Codes and the Cartier Operator

Alain Couvreur

CODES AND THE CARTIER OPERATOR

ALAIN COUVREUR

ABSTRACT. In this article, we present a new construction of codes from algebraic curves. Given a curve over a non-prime finite field, the obtained codes are defined over a subfield. We call them *Cartier Codes* since their construction involves the Cartier operator. This new class of codes can be regarded as a natural geometric generalisation of classical Goppa codes. In particular, we prove that a well-known property satisfied by classical Goppa codes extends naturally to Cartier codes. We prove general lower bounds for the dimension and the minimum distance of these codes and compare our construction with a classical one: the subfield subcodes of Algebraic Geometry codes. We prove that every Cartier code is contained in a subfield subcode of an Algebraic Geometry code and that the two constructions have similar asymptotic performances.

We also show that some known results on subfield subcodes of Algebraic Geometry codes can be proved nicely by using properties of the Cartier operator and that some known bounds on the dimension of subfield subcodes of Algebraic Geometry codes can be improved thanks to Cartier codes and the Cartier operator.

MSC: 11G20, 14G50, 94B27
Key words: Algebraic Geometry codes, differential forms, Cartier operator, subfield subcodes, classical Goppa codes.

INTRODUCTION

It is well-known that, with a high probability, a random code is good. However, getting explicit asymptotically good families of codes is not a simple task. In the beginning of the eighties Tsfasman, Vlăduţ and Zink [16] and independently Ihara [7], proved the existence of asymptotically good infinite families of Algebraic Geometry codes (AG codes) over $\mathbf{F}_q$ for all $q \geq 5$. They proved in particular that for a square $q \geq 49$, some families of AG codes over $\mathbf{F}_q$ beat the Gilbert–Varshamov bound.

For small values of q and in particular for $q = 2$, the use of AG codes does not seem to be suitable to produce asymptotically good families of codes. A classical approach to construct good codes over small fields is to construct good codes over a finite extension and then use a "descent" operation such as *trace codes* or *subfield subcodes* (see [13, Chapter 9]). This is for instance the point of BCH codes, classical Goppa codes or more generally of alternant codes. For this reason, studying subfield subcodes of AG code is natural.

As far as we know, the first contributions on subfield subcodes of AG codes are due to Katsman and Tsfasman [8] and independently to Wirtz [17]. Both obtained lower bounds for the dimension of such codes exceeded the generic formulas for subfield subcodes. Upper bounds on the covering radius and the minimum distance of such codes are proved by Skorobogatov in [11]. Subsequently, Stichtenoth showed in [12] that the lower bounds for the dimension due to Katsman et al. and Wirtz are the consequence of a general result on subfield subcodes.

This article presents a new construction of codes on a finite field $\mathbf{F}_q$ from a curve over an extension $\mathbf{F}_{q^\ell}$. Our method differs from that of the above-cited references

since it is not based on the use of the subfield subcode operation. The key point of our method is to use differentials fixed by Cartier, that is logarithmic differentials. This is the reason why, we call these codes *Cartier codes* and denote them by $Car_q(D,G)$. These *Cartier codes* can be regarded as a natural generalisation of classical Goppa codes, which turn out to be Cartier codes from a curve of genus 0. Moreover, it is well-known that given a squarefree polynomial f, the classical Goppa codes associated to f^{q-1} and f^q are equal and, as we show in Theorem 4.4, this property extends naturally to Cartier codes.

We then study the relations between Cartier codes and the subfield subcodes of AG codes. We prove that a Cartier code is a always a subcode of such a subfield subcode and prove Theorem 5.1 yielding an upper bound for the dimension of the corresponding quotient space. We discuss the minimum distance of Cartier codes and prove two lower bounds for their dimensions in Theorems 6.1 and 6.3. Finally, thanks to Cartier codes and the Cartier operator, we improve in Corollary 6.5 the known estimates for the dimension of subfield subcodes of AG codes $C_\Omega(D,G)_{|\mathbf{F}_q}$ when G is non-positive. We also observe that Cartier codes have similar asymptotic performances as subfield subcodes of AG codes.

Thanks to our approach involving the Cartier operator, we are able to give new proofs of some results on subfield subcodes of AG codes. Such new proofs, which are clearly less technical than the original ones are presented in §4.1 and Remark 5.2. As far as we know, the Cartier operator has never been used in algebraic geometric coding theory up to now.

This article is organised as follows. Basic notions on subfield subcodes and classical Goppa codes are recalled in Section 1. Section 2 is a brief review on AG codes and known results on their subfield subcodes. After recalling the definition together with some basic features of the Cartier operator, we prove a vanishing property of this map in Section 3. In Section 4, we introduce Cartier codes. We compare them with subfield subcodes of AG codes in Section 5. In Section 6, we discuss the parameters and the asymptotic performances of Cartier codes and subfield subcodes of AG codes. Section 7 is devoted to examples of Cartier codes from the Klein quartic which illustrate the previous results.

1. Preliminaries: Classical Goppa codes

Notation 1.1. Consider a finite extension $\mathbf{F}_{q^\ell}/\mathbf{F}_q$ of finite fields and let C be a code of length n over $\mathbf{F}_{q^\ell}$. The subfield subcode $C \cap \mathbf{F}_q^n$ over $\mathbf{F}_q$ is denoted by $C_{|\mathbf{F}_q}$.

Lemma 1.2. *Let C be a code over $\mathbf{F}_{q^\ell}$ with parameters $[n, n-r, d]_{q^\ell}$, then $C_{|\mathbf{F}_q}$ has parameters $[n, \geq n-\ell r, \geq d]_q$.*

Proof. [13, Lemma 9.1.3] □

Definition 1.3 (Classical Goppa codes)**.** Let $L := (\alpha_1, \dots, \alpha_n)$ be an ordered n–tuple of distinct elements of a field $\mathbf{F}_{q^\ell}$. Let $f \in \mathbf{F}_{q^\ell}[x]$ be a polynomial which does not vanish at any of the elements of L. The Goppa code $\Gamma_q(L,f)$ is defined by

$$\Gamma_q(L,f) := \left\{ (c_1,\dots,c_n) \in \mathbf{F}_q^n \;\middle|\; \sum_{i=1}^{n} \frac{c_i}{x-\alpha_i} \equiv 0 \mod (f) \right\}.$$

One can prove that $\Gamma_q(L,f)$ is alternant, i.e. is a subfield subcode of a Generalised Reed–Solomon code over $\mathbf{F}_{q^\ell}$ ([9, Theorem 12.3.4]) with parameters $[n, n-\deg(f), \deg(f)+1]_{q^\ell}$. From Lemma 1.2, the code $\Gamma_q(L,f)$ has parameters

$$[n, \geq n-\ell\deg(f), \geq \deg(f)+1]_q.$$

These estimates can be improved in some situations thanks to the following well–known result.

Theorem 1.4. *Let L and f be as in Definition 1.3. If f is squarefree. Then,*

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

Thus, the parameters of this code satisfy $[n, \geq n - \ell(q-1)\deg(f), \geq q\deg(f)+1]_q$.

Proof. See [14] or [1, Theorem 4.1]. □

Another proof of Theorem 1.4 involving the Cartier operator is given in § 4.1.

Remark 1.5. A more general version of the statement could be, let $f_1, \ldots, f_s$ and $h_1, \ldots, h_t$ be irreducible polynomials in $\mathbf{F}_{q^\ell}[x]$, let $a_1, \ldots, a_s, b_1, \ldots, b_t$ be positive integers such that for all i, $a_i \equiv q-1 \mod q$ and for all j, $b_j \not\equiv q-1 \mod q$, then

$$\Gamma_q(L, f_1^{a_1} \cdots f_s^{a_s} h_1^{b_1} \ldots h_t^{b_t}) = \Gamma_q(L, f_1^{a_1+1} \cdots f_s^{a_s+1} h_1^{b_1} \ldots h_t^{b_t}).$$

2. Algebraic Geometry codes

2.1. **Caution.** Since AG codes have been introduced by Goppa in [5], they are frequently referred as *Goppa codes* or *geometric Goppa codes*. However, AG codes are not a generalisation of classical Goppa codes since they do not involve the subfield subcode operation. Actually, AG codes are a generalisation of Reed–Solomon Codes.

2.2. **Context, notation and prerequisites.** In this article, a curve is smooth projective and geometrically irreducible. Given a curve X over a field $\mathbf{F}$. We denote by F its function field, by $\Omega_{F/\mathbf{F}}$ its space of rational differential forms and by g its genus. Given a place P of F, we denote respectively by $\mathcal{O}_{X,P}$, $\mathfrak{m}_{X,P}$, $\mathbf{F}_q(P)$ and ν_P the local ring at P, its maximal ideal, the residue field and the valuation at P. For a divisor A on X, we denote by $L(A)$ the space $L(A) := H^0(X, \mathcal{O}_X(A))$ and by $\Omega(A)$ the space $\Omega(A) := H^0(X, \Omega_X \otimes \mathcal{O}_X(-A))$. The $\mathbf{F}_q$–dimensions of these spaces are respectively denoted by $h^0(A)$ and $h^1(A)$.

Definition 2.1. Let X be a curve over $\mathbf{F}_q$, let G be a divisor on X and $P_1, \ldots, P_n$ be distinct rational points of X avoiding the support of G. Set $D := P_1 + \cdots + P_n$. The code $C_\Omega(D, G)$ is defined as the image of the map

$$\mathrm{res}_D : \begin{cases} \Omega(G-D) & \longrightarrow & \mathbf{F}_q^n \\ \omega & \longmapsto & (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) \end{cases}.$$

If $\deg(G) > 2g-2$ (or at least if $h^1(G) = 0$), then the dimension and the minimum distance of such a code satisfy the following well–known lower bounds.

$$\dim(C_\Omega(D,G)) \geq n - (\deg(G) + 1 - g) \tag{1}$$

$$d(C_\Omega(D,G)) \geq \deg(G) + 2 - 2g. \tag{2}$$

Example 2.2. With the notations of Definition 1.3, let X be the projective line over $\mathbf{F}_q$, let $P_1, \ldots, P_n$ be the points of coordinates $((\alpha_1 : 1), \ldots, (\alpha_n : 1))$ and P be the point $(1 : 0)$. Regarding f as a rational function on $\mathbf{P}^1$, let $E := (f)_0$ be the divisor of the zeroes of f. The Goppa code $\Gamma_q(L, f)$ is nothing but $C_\Omega(D, E - P)_{|\mathbf{F}_q}$ (see [6, Example 3.4]).

To conclude these prerequisites, we recall the following definition which is useful in what follows.

Definition 2.3. A positive divisor G on a curve X is said to be *reduced* if the corresponding subscheme of X is reduced. That is, G is a formal sum of places $G = m_1Q_1 + \cdots + m_sQ_s$, where all the m_i's are equal to 1.

2.3. **Subfield subcodes of Algebraic Geometry codes.** Given a curve X on $\mathbf{F}_{q^\ell}$ with $\mathbf{F}_{q^\ell}$–divisors D, G as in Definition 2.1. Let us consider the code $C_\Omega(D,G)_{|\mathbf{F}_q}$. Lemma 1.2 together with (1) and (2) assert that if $h^1(G) = 0$, then this code over $\mathbf{F}_q$ has parameters

$$[n, k \geq n - \ell(\deg(G) + 1 - g), d \geq \deg(G) + 2 - 2g].$$

The lower bound for the dimension has been improved by Kastman and Tsfasman [8] and independently by Wirtz [17] under some condition on G. Namely, if $\deg(G) > 2g-2$ and $G \geq qG_1 \geq 0$ for some divisor G_1, then from [17, Theorem 1],

$$k \geq n - 1 - \ell \deg(G - G_1) + \ell h^1(G_1). \tag{3}$$

Subsequently, Stichtenoth proved the following generalisation of (3).

Theorem 2.4 ([12, Theorem 4])**.** *Let X be a curve over $\mathbf{F}_{q^\ell}$. Let G, D be as in Definition 2.1 and $G \geq qG_1$ (possibly non positive), then*

$$\dim(C_\Omega(D,G)_{|\mathbf{F}_q}) \geq \begin{cases} n - 1 - \ell(h^0(G) - h^0(G_1)) & \text{if} \quad G \geq 0 \\ n - \ell(h^0(G) - h^0(G_1)) & \text{if} \quad G \not\geq 0 \end{cases}.$$

Remark 2.5. The original statement [12, Theorem 4] requires the hypothesis $\deg(G) < n$. This hypothesis is actually useless. Indeed, [12, Theorem 1] gives

$$\dim(C_\Omega(D,G)_{|\mathbf{F}_q}) \geq \begin{cases} n - 1 - \ell(h^0(G) - h^0(G-D) - h^0(G_1) + h^0(G_1 - D)) & \text{if} \quad G \geq 0 \\ n - \ell(h^0(G) - h^0(G-D) - h^0(G_1) + h^0(G_1 - D)) & \text{if} \quad G \not\geq 0 \end{cases},$$

which is at least as good as Theorem 2.4.

Remark 2.6. For $h^1(G) = 0$ and $G \geq 0$, Theorem 2.4 gives exactly (3).

On the other hand, Wirtz proposed also a generalisation of Theorem 1.4.

Theorem 2.7 ([17, Theorem 2])**.** *Let X, D, G, G_1 be as in Theorem 2.4. Assume that $\deg(G_1) \geq 2g-2$ and $G_1 \geq 0$. Let G_U be the reduced divisor defined as the sum of the places P such that $v_P(G) \equiv q - 1 \mod q$. Then,*

$$C_\Omega(D,G)_{|\mathbf{F}_q} = C_\Omega(D, G + G_U)_{|\mathbf{F}_q}.$$

3. The Cartier operator

The Cartier operator is a semi-linear endomorphism of the space of rational differential forms in positive characteristic. In terms of Serre duality, it corresponds to the adjoint of the Frobenius map.

We keep the context of Section 2. Moreover, in what follows, x denotes a separating element of $F/\mathbf{F}_q$ ([13, §3.10]). We denote by p the characteristic of F and by $\mathbf{F}_p$ the corresponding prime field.

Definition 3.1 (The Cartier operator)**.** Let $\omega \in \Omega_{F/\mathbf{F}_q}$. There exists $f_0, \ldots, f_{p-1}$ such that $\omega = (f_0^p + f_1^p x + \cdots + f_{p-1}^p x^{p-1})\,dx$. The Cartier operator $\mathscr{C}$ is defined by

$$\mathscr{C}(\omega) := f_{p-1}\,dx.$$

The definition does not depend on the choice of x (see [10, Proposition 1]).

3.1. **Local and global Properties of the Cartier operator.** We refer the reader to [3, 4, 10, 15] for the proofs of the following statements.

Proposition 3.2 (Local properties of $\mathscr{C}$)**.** *Let P be a place of F. For all $\omega \in \Omega_{F/\mathbf{F}_{q^\ell}}$,*

(i) $v_P(\omega) \geq 0 \implies v_P(\mathscr{C}(\omega)) \geq 0$;
(ii) $v_P(\omega) \leq -2 \implies v_P(\mathscr{C}(\omega)) > v_P(\omega)$;
(iii) $v_P(\omega) = -1 \implies v_P(\mathscr{C}(\omega)) = -1$;
(iv) $res_P(\mathscr{C}(\omega)) = res_P(\omega)^{1/p}$.

Proposition 3.3 (Global Properties of $\mathscr{C}$)**.** *For all $\omega \in \Omega_{F/\mathbf{F}_q}$ and all $f \in F$,*

(i) $\mathscr{C}(f^p\omega) = f\mathscr{C}(\omega)$;
(ii) $\mathscr{C}(\omega) = 0 \iff \exists h \in F,\ \omega = dh$;
(iii) $\mathscr{C}(\omega) = \omega \iff \exists h \in F,\ \omega = \frac{dh}{h}$.

Notation 3.4. From now on, for $q = p^\ell$, we denote by $\mathscr{C}_q$ the ℓ times iterated Cartier operator $\mathscr{C}_q := \mathscr{C}^\ell$. This map is $\mathbf{F}_q$–linear. Replacing p by q, Propositions 3.2(i–iv) and 3.3(i) extend naturally to $\mathscr{C}_q$.

Corollary 3.5. *Let $\omega \in \Omega_{F/\mathbf{F}_q}$ and P be a place of F . Then*

$$v_P(\mathscr{C}_q(\omega)) \geq \left\lfloor \frac{v_P(\omega)}{q} \right\rfloor$$

and the above inequality holds even if $v_P(\omega)$ is negative.

Proof. Set $s := v_P(\omega)$ and let b, r be such that $s = bq + r$ with $q > r \geq 0$. Clearly, $b = \lfloor s/q \rfloor$. Let z be a uniformising parameter at P . There exists $\mu \in \Omega_{F/\mathbf{F}_q}$ with $v_P(\mu) \geq 0$ such that $\omega = z^{bq}\mu$. Then, from Proposition 3.3(i), we have $\mathscr{C}_q(\omega) = z^b\mathscr{C}_q(\mu)$ and, from Proposition 3.2(i), we have $v_P(\mathscr{C}_q(\mu)) \geq 0$. Thus, $v_P(\mathscr{C}_q(\omega)) \geq b$, which concludes the proof. □

Corollary 3.6. *Let H be a (possibly non-positive) divisor on X and H_1 be another divisor such that $H \geq qH_1$. Then, for all $\omega \in \Omega(H)$, we have $\mathscr{C}_q(\omega) \in \Omega(H_1)$.*

Proof. It is a straightforward consequence of Corollary 3.5. □

3.2. **The key vanishing lemma.** The following result is crucial in what follows.

Theorem 3.7. *Let $\omega \in \Omega_{F/\mathbf{F}_q}$, let P be a place of F and s be a positive integer. Assume that $\mathscr{C}_q(\omega) = \omega$ and $v_P(\omega) \geq sq - 1$ for some positive integer s, then $v_P(\omega) \geq sq$.*

Proof. Let z be a uniformising parameter at P. The differential form ω is of the form $\omega = z^{sq-1}\mu$, where $v_P(\mu) \geq 0$. Set $\alpha := \mathrm{res}_P(z^{-1}\mu) \in \mathbf{F}_q(P)$. Since the residue field $\mathbf{F}_q(P)$ is perfect, $\alpha^{1/q}$ is also an element of $\mathbf{F}_q(P)$. Let $a \in \mathscr{O}_{X,P}$ be a function such that $a \equiv \alpha^{1/q} \mod \mathfrak{m}_{X,P}$. Then, $v_P(\mu - a^q dz) \geq 1$ and hence $\mu = a^q dz + z\eta$ with $v_P(\eta) \geq 0$. Therefore, we have $\omega = z^{sq-1}(a^q dz + z\eta)$. Applying $\mathscr{C}_q$ and using Propositions 3.2 and 3.3, we get

$$\begin{aligned} \mathscr{C}_q(\omega) &= az^s\mathscr{C}_q\left(\frac{dz}{z}\right) + z^s\mathscr{C}_q(\eta) \\ &= az^{s-1}dz + z^s\mathscr{C}_q(\eta). \end{aligned}$$

Since $v_P(\eta) \geq 0$, from Proposition 3.2(i), we have $v_P(\mathscr{C}_q(\eta)) \geq 0$. In addition, since $s > 0$ we have $s - 1 < sq - 1$ and the assumption $\mathscr{C}_q(\omega) = \omega$, entails $v_P(a) > 0$, that is $v_P(\omega) = v_P(z^{sq-1}(a^q dz + z\eta)) \geq sq$. □

4. Codes defined using the Cartier operator

In this section, we introduce a new class of codes which turn out to be a natural geometric generalisation of classical Goppa codes.

4.1. **Motivation.** To motivate our construction, let us give an alternative proof of Theorem 1.4. In some sense, it is a geometric version of the proof based on the error–locator polynomial [9, Theorem 12.6].

Proof of Theorem 1.4. Inclusion "$\supseteq$" is elementary. Conversely, using the notations of Example 2.2, we know that $\Gamma_q(L, f^{q-1}) = C_\Omega(D, (q-1)E-P)_{|\mathbf{F}_q}$, where E is the divisor of the zeroes of f. Let $c \in C_\Omega(D,(q-1)E-P)_{|\mathbf{F}_q}$. It is the image of a 1–form $\omega \in \Omega((q-1)E-P-D)$ by the map res_D introduced in Definition 2.1. The residues of ω at $P_1,\dots,P_n$ are in $\mathbf{F}_q$. Since ω is regular everywhere but at the P_i's and at P, then from the residue formula, $\mathrm{res}_P(\omega) \in \mathbf{F}_q$.

From Proposition 3.2(iii), the 1–form $\mathscr{C}_q(\omega)$ has valuation ≥ -1 at the P_i's and at P. From Prop 3.2(i) the form $\mathscr{C}_q(\omega)$ is regular out of the P_i's and P. Finally, from Proposition 3.2(iv), the 1–form $\mathscr{C}_q(\omega)$ has the same residues as ω at these points. Thus, $\mathscr{C}_q(\omega)-\omega$ has residues equal to 0 at all the P_i's and at P. Therefore, it is regular everywhere on $\mathbf{P}^1$ and hence is zero. Consequently, $\mathscr{C}_q(\omega)=\omega$. In addition, since f is squarefree, the divisor E is reduced and, using Theorem 3.7, we conclude that $\omega \in \Omega((q-1)E-P-D)$ entails $\omega \in \Omega(qE-P-D)$ and hence $c \in C_\Omega(D,qE-P)_{|\mathbf{F}_q} = \Gamma_q(L,f^q)$. □

If one tries to generalise these arguments to a higher genus curve, the proof fails since, nonzero regular differential forms exist. Therefore, the point of the following construction is to restrict to differential forms fixing $\mathscr{C}_q$.

4.2. **Context.** In this section, X is a curve of genus g over $\mathbf{F}_{q^\ell}$ with $\ell \geq 1$. Let $P_1,\dots,P_n$ a family of $\mathbf{F}_{q^\ell}$–rational points of X and set $D := P_1+\cdots+P_n$. Recall that the function field of X is denoted by F and its space of rational differential forms by $\Omega_{F/\mathbf{F}_{q^\ell}}$. Recall also that we denote by $\mathscr{C}_q$ and the map $\mathscr{C}^\ell$ where $q=p^\ell$ and p is the characteristic.

4.3. **The codes.**

Notation 4.1. Let φ be an endomorphism of a vector space E and $A \subset E$, we denote by A^φ the set of elements of A fixed by φ, that is $A^\varphi := A \cap \ker(\varphi - \mathrm{Id})$.

Definition 4.2 (The code $Car_q(D,G)$)**.** Let G be a divisor on X whose support avoids that of D. The code $Car_q(D,G)$ is a code over $\mathbf{F}_q$ defined as the image of the map.

$$\mathrm{res}_D : \left\{ \begin{array}{ccc} \Omega(G-D)^{\mathscr{C}_q} & \longrightarrow & \mathbf{F}_q^n \\ \omega & \longmapsto & (\mathrm{res}_{P_1}(\omega),\dots,\mathrm{res}_{P_n}(\omega)) \end{array} \right. .$$

Even if $\Omega(G-D)$ is defined over $\mathbf{F}_{q^\ell}$, the code is actually defined over $\mathbf{F}_q$ because of Proposition 3.2(iv). This observation has in particular the following consequence.

Proposition 4.3. *The code $Car_q(D,G)$ is a subcode of $C_\Omega(D,G)_{|\mathbf{F}_q}$.*

In §7.2, we give explicit examples where $Car_q(D,G)$ is a proper subcode $C_\Omega(D,G)_{\mathbf{F}_q}$
The following theorem is a generalisation of Theorem 1.4.

Theorem 4.4. *Let X, D be as in §4.2 and G be a divisor on X whose support avoids that of D. Let G_U be sum of the places P such that $v_P(G) \geq 0$ and $v_P(G) \equiv q-1 \mod q$. Then,*

$$Car_q(D,G) = Car_q(D,G+G_U).$$

Proof. It is a straightforward consequence of Theorem 3.7. □

Corollary 4.5. *Let G_0 be a reduced positive divisor on X and E be another positive divisor. Assume that G_0, E and D have pairwise disjoint supports, then*

$$Car_q(D,(q-1)G_0-E) = Car_q(D,qG_0-E).$$

Remark 4.6. Compared to Wirtz's Theorem 2.7, Theorem 4.4 holds for all divisor G without any condition on its degree, while there exist divisors G such that $C_\Omega(D,G+G_U)_{|\mathbf{F}_q} \subsetneq C_\Omega(D,G)_{|\mathbf{F}_q}$ (see §7.1). For this reason, our new construction seems to be a more natural geometric generalisation of classical Goppa codes than subfield subcodes of AG codes.

5. Comparing the two constructions

Theorem 5.1. *Let X, D, G be as in Definition 2.1 and G_1 be a divisor such that $G \geq qG_1$ and $G \geq G_1$. Then,*

$$\dim_{\mathbf{F}_q} C_\Omega(D,G)_{|\mathbf{F}_q} \big/ Car_q(D,G) \leq \ell h^1(G_1).$$

In particular, $h^1(G_1) = 0 \implies C_\Omega(D,G)_{|\mathbf{F}_q} = Car_q(D,G)$.

Proof. First, notice that $G - D \geq q(G_1 - D)$ and hence, from Corollary 3.5, for all $\omega \in \Omega(G-D)$, we have $\mathscr{C}_q(\omega) \in \Omega(G_1 - D)$. Corollary 3.5 also asserts that if $\omega \in \Omega(G)$, then $\mathscr{C}_q(\omega) \in \Omega(G_1)$.

Now, consider the following morphism of exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega(G) & \longrightarrow & \Omega(G-D) & \xrightarrow{\mathrm{res}_D} & C_\Omega(D,G) & \longrightarrow & 0\,, \\
 & & \downarrow{\scriptstyle \mathscr{C}_q - Id} & & \downarrow{\scriptstyle \mathscr{C}_q - Id} & & \downarrow{\scriptstyle \phi^{-1} - Id} & & \\
0 & \longrightarrow & \Omega(G_1) & \longrightarrow & \Omega(G_1 - D) & \xrightarrow{\mathrm{res}_D} & C_\Omega(D,G_1) & \longrightarrow & 0
\end{array}$$

where res_D is the map introduced in Definition 2.1 and $\phi : \mathbf{F}_{q^\ell}^n \to \mathbf{F}_{q^\ell}^n$ is the coordinate-wise Frobenius map $(c_1,\ldots,c_n) \mapsto (c_1^q,\ldots,c_n^q)$. The left-hand square is clearly commutative and the commutativity of the right–hand one is an easy consequence of Proposition 3.2(iv).

From the Snake Lemma, we get the exact sequence

$$0 \longrightarrow \Omega(G)^{\mathscr{C}_q} \longrightarrow \Omega(G-D)^{\mathscr{C}_q} \longrightarrow C_\Omega(D,G)_{|\mathbf{F}_q} \longrightarrow \Omega(G_1)\big/(\mathscr{C}_q - Id)\Omega(G)\,,$$

which naturally entails

$$0 \longrightarrow Car_q(D,G) \longrightarrow C_\Omega(D,G)_{|\mathbf{F}_q} \longrightarrow \Omega(G_1)\big/(\mathscr{C}_q - Id)\Omega(G)\cdot$$

This yields the result. □

Remark 5.2. Wirtz's Theorem 2.7 is a straightforward consequence of the previous results. Indeed, the condition $\deg(G_1) > 2g-2$ in the statement asserts that $h^1(G_1) = 0$ and hence, from Theorem 5.1, we have $Car_q(D,G) = C_\Omega(D,G)_{|\mathbf{F}_q}$. Applying Theorem 4.4 to the Cartier Codes, we get Wirtz's result.

6. Parameters of Cartier codes

In this section, we give lower bounds for the parameters of Cartier codes and discuss in particular their dimension by giving two distinct lower bounds. The first one derives from Stichtenoth's Theorem 2.4 together with Theorem 5.1. The second one is direct and is proved without using subfield subcodes of AG codes.

Since we always have $Car_q(D,G) \subset C_\Omega(D,G)_{|\mathbf{F}_q}$ (Proposition 4.3), this second lower bound holds for subfield subcodes of AG codes and improves in some situations Stichtenoth's bound.

6.1. **Minimum distance.** In what follows, we denote by $d(C)$ the minimum distance of a code C. A natural lower bound for the minimum distance of the codes $Car_q(D,G)$ is given by the inclusion $Car_q(D,G) \subset C_\Omega(D,G)$ and the Goppa designed distance. Hence

$$d(Car_q(D,G)) \geq d(C_\Omega(D,G)) \geq \deg(G) + 2 - 2g.$$

Moreover, Theorem 4.4 improves the minimum distance in some situation. Namely, in the context of Theorem 4.4, we have

$$d(Car_q(D,G)) \geq \deg(G + G_U) + 2 - 2g.$$

6.2. **First lower bound for the dimension.**

Theorem 6.1. *Let X, D, G be as in Definition 2.1, let G be a divisor on X and G_1 be a divisor such that $G \geq qG_1$ and $G \geq G_1$. Then*

$$\dim_{\mathbf{F}_q}(Car_q(D,G)) \geq \begin{cases} n-1-\ell(h^0(G)-h^0(G_1)+h^1(G_1)) & \text{if} \quad G \geq 0 \\ n-\ell(h^0(G)-h^0(G_1)+h^1(G_1)) & \text{if} \quad G \ngeq 0 \end{cases}. \tag{4}$$

Moreover, if $h^1(G) = 0$, then

$$\dim_{\mathbf{F}_q}(Car_q(D,G)) \geq \begin{cases} n-1-\ell\deg(G-G_1) & \text{if} \quad G \geq 0 \\ n-\ell\deg(G-G_1) & \text{if} \quad G \ngeq 0 \end{cases}. \tag{5}$$

Proof. Inequalities (4) are a straightforward consequence of Theorems 2.4 and 5.1. Inequalities (5) are consequences of (4) together with the Riemann–Roch Theorem. □

Corollary 6.2. *Let G_0 be a reduced positive divisor on X whose support is disjoint from that of D and such that $h^1(qG_0) = 0$. Then the code $Car_q(D, qG_0)$ has parameters satisfying*

$$\begin{array}{rcl} k & \geq & n-1-\ell(q-1)\deg(G_0) \\ d & \geq & q\deg(G_0)+2-2g \end{array}$$

Proof. From Theorem 4.4, we have $Car_q(D,qG_0) = Car_q(D,(q-1)G_0)$. Then, apply Theorem 6.1 to $Car_q(D,(q-1)G_0)$ to get the dimension and apply the bounds of §6.1 to $Car_q(D,qG_0)$ to get the minimum distance. □

6.3. **Second lower bound for the dimension.** The lower bounds for the dimension of Cartier codes of Theorem 6.1 come from Stichtenoth's estimates for the dimension of subfield subcodes. Here, we state a bound which can be proven directly without using subfield subcodes.

Theorem 6.3. *Let X, D, G be as in Definition 2.1. Let G^+, G^- be the two positive divisors with disjoint supports such that $G = G^+ - G^-$. Assume that G^- is reduced and*

that G^+, G^- and D have pairwise disjoint supports. Let s_{G^-} be the number of places supporting G^-. Then,

$$\dim_{\mathbf{F}_q} Car_q(D,G) \geq n-1+s_{G^-}-\ell\deg(G^+)-h^1(G).$$

Proof. Step 1. The code $Car_q(D,G)$ is the image of the $\mathbf{F}_q$–linear map

$$\phi : \left\{ \begin{array}{ccc} \Omega(G-D)^{\mathscr{C}_q} & \longrightarrow & \mathbf{F}_q^n \\ \omega & \longmapsto & (\mathrm{res}_{P_1}(\omega),\ldots,\mathrm{res}_{P_n}(\omega)) \end{array} \right. .$$

The kernel of the map is $\Omega(G)^{\mathscr{C}_q}$ whose $\mathbf{F}_q$–dimension is bounded above by $h^1(G)$. Indeed, notice that $\Omega(G) \supseteq \Omega(G)^{\mathscr{C}_q} \otimes_{\mathbf{F}_q} \mathbf{F}_{q^\ell}$.

Now, let us bound below the dimension of $\Omega(G-D)^{\mathscr{C}_q}$.

Step 2. Obviously, we have $G-D \geq q(-G^- - D)$. Thus, from Corollary 3.5, the following map is well–defined.

$$\mathscr{C}_q - Id : \Omega(G-D) \longrightarrow \Omega(-G^- - D) \tag{6}$$

and the $\mathbf{F}_q$–space, $\Omega(G-D)^{\mathscr{C}_q}$ is its kernel. From now on, denote by V the image of the above map. Notice that V is an $\mathbf{F}_q$–subspace of $\Omega(-G^- - D)$ and not an $\mathbf{F}_{q^\ell}$–subspace in general. We claim that the map (6) is not surjective and will construct a proper $\mathbf{F}_q$–subspace of $\Omega(-G^- - D)$ containing V.

Step 3. Recall that, given a place P of X, we denote by $\mathbf{F}_{q^\ell}(P)$ the corresponding residue field. Let $Q_1,\ldots,Q_{s_{G^-}}$ be the places supporting G^-. Now, consider the $n-1+s_{G^-}$ following $\mathbf{F}_q$–linear forms on $\Omega(-G^- - D)$:

$$\psi_P : \omega \to \mathrm{Tr}_{\mathbf{F}_{q^\ell}(P)/\mathbf{F}_q}(\mathrm{res}_P(\omega)) \quad \text{for } P \in \{Q_1,\ldots,Q_{s_{G^-}},P_1,\ldots,P_{n-1}\}. \tag{7}$$

Elements of V are of the form $\mathscr{C}_q(\omega)-\omega$ and hence, from Proposition 3.2(iv), the traces of their residues are always zero. Therefore, the above–described maps ψ_P vanish on V.

In addition, the $\mathbf{F}_q$–linear forms ψ_P described in (7) are independent on $\Omega(-G^- - D)$. Indeed, for all place $P \in \{Q_1,\ldots,Q_{s_{G^-}},P_1,\ldots,P_{n-1}\}$, Riemann–Roch Theorem asserts that $\Omega(0) \subsetneq \Omega(-P-P_n)$. Then, choose a form $\omega_P \in \Omega(-P-P_n)\setminus\Omega(0)$. From the residue formula, $\mathrm{res}_P(\omega_P) \neq 0$ for all P. The forms $\omega_{Q_1},\ldots,\omega_{Q_{s_{G^-}}},\omega_{P_1},\ldots,\omega_{P_{n-1}}$ are elements of $\Omega(-G^- - D)$ and provide a dual basis for the $\mathbf{F}_q$–linear forms described in (7), which yields the independence of these maps.

Finally, V is contained in the intersection of the kernels of $n-1+s_{G^-}$ independent $\mathbf{F}_q$–linear forms on $\Omega(-G^- - D)$ and hence its codimension in this space is at least $n-1+s_{G^-}$.

Step 4. From Riemann–Roch Theorem and the previous step, the dimension of the image V of the map (6) satisfies

$$\dim_{\mathbf{F}_q}(V) \leq \ell(g+n-1+\deg G^-)-(n-1+s_{G^-}). \tag{8}$$

On the other hand, from Riemann–Roch Theorem, we also have

$$\dim_{F_q}\Omega(G-D) \geq \ell(n-\deg G+g-1). \tag{9}$$

Combining (8), (9) and Step 1, we get the result. □

Remark 6.4. For $G_1 \geq 0$ reduced, $G = qG_1$ and $h^1(G)=0$, then Theorem 6.3 gives the same bound as Theorem 6.1.

6.4. **When Cartier Codes improve the bounds on the dimension of subfield subcodes of Algebraic Geometry codes.**

Corollary 6.5. *Let G_0, G^- be two positive reduced divisors on X such that G_0, G^- and D have pairwise disjoint supports and $h^1(G_0 - G^-) = 0$. Set $G := qG_0 - G^-$ and let s_{G^-} be as in Theorem 6.3. Then,*

$$\dim_{\mathbf{F}_q} C_\Omega(D, qG_0 - G^-)_{|\mathbf{F}_q} \geq n - 1 + s_{G^-} - \ell(q-1)\deg(G_0),$$

which improves Theorem 2.4 as soon as $s_{G^-} > 1$.

Proof. Set $G_1 := G_0 - G^-$. Clearly, we have $G \geq qG_1$ and $G \geq G_1$. From Theorem 5.1, the assumption $h^1(G_0 - G^-) = h^1(G_1) = 0$ entails $Car_q(D,G) = C_\Omega(D,G)_{|\mathbf{F}_q}$. Then, from Theorem 4.4, we have $Car_q(D,(q-1)G_0 - G^-) = Car_q(D, qG_0 - G^-)$. We conclude using Theorem 6.3. □

As a comparison, Stichtenoth's Theorem 2.4, yields $n - \ell(q-1)\deg(G_0)$ as a lower bound for the dimension instead of $n - 1 + s_{G^-} - \ell(q-1)\deg(G_0)$.

6.5. **Infinite families of codes.** Given an infinite family of codes $(C_i)_{i\in\mathbf{N}}$ with parameters $[n_i, k_i, d_i]$ with $n_i \to +\infty$, recall that we denote by R and δ the asymptotic parameters of the family defined as:

$$R := \limsup_{i\to+\infty} \frac{k_i}{n_i} \qquad \delta := \limsup_{i\to+\infty} \frac{d_i}{n_i}.$$

In [8], the authors discuss the asymptotic performances of subfield subcodes of AG codes. For all even ℓ, i.e. when q^ℓ is a square, they prove the existence of infinite families of such codes whose asymptotic parameters satisfy

$$R \geq 1 - \frac{2(q-1)\ell}{q(q^{\ell/2}-1)} - \frac{(q-1)\ell}{q}\delta \qquad \text{for} \qquad \frac{q-2}{q^{\ell/2}-1} \leq \delta \leq \frac{q}{m(q-1)} - \frac{2}{q^{\ell/2}-1}. \tag{10}$$

They prove in particular that such codes reach the Gilbert Varshamov bound for $\delta \sim 0$.

Now, let G_0 be a reduced positive divisor on X such that $q\deg(G_0) > 2g-2$ and consider a family of codes of the form $Car_q(D, qG_0) = Car_q(D,(q-1)G_0)$. Then, from Corollary 6.2, their parameters satisfy

$$k \geq n - 1 - \frac{2(q-1)\ell}{q}g - \frac{(q-1)\ell}{q}d.$$

If ℓ is even and hence if q^ℓ is a square, then the Drinfel'd Vlăduţ Theorem ([15, Theorem 3.2.3]) asserts the existence of a family of Cartier codes whose parameters R, δ satisfy exactly the left–hand inequality of (10). In addition, the existence of a reduced positive divisor G_0 with $q\deg(G_0) > 2g-2$ is asserted whenever the conditions on δ of (10) hold. See [8] for further details on the construction of such a divisor.

As a conclusion, Cartier codes and Subfield subcodes of AG codes have similar asymptotic performances.

7. An Example

Computations are made using Magma [2]. A program generating Cartier Codes is available on the author's webpage.

Consider the Klein Quartic of equation $x^3y + y^3z + xz^3$ over $\mathbf{F}_8$. This curve has genus 3. It has 24 $\mathbf{F}_8$–points including $P_1 := (0:1:0)$, $P_2 := (0:0:1)$ and $P_3 := (1:0:0)$. Denote by $Q_1, \ldots, Q_{21}$ the other rational points. We also introduce 3 places of degree 2. Let w be a primitive element of $\mathbf{F}_8/\mathbf{F}_2$ with minimal polynomial $T^3 + T + 1$ and R_1, R_2, R_3 be the three places of degree 2 defined by the ideals: $\langle y^2 + w^5yz + w^3z^2, x + w^3y + wz\rangle$, $\langle y^2 + w^3yz + w^6z^2, x + w^6y + w^2z\rangle$, $\langle y^2 + yz + z^2, x + y + z\rangle$.

We will construct codes over $\mathbf{F}_2$, i.e. $\ell = 3$. Set

$$\begin{array}{rcl} D & := & Q_1 + \cdots + Q_{21} \\ G_0 & := & R_1 + R_2 + R_3 \\ G^- & := & P_1 + P_2 + P_3. \end{array}$$

Computer-aided calculations give

$$h^1(G_0 - G^-) = 0 \qquad h^1(-G^-) = 5 \tag{11}$$

and the following triple of parameters:

$$\begin{array}{lll} Car_2(D, G_0 - G^-): & [21,6,8]_2 & C_\Omega(D, G_0 - G^-)_{|\mathbf{F}_2}: \quad [21,18,2]_2 \\ Car_2(D, 2G_0 - G^-): & [21,6,8]_2 & C_\Omega(D, 2G_0 - G^-)_{|\mathbf{F}_2}: \quad [21,6,8]_2 \end{array} \tag{12}$$

This example illustrates several results presented before.

7.1. **Illustration of Theorem 4.4.** Theorem 4.4 asserts that

$$Car_2(D, G_0 - G^-) = Car_2(D, 2G_0 - G^-).$$

It is confirmed in (12). Indeed, the inclusion $Car_q(D, G_0 - G^-) \supseteq Car_q(D, 2G_0 - G^-)$ is obvious and both codes have dimension 6. On the other hand, computing the parameters of the codes $C_\Omega(D, G_0 - G^-)_{|\mathbf{F}_2}$ and $C_\Omega(D, 2G_0 - G^-)_{\mathbf{F}_2}$ we observe that the codes are distinct and have respective parameters $[21,18,2]_2$ and $[21,6,8]_2$. Here, Theorem 4.4 holds while

$$C_\Omega(2G_0 - G^-)_{|\mathbf{F}_2} \subsetneq C_\Omega(D, G_0 - G^-)_{|\mathbf{F}_2}.$$

7.2. **Illustration of Theorem 5.1.** Set $G_1 := G_0 - G^-$, we have $2G_0 - G^- \geq 2G_1$ and $2G_0 - G^- \geq G_1$. From (11), G_1 is non special. Thus, Theorem 5.1 asserts that $Car_2(D, 2G_0 - G^-) = C_\Omega(D, 2G_0 - G^-)_{|\mathbf{F}_2}$, which is confirmed by the experience: they both have dimension 6 and, from Proposition 4.3, the Cartier code is contained in the second one.

On the other hand, if we compare $Car_2(D, G_0 - G^-)$ and $C_\Omega(D, G_0 - G^-)_{\mathbf{F}_2}$ one can apply Theorem 5.1 with $G_1 = -G^-$. Then, from (11), we have $h^1(-G^-) = 5$. Since $\ell = 3$, the difference between the codimensions of the codes is at most 15. The actual codimension is 12. It is in particular an example of non equality

$$Car_2(D, G_0 - G^-) \subsetneq C_\Omega(D, G_0 - G^-)_{|\mathbf{F}_2}.$$

7.3. **Illustration of Theorem 6.3.** In this example, Stichtenoth's Theorem 2.4 asserts that $\dim C_\Omega(D, G)_{|\mathbf{F}_2} \geq 3$, while Theorem 6.3 (or Corollary 6.5) asserts that this dimension is at least 5 (we have $s_{G^-} = 3$). As said before, the actual dimension is 6.

CONCLUSION

We give a new construction of codes which seems to be the most natural algebraic geometric generalisation of classical Goppa codes. In particular these codes satisfy equalities which are very similar to the relation $\Gamma(L, f^{q-1}) = \Gamma(L, f^q)$ satisfied by Goppa codes.

In addition, we are able to bound below their parameters. Our bounds on the dimension are obtained by two different manners, first by bounding above the codimension of the Cartier code as a subcode of the corresponding subfield subcode

(Theorems 5.1 and 6.1). Second, by a direct proof without using the known estimates on the dimension of subfield subcodes. This second bound has a nice application to subfield subcodes of AG codes, since it improves in some situations Stichtenoth's bound for the dimension (Theorem 2.4).

ACKNOWLEDGEMENTS

The author wishes to thank Daniel Augot who encouraged him to work on this topic. He also expresses his gratitude to Niels Borne for many inspiring discussions. A part of this work has been done when the author was a Post Doc researcher supported by the French ANR Defis program under contract ANR-08-EMER-003 (COCQ project). Special thanks to the anonymous referee for his/her efficiency and for the relevance of his/her comments.

REFERENCES

[1] D. J. Bernstein, T. Lange, and C. Peters. Wild McEliece. Cryptology ePrint Archive, Report 2010/410, 2010. `http://eprint.iacr.org/`.

[2] 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).

[3] P. Cartier. Une nouvelle opération sur les formes différentielles. *C. R. Acad. Sci. Paris*, 244:426–428, 1957.

[4] P. Cartier. Questions de rationalité des diviseurs en géométrie algébrique. *Bull. Soc. Math. France*, 86:177–251, 1958.

[5] V. D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6):1289–1290, 1981.

[6] T. Høholdt and R. Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 41(6, part 1):1589–1614, 1995.

[7] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28:721–724, 1981.

[8] 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.

[9] 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.

[10] C. S. Seshadri. L'opération de Cartier. Applications. In *Variétés de Picard*, volume 4 of *Séminaire Claude Chevalley*. Secrétariat Mathématiques, Paris, 1958-1959.

[11] A. N. Skorobogatov. The parameters of subcodes of algebraic-geometric codes over prime subfields. *Discrete Appl. Math.*, 33(1–3):205–214, 1991.

[12] H. Stichtenoth. On the dimension of subfield subcodes. *IEEE Trans. Inform. Theory*, 36(1):90–93, 1990.

[13] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[14] 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.

[15] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[16] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

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

INRIA SACLAY ÎLE-DE-FRANCE — CNRS LIX, UMR 7161, ÉCOLE POLYTECHNIQUE, 91128 PALAISEAU CEDEX

E-mail address: `alain.couvreur@lix.polytechnique.fr`