Algebraic geometric codes on surfaces

Yves Aubry

ALGEBRAIC GEOMETRIC CODES ON SURFACES

Yves Aubry

Equipe "Arithmétique et Théorie de l'Information"
Laboratoire de Mathématiques Discrètes du C.N.R.S.
Luminy Case 916. 13288 Marseille Cedex 9. France.

Abstract : *For a given algebraic variety V defined over a finite field and a very ample divisor D on V, we give a construction of a linear code $C_{V,D}$. If V is a curve, we recover the algebraic geometric Goppa codes. We are interested here to the case where V is an algebraic surface, and we give in some cases the parameters of such corresponding codes. We compare these parameters to the Singleton bound and to those of Goppa codes. In order to compute these parameters, we use the Riemann-Roch theorem for surfaces.*

Résumé : *Pour toute variétée algébrique V définie sur un corps fini et pour tout diviseur très ample D sur V, nous donnons une construction d'un code linéaire $C_{V,D}$. Si V est une courbe, on retrouve les codes de Goppa géométriques. Nous nous intéressons ici au cas où V est une surface algébrique, et l'on donne dans certains cas les paramètres des codes correspondants. Nous comparons ces paramètres à la borne de Singleton et à ceux des codes de Goppa. Nous utilisons pour calculer ces paramètres le théorème de Riemann-Roch pour les surfaces.*

1. Introduction.

Algebraic geometric codes are already studied on curves. We give here a general construction of linear codes from a given algebraic variety V. This will be done in two steps : the first one is an embedding of V by means of a divisor D, and the second one corresponds to hyperplane sections of the embedded variety. If we omit the first step, it is just the projective Reed-Muller codes studied in [1].

Let $\mathbb{F}_q$ be the finite field with q elements, and $\overline{\mathbb{F}_q}$ an algebraic closure of $\mathbb{F}_q$. Let V be a nonsingular absolutely irreducible algebraic variety defined over $\mathbb{F}_q$ and D a divisor on V defined over $\mathbb{F}_q$. If $\mathbb{F}_q(V)$ denotes the function field of V, and (f) the principal divisor associated to a rational function f, we set

$$L(D) = \{f \in \mathbb{F}_q(V)^* \mid (f) \geqslant -D\} \cup \{0\}.$$

The space $L(D)$ is a finite-dimensional $\mathbb{F}_q$-vector space for every D; we set $\ell(D) = \dim_{\mathbb{F}_q} L(D) = m$. We suppose that the divisor D is very ample, and let Φ_D be the

associated embedding of V in the projective space $\mathbb{P}^{m-1}(\overline{\mathbb{F}_q})$. Let us in few words, explicit this embedding.
Let $\{\varphi_0, \varphi_1, \dots, \varphi_{m-1}\}$ be a basis of the vector space $L(D)$ over $\mathbb{F}_q$, and $D_0 = D + (\varphi_0)$. We have an isomorphism between the vector spaces $L(D)$ and $L(D_0)$ sending f to $f.\varphi_0^{-1}$, which sends the basis $\{\varphi_0, \varphi_1, \dots, \varphi_{m-1}\}$ to $\{1, \frac{\varphi_1}{\varphi_0}, \dots, \frac{\varphi_{m-1}}{\varphi_0}\}$.
Let

$$\begin{array}{rccc} \Lambda_0 : & L(D_0) & \longrightarrow & \mathbb{F}_q[X_0, X_1, \dots, X_{m-1}]_1^0 \\ & \lambda_0 + \sum_{i=1}^{m-1} \lambda_i \frac{\varphi_i}{\varphi_0} & \longmapsto & \sum_{i=0}^{m-1} \lambda_i X_i \end{array}$$

be an isomorphism of $L(D_0)$ onto the vector space of linear homogeneous polynomials with m variables over $\mathbb{F}_q$. We have $\Lambda_0^{-1}(X_i) = \frac{\varphi_i}{\varphi_0}$. Denote $\Lambda_0^{-1}(X_i)$ by f_0^i. Finally, if $\operatorname{Supp} D$ denotes the support of the divisor D, let

$$\begin{array}{rccc} \Phi_0 : & V - \operatorname{Supp}(D_0) & \longrightarrow & \mathbb{P}^{m-1} \\ & p & \longmapsto & (1 : f_0^1(p) : \dots : f_0^{m-1}(p)) \end{array}$$

We can proceed in the same way to define regular maps Φ_i with divisors $D_i = D + (\varphi_i)$. It is easy to see that if $p \in V$, if $p \notin \operatorname{Supp}(D_{i_0})$ and if $p \notin \operatorname{Supp}(D_{j_0})$, then $\Phi_{i_0}(p) = \Phi_{j_0}(p)$. Moreover, since the divisor D is very ample, in particular the complete linear system $\mid D \mid$ has no base points, and then for all $p \in V$, there exist an effective divisor D_i linearly equivalent to D, $D_i = D + (\varphi_i)$, such that $p \notin \operatorname{Supp}(D_i)$. Thus, all the points of V can be embedded in $\mathbb{P}^{m-1}$ via a map Φ_i, and we define the embedding Φ_D by $\Phi_D(p) = \Phi_i(p)$.

Furthermore, $\tilde{V} = \Phi_D(V)$ is not contained in any hyperplane (indeed, since $L(D)$ and $\mathbb{F}_q[X_0, X_1, \dots, X_{m-1}]_1^0$ are isomorphic, the only rational function which is zero everywhere is the zero function). Thus, we have :

PROPOSITION 1.1. – *Under the above hypothesis, $\tilde{V} = \Phi_D(V)$ is a smooth projective subvariety of $\mathbb{P}^{m-1}(\overline{\mathbb{F}_q})$, and we have a one-to-one and onto map*

$$\Phi_D : V(\mathbb{F}_q) \longrightarrow \tilde{V}(\mathbb{F}_q) \subset \mathbb{P}^{m-1}(\mathbb{F}_q)$$

Furthermore, $\tilde{V}$ is not contained in any hyperplane.

Now, let us construct the "hyperplane section code" $C_{V,D}$ associated to the projective algebraic variety $\tilde{V}$.
Let W_i be the set of points with homogeneous coordinates $(x_0 : x_1 : \dots : x_{m-1})$ in $\mathbb{P}^{m-1}(\mathbb{F}_q)$ such that

$$x_0 = x_1 = \dots = x_{i-1} = 0, \qquad x_i \neq 0.$$

It is clear that the family $\{W_i\}_{0 \leqslant i \leqslant m-1}$ is a partition of $\mathbb{P}^{m-1}(\mathbb{F}_q)$.
Then, we define $C_{V,D}$ to be the image of the following map Ψ

$$\begin{array}{rccc} \Psi : & \mathbb{F}_q[X_0, X_1, \dots, X_{m-1}]_1^0 & \longrightarrow & \mathbb{F}_q^{\,\sharp \tilde{V}(\mathbb{F}_q)} \\ & h & \longmapsto & \left(\frac{h(x)}{x_i}\right)_{x = (x_0 : \dots : x_{m-1}) \in \tilde{V}(\mathbb{F}_q) \cap W_i} \end{array}$$

where $\tilde{V}(\mathbb{F}_q)$ denotes the set of rational points over $\mathbb{F}_q$ of $\tilde{V}$. Furthermore, if we suppose that $\tilde{V}(\mathbb{F}_q)$ is not contained in $H(\mathbb{F}_q)$, for all hyperplane H of $\mathbb{P}^{m-1}(\overline{\mathbb{F}_q})$, we can give an estimation of the parameters of the code $C_{V,D}$.

THEOREM 1.2. – *The code $\mathcal{C}_{V,D}$ defined above has parameters :*

$$\begin{aligned} \operatorname{length} \mathcal{C}_{V,D} &= \sharp\tilde{V}(\mathbb{F}_q) = \sharp V(\mathbb{F}_q) \\ \dim \mathcal{C}_{V,D} &= \ell(D) \\ \operatorname{dist} \mathcal{C}_{V,D} &= \sharp\tilde{V}(\mathbb{F}_q) - \max\{\sharp(\tilde{V} \cap H(\mathbb{F}_q))\} \end{aligned}$$

where H describes the set of all hyperplanes of $\mathbb{P}^{m-1}(\mathbb{F}_q)$.

Proof. The embedding of V is such that $\tilde{V}$ is not contained in any hyperplane, so the map Ψ is one-to-one, and thus the dimension of the code $\mathcal{C}_{V,D}$ is equal to the dimension of $\mathbb{F}_q[X_0, X_1, \ldots, X_{m-1}]_1^0$ over $\mathbb{F}_q$, which is clearly m, i.e $\ell(D)$. The length of $\mathcal{C}_{V,D}$ is $\sharp\tilde{V}(\mathbb{F}_q) = \sharp V(\mathbb{F}_q)$ by the above proposition. The minimal distance of $\mathcal{C}_{V,D}$ is obvious. □

2. Algebraic geometric Goppa Codes.

If we take for the variety V a nonsingular curve C of genus g defined over $\mathbb{F}_q$, take a divisor D defined over $\mathbb{F}_q$ on it, such that $\deg D > 2g$ (then, D is a very ample divisor on C). Let $\mathcal{E} = \{P_1, \ldots, P_n\} \subset C(\mathbb{F}_q)$, with $n > \deg D$ and such that none of the P_i belongs to the support of D. Let $\{\varphi_0, \varphi_1, \ldots, \varphi_{m-1}\}$ be a basis of the vector space $L(D)$ over $\mathbb{F}_q$, and Φ_D the corresponding embedding

$$\Phi_D : C(\mathbb{F}_q) \longrightarrow \tilde{C}(\mathbb{F}_q) \subset \mathbb{P}^{m-1}(\mathbb{F}_q)$$

The restriction of the map Φ_D to the set $\mathcal{E}$ sends the point $P \in \mathcal{E}$ to the point $x_P = (\varphi_0(P) : \cdots : \varphi_{m-1}(P)) \in \tilde{C}(\mathbb{F}_q)$. Denote by $\tilde{\mathcal{E}}$ the image of $\mathcal{E}$ by Φ_D.

Moreover, we have seen that the projective space $\mathbb{P}^{m-1}(\mathbb{F}_q)$ can be partitioned using the sets W_i. Then, for each equivalence class corresponding to a projective point, we can choose the representant which have for the first non-zero coordinate the value 1 (i.e. if $x = (x_0 : \cdots : x_{m-1}) \in W_i$, we take $x_i = 1$). Thus the map Ψ defined in § 1 is just the following one

$$\begin{array}{cccc} \Psi : & \mathbb{F}_q[X_0, X_1, \ldots, X_{m-1}]_1^0 & \longrightarrow & \mathbb{F}_q^{\sharp\tilde{\mathcal{E}}} \\ & h & \longmapsto & (h(x))_{x \in \tilde{\mathcal{E}}} \end{array}$$

If $h = \sum_{j=0}^{m-1} \lambda_j X_j$ is a linear form in $\mathbb{F}_q[X_0, X_1, \ldots, X_{m-1}]_1^0$, then

$$h(x_P) = \sum_{j=0}^{m-1} \lambda_j \varphi_j(P) = f_h(P)$$

where f_h belongs to $L(D)$. Then, we have

$$(h(x_P))_{x_P \in \tilde{\mathcal{E}}} = (f_h(P))_{P \in \mathcal{E}}.$$

But, it is nothing else that the geometric Goppa code defined over the curve C which is the image of the map (see [2])

$$\begin{array}{cccc} \mathcal{G}_{C,D,\mathcal{E}} : & L(D) & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & (f(P))_{P \in \mathcal{E}} \end{array}$$

Remark. The hypothesis saying that the points P of $\mathcal{E}$ not belong to the support of the divisor D is not necessary in our construction. Furthermore, the embedded curve $\tilde{C}$ has degree equal to $\deg D$ and a curve $\tilde{C}$ has at most $\deg \tilde{C}$ points in common with a hyperplane. The estimation of the number of points of hyperplane sections of $\tilde{C}$ is the same that the estimation of the number of zeros of a rational function over the curve C of $L(D)$. Thus, the parameters of this code are the same as those of Goppa code where the set $\mathcal{E}$ is $C(\mathbb{F}_q)$, i.e. where the evaluation is made over all the rationals points over $\mathbb{F}_q$ of C; namely

$$\operatorname{length} \mathcal{C}_{C,D} = \sharp C(\mathbb{F}_q)$$

$$\dim \mathcal{C}_{C,D} = \ell(D) = \deg D + 1 - g$$

$$\operatorname{dist} \mathcal{C}_{C,D} \geqslant \sharp C(\mathbb{F}_q) - \deg D.$$

3. Surfaces.

Let S be a nonsingular projective algebraic surface, D a very ample divisor on S and $\mathcal{C}_{S,D}$ the corresponding code. Recall the property that a divisor D on a surface is very ample if and only if the linear system $\mid D - P - Q \mid$ has dimension $\dim \mid D \mid -2$, for all $P, Q \in S$; and that the arithmetic genus $p_a(S)$ of S is defined by $p_a(S) = P_S(0) - 1$ where P_S is the Hilbert polynomial of S.
By the Riemann-Roch theorem, we have (see [3 p. 362]) :

$$\ell(D) = s(D) - \ell(K - D) + \frac{1}{2} D.(D - K) + 1 + p_a(S)$$

where $s(D)$ is the superabundance od D and K the canonical divisor on S.

PROPOSITION **3.1.** – *(i) If the divisor D is such $D^2 > K.D$, then*

$$\dim \mathcal{C}_{S,D} \geqslant \frac{1}{2} D.(D - K) + 1 + p_a(S).$$

(ii) We have

$$\operatorname{dist} \mathcal{C}_{S,D} \geqslant \sharp S(\mathbb{F}_q) - D^2(q + 1).$$

Proof. (i) If $\ell(K - D) > 0$, then the divisor $K - D$ is effective, and since D is a very ample divisor on S, we get $(K - D).D > 0$, i.e $D^2 < K.D$. So, if we take D such that $D^2 > K.D$, we have $\ell(K - D) = 0$. In this case, since $s(D) \geqslant 0$, we have :

$$\ell(D) \geqslant \frac{1}{2} D.(D - K) + 1 + p_a(S)$$

and we conclude by theorem 1.2.

(ii) Moreover, the degree of the surface $\tilde{S}$ is equal to the self-intersection number D^2, and for any hyperplane H, $\tilde{S} \cap H$ is a curve of degree equal to the degree of $\tilde{S}$. Then, using the fact (communicated by Gilles Lachaud) that a curve of degree d has at most $d(q+1)$ rational points over $\mathbb{F}_q$, we have :

$$\sharp(\tilde{S} \cap H(\mathbb{F}_q)) \leqslant \deg \tilde{S} \cdot (q+1) = D^2(q+1).$$

Thus, via the theorem 1.2, we obtain for the minimal distance of the code $C_{S,D}$ the lower bound :

$$\operatorname{dist} C_{S,D} \geqslant \sharp S(\mathbb{F}_q) - D^2(q+1).$$

□

4. An example : the nondegenerate hyperbolic quadric surface in $\mathbb{P}^3$.

Let Q be the surface in $\mathbb{P}^3(\mathbb{F}_q)$ defined by the equation

$$XY - ZW = 0.$$

We have $\sharp Q(\mathbb{F}_q) = (q+1)^2$, and the arithmetic genus of Q is equal to 0. It is well-known that the *divisor class group* $\mathrm{Cl}(Q)$ of divisor modulo the linear equivalence (i.e. modulo the principal divisors), is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$. Let D and D' be two divisors on Q of type (a, b) and (a', b'), then the intersection pairing (used in the Riemann-Roch theorem) on Q is given by (see [3]) :

$$D.D' = ab' + a'b.$$

The canonical divisor K has type $(-2, -2)$, and a divisor D of type (a, b) is very ample if and only if $a > 0$ and $b > 0$.
Thus for divisors D of type (a, b) with a and $b > 0$, we obtain a family of $[n, k, d]$-codes $C_{Q,D}$ with :

$$n = q^2 + 2q + 1, \quad k \geqslant ab + a + b + 1, \quad d \geqslant q^2 + 2(1 - ab)q + 1 - 2ab.$$

Indeed, the dimension and minimal distance are given by the proposition 3.1 since $D^2 > K.D$ (because $ab > -a - b$) and $\tilde{Q}$ has degree $D^2 = 2ab$.

5. Ruled Surfaces.

We can generalize the previous example to ruled surfaces. Indeed, if S is a (geometrically) ruled surface on a nonsingular curve C, we can associate to S an invariant e, and it can be shown (see [3 p. 373]) that all divisor D on S is numerically equivalent to $aC_0 + bf$ for $a, b \in \mathbb{Z}$, with

$$C_0.f = 1, \qquad f^2 = 0, \qquad C_0^2 = -e \qquad (*)$$

(recall that two divisors D and D' are said to be *numerically equivalent* if for any divisor E on S, we have $D.E = D'.E$).
Thus, for a given ruled surface S with base curve C and a chosen divisor D on S (with the notations above-mentioned), we have the

PROPOSITION 5.1. – *Let $D = aC_0 + bf$ be a very ample divisor on the ruled surface S of invariant e, such that $a(2b - e - ea - 2g + 2) + 2b > 0$, and let g be the genus of the base curve C. Then the $[n, k, d]$-code $C_{S,D}$ is such that*

$$n \leqslant (q+1)(q+1+g\lfloor 2\sqrt{q}\rfloor)$$

$$k \geqslant (a+1)(b+1-g-\frac{ea}{2})$$

$$d \geqslant (q+1)(q+1-g\lfloor 2\sqrt{q}\rfloor - 2ab + ea^2).$$

Moreover, if D is a nonsingular curve of genus $g(D)$, then

$$k \geqslant 2ab - ea^2 - g(D) + 2 - g.$$

Proof. The length of the code is equal to $\sharp S(\mathbb{F}_q)$ which is $(q+1) \times \sharp C(\mathbb{F}_q)$ and by the Serre-Weil bound ($\lfloor\,\rfloor$ denotes the integer part), we have the result.
The dimension is given by the Riemann-Roch theorem, using the fact that the canonical divisor K of S is numerically equivalent to $-2C_0 + (2g - 2 - e)f$, using the properties $(*)$, knowing that the arithmetical genus of a ruled surface is the opposite of the genus of the base curve, and that $\ell(K - D) = 0$ since the hypothesis on a and b is just $D^2 > K.D$.
The minimal distance follows seeing that $D^2 = 2ab - ea^2$.
Moreover, if D is a nonsingular curve of genus $g(D)$, by the Adjunction formula (see [3 p. 361]) we have : $2g(D) - 2 = D.(D + K)$, thus $D.K = 2g(D) - 2 - D^2$. So the result follows using the Riemann-Roch theorem. □

COROLLARY – *Let $D = aC_0 + bf$ with $a > 0$, $b > ae$ and $a(2b - e - ea + 2) + 2b > 0$ be a divisor on the rational ruled surface S of invariant $e \geqslant 0$ with base curve $C = \mathbb{P}^1$. Then the $[n, k, d]$-code $C_{S,D}$ is such that*

$$n = q^2 + 2q + 1$$

$$k \geqslant (a+1)(b+1-\frac{ea}{2})$$

$$d \geqslant (q+1)(q+1-2ab+ea^2).$$

Proof. In the case of rational ruled surface, we have a criterion for a divisor to be very ample and this is exactly the hypothesis $a > 0$ and $b > ae$ of the corollary (see [3 p. 380]), furthermore $a(2b - e - ea + 2) + 2b > 0$ gives $D^2 > K.D$ (remark that if $2b > a$, we have $D^2 > K.D$). The corollary follows knowing that $\sharp\mathbb{P}^1(\mathbb{F}_q) = q + 1$, and that the genus of $\mathbb{P}^1$ is equal to 0. □

Remark. We recover the preceding example of the quadric in the particular case where C is equal to the projective line $\mathbb{P}^1$ (and then $e = g = 0$).

It is easy to construct a ruled surface of any invariant $e > 0$. Indeed, (see [3 p. 374]) take C be any curve embedded in $\mathbb{P}^n$ of degree d, and consider the cone over C in $\mathbb{P}^{n+1}$ with vertex P. If we blow up the point P, we obtain a ruled surface S over C with invariant $e = d$.
Hence, consider the algebraic-geometric Goppa code $\mathcal{G}_{C,G,\mathcal{E}}$ defined over a rational curve C, of degree d, with effective divisor G as in § 2. Then we can consider the ruled surface S of base curve C as above, and take on it the divisor $D = C_0 + (\deg G)f$. If we suppose that $\deg G > d$ then the divisor D is very ample (see the proof of the above corollary), and we can consider the code $\mathcal{C}_{S,D}$. Note that, since C is a rational curve, the code $\mathcal{G}_{C,G,\mathcal{E}}$ is M.D.S. (see [2]), i.e. reaches the following Singleton bound

$$k + d \leqslant n + 1$$

for any $[n, k, d]$-code. Let us compare the relative distance (i.e $\delta(\mathcal{C}) = \frac{\operatorname{dist} \mathcal{C}}{\operatorname{length} \mathcal{C}}$) of these codes. With the above notations, we have

PROPOSITION 5.2. – *If $\deg G = d + 1$, the relative distances of $\mathcal{G}_{C,G,\mathcal{E}}$ and $\mathcal{C}_{S,D}$ differ at most of $\frac{1}{\sharp C(\mathbb{F}_q)}$, and the code $\mathcal{C}_{S,D}$ has a length which is $(q+1)$ times those of $\mathcal{G}_{C,G,\mathcal{E}}$.*

Proof. Indeed, by the estimations of §2 we have

$$\delta(\mathcal{G}_{C,G,\mathcal{E}}) \geqslant \frac{\sharp\mathcal{E} - \deg G}{\sharp\mathcal{E}} \qquad \text{with} \quad \sharp\mathcal{E} \leqslant \sharp C(\mathbb{F}_q)$$

and by the corollary we have

$$\delta(\mathcal{C}_{S,D}) \geqslant \frac{\sharp C(\mathbb{F}_q) - 2\deg G + d}{\sharp C(\mathbb{F}_q)}.$$

Then, if we take $\deg G = d + 1$, we get the result and thus, the relative distances are asymptotically equal. Moreover, since S is a ruled surface of base curve C, the length of the code $\mathcal{C}_{S,D}$ is equal to $(q+1)\sharp C(\mathbb{F}_q)$, i.e. $(q+1)^2$ since the curve C is rational and thus has a zero genus. Remark that the dimensions are $d+4$ for $\mathcal{C}_{S,D}$ and $d+2$ for the other one. □

We conclude this paper by a simple example where we can compute exactly the parameters, and where we recover a projective Reed-Muller code.
Consider the simple rational ruled surface, namely the projective plane $\mathbb{P}^2(\mathbb{F}_q)$. The group $\mathrm{Cl}(\mathbb{P}^2)$ is $\cong \mathbb{Z}$ and the class h of a line is a generator. We have the following relations :

$$h^2 = 1,\ C.D = nm,\ K = -3h$$

where C and D are divisors linearly equivalent to nh and mh, and where K is the canonical divisor. Then, take the divisor $D = h$ and consider the associated code $\mathcal{C} = \mathcal{C}_{\mathbb{P}^2,D}$. We get :

$$\operatorname{length} \mathcal{C} = q^2 + q + 1,\ \dim \mathcal{C} \geqslant 3,\ \operatorname{dist} \mathcal{C} = q^2.$$

Furthermore, by the Griesmer bound, for any $[n, k, d]$-code over $\mathbb{F}_q$, we have

$$n - k - d + 1 \geqslant \lceil \frac{d}{q} \rceil - 1$$

where $\lceil \frac{d}{q} \rceil$ denotes the smallest integer $\geqslant \frac{d}{q}$. Then, we have

$$\dim C \leqslant q^2 + q + 1 - q^2 + 1 - q + 1 = 3.$$

Thus, we get $\dim C = 3$, and the code C reaches the Griesmer bound. We recover the well-known projective Reed-Muller code of order 1 associated to $\mathbb{P}^2(\mathbb{F}_q)$ (see [4]).

References.

[1] Y. Aubry, Reed-Muller codes associated to projective algebraic varieties. *Lecture Notes in Math.* **1518**, *Coding theory and algebraic geometry*, pp. 4-17, (1991).

[2] V. D. Goppa, *Geometry and codes*, Kluwer Acad. Publ., (1988).

[3] R. Hartshorne, *Algebraic Geometry*. Graduate Texts in Math. **52**, Springer-Verlag, New-York, (1977).

[4] G. Lachaud, The parameters of projective Reed-Muller codes. *Discrete Math.*, vol. **81**, 217-221, (1990).