Diviseurs de la forme $2D - G$ sans sections et rang de la multiplication dans les corps finis

Hugues Randriam

24 mars 2011

Résumé

Soient X une courbe algébrique, définie sur un corps parfait, et G un diviseur sur X. Si X a suffisamment de points, on montre comment construire un diviseur D sur X tel que $l(2D - G) = 0$, pour toute valeur de $\deg D$ telle que ceci soit compatible avec le théorème de Riemann-Roch (*i.e.* jusqu'à $\deg D = \left\lfloor \frac{1}{2}(g(X) - 1 + \deg G) \right\rfloor$). On généralise aussi cette construction au cas d'un nombre fini de contraintes $l(k_i D - G_i) = 0$, où $|k_i| \leq 2$.

Un résultat de ce type avait été énoncé par Shparlinski-Tsfasman-Vladut, en relation avec la méthode de Chudnovsky-Chudnovsky pour estimer la complexité bilinéaire de la multiplication dans les corps finis par interpolation sur les courbes ; malheureusement leur preuve était erronée. Ainsi notre travail permet de corriger la preuve de Shparlinski-Tsfasman-Vladut et montre que leur estimation $m_q \leq 2\left(1 + \frac{1}{A(q)-1}\right)$ est valable, du moins dès lors que $A(q) \geq 5 - \frac{14q^2-4}{q^4+2q^2-1}$. On corrige aussi un énoncé de Ballet qui souffre du même problème, et on indique enfin quelques autres applications possibles.

Abstract

Let X be an algebraic curve, defined over a perfect field, and G a divisor on X. If X has sufficiently many points, we show how to construct a divisor D on X such that $l(2D - G) = 0$, for any value of $\deg D$ such that this is compatible with the Riemann-Roch theorem (that is, up to $\deg D = \left\lfloor \frac{1}{2}(g(X) - 1 + \deg G) \right\rfloor$). We also generalize this construction to the case of a finite number of constraints, $l(k_i D - G_i) = 0$, where $|k_i| \leq 2$.

Such a result was previously claimed by Shparlinski-Tsfasman-Vladut, in relation with the Chudnovsky-Chudnovsky method for estimating the bilinear complexity of the multiplication in finite fields based on interpolation on curves; unfortunately, their proof was flawed. So our work fixes the proof of Shparlinski-Tsfasman-Vladut and shows that their estimate $m_q \leq 2\left(1 + \frac{1}{A(q)-1}\right)$ holds, at least when $A(q) \geq 5 - \frac{14q^2-4}{q^4+2q^2-1}$. We also fix a statement of Ballet that suffers from the same problem, and then we point out a few other possible applications.

Introduction

Plusieurs questions de mathématiques discrètes et d'informatique théorique se ramènent au problème suivant :

Problème I. *Soient X une courbe algébrique sur un corps K, et $r \geq 1$ un entier naturel. Étant donnés des entiers relatifs $k_1, \ldots, k_r \in \mathbb{Z}$ et des diviseurs K-rationnels $G_1, \ldots, G_r$ sur X, construire un diviseur K-rationnel D sur X, tel que les diviseurs $k_1 D - G_1, \ldots, k_r D - G_r$ soient sans sections :*

$$l(k_1 D - G_1) = \cdots = l(k_r D - G_r) = 0. \tag{1}$$

(Ici, "courbe" signifiera toujours : courbe projective lisse géométriquement irréductible.)

Citons quelques questions rentrant dans ce cadre (on supposera en général que K est un corps fini $\mathbb{F}_q$) :

- la construction de codes linéaires intersectants ou, plus généralement, de codes séparants ou "frameproof" ([36])
- l'estimation de la complexité bilinéaire de la multiplication dans les corps finis, par interpolation sur les courbes ([14])
- la construction de systèmes de partage de secret linéaires avec propriété de multiplication ([13]).

En fait, ces sujets ne sont pas complètement indépendants : les liens entre codes intersectants et complexité bilinéaire sont connus de longue date ([20]), et par ailleurs, l'existence d'algorithmes de multiplication à faible complexité permet parfois, par des arguments de descente du corps de base, d'améliorer certaines constructions de systèmes de partage de secret ([10]).

Suivant l'approche de [24], elle-même inspirée de [36], le problème I peut se reformuler comme suit (voir aussi [9]).

Notons g le genre de X, et J sa jacobienne. Supposant que X admette au moins un point K-rationnel, notons $j : X \longrightarrow J$ le plongement d'Abel-Jacobi associé, $W_1 = j(X)$ son image, et plus généralement $0 = W_0 \subset W_1 \subset W_2 \subset \cdots \subset W_{g-1} = \Theta \subset W_g = J$ les sommes itérées de W_1 avec elle-même, ou de façon équivalente, les images des applications d'Abel-Jacobi supérieures (et $W_i = \emptyset$ si $i < 0$). Notons aussi $\mathcal{H} = J(K)$.

Problème II. *Avec les notations précédentes, étant donnés un entier $r \geq 1$, des entiers relatifs $k_1, \ldots, k_r$ et $n_1, \ldots, n_r \in \mathbb{Z}$, et des éléments $\kappa_1, \ldots, \kappa_r \in \mathcal{H}$, trouver un entier d tel que $k_1^{-1}(W_{k_1 d - n_1} + \kappa_1)$, $\ldots$, $k_r^{-1}(W_{k_r d - n_r} + \kappa_r)$ ne recouvrent pas $\mathcal{H}$.*

On passe du problème I au problème II en posant $n_i = \deg G_i$ et $\kappa_i = j(G_i)$ pour $1 \leq i \leq r$, et $d = \deg D$.

Souvent, on demandera que cette construction optimise une certaine fonction de d. Par exemple, le théorème de Riemann-Roch (ou le fait que $W_g = J$) impose que, si un tel d existe, il vérifie nécessairement

$$\max(k_1 d - n_1, \ldots, k_r d - n_r) \leq g - 1. \tag{2}$$

On pourra vouloir essayer de maximiser cette dernière quantité.

C'est ce qui est fait dans ce travail : on montre que, sous de bonnes conditions, la borne (2) peut essentiellement être atteinte ; on aura notamment besoin pour cela de supposer que X a suffisamment de points.

Indiquons maintenant quelques méthodes utilisées pour attaquer les problèmes I et II.

(i) Argument de degré : si d vérifie $\max(k_1 d - n_1, \ldots, k_r d - n_r) < 0$, alors d est trivialement solution du problème II, et mieux, n'importe quel diviseur D de degré d est solution du problème I.

(ii) Argument de cardinalité : pour que les $k_i^{-1}(W_{k_i d - n_i} + \kappa_i)$ ne recouvrent pas $\mathcal{H}$, il suffit que leur réunion (ou plus précisément, celle de leurs points rationnels) soit de cardinalité strictement plus petite. Il s'agit donc de pouvoir majorer les $|k_i^{-1}(W_{k_i d - n_i} + \kappa_i)(K)|$.
Remarquons que le point (i) en est un cas particulier, car si $k_i d - n_i < 0$, alors $W_{k_i d - n_i}$ est vide. Cet argument est utilisé notamment dans [14].
En général on peut utiliser la majoration $|k^{-1}(W)(K)| \leq |\mathcal{H}[k]||W(K)|$, valable pour toute sous-variété W de J (où $\mathcal{H}[k]$ est le sous-groupe de k-torsion de $\mathcal{H}$), ce qui donne une condition suffisante sur d :

$$|\mathcal{H}[k_1]||W_{k_1 d - n_1}(K)| + \cdots + |\mathcal{H}[k_r]||W_{k_r d - n_r}(K)| < |\mathcal{H}|. \qquad (3)$$

Une telle approche est utilisée dans [29], mais avec une erreur : les auteurs ont oublié la contribution de la torsion. Elle est utilisée aussi, de façon correcte, dans [36], dans le cas d'une seule contrainte ; et enfin le cas général est traité, sous une forme essentiellement identique à celle présentée ici, dans [9] (où l'erreur de [29] est signalée).
Pour exploiter (3), il faut pouvoir estimer les $|W_n(K)|$ et les $|\mathcal{H}[k]|$. Pour le second point, on dispose de la majoration classique et valable en toute généralité $|\mathcal{H}[k]| \leq k^{2g}$ (utilisée par exemple dans [36]) ; mais quitte à choisir convenablement la courbe X, on peut vouloir espérer faire mieux. On s'intéressera notamment au cas asymptotique, où le genre g tend vers l'infini, et où le nombre de points de X croît linéairement avec g. On cherche donc des courbes ayant "beaucoup" de points mais dont le groupe de classes ait "peu" de k-torsion. Il est naturel d'introduire une constante mesurant la croissance de cette k-torsion par rapport à g dans une telle famille de courbes, et ceci a été fait, indépendamment :
– dans [9], avec la "limite de torsion" $J_k(q, a)$
– dans [24], avec la constante $\delta_k^-(q)$.
Ces deux quantités sont reliées par la formule $J_k(q, A(q)) = \delta_k^-(q) \log_q k$. Dans [24] on trouve des arguments heuristiques en faveur de la conjecture $\delta_k^-(q) = 0$.

(iii) Construction explicite : il s'agit de construire effectivement un diviseur D solution du problème I (par contraste avec la méthode (ii), qui est non-constructive). Ceci est fait, au moins pour l'application aux codes intersectants, dans [25], et on se propose ici de généraliser et d'améliorer encore ces résultats.

Notre construction repose sur l'hypothèse que X a suffisamment de points ; essentiellement, on demande une inégalité du type $\frac{|X(K)|}{g} \geq C(k_1, \ldots, k_r)$, pour une constante $C(k_1, \ldots, k_r)$ qu'on essaiera d'estimer aussi précisément que possible, du moins lorsque tous les k_i sont de valeur absolue au plus 2 (ce qui suffit pour les applications mentionnées ici).

Si l'on veut utiliser cette méthode dans un cadre asymptotique, avec g tendant vers l'infini, on voit qu'il faut supposer que r est fixé. C'est le cas pour les applications aux codes intersectants ($r = 1$) ou à la complexité bilinéaire de la multiplication ($r = 2$). Il se trouve que la construction fournit alors un diviseur D dont le degré est essentiellement celui qu'aurait donné la méthode (ii) sous l'hypothèse que les $\delta_{k_i}^-(q)$ sont tous nuls ; et le théorème de Riemann-Roch, sous la forme d'une version asymptotique de l'inégalité (2), implique qu'on ne peut pas faire mieux.

En revanche, pour les applications au partage de secret, en général r croît avec g, ce qui semble interdire l'usage de notre méthode, du moins sous ses formes les plus naïves.

1 Formules de Plücker

On donne une variante des formules de Plücker d'ordre 1 et 2 adaptée à nos besoins (on appellera ici formule de Plücker toute estimation sur le nombre de points en lesquels la suite des sauts de Weierstrass d'un diviseur, jusqu'à un ordre donné, diffère de son comportement générique ; pour une version plus générale, voir par exemple [19]).

Ce premier lemme correspond à l'ordre 1 :

Lemme 1. *Soient X une courbe de genre g sur un corps K, et $\mathcal{S} \subset X(K)$ un ensemble de points de X.*

a) Soit A un diviseur K-rationnel sur X tel que

$$i(A) = l(A) - (\deg A + 1 - g) \geq 1. \tag{4}$$

Supposons que pour tout $P \in \mathcal{S}$ on ait $l(A + P) > l(A)$. Alors

$$|\mathcal{S}| \leq g - l(A). \tag{5}$$

(Si $\deg A = -1$ on a aussi $|\mathcal{S}| \leq 1$.)

b) Soit B un diviseur K-rationnel sur X tel que

$$l(B) \geq 1. \tag{6}$$

Supposons que pour tout $P \in \mathcal{S}$ on ait $l(B - P) > l(B) - 1$. Alors

$$|\mathcal{S}| \leq \deg B + 1 - l(B). \tag{7}$$

(Si $\deg B = 2g - 1$ on a aussi $|\mathcal{S}| \leq 1$.)

Démonstration. C'est un résultat classique : pour a), voir par exemple [25], lemme 10 ; et b) lui est équivalent par Riemann-Roch (poser $A = \Omega - B$ où Ω est un diviseur canonique), mais on peut aussi le prouver directement : les hypothèses impliquent que $l(B') = l(B)$, où $B' = B - \sum_{P\in\mathcal{S}} P$, de sorte que $l(B) = l(B') \leq 1 + \deg B' = 1 + \deg B - |\mathcal{S}|$, d'où la conclusion.

(Si $\deg B = 2g-1$, on a $g \geq 1$ car $l(B) \geq 1$, et par ailleurs $l(B-P) > l(B)-1$ si et seulement si $B - P \sim \Omega$. Si on a aussi $l(B - P') > l(B) - 1$, alors $P' \sim P$, donc $P' = P$.) □

Le cœur technique de l'article est ce second lemme, qui correspond à l'ordre 2, et qui raffine le lemme 12 de [25].

Pour tout $q > 1$ et pour tout entier $n \geq 2$ on pose

$$\begin{aligned} G_q(n) &= \sum_{k=1}^{n-2} \frac{(q^{n-k}-1)(q^{n-k-1}-1)}{(q^n-1)(q^{n-1}-1)} \\ &= \frac{1}{q^2-1} - \frac{1-\frac{(q-1)n}{q^n-1}}{(q-1)(q^{n-1}-1)} \end{aligned} \tag{8}$$

(c'est une fonction croissante de n, car chacun des termes dans la somme qui la définit l'est, et qui tend vers $\frac{1}{q^2-1}$ à l'infini).

Alors :

Lemme 2. *Soient X une courbe de genre g sur un corps K, supposé* parfait, *et $\mathcal{S} \subset X(K)$ un ensemble de points de X.*

a) Soit A un diviseur K-rationnel sur X tel que $\deg A \geq -2$ *et*

$$i(A) = l(A) - (\deg A + 1 - g) \geq 2. \tag{9}$$

Supposons que pour tout $P \in \mathcal{S}$ on ait $l(A + 2P) > l(A)$. Alors

$$|\mathcal{S}| \;\leq\; 3g + 3 \;+\; \deg A \;-\; 3l(A). \tag{10}$$

Si de plus K est un corps fini $\mathbb{F}_q$, on a aussi

$$|\mathcal{S}| \leq \left(1 + \frac{q^{i(A)-2}-1}{q^{i(A)}-1}\right)^{-1} (6g - 6 \;-\; 2\deg A \;-\; 2\,G_q(i(A))\,|X(\mathbb{F}_q)|\,) \tag{11}$$

et plus généralement, pour tout entier w tel que $2 \leq w \leq i(A)$,

$$\begin{aligned} |\mathcal{S}| \leq (i(A) - w) + \left(1 + \frac{q^{w-2}-1}{q^w-1}\right)^{-1} (6g - 6 \;-\; 2\deg A \;-\; 4(i(A)-w) \\ -\; 2\,G_q(w)\,|X(\mathbb{F}_q)|\,). \end{aligned} \tag{12}$$

b) Soit B un diviseur K-rationnel sur X tel que $\deg B \leq 2g$ *et*

$$l(B) \geq 2. \tag{13}$$

Supposons que pour tout $P \in \mathcal{S}$ on ait $l(B-2P) > l(B)-2$. Alors

$$|\mathcal{S}| \ \leq \ 2\deg B \ + \ 2g+4 \ - \ 3l(B). \tag{14}$$

Si de plus K est un corps fini $\mathbb{F}_q$, on a aussi

$$|\mathcal{S}| \leq \left(1+\frac{q^{l(B)-2}-1}{q^{l(B)}-1}\right)^{-1} (2\deg B \ + \ 2g-2 \ - \ 2\,G_q(l(B))\,|X(\mathbb{F}_q)|\,) \tag{15}$$

et plus généralement, pour tout entier w tel que $2 \leq w \leq l(B)$,

$$|\mathcal{S}| \leq (l(B)-w) + \left(1+\frac{q^{w-2}-1}{q^{w}-1}\right)^{-1} (2\deg B \ + \ 2g-2 \ - \ 4(l(B)-w) \\ - \ 2\,G_q(w)\,|X(\mathbb{F}_q)|\,). \tag{16}$$

Démonstration. Remarquons que a) et b) sont équivalents, par Riemann-Roch. Il suffit donc de prouver b), et pour ce faire, on procède en six étapes.

Étape 1. Préliminaires et notations.

Par hypothèse, $\deg B \leq 2g$, et $l(B) \geq 2$ donc $\deg B \geq 1$, ce qui implique, par le théorème de Clifford,

$$l(B) \leq 1 + \frac{\deg B}{2}. \tag{17}$$

Pour tout $x \in \mathcal{L}(B) \setminus \{0\}$ on note $E_x = B + \operatorname{div} x \geq 0$. Si V est un sous-K-espace vectoriel non nul de $\mathcal{L}(B)$, on définit son lieu base E_V comme le pgcd des E_x pour $x \in V \setminus \{0\}$; de façon équivalente, E_V est le plus grand diviseur tel que $V \subset \mathcal{L}(B-E_V) \subset \mathcal{L}(B)$. Alors V définit un morphisme $\phi_V : X \longrightarrow \mathbb{P}^{\dim V-1}$ de degré $\deg B - \deg E_V$.

Étape 2. Réduction au cas séparable. On montre le résultat suivant (voir aussi le début de la preuve de [25], lemme 12) :

Soit $V \subset \mathcal{L}(B)$ de dimension $\dim V \geq 2$. Alors il existe $V' \subset \mathcal{L}(B)$ de dimension $\dim V' = 2$ tel que $\phi_{V'} : X \longrightarrow \mathbb{P}^1$ soit séparable et $E_{V'} \geq E_V$.

En effet, remarquons tout d'abord que quitte à remplacer V par un sous-espace (ce qui ne peut que faire augmenter E_V), on peut supposer $\dim V = 2$.

Si maintenant K est de caractéristique nulle, ou plus généralement si ϕ_V est déjà séparable, il n'y a rien à montrer (on prend $V' = V$). Supposons donc K de caractéristique $p > 0$, et ϕ_V de degré d'inséparabilité $p^m > 1$. Choisissons une base $x, y \in V$ et posons $f = y/x \in K(X)$. Dans l'équivalence de catégories entre courbes algébriques et corps de fonctions, ϕ_V est le morphisme associé à l'inclusion $K(f) \subset K(X)$, de degré d'inséparabilité p^m. Puisque K est supposé parfait, cela signifie qu'on peut écrire $f = g^{p^m}$ avec $K(g) \subset K(X)$ séparable.

Par hypothèse $\operatorname{div} x, \operatorname{div} y \geq -B$, donc

$$\operatorname{div} gx = \operatorname{div} x + \frac{1}{p^m}\operatorname{div} f = \left(1 - \frac{1}{p^m}\right)\operatorname{div} x + \frac{1}{p^m}\operatorname{div} y \geq -B. \tag{18}$$

Ainsi $gx \in \mathcal{L}(B)$, et on note $V' \subset \mathcal{L}(B)$ le sous-espace de base x, gx. Alors $\phi_{V'}$ est le morphisme associé à l'inclusion de corps de fonctions $K(g) \subset K(X)$, donc est bien séparable. Il ne nous reste plus qu'à montrer $E_{V'} \geq E_V$.

Par définition, $E_V = \operatorname{pgcd}(E_x, E_y)$. Posons donc $E_x = E_V + E'_x$ et $E_y = E_V + E'_y$, avec $E'_x, E'_y \geq 0$ étrangers. Alors $E_{gx} = E_V + \left(1 - \frac{1}{p^m}\right) E'_x + \frac{1}{p^m} E'_y$ donc

$$E_{V'} = \operatorname{pgcd}(E_x, E_{gx}) = E_V + \left(1 - \frac{1}{p^m}\right) E'_x \ \geq \ E_V \tag{19}$$

ce qu'il fallait démontrer.

Étape 3. Une formule générale. On montre :

Soient $V \subset \mathcal{L}(B)$ un sous-espace de dimension $\dim V \geq 2$, et E un diviseur sur X tel que $0 \leq E \leq E_V$. Alors

$$|\mathcal{S}| \ \leq \ 2\deg B \ + \ 2g - 2 \ - \ 2\deg E \ + \ |\mathcal{S} \cap \operatorname{Supp} E|. \tag{20}$$

Remarquons que la fonction $E \ \mapsto \ 2\deg B + 2g - 2 - 2\deg E + |\mathcal{S} \cap \operatorname{Supp} E|$ est une fonction décroissante de E. Il suffit donc de prouver (20) lorsque $E = E_V$. De plus, quitte à remplacer V par V' fourni par l'étape 2, on peut aussi supposer que $\dim V = 2$ et que $\phi_V : X \longrightarrow \mathbb{P}^1$ est séparable.

Notons R le diviseur de ramification de ϕ_V. Si $P \in \mathcal{S} \setminus \operatorname{Supp} E_V$ on a $V \not\subset \mathcal{L}(B - P)$, donc $l(B - P) = l(B) - 1$, et par ailleurs $l(B - 2P) > l(B) - 2$, d'où nécessairement

$$\mathcal{L}(B - 2P) = \mathcal{L}(B - P). \tag{21}$$

Si maintenant $t \in K(\mathbb{P}^1)$ est une uniformisante en $\phi_V(P)$, alors $\phi_V^* t$ s'annule en P, et par (21), son ordre d'annulation est au moins 2. Cela signifie que ϕ_V est ramifié en P, d'où

$$\deg R \geq |\mathcal{S} \setminus \operatorname{Supp} E_V|. \tag{22}$$

Par ailleurs la formule d'Hurwitz donne

$$2g - 2 = -2\deg \phi_V + \deg R \tag{23}$$

avec $\deg \phi_V = \deg B - \deg E_V$, d'où il découle (20).

Étape 4. Choix d'un sous-espace et preuve de (14)**.**

Si $l(B) = 2$, on prend $V = \mathcal{L}(B)$ et $E = 0$ dans (20), ce qui prouve (14) dans ce cas particulier.

Si par ailleurs $|\mathcal{S}| < l(B) - 2$, alors (14) est conséquence de (17).

On peut donc supposer $l(B) \geq 3$ et $|\mathcal{S}| \geq l(B) - 2$. Notons $P_1, \ldots, P_{|\mathcal{S}|}$ les éléments de $\mathcal{S}$, et posons

$$E = 2(P_1 + \cdots + P_{l(B)-2}). \tag{24}$$

Alors pour tout i on a $l(B-2P_i) \geq l(B)-1$, donc

$$l(B-E) \geq 2. \tag{25}$$

Ainsi en posant $V = \mathcal{L}(B-E)$ on satisfait aux hypothèses de (20), avec
- $\deg E = 2(l(B)-2)$
- $|\mathcal{S} \cap \operatorname{Supp} E| = l(B)-2$

ce qui donne bien (14).

Étape 5. Preuve de (15)**.**

On suppose maintenant $K = \mathbb{F}_q$.

Pour tout sous-espace $V \subset \mathcal{L}(B)$ de dimension $\dim V = 2$, et pour tout point $P \in X(\mathbb{F}_q)$, notons $\nu_{P,V} = v_P(E_V) \geq 0$ la multiplicité de P dans E_V, et posons

$$F_V = \sum_{P \in X(\mathbb{F}_q)} \nu_{P,V} P \tag{26}$$

de sorte que F_V est le plus grand diviseur de E_V supporté par $X(\mathbb{F}_q)$. Posons alors

$$d_V = 2\deg F_V - |\mathcal{S} \cap \operatorname{Supp} F_V| = \sum_{P \in X(\mathbb{F}_q)} 2\nu_{P,V} \; - \; |\{P \in \mathcal{S} \mid \nu_{P,V} \geq 1\}|. \tag{27}$$

En remarquant que

$$\sum_{P \in X(\mathbb{F}_q)} 2\nu_{P,V} = \sum_{P \in X(\mathbb{F}_q)} \left(2 \sum_{k \geq 1} \mathbf{1}_{\{\nu_{P,V} \geq k\}} \right) \tag{28}$$

et

$$|\{P \in \mathcal{S} \mid \nu_{P,V} \geq 1\}| = \sum_{P \in \mathcal{S}} \mathbf{1}_{\{\nu_{P,V} \geq 1\}} \tag{29}$$

on peut aussi écrire

$$\begin{aligned} d_V = & \sum_{P \in X(\mathbb{F}_q) \setminus \mathcal{S}} \left(2 \sum_{k \geq 1} \mathbf{1}_{\{\nu_{P,V} \geq k\}} \right) \\ & + \sum_{P \in \mathcal{S}} \left(\mathbf{1}_{\{\nu_{P,V} \geq 1\}} + 2 \sum_{k \geq 2} \mathbf{1}_{\{\nu_{P,V} \geq k\}} \right) \end{aligned} \tag{30}$$

On considère maintenant d_V et les $\nu_{P,V}$ comme des variables aléatoires, en supposant que V est tiré selon la loi de probabilité uniforme sur l'ensemble des sous-espaces de dimension 2 de $\mathcal{L}(B)$. La formule précédente permet alors de calculer l'espérance de d_V :

$$\begin{aligned} \mathbf{E}[d_V] = & \sum_{P \in X(\mathbb{F}_q) \setminus \mathcal{S}} \left(2 \sum_{k \geq 1} \mathbf{P}[\nu_{P,V} \geq k] \right) \\ & + \sum_{P \in \mathcal{S}} \left(\mathbf{P}[\nu_{P,V} \geq 1] + 2 \sum_{k \geq 2} \mathbf{P}[\nu_{P,V} \geq k] \right). \end{aligned} \tag{31}$$

Remarquons que, par définition de E_V, on a l'équivalence :

$$\nu_{P,V} \geq k \qquad \Longleftrightarrow \qquad V \subset \mathcal{L}(B - kP). \tag{32}$$

Puisque le nombre de sous-espaces de dimension 2 dans un espace de dimension d est $\frac{(q^d-1)(q^{d-1}-1)}{(q^2-1)(q-1)}$, ceci donne

$$\begin{aligned} \mathbf{P}[\nu_{P,V} \geq k] &= \frac{(q^{l(B-kP)}-1)(q^{l(B-kP)-1}-1)}{(q^{l(B)}-1)(q^{l(B)-1}-1)} \\ &= g_q(\, l(B),\; l(B) - l(B-kP)\,) \end{aligned} \tag{33}$$

où la fonction

$$g_q(x,y) = \frac{(q^{x-y}-1)(q^{x-y-1}-1)}{(q^x-1)(q^{x-1}-1)} \tag{34}$$

est croissante en x (pour $x \geq 2$) et décroissante en y (pour $0 \leq y < x$). Pour tout $P \in X(\mathbb{F}_q)$ et tout $k \geq 1$ on a $l(B) - l(B-kP) \leq k$, de sorte que

$$\mathbf{P}[\nu_{P,V} \geq k] \geq g_q(l(B), k), \tag{35}$$

et si en outre $P \in \mathcal{S}$ et $k \geq 2$, on a alors même $l(B) - l(B-kP) \leq k-1$, d'où dans ce cas :

$$\mathbf{P}[\nu_{P,V} \geq k] \geq g_q(l(B), k-1). \tag{36}$$

Reportant tout ceci dans (31) on trouve

$$\begin{aligned} \mathbf{E}[d_V] &\geq (|X(\mathbb{F}_q)| - |\mathcal{S}|) \sum_{k=1}^{l(B)-2} 2\, g_q(l(B),k) \\ &\qquad + |\mathcal{S}| \left(g_q(l(B),1) + \sum_{k=2}^{l(B)-1} 2\, g_q(l(B),k-1) \right) \\ &= |X(\mathbb{F}_q)| \sum_{k=1}^{l(B)-2} 2\, g_q(l(B),k) \;+\; |\mathcal{S}|\, g_q(l(B),1) \end{aligned} \tag{37}$$

soit

$$\mathbf{E}[d_V] \geq 2\, G_q(l(B))\, |X(\mathbb{F}_q)| \;+\; \frac{q^{l(B)-2}-1}{q^{l(B)}-1}\, |\mathcal{S}|. \tag{38}$$

Puisque cette inégalité est vraie en moyenne, il existe au moins un V pour lequel elle est vérifiée. Choisissons donc un tel V, et appliquons (20) avec $E = F_V$. On trouve alors

$$\begin{aligned} |\mathcal{S}| \;&\leq\; 2 \deg B \;+\; 2g - 2 \;-\; d_V \\ &\leq\; 2 \deg B \;+\; 2g - 2 \;-\; 2\, G_q(l(B))\, |X(\mathbb{F}_q)| \;-\; \frac{q^{l(B)-2}-1}{q^{l(B)}-1}\, |\mathcal{S}| \end{aligned} \tag{39}$$

ce qui donne bien (15).

Étape 6. Preuve de (16)**.**

Soit maintenant w un entier tel que $2 \leq w \leq l(B)$.

Commençons par montrer que le second terme de la somme dans (16) est positif :

$$2\deg B \,+\, 2g-2 \,-4(l(B)-w) \,-\, 2\,G_q(w)\,|X(\mathbb{F}_q)| \;\geq\; 0. \tag{40}$$

En effet, par (17) on a $2\deg B - 4l(B) \geq -4$, par hypothèse on a $w \geq 2$ donc $4w \geq 8$, tandis que $G_q(w) \leq \frac{1}{q^2-1}$, et $|X(\mathbb{F}_q)| \leq q+1+2g\sqrt{q}$ par la borne de Weil. La quantité qui nous intéresse est donc minorée par $2g+2-2\frac{q+1+2g\sqrt{q}}{q^2-1} = 2g(1-\frac{2\sqrt{q}}{q^2-1}) + 2(1-\frac{1}{q-1})$, ce qui est bien positif, puisque $q \geq 2$.

On en déduit que, si w est choisi de façon que $|\mathcal{S}| \leq l(B)-w$, alors (16) est bien vérifiée.

Supposons donc maintenant $|\mathcal{S}| > l(B)-w$.

Notant toujours $P_1, \ldots, P_{|\mathcal{S}|}$ les éléments de $\mathcal{S}$, on pose

$$B' = B - 2(P_1 + \cdots + P_{l(B)-w}) \tag{41}$$

et

$$\mathcal{S}' = \{P_{l(B)-w+1}, \ldots, P_{|\mathcal{S}|}\}. \tag{42}$$

On a alors $l(B') \geq w \geq 2$, et $l(B'-2P) > l(B')-2$ pour tout $P \in \mathcal{S}'$. Appliquant (15) à B' et $\mathcal{S}'$, on trouve alors

$$\begin{aligned}
|\mathcal{S}'| &= |\mathcal{S}| - (l(B)-w) \\
&\leq \left(1+\frac{q^{l(B')-2}-1}{q^{l(B')}-1}\right)^{-1} (2\deg B' \,+\, 2g-2 \,-\, 2\,G_q(l(B'))\,|X(\mathbb{F}_q)|\,) \\
&\leq \left(1+\frac{q^{w-2}-1}{q^{w}-1}\right)^{-1} (2\deg B - 4l(B) + 4w \,+\, 2g-2 \,-\, 2G_q(w)|X(\mathbb{F}_q)|)
\end{aligned} \tag{43}$$

ce qu'il fallait démontrer. □

Remarque 3. En caractéristique nulle on pourrait généraliser ces résultats à un ordre quelconque s, en montrant que pour tout diviseur A de degré $\deg A \geq -s$ tel que $i(A) \geq s$, le nombre de points P tels que $l(A+sP) > l(A)$ est majoré essentiellement par $s^2 g$. Ces points sont en effet ceux où un certain wronskien s'annule, et la majoration est donnée par le degré du faisceau inversible dont ce wronskien est une section.

Comme expliqué dans la remarque finale de [25], cela n'est pas vrai cependant en caractéristique positive dès lors que $s \geq 3$. En effet, pour que le raisonnement indiqué ci-dessus soit valable, il faut s'assurer que ce wronskien n'est pas identiquement nul. Pour $s = 2$, ceci est rendu possible par l'étape 2 de la preuve, qui ne se généralise pas à l'ordre supérieur.

Ceci peut s'interpréter, en termes de théorie des sauts de Weierstrass, par l'existence, en caractéristique positive, de diviseurs dont la suite des invariants

d'Hermite générique ([19][31]) commence bien par $\epsilon_0 = 0$ et $\epsilon_1 = 1$ (ce qui équivaut au résultat de séparabilité prouvé à l'étape 2), mais vérifie $\epsilon_{s-1} > s-1$ pour $s \geq 3$. De tels diviseurs sont "rares" ([22]), mais pour les applications qu'on a en vue par la suite, il n'est pas clair qu'on puisse les éviter.

2 Construction de diviseurs ordinaires

Définition 4. *Soit X une courbe de genre $g \geq 1$ sur un corps K. On dit qu'un diviseur D sur X est* ordinaire *s'il vérifie*

$$l(D) = \max(0, \deg D + 1 - g), \tag{44}$$

autrement dit, $l(D) = 0$ si $\deg D \leq g-1$, et $l(D) = \deg D + 1 - g$ si $\deg D \geq g-1$.

Dans le cas contraire on dit que D est exceptionnel.

On remarque que ces propriétés ne dépendent que de la classe d'équivalence linéaire de D. De plus, D est ordinaire (resp. exceptionnel) si et seulement si $\Omega - D$ l'est, où Ω est un diviseur canonique. En fait, D est exceptionnel si et seulement si D et $\Omega - D$ sont tous les deux spéciaux (ce qui implique $0 \leq \deg D \leq 2g-2$). Si $0 \leq d \leq g-1$, les classes de diviseurs exceptionnels de degré d sont paramétrées par la sous-variété $W_d \subset J$ introduite au début de ce texte.

On s'intéresse ici au problème suivant :

Problème III. *Soient X une courbe algébrique sur un corps K, et $r \geq 1$ un entier. Étant donnés des entiers $s_1, \ldots, s_r \geq 1$, des diviseurs K-rationnels $T_1, \ldots, T_r$ sur X, et un entier $d \in \mathbb{Z}$, construire un diviseur K-rationnel D sur X de degré $\deg D = d$, tel que les diviseurs $s_1 D - T_1, \ldots, s_r D - T_r$ soient ordinaires.*

Indiquons comment le problème I peut se ramener à ce problème III. Dans le problème I, on se donne des entiers $k_1, \ldots, k_r$, positifs ou négatifs, et on veut trouver un diviseur D de degré d tel que

$$l(k_1 D - G_1) = \cdots = l(k_r D - G_r) = 0. \tag{45}$$

Une condition nécessaire sur d pour que ce soit possible est donnée par (2), et peut se traduire en

$$\max_{k_i<0} \left\lceil \frac{g-1+n_i}{k_i} \right\rceil = d^- \ \leq \ d \ \leq \ d^+ = \min_{k_i>0} \left\lfloor \frac{g-1+n_i}{k_i} \right\rfloor \tag{46}$$

où $n_i = \deg G_i$.

Ainsi, une condition nécessaire pour que le problème I soit résoluble est que

$$d^- \leq d^+. \tag{47}$$

Supposons cette condition vérifiée, et choisissons d vérifiant (46). Posons :

– $s_i = k_i$ et $T_i = G_i$ si $k_i > 0$
– $s_i = -k_i$ et $T_i = -\Omega - G_i$ si $k_i < 0$

où, comme précédemment, Ω est un diviseur canonique sur X.

Supposons alors qu'on trouve D de degré $\deg D = d$ solution du problème III pour ces choix de s_i et T_i. Ainsi, tous les $s_i D - T_i$ sont supposés ordinaires. Alors :

– si $k_i > 0$, on a $\deg(s_i D - T_i) \leq g - 1$ par (46), donc $l(s_i D - T_i) = 0$, donc $l(k_i D - G_i) = 0$
– si $k_i < 0$, on a $\deg(s_i D - T_i) \geq g - 1$ par (46), donc $l(s_i D - T_i) = \deg(s_i D - T_i) + 1 - g$, d'où par Riemann-Roch $l(k_i D - G_i) = 0$.

Ainsi D est bien solution du problème I.

On explique maintenant comment résoudre le problème III lorsque K est parfait, que les s_i valent 1 ou 2, et que X a suffisamment de points (on supposera toujours $g \geq 1$).

On introduit deux fonctions $f_{1,X}$ et $f_{2,X}$ définies sur $\mathbb{Z}$, comme suit. Tout d'abord,

$$f_{1,X}(a) = \begin{cases} 1 & \text{si } a = -1 \\ g & \text{si } 0 \leq a \leq g-2 \\ 0 & \text{sinon.} \end{cases} \tag{48}$$

La définition de $f_{2,X}$ est un peu plus compliquée. On pose

$$f_{2,X}(g-2) = g \tag{49}$$

puis, si $-2 \leq a \leq g-3$ et que $K = \mathbb{F}_q$ est un corps fini :

$$f_{2,X}(a) = \min_{2 \leq w \leq g-1-a} \Big\lfloor (g-1-a-w) + \left(1 + \frac{q^{w-2}-1}{q^w - 1}\right)^{-1} (2g-2+2a+4w - 2G_q(w)|X(\mathbb{F}_q)|) \Big\rfloor \tag{50}$$

ou bien, si $-2 \leq a \leq g-3$ et que K est infini :

$$f_{2,X}(a) = 3g + 3 + a, \tag{51}$$

et enfin $f_{2,X}(a) = 0$ si $a < -2$ ou $a > g-2$.

Lemme 5. *Avec les notations qui précèdent, soient A un diviseur sur X et $\mathcal{S} \subset X(K)$ un ensemble de points. Soit aussi $s \in \{1, 2\}$. On suppose que A est ordinaire, mais que $A + sP$ est exceptionnel pour tout $P \in \mathcal{S}$. Alors*

$$|\mathcal{S}| \leq f_{s,X}(\deg A). \tag{52}$$

Démonstration. On pose $a = \deg A$, et on distingue selon que $s = 1$ ou $s = 2$.

(i) Supposons $s = 1$.
– Si $a \leq -2$ ou $a \geq 2g-2$, alors $A + P$ est toujours ordinaire, donc $\mathcal{S}$ est vide, et on a bien $f_{1,X}(a) = 0$.

- Si $g-1 \leq a \leq 2g-3$, alors A ordinaire signifie $l(A) = a+1-g$, donc $A+P$ est ordinaire par Riemann-Roch, et on conclut de même.
- Si $-1 \leq a \leq g-2$, alors A ordinaire signifie $l(A) = 0$, et $A+P$ exceptionnel signifie $l(A+P) = 1$. On conclut grâce au lemme 1.a.

(ii) Supposons $s = 2$.
- Si $a \leq -3$ ou $a \geq 2g-1$, alors $A+2P$ est toujours ordinaire, donc $\mathcal{S}$ est vide, et on a bien $f_{2,X}(a) = 0$.
- Si $g-1 \leq a \leq 2g-2$, alors A ordinaire signifie $l(A) = a+1-g$, donc $A+2P$ est ordinaire par Riemann-Roch, et on conclut de même.
- Si $a = g-2$, alors A ordinaire signifie $l(A) = 0$, et $A+2P$ exceptionnel signifie $l(A+2P) = 2$, donc $l(A+P) = 1$. Le lemme 1.a donne alors bien $|\mathcal{S}| \leq g = f_{2,X}(a)$.
- Enfin si $-2 \leq a \leq g-3$, alors A ordinaire signifie $l(A) = 0$, et $A+2P$ exceptionnel signifie $l(A+2P) \geq 1$. On conclut alors grâce au lemme 2.a, (en remarquant notamment, dans (12), qu'ici $i(A) = g-1-a$).

□

Proposition 6. *Soient X une courbe de genre g sur un corps K parfait, et $r \geq 1$ un entier. On suppose donnés des entiers $s_1, \ldots, s_r \in \{1,2\}$, des diviseurs K-rationnels $T_1, \ldots, T_r$ sur X, et un entier $d \in \mathbb{Z}$. On notera $t_i = \deg T_i$. Soit aussi D_0 un diviseur K-rationnel sur X, de degré $\deg D_0 = d_0 \leq d$, tel que les $s_i D_0 - T_i$ soient ordinaires (c'est vrai par exemple si $d_0 \leq \min_i \left\lfloor \frac{t_i - 1}{s_i} \right\rfloor$). Soit enfin $\mathcal{S} \subset X(K)$ un ensemble de points tel que*

$$|\mathcal{S}| > \max_{d_0 \leq d' < d} \sum_{i=1}^{r} f_{s_i,X}(s_i d' - t_i). \tag{53}$$

Alors il existe un diviseur K-rationnel D sur X, de degré $\deg D = d$, tel que les $s_i D - T_i$ soient ordinaires. De plus on peut choisir D de façon que $D - D_0$ soit effectif et à support dans $\mathcal{S}$.

Démonstration. On construit D de proche en proche. Soit d' tel que $d_0 \leq d' < d$, et supposons construit D' de degré de degré $\deg D' = d'$, tel que les $s_i D' - T_i$ soient ordinaires, et tel que $D' - D_0$ soit effectif et à support dans $\mathcal{S}$. Le lemme 5 appliqué avec $s = s_i$ et $A = s_i D' - T_i$ montre qu'il y a au plus $f_{s_i,X}(s_i d' - t_i)$ points tels que $s_i(D'+P) - T_i$ soit exceptionnel. Grâce à (53), on peut donc trouver $P \in \mathcal{S}$ tel que les $s_i(D'+P) - T_i$ soient ordinaires, et par construction $(D'+P) - D_0$ est encore effectif et à support dans $\mathcal{S}$. On conclut alors par récurrence sur d'. □

Remarque 7. La restriction imposée aux s_i de valoir 1 ou 2 résulte des particularités de la caractéristique positive indiquées dans la remarque 3. En caractéristique nulle, on pourrait donc énoncer une variante de la proposition 6 valable sans restriction sur les s_i. Pour les applications auxquelles on s'intéresse ici, cela n'est cependant pas nécessaire.

Pour la suite il pourra être utile de préciser quelques propriétés des $f_{s,X}$.

Le corps K étant donné, pour tout réel ν on introduit deux fonctions $\phi_{1,\nu}$ et $\phi_{2,\nu}$ définies sur $\mathbb{R}$, comme suit :

$$\phi_{1,\nu}(\alpha) = \begin{cases} 1 & \text{si } 0 \leq \alpha \leq 1 \\ 0 & \text{si } \alpha < 0 \text{ ou } \alpha > 1 \end{cases} \tag{54}$$

et

$$\phi_{2,\nu}(\alpha) = \begin{cases} \frac{3q^2+1}{q^2+1} + \frac{q^2-1}{q^2+1}\alpha - \frac{2q^2}{q^4-1}\nu & \text{si } 0 \leq \alpha < 1 \text{ et } |K| = q < +\infty \\ 3+\alpha & \text{si } 0 \leq \alpha < 1 \text{ et } K \text{ infini} \\ 4 & \text{si } \alpha = 1 \\ 0 & \text{si } \alpha < 0 \text{ ou } \alpha > 1 \end{cases} \tag{55}$$

(remarquons que l'expression pour K infini peut s'obtenir comme limite du cas fini quand $q \longrightarrow \infty$).

Lemme 8. *Avec les notations précédentes, soit $s \in \{1, 2\}$.*

a) Pour toute courbe X sur K, la fonction $f_{s,X}(a)$ est une fonction croissante de a pour $a \leq g - 1 - s$.
Son maximum sur $\mathbb{Z}$ est $f_{s,X}(g-1-s) = s^2 g$.

b) Soient α et ν deux réels, avec $\alpha \notin \{0, 1\}$. Pour tout entier $j \geq 1$, on se donne une courbe $X^{(j)}$ de genre $g^{(j)}$ sur K, et un entier $a^{(j)} \in \mathbb{Z}$. On suppose que, lorsque j tend vers l'infini, on a $g^{(j)} \longrightarrow \infty$, et :
– $\frac{a^{(j)}}{g^{(j)}} \longrightarrow \alpha$
– $\liminf \frac{|X^{(j)}(K)|}{g^{(j)}} \geq \nu$.
Alors, quand j tend vers l'infini,

$$\limsup \frac{f_{s,X^{(j)}}(a^{(j)})}{g^{(j)}} \leq \phi_{s,\nu}(\alpha). \tag{56}$$

Démonstration. Pour a), le seul point non trivial est la croissance de $f_{2,X}$ sur l'intervalle $-2 \leq a \leq g-3$ lorsque $|K| = q < \infty$. Sous cette hypothèse, posons

$$\widetilde{f_{2,X}}(a,w) = (g-1-a-w) + \left(1 + \frac{q^{w-2}-1}{q^w-1}\right)^{-1} (2g-2+2a+4w-2G_q(w)|X(\mathbb{F}_q)|) \tag{57}$$

de sorte que $f_{2,X}(a) = \min_{2 \leq w \leq g-1-a} \lfloor \widetilde{f_{2,X}}(a,w) \rfloor$.

Pour $w \geq 2$, on a $\frac{q^{w-2}-1}{q^w-1} \leq \frac{1}{q^2}$, d'où $\left(1 + \frac{q^{w-2}-1}{q^w-1}\right)^{-1} \geq 1 - \frac{1}{q^2+1}$, de sorte qu'à w fixé, $\widetilde{f_{2,X}}(a,w)$ est fonction croissante de a. On conclut alors en passant au min sur w.

De même pour b), le seul cas non trivial est celui où $s = 2$ et $0 \leq \alpha < 1$, avec $|K| = q < \infty$. On se placera donc sous cette hypothèse.

Puisque $\frac{a^{(j)}}{g^{(j)}} \longrightarrow \alpha < 1$ on peut, pour tout j assez grand, choisir un entier $w^{(j)}$ vérifiant $2 \leq w^{(j)} \leq g^{(j)} - 1 - a^{(j)}$, et de façon que :

– $w^{(j)} \longrightarrow \infty$
– $\frac{w^{(j)}}{g^{(j)}} \longrightarrow 0$.

Alors $\frac{q^{w^{(j)}-2}-1}{q^{w^{(j)}}-1} \longrightarrow \frac{1}{q^2}$ et $G_q(w^{(j)}) \longrightarrow \frac{1}{q^2-1}$, et en remplaçant dans (57),

$$\limsup \frac{\widetilde{f_{2,X^{(j)}}}(a^{(j)}, w^{(j)})}{g^{(j)}} \leq 1 - \alpha + \left(1 - \frac{1}{q^2+1}\right)\left(2 + 2\alpha - 2\frac{\nu}{q^2-1}\right). \quad (58)$$

On conclut alors puisque $\limsup \frac{f_{2,X^{(j)}}(a^{(j)})}{g^{(j)}} \leq \limsup \frac{\widetilde{f_{2,X^{(j)}}}(a^{(j)},w^{(j)})}{g^{(j)}}$. □

Grâce à ce lemme on pourrait, si on le souhaitait, énoncer une version "asymptotique" de la proposition précédente. Cependant, le faire de façon optimale nécessiterait, dans le cas général, une distinction de cas assez fastidieuse liée aux discontinuités des $\phi_{s,\nu}$ en 0 et 1. On se contentera donc de le faire dans le cadre des deux applications qui nous intéressent, à savoir la construction de codes linéaires intersectants ($r = 1$ et $s_1 = 2$), et celle d'algorithmes de multiplication dans les corps finis de faible complexité bilinéaire ($r = 2$ et $s_1 = 1$, $s_2 = 2$).

Comme indiqué dans l'introduction, le cas des systèmes de partage de secret avec propriété de multiplication semble en revanche moins bien s'y prêter (r variable).

3 Application aux codes linéaires intersectants

On commence par rappeler quelques définitions et résultats de [24][25][36].

Un code linéaire intersectant de paramètres $[n, k]$ sur un corps K est un sous-espace vectoriel $C \subset K^n$ de dimension k tel que, pour tous $c, c' \in C$ non nuls, les supports de c et c' s'intersectent (*i.e.* il existe i tel que $c_i c'_i \neq 0$).

On note R_K le rendement asymptotique maximal, c'est-à-dire la lim sup du rapport k/n, qu'un tel code peut atteindre. Si $K = \mathbb{F}_q$, on notera aussi R_q pour $R_{\mathbb{F}_q}$.

Soit X une courbe de genre g sur un corps K. Soient $P_1, \ldots, P_n \in X(K)$ des points de X, deux à deux distincts, et pour chaque i, soit z_i une uniformisante en P_i. On notera G la donnée de ces P_i et z_i (par abus de notation, on écrira aussi parfois $G = P_1 + \cdots + P_n$, le diviseur sur X somme des P_i). Alors :

Définition 9. *Pour tout diviseur K-rationnel D sur X, le code de Goppa généralisé $C(G, D) \subset K^n$ est l'image de l'application d'évaluation*

$$\begin{array}{rccc} \mathrm{ev}_{G,D} : & \mathcal{L}(D) & \longrightarrow & K^n \\ & f & \mapsto & ((z_1^{\nu_1} f)(P_1), \ldots, (z_n^{\nu_n} f)(P_n)) \end{array} \quad (59)$$

où $\nu_i = v_{P_i}(D)$ est la valuation de D en P_i.

Lorsque D varie, la collection des $\mathrm{ev}_{G,D}$ définit un morphisme de K-algèbres

$$\mathrm{ev}_G : \bigoplus_{D \in \mathrm{Div}_{\mathbb{F}_q}(X)} \mathcal{L}(D) \longrightarrow K^n, \quad (60)$$

où $\bigoplus_D \mathcal{L}(D)$ est munie de sa structure de K-algèbre graduée provenant de la multiplication dans le corps de fonctions $K(X)$, et où K^n est muni de la multiplication composante par composante.

De façon plus concrète, pour tous diviseurs D et D', le diagramme

$$\begin{array}{ccc} \mathcal{L}(D) \times \mathcal{L}(D') & \xrightarrow{\mathrm{ev}_{G,D} \times \mathrm{ev}_{G,D'}} & K^n \times K^n \\ \downarrow & & \downarrow \\ \mathcal{L}(D+D') & \xrightarrow{\mathrm{ev}_{G,D+D'}} & K^n \end{array} \tag{61}$$

commute, envoyant $(f, f') \in \mathcal{L}(D) \times \mathcal{L}(D')$ sur

$$((z_1^{\nu_1+\nu_1'} f f')(P_1), \ldots, (z_n^{\nu_n+\nu_n'} f f')(P_n)) \in K^n \tag{62}$$

(où $\nu_i = v_{P_i}(D)$ et $\nu_i' = v_{P_i}(D')$).

Alors :

Proposition 10 (critère de Xing, [36] Th. 3.5, ou [25] Th. 7)**.** *Avec les notations qui précèdent, supposons* $\deg D < n = \deg G$ *et*

$$l(2D - G) = 0. \tag{63}$$

Alors $C(G, D) \subset K^n$ *est un code linéaire intersectant, de dimension* $l(D)$*.*

La preuve résulte de la commutativité du diagramme (61), avec $D' = D$, et du fait que $\ker \mathrm{ev}_{G,2D} = \mathcal{L}(2D - G)$. Pour plus de détails, voir par exemple [25].

On en déduit :

Proposition 11. *Soient* X *une courbe de genre* g *sur un corps* K*, supposé parfait,* $\mathcal{S} \subset X(K)$ *un ensemble de points de* X*, et* n *un entier naturel tel que* $g \leq n \leq |X(K)|$*. Soit* d *un entier naturel vérifiant*

$$d \leq \frac{n + g - 1}{2} \tag{64}$$

et

$$|\mathcal{S}| > f_{2,X}(2d - 2 - n). \tag{65}$$

Alors il existe des diviseurs D *de degré* d*, à support dans* $\mathcal{S}$*, et* G *de degré* n *sur* X*, tels que le code* $C = C(G, D) \subset K^n$ *soit intersectant et de dimension* $\dim C \geq d + 1 - g$*.*

En particulier, si $|X(K)| > 4g$*, il existe un code linéaire intersectant* $C \subset K^n$ *de dimension* $\dim C \geq \left\lfloor \frac{n+g-1}{2} \right\rfloor + 1 - g \geq \frac{n-g}{2}$*.*

Démonstration. Choisissons $P_1, \ldots, P_n \in X(K)$ deux à deux distincts, avec $P_1 \in \mathcal{S}$, et appliquons la proposition 6 avec $r = 1$, $s_1 = 2$, $T_1 = G = P_1 + \cdots + P_n$, $d_0 = \left\lfloor \frac{n-1}{2} \right\rfloor$, $D_0 = d_0 P_1$. Le lemme 8.a et (65) impliquent que (53) est vérifiée, et on en déduit l'existence d'un diviseur D de degré d à support dans $\mathcal{S}$ tel que $2D - G$ soit ordinaire. Alors par (64) on a $2d - n \leq g - 1$ donc $l(2D - G) = 0$,

et aussi $d < n$, et le critère de Xing montre que le code $C(G, D)$ vérifie les conditions demandées.

La dernière assertion résulte du fait que $f_{2,X}(g-3) = 4g$, de sorte qu'on peut prendre $\mathcal{S} = X(K)$ et $d = \lfloor \frac{n+g-1}{2} \rfloor$. □

Corollaire 12. *Soient K un corps parfait, et $\nu > 1$ un réel. Pour tout entier $j \geq 1$, on se donne une courbe $X^{(j)}$ de genre $g^{(j)}$ sur K, et on suppose que, lorsque j tend vers l'infini, on a $g^{(j)} \longrightarrow \infty$ et*

$$\liminf \frac{|X^{(j)}(K)|}{g^{(j)}} \geq \nu. \tag{66}$$

Alors pour j assez grand, il existe des diviseurs $D^{(j)}$ et $G^{(j)}$ sur $X^{(j)}$ tels que le code $C(G^{(j)}, D^{(j)})$ soit intersectant de paramètres $[n^{(j)}, k^{(j)}]$ avec, lorsque j tend vers l'infini, $\frac{n^{(j)}}{g^{(j)}} \longrightarrow \nu$ et

$$\liminf \frac{k^{(j)}}{n^{(j)}} \geq \min\left(1 - \frac{5}{2\nu}, \frac{1}{2} - \frac{1}{2\nu}\right). \tag{67}$$

Lorsque $|K| = q < +\infty$, cette dernière condition peut être améliorée en

$$\liminf \frac{k^{(j)}}{n^{(j)}} \geq \min\left(1 - \frac{5}{2\nu} + \frac{2 - \frac{2}{\nu} + \frac{1}{q^2-1}}{q^2-1}\,,\ \frac{1}{2} - \frac{1}{2\nu}\right). \tag{68}$$

Démonstration. Pour tout $\epsilon > 0$, posons $\nu_\epsilon = \nu - \epsilon$. Choisissons un tel ϵ suffisamment petit, de sorte que $\nu > \nu_\epsilon > \nu_{2\epsilon} > 1$.

Pour tout j suffisamment grand, choisissons un entier $n_\epsilon^{(j)}$, en faisant en sorte que $\frac{n_\epsilon^{(j)}}{g^{(j)}} \longrightarrow \nu_\epsilon$ lorsque j tend vers l'infini. Pour j assez grand on aura donc $g^{(j)} \leq n_\epsilon^{(j)} \leq |X^{(j)}(K)|$.

Soit δ_ϵ le plus grand réel vérifiant les inégalités

$$\delta_\epsilon \leq \frac{\nu_{2\epsilon} + 1}{2} \tag{69}$$

et

$$\nu_\epsilon \geq \phi_{2,\nu_\epsilon}(2\delta_\epsilon - \nu_\epsilon). \tag{70}$$

Autrement dit, si K est infini,

$$\delta_\epsilon = \min\left(\nu_\epsilon - \frac{3}{2}, \frac{\nu_{2\epsilon} + 1}{2}\right) \tag{71}$$

ou bien, si $|K| = q < +\infty$,

$$\delta_\epsilon = \min\left(\nu_\epsilon - \frac{3}{2} + \frac{2\nu_\epsilon - 2 + \frac{\nu_\epsilon}{q^2-1}}{q^2-1}\,,\ \frac{\nu_{2\epsilon} + 1}{2}\right). \tag{72}$$

Pour tout j suffisamment grand, choisissons un entier $d_\epsilon^{(j)}$, en faisant en sorte que $\frac{d_\epsilon^{(j)}}{g^{(j)}} \longrightarrow \delta_\epsilon$ lorsque j tend vers l'infini. Alors, pour j assez grand, on aura par (69) :

$$d_\epsilon^{(j)} \leq \frac{n_\epsilon^{(j)} + g^{(j)} - 1}{2} \tag{73}$$

et, par le lemme 8.b et (70) :

$$|X^{(j)}(K)| > f_{2,X^{(j)}}(2d_\epsilon^{(j)} - 2 - n_\epsilon^{(j)}). \tag{74}$$

On est donc en mesure d'appliquer la proposition précédente, ce qui nous fournit, pour j assez grand, un code linéaire intersectant $C_\epsilon^{(j)}$ de paramètres $[n_\epsilon^{(j)}, k_\epsilon^{(j)}]$, avec $k_\epsilon^{(j)} \geq d_\epsilon^{(j)} + 1 - g^{(j)}$. On trouve alors, pour j tendant vers l'infini :

$$\liminf \frac{k_\epsilon^{(j)}}{n_\epsilon^{(j)}} \geq \frac{\delta_\epsilon - 1}{\nu_\epsilon} = \min\left(1 - \frac{5}{2\nu_\epsilon}, \frac{1}{2}\frac{\nu_{2\epsilon}}{\nu_\epsilon} - \frac{1}{2\nu_\epsilon}\right) \tag{75}$$

si K est infini, tandis que si $|K| = q < +\infty$:

$$\liminf \frac{k_\epsilon^{(j)}}{n_\epsilon^{(j)}} \geq \frac{\delta_\epsilon - 1}{\nu_\epsilon} = \min\left(1 - \frac{5}{2\nu_\epsilon} + \frac{2 - \frac{2}{\nu_\epsilon} + \frac{1}{q^2-1}}{q^2-1}\,,\ \frac{1}{2}\frac{\nu_{2\epsilon}}{\nu_\epsilon} - \frac{1}{2\nu_\epsilon}\right). \tag{76}$$

Ceci étant vrai pour tout $\epsilon > 0$ assez petit, on conclut par un argument diagonal. □

Lorsque $|K| = q < +\infty$, on note $A(q)$ le plus grand réel tel qu'il existe une suite de courbes $X^{(j)}$ de genre $g^{(j)}$ sur K, avec $g^{(j)} \longrightarrow \infty$ et $\frac{|X^{(j)}(K)|}{g^{(j)}} \longrightarrow A(q)$ lorsque j tend vers l'infini.

On sait que $0 < A(q) \leq \sqrt{q} - 1$, et que l'inégalité de droite est une égalité au moins quand q est un carré ([15][18][34]).

Corollaire 13. *Si $A(q) \geq 4 - \frac{12q^2-4}{q^4+2q^2-1}$, on a*

$$R_q \geq \frac{1}{2} - \frac{1}{2A(q)}. \tag{77}$$

Démonstration. On applique le corollaire précédent avec $\nu = A(q)$ (en remarquant que la valeur critique $\nu = 4 - \frac{12q^2-4}{q^4+2q^2-1}$ est celle qui rend égaux les deux termes dans le min dans (68)). □

Ceci améliore le théorème 2 de [25], qui parvient à la même conclusion, mais sous l'hypothèse plus restrictive $A(q) > 8$.

On a essayé ici de tenir compte systématiquement de la finitude de K lorsque cela permettait d'affiner les estimations. On aurait pu s'en passer, ce qui aurait beaucoup simplifié les calculs, mais alors on aurait prouvé le corollaire seulement sous l'hypothèse $A(q) \geq 4$. Il n'est pas clair que ceci soit restrictif : existe-t-il

un q tel que $4 - \frac{12q^2-4}{q^4+2q^2-1} \leq A(q) < 4$? Si c'est le cas, il serait amusant d'en exhiber un.

D'un autre côté, si K est infini, la théorie développée ici est essentiellement superflue. L'ensemble $\mathbb{P}^1(K)$ étant infini, on montre facilement $R_K \geq \frac{1}{2}$ (et même, en fait, $R_K = \frac{1}{2}$) sans avoir besoin d'utiliser de courbes de genre supérieur.

4 Application à la complexité bilinéaire de la multiplication : la borne de Shparlinski-Tsfasman-Vladut

On commence par faire quelques rappels d'ordre général sur la complexité bilinéaire de la multiplication dans une extension de corps. Pour un survol plus complet de ces questions, on pourra consulter [8].

Fixons un corps K. Si $E_1, \ldots, E_s$ sont des K-espaces vectoriels de dimension finie, on définit le *rang tensoriel* d'un élément $t \in E_1 \otimes \cdots \otimes E_s$ comme la longueur minimale d'une décomposition de t en somme de tenseurs élémentaires.

Si $b : E_1 \times E_2 \longrightarrow E_3$ est une application K-bilinéaire, on définit la *complexité bilinéaire* de b comme le rang tensoriel de l'élément $\widetilde{b} \in E_1^\vee \otimes E_2^\vee \otimes E_3$ naturellement déduit de b.

Si L est une extension finie de K, on notera $\mu_K(L)$ la complexité bilinéaire de l'application de multiplication $L \times L \longrightarrow L$, considérée comme une application K-bilinéaire. Ainsi, plus concrètement, $\mu_K(L)$ est le plus petit entier n tel qu'il existe des formes linéaires $\phi_1, \ldots, \phi_n$ et $\psi_1, \ldots, \psi_n : L \longrightarrow K$, et des éléments $w_1, \ldots, w_n \in L$, tels que pour tous $x, y \in L$ on ait

$$xy = \phi_1(x)\psi_1(y)w_1 + \cdots + \phi_n(x)\psi_n(y)w_n. \tag{78}$$

Plus généralement, on appelle *algorithme de multiplication* de longueur n pour L/K la donnée d'une décomposition du type (78). Un tel algorithme est dit *symétrique* si $\phi_i = \psi_i$ pour tout i.

Un algorithme de multiplication (78) étant donné, on peut, suivant [17][20][35], lui associer deux codes linéaires C_ϕ et $C_\psi \subset K^n$, images des applications d'évaluation

$$\begin{array}{rccc} \phi : & L & \longrightarrow & K^n \\ & x & \mapsto & (\phi_1(x), \ldots, \phi_n(x)) \end{array} \quad \text{et} \quad \begin{array}{rccc} \psi : & L & \longrightarrow & K^n \\ & y & \mapsto & (\psi_1(y), \ldots, \psi_n(y)) \end{array} \tag{79}$$

respectivement. Le fait que L est une K-algèbre *intègre* implique, d'une part, que ces applications sont injectives, donc C_ϕ et C_ψ ont dimension $k = [L : K]$, et d'autre part, que pour tous $c \in C_\phi$ et $c' \in C_\psi$ non nuls, les supports de c et c' s'intersectent (en particulier, si l'algorithme est symétrique, $C_\phi = C_\psi$ est un *code linéaire intersectant* comme défini dans la section précédente). Ainsi, toute borne supérieure sur le rendement de telles paires de codes se traduit en une minoration de $\mu_K(L)$. Par exemple, on montre facilement par un argument

de projection que C_ϕ et C_ψ ont distance minimale au moins k, ce qui implique alors $n \geq 2k-1$ (borne de Singleton). Ainsi,

$$\mu_K(L) \geq 2[L:K] - 1. \tag{80}$$

Inversement, la méthode de Chudnovsky et Chudnovsky ([14], voir aussi ci-dessous) permet d'obtenir une majoration de $\mu_K(L)$ linéaire en $[L:K]$. Ceci motive l'introduction de constantes

$$m_K = \liminf_{[L:K]\to\infty} \frac{\mu_K(L)}{[L:K]} \qquad \text{et} \qquad M_K = \limsup_{[L:K]\to\infty} \frac{\mu_K(L)}{[L:K]}. \tag{81}$$

Le cas le plus intéressant est celui où $K = \mathbb{F}_q$ est un corps fini. On notera alors

$$\mu_q(k) = \mu_{\mathbb{F}_q}(\mathbb{F}_{q^k}), \tag{82}$$

et

$$m_q = m_{\mathbb{F}_q} = \liminf_{k\to\infty} \frac{\mu_q(k)}{k} \quad \text{et} \quad M_q = M_{\mathbb{F}_q} = \limsup_{k\to\infty} \frac{\mu_q(k)}{k}. \tag{83}$$

Conservant les notations de la section précédente, et notamment celles des applications d'évaluation généralisées $\mathrm{ev}_{G,D}$ et des codes $C(G,D)$, on peut maintenant énoncer :

Théorème 14 (Chudnovsky-Chudnovsky, [14]). *Soit X une courbe sur un corps K. On note G la donnée de points $P_1, \ldots, P_n \in X(K)$ deux à deux distincts (et d'une uniformisante en chaque P_i). On suppose qu'il existe un diviseur K-rationnel D sur X, et un point fermé Q de X hors du support de D, de corps résiduel $L = K(Q)$, tels que :*

a) l'application d'évaluation $\mathrm{ev}_{Q,D} : \mathcal{L}(D) \longrightarrow L$ est surjective

b) l'application d'évaluation $\mathrm{ev}_{G,2D} : \mathcal{L}(2D) \longrightarrow K^n$ est injective.

Alors il existe un algorithme de multiplication symétrique de longueur n pour L/K, et tel que le code intersectant $C_\phi = C_\psi$ associé soit un sous-code de $C(G,D)$. En particulier, $\mu_K(L) \leq n$.

Démonstration. Choisissons une section $\sigma : L \longrightarrow \mathcal{L}(D)$ de $\mathrm{ev}_{Q,D}$, posons

$$\phi = \mathrm{ev}_{G,D} \circ \sigma : L \longrightarrow K^n, \tag{84}$$

et notons ϕ_i les composantes de ϕ (et $\psi_i = \phi_i$). Par ailleurs, via b), étendons l'application d'évaluation $\mathrm{ev}_{Q,2D} : \mathcal{L}(2D) \longrightarrow L$ en une application K-linéaire $w : K^n \longrightarrow L$, et notons $w_1, \ldots, w_n \in L$ l'image par w des éléments de la base canonique de K^n. Alors, la commutativité du diagramme (61), avec $D' = D$, appliquée d'une part pour l'évaluation en G, et d'autre part pour l'évaluation en Q, montre que (78) est bien vérifiée : plus précisément, si $x, y \in L$ et $f = \sigma(x)$, $g = \sigma(y)$,

$$\begin{aligned} \phi_1(x)\phi_1(y)w_1 + \cdots + \phi_n(x)\phi_n(y)w_n &= w(\mathrm{ev}_{G,D}(f)\,\mathrm{ev}_{G,D}(g)) \\ &= w(\mathrm{ev}_{G,2D}(fg)) \\ &= \mathrm{ev}_{Q,2D}(fg) \\ &= \mathrm{ev}_{Q,D}(f)\,\mathrm{ev}_{Q,D}(g) = xy. \end{aligned} \tag{85}$$

Enfin on a bien $C_\phi \subset C(G,D)$ par (84). □

Proposition 15. *Soit X une courbe de genre g sur un corps K, munie de points K-rationnels $P_1, \ldots, P_n \in X(K)$ deux à deux distincts, et d'un point fermé Q de corps résiduel $L = K(Q)$ de degré $k = [L : K]$. Soit aussi D un diviseur K-rationnel sur X de degré $d = \deg D$, de support ne contenant pas Q, et tel que :*

a) $2D - G$ et $D - Q$ sont ordinaires

b) $2d - n \leq g - 1 \leq d - k$

où $G = P_1 + \cdots + P_n$ (avec notre abus de notation habituel). Alors X, G, D, Q vérifient les hypothèses du théorème 14, de sorte que $\mu_K(L) \leq n$.

Démonstration. Les hypothèses faites sur $2D - G$ et $D - Q$ signifient précisément :

$$l(2D - G) = 0 \tag{86}$$

et

$$l(D - Q) = \deg(D - Q) + 1 - g. \tag{87}$$

Alors $D \geq D - Q$ et (87) impliquent $l(D) = \deg(D) + 1 - g$. Par ailleurs, $\ker \mathrm{ev}_{Q,D} = \mathcal{L}(D - Q)$, de sorte que

$$\dim \mathrm{im}\, \mathrm{ev}_{Q,D} = l(D) - l(D - Q) = \deg(Q) = k, \tag{88}$$

donc $\mathrm{ev}_{Q,D}$ est bien surjective. Enfin, $\ker \mathrm{ev}_{G,2D} = \mathcal{L}(2D - G) = \{0\}$ par (86), donc $\mathrm{ev}_{G,2D}$ est bien injective. □

Corollaire 16. *Soit X une courbe de genre $g \geq 1$ sur un corps K parfait, munie d'un point fermé Q de corps résiduel $L = K(Q)$ de degré $k = [L : K] > 1$, et d'un ensemble de points rationnels $\mathcal{S} \subset X(K)$. Soit n un entier naturel tel que*

$$2k + g - 1 \leq n \leq |X(K)| \tag{89}$$

et

$$|\mathcal{S}| > g + f_{2,X}(2k + 2g - 4 - n). \tag{90}$$

Alors il existe des diviseurs D de degré $d = k + g - 1$, à support dans $\mathcal{S}$, et G de degré n sur X, tels que X, G, D, Q vérifient les hypothèses du théorème 14. En particulier, on a $\mu_K(L) \leq n$.

Démonstration. Choisissons $P_1, \ldots, P_n \in X(K)$ deux à deux distincts, avec $P_1 \in \mathcal{S}$, et appliquons la proposition 6 avec

- $r = 2$
- $s_1 = 1$
- $T_1 = Q, \ t_1 = k$
- $s_2 = 2$
- $T_2 = G = P_1 + \cdots + P_n, \ t_2 = n$
- $D_0 = d_0 P_1, \ d_0 = \min(k - 1, \lfloor \frac{n-1}{2} \rfloor)$
- $d = k + g - 1$.

Pour tout entier d' posons

$$f(d') = f_{1,X}(d'-k) + f_{2,X}(2d'-n). \tag{91}$$

La proposition 6 s'applique dès lors que, pour tout d' tel que $d_0 \leq d' < d$, on a

$$|\mathcal{S}| > f(d'). \tag{92}$$

Or par (90) on a $|\mathcal{S}| > g + f_{2,X}(2k+2g-4-n) = f(d-1)$, donc par le lemme 8.a, (92) est bien vraie pour tout $d' < d$.

La proposition 6 fournit alors D de degré d, à support dans $\mathcal{S}$, tel que $2D-G$ et $D-Q$ soient ordinaires. Puisque $k > 1$, le support de D ne rencontre pas Q. Enfin, par (89), on a $2d - n \leq g - 1 = d - k$, et on peut alors conclure grâce à la proposition 15. □

Corollaire 17. *Soient K un corps parfait, et $\kappa > 0$ et $\nu > 2$ deux réels. On supposera que κ et ν vérifient la condition suivante :*

$$\kappa < \begin{cases} \frac{\nu-2}{2} & \text{si } \nu \leq 4 \\ \nu - 3 & \text{si } 4 < \nu < 5 \\ \frac{\nu-1}{2} & \text{si } \nu \geq 5. \end{cases} \tag{93}$$

Pour tout entier $j \geq 1$, on se donne une courbe $X^{(j)}$ de genre $g^{(j)}$ sur K, munie d'un point fermé $Q^{(j)}$ de corps résiduel $L^{(j)} = K(Q^{(j)})$ de degré $k^{(j)} = [L^{(j)} : K]$, et on suppose que, lorsque j tend vers l'infini, on a $g^{(j)} \longrightarrow \infty$,

$$\liminf \frac{|X^{(j)}(K)|}{g^{(j)}} \geq \nu, \tag{94}$$

et

$$\frac{k^{(j)}}{g^{(j)}} \longrightarrow \kappa. \tag{95}$$

Alors, pour tout j assez grand, il existe des diviseurs $D^{(j)}$, $G^{(j)}$ sur $X^{(j)}$ tels que $X^{(j)}, G^{(j)}, D^{(j)}, Q^{(j)}$ vérifient les hypothèses du théorème 14, et fournissent un algorithme de multiplication symétrique de longueur $n^{(j)}$ pour L/K, avec

$$\frac{n^{(j)}}{g^{(j)}} \longrightarrow \nu \tag{96}$$

quand j tend vers l'infini. En particulier, on a

$$\limsup_{j\to\infty} \frac{1}{k^{(j)}} \mu_K(L^{(j)}) \leq \frac{\nu}{\kappa}. \tag{97}$$

Lorsque $|K| = q < +\infty$, la conclusion reste valide en remplaçant la condition (93) par la condition plus faible

$$\kappa < \begin{cases} \frac{\nu-2}{2} & \text{si } \nu \leq 4 - \frac{10q^2-2}{q^4+2q^2-1} \\ \left(1-\frac{1}{q^2}\right)^{-2}\nu - 3\left(1-\frac{1}{q^2}\right)^{-1} & \text{si } 4 - \frac{10q^2-2}{q^4+2q^2-1} < \nu < 5 - \frac{14q^2-4}{q^4+2q^2-1} \\ \frac{\nu-1}{2} & \text{si } \nu \geq 5 - \frac{14q^2-4}{q^4+2q^2-1}. \end{cases} \tag{98}$$

Démonstration. Compte tenu de la définition (55) de $\phi_{2,\nu}$, on remarque que la condition (93), ou la condition (98) si K est fini, implique :

$$2\kappa + 1 < \nu \tag{99}$$

et

$$\nu > 1 + \phi_{2,\nu}(2\kappa + 2 - \nu). \tag{100}$$

Pour tout j assez grand, choisissons un entier $n^{(j)} \leq |X^{(j)}(K)|$, en faisant en sorte qu'à l'infini

$$\frac{n^{(j)}}{g^{(j)}} \longrightarrow \nu. \tag{101}$$

Alors pour j assez grand on aura

$$2k^{(j)} + g^{(j)} - 1 \leq n^{(j)} \tag{102}$$

par (99), et

$$|X^{(j)}(K)| > g^{(j)} + f_{2,X^{(j)}}(2k^{(j)} + 2g^{(j)} - 4 - n^{(j)}) \tag{103}$$

par (100) et le lemme 8.b. On peut alors appliquer le corollaire précédent (avec $\mathcal{S} = X^{(j)}(K)$), ce qui permet de conclure. □

Comme dans la section précédente, on note $A(q)$ le plus grand réel tel qu'il existe une suite de courbes $X^{(j)}$ de genre $g^{(j)}$ sur $\mathbb{F}_q$, avec $g^{(j)} \longrightarrow \infty$ et $\frac{|X^{(j)}(K)|}{g^{(j)}} \longrightarrow A(q)$ lorsque j tend vers l'infini.

On note aussi $A'(q)$ le plus grand réel tel qu'il existe une suite de courbes $X^{(j)}$ de genre $g^{(j)}$ sur $\mathbb{F}_q$, avec $g^{(j)} \longrightarrow \infty$ et $\frac{|X^{(j)}(K)|}{g^{(j)}} \longrightarrow A'(q)$ lorsque j tend vers l'infini, et avec la condition supplémentaire

$$\frac{g^{(j+1)}}{g^{(j)}} \longrightarrow 1. \tag{104}$$

Corollaire 18. *Si* $A(q) \geq 5 - \frac{14q^2-4}{q^4+2q^2-1}$, *on a*

$$m_q \leq 2\left(1 + \frac{1}{A(q)-1}\right). \tag{105}$$

Si $A'(q) \geq 5 - \frac{14q^2-4}{q^4+2q^2-1}$, *on a*

$$M_q \leq 2\left(1 + \frac{1}{A'(q)-1}\right). \tag{106}$$

En particulier, si $q \geq 49$ *est un carré, on a*

$$M_q \leq 2\left(1 + \frac{1}{\sqrt{q}-2}\right). \tag{107}$$

Démonstration. Considérons une suite de courbes $X^{(j)}$ sur $\mathbb{F}_q$, de genre $g^{(j)}$ tendant vers l'infini, avec $\frac{|X^{(j)}(K)|}{g^{(j)}} \longrightarrow A(q)$. Posons $\kappa_\epsilon = \frac{A(q)-1-\epsilon}{2}$, de sorte que $\kappa_\epsilon > 0$ si $\epsilon > 0$ est choisi assez petit. Pour tout j assez grand, choisissons un entier $k^{(j)}$, en faisant en sorte que $\frac{k^{(j)}}{g^{(j)}} \longrightarrow \kappa_\epsilon$ quand j tend vers l'infini. Par la borne de Weil, si j est assez grand, $X^{(j)}$ admet au moins un point $Q^{(j)}$ de degré exactement $k^{(j)}$ (cf. [30] Cor. V.2.10.c). On peut alors appliquer le corollaire précédent avec $\kappa = \kappa_\epsilon$ et $\nu = A(q)$, ce qui donne

$$m_q \leq \limsup_{j\to\infty} \frac{1}{k^{(j)}} \mu_q(k^{(j)}) \leq \frac{\nu}{\kappa_\epsilon} = 2\left(1 + \frac{1+\epsilon}{A(q)-1-\epsilon}\right), \tag{108}$$

et puisque ceci vaut pour tout ϵ, on en déduit (105).

Considérons maintenant une suite de courbes $X^{(j)}$ sur $\mathbb{F}_q$, de genre $g^{(j)}$ tendant vers l'infini, avec $\frac{|X^{(j)}(K)|}{g^{(j)}} \longrightarrow A'(q)$, et

$$\frac{g^{(j+1)}}{g^{(j)}} \longrightarrow 1. \tag{109}$$

Posons $\kappa_\epsilon = \frac{A'(q)-1-\epsilon}{2}$, de sorte que $\kappa_\epsilon > 0$ si $\epsilon > 0$ est choisi assez petit. Pour tout entier k assez grand, notons j_k le plus petit entier tel que

$$2k + (1+\epsilon)g^{(j_k)} - 1 \leq |X^{(j_k)}(K)|. \tag{110}$$

Alors, grâce à (109), on a

$$\frac{k}{g^{(j_k)}} \longrightarrow \kappa_\epsilon \tag{111}$$

quand k tend vers l'infini. De même que précédemment, si k est assez grand, $X^{(j_k)}$ admet un point $Q^{(k)}$ de degré exactement k, et on peut appliquer le corollaire précédent pour trouver

$$M_q = \limsup_{k\to\infty} \frac{1}{k} \mu_q(k) \leq \frac{\nu}{\kappa_\epsilon} = 2\left(1 + \frac{1+\epsilon}{A'(q)-1-\epsilon}\right), \tag{112}$$

et on conclut en faisant tendre ϵ vers 0.

La dernière assertion résulte du fait que, si q est un carré, on a $A(q) = A'(q) = \sqrt{q} - 1$ (voir [29], "Claim" p. 163). □

On a ainsi démontré le résultat principal de [29], dont la preuve était incomplète (comme indiqué dans [9]). Par ailleurs, notre méthode a l'avantage d'être constructive, du moins sous l'hypothèse que l'on sait construire explicitement les courbes X, *ainsi que les points Q sur ces courbes*, qui interviennent dans la preuve (il serait par ailleurs intéressant d'étudier si une telle construction ne peut pas s'obtenir par une modification simple d'autres méthodes de construction de courbes déjà connues) ; un tel couple (X, Q) étant donné, les propositions 6 et 15 permettent en effet de construire un algorithme de multiplication pour $K(Q)/K$ en temps polynômial en le genre g de X, qui approche la limite donnée dans le dernier corollaire quand g tend vers l'infini. Ceci répond (de manière positive) à la remarque finale de [29].

5 Épilogue

Il est possible de raffiner les résultats obtenus dans la section précédente, au moins dans deux directions.

Tout d'abord, on peut vouloir non pas une borne sur m_q ou M_q, asymptotique, mais une borne explicite sur $\mu_q(k)$ pour toute valeur de k. Suivant la méthode de [3][4][6], c'est possible dès lors qu'on dispose de familles de courbes dont on sache précisément minorer le nombre de points et majorer la croissance du genre. Par exemple, le corollaire 18 montre que, si $q \geq 49$ est un carré, alors pour tout $\epsilon > 0$ il existe un entier k_ϵ tel que pour tout $k \geq k_\epsilon$ on ait

$$\frac{1}{k}\mu_q(k) \leq 2\left(1 + \frac{1+\epsilon}{\sqrt{q}-2}\right). \tag{113}$$

En étant plus soigneux dans la preuve, on peut espérer une estimation explicite de ce k_ϵ.

Par ailleurs, on peut aussi vouloir combiner notre construction avec des variantes de l'algorithme de Chudnovsky-Chudnovsky par interpolation en des points de degré supérieur, ou avec multiplicités ([7][1][12]). Ceci est intéressant notamment pour obtenir des informations sur les $\mu_q(k)$ lorsque q n'est pas un carré.

On indique ici quelques raffinements de ce type, sans chercher à être exhaustif. Par souci de simplicité, on ne cherchera pas non plus à exploiter les résultats des sections 1 et 2 dans toute leur généralité ; la suite de l'exposé reposera uniquement sur le résultat suivant, qui est une version faible de la proposition 6 :

Proposition 19. *Soient X une courbe de genre g sur un corps fini $\mathbb{F}_q$, et $r \geq 1$ un entier. On suppose donnés des entiers $s_1, \ldots, s_r \in \{1, 2\}$ et des diviseurs $\mathbb{F}_q$-rationnels $T_1, \ldots, T_r$ sur X. On suppose enfin*

$$|X(\mathbb{F}_q)| > \sum_{i=1}^{r} (s_i)^2 g. \tag{114}$$

Alors, pour tout entier d, il existe un diviseur $\mathbb{F}_q$-rationnel D sur X, de degré $\deg D = d$, à support dans $X(\mathbb{F}_q)$, tel que les $s_i D - T_i$ soient ordinaires.

Démonstration. On applique la proposition 6 avec $\mathcal{S} = X(\mathbb{F}_q)$, et le lemme 8.a. □

Remontant en arrière, on observe que ce résultat n'utilise pas le lemme 2 dans toute sa généralité, mais uniquement à travers la formule (10). Ainsi si l'on s'intéresse uniquement aux résultats de cette section, il est possible de simplifier considérablement les preuves et les calculs.

Corollaire 20. *Soient X une courbe de genre g sur un corps fini $\mathbb{F}_q$, munie de deux diviseurs $\mathbb{F}_q$-rationnels Q et G. On note $k = \deg Q$ et $n = \deg G$, et on suppose*

$$|X(\mathbb{F}_q)| > 5g \tag{115}$$

et

$$n \geq 2k + g - 1. \tag{116}$$

Alors il existe un diviseur $\mathbb{F}_q$-rationnel D sur X, à support dans $X(\mathbb{F}_q)$, tel que $D - Q$ soit non-spécial de degré $g - 1$, et $2D - G$ sans sections.

En particulier, si $n = 2k + g - 1$, alors $D - Q$ et $2D - G$ sont non-spéciaux de degré $g - 1$.

Démonstration. On applique la proposition précédente avec $r = 2$, $s_1 = 1$, $T_1 = Q$, $s_2 = 2$, $T_2 = G$, et $d = k + g - 1$ (en remarquant que pour un diviseur de degré inférieur à $g - 1$, ordinaire équivaut à sans sections, et en degré $g - 1$, ordinaire équivaut à non-spécial). □

Une variante de ce résultat est énoncée par Ballet ([5], Prop. 2.1) ; malheureusement la preuve qui en est donnée reproduit l'erreur signalée par [9] dans [29] (l'auteur veut majorer le nombre de classes de diviseurs $[D]$ telles que $2D - G$ soit spécial, par le nombre de diviseurs effectifs de degré $g - 1$; pour cela il associe à toute telle classe un diviseur effectif $E \sim 2D - G$, et conclut en affirmant que cette application $[D] \mapsto E$ est injective ; cela n'est malheureusement pas vrai en général : si le groupe de classes contient de la 2-torsion, on peut trouver deux diviseurs D et D' non linéairement équivalents mais tels que $2D - G$ et $2D' - G$ le soient ; alors si par exemple le système linéaire correspondant est de dimension 1, il n'y a qu'un seul choix possible pour E, et on aura $[D] \mapsto E$ et $[D'] \mapsto E$).

Cette proposition assurait l'existence de diviseurs qui jouent un rôle central dans les résultats de [5] ; ceux-ci étaient donc compromis. En lui substituant notre méthode de construction de diviseurs, sous la forme du corollaire 20, on va pouvoir corriger cet état de fait (cela ne fonctionne cependant que si les courbes mises en jeu ont suffisamment de points).

On commence par donner un critère numérique simple pour estimer la complexité bilinéaire (qui remplace le théroème 2.1.(1) de [5]).

Lemme 21. *Soit X une courbe de genre g sur un corps fini $\mathbb{F}_q$ avec*

$$|X(\mathbb{F}_q)| > 5g. \tag{117}$$

Alors pour tout entier k dans l'intervalle

$$\left\lceil 2 \log_q \frac{2g+1}{\sqrt{q}-1} \right\rceil \; < \; k \; \leq \; \frac{|X(\mathbb{F}_q)| + 1 - g}{2} \tag{118}$$

on a

$$\mu_q(k) \leq 2k + g - 1. \tag{119}$$

Démonstration. Par [30] Cor. V.2.10.c, la première inégalité dans (118) implique que X admet (au moins) un point Q de degré k. D'autre part, la seconde inégalité dans (118) implique que X contient au moins $n = 2k + g - 1$ points $P_1, \ldots, P_n$ de degré 1. Posant $G = P_1 + \cdots + P_n$, on conclut alors par le corollaire 20 et la proposition 15. □

Par exemple ([35]), en prenant $X = \mathbb{P}^1$, et compte tenu de (80), on trouve :

$$\mu_q(k) = 2k - 1 \qquad \text{pour } k \leq \frac{q}{2} + 1. \tag{120}$$

En prenant pour X une courbe elliptique convenable, on trouverait aussi ([28]) :

$$\mu_q(k) \leq 2k \qquad \text{pour } k < \frac{q + e(q) + 1}{2} \tag{121}$$

avec $e(q) \lesssim 2\sqrt{q}$, et en particulier $e(q) = 2\sqrt{q}$ si q est un carré.

On pourrait procéder de même avec des courbes de genre 2, 3, etc.

Un autre point de vue, équivalent, est le suivant. Pour tout entier k, notons $\mathcal{X}_{q,k}$ l'ensemble des courbes (à isomorphisme près) X sur $\mathbb{F}_q$, de genre noté $g(X)$, vérifiant :

a) $g(X) \leq \frac{1}{2}(q^{(k-1)/2}(q^{1/2} - 1) - 1)$

b) $|X(\mathbb{F}_q)| > 5g(X)$

c) $|X(\mathbb{F}_q)| - g(X) \geq 2k - 1$.

Alors :

Lemme 22. *Pour tout corps fini $\mathbb{F}_q$, et pour tout entier k tel que $\mathcal{X}_{q,k}$ soit non vide, on a*

$$\frac{1}{k}\mu_q(k) \leq 2 + \frac{\min_{X \in \mathcal{X}_{q,k}} g(X) - 1}{k}. \tag{122}$$

Démonstration. C'est une reformulation du lemme précédent. □

Par rapport à d'autres résultats semblables dans la littérature, notre méthode de construction de diviseurs autorise une condition de dépendance plus faible entre k, g, et le nombre de points de la courbe. Par exemple, le théorème 1.1 de [3] (ou plus précisément son corollaire 2.1) arrive à la même conclusion, mais en remplaçant la seconde inégalité de (118) par $k \leq \frac{|X(\mathbb{F}_q)|+1-2g}{2}$, ou ce qui revient au même, en remplaçant la condition c) définissant $\mathcal{X}_{q,k}$ par la condition plus forte $|X(\mathbb{F}_q)| - 2g(X) \geq 2k - 1$. En contrepartie cependant, notre méthode exige que les courbes considérées aient suffisamment de points, comme exprimé par la condition b) ci-dessus.

On peut maintenant continuer en suivant les arguments [5]. En fait, on va donner une version légèrement plus précise du résultat qui y était énoncé.

On considère la fonction psi de Dedekind, définie pour tout entier N par

$$\psi(N) = N \prod_{\substack{l \mid N \\ l \text{ premier}}} \left(1 + \frac{1}{l}\right). \tag{123}$$

Lemme 23. *Soient p un nombre premier et N un entier premier à p. Alors la courbe modulaire $X_0(N)$ est lisse sur $\mathbb{F}_p$, de genre*

$$g_0(N) \leq \frac{\psi(N)}{12}, \tag{124}$$

et possède

$$|X_0(N)(\mathbb{F}_{p^2})| \geq (p-1)\frac{\psi(N)}{12} \tag{125}$$

points sur $\mathbb{F}_{p^2}$.

Démonstration. Voir [33], § 4.1. □

Remarque 24. En fait on peut être légèrement plus précis dans le lemme. La formule de Hurwitz donne une expression exacte

$$g_0(N) = \frac{\psi(N)}{12} + 1 - \frac{\nu_\infty(N)}{2} - \frac{\nu_3(N)}{3} - \frac{\nu_2(N)}{4} \tag{126}$$

avec

- $\nu_\infty(N) = \sum_{d|N} \phi(\mathrm{pgcd}(d, \frac{N}{d})) = \prod_{l^\nu || N} \begin{cases} 2l^{\frac{\nu-1}{2}} & \text{si } \nu \text{ impair} \\ (l+1)l^{\frac{\nu}{2}-1} & \text{si } \nu \text{ pair} \end{cases}$
- $\nu_3(N) = \begin{cases} \prod_{l|N} \left(1 + \left(\frac{-3}{l}\right)\right) & \text{si } 9 \nmid N \\ 0 & \text{si } 9 \mid N \end{cases}$
- $\nu_2(N) = \begin{cases} \prod_{l|N} \left(1 + \left(\frac{-1}{l}\right)\right) & \text{si } 4 \nmid N \\ 0 & \text{si } 4 \mid N \end{cases}$

tandis que la relation d'Eichler-Shimura donne

$$|X_0(N)(\mathbb{F}_{p^2})| = p^2 + 1 + pg_0(N) - \mathrm{tr}\, T_{p^2} \tag{127}$$

où l'opérateur de Hecke T_{p^2} agit sur l'espace des formes paraboliques $S_2(\Gamma_0(N))$, sa trace pouvant se calculer explicitement, par exemple par la formule donnée dans [21], Th. 6.8.4 et Rem. 6.8.1, pp. 263–264 :

$$\mathrm{tr}\, T_{p^2} = \frac{\psi(N)}{12} + \delta(N, p^2) - \sum_t a(t) \sum_f b(t,f)c(t,f) \tag{128}$$

où $\delta(N, p^2) = p^2+p+1$ si $N > 1$. Les termes $a(t)\sum_f b(t,f)c(t,f)$ sont positifs, et leur contribution à la somme peut s'exprimer simplement pour certaines valeurs particulières de t :

- $\frac{1}{2}\, p\, \nu_\infty(N)$ pour $t = \pm 2p$
- $\frac{1}{3}\left(p + 1 - \left(\frac{-3}{p}\right)\right)\nu_3(N)$ pour $t = \pm p$ (si $3 \nmid N$)
- $\frac{1}{4}\left(p + 1 - \left(\frac{-1}{p}\right)\right)\nu_2(N)$ pour $t = 0$ (si $2 \nmid N$)

de sorte que pour $N > 1$ premier à $6p$:

$$|X_0(N)(\mathbb{F}_{p^2})| = (p-1)\frac{\psi(N)}{12} + \frac{1-\left(\frac{-3}{p}\right)}{3}\nu_3(N) + \frac{1-\left(\frac{-1}{p}\right)}{4}\nu_2(N) + \sum_{t \neq 0, \pm p, \pm 2p} a(t) \sum_f b(t,f)c(t,f). \tag{129}$$

On obtiendrait des formules analogues pour $2|N$ ou $3|N$.

Pour toute partie infinie $\mathcal{A}$ de $\mathbb{N}$ et pour tout réel $x > 0$ on note

$$\lceil x \rceil_{\mathcal{A}} = \min \mathcal{A} \cap [x, +\infty[\tag{130}$$

le plus petit élément de $\mathcal{A}$ supérieur ou égal à x, et on pose

$$\epsilon_{\mathcal{A}}(x) = \sup_{y \geq x} \frac{\lceil y \rceil_{\mathcal{A}} - y}{y}, \tag{131}$$

de sorte que la fonction $\epsilon_{\mathcal{A}}$ est décroissante, et que pour tout $x > 0$, l'intervalle $[x, (1 + \epsilon_{\mathcal{A}}(x))x]$ contient au moins un élément de $\mathcal{A}$.

Ainsi, si p est un nombre premier, $\lceil x \rceil_{\psi(\mathbb{N} \setminus p\mathbb{N})}$ est le plus petit $n \geq x$ qui puisse s'écrire sous la forme $n = \psi(N)$ pour un entier N premier à p, et :

Lemme 25. *Avec ces notations, pour $p \neq 2$, on a*

$$\lceil x \rceil_{\psi(\mathbb{N} \setminus p\mathbb{N})} \leq 2x \quad \textit{pour tout } x \geq \frac{3}{2}, \tag{132}$$

ou autrement dit :

$$\epsilon_{\psi(\mathbb{N} \setminus p\mathbb{N})}(3/2) \leq 1. \tag{133}$$

Démonstration. Si $j = \lfloor \frac{\log 2x/3}{\log 2} \rfloor$, on a bien $x < 3 \cdot 2^j = \psi(2^{j+1}) \leq 2x$. □

Proposition 26. *Soit $p \geq 7$ un nombre premier. Alors pour tout $k > \frac{p^2+p+1}{2}$ on a*

$$\frac{1}{k}\mu_{p^2}(k) \leq 2 + \frac{\frac{1}{12}\left\lceil \frac{24k-12}{p-2} \right\rceil_{\psi(\mathbb{N} \setminus p\mathbb{N})} - 1}{k}. \tag{134}$$

Démonstration. On choisit N premier à p tel que $\psi(N) = \left\lceil \frac{24k-12}{p-2} \right\rceil_{\psi(\mathbb{N} \setminus p\mathbb{N})}$ et on pose $X = X_0(N)$. Alors par (124) et (125) on a $|X(\mathbb{F}_{p^2})| - g(X) \geq (p-2)\frac{\psi(N)}{12}$ donc la condition c) précédant le lemme 22 est bien vérifiée.

De même $|X(\mathbb{F}_{p^2})| - 5g(X) \geq (p-6)\frac{\psi(N)}{12}$ donc pour $p \geq 7$ la condition b) est bien vérifiée elle aussi.

Enfin par le lemme 25 on a $\psi(N) = \left\lceil \frac{24k-12}{p-2} \right\rceil_{\psi(\mathbb{N} \setminus p\mathbb{N})} \leq \frac{48k-24}{p-2}$ donc

$$g(X) \leq \frac{\psi(N)}{12} \leq \frac{4k-2}{p-2}, \tag{135}$$

et pour $p \geq 7$ et $k > \frac{p^2+p+1}{2}$, on montre facilement que cette dernière quantité est majorée par $\frac{1}{2}(p^{k-1}(p-1)-1)$. Ainsi la condition a) est vérifiée, et on peut conclure grâce au lemme 22. □

Remarque 27. Grâce à cette proposition, toute majoration (effective) de la fonction $\lceil . \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$, ou de $\epsilon_{\psi(\mathbb{N}\setminus p\mathbb{N})}$, se traduit en une majoration (effective) des $\mu_{p^2}(k)$. Il s'agit donc, pour un réel $x > 0$ donné, de trouver un entier N premier à p tel que $\psi(N)$ soit supérieur à x mais aussi petit que possible. Une première analyse fournit deux approches naturelles à ce problème.

Tout d'abord, on peut chercher N parmi les entiers n'ayant que des petits facteurs premiers. En effet, soit $\mathcal{B} = \{l_1, \ldots, l_B\}$ un ensemble de nombres premiers, $p \notin \mathcal{B}$. Posons $N_{\mathcal{B}} = \prod_{i=1}^{B} l_i$ et supposons $\psi(N_{\mathcal{B}}) = \prod_{i=1}^{B}(l_i + 1) < x$. Alors si $N = N' N_{\mathcal{B}}$ où N' a tous ses facteurs premiers dans $\mathcal{B}$, on a $\psi(N) = N'\psi(N_{\mathcal{B}})$. Ainsi, si l'on sait trouver un entier $N' \geq \frac{x}{\psi(N_{\mathcal{B}})}$ aussi petit que possible ayant tous ses facteurs premiers dans $\mathcal{B}$, on en déduit une majoration de $\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$. Pour $\mathcal{B} = \{2\}$ on retrouve le lemme 25. Il serait intéressant d'optimiser le choix de $\mathcal{B}$ (dépendant éventuellement de x) pour obtenir de meilleures estimations.

À l'opposé, on peut aussi chercher N parmi les entiers n'ayant que des grands facteurs premiers. En effet, si N n'a aucun facteur premier inférieur à $N^{1/u}$, alors $\psi(N) \leq N\left(1 + \frac{1}{N^{1/u}}\right)^u$, et si on sait trouver un tel $N \geq x$ aussi petit que possible, on peut espérer, en optimisant préalablement u, obtenir une majoration approchant suffisamment $\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})}$. Le cas extrême est celui où l'on prend $u = 1$, c'est-à-dire où l'on cherche N premier. On obtient alors la majoration

$$\lceil x \rceil_{\psi(\mathbb{N}\setminus p\mathbb{N})} \leq \lceil x - 1 \rceil_{\mathcal{P}} + 1 \quad \text{pour } x > p + 1 \tag{136}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers (en effet, $N = \lceil x - 1 \rceil_{\mathcal{P}}$ est un nombre premier strictement plus grand que p, et $\psi(N) = N + 1 \geq x$). Ceci permet de mettre à profit tous les résultats connus sur la fonction $\epsilon_{\mathcal{P}}$; par exemple le postulat de Bertrand, prouvé par Tchebychev, donne $\epsilon_{\mathcal{P}}(1) = 1$, et combiné avec (136), il fournit une majoration essentiellement équivalente à celle du lemme 25. D'autres estimations plus fines sont connues, et on les utilisera dans le corollaire ci-dessous. Il serait intéressant cependant, là aussi, d'étudier si un choix convenable de $u > 2$, dépendant éventuellement de x, permet de faire signicativement mieux.

Corollaire 28. *Soit $p \geq 7$ un nombre premier. Alors*

(i) pour tout $k > \frac{p^2+p+1}{2}$,

$$\frac{1}{k}\mu_{p^2}(k) \leq 2\left(1 + \frac{1 + \epsilon_{\mathcal{P}}\left(\frac{24k}{p-2}\right)}{p-2}\right) \tag{137}$$

(ii) pour tout $k \geq 1$,

$$\frac{1}{k}\mu_{p^2}(k) \leq 2\left(1 + \frac{2}{p-2}\right) \tag{138}$$

(iii) pour tout $k \geq 1$,

$$\frac{1}{k}\mu_{p^2}(k) \leq 2\left(1 + \frac{1 + \frac{10}{139}}{p-2}\right) \tag{139}$$

(iv) pour tout $k \geq e^{50} p$,

$$\frac{1}{k}\mu_{p^2}(k) \leq 2\left(1 + \frac{1,000\,000\,005}{p-2}\right) \tag{140}$$

(v) pour tout $k \geq 16\,531\,(p-2)$,

$$\frac{1}{k}\mu_{p^2}(k) \leq 2\left(1 + \frac{1 + \frac{1}{25\log^2 \frac{24k}{p-2}}}{p-2}\right) \tag{141}$$

(vi) pour tout k *assez grand,*

$$\frac{1}{k}\mu_{p^2}(k) \leq 2\left(1 + \frac{1 + \frac{1}{k^{0,475}}}{p-2}\right). \tag{142}$$

Démonstration. Le point (i) découle de la proposition 26, de (136), et de l'inégalité évidente $\left\lceil \frac{24k-12}{p-2} - 1 \right\rceil_{\mathcal{P}} \leq \left\lceil \frac{24k}{p-2} \right\rceil_{\mathcal{P}}$.

Le point (ii) découle de (121), de la proposition 26, et du lemme 25.

En remarquant que pour $p \geq 7$ et $k > \frac{p^2+p+1}{2}$ on a $\frac{24k}{p-2} > 139$, le point (iii) découle de (121), de (i) et de l'égalité $\epsilon_{\mathcal{P}}(139) = 10/139$. Pour montrer cette dernière, on remarque que si $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, ... est la suite des nombres premiers, alors pour tous $n \leq n'$ on a

$$\epsilon_{\mathcal{P}}(p_n) = \max\left(\epsilon_{\mathcal{P}}(p_{n'}),\ \max_{n \leq j < n'} \frac{p_{j+1} - p_j}{p_j}\right). \tag{143}$$

On pose $p_n = 139$, on majore $\epsilon_{\mathcal{P}}(p_{n'})$ pour $p_{n'} = 2\,010\,881$ au moyen de [26] (ou bien pour $p_{n'} = 396\,833$ au moyen de [16]) et on conclut en calculant explicitement les derniers termes pour $n \leq j < n'$.

Enfin les points (iv), (v) et (vi) se déduisent de (i) et des estimations de [23], [16], et [2], respectivement. □

En utilisant d'autres familles de courbes (par exemple celles utilisées dans [29]), on pourrait obtenir des résultats semblables pour $q = p^{2m}$ avec m quelconque. Ce cas est étudié aussi dans [5], cependant, signalons encore une petite imprécision dans la preuve : l'auteur applique le postulat de Bertrand sans prendre garde qu'il n'a pas affaire à l'ensemble de tous les nombres premiers, mais seulement à ceux qui se scindent complètement dans une certaine extension abélienne L de $\mathbb{Q}$. Sur le principe, cette stratégie de preuve reste correcte, mais il faut pour cela substituer au postulat de Bertrand une estimation sur la taille des intervalles contenant des nombres premiers dans une suite arithmétique donnée.

On peut aussi obtenir des estimations pour q quelconque (non nécessairement carré), cependant l'utilisation de la méthode de Chudnovsky-Chudnovsky telle que présentée dans le théorème 14, où l'on évalue en des points simples de degré 1, semble ne pas conduire aux meilleurs résultats. Diverses variantes de la

méthode relâchant cette dernière condition ont été introduites ([7][1]), la plus générale étant celle de [12], qui autorise un diviseur d'évaluation G quelconque.

On va voir ci-dessous comment notre méthode de construction de diviseurs permet de préciser certains résultats de [12]. On reprend les notations qui y sont introduites, et en particulier, pour tout corps fini $\mathbb{F}_q$, on note $\widehat{M_q}(u)$ la complexité bilinéaire (sur $\mathbb{F}_q$) de la multiplication dans l'anneau local $\mathbb{F}_q[[t]]/t^u$.

Proposition 29. *Soient X une courbe de genre g sur un corps fini $\mathbb{F}_q$, et $k > 1$ un entier naturel. Soit aussi*

$$G = u_1 P_1 + \cdots + u_N P_N \tag{144}$$

un diviseur effectif sur X, où les P_i sont des points fermés de degrés arbitraires. On suppose que X admet un point fermé Q de degré k (c'est le cas par exemple si $2g + 1 \leq q^{(k-1)/2}(q^{1/2} - 1)$), et que

$$|X(\mathbb{F}_q)| > 5g \tag{145}$$

et

$$\deg G \geq 2k + g - 1. \tag{146}$$

Alors

$$\mu_q(k) \leq \sum_{i=1}^{N} \mu_q(\deg(P_i)) \widehat{M}_{q^{\deg(P_i)}}(u_i). \tag{147}$$

Démonstration. Le corollaire 20 assure l'existence d'un diviseur D tel que $D-Q$ soit non-spécial de degré $g-1$, et $2D-G$ sans sections. Quitte à remplacer D par un diviseur linéairement équivalent on peut, par le théorème d'approximation forte, supposer que D est de support disjoint de Q et G (on pourrait aussi modifier les énoncés de [12] par l'introduction d'applications d'évaluation généralisées comme dans notre définition 9). En reprenant les notations de [12], la condition que $D - Q$ est non-spécial implique que l'application d'évaluation $\mathcal{L}(D) \longrightarrow \mathcal{O}_Q/Q$ est surjective, tandis que celle que $2D - G$ est sans sections implique que

$$\phi : \mathcal{L}(2D) \longrightarrow \mathcal{O}_{P_1}/P_1^{u_1} \times \cdots \times \mathcal{O}_{P_N}/P_N^{u_N} \tag{148}$$

est injective, ce qui permet d'appliquer le théorème 3.1 de [12] et de conclure. □

On remarquera que notre proposition améliore le théorème 3.2 de [12], qui demande $\deg G \geq 2k + 2g - 1$. De façon équivalente, notre proposition donne un critère numérique simple pour assurer la validité des hypothèses du théorème 3.6 de [12], et plus particulièrement l'injectivité de l'application ϕ qui y est demandée (en notant par ailleurs une imprécision dans l'énoncé de ce théorème 3.6 : il ne suffit pas de demander que D soit non-spécial, c'est $D - Q$ qui doit l'être).

Cependant, comme précédemment, notre méthode exige en contrepartie que la courbe ait suffisamment de points de degré 1, par la condition $|X(\mathbb{F}_q)| > 5g$. On pourrait relâcher très légèrement cette condition, en utilisant la proposition 6 dans toute sa généralité, plutôt que la proposition 19 qui en est un cas

particulier. Ceci n'apporterait toutefois que peu de marge de manœuvre supplémentaire, il resterait une condition de cardinalité sur le nombre de points de la courbe. S'affranchir d'une telle condition, avec notamment pour objectif la possibilité de couvrir le cas où q est petit, semble encore un problème ouvert dans notre approche.

Remarquons enfin que, même pour q grand, cette condition $|X(\mathbb{F}_q)| > 5g$ n'est pas anodine dans la recherche d'une bonne famille de courbes ; en effet, par l'intermédiaire de la borne de Drinfeld-Vladut généralisée ([27][32]), elle impose aussi des contraintes sur le nombre de points de degré supérieur. Illustrons ceci par un exemple. Pour toute courbe X sur $\mathbb{F}_q$, notons $N_m(X/\mathbb{F}_q)$ le nombre de points fermés de degré m de X, de sorte que pour tout n on a

$$|X(\mathbb{F}_{q^n})| = \sum_{m|n} m N_m(X/\mathbb{F}_q). \tag{149}$$

Si dans la proposition 29 on se restreint à ne considérer que des points de degré 1 ou 2, et sans multiplicités ($u_i = 1$), on trouve (voir aussi [7]) : s'il existe une courbe X de genre g sur $\mathbb{F}_q$ telle que :

(i) $N_k(X/\mathbb{F}_q) > 0$ (c'est le cas par exemple si $2g + 1 \leq q^{(k-1)/2}(q^{1/2} - 1)$)

(ii) $N_1(X/\mathbb{F}_q) > 5g$

(iii) $N_1(X/\mathbb{F}_q) + 2N_2(X/\mathbb{F}_q) \geq 2k + g - 1$

alors

$$\mu_q(k) \leq N_1(X/\mathbb{F}_q) + 3N_2(X/\mathbb{F}_q). \tag{150}$$

Or la borne de Drinfeld-Vladut généralisée implique, pour toute famille de courbes de genre tendant vers l'infini :

$$\limsup \frac{1}{g}\left(\frac{N_1(X/\mathbb{F}_q)}{\sqrt{q}-1} + \frac{2N_2(X/\mathbb{F}_q)}{q-1}\right) \leq 1 \tag{151}$$

de sorte que la condition (ii) implique que, dans (iii), on aura au mieux :

$$\limsup \frac{1}{g}\left(N_1(X/\mathbb{F}_q) + 2N_2(X/\mathbb{F}_q)\right) \leq q - 5\sqrt{q} - 1. \tag{152}$$

Cela interdit notamment d'utiliser des familles de courbes optimales, pour lesquelles $\frac{1}{g}2N_2(X/\mathbb{F}_q) \longrightarrow q - 1$.

Références

[1] N. Arnaud, *Evaluations dérivées, multiplication dans les corps finis et codes correcteurs*, thèse de doctorat, Luminy, 2006.

[2] R. C. Baker, G. Harman & J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. **83** (2001) 532–562.

[3] S. Ballet, *Curves with many points and multiplication complexity in any extension of* $\mathbb{F}_q$, Finite Fields Appl. **5** (1999) 364–377.

[4] S. Ballet, *Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of* $\mathbb{F}_q$, Finite Fields Appl. **9** (2003) 472–478.

[5] S. Ballet, *On the tensor rank of the multiplication in the finite fields*, J. Number Theory **128** (2008) 1795–1806.

[6] S. Ballet & J. Chaumine, *On the bounds of the bilinear complexity of multiplication in some finite fields*, Appl. Algebra Engrg. Comm. Comput. **15** (2004) 205–211.

[7] S. Ballet & R. Rolland, *Multiplication algorithm in a finite field and tensor rank of the multiplication*, J. Algebra **272** (2004) 173–185.

[8] S. Ballet & R. Rolland, "On the bilinear complexity of the multiplication in finite fields", in : Y. Aubry & G. Lachaud (eds.), *Arithmetic, Geometry and Coding Theory (AGCT 2003)*, Séminaires et congrès **11**, Société Mathématique de France, 2005, pp. 179–188.

[9] I. Cascudo, *On asymptotically good strongly multiplicative linear secret sharing*, thèse de doctorat, université d'Oviedo, 2010.

[10] I. Cascudo, H. Chen, R. Cramer & C. Xing, "Asymptotically good ideal linear secret sharing with strong multiplication over *any* fixed finite field", in : S. Halevi (ed.), *Advances in cryptology – CRYPTO 2009*, Lecture Notes in Comp. Science **5677**, Springer-Verlag, 2009, pp. 466–486.

[11] I. Cascudo, R. Cramer & C. Xing (2010) ? ? ?

[12] M. Cenk & F.Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010) 172–186.

[13] H. Chen & R. Cramer, "Algebraic geometric secret sharing schemes and secure multi-party computations over small fields", in : C. Dwork (ed.), *Advances in cryptology – CRYPTO 2006*, Lecture Notes in Comp. Science **4117**, Springer-Verlag, 2006, pp. 521–536.

[14] D. V. & G. V. Chudnovsky, *Algebraic complexities and algebraic curves over finite fields*, Proc. Nat. Acad. Sci. USA **84** (1987) 1739–1743.

[15] V. G. Drinfeld & S. G. Vladut, *Number of points of an algebraic curve*, Funct. Anal. **17** (1983) 53–54.

[16] P. Dusart, *Estimates of some functions over primes without R.H.*, à paraître. — `http://arxiv.org/abs/1002.0442`

[17] C. Fiduccia & Y. Zalcstein, *Algebras having linear multiplicative complexities*, J. Assoc. Comput. Mach. **24** (1977) 311–331.

[18] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981) 721–724.

[19] D. Laksov, *Wronskians and Plücker formulas for linear systems on curves*, Ann. Sci. École Norm. Sup. **17** (1984) 45–56.

[20] A. Lempel & S. Winograd, *A new approach to error-correcting codes*, IEEE Trans. Inform. Theory **23** (1977) 503–508.

[21] T. Miyake, *Modular forms*, Springer-Verlag, 1989.

[22] A. Neeman, *Weierstrass points in characteristic p*, Invent. Math. **75** (1984) 359–376.

[23] O. Ramaré & Y. Saouter, *Short effective intervals containing primes*, J. Number Theory **98** (2003) 10–33.

[24] H. Randriam, "Hecke operators with odd determinant and binary frameproof codes beyond the probabilistic bound ?", in *Proc. of ITW 2010 Dublin – IEEE Information Theory Workshop, Dublin, Ireland, 2010.*

[25] H. Randriambololona, $(2,1)$*-separating systems beyond the probabilistic bound*, à paraître. — `http://arxiv.org/abs/1010.5764`

[26] L. Schoenfeld, *Sharper bounds for the Chebyshev functions* $\theta(x)$ *and* $\psi(x)$*, II*, Math. Comp. **30** (1976), 337–360.

[27] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algÃ¯brique sur un corps fini*, C. R. Acad. Sci. Paris SÃ¯r. I Math. **296** (1983) 397–402.

[28] M. A. Shokrollahi, *Optimal algorithms for multiplication in certain finite fields using elliptic curves*, SIAM J. Comput. **21** (1992) 1193–1198.

[29] I. Shparlinski, M. Tsfasman & S. Vladut, "Curves with many points and multiplication in finite fields", in : H. Stichtenoth & M. A. Tsfasman (eds.), *Coding theory and algebraic geometry (Luminy, 1991)*, Lecture Notes in Math. **1518**, Springer-Verlag, 1992, pp. 145–169.

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

[31] K.-O. Stöhr & F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986) 1–19.

[32] M. A. Tsfasman, "Some remarks on the asymptotic number of points", in : H. Stichtenoth & M. A. Tsfasman (eds.), *Coding theory and algebraic geometry (Luminy, 1991)*, Lecture Notes in Math. **1518**, Springer-Verlag, 1992, pp. 178–192.

[33] M. A. Tsfasman & S. G. Vladut, *Algebraic-geometric codes*, Kluwer Academic Publishers, 1991.

[34] M. A. Tsfasman, S. G. Vladut & T. Zink, *Modular curves, Shimura curves, and Goppa codes better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982) 21–28.

[35] S. Winograd, *Some bilinear forms whose multiplicative complexity depends on the field of constants*, Math. Systems Theory **10** (1977) 169–180.

[36] C. Xing, *Asymptotic bounds on frameproof codes*, IEEE Trans. Inform. Theory **48** (2002) 2991–2995.