Construction of rational surfaces yielding good codes

Alain Couvreur

▶ **To cite this version:**

HAL Id: inria-00547454

https://hal.inria.fr/inria-00547454

Submitted on 16 Dec 2010

CONSTRUCTION OF RATIONAL SURFACES YIELDING GOOD CODES

ALAIN COUVREUR

ABSTRACT. In the present article, we consider Algebraic Geometry codes on some rational surfaces. The estimate of the minimum distance is translated into a point counting problem on plane curves. This problem is solved by applying the upper bound *à la Weil* of Aubry and Perret together with the bound of Homma and Kim for plane curves. The parameters of several codes from rational surfaces are computed. Among them, the codes defined by the evaluation of forms of degree 3 on an elliptic quadric are studied. As far as we know, such codes have never been treated before. Two other rational surfaces are studied and very good codes are found on them. In particular, a $[57, 12, 34]$ code over $\mathbf{F}_7$ and a $[91, 18, 53]$ code over $\mathbf{F}_9$ are discovered, these codes beat the best known codes up to now.

INTRODUCTION

Algebraic Geometry codes have been first introduced by Goppa in [7] in 1981. A few time after, Tsfasman Vlăduţ and Zink proved in [20] that some families of error–correcting codes beat the Gilbert–Varshamov bound. This unexpected result motivated hundreds of publications on Algebraic Geometry codes.

Goppa's construction ([7]) provides codes from algebraic curves. This approach is extended to arbitrary dimensional varieties by Manin in [21]. However, only few results are known on codes on higher dimensional varieties. Indeed, if the estimation of the minimum distance is an elementary task for codes on curves, it becomes a very hard problem in the higher dimensional case. Therefore, most of the known works on codes from varieties of dimension at least 2, deal with the estimate of the minimum distance of codes on varieties having some particular arithmetical or geometrical property. Among the others (the list is not exhaustive), codes on quadric varieties are studied by Aubry in [1], the parameters of codes on Hermitian surfaces are computed in [4] and [5] and lower bounds for the minimum distance of codes from surfaces with a small arithmetical Picard number are computed by Zarzar in [22].

The work of Zarzar [22] is of particular interest. It shows that surfaces with a small arithmetical Picard number (i.e. the Rank of the Neron–Severi group) provide in general codes with a good minimum distance for given length and dimension. Basically, to have a high minimum distance, the global sections of the line bundle $\mathcal{L}$ used to produce the code should not vanish at too many rational points of the surface. If the arithmetical Picard number is small, the vanishing locus of a global section of $\mathcal{L}$ cannot break into too many irreducible components and hence cannot have too many rational points. The work of Zarzar should be compared with that of Aubry [1] and Edoukou [6] in which codes on elliptic

quadrics turn out to be better than codes on hyperbolic quadrics. Recall that the first ones have arithmetical Picard number 1 and the other ones arithmetical Picard number 2.

Therefore, surfaces with a small arithmetical Picard number seem to be suitable to produce good codes. On the other hand, the estimate of the minimum distance remains a difficult task which is almost equivalent to a problem of estimating the maximal number of rational points of an element of a linear system of curves.

The purpose of the present article is to consider rational surfaces obtained by blowing up the projective plane at few closed points. Such a surface has a small Picard number. Moreover, since the surface is rational, the estimate of the minimum distance is translated into a problem of point counting for plane curves. For any curve, one can use the bound of Aubry and Perret [2]. This bound is sharp when the base field is large. In addition, for plane curves and the bound from Homma and Kim [11] is suitable and sharper that Aubry and Perret's one when the base field is small.

Using this approach, we first study codes on elliptic quadrics and are able to give a lower bound for the minimum distance of the codes obtained by evaluation of forms of degree 3. As far as we know, this study has never been done up to now. Afterwards, we study the codes from two other rational surfaces. The first one (the surface Y) is the projective plane blown up at one rational point and a closed points of degree 4. The second one (the surface Z) is obtained by blowing up the projective plane at one closed point of degree 3. Both surfaces provide good codes. In particular, the surface Z yields a $[57, 12, 34]$ code over $\mathbf{F}_7$ and a $[91, 18, 53]$ code over $\mathbf{F}_9$ which both beat the best known codes given in [8] and [12].

Outline of the article. Prerequisites on Algebraic Geometry codes on surfaces and maximum number of rational points of a curve are recalled in Section 1. Codes on elliptic quadrics in $\mathbf{P}^3$ are studied in Section 2, in particular, the parameters of the code obtained by the evaluation of forms of degree 3 are estimated. In Section 3, we present the construction of two other rational surfaces. Explicit examples of codes on these surfaces are studied and turn out to be very good. In particular, the second surface (the surface Z) provides two codes which beat the best known codes up to now: a $[57, 12, 34]$ code over $\mathbf{F}_7$ and a $[91, 18, 53]$ code over $\mathbf{F}_9$.

1. Prerequisites

In this section, we briefly recall some definitions and properties in algebraic geometry and algebraic geometric coding theory. For further details, we refer the reader to [9] and [15] for algebraic geometry and to [17] and [19] for Algebraic Geometry codes.

1.1. **Notations.** In what follows, X denotes a smooth projective geometrically irreducible surface over a finite field $\mathbf{F}_q$.

1.1.1. *Divisors, linear equivalence and intersection product.* The linear equivalence between two divisors D, D' on X is denoted by $D \sim D'$. The *Picard group* of X, which is the group of linear equivalence classes of divisors, is denoted by $\mathrm{Pic}_{\mathbf{F}_q}(X)$. If X is rational, then its Picard group is finitely generated and its rank is called the *Picard number* of X.

One can define a natural pairing on $\mathrm{Pic}_{\mathbf{F}_q}(X)$ called the *intersection product* ([9] Chapter V, Theorem 1.1). Given two divisor classes D, D' on X, their intersection product is denoted by $D.D'$. Moreover, we denote by D^2 the self-intersection of the class D, that is $D^2 := D.D$.

1.1.2. *Invertible sheaves and line bundles.* Recall that there is a one-to-one correspondence between linear equivalence classes of divisors, isomorphism classes of line bundles over X and isomorphism classes of invertible sheaves on X ([16] Chapter VI §1.4). Given a line bundle $\mathcal{L}$ over X, its space of global sections is denoted by $H^0(X, \mathcal{L})$.

Finally, given an integer m, we denote by $\mathcal{O}_X(m)$ the m–*th twisting sheaf* over X ([9] Chapter II, page 117). If $m \geq 0$, then, given an embedding $X \hookrightarrow \mathbf{P}^r$, the space of global sections $H^0(X, \mathcal{O}_X(m))$ is the space of the restrictions to X of homogeneous polynomials of degree m in $r + 1$ variables. To this sheaf corresponds a line bundle (up to isomorphism), which we also denote by $\mathcal{O}_X(m)$ for convenience's sake.

1.2. **Algebraic Geometry codes.** First, let us recall the definition of an Algebraic Geometry code on a surface.

Definition 1.1 (Manin [21]). Let X be a smooth projective geometrically irreducible surface over a finite field $\mathbf{F}_q$ and $\mathcal{L}$ be a line bundle over X. Let $P_1, \ldots, P_n$ be the set of rational points of X. The code $C_L(X, \mathcal{L})$ is defined as the image of the map

$$(1) \qquad \mathrm{ev} : \left\{ \begin{array}{ccc} H^0(X, \mathcal{L}) & \to & \bigoplus \mathcal{L}_{P_i} \simeq \mathbf{F}_q^n \\ f & \mapsto & (f_{P_1}, \ldots, f_{P_n}) \end{array} \right. .$$

Remark 1.2. Obviously, the above definition depends on the choices of coordinates on the fibres. However, choosing other systems of coordinates yields another code which is isometric to the first one for the Hamming distance. Thus, to study the minimum distance of $C_L(X, \mathcal{L})$, the choice of coordinates on the fibres does not matter.

1.3. **The parameters of codes on surfaces.** Let us recall briefly how to estimate the parameters of a code $C_L(X, \mathcal{L})$.

- The length is elementary: it is the number n of rational points at which sections of the line bundle are evaluated. In the present article, we always consider the whole set of rational points of the surface.
- For the dimension, denote by S the space of global sections of $\mathcal{L}$ vanishing at all the P_i's (this space is in general zero in the following examples). Then, the dimension k of the code is

$$k = \dim H^0(X, \mathcal{L}) - \dim S.$$

- The minimum distance d is

$$d = n - \max \left\{ \sharp V(f)(\mathbf{F}_q) \mid f \in H^0(X, \mathcal{L}) \setminus S \right\},$$

  where $V(f)$ denotes the vanishing locus of f.

Remark 1.3. Using the above notations. If one proves that

$$\max \left\{ \sharp V(f)(\mathbf{F}_q) \mid f \in H^0(X, \mathcal{L}) \setminus \{0\} \right\} \leq n,$$

then the evaluation map described in (1) is obviously injective and hence $S = \{0\}$ and the dimension of the code is that of $H^0(X, \mathcal{L})$.

Obviously, for such codes, the only parameter whose computation is hard is the minimum distance. In general, one only looks for lower bounds. It is worth noting that finding a lower bound for the minimum distance is equivalent with finding an upper bound on the number of rational points of the vanishing locus $V(f)$ of an element $f \in H^0(X, \mathcal{L}) \setminus S$. Therefore, bounds on the number of rational points of a curve play a central rule in the present article.

1.4. **Bounds on the number of rational points of curves.** Since the vanishing locus $V(f)$ of $f \in H^0(X, \mathcal{L})$ is not always smooth and irreducible, the classical Weil bound is not suitable for the present problem. However, Aubry and Perret's bound is suitable.

Theorem 1.4 (Aubry Perret [2]). *Let C be a geometrically irreducible curve over $\mathbf{F}_q$ with arithmetical genus p_C, then*

$$|\sharp C(\mathbf{F}_q) - (q + 1)| \leq p_C \lfloor 2\sqrt{q} \rfloor.$$

Proof. Denote by g_C the geometric genus of C. From [2] §4.1, we have

$$|\sharp C(\mathbf{F}_q) - (q + 1)| \leq (p_C - g_C) + g_C \lfloor 2\sqrt{q} \rfloor.$$

Since $g_C \leq p_C$ and $\lfloor 2\sqrt{q} \rfloor \geq 1$, we get the result. $\square$

Remark 1.5. Notice that a version of Aubry Perret's bound exists for reducible curves in [3]. However, in what follows, when we treat the reducible case, we work component by component.

Aubry Perret's bounds are sharp for large values of q but can be largely improved when q is small. In addition, since we are looking for codes on rational surfaces, most of the curves we will deal with are plane. For plane curves and small values of q, one can use another bound. The following result has been first partially conjectured by Sziklai in [18] and then proved by Homma and Kim in [11].

Theorem 1.6 (Homma Kim [11]). *Let d be a positive integer and C be a plane curve of degree d without $\mathbf{F}_q$–linear component. Then,*

$$\sharp C(\mathbf{F}_q) \leq (d - 1)q + 1$$

except for the case $q = 4$, $d = 4$ and C is projectively equivalent to the curve

$$(2) \qquad K: \quad x^4 + y^4 + z^4 + x^2 y^2 + y^2 z^2 + z^2 x^2 + x^2 yz + xy^2 z + xyz^2 = 0.$$

In the exceptional case above, we have $\sharp C(\mathbf{F}_4) = 14$.

The following corollary of Theorem 1.6 has been suggested by a reviewer.

Corollary 1.7. *Let C be a plane curve of degree d which is not a union of d lines, then*

$$\sharp C(\mathbf{F}_q) \leq (d - 1)q + 2.$$

Proof. If C does not contain any $\mathbf{F}_q$–rational line, then it is a straightforward consequence of Theorem 1.6. Assume that C contains $\mathbf{F}_q$–rational lines and set $C = C_1 \cup C_2$, where C_2 does not contain any $\mathbf{F}_q$–rational line and C_1 is a union of $\mathbf{F}_q$–rational lines. Set $r := \deg(C_1)$. By assumption on C, we have $r < d$. From [14], we have $\sharp C_1(\mathbf{F}_q) \leq rq + 1$ and, if C_2 does not correspond to the exceptional case of Theorem 1.6, then $\sharp C_2(\mathbf{F}_q) \leq (d - r - 1)q + 1$ and we get the result using Theorem 1.6.

In the exceptional case: $q = 4$ and C_2 is projectively equivalent to the curve K described in (2). One checks easily that $K(\mathbf{F}_4) = \mathbf{P}^2(\mathbf{F}_4) \setminus \mathbf{P}^2(\mathbf{F}_2)$. Therefore, each $\mathbf{F}_4$–rational line meets C_2 at least at one $\mathbf{F}_4$–rational point. Therefore, the inequality holds in the exceptional case.   □

2. Codes on an elliptic quadric surface

In this section, we study codes on elliptic quadric surfaces. We refer the reader [10] Part IV, Table 15.4 and §15.3.ɪɪ for a definition of an *elliptic quadric* and for the basic properties of this surface. The aim of this study is first to estimate the parameters of such codes and second to motivate Section 3 in which other rational surfaces yielding good codes are constructed.

2.1. **Previous works on the topic.** Codes of the form $C_L(X, \mathcal{O}_X(2))$ on arbitrary dimensional quadric varieties are first considered by Aubry in [1]. Afterwards, the more specific case of codes $C_L(X, \mathcal{O}_X(2))$ on quadric surfaces is studied in depth by Edoukou in [6]. In both works, it appears that elliptic quadrics turn out to be the ones which provide the best codes in terms of parameters. However, as far as we know, there does not exist any work on the topic using the property of rationality of these varieties.

2.2. **Context and notations.** In this section, we present a new approach for the study of codes on smooth elliptic quadrics and state a lower bound for the minimum distance of the code $C_L(X, \mathcal{O}_X(3))$. This approach is based on the fact that a smooth quadric in $\mathbf{P}^3$ can be obtained by blowing up $\mathbf{P}^2$ at 2 points and then by blowing down the resulting surface along a line.

2.2.1. *Construction of quadrics from the projective plane.* Let P denote a closed point of degree 2 of $\mathbf{P}^2$. After a base field extension, P splits in two conjugated points p and p^φ defined over $\mathbf{F}_{q^2}$, where φ denotes the Frobenius map. We denote by L the unique rational line of $\mathbf{P}^2$ containing P. The surface $\widetilde{X}$ is the surface obtained by blowing up $\mathbf{P}^2$ at P. The blow up map is denoted by $\pi : \widetilde{X} \to \mathbf{P}^2$. We denote by $\widetilde{L}$ the strict transform of L by π and by E the exceptional divisor. Over $\mathbf{F}_{q^2}$, the divisor E splits into a union of two conjugated lines e and e^φ. On $\widetilde{X}$, we have $\widetilde{L}^2 = -1$ and hence, by Castelnuovo's criterion (x[9] Chapter V, Theorem 5.7), this curve is the exceptional divisor of some blow up map. Finally, the surface X obtained by blowing down $\widetilde{X}$ at $\widetilde{L}$ is isomorphic to an elliptic quadric of $\mathbf{P}^3$. We denote by $\psi : \widetilde{X} \to X$ this blow down map and by Q and H the respective images of $\widetilde{L}$ and E by ψ. The divisor H is prime but splits over $\mathbf{F}_{q^2}$ into a pair of conjugated lines denoted by h and h^φ.
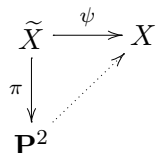
$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{\ \psi\ } & X \\ {\scriptstyle \pi}\Big\downarrow & \nearrow & \\ \mathbf{P}^2 & & \end{array}$$

Figure 1 summarises the above described notations.
Now, let us summarise some properties of the involved surfaces

Summary
- About $\mathbf{P}^2$
  (A) $\operatorname{Pic}_{\mathbf{F}_q}(\mathbf{P}^2) \cong \mathbf{Z}L$ and $L^2 = 1$.
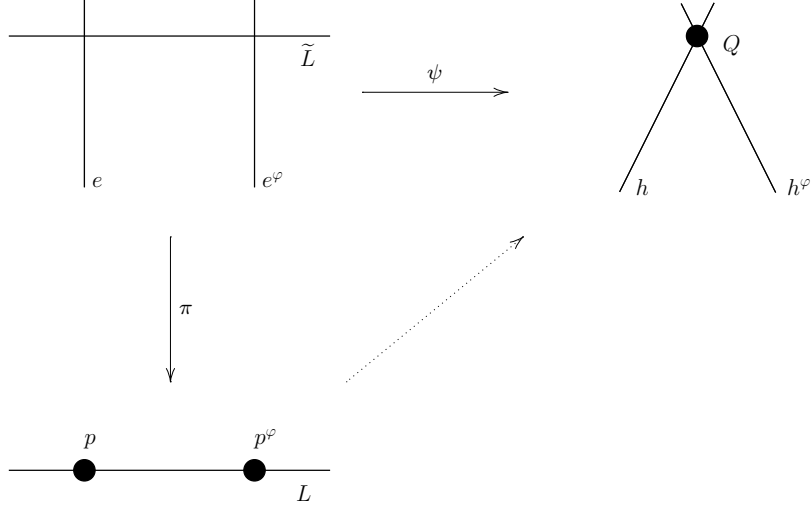
FIGURE 1. Illustration of the construction of X from $\mathbf{P}^2$.

- About $\widetilde{X}$.
  - (B) $\mathrm{Pic}_{\mathbf{F}_q}(\widetilde{X}) \cong \mathbf{Z}E \oplus \mathbf{Z}\widetilde{L}$ and $E^2 = -2$, $E.\widetilde{L} = 2$, $\widetilde{L}^2 = -1$.
  - (C) $\pi^\star L = \widetilde{L} + E$.
  - (D) $E = e + e^\varphi$.
- About X
  - (E) H corresponds to the cut out of X by its tangent plane at Q.
  - (F) $\mathrm{Pic}_{\mathbf{F}_q}(X) \cong \mathbf{Z}H$, with $H^2 = 2$.
  - (G) $\psi^\star H = 2\widetilde{L} + E$.
  - (H) $H = h + h^\varphi$.

To estimate the minimum distance of functional codes on an elliptic quadric, the two following lemmas are useful.

Lemma 2.1. *Let D be an effective divisor on X containing Q and which is smooth at this point. Let s be the positive integer such that $D \sim sH$. Let $\widetilde{D}$ be the strict transform of D by ψ and D' be the image of $\widetilde{D}$ by π. Then,*

  (i) $\sharp D(\mathbf{F}_q) = \sharp D'(\mathbf{F}_q)$;
  (ii) D' is singular at P with multiplicity $s - 1$;
  (iii) D' has degree $2s - 1$.

Figure 2 illustrates the case $s = 3$.

Remark 2.2. The assertion "D is effective and $D \sim sH$" is equivalent to "D is a cut out of X by a surface of degree s which has no common component with X".

Proof of Lemma 2.1. Since π consists in blowing up $\mathbf{P}^2$ at a nonrational closed point, it has no influence on the number of rational points. Thus $\sharp D'(\mathbf{F}_q) = \sharp \widetilde{D}(\mathbf{F}_q)$. Moreover, since D is smooth at Q, we have $\sharp D(\mathbf{F}_q) = \sharp \widetilde{D}(\mathbf{F}_q)$. This proves (i).

Recall that H denotes the intersection divisor of X by its tangent plane at Q and that $\psi^\star H = 2\widetilde{L} + E$. Therefore, the strict transform of H by ψ equals
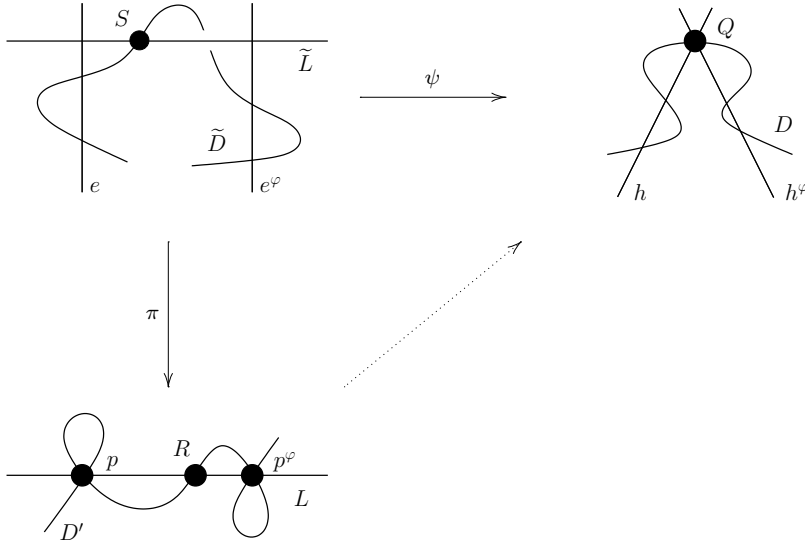
FIGURE 2. The divisors $D, \widetilde{D}$ and D' for $s = 3$.

E. Since D contains Q and is smooth at it, it has a rational tangent line at Q. Moreover, since h and h^φ are not defined over $\mathbf{F}_q$, then D meets h and h^φ transversally at Q. Since $D \sim sH$, it meets h (resp. h^φ) at $s-1$ geometric points (counted with multiplicities) out of Q.

Therefore, $\widetilde{D}$ meets e (resp. e^φ) at $s-1$ geometric points counted with multiplicities. This gives

$$(3) \qquad \widetilde{D}.E = 2(s-1)$$

Moreover, after contracting e and e^φ (i.e. applying π), the image D' of $\widetilde{D}$ is singular with multiplicity $s-1$ at p and p^φ, that is at P. This proves (ii).

Finally, since D is smooth at Q, we have

$$(4) \qquad \psi^\star D = \widetilde{D} + \widetilde{L} \quad \text{and} \quad \widetilde{D}.\widetilde{L} = 1.$$

Indeed, recall that $\widetilde{L}$ is the exceptional divisor of ψ. Moreover, since D' is the image of $\widetilde{D}$ by π and since $\widetilde{D}$ and E have no common component, then $\widetilde{D}$ is also the strict transform of D' by π. Thus, since it has already been proved that D' has multiplicity $s-1$ at P, we get

$$(5) \qquad \pi^\star D' = \widetilde{D} + (s-1)E.$$

Since the degree of D' equals the intersection product $D'.L$, using (B), (C), (3), (4), (5) and [9] Chapter V, Proposition 3.2(a), we get

$$
\begin{aligned}
D'.L = \pi^\star D'.\pi^\star L &= \widetilde{D}.\widetilde{L} + (s-1)E.\widetilde{L} + \widetilde{D}.E + (s-1)E^2 \\
&= 1 + 2(s-1) + 2(s-1) - 2(s-1) = 2s-1,
\end{aligned}
$$

which proves (iii). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

In our particular case, the following Proposition gives a sharper bound than that of Homma and Kim (Theorem 1.6).

Proposition 2.3. *Let s be an integer such that $s \geq 2$ and $D \subset X$ be an $\mathbf{F}_{q^-}$ irreducible curve such that $D \sim sH$. Then*

$$\sharp D(\mathbf{F}_q) \leq q(2s - 2).$$

Proof. Step 1. Assume that D has at least one nonsingular rational point. Recall that the automorphism group of an elliptic quadric acts transitively on its set of rational points ([10] Part IV, Theorem 15.3.19). Thus, after applying a suitable automorphism, one can assume that D contains Q and is smooth at it. From Lemma 2.1, there exists a plane curve D' of degree $2s - 1$ which is singular with multiplicity $s - 1$ at P (which has degree 2). Moreover $\sharp D'(\mathbf{F}_q) = \sharp D(\mathbf{F}_q)$. Therefore, as illustrated by Figure 2, the line L containing P meets D' at a unique other geometric point R. This point R is thus rational and smooth (it is actually the image by π of the preimage S of Q by $\psi_{|\widetilde{D}} : \widetilde{D} \to D$).

Now, consider the linear system of lines containing R. This linear system has $(q + 1)$ rational elements $L_1, \ldots, L_{q+1}$ which cover all the rational points of $\mathbf{P}^2$. Among the L_i's, one finds the line L which meets D' only at P and R and hence meets D' at only one rational point (the point R). Since D' is smooth at R, the tangent $T_R D'$ to D' at R is rational and hence is one of the L_i's. Moreover, a simple argument based on Bézout's Theorem proves that $T_R D' \neq L$. Finally, we get

$$\sharp D'(\mathbf{F}_q) \leq q(2s - 2).$$

Step 2. If all the rational points of D are singular, then, from Lemma 2.4 below, $\sharp D(\mathbf{F}_q) \leq s(s + 1) - 2q$. There remains to check that $s(q + 1) - 2q \leq q(2s - 2)$ for all $s \geq 2$ and $q \geq 2$, which is elementary. $\qquad\square$

Lemma 2.4. *Let s be a positive integer and $D \subset X$ be an $\mathbf{F}_q$–irreducible curve such that $D \sim sH$. Assume moreover that the rational points of D are all singular. Then*

$$\sharp D(\mathbf{F}_q) \leq \begin{cases} 1 & \text{if} \quad s = 1 \\ s(q + 1) - 2q & \text{if} \quad s \geq 2 \end{cases}.$$

Proof. If $s = 1$, then, D is a cut out of X by a plane. Thus, D is an irreducible plane conic. Since it is assumed to be singular, it is a union of two conjugated lines meeting at a single point which is the only rational point of D.

Now, assume that $s \geq 2$. Choose two distinct rational points A, B of D (if they do not exist, then $\sharp D(\mathbf{F}_q)$ satisfies obviously the upper bound). Consider the set of $q + 1$ rational plane cut outs $H_1, \ldots, H_{q+1}$ of X containing A and B. These plane cut outs cover all the rational points of X and each one of them contains A and B. Using that D is singular at all of its rational points, we obtain

$$\begin{aligned} D.(H_1 + \cdots + H_{q+1}) &\geq 2\sharp(D(\mathbf{F}_q) \setminus \{A, B\}) + 2(q + 1)\sharp\{A, B\} \\ \Rightarrow \qquad 2s(q + 1) &\geq 2(\sharp D(\mathbf{F}_q) - 2) + 4(q + 1) \\ \Rightarrow \qquad s(q + 1) - 2q &\geq \sharp D(\mathbf{F}_q). \end{aligned}$$

$$\qquad\square$$

2.3. Application to the study of $C_L(X, \mathcal{O}_X(3))$.

For a fixed base field $\mathbf{F}_q$, the code $C_L(X, \mathcal{O}_X(3))$ has length $n = q^2 + 1$, which is the number of rational points of X ([10] Part IV, Table 15.4). To compute the dimension and the minimum distance of this code, we need Lemma 2.5 and Proposition 2.7 below. The parameters of this code are summarised further in Theorem 2.8.

Lemma 2.5. *Let m be a nonnegative integer. The dimension of $H^0(X, \mathcal{O}_X(m))$ is $(m+1)^2$.*

Proof. Let F be a homogeneous polynomial of degree 2 such that $F(x, y, z, t) = 0$ is an equation of X. The space $H^0(X, \mathcal{O}_X(m))$ corresponds to the space of homogeneous forms of degree m modulo the forms vanishing on X, that is the multiples of F. Thus, we have the isomorphism

$$H^0(X, \mathcal{O}_X(m)) \cong H^0(\mathbf{P}^3, \mathcal{O}_{\mathbf{P}^3}(m))/H^0(\mathbf{P}^3, \mathcal{O}_{\mathbf{P}^3}(m-2)).F,$$

which entails

$$\begin{aligned}
\dim H^0(X, \mathcal{O}_X(m)) &= \dim H^0(\mathbf{P}^3, \mathcal{O}_{\mathbf{P}^3}(m)) - \dim H^0(\mathbf{P}^3, \mathcal{O}_{\mathbf{P}^3}(m-2)) \\
&= \binom{m+3}{3} - \binom{m+1}{3} = (m+1)^2.
\end{aligned}$$

$\square$

Remark 2.6. Lemma 2.5 entails that the dimension of $C_L(X, \mathcal{O}_X(3))$ has dimension at most 16. Since we must have $n \geq k \geq 16$ and $n = q^2 + 1$, the study of such codes makes sense only for $q \geq 4$. It starts to be interesting for $q \geq 5$. Therefore in the following statements, we assume that $q \geq 5$.

Proposition 2.7. *Assume that $q \geq 5$. Let C be an effective divisor on X such that $C \sim 3H$. Then,*

$$\sharp C(\mathbf{F}_q) \leq \max(3q+3, \ \min(4q, \ q+1+4\lfloor 2\sqrt{q}\rfloor)).$$

Proof. Using that $\mathrm{Pic}_{\mathbf{F}_q}(X)$ is generated by H, we separate the proof in three cases:

   (i) $C = C_1 \cup C_2 \cup C_3$, where the C_i's are $\mathbf{F}_q$–irreducible and are all three linearly equivalent to H;
   (ii) $C = C_1 \cup C_2$, where C_1, C_2 are $\mathbf{F}_q$–irreducible and $C_1 \sim H$ and $C_2 \sim 2H$;
   (iii) C is $\mathbf{F}_q$–irreducible.

   To treat these distinct cases, we need to compute the arithmetical genus of a geometrically irreducible (possibly singular) curves embedded in X. For that, we use the adjunction formula ([13] Chapter IV §2 Proposition 5) asserting that the arithmetical genus of a geometrically irreducible curve (possibly singular) C embedded in X is

$$p_a(C) = 1 + \frac{1}{2}C.(K+C),$$

where K denotes the canonical class of X. From [9] Chapter II, Example 8.20.3, we get $K \sim -2H$. Therefore, if C is a geometrically irreducible curve embedded in X, we get

(6) $$C \sim aH \implies p_a(C) = 1 + a(a-2).$$

   The case (i) is elementary, in this situation C is a union of 3 plane cut outs of X. Such cut outs are plane $\mathbf{F}_q$–irreducible conics and hence have either 1 (a pair of conjugated lines) or $q+1$ (a smooth plane conic) rational points. Thus, in situation (i), $\sharp C(\mathbf{F}_q) \leq 3q+3$.

   In situation (ii), as in the previous case we have $\sharp C_1 \leq q+1$. If C_2 is not geometrically irreducible, then its rational points are singular (they lie at the intersection of irreducible components defined over $\overline{\mathbf{F}}_q$). Therefore, from Lemma 2.4, we get $\sharp C_2 \leq 2$. Now, if C_2 is geometrically irreducible, then, using (6), one proves that $p_a(C_2) = 1$ and from Aubry and Perret's bound, $\sharp C_2(\mathbf{F}_q) \leq$

$q + 1 + \lfloor 2\sqrt{q} \rfloor$. An easy computation proves that $q + 1 + \lfloor 2\sqrt{q} \rfloor \leq 2q + 2$ for all $q \geq 2$. Thus, we also have $\sharp C(\mathbf{F}_q) \leq 3q + 3$.

In case (iii), if C is not geometrically irreducible, then, as in the previous case, one proves that $\sharp C(\mathbf{F}_q) \leq q + 2$ by using Lemma 2.4. If it is geometrically irreducible, then using (6), one proves that $p_a(C) = 4$ and from Proposition 2.3 together with Theorem 1.4, we get $\sharp C(\mathbf{F}_q) \leq \min(4q, q + 1 + 4\lfloor 2\sqrt{q} \rfloor)$. $\qquad\square$

Finally, we are able to estimate the parameters of the code $C_L(X, \mathcal{O}_X(3))$. This is the purpose of the following theorem.

Theorem 2.8. *Let X be an elliptic quadric over $\mathbf{F}_q$ with $q \geq 5$. The code $C_L(X, \mathcal{O}_X(3))$ has parameters $[q^2 + 1, 16, \geq \delta]$, where*

$$\delta = q^2 + 1 - \max(3q + 3, \ \min(4q, \ q + 1 + 4\lfloor 2\sqrt{q} \rfloor)).$$

That is:

$$\delta = \begin{cases} q^2 + 1 - 4q & if & q \leq 7 \\ q^2 - q - 4\lfloor 2\sqrt{q} \rfloor & if & 8 \leq q \leq 13 \\ q^2 - 2 - 3q & if & q \geq 16. \end{cases}$$

Proof. The length has already been computed above. For the minimum distance, it is a straightforward consequence of Proposition 2.7. The dimension is a straightforward consequence of Lemma 2.5 together with Remark 1.3. $\qquad\square$

Table 1 gives the parameters of such codes for small values of q. In addition, the lower bound for the minimum distance is compared with the best known minimum distance for the same length and dimension. It shows that codes of the form $C_L(X, \mathcal{O}_X(3))$ are good compared to the table of the best known codes [8] and [12].

q	n	k	d	Best d up to now
5	26	16	≥ 6	8
7	50	16	≥ 22	26
8	65	16	≥ 36	38
9	82	16	≥ 48	52

TABLE 1. Parameters of $C_L(X, \mathcal{O}_X(3))$, when X is an elliptic quadric.

2.4. **A remark about the study of $C_L(X, \mathcal{O}_X(2))$.** The code $C_L(X, \mathcal{O}_X(2))$ is studied in [6] when X is a quadric of any kind. However, it is interesting to note that the elliptic case can be easily obtained from our work. Using the previous methods, one gets the following proposition which corresponds to [6] Proposition 6.6.

Proposition 2.9. *Let X' be a quadric surface distinct from X, let C be the intersection of X and X', then*

$$\sharp C(\mathbf{F}_q) \leq 2q + 2$$

and this upper bound is reached. Thus, the parameters of the code $C_L(X, \mathcal{O}_X(2))$ are $[q^2 + 1, 9, q^2 - 2q - 1]$.

Proof. Two cases must be considered:

(i) C is a union of two plane cut outs;

(ii) C is $\mathbf{F}_q$–irreducible.

Case (i) yields $\sharp C(\mathbf{F}_q) \leq 2q+2$ and this upper bound is reached when both plane cut outs have $q + 1$ rational points and do not meet at rational points. Case (ii) yields $\sharp C(\mathbf{F}_q) \leq q + 1 + \lfloor 2\sqrt{q} \rfloor$ from Theorem 1.4 which is smaller than $2q + 2$ for all q. $\qquad\square$

3. Constructions of rational surfaces yielding good codes

Consider the case of the code $C_L(X, \mathcal{O}_X(n))$ on an elliptic quadric. By the blow up and blow down operation, the linear system associated to $\mathcal{O}_X(n)$ on X corresponds to a linear system in $\mathbf{P}^2$ having the closed point P as a base point. Therefore, such curves defined over $\mathbf{F}_q$ cannot contain any rational line of $\mathbf{P}^2$ but L whose strict transform is contracted. Thus, the elements of the linear system cannot have *too many* $\mathbf{F}_q$–irreducible components.

This is the motivation of the following examples. We will give some particular linear systems of $\mathbf{P}^2$ whose $\mathbf{F}_q$–rational elements cannot break into too many $\mathbf{F}_q$–irreducible components and compute the maximal number of rational points of the elements of the linear system. Such a linear system provides a line bundle $\mathcal{L}$ over a rational surface X obtained from $\mathbf{P}^2$ after some possible blow ups and blow downs. The parameters of the code $C_L(X, \mathcal{L})$ on this surface arise from the properties of the linear system.

3.1. The projective plane blown up at a rational point and a point of degree 4.

3.1.1. *Context.* Consider the projective plane $\mathbf{P}^2$ and let P be a rational point. Denote by φ the Frobenius map. Let l and l^φ be a pair of conjugated lines defined over $\mathbf{F}_{q^2}$ and meeting at P. Denote by D the $\mathbf{F}_q$–rational conic $D := l \cup l^\varphi$. Let R be a closed point of degree 4 of D. Over $\mathbf{F}_{q^4}$, this point splits into 4 points $r, r^\varphi, r^{\varphi^2}$ and r^{φ^3}, where φ denotes the Frobenius map. The following picture illustrates this context.
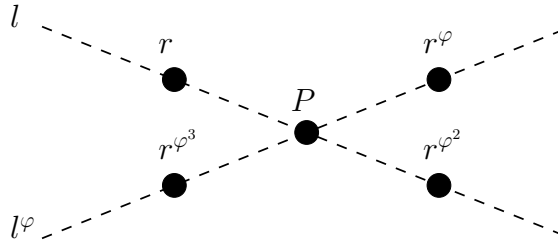
Definition 3.1 (The surface Y). Let Y be the surface obtained from $\mathbf{P}^2$ by blowing up P and R. We denote by $\pi : Y \to \mathbf{P}^2$ the blow up map and by E and F the exceptional divisors above P and R respectively.

Definition 3.2 (The line bundle $\mathcal{F}_i$). Let $i \geq 4$ be an integer. Let Λ_i be the linear system of plane curves of degree i containing R with multiplicity at least 1 and P with multiplicity at least 2. Let $\mathcal{F}_i$ be the line bundle over Y associated to the linear system $\pi^\star \Lambda_i - 2E - F$.

Remark 3.3. The linear system $\pi^\star \Lambda_i - 2E - F$ is base point free for all $i \geq 4$ and very ample for $i \geq 5$ (use [9] Chapter II, Remark 7.8.2).

3.1.2. *The code $C_L(Y, \mathcal{F}_4)$.*

Theorem 3.4. *The parameters of the code $C_L(Y, \mathcal{F}_4)$ are*

$$[(q+1)^2, 8, q^2 - q - 2].$$

Proof. The code has length $n = \sharp Y(\mathbf{F}_q) = (q+1)^2$.

For the dimension, we need to know the dimension of the linear system Λ_4. The dimension of the linear system of plane quartics is 14. The interpolating condition at P imposes 3 constraints and the vanishing condition at R imposes 4 other constraints. These 7 constraints can be proved to be independent (details are left to the reader) and hence the dimension of Λ_4 is 7 and that of $H^0(Y, \mathcal{F}_i)$ is 8. Using Remark 1.3 together with Proposition 3.5 below, we see that the dimension of the code is also 8.

The minimum distance d is given by Proposition 3.5. $\square$

Caution. This example is pretty different from the former one since here a divisor $C \in \Lambda_i$ and the divisor $C' := \pi^\star C - 2E - F$ have not always the same number of rational points. Indeed, from C to C', the point P may "split" into two distinct rational points or into a closed point of degree 2. Moreover, if C has multiplicity ≥ 3 at P, then C' contains the whole curve E.

**Proposition 3.5.** *Let C be a curve in the linear system $\pi^\star \Lambda_4 - 2E - F$, then*

$$\sharp C(\mathbf{F}_q) \leq 3q + 3$$

and the bound is reached.

Proof. Let B be the plane curve corresponding to C in Λ_4 (i.e. $B = \pi(C)$). We separate the proof in four distinct cases.

(i) $B = B_1 \cup B_2$, where B_1 is an $\mathbf{F}_q$–irreducible conic containing R and avoiding P and B_2 is a conic which is singular at P.

(ii) $B = B_1 \cup B_2$, where B_1 is an $\mathbf{F}_q$–irreducible conic containing P and R (notice that in this situation $B_1 = l \cup l^\varphi$ and hence is singular at P) and B_2 is an arbitrary conic.

(iii) $B = B_1 \cup B_2$, where B_1 is an $\mathbf{F}_q$–irreducible cubic containing R and P and B_2 is a line containing P.

(iv) B is an $\mathbf{F}_q$–irreducible quartic containing R and singular with multiplicity 2 at P.

The four distinct situations are illustrated by the following pictures.

(i)   (ii)
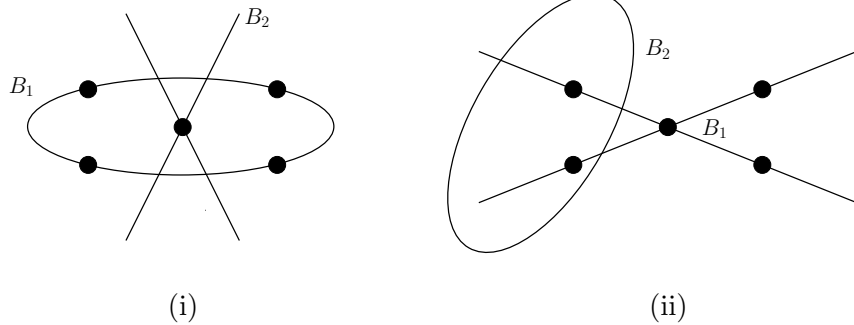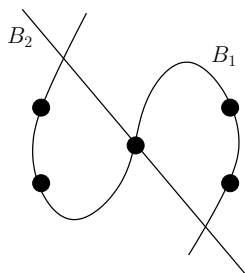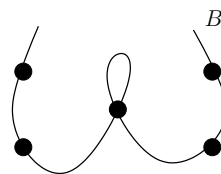
(iii)   (iv)

Let us make a few remarks about these distinct cases in order to make sure they are the only possible ones. First, notice that for case (iii) if B_1 is a cubic, then it must contain P since B_2 is a line and hence cannot be singular at P. Moreover if B_1 is singular at P, then, from Bézout's Theorem, it would contain l and l^φ and hence would not be $\mathbf{F}_q$–irreducible. Thus, B_1 must be smooth at P and hence B_2 must contain P. This situation is interesting since in this case the multiplicity of B at P cannot be ≥ 3 and hence C cannot contain E. By the same manner in case (iv), the curve B cannot be singular with multiplicity > 2 at P.

Now let us treat these distinct cases. In case (i), the worst situation is when B_1 is smooth and B_2 is a union of two rational lines containing P and which do not meet B_1 at rational points. Then $C = \widetilde{B}_1 + \widetilde{B}_2$. The curve $\widetilde{B}_2$ is union of two skew lines, thus $\sharp\widetilde{B}_2(\mathbf{F}_q) = 2q + 2$ and the curve $\widetilde{B}_1$ is isomorphic to B_1. Thus, $\sharp C(\mathbf{F}_q) \leq 3q + 3$ and this upper bound is reached since the worst case happens for some C.

In case (ii), the curve B_1 equals $D = l \cup l^\varphi$. The worst situation is when B_2 is a pair of rational lines containing P. In this situation

$$C = \widetilde{B}_1 \cup \widetilde{B}_2 \cup E.$$

The curve $\widetilde{B}_1$ is a union of two skew conjugated lines over $\mathbf{F}_{q^2}$ and hence has no rational points. Thus, $\sharp C(\mathbf{F}_q) \leq 3q + 1$.

In case (iii), we have $C = \widetilde{B}_1 + \widetilde{B}_2$ and the components are respectively isomorphic to B_1 and B_2. Thus, applying Corollary 1.7 to each irreducible component, we get $\sharp C(\mathbf{F}_q) \leq 3q + 3$.

In case (iv), from Corollary 1.7, we have $\sharp B(\mathbf{F}_q) \leq 3q+2$. Moreover, as noticed before, B has multiplicity exactly 2 at P, then $C = \widetilde{B}$ and C contains at most 2 rational points above P. Thus, $\sharp C(\mathbf{F}_q) \leq 3q + 3$. $\qquad\square$

Table 2 gives the parameters of the code $C_L(Y, \mathcal{F}_4)$ for small values of q. In the right column, the minimum distance of the best known code for the same length and dimension is given. This shows that these codes are good.

3.2. The projective plane blown up at a point of degree 3.

3.2.1. *Context.* Consider the projective plane and a closed point P of degree 3 which is not contained in any rational line. After a base field extension, P splits into three non collinear points p, p^φ and p^{φ^2}, where φ denotes the Frobenius map.

Definition 3.6 (The surface Z)**.** Let Z be the projective plane blown up at P. We denote by $\pi : Z \to \mathbf{P}^2$ the blow up map and by E the exceptional divisor.

q	n	k	d	Best d up to now
3	16	8	4	6
4	25	8	10	12
5	36	8	18	21
7	64	8	40	41
8	81	8	54	58
9	100	8	70	75

TABLE 2. Parameters of the code $C_L(Y, \mathcal{F}_4)$.

Definition 3.7 (The line bundles $\mathcal{L}_i$)**.** Let $i \geq 3$ be an integer. Let Γ_i be the linear system of plane curves of degree i containing P. We call $\mathcal{L}_i$ the line bundle over Z associated to $\pi^\star \Gamma_i - E$.

Let us study some codes on Z.

3.2.2. The code $C_L(Z, \mathcal{L}_3)$.

Theorem 3.8. *The parameters of $C_L(Z, \mathcal{L}_3)$ are*

$$[q^2 + q + 1, 7, q^2 - q - 1].$$

Proof. Since Z is obtained from $\mathbf{P}^2$ by blowing up non rational points, it has the same number of rational points as $\mathbf{P}^2$. Thus, the length is $n = q^2 + q + 1$. The linear system Γ_3 has dimension 6 ([9] Chapter V, Corollary 4.4(a)), thus the dimension of the code is $k = 7$. The minimum distance is given by Proposition 3.9 below. $\square$

Proposition 3.9. *Let C be an $\mathbf{F}_q$–rational element of the linear system Γ_3 (see Definition 3.7). Then,*

$$\sharp C(\mathbf{F}_q) \leq 2q + 2$$

and this upper bound is reached.

Proof. Consider the $\mathbf{F}_q$–irreducible components of C containing P. Since P has degree 3 and is not contained in any rational line, these $\mathbf{F}_q$–irreducible components are either a conic or an $\mathbf{F}_q$–irreducible cubic. Thus there are two possibilities.

   (i) $C = C_1 \cup C_2$ where C_1 is an $\mathbf{F}_q$–irreducible conic containing P and C_2 is a rational line.
  (ii) C is an $\mathbf{F}_q$–irreducible cubic.

The two distinct cases are illustrated by the pictures below.

   In both cases, C is not a union of $\mathbf{F}_q$–rational lines and the upper bound is a straightforward consequence of Corollary 1.7. In case (i), if C_2 does not meet C_1 at rational points, then $\sharp C(\mathbf{F}_q) = 2q + 2$ and hence the bound is reached. $\square$
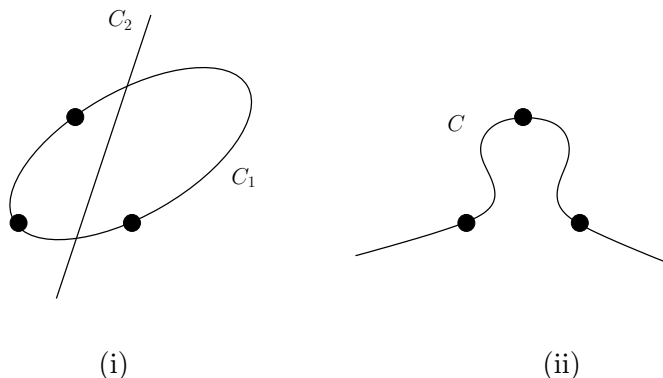
(i)   (ii)

Table 3 gives the parameters of the code $C_L(Z, \mathcal{L}_3)$ for several values of q. The right hand column gives the best known minimum distance for these fixed length and dimension. This show that these codes for small values of q are as good as the best known codes.

q	n	k	d	Best d up to now
3	13	7	5	5
4	21	7	11	11
5	31	7	19	19
7	57	7	41	41
8	73	7	55	55
9	91	7	71	71

TABLE 3. Parameters of the code $C_L(Z, \mathcal{L}_3)$.

3.2.3. *The code $C_L(Z, \mathcal{L}_4)$.*

Theorem 3.10. *The parameters of $C_L(Z, \mathcal{L}_4)$ are*

$$[q^2 + q + 1, 12, q^2 - 2q - 1].$$

Proof. The length is $n = q^2 + q + 1$ (as for $C_L(Z, \mathcal{L}_3)$). The dimension of the linear system Γ_4 is 11, since the linear system of plane quartics is 14 and the vanishing condition at P imposes 3 independent constraints (details are left to the reader). Thus, the code has dimension $k = 12$. Its minimum distance is given by the following Proposition. □

Proposition 3.11. *Assume that $q \geq 4$. Let C be an $\mathbf{F}_q$–rational element of Γ_4. Then,*

$$\sharp C(\mathbf{F}_q) \leq 3q + 2$$

and this upper bound is reached.

Proof. The curve C can be of the form:
   (i) $C = C_1 \cup C_2$ where C_1 is an $\mathbf{F}_q$–irreducible conic containing the point P and C_2 is a conic (possibly reducible);
  (ii) $C = C_1 \cup C_2$ where C_1 is an $\mathbf{F}_q$–irreducible cubic containing the point P and C_2 is an $\mathbf{F}_q$–rational line;
 (iii) C is an $\mathbf{F}_q$–irreducible quartic.

The three distinct situations are illustrated by the following pictures.

(i)   (ii)
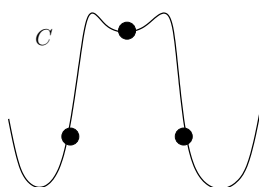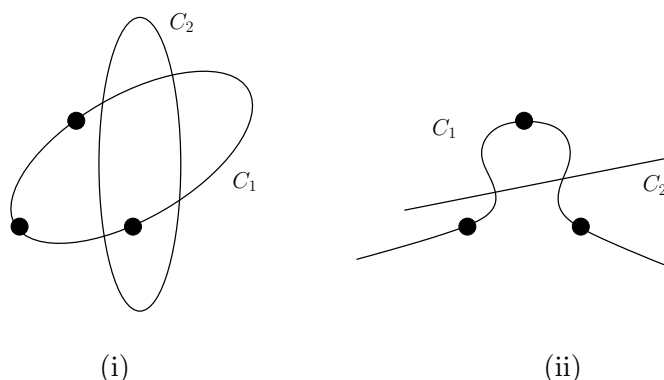
(iii)

In these three cases, C is not a union of $\mathbf{F}_q$–rational lines. Then, the upper bound is a straightforward consequence of Corollary 1.7. In case (i), if C_2 is a union of two $\mathbf{F}_q$–rational lines which do not meet C_1 at rational points (it is possible as soon as $q \geq 4$, the details are left to the reader), then $\sharp C(\mathbf{F}_q) = 3q+2$ and hence the upper bound is reached. $\square$

Table 4 gives the parameters of this code for several values of q. Comparing the minimum distance with the best known minimum distance for a fixed length and dimension, we see that these codes are almost as good as some best known codes in [8] and [12]. In addition, we get a $[57, 12, 34]$ code over $\mathbf{F}_7$ which is up to now better than the best known code for these fixed length and dimension.

q	n	k	d	Best d up to now
4	21	12	7	7
5	31	12	14	14
7	**57**	**12**	**34**	33
8	73	12	47	48
9	91	12	62	62

TABLE 4. Parameters of the code $C_L(Z, \mathcal{L}_4)$.

Computer construction using Magma. A MAGMA script to construct such a $[57, 12, 34]$ code is available on `http://www.lix.polytechnique.fr/Labo/Alain.Couvreur/doc_rech/bestF7.mgm`.

Actualisation of the tables of best codes and generation of other best codes. The $[57, 12, 34]$ code over $\mathbf{F}_7$ has been sent to `www.codetables.de`. The code has been proved by computer to be equivalent to a consta-cyclic code (invariant by shifting by one position and multiplication of the first bit by a fixed constant). Moreover, by computer-aided calculation, the minimum distance has been confirmed to be 34. Afterwards, using classical operations on codes (shortening, puncturing, concatenation...) Markus Grassl from `www.codetables.de` provided ten new codes beating the best known minimum distances. These new best codes are available on `www.codetables.de`.

3.2.4. *The code* $C_L(Z, \mathcal{L}_5)$.

Theorem 3.12. *The parameters of* $C_L(Z, \mathcal{L}_5)$ *are*

$$[q^2 + q + 1, 18, q^2 - 3q - 1].$$

Proof. The length is $n = q^2 + q + 1$ (as for $C_L(Z, \mathcal{L}_3)$). The dimension of the linear system of plane quintics is 20. The vanishing condition at P imposes 3 independent constraints and hence the dimension of Γ_5 is 17. Thus, the code has dimension $k = 18$. Notice that, in order to have $n \geq k$, the integer q must be above 4. The relevant cases appear for $q \geq 5$, which is what is assumed from now on. The minimum distance of the code is given by the following result. $\square$

**Proposition 3.13.** *Assume that $q \geq 5$. Let C be an $\mathbf{F}_q$–rational element of Γ_5, then*

$$\sharp C(\mathbf{F}_q) \leq 4q + 2$$

and this bound is reached.

Proof. The curve C can be of the form:

 (i) $C = C_1 \cup C_2$, where C_1 is an $\mathbf{F}_q$–irreducible conic containing the closed point P and C_2 is a cubic (possibly reducible);
 (ii) $C = C_1 \cup C_2$, where C_1 is an $\mathbf{F}_q$–irreducible cubic containing P and C_2 is a conic (possibly reducible);
(iii) $C = C_1 \cup C_2$, where C_1 is an $\mathbf{F}_q$–irreducible quartic containing P and C_2 is a line;
 (iv) C is an $\mathbf{F}_q$–irreducible quintic.

The pictures below illustrate these different cases.

(i)   (ii)

(iii)   (iv)
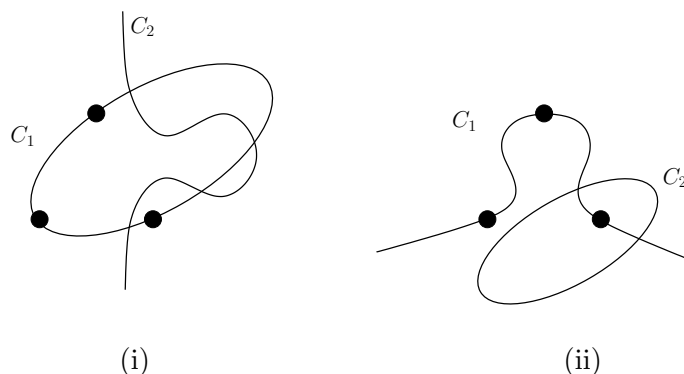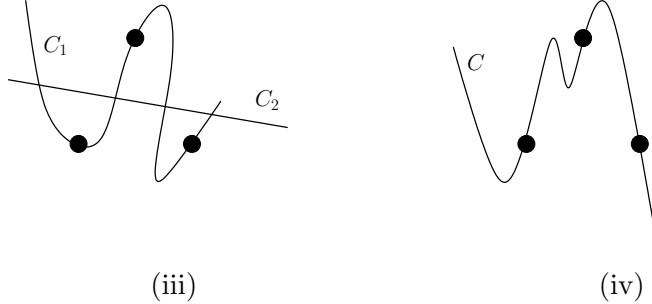
Since the curve C cannot be a union of $\mathbf{F}_q$–rational lines, the upper bound is a straightforward consequence of Corollary 1.7. In case (i), if C_2 is a union of three concurrent $\mathbf{F}_q$–rational lines which do not meet C_1 at rational points (it is possible as soon as $q \geq 7$), then $\sharp C(\mathbf{F}_q) = 4q + 2$. If $q = 5$, then the bound is reached in situation (iii). Let us give an explicit example. Assume that P is defined by the equations $x^2 + xz + yz$, $xy + yz + z^2$ and $4xz + y^2$. Then the upper bound is reached by the curve of equation

$$x(x^4 + 2x^3y + 3x^3z + 3x^2y^2 + 4x^2yz + 3x^2z^2 + 2xy^3 +$$

$$4xy^2z + xyz^2 + 3xz^3 + 2y^4 + 4y^3z + 2y^2z^2 + 4yz^3 + 2z^4) = 0,$$

which has 22 rational points.   □

Table 5 gives the parameters of $C_L(Z, \mathcal{L}_5)$ for some values of q. It shows that these codes are almost as good as the best known codes. In addition over $\mathbf{F}_9$, we get a $[91, 18, 53]$ code which is better than the best known codes up to now. Indeed, for this length and dimension the best minimum distance given by [8] and [12] is 52.

q	n	k	d	Best d up to now
5	31	18	9	9
7	57	18	27	27
8	73	18	39	40
9	**91**	**18**	**53**	52

TABLE 5. Parameters of the code $C_L(Z, \mathcal{L}_5)$.

Computer construction using Magma. A MAGMA script to construct such a $[91, 18, 53]$ code is available on `http://www.lix.polytechnique.fr/Labo/Alain.Couvreur/doc_rech/bestF9.mgm`.

Actualisation of the tables of best known codes. The $[91, 18, 53]$ code over $\mathbf{F}_9$ has been sent to `www.codetables.de`. It has been proved to be equivalent to a cyclic code over $\mathbf{F}_9$ and its dimension has been confirmed to be 53 by computer-aided calculations.

Acknowledgements

The author wishes to thank Christophe Ritzenthaler for inspiring discussions and Markus Grassl from `www.codetables.de` for his investigations on the best codes presented in this article. He is also very grateful to the anonymous referees for their relevant comments and suggestions.

References

[1] Y. Aubry. Reed-Muller codes associated to projective algebraic varieties. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 4–17. Springer, Berlin, 1992.

[2] Y. Aubry and M. Perret. Coverings of singular curves over finite fields. *manuscripta mathematica*, 88(1):467–478, 1995.

[3] Y. Aubry and M. Perret. On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields. *Finite Fields Appl.*, 10(3):412–431, 2004.

[4] I. M. Chakravarti. Geometric construction of some families of two-class and three-class association schemes and codes from nondegenerate and degenerate Hermitian varieties. *Discrete Math.*, 111(1-3):95–103, 1993. Graph theory and combinatorics (Marseille-Luminy, 1990).

[5] F. A. B. Edoukou. Codes defined by forms of degree 2 on Hermitian surfaces and Sørensen's conjecture. *Finite Fields Appl.*, 13(3):616–627, 2007.

[6] F. A. B. Edoukou. Codes defined by forms of degree 2 on quadric surfaces. *IEEE Trans. Inform. Theory*, 54(2):860–864, 2008.

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

[8] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2010-07-22.

[9] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[10] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985. Oxford Science Publications.

[11] M. Homma and S. J. Kim. Sziklai's conjecture on the number of points of a plane curve over a finite field iii. *Finite Fields and Their Applications*, In Press, Corrected Proof:–, 2010.

[12] R. Schürer and W. C. Schmid. MinT - new features and new results. In *Monte Carlo and Quasi-Monte Carlo Methods 2008*, pages 171–189. Springer, Berlin, 2009. Available online on `http://mint.sbg.ac.at`.

[13] J.-P. Serre. *Groupes algébriques et corps de classes*. Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[14] J.-P. Serre. Lettre à M. Tsfasman. *Astérisque*, 198-200:351–353, 1991. Journées Arithmétiques, 1989 (Luminy).

[15] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994.

[16] I. R. Shafarevich. *Basic algebraic geometry. 2*. Springer-Verlag, Berlin, second edition, 1994. Schemes and complex manifolds, Translated from the 1988 Russian edition by Miles Reid.

[17] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[18] P. Sziklai. A bound on the number of points of a plane curve. *Finite Fields and Their Applications*, 14(1):41–43, 2008.

[19] 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.

[20] 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.

[21] S. G. Vlăduts and Y. I. Manin. Linear codes and modular curves. In *Current problems in mathematics, Vol. 25*, Itogi Nauki i Tekhniki, pages 209–257. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[22] M. Zarzar. Error-correcting codes on low rank surfaces. *Finite Fields Appl.*, 13(4):727–737, 2007.

INRIA Saclay Île-de-France, Projet TANC – École Polytechnique, Laboratoire LIX, CNRS, UMR 7161, 91128 Palaiseau Cedex, France

E-mail address: alain.couvreur@inria.fr