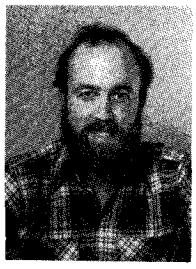
Un exemple de codes géométriques : les codes elliptiques (*)

An exemple of geometric codes: the elliptic codes



Yves DRIENCOURT

Université Aix-Marseille-II et CIRM, 70, route Léon-Lachamp, LUMINY, Case n° 916, 13288 MARSEILLE CEDEX 9.

Yves Driencourt, enseignant actuellement à l'Université de Marseille, a consacré jusqu'à présent ses recherches à la théorie analytique des nombres. Il s'intéresse par ailleurs aux connexions entre théorie du codage et géométrie algébrique suivant les idées de V. D. Goppa et Yu. I. Manin.

RÉSUMÉ

On montre explicitement, en appliquant la théorie développée par Goppa au cas des courbes de genre 1, comment construire la matrice génératrice et la matrice de contrôle d'un code elliptique sur un corps de caractéristique 2.

MOTS CLÉS

Courbe elliptique, diviseur, point rationnel, fonction rationnelle, forme différentielle, code elliptique.

SUMMARY

Following the method of V. D. Goppa, we show explicitly, in the case of genus one, how to construct the check-parity matrix and the generator matrix for an elliptic code over a field of characteristic 2.

KEY WORDS

Elliptic curve, divisor, rational point, rational function, differential form, elliptic code.

Introduction

Le but du présent article est d'expliciter la construction de codes géométriques définis par Goppa [5, 6] à partir de courbes algébriques en prenant l'exemple des courbes elliptiques.

Les codes de Goppa classiques, tels qu'ils figurent dans la littérature depuis les années 70, sont obtenus comme codes géométriques à partir de la droite projective $\mathbf{P}^1(\mathbf{F}_q)$. D'autres classes de codes bien connus, tels les codes BCH, peuvent également s'obtenir à partir de la droite [9]. Goppa lui-même donne d'autres exemples de courbes permettant de construire, entre autres, les codes de Hamming.

(*) Travail réalisé au sein de l'ATP n° 399 du CNRS (Y. Colombé, G. Lachaud, J. F. Michon). Université Paris-VII, UER de Mathématiques et Informatique, Tour 45-55, 5e étage, 2, place Jussieu, 75251 Paris Cedex 05.

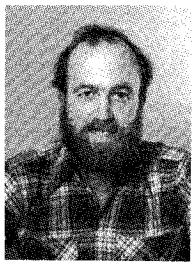
A coté de ce travail consistant à montrer comment de nombreux codes connus s'interprètent comme codes géométriques, il paraît très intéressant de mettre à jour de nouvelles classes de codes et d'étudier leurs performances. Ce dernier point a fait l'objet de nombreuses études en Union Soviétique : Manin, Vladut, Tsfasman et autres ont découvert des familles de codes ayant de très bonnes propriétés asymptotiques (i. e. dépassant la borne de Varshamov-Gilbert).

L'exposé qui suit a un but plus modeste : après avoir redonné rapidement le matériel de géométrie algébrique nécessaire, notamment le théorème de Riemann-Roch et quelques rudiments sur les courbes elliptiques, on montre comment construire la matrice génératrice ou la matrice de contrôle d'un code elliptique à partir de la donnée d'une courbe et de ses points rationnels.

Pour une introduction plus détaillée aux travaux de Goppa, on renvoie le lecteur aux exposés très complets de G. Lachaud [7] et J. F. Michon [10]. Enfin

Un exemple de codes géométriques : les codes elliptiques (*)

An exemple of geometric codes: the elliptic codes



Yves DRIENCOURT

Université Aix-Marseille-II et CIRM, 70, route Léon-Lachamp, LUMINY, Case n° 916, 13288 MARSEILLE CEDEX 9.

Yves Driencourt, enseignant actuellement à l'Université de Marseille, a consacré jusqu'à présent ses recherches à la théorie analytique des nombres. Il s'intéresse par ailleurs aux connexions entre théorie du codage et géométrie algébrique suivant les idées de V. D. Goppa et Yu. I. Manin.

RÉSUMÉ

On montre explicitement, en appliquant la théorie développée par Goppa au cas des courbes de genre 1, comment construire la matrice génératrice et la matrice de contrôle d'un code elliptique sur un corps de caractéristique 2.

MOTS CLÉS

Courbe elliptique, diviseur, point rationnel, fonction rationnelle, forme différentielle, code elliptique.

SUMMARY

Following the method of V. D. Goppa, we show explicitly, in the case of genus one, how to construct the check-parity matrix and the generator matrix for an elliptic code over a field of characteristic 2.

KEY WORDS

Elliptic curve, divisor, rational point, rational function, differential form, elliptic code.

Introduction

Le but du présent article est d'expliciter la construction de codes géométriques définis par Goppa [5, 6] à partir de courbes algébriques en prenant l'exemple des courbes elliptiques.

Les codes de Goppa classiques, tels qu'ils figurent dans la littérature depuis les années 70, sont obtenus comme codes géométriques à partir de la droite projective $\mathbf{P}^1(\mathbf{F}_q)$. D'autres classes de codes bien connus, tels les codes BCH, peuvent également s'obtenir à partir de la droite [9]. Goppa lui-même donne d'autres exemples de courbes permettant de construire, entre autres, les codes de Hamming.

(*) Travail réalisé au sein de l'ATP n° 399 du CNRS (Y. Colombé, G. Lachaud, J. F. Michon). Université Paris-VII, UER de Mathématiques et Informatique, Tour 45-55, 5e étage, 2, place Jussieu, 75251 Paris Cedex 05.

A coté de ce travail consistant à montrer comment de nombreux codes connus s'interprètent comme codes géométriques, il paraît très intéressant de mettre à jour de nouvelles classes de codes et d'étudier leurs performances. Ce dernier point a fait l'objet de nombreuses études en Union Soviétique : Manin, Vladut, Tsfasman et autres ont découvert des familles de codes ayant de très bonnes propriétés asymptotiques (i. e. dépassant la borne de Varshamov-Gilbert).

L'exposé qui suit a un but plus modeste : après avoir redonné rapidement le matériel de géométrie algébrique nécessaire, notamment le théorème de Riemann-Roch et quelques rudiments sur les courbes elliptiques, on montre comment construire la matrice génératrice ou la matrice de contrôle d'un code elliptique à partir de la donnée d'une courbe et de ses points rationnels.

Pour une introduction plus détaillée aux travaux de Goppa, on renvoie le lecteur aux exposés très complets de G. Lachaud [7] et J. F. Michon [10]. Enfin

les résultats obtenus par J. F. Michon et l'auteur, notamment sur les codes elliptiques, ont été annoncés dans une note aux *Comptes rendus* [3].

1. Courbes projectives

Soient $\mathbf{F}_q$ le corps fini à q éléments, où q est la puissance d'un nombre premier p (la caractéristique du corps $\mathbf{F}_q$) et $\bar{\mathbf{F}}_q$ sa cloture algébrique. On notera C une courbe plane projective définie sur $\mathbf{F}_q$, c'est-à-dire l'ensemble des zéros d'un polynôme homogène F (X, Y, Z) à coefficients dans $\mathbf{F}_q$. Les points de la courbe sont les racines $(a, b, c) \in (\bar{\mathbf{F}}_q)^3$ de F et on dit qu'un tel point est rationnel sur $\mathbf{F}_{q^m}$ pour $m \geqq 1$ si $(a, b, c) \in (\mathbf{F}_{q^m})^3$. Pour étudier une courbe projective, on doit fréquemment se ramener à une courbe affine en se plaçant dans l'un des trois hyperplans affines $U_i = \{(x_1, x_2, x_3)/x_i \neq 0\}$ $(i = 1, 2, 3)$ dont la réunion est $\mathbf{P}^1(\mathbf{F}_q)$. On le fait en remplaçant la coordonnée correspondante par 1 [par exemple se placer dans U_3 consiste à étudier la courbe affine d'équation $F(x, y, 1) = 0$].

La courbe C qu'on étudie est supposée irréductible, ce qui signifie que le polynôme F est irréductible sur $\bar{\mathbf{F}}_q$. Rappelons maintenant quelques définitions en les illustrant d'exemples (une bonne référence pour l'exposé systématique du matériel utilisé dans l'étude des courbes est le livre de W. Fulton : *Algebraic Curves* [4], *voir* également l'introduction de l'article de Goppa [6]). Plaçons nous dans le plan affine $z \neq 0$ et notons P le point (0,0,1) (on peut toujpurs s'y ramener par changement de variable) en supposant qu'il appartient à C. On écrit :

$$F(X, Y, 1) = F_m + F_{m+1} + \ldots + F_n$$

avec $F_m \neq 0$ et F_i homogène (en X et Y) de degré i. On appelle m la *multiplicité* de F au point P et on la note $m_p(F)$. On dit que P est un point *simple* si $m_P(F) = 1$, *multiple* (ou *singulier*) si $m_P(F) > 1$. Les tangentes en P à la courbe C sont données par l'équation $F_m = 0$. Si F possède m tangentes distinctes en P, on dit que P est un point *multiple ordinaire*.

Exemple : $zy^2 - x^3 - x^2 z = 0$. En faisant $z = 1$, on écrit $F = Y^2 - X^2 - X^3$ montrant que P est un point double dont les tangentes à C sont données par l'équation $y^2 - x^2 = 0$. C'est donc un point double ordinaire si la caractéristique est différente de 2. Pour le point $(0, 1, 0) = P^\infty$ (appelé traditionnellement le point à l'infini), on fait $y = 1$ pour changer d'hyperplan affine, d'où l'équation $z - x^2 - x^3 = 0$, montrant que P_∞ est un point simple.

Notons que chaque courbe possède tout au plus un nombre fini de points singuliers (ils sont donnés par l'annulation des trois dérivées partielles F'_X, F'_Y et F'_Z), les multiplicités m_P devant satisfaire l'inéquation

$$\sum_P m_P (m_P - 1) \leqq (n-1)(n-2)$$

si n est le degré de F. La demi-différence de ces deux nombres représente un invariant important de la courbe appelé son *genre*. C'est un entier positif ou nul que l'on note g. Sans insister davantage, disons simplement qu'il représente en quelque sorte le degré de complexité de la courbe. Dans l'exemple précédant le genre est 0 (il y a un unique point double).

On considérera dans ce qui suit une courbe C sans point singulier (courbe *non singulière* ou bien *lisse*).

Pour un point P appartenant à deux courbes distinctes $F = 0$ et $G = 0$, on définit la *multiplicité d'intersection* de F et de G au point P que l'on note $I_P(F, G)$. Sans entrer dans le détail de la définition (qui fait appel à la notion d'anneau local d'une courbe en un point) notons qu'il existe un algorithme simple permettant de calculer ce nombre à partir des équations $F = 0$ et $G = 0$ [4] et que l'on a la relation suivante

$$\sum_P I_P(F, G) = \deg(F) . \deg(G)$$

(théorème de Bezout).

On note $\mathbf{F}_q(C)$ le corps des fonctions rationnelles sur la courbe C (ce sont, à équivalence près modulo l'équation de C, les quotients de polynômes homogènes de même degré, à coefficients dans $\mathbf{F}_q$, le dénominateur ne s'annulant pas au point où on l'exprime) et $\Omega_{\mathbf{F}_q}(C)$ l'espace vectoriel des formes différentielles définies sur $\mathbf{F}_q$. Rappelons que, considéré comme espace vectoriel sur $\mathbf{F}_q(C)$, il est de dimension 1. En notant ω_0 la forme de base, on écrit donc toute forme différentielle $\omega = f\,\omega_0$ pour une certaine fonction rationnelle f.

2. Le théorème de Riemann-Roch

Un *diviseur* sur C est une combinaison linéaire formelle à cœfficients dans $\mathbf{Z}$ (presque tous nuls) des points de C. Soit $D = \sum_P n_P P$ un diviseur. On définit le degré de D par $\deg(D) = \sum_P n_P$ et on dit que D est *positif* (ou bien *effectif*) si $n_P \geqq 0$ pour tout P, d'où une relation d'ordre sur les diviseurs.

Si Φ est une courbe plane ne contenant pas C comme composante, on définit le diviseur de Φ noté $\mathrm{div}(\Phi)$ comme étant $\sum_{P \in C} I_P(\Phi, C).P$. $\mathrm{Div}(\Phi)$ est donc de degré égal au produit des degrés des courbes Φ et C par le théorème de Bezout. On peut définir le diviseur d'une fonction rationnelle f en posant

$$\mathrm{div}(f) = \mathrm{div}(\Phi) - \mathrm{div}(\Psi) \text{ si } f = \Phi/\Psi$$

quotient de deux polynômes homogènes de même degré. On constate ainsi que le degré du diviseur d'une fonction rationnelle est nul. Il existe une autre définition équivalente du diviseur de f, c'est

$$\mathrm{div}(f) = \sum_{P \in C} v_P(f) . P$$

où $v_P(f)$ est l'ordre de la fonction f au point P : en tout point P de la courbe, on peut en effet donner un développement de f suivant un paramètre local t, du type

$$f = \sum_{n \geqq n_0} a_n t^n, \qquad a_{n_0} \neq 0$$

et on pose $n_0 = v_P(f)$. Si $n_0 > 0$ (resp. $n_0 < 0$) on dit que P est un zéro (resp. un pôle) de f. Le résultat précédent ($\deg(\mathrm{div}(f)) = 0$) s'interprête en disant que si on les compte avec leur multiplicité, f possède autant de zéros que de pôles.

A partir de l'écriture $\omega = f dg$ où f et g sont des fonctions rationnelles, on écrit le développement de ω suivant un paramètre local t au point P à partir de ceux de f et g en dérivant formellement celui de g et en effectuant le produit :

$$\omega = \left(\sum_{n \geqq n_0} a_n t^n \right) dt, \qquad a_{n_0} \neq 0.$$

On pose $n_0 = v_p(\omega)$ et on définit le *diviseur de* ω par la formule

$$\mathrm{div}(\omega) = \sum_{P \in C} v_P(\omega) . P$$

On définit également le *résidu* $\mathrm{Res}_P(\omega) = a_{-1}$ en montrant qu'il ne dépend pas du choix de l'uniformisante locale t et on a le résultat suivant :

Théorème (des « résidus ») : *Pour toute*

$$\omega \in \Omega_{\mathbf{F}_q}(C) : \sum_{P \in C} \mathrm{Res}_P(\omega) = 0.$$

Deux diviseurs D et D' sont dits *équivalents* si $D' = D + \mathrm{div}(f)$ avec $f \in \mathbf{F}_q(C)$. Puisque $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$, les diviseurs de fonctions rationnelles forment un sous-groupe du groupe des diviseurs de degré 0 sur C. En particulier les diviseurs de formes différentielles sont équivalents et forment une unique classe appelée *classe canonique.* Ils ont donc tous le même degré. On appelle *diviseur canonique* un représentant $K = \mathrm{div}(\omega_0)$ de cette classe.

Pour un diviseur quelconque D, on définit les $\mathbf{F}_q$-espaces vectoriels :

$$L(D) = \{ f \in \mathbf{F}_q(C) / \mathrm{div}(f) \geqq -D \}$$
$$\Omega(D) = \{ \omega \in \Omega_{\mathbf{F}_q}(C) / \mathrm{div}(\omega) \geqq D \}.$$

On montre qu'ils sont de dimension finie et le *théorème de Riemann-Roch* donne une relation entre les dimensions de ces espaces :

$$\dim L(D) - \dim \Omega(D) = \deg(D) + 1 - g$$

où g est le genre de la courbe C. Notons qu'en écrivant $\omega = f \omega_0$, $f \in \mathbf{F}_q(C)$, on a :

$$\mathrm{div}(\omega) \geqq D \iff \mathrm{div}(f) \geqq D - \mathrm{div}(\omega_0)$$

d'où un isomorphisme de $\Omega(D)$ sur $L(K-D)$ (dépendant évidemment du choix de ω_0) permettant d'écrire le théorème de Riemann-Roch sous la forme :

$$\dim L(D) - \dim L(K-D) = \deg(D) + 1 - g.$$

Les corollaires suivants du théorème de Riemann-Roch sont importants :

(i) $\dim \Omega(0) = g$;
(ii) $\deg(D) < 0 \Rightarrow \dim \Omega(D) = g - 1 - \deg(D)$;
(iii) $\deg(K) = 2g - 2$
(iv) $\deg(D) > 2g - 2 \Rightarrow \Omega(D) = \{0\}$.

(i) provient du fait que seules les fonctions constantes sont de diviseur $\geqq 0$, (ii) du fait qu'il n'y a pas de fonction rationnelle de diviseur strictement positif (s'il y a des zéros, il y a automatiquement des pôles). (iii) s'obtient en faisant $D = K$ puisque $L(0)$ est de dimension 1 et $L(K) \simeq \Omega(0)$ de dimension g, enfin (iv) en observant que dans ces conditions $\deg(K-D) < 0$ et donc $L(K-D) \simeq \Omega(D) = \{0\}$.

3. La construction des codes géométriques (Goppa)

Soit (D, G) un couple de diviseurs définis sur $\mathbf{F}_q$ vérifiant :

(*a*) $D = P_1 + \ldots + P_n$ où les P_i sont des points rationnels sur $\mathbf{F}_q$, tous distincts.

(*b*) G est positif et globalement rationnel.

(*c*) Les supports de D et G sont disjoints.

On considère, pour $2g - 2 < \deg(G) \leqq n + 2g - 2$, le code C_Ω de longueur n, image de l'application

$$\varphi_\Omega : \quad \Omega(G-D) \to \mathbf{F}_q^n$$

telle que

$$\varphi_\Omega(\omega) = (\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega))$$

et pour $0 \leqq \deg(G) < n$, le code C_L, de longueur n également, image de l'application

$$\varphi_L : \quad L(G) \to \mathbf{F}_q^n$$

telle que

$$\varphi_L(f) = (f(P_1), \ldots, f(P_n)).$$

Théorème (Goppa) : *Dans les conditions indiquées, le code* C_Ω *est de dimension* $\geqq n - \deg(G) - 1 + g$ [*resp.* C_L *de dimension* $\geqq \deg(G) - 1 + g$] *et de distance minimale* $d \geqq \deg(G) - 2g + 2$ [*resp.* $\geqq n - \deg(G)$]. *De plus si* $2g - 2 < \deg(G) < n$, *on a :*

★ $\dim C_\Omega = n - \deg(G) - 1 + g$;
★ $\dim C_L = \deg(G) + 1 - g$;
★ $C_L = C_\Omega^\perp$.

Prouvons les assertions concernant l'espace $\Omega(G-D)$ [on procède de même pour $L(G)$]. La condition $\deg(G) \leqq n + 2g - 2$ assure que le code C_Ω n'est pas réduit à $\{0\}$ (*cf.* les conditions de non-nullité des espaces Ω). On calcule $\mathrm{Ker}\, \varphi_\Omega = \Omega(G) = \{0\}$ si $\deg(G) > 2g - 2$, donc $\Omega(G-D) \simeq C_\Omega$. On obtient alors la dimension par le théorème de Riemann-Roch et ses corollaires :

$$\dim \Omega(G-D) = n - \deg(G) - 1 + g + \dim L(G-D)$$

par suite si $\deg(G) < n$, on a $L(G-D) = \{0\}$ et

$$\dim \Omega(G-D) = n - \deg(G) - 1 + g,$$

si on a que $n \leqq \deg(G) \leqq n + 2g - 2$, on peut seulement conclure que

$$\dim \Omega(G-D) \geqq n - \deg(G) - 1 + g.$$

Pour ce qui concerne la distance minimale, soit $\omega \in \Omega(G-D)$ telle que $\varphi_\Omega(\omega)$ soit de poids $d.\omega$ a donc des résidus non nuls en d points

$$P_{i_1}, \ldots, P_{i_d} \in \{P_1, \ldots, P_n\}$$

donc

$$\operatorname{div}(\omega) \geqq G - \{P_{i_1} + \ldots + P_{i_n}\}$$

et en prenant les degrés : $2g-2 \geqq \deg(G) - d$.

Enfin pour ce qui est de l'orthogonalité, on a, pour $2g-2 < \deg(G) < n$, l'égalité pour les dimensions, ce qui fait que $\dim C_\Omega + \dim C_L = n$. Par ailleurs

$$(\varphi_L(f) \mid \varphi_\Omega(\omega)) = \sum_{i=1}^{n} f(P_i)\, \operatorname{Res}^{P_i}(\omega) = \sum_{i=1}^{n} \operatorname{Res}^{P_i}(f\omega) = 0$$

par le théorème des résidus car $f\omega \in \Omega(-D)$ et donc n'a de pôles éventuels qu'aux points P_i. Donc $C_L \subset C_\Omega^\perp$ et on a l'égalité à cause des dimensions.

4. Séries linéaires

Nous allons maintenant montrer comment cette notion conduit à une base de l'espace $L(D)$ pour un diviseur positif D. Partons d'abord d'un diviseur quelconque D et d'un sous-espace vectoriel V de $L(D)$. On appelle *série linéaire* l'ensemble des diviseurs positifs de la forme $\operatorname{div}(f)+D$, où $f \in L(D)$. Si $V = L(D)$, on dit que la série est complète (elle contient tout diviseur positif équivalent à D). On la note $|D|$. Soit $(f_0, \ldots, f_r)$ une base de V. L'application

$$\operatorname{div}(\sum \lambda_i f_i) + D \mapsto (\lambda_0, \ldots, \lambda_r)$$

est une bijection de la série linéaire sur l'espace projectif $\mathbf{P}^r$ [en effet deux fonctions f et g définissent le même diviseur si et seulement si $f = \lambda g$ avec $\lambda \in k^*$, puisque $L(0)$ est de dimension 1]. On peut donc munir la série linéaire d'une structure d'espace projectif dont la dimension est celle de V diminuée de 1. En particulier on a :

$$\dim L(D) = \dim |D| + 1.$$

Soient D et D′ deux diviseurs positifs équivalents : il existe donc une fonction rationnelle f telle que $D = D' + \operatorname{div}(f)$. Supposons qu'il existe une courbe Φ de degré m passant par D. On a donc $\operatorname{div}(\Phi) = D + A$ avec A positif. On veut montrer qu'il existe alors une courbe Ψ de degré m telle que $\operatorname{div}(\Psi) = D' + A$. Pour cela, il suffit de voir qu'on peut écrire f sous la forme Φ/Ψ pour un certain polynôme homogène Ψ, nécessairement de même degré que Φ : en effet, on aura alors $D = D' + \operatorname{div}(\Phi) - \operatorname{div}(\Psi)$ d'où $\operatorname{div}(\Psi) = D' + A$. En écrivant $f = g/h$, on cherche donc Ψ telle que $g\Psi - h\Phi \equiv 0 \bmod F$ ($F = 0$ étant l'équation de C), i.e. étant données g, h et Φ, on cherche des courbes Ψ et R telles que $h\Phi = g\Psi + RF$. Mais ceci est une conséquence du théorème de Noether sur les courbes [4]. Il en résulte que $|D|$ est l'ensemble des diviseurs positifs D′ tels que $D' + A = \operatorname{div}(\Psi)$ où Ψ est une courbe de degré m. Dans ces conditions, on a fabriqué des fonctions de $L(D)$ puisque

$$\operatorname{div}(\Psi/\Phi) = D' - D \geqq -D$$

donc $\Psi/\Phi \in L(D)$. On connaît par ailleurs la dimension r de $L(D)$ par le théorème de Riemann-Roch. Pour trouver une base de $L(D)$, il suffit donc d'exhiber $r-1$ courbes de degré m $\Psi_1, \ldots, \Psi_{r-1}$ passant par A telles que les fonctions

$$1, \quad \Psi_1/\Phi, \quad \ldots, \quad \Psi_{r-1}/\Phi$$

soient linéairement indépendantes.

5. Courbes elliptiques

Soit C une courbe projective non singulière de genre 1 possédant un point rationnel P sur $\mathbf{F}_q$. Alors C est isomorphe à une cubique plane d'équation :

$$(1) \quad \begin{cases} y^2 z + a_1 xyz + a_3 yz^2 \\ \qquad = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3, \\ a_i \in \mathbf{F}_q \end{cases}$$

Ceci provient du théorème de Riemann-Roch : en effet on calcule

$$\dim L(nP) = \deg(nP) - g + 1 = n$$

pour tout entier $n > 0$. Il en résulte qu'il existe une fonction rationnelle x possédant un unique pôle d'ordre deux exactement en P et une fonction y possédant un unique pôle d'ordre trois exactement en P. Il y a donc sept fonctions dans $L(6P)$ à savoir : 1, x, x^2, x_3, xy, y et y^2, il s'ensuit qu'il doit y avoir une relation de dépendance entre elles...

Notons qu'il n'y a qu'un seul point à l'infini sur la courbe : (0, 1, 0) noté P_∞ et qu'il est facile de voir que c'est le point P utilisé. En effet on détermine

$$C \cap \{x = 0\} = \{P_\infty, P_1, P_2\}$$

[P_1 et P_2 étant les points $(0, \alpha, 1)$ et $(0, \beta, 1)$ où α et β sont les racines de $y^2 + a_3 y = a_6$] et

$$C \cap \{z = 0\} = \{P_\infty\}$$

ce qui permet d'écrire

$$\operatorname{div}\left(\frac{x}{z}\right) = P_\infty + P_1 + P_2 - 3P_\infty = P_1 + P_2 - 2P_\infty.$$

De même on obtiendrait

$$\operatorname{div}\left(\frac{y}{z}\right) = P_1' + P_2' + P_3' - 3P_\infty$$

où P_i' est le point $(\alpha_i, 0, 1)$, α_i solution de $x^3 + a_2 x^2 + a_4 x + a_6 = 0$.

On a montré au passage — nous l'utiliserons par la suite — que :

$$(2) \quad \begin{cases} I_{P_\infty}(x, F) = 1 \\ I_{P_\infty}(y, F) = 0 \\ I_{P_\infty}(z, F) = 3 \end{cases}$$

où $F(x, y, z) = 0$ désigne l'équation (1).

Réciproquement une cubique d'équation (1) représente une courbe de genre 1 si et seulement si elle est non singulière. On peut montrer que ceci équivaut au fait que $\Delta \neq 0$ (où Δ est un certain polynôme en $a_1, \ldots, a_6$ appelé le discriminant). Pour un exposé plus détaillé de ces questions et une classification des courbes elliptiques définies sur $\mathbf{F}_2$, *voir* [2]. Nous nous contenterons ici de traiter le cas d'une courbe elliptique d'équation

$$y^2 + y = u(x)$$

où $u(X)$ est un polynôme unitaire de degré 3 de $\mathbf{F}_2[X]$. On peut vérifier facilement qu'une telle courbe possède 1, 3 ou 5 points rationnels sur $\mathbf{F}_2$ suivant $u(X)$. On est donc naturellement conduit à étudier les points rationnels sur $\mathbf{F}_q$ où $q = 2^m$ pour en avoir un nombre plus important. Un fait remarquable est qu'on peut prévoir à l'avance, sans les déterminer explicitement, le nombre de points rationnels sur $\mathbf{F}_{q^m}$ si on en connaît le nombre sur $\mathbf{F}_q$ (q étant ici un entier quelconque) à l'aide de la fonction zêta de la courbe C [2]. Ceci est important pour nous dans la mesure où le nombre de points rationnels sur $\mathbf{F}_{q^m}$ détermine la longueur maximale du code sur $\mathbf{F}_{q^m}$. Pour ce qui concerne $\mathbf{F}_2$, on peut facilement obtenir le tableau suivant :

Nombre de points rationnels sur $\mathbf{F}_{2^r}$ pour

$r=1$	$r=2$	$r=3$	$r=4$	$r=5$
1	5	13	25	41
3	9	9	9	33
5	5	5	25	25

6. L'algorithme de codage pour $g=1$

Il est donné explicitement dans [5] et pour $g=1$ il se présente sous la forme simplifiée que voici :

(1) Donnée d'une cubique non singulière définie sur $\mathbf{F}_q$ ($q=2^m$) par son équation sous la forme (1) (pour simplifier les calculs nous nous limiterons dans ce qui suit à une courbe définie sur $\mathbf{F}_2$).

(2) Recherche des points rationnels par inspection.

On pose $D = P_1 + \ldots + P_n$ où les P_i sont les points rationnels utilisés pour construire le code (ils ne figurent pas nécessairement tous).

(3) Donnée d'un diviseur positif G rationnel sur $\mathbf{F}_q$ et tel que les supports de D et G soient disjoints.

(4) Donnée d'une courbe φ_0 de degré l passant par G [l'entier l dépendant de deg(G)].

(5) Calcul de $\mathrm{div}(\varphi_0) = G + H$.

(6) Recherche de $r-1$ ($r = \deg(G)$) courbes de degré l passant par H $\varphi_1, \ldots, \varphi_{r-1}$ telles que les fonctions $1, \varphi_1/\varphi_0, \ldots, \varphi_{r-1}/\varphi_0$ soient indépendantes [en effet on sait par le théorème de Riemann-Roch que $\dim L(G) = \deg(G) - g + 1 = r$].

(7) On écrit la matrice de contrôle du code en mettant en i-ième colonne les $\varphi_j(P_i)/\varphi_0(P_i)$ pour $j = 0, 1, \ldots, r-1$.

7. Exemple de code elliptique

On pose $G = dP_\infty$ où $P_\infty = (0, 1, 0)$ et on prend pour support de D l'ensemble des points rationnels sur $\mathbf{F}_q$ à part P_∞. On choisit pour φ_0 la fonction z^δ où $\delta = [d/2]$. Il nous faut donc trouver $d-1$ courbes $\varphi_1, \ldots, \varphi_{d-1}$ de degré δ passant par $(3\delta - d)P_\infty$ telles que les fonctions $\psi_i = \varphi_i/\varphi_0$ et la fonction constante soient indépendantes. Il suffit de considérer les courbes

$$xz^{\delta-1}, \quad x^2 z^{\delta-2}, \quad \ldots, \quad x^\delta$$
$$yz^{\delta-1}, \quad yxz^{\delta-2}, \quad \ldots, \quad yx^{\delta'} z^{\delta-\delta'-1}$$

où l'on a posé $\delta' = [(d-3)/2]$. En effet ces courbes vérifient bien les conditions imposées et si on écrit

$$\lambda_0 + \sum_{i=1}^{d-1} \lambda_i \psi_i = 0 \qquad (\lambda_i \in \mathbf{F}_q)$$

on est conduit, en repassant aux φ_i, à une congruence modulo l'équation de la courbe, qui est en fait une égalité car $\sum \lambda_i \varphi_i$ ne contient pas y^2. Vue la définition des φ_i, on obtient donc visiblement $\lambda_i = 0$ pour tout i.

En notant $P_i = (\alpha_i, \beta_i, 1)$ et $\bar{P}_i = (\alpha_i, \gamma_i, 1)$ où $\gamma_i = \beta_i + 1$ les points de même abscisse sur la courbe C, on obtient la matrice de contrôle du code C_Ω sous la forme suivante

$$\begin{bmatrix} 1 & \ldots & 1 & 1 & \ldots \\ \alpha_1 & \ldots & \alpha_i & \alpha_i & \ldots \\ \vdots & & \vdots & \vdots & \\ \alpha_1^\delta & \ldots & \alpha_i^\delta & \alpha_i^\delta & \ldots \\ \beta_1 & \ldots & \beta_i & \gamma_i & \ldots \\ \beta_1 \alpha_1 & \ldots & \beta_i \alpha_i & \gamma_i \alpha_i & \ldots \\ \vdots & & \vdots & \vdots & \\ \beta_1 \alpha_1^{\delta'} & \ldots & \beta_i \alpha_i^{\delta'} & \gamma_i \alpha_i^{\delta'} & \ldots \end{bmatrix}$$

D'un autre côté si l'on veut traiter l'optique formes différentielles, on est conduit à rechercher une base de $\Omega(G-D)$ permettant de construire la base du code C_Ω. On commence par remarquer que $\mathrm{div}(\omega_0) = 0$ si ω_0 désigne la base de $\Omega(0)$ [en effet $\dim \Omega(0) = 1$ et $\deg(\mathrm{div}(\omega_0)) = 0$ d'après les corollaires du théorème de Riemann-Roch] et qu'on peut prendre $\omega_0 = dx$. Il s'ensuit que $\Omega(G-D)$ est isomorphe à $L(D-G)$ dont il suffit de construire une base. On ne peut plus procéder comme ci-dessus à l'aide des séries linéaires puisque le diviseur $D-G$ n'est pas positif. Cependant il existe un algorithme, dû à Coates, permettant cette construction. Il suffit de l'adapter au cas d'un corps de caractéristique >0, ce qui est exposé en détail dans [2]. Toutefois le cas que nous avons à traiter ne présente pas de grande difficulté et peut se résoudre à la main. Reprenons les notations ci-dessus, appelons A l'ensemble des abscisses des points rationnels et a son cardinal. On peut donc écrire

$$D = \sum_{i=1}^{a} (P_i + \bar{P}_i)$$

$$\mathrm{div}\,(x + \alpha_i z) = P_i + \bar{P}_i + P_\infty.$$

En posant

$$f(X, Z)=\prod_{\alpha\in A}(X+\alpha Z)$$

on a div $(f)=D+aP_\infty$. On cherche donc des éléments de $L(D-G)$ en prenant f comme dénominateur et en s'arrageant, au vu des égalités (2), pour que le numérateur ait un diviseur $\geqq(d+a)P_\infty$, tout en étant de degré a et en faisant en sorte que les fonctions obtenues soient linéairement indépendantes. On obtient ainsi les fonctions

$$\frac{z^a}{f},\ \frac{xz^{a-1}}{f},\ \ldots,\ \frac{x^{a-\delta'-2}z^{\delta'+2}}{f}$$
$$\frac{yz^{a-1}}{f},\ \frac{yxz^{a-2}}{f},\ \ldots,\ \frac{yx^{a-\delta-2}z^{\delta+1}}{f}.$$

qui forment bien une base de $L(D-G)$ pour des raisons analogues à celles exposées plus haut. En multipliant par dx, on a finalement obtenu une base de $\Omega(G-D)$. Il nous reste à calculer les résidus de ces formes différentielles. Pour cela il nous faut obtenir le développement de ω suivant un paramètre local au voisinage du point $P=(\alpha, y(\alpha), 1)$ [rappelons que pour α donné $y(\alpha)$ peut prendre deux valeurs distinctes]. Il est facile de voir qu'on peut prendre $x+\alpha$ comme uniformisante et que

$$y=y(\alpha)+*(x+\alpha)+\ldots$$

au voisinage de P. Il en résulte que l'on a

$$\mathrm{Res}_P\left(\frac{x^\lambda}{f}dx\right)=\frac{\alpha^\lambda}{f'(\alpha)}$$

et

$$\mathrm{Res}_P\left(y\frac{x^\mu}{f}d^x\right)=\frac{\alpha^\mu y(\alpha)}{f'(\alpha)}$$

où

$$f'(\alpha)=\prod_{\substack{\alpha'\in A\\ \alpha'\neq\alpha}}(\alpha+\alpha').$$

On peut maintenant écrire la matrice génératrice du code C_Ω, en reprenant les mêmes notations que ci-dessus :

$$\begin{bmatrix} 1 & \ldots & 1 & 1 & \ldots \\ \alpha_1 & \ldots & \alpha_i & \alpha_i & \ldots \\ \vdots & & \vdots & \vdots & \\ \alpha_1^{a-\delta'-2} & \ldots & \alpha_i^{a-\delta'-2} & \alpha_i^{a-\delta'-2} & \ldots \\ \beta_1 & \ldots & \beta_i & \gamma_i & \ldots \\ \beta_1\alpha_1 & \ldots & \beta_i\alpha_i & \gamma_{i\alpha i} & \ldots \\ \vdots & & \vdots & \vdots & \\ \beta_1\alpha_1^{a-\delta-2} & \ldots & \beta_i\alpha_i^{a-\delta-2} & \gamma_i\alpha_i^{a-\delta-2} & \ldots \end{bmatrix}$$
$$\times\begin{bmatrix} f'(\alpha_1)^{-1} & & & & \\ & \ddots & & & \\ & & f'(\alpha_i)^{-1} & & \\ & & & f'(\alpha_i)^{-1} & \\ & & & & \ddots \end{bmatrix}$$

En résumé, le code C_Ω qu'on a obtenu à partir d'une courbe elliptique définie sur $\mathbf{F}_2$ d'équation

$$y^2+y=u(x)$$

possédant $2a+1$ points rationnels sur $\mathbf{F}_q$ $(q=2^m)$ dont $P_\infty=(0, 1, 0)$, en prenant comme diviseurs $G=dP_\infty$ et $D=\sum_{i\neq\infty}P_i$ a pour paramètres :

$$\begin{cases} n=2a \\ k=2a-d \\ \text{dist. min.}\geqq d. \end{cases}$$

En raison de la borne de Singleton, la distance minimale est soit d, soit $d+1$ auquel cas le code est MDS. Notons par ailleurs que le fait de pouvoir construire indépendamment la matrice de contrôle et la matrice génératrice donne une condition simple permettant de construire des codes elliptiques autoduaux, et que des transformations simples opérées sur la matrice de contrôle conduisent à une méthode permettant de corriger environ $d/4$ erreurs [1].

Conclusion

Nous nous sommes efforcés dans cet article de présenter la construction d'un nouveau code géométrique, le plus simple possible, pour rendre cette notion accessible aux spécialistes du codage non familiers avec les outils mathématiques employés ici. De plus amples développements pourront être trouvés dans les articles cités en référence.

La réalisation pratique (i. e. logicielle) des codes elliptiques présentés ci-dessus a été réalisée avec l'aide de J. F. Michon. Elle se présente sous forme d'un programme (écrit en Pascal et Assembleur) et tournant sur micro-ordinateur IBM-PC ou compatible permettant de générer automatiquement des codes elliptiques : il comporte un classement des courbes à isomorphisme près sur $\mathbf{F}_{2^m}$ $(m\leqq 5)$, puis toute une procédure interactive permettant le choix d'une courbe, l'étude éventuelle de son groupe de points rationnels, le choix des points sur la courbe pour réaliser un code, etc.

Cette théorie toute nouvelle des codes géométriques a d'ores et déjà permis d'obtenir des résultats extrêmement intéressants, la plupart d'entre eux devant être attribués aux mathématiciens soviétiques :

- la construction de nouvelles familles de codes dépassant la borne de Varshamov-Gilbert (Tsfasman, Vladut et Zink);
- la mise au point de codes binaires permettant d'améliorer les tables de [8] à l'aide de courbes algébriques de genre 1, 2 et 3 (Barg, Katsman et Tsfasman). En particulier, l'un des exemples fournis par les auteurs utilise un code elliptique sur $\mathbf{F}_{16}$, que l'on peut construire facilement à l'aide des résultats indiqués ci-dessus;
- l'étude de la complexité algorithmique de construction de codes dépassant la borne de Varshamov-Gilbert (Vladut);

• la construction d'empilements de sphères très denses de $\mathbf{R}_N$ (Litsyn et Tsfasman).

Cette liste de résultats, non exhaustive, suffirait largement à souligner l'apport positif de la nouvelle vision de la théorie de l'information proposée par Goppa. Mais en fait l'apport d'une perspective géométrique (au sens Géométrie Algébrique) nous semble plus profond que le moyen de fabriquer de nouveaux codes. Elle fournit des outils pour travailler sur des problèmes de nature « digitale » et montre, si cela est encore nécessaire, le caractère imprévisible des applications des mathématiques. Les outils sous-jacents à l'étude des codes géométriques sont extrêmement sophistiqués, ne pouvant être maîtrisés que par des chercheurs spécialisés ayant acquis une longue formation. Aucune application de ce type de mathématique n'était soupçonnée. Le bilan de notre expérience sur le codage nous porte à croire que ces outils, loin d'être d'emploi limité, sont en fait d'une extraordinaire généralité car ils substituent (de façon formellement analogique, il ne s'agit pas de simulation !) à des raisonnements faits sur des objets « continus » des techniques discrètes et montrent comment énoncer les lois qui gouvernent le comportement d'objets binaires.

Que ce soit en

– théorie de l'information, entropie, codages divers;

– transformation de Fourier et ses analogiques binaires;

– cryptographie « mathématique »;

– calcul rapide et architectures;

– optique intégrée;

– reconnaissance de formes,

et par conséquent dans tous les domaines utilisateurs de ces concepts, il nous semble utile de développer cette attitude de recherche de structures mathématiques « transposables ».

Manuscrit reçu en janvier 1986

BIBLIOGRAPHIE

[1] Y. Driencourt, *Some properties of elliptic codes over a field of characteristic* 2, dans *Algebraic Algorithms and Error-Correcting Codes; Proc. 3rd Int. Conf.*, AAECC-3, Grenoble, 1985; *Lect. Notes in Comp. Sc.*, n° 229.

[2] Y. Driencourt et J. F. Michon, Elliptic codes over a field of characteristic 2, *J. of Pure and Applied Algebra* (à paraître).

[3] Y. Driencourt et J. F. Michon, Remarques sur les codes géométriques, *C.R. Acad. Sc.*, 301, 1985, p. 15-17.

[4] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.

[5] V. D. Goppa, Algebraico-Geometric Codes, *Izv. Akad. Nauk, S.S.S.R.*, 46, 1982 = *Math. U.S.S.R. Izvestia*, 21, 1983, p. 75-91.

[6] V. D. Goppa, Codes and Information, *Uspekhi Math. Nauk*, 39, n° 1, 1984, p. 77-120= *Russ. Math. Surveys*, 39, n° 1, 1984, p. 87-141.

[7] G. Lachaud, Les codes géométriques de Goppa, *Séminaire Bourbaki*, n° 641, fév. 1985.

[8] F. J. Macwilliams et N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[9] J. F. Michon, *Les codes BCH comme codes géométriques*, preprint.

[10] J. F. Michon, Codes de Goppa, *Sém. Th. Nombres*, Bordeaux, 1983-1984, exp. n° 7.