BULLETIN DE LA S. M. F.

D. LE BRIGAND
J.J. RISLER

Algorithme de Brill-Noether et codes de Goppa

Bulletin de la S. M. F., tome 116, n° 2 (1988), p. 231-253
<http://www.numdam.org/item?id=BSMF_1988__116_2_231_0>

Bull. Soc. math. France,
116, 1988, p. 231–253.

ALGORITHME DE BRILL-NOETHER ET CODES DE GOPPA

PAR

D. LE BRIGAND et J.J. RISLER (*)

RÉSUMÉ. — Soit C une courbe projective plane définie sur un corps k, n'ayant que des singularités ordinaires, l'algorithme classique de Brill-Noether permet de construire une base du k-espace vectoriel $\mathcal{L}(D)$ où D est un diviseur effectif, rationnel sur k, de C.

Dans cet article nous généralisons l'algorithme à une courbe projective plane ayant des singularités quelconques. Dans le cadre de la théorie des codes, l'intérêt de cette généralisation est qu'elle permet de construire de "bons" codes associés à des courbes ayant un grand nombre de points rationnels sur un corps fini. Comme application, nous donnons un exemple de code dont les paramètres sont situés au-dessus de la borne de Varshamov-Gilbert; ce code est construit à l'aide d'une courbe ayant un point singulier non ordinaire et dont le nombre de points rationnels sur $\mathbf{F}_{16}$ atteint la borne de Weil.

ABSTRACT. — Let C be a projective plane curve, defined on a field k, with ordinary singular points; the classical Brill-Noether algorithm gives a construction of a basis of the k-vector space $\mathcal{L}(D)$, D being an effective, k-rational, divisor of C.

In this paper, we present a generalisation of the Brill-Noether algorithm to a projective plane curve having non ordinary singularities. In the frame work of Code Theory, that generalisation gives a construction of "good" codes associated with curves having many rational points over a given finite field. We give, as an example, the construction of a code, the parameters of which are better than Varshamov-Gilbert bound; this code is associated with a curve having a non ordinary singular point and the maximum number of rational points over $\mathbf{F}_{16}$ within the Weil bound.

Introduction

Soit C une courbe projective, plane, définie sur un corps k, D un diviseur effectif de C. L'algorithme de Brill-Noether permet, à partir de

(*) Texte reçu le 3 octobre 1986, révisé le 19 mai 1987.

D. LE BRIGAND, Université P. et M. Curie, U.A. 213, Tour 45–46, 5ième étage, 4 Place Jussieu, 75252 PARIS Cedex 05, France.

J.J. RISLER, Université P. et M. Curie, U.A. 189, Tour 55–65, 5ième étage, 4 Place Jussieu, 75252 PARIS Cedex 05, France.

Ce travail a été réalisé dans le cadre de l'A.T.P. n° 904 188 du C.N.R.S.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037-9484/1988/231/$ 5.00

l'équation de C et du diviseur D, d'exhiber une base de l'espace vectoriel (sur k) $\mathcal{L}(D)$; cet algorithme utilise la notion d'*adjointe* d'une courbe plane et est classiquement présenté uniquement dans le cas où C n'a que des *singularités ordinaires* (*cf.* [A], [F] ou [W]). (Remarquons que cela est théoriquement suffisant puisque toute courbe plane C est birationnellement équivalente à une courbe plane $\overline{C}$ n'ayant comme singularités que des points doubles ordinaires).

Nous généralisons dans cet article l'algorithme de Brill-Noether au cas où les singularités de C sont quelconques.

Comme l'algorithme de Brill-Noether (*cf.* [G1]) sert à construire les matrices génératrices des codes de Goppa, cette généralisation nous permet de donner un algorithme pour construire des codes géométriques définis à l'aide d'une courbe plane ayant des singularités quelconques. L'article se termine par un exemple de construction d'un tel code, défini sur $\mathbb{F}_{16}$. Ce code a pour longueur 32, dimension 4 et distance minimale 27 : il a donc des paramètres "excellents", ce qui montre qu'il est sûrement intéressant de considérer des courbes ayant des singularités quelconques.

Nous remercions F. CATANESE, de Pise, pour une conversation qui a été déterminante dans l'élaboration de cet article et Mme ORION qui a bien voulu en assurer la frappe.

0. Références

Nous utilisons dans cet article certains résultats de [F], mais sur un corps *non algébriquement clos* (un corps fini en l'occurrence). Les résultats de [F] se transposent immédiatement à ce cas; pour une référence sur la géométrie des courbes sur un corps quelconque, *cf.* [C].

1. Définitions — Rappels — Notations

Soient k un corps fini, $\bar{k}$ une clôture algébrique de k, S une surface projective lisse définie sur k.

1.1. Courbes algébriques ([F, p. 103,...]). — Soit X une courbe lisse définie sur k, contenue dans S. On supposera X absolument irréductible sur k, *i.e.* irréductible sur $\bar{k}$. La donnée d'une telle courbe est équivalente à celle de son *corps de fonctions rationnelles* $k(X)$ noté K : ce dernier est une extension de type fini et de degré de transcendance 1 de k; k est algébriquement fermé dans K.

Les points de X à coordonnées dans k sont les *points rationnels de* X.

On appelle *place de* X (ou de K) une somme formelle de points de X à coordonnées dans $\bar{k}$ invariante par l'action du groupe de Galois de $\bar{k}$ sur k. Il existe une correspondance biunivoque entre les places γ de X et les

anneaux de valuation discrète $\mathcal{O}_\gamma(X)$ de K : ord_γ désignera la valuation de $\mathcal{O}_\gamma(X)$, (*cf.* [C, p. 2]).

1.2. Diviseur rationnel. — Un diviseur D sur X, rationnel sur k, est une somme formelle de places :

$$D = \sum_\gamma n_\gamma \gamma \qquad n_\gamma \in \mathbb{Z};$$

où $n_\gamma = 0$ sauf pour un nombre fini de places γ.

Un diviseur D sera dit *effectif* si

$$D = \sum_\gamma n_\gamma \gamma \qquad \text{avec} \quad n_\gamma \geq 0,$$

pour toute place γ de X. Le *degré* d'un diviseur $D = \sum_\gamma n_\gamma \gamma$ est $\deg D = \sum_\gamma n_\gamma$. Le *support* d'un diviseur D est $\mathrm{supp}\, D = \{\gamma \mid n_\gamma \neq 0\}$.

Si f est un élément de K^* on lui associe un diviseur (f) sur X en posant :

$$(f) = \sum_\gamma \mathrm{ord}_\gamma(f)\gamma$$

et on a $\deg(f) = 0$ pour tout f dans K^* (*cf.* [C, p. 18]). Deux diviseurs $D = \sum_\gamma n_\gamma \gamma$ et $D' = \sum_\gamma n'_\gamma \gamma$ seront dits *équivalents* s'il existe f dans K^* tel que $D - D' = (f)$.

Remarquons que deux diviseurs équivalents ont le même degré.

On peut définir une relation d'ordre sur l'ensemble des diviseurs sur $\widetilde{X}$ de la façon suivante :

$$D \leq D'$$

si et seulement si pour toute place γ de X on a $n_\gamma \leq n_{\gamma'}$.

A tout diviseur D sur X est associé un k-espace vectoriel noté $\mathcal{L}(D)$:

$$\mathcal{L}(D) = \{f \in K^* \mid (f) \geq -D\} \cup \{0\}.$$

La dimension $\ell(D)$ de $\mathcal{L}(D)$ est finie et ne dépend que de la classe de D pour l'équivalence linéaire. Dans le cas où $S = \mathbb{P}^2(k)$, $\ell(D)$ est donnée par le *théorème de Riemann-Roch* (*cf.* [F, p. 210])

$$\ell(D) = \deg D + 1 - g + \ell(\mathcal{K} - D)$$

où g est le genre de X, $\mathcal{K}$ la classe canonique et si $\deg D \geq 2g - 1$, on a :

$$\ell(D) = \deg D + 1 - g.$$

(*cf.* [C, p. 32]).

1.3 Diviseur intersection. — *Un diviseur rationnel $\mathcal{D}$ sur une surface lisse S* est une somme formelle de courbes irréductibles $\mathcal{C}_i$ contenues dans S et définies sur k :

$$\mathcal{D} = \sum_i n_i \mathcal{C}_i, \qquad n_i \in \mathbb{Z};$$

(*cf.* [Sh, p. 127]) où $n_i = 0$ sauf pour un nombre fini d'indices i.

Si X est une courbe lisse de S, $\mathcal{C}$ une autre courbe définie sur k contenue dans S et ne contenant pas X comme composante, on associe à $\mathcal{C}$ un diviseur sur X en posant :

$$\mathcal{C} \cdot X = \sum_{x \in \mathcal{C} \cap X} m_x(\mathcal{C}, X)x.$$

$\mathcal{C} \cdot X$ est appelé *diviseur intersection de $\mathcal{C}$ avec X*; pour tout x de $\mathcal{C} \cap X$, $m_x(\mathcal{C}, X)$ est la *multiplicité d'intersection de $\mathcal{C}$ et X au point x*, définie de la façon suivante :

Soit $\mathcal{O}_x$ l'anneau local de S en x, Φ (resp. F) une équation de $\mathcal{C}$ (resp. X) dans $\mathcal{O}_x$, alors :

$$m_x(\mathcal{C}, X) = \dim_{\bar{k}} \mathcal{O}_x/(\Phi, F)$$

(*cf.* [B, p. 4]). Remarquons que $\mathcal{C} \cdot X$ est un diviseur rationnel effectif.

De même si $\mathcal{D}$ est un diviseur sur S : $\mathcal{D} = \sum_i n_i \mathcal{C}_i$ où pour tout i $\mathcal{C}_i$ ne contient pas X comme composante, on peut lui associer un diviseur sur X en posant :

$$\mathcal{D} \cdot X = \sum_i n_i (\mathcal{C}_i \cdot X).$$

Dans la suite nous supposerons que tous les objets et morphismes sont définis sur k (quitte à prendre une extension du corps de départ).

1.4. Éclatements (*cf.* [B, p. 15-16 dans le cas $k = \mathbb{C}$]).

Définition. — Soit S une surface projective lisse, P_1 un point de S, l'*éclatement de P_1 dans S* est un morphisme birationnel :

$$\pi_1 : S_1 \longrightarrow S$$

tel que :

S_1 est une surface projective lisse, définie sur k;
la restriction de π_1 à $\pi_1^*(S - P_1)$ est un isomorphisme sur $S - P_1$;
$E_1 = \pi_1^*(P_1)$ est isomorphe à $\mathbb{P}^1$.

E_1 est *le diviseur exceptionnel de l'éclatement.*

Si C est une courbe de S et P_1 un point de C de multiplicité r_1, l'adhérence de $\pi_1^*(C - P_1)$ dans S_1 est une courbe C_1 appelée *transformée stricte de C dans S_1* et on a :

$$\pi_1^*(C) = C_1 + r_1 E_1.$$

La restriction $\tilde{\pi}_1$ de π_1 à C_1 est *l'éclatement du point P_1 dans C*; le diagramme suivant :

$$\begin{array}{ccc} C_1 & \hookrightarrow & S_1 \\ \downarrow{\scriptstyle \tilde{\pi}_1} & & \downarrow{\scriptstyle \pi_1} \\ C & \hookrightarrow & S \end{array}$$

est commutatif.

Pratiquement l'éclatement π_1 se fait de la façon suivante :

Soient U un ouvert de S, contenant P_1, (x, y) des coordonnées locales au voisinage de P_1, U_1 la sous-variété de $U \times \mathbb{P}^1$ d'équation : $xY - yX = 0$ où (X, Y) désigne les coordonnées homogènes dans $\mathbb{P}^1$. La projection p_1 :

$$\begin{array}{ccc} U_1 & \longrightarrow & U \\ (x, y, X, Y) & \mapsto & (x, y) \end{array}$$

est un isomorphisme au-dessus des points de U tels que x ou y soit non nul et :

$$p_1^{-1}(P_1) = \{P_1\} \times \mathbb{P}^1.$$

Les points de $E_1 \cap C_1$ s'identifient aux directions tangentes à S en P_1.

1.5. Nous aurons besoin dans la suite du lemme suivant :

Soit V un ouvert non vide de C, on note $\Gamma(V)$ l'ensemble des fonctions rationnelles sur C qui sont définies en tout point de V, alors on a avec les mêmes notations que plus haut et en supposant que $x = 0$ est l'équation de E_1 (*cf.* [F, p. 165]) :

LEMME. — *Il existe un voisinage affine W de P_1 dans C tel que $\pi_1^{-1}(W)$ soit une sous-variété affine ouverte W' de C_1 et on a :*

$$x^{r_1 - 1}\Gamma(W') \subset \Gamma(W).$$

1.6. Normalisée d'une courbe. — Soit C une courbe définie sur k, absolument irréductible sur k, contenue dans une surface lisse S. Si P_1 est

un point singulier de C, on éclate ce point dans S et on a le diagramme commutatif :

$$\begin{array}{ccc} C_1 & \longrightarrow & S_1 \\ \downarrow{\scriptstyle \tilde{\pi}_1} & & \downarrow{\scriptstyle \pi_1} \\ C & \longrightarrow & S \end{array}$$

Si C_1 est une courbe lisse dans S_1, C_1 est la normalisée, notée $\widetilde{C}$, de C; sinon on éclate un point singulier P_2 de C_1, *etc.* On sait qu'au bout d'un nombre fini N d'éclatements ponctuels, la transformée stricte C_N de C_{N-1} par π_N sera une courbe lisse : c'est la normalisée $\widetilde{C}$ de C (*cf.* [F, p. 180]). La surface lisse S_N sera notée $\widetilde{S}$.

Posons $\pi = \pi_N \circ \cdots \circ \pi_1$; π_i est l'éclatement d'un point P_i de S_{i-1} de multiplicité r_i sur C_{i-1} ($C_0 = C$; $S_0 = S$). On notera $\tilde{\pi} : \widetilde{C} \to C$ le *morphisme de normalisation* qui rend commutatif le diagramme :

$$\begin{array}{ccc} \widetilde{C} & \hookrightarrow & \widetilde{S} \\ \downarrow{\scriptstyle \tilde{\pi}} & & \downarrow{\scriptstyle \pi} \\ C & \hookrightarrow & S \end{array}$$

Si P est un point singulier de C, les points P_i qui se projettent sur P sont appelées classiquement *points infiniment voisins de* P.

Les places γ de $\widetilde{C}$ telles que $\tilde{\pi}_*(\gamma) = P$ seront appelées *places au-dessus de* P.

1.7. Diviseur sur la normalisée d'une courbe. — Soit D un diviseur effectif sur S, on peut lui associer le diviseur $\pi^*(D)$ sur $\widetilde{S}$. Si $\pi^*(D)$ ne contient pas $\widetilde{C}$ comme composante, il définit un diviseur sur $\widetilde{C}$ comme on l'a vu dans § 1.3. Nous appliquerons ce résultat par la suite dans les cas suivants :

a) Soit E_i le diviseur exceptionnel du ième éclatement π_i et π'_i le morphisme

$$\widetilde{S} \longrightarrow S_i \qquad \left(\pi'_i = \pi_N \circ \cdots \circ \pi_{i+1}\,;\ \pi'_0 = \pi\right).$$

On notera $\widetilde{E}_i$ le diviseur effectif sur $\widetilde{C}$ associé au diviseur sur $\widetilde{S}$: $\pi_i'^*(E_i)$ (il est clair que ce dernier ne contient pas $\widetilde{C}$ comme composante). On a donc :

$$\widetilde{E}_i = \pi_i'^*(E_i) \cdot \widetilde{C}.$$

b) Soit $\mathfrak{C}$ une courbe tracée sur S ne contenant pas C comme composante. On notera $(\mathfrak{C})$ le diviseur effectif sur $\widetilde{C}$ associé au diviseur sur $\widetilde{S}$, $\pi^*(\mathfrak{C})$:

$$(\mathfrak{C}) = \pi^*(\mathfrak{C}) \cdot \widetilde{C}.$$

Il résulte de l'hypothèse que $\pi^*(\mathfrak{C})$ ne contient pas $\widetilde{C}'$ comme composante).

1.8. Courbes projectives planes. Formes. — On se place maintenant dans le cas où $S = \mathbb{P}^2(k)$.

Un polynôme homogène de $k[X, Y, Z]$ de degré d est *une forme de degré d.*

Une *courbe projective plane* C définie sur k admet pour équation $\varphi(X, Y, Z) = 0$ où φ est une forme. On notera une courbe plane C d'équation $\varphi = 0$: $C(\varphi = 0)$.

On dira qu'une courbe plane C est à *singularités ordinaires* si en chaque point singulier P de C de multiplicité r, la courbe a r tangentes distinctes. Si C est une courbe plane absolument irréductible sur k, n'ayant que des singularités ordinaires $P_1, \ldots, P_n$ de multiplicités respectives $r_1, \ldots, r_n$, le *genre* de C est égal :

$$g = \tfrac{1}{2}(m-1)(m-2) - \tfrac{1}{2}\sum_{j=1}^{n} r_j(r_j - 1)$$

(*cf.* [F, p. 199]) où m est le degré de la forme φ qui définit C (g est en fait le genre de la normalisée $\widetilde{C}$ de C).

Soit C une courbe projective plane singulière, $\tilde{\pi} : \widetilde{C} \to C$ le morphisme de normalisation de C. Si $\tilde{\pi}$ est composé de N éclatements ponctuels de centre $P_1, \ldots, P_N$ ayant les multiplicités respectives $r_1, \ldots, r_N$ sur les transformées strictes successives C_i, alors *le genre de* $\widetilde{C}$ (*ou de* C) est égal à (*cf.* [A]) :

$$g = \tfrac{1}{2}(m-1)(m-2) - \tfrac{1}{2}\sum_{j=1}^{N} r_j(r_j - 1).$$

Soient $C(F = 0)$ une courbe plane singulière, $\tilde{\pi} : \widetilde{C} \to C$ le morphisme de normalisation, $\mathfrak{C}(\varphi = 0)$ une autre courbe plane ne contenant pas C comme composante. Le diviseur sur $\widetilde{C}$ associé à $\mathfrak{C}$ est égal à :

$$(\mathfrak{C}) = \sum_{\gamma} \operatorname{ord}_\gamma(\varphi)\gamma$$

où $\operatorname{ord}_\gamma(\varphi)$ est défini de la façon suivante : si γ est une place au-dessus d'un point singulier P de C, (x, y) des coordonnées locales au voisinage

de P, $\varphi_*(x,y)$ l'équation locale de $\mathfrak{C}$ au voisinage de P et $\bar{\varphi}$ l'image de φ_* dans $\mathcal{O}_P(C) \subset K$, alors on pose :

$$\mathrm{ord}_\gamma(\varphi) = \mathrm{ord}_\gamma(\bar{\varphi})$$

(*cf.* [F, p. 182]). Si $\gamma_1, \ldots, \gamma_\ell$ sont les places de $\widetilde{C}$ au-dessus de P, on décompose chaque γ_i en une somme formelle de points à coordonnées dans $\bar{k}$:

$$\gamma_i = \sum_{j=1}^{n_i} Q_{ji}.$$

Un point Q_{ji} ainsi obtenu appartient au support d'une seule place γ_i, on peut donc poser sans ambiguité :

$$\mathrm{ord}_{Q_{ji}} = \mathrm{ord}_{\gamma_i}.$$

Alors on a :

$$m_P(\mathfrak{C}, C) = \sum_{i=1}^{\ell} \sum_{j=1}^{n_i} \mathrm{ord}_{Q_{ji}}(\bar{\varphi}).$$

2. Adjointe d'une courbe C contenue dans une surface

Il est entendu une fois pour toutes que les courbes $\mathfrak{C}$ de S considérées ne contiennent pas C comme composante.

Les objets et morphismes considérés dans ce paragraphe seront toujours supposés définis sur k.

2.1. Soit S une surface algébrique lisse et projective, C une courbe réduite (non nécessairement lisse) contenue dans S. On note comme dans le paragraphe précédent par $\tilde{\pi} : \widetilde{C} \to C$ le morphisme de normalisation de C et $\tilde{\pi} = \tilde{\pi}_N \circ \cdots \circ \tilde{\pi}_1$. Pour chaque i, $i = 1, \ldots, N$, on a le diagramme commutatif :

$$\begin{array}{ccc} C_i & \hookrightarrow & S_i \\ \downarrow{\scriptstyle \tilde{\pi}_i} & & \downarrow{\scriptstyle \pi_i} \\ C_{i-1} & \hookrightarrow & S_{i-1} \end{array}$$

où π_i est l'éclatement dans la surface lisse S_{i-1} d'un point $P_i \in C_{i-1}$ de multiplicité r_i ($r_i > 1$) sur C_{i-1} ; E_i désigne le diviseur exceptionnel de l'éclatement π_i, $E_i = \pi_i^*(P_i)$, π_i' le morphisme : $\widetilde{S} \to S_i$, ($\pi_0' = \pi$) et $\widetilde{E}_i$ le diviseur sur $\widetilde{C}$ défini par $\pi_i'^*(E_i)$ (*cf.* § 1.7).

2.2. Définition. — Une courbe $\mathfrak{C} \subset S$ est dite *adjointe de C* si l'on a :

$$(\mathfrak{C}) \geq \sum_{i=1}^{N} (r_i - 1)\widetilde{E}_i.$$

Le diviseur $\sum_{i=1}^{N}(r_i - 1)\widetilde{E}_i$ est appelé *diviseur d'adjonction de C.*

2.3. Exemples.

a) Si C est lisse, toute courbe est une adjointe de C (en effet le diviseur d'adjonction est réduit à (0)).

b) LEMME. — *Si C n'a que des singularités ordinaires P_j de multiplicités r_j, une courbe $\mathfrak{C}$ est une adjointe de C si et seulement si on a pour tout j : $e_{P_j}(\mathfrak{C}) \geq r_j - 1$ où $e_{P_j}(\mathfrak{C})$ désigne la multiplicité de $\mathfrak{C}$ en P_j.*

Démonstration. — Pour désingulariser C il faut faire éclater *une fois* chaque point P_j ; comme ces éclatements sont indépendants les uns des autres on peut supposer que C a une seule singularité ordinaire P de multiplicité r. Soit π_1 l'éclatement du point P dans S.

Le diviseur $\widetilde{E}_1$ sur $\widetilde{C}$ contient exactement r points $Q_1, \ldots, Q_r$, à coordonnées dans $\bar{k}$, qui correspondent aux r tangentes distinctes de C en P :

$$\widetilde{E}_1 = \sum_{i=1}^{r} Q_i.$$

Soit $\mathfrak{C}$ une courbe de S telle que $e_P(\mathfrak{C}) \geq r - 1$. On a (*cf.* § 1.4) :

$$\pi_1^*(\mathfrak{C}) = \mathfrak{C}_1 + e_P(\mathfrak{C})E_1$$

où $\mathfrak{C}_1$ est la transformée stricte de $\mathfrak{C}$ par π_1.

Par suite :

$$(\mathfrak{C}) = \pi_1^*(\mathfrak{C}) \cdot \widetilde{C} \geq e_P(\mathfrak{C})\widetilde{E}_1$$

et la courbe $\mathfrak{C}$ est une adjointe de C.

Réciproquement si $\mathfrak{C}$ est une adjointe de C on a

$$(H) \qquad (\mathfrak{C}) \geq \sum_{j} (r_j - 1)\widetilde{E}_j$$

et $\widetilde{E}_j = \sum_{i=1}^{r_j} Q_{ji}$.

Si pour un certain j on a $e_{P_j}(\mathfrak{C}) = e < r_j - 1$, il existe au moins une branche de C à laquelle $\mathfrak{C}$ n'est pas tangente en P_j. Si Q_{ji} est un des

points de $\widetilde{E}_j$ correspondant à cette branche, le coefficient de Q_{ji} dans $(\mathfrak{C})$ est égal à e ce qui contredit l'hypothèse (H).

Remarque. — On retrouve bien la définition classique d'une adjointe (*cf.* [F, p. 190]).

c) Considérons la courbe projective plane C d'équation $Y^2T = X^3$, C a une seule singularité, qui est non ordinaire, en $P_1 = (0,0,1)$ de multiplicité $r_1 = 2$. Le morphisme $\tilde{\pi}$ est constitué d'un seul éclatement, celui de P_1, et si Q_1 est l'unique point de $\widetilde{C}$ tel que

$$\tilde{\pi}(Q_1) = P_1$$

on a $\widetilde{E}_1 = 2Q_1$ (le diviseur E_1 est tangent à $\widetilde{C}$ en Q_1).

On en déduit immédiatement qu'une courbe plane $\mathfrak{C}$, ne contenant pas C comme composante, est une adjointe de C si $\mathfrak{C}$ passe par P_1 ; en effet on a :

$$(\mathfrak{C}) = \sum_{\gamma} \mathrm{ord}_{\gamma}(\mathfrak{C})\gamma$$

et pour $\gamma = Q_1$, on a $\mathrm{ord}_{\gamma}(\mathfrak{C}) = m_{P_1}(\mathfrak{C}_1 C)$.

Par suite la condition $(\mathfrak{C}) \geq E_1$, implique $m_{P_1}(\mathfrak{C}, C) \geq 2$. Or $m_{P_1}(\mathfrak{C}, C) \geq e_{P_1}(\mathfrak{C}) \times e_{P_1}(C) = e_{P_1} \times 2$; donc si $e_{P_1}(\mathfrak{C}) \geq 1$ la courbe $\mathfrak{C}$ sera une adjointe de C.

2.4. Il résulte de la définition des diviseurs $\widetilde{E}_i$ et de celles des adjointes que, si une courbe $\mathfrak{C}$, contenue dans une surface S, "passe" par chaque point infiniment voisin P_i avec une multiplicité supérieure ou égale à $r_i - 1$, $(1 \leq i \leq N$, N désignant le nombre d'éclatements nécessaires pour désingulariser $C)$, alors $\mathfrak{C}$ est une adjointe de C.

Cette condition est souvent prise comme définition de l'adjointe d'une courbe (*cf.* [A]), mais elle est plus restrictive que la définition que nous avons donnée : en effet on voit dans l'exemple 2.3.c) que si $\mathfrak{C}$ passe par P_1 avec la multiplicité 1, sans admettre $Y = 0$ comme tangente, $\mathfrak{C}$ sera une adjointe de C au sens de notre définition mais ne vérifiera pas la condition ci-dessus.

2.5. Nous allons maintenant donner une autre condition suffisante sur $\mathfrak{C}$ pour être adjointe de C au sens de notre définition.

Soit C une courbe réduite contenue dans S.

Plaçons-nous au voisinage d'un point singulier P_0 de C et notons $\pi_0 : \widetilde{S}_0 \to S$ le morphisme composé des éclatements désingularisant C au voisinage de P_0 : π_0 est composé de p-éclatements qui sont certains des éclatements de la suite qui compose π.

Notons $E'_i \subset \widetilde{S}_0$ le transformé strict du diviseur exceptionnel E_i du ième éclatement, par le morphisme

$$\pi'_{i,0} : \widetilde{S}_0 \to S_i \quad (0 \leq i \leq p-1,\ \pi'_0 = \pi_0).$$

On a alors :

2.6. LEMME. — $\pi_0^*(P_0) = n_1 E'_1 + \cdots + n_p E'_p, \qquad (E'_p = E_p).$

Preuve. — En effet on a $\pi_1^*(P_0) = E_1$. Le morphisme π_2 est l'éclatement d'un point P_2 de E_1 ; on a donc :

$$\pi_2^*(E_1) = E'_1 + E_2$$

avec l'abus de langage consistant à noter de la même façon les transformées strictes de E_j sur $\widetilde{S}_0$ et sur S_i (pour $j < i$). Plus généralement π_i est l'éclatement d'un point P_i de E_ℓ avec $\ell < i$. Alors :

1. si $P_i \notin E_k \qquad \forall k < i,\ k \neq \ell$, on a:

$$\begin{cases} \pi_i^*(E_\ell) = E'_\ell + E_i, \\ \pi_i^*(E_k) = E'_k, \end{cases}$$

$\forall k < i,\ k \neq \ell$ (avec le même abus de langage que précédemment).

2. si $P_i \in E_\ell \cap E_k$ pour un certain $k,\ k < i,\ k \neq \ell$, on a :

$$\begin{cases} \pi_i^*(E_\ell) = E'_\ell + E_i, \\ \pi_i^*(E_k) = E'_k + E_i, \\ \pi_i^*(E_m) = E'_m, \end{cases}$$

$\forall m < i, m \neq k$ et ℓ. Dans le cas 1, on a $n_i = n_\ell$ et dans le cas 2 : $n_i = n_\ell + n_k$. On est toujours dans l'un de ces deux cas car trois diviseurs E'_j n'ont jamais de point commun.

2.7. On a :

$$\widetilde{E}_i = \pi'^*_{i,0}(E_i) \cdot \widetilde{C} = E'_i \cdot \widetilde{C},$$
$$E_i = \pi_i^*(P_i).$$

Le LEMME 2.6 appliqué en P_i au morphisme $\pi'_{i-1,0}$: $\widetilde{S}_0 \to S_{i-1}$ donne :

$$\begin{aligned} \widetilde{E}_i &= \pi'^*_{i-1,0}(P_i) \cdot \widetilde{C} \\ &= \left(m_{i,i} E'_i + m_{i,i+1} E'_{i+1} + \cdots + m_{i,p} E_p\right) \cdot \widetilde{C}. \end{aligned}$$

Si une courbe $\mathfrak{C}$, contenue dans S, a une multiplicité e_0 au point P_0, elle vérifiera la condition d'adjonction en ce point si :

$$(\mathfrak{C}) = \pi_0^*(\mathfrak{C}) \cdot \widetilde{C} \geq \sum_{i=1}^{p} (r_i - 1)\widetilde{E}_i.$$

Comme on a :

$$\pi_0^*(\mathfrak{C}) \geq e_0\, \pi_0^*(P_0) = \sum_{i=1}^{p} n_i e_0 E_i'$$

il suffit donc que pour tout i, $1 \leq i \leq p$, on ait :

$$n_i e_0 \geq \sum_{j=1}^{i} m_{j,i}(r_j - 1)$$

soit

$$e_0 \geq \sup_{1 \leq i \leq p} \frac{1}{n_i} \sum_{j=1}^{i} m_{j,i}(r_j - 1) = a_{P_0}.$$

Nous venons de prouver le théorème suivant :

2.8. THÉORÈME. — *Soit C une courbe réduite contenue dans une surface lisse S ; une courbe $\mathfrak{C}$ de S est une adjointe de C si $\mathfrak{C}$ a en chaque point singulier P de C une multiplicité supérieure ou égale à a_P où, avec les notations précédentes, on a:*

$$a_P = \sup_{1 \leq i \leq p} \frac{1}{n_i} \sum_{j=i}^{i} m_{j,i}(r_j - 1).$$

3. Théorème des résidus

On se place dans le cas $S = \mathbb{P}^2(k)$. Posons $E = \sum(r_i - 1)\widetilde{E}_i$; E est le diviseur d'adjonction sur C.

3.1. THÉORÈME DES RÉSIDUS. — *Supposons C absolument irréductible sur k ; soient D et D' deux diviseurs effectifs sur C, linéairement équivalents, E le diviseur d'adjonction sur C, G une forme de degré p telle que :*

$$(G) = A + E + D \qquad \textit{(avec } A \textit{ effectif).}$$

Alors il existe une forme G' de même degré p telle que

$$(G') = A + E + D'.$$

Démonstration (*cf.* [F, p. 190]). — Les diviseurs D et D' étant équivalents il existe par définition des formes H et H' de même degré telles que

$$D + (H) = D' + (H')$$

(*cf.* [F, p. 189]). On a alors :

$$\begin{aligned}(GH) &= (G) + (H)\\ &= A + E + D + (H)\\ &= A + E + D' + (H').\end{aligned}$$

On a donc $(GH) \geq E + (H')$.

Si G est une forme, $\overline{G}$ désignera l'image de G dans $\mathcal{O}_P(C)$.

Nous allons appliquer à GH le lemme suivant :

3.2. LEMME. — *Soient E le diviseur d'adjonction sur C, M et L deux formes telles que :*

$$(M) \geq E + (L).$$

Alors on a :

$$\overline{M} \in \overline{L}\,\mathcal{O}_P(C) \qquad \forall P \in C.$$

Preuve du Lemme. — La question est locale en chaque point P de C.

Si donc P est un point de C, on va raisonner par récurrence sur le nombre minimal d'éclatements nécessaires pour désingulariser la courbe C au voisinage de P.

Si P est lisse, le lemme est évident.

Soient donc $P \in C$ un point de multiplicité r, $\tilde{\pi}_1 : C_1 \to C$ l'éclatement du point P, $W \subset C$ un voisinage affine de P dans C tel que le LEMME 1.5 soit vérifié ($W_1 = \tilde{\pi}_1^{-1}(W)$ est alors un ouvert affine de C_1 contenant tous les points P_i de C_1 tels que $\tilde{\pi}_1(P_i) = P$).

Nous supposerons que $X = 0$ est une équation du diviseur exceptionnel E_1 de π_1 et que P est dans la carte affine $T = 1$. Si G est une forme, nous noterons $\mathrm{Div}_P(\overline{G})$ (*resp.* E_P) le diviseur sur $\widetilde{C}$ defini par $\overline{G}$ (*resp.* E) aux places qui sont au-dessus de P.

Revenons à la preuve du LEMME 3.2.

Posons $\varphi = \overline{M}/\overline{L}$ dans le corps des fractions de $\mathcal{O}_P(C)$ et soient φ_1 (*resp.* $\overline{M}_1$, $\overline{L}_1$), les transformées totales par π_1 de φ (*resp.* $\overline{M}$, $\overline{L}$).

Enfin posons $\varphi_1 = X^{r-1}\varphi_2$. On a alors :

$$\left.\begin{aligned}\mathrm{Div}_P(\overline{M}) &= \mathrm{Div}_P(\overline{M}_1)\\ \mathrm{Div}_P(\overline{L}) &= \mathrm{Div}_P(\overline{L}_1)\end{aligned}\right\} \quad \text{par définition.}$$

De plus, $\mathrm{Div}_P(\overline{M}) \geq E_P + \mathrm{Div}_P(\overline{L})$ par hypothèse. Si on pose $E_P = (r-1)\,\mathrm{Div}_P(\overline{X}) + E'_P$, on a :

$$\mathrm{Div}(\overline{M}_1) \geq E'_P + (r-1)\,\mathrm{Div}_P(\overline{X}) + \mathrm{Div}_P(\overline{L}_1);$$

$X = 0$ étant par hypothèse une équation du diviseur exceptionnel de π_1, E'_P est égal au diviseur d'adjonction de C_1 aux places de $\widetilde{C}_1 = \widetilde{C}$ qui sont au-dessus de P.

On a alors par hypothèse de récurrence :

$$\varphi_2 = \overline{M}_1 / \overline{L}_1 (\overline{X})^{r-1} \in \mathcal{O}_{P_i}(C_1)$$

pour tout point P_i de C_1 tel que $\tilde{\pi}_1(P_i) = P$.

On obtient alors par le LEMME 1.5 :

$$\varphi \in \mathcal{O}_P(C).$$

3.3. *Fin de la démonstration du* THÉORÈME 3.1. En appliquant à GH le LEMME 3.2 on obtient :

$$\overline{GH} \in \overline{H}'\mathcal{O}_P(C) \qquad \forall P \in C.$$

On peut alors utiliser le "*théorème fondamental de* Max NOETHER" ([F, p. 120]).

Il existe une forme G' de même degré que G telle que :

$$GH = G'H' + BF,$$

F étant une équation de C. On a alors :

$$(GH) = (G'H')\,,$$

soit $$(G') = (G) + (H) - (H')$$

d'où $$(G') = A + E + D'.$$

4. L'algorithme de Brill-Noether

Soit C une courbe plane définie sur k et absolument irréductible. Soit D un diviseur rationnel effectif sur la normalisée $\widetilde{C}$ de C.

L'algorithme va construire une base de $\mathcal{L}(D)$.

4.1. PROPOSITION. — *Soit E le diviseur d'adjonction sur C, G_0 une forme de degré ℓ telle que :*

$$(G_0) = E + D + A,$$

où A est effectif; alors on a

$$\mathcal{L}(D) = \left\{ \varphi \in k(C) \mid \varphi = \overline{G}/\overline{G}_0 \right\}$$

où G décrit l'espace des formes de degré ℓ, non divisibles par l'équation de C et telles que $(G) \geq E + A$.

Démonstration.

a) Si φ s'écrit $\overline{G}/\overline{G}_0$ comme dans l'énoncé du lemme on a :

$$(\varphi) = D' - D \geq -D$$

car D' est effectif; donc $\varphi \in \mathcal{L}(D)$.

b) Réciproquement soit $\psi \in \mathcal{L}(D)$. On peut donc écrire $(\psi) = D_1 - D$ où D_1 est un diviseur effectif sur $\widetilde{C}$ linéairement équivalent à D.

D'après la PROPOSITION 3.1, il existe une forme G_1 de même degré que G_0 telle que :

$$(G_1) = E + D' + A.$$

La fonction $\psi_1 = \overline{G}_1/\overline{G}_0$ a alors le même diviseur que la fonction ψ : ces deux fonctions diffèrent donc par une constante et ψ est bien de la forme voulue.

4.2. Plan de l'algorithme.

Les données sont :

l'équation de C : forme $F(X,Y,T) = 0$ de degré m;

le diviseur D : si S_c est le lieu singulier de C, nous supposerons que les supports de D et de $\tilde{\pi}^{-1}(S_c)$ sont disjoints.

1. Déterminer une condition d'adjonction : pour cela on doit rechercher

a) les points singuliers de C (on les suppose rationnels sur k) et leurs multiplicités,

b) pour chaque point singulier, l'entier a_P défini dans le THÉORÈME 2.8.

2. Trouver une forme G_0 de degré ℓ ("assez grand") telle que

a) G_0 non divisible par F,

b) $G_0 = 0$ est l'équation d'une adjointe de C et on a $(G_0) \geq 0$.

b1) Si $\ell < m$, F étant irréductible, cette condition sera réalisée.

Si $\ell \geq m$, on cherchera une base d'un supplémentaire V de l'espace des formes de degré ℓ dont l'équation est divisible par F.

b2) Puis on écrira qu'un élément générique G de V "passe" par chaque point singulier P de C avec une multiplicité $\geq a_P$.

b3) Si $D = \sum_\gamma n_\gamma \gamma$, $n_\gamma \geq 0$, pour chaque place γ telle que $n_\gamma > 0$ on détermine (si possible) une paramétrisation locale $(x(t), y(t))$ et on écrit que la valuation de G en t est $\geq n_\gamma$.

On sélectionne une forme G_0 vérifiant les conditions précédentes.

3. Déterminer le diviseur "résiduel" : $E' = (G_0) - D$.

4. Trouver une base sur k de l'espace des formes G de degré ℓ telles que :

$$(G) \geq E'.$$

5. Si $\{G_0, \ldots, G_n\}$ est une telle base, une base de $\mathcal{L}(D)$ est donnée par

$$\left\{1, \overline{G}_1/\overline{G}_0, \ldots, \overline{G}_n/\overline{G}_0\right\}$$

d'après la PROPOSITION 4.1.

4.3. Remarque sur l'entier n ($n = \dim_k \mathcal{L}(D)$). — D'après le théorème de Riemann-Roch on a :

$$n \geq \deg D - g + 1$$

avec égalité si $\deg D \geq 2g - 1$.

Rappelons que le genre g de la courbe C est donné par :

$$g = \tfrac{1}{2}(m-1)(m-2) - \tfrac{1}{2}\sum_{i=1}^{N} r_i(r_i - 1)$$

(*cf.* 1.8); où les points P_i, $i = 1, \ldots, N$ sont les centres des éclatements nécessaires pour désingulariser la courbe C.

4.4. Remarques sur le diviseur D. — Dans 4.2 nous avons supposé que les supports de D et $\tilde{\pi}^{-1}(S_c)$ étaient disjoints. Cette hypothèse permet d'affirmer que si $G_0 = 0$ est l'équation d'une adjointe de C et si $(G_0) \geq D$, on a bien $(G_0) \geq D + E$ où E est le diviseur d'adjonction; on peut donc appliquer la PROPOSITION 4.1.

Toutefois dans les exemples on pourra prendre des diviseurs rationnels D contenant des points de $\tilde{\pi}^{-1}(S_c)$ si on est assuré que le diviseur résiduel E' est plus grand que le diviseur d'adjonction E.

4.5. Remarque sur l'entier ℓ (ℓ = degré des adjointes). — La dimension r de l'espace V des formes de degré ℓ non divisibles par l'équation de G est égale à :

$$r = \begin{cases} r_1 = \frac{1}{2}\ell(\ell+3) & \text{si } \ell \leq m, \\ r_1 - \frac{1}{2}(\ell-m)(\ell-m+3) & \text{si } \ell > m. \end{cases}$$

La condition d'adjonction conduit à $\frac{1}{2}\sum_P a_P(a_P+1)$ conditions indépendantes, où la somme est prise sur tous les points singuliers P de C et les entiers a_P sont ceux définis dans le THÉORÈME 2.8.

Si $D = \sum_\gamma n_\gamma \gamma$, écrire qu'une forme G_0 est telle que $(G_0) \geq D$ conduit à d conditions (d à déterminer dans chaque cas).

Pour qu'une forme G_0 vérifiant les hypothèses de l'algorithme existe il faudra que son degré ℓ soit tel que :

$$r - \frac{1}{2}\sum_P a_P(a_P+1) - d \geq 0.$$

5. Application : codes de Goppa

5.1. Rappelons brièvement la construction des codes de Goppa telle qu'elle est exposée dans [G1,G2,VM,...].

On se place sur le corps fini $k = \mathbb{F}_q$, avec $q = p^r$ et p premier, et on considère une courbe plane $C(F=0)$ définie et absolument irréductible sur k, de genre g.

Soient G et D deux diviseurs rationnels effectifs sur la normalisée $\widetilde{C}$ de C vérifiant les conditions :

a) $D = Q_1 + \cdots + Q_n$ où les Q_i sont des points de $\widetilde{C}$ deux à deux distincts et rationnels sur k.

b) les supports de D et G sont disjoints.

c) $\deg G < n$.

Alors, le code de Goppa associé à D, G et C est l'image de l'aplication linéaire :

$$\Phi : \mathcal{L}(G) \longrightarrow (\mathbb{F}_q)^n,$$
$$\Phi(f) = \big(f(Q_1), \ldots, f(Q_n)\big).$$

L'application Φ est injective grâce à l'hypothèse c). Le code obtenu est de type $[n, k, d]$ où

$$n = \deg D,$$
$$k \geq \deg G - g + 1, \qquad \text{(avec égalité si} \quad \deg G \geq 2g - 1),$$
$$d \geq n - \deg G.$$

Dans [G], GOPPA considère des courbes planes à singularités ordinaires. Nous donnons ici un exemple de code de Goppa associé à une courbe plane ayant des singularités quelconques.

5.2. On se place sur le corps $k = \mathbb{F}_{16}$ et on considère la courbe plane C d'équation :

$$Y^2Z^3 + YZ^4 + X^5 = 0.$$

Remarque. — Cette courbe est citée dans [Se] : elle a la propriété d'avoir "beaucoup" de points rationnels sur $\mathbb{F}_{16}$ (en fait, elle a le maximum de points rationnels possibles compatible avec la borne de Weil, *cf.* plus loin).

Le degré de C est $m = 5$. La courbe a un seul point singulier, non ordinaire, $P_1 = (0, 1, 0)$ de multiplicité $r_1 = 3$.

La normalisée $\widetilde{C}$ s'obtient en éclatant deux fois :

1^er *éclatement* π_1 ; on éclate le point P_1 : dans la carte $Y = 1$, on fait la changement de variable :

$$X' = X,$$
$$Z' = ZX'.$$

Le diviseur exceptionnel E_1 de π_1 a pour équation : $X' = 0$. La transformée stricte C_1 de C a pour équation locale au voisinage du point infiniment voisin $P_2 = (0, 0)$:

$$X'^2 + X'Z'^4 + Z'^3 = 0.$$

2^e *éclatement* π_2 ; on éclate le point P_2 : P_2 est de multiplicité $r_2 = 2$ sur C_1, on fait le changement de variable :

$$X'' = X'Z'',$$
$$Z'' = Z'.$$

Le diviseur exceptionnel E_2 de π_2 a pour équation $Z'' = 0$.

La transformée stricte C_2 de C_1 a pour équation locale au voisinage du point infiniment voisin $P_3 = (0,0)$:

$$Z'' + X''^2 + X''Z''^3 = 0.$$

P_3 est un point lisse de C_2 et $C_2 = \widetilde{C}$. Le genre g de $\widetilde{C}$ (ou de C) est égal à :

$$g = \tfrac{1}{2}(m-1)(m-2) - \tfrac{1}{2}\sum_{i=1}^{3} r_i(r_i - 1),$$

soit $g = 2$. Avec les notations du paragraphe 2.4, on a :

$$n_1 = n_2 = 1\,; \quad m_{11} = m_{12} = m_{22} = 1.$$

Le diviseur d'adjonction est :

$$E = 3\,P_3.$$

Une courbe plane $\mathfrak{C}$ sera adjointe de C si :

$$e_{P_1}(\mathfrak{C}) \geq 3 \qquad (a_{P_1} = 3).$$

Cherchons les points de $\widetilde{C}$ qui sont rationnels sur $\mathbb{F}_{16}$. Leur nombre n_0 est majoré par la borne de Weil (*cf.* [Se]). :

$$n_0 \leq q + 1 + 2g\sqrt{q}\,; \qquad \text{ici} \quad q = 16, \quad \text{d'où } n_0 \leq 33.$$

Nous allons voir que dans cet exemple la borne de Weil est atteinte.

Soit α une racine primitive quinzième de 1 vérifiant $\alpha^4 + \alpha + 1 = 0$; la racine α engendre $\mathbb{F}_{16}$.

La courbe plane C a 33 points rationnels sur $\mathbb{F}_{16}$:

$$\begin{array}{lll}
Q_0 = (0,01); \quad Q_1 = (0,1,0)(= P_1); \quad Q_2 = (0,1,1) & & \\
Q_3\,,\ldots,Q_7 \;:\; (a,\alpha,1) & \text{où} & a = \alpha,\alpha^4,\alpha^7,\alpha^{10},\alpha^{13} \\
Q_8\,,\ldots,Q_{12} \;:\; (a,\alpha^2,1) & \ldots & a = \alpha^2,\alpha^5,\alpha^8,\alpha^{11},\alpha^{14} \\
Q_{13},\ldots,Q_{17} \;:\; (a,\alpha^4,1) & \ldots & a = \alpha,\alpha^4,\alpha^7,\alpha^{10},\alpha^{13} \\
Q_{18},\ldots,Q_{22} \;:\; (a,\alpha^5,1) & \ldots & a = 1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12} \\
Q_{23},\ldots,Q_{27} \;:\; (a,\alpha^8,1) & \ldots & a = \alpha^2,\alpha^5,\alpha^8,\alpha^{11},\alpha^{14} \\
Q_{28},\ldots,Q_{32} \;:\; (a,\alpha^{10},1) & \ldots & a = 1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12}.
\end{array}$$

Si on note de la même façon les points rationnels lisses de C et les points correspondants de $\widetilde{C}$, on voit que $\widetilde{C}$ a aussi 33 points rationnels qui sont :

$$Q_0,\ P_3,\ Q_2,\ Q_3,\ldots,Q_{32}.$$

Considérons les diviseurs effectifs rationnels sur $\mathbb{F}_{16}$ de $\widetilde{C}$:

$$\begin{cases} D = P_3 + Q_2 + Q_3 + \cdots + Q_{32}, \\ G = 5\,Q_0, \end{cases}$$

et cherchons le code de Goppa associé à D, G et C, image de l'application linéaire :

$$\Phi : \mathcal{L}(G) \longrightarrow (\mathbb{F}_{16})^{32},$$
$$\Phi(f) = \big(f(P_3), f(Q_2), \ldots, f(Q_{32})\big).$$

Comme $\deg G \geq 2g - 1$, ses paramètres vérifieront :

$$\begin{cases} k = \dim \mathcal{L}(G) = \deg G - g + 1 = 4, \\ n = 32, \\ d \geq n - \deg G = 27. \end{cases}$$

Considérons l'espace vectoriel des formes de degré 7. Une base de cet espace est :

$$\begin{aligned} \Lambda_0 &= Z^7\,;\ \Lambda_1 = XZ^6 \ldots\,;\ \Lambda_7 = X^7 \\ \Lambda_8 &= YZ^6\,;\ \ldots\,;\ \Lambda_{14} = YX^6 \\ &\cdots \\ \Lambda_{33} &= Y^6Z\,;\ \Lambda_{34} = Y^6X \\ \Lambda_{35} &= Y^7. \end{aligned}$$

Le sous-espace des formes dont l'équation est divisible par celle de C est engendré par :

$$\begin{aligned} \Lambda'_5 &= \Lambda_5 + \Lambda_8 + \Lambda_{15} \\ \Lambda'_6 &= \Lambda_6 + \Lambda_9 + \Lambda_{16} \\ \Lambda'_7 &= \Lambda_7 + \Lambda_{10} + \Lambda_{17} \\ \Lambda'_{13} &= \Lambda_{13} + \Lambda_{15} + \Lambda_{21} \\ \Lambda'_{14} &= \Lambda_{14} + \Lambda_{16} + \Lambda_{22} \\ \Lambda'_{20} &= \Lambda_{20} + \Lambda_{21} + \Lambda_{26}. \end{aligned}$$

On factorise par ce sous-espace et on cherche dans le sous-espace obtenu une forme φ_0 "passant" par $G + E$.

Soit $\varphi_0 = \Lambda_{30} = Y^5Z^2$. Le diviseur sur $\widetilde{C}$ associé à φ_0 est :

$$(\varphi_0) = \operatorname{ord}_{Q_0}(\bar{\varphi}_0)Q_0 + \operatorname{ord}_{P_3}(\bar{\varphi}_0)P_3.$$

Une paramétrisation de $\widetilde{C}$ au voisinage de Q_0 est :

$$\begin{cases} x = t \\ y = t^5 + t^{10} + \cdots \end{cases}$$

d'où $\mathrm{ord}_{Q_0}(\bar{\varphi}_0) = 25$. Une paramétrisation de $\widetilde{C}$ au voisinage de P_3 est :

$$\begin{cases} x = t^3 \\ z = t^5 + t^{10} + \cdots \end{cases}$$

d'où $\mathrm{ord}_{P_3}(\bar{\varphi}_0) = 10$. On a donc $(\varphi_0) = 25\,Q_0 + 10\,P_3$. Le diviseur résiduel est $E' = 20\,Q_0 + 10\,P_3$; il est bien plus grand que le diviseur d'adjonction E (*cf.* § 4.4).

Une base de l'espace vectoriel des formes qui "passent" par E' est :

$$\begin{cases} \varphi_0 = \Lambda_{30} = Y^5 Z^2, \\ \varphi_1 = \Lambda_{26} = Y^4 Z^3, \\ \varphi_2 = \Lambda_{27} = XY^4 Z^2, \\ \varphi_3 = \Lambda_{28} = X^2 Y^4 Z. \end{cases}$$

Une base de $\mathcal{L}(G)$ est donc :

$$\left\{1,\ \bar{\varphi}_1/\bar{\varphi}_0,\ \bar{\varphi}_2/\bar{\varphi}_0,\ \bar{\varphi}_3/\bar{\varphi}_0\right\}.$$

Posons $\psi_1 = 1$; $\psi_{j+1} = \bar{\varphi}_j/\bar{\varphi}_0$, $j = 1, 2, 3$. La matrice génératrice du code est :

$$\mathcal{M} = \Big(\psi_i(P_3), \psi_i(Q_2), \ldots, \psi_i(Q_{32})\Big)_{i=1,\ldots,4}.$$

Quand on met $\mathcal{M}$ sous forme canonique :

$$\mathcal{M}' = (I_4, \overline{M})$$

on trouve un mot du code de poids 27.

La distance minimum du code est donc 27 et le code a les paramètres [32, 4, 27].

La matrice du code obtenu, mise sous forme canonique, se trouve *Figure* 1.

$$\begin{bmatrix} 15 & 0 & 0 & 0 & 15 & 8 & 6 & 10 & 4 & 10 & 9 & 8 & 11 & 11 & 15 & 3 \\ 0 & 15 & 0 & 0 & 11 & 4 & 2 & 8 & 3 & 8 & 12 & 9 & 0 & 0 & 8 & 1 \\ 0 & 0 & 15 & 0 & 9 & 11 & 8 & 10 & 11 & 11 & 7 & 6 & 12 & 0 & 6 & 8 \\ 0 & 0 & 0 & 15 & 2 & 14 & 6 & 2 & 2 & 13 & 12 & 1 & 0 & 12 & 14 & 11 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 5 & 3 & 7 & 15 & 1 & 3 & 5 & 3 & 4 & 12 & 10 & 7 & 1 & 15 & 3 \\ 14 & 10 & 6 & 13 & 7 & 9 & 2 & 12 & 2 & 6 & 3 & 5 & 1 & 8 & 2 & 4 \\ 5 & 11 & 5 & 13 & 3 & 13 & 4 & 5 & 5 & 1 & 15 & 6 & 15 & 8 & 13 & 8 \\ 3 & 11 & 4 & 9 & 4 & 2 & 11 & 11 & 7 & 6 & 10 & 6 & 14 & 4 & 14 & 12 \end{bmatrix}$$

Figure 1

Notations. — Les chiffres à l'intérieur de la matrice représentent les exposants i des α^i où α est le générateur de F_{16}.

Remarque. — 15 correspond à $\alpha^{15} = 1$. Le deuxième vecteur ligne est de poids 27.

Bien que ce code ne soit pas MDS, ses paramètres $R = k/n$, $\delta = d/n$ sont situés au-dessus de la borne de Varshamov-Gilbert d'où l'intérêt de sa construction. De plus on a le résultat suivant :

En utilisant la même courbe C, le même diviseur D et le diviseur $G = 18Q_0$ on construit, de la même façon, un code sur $\mathbb{F}_{16}$ de paramètres [32, 17, 14] (*cf.* [LB]). En concaténant ce code avec un code non-linéaire $[5, 2^5, 1]$ on peut obtenir un code binaire ayant les paramètres $[159, 2^{69}, 27]$; ce code a des paramètres meilleurs que ceux figurant dans la table de [MW–S]. Pour une démonstration de ce fait voir [D–M].

BIBLIOGRAPHIE

[A] ABYANKHAR (S.S.). — Historical ramblings in algebraic geometry and related algebra, pp. 409–448. — *Amer. Math. Monthly*, 1976.

[B] BEAUVILLE (A.). — Surfaces algébriques complexes, [Astérisque, n° **54**], *S.M.F.*, 1978.

[C] CHEVALLEY (C.). — *Introduction to the theory of algebraic functions.* — Amer. Math. Soc., 1951.

[D–M] DRIENCOURT (Y.) et MICHON (J.F.). — Rapport sur les codes, *Univ. Aix-Marseille II et CIRM-Univ. Paris 7*, Octobre 1986.

[F] FULTON (W.). — Algebraic curves, *Lectures Notes*, Benjamin, 1969.

[G1] GOPPA (V.D.). — Algebraico-Geometric Codes, *Math. USSR Izv.*, t. **21**, 1983, p. 75–91.

[G2] GOPPA (V.D.). — Codes and information, *Russian Math. Surveys*, t. **24**, 1984, p. 387–141.

[LB] LE BRIGAND (D.). — A (32, 17, 14)-code coming from a singular curve, à *paraître dans la Revue du Signal.*

[MW–S] MACWILLIAMS (F.J.) and SLOANE (N.J.A.). — *The theory of error-correcting codes.* — North-Holland, Amsterdam, 1977.

[Se] SERRE (J.P.). — *Résumé du cours de l'année* 1984–1985. — Paris, Collège de France, 1985.

[Sh] SHAFAREVICH (I.R.). — *Basic algebraic geometry.* — Springer-Verlag, 1977.

[VM] VLADUT (S.G.) et MANIN (Yu.I.). — Codes linéaires et courbes modulaires, [traduction française par DEZA (M) et LE BRIGAND (D.)], Juin 1985, *Publ. de l'Univ. P. et M. Curie*, n°**72**.

[W] WALKER (R.J.). — *Algebraic curves.* — Springer-Verlag, 1978.