma_q\left(L, g^a\right)$ and $\Gamma_q\left(L, g^{a+1}\right)$ is $m\deg(g)$. Here the difference is smaller than $\deg(g)$ and is not multiplied by m. Thus, the difference is small compared to the general case. This statement is of interest, since, using the very same argument as above, one can prove using [12] that, if the support L is full (*i.e.* $n = q^m$), then $\Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q+1}\right)$ is a subfield subcode of a Reed–Solomon code and hence has a dimension larger than the designed dimension for general alternant codes. By this manner, Theorem 4 provides an improved lower bound for the dimension of codes $\Gamma_q\left(L, g^{q^{m-1}+q^{m-2}+\cdots+q}\right)$, where g has degree 1.

Outline of the article

This article is organised as follows. Elementary properties of Goppa codes are recalled and discussed in Section 1. The particular case of Goppa codes whose Goppa polynomial sends every entry of L into a proper subfield of $\mathbb{F}_{q^m}$ is discussed in Section 2. Section 3 is devoted to the proofs of the main results of the article, namely Theorems 1 and 4. Finally, some numerical examples illustrating our results are presented in Section 4.

1 Some Well Known Properties of Goppa Codes

Notation 1. For a given support $L = (\alpha_1, \ldots, \alpha_n)$ of pairwise distinct elements of $\mathbb{F}_{q^m}$, we denote by π_L the polynomial

$$\pi_L \stackrel{\text{def}}{=} \prod_{i=1}^{n} (x - \alpha_i).$$

We denote by π_L' its first derivative. Finally, for a positive integer a, we denote by $\mathbb{F}_{q^m}[x]_{<a}$ the subspace of $\mathbb{F}_{q^m}[x]$ of polynomials of degree less than a.

Recall that q-ary Goppa codes are alternant codes, *i.e.* subfield subcodes over $\mathbb{F}_q$ of a Generalised Reed–Solomon (GRS) code over $\mathbb{F}_{q^m}$. Therefore, from Delsarte's Theorem [17, Theorem 7.7.11], the dual of the Goppa code, is the trace of a GRS code.

Lemma 5. *Let L be a support and $h \in \mathbb{F}_{q^m}[x]$ with no roots in L and $C, C^\perp$ be the GRS codes defined by*

$$C \stackrel{def}{=} \left\{ \left(\frac{h(\alpha_1) f(\alpha_1)}{\pi'_L(\alpha_1)}, \ldots, \frac{h(\alpha_n) f(\alpha_n)}{\pi'_L(\alpha_n)} \right) \;\middle|\; \alpha_i \in L,\ f \in \mathbb{F}_{q^m}[x]_{<n-t} \right\};$$
$$C^\perp = \left\{ \left(\frac{f(\alpha_1)}{h(\alpha_1)}, \ldots, \frac{f(\alpha_n)}{h(\alpha_n)} \right) \;\middle|\; \alpha_i \in L,\ f \in \mathbb{F}_{q^m}[x]_{<t} \right\}.$$

Then, $\Gamma_q(L,h) = C_{|\mathbb{F}_q}$ and $\Gamma_q(L,h)^\perp = \mathrm{Tr}(C^\perp)$ where Tr *denotes the map* $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *applied component-wise.*

Proof. See [17, Theorems 12.4 and 12.5] for binary Goppa codes. The q–ary case is obtained using the very same proof. □

The following elementary lemma is useful in what follows.

Lemma 6. *Let $L = (\alpha_1, \ldots, \alpha_n)$ be a support and $g, h \in \mathbb{F}_{q^m}[x]$ be two relatively prime polynomials such that both have no roots among the entries of L. Set $n - a = \dim_{\mathbb{F}_q} \Gamma_q(L,g)$ and $n - b = \dim_{\mathbb{F}_q} \Gamma_q(L,h)$ Then,*

$$\Gamma_q(L, gh) = \Gamma_q(L,g) \cap \Gamma_q(L,h); \tag{3}$$
$$\dim_{\mathbb{F}_q} \Gamma_q(L, gh) \geqslant n - a - b. \tag{4}$$

Proof. The Chinese remainder Theorem in the ring $\mathbb{F}_{q^m}[x, \frac{1}{\pi_L}]$ asserts that

$$\sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \mod (gh) \iff \begin{cases} \sum_{i=1}^{n} \frac{c_i}{x-\alpha_i} \equiv 0 \mod (g) \\ \sum_{i=1}^{n} \frac{c_i}{x-\alpha_i} \equiv 0 \mod (h). \end{cases}$$

This yields (3) and implies that $\Gamma_q(L,gh)^\perp = \Gamma_q(L,g)^\perp + \Gamma_q(L,h)^\perp$, which gives (4). □

Remark 1. Let L, g be as in Theorem 1 and $h \in \mathbb{F}_{q^m}[x]$ be a polynomial prime to g and with no roots in L. Then, Theorem 1 generalises as:

$$\Gamma_q\left(L, hg^{q^{m-1}+\cdots+q-1}\right) = \Gamma_q\left(L, hg^{q^{m-1}+\cdots+q}\right) = \Gamma_q\left(L, hg^{q^{m-1}+\cdots+q+1}\right).$$

The Goppa codes described above for $m = 2$ are proposed for cryptographic applications in [2].

Lemma 7. *Let L, L' be two supports such that L can be obtained from L' by removing some entries without changing the ordering. Let $g \in \mathbb{F}_{q^m}[x]$ be a polynomial with no roots in L' (and hence in L), then $\Gamma_q(L,g)$ is equal to the shortening of $\Gamma_q(L',g)$ on L.*

Proof. This follows immediately by viewing $\sum_{\alpha \in L} \frac{c_\alpha}{x-\alpha}$ as the sum $\sum_{\beta \in L'} \frac{c_\beta}{x-\beta}$ such that $c_\beta = 0$ for all $\beta \in L' \setminus L$. □

2 Goppa Codes and Subfield Subcodes of Reed–Solomon Codes

Definition 8 (Diagonal equivalence)**.** Let C, C' be two codes in $\mathbb{F}_q^n$. C, C' are said to be *diagonally equivalent* and we write $C \sim_{\mathbb{F}_q} C'$ in this case, if C' is the image of C by a Hamming isometry of $\mathbb{F}_q^n$ of the form:

$$\begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (x_1, \ldots, x_n) & \longmapsto & (u_1 x_1, \ldots, u_n x_n) \end{cases},$$

where the u_i's are all in $\mathbb{F}_q^\times$. This choice of terminology comes from the fact that the codes can be sent onto each other using an invertible diagonal matrix.

Here, we reformulate for our purpose some results stated in [12].

Proposition 9. *Let L be an n–tuple of pairwise distinct elements of $\mathbb{F}_{q^m}$ and g, h be two polynomials in $\mathbb{F}_{q^m}[x]$ which have no roots among the entries of L (but possibly elsewhere in $\mathbb{F}_{q^m}$), such that* $\deg(g) = \deg(h)$*, then the codes $\Gamma_q\left(L, g^{q^{m-1}+\cdots+q+1}\right)$ and $\Gamma_q\left(L, h^{q^{m-1}+\cdots+q+1}\right)$ are diagonally equivalent.*

Proof. For all $\alpha \in L$, note that $g^{q^{m-1}+\cdots+q+1}(\alpha)$ (resp. $h^{q^{m-1}+\cdots+q+1}(\alpha)$) is nothing but $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(g(\alpha))$ (resp. $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(h(\alpha))$) and hence is in $\mathbb{F}_q$. Thus both Goppa polynomials send every entry of L into $\mathbb{F}_q$. One concludes using [12, Proposition 3.5]. □

Remark 2. The result stated in [12] concerns codes on a support avoiding 0. However, their result extends straightforwardly to a full support.

Corollary 10. *Let g be a polynomial in $\mathbb{F}_{q^m}[x]$ with no roots in $\mathbb{F}_{q^m}$ and L_0 be a "full support", i.e. an ordered q^m–tuple containing all the elements of $\mathbb{F}_{q^m}$, then we have the diagonal equivalence of codes*

$$\Gamma_q\left(L_0, g^{q^{m-1}+q^{m-2}+\cdots+q+1}\right) \sim_{\mathbb{F}_q} RS_k(L_0)_{|\mathbb{F}_q},$$

where $RS_k(L_0)_{|\mathbb{F}_q}$ denotes the subfield subcode of the Reed–Solomon code over $\mathbb{F}_{q^m}$ of dimension $k = q^m - \deg(g)(q^{m-1}+q^{m-2}+\cdots+q+1)$ with full support. In particular the diagonal equivalence class of this code depends only on the degree of g.

Proof. See [12, §3]. □

It is worth noting that a subfield subcode of a full support Reed–Solomon code is nothing but an extended BCH code. In [12, Theorem 4.4], the authors give a formula for the dimension of such codes involving the number and the size of some cyclotomic classes. See Section 4 for further discussion.

Remark 3. Corollary 10 holds for every Goppa Polynomial sending every entry of the support into $\mathbb{F}_q$. In particular, this gives another interpretation of Véron's results [23] showing that the dimension of Goppa codes with a Goppa polynomial of the form $g + g^q + \cdots + g^{q^{m-1}}$ exceeds the generic bound for alternant codes. Indeed, since such a Goppa polynomial sends every entry of the support into $\mathbb{F}_q$, the corresponding Goppa code is $\mathbb{F}_q$–equivalent to a BCH code.

3 Proof of Theorems 1 and 4

3.1 Notation

In what follows we frequently consider $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^n$ as rings for their canonical product ring structure. The component-wise product of two n–tuples a, b in $\mathbb{F}_{q^m}^n$ is denoted by

$$a \star b \stackrel{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n).$$

We also allow ourselves the notation a^s to denote the component-wise s–th power and $1/a$ for the component-wise inverse when a is in $(\mathbb{F}_{q^m}^\times)^n$. Recall that $\mathrm{Tr} : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^n$ is the component-wise trace map. In the same manner, $\mathrm{N} : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^n$ is the component-wise norm map. Furthermore, we denote by ev_L the *evaluation* function:

$$\mathrm{ev}_L : \left\{ \begin{array}{ccc} \mathbb{F}_{q^m}[x] & \longrightarrow & \mathbb{F}_{q^m}^n \\ f & \longmapsto & \big(f(\alpha_1), \ldots, f(\alpha_n)\big) \end{array} \right. . \tag{5}$$

This turns out to be a ring homomorphism. We also need to introduce the map τ defined as the composition of ev_L and Tr, namely:

$$\tau : \left\{ \begin{array}{ccc} \mathbb{F}_{q^m}[x] & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & \mathrm{Tr}(\mathrm{ev}_L(f)) \end{array} \right. . \tag{6}$$

Finally, for convenience, we denote by e the integer

$$e \stackrel{\text{def}}{=} q^{m-1} + q^{m-2} + \cdots + q.$$

3.2 Preliminaries

3.2.1 Local reformulation

Thanks to Lemma 6, one can assume that g is a power h^s of an irreducible polynomial $h \in \mathbb{F}_{q^m}[x]$ with $s \geqslant 1$. Hence we are reduced to prove the following statement.

Theorem 11 (Local version of Theorems 1 and 4)**.** *Let $L \in \mathbb{F}_{q^m}^n$ be a support and $g \in \mathbb{F}_{q^m}[x]$ be a polynomial of degree t which is either irreducible or a power of an irreducible polynomial. Only two cases can occur:*

(i) g has no roots in $\mathbb{F}_{q^m}$ then $\Gamma_q\left(L, g^e\right) = \Gamma_q\left(L, g^{e+1}\right)$;

(ii) or $g = (x-\rho)^t$ for some $t \geqslant 1$ and some $\rho \in \mathbb{F}_{q^m}$ which does not appear in the entries of L, then:

$$\dim_{\mathbb{F}_q} \Gamma_q\left(L, g^e\right) - \dim_{\mathbb{F}_q} \Gamma_q\left(L, g^{e+1}\right) \leqslant 1.$$

3.2.2 Duality and role of the norm

Theorem 11 can be reformulated using duality together with an argument involving the norm $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ which is strongly related to the results of Section 2.

Proposition 12. *Theorem 11 (i) and (ii) are respectively equivalent to*

(i') If g has no roots in $\mathbb{F}_{q^m}$ then $\tau\left(\mathbb{F}_{q^m}[x]_{<(e+1)t}\right) = \tau\left(g\mathbb{F}_{q^m}[x]_{<et}\right)$.

(ii') If $g = (x-\rho)^t$ for some $\rho \in \mathbb{F}_{q^m}$ and some $t \geqslant 1$, then

$$\dim_{\mathbb{F}_q} \tau\left(\mathbb{F}_{q^m}[x]_{<(e+1)t}\right) - \dim_{\mathbb{F}_q} \tau\left(g\mathbb{F}_{q^m}[x]_{<et}\right) \leqslant 1.$$

Proof. Let us prove that Theorem 11 (i) is equivalent to (i'). Let g be a polynomial with no roots in $\mathbb{F}_{q^m}$. By using Lemma 5, Theorem 11 (i) is equivalent to its dual reformulation, namely

$$\left\{ \mathrm{Tr}\left(\frac{\mathrm{ev}_L(f)}{\mathrm{ev}_L\left(g^{e+1}\right)}\right) \;\middle|\; f \in \mathbb{F}_{q^m}[x]_{<(e+1)t} \right\} = \left\{ \mathrm{Tr}\left(\frac{\mathrm{ev}_L(f)}{\mathrm{ev}_L\left(g^{e}\right)}\right) \;\middle|\; f \in \mathbb{F}_{q^m}[x]_{<et} \right\} \tag{7}$$

Note that

$$\begin{aligned} \left\{ \mathrm{Tr}\left(\frac{\mathrm{ev}_L(f)}{\mathrm{ev}_L\left(g^{e}\right)}\right) \;\middle|\; f \in \mathbb{F}_{q^m}[x]_{<et} \right\} &= \left\{ \mathrm{Tr}\left(\frac{\mathrm{ev}_L(f) \star \mathrm{ev}_L(g)}{\mathrm{ev}_L(g)^{e} \star \mathrm{ev}_L(g)}\right) \;\middle|\; f \in \mathbb{F}_{q^m}[x]_{<et} \right\} & (8) \\ &= \left\{ \mathrm{Tr}\left(\frac{\mathrm{ev}_L(h)}{\mathrm{ev}_L(g)^{e+1}}\right) \;\middle|\; h \in g\mathbb{F}_{q^m}[x]_{<et} \right\}. & (9) \end{aligned}$$

In addition, since $\mathrm{ev}_L\left(g^{e+1}\right) = \mathrm{N}\left(\mathrm{ev}_L(g)\right)$, this vector has its entries in $\mathbb{F}_q$. Hence these denominators can be pulled out of the traces. Therefore, (7) is equivalent to

$$\left\{ \frac{1}{\mathrm{ev}_L(g)^{e+1}} \star \mathrm{Tr}\left(\mathrm{ev}_L(f)\right) \;\middle|\; f \in \mathbb{F}_{q^m}[x]_{<(e+1)t} \right\} = \left\{ \frac{1}{\mathrm{ev}_L(g)^{e+1}} \star \mathrm{Tr}\left(\mathrm{ev}_L(h)\right) \;\middle|\; h \in g\mathbb{F}_{q^m}[x]_{<et} \right\}. \tag{10}$$

Finally, this equality is clearly equivalent to

$$\left\{ \mathrm{Tr}\left(\mathrm{ev}_L(f)\right) \mid f \in \mathbb{F}_{q^m}[x]_{<(e+1)t} \right\} = \left\{ \mathrm{Tr}\left(\mathrm{ev}_L(h)\right) \mid h \in g\mathbb{F}_{q^m}[x]_{<et} \right\}. \tag{11}$$

This concludes the proof. The proof of the equivalence between Theorem 11 (ii) and *(ii')* is the very same one replacing equalities by inclusions with codimension 1. □

3.2.3 The spaces K and T

Proposition 13 below explains that the proof of Proposition 12, which is equivalent to Theorem 11, can be achieved by proving the existence of two special vector spaces K and T.

Proposition 13. *If there exists a subspace K of $\mathbb{F}_{q^m}[x]_{<(e+1)t}$ satisfying:*

(I) $K \subset \ker \tau$

(II) $K \cap g\mathbb{F}_{q^m}[x]_{<et} = \{0\}$

(III) $\dim_{\mathbb{F}_q} K = mt - 1$

then it implies:

$$\dim_{\mathbb{F}_q} \tau\left(\mathbb{F}_{q^m}[x]_{<(e+1)t}\right) - \dim_{\mathbb{F}_q} \tau\left(g\mathbb{F}_{q^m}[x]_{<et}\right) \leqslant 1.$$

In addition, if g has no roots in $\mathbb{F}_{q^m}$, and if there exists another $\mathbb{F}_q$subspace T of $\mathbb{F}_{q^m}[x]_{<(e+1)t}$ such that

(IV) $K \oplus T \subset \ker \tau$ *and* $\mathbb{F}_{q^m}[x]_{<(e+1)t} = K \oplus T \oplus g\mathbb{F}_{q^m}[x]_{<et}$,

then the equality $\tau\left(\mathbb{F}_{q^m}[x]_{<(e+1)t}\right) = \tau\left(g\mathbb{F}_{q^m}[x]_{<et}\right)$ holds.

Proof. This follows basically from the fact that $\dim_{\mathbb{F}_q}\left(\mathbb{F}_{q^m}[x]_{<(e+1)t}\right) = m(e+1)t$ whereas $\dim_{\mathbb{F}_q}\left(\mathbb{F}_{q^m}[x]_{<et}\right) = met$. If such a space K exists, then from (II) and (III), we get the existence of an $\mathbb{F}_q$–one–dimensional subspace T_0 of $\mathbb{F}_{q^m}[x]_{<(e+1)t}$ such that $\mathbb{F}_{q^m}[x]_{<(e+1)t} = K \oplus T_0 \oplus g\mathbb{F}_{q^m}[x]_{<et}$. Then, (I) leads to Proposition 12 (ii') or equivalently Theorem 11 (ii). If in addition, there exists a space T satisfying (IV), then we clearly get Proposition 12 (i') or equivalently Theorem 11 (i). □

From now on, the polynomial g is assumed to be either irreducible or of the form $g = h^s$ for some irreducible polynomial $h \in \mathbb{F}_{q^m}[x]$ and some integer $s > 1$. The degree of g is denoted by t.

3.3 The construction of K and the existence of T

First, we recall a well known result concerning elements whose trace is zero (see [15, Theorem 2.25] for a proof).

Lemma 14. *For all $\alpha \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$, there exists $\beta \in \mathbb{F}_{q^m}$ such that $\alpha = \beta - \beta^q$.*

We look for an $\mathbb{F}_q$–subspace $K \subset \mathbb{F}_{q^m}[x]_{<(e+1)t}$ satisfying (I), (II) and (III) of Proposition 13. Notice that we have $\ker \tau = \left\{a \in \mathbb{F}_{q^m}[x]_{<(e+1)t} \mid \mathrm{Tr}(\mathrm{ev}_L(a)) = 0\right\}$. This point, together with Lemma 14, explain the rationale behind the following definition.

Definition 15. We denote by K the image of the map

$$\mu : \left\{ \begin{array}{ccc} \mathbb{F}_{q^m}[x]_{<t} & \longrightarrow & \mathbb{F}_{q^m}[x] \\ a & \longmapsto & a^q - a \end{array} \right. . \tag{12}$$

Lemma 16. *We have, $K \subset \ker \tau$ and $\dim_{\mathbb{F}_q} K = mt - 1$.*

Proof. First, let us check that $K \subset \mathbb{F}_{q^m}[x]_{<(e+1)t}$. Let a be an element of $\mathbb{F}_{q^m}[x]_{<t}$, we have $a^q - a \in \mathbb{F}_{q^m}[x]_{<qt}$. Since, $e = q^{m-1} + \cdots + q$ and $m \geqslant 2$, we have $e \geqslant q$ and hence $a^q - a \in \mathbb{F}_{q^m}[x]_{<(e+1)t}$. Next, by definition of Tr and its elementary properties, we have:

$$\mathrm{Tr}\left(\mathrm{ev}_L\left(a^q - a\right)\right) = \mathrm{Tr}\left(\mathrm{ev}_L(a)^q\right) - \mathrm{Tr}\left(\mathrm{ev}_L(a)\right) = 0.$$

This yields the inclusion $K \subset \ker \tau$. To get the dimension, we prove that $\dim_{\mathbb{F}_q} \ker \mu = 1$. Let a be an element of $\ker \mu$, *i.e.* a is a polynomial in $\mathbb{F}_{q^m}[x]_{<t}$ satisfying $a(x)^q = a(x)$. Then the degree of a is zero and a is nothing but a constant polynomial satisfying $a^q = a$. Thus, $\ker \mu$ consists in the subspace of constant polynomials lying in $\mathbb{F}_q$. □

In what follows some proofs require the use of congruences modulo some polynomials. For this reason we introduce the following notation.

Notation 2. For $f \in \mathbb{F}_{q^m}[x]$ and for all $a \in \mathbb{F}_{q^m}[x]$, we denote by $a \mod (f)$ the class of a in $\mathbb{F}_{q^m}[x]/(f)$. In the same manner, the image of K by the canonical map $\mathbb{F}_{q^m}[x] \to \mathbb{F}_{q^m}[x]/(f)$ will be denoted by $(K \mod f)$. Finally, after the map μ introduced in (12) we define for all $f \in \mathbb{F}_{q^m}[x]$, the map μ_f as

$$\mu_f : \begin{cases} \mathbb{F}_{q^m}[x]/(f) & \longrightarrow & \mathbb{F}_{q^m}[x]/(f) \\ a \mod (f) & \longmapsto & a^q - a \mod (f) \end{cases}. \tag{13}$$

Lemma 17. *Let h be an irreducible polynomial of degree r such that $g = h^s$ for some positive integer s (possibly $s = 1$). Viewing $\mathbb{F}_{q^m}[x]/(h)$ as the finite field $\mathbb{F}_{q^{mr}}$ it turns out that $K \mod (h)$ satisfies:*

$$K \mod (h) = \ker \mathrm{Tr}_{\mathbb{F}_{q^{mr}}/\mathbb{F}_q}.$$

Remark 4. In particular, if g is irreducible (s=1) then $K \mod (g) = \ker \mathrm{Tr}_{\mathbb{F}_{q^{mt}}/\mathbb{F}_q}$.

Proof. Since $r \stackrel{\text{def}}{=} \deg(h) \leqslant t$, the map $\mathbb{F}_{q^m}[x]_{<t} \to \mathbb{F}_{q^m}[x]/(h)$ is surjective and hence $(K \mod (h))$ is nothing but the image of μ_h (see (13) in Notation 2). Considering the quotient ring $\mathbb{F}_{q^m}[x]/(h)$ as the finite field $\mathbb{F}_{q^{mr}}$ we conclude by using Lemma 14. □

Proposition 18. *We have*

$$\dim_{\mathbb{F}_q}(K \mod (g)) = mt - 1.$$

Proof. If g is irreducible, then it is a straightforward consequence of Lemma 17. Let us assume that g is of the form h^s for some irreducible polynomial h and some integer $s > 1$. Recall that the space $K \mod (g)$ is nothing but the image of μ_g (see (13) in Notation 2). Therefore, we wish to prove that $\dim_{\mathbb{F}_q} \ker \mu_g = 1$. We will show that $\ker \mu_g$ is isomorphic to $\mathbb{F}_q$.
Let $a \in \mathbb{F}_{q^m}[x]$ such that $(a \mod (g)) \in \ker \mu_g$. That is

$$a \equiv a^q \mod (g) \tag{14}$$

Since $g = h^s$, we have *a fortiori* $a \equiv a^q \mod (h)$. Since $\mathbb{F}_{q^m}[x]/(h)$ is a field containing $\mathbb{F}_q$, then $a \mod (h)$ is represented by a constant polynomial lying in $\mathbb{F}_q$. Therefore, there exists $\alpha \in \mathbb{F}_q$ and $a_1(x) \in \mathbb{F}_{q^m}[x]$, such that

$$a(x) = \alpha + h(x)a_1(x).$$

From (14), we get $a \equiv a^{q^i} \mod (g)$ for all $i > 0$. Choose i such that $q^i \geqslant s$. Then, $h^{q^i} \equiv 0 \mod (g)$ since $g = h^s$. Therefore, $a \equiv a^{q^i} \mod (g)$ entails

$$a \equiv \alpha^{q^i} \mod (g).$$

Finally, since $\alpha \in \mathbb{F}_q$, we have $\alpha^{q^i} = \alpha$ which entails $a \equiv \alpha \mod (g)$. This yields an $\mathbb{F}_q$–isomorphism between $\ker \mu_g$ and $\mathbb{F}_q$, which concludes the proof. □

Corollary 19. $K \cap g\mathbb{F}_{q^m}[x]_{<et} = \{0\}$.

Proof. From Lemma 16, the space K has $\mathbb{F}_q$–dimension $mt - 1$ and, from Proposition 18, $K \mod (g)$ has $\mathbb{F}_q$–dimension $mt - 1$ too. Thus, the canonical projection $K \to \mathbb{F}_{q^m}[x]/(g)$ is injective and its kernel, which is nothing but $K \cap g\mathbb{F}_{q^m}[x]$ is equal to zero. Consequently, $K \cap g\mathbb{F}_{q^m}[x]_{<et}$ is zero too. □

Proposition 20. *The $\mathbb{F}_q$–space K of Definition 15 satisfies Conditions (I), (II) and (III) of Proposition 13.*

Proof. Lemma 16 yields Condition (I). Lemma 16 also yields Condition (III) and Corollary 19 gives Condition (II). □

Therefore, we proved Theorem 11 (ii) and there remains to prove Theorem 11 (i). Thus, from now on, we assume that g has no roots in $\mathbb{F}_{q^m}$ and we will prove the existence of a one–dimensional $\mathbb{F}_q$–space T satisfying (IV). The strategy to find such a T is to choose it as $T = \langle \lambda a^{e+1} \rangle_{\mathbb{F}_q}$ for some $a \in \mathbb{F}_{q^m}[x]_{<t}$ and some $\lambda \in \mathbb{F}_{q^m}^{\times}$ satisfying $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\lambda) = 0$. Clearly, we have the following statement.

Lemma 21. *For any nonzero element $\lambda \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\lambda) = 0$ and for any $a \in \mathbb{F}_{q^m}[x]_{<t}$, we have*

$$\lambda a^{e+1} \in \ker \tau.$$

Proof. We first observe that for all $a \in \mathbb{F}_{q^m}[x]_{<t}$, we have $\lambda a^{e+1} \in \mathbb{F}_{q^m}[t]_{<(e+1)t}$, which is elementary. We finish the proof with

$$\mathrm{Tr}\left(\mathrm{ev}_L\left(\lambda a^{e+1}\right)\right) = \mathrm{Tr}\left(\lambda \cdot \mathrm{N}(\mathrm{ev}_L(a))\right) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\lambda) \cdot \mathrm{N}\left(\mathrm{ev}_L(a)\right) = 0.$$

□

The following proposition is the key to conclude the proof of Theorem 1.

Proposition 22. *Let $r > 1$ be an integer and $\mathbb{F}_{q^{mr}}$ be the degree r extension of $\mathbb{F}_{q^m}$. Let $\lambda \in \mathbb{F}_{q^m}^{\times}$ be such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\lambda) = 0$. Then, there exists $\alpha \in \mathbb{F}_{q^{mr}}$ such that*

$$\mathrm{Tr}_{\mathbb{F}_{q^{mr}}/\mathbb{F}_q}(\lambda \alpha^{e+1}) \neq 0.$$

Proof. Set $Z \stackrel{\text{def}}{=} \left\{ z \in \mathbb{F}_{q^{mr}} \;\middle|\; \mathrm{Tr}_{\mathbb{F}_{q^{mr}}/\mathbb{F}_q}(\lambda z^{e+1}) = 0 \right\}$. Our point is to show that $|Z| < q^{mr}$. For all $z \in Z$, we have

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{q^{mr}}/\mathbb{F}_q}(\lambda z^{e+1}) &= \lambda z^{e+1} + \lambda^q \left(z^{e+1}\right)^q + \cdots + \lambda^{q^{mr-1}} \left(z^{e+1}\right)^{q^{mr-1}} \\ &= \lambda z^{q^{m-1}+\cdots+1} + \lambda^q z^{q^m+\cdots+q} + \cdots + \lambda^{q^{mr-1}} z^{q^{mr+m-2}+\cdots+q^{mr-1}}.\end{aligned}$$

Using the relation $z^{q^{mr}} = z$, we get

$$\mathrm{Tr}_{\mathbb{F}_{q^{mr}}/\mathbb{F}_q}(\lambda z^{e+1}) = \lambda z^{R_0(q)} + \lambda^q z^{R_1(q)} + \cdots + \lambda^{q^{mr-1}} z^{R_{mr-1}(q)}$$

where $R_0(q), \ldots, R_{mr-1}(q)$ are integers $< q^{mr}$ which are sums of m distinct powers of q with exponents $< mr$. Namely,

$$\begin{aligned}R_0(q) &= q^{m-1} + q^{m-2} + \cdots + q + 1 \\ R_1(q) &= q^m + q^{m-1} + \cdots + q^2 + q \\ &\vdots \\ R_{mr-1}(q) &= q^{m-2} + \cdots + q + 1 + q^{mr-1}.\end{aligned}$$

For all i, we have $R_i(q) < q^{mr}$. Next, it is not difficult to check that, since by assumption $r \geqslant 2$, the $R_i(q)$'s are pairwise distinct since they have pairwise distinct q–adic expansions. Let $Q \in \mathbb{F}_{q^{mr}}[x]$ be the polynomial

$$Q(x) \stackrel{\text{def}}{=} \lambda x^{R_0(q)} + \lambda^q x^{R_1(q)} + \cdots + \lambda^{q^{mr-1}} x^{R_{mr-1}(q)}.$$

The elements of Z are roots of Q lying in $\mathbb{F}_{q^{mr}}$. Since the R_i's are pairwise distinct and λ is assumed to be nonzero, the polynomial Q is nonzero. In addition, its degree is strictly less than q^{mr}. Consequently, Q has strictly less than q^{mr} roots. Therefore, $|Z| < q^{mr}$, which concludes the proof. □

Proposition 23. *Assume that g has no roots in $\mathbb{F}_{q^m}$. Let λ be a nonzero element of $\mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\lambda) = 0$. Then, there exists $a \in \mathbb{F}_{q^m}[x]_{<t}$ such that*

(i) $K \cap \langle \lambda a^{e+1} \rangle_{\mathbb{F}_q} = \{0\}$;

(ii) $K \oplus \langle \lambda a^{e+1} \rangle_{\mathbb{F}_q} \subset \ker \tau$;

(iii) $K \oplus \langle \lambda a^{e+1} \rangle_{\mathbb{F}_q} \oplus g\mathbb{F}_{q^m}[x]_{<et} = \mathbb{F}_{q^m}[x]_{<(e+1)t}$.

Proof. Recall that g is assumed to be of the form $g = h^s$ where h is irreducible and $s \geqslant 1$. The degree of h is denoted by r so that $t = sr$. The case $s = 1$ corresponds to g irreducible.
Since h is assumed to have no roots in $\mathbb{F}_{q^m}$, we necessarily have $r = \deg(h) \geqslant 2$. Thus, one can apply Proposition 22, which asserts the existence of $\alpha \in \mathbb{F}_{q^{mr}} \simeq \mathbb{F}_{q^m}[x]/(h)$ such that $\lambda \alpha^{e+1} \notin \ker \mathrm{Tr}_{\mathbb{F}_{q^{mr}}/\mathbb{F}_q}$. From Lemma 17, this asserts the existence of $\alpha \in \mathbb{F}_{q^m}[x]/(h)$ such that

$$\lambda \alpha^{e+1} \notin (K \mod (h)). \tag{15}$$

Let α_0 be a lift of α in $\mathbb{F}_{q^m}[x]/(g)$. Then, we clearly have

$$\lambda\alpha_0^{e+1} \notin (K \mod (g)). \tag{16}$$

Indeed, if we had $\lambda\alpha_0^{e+1} \in (K \mod (g))$, then reducing modulo (h) we would contradict (15). From Proposition 18, we know that $K \mod (g)$ has $\mathbb{F}_q$-codimension 1 in $\mathbb{F}_{q^m}[x]/(g)$ and hence (16) yields

$$(K \mod (g)) \oplus \langle \lambda\alpha_0^{e+1} \rangle_{\mathbb{F}_q} = \mathbb{F}_{q^m}[x]/(g). \tag{17}$$

Now, let $a \in \mathbb{F}_{q^m}[x]_{<t}$ be a lift of α_0. Here again, we clearly have $\lambda a^{e+1} \notin K$. This proves (i). Afterwards, (ii) is a direct consequence of Lemma 21.
Finally, from Lemma 16, we have

$$\dim_{\mathbb{F}_q} K \oplus \langle \lambda a^{e+1} \rangle_{\mathbb{F}_q} = mt. \tag{18}$$

Since mt is nothing but the $\mathbb{F}_q$–dimension of $\mathbb{F}_{q^m}[x]/(g)$, we see that (17) together with (18) prove that the space $K \oplus \langle \lambda a^{q+1} \rangle_{\mathbb{F}_q}$ is isomorphic to its reduction modulo (g), which entails:

$$(K \oplus \langle \lambda a^{e+1} \rangle_{\mathbb{F}_q}) \cap g\mathbb{F}_{q^m}[x] = \{0\}.$$

This leads to (iii) and terminates the proof. □

Conclusion. Proposition 23 gives the existence of a vector space T satisfying Condition (IV) of Proposition 13. This concludes the proof of Theorem 11 (i) and hence of Theorem 1.

Remark 5. It is worthwhile noting that the condition "g has no roots in $\mathbb{F}_{q^m}$" is necessary to prove the result since it is necessary to prove Proposition 22. Indeed, it is easy to see that if g had roots in $\mathbb{F}_{q^m}$, then we would need to prove Proposition 22 for $r = 1$. However, the proof of Proposition 22 does not hold for $r = 1$, since in that case all the $R_i(q)$'s in the proof would be equal and the polynomial Q would be zero. Using MAGMA [7], it is easy to compute examples of Goppa codes $\Gamma_q(L, g^e)$ and $\Gamma_q(L, g^{e+1})$, which are distinct when g has roots in $\mathbb{F}_{q^m}$. Thus, one cannot expect better than Theorem 4. This is illustrated by the examples in § 4.2.

4 Examples

In this section we consider some specific situations to illustrate our results. We first focus on the case of quadratic extensions, that is to say $m = 2$. Next, we illustrate Theorem 11 by considering such codes with a polynomial g of degree 1 and an extension degree that is equal to 3.

4.1 Wild Goppa codes from quadratic extensions

In this subsection, the extension degree m will be equal to 2. In this particular situation, our Theorem 1 asserts that for a squarefree polynomial g with no roots in $\mathbb{F}_{q^2}$, we have

$$\Gamma_q(L, g^{q-1}) = \Gamma_q(L, g^q) = \Gamma_q(L, g^{q+1}).$$

Therefore, the minimum distance of this code is bounded below by $\deg(g)(q+1)+1$ instead of $\deg(g)q+1$, which was its designed distance up to now. Another striking fact is that its dimension is also larger than the lower bound $n - 2\deg(g)(q-1)$. This is a consequence of the results of § 2, which assert that such a code is diagonally equivalent to a subfield subcode of a Reed–Solomon code or a shortening of it. The following statement yields a lower bound for the dimension of these wild Goppa codes.

Theorem 24. *Let $g \in \mathbb{F}_{q^2}[x]$ be a polynomial of degree $t \geqslant 2$ with no roots in $\mathbb{F}_{q^2}$ and L be a support of length n, then*

$$\dim_{\mathbb{F}_q} \Gamma_q(L, g^{q+1}) \geqslant n - 2t(q+1) + t(t+2).$$

In addition, the inequality is an equality when L is a full-support or a support of length $q^2 - 1$.

Proof. First, let us assume that L is a full support, *i.e.* $n = q^2$. From Corollary 10, the Goppa code $\Gamma_q\left(L, g^{q+1}\right)$ is $\mathbb{F}_q$–equivalent to the subfield subcode of $RS_{q^2-t(q+1)}(L)$. The dimension of such a code is bounded below in [12]. This bound concerns codes supported by $\mathbb{F}_{q^m} \setminus \{0\}$ and its shortenings. However, the case of a full support can easily be deduced from that of the support $\mathbb{F}_{q^m} \setminus \{0\}$, since the latter is nothing but the shortening of the former at one position.
Before stating this lower bound, let us recall some notions and notation on cyclotomic classes. We call a *cyclotomic class* an orbit of $\mathbb{Z}/(q^2-1)\mathbb{Z}$ for the multiplication by q. One sees easily that, in this situation, cyclotomic classes contain either one or two elements. For instance $\{0\}$, $\{q+1\}$ or $\{1, q\}$ are cyclotomic classes. From now, on, we denote by B the set of smallest elements in the cyclotomic classes. For all $b \in B$, we denote by I_b the corresponding class and by n_b the cardinality of I_b. In addition, we denote by A the set $\{0, \ldots, t(q+1)-1\}$. From [12, Theorem 4.4] (applied to $m = 2$), we have

$$\dim_{\mathbb{F}_q}(RS_{q^2-t(q+1)}(L))_{|\mathbb{F}_q} = q^2 - 2t(q+1) + \sum_{b \in B \cap A} (2(|I_b \cap A| - 1) + 2 - n_b). \tag{19}$$

Actually, [12, Theorem 4.4] is an inequality, but below this statement in [12], the equality cases are discussed and equality holds always for a full support.
The sum in (19) involves two kinds of cyclotomic classes, namely:

- the classes I_b with $I_b \subset A$ and $n_b = 1$. These classes are $\{0\}, \{q+1\}, \ldots, \{(t-1)(q+1)\}$. Their number is equal to t.
- the classes I_b with $I_b \subset A$ and $n_b = 2$. These classes are of the form $\{a_0 + a_1 q, a_0 q + a_1\}$ for $(a_0, a_1) \in \{0, \ldots, t\}^2$ and $a_0 \neq a_1$. The number of such classes is $\binom{t+1}{2}$.

It is easy to observe that the other cyclotomic classes have no contribution in the sum in (19). Consequently, we get

$$\begin{aligned}\dim_{\mathbb{F}_q}(RS_{q^2-t(q+1)}(L))_{|\mathbb{F}_q} &= q^2 - 2t(q+1) + 2\binom{t+1}{2} + t \\ &= q^2 - 2t(q+1) + t(t+2).\end{aligned}$$

Now, if L is an arbitrary support, then, from Lemma 7, the code $\Gamma_q\left(L, g^{q+1}\right)$ is the shortening of a full support Goppa code. Hence it is $\mathbb{F}_q$–equivalent to the shortening of $RS_{q^2-r(q+1)}(L_0)_{|\mathbb{F}_q}$, where L_0 denotes a full support. Therefore, the general case results straightforwardly from the full support case. □

Remark 6. If we reconsider the wild Goppa code $\Gamma_q\left(L, g^{q-1}\right)$ whose designed dimension is $n - 2t(q-1)$, we see that if $t \geqslant 3$ then the actual dimension is larger and the difference between the actual and the designed dimension is $t(t-2)$. It is quadratic in t.

Table 1 lists the parameters of some of these codes. It turns out that all these parameters reach those of the best known codes listed in [10].

	$q=5$	$q=7$	$q=8$	$q=9$
$\deg(g)=3$	[25 , 4 , ⩾ 19]	[49, 16, ⩾ 25]	[64, 25, ⩾ 28]	[81, 36, ⩾ 31]
$\deg(g)=4$	-	[49, 9, ⩾ 33]	[64, 16, ⩾ 37]	[81, 25, ⩾ 41]
$\deg(g)=5$	-	[49, 4, ⩾ 41]	[64, 9, ⩾ 46]	[81, 16, ⩾ 51]
$\deg(g)=6$	-	-	[64, 4, ⩾ 55]	[81, 9, ⩾ 61]
$\deg(g)=7$	-	-	-	[81, 4, ⩾ 71]

Table 1: Parameters of Wild Goppa codes over a quadratic extension ($m = 2$).

4.2 Further examples

Now, let us consider the case of cubic extensions, that is $m = 3$ and the particular case of a polynomial g of degree 1. First, let us state a general result on the dimension of such codes from cubic extensions.

Theorem 25. *Let $g \in \mathbb{F}_{q^3}[x]$ be a polynomial of degree t and $L \in \mathbb{F}_{q^3}^n$ be a support of length n avoiding the roots of g. Then,*

$$\dim_{\mathbb{F}_q} \Gamma_q\left(L, g^{q^2+q+1}\right) \geqslant n - 3t(q^2+q+1) + 2t + 2t(t+1)(t+2) + 3(q-1-t)t(t+1)$$

and equality holds if L is a full support or has length q^3-1.

Proof. We use the very same techniques as in the proof of Theorem 24 and use the same notation with the only change that here cyclotomic classes are subsets of $\mathbb{Z}/(q^3-1)\mathbb{Z}$ and $A = \{0, \dots, t(q^2+q+1)-1\}$. Here [12, Theorem 4.4] asserts that

$$\dim_{\mathbb{F}_q} \Gamma_q\left(L, g^{q^2+q+1}\right) \geqslant n - 3t(q^2+q+1) + \sum_{b \in B \cap A} (m(|I_b \cap A| - 1) + m - n_b). \tag{20}$$

We consider three kinds of cyclotomic classes.

- The classes $\{0\}, \{q^2+q+1\}, \dots, \{(t-1)(q^2+q+1)\}$. Their number is t, they satisfy $n_b = 1$ and $|I_b \cap A| = 1$. They yield a term $2t$ in the sum in the second member of (20).
- The classes $\left\{\{a_0 + a_1 q + a_2 q^2\}, \{a_2 + a_0 q + a_1 q^2\}, \{a_1 + a_2 q + a_0 q^2\}\right\}$ for $a_i \leqslant t$ and at least one of the a_i's is distinct from the others. They satisfy $n_b = 3$, $|I_b \cap A| = 3$ and their number is $\frac{(t+1)^3-(t+1)}{3}$. They provide a term $2t(t+1)(t+2)$ in the sum in the second member of (20).
- The classes $\left\{\{a_0 + a_1 q + a_2 q^2\}, \{a_2 + a_0 q + a_1 q^2\}, \{a_1 + a_2 q + a_0 q^2\}\right\}$ for $t < a_2 \leqslant q-1$ and $0 \leqslant a_0 < t$ and $0 \leqslant a_1 \leqslant t$. They satisfy $n_b = 3$ and $|I_b \cap A| = 2$. Their number is $(q-1-t)((t+1)^2 - (t+1))$ and they provide a term $3(q-1-t)t(t+1)$ in the sum in the second member of (20).

It can be checked that no other cyclotomic class contributes in the sum in (20) and combining the three above items, we get the result. □

Now, let us focus on the case of a polynomial g of degree 1. For the support L we take a vector of length q^3-1 listing every element of $\mathbb{F}_{q^3}$ but the single root of g. Here, Theorem 25 gives

$$\dim_{\mathbb{F}_q} \Gamma_q\left(L, g^{q^2+q+1}\right) \geqslant (q^3-1) - 3(q^2+q+1) + 14 + 6(q-2). \tag{21}$$

On the other hand, the classical bound for alternant codes yields

$$\dim_{\mathbb{F}_q} \Gamma_q\left(L, g^{q^2+q}\right) \geqslant (q^3-1) - 3(q^2+q). \tag{22}$$

Obviously, since we have the inclusion $\Gamma_q\left(L, g^{q^2+q+1}\right) \subset \Gamma_q\left(L, g^{q^2+q}\right)$, and comparing the bounds, we see that (22) is far from being sharp and that (21) gives a better lower bound for the dimension of the code $\Gamma_q\left(L, g^{q^2+q}\right)$. In addition, Theorem 4 asserts that $\Gamma_q\left(L, g^{q^2+q}\right)$ might have one dimension more than $\Gamma_q\left(L, g^{q^2+q+1}\right)$. This is what happens in general. In Table 2, we give the parameters of such Goppa codes when the polynomial g is x. The true dimensions have been verified with MAGMA [7]. They coincide with the above discussed lower bounds.

	$q=4$	$q=5$	$q=7$	$q=8$
$\Gamma_q\left(L, x^{q^2+q+1}\right)$	[63, 26, ⩾ 22]	[124, 63, ⩾ 32]	[342, 215, ⩾ 58]	[511, 342, ⩾ 74]
$\Gamma_q\left(L, x^{q^2+q}\right)$	[63, 27, ⩾ 21]	[124, 64, ⩾ 31]	[342, 216, ⩾ 57]	[511, 343, ⩾ 73]

Table 2: Parameters of wild Goppa codes with $g = x$ and $m = 3$.

Conclusion

We proved two new identities relating so–called wild Goppa codes. The first one asserts that if g is a polynomial with no roots in $\mathbb{F}_{q^m}$, then $\Gamma_q\left(L, g^{q^{m-1}+\cdots+q^2+q}\right) = \Gamma_q\left(L, g^{q^{m-1}+\cdots+q^2+q+1}\right)$. The second one asserts that if g has roots in $\mathbb{F}_{q^m}$ then, the equality fails but the difference of the $\mathbb{F}_q$–dimensions of the two codes is bounded above by the number of distinct roots of g in $\mathbb{F}_{q^m}$. The corresponding codes are of particular interest since they turn out to be extended or shortened BCH codes and have a very high dimension compared to the designed dimension of alternant codes.
It should be pointed out that the proofs of our main results in the present article involve duals of Goppa codes. Getting direct proofs of such identities involving only the rational fractions used to define Goppa codes would be of interest.

Acknowledgements

The authors express their deep gratitude to Sergey Bezzateev for his careful reading and its relevant comments on this work.

References

[1] D. J. Bernstein, T. Lange, and C. Peters. Wild McEliece. In *Selected Areas in Cryptography*, pages 143–158, 2010.

[2] D. J. Bernstein, T. Lange, and C. Peters. Wild McEliece incognito. In *PQCrypto*, pages 244–254, 2011.

[3] S. V. Bezzateev and N. A. Shekhunova. A subclass of binary Goppa codes with improved estimation of the code dimension. *Des. Codes Cryptogr.*, 14(1):23–38, 1998.

[4] S. V. Bezzateev and N. A. Shekhunova. Chain of separable binary Goppa codes and their minimal distance. *IEEE Trans. Inform. Theory*, 54(12):5773–5778, 2008.

[5] S. V. Bezzateev and N. A. Shekhunova. Cumulative-Separable codes. ArXiv:1005.1524v1, 2010.

[6] J. Bierbrauer and Y. Edel. New code parameters from Reed-Solomon subfield codes. *IEEE Trans. Inform. Theory*, 43(3):953–968, 1997.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] A. Couvreur. Codes and the Cartier operator. To appear in Proc. Amer. Math. Soc., 2012. ArXiv:1206.4728.

[9] V. D. Goppa. A new class of linear correcting codes. *Probl. Peredachi Inf.*, 6(3):24–30, 1970.

[10] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2013-09-05.

[11] M. Hattori, R. J. McEliece, and G. Solomon. Subspace subcodes of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 44(5):1861–1880, 1998.

[12] F. Hernando, K. Marshall, and M. E. O'Sullivan. The dimension of subcode-subfields of shortened generalized Reed–Solomon codes. *Des. Codes Cryptogr.*, 69(1):131–142, 2012.

[13] G. L. Katsman and M. A. Tsfasman. A remark on algebraic geometric codes. In *Representation theory, group rings, and coding theory*, volume 93 of *Contemp. Math.*, pages 197–199. Amer. Math. Soc., Providence, RI, 1989.

[14] Q. Liao. On Reed-Solomon codes. *Chin. Ann. Math. Ser. B*, 32(1):89–98, 2011.

[15] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[16] M. Loeloeian and J. Conan. A transform approach to Goppa codes. *IEEE Trans. Inform. Theory*, 33(1):105–115, 1987.

[17] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[18] R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[19] A. Roseiro, J. Hall, J. Adney, and M. Siegel. The trace operator and redundancy of Goppa codes. *IEEE Trans. Inform. Theory*, 38(3):1130–1133, 1992.

[20] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa. Further results on Goppa codes and their applications to constructing efficient binary codes. *IEEE Trans. Inform. Theory*, 22(5):518–526, 1976.

[21] M. Van Der Vlugt. The true dimension of certain binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(2):397–398, 1990.

[22] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999.

[23] P. Véron. Goppa codes and trace operator. *IEEE Trans. Inform. Theory*, 44(1):290–294, 1998.

[24] P. Véron. True dimension of some binary quadratic trace Goppa codes. *Des. Codes Cryptogr.*, 24(1):81–97, 2001.

[25] P. Véron. Proof of conjectures on the true dimension of some binary Goppa codes. *Des. Codes Cryptogr.*, 36(3):317–325, 2005.

[26] M. Wirtz. On the parameters of Goppa codes. *IEEE Trans. Inform. Theory*, 34(5, part 2):1341–1343, 1988. Coding techniques and coding theory.