# Géométrie algébrique en théorie de l'information : cryptographie et codes correcteurs.

Présentation du domaine de recherche.

Ivan Boyer
Sous la direction de Jean-François Mestre.

20 octobre 2009

## Table des matières



Dans notre société de communication, deux problématiques majeures apparaissent au moment d'échanger des informations : la confidentialité d'une part et l'exactitude d'autre part. Il est intéressant de noter que la géométrie algébrique y trouve une place de plus en plus importante, notamment dans la possibilité de trouver des courbes ayant beaucoup de points rationnels.

On présente d'une part la cryptographie à clé publique basée sur des courbes elliptiques. La taille des clés et la rapidité sont supérieures à celle du système Rsa mais encore trop jeune pour bénéficier de la même confiance. On verra notamment l'algorithme de Schoof et des améliorations pratiques.

D'autre part, on expliquera l'intérêt de courbes algébriques ayant beaucoup de points rationnels dans l'utilisation de codes correcteurs. On présentera quelques bornes d'efficacité à notre disposition, notamment la borne Tvz . On verra enfin ce que l'on sait du nombre maximum de points rationnels sur une courbe lorsque l'on fixe son genre (par exemple les courbes elliptiques et la borne de Hasse-Weil en genre 1).

## 1 Compter les points rationnels d'une courbe elliptique.

### 1.1 Cryptographie à clé publique.

En 1985, N. Koblitz et V. Miller proposèrent indépendamment d'utiliser des courbes elliptiques dans des procédés cryptographiques à clé publique. Leurs techniques reposent sur la notion de fonction à sens unique :

**Définition 1.1** (Fonction à sens unique)**.** *Soit $f : \Sigma \to \Sigma'$ une fonction. On dit qu'elle est à* sens unique *si*

*(i) Pour $x \in \Sigma$, $f(x)$ peut être calculé en temps polynomial.*

*(ii) Il n'y a pas d'algorithme polynomial tel, qu'étant donné $y \in \Sigma'$, il décide si $y \notin \mathrm{im}(f)$ et donne dans le cas contraire un $x \in \Sigma$ tel que $f(x) = y$.*

Le procédé d'échange de clés de Diffie et Hellman repose sur une fonction dont on espère qu'elle est à sens unique[†] : Alice et Bob commencent par décider d'un groupe $(G, \oplus)$ et d'un élément $P \in G$. Ensuite, ils choisissent chacun de leur côté des entiers $e_A$ et $e_B$ puis rendent publiques les quantités $[e_A]P$ et $[e_B]P$.

†. On ne sait pas le prouver ; on aurait alors **P≠NP** !

Ensuite, tous deux peuvent calculer la quantité $[e_A e_B]P$ qui sera leur clé commune permettant d'utiliser des techniques cryptographiques symétriques. Comme ce procédé ne dépend que du sous-groupe engendré par $P$, on peut choisir en fait $G = \langle P \rangle$ cyclique. La sécurité de ce système repose sur :

**Définition 1.2** (Problème du Logarithme Discret, DLP [†]). *Soit $G = \langle b \rangle$ un groupe cyclique d'ordre [‡] $n$. On appelle* logarithme discret *la fonction*

$$\begin{aligned} \log_b : G &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ b^k &\longmapsto k \mod n \ . \end{aligned}$$

## 1.2 Courbes elliptiques : loi de groupe.

Afin de mettre en place ces idées, il nous faut trouver un groupe où l'on sache calculer facilement sans que le DLP soit facile. Pour cela, on considère une courbe elliptique $E$ définie sur un corps $\mathbb{F}_q$ dont on notera $p$ la caractéristique. Pour simplifier, on supposera $p \neq 2, 3$ de sorte que l'on puisse écrire une équation de $E$ sous la forme $y^2 = x^3 + ax + b$, avec $\Delta = 4a^3 - 27b^2 \neq 0$ (la courbe est lisse).

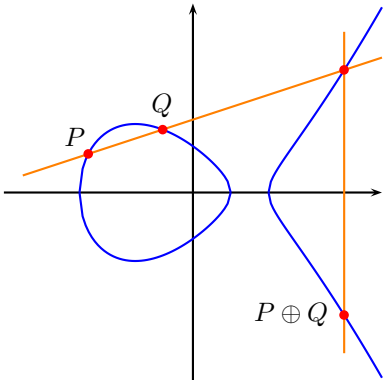



FIGURE 1: Loi de groupe sur une courbe elliptique.

**Proposition 1.3** (Formules d'addition). *Soient $(x_1, y_1)$ et $(x_2, y_2)$ deux points de $E$ distincts de $\mathcal{O}$ (le point à l'infini), non opposés l'un de l'autre. La loi d'addition par cordes et tangentes, illustrée ci-contre, est donnée algébriquement par les formules :*

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad \text{où } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } x_1 \neq x_2, \\ \dfrac{3x_1 + a}{2y_1} & \text{sinon.} \end{cases}$$

Grâce à ces formules on peut calculer rapidement dans ce groupe abélien : on peut notamment calculer la multiplication par $m \in \mathbb{N}$ (notée dans dans ce contexte $[m]$) par exponentiation rapide.

Afin de ne pas faciliter la résolution du DLP, il faut pouvoir trouver une courbe dont le groupe a un cardinal possédant un très grand facteur premier. Pour cela, il nous faut calculer ce cardinal efficacement. Il existe des méthodes élémentaires ; on peut par exemple citer la formule :

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + ax + b}{q} \right).$$

Le problème est que la complexité de cette méthode est bien trop élevée [¶]. Le point de départ des algorithmes $l$–adiques vient de la propriété cruciale que le nombre de points d'une courbe elliptique peut être encadré :

**Théorème 1.4** (Borne de Hasse). *On a l'encadrement :*

$$\big| |E(\mathbb{F}_q)| - (q+1) \big| \leqslant 2\sqrt{q}.$$

L'idée fondamentale est alors de déterminer ce cardinal modulo des petits nombres premiers puis de le retrouver avec le théorème des restes chinois. Une application élémentaire du théorème des nombres premiers nous dit qu'il suffit de savoir le faire pour $O(\log q)$ nombres premiers de taille $O(\log q)$. Ainsi, la recherche d'un algorithme polynomial pour trouver $|E(\mathbb{F}_q)|$ se réduit à en trouver un qui calcule $|E(\mathbb{F}_q)| \mod l$ pour un nombre premier $l$ de taille de l'ordre de $\log q$.

## 1.3 Outils algébriques et algorithme de Schoof.

Avant d'exposer les principales idées de l'algorithme de Schoof, il faut rappeler quelques outils algébriques essentiels dont on trouvera des précisions dans l'incontournable [Sil86].

**Définition 1.5** (Isogénies). *On dit qu'un morphisme algébrique $\varphi$ entre deux courbes elliptiques $E_1$ et $E_2$ est une* isogénie *si $\varphi(\mathcal{O}_1) = \mathcal{O}_2$. Si de plus $\varphi$ n'est pas constante, on dit que $E_1$ et $E_2$ sont* isogènes.

†. Discrete Logarithm Problem en anglais.
‡. Il est facile de voir que la difficulté se réduit aux ordres premiers.
¶. Elle est ici exponentielle en la taille de $q$.

La condition sur le point à l'infini semble faible. Il n'en est rien :

**Proposition 1.6.** *Une isogénie $\varphi : E_1 \to E_2$ est aussi un morphisme de groupe.*

Deux isogénies jouent un rôle fondamental dans l'algorithme de Schoof. La première, sur laquelle repose toute l'idée de l'algorithme, est le Frobénius. En effet, il permet de déterminer les points de la courbe qui sont à coordonnées dans $\mathbb{F}_q$ : ce seront naturellement ceux qui sont dans le noyau de $\pi_E - \mathrm{Id}$ où l'on a défini :

**Définition 1.7.** *Soit $E$ une courbe elliptique définie sur $\mathbb{F}_q$. On appelle* morphisme de Frobenius *le morphisme algébrique*

$$\begin{aligned} \pi_E : E(\overline{\mathbb{F}_q}) &\longrightarrow E(\overline{\mathbb{F}_q}) \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

C'est bien une isogénie puisqu'elle envoie le point à l'infini sur lui-même [†]. A ce stade, il nous faut quelques propriétés usuelles vérifiées par les isogénies pour pouvoir déterminer le cardinal du noyau de $\pi_E - \mathrm{Id}$ :

**Proposition 1.8.** *Une isogénie $\varphi$ non nulle est surjective et possède un noyau fini. Lorsqu'elle est séparable, on a de plus $|\ker \varphi| = \deg \varphi$.*

*Pour toute isogénie $\varphi : E_1 \to E_2$ il existe une unique isogénie $\hat{\varphi} : E_2 \to E_1$ vérifiant*

$$\hat{\varphi} \circ \varphi = [m]_{E_1} \text{ et } \varphi \circ \hat{\varphi} = [m]_{E_2},$$

*où $m = \deg \varphi$. On a de plus $\widehat{\lambda \circ \varphi} = \hat{\lambda} \circ \hat{\varphi}$ et $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$, pour des isogénies $\lambda : E_2 \to E_3$ et $\psi : E_1 \to E_2$.*

On a en particulier $\hat{\hat{\varphi}} = \varphi$ ce qui justifie la qualification de dualité. On définit finalement :

**Définition 1.9** (Norme et trace)**.** *Soit $\varphi : E \to E$ une isogénie. On définit sa* norme *et sa* trace *par*

$$\mathrm{N}\,\varphi = \varphi \circ \hat{\varphi} \in \mathbb{N} \quad \textit{et} \quad \mathrm{tr}\,\varphi = \varphi + \hat{\varphi} \in \mathbb{Z}.$$

Maintenant on écrit d'une part

$$\begin{aligned} |E(\mathbb{F}_q)| = \deg(\pi_E - \mathrm{Id}) = \mathrm{N}(\pi_E - \mathrm{Id}) = (\pi_E - \mathrm{Id}) \circ \widehat{(\pi_E - \mathrm{Id})} &= (\pi_E - \mathrm{Id}) \circ (\hat{\pi}_E - \mathrm{Id}) \\ &= q + 1 - (\pi_E + \hat{\pi}_E) = q + 1 - \mathrm{tr}\,\pi_E. \end{aligned}$$

et, d'autre part, on compose par $\pi_E$ l'égalité $\mathrm{tr}\,\pi_E = \pi_E + \hat{\pi}_E$ : on obtient $(\mathrm{tr}\,\pi_E)\pi_E = \pi_E^2 + q$. Ce sont les propriétés fondatrices de l'algorithme de Schoof :

**Proposition 1.10.**

*(i) Le cardinal de $E(\mathbb{F}_q)$ est donné par la trace de $\pi$ : $|E(\mathbb{F}_q)| = q + 1 - \mathrm{tr}\,\pi_E$.*

*(ii) L'endomorphisme $\pi_E$ vérifie, dans* End $E$*, l'équation*

$$\pi_E^2 - (\mathrm{tr}\,\pi_E)\pi_E + q = 0.$$

Ainsi, suivant le principe que l'on a décrit dans le paragraphe précédent, on va chercher à déterminer $\mathrm{tr}\,\pi_E \mod l$ pour différents $l$. Pour cela, on réduit l'équation « modulo » $l$. On note $q'$ l'entier $0 < q' < l$ congru à $q$ modulo $l$ et on a la proposition :

**Proposition 1.11.** *La relation*

$$\pi_E^2 - t'\pi_E + q' \qquad t' = 0, 1, 2, \ldots, l-1 \tag{$\star$}$$

*est vérifiée sur le sous-groupe $E[l]$ des points de $l$–torsions si et seulement si $t' \equiv \mathrm{tr}\,\pi_E \mod l$.*

Notons qu'il suffit en fait de vérifier la relation sur une partie de $E[l]$ non réduite à $\{\mathcal{O}\}$. Le problème est de trouver un point de $E[l]\backslash\{\mathcal{O}\}$ (et donc le sous-groupe d'ordre $l$ qu'il engendre).

L'idée de Schoof (voir [Sch85]) est alors d'utiliser les polynômes de divisions. Ce sont des polynômes qui caractérisent, pour un entier $m$ donné, les points de $m$–torsion. Concrètement, il n'est pas difficile de trouver ces polynômes : il suffit par exemple d'écrire le morphisme rationnel $[m]$ puis de n'en garder que les dénominateurs [‡] ; il s'agira en effet des polynômes annulateurs des points qui s'envoient sur le point infini, élément neutre du groupe. La forme particulière d'une équation de Weierstrass nous donne des polynômes ayant une forme relativement simple :

†. On devrait écrire l'expression du Frobénius en coordonnées projectives, $[X, Y, Z] \mapsto [X^q, Y^q, Z^q]$, ce qui montre clairement que l'image de $\mathcal{O} = [0, 1, 0]$ est bien lui-même.

‡. Encore une fois, on préfère garder une notation affine des morphismes ; sinon, il faut écrire le morphisme $[m]$ avec des polynômes homogènes et résoudre $[F_m, G_m, H_m] = [0, 1, 0]$.

**Proposition 1.12.** *Les polynômes de division peuvent se calculer grâce aux formules suivantes :*

$$\begin{aligned}
\Psi_1 &= 1, \qquad \Psi_2 = 2y,\\
\Psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\Psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
\Psi_{2m+1} &= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \qquad (m \geqslant 2),\\
2y\Psi_{2m} &= \Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) \qquad (m \geqslant 3).
\end{aligned}$$

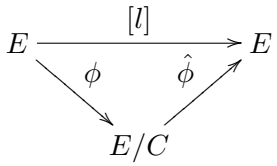
Une fois ces polynômes à notre disposition, il nous suffit de chercher quel $t'$ vérifie la relation $(\star)$ dans l'anneau $\mathbb{F}_q[X,Y]/\langle \Psi_m(X,Y), Y^2 - X^3 - aX - b\rangle$, dans lequel on sait calculer efficacement.

## 1.4 L'algorithme Sea.

Néanmoins, de l'avis de Schoof lui-même, son algorithme tel quel n'est pas très performant notamment à cause du degré élevé des polynômes de division. Même si cela est maintenant à relativiser, Atkin et Elkies ont proposé quelques méthodes pour améliorer la complexité, en travaillant avec des polynômes de plus petite taille. L'idée principale est de trouver un facteur de $\Psi_l$ de degré beaucoup plus petit, en l'occurrence $\frac{l-1}{2}$. Cela revient à factoriser l'isogénie $[l]$ de degré $l^2$ par une isogénie de degré $l$. Le noyau d'une telle isogénie serait alors $\mathbb{Z}/l\mathbb{Z}$ qui est cyclique. Soit $C$ un des $l+1$ sous-groupes cycliques d'ordre $l$ de $E[l] \simeq (\mathbb{Z}/l\mathbb{Z})^2$.

**Proposition 1.13.** *Il existe une unique courbe elliptique $E'$ et une isogénie séparable $\phi : E \to E'$ telle que $\ker\phi = C$. On note $E/C$ cette courbe elliptique et on dit qu'elle est $l$–isogène à $E$.*

On peut résumer l'idée principale de ces améliorations par le diagramme suivant : l'algorithme de Schoof utilise la flèche $[l]$ tandis que les améliorations d'Atkin et Elkies reposent sur $\phi$ :




Pour trouver ces courbes $l$–isogènes à $E$, on doit faire appel à un invariant très important dans la théorie des courbes elliptiques : l'invariant modulaire ou $j$–invariant. Sans entrer dans les détails, disons que cet invariant décrit les courbes elliptiques à isomorphisme près sur une clôture algébrique.

**Théorème 1.14.** *Soit $E/K$ une courbe elliptique définie sur un corps $K$ de caractéristique différente de $l$. Soit $j$ son invariant : alors, les $l+1$ zéros de $\Phi_n(X,j)$ dans $\overline{K}$ sont précisément les $j$–invariants des courbes $E'$ $l$–isogènes à $E$.*

Le reste est assez technique à présenter mais plutôt bien maîtrisé à l'heure actuelle. Même si l'on peut encore chercher à l'améliorer, l'algorithme Sea obtenu est finalement assez performant pour répondre à nos besoins : la complexité chute en $\tilde{O}((\log q)^4)$ et les améliorations d'Atkin agissent fortement sur la constante cachée dans le $O$.

Mentionnons pour finir que le nombre de points d'une courbe elliptique peut être relié étroitement à celui de son anneau d'endomorphismes. Si l'on connaît ce dernier à l'avance, alors, on peut trouver plus facilement le nombre de points rationnels : on utilise l'algorithme de Cornaccia. Cet algorithme est très efficace mais probabiliste puisqu'il repose sur l'extraction d'une racine carrée dans $F_q$. Notons que Schoof, dans son article original ([Sch85]) a eu l'idée de « renverser » cet algorithme pour en tirer le résultat surprenant :

**Théorème 1.15** (Schoof (1985))**.** *Soit $D \in \mathbb{Z}$ un entier fixé. Soit $p \equiv 1 \mod 4$ [†] un nombre premier tel que $\left(\frac{D}{p}\right) = +1$. Alors, il existe un algorithme* déterministe *et polynomial en $\log p$ calculant la racine carrée de $D$ modulo $p$, i.e. $y \in \mathbb{F}_p$, $y^2 \equiv D \mod p$. Cet algorithme dépend exponentiellement de la taille ($\log D$) de l'entier $D$.*

†. Le cas $p = 2$ n'a aucun intérêt et pour $p \equiv -1 \mod 4$, la racine carrée, si elle existe, s'obtient polynomialement en élevant à la puissance $\frac{p+1}{4}$.

# 2 Codes correcteurs géométriques.

## 2.1 Enjeux.

Une autre partie de la théorie de l'information fait appel à la géométrie algébrique : ce sont les codes correcteurs. Il s'agit de s'assurer que le message transmis est reçu sans erreur et dans le cas contraire, d'essayer de corriger ces erreurs. L'idée générale est de se placer sur un alphabet fini ($\mathbb{F}_q$ dans nos applications), de considérer une partie de $\mathbb{F}_q^n$, « le code » (généralement un sous-espace vectoriel) tels que deux mots de codes soient suffisamment éloignés, au sens de la distance de Hamming, qui compte le nombre de composantes différentes.

L'émetteur code le message à envoyer grâce à une fonction injective (généralement linéaire). Le récepteur vérifiera que le message est dans le code [†] et à défaut cherchera le mot de code le plus proche. Pour les détails et les définitions, on pourra par exemple se reporter à [vL82].

Deux quantités fondamentales interviennent pour juger de la qualité d'un code : son rendement $R$, c'est-à-dire le rapport du nombre de symboles du mot à coder par celui transmis, et sa distance minimale relative $\delta$, *i.e.* le rapport de la distance minimale entre deux mots de codes distincts et la taille du code. Des bornes élémentaires relient ces deux quantités :

Les excellentes familles de codes sont définies comme des ensembles de codes dont les paramètres $(\delta_n, R_n)$ ont un point d'accumulation (quand la longueur du code tend vers l'infini) au-dessus de la borne de Gilbert–Varshamov. Les codes de Goppa sur $\mathbb{F}_q$ atteignent cette borne mais il a fallu attendre assez longtemps et l'utilisation centrale de géométrie algébrique pour la dépasser.

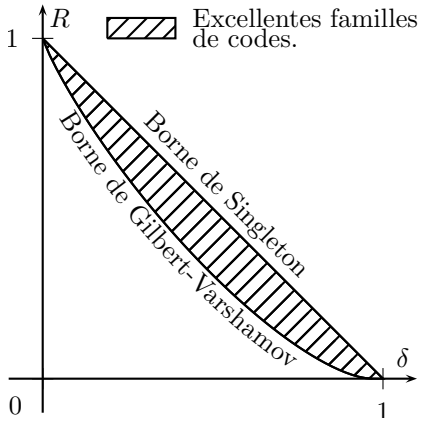


FIGURE 2: Bornes asymptotiques pour $q = 32$.

## 2.2 Codes géométriques.

On considère un objet géométrique $\mathcal{X}$ et un ensemble $\mathcal{P} = \{P_1, \ldots, P_n\}$ de points sur $\mathcal{X}$. On suppose ensuite que l'on dispose d'un $\mathbb{F}_q$–espace vectoriel $L$ de fonctions de $\mathcal{X}$ à valeurs dans $\mathbb{F}_q$. On peut alors définir une fonction d'évaluation :

$$\begin{aligned} \mathrm{ev}_{\mathcal{P}} : L &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) \ . \end{aligned}$$

L'image de $\mathrm{ev}_{\mathcal{P}}$ est un code linéaire que l'on qualifiera de géométrique. Quitte à remplacer $L$ par $L/\ker \mathrm{ev}_{\mathcal{P}}$, on peut supposer que l'application est bien injective.

Un premier exemple simple mais important est celui où l'on choisit pour $\mathcal{X}$ la droite affine $\mathbb{F}_q$ et $\{P_1, \ldots, P_n\}$ un ensemble de $n$ points distincts de $\mathbb{F}_q$. L'espace vectoriel $L$ peut être choisi comme l'espace des polynômes à coefficients dans $\mathbb{F}_q$, de degré au plus $k-1$ avec $k \leqslant n$. On obtient ainsi le code classique dit de Reed–Solomon (RS) dont la distance minimale est $n-k+1$ et le rendement $k/n$ pourraient atteindre la borne asymptotique de Gilbert–Varshamov si l'on n'était pas limité par le choix de $n$ points distincts de $\mathbb{F}_q$.

Un autre exemple très important est celui des codes de Goppa classiques [‡] : en effet, ils sont à la base d'une famille de codes qui atteint la borne de Gilbert–Varshamov, sans toutefois la dépasser.

Ces deux exemples, que l'on qualifie de classiques, peuvent être réinterprétés dans le cadre plus général des codes géométriques des paragraphes suivants, où l'on choisit $\mathcal{X} = \mathrm{P}^1(\mathbb{F}_q)$. Cette variété a l'avantage de donner une construction « simple » de ces codes mais est limité par son nombre de points.

Plus formellement, on choisit désormais pour $\mathcal{X}$ une courbe projective lisse définie sur un corps fini $K$ : un des enjeux cruciaux sera donc de trouver une telle courbe avec beaucoup de points rationnels. Cela permettra déjà de construire des codes de grande taille, mais seront-ils bons pour autant ?

Pour cela, il faut étudier la distance minimale : elle est d'autant plus grande que le nombre de points d'évaluation imposant l'égalité de deux fonctions est petit. L'idée est alors de se restreindre aux fonctions rationnelles sur $\mathcal{X}$ dont on impose des pôles ou des zéros.

On introduit dès lors la notion de diviseur sur la courbe $\mathcal{X}$ : c'est un élément du groupe abélien libre engendré par les points de $\mathcal{X}$ (à coordonnées dans $\overline{K}$). On rappelle qu'un tel diviseur est dit défini sur $K$ s'il

†. Cela ne certifie pas que la transmission est correcte mais on peut fixer une probabilité d'erreur.

‡. Il s'agit en fait des codes de Goppa géométriques, présentés un peu plus loin, où l'on se place sur $\mathrm{P}^1(\mathbb{F}_q)$.

est invariant par $\mathrm{Gal}_{\overline{K}/K}$. Par exemple le diviseur d'une fonction rationnelle à coefficients dans $K$ est défini sur $K$ ; un tel diviseur est appelé principal et son degré est nul (la somme de ses coefficients est nulle).

Maintenant, pour imposer le comportement d'une fonction, on choisit un diviseur $D$ et on impose que $\mathrm{div}\, f + D \geqslant 0$ : ainsi, les pôles de $f$ sont dans l'ensemble $\{P, n_P > 0\}$ dont l'ordre n'excède pas $n_P$ et chaque point de l'ensemble $\{P, n_P < 0\}$ est un zéro d'ordre au moins $n_P$ de $f$.

**Le théorème de Riemann–Roch.** L'outil fondamental utilisé ici est le théorème de Riemann–Roch dont on rappelle brièvement l'énoncé. Pour cela, introduisons l'espace vectoriel

$$\mathscr{L}(D) = \{f \in \overline{K}(\mathcal{X})^*, \quad \mathrm{div}\, f + D \geqslant 0\} \cup \{0\}.$$

**Théorème 2.1** (Riemann–Roch)**.** *Soit $G$ un diviseur. L'espace vectoriel $\mathscr{L}(G)$ a une dimension finie que l'on note $\ell(G)$. Plus précisément, si $G < 0$, $\mathscr{L}(G) = \{0\}$. Sinon, soit $W_{\mathcal{X}} = \mathrm{div}\, \omega_{\mathcal{X}}$ où $\omega_{\mathcal{X}}$ est une différentielle non nulle sur $\mathcal{X}$ : alors, il existe un entier $g$, le genre de $\mathcal{X}$, tel que*

$$\ell(G) - \ell(W_{\mathcal{X}} - G) = \deg G - g + 1.$$

*En particulier, $\ell(W_{\mathcal{X}}) = g$, $\deg(W_{\mathcal{X}}) = 2g - 2$ et $\deg G > 2g - 2 \Rightarrow \ell(G) = \deg G - g + 1$.*

**Remarque 2.2.** Le théorème de Riemman–Roch s'énonce pour un corps algébriquement clos. Néanmoins, si $G$ est défini sur $K$ alors, $\mathrm{Gal}_{\overline{K}/K}$ agit sur $\mathscr{L}(G)$ et on peut alors en trouver une base constituée de fonctions dans $K(\mathcal{X})$. C'est en fait ce résultat que l'on utilise dans notre cas puisque l'application aux codes correcteurs nécessite de se placer sur $\mathbb{F}_q$ et non sur sa clôture algébrique.

Le théorème de Riemann–Roch peut se réénoncer en terme de différentielles : si $G$ est un diviseur, on introduit l'espace vectoriel

$$\Omega(G) = \{\omega \in \Omega(\mathcal{X}),\ \mathrm{div}\, \omega - G \geqslant 0\} \cup \{0\}$$

et on dote $\delta(G)$ la dimension de cet espace vectoriel.

**Théorème 2.3.** *Soit $W_{\mathcal{X}}$ le diviseur d'une différentielle non nulle sur $\mathcal{X}$. Alors,*

$$\delta(G) = \ell(W_{\mathcal{X}} - G).$$

**Les codes géométriques.** Les deux points de vue du théorème de Riemann–Roch conduisent à la construction de deux types de codes géométriques. D'une part, on construit les codes de Reed–Solomon géométriques en choisissant une courbe lisse $\mathcal{X}$ définie sur $\mathbb{F}_q$, un diviseur positif $G$ défini sur $\mathbb{F}_q$ et $n$ points rationnels $(P_1, \ldots, P_n)$ de $\mathcal{X}$ n'appartenant pas au support de $G$. Notons $D$ le diviseur $\sum(P_i)$ et $L$ l'espace vectoriel $\mathscr{L}_{\mathbb{F}_q}(G) = \{f \in \mathbb{F}_q(\mathcal{X}), \mathrm{div}(f) + G \geqslant 0\} \cup \{0\}$. On considère alors le code construit par l'évaluation $\mathrm{ev}_{\mathcal{P}}$ des fonctions de $L$ aux points $P_i$. Remarquons que puisque $D$ et $G$ ont des supports disjoints, les fonctions de $f$ n'ont pas de pôles en les $P_i$.

On note ces codes $\mathcal{C}(D, G)$ . Si on choisit $\deg G < n$ alors l'évaluation $\mathrm{ev}_{\mathcal{P}}$ est bien injective puisque si jamais on a $\mathrm{ev}_{\mathcal{P}}(f) = 0$ pour $f \neq 0$ alors, $\mathrm{div}(f) \geqslant D - G > 0$, ce qui est impossible. Voyons maintenant les caractéristiques des codes $\mathcal{C}(D, G)$ :

**Théorème 2.4.** *Supposons que $\deg G < n$. Alors, le code $\mathcal{C}(D, G)$ a pour dimension*

$$k \geqslant \deg G - g + 1,$$

*avec égalité si $\deg G > 2g - 2$. De plus, sa distance minimale vérifie l'inégalité*

$$d \geqslant n - \deg G.$$

On remarque que l'on a l'inégalité $k + d \geqslant n - g + 1$ ou encore $R + \delta \geqslant 1 - \frac{1-g}{n}$. La première inégalité est à rapprocher de $k + d = n + 1$ que l'on a pour les codes RS, qui peuvent être interprétés comme un cas particulier.

Mentionnons maintenant la deuxième classe de codes géométriques : les codes de Goppa géométriques $\mathcal{C}^*(D, G)$, où $D$ et $G$ sont des diviseurs choisis comme ci-dessus. Par contre, on choisit pour $L$ l'espace $\Omega(G - D)$ et la fonction d'évaluation $\mathrm{ev}^*_{\mathcal{P}} : \omega \to (\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega))$. D'une manière comparable aux codes de Reed–Solomon géométriques, on constate que cette fonction d'évaluation est injective dès que $\deg G > 2g - 2$.

**Théorème 2.5.** *Soit $G$ un diviseur vérifiant $\deg G > 2g-2$. Le code $\mathcal{C}^*(D,G)$ a pour dimension*

$$k \geqslant n - \deg G + g - 1$$

*avec égalité si $\deg G < n$. Sa distance minimale vérifie*

$$d \geqslant \deg G - 2g + 2.$$

On justifie la notation $\mathcal{C}^*$ en montrant que les codes $\mathcal{C}(D,G)$ et $\mathcal{C}^*(D,G)$ sont duaux (la matrice génératrice de l'un et la matrice de parité de l'autre).

De plus, comme dans le cas des codes de Reed–Solomon, on note que l'on a $k+d \geqslant n-g+1$. Ceci n'est pas une coïncidence puisque les deux catégories de codes sont étroitement liées :

**Proposition 2.6.** *Soit $\{P_1,\dots,P_n\}$ un ensemble de $n$ points rationnels sur $\mathcal{X}$. Alors, il existe une différentielle $\omega$ avec des pôles simples en les $P_i$ tels que $\mathrm{Res}_{P_i}(\omega)=1$. De plus, pour $G$ ayant un support disjoint de $P$,*

$$\mathcal{C}^*(D,G) = \mathcal{C}(D, \operatorname{div}\omega + D - G).$$

Plus généralement, on peut montrer qu'il n'existe « globalement » qu'une seule catégorie de codes géométriques.

**Proposition 2.7.** *Soit $C$ un code $q$–aire. Alors, on peut trouver une courbe $\mathcal{X}$ définie sur $\mathbb{F}_q$ et deux diviseurs $D$ et $G$ vérifiant les propriétés habituelles, tels que $C$ soit un sous-code de $\mathcal{C}(D,G)$.*

## 2.3 Des courbes avec beaucoup de points rationnels.

Comme on l'a vu dans la section précédente, il apparaît fondamental de pouvoir trouver des courbes ayant beaucoup de points rationnels : ce seront de bonnes candidates pour construire des codes géométriques. Commençons par les définitions et notations suivantes.

**Définition 2.8.** *On note $N_q(g)$ le nombre maximum de points rationnels d'une courbe projective absolument irréductible, lisse, de genre $g$, définie sur $\mathbb{F}_q$. On note aussi*

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

La dernière quantité peut être motivée par la borne de Hasse–Weil qui généralise le théorème 1.4 en genre supérieur :

**Théorème 2.9** (Hasse–Weil)**.** *Soit $\mathcal{X}$ une courbe projective lisse, absolument irréductible, de genre $g$ définie sur $\mathbb{F}_q$. Alors, le nombre de points rationnels $|\mathcal{X}(\mathbb{F}_q)|$ vérifie les inégalités*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \leqslant 2g\sqrt{q}.$$

Maintenant, on peut s'intéresser d'une part aux résultats asymptotiques sur $A(q)$ et d'autre part aux quantités $N_q(g)$ à $q$ et $g$ fixées.

**Résultats asymptotiques : la borne Tvz.** Le théorème de Hasse–Weil nous donne une première idée de $A(q)$ puisque l'on a facilement l'inégalité $A(q) \leqslant 2\sqrt{q}$. Néanmoins, cette borne n'est pas optimale. En fait, on a le théorème :

**Théorème 2.10** (Drinfeld–Vlăduţ)**.** *On a l'inégalité*

$$A(q) \leqslant \sqrt{q} - 1,$$

*qui est en fait une égalité si $q$ est un carré.*

**Corollaire 2.11** (Borne Tvz)**.** *On fixe $q = p^{2k}$ un carré. Pour chaque $R$, il existe une asymptotiquement bonne famille de codes dont le taux d'information tend vers $R$ et la distance relative tend vers un $\delta$ vérifiant*

$$R + \delta \geqslant 1 - \frac{1}{\sqrt{q}-1}.$$

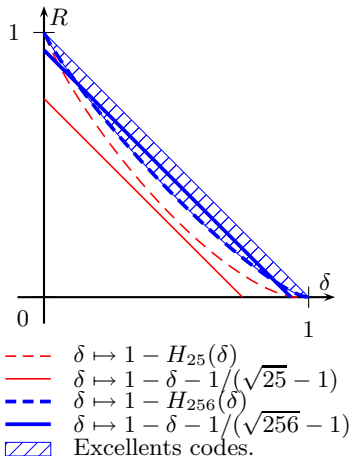



FIGURE 3: Borne TVZ.

Cette borne est meilleure que celle de Gilbert–Varshamov dès que $q \geqslant 49$, comme l'illustre la figure ci-contre où l'on a pris $q = 25$ et $q = 256$. La démonstration est intéressante puisqu'elle met vraiment en avant le lien entre excellents codes et nombres de points rationnels.

Comme $q$ est un carré, on a égalité dans le théorème de Drinfeld–Vlăduţ : il existe une suite de courbes $\mathcal{X}_l$ définies sur $\mathbb{F}_q$ de genre $g_l$ ayant $n_l+1$ points rationnels, $(P_0, \dots, P_{n_l})$, avec la propriété

$$\lim_{l\to\infty} \frac{n_l+1}{g_l} = \sqrt{q} - 1.$$

Pour chacune de ces courbes, on choisit $D = \sum_{i=1}^{n_l}(P_i)$ et $G = m_l(P_0)$ avec $m_l$ vérifiant $m_l < n_l$ et† $\frac{m_l - g_l + 1}{n_l} \to R$. Ainsi, le code $\mathcal{C}(D,G)$ de longueur $n_l$ vérifie, si l'on note $d_l$ sa distance minimale et $k_l$ sa dimension,

$$k_l + d_l \geqslant n_l + 1 - g_l \Longrightarrow R_l + \delta_l \geqslant 1 - \frac{g_l - 1}{n_l}.$$

En faisant tendre $l$ vers l'infini et quitte à extraire une sous-suite pour que $(\delta_l)_l$ converge, on a montré le résultat.

On peut démontrer le théorème 2.10 de Drinfeld–Vlăduţ en utilisant les *conjectures de Weil* et une formule explicite due à Serre ([Ser84]). En fait, on peut exhiber une suite de courbes dans le cas $q = p^{2k}$, qui montre que $A(q) \geqslant \sqrt{q} - 1$ : ce sont les courbes hermitiennes : on se place sur $\mathbb{F}_q$ avec $q = r^2 = p^{2k}$ et on considère le polynôme $F(X,Z) = X^{r+1} - Z^r - Z$. On construit une suite de courbes $\mathcal{X}_n$ définies par les idéaux‡

$$\mathcal{I}_n = \langle F(X_1,X_2), F(X_2,X_3), \dots, F(X_{n-1},X_n)\rangle \subset \mathbb{F}_q[X_1, X_2, \dots, X_n].$$

Ces idéaux sont premiers et définissent des variétés algébriques irréductibles ; comme elles sont de degré de transcendance 1, ce sont des courbes irréductibles.

**Estimations de $N_q(g)$.** Commençons par présenter les premiers résultats obtenus par Serre ([Ser84]). Tout d'abord, dans le cas où $q$ n'est pas un carré, Serre améliore la borne de Weil :

**Proposition 2.12** (Serre)**.** *Soit $\mathcal{X}$ une courbe projective lisse absolument irréductible. Soit $g$ son genre. Alors, son nombre de points rationnels sur $\mathbb{F}_q$ vérifie*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \leqslant g[2\sqrt{q}],$$

*où $[x]$ dénote la partie entière de $x$.*

La démonstration de ce théorème fait intervenir les célèbres *conjectures de Weil*¶ que l'on ne saurait passer sous silence dans la recherche du nombre de points rationnels sur les corps finis.

**Théorème 2.13** (Conjectures de Weil)**.** *Soit $\mathcal{X}$ une courbe définie sur $\mathbb{F}_q$, lisse, complètement irréductible et de genre $g$. Alors, si l'on note $|\mathcal{X}(\mathbb{F}_{q^n})|$ le nombre de points rationnels de $\mathcal{X}$ sur $\mathbb{F}_{q^n}$, la fonction zêta de $\mathcal{X}$ définie par*

$$Z_{\mathcal{X}}(T) \stackrel{\text{def}}{=} \exp\left(\sum_{n=1}^{\infty} |\mathcal{X}(\mathbb{F}_{q^n})| \frac{T^n}{n}\right),$$

*est une fraction rationnelle à coefficients entiers. Plus précisément, il existe un polynôme $P_{\mathcal{X}}(T)$ de degré $2g$ à coefficients entiers et de terme constant 1 tel que*

$$Z_{\mathcal{X}}(T) = \frac{P_{\mathcal{X}}(T)}{(1-T)(1-qT)}.$$

*Enfin, si l'on note $P_X(T) = \prod(1-\omega_j T)(1-\overline{\omega}_j T)$ alors, $|\omega_j| = \sqrt{q}$.*

En particulier, $|\mathcal{X}(\mathbb{F}_q)|$ est donné par la valeur en 0 de la dérivée logarithmique de $Z_{\mathcal{X}}$ : $|\mathcal{X}(\mathbb{F}_q)| = q + 1 - \sum(\omega_j + \overline{\omega}_j)$.

†. Ceci est possible puisque l'on peut supposer $R < 1 - \frac{1}{\sqrt{q}-1}$ sans quoi il n'y a rien à montrer.

‡. Il faudrait, pour être exact, homogénéiser les polynômes engendrant $\mathcal{I}_n$.

¶. On continue à les appeler *conjectures* bien qu'elles aient été démontrées en 1973 grâce aux travaux de Dwork, Grothendieck puis Deligne.

**Les genres 1 et 2.** On appellera l'inégalité de la proposition 2.12, la borne de Weil–Serre. Celle-ci est presque optimale en petit genre. En effet, on a un théorème de Hasse et Deuring :

**Théorème 2.14.** *Soit $q = p^n$ et $m = [2\sqrt{q}]$. Alors,*

$$N_q(1) = q + 1 + m$$

*sauf si $m \equiv 0 \mod p$, $n \geqslant 3$ et $n$ est impair. Sous ces conditions, $N_q(1) = q + m$.*

Le cas $g = 2$ est un peu plus délicat. Avec Serre, on note $m = [2\sqrt{q}]$ et on dit que $q = p^n$ avec $n$ impair est *spécial* s'il vérifie l'une des conditions suivantes :

*(i)* $m \equiv 0 \mod p$.

*(ii)* il existe $x \in \mathbb{Z}$ tel que $q = x^2 + 1$ ou $q = x^2 + x + 1$ ou $q = x^2 + x + 2$.

On justifiera un peu plus loin cette dernière condition un peu mystérieuse.

**Théorème 2.15.** *On a $N_4(2) = 10$, $N_9(2) = 20$. Sinon, si $q$ n'est pas spécial alors,*

$$N_q(2) = q + 1 + 2m.$$

*Si $q$ est spécial alors,*

$$N_q(2) = \begin{cases} q + 2m & \text{si } \{m\} > \frac{\sqrt{5}-1}{2}, \\ q + 2m - 1 & \text{sinon,} \end{cases}$$

*où l'on a noté $\{x\} = x - [x]$ la partie fractionnaire de $x$.*

**Le genre 3.** Le cas $g = 3$ est bien plus compliqué et est toujours l'objet de recherches à l'heure actuelle. Un problème très naturel qui apparaît dans les cas $g = 2, 3$, est de savoir s'il existe une constante dépendante de $g$ telle que pour tout $q$,

$$q + 1 + 2m - N_q(g) \leqslant C(g).$$

Par exemple, les deux théorèmes 2.14 et 2.15 nous donnent $C(1) = 2$ et $C(2) = 1 + \sqrt{5}$, mais on ne sait pas montrer l'existence d'une telle constante en genre 3 et encore moins en genre quelconque ! Voyons, sans rentrer dans tous les détails, ce que l'on peut dire du genre 3. Le principal résultat général en genre 3 qui tente de répondre à la question précédente est le théorème suivant énoncé par Lauter. On peut consulter [LR07] et [Lau02].

**Théorème 2.16.** *Il existe une courbe (projective, lisse et absolument irréductible) de genre 3 sur $\mathbb{F}_q$ telle que*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \geqslant 3m - 3,$$

*où $m = [2\sqrt{q}]$.*

Le problème est que l'on ne sait pas si la courbe donnée par ce théorème a le nombre maximal ou minimal de points ! A la différence des courbes elliptiques (ou hyperelliptiques), on ne peut pas résoudre simplement cette complication avec une tordue quadratique.

Pour arriver à ce théorème, on commence par prendre une courbe elliptique $E$ qui possède le nombre maximal de points sur le corps $\mathbb{F}_q$. On considère ensuite naturellement la variété abélienne $E \times E \times E$ qui possède beaucoup de points rationnels.

Les jacobiennes de courbes permettent de passer des variétés abéliennes aux courbes. De plus, il est possible de relier le nombre de points rationnels d'une courbe $C$ à celui de sa jacobienne $\mathrm{Jac}(C)$ (et donc à celui de toute variété abélienne $A$ isogène *sur* $\mathbb{F}_q$ à $\mathrm{Jac}(C)$). Plus précisément, le nombre de points rationnels de $C$ est $q + 1 + \operatorname{tr} \mathrm{Fr}_A$, ce qui explique le choix de $E \times E \times E$ pour $A$.

Néanmoins, toute variété abélienne n'est pas isogène sur $\mathbb{F}_q$ à la jacobienne d'une courbe. On sait déjà (en dimension $g = 3$) que lorsque l'on se place sur une clôture algébrique de $\mathbb{F}_q$, ceci n'est vrai que lorsque la variété abélienne est principalement polarisée et indécomposable.

Pour y remédier, on commence par fixer un entier $a$ premier avec la caractéristique $p$ du corps $\mathbb{F}_q$ et tel que $d = a^2 - 4q$ soit négatif : ce sera le discriminant de l'équation caractéristique du Frobenius d'une courbe elliptique $E$ dont la trace est $a$. Avec le théorème 2.14 on peut prendre $a = -m$ où $-m + 1$. On pose $R = \mathbb{Z}[X]/(X^2 - aX + q)$ qui est un ordre (engendré par le Frobenius) dans le corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$. Pour simplifier, on suppose que c'est l'ordre maximal, c'est-à-dire l'anneau des entiers. On note $\mathrm{Ab}(a, q)$ la catégorie des variétés abéliennes isogènes sur $\mathbb{F}_q$ à un produit de copies de $E$ et $\mathrm{Mod}(R)$ la catégorie des $R$–modules sans torsion de type fini. Par exemple, $\mathrm{Hom}(E, A)$ est un objet de cette catégorie.

**Proposition 2.17.** *Le foncteur $T : \mathrm{Ab}(a,q) \to \mathrm{Mod}(R)$, défini par $T(A) = \mathrm{Hom}(E, A)$, est une équivalence de catégorie. Le foncteur $S$ inverse de $T$ est donné par la variété abélienne $S(L) = L \otimes_R E$ que l'on abrègera en $A_L$.*

En fait, munir $A_L$ d'une polarisation revient exactement à faire de $L$ un $R$–module hermitien :

**Théorème 2.18** (Serre)**.** *Une variété abélienne $A_L$ principalement polarisée est indécomposable si et seulement si $L$ est indécomposable comme module hermitien (de discriminant 1).*

Ainsi, pour obtenir une variété abélienne $A$ indécomposable, isogène sur $\mathbb{F}_q$ à $E \times E \times E$, il faut et il suffit qu'il existe un $R$–module hermitien indécomposable. Un théorème, énoncé par Hoffmann, règle le cas des modules hermitiens indécomposables en dimension 2 et 3 :

**Théorème 2.19.** *On rappelle que $d$ est le discriminant de l'anneau $R$. Alors, il n'existe aucun $R$–module hermitien indécomposable de discriminant 1 si et seulement si*

*(i) on est en dimension 2 et $d = -3, -4$ ou $-7$,*

*(ii) on est en dimension 3 et $d = -3, -4, -8$ ou $-11$.*

Par exemple, en dimension 2, on peut vérifier que les exceptions correspondent exactement, outre le cas $m \equiv 0 \mod p$, aux discriminants qui apparaissent dans le cas *spécial (ii)* du théorème 2.15. En dimension 3, c'est ce qui explique, dans le théorème 2.16, le défaut de 3 par rapport à la borne de Weil–Serre.

Il nous reste encore un écueil : l'isogénie entre $E \times E \times E$ n'est pas forcément définie sur $\mathbb{F}_q$. En fait on a le résultat :

**Théorème 2.20.** *Soit $L$ un $R$–module hermitien indécomposable de rang 3. Alors, il existe une courbe $C$ définie sur $\mathbb{F}_q$ telle que $\mathrm{Jac}(C)$ est isomorphe sur $\mathbb{F}_q$ à $A_L$ **ou** à sa tordue quadratique. De plus, si $C$ n'est pas hyperelliptique, les deux cas s'excluent.*

On trouve ainsi une courbe de genre 3 dont le nombre de points rationnels sur $\mathbb{F}_q$ est soit $q+1+3m$ soit $q+1-3m$, ce qui, avec une étude détaillée des cas du théorème 2.19 en genre 3, conduit à une preuve du théorème 2.16.

### 2.4 Conclusion – Questions ouvertes.

Que ce soit à travers la cryptographie ou les codes correcteurs d'erreurs, compter les points d'une variété algébrique définie sur un corps fini s'avère un sujet riche dont on connaît déjà de nombreuses applications pratiques. Paradoxalement, il reste encore beaucoup de questions naturelles en suspens. Même pour les résultats asymptotiques que le théorème de Drinfeld–Vlăduţ semble régler de façon satisfaisante, il reste une zone d'ombre. Ce théorème traite le cas d'une puissance paire d'un nombre premier, mais qu'en est-il du cas impair ? Serre a montré que l'on pouvait minorer $A(q)$ par $c \log q$ (pour une constante $c > 0$) mais l'encadrement $c \log q \leqslant A(q) \leqslant \sqrt{q} - 1$ est loin d'être précis !

Les estimations de $N_q(g)$, centrales dans la construction de codes géométriques, sont finalement encore assez mal maîtrisées : la section précédente présente la majeure partie de ce que l'on connaît à l'heure actuelle quand on fixe un genre. Une autre approche consiste à choisir des formes particulières pour $q$, ou encore de chercher des familles infinies pour lesquelles on a une propriété intéressante sur $N_q(g)$,... De plus, outre la recherche théorique de courbes optimales, il se pose aussi le problème de la construction effective (et efficace) de telles courbes.

## Bibliographie


[Lau02] K. Lauter – « The maximum or minimum number of rational points on genus three curves over finite fields », *Compositio Mathematica* **134** (2002), p. 87–111, avec un appendice de J.-P. Serre.

[LR07] G. Lachaud et C. Ritzenthaler – « On a conjecture of Serre on abelian threefolds », `http://arxiv.org/abs/0710.3303v1`, 2007.

[Sch85] R. Schoof – « Elliptic curves over finite fields and the computation of square roots mod $p$ », *Mathematics of Computation* **44** (1985), no. 170, p. 483–494.

[Ser84] J.-P. Serre – « Nombres de points des courbes algébriques sur $\mathbb{F}_q$ », Oeuvres – Collected papers, vol. 3, Springer, 1972–1984, p. 664–668.

[Sil86] J. H. Silverman – *The arithmetic of elliptic curves*, GTM 106, Springer, 1986.

[vL82] J. H. van Lint – *Introduction to coding theory*, GTM 86, Springer, 1982.