THÈSE DE DOCTORAT DE
L'UNIVERSITÉ D'AIX-MARSEILLE

Discipline

Mathématiques

École doctorale de mathématiques et d'informatique d'Aix-Marseille (ED184)

Présentée et soutenue publiquement le 12 décembre 2012 par

Julia PIELTANT

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ D'AIX-MARSEILLE

Titre :

Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis.

Directeur de thèse : Stéphane BALLET

COMPOSITION DU JURY

Daniel AUGOT	Directeur de recherche, INRIA/LIX, Saclay	
Stéphane BALLET	Maître de conférences HDR, AMU/IML, Marseille	
Gilles LACHAUD	Directeur de recherche émérite, CNRS/IML, Marseille	
Reynald LERCIER	Chercheur HDR, DGA & IRMAR, Rennes	Rapporteur
Traian MUNTEAN	Professeur des universités, AMU/eRISCS, Marseille	Invité
Ferruh ÖZBUDAK	Professeur des universités, METU, Ankara (Turquie)	Rapporteur
François RODIER	Directeur de recherche CNRS/IML, Marseille	
Robert ROLLAND	Chercheur HDR, AMU/IML/eRISCS	
Serge VLĂDUŢ	Professeur des universités, AMU/IML, Marseille	

Remerciements

Avant toute chose, je souhaite remercier chaleureusement mon directeur de thèse, Stéphane Ballet, pour son aide, sa bienveillance, sa confiance et son implication tout au long de cette thèse. J'ai apprécié ses nombreux conseils et sa disponibilité en toutes circonstances — même coincé aux antipodes avec bien d'autres soucis en tête !

Cette thèse n'aurait pu être réalisée sans le support des contrats de valorisation du Groupe eRISCS dirigé par Traian Muntean, qui m'a de surcroît laissée bénéficier d'une grande liberté dans mon travail pendant ces trois années : je l'en remercie pour cela, et pour sa détermination à résoudre les problèmes administratifs liés à l'obtention de mon contrat doctoral. Je n'oublie pas que d'autres ont dû se joindre à lui pour venir à bout de ces déboires initiaux ; merci particulièrement à Robert Rolland, à Gilles Lachaud et bien sûr encore une fois à Stéphane pour leur intervention dans cet épisode désormais classé.

Je remercie vivement Reynald Lercier et Ferruh Özbudak d'avoir accepté le lourd travail de rapporter cette thèse, et ce dans un délai assez court. Mes remerciements vont aussi à Daniel Augot, Gilles Lachaud, Traian Muntean, François Rodier, Robert Rolland et Serge Vlăduţ qui me font l'honneur de faire partie de mon jury.

Un merci avec multiplicité à Daniel Augot, ainsi qu'à Alain Couvreur, qui ont trouvé le moyen idéal pour me permettre de finir cette thèse sans soucis grâce au financement de l'Inria et d'envisager sereinement l'année à venir au sein de leur équipe.

Merci à l'équipe administrative et informatique de l'IML, pour leur travail qui simplifie le nôtre.

Je voudrais remercier Hugues Randriambololona, pour m'avoir fait part de son travail et s'être intéressé au mien. Merci aussi à Jean Chaumine pour sa relecture attentive de ce manuscrit.

Merci à tous les membres de l'IML et notamment de l'équipe ATI pour leur accueil. Au cours de ces trois années, bien des affinités se sont créées et elles ont largement dépassé le cadre professionnel. Merci donc à tous ceux qui ont participé à la bonne ambiance générale : Virgile, Safia, Christophe et Christophe Junior, Marc le virevoltant et Marc le boxeur, Hamish, Tammam, Yih-Dar, Yves, Florian, Joël, Émilie, Jean-Baptiste, Mila, Florent et tous ceux que j'oublie. Et bien sûr, merci

particulièrement à Stéphanie avec qui ce fut un plaisir de partager le bureau 110 !

Merci également à mes nouveaux camarades du LIX, qui m'ont accueillie avec sympathie dans leur équipe !

Mes remerciements vont aussi à ceux qui, en dehors du labo, ont été là pour partager de bons moments loin de la thèse. Merci notamment à Caro, à Marjorie, à Alban pour leur amitié indéfectible ! Merci aussi aux Loùmassiens de m'avoir ouvert les portes de leur famille et de leur demeure qui a toujours un air de vacances.

Je remercie mes parents de m'avoir permis de faire les études de mon choix, et de m'avoir aidée pendant toutes ces années.

Enfin, merci infiniment à toi qui partage ma vie, pour ta patience, ton soutien et ta présence si importante à mes côtés...

Table des matières

Introduction générale

L'élaboration d'une technique efficace de multiplication est un problème central en théorie de la complexité algébrique. Dans ce cadre s'insèrent, par exemple, les problèmes de la détermination de la complexité du produit de deux polynômes ou de deux matrices carrées, qui ont été largement étudiés. Un autre cas naturel à considérer est celui de la complexité de la multiplication dans les corps finis, qui est notamment au cœur des protocoles cryptographiques : le chiffrement et le déchiffrement reposent sur l'efficacité de la multiplication, qui a donc un impact direct sur la sécurité d'un protocole. C'est pourquoi, dans les 30 dernières années, un intérêt considérable a été porté au problème de la détermination de cette complexité.

Considérons $\mathbb{F}_q$ le corps fini à q éléments, où q est une puissance d'un nombre premier et soit $\mathbb{F}_{q^n}$ une extension de degré n de $\mathbb{F}_q$. Cette extension peut être obtenue comme quotient de l'anneau de polynômes $\mathbb{F}_q[X]$ par un idéal engendré par un polynôme irréductible sur $\mathbb{F}_q$; ainsi, la complexité du produit de deux polynômes de degré inférieur ou égal à n à coefficients dans $\mathbb{F}_q$ permet de donner une estimation de la complexité de la multiplication dans $\mathbb{F}_{q^n}$. Dans cette thèse, on s'intéresse plus précisément à la complexité dite bilinéaire de la multiplication dans les extensions finies de $\mathbb{F}_q$.

On appelle complexité de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ le nombre d'opérations élémentaires dans $\mathbb{F}_q$ nécessaires pour calculer le produit de deux éléments de $\mathbb{F}_{q^n}$. Ces opérations peuvent être de différents types :

- addition,
- multiplication scalaire, c'est-à-dire multiplication par une constante ne dépendant pas des éléments de $\mathbb{F}_{q^n}$ dont on effectue le produit,
- multiplication non-scalaire ou bilinéaire, c'est-à-dire multiplication de deux éléments de $\mathbb{F}_q$ dépendant directement des éléments de $\mathbb{F}_{q^n}$ dont on effectue le produit.

Le nombre de multiplications bilinéaires nécessaires pour effectuer le produit de deux éléments quelconques de $\mathbb{F}_{q^n}$ est appelé complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Remarquons que la complexité globale de la multiplication dans $\mathbb{F}_{q^n}$ dépend de la base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ choisie. En effet, le passage d'une base à une autre correspond à l'application d'un isomorphisme de $\mathbb{F}_q$-espaces vectoriels, ou encore à la multiplication d'un vecteur-coordonnées par une matrice carrée de taille n à coefficients dans $\mathbb{F}_q$. Les coefficients de cette matrice dépendent uniquement des bases considérées et non pas du vecteur-coordonnées. Autrement dit, passer d'une

base à une autre se réduit à effectuer deux sortes d'opérations :

- la somme de deux éléments de $\mathbb{F}_q$: $(x, y) \mapsto x + y$,
- le produit d'une coordonnée du vecteur par une constante $c \in \mathbb{F}_q$: $x \mapsto cx$.

La complexité bilinéaire de la multiplication ne tient pas compte de ces types d'opérations, en conséquence elle est indépendante de la base choisie pour la représentation de $\mathbb{F}_{q^n}$ et est donc en quelque sorte « intrinsèque » à cette extension. La détermination de cette complexité est de plus reliée au problème abstrait de la détermination du rang de tenseur de la multiplication dans les corps finis et présente donc aussi un intérêt théorique.

Ce manuscrit comporte cinq chapitres.

Dans le chapitre 1, en suivant les grandes lignes de [Sti08], on rappelle les notions principales concernant les corps de fonctions algébriques, ainsi que les extensions qui permettent de construire des tours de corps de fonctions. On donne aussi quelques résultats importants à propos des diviseurs de dimension nulle [BRR10], dont l'étude est d'un intérêt particulier pour l'algorithme de type Chudnovsky. Cet algorithme, introduit en 1987 par Chudnovsky et Chudnovsky dans [CC87], est dans la lignée des algorithmes de type évaluation-interpolation tels que ceux de Karatsuba [KO63] ou Toom [Too63]. Il sera présenté en détail dans le chapitre 2, où l'on dressera un aperçu historique des évolutions que différents auteurs, parmi lesquels Shparlinski, Tsfasman et Vlăduţ [STV92], Ballet et Rolland [BR04], Arnaud [Arn06], Cenk et Özbudak [CÖ10], et Randriambololona [Ran12], ont apportés depuis la fin des années 80. On définira aussi dans ce chapitre le rang de tenseur de la multiplication dans les algèbres, que l'on reliera à la complexité bilinéaire de la multiplication en montrant l'équivalence entre ces deux notions. En particulier, on distinguera deux types de complexité bilinéaire, la complexité symétrique et la complexité asymétrique, pour lesquelles on rappellera les principales bornes uniformes et asymptotiques connues dans le cas des corps finis.

Dans le chapitre 3, on présente des tours de corps de fonctions algébriques qui sont des versions modifiées [BR04, BLBR09] des tours bien connues de Garcia, Stichtenoth et Rück [GS95, GSR03]. Ces tours ont des propriétés intéressantes pour la détermination de bornes pour la complexité bilinéaire ; en particulier, relativement au genre des étages, elles ont un grand nombre de places rationnelles ou de places de petit degré dans le cas où l'on considère une tour obtenue par descente du corps de définition d'une tour asymptotiquement optimale. On établira un certain nombre de résultats techniques à propos de ces tours qui nous permettront de nous assurer que celles-ci sont bien adaptées aux spécialisations de l'algorithme de type Chudnovsky que l'on donnera dans les deux derniers chapitres.

Les chapitres 4 et 5 présentent les nouvelles bornes obtenues dans cette thèse pour la complexité bilinéaire symétrique d'une part, et pour la complexité bilinéaire asymétrique d'autre part. Ces bornes sont essentiellement des bornes uniformes, et certaines d'entre elles donnent en outre de nouvelles bornes asymptotiques. En particulier, on établit la meilleure borne uniforme connue pour la complexité bilinéaire, aussi bien symétrique qu'asymétrique, de la multiplication dans les extensions finies de $\mathbb{F}_2$ qui est un cas fondamental pour les utilisations concrètes à des fins cryptogra-

phiques. Plus précisément, on obtient :

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{477}{26}n + \frac{45}{2}$$

et

$$\mu_2(n) \leq \frac{189}{22}n + 18.$$

On améliore aussi les bornes uniformes symétriques et asymétriques sur $\mathbb{F}_q$, $\mathbb{F}_{q^2}$, $\mathbb{F}_p$ et $\mathbb{F}_{p^2}$ précédemment connues. De plus, on formalise une méthode générale permettant d'obtenir une borne uniforme pour la complexité bilinéaire à partir d'une tour de corps de fonctions dont le genre et le nombre de places de chaque étage vérifient certaines hypothèses.

Chapitre 1

Préliminaires

1.1 Quelques rappels sur les corps de fonctions algébriques

Cette section présente les notions et résultats principaux concernant les corps de fonctions algébriques qui seront utiles tout au long de ce mémoire. On suit essentiellement la présentation de [Sti08], dont on adoptera généralement les notations et où l'on pourra trouver les démonstrations des résultats classiques énoncés ici.

Dans cette section, K désigne un corps quelconque.

1.1.1 Places

Définition 1.1.1.1. *Un corps de fonctions algébriques F/K en une variable sur K est une extension de corps $F \supseteq K$ telle que F est une extension algébrique finie de $K(x)$ pour un élément $x \in F$ transcendant sur K.*

L'ensemble $\tilde{K} := \{z \in F \mid z \text{ est algébrique sur } K\}$ est un sous-corps de F appelé corps des constantes de F/K. On a $K \subseteq \tilde{K} \subseteq F$ et on vérifie facilement que $F/\tilde{K}$ est un corps de fonctions sur $\tilde{K}$.

Définition 1.1.1.2. *On dit que K est le corps plein des constantes de F si K est algébriquement clos dans F, c'est-à-dire si $K = \tilde{K}$.*

Remarques.

1) Un corps de fonctions F/K est souvent représenté comme une extension algébrique simple d'un corps de fonctions rationnelles $K(x)$, i.e. $F = K(x, y)$ où $\phi(y) = 0$ pour un polynôme irréductible $\phi(T) \in K(x)[T]$. En particulier, le corps de fonctions le plus simple est évidemment le corps des fonctions rationnelles $K(x)$. D'un point de vue géométrique, dans ce cas, la courbe lisse projective associée à $K(x)$ est clairement la droite projective. En fait, on a le lien suivant : si F/K est le corps des fonctions rationnelles sur la courbe $\mathscr{C}$, alors F/K est une extension de degré n d'une extension transcendante pure $K(x)$ si et seulement si il y a un morphisme non-constant (appelé aussi revêtement) $f : \mathscr{C} \to \mathbb{P}^1$ de degré $\deg f = n$, où $\mathbb{P}^1$ désigne la droite projective. Plus généralement dans ce même cas, tout élément $z \in F$ transcendant sur K définit un revêtement φ de la droite projective

$\mathbb{P}^1$, dont le degré divise $\deg f = [F : K(x)]$. De plus, on a le degré de φ qui est égal au degré du diviseur des zéros (ou ce qui revient au même des pôles) de z, à savoir $\deg \varphi = \deg(z)_0 = \deg(z)_\infty$ (voir Théorème 1.1.3.6).

2) Si la courbe $\mathscr{C}$ est absolument irréductible (c'est-à-dire irréductible dans toute extension de K ; on dit aussi que $\mathscr{C}$ est géométriquement irréductible), le corps plein des constantes du corps de fonctions algébriques F/K associé à la courbe $\mathscr{C}$ est K. Dans les autres cas, il est possible que le corps plein des constantes contienne strictement K.
Par exemple, considérons le corps de fonctions algébriques $F/\mathbb{F}_q = \mathrm{Frac}\left(\mathbb{F}_q[X,Y]/\langle Y^2+1\rangle\right)$ associé à la courbe $\mathscr{C}$ d'équation affine $Y^2+1=0$, où -1 n'est pas un carré dans $\mathbb{F}_q$. Alors, $\mathscr{C}$ est clairement irréductible sur $\mathbb{F}_q$ mais pas absolument irréductible et $F/\mathbb{F}_q = \mathbb{F}_{q^2}(X)$.

Définition 1.1.1.3. *Un anneau de valuation d'un corps de fonctions algébriques F/K est un anneau $\mathcal{O} \subseteq F$ qui vérifie les deux propriétés suivantes :*

(i) $K \subsetneq \mathcal{O} \subsetneq F$,

(ii) pour tout $z \in F$, *on a* $z \in \mathcal{O}$ *ou* $z^{-1} \in \mathcal{O}$.

Notons que si $\mathcal{O}$ est un anneau de valuation du corps de fonctions algébriques F/K, alors $\mathcal{O}$ est un anneau local. Son unique idéal maximal est $P := \mathcal{O}\backslash\mathcal{O}^\times$, où $\mathcal{O}^\times := \{z \in \mathcal{O} \mid \exists\, w \in \mathcal{O} \text{ tel que } zw = 1\}$ est le groupe des unités de $\mathcal{O}$. De plus, P est un idéal principal. Un élément $t \in F$ tel que $P = t\mathcal{O}$ est appelé élément primitif ou paramètre local de P. Tout $0 \neq z \in F$ admet alors une unique écriture de la forme $z = t^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathcal{O}^\times$, et tout idéal $\{0\} \neq I \subseteq \mathcal{O}$ est de la forme $I = t^n\mathcal{O}$ pour un certain $n \in \mathbb{N}$.

Définition 1.1.1.4. *Une place P dans le corps de fonctions algébriques F/K est l'idéal maximal d'un certain anneau de valuation de F/K. L'ensemble de toutes les places dans F/K sera noté $\mathbb{P}_F$.*

Si $\mathcal{O}$ est un anneau de valuation de F/K et P est son idéal maximal, alors $\mathcal{O}$ est uniquement déterminé par P. En effet, on a $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. Ainsi, on note $\mathcal{O}_P := \mathcal{O}$, appelé l'anneau de valuation de la place P.

Pour toute place $P \in \mathbb{P}_F$ on peut définir une valuation discrète de F/K $v_P : F \to \mathbb{Z} \cup \{\infty\}$ de la façon suivante : on choisit $t_P \in F$ un paramètre local de P et on pose $v_P(0) := \infty$ et $v_P(z) := n$ pour tout $0 \neq z \in F$ tel que $z = t^n u$ où $n \in \mathbb{Z}$ et $u \in \mathcal{O}_P^\times$. Cette définition est valable car l'entier n dans l'écriture de z ne dépend que de la place P et non pas du choix du paramètre local t_P.

On a alors les caractérisations suivantes :

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \mid v_P(z) \geq 0\}, \\ \mathcal{O}_P^\times &= \{z \in F \mid v_P(z) = 0\}, \\ P &= \{z \in F \mid v_P(z) > 0\}. \end{aligned}$$

Définition 1.1.1.5. *Soient $z \in F$ et $P \in \mathbb{P}_F$.*

(a) Si $v_P(z) > 0$, on dit que P est un zéro de z et on appelle $m := v_P(z)$ l'ordre du zéro P.

(b) Si $v_P(z) < 0$, on dit que P est un pôle de z et on appelle $m := -v_P(z)$ l'ordre du pôle P.

Définition 1.1.1.6. *Le corps $F_P := \mathcal{O}_P/P$ est appelé corps de classe résiduel de P. On définit l'application de classe résiduelle relativement à P par*

$$\begin{array}{ccc} F & \longrightarrow & F_P \cup \{\infty\} \\ x & \longmapsto & x(P) \end{array}$$

où $x(P)$ est la classe de x modulo P si $x \in \mathcal{O}_P$ et $x(P) := \infty$ sinon.

Cette application permet de considérer K comme un sous-corps de F_P. En effet, comme $K \subseteq \mathcal{O}_P$ et que $K \cap P = \{0\}$, l'application de classe résiduelle $\mathcal{O}_P \to \mathcal{O}_P/P$ induit une injection canonique de K dans $\mathcal{O}_P/P$. (Notons qu'il en est de même pour $\tilde{K}$.) Ceci donne un sens à la définition suivante :

Définition 1.1.1.7. *On appelle degré de la place P, et on note* $\deg P := [F_P : K]$.

Le degré d'une place est toujours fini, en particulier :

Proposition 1.1.1.8. *Si P est une place de F/K et $0 \neq x \in P$, alors*

$$\deg P \leq [F : K(x)] < \infty.$$

L'ensemble $\mathbb{P}_F$ des places d'un corps de fonctions F/K est non-vide, plus précisément :

Proposition 1.1.1.9. *Tout élément d'un corps de fonctions algébrique F/K qui est transcendant sur K a au moins un zéro et un pôle.*

Une conséquence de ce résultat est que le corps des constantes $\tilde{K}$ est une extension finie (et bien sûr algébrique) de K.

1.1.2 Indépendance des valuations

L'indépendance des valuations est un résultat important qui intervient notamment dans le problème du déplacement du support d'un diviseur ; cela nous permettra d'établir un lemme très utile pour l'utilisation pratique de l'algorithme de type Chudnovsky. Le théorème d'indépendance, ou théorème d'approximation faible, dit que si $v_1, ..., v_n$ sont des valuations discrètes deux à deux distinctes de F/K et que l'on connaît les $n-1$ premières valuations $v_1(z), \ldots, v_{n-1}(z)$ d'un élément $z \in F$, alors on ne peut rien dire sur la n-ième valuation $v_n(z)$.

Théorème 1.1.2.1. ***Théorème d'approximation faible.*** *Soient F/K un corps de fonctions, $P_1, \ldots, P_n$ des places distinctes deux à deux de F/K, $x_1, \ldots, x_n \in F$, et $r_1, \ldots, r_n \in \mathbb{Z}$. Alors il y a un élément $x \in F$ tel que*

$$v_{P_i}(x - x_i) = r_i \text{ pour } i = 1, \ldots, n.$$

Ce théorème joue un rôle important dans la démonstration des deux résultats suivants.

Corollaire 1.1.2.2. *Tout corps de fonctions a un nombre infini de places.*

Proposition 1.1.2.3. *Soient F/K un corps de fonctions et $P_1, \ldots, P_r$ des zéros de l'élément $x \in F$. Alors*

$$\sum_{i=1}^{r} v_{P_i}(x). \deg P_i \leq [F : K(x)].$$

Corollaire 1.1.2.4. *Dans un corps de fonctions F/K, tout élément $0 \neq x \in F$ n'a qu'un nombre fini de zéros et de pôles.*

1.1.3 Diviseurs

À partir de maintenant F/K dénotera toujours un corps de fonctions algébriques en une variable sur K, où K est le corps plein des constantes. Cette hypothèse n'est pas critique pour la théorie, puisque comme on l'a rappelé dans le paragraphe 1.1.1, le corps des constantes $\tilde{K}$ est une extension finie de K, et F peut être vu comme un corps de fonctions sur $\tilde{K}$.

Définition 1.1.3.1. *Le groupe abélien libre engendré par les places de F/K est noté* $\mathrm{Div}(F)$ *et appelé le groupe des diviseurs de F/K. Les éléments de* $\mathrm{Div}(F)$ *sont appelés diviseurs de F/K.*

Un diviseur de F/K est donc une somme formelle $\mathcal{D} = \sum_{P \in \mathbb{P}_F} n_P P$, où les $n_P \in \mathbb{Z}$ sont presque tous nuls. On somme deux diviseurs $\mathcal{D} = \sum_{P \in \mathbb{P}_F} n_P P$ et $\mathcal{D}' = \sum_{P \in \mathbb{P}_F} n'_P P$ en sommant terme à terme les coefficients de chacun des diviseurs :

$$\mathcal{D} + \mathcal{D}' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

Définition 1.1.3.2. *On appelle support d'un diviseur $\mathcal{D} = \sum_{P \in \mathbb{P}_F} n_P P \in \mathrm{Div}(F)$ l'ensemble* $\operatorname{supp} \mathcal{D} := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$.

Définition 1.1.3.3. *Pour $Q \in \mathbb{P}_F$ et $\mathcal{D} = \sum_{P \in \mathbb{P}_F} n_P P \in \mathrm{Div}(F)$, on définit la valuation de $\mathcal{D}$ en Q, notée $v_Q(\mathcal{D})$, en posant $v_Q(\mathcal{D}) := n_Q$.*

Grâce à la définition précédente, on peut définir une relation d'ordre partielle sur $\mathrm{Div}(F)$, en posant pour $\mathcal{D}_1, \mathcal{D}_2 \in \mathrm{Div}(F)$:

$$\mathcal{D}_1 \leq \mathcal{D}_2 \iff v_P(\mathcal{D}_1) \leq v_P(\mathcal{D}_2), \text{ pour tout } P \in \mathbb{P}_F.$$

Définition 1.1.3.4. *Un diviseur $\mathcal{D} \geq 0$ est dit positif ou effectif.*

Notons que dans la définition précédente, 0 dénote l'élément neutre du groupe $\mathrm{Div}(F)$, c'est-à-dire le diviseur dont tous les coefficients sont nuls.

On étend la notion de degré à tout diviseur $\mathcal{D} \in \mathrm{Div}(F)$, en posant

$$\deg \mathcal{D} := \sum_{P \in \mathbb{P}_F} v_P(\mathcal{D}) \deg P.$$

On obtient alors un morphisme $\deg : \mathrm{Div}(F) \to \mathbb{Z}$.

Le corollaire 1.1.2.4 nous assure que la définition suivante a un sens :

Définition 1.1.3.5. *Soit $0 \neq x \in F$. Notons Z et N respectivement l'ensemble des zéros et l'ensemble des pôles de x dans $\mathbb{P}_F$. On définit*

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \text{ le diviseur des zéros de } x$$

et

$$(x)_\infty := \sum_{P \in N} (-v_P(x))P, \text{ le diviseur des pôles de } x.$$

On pose alors

$$(x) := (x)_0 - (x)_\infty,$$

appelé le diviseur principal de x.

Notons que pour tout $0 \neq x \in F$, on a $(x)_0 \geq 0$, $(x)_\infty \geq 0$ et

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P.$$

Le corps K étant supposé algébriquement clos, les éléments $0 \neq x \in F$ qui sont constants sont alors caractérisés par :

$$x \in K \iff (x) = 0.$$

Rappelons — en anticipant un peu — que l'on a le théorème suivant, dont la démonstration repose sur les espaces de Riemann-Roch qui seront l'objet du prochain paragraphe :

Théorème 1.1.3.6. *Tout diviseur principal est de degré 0. Plus précisément, pour $x \in F\backslash K$, on a $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$.*

Définition 1.1.3.7. *L'ensemble $\mathrm{Princ}(F) := \{(x) \mid 0 \neq x \in F\}$ est un sous-groupe de $\mathrm{Div}(F)$ appelé groupe des diviseurs principaux de F/K.*
Le groupe quotient $\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F)$ est appelé groupe des classes de diviseurs.

Pour $\mathcal{D} \in \mathrm{Div}(F)$, on notera $[\mathcal{D}]$ l'élément correspondant du groupe quotient $\mathrm{Cl}(F)$. Deux diviseurs $\mathcal{D}, \mathcal{D}' \in \mathrm{Div}(F)$ sont dits équivalents, noté $\mathcal{D} \sim \mathcal{D}'$, si $[\mathcal{D}] = [\mathcal{D}']$ c'est-à-dire si $\mathcal{D} = \mathcal{D}' + (x)$ pour un certain $x \in F\backslash\{0\}$. On vérifie facilement que l'on définit bien ainsi une relation d'équivalence.

D'après le théorème 1.1.3.6, des diviseurs équivalents sont de même degré, on peut donc poser $\deg[\mathcal{A}] := \deg \mathcal{A}$, pour toute classe de diviseur $[\mathcal{A}] \in \mathrm{Cl}(F)$.

Lorsque le corps des constantes est un corps fini, le cas des classes diviseurs de degré 0 joue un rôle fondamental, notamment dans le problème de l'existence des diviseurs de dimension nulle, qui sera traité plus loin.

Définition 1.1.3.8. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques dont le corps des constantes est le corps fini $\mathbb{F}_q$. L'ensemble $\mathrm{Div}^0(F) := \{\mathcal{A} \in \mathrm{Div}(F) \mid \deg \mathcal{A} = 0\}$ est un sous-groupe de $\mathrm{Div}(F)$ appelé groupe des diviseurs de degré zéro de $F/\mathbb{F}_q$. Le groupe quotient $\mathrm{Cl}^0(F/\mathbb{F}_q) := \mathrm{Div}^0(F)/\mathrm{Princ}(F) = \{[\mathcal{A}] \in \mathrm{Cl}(F/\mathbb{F}_q) \mid \deg[\mathcal{A}] = 0\}$ est appelé groupe des classes de diviseurs de degré zéro de $F/\mathbb{F}_q$.*

Proposition 1.1.3.9. *Le groupe* $\mathrm{Cl}^0(F/\mathbb{F}_q)$ *est de cardinal fini. Son ordre est appelé le nombre de classes de diviseurs de degré 0 de* $F/\mathbb{F}_q$ *et est noté* h_F.

Si $[\mathcal{B}] \in \mathrm{Cl}(F/\mathbb{F}_q)$ est de degré n, l'application

$$\begin{array}{ccc} \mathrm{Cl}^0(F/\mathbb{F}_q) & \longrightarrow & \{[\mathcal{A}] \in \mathrm{Cl}(F/\mathbb{F}_q) \mid \deg[\mathcal{A}] = n\} \ , \\ [\mathcal{A}] & \longmapsto & [[\mathcal{A}] + [\mathcal{B}]] \end{array}$$

est clairement bijective. On en déduit que, pour tout $n \in \mathbb{N}$, l'ensemble des classes de diviseurs de degré n, noté $\mathrm{Cl}^n(F/\mathbb{F}_q)$, est aussi de cardinal h_F.

1.1.4 Espaces et théorème de Riemann-Roch

Définition 1.1.4.1. *Soit* $\mathcal{D} \in \mathrm{Div}(F)$. *On définit l'espace de Riemann-Roch associé au diviseur* $\mathcal{D}$ *par* $\mathcal{L}(\mathcal{D}) := \{x \in F \mid (x) \geq -\mathcal{D}\} \cup \{0\}$.

Cette définition signifie que si $\mathcal{D} := \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$ où pour tous $i \in \{1, \ldots, r\}$ et $j \in \{1, \ldots, s\}$, $n_i > 0$, $m_j > 0$ et $P_i, Q_j \in \mathbb{P}_F$, alors $x \in F \backslash \{0\}$ est un élément de $\mathcal{L}(\mathcal{D})$ si et seulement si les deux conditions suivantes sont vérifiées :

(i) pour tout $j \in \{1, \ldots, s\}$, Q_j est un zéro de x d'ordre au moins m_j,

(ii) les pôles de x appartiennent à l'ensemble $\{P_1, \ldots, P_r\}$ et si P_i est un pôle de x alors son ordre est au plus n_i.

La proposition suivante rappelle les principales propriétés liées à ces espaces.

Proposition 1.1.4.2. *Soit* $\mathcal{D} \in \mathrm{Div}(F)$. *Alors*

(a) $\mathcal{L}(\mathcal{D})$ *est un* K*-espace vectoriel.*

(b) $\mathcal{L}(\mathcal{D}) \neq \{0\}$ *si et seulement si il existe un diviseur* $\mathcal{D}' \sim \mathcal{D}$ *tel que* $\mathcal{D}' \geq 0$.

(c) Si $\mathcal{D}'$ *est un diviseur équivalent à* $\mathcal{D}$ *alors* $\mathcal{L}(\mathcal{D})$ *et* $\mathcal{L}(\mathcal{D}')$ *sont isomorphes en tant que* K*-espaces vectoriels.*

(d) $x \in \mathcal{L}(\mathcal{D})$ *si et seulement si* $v_P(x) \geq -v_P(\mathcal{D})$ *pour tout* $P \in \mathbb{P}_F$.

(e) $\mathcal{L}(0) = K$.

(f) Si $\deg \mathcal{D} < 0$ *alors* $\mathcal{L}(\mathcal{D}) = \{0\}$. *En particulier,* $\mathcal{L}(\mathcal{D}) = \{0\}$ *dès que* $\mathcal{D} < 0$.

Définition 1.1.4.3. *Pour* $\mathcal{D} \in \mathrm{Div}(F)$, *on définit la dimension du diviseur* $\mathcal{D}$ *en posant* $\dim \mathcal{D} := \dim \mathcal{L}(\mathcal{D})$. *On notera aussi parfois* $\ell(\mathcal{D})$ *la dimension du diviseur* $\mathcal{D}$.

D'après le (c) de la proposition précédente, des diviseurs équivalents ont même dimension. On désignera donc de la même façon la dimension d'un diviseur et la dimension de sa classe. De plus, grâce au (b) de cette même proposition, on obtient la caractérisation suivante des diviseurs de dimension nulle :

Lemme 1.1.4.4. ***Caractérisation des diviseurs de dimension nulle.***
Soit $\mathcal{D} \in \mathrm{Div}(F)$. *On a l'équivalence*

$$\dim \mathcal{D} = 0 \iff \nexists\ \mathcal{D}' \in \mathrm{Div}(F) \text{ tel que } \mathcal{D}' \sim \mathcal{D} \text{ et } \mathcal{D}' \geq 0.$$

Enfin, on définit le genre, qui est l'invariant le plus important d'un corps de fonctions algébriques.

Définition 1.1.4.5. *On appelle genre de F/K l'entier positif*

$$g(F/K) := \max\left\{ \deg \mathcal{D} - \dim \mathcal{D} + 1 \mid \mathcal{D} \in \mathrm{Div}(F) \right\}.$$

Le genre sera parfois noté g_F, ou plus simplement g s'il n'y a pas d'ambiguité sur le corps de fonctions algébriques auquel on fait référence.

Définition 1.1.4.6. *Pour tout $\mathcal{D} \in \mathrm{Div}(F)$, on appelle indice de spécialité de $\mathcal{D}$ et on note*

$$i(\mathcal{D}) := \dim \mathcal{D} - \deg \mathcal{D} + g_F - 1.$$

Un diviseur $\mathcal{D} \in \mathrm{Div}(F)$ tel que $i(\mathcal{D}) = 0$ est dit non-spécial ; dans le cas contraire, il est dit spécial.

Remarquons que l'indice de spécialité d'un diviseur ne dépend que de sa classe dans le groupe quotient $\mathrm{Cl}(F)$. Notons aussi que l'indice de spécialité est un entier positif d'après la définition de g_F.

On verra dans la suite que les diviseurs non-spéciaux, et particulièrement ceux de degré $g-1$, interviennent de façon naturelle dans l'algorithme de type Chudnovsky et que pouvoir établir leur existence contribue à l'amélioration des bornes du rang de tenseur.

Définition 1.1.4.7. *Si F/K est un corps de fonctions algébriques de genre g, on appelle diviseur canonique de F/K un diviseur de degré $2g-2$ et de dimension g.*

Il existe toujours un diviseur canonique et les diviseurs canoniques sont tous équivalents. En conséquence, les diviseurs canoniques constituent à eux seuls toute une classe de diviseurs, appelée la classe canonique de F/K.

De plus, par dualité, on a le résultat suivant :

Théorème 1.1.4.8. *Soient $\mathcal{D}$ un diviseur quelconque et $\mathcal{W}$ un diviseur canonique de F/K. Alors*

$$i(\mathcal{D}) = \dim(\mathcal{W} - \mathcal{D}).$$

On peut maintenant énoncer le théorème de Riemann-Roch :

Théorème 1.1.4.9. ***Théorème de Riemann-Roch.*** *Soit F/K un corps de fonctions algébriques de genre g et soit $\mathcal{W}$ un diviseur canonique de F/K. Pour tout diviseur $\mathcal{D} \in \mathrm{Div}(F)$, on a*

$$\dim \mathcal{D} = \deg \mathcal{D} + 1 - g + \dim(\mathcal{W} - \mathcal{D}).$$

Un autre résultat intéressant est donné par le théorème d'approximation fort, qui est une amélioration du théorème d'approximation faible.

Théorème 1.1.4.10. ***Théorème d'approximation fort.*** *Soit F/K un corps de fonctions algébriques. Soient $S \subsetneq \mathbb{P}_F$ un sous-ensemble propre de $\mathbb{P}_F$ et $P_1, \ldots, P_N \in S$. Supposons que $x_1, \ldots, x_r \in F$ et $n_1, \ldots, n_r \in \mathbb{Z}$ soient donnés.*
Alors il existe un élément $x \in F$ tel que

$$\begin{array}{rrcl} \forall\, i \in \{1,\ldots,r\}, & v_{P_i}(x - x_i) & = & n_i, \\ \text{et } \forall\, P \in S\backslash\{P_1,\ldots,P_N\}, & v_P(x) & \geq & 0. \end{array}$$

En particulier, ce théorème permet d'établir le lemme suivant qui sera utile dans la suite.

Lemme 1.1.4.11. ***Déplacement du support.*** *Soit F/K un corps de fonctions algébriques. Soit $T := \{P_1, \ldots, P_N\}$ un ensemble de places de F de degrés quelconques. Alors pour tout $\mathcal{D} \in \mathrm{Div}(F)$, il existe $\mathcal{D}' \in \mathrm{Div}(F)$ tel que $\mathcal{D} \sim \mathcal{D}'$ et $\mathrm{supp}\,\mathcal{D}' \cap T = \varnothing$.*

Preuve. On cherche $x \in F$ tel que $\mathrm{supp}(\mathcal{D} + (x)) \cap T = \varnothing$. On applique le théorème d'approximation fort à $S := T$ et à $x_1, \ldots, x_N \in F$ et $n_1, \ldots, n_N \in \mathbb{Z}$ définis de la façon suivante :

- si $P_i \notin \mathrm{supp}\,\mathcal{D}$, alors $x_i := 0$ et $n_i := 0$,
- si $P_i \in \mathrm{supp}\,\mathcal{D}$, alors $x_i := 0$ et $n_i := -v_{P_i}(\mathcal{D})$.

Remarquons que comme $\mathbb{P}_F$ est de cardinal infini, T est bien un sous-ensemble propre de $\mathbb{P}_F$. On pose alors $\mathcal{D}' := \mathcal{D} + (x)$, où $x \in F$ est donné par le théorème d'approximation fort, donc vérifie pour tout $i \in \{1, \ldots, N\}$, $v_{P_i}(x) = 0$ si $P_i \notin \mathrm{supp}\,\mathcal{D}$ et $v_{P_i}(x) = -v_{P_i}(\mathcal{D})$ si $P_i \in \mathrm{supp}\,\mathcal{D}$. Ainsi, $\mathcal{D} \sim \mathcal{D}'$ et pour tout $P_i \in T$, $v_{P_i}(\mathcal{D}') = v_{P_i}(\mathcal{D}) + v_{P_i}(x) = 0$, c'est-à-dire $P_i \notin \mathrm{supp}\,\mathcal{D}'$. □

Enfin, notons que par le théorème de Riemman-Roch, on connait précisément la dimension d'un diviseur $\mathcal{D}$ tel que $\deg \mathcal{D} \geq 2g - 1$ en fonction de son degré. En effet, dans ce cas, on a $i(\mathcal{D}) = \dim(\mathcal{W} - \mathcal{D}) = 0$ (où $\mathcal{W}$ est un diviseur canonique) puisque $\deg(\mathcal{W} - \mathcal{D}) < 0$. En revanche, lorsque $\deg \mathcal{D} \leq 2g - 2$, on a seulement l'inégalité

$$\dim \mathcal{D} \geq \deg \mathcal{D} + 1 - g.$$

Le théorème de Clifford donne alors une majoration pour la dimension de $\mathcal{D}$:

Théorème 1.1.4.12. ***Théorème de Clifford.*** *Pour tout diviseur $\mathcal{D}$ de F/K tel que $0 \leq \deg \mathcal{D} \leq 2g - 2$, on a*

$$\dim \mathcal{D} \leq 1 + \frac{1}{2} \deg \mathcal{D}.$$

1.1.5 Corps de fonctions algébriques sur un corps des constantes finis

Jusqu'à présent, nous avons rappelé les bases de la théorie des corps de fonctions algébriques sur un corps quelconque. Nous allons maintenant considérer le cas particulier où le corps des constantes est un corps fini. Notre intérêt principal concerne les places de degré 1 d'un corps de fonctions et le groupe des classes de diviseurs de degré 0.

Dans cette section, F dénote donc un corps de fonctions algébriques de genre g dont le corps des constantes est le corps fini $\mathbb{F}_q$.

La fonction Zêta d'un corps de fonctions

Considérons l'ensemble suivant :

$$\mathbb{A}_n := \{\mathcal{D} \in \mathrm{Div}(F) \mid \mathcal{D} \geq 0 \text{ et } \deg \mathcal{D} = n\}, \tag{1.1}$$

et notons

$$A_n := |\mathbb{A}_n| \tag{1.2}$$

son cardinal.
On sait que pour tout entier n, l'ensemble $\mathbb{A}_n$ est fini ; en particulier, $A_0 = 1$ car $\mathbb{A}_0 = \{0\}$ et A_1 est le nombre de places de degré 1 dans F. De plus, on a les résultats suivants :

Proposition 1.1.5.1. *(a) Pour une classe fixée de diviseurs $[\mathcal{C}] \in \mathrm{Cl}(F)$, on a*

$$\big|\{\mathcal{A} \in [\mathcal{C}] \mid \mathcal{A} \geq 0\}\big| = \frac{1}{q-1}(q^{\dim[\mathcal{C}]} - 1).$$

(b) Pour tout entier $n > 2g - 2$,

$$A_n = \frac{h_F}{q-1}(q^{n+1-g} - 1).$$

(c) D'après [NX96, (6)], si $g \geq 2$ alors on a

$$2\sum_{n=0}^{g-2} q^{\frac{g-1-n}{2}} A_n + A_{g-1} \leq \frac{h_F}{(q^{1/2}-1)^2}. \tag{1.3}$$

En particulier,

$$\frac{h_F}{(q^{1/2}-1)^2} > A_{g-1}. \tag{1.4}$$

Enfin, les entiers A_n définis par (1.2) interviennent dans la définition de la fonction Zêta de $F/\mathbb{F}_q$:

Définition 1.1.5.2. *La série formelle*

$$Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]]$$

est appelée la fonction Zêta de $F/\mathbb{F}_q$.

Rappelons que cette série formelle converge pour $|t| < q^{-1}$. De plus, $Z(t)$ peut être étendue à une fonction rationnelle sur $\mathbb{C}$ et a un pôle simple en $t = 1$. Plus précisément :

Proposition 1.1.5.3. *(a) Tout corps de fonctions $F/\mathbb{F}_q$ de genre 0 est rationnel, et sa fonction Zêta est*

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

(b) Si $F/\mathbb{F}_q$ est de genre $g \geq 1$, sa fonction Zêta peut s'écrire sous la forme $Z(t) = F(t) + G(t)$ avec

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[\mathcal{C}] \leq 2g-2} q^{\dim[\mathcal{C}]} \cdot t^{\deg[\mathcal{C}]}$$

et

$$G(t) = \frac{h_F}{q-1}\big(q^g t^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t}\big).$$

De plus, la fonction Zêta satisfait la relation importante suivante :

Proposition 1.1.5.4. *La fonction Zêta de $F/\mathbb{F}_q$ satisfait l'équation fonctionnelle*

$$Z(t) = q^{g-1}t^{2g-2}Z(\frac{1}{qt}).$$

Définition 1.1.5.5. *Le polynôme $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ est appelé le L-polynôme de $F/\mathbb{F}_q$.*

D'après la proposition 1.1.5.3, il est clair que $L(t)$ est un polynôme de degré au plus $2g$. De plus, $L(t)$ contient toutes les informations sur les nombres A_n pour $n \geq 0$ puisque

$$L(t) = (1-qt)(1-t)\sum_{n=0}^{\infty} A_n t^n. \tag{1.5}$$

Théorème 1.1.5.6. *(a) $L(t) \in \mathbb{Z}[t]$ et $\deg L(t) = 2g$.*

(b) (Équation fonctionnelle) $L(t) = q^g t^{2g} L(1/qt)$.

(c) $L(1) = h_F$.

(d) Si on écrit $L(t)$ sous la forme $L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}$, alors on a :

(1) $a_0 = 1$ et $a_{2g} = q^g$.

(2) $a_{2g-i} = q^{g-i}a_i$ pour $0 \leq i \leq g$.

(3) $a_1 = N - (q+1)$ où N est le nombre de places $P \in \mathbb{P}_F$ de degré 1.

(e) $L(t)$ se factorise dans $\mathbb{C}[t]$ sous la forme

$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t). \tag{1.6}$$

Les nombres complexes $\alpha_1, \ldots, \alpha_{2g}$ sont des entiers algébriques et ils peuvent être ordonnés de sorte que $\alpha_i\alpha_{g+i} = q$ pour $i = 1, \ldots, g$.

(f) Si $L_r(t) := (1-t)(1-q^r t)Z_r(t)$ dénote le L-polynôme de l'extension du corps des constantes $F_r = F\mathbb{F}_{q^r}$, où $Z_r(t)$ est la fonction Zêta de F_r, alors :

$$L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t),$$

où les α_i sont donnés par (1.6).

Rappelons que F_r, l'extension du corps des constantes de $F/\mathbb{F}_q$ de degré r, est le compositum de F et $\mathbb{F}_{q^r}$:

$$F_r := F\mathbb{F}_{q^r} \subseteq \bar{F}$$

où $\bar{F} = F\bar{\mathbb{F}}_q$ pour une clôture algébrique $\bar{\mathbb{F}}_q$ fixée de $\mathbb{F}_q$.
En particulier, les fonctions Zêta de F et F_r sont reliées par :

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t)$$

pour tout $t \in \mathbb{C}$ (où ζ parcourt l'ensemble des racines r-ième de l'unité).
Notons que cette relation permet d'établir la proposition importante suivante :

Proposition 1.1.5.7. *Pour tout $k \in \mathbb{Z}$, il existe un diviseur de degré k dans $F/\mathbb{F}_q$.*

De plus, le théorème précédent montre que le nombre

$$N(F/\mathbb{F}_q) := N = \big|\{P \in \mathbb{P}_F \mid \deg P = 1\}\big| \tag{1.7}$$

de places rationnelles de $F/\mathbb{F}_q$ peut être facilement calculé si le L-polynôme $L(t)$ de $F/\mathbb{F}_q$ est connu.
Plus généralement, pour $r \geq 1$, on définit l'entier

$$N_r := N(F_r/\mathbb{F}_{q^r}) = \big|\{P \in \mathbb{P}_{F_r} \mid \deg P = 1\}\big|. \tag{1.8}$$

Voici un corollaire important du résultat précédent. En particulier, il joue un rôle essentiel dans l'établissement du théorème de Hasse-Weil.

Corollaire 1.1.5.8. *Pour tout $r \geq 1$, on a*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r,$$

où $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ sont les réciproques des racines de $L(t)$. En particulier, comme $N_1 = N(F/\mathbb{F}_q)$, on a

$$N(F/\mathbb{F}_q) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Bornes sur le nombre de places rationnelles et le genre

Théorème 1.1.5.9. ***Borne de Hasse-Weil.*** *Le nombre N de places de $F/\mathbb{F}_q$ de degré 1 satisfait l'inégalité suivante :*

$$|N - (q+1)| \leq 2gq^{1/2}.$$

Ce résultat important est dû à Hasse pour le cas particulier où $g = 1$ et à Weil pour le cas général.
Remarquons qu'en appliquant cette borne à $F_r/\mathbb{F}_{q^r}$, l'extension du corps des constantes de $F/\mathbb{F}_q$ de degré r, on obtient :

$$|N_r - (q^r + 1)| \leq 2gq^{r/2}.$$

Définition 1.1.5.10. *Un corps de fonctions algébriques $F/\mathbb{F}_q$ de genre g, qui atteint la borne de Hasse-Weil, c'est-à-dire qui a exactement $q + 1 + 2gq^{1/2}$ places de degré 1 est dit maximal.*

Une condition nécessaire pour que $F/\mathbb{F}_q$ soit maximal est donc que q soit un carré. De plus, le résultat suivant, dû à Ihara [Iha81], montre qu'un corps de fonctions ne peut être maximal que si son genre est petit relativement à q :

Proposition 1.1.5.11. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques maximal de genre g. Alors $g \leq \frac{1}{2}(q - q^{1/2})$.*

On définit

$$B_r := B_r(F/\mathbb{F}_q) := \big|\{P \in \mathbb{P}_F \ ; \ \deg P = r\}\big|,$$

le nombre de places de degré r dans $F/\mathbb{F}_q$. En particulier, remarquons que $B_1 = N(F/\mathbb{F}_q)$. De plus, les quantités N_r et B_s sont reliées par l'égalité suivante :

$$N_r = \sum_{d|r} d \cdot B_d. \tag{1.9}$$

Par la formule d'inversion de Möbius, (1.9) devient :

$$r \cdot B_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) \cdot N_d \tag{1.10}$$

où $\mu : \mathbb{N} \to \{-1, 0, 1\}$ est la fonction de Möbius, définie par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{s'il existe un entier } k > 1 \text{ tel que } k^2 | n, \\ (-1)^l & \text{si } n \text{ est le produit de } l \text{ premiers distincts.} \end{cases}$$

On définit

$$S_r := -\sum_{i=1}^{2g} \alpha_i^r \tag{1.11}$$

où $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ sont les réciproques des racines de $L(t)$ (si $g = 0$, on pose $S_r := 0$). Par le corollaire 1.1.5.8, on a alors

$$N_r = q^r + 1 + S_r. \tag{1.12}$$

Ainsi, comme

$$\sum_{d|r} \mu\left(\frac{r}{d}\right) = 0 \text{ pour } r > 1,$$

en remplaçant (1.12) dans (1.10), on obtient :

$$B_r = \frac{1}{r} \cdot \sum_{d|r} \mu\left(\frac{r}{d}\right)(q^d + S_d).$$

Une des conséquences de ce résultat est donnée par le lemme suivant [Sti08, Corollary 5.2.10], qui sera très utile :

Lemme 1.1.5.12. ***Existence d'une place de degré*** n. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g. Si n est un entier tel que*

$$2g + 1 \leq q^{\frac{n-1}{2}}(\sqrt{q} - 1),$$

alors il existe au moins une place de degré n dans $F/\mathbb{F}_q$.

Enfin, on rappelle la borne suivante, due à Serre et qui est un raffinement de la borne de Hasse-Weil :

Théorème 1.1.5.13. ***Borne de Serre.*** *Le nombre $N = N(F/\mathbb{F}_q)$ de places de $F/\mathbb{F}_q$ de degré 1 satisfait l'inégalité suivante :*

$$|N - (q + 1)| \leq g[2q^{1/2}],$$

où $[\cdot]$ dénote la partie entière.

Bornes asymptotiques pour le nombre de places rationnelles

On a vu dans le paragraphe précédent que lorsque le genre du corps de fonctions considéré est petit par rapport au cardinal q du corps de base, on connait des bornes pour le nombre de places rationnelles. Ici, on s'intéresse au cas complémentaire où le genre est grand par rapport à q. Dans ce cas, la borne de Hasse-Weil ne donne pas une bonne approximation du nombre de places rationnelles, comme l'a noté Ihara dans [Iha81]. Cela motive l'introduction et l'étude des quantités suivantes :

Définition 1.1.5.14. *(a) Pour tout entier g, on définit*

$$N_q(g) := \max\{N(F) \mid F \text{ est un corps de fonctions sur } \mathbb{F}_q \text{ de genre } g\}.$$

(b) On appelle constante d'Ihara l'entier suivant :

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

Notons que la borne de Serre donne trivialement que $0 \leq A(q) \leq [2q^{1/2}]$. De façon générale, hormis le cas où q est un carré, la valeur exacte de $A(q)$ n'est pas connue ; cependant, on sait que :

(a) $A(q) > 0$ pour tout $q = p^e$ puissance d'un nombre premier p ($e \geq 1$). Plus précisément, il existe une constante $c > 0$ telle que pour tout q, $A(q) \geq c \cdot \log q$.

(b) si $q = \ell^2$ alors $A(q) = q^{1/2} - 1$.

(c) si $q = \ell^3$ alors $A(q) \geq \frac{2(\ell^2-1)}{\ell+2}$.

(d) si p est premier et $n = 2m + 1 \geq 3$ est un entier impair, alors

$$A(p^n) \geq \frac{2(p^{m+1} - 1)}{p + 1 + \epsilon} \text{ où } \epsilon = \frac{p-1}{p^m - 1}.$$

En particulier, $A(p^{2m+1}) > p^m - 1$. Ces derniers résultats proviennent de la construction récente d'une nouvelle tour récursive due à Garcia, Stichtenoth, Bassa, Beelen [GSBB12].

Quant à la meilleure borne supérieure connue, elle est due à Drinfeld et Vlăduţ :

Théorème 1.1.5.15. ***Borne de Drinfeld-Vlăduţ.*** *La constante d'Ihara admet la borne suivante :*

$$A(q) \leq q^{1/2} - 1.$$

D'après le (b) ci-dessus, cette borne est atteinte dans le cas où q est un carré.

1.2 Extensions et tours de corps de fonctions algébriques

1.2.1 Extensions de corps de fonctions algébriques

Tout corps de fonctions peut être vu comme une extension finie du corps des fonctions rationnelles. Aussi, il est intéressant de chercher des extensions de corps F'/F des corps de fonctions algébriques. Dans cette section, on rappelle quelques définitions et résultats fondamentaux relatifs aux extensions de corps de fonctions algébriques qui seront utiles par la suite [Sti08].

Extensions algébriques de corps de fonctions

Définition 1.2.1.1. *(a) Un corps de fonctions algébriques F'/K' est appelé extension algébrique de F/K si $F' \supseteq F$ est une extension de corps algébrique et $K' \supseteq K$.*

(b) L'extension algébrique F'/K' de F/K est appelée extension du corps des constantes si $F' = FK'$, le compositum de F et K'.

(c) L'extension algébrique F'/K' de F/K est dite finie si $[F' : F] < \infty$.

(d) L'extension algébrique F'/K' de F/K est appelée extension de Galois si elle est finie et si son groupe d'automorphismes

$$Aut(F'/F) := \{\sigma : F' \to F' \text{ isomorphisme} \mid \forall\, a \in F,\, \sigma(a) = a\}$$

est d'ordre $[F' : F]$. Dans ce cas, on dit que $Aut(F'/F)$ est le groupe de Galois de F'/F et on le note $Gal(F'/F) := Aut(F'/F)$.

On peut aussi considérer des extensions quelconques (pas nécessairement algébriques) de corps de fonctions, cependant nous nous restreignons aux extensions algébriques car ce sont celles-ci qui seront considérées dans la suite.

Proposition 1.2.1.2. *Soit F'/K' une extension algébrique de F/K. Alors :*

(1) K'/K est algébrique.

(2) F'/K' est une extension finie de F/K si et seulement si $[K' : K] < \infty$.

(3) Si $F_1 = FK'$, alors F_1/K' est une extension du corps des constantes de F/K, et F'/K' est une extension finie de F_1/K' ayant le même corps des constantes.

Nous allons maintenant considérer deux cas particuliers très importants d'extensions de Galois d'un corps de fonctions : les extensions de Kummer et les extensions d'Artin-Schreier. Ces deux types d'extensions seront en effet utilisées pour la construction des tours étudiées dans le chapitre 3.

Les extensions de Kummer

Proposition 1.2.1.3. *Soit F/K un corps de fonctions algébriques tel que K contient une racine n-ième primitive de l'unité, pour $n > 1$ vérifiant* $\gcd(n, \operatorname{char} K) = 1$. *Supposons que $u \in F$ est un élément satisfaisant*

$$u \neq w^d \text{ pour tout } w \in F \text{ et } d \mid n, d > 1.$$

Soit

$$F' = F(y) \text{ avec } y^n = u.$$

Une telle extension F' est appelée extension de Kummer de F. On a alors les propriétés suivantes :

(a) Le polynôme $\Phi(T) = T^n - u$ est le polynôme minimal de y sur F (en particulier, il est irréductible sur F). L'extension F'/F est de Galois de degré n, son groupe de Galois est cyclique et tous les automorphismes de F'/F sont donnés par $\sigma(u) = \zeta u$, où $\zeta \in K$ est une racine n-ième de l'unité.

(b) Si K' dénote le corps des constantes de F' et g et g' les genres respectifs de F/K et F'/K', alors

$$g' = 1 + \frac{n}{[K' : K]}\Big(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\Big(1 - \frac{r_P}{n}\Big)\deg P\Big)$$

où

$$r_P := \operatorname{pgcd}\big(n, v_P(u)\big) > 0.$$

On peut remarquer que toute extension de corps cyclique F'/F de degré n est une extension de Kummer, pourvu que n soit relativement premier avec la caractéristique de K, et que F contienne toutes les racines n-ième de l'unité, d'après un résultat bien connu de la théorie de Galois.

Corollaire 1.2.1.4. *Soient F/K un corps de fonctions et $F' = F(y)$ avec $y^n = u \in F$, où $n \not\equiv 0 \pmod{\operatorname{char} K}$ et K contient une racine n-ième primitive de l'unité. S'il y a une place $Q \in \mathbb{P}_F$ telle que $\operatorname{pgcd}\big(v_Q(u), n\big) = 1$, alors K est le corps plein des constantes de F', l'extension F'/F est cyclique de degré n, et*

$$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P \in \mathbb{P}_F}(n - r_P)\deg P.$$

Remarque. En fait, l' assertion (b) de la proposition 1.2.1.3 et le corollaire 1.2.1.4 sont encore valables sans l'hypothèse que K contienne une racine n-ième primitive de l'unité, à la seule exception que $F(y)/F$ n'est plus de Galois si K ne contient pas toutes les racines n-ième de l'unité.

Les extensions d'Artin-Schreier

Tout d'abord, énonçons la proposition dite des extensions d'Artin-Schreier.

Proposition 1.2.1.5. *Soit F/K un corps de fonctions algébriques de caractéristique $p > 0$. Supposons que $u \in F$ est un élément qui satisfait la condition suivante :*

$$u \neq w^p - w \text{ pour tout } w \in F.$$

Soit

$$F' = F(y) \text{ avec } y^p - y = u.$$

Une telle extension F'/F est appelée une extension d'Artin-Schreier de F. Pour $P \in \mathbb{P}_F$, on définit l'entier m_P par

$$m_P := \begin{cases} m & \text{s'il existe un élément } z \in F \text{ satisfaisant} \\ & v_P(u - (z^p - z)) = -m < 0 \text{ et } m \not\equiv 0 \pmod{p}, \\ -1 & \text{si } v_P(u - (z^p - z)) \geq 0 \text{ pour un élément } z \in F. \end{cases}$$

Cet entier m_P est bien défini car étant donnés $u \in F$ et $P \in \mathbb{P}_F$, on se situe bien dans un (seul) des deux cas précédents.
On a alors :

(a) F'/F est une extension de Galois cyclique de degré p. Les automorphismes de F'/F sont donnés par $\sigma(y) = y + \nu$, avec $\nu = 1, \ldots, p-1$.

(b) S'il existe au moins une place $Q \in \mathbb{P}_F$ pour laquelle $m_Q > 0$, alors K est algébriquement clos dans F', et

$$g' = g \cdot p + \frac{p-1}{2}\big(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg P\big),$$

où g et g' sont les genres respectifs de F/K et F'/K.

Il est intéressant de noter que la plupart des arguments utilisés dans la démonstration de ce résultat (voir [Sti08, §3.7]) s'appliquent en fait dans le cadre plus général suivant :

Proposition 1.2.1.6. *Soit F/K un corps de fonctions algébriques dont le corps des constantes K est de caractéristique $p > 0$. Soit $a(T)$ un polynôme de degré p^n dit additif, c'est-à-dire de la forme*

$$a(T) = \sum_{i=0}^{n} a_i T^{p^i} \in K[T]$$

et supposons qu'il soit séparable et que toutes ses racines soient dans K. Soit $u \in F$. On suppose que pour toute place $P \in \mathbb{P}_F$, il existe un élément $z \in F$ tel que

$$v_P(u - a(z)) \geq 0 \tag{1.13}$$

ou

$$v_P(u - a(z)) = -m \text{ avec } m > 0 \text{ et } m \not\equiv 0 \pmod{p}. \tag{1.14}$$

On pose $m_P := -1$ dans le cas (1.13) et $m_P := m$ dans le cas (1.14) ; alors cet entier est bien défini. Considérons l'extension $F' := F(y)$ de F, où y satisfait l'équation

$$a(y) = u.$$

S'il existe au moins une place $Q \in \mathbb{P}_F$ avec $m_Q > 0$, alors on a les propriétés suivantes :

(a) L'extension F'/F est une extension de Galois, $[F' : F] = p^n$ et le groupe de Galois de F'/F est isomorphe au groupe additif $\{\alpha \in K \mid a(\alpha) = 0\} \simeq (\mathbb{Z}/p\mathbb{Z})^n$; on dit alors que F'/F est une extension abélienne d'exposant p et de degré p^n.

(b) K est algébriquement clos dans F', c'est donc le corps des constantes de F'.

(c) Les genres de F et F', notés respectivement g et g' sont reliés par la formule suivante :

$$g' = g \cdot p^n + \frac{p^n - 1}{2}\big(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg P\big).$$

1.2.2 Tours de corps de fonctions

Les tours de corps de fonctions ont un intérêt particulier dans l'étude de la constante d'Ihara $A(q)$: elles en fournissent en effet une borne inférieure. Cependant, elles sont aussi très utiles pour la détermination de la complexité bilinéaire. En effet, dans ce but, on doit disposer, pour tout n, d'un corps de fonctions qui convienne pour l'algorithme de type Chudnovsky dans $\mathbb{F}_{q^n}$; en particulier, on veut

(1) pour tout entier N (dépendant de n), déterminer un corps de fonctions algébriques ayant au moins N places de petit degré — idéalement rationnelles,

(2) que ce nombre de places rationnelles, ou à défaut, de petit degré, soit grand par rapport au genre.

Ceci nous amène à considérer en particulier des tours de corps de fonctions algébriques qui sont asymptotiquement optimales, c'est-à-dire dont le rapport entre le nombre de places rationnelles et le genre tend vers la borne de Drinfeld-Vlăduţ. De plus, on s'intéressera à des tours $\{F_i\}_{i\geq 1}$ les plus denses possibles, c'est-à-dire dont le ratio $g(F_{i+1})/g(F_i)$ des genres de deux étages consécutifs soit le plus proche possible de 1. En effet, ces tours jouent un rôle fondamental pour la détermination de la complexité : les meilleures tours pour l'obtention de bornes pour $\mu_q(n)$ sont celles qui sont les plus denses. D'après la formule du genre d'Hurwitz [Sti08, Theorem 3.4.13], dans une tour, on peut au mieux espérer avoir :

$$\lim_{i\to\infty} \frac{g(F_{i+1})}{g(F_i)} = [F_{k+1} : F_k] = 2,$$

ce qui explique que les tours quadratiques (i.e. dont chaque étage est une extension quadratique du précédent) sont d'un intérêt particulier.

Définition 1.2.2.1. *Une tour de corps de fonctions sur $\mathbb{F}_q$ est une suite infinie $\mathcal{T} = (F_1, F_2, F_3, \ldots)$ de corps de fonctions $F_i/\mathbb{F}_q$ qui vérifient les conditions suivantes :*

(i) $F_1 \subsetneq F_2 \subsetneq F_3 \subsetneq \cdots \subsetneq F_r \subsetneq F_{r+1} \subsetneq \cdots$,

(ii) pour tout $i \geq 1$, l'extension F_{i+1}/F_i est finie et séparable,

(iii) la suite des genres tend vers l'infini : $\lim_{i\to\infty} g(F_i) = +\infty$.

Pour une tour $\mathcal{T}/\mathbb{F}_q$ comme dans la définition précédente, on notera

$$\lambda(\mathcal{T}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

On a alors $0 \leq \lambda(\mathcal{T}) \leq A(q)$ et on dira de la tour $\mathcal{T}$ qu'elle est :
- asymptotiquement bonne si $\lambda(\mathcal{T}) > 0$,
- asymptotiquement mauvaise si $\lambda(\mathcal{T}) = 0$,
- asymptotiquement optimale si $\lambda(\mathcal{T}) = A(q)$.

En particulier, une tour asymptotiquement optimale sur $\mathbb{F}_{q^2}$ tend vers la borne de Drinfeld-Vlăduţ et présente donc un intérêt considérable dans le cadre de l'obtention de bornes pour la complexité bilinéaire avec l'algorithme de type Chudnovsky. On définira dans le chapitre 3 les tours qui seront utilisées pour obtenir nos résultats ; il s'agit de tours dites récursives :

Définition 1.2.2.2. *Soient $f(Y) \in \mathbb{F}_q(Y)$ et $h(X) \in \mathbb{F}_q(X)$ deux fonctions rationnelles non-constantes, et soit $\mathcal{T} = (F_1, F_2, F_3, \ldots)$ une tour de corps de fonctions sur $\mathbb{F}_q$. Supposons qu'il existe des éléments $x_i \in F_i$, pour $i = 1, 2, 3, \ldots$, tels que*

(i) x_1 *est transcendant sur* $\mathbb{F}_q$ *et* $F_1 = \mathbb{F}_q(x_1)$ *est le corps des fonctions rationnelles sur* $\mathbb{F}_q$.

(ii) pour tout $i \geq 1$, $F_i = \mathbb{F}_q(x_1, x_2, \ldots, x_i)$,

(iii) pour tout $i \geq 1$, *les éléments* x_i *et* x_{i+1} *sont reliés par* $f(x_{i+1}) = h(x_i)$,

(iv) $[F_2 : F_1] = \deg f(Y)$.

Alors, on dit que la tour $\mathcal{T}$ *est définie récursivement sur* $\mathbb{F}_q$ *par l'équation*

$$f(Y) = h(X).$$

Remarques.

1) Ici, $\deg f(Y)$ est par définition le maximum des degrés de $f_1(Y)$ et $f_2(Y)$ pour $f_1(Y), f_2(Y) \in \mathbb{F}_q[Y]$ tels que $f_2(Y) \neq 0$ et $f(Y) = f_1(Y)/f_2(Y)$.
2) Pour tout $i \geq 1$, on a $[F_{i+1} : F_i] \leq \deg f(Y)$. En effet, d'après l'hypothèse (iii) de la définition précédente, le $(i+1)$-ième étage de la tour est défini comme extension algébrique de l'étage inférieur par $F_{i+1} = F_i(x_{i+1})$ où l'élément x_{i+1} est racine d'un polynôme de $F_i[Y]$ de degré au plus $\deg f(Y)$.

1.3 Le problème de l'existence de diviseurs de dimension nulle

L'amélioration des bornes de la complexité bilinéaire repose actuellement sur l'amélioration ainsi que l'utilisation optimisée des algorithmes de type Chudnosky. Or cela repose fondamentalement sur la géométrie des espaces de Riemann-Roch, et en particulier sur l'existence de diviseurs ayant de bonnes propriétés : on sera ainsi amené à rechercher des diviseurs de dimension nulle de plus petit degré possible. D'après le théorème de Riemann-Roch, il s'agit au mieux de diviseurs de degré $g-1$, qui sont alors de plus non-spéciaux. À défaut, on recherchera des diviseurs de dimension nulle et de degré $g-k$, pour $k \geq 1$ un entier que l'on choisira le plus petit possible.

Dans un premier temps, on présente quelques résultats sur les diviseurs non-spéciaux obtenus par Ballet et Le Brigand [BLB06] qui seront utiles dans la deuxième partie du chapitre 4. On s'intéressera ensuite à l'existence de diviseurs de dimension nulle et de petit degré (cf [BRR10]).

1.3.1 Le cas des diviseurs non-spéciaux de degré $g-1$

L'existence d'un diviseur non-spécial de degré $g-1$ est un cas limite très intéressant voire fondamental quant à l'utilisation optimale de tout algorithme de type Chudnovsky, c'est pourquoi un intérêt particulier est donné à la détermination de conditions d'existence de tels diviseurs.

Lemme 1.3.1.1. *S'il existe un diviseur effectif* $\mathcal{D}$ *non-spécial et de degré* g *et une place rationnelle* P *qui n'est pas dans le support de* $\mathcal{D}$, *alors* $\mathcal{D} - P$ *est un diviseur non-spécial de degré* $g-1$.

Preuve. On a $\deg(\mathcal{D}-P) = g-1$, donc $\dim(\mathcal{D}-P) = i(\mathcal{D}-P)$. Comme $\mathcal{D} \geq \mathcal{D} - P$ et $\mathcal{D} \not\sim \mathcal{D} - P$, on a $\mathcal{L}(\mathcal{D}) \supsetneq \mathcal{L}(\mathcal{D} - \mathcal{P})$. Or $\mathcal{L}(\mathcal{D}) = \mathbb{F}_q$ car $\dim \mathcal{D} = i(\mathcal{D}) + 1 = 1$,

d'où $\mathcal{L}(\mathcal{D}-\mathcal{P})=\{0\}$ et donc $i(\mathcal{D}-P)=0$. □

Proposition 1.3.1.2. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre $g\geq 1$.*

(a) S'il existe $T\subseteq\mathbb{P}_F$ un ensemble de places de degré 1 tel que $|T|\geq g$, alors il existe un diviseur effectif $\mathcal{D}$ non-spécial de degré g tel que $\operatorname{supp}\mathcal{D}\subseteq T$.

(b) Si $B_1(F/\mathbb{F}_q)\geq g+1$, alors il existe un diviseur $\mathcal{D}$ non-spécial de degré $g-1$ dont le support ne contient que des places de degré 1.

Preuve. Le résultat (a) est l'objet de [Sti08, Proposition 1.6.12]. On obtient (b) par application de (a). En effet, comme $B_1(F/\mathbb{F}_q)\geq g+1$, il existe $T\subseteq\mathbb{P}_F$ un ensemble de places de degré 1 tel que $|T|=g+1$ et on a donc, d'après (a), l'existence d'un diviseur effectif $\mathcal{A}$ non-spécial de degré g tel que $\operatorname{supp}\mathcal{A}\subseteq T\backslash\{P\}$, pour une place fixée $P\in T$. Ainsi, comme $P\notin\operatorname{supp}\mathcal{A}$, le diviseur $\mathcal{D}:=\mathcal{A}-P$ est non-spécial de degré $g-1$ d'après le lemme 1.3.1.1. □

Proposition 1.3.1.3. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre $g\geq 1$. Si $A_{g-1}<h_F$, alors il existe un diviseur non-spécial de degré $g-1$.*

Preuve. Pour tout $d\geq 1$ tel que $\mathbb{A}_d\neq\varnothing$ et tout choix de $\mathcal{D}_0\in\mathbb{A}_d$, on définit l'application $\psi_{d,\mathcal{D}_0}$ suivante :

$$\begin{array}{rccc}\psi_{d,\mathcal{D}_0}: & \mathbb{A}_d & \longrightarrow & \mathrm{Cl}^0(F/\mathbb{F}_q)\\ & \mathcal{D} & \longmapsto & [\mathcal{D}-\mathcal{D}_0]\end{array}$$

Montrons d'abord que pour tout corps de fonctions algébriques, on a $1\leq h_F\leq A_g$. Soit $\mathcal{A}$ un diviseur de degré g ; un tel diviseur existe bien d'après la proposition 1.1.5.7. Par le théorème de Riemann-Roch, on a $\dim\mathcal{A}\geq 1$, donc on peut trouver un diviseur effectif $\mathcal{D}_0$ équivalent à $\mathcal{A}$. On a ainsi $\mathcal{D}_0\in\mathbb{A}_g$, donc l'application $\psi_{g,\mathcal{D}_0}$ est bien définie. On montre alors que cette application est surjective. En effet, pour tout $[\mathcal{R}]\in\mathrm{Cl}^0(F/\mathbb{F}_q)$, on a $\deg([\mathcal{R}+\mathcal{D}_0])=g$, donc $\dim([\mathcal{R}+\mathcal{D}_0])\geq 1$, d'où l'existence d'un diviseur effectif $\mathcal{D}$ équivalent à $\mathcal{R}+\mathcal{D}_0$; en particulier, $\mathcal{D}\in\mathbb{A}_g$. Finalement, on a $\psi_{g,\mathcal{D}_0}(\mathcal{D})=[\mathcal{D}-\mathcal{D}_0]=[\mathcal{R}]$, d'où la surjectivité de $\psi_{g,\mathcal{D}_0}$. Ainsi, on a $|\mathrm{Cl}^0(F/\mathbb{F}_q)|\leq|\mathbb{A}_g|$, i.e. $h_F\leq A_g$.
Dans le cas où $g=1$, on a $h_F=A_1$. En effet, d'une part $h_F\leq A_1$ et d'autre part, comme deux places de degré 1 distinctes ne sont pas équivalentes, on a $h_F\geq A_1$. Ainsi, comme $A_0=1=g$ et $h_F=A_1=B_1(F/\mathbb{F}_q)$, on a l'équivalence :

$$A_0<h_F\Longleftrightarrow g+1\leq B_1(F/\mathbb{F}_q)$$

ce qui, d'après la proposition 1.3.1.2(b), entraîne l'existence d'un diviseur non-spécial de degré $g-1$.
On considère maintenant le cas où $g>1$. Comme un diviseur de degré $g-1$ est non-spécial si et seulement si il est de dimension nulle, il suffit (d'après Proposition 1.1.4.2(b)) de démontrer qu'il existe un diviseur de degré $g-1$ qui ne soit équivalent à aucun diviseur effectif. Si $A_{g-1}=0$, alors le résultat est prouvé. Sinon, on peut trouver un diviseur effectif $\mathcal{D}_0$ de degré $g-1$. On considère alors l'application $\psi_{g-1,\mathcal{D}_0}$.

Comme par hypothèse $A_{g-1} < h_F$, cette application n'est pas surjective donc il existe un diviseur $\mathcal{R}$ de degré 0 tel que $[\mathcal{R}] \notin \psi_{g-1,\mathcal{D}_0}(\mathbb{A}_{g-1})$. Ainsi, le diviseur $\mathcal{D} := \mathcal{R} + \mathcal{D}_0$ n'est équivalent à aucun diviseur effectif et vérifie $\deg \mathcal{D} = g - 1$, d'où $\dim \mathcal{D} = 0$ et $\mathcal{D}$ est non-spécial. □

Cette proposition permet d'obtenir le théorème suivant, qui constitue le résultat principal de ce paragraphe.

Théorème 1.3.1.4. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre $g \geq 2$. Si $q \geq 4$, alors il existe un diviseur non-spécial de degré $g - 1$.*

Preuve. D'après l'inégalité (1.4) rappelée dans la proposition 1.1.5.1, on a

$$A_{g-1} < \frac{h_F}{(q^{1/2} - 1)^2}.$$

Si $q \geq 4$, alors $(q^{1/2} - 1)^2 \geq 1$ et donc on a $A_{g-1} < h_F$, d'où le résultat d'après la proposition 1.3.1.3(b). □

1.3.2 Le cas général

Dans cette section $F/\mathbb{F}_q$ est un corps de fonctions algébriques de genre g et dont $\mathbb{F}_q$ est le corps plein des constantes. On présente ici des résultats de [BRR10] qui permettent d'établir l'existence d'un diviseur de dimension nulle et de degré aussi grand que possible, à savoir au mieux $g - 1$.

Notons d'abord que le cas de l'existence d'un diviseur de dimension nulle et de degré exactement $g - 1$ constitue un cas limite, dans le sens où dès lors qu'il existe un diviseur $\mathcal{D}$ de dimension nulle et de degré $g - k$ pour $k \geq 1$, il existe des diviseurs de dimension nulle et de tout degré inférieur à $g - k$ sous réserve que $F/\mathbb{F}_q$ contienne au moins une place rationnelle P. En effet, dans ce cas, pour tout entier $l \geq k$ le diviseur $\mathcal{D} - lP$ est de dimension nulle. Si ce n'était pas le cas, $\mathcal{D} - lP$ serait équivalent à un diviseur effectif donc on pourrait trouver un élément $x \in F$ tel que $\mathcal{D} - lP + (x) \geq 0$; ainsi, on aurait $\mathcal{D} + (x) \geq 0$ et donc $\mathcal{D}$ serait équivalent à un diviseur effectif, ce qui est impossible puisque $\dim \mathcal{D} = 0$.

Le lemme suivant est la clé des résultats qui seront établis dans ce paragraphe :

Lemme 1.3.2.1. *Pour tout entier n tel que $A_n < h_F$, il existe un diviseur de degré n et de dimension nulle. Plus précisément, si l'on note h_n^0 le nombre de classes de diviseurs de degré n et de dimension nulle, on a $h_n^0 \geq h_F - A_n$.*

Preuve. Soient $\mathcal{D}_0 \in \mathrm{Div}(F)$ un diviseur de degré 1 (l'existence de $\mathcal{D}_0$ est assurée par la proposition 1.1.5.7) et n un entier tel que $A_n < h_F$. On définit la fonction suivante :

$$\begin{array}{rccc} \psi : & \{\mathcal{A} \in \mathrm{Div}(F) \mid \deg \mathcal{A} = n\} & \longrightarrow & \mathrm{Cl}^0(F/\mathbb{F}_q) \\ & \mathcal{D} & \longmapsto & [\mathcal{D} - n\mathcal{D}_0] \end{array}$$

Comme $A_n < h_F$, la restriction de ψ à $\mathbb{A}_n$, n'est pas surjective. En particulier, il y a au moins $|\mathrm{Cl}^0(F/\mathbb{F}_q)| - |\mathbb{A}_n|$ classes distinctes $[\mathcal{A}] \in \mathrm{Cl}^0(F/\mathbb{F}_q)$ pour lesquelles $[\mathcal{A}] \notin \psi(\mathbb{A}_n)$, c'est-à-dire pour lesquelles $[\mathcal{A} + n\mathcal{D}_0] \notin \mathbb{A}_n$; pour toutes ces classes, on a donc $\deg[\mathcal{A} + n\mathcal{D}_0] = n$ par construction et $\dim[\mathcal{A} + n\mathcal{D}_0] = 0$ car sinon $\mathcal{A} + n\mathcal{D}_0$ serait équivalent à un diviseur effectif de dimension n. □

Théorème 1.3.2.2. *Il existe un diviseur de dimension nulle et de degré $g - k$ dans les cas suivants :*

(i) pour tout $k \geq 5$ si $q = 2$,

(ii) pour tout $k \geq 2$ si $q = 3$,

(iii) pour tout $k \geq 1$ si $q \geq 4$.

Preuve. Notons que le cas $q \geq 4$ et $k = 1$ est déjà établi par le théorème 1.3.1.4. En effectuant le changement de variable $i = g - n$ et en notant que $A_0 = 1$, on peut réécriré l'inégalité (1.3) de la proposition 1.1.5.1 sous la forme :

$$2q^{\frac{g-1}{2}} + 2\sum_{i=2}^{g-1} q^{\frac{i-1}{2}} A_{g-i} + A_{g-1} \leq \frac{h_F}{(q^{1/2}-1)^2}.$$

Comme $A_i \geq 0$ pour tout $i \geq 1$, on a pour tout $2 \leq k \leq g-1$:

$$2q^{\frac{g-1}{2}} + 2q^{\frac{k-1}{2}} A_{g-k} \leq \frac{h_F}{(q^{1/2}-1)^2}$$

et donc

$$A_{g-k} \leq \frac{h_F}{2q^{\frac{k-1}{2}}(q^{1/2}-1)^2} - q^{\frac{g-k}{2}} < \frac{h_F}{2q^{\frac{k-1}{2}}(q^{1/2}-1)^2}.$$

Ainsi, le lemme précédent permet de conclure puisque

$$2q^{\frac{k-1}{2}}(q^{1/2}-1)^2 > 1 \text{ dès que } \begin{cases} q \geq 4 \text{ et } k \geq 1 \\ q = 3 \text{ et } k \geq 1 \\ q = 2 \text{ et } k \geq 5. \end{cases}$$

□

Remarque. Dans [BRR10], les auteurs ont de plus établi des résultats de densité sur les diviseurs dont l'existence est donnée par le théorème précédent : ils ont montré qu'en effectuant des tirages aléatoires parmi les diviseurs de degré $g - k$, on a une très grande probabilité d'obtenir un diviseur de dimension nulle. Cette propriété est très intéressante car elle assure que l'on puisse trouver facilement un diviseur qui ait les propriétés attendues pour l'implémentation de l'algorithme de type Chudnovsky. Plus précisément, le résultat est le suivant :

Proposition 1.3.2.3. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g. Considérons l'ensemble des diviseurs de degré $g - k$ avec $k \geq 1$ fixé, muni de la loi de probabilité uniforme. On pose*

$$\beta_q = \begin{cases} \frac{2(\sqrt{q}-1)^2}{\sqrt{q}} & si \quad k \geq 2, \\ \frac{(\sqrt{q}-1)^2}{\sqrt{q}} & si \quad k = 1. \end{cases}$$

Si $k \geq -2\log_q(\beta_q)$ *alors la probabilité* $p(k)$ *d'obtenir un diviseur de degré* $g-k$ *de dimension nulle est telle que*

$$p(k) \geq 1 - \frac{1}{\beta_q q^{\frac{k}{2}}}.$$

Cette borne, dont on peut remarquer qu'elle est indépendante de g, croît très vite vers 1, même pour des petites valeurs de k.

Chapitre 2

Complexité de la multiplication et algorithmes de type Chudnovsky

2.1 Complexité de la multiplication dans les extensions finies de $\mathbb{F}_q$

2.1.1 Complexité, complexité bilinéaire et rang de tenseur

Notons $K := \mathbb{F}_q$, où q est une puissance d'un nombre premier et $K_n[X]$ le K-espace vectoriel des polynômes à coefficients dans K et de degré inférieur ou égal à n. Si $P(X) \in K_n[X]$ est un polynôme de degré n irréductible sur $K_n[X]$, alors $\mathbb{F}_{q^n}$ est isomorphe à $K_n[X]/\big(P(X)\big)$. Ainsi, à tout élément de $\mathbb{F}_{q^n}$ correspond la classe modulo $P(X)$ d'un certain polynôme de degré $n-1$. Déterminer la complexité de la multiplication dans $\mathbb{F}_{q^n}$, c'est déterminer le nombre minimal d'opérations nécessaires pour calculer, pour tous polynômes $R(X)$ et $S(X)$ de $K_n[X]$, les coefficients du produit $R(X)S(X) \pmod{P(X)}$.

Cependant, dans cette complexité de la multiplication, différents types d'opérations élémentaires interviennent. En effet, les additions et les multiplications dites scalaires, c'est-à-dire qui sont indépendantes des éléments de $\mathbb{F}_{q^n}$ dont on effectue le produit, sont de nature différente des multiplications dites bilinéaires, c'est-à-dire qui dépendent des deux éléments de $\mathbb{F}_{q^n}$ dont on effectue le produit. Ainsi, les opérations des deux premiers types peuvent faire l'objet d'un traitement particulier (FPGA, circuits dédiés, ...) afin d'optimiser leur efficacité. Ici, on s'intéressera au cas des multiplications bilinéaires, qui correspondent en particulier au nombre de portes binaires nécessaires dans un circuit.

À titre d'exemple, et afin d'éclaircir les différentes notions de complexité qui viennent d'être introduites, calculons le nombre d'opérations de chaque type intervenant dans la multiplication « naïve » de deux éléments x et y de $\mathbb{F}_{q^n}$.

On se donne $\mathcal{B} := (e_1, \ldots, e_n)$ une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ et on note $x = \sum_{i=1}^n x_i e_i$ et $y = \sum_{i=1}^n y_i e_i$ les écritures de x et y dans cette base. On définit pour tous $i, j \in \{1, \ldots, n\}$, les coordonnées $\left\{\xi_{i,j}^k\right\}_{k=1,\ldots,n}$ du produit $e_i e_j$ dans

cette base :

$$e_i e_j = \sum_{k=1}^{n} \xi_{i,j}^k e_k.$$

Alors on a

$$xy = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \xi_{i,j}^k \right) e_k.$$

Ainsi, pour obtenir les coordonnées dans la base $\mathcal{B}$ du produit xy, on dénombre :

- n^2 multiplications bilinéaires : ce sont les produits $x_i y_j$,
- n^3 multiplications scalaires : ce sont les multiplications des éléments $x_i y_j$ par les coefficients $\xi_{i,j}^k$ (qui ne dépendent que du choix de la base $\mathcal{B}$ et pas des éléments x et y à multiplier),
- $n(n-1)(n+1)$ additions d'éléments de $\mathbb{F}_q$.

Cet exemple montre bien que la part des opérations scalaires dans la complexité globale de la multiplication peut être conséquente. Cependant, le problème de la détermination du nombre de multiplications bilinéaires présente l'intérêt supplémentaire d'être relié au problème abstrait strictement mathématique de la détermination du rang de tenseur de la multiplication. En effet, $\mathrm{Bil}(\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, \mathbb{F}_{q^n})$, le $\mathbb{F}_q$-espace vectoriel des formes bilinéaires de $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ dans $\mathbb{F}_{q^n}$ est isomorphe au produit tensoriel $\mathbb{F}_{q^n}^\star \otimes \mathbb{F}_{q^n}^\star \otimes \mathbb{F}_{q^n}$, où $\mathbb{F}_{q^n}^\star$ est le dual de $\mathbb{F}_{q^n}$ en tant que $\mathbb{F}_q$-espace vectoriel, comme l'indique le résultat suivant (cf [BCS97, Proposition 14.16]) :

Proposition 2.1.1.1.

$$\mathrm{Bil}(\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, \mathbb{F}_{q^n}) \simeq \mathbb{F}_{q^n}^\star \otimes \mathbb{F}_{q^n}^\star \otimes \mathbb{F}_{q^n}$$

Plus généralement, on va présenter ici la notion de rang de tenseur de la multiplication, et son lien avec la complexité bilinéaire dans le cadre des algèbres.

Soit $\mathcal{A}$ une F-algèbre, où F est un corps et notons $m_{\mathcal{A}}$ la multiplication dans $\mathcal{A}$. Comme $m_{\mathcal{A}}$ est une application bilinéaire de $\mathcal{A} \times \mathcal{A}$ dans $\mathcal{A}$, cela implique que $m_{\mathcal{A}}$ correspond à une application linéaire M du produit tensoriel $\mathcal{A} \otimes \mathcal{A}$ dans $\mathcal{A}$ et que l'on peut donc représenter M par un tenseur $t_{\mathcal{A}} \in \mathcal{A}^\star \otimes \mathcal{A}^\star \otimes \mathcal{A}$ où $\mathcal{A}^\star$ est le dual de $\mathcal{A}$ sur F. Ainsi, le produit de deux éléments x et y de $\mathcal{A}$ s'obtient par convolution du tenseur $t_{\mathcal{A}}$ avec le tenseur $x \otimes y \in \mathcal{A} \otimes \mathcal{A}$. Le rang de ce tenseur $t_{\mathcal{A}}$ est défini comme le nombre minimal λ de tenseurs élémentaires (de rang 1) de la forme $a_i \otimes b_i \otimes c_i$ tels que $t_{\mathcal{A}}$ puisse être représenté de la façon suivante :

$$t_{\mathcal{A}} = \sum_{i=1}^{\lambda} a_i \otimes b_i \otimes c_i \tag{2.1}$$

où $a_i \in \mathcal{A}^\star$, $b_i \in \mathcal{A}^\star$, $c_i \in \mathcal{A}$.
Dans ce cas, pour tous $x, y \in \mathcal{A}$, on a

$$xy = \sum_{i=1}^{\lambda} a_i(x) b_i(y) c_i. \tag{2.2}$$

Définition 2.1.1.2. *On appelle algorithme $\mathscr{U}$ de multiplication bilinéaire dans $\mathcal{A}$ de complexité λ sur F la donnée de $a_1, \ldots, a_\lambda, b_1, \ldots, b_\lambda \in \mathcal{A}^\star$ et $c_1, \ldots, c_\lambda \in \mathcal{A}$ qui satisfont (2.2). L'entier λ est alors noté $\mu(\mathscr{U})$.*
La complexité bilinéaire de la multiplication dans $\mathcal{A}$ sur F, notée $\mu_F(\mathcal{A})$, est la complexité minimale sur F de tous les algorithmes de multiplication bilinéaire dans $\mathcal{A}$, c'est-à-dire :

$$\mu_F(\mathcal{A}) := \min_{\mathscr{U}} \mu(\mathscr{U})$$

où $\mathscr{U}$ parcourt l'ensemble des algorithmes de multiplication bilinéaire dans $\mathcal{A}$ sur F.

Réciproquement, tout algorithme $\mathscr{U}$ de multiplication bilinéaire dans $\mathcal{A}$ peut être obtenu à partir d'une décomposition de type (2.1).

Si l'on se limite aux cas particuliers où les formes linéaires a_i et b_i coïncident, on parle alors complexité bilinéaire symétrique :

Définition 2.1.1.3. *Un algorithme de multiplication bilinéaire de type (2.2) est dit symétrique si pour tout $i \in \{1, \ldots, \lambda\}$, on a $a_i = b_i$.*
La complexité bilinéaire symétrique de la multiplication dans $\mathcal{A}$ sur F, notée $\mu_F^{\mathrm{sym}}(\mathcal{A})$, est la complexité minimale de tous les algorithmes symétriques de multiplication bilinéaire dans $\mathcal{A}$ sur F, c'est-à-dire :

$$\mu_F^{\mathrm{sym}}(\mathcal{A}) := \min_{\mathscr{U}^{\mathrm{sym}}} \mu(\mathscr{U}^{\mathrm{sym}})$$

où $\mathscr{U}^{\mathrm{sym}}$ parcourt l'ensemble des algorithmes symétriques de multiplication bilinéaire dans $\mathcal{A}$ sur F.

Remarquons que la complexité bilinéaire et la complexité bilinéaire symétrique sont trivialement reliées par l'inégalité suivante :

$$\mu_F(\mathcal{A}) \leq \mu_F^{\mathrm{sym}}(\mathcal{A}).$$

Le rang de tenseur de la multiplication dans une extension de degré n du corps fini $\mathbb{F}_q$ correspond au cas particulier où $F = \mathbb{F}_q$ et $\mathcal{A} = \mathbb{F}_{q^n}$, que l'on notera de façon plus concise comme suit :

Définition 2.1.1.4. *On pose*

$$\mu_q(n) := \mu_{\mathbb{F}_q}(\mathbb{F}_{q^n}),$$

et

$$\mu_q^{\mathrm{sym}}(n) := \mu_{\mathbb{F}_q}^{\mathrm{sym}}(\mathbb{F}_{q^n}).$$

Enfin, on définit les quantités suivantes, qui représentent la complexité bilinéaire, symétrique ou non, de la multiplication dans l'algèbre $\mathbb{F}_{q^m}[t]/(t^l)$ sur $\mathbb{F}_q$, et qui ont été introduites par Randriambololona dans [Ran12] :

Définition 2.1.1.5.

$$\mu_q(m, l) := \mu_{\mathbb{F}_q}(\mathbb{F}_{q^m}[t]/(t^l)).$$

et

$$\mu_q^{\mathrm{sym}}(m, l) := \mu_{\mathbb{F}_q}^{\mathrm{sym}}(\mathbb{F}_{q^m}[t]/(t^l)).$$

Remarquons que la complexité bilinéaire classique dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ peut être vue comme un cas particulier de cette quantité :

$$\mu_q(n) = \mu_q(n,1) \text{ et } \mu_q^{\text{sym}}(n) = \mu_q^{\text{sym}}(n,1).$$

2.1.2 Algorithme de multiplication de type Chudnovsky

En 1987, D.V. Chudnovsky et G.V. Chudnovsky présentent un principe de construction d'algorithmes de multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, basé sur l'interpolation sur des points rationnels des courbes algébriques définies sur $\mathbb{F}_q$. Cet algorithme peut être vu comme une généralisation de l'interpolation polynomiale, et notamment de l'algorithme de Karatsuba. Depuis lors, des généralisations successives de cet algorithme, qui prennent en compte des points de degré quelconque et de nouvelles évaluations, ont été données par Ballet et Rolland [BR04], Chaumine [Cha06], Arnaud [Arn06], Cenk et Özbudak [CÖ10], et Randriambololona [Ran12].

S'il a d'abord permis d'établir que le rang de tenseur de la multiplication dans $\mathbb{F}_{q^n}$ était linéaire en n, cet algorithme en fournit désormais les meilleures bornes connues dans le cas d'extensions de degré grand relativement au cardinal du corps de base — le cas des petites extensions étant bien connu. Ce sont ces résultats classiques que nous allons détailler dans le paragraphe suivant.

2.1.3 Résultats classiques

Soit

$$P(X) = \sum_{i=0}^{n} a_i X^i$$

un polynôme irréductible unitaire de degré n à coefficients dans un corps K. Soient

$$R(X) = \sum_{i=0}^{n-1} x_i X^i$$

et

$$S(X) = \sum_{i=0}^{n-1} y_i X^i$$

deux polynômes de degré inférieur ou égal à $n-1$.

Fiduccia et Zalcstein (cf. [FZ77],[BCS97, Proposition 14.47]) ont étudié le problème général de la détermination des coefficients du produit $R(X)S(X)$ et ont montré que cela nécessitait au moins $2n-1$ multiplications. Dans le cas où le corps K est infini, un algorithme atteignant exactement cette borne avait déjà été donné par Toom dans [Too63]. Dans [Win77], Winograd décrit tous les algorithmes qui atteignent la borne $2n-1$. De plus, il a montré dans [Win79] que tout algorithme calculant les coefficients du produit $R(X)S(X) \pmod{P(X)}$ et dont la complexité bilinéaire est exactement $2n-1$ calcule nécessairement les coefficients du produit $R(X)S(X)$ et par conséquent fait appel à un des algorithmes décrit dans [Win77].

Ces algorithmes utilisent des techniques d'interpolation et ne peuvent donc être appliqués dans le cas où le cardinal du corps K est petit par rapport à n (à savoir précisément $< 2n-2$). Autrement dit, on a le résultat suivant :

Théorème 2.1.3.1. *Si K est un corps tel que $|K| < 2n-2$, alors tout algorithme calculant les coefficients du produit $R(X)S(X) \pmod{P(X)}$ est de complexité bilinéaire strictement supérieure à $2n-1$.*

Grâce aux résultats de Winograd et de Groote [dG83], et en appliquant le Théorème 2.1.3.1 à l'extension $\mathbb{F}_{q^n}$ du corps fini $\mathbb{F}_q$, on obtient :

Théorème 2.1.3.2. *La complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ vérifie*

$$\mu_q(n) \geq 2n-1,$$

avec égalité si et seulement si

$$n \leq \frac{q}{2} + 1.$$

De plus, dans ce cas on peut toujours se ramener à un algorithme symétrique, donc

$$\mu_q^{\mathrm{sym}}(n) = \mu_q(n) = 2n-1 \text{ pour tout } n \leq \frac{q}{2} + 1.$$

Dans [Sho92], Shokrollahi étend la plage des degrés d'extension pour lesquels on connaît la valeur exacte de $\mu_q^{\mathrm{sym}}(n)$ en appliquant l'algorithme de Chudnovsky-Chudnovsky avec des corps de fonctions elliptiques (c'est-à-dire des corps de fonctions de courbes elliptiques). D'après un résultat de Waterhouse [Wat69], on sait en effet qu'il existe de tels corps de fonctions ayant $q+1+\epsilon(q)$ places rationnelles, ce qui permet d'établir le résultat suivant :

Théorème 2.1.3.3. *La complexité bilinéaire symétrique de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est égale à $2n$ pour tout entier n tel que*

$$\frac{q}{2} + 1 < n < \frac{1}{2}\big(q+1+\epsilon(q)\big)$$

où ϵ est la fonction définie par

$$\epsilon(q) = \begin{cases} 2\sqrt{q} \text{ si } q \text{ est un carré parfait,} \\ \text{le plus grand entier plus petit que } 2\sqrt{q} \text{ premier à } q \text{ sinon.} \end{cases}$$

À ce jour, on ne sait toujours pas si la réciproque est vraie ; à savoir : si $\mu_q^{\mathrm{sym}}(n) = 2n$, a-t-on nécessairement $\frac{q}{2} + 1 < n < \frac{1}{2}\big(q+1+\epsilon(q)\big)$?

Notons que si $q = 2$ ou 3, alors $\frac{q}{2} + 1 \geq \frac{1}{2}(q+1+\epsilon(q))$ donc le théorème 2.1.3.2 donne une meilleure borne que le théorème 2.1.3.3, et ce, pour une plage de n plus étendue.

Ainsi, la complexité bilinéaire symétrique $\mu_q^{\mathrm{sym}}(n)$ est précisément connue pour certaines valeurs de n et q. En revanche, lorsque n est grand par rapport à q, estimer

$\mu_q^{\mathrm{sym}}(n)$ s'avère être un problème délicat. On verra dans le paragraphe suivant que différentes bornes supérieures ont été établies. Cependant, l'algorithme de Chudnovsky-Chudnovsky appliqué à une suite asymptotiquement adéquate de corps de fonctions algébriques permet d'affirmer que la complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est linéaire en le degré n de l'extension ; autrement dit :

Théorème 2.1.3.4. *Pour tout entier q puissance d'un nombre premier, il existe une constante C_q telle que*

$$\mu_q^{\mathrm{sym}}(n) \leq C_q n.$$

Remarque. S'il ne permet pas d'établir de valeur exacte pour $\mu_q(n)$, le théorème 2.1.3.3 en donne tout de même une borne supérieure en vertu de la relation $\mu_q(n) \leq \mu_q^{\mathrm{sym}}(n)$. En outre, le théorème précédent établit la linéarité de $\mu_q(n)$ par rapport à n.

2.1.4 Bornes asymptotiques

Dans [STV92], Shparlinski, Tsfasman et Vlăduţ ont étudié plus précisément l'algorithme présenté par D.V. et G.V. Chudnovsky, et en ont tiré d'intéressantes conclusions quant à sa complexité. En particulier, ils ont introduit les deux quantités suivantes dans le but d'étudier la linéarité du rang de tenseur :

Définition 2.1.4.1. *Posons*

$$M_q^{\mathrm{sym}} := \limsup_{k\to\infty} \frac{\mu_q^{\mathrm{sym}}(k)}{k},$$

et

$$m_q^{\mathrm{sym}} := \liminf_{k\to\infty} \frac{\mu_q^{\mathrm{sym}}(k)}{k}.$$

On a vu précédemment que si le cardinal du corps de base est trop petit par rapport au degré de l'extension considérée, on ne peut pas utiliser la méthode d'interpolation de Winograd. L'algorithme de Chudnovsky-Chudnovsky présenté dans [CC88] permet d'outrepasser ce problème en utilisant des techniques d'interpolation sur des courbes algébriques ayant suffisamment de points rationnels sur le corps sur lequel elles sont définies. En utilisant cet algorithme, D.V. et G.V. Chudnovsky ont affirmé que la complexité bilinéaire symétrique de la multiplication dans les extensions finies de $\mathbb{F}_q$ était asymptotiquement linéaire en le degré de l'extension. Cependant, Shparlinski, Tsfasman et Vlăduţ ont souligné que les frères Chudnovsky avaient démontré que m_q^{sym} était borné, et non M_q^{sym}, ce qui ne suffit pas à établir la linéarité de la complexité bilinéaire. Pour cela, il est nécessaire d'établir que M_q^{sym} est borné, ce qui était l'objet de [STV92]. Malheureusement, une erreur dans cet article a récemment été mise au jour par Cascudo, Cramer et Xing, et a un impact sur la démonstration de ce résultat, ainsi que sur les améliorations qui avaient été apportées aux estimations de bornes inférieures pour m_q^{sym}. Ce problème sera explicité dans la section 2.2. Néanmoins, des travaux ultérieurs de Ballet [Bal99], qui ne sont pas affectés par la même erreur, permettent d'établir définitivement la linéarité de $\mu_q^{\mathrm{sym}}(n)$ par rapport à n.

Remarque. On définit les pendants non nécessairement symétriques de ces bornes asymptotiques en notant

$$M_q := \limsup_{k\to\infty} \frac{\mu_q(k)}{k},$$

et

$$m_q := \liminf_{k\to\infty} \frac{\mu_q(k)}{k}.$$

2.1.5 Bornes uniformes et asymptotiques connues

Rappelons d'abord les premiers résultats dus à Shparlinski, Tsfasman et Vlăduţ [STV92, Lemme 1.2 et Corollaire 1.3] qui lient d'une part la complexité bilinéaire de la multiplication dans des extensions successives de $\mathbb{F}_q$, et d'autre part les notions de complexité bilinéaire uniforme et asymptotiques introduites précédemment :

Lemme 2.1.5.1. *Pour tout entier q, puissance d'un nombre premier, et tous entiers $n, m \geq 1$, on a les inégalités suivantes :*

$$\mu_q^{\mathrm{sym}}(m) \leq \mu_q^{\mathrm{sym}}(mn) \leq \mu_q^{\mathrm{sym}}(n)\mu_{q^n}^{\mathrm{sym}}(m),$$

$$m_q^{\mathrm{sym}} \leq m_{q^n}^{\mathrm{sym}} \cdot \mu_q^{\mathrm{sym}}(n)/n,$$

et

$$M_q^{\mathrm{sym}} \leq M_{q^n}^{\mathrm{sym}} \cdot \mu_q^{\mathrm{sym}}(n).$$

Les deux dernières inégalités se déduisent de façon immédiate de la première, qui découle elle-même de la définition même de $\mu_q^{\mathrm{sym}}(nm)$, puisque $\mathbb{F}_{q^{mn}}$ est une extension de $\mathbb{F}_{q^n}$. Notons que ces inégalités sont aussi vraies pour les équivalents non-symétriques de ces quantités.

Toute borne uniforme, c'est-à-dire toute constante C_q telle que définie dans le théorème 2.1.3.4, fournit une estimation pour la complexité asymptotique sur $\mathbb{F}_q$, puisque l'on a toujours les inégalités suivantes :

$$M_q \leq M_q^{\mathrm{sym}} \leq C_q.$$

Les bornes purement asymptotiques, c'est-à-dire qui ne découlent pas d'une telle constante C_q sont rares ; c'est le cas de celles rappelées dans la proposition suivante :

Proposition 2.1.5.2. *Soit q une puissance d'un premier p.*

m_2^{sym}	$\geq$ 3.52		[*BD78, BD80*]
m_q^{sym}	$\geq$ $2\left(1+\frac{1}{q-1}\right)$	*pour tout $q > 2$.*	[*STV92*]
m_q	$\geq$ $2\left(1+\frac{1}{A(q)-1}\right)$	*pour tout $q > 2$ tel que $A(q) > 5$.*	[*Ran12*]
M_q	$\leq$ $2\left(1+\frac{1}{\sqrt{q}-2}\right)$	*pour $q = p^{2r} \geq 49$.*	[*Ran12*]
M_p	$\leq$ $3\left(1+\frac{2}{p-2}\right)$	*pour tout $p > 3$.*	[*Ran12*]
M_q	$\leq$ $3\left(1+\frac{p}{q-2}\right)$	*pour $q = p^r$, où r est impair.*	[*Ran12*]

De plus, dans [CCXY12], les auteurs établissent les bornes purement asymptotiques suivantes pour les corps de petit cardinal :

$$M_2^{\mathrm{sym}} \leq 7.47, \qquad M_3^{\mathrm{sym}} \leq 5.49, \qquad M_4^{\mathrm{sym}} \leq 4.98, \qquad M_5^{\mathrm{sym}} \leq 4.8 \qquad M_7^{\mathrm{sym}} \leq 3.82,$$
$$M_8^{\mathrm{sym}} \leq 3.74, \qquad M_9^{\mathrm{sym}} \leq 3.68, \qquad M_{11}^{\mathrm{sym}} \leq 3.62, \qquad M_{13}^{\mathrm{sym}} \leq 3.59.$$

Certaines valeurs exactes de $\mu_q(n)$ sont souvent utiles, parmi lesquelles :

$$\mu_q^{\mathrm{sym}}(2) = 3 \text{ pour tout } q \text{ puissance d'un premier,}$$
$$\mu_2^{\mathrm{sym}}(4) = 9, \qquad \mu_4^{\mathrm{sym}}(4) = \mu_4^{\mathrm{sym}}(5) = 8, \qquad \mu_2^{\mathrm{sym}}(6) = 15.$$

Le premier résultat est une conséquence de la méthode de Karatsuba ; les suivants sont établis dans [CC88].

De plus, notons que de nombreuses bornes pour $\mu_q^{\mathrm{sym}}(n)$, où $q = 2, 3, 4$, sont données dans [CÖ10] pour des petites valeurs de n.

Concernant $\mu_q(m, l)$, voici quelques bornes déjà établies dans [Ran12] ; ces bornes sont établies spécifiquement pour la complexité non-symétrique :

$$\begin{array}{rcll} \mu_q(2,2) & \leq & 9 & \text{pour } q = 2 \text{ ou } 3, \\ \mu_q(2,2) & \leq & 8 & \text{pour } q = 4 \text{ ou } 5, \\ \mu_q(2,2) & \leq & 7 & \text{pour } q \geq 7, \\ \mu_q(4,2) & \leq & 16 & \text{pour } q = 9, 11 \text{ ou } 13, \\ \mu_q(4,2) & \leq & 15 & \text{pour } q \geq 16, \end{array}$$

$$\mu_2(4,2) \leq 24, \qquad \mu_3(4,2) \leq 21, \qquad \mu_4(4,2) \leq 20,$$
$$\mu_5(4,2) \leq 19, \qquad \mu_7(4,2) \leq 18, \qquad \mu_8(4,2) \leq 17.$$

De plus, d'après [CÖ08], on a $\mu_q(1,2) \leq \mu_q^{\mathrm{sym}}(1,2) \leq 3$ pour tout q puissance d'un premier.
Plus généralement, pour tout entier non-premier $m = de$, avec $d, e \geq 2$, on a

$$\mu_q(m, l) \leq \mu_q(d)\mu_{q^d}(e, l),$$

cette inégalité étant toujours valable dans le cas symétrique :

$$\mu_q^{\mathrm{sym}}(m, l) \leq \mu_q^{\mathrm{sym}}(d)\mu_{q^d}^{\mathrm{sym}}(e, l).$$

De plus, Randriambololona a établi les bornes uniformes suivantes pour la complexité non-symétrique :

Proposition 2.1.5.3. *Si $q = p^r > 5$ est une puissance d'un nombre premier, alors pour tout $n \geq 1$, on a :*

$$\mu_q(n) \leq \begin{cases} 3\left(1 + \frac{2}{p-2}\right) n & \text{si } r = 1, \\ 2\left(1 + \frac{2}{\sqrt{q}-2}\right) n & \text{si } r = 2, \\ 3\left(1 + \frac{p}{q-2}\right) n & \text{si } r \geq 3 \text{ est impair.} \end{cases}$$

Pour finir, rappelons quelques bornes explicites pour C_q qui étaient alors connues au moment où ce travail de thèse a été entrepris (ce sont donc des bornes pour $\mu_q^{\mathrm{sym}}(n)$).

Proposition 2.1.5.4. *Des estimations établies pour la constante C_q définie dans le théorème 2.1.3.4 sont :*

$$C_q = \begin{cases} \text{si } q = 2 & \text{alors } 54 & \text{[Bal99]} \\ \text{sinon si } q = 3 & \text{alors } 27 & \text{[Bal99]} \\ \text{sinon si } q = p \geq 5 & \text{alors } 3(1 + \frac{4}{q-3}) & \text{[BC04]} \\ \text{sinon si } q = p^2 \geq 25 & \text{alors } 2(1 + \frac{2}{\sqrt{q}-3}) & \text{[BC04]} \\ \text{sinon si } q = p^{2k} \geq 16 & \text{alors } 2(1 + \frac{p}{\sqrt{q}-3}) & \text{[Bal03]} \\ \text{sinon si } q \geq 16 & \text{alors } 3(1 + \frac{2p}{q-3}) & \text{[BR04], [BLBR09] et [BLB06]} \\ \text{sinon si } q > 3 & \text{alors } 6(1 + \frac{p}{q-3}) & \text{[Bal03].} \end{cases}$$

Ces résultats proviennent de travaux des différents auteurs sus-cités, et sont basés sur les idées générales suivantes : utilisation et densification de tours de corps de fonctions algébriques ([Bal99, Bal03]) ; utilisation de places de degré supérieur, densification de tour et descente du corps de définition en caractéristique 2 ([BR04]) ; utilisation de places de degré supérieur et descente du corps de définition en toute caractéristique ([BLBR09]). Ces techniques seront détaillées plus précisément dans la prochaine section.

2.2 Historique de l'algorithme de type Chudnovsky

Depuis la présentation en 1987 de l'algorithme de D.V et G.V. Chudnovsky [CC88], de nombreuses améliorations se sont succédées. L'objectif de ce chapitre est de faire un panorama historique de ces évolutions, dont les dernières sont intervenues récemment, alors que cette thèse était en cours.

2.2.1 Algorithme initial de Chudnovsky-Chudnovsky

En 1987, D.V. Chudnovsky et G.V. Chudnovsky présentent un principe de construction d'algorithmes de multiplication bilinéaire symétrique dans $\mathbb{F}_{q^n}$, basé sur l'interpolation sur des places rationnelles de corps de fonctions algébriques définis sur $\mathbb{F}_q$ et dont la complexité est linéaire par rapport au degré n de l'extension [CC87, CC88]. Plus précisément, l'algorithme symétrique de Chudnovsky-Chudnovsky est le suivant :

Théorème 2.2.1.1. *Supposons que l'on dispose d'un corps de fonctions algébriques $F/\mathbb{F}_q$, d'une place Q de degré n, d'un ensemble $\mathscr{P} := \{P_1, \ldots, P_N\}$ de places de degré 1 et d'un diviseur $\mathcal{D}$ défini sur $\mathbb{F}_q$ tel que $Q, P_1, \ldots, P_N$ n'appartiennent pas au support de $\mathcal{D}$.*

Supposons que les conditions suivantes soient vérifiées :

(i) la fonction d'évaluation

$$\begin{array}{rccc} Ev_Q: & \mathcal{L}(\mathcal{D}) & \longrightarrow & F_Q \simeq \mathbb{F}_{q^n} \\ & f & \longmapsto & f(Q) \end{array}$$

est surjective,

(ii) la fonction d'évaluation

$$\begin{array}{rccc} Ev_{\mathscr{P}}: & \mathcal{L}(2\mathcal{D}) & \longrightarrow & F_{P_1} \times \cdots \times F_{P_N} \simeq \mathbb{F}_q^N \\ & f & \longmapsto & \big(f(P_1), \ldots, f(P_N)\big) \end{array}$$

est injective.

Alors on peut effectuer la multiplication de tous éléments $x, y \in \mathbb{F}_{q^n}$ avec au plus N multiplications bilinéaires, i.e. :

$$\mu_q^{\mathrm{sym}}(n) \leq N.$$

Donnons quelques précisions sur le principe général de fonctionnement de cet algorithme. Comme Q est une place de degré n, le corps de classe résiduel F_Q de la place Q est une extension de degré n de $\mathbb{F}_q$ et peut donc être identifié à $\mathbb{F}_{q^n}$. De plus, Ev_Q étant surjective, on peut associer à tous $x, y \in \mathbb{F}_{q^n}$ des éléments du $\mathbb{F}_q$-espace vectoriel $\mathcal{L}(\mathcal{D})$, notés respectivement f et g. En appliquant la fonction d'évaluation $Ev_{\mathscr{P}}$, on obtient deux N-uplets $\big(f(P_1), \ldots, f(P_N)\big)$ et $\big(g(P_1), \ldots, g(P_N)\big)$ d'éléments de $\mathbb{F}_q$ car les places $P_1, \ldots, P_N$ sont de degré 1. On définit alors $h := fg$ par

$$\big(h(P_1), \ldots, h(P_N)\big) = \big(f(P_1)g(P_1), \ldots, f(P_N)g(P_N)\big). \tag{2.3}$$

On sait qu'un tel élément h appartient à $\mathcal{L}(2\mathcal{D})$ puisque $f, g \in \mathcal{L}(\mathcal{D})$. De plus, par injectivité de $Ev_{\mathscr{P}}$, $h \in \mathcal{L}(2\mathcal{D})$ est uniquement déterminé par (2.3). Finalement, on a

$$xy = Ev_Q(f)Ev_Q(g) = \tilde{Ev}_Q(h)$$

où $\tilde{Ev}_Q$ est l'application de classe résiduelle relativement à Q, dont Ev_Q est la restriction à $\mathcal{L}(\mathcal{D})$.

Concrètement, afin de rendre l'implémentation de cet algorithme plus aisée, on procède de la façon suivante. On choisit un diviseur effectif $\mathcal{D}$ tel que $\dim \mathcal{D} = n$, de sorte que Ev_Q soit un isomorphisme et que $\mathcal{L}(\mathcal{D}) \subsetneq \mathcal{L}(2\mathcal{D})$. En pratique, un tirage au sort parmi les diviseurs (effectifs) de dimension n s'avère être un moyen efficace pour trouver un tel diviseur. On peut alors considérer comme base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ l'image d'une base de $\mathcal{L}(\mathcal{D})$ par Ev_Q. Notons $\mathcal{B} := (f_1, \ldots, f_n)$ une base de $\mathcal{L}(\mathcal{D})$ et complétons-la en une base de $\mathcal{L}(2\mathcal{D})$, $\mathcal{B}' := (f_1, \ldots, f_n, f_{n+1}, \ldots, f_{\tilde{N}})$, où $\tilde{N} := \dim \mathcal{L}(2\mathcal{D}) \leq N$ puisque $Ev_{\mathscr{P}}$ est injective.

On note Γ la matrice de l'application $Ev_{\mathscr{P}} : \mathcal{L}(2\mathcal{D}) \to \mathbb{F}_q^N$ dans la base $\mathcal{B}'$. Comme $Ev_{\mathscr{P}}$ est injective sur $\mathcal{L}(2\mathcal{D})$, quitte à supprimer certaines places dans l'ensemble $\mathscr{P}$, on peut supposer que $Ev_{\mathscr{P}}$ est aussi surjective, de sorte que Γ est inversible. En particulier, on a alors $N = \tilde{N}$. Comme $Q \notin \mathrm{supp}(\mathcal{D}) = \mathrm{supp}(2\mathcal{D})$, on a $\mathcal{L}(\mathcal{D}) \subseteq \mathcal{O}_Q$

et $\mathcal{L}(2\mathcal{D}) \subseteq \mathcal{O}_Q$. On peut donc considérer les images des éléments de la base $\mathcal{B}'$ par $\tilde{Ev}_Q$ et on obtient un système de N équations linéaires :

$$\begin{cases} f_1(Q) &= \sum_{i=1}^{n} c_1^i Ev_Q(f_i) \\ &\vdots \\ f_N(Q) &= \sum_{i=1}^{n} c_N^i Ev_Q(f_i) \end{cases}$$

avec $c_r^i \in \mathbb{F}_q$ pour tous $1 \leq r \leq N$ et $1 \leq i \leq n$; ce qui nous permet de définir la matrice C de l'application $\tilde{Ev}_Q$ sur $\mathcal{B}'$:

$$C := \begin{pmatrix} c_1^1 & \cdots & c_1^n \\ c_2^1 & \cdots & c_2^n \\ \vdots & & \vdots \\ c_N^1 & \cdots & c_N^n \end{pmatrix}$$

On obtient alors le produit $z := xy$ de deux éléments $x, y \in \mathbb{F}_{q^n}$ grâce à l'algorithme suivant :

Entrées : $x = \sum_{i=1}^{n} x_i \, Ev_Q(f_i)$, $y = \sum_{i=1}^{n} y_i \, Ev_Q(f_i)$ //$x_i, y_i \in \mathbb{F}_q$

`1re étape :`
$\Gamma_0 \leftarrow$ matrice formée des n premières colonnes de Γ
$(X_1, \ldots, X_N) \leftarrow (x_1, \ldots, x_n){\Gamma_0}^{\mathrm{t}}$
$(Y_1, \ldots, Y_N) \leftarrow (y_1, \ldots, y_n){\Gamma_0}^{\mathrm{t}}$

`2e étape :`
$(Z_1, \ldots, Z_N) \leftarrow (X_1Y_1, \ldots, X_NY_N)$

`3e étape :`
$(z_1, \ldots, z_n) \leftarrow (Z_1, \ldots, Z_N)(\Gamma^{\mathrm{t}})^{-1}C$

Sorties : $z = \sum_{i=1}^{n} z_i \, Ev_Q(f_i)$ //$z := xy$

Algorithme 1 : Algorithme explicite de multiplication dans $\mathbb{F}_{q^n}$

On peut remarquer que les seules multiplications bilinéaires qui interviennent dans cet algorithme se trouvent à la 2e étape, ce qui permet de conclure que

$$\mu_q^{\mathrm{sym}}(n) \leq N.$$

Ainsi, pour obtenir une borne intéressante pour la complexité bilinéaire, il s'agit d'optimiser le nombre N de places de degré 1 utilisées dans la seconde fonction d'évaluation ; celui-ci dépend à la fois du degré n de l'extension considérée, ainsi que du genre g du corps de fonctions $F/\mathbb{F}_q$. En effet, si le diviseur $\mathcal{D}$ choisi pour l'algorithme est non-spécial et de dimension n (c'est le cas en pratique), alors il est de degré $n + g - 1$ et donc l'espace $\mathcal{L}(2\mathcal{D})$ est de dimension $\dim 2\mathcal{D} = 2n + g - 1$.

Une condition nécessaire pour que la seconde fonction d'évaluation soit injective est donc

$$N \geq 2n + g - 1, \tag{2.4}$$

avec égalité dans le meilleur des cas, ce qui donne comme meilleure borne possible pour la complexité bilinéaire : $\mu_q^{\mathrm{sym}}(n) \leq 2n + g - 1$. Cependant, la condition (2.4) ne suffit pas à assurer de l'injectivité de $Ev_{\mathscr{P}}$. On peut la remplacer par la condition plus forte suivante :

$$N \geq 2n + 2g - 1, \tag{2.5}$$

qui est alors suffisante. En effet, dans ce cas, le noyau $\mathcal{L}\big(2\mathcal{D} - \sum_{i=1}^{N} P_i\big)$ de $Ev_{\mathscr{P}}$ est trivial car $\deg\big(2\mathcal{D} - \sum_{i=1}^{N} P_i\big) < 0$. Notons que remplacer (2.4) par (2.5) ne change pas la borne $\mu_q^{\mathrm{sym}}(n) \leq 2n + g - 1$, car le rang de $Ev_{\mathscr{P}}$ reste $2n + g - 1$. Autrement dit, même si l'on dispose de $2n + 2g - 1$ places rationnelles sur lesquelles effectuer les évaluations, on sait qu'il suffit théoriquement d'en choisir un sous-ensemble de cardinal $2n + g - 1$ pour obtenir une application $Ev_{\mathscr{P}}$ injective.

Lorsque n augmente, l'enjeu est le suivant : trouver un corps de fonctions algébriques de genre minimal avec suffisamment de places rationnelles pour que (2.4), voire (2.5), soit satisfaite.

D'autre part, on a les conditions suffisantes suivantes pour établir l'existence d'un diviseur $\mathcal{D}$ qui convienne :

Lemme 2.2.1.2. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g. S'il existe dans $F/\mathbb{F}_q$*

(i) une place Q de degré n,

(ii) un diviseur $\mathcal{G}$ non-spécial de degré $g - 1$,

alors il existe un diviseur $\mathcal{D}$ non-spécial de degré $n + g - 1$ tel que la fonction d'évaluation $Ev_Q : \mathcal{L}(\mathcal{D}) \to F_Q \simeq \mathbb{F}_{q^n}$ est bien définie (c'est-à-dire que $Q \notin \operatorname{supp}\mathcal{D}$) et est bijective.

Preuve. Soit $\mathcal{D}_1 := \mathcal{G} + Q$. Par le lemme 1.1.4.11 de déplacement du support, on peut choisir un diviseur $\mathcal{D}$ équivalent à $\mathcal{D}_1$ et dont le support ne contienne pas Q. On a alors $\deg\mathcal{D} = n + g - 1$ et $\dim\mathcal{L}(\mathcal{D} - Q) = \dim\mathcal{G} = 0$, donc $Ev_Q : \mathcal{L}(\mathcal{D}) \to F_Q$ est injective. En particulier, on a $\dim\mathcal{D} \leq \dim F_Q = n$. D'autre part, comme $\dim\mathcal{D} = \deg\mathcal{D} - g + 1 + i(\mathcal{D}) \geq n$, on a finalement $\dim\mathcal{D} = n$ ce qui établit la bijectivité de Ev_Q et implique de plus que $i(\mathcal{D}) = 0$. □

Finalement, on peut énoncer le théorème suivant qui synthétise ce qui vient d'être établi :

Théorème 2.2.1.3. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g avec au moins N places rationnelles tel que*

(i) il existe une place de degré n,

(ii) il existe un diviseur non-spécial de degré $g - 1$,

(iii) $N \geq 2n + 2g - 1$.

Alors on a

$$\mu_q^{\mathrm{sym}}(n) \leq 2n + g - 1.$$

2.2.2 Utilisation de places de degré supérieur

Afin d'obtenir plus facilement l'injectivité de la seconde fonction d'évaluation, l'utilisation de places de degré supérieur a été envisagée par Ballet et Rolland dans [BR04] pour le cas des places de degré 2, puis généralisée à des places de degré quelconque dans [CÖ10] par Cenk et Özbudak. L'algorithme symétrique modifié est alors le suivant :

Théorème 2.2.2.1. *Soient $F/\mathbb{F}_q$ un corps de fonctions algébriques, Q une place de degré n, $\mathscr{P} := \{P_1, \ldots, P_N\}$ un ensemble de places de degré quelconque et $\mathcal{D}$ un diviseur défini sur $\mathbb{F}_q$ tel que les places $Q, P_1, \ldots, P_N$ n'appartiennent pas au support de $\mathcal{D}$. Si les conditions suivantes sont vérifiées :*

(i) la fonction d'évaluation

$$\begin{array}{rccc} Ev_Q : & \mathcal{L}(\mathcal{D}) & \longrightarrow & F_Q \simeq \mathbb{F}_{q^n} \\ & f & \longmapsto & f(Q) \end{array}$$

est surjective,

(ii) la fonction d'évaluation

$$\begin{array}{rccc} Ev_{\mathscr{P}} : & \mathcal{L}(2\mathcal{D}) & \longrightarrow & F_{P_1} \times \cdots \times F_{P_N} \simeq \mathbb{F}_q^{\deg P_1} \times \ldots \times \mathbb{F}_q^{\deg P_N} \\ & f & \longmapsto & \big(f(P_1), \ldots, f(P_N)\big) \end{array}$$

est injective.

Alors cet algorithme symétrique de type Chudnovsky donne la borne suivante :

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i).$$

En effet, la seule différence avec l'algorithme initial de Chudnovsky-Chudnovsky réside dans l'obtention du N-uplet $\big(h(P_1), \ldots, h(P_N)\big)$ comme produit terme à terme des deux N-uplets $\big(f(P_1), \ldots, f(P_N)\big)$ et $\big(g(P_1), \ldots, g(P_N)\big)$. Ces N-uplets n'étant plus constitués d'éléments de $\mathbb{F}_q$ mais d'éléments de $\mathbb{F}_{q^{\deg P_i}}$, la détermination de chacun des $h(P_i)$ nécessite donc $\mu_q^{\mathrm{sym}}(\deg P_i)$ multiplications dans $\mathbb{F}_q$.

On peut alors énoncer un résultat analogue au théorème 2.2.1.3 :

Théorème 2.2.2.2. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g avec au moins N_k places de degré k pour $1 \leq k \leq d$. Si*

(i) il existe une place de degré n,

(ii) il existe un diviseur non-spécial de degré $g-1$,

(iii) $\sum_{k=1}^{d} kN_k \geq 2n + 2g - 1$.

Alors on a

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{k=1}^{d} \mu_q^{\mathrm{sym}}(k) N_k.$$

2.2.3 Évaluations d'ordre supérieur

En 2006 et 2010, Arnaud et Cenk-Özbudak introduisent dans [Arn06] et [CÖ10] une notion généralisée d'évaluation, les évaluations d'ordre supérieur (ou « évaluations dérivées »), qui consiste à ré-utiliser les mêmes places en effectuant des évaluations avec multiplicité. Cette technique permet d'optimiser l'utilisation des places de petit degré, places dont la contribution à la complexité bilinéaire est la plus faible comme on a pu le voir dans la section précédente. Bien que ces deux travaux reposent sur des idées semblables, ils proviennent de réflexions indépendantes, les résultats de Nicolas Arnaud n'ayant pas été publiés. De plus, le travail de Cenk et Özbudak est plus général que celui d'Arnaud, les évaluations pouvant dépasser l'ordre 2.

Soient P une place de degré quelconque d'un corps de fonctions $F/\mathbb{F}_q$ et t un paramètre local fixé pour cette place. Toute fonction $f \in F$ régulière en P admet alors un unique développement local de la forme :

$$f = \alpha_0 + \alpha_1 t + \alpha_2 t^2 + \cdots \quad \text{où } \alpha_0, \alpha_1, \alpha_2 \ldots \in \mathbb{F}_{q^{\deg P}}.$$

On note $f(P) = f^{(0)}(P) := \alpha_0$ l'évaluation de f en P et $f'(P) = f^{(1)}(P) := \alpha_1$, $\ldots, f^{(l-1)}(P) := \alpha_{l-1}$ les évaluations d'ordre supérieur de f en P.

On dit qu'on utilise une place P avec multiplicité $l \geq 1$ lorsque les l premières évaluations en P, $f(P), f^{(1)}(P), \ldots, f^{(l-1)}(P)$, sont prises en compte dans la deuxième fonction d'évaluation de l'algorithme :

Théorème 2.2.3.1. *Supposons que l'on dispose d'un corps de fonctions algébriques $F/\mathbb{F}_q$, d'une place Q de degré n, d'un ensemble $\mathscr{P} := \{P_1, \ldots, P_N\}$ de places de degré quelconque et d'un diviseur $\mathcal{D}$ défini sur $\mathbb{F}_q$ tel que les places $Q, P_1, \ldots, P_N$ n'appartiennent pas au support de $\mathcal{D}$.*
Pour toute place $P_i \in \mathscr{P}$, on fixe un paramètre local t_i.
Supposons que

(i) la fonction d'évaluation

$$\begin{array}{rccc} Ev_Q : & \mathcal{L}(\mathcal{D}) & \longrightarrow & F_Q \simeq \mathbb{F}_{q^n} \\ & f & \longmapsto & f(Q) \end{array}$$

est surjective,

(ii) l'application $\mathbb{F}_q$-linéaire

$$\begin{array}{rccc} \varphi : & \mathcal{L}(2\mathcal{D}) & \longrightarrow & (\mathbb{F}_{q^{\deg P_1}})^{l_1} \times (\mathbb{F}_{q^{\deg P_2}})^{l_2} \times \cdots \times (\mathbb{F}_{q^{\deg P_N}})^{l_N} \\ & f & \longmapsto & \big(f(P_1), f^{(1)}(P_1), \ldots, f^{(l_1-1)}(P_1), f(P_2), f^{(1)}(P_2), \ldots, \\ & & & f^{(l_2-1)}(P_2), \ldots, f(P_N), f^{(1)}(P_N), \ldots, f^{(l_N-1)}(P_N)\big) \end{array}$$

est injective.

Alors on a la borne suivante pour la complexité bilinéaire symétrique de la multiplication :

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i) \mu_{q^{\deg P_i}}^{\mathrm{sym}}(1, l_i). \tag{2.6}$$

Précisons un peu le calcul de cette borne. Le recours aux évaluations d'ordre supérieur complexifie la façon d'obtenir $\varphi(fg)$ à partir des deux « évaluations » $\varphi(f)$ et $\varphi(g)$. En effet, $(fg)^{(k)}(P_i)$, le k-ième terme du développement local en P_i du produit fg, s'obtient à partir des développements locaux jusqu'à l'ordre k en P_i de chacune des deux fonctions f et g de la façon suivante :

$$(fg)^{(k)}(P_i) = \sum_{j=0}^{k} f^{(j)}(P_i) g^{(k-j)}(P_i).$$

Ainsi, obtenir les l_i éléments $(fg)(P_i), (fg)^{(1)}(P_i), \ldots, (fg)^{(l_i-1)}(P_i)$ de $\mathbb{F}_{q^{\deg P_i}}$ revient à calculer les l_i premiers coefficients du produit des deux polynômes suivants de $\mathbb{F}_{q^{\deg P_i}}[t]$:

$$\sum_{u=0}^{l_i-1} f^{(u)}(P_i) t^u$$

et

$$\sum_{u=0}^{l_i-1} g^{(u)}(P_i) t^u.$$

Par définition, la complexité bilinéaire sur $\mathbb{F}_{q^{\deg P_i}}$ de ce produit est donnée par la quantité $\mu^{\mathrm{sym}}_{\mathbb{F}_{q^{\deg P_i}}}\big(\mathbb{F}_{q^{\deg P_i}}[t]/(t^{l_i})\big) = \mu^{\mathrm{sym}}_{q^{\deg P_i}}(1, l_i)$. Le calcul du développement local de $(fg)(P_i)$ jusqu'à l'ordre $l_i - 1$ nécessite donc $\mu^{\mathrm{sym}}_q(\deg P_i)\mu^{\mathrm{sym}}_{q^{\deg P_i}}(1, l_i)$ multiplications d'éléments de $\mathbb{F}_q$, d'où l'obtention de la borne (2.6) en effectuant ce calcul pour chacune des places $P_1, \ldots, P_N$.

Si l'on reformule les hypothèses en regroupant les places de même degré et de même multiplicité dans l'ensemble $\mathscr{P}$, le théorème 2.2.1.3 devient :

Théorème 2.2.3.2. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g. Pour $k, l \in \mathbb{N}$ tels que $1 \leq k \leq d$ et $l \geq 1$, on choisit des entiers $n_{k,l} \geq 0$ pour lesquels*

$$\sum_{l \geq 1} n_{k,l} \leq B_k(F/\mathbb{F}_q). \tag{2.7}$$

Si

(i) il existe une place de degré n,

(ii) il existe un diviseur non-spécial de degré $g - 1$,

(iii) $\sum_{k=1}^{d} k \cdot \big(\sum_{l \geq 1} l n_{k,l}\big) \geq 2n + 2g - 1$.

Alors on a

$$\mu^{\mathrm{sym}}_q(n) \leq \sum_{k=1}^{d} \mu^{\mathrm{sym}}_q(k) \Big(\sum_{l \geq 1} n_{k,l} \mu^{\mathrm{sym}}_{q^k}(1, l) \Big).$$

Dans cet énoncé, pour $1 \leq k \leq d$ et $l \geq 1$ fixés, l'entier $n_{k,l}$ représente le nombre de places de degré k utilisées avec multiplicité l dans l'algorithme : en particulier, comme l'impose la contrainte (2.7), seul un nombre fini d'entre eux sont non-nuls.

2.2.4 Le problème de la 2-torsion

Détaillons le principe général d'obtention de bornes explicites pour $\mu_q(n)$ grâce à l'algorithme de type Chudvnosky. Dans un soucis de clarté, on considère la version initiale de l'algorithme présentée en début de chapitre. Le principe est analogue dans les versions postérieures.

Pour multiplier dans $\mathbb{F}_{q^n}$, on se place sur un corps de fonctions $F/\mathbb{F}_q$ de genre g dans lequel on dispose

- d'une place de degré n (il suffit pour cela que $2g+1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$, d'après le lemme 1.1.5.12),
- de $2n+g-1$ places de degré 1, $P_1, \ldots, P_{2n+g-1}$, comme on l'a expliqué dans la section 2.2.1. On pose $\mathcal{A} := \sum_{i=1}^{2n+g-1} P_i$.

On cherche alors à déterminer s'il existe un diviseur $\mathcal{D}$ qui convient pour l'algorithme. Plus précisément, on cherche un diviseur $\mathcal{D}$ de degré $n+g-1$ qui vérifie les deux conditions suivantes :

(1) $\dim(\mathcal{D}-Q) = 0$, de sorte que la première fonction d'évaluation soit injective. Ainsi, on a $\mathrm{Im}(Ev_Q) \subseteq F_Q \simeq \mathbb{F}_{q^n}$, et comme d'autre part

$$\dim \mathcal{D} = \deg \mathcal{D} - g + 1 + i(\mathcal{D}) \geq n$$

par le théorème de Riemann-Roch, on a finalement $\dim \mathcal{D} = n$, donc Ev_Q est surjective et de plus, $\mathcal{D}$ est non-spécial.

(2) $\dim(2\mathcal{D}-\mathcal{A}) = 0$, c'est-à-dire que le noyau de la seconde fonction d'évaluation est trivial.

Dans [STV92], un argument de dénombrement est apporté pour établir qu'un tel diviseur existe. Malheureusement, cet argument est erroné, ainsi que cela a été signalé par Cascudo, Cramer et Xing en 2010 (voir [Cas10, Remark 12.4]). Expliquons plus précisément ce qu'il en est.

Le raisonnement dans [STV92] est le suivant : comme les propriétés attendues pour le diviseur $\mathcal{D}$ ne dépendent que de sa classe (puisqu'on ne lui impose que des conditions de dimension et de degré, lesquels sont invariants au sein d'une même classe), on peut se ramener à déterminer l'existence d'une classe de diviseurs $[\mathcal{D}]$ qui satisfait les propriétés demandées. Pour cela, il suffit de s'assurer que le nombre de classes de diviseurs pour lesquelles une des deux conditions (1) ou (2) est fausse est strictement inférieur à h_F, le nombre de classe de F. De plus, en vertu de la proposition 1.1.4.2(b), il y a toujours au moins un diviseur effectif dans une classe de diviseurs de dimension non-nulle. Jusque-là, le raisonnement est correct. L'erreur est d'en conclure que le nombre de diviseurs pour lesquels au moins une des deux conditions (1) ou (2) est fausse est au plus $2A_{g-1}$. Rappelons que $A_i := \big|\{\mathcal{D} \in \mathrm{Div}(F) \mid \mathcal{D} \geq 0 \text{ et } \deg \mathcal{D} = i\}\big|$.

En effet, présentons les choses de façon à mettre en lumière le problème : on veut déterminer le nombre de classes de diviseurs pour lesquelles au moins une des deux

conditions (1) ou (2) est fausse. On considère les applications suivantes :

$$\begin{array}{rccc} G: & \mathrm{Cl}^{n+g-1}(F) & \longrightarrow & \mathrm{Cl}^{g-1}(F) \\ & [\mathcal{D}] & \longmapsto & [\mathcal{D}]-[Q] \end{array}$$

et

$$\begin{array}{rccc} H: & \mathrm{Cl}^{n+g-1}(F) & \longrightarrow & \mathrm{Cl}^{g-1}(F) \\ & [\mathcal{D}] & \longmapsto & 2\,[\mathcal{D}]-[\mathcal{G}] \end{array}$$

et on pose $\mathrm{Cl}^i_{\mathrm{eff}}(F) := \{[\mathcal{A}] \in \mathrm{Cl}^i(F) \mid \exists\, \mathcal{A}' \in [\mathcal{A}] \text{ tel que } \mathcal{A}' \geq 0\}$.

La condition (1) n'est pas vérifiée pour toutes les classes de diviseurs $[\mathcal{D}]$ telles que $\mathcal{L}(\mathcal{D}-Q) \neq \{0\}$. Or d'après la proposition 1.1.4.2(b), on a

$$\mathcal{L}(\mathcal{D}-Q) \neq \{0\} \Longleftrightarrow [\mathcal{D}-Q] \in \mathrm{Cl}^{g-1}_{\mathrm{eff}}(F).$$

On a donc au plus $\left|G^{-1}\left(\mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)\right)\right|$ classes de diviseurs $[\mathcal{D}]$ pour lesquelles $G([\mathcal{D}]) \in \mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)$. Comme G est injective, il y a au plus $\left|\mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)\right|$ telles classes de diviseurs. Or $\left|\mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)\right| \leq A_{g-1}$, il y a donc finalement au plus A_{g-1} classes de diviseurs pour lesquelles la condition (1) n'est pas vérifiée.

D'autre part, (2) n'est pas vérifiée pour toutes les classes de diviseurs $[\mathcal{D}]$ telles que $\mathcal{L}(2\mathcal{D}-\mathcal{G}) \neq \{0\}$. Ainsi, il y a au plus $\left|H^{-1}\left(\mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)\right)\right|$ classes de diviseurs $[\mathcal{D}]$ pour lesquelles $H([\mathcal{D}]) \in \mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)$. Or cette fois, H n'est pas injective : on a $\left|H^{-1}\left(\mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)\right)\right| = J[2] \cdot \left|\mathrm{Cl}^{g-1}_{\mathrm{eff}}(F)\right|$ où $J[2] := \left|\{[\mathcal{A}] \in \mathrm{Cl}^0(F)\,;\, 2[\mathcal{A}] = 0\}\right|$. Il y a donc au plus $J[2] \cdot A_{g-1}$ classes de diviseurs pour lesquelles la condition (2) n'est pas vérifiée.

Finalement, les deux conditions (1) et (2) sont vérifiées simultanéement dès que $A_{g-1} + J[2] \cdot A_{g-1} < h_F$. Cette hypothèse est plus forte que $2A_{g-1} < h_F$, qui est celle demandée dans [STV92], ce qui explique que les bornes établies avec cette dernière condition ne sont pas valides. Notons que cette erreur affecte aussi les résultats obtenus par Ballet dans [Bal08a] et [Bal08b], puisqu'ils reposent sur un raisonnement similaire.

En général, on ne connait pas précisément $J[2]$, il est donc difficile d'établir l'existence du diviseur $\mathcal{D}$ souhaité ; d'où l'intérêt de la version asymétrique de l'algorithme présentée ci-après.

2.2.5 Algorithme asymétrique

Récemment, Randriambolona a présenté dans [Ran12] une dernière généralisation de l'algorithme de type Chudnovsky. C'est la première version de l'algorithme qui, par construction, n'est pas nécessairement symétrique. Cette propriété est recherchée pour contrer le problème de la 2-torsion vu dans le paragraphe précédent. Une autre avancée notable est l'utilisation de la quantité $\mu_q(m,l)$, qui permet d'estimer plus précisément le coût de l'utilisation simultanée de places de degré m avec multiplicité l puisque l'on a :

$$\mu_q(m,l) \leq \mu_q(m) \times \mu_{q^m}(1,l).$$

Énoncé avec le vocabulaire général des faisceaux dans l'article original [Ran12], on en donne ici un point de vue du domaine des corps de fonctions algébriques.

Théorème 2.2.5.1. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques et soient $m, l \geq 1$ deux entiers. Soient Q une place de degré m, et $P_1, \ldots, P_N$ des places de degré quelconque, qui seront utilisées avec multiplicités respectives $l_1, \ldots, l_N \geq 1$. Supposons qu'il existe deux diviseurs $\mathcal{D}_1$ et $\mathcal{D}_2$ dans $F/\mathbb{F}_q$, tels que :*

(i) les fonctions d'évaluation

$$\begin{array}{ccc} \mathcal{L}(\mathcal{D}_1) & \longrightarrow & \mathcal{O}_X(\mathcal{D}_1)|_{Q^{[l]}} \simeq \mathbb{F}_{q^m}[t]/(t^l) \\ f & \longmapsto & t_Q^{-v_Q(\mathcal{D}_1)} f \mod (t_Q^l) \end{array}$$

et

$$\begin{array}{ccc} \mathcal{L}(\mathcal{D}_2) & \longrightarrow & \mathcal{O}_X(\mathcal{D}_2)|_{Q^{[l]}} \\ f & \longmapsto & t_Q^{-v_Q(\mathcal{D}_2)} f \mod (t_Q^l) \end{array}$$

sont surjectives (où $t_Q^{-v_Q(\mathcal{D}_i)}$ est un générateur local pour $\mathcal{O}_X(\mathcal{D}_i)$ en Q),

(ii) la fonction d'évaluation

$$\begin{array}{ccc} \mathcal{L}(\mathcal{D}_1+\mathcal{D}_2) & \longrightarrow & \displaystyle\prod_{i=1}^{N} \mathcal{O}_X(\mathcal{D}_1+\mathcal{D}_2)\big|_{P_i^{[l_i]}} \simeq \prod_{i=1}^{N} \mathbb{F}_{q^{\deg P_i}}[t]/(t^{l_i}) \\ f & \longmapsto & \big(t_{P_1}^{-v_{P_1}(\mathcal{D}_1+\mathcal{D}_2)} f \mod (t_{P_1}^{l_1}), \ldots, t_{P_N}^{-v_{P_N}(\mathcal{D}_1+\mathcal{D}_2)} f \mod (t_{P_N}^{l_N})\big) \end{array}$$

est injective.

Alors on a la borne suivante pour la complexité bilinéaire de la multiplication :

$$\mu_q(m,l) \leq \sum_{i=1}^{N} \mu_q(\deg P_i, l_i). \tag{2.8}$$

Notons que dans cette version de l'algorithme, en raison du choix de la définition des fonctions d'évaluations utilisées, aucune supposition n'est faite sur le support des diviseurs $\mathcal{D}_1$ et $\mathcal{D}_2$. Cependant, celles qui étaient faites sur le diviseur $\mathcal{D}$ dans les versions précédentes n'étaient pas restrictives, en raison du lemme de déplacement du support 1.1.4.11.

Cette généralisation de l'algorithme permet d'effectuer la multiplication de deux éléments de $\mathbb{F}_{q^m}[t]/(t^l)$ où l est possiblement strictement supérieur à 1. De plus, une quantité de même « type » $\mu_q(k,j)$, apparaît de part et d'autre de l'inégalité, ce qui permet à la fois d'obtenir des bornes supérieures en fonction de cette quantité, mais aussi d'en déduire pour celle-ci de façon récursive ; une fois les bornes nécessaires pré-établies, on peut utiliser l'algorithme avec $l = 1$ pour obtenir des estimations de $\mu_q(n)$. Cependant, le grand intérêt de cette version est de faciliter les conditions d'existence des diviseurs $\mathcal{D}_1$ et $\mathcal{D}_2$ qui satisfont (i) et (ii). Dans les versions précédentes, un seul diviseur $\mathcal{D}$ était à déterminer, mais avec des contraintes plus fortes. Ici, si l'on note $\mathcal{A}$ le diviseur suivant :

$$\mathcal{A} = \sum_{i=1}^{N} l_i P_i$$

alors des conditions suffisantes pour que les diviseurs $\mathcal{D}_1$ et $\mathcal{D}_2$ satisfassent (i) et (ii) sont :

(i') les diviseurs $\mathcal{D}_1 - lQ$ et $\mathcal{D}_2 - lQ$ sont non-spéciaux :

$$i(\mathcal{D}_1 - lQ) = i(\mathcal{D}_2 - lQ) = 0,$$

(ii') le diviseur $\mathcal{D}_1 + \mathcal{D}_2 - \mathcal{A}$ est de dimension nulle :

$$\dim(\mathcal{D}_1 + \mathcal{D}_2 - \mathcal{A}) = 0.$$

Plus précisément, (ii) et (ii') sont équivalentes alors que (i') implique seulement (i) a priori. Ces conditions sont vérifiées sous les hypothèses du théorème suivant, qui est l'analogue dans cette généralisation, du théorème 2.2.1.3 :

Théorème 2.2.5.2. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre $g \geq 2$, et soient $m, l \geq 1$ deux entiers. Considérons, pour $d, u \geq 1$, des entiers $n_{d,u} \geq 0$, nuls sauf pour un nombre fini d'entre eux et tels pour tout d, on ait :*

$$\sum_{u \geq 1} n_{d,u} \leq B_d(F/\mathbb{F}_q). \tag{2.9}$$

Si

(i) il existe une place de degré m dans $F/\mathbb{F}_q$,

(ii) $\sum_{d,u \geq 1} n_{d,u} du \geq 2ml + 3e + g - 1$, où la constante e est définie par

$$e = \begin{cases} 2 & si\ q = 2, \\ 1 & si\ q = 3, 4, 5, \\ 0 & si\ q \geq 7. \end{cases}$$

Alors on a

$$\mu_q(m, l) \leq \sum_{d,u \geq 1} n_{d,u} \mu_q(d, u).$$

En plus de ce résultat, Randriambololona a aussi donné une preuve constructive de l'existence de ces diviseurs $\mathcal{D}_1$ et $\mathcal{D}_2$.

Enfin, il est important de garder à l'esprit que, contrairement aux versions antérieures, toutes les bornes obtenues avec cette version de l'algorithme, sont, sauf dans le cas où l'on peut choisir $\mathcal{D}_1 = \mathcal{D}_2$, des bornes pour $\mu_q(m, l)$ et non pour $\mu_q^{\mathrm{sym}}(m, l)$, et donc ne permettent en définitive d'obtenir que des estimations pour $\mu_q(n)$ et non pour $\mu_q^{\mathrm{sym}}(n)$. Dans le cadre exclusif de la détermination de la complexité bilinéaire de la multiplication dans les extensions des corps finis, cette différence n'est pas gênante — hormis un éventuel surcoût en terme de complexité linéaire puisqu'il y a trois fonctions à implémenter, au lieu de deux dans le cadre de l'algorithme symétrique. Signalons cependant que dans des domaines qui reposent sur des principes similaires à celui de l'algorithme de type Chudnovsky mais qui ne seront pas étudiés ici, tels que le calcul multi-parties ou les systèmes d'équations de Riemann-Roch et certaines de leurs applications (partage de secret, frameproof codes) la symétrie de l'algorithme est fondamentale (voir [Cas10]).

Chapitre 3

De « bonnes » tours de corps de fonctions algébriques

On présente dans la section 3.1 les tours de corps de fonctions algébriques qui seront utilisées pour l'amélioration des bornes dans les chapitres suivants. Puis, dans la section 3.2, on établit une série de lemmes techniques relatifs à des propriétés de ces tours, utiles pour l'établissement des bornes.

3.1 Tours de Garcia-Stichtenoth

3.1.1 Tour de Garcia-Stichtenoth d'extensions d'Artin-Schreier de corps de fonctions

On présente ici une version modifiée de la tour de Garcia-Stichtenoth introduite dans [GS95] et définie sur les corps $\mathbb{F}_{q^2}$ où $q = p^r \geq 4$ et r est un entier positif.

Notons $\mathcal{T}_1$ la tour abélienne élémentaire initialement construite par Garcia et Stichtenoth sur $\mathbb{F}_{q^2}$. Elle est définie par la suite $(F_1, F_2, F_3, \ldots)$ où $F_1 := \mathbb{F}_{q^2}(x_1)$ est le corps des fonctions rationnelles sur $\mathbb{F}_{q^2}$ et pour tout $k \geq 1$,

$$F_{k+1} := F_k(z_{k+1})$$

où z_{k+1} satisfait l'équation

$$z_{k+1}^q + z_{k+1} = x_k^{q+1}$$

avec

$$x_k := z_k / x_{k-1} \text{ dans } F_k \text{ pour tout } k \geq 2.$$

Notons que F_2 est alors le corps des fonctions Hermitien sur $\mathbb{F}_{q^2}$.
Dans toute cette section, on notera g_k le genre de F_k ; rappelons qu'il est donné par la formule suivante :

$$g_k = \begin{cases} q^k + q^{k-1} - q^{\frac{k+1}{2}} - 2q^{\frac{k-1}{2}} + 1 & \text{si } k \equiv 1 \pmod 2, \\ q^k + q^{k-1} - \frac{1}{2}q^{\frac{k}{2}+1} - \frac{3}{2}q^{\frac{k}{2}} - q^{\frac{k}{2}-1} + 1 & \text{si } k \equiv 0 \pmod 2. \end{cases} \tag{3.1}$$

On note $\mathcal{T}_2$ la tour complétée présentée par Ballet dans [Bal03] :

$$\mathcal{T}_2 := F_{1,0} \subseteq F_{1,1} \subseteq \cdots \subseteq F_{1,r} = F_{2,0} \subseteq F_{2,1} \subseteq \cdots \subseteq F_{2,r} \subseteq \cdots$$

où les étages intermédiaires satisfont $F_k \subseteq F_{k,s} \subseteq F_{k+1}$ pour tout entier $s \in \{0, \dots, r\}$, avec $F_{k,0} := F_k$ et $F_{k,r} := F_{k+1}$. Rappelons que chaque extension $F_{k,s}/F_k$ est galoisienne de degré p^s avec corps plein des constantes $\mathbb{F}_{q^2}$, et que cette tour est asymptotiquement optimale sur $\mathbb{F}_{q^2}$.

Dans [BR04], Ballet et Rolland ont montré que la descente du corps de définition de chacun des étages de la tour complétée $\mathcal{T}_2$ de $\mathbb{F}_{q^2}$ sur $\mathbb{F}_q$ est possible. Autrement dit, on peut définir la tour $\mathcal{T}_3/\mathbb{F}_q$ suivante :

$$\mathcal{T}_3 := G_{1,0} \subseteq G_{1,1} \subseteq \cdots \subseteq G_{1,r} = G_{2,0} \subseteq G_{2,1} \subseteq \cdots \subseteq G_{2,r} \subseteq \cdots$$

où pour tous $k \geq 1$ et $s \in \{0, \dots, r\}$, on a $G_k \subseteq G_{k,s} \subseteq G_{k+1}$, $G_{k,0} := G_k$ et $G_{k,r} := G_{k+1}$. De plus, cette tour est reliée à la tour $\mathcal{T}_2$ par

$$F_{k,s} = \mathbb{F}_{q^2} G_{k,s} \text{ pour tous } k \text{ et } s,$$

c'est-à-dire que $\mathbb{F}_{k,s}/\mathbb{F}_{q^2}$ est l'extension du corps des constantes de $G_{k,s}/\mathbb{F}_q$. Notons que cette tour est bien définie d'après [BR04] et [BLBR09], où en particulier, il a été prouvé le résultat suivant :

Proposition 3.1.1.1. *Soit $q = p^r \geq 4$ une puissance d'un premier p. Pour tous entiers $k \geq 1$ et $s \in \{0, \dots, r\}$, il existe un étage $F_{k,s}/\mathbb{F}_{q^2}$ (respectivement $G_{k,s}/\mathbb{F}_q$) de genre $g_{k,s}$ avec $M_{k,s}$ places rationnelles dans $F_{k,s}/\mathbb{F}_{q^2}$ (respectivement $M_{k,s} := B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q)$ où $B_1(G_{k,s}/\mathbb{F}_q)$ et $B_2(G_{k,s}/\mathbb{F}_q)$ dénotent respectivement le nombre de places de degré 1 et 2 dans $G_{k,s}/\mathbb{F}_q$) tel que :*
(1) $\big(g_k - 1\big)p^s + 1 \leq g_{k,s} \leq \frac{g_{k+1}}{p^{r-s}} + 1$,
(2) $M_{k,s} \geq (q^2 - 1)q^{k-1}p^s$.

On s'intéresse maintenant à la descente du corps de définition des étages de la tour $\mathcal{T}_2$ de $\mathbb{F}_{q^2}$ sur $\mathbb{F}_p$. Il n'y a pas de résultat général à ce sujet, mais on peut montrer que c'est possible dans le cas particulier de la caractéristique 2. C'est l'objet du prochain résultat, obtenu dans [BR11]. Notons que dans un souci de clarté, on continuera à utiliser la variable p sans perdre de vue que dans ce cadre exclusif $p = 2$. On rappelle aussi la démonstration de ce résultat qui donne les équations explicites de chacun des étages de la tour descendue sur $\mathbb{F}_2$.

Proposition 3.1.1.2. *Posons $p = 2$. Si $q = p^2$, alors la descente du corps de définition de la tour $\mathcal{T}_2$ de $\mathbb{F}_{q^2}$ sur $\mathbb{F}_p$ est possible. Plus précisément, il existe une tour $\mathcal{T}_4$ définie sur $\mathbb{F}_p$ et donnée par la suite :*

$$\mathcal{T}_4 := H_{1,0} \subseteq H_{1,1} \subseteq H_{1,2} = H_{2,0} \subseteq H_{2,1} \subseteq H_{2,2} = H_{3,0} \subseteq \cdots$$

et reliée aux tours $\mathcal{T}_2/\mathbb{F}_{q^2}$ et $\mathcal{T}_3/\mathbb{F}_q$ par

$$F_{k,s} = \mathbb{F}_{q^2} H_{k,s} \text{ pour tous } k \geq 1 \text{ et } s \in \{0, 1, 2\},$$

et

$$G_{k,s} = \mathbb{F}_q H_{k,s} \text{ pour tous } k \geq 1 \text{ et } s \in \{0, 1, 2\},$$

c'est-à-dire que $F_{k,s}/\mathbb{F}_{q^2}$ est l'extension du corps des constantes de $G_{k,s}/\mathbb{F}_q$ et $H_{k,s}/\mathbb{F}_p$, et que $G_{k,s}/\mathbb{F}_q$ est l'extension du corps des constantes de $H_{k,s}/\mathbb{F}_p$.

Preuve. Soit x_1 un élément transcendant sur $\mathbb{F}_2$ et posons

$$H_1 = \mathbb{F}_2(x_1),\ G_1 = \mathbb{F}_4(x_1),\ F_1 = \mathbb{F}_{16}(x_1).$$

Pour $k \geq 1$, on définit de façon récursive :

1. z_{k+1} tel que $z_{k+1}^4 + z_{k+1} = x_k^5$,
2. t_{k+1} tel que $t_{k+1}^2 + t_{k+1} = x_k^5$ (ou encore $t_{k+1} = z_{k+1}(z_{k+1}+1)$),
3. $x_{k+1} = z_{k+1}/x_k$,
4. $H_{k,1} = H_{k,0}(t_{k+1}) = H_k(t_{k+1})$, $H_{k+1,0} = H_{k+1} = H_k(z_{k+1})$;
   $G_{k,1} = G_{k,0}(t_{k+1}) = G_k(t_{k+1})$, $G_{k+1,0} = G_{k+1} = G_k(z_{k+1})$;
   $F_{k,1} = F_{k,0}(t_{k+1}) = F_k(t_{k+1})$, $F_{k+1,0} = F_{k+1} = F_k(z_{k+1})$.

D'après [BLBR09], la tour $\left(F_{k,i}\right)_{k\geq 1, i=0,1}$ est la tour densifiée de Garcia-Stichtenoth $\mathcal{T}_2$ sur $\mathbb{F}_{16}$, définie précédemment et les deux autres tours sont respectivement les descentes de la tour $\mathcal{T}_2$ sur $\mathbb{F}_4$ et sur $\mathbb{F}_2$. □

Enfin, on rappelle les propriétés suivantes de la tour $\mathcal{T}_4$:

Proposition 3.1.1.3. *Soit $q = p^2 = 4$. Pour tous $k \geq 1$ et $s \in \{0,1,2\}$, l'étage $H_{k,s}$ de la tour $\mathcal{T}_4/\mathbb{F}_p$, de genre $g(H_{k,s}/\mathbb{F}_p)$ avec $B_1(H_{k,s}/\mathbb{F}_p)$ places de degré un, $B_2(H_{k,s}/\mathbb{F}_p)$ places de degré deux et $B_4(H_{k,s}/\mathbb{F}_p)$ places de degré quatre vérifie :*

(1) $H_k/\mathbb{F}_p \subseteq H_{k,s}/\mathbb{F}_p \subseteq H_{k+1}/\mathbb{F}_p$ *avec* $H_{k,0} = H_k$ *et* $H_{k,2} = H_{k+1}$,

(2) $g(H_{k,s}/\mathbb{F}_p) \leq \frac{g(H_{k+1}/\mathbb{F}_p)}{p^{2-s}} + 1$ *avec* $g(H_{k+1}/\mathbb{F}_p) = g_{k+1} \leq q^{k+1} + q^k$,

(3) $B_1(H_{k,s}/\mathbb{F}_p) + 2B_2(H_{k,s}/\mathbb{F}_p) + 4B_4(H_{k,s}/\mathbb{F}_p) \geq (q^2-1)q^{k-1}p^s$.

3.1.2 Tour de Garcia-Stichtenoth d'extensions de Kummer de corps de fonctions

Dans cette section, on présente une seconde tour de Garcia-Stichtenoth ayant de bonnes propriétés.

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geq 3$. On considère la tour $\mathcal{T}_5$ définie sur $\mathbb{F}_q$ de façon récursive par l'équation :

$$y^2 = \frac{x^2+1}{2x}.$$

Cette tour, qui a été introduite et étudiée dans [GSR03], est constituée de la suite $(L_0, L_1, L_2, \ldots)$ de corps de fonctions algébriques, où $L_n := \mathbb{F}_q(x_0, x_1, \ldots, x_n)$ avec

$$x_{i+1}^2 = \frac{x_i^2+1}{2x_i} \text{ pour tout } i \geq 0.$$

Notons ici aussi que L_0 est le corps des fonctions rationnelles.

Pour tout nombre premier $p \geq 3$, la tour $\mathcal{T}_5/\mathbb{F}_{p^2}$ est asymptotiquement optimale sur $\mathbb{F}_{p^2}$. De plus, pour tout entier $k \geq 0$, $L_k/\mathbb{F}_{p^2}$ est l'extension du corps

des constantes de $L_k/\mathbb{F}_p$.

Enfin, on rappelle que Ballet et Chaumine ont établi dans [BC04] que le genre chaque étage L_k des tours $\mathcal{T}_5/\mathbb{F}_{p^2}$ et $\mathcal{T}_5/\mathbb{F}_p$ est donné par la formule suivante :

$$g(L_k) = \begin{cases} 2^{k+1} - 3 \cdot 2^{\frac{k}{2}} + 1 & \text{si } k \equiv 0 \pmod 2, \\ 2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}} + 1 & \text{si } k \equiv 1 \pmod 2. \end{cases} \tag{3.2}$$

et que l'on a les bornes suivantes pour le nombre de places rationnelles dans L_k sur $\mathbb{F}_{p^2}$ et pour le nombre de places de degré un et deux sur $\mathbb{F}_p$:

$$B_1(L_k/\mathbb{F}_{p^2}) \geq 2^{k+1}(p-1) \tag{3.3}$$

et

$$B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p) \geq 2^{k+1}(p-1). \tag{3.4}$$

3.2 Résultats techniques utiles

On établit ici des bornes concernant le genre et le nombre de places (rationnelles, de degré 1 et 2 ou de degré 1, 2 et 4) des tours présentées dans la section précédente et qui seront utiles pour établir l'existence, pour chaque entier n, d'un étage de chacune des tours permettant d'appliquer l'algorithme de type Chudnovsky pour multiplier dans $\mathbb{F}_{q^n}$.

3.2.1 Pour les tours de Garcia-Stichtenoth d'extensions d'Artin-Schreier

Dans cette section, $q = p^r$ où p est un nombre premier et $r \geq 1$ est un entier. On dénotera indifféremment le genre d'un même étage des trois tours $\mathcal{T}_2/\mathbb{F}_{q^2}$, $\mathcal{T}_3/\mathbb{F}_q$ et $\mathcal{T}_4/\mathbb{F}_2$ de la façon suivante :

$$g_{k,s} = g(F_{k,s}/\mathbb{F}_{q^2}) \text{ ou } g(G_{k,s}/\mathbb{F}_q) \text{ ou } g(H_{k,s}/\mathbb{F}_2),$$

en particulier, $g_k := g_{k,0} = g_{k-1,r}$.
On pose

$$\Delta g_{k,s} := g_{k,s+1} - g_{k,s}.$$

Lemme 3.2.1.1. *Si $q \geq 4$, alors on a les bornes suivantes pour le genre des étages des tours $\mathcal{T}_2/\mathbb{F}_{q^2}$, $\mathcal{T}_3/\mathbb{F}_q$ et $\mathcal{T}_4/\mathbb{F}_2$ (dans ce dernier cas, on convient que $q = 4$ et $p = r = 2$) :*

i) $g_k > q^k$ *pour tout* $k \geq 4$,
de plus, pour la tour $\mathcal{T}_4/\mathbb{F}_2$, *on a aussi* $g_k > pq^{k-1}$ *pour tout* $k \geq 3$,

ii) $g_k \leq q^{k-1}(q+1) - \sqrt{q}q^{\frac{k}{2}}$,

iii) $g_{k,s} \leq q^{k-1}(q+1)p^s$ *pour tous* $k \geq 1$ *et* $s \in \{0, \ldots, r\}$,

iv) $g_{k,s} \leq \frac{q^k(q+1) - q^{\frac{k}{2}}(q-1)}{p^{r-s}}$ *pour tous* $k \geq 2$ *et* $s \in \{0, \ldots, r\}$.

Preuve.

i) D'après la formule (3.1) du genre des tours rappelée à la section 3.1.1, on sait que si $k \equiv 1 \pmod 2$, alors

$$g_k = q^k + q^{k-1} - q^{\frac{k+1}{2}} - 2q^{\frac{k-1}{2}} + 1 = q^k + q^{\frac{k-1}{2}}(q^{\frac{k-1}{2}} - q - 2) + 1.$$

Comme $q > 3$ et $k \geq 4$, on a $q^{\frac{k-1}{2}} - q - 2 > 0$, d'où $g_k > q^k$.
Sinon, $k \equiv 0 \pmod 2$, et donc

$$g_k = q^k + q^{k-1} - \frac{1}{2}q^{\frac{k}{2}+1} - \frac{3}{2}q^{\frac{k}{2}} - q^{\frac{k}{2}-1} + 1 = q^k + q^{\frac{k}{2}-1}(q^{\frac{k}{2}} - \frac{1}{2}q^2 - \frac{3}{2}q - 1) + 1.$$

Comme $q > 4$ et $k \geq 4$, on a $q^{\frac{k}{2}} - \frac{1}{2}q^2 - \frac{3}{2}q - 1 > 0$, d'où $g_k > q^k$.
Quant à la seconde borne pour g_k dans le cas de la tour $\mathcal{T}_4/\mathbb{F}_2$, notons qu'elle est déjà établie pour tout $k \geq 4$, car alors $g_k > q^k \geq pq^{k-1}$. Pour $k = 3$, il suffit de constater que $g_3 - pq^2 = q^3 - 2q + 1 - pq^2 = 25 > 0$.

ii) C'est une conséquence directe de la formule (3.1) car pour tout $k \geq 1$, on a $2q^{\frac{k-1}{2}} \geq 1$ ce qui permet de conclure si k est impair, et $\frac{3}{2}q^{\frac{k}{2}} + q^{\frac{k}{2}-1} \geq 1$ d'où le résultat pour les k pairs puisque $\frac{1}{2}q \geq \sqrt{q}$.

iii) Si $s = r$, alors d'après la formule (3.1), on a

$$g_{k,s} = g_{k+1} \leq q^{k+1} + q^k = q^{k-1}(q+1)p^s.$$

Sinon, $s < r$ et les propositions 3.1.1.1 et 3.1.1.3 donnent $g_{k,s} \leq \frac{g_{k+1}}{p^{r-s}} + 1$. De plus, comme $q^{\frac{k+2}{2}} \geq q$ et $\frac{1}{2}q^{\frac{k+1}{2}+1} \geq q$, on obtient $g_{k+1} \leq q^{k+1} + q^k - q + 1$ d'après la formule (3.1). Ainsi, on obtient

$$\begin{aligned} g_{k,s} &\leq \frac{q^{k+1} + q^k - q + 1}{p^{r-s}} + 1 \\ &= q^{k-1}(q+1)p^s - p^s + p^{s-r} + 1 \\ &\leq q^{k-1}(q+1)p^s + p^{s-r} \\ &\leq q^{k-1}(q+1)p^s \ \text{ car } 0 \leq p^{s-r} < 1 \text{ et } g_{k,s} \in \mathbb{N}. \end{aligned}$$

iv) Les propositions 3.1.1.1 et 3.1.1.3 donnent $g_{k,s} \leq \frac{g_{k+1}}{p^{r-s}} + 1$, donc d'après ii) on a $g_{k,s} \leq \frac{q^k(q+1) - \sqrt{q}q^{\frac{k+1}{2}}}{p^{r-s}} + 1$ d'où le résultat car $p^{r-s} \leq q^{\frac{k}{2}}$ pour tout $k \geq 2$.

□

Le cas particulier de la tour $\mathcal{T}_4/\mathbb{F}_2$

Dans ce paragraphe, on fixe $q = p^2 = 4$. Cependant, pour plus de clarté, on conserve les variables p et q dans les énoncés et les démonstrations.

Lemme 3.2.1.2. *Pour tous $k \geq 1$ et $s \in \{0, 1\}$, on définit $D_{k,s} := p^{s+1}q^{k-1}$. On a alors*

i) $\Delta g_{k,s} := g_{k,s+1} - g_{k,s} \geq D_{k,s}$,

ii) $B_1(H_{k,s}/\mathbb{F}_p) + 2B_2(H_{k,s}/\mathbb{F}_p) + 4B_4(H_{k,s}/\mathbb{F}_p) > 2D_{k,s}$.

Preuve.

i) D'après la formule du genre de Hurwitz [Sti08, Theorem 3.4.13], on a $g_{k,s+1} - 1 \geq p(g_{k,s} - 1)$ pour tous entiers $k \geq 1$ et $s = 0, 1$, donc $g_{k,s+1} - g_{k,s} \geq (p-1)(g_{k,s} - 1)$. En appliquant s fois successives la formule du genre de Hurwitz, on obtient $g_{k,s+1} - g_{k,s} \geq (p-1)p^s(g_k - 1)$. Ainsi, pour $k \geq 3$ on a $g_{k,s+1} - g_{k,s} \geq (p-1)p^{s+1}q^{k-1}$ car $g_k > pq^{k-1}$ d'après le lemme 3.2.1.1 i). De plus, pour $k = 1$ ou 2, on calcule avec KASH [DFK+97] les genres des étages de la tour : $g_1 = 0$, $g_{1,1} = 2$, $g_2 = 6$, $g_{2,1} = 23$ et $g_3 = 57$. On vérifie alors que le résultat est toujours valable dans ces cas.

ii) C'est évident car $q^2 - 1 > p^2$ et d'après la proposition 3.1.1.3 on a $B_1(H_{k,s}/\mathbb{F}_2) + 2B_2(H_{k,s}/\mathbb{F}_2) + 4B_4(H_{k,s}/\mathbb{F}_2) \geq (q^2-1)q^{k-1}p^s$.

□

Lemme 3.2.1.3. *Pour tous $k \geq 1$ et $s \in \{0, 1, 2\}$, on a*

$$\sup\Big\{n \in \mathbb{N} \;\Big|\; \sum_{i=1,2,4} iB_i(H_{k,s}/\mathbb{F}_2) \geq 2n + 2g_{k,s} + 7\Big\} \geq \frac{5}{2}q^{k-1} - \frac{7}{2}.$$

Preuve. D'après la proposition 3.1.1.3 et le lemme 3.2.1.1 iii), on a

$$\begin{aligned}\sum_{i=1,2,4} iB_i(H_{k,s}/\mathbb{F}_2) - 2g_{k,s} - 7 &\geq (q^2-1)q^{k-1}p^s - 2q^{k-1}(q+1)p^s - 7 \\ &= p^s q^{k-1}(q+1)(q-3) - 7.\end{aligned}$$

Ainsi

$$\sup\Big\{n \in \mathbb{N} \;\Big|\; \sum_{i=1,2,4} iB_i(H_{k,s}/\mathbb{F}_2) \geq 2n + 2g_{k,s} + 7\Big\} \geq \frac{1}{2}p^s q^{k-1}(q+1)(q-3) - \frac{7}{2}$$

et on obtient le résultat car $q = 4$ et $s \geq 0$. □

Lemme 3.2.1.4. *Pour tous $k \geq 1$ et $s \in \{0, 1, 2\}$, on a*

$$\sup\Big\{n \in \mathbb{N} \;\Big|\; \sum_{i=1,2,4} iB_i(H_{k,s}/\mathbb{F}_2) \geq 2n + g_{k,s} + 5\Big\} \geq 5p^s q^{k-1} - \frac{5}{2}.$$

Preuve. D'après la proposition 3.1.1.3 et le lemme 3.2.1.1 iii), on a

$$\begin{aligned}\sum_{i=1,2,4} iB_i(H_{k,s}/\mathbb{F}_2) - g_{k,s} - 5 &\geq (q^2-1)q^{k-1}p^s - q^{k-1}(q+1)p^s - 5 \\ &= p^s q^{k-1}(q+1)(q-2) - 5\end{aligned}$$

d'où le résultat puisque $q = 4$. □

Lemme 3.2.1.5. *Pour tout entier $n \geq 2$ il existe un étage $H_{k,s}/\mathbb{F}_2$ de la tour $\mathcal{T}_4/\mathbb{F}_2$ pour lequel les deux conditions suivantes sont satisfaites :*

(1) il existe une place de degré n dans $H_{k,s}/\mathbb{F}_2$,

(2) $B_1(H_{k,s}/\mathbb{F}_2) + 2B_2(H_{k,s}/\mathbb{F}_2) + 4B_4(H_{k,s}/\mathbb{F}_2) \geq 2n + 2g_{k,s} + 7$.

De plus, le premier étage pour lequel ces conditions sont vérifiées est le premier étage pour lequel la condition (2) est vérifiée.

Preuve. Fixons un entier $n \geq 28$. On commence par montrer que pour tout entier k tel que $2 \leq k \leq \frac{1}{4}(n-12)$, on a $2g_{k,s} + 1 \leq p^{\frac{n-1}{2}}(p^{\frac{1}{2}} - 1)$ pour tout $s \in \{0,1,2\}$, et donc la condition (1) est vérifiée d'après le lemme 1.1.5.12. En effet, pour un tel entier k, on a $6 \leq \frac{n}{2} - 2k$ i.e. $p^6 \leq p^{\frac{n}{2}-2k}$. Comme $5p^{\frac{7}{2}} \leq p^6$, on obtient $5p^{\frac{7}{2}} \leq p^{\frac{n}{2}-2k}$ ou de façon équivalente $5p^{2k+1} \leq p^{\frac{n-1}{2}-2}$, ce qui donne $5p^{2k+1} \leq p^{\frac{n-1}{2}}(p^{\frac{1}{2}} - 1)$. On conclut en montrant que $2g_{k,s} + 1 \leq 5p^{2k+1}$: en effet, d'après le lemme 3.2.1.1 iv), comme $k \geq 2$, pour tout $s \in \{0,1,2\}$, on a

$$\begin{aligned}
2g_{k,s} + 1 &\leq 2\frac{q^k(q+1) - q^{\frac{k}{2}}(q-1)}{p^{2-s}} + 1 \\
&= 2\left(q^{k-1}(q+1) - q^{\frac{k}{2}}\frac{q-1}{q}\right)p^s + 1 \\
&= 2q^{k-1}(q+1)p^s - 2q^{\frac{k}{2}}\frac{q-1}{q}p^s + 1 \\
&\leq 2q^{k-1}(q+1)p^s \quad \text{car } 2q^{\frac{k}{2}}\frac{q-1}{q}p^s \geq 1 \\
&= 2p^{2(k-1)}(p^2+1)p^s \\
&= 5p^{2k-1}p^s \quad \text{car } p = 2
\end{aligned}$$

d'où le résultat puisque $p^s \leq p^2$.
On prouve maintenant que pour $k \geq \frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right)$, la condition (2) est satisfaite. En effet, pour un tel entier k, on a $2n + 6 \leq \frac{5}{4}p^{2k}$, donc $2n + 6 \leq \frac{5}{4}p^{2k}p^s$ pour tout $s \in \{0,1,2\}$. Comme $p = 2$, on a $\frac{5}{4}p^{2k}p^s = \left(p^4 - 1 - p(p^2+1)\right)p^{2k-2}p^s$, d'où

$$2n + p^{2k-1}(p^2+1)p^s + 6 \leq (p^4-1)p^{2k-2}p^s. \tag{3.5}$$

Rappelons que l'on a obtenu plus haut $2g_{k,s} + 1 \leq p^{2k-1}(p^2+1)p^s$, donc $2n + 2g_{k,s} + 7 \leq 2n + p^{2k-1}(p^2+1)p^s + 6$ et l'inégalité (3.5) donne le résultat puisque l'on sait que $B_1(H_{k,s}/\mathbb{F}_p) + 2B_2(H_{k,s}/\mathbb{F}_p) + 4B_4(H_{k,s}/\mathbb{F}_p) \geq (q^2-1)q^{k-1}p^s$ d'après la proposition 3.1.1.3.
Finalement, on a montré que pour tous entiers $n \geq 28$ et $k \geq 2$ tels que $\frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right) \leq k \leq \frac{1}{4}(n-12)$, les conditions (1) et (2) sont vérifiées simultanément. Notons que pour tout $n \geq 28$, on a $\frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right) > 2$. De plus, l'intervalle $\left[\frac{1}{2}\log_p\left(\frac{4}{5}(2n+6)\right); \frac{1}{4}(n-12)\right]$ est de longueur supérieure à 1 dès que $n \geq 28$, et cet intervalle *grossit* avec n. Ainsi, pour tout entier $n \geq 28$, on sait qu'il existe un entier $k > 2$ dans cet intervalle et donc qu'il existe un étage de la tour correspondant $H_{k,s}$. De plus, cet étage $H_{k,s}$ (qui est celui tel que le couple d'entier (k,s) est minimal) pour lequel les deux conditions (1) et (2) sont vérifiées, est le premier étage pour

lequel la condition (2) est vérifiée, car pour tout entier $k \leq \frac{1}{4}(n-12)$ il existe une place de degré n dans $H_{k,s}/\mathbb{F}_2$. Enfin, on termine la preuve en calculant, pour les premiers étages de la tour, le nombre de places de degré un, deux, quatre et n pour $n < 28$. On utilise à cette fin le package KASH [DFK+97], et on obtient les résultats suivants :

- $g(H_1/\mathbb{F}_2) = 0$, $N_1(H_1/\mathbb{F}_2) = 3$, $N_2(H_1/\mathbb{F}_2) = 1$ et $N_4(H_1/\mathbb{F}_2) = 3$. La condition (2) est donc satisfaite pour tout $n \leq 5$; de plus, on vérifie que $N_3(H_1/\mathbb{F}_2) > 0$ et $N_5(H_1/\mathbb{F}_2) > 0$. Ainsi, pour tout entier $n \leq 5$, le premier étage qui vérifie simultanément les deux conditions (1) et (2) est $H_1/\mathbb{F}_2$.
- $g(H_{1,1}/\mathbb{F}_2) = 2$, $N_1(H_{1,1}/\mathbb{F}_2) = 3$, $N_2(H_{1,1}/\mathbb{F}_2) = 1$ et $N_4(H_{1,1}/\mathbb{F}_2) = 7$. La condition (2) est donc satisfaite pour tout $n \leq 11$; de plus, on vérifie que $N_i(H_{1,1}/\mathbb{F}_2) > 0$ pour tous les entiers $i \in \{6, \ldots, 11\}$. Ainsi, pour tout entier $n \in \{6, \ldots, 11\}$, le premier étage qui vérifie simultanément les deux conditions (1) et (2) est $H_{1,1}/\mathbb{F}_2$.
- $g(H_2/\mathbb{F}_2) = 6$, $N_1(H_2/\mathbb{F}_2) = 3$, $N_2(H_2/\mathbb{F}_2) = 1$ et $N_4(H_2/\mathbb{F}_2) = 15$. Ainsi, la condition (2) est satisfaite pour tout $n \leq 23$; de plus, on sait que $N_i(H_2/\mathbb{F}_2) > 0$ pour tout entier $i \in \{12, \ldots, 23\}$ puisque dans ce cas, on a $2g(H_2/\mathbb{F}_2) + 1 \leq 2^{\frac{i-1}{2}}(\sqrt{2}-1)$. En effet, $2g(H_2/\mathbb{F}_2) + 1 = 13$ et $2^{\frac{i-1}{2}}(\sqrt{2}-1) \geq 2^{\frac{12-1}{2}}(\sqrt{2}-1) \geq 18$ pour tout entier $i \in \{12, \ldots, 23\}$. Ainsi, pour tout entier $n \in \{12, \ldots, 23\}$, le premier étage qui vérifie simultanément les deux conditions (1) et (2) est $H_2/\mathbb{F}_2$.
- $g(H_{2,1}/\mathbb{F}_2) = 23$, $N_1(H_{2,1}/\mathbb{F}_2) = 4$, $N_2(H_{2,1}/\mathbb{F}_2) = 1$ et $N_4(H_{2,1}/\mathbb{F}_2) = 28$. Ainsi, la condition (2) est satisfaite pour tout $n \leq 32$; de plus, on sait que $N_i(H_2/\mathbb{F}_2) > 0$ pour tout entier $i \in \{24, \ldots, 27\}$ puisque dans ce cas, on a $2g(H_{2,1}/\mathbb{F}_2) + 1 \leq 2^{\frac{n-1}{2}}(\sqrt{2}-1)$. En effet, $2g(H_{2,1}/\mathbb{F}_2) + 1 = 47$ et $2^{\frac{i-1}{2}}(\sqrt{2}-1) \geq 2^{\frac{24-1}{2}}(\sqrt{2}-1) \geq 1199$ pour tout entier $i \in \{24, \ldots, 27\}$. Ainsi, pour tout entier $n \in \{24, \ldots, 27\}$, le premier étage qui vérifie simultanément les deux conditions (1) et (2) est $H_{2,1}/\mathbb{F}_2$.

Remarquons que là encore, c'est la condition (2) qui oblige à utiliser l'étage $(k, s+1)$ au lieu de l'étage (k, s), car elle n'est pas satisfaite dans ce dernier étage. □

Le cas des tours $\mathcal{T}_2/\mathbb{F}_{q^2}$ et $\mathcal{T}_3/\mathbb{F}_q$

Dans cette section, on suppose que $q := p^r \geq 4$ où est p un nombre premier quelconque. Pour tous $k \geq 1$ et $s \in \{0, \ldots, r\}$, on note

$$M_{k,s} := B_1(F_{k,s}/\mathbb{F}_{q^2}) = B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q).$$

Lemme 3.2.1.6. *Soit $D_{k,s} := (p-1)p^s q^k$. On a*

i) $\Delta g_{k,s} \geq D_{k,s}$,

ii) $M_{k,s} \geq D_{k,s}$.

Preuve.

i) D'après la formule du genre de Hurwitz [Sti08, Theorem 3.4.13], on a $g_{k,s+1} - 1 \geq p(g_{k,s} - 1)$, donc $g_{k,s+1} - g_{k,s} \geq (p-1)(g_{k,s} - 1)$. En appliquant s

fois successives la formule du genre de Hurwitz, on obtient $g_{k,s+1} - g_{k,s} \geq (p-1)p^s\big(g(G_k)-1\big)$. Ainsi, $g_{k,s+1} - g_{k,s} \geq (p-1)p^s q^k$, pour tout $k \geq 4$ d'après le lemme 3.2.1.1 i). Les cas $k = 1, 2, 3$ sont traités au cas par cas (pour les petites valeurs de q), avec les valeurs obtenues avec KASH [DFK+97] et regroupées dans la table de la preuve du lemme 3.2.1.10.

ii) D'après la proposition 3.1.1.1, on a

$$\begin{aligned} M_{k,s} &\geq (q^2-1)q^{k-1}p^s \\ &= (q+1)(q-1)q^{k-1}p^s \\ &\geq (q-1)q^k p^s \\ &\geq (p-1)q^k p^s. \end{aligned}$$

□

Lemme 3.2.1.7. *Pour tous $k \geq 1$ et $s \in \{0, \ldots, r\}$, on a*

$$\sup\left\{n \in \mathbb{N} \;\middle|\; M_{k,s} \geq 2n + 2g_{k,s} - 1\right\} \geq \frac{1}{2}(q+1)q^{k-1}p^s(q-3).$$

Preuve. D'après la proposition 3.1.1.1 et le lemme 3.2.1.1 iii), on a

$$\begin{aligned} M_{k,s} - 2g_{k,s} + 1 &\geq (q^2-1)q^{k-1}p^s - 2q^{k-1}(q+1)p^s + 1 \\ &= (q+1)q^{k-1}p^s\big((q-1)-2\big) + 1 \\ &\geq (q+1)q^{k-1}p^s(q-3) \end{aligned}$$

d'où $\sup\left\{n \in \mathbb{N} \mid M_{k,s} \geq 2n + 2g_{k,s} - 1\right\} \geq \frac{1}{2}(q+1)q^{k-1}p^s(q-3)$. □

Lemme 3.2.1.8. *Pour tous $k \geq 1$ et $s \in \{0, \ldots, r\}$, on a*

$$\sup\left\{n \in \mathbb{N} \;\middle|\; M_{k,s} \geq 2n + g_{k,s} - 1\right\} \geq \frac{1}{2}(q+1)q^{k-1}p^s(q-2).$$

Preuve. D'après la proposition 3.1.1.1 et le lemme 3.2.1.1 iii), on a

$$\begin{aligned} M_{k,s} - g_{k,s} + 1 &\geq (q^2-1)q^{k-1}p^s - q^{k-1}(q+1)p^s + 1 \\ &= (q+1)q^{k-1}p^s\big((q-1)-1\big) + 1 \\ &\geq (q+1)q^{k-1}p^s(q-2). \end{aligned}$$

□

Les deux prochains lemmes établissent l'existence d'un étage pour chacune des deux tours qui soit optimal pour l'algorithme de type Chudnovsky.

Lemme 3.2.1.9. *Si $n \geq \frac{1}{2}\left(q^2 + 1 + \epsilon(q^2)\right)$, alors il existe un étage $F_{k,s}/\mathbb{F}_{q^2}$ de la tour $\mathcal{T}_2/\mathbb{F}_{q^2}$ pour lequel les trois conditions suivantes sont satisfaites :*

(1) il existe un diviseur non-spécial de degré $g_{k,s} - 1$ dans $F_{k,s}/\mathbb{F}_{q^2}$,

(2) il existe une place de degré n dans $F_{k,s}/\mathbb{F}_{q^2}$,

(3) $B_1(F_{k,s}/\mathbb{F}_{q^2}) \geq 2n + 2g_{k,s} - 1$.

De plus, le premier étage pour lequel ces trois conditions sont vérifiées simultanément est le premier étage pour lequel la condition (3) est vérifiée.

Preuve. Notons que $n \geq 9$ car $q \geq 4$ et $n \geq \frac{1}{2}(q^2+1) \geq 8.5$. On fixe $1 \leq k \leq n-4$ et $s \in \{0, \ldots, r\}$. On commence par démontrer que dans ce cas, la condition (2) est vérifiée. Le lemme 3.2.1.1 iv) donne :

$$\begin{aligned} 2g_{k,s}+1 &\leq 2\frac{q^k(q+1) - q^{\frac{k}{2}}(q-1)}{p^{r-s}} + 1 \\ &= 2p^s\left(q^{k-1}(q+1) - q^{\frac{k}{2}}\frac{q-1}{q}\right) + 1 \\ &\leq 2q^{k-1}p^s(q+1) \quad \text{car } 2p^s q^{\frac{k}{2}}\frac{q-1}{q} \geq 1 \qquad (3.6) \\ &\leq 2q^k(q^2-1). \end{aligned}$$

D'autre part, $n-1 \geq k+3 > k+\frac{1}{2}+2$ donc $n-1 \geq \log_q(q^k) + \log_q(2) + \log_q(q+1)$. Cela implique que $q^{n-1} \geq 2q^k(q+1)$, et donc $q^{n-1}(q-1) \geq 2q^k(q^2-1)$. Ainsi, on a $2g_{k,s}+1 \leq q^{n-1}(q-1)$ ce qui assure que la condition (2) est vérifiée d'après le lemme 1.1.5.12. On suppose désormais de plus que $k \geq \log_q\left(\frac{2n}{5}\right)+1$. Remarquons que pour tout $n \geq 9$, il existe bien un tel entier k puisque la taille de l'intervalle $[\log_q\left(\frac{2n}{5}\right)+1, n-4]$ est supérieure à $9-4-\log_4\left(\frac{2\cdot 9}{5}\right)-1 \geq 3 > 1$. De plus, un tel entier k vérifie $q^{k-1} \geq \frac{2}{5}n$, donc $n \leq \frac{1}{2}q^{k-1}(q+1)(q-3)$ car $q \geq 4$. On a alors

$$\begin{aligned} 2n+2g_{k,s}-1 &\leq 2n+2g_{k,s}+1 \\ &\leq 2n+2q^{k-1}p^s(q+1) \quad \text{d'après (3.6)} \\ &\leq q^{k-1}(q+1)(q-3) + 2q^{k-1}p^s(q+1) \\ &\leq q^{k-1}p^s(q+1)(q-1) \\ &= (q^2-1)q^{k-1}p^s \end{aligned}$$

ce qui implique que $B_1(F_{k,s}/\mathbb{F}_{q^2}) \geq 2n+2g_{k,s}-1$ d'après la proposition 3.1.1.1. Ainsi, pour tout entier $k \in [\log_q\left(\frac{2n}{5}\right)+1, n-4]$, les conditions (2) and (3) sont simultanément satisfaites et c'est le cas dès que l'entier k satisfait la condition (3). Pour conclure, remarquons que pour les entiers k qui satisfont ces deux conditions, la condition (1) est aussi satisfaite d'après le théorème 1.3.1.4 qui s'applique puisque $q \geq 4$ et $g_{k,s} \geq g_2 \geq 6$ d'après la formule (3.1). □

Lemme 3.2.1.10. *Si $n \geq \frac{1}{2}(q+1+\epsilon(q))$, alors il existe un étage $G_{k,s}/\mathbb{F}_q$ de la tour $\mathcal{T}_3/\mathbb{F}_q$ pour lequel les trois conditions suivantes sont satisfaites :*

(1) il existe un diviseur non-spécial de degré $g_{k,s}-1$ dans $G_{k,s}/\mathbb{F}_q$,

(2) il existe une place de degré n dans $G_{k,s}/\mathbb{F}_q$,

(3) $B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q) \geq 2n + 2g_{k,s} - 1$.

De plus, le premier étage pour lequel ces trois conditions sont vérifiées simultanément est le premier étage pour lequel la condition (3) est vérifiée.

Preuve. Notons que $n \geq 5$ car $q \geq 4$, $\epsilon(q) \geq \epsilon(4) = 4$, d'où $n \geq \frac{1}{2}(q+1+\epsilon(q)) \geq 4.5$. On considère d'abord le cas où $n \geq 12$. Fixons $1 \leq k \leq \frac{n-5}{2}$ et $s \in \{0, \ldots, r\}$. On a $2p^s q^{k-1} \frac{q+1}{\frac{\sqrt{q}}{2}} \leq q^{\frac{n-1}{2}}$ car

$$\frac{n-1}{2} \geq k+2 = k - \frac{3}{2} + 1 + 1 + \frac{3}{2} \geq \log_q(q^{k-\frac{3}{2}}) + \log_q(4) + \log_q(p^s) + \log_q(q+1).$$

Ainsi, $2p^s q^{k-1}(q+1) \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$ car $\frac{\sqrt{q}}{2} \leq \sqrt{q}-1$ pour $q \geq 4$. D'après l'inégalité (3.6) obtenue dans la preuve précédente, cela prouve que la condition (2) est satisfaite.
Le même raisonnement que dans la preuve précédente montre que la condition (3) est aussi satisfaite dès que $k \geq \log_q\left(\frac{2n}{5}\right) + 1$. De plus, pour $n \geq 12$, l'intervalle $[\log_q\left(\frac{2n}{5}\right)+1, \frac{n-5}{2}]$ contient au moins un entier et le plus petit d'entre eux est le plus petit entier k pour lequel la condition (3) est vérifiée. En outre, pour un tel entier k, le théorème 1.3.1.4 assure que la condition (1) est aussi vérifiée.

Pour finir, on considère les cas où $5 \leq n \leq 11$. Pour toutes les valeurs de n et $q = p^r$ pour lesquelles on a à la fois $n \geq \frac{1}{2}(q+1+\epsilon(q))$ et $5 \leq n \leq 11$, il faut vérifier que les conditions (1), (2) et (3) sont bien vérifiées. On utilise pour cela le package KASH [DFK+97] pour modéliser les premiers étages de la tour $\mathcal{T}_3/\mathbb{F}_q$ et calculer leur genre et leur nombre de places de degré 1 et 2. Ainsi, on détermine le premier étage $G_{k,s}/\mathbb{F}_q$ qui satisfasse simultanément les trois conditions (1), (2) et (3). On résume les résultats obtenus dans la table suivante :

$q = p^r$	2^2	2^3	3^2
$\epsilon(q)$	4	5	6
$\frac{1}{2}(q+1+\epsilon(q))$	4.5	7	8
entiers n à considérer	$5 \leq n \leq 11$	$7 \leq n \leq 11$	$8 \leq n \leq 11$
étages (k,s) correspondants	$(1,1)$	$(1,1)$	$(1,1)$
$B_1(G_{k,s}/\mathbb{F}_q)$	5	9	10
$B_2(G_{k,s}/\mathbb{F}_q)$	14	124	117
$\Gamma(G_{k,s}/\mathbb{F}_q)$	15	117	113
$g_{k,s}$	2	12	9
$2g_{k,s}+1$	5	25	19
$q^{\frac{n-1}{2}}(\sqrt{q}-1) \geq \ldots$	16	936	4374

$q = p^r$	5	7	11	13
$\epsilon(q)$	4	5	6	7
$\frac{1}{2}(q+1+\epsilon(q))$	5	6.5	9	10.5
entiers n à considérer	$5 \leq n \leq 11$	$7 \leq n \leq 11$	$9 \leq n \leq 11$	$n = 11$
étages (k,s) correspondants	$(2,0)$	$(2,0)$	$(2,0)$	$(2,0)$
$N_1(G_{k,s}/\mathbb{F}_q)$	6	8	12	14
$N_2(G_{k,s}/\mathbb{F}_q)$	60	168	660	1092
$\Gamma(G_{k,s}/\mathbb{F}_q)$	53	151.5	611.5	1021.5
$g_{k,s}$	10	21	55	78
$2g_{k,s}+1$	21	43	11	157
$q^{\frac{n-1}{2}}(\sqrt{q}-1) \geq \ldots$	30	564	33917	967422

Dans cette table, on peut vérifier que pour chaque valeur de q et de n à considérer et tout étage $G_{k,s}/\mathbb{F}_q$ correspondant, on a simultanément :

- $g_{k,s} \geq 2$, donc la condition (1) est vérifiée d'après le théorème 1.3.1.4,
- $2g_{k,s}+1 \leq q^{\frac{n-1}{2}}(\sqrt{q}-1)$, donc la condition (2) est vérifiée,
- $\Gamma(G_{k,s}/\mathbb{F}_q) := \frac{1}{2}\big(B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q) - 2g_{k,s}+1\big) \geq n$ donc la condition (3) est vérifiée.

□

3.2.2 Pour les tours de Garcia-Stichtenoth d'extensions de Kummer

Dans toute cette section, $p \geq 3$ est un nombre premier et on note g_k le genre de l'étage L_k dans les tours $\mathcal{T}_5/\mathbb{F}_{p^2}$ et $\mathcal{T}_5/\mathbb{F}_p$. De plus, on pose

$$M_k := B_1(L_k/\mathbb{F}_{p^2}) = B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p).$$

Le lemme suivant est une conséquence directe de la formule (3.2) :

Lemme 3.2.2.1. *Le genre des étages des tours $\mathcal{T}_5/\mathbb{F}_{p^2}$ et $\mathcal{T}_5/\mathbb{F}_p$ vérifient pour tout $k \geq 0$:*

i) $g_k \leq 2^{k+1} - 2\cdot 2^{\frac{k+1}{2}} + 1$,

ii) $g_k \leq 2^{k+1}$.

Lemme 3.2.2.2. *Pour tout $k \geq 0$, on pose $\Delta g_k := g_{k+1} - g_k$. Alors on a $M_k \geq \Delta g_k \geq 2^{k+1} - 2^{\frac{k+1}{2}}$.*

Preuve. Si k est pair, alors $\Delta g_k = 2^{k+1} - 2^{\frac{k}{2}}$, sinon $\Delta g_k = 2^{k+1} - 2^{\frac{k+1}{2}}$ donc la seconde inégalité est clairement vérifiée. De plus, comme $p \geq 3$, la première inégalité découle des bornes (3.3) et (3.4) qui donnent $M_k \geq 2^{k+2}$. □

Lemme 3.2.2.3. *Pour tout $k \geq 0$, on a*

$$\sup\Big\{n \in \mathbb{N} \;\Big|\; M_k \geq 2n + 2g_k - 1\Big\} \geq 2^k(p-3) + 2.$$

Preuve. D'après les bornes (3.3) et (3.4) pour M_k et le lemme 3.2.2.1 ii), on obtient

$$\begin{aligned} M_k - 2g_k + 1 &\geq 2^{k+1}(p-1) - 2(2^{k+1} - 2\cdot 2^{\frac{k+1}{2}} + 1) + 1 \\ &= 2^{k+1}(p-3) + 4\cdot 2^{\frac{k+1}{2}} - 1 \\ &\geq 2^{k+1}(p-3) + 4 \text{ car } k \geq 0. \end{aligned}$$

□

Lemme 3.2.2.4. *Pour tout $k \geq 0$, on a*

$$\sup\Big\{n \in \mathbb{N} \;\Big|\; M_k \geq 2n + g_k - 1\Big\} \geq 2^k(p-2) + 2^{\frac{k+1}{2}}, \textit{ si } p > 5$$

et

$$\sup\Big\{n \in \mathbb{N} \;\Big|\; M_k \geq 2n + g_k + 2\Big\} \geq 2^k(p-2) + 2^{\frac{k+1}{2}} - 1, \textit{ si } p = 3 \textit{ ou } 5.$$

Preuve. D'après les bornes (3.3) et (3.4) pour M_k et le lemme 3.2.2.1 i), on obtient

$$\begin{aligned} M_k - g_k + 1 &\geq 2^{k+1}(p-1) - (2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}} + 1) + 1 \\ &= 2^{k+1}(p-2) + 2 \cdot 2^{\frac{k+1}{2}} \end{aligned}$$

De même, on a

$$\begin{aligned} M_k - g_k - 2 &\geq 2^{k+1}(p-1) - (2^{k+1} - 2 \cdot 2^{\frac{k+1}{2}} + 1) - 2 \\ &= 2^{k+1}(p-2) + 2 \cdot 2^{\frac{k+1}{2}} - 3 \end{aligned}$$

ce qui donne le résultat si $p = 3$ ou 5. □

On peut maintenant établir l'existence d'un étage de chacune de ces tours qui convienne pour appliquer l'algorithme de type Chudnovsky.

Lemme 3.2.2.5. *Si $p \geq 5$ et $n \geq \frac{1}{2}\left(p^2 + 1 + \epsilon(p^2)\right)$, alors il existe un étage $L_k/\mathbb{F}_{p^2}$ de la tour $\mathcal{T}_5/\mathbb{F}_{p^2}$ pour lequel les trois conditions suivantes sont satisfaites :*

(1) il existe un diviseur non-spécial de degré $g_k - 1$ dans $L_k/\mathbb{F}_{p^2}$,

(2) il existe une place de degré n dans $L_k/\mathbb{F}_{p^2}$,

(3) $B_1(L_k/\mathbb{F}_{p^2}) \geq 2n + 2g_k - 1$.

De plus, le premier étage pour lequel ces trois conditions sont vérifiées simultanément est le premier étage pour lequel la condition (3) est vérifiée.

Preuve. Fixons $n \geq \frac{1}{2}(5^2 + 1 + \epsilon(5^2)) = 18$. On commence par prouver que pour tout entier k tel que $2 \leq k \leq n-2$, on a $2g_k + 1 \leq p^{n-1}(p-1)$, et donc la condition (2) est vérifiée d'après le lemme 1.1.5.12. En effet, pour un tel entier k, comme $p \geq 5$ on a $k \leq \log_2(p^{n-2}) \leq \log_2(p^{n-1} - 1)$, donc $k + 2 \leq \log_2\left(4(p^{n-1} - 1)\right)$, d'où $2^{k+2} + 1 \leq 4p^{n-1}$ car $\log_2\left(4(p^{n-1} - 1)\right) \leq \log_2(4p^{n-1} - 1)$. Ainsi, on a $2 \cdot 2^{k+1} + 1 \leq p^{n-1}(p-1)$ car $p \geq 5$, d'où le résultat d'après le lemme 3.2.2.1 ii).
On montre mantenant que pour $k \geq \log_2(2n-1) - 2$, la condition (3) est vérifiée. En effet, pour un tel entier k, on a $k + 2 \geq \log_2(2n-1)$, donc $2^{k+2} \geq 2n - 1$. On a alors $2^{k+3} \geq 2n + 2^{k+2} - 1$ et donc $2^{k+1}(p-1) \geq 2^{k+1} \cdot 4 \geq 2n + 2^{k+2} - 1$ car $p \geq 5$. Ainsi on a $B_1(L_k/\mathbb{F}_{p^2}) \geq 2n + 2g_k - 1$ d'après la borne (3.3) et le lemme 3.2.2.1 ii).
On a donc montré que pour tous entiers $n \geq 18$ et $k \geq 2$ tels que $\log_2(2n-1) - 2 \leq k \leq n-2$, les conditions (2) et (3) sont simultanément satisfaites. De plus, pour tout $n \geq 18$, il existe bien au moins un entier $k \geq 2$ dans l'intervalle $\left[\log_2(2n-1) - 2; n-2\right]$. En effet, $\log_2(2 \cdot 18 - 1) - 2 \simeq 3.12 > 2$ donc la taille de l'intervalle est supérieure à 1 pour $n = 18$ et celle-ci augmente avec n.
Enfin, remarquons que pour un tel entier k, la condition (1) est systématiquement satisfaite d'après le théorème 1.3.1.4 puisque $p^2 \geq 4$ et $g_k \geq g_2 = 3$ d'après la formule (3.2). □

Lemme 3.2.2.6. *Si $p \geq 5$ et $n \geq \frac{1}{2}\left(p + 1 + \epsilon(p)\right)$, alors il existe un étage $L_k/\mathbb{F}_p$ de la tour $\mathcal{T}_5/\mathbb{F}_p$ pour lequel les trois conditions suivantes sont satisfaites :*

(1) il existe un diviseur non-spécial de degré $g_k - 1$ dans $L_k/\mathbb{F}_p$,

(2) il existe une place de degré n dans $L_k/\mathbb{F}_p$,

(3) $B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p) \geq 2n + 2g_k - 1$.

De plus, le premier étage pour lequel ces trois conditions sont vérifiées simultanément est le premier étage pour lequel la condition (3) est vérifiée.

Preuve. Fixons $n \geq \frac{1}{2}(5 + 1 + \epsilon(5)) = 5$. On commence par prouver que pour tout entier k tel que $2 \leq k \leq n-3$, on a $2g_k + 1 \leq p^{\frac{n-1}{2}}(\sqrt{p} - 1)$, et donc la condition (2) est vérifiée d'après le lemme 1.1.5.12. En effet, pour un tel entier k, comme $p \geq 5$ et $n \geq 5$, on a $\log_2(p^{\frac{n-1}{2}} - 1) \geq \log_2(5^{\frac{n-1}{2}} - 1) \geq \log_2(2^{n-1}) = n - 1$. Ainsi $k + 2 \leq n - 1 \leq \log_2(p^{\frac{n-1}{2}} - 1)$ et le lemme 3.2.2.1 ii) implique que $2g_k + 1 \leq 2^{k+2} + 1 \leq p^{\frac{n-1}{2}} \leq p^{\frac{n-1}{2}}(\sqrt{p} - 1)$, d'où le résultat.
Le même raisonnement que dans la preuve précédente montre que la condition (3) est aussi satisfaite dès que $k \geq \log_2(2n-1) - 2$. Ainsi, pour tous entiers $n \geq 5$ et $k \geq 2$ tels que $\log_2(2n-1) - 2 \leq k \leq n - 3$, les conditions (2) et (3) sont satisfaites simultanément. De plus, la taille de l'intervalle $\left[\log_2(2n-1) - 2; n - 3\right]$ augmente avec n, et donc cet intervalle contient toujours, pour tout $n \geq 5$, au moins un entier $k \geq 2$. Enfin, de même que précédemment, la condition (1) est satisfaite pour de tels entiers k grâce au théorème 1.3.1.4. □

Les deux derniers lemmes sont démontrés pour $p \geq 5$. Cependant, en regardant attentivement les démonstrations, on constate que cette hypothèse est nécessaire seulement

- pour obtenir la condition (2) du lemme 3.2.2.5 car pour $p = 3$, il est impossible d'avoir $2^{k+1}(p-1) \geq 2n + 2^{k+2} - 1$,
- pour obtenir la condition (1) du lemme 3.2.2.6, car elle découle du théorème 1.3.1.4, qui nécessite $p \geq 4$.

Ainsi, si l'on affaiblit les conditions à satisfaire, à savoir : demander $2n + g_k - 1$ (ou $2n + g_k + 2$) places rationnelles (ou de degré 1 et 2) au lieu de $2n + 2g_k - 1$, et renoncer à l'existence du diviseur non-spécial de degré $g_k - 1$, alors on peut énoncer le résultat dans le cas où $p = 3$. Plus précisément, on a les résultats suivants :

Lemme 3.2.2.7. *Si $p \geq 3$ et $n \geq \frac{1}{2}\left(p^2 + 1 + \epsilon(p^2)\right)$, alors il existe un étage $L_k/\mathbb{F}_{p^2}$ de la tour $\mathcal{T}_5/\mathbb{F}_{p^2}$ pour lequel les deux conditions suivantes sont satisfaites :*

(1) il existe une place de degré n dans $L_k/\mathbb{F}_{p^2}$,

(2) $B_1(L_k/\mathbb{F}_{p^2}) \geq 2n + g_k - 1$.

De plus, le premier étage pour lequel ces deux conditions sont vérifiées simultanément est le premier étage pour lequel la condition (2) est vérifiée.

Lemme 3.2.2.8. *Si $p \geq 3$ et $n \geq \frac{1}{2}\left(p + 1 + \epsilon(p)\right)$, alors il existe un étage $L_k/\mathbb{F}_p$ de la tour $\mathcal{T}_5/\mathbb{F}_p$ pour lequel les deux conditions suivantes sont satisfaites :*

(1) il existe une place de degré n dans $L_k/\mathbb{F}_p$,

(2) $B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p) \geq 2n + g_k + 2$.

De plus, le premier étage pour lequel ces deux conditions sont vérifiées simultanément est le premier étage pour lequel la condition (2) est vérifiée.

Chapitre 4

Bornes pour la complexité bilinéaire symétrique

4.1 Amélioration des bornes sur $\mathbb{F}_2$

Les résultats de cette section ont fait l'objet d'une publication dans *Journal of Complexity* en collaboration avec S. Ballet [BP11].

En particulier, en spécialisant l'algorithme 2.2.3.1 sur des places de degré un, deux et quatre, et grâce à l'existence de diviseurs ayant de bonnes propriétés, nous obtenons la borne suivante :

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{477}{26}n + \frac{45}{2}$$

qui est actuellement la meilleure borne uniforme connue pour la complexité bilinéaire symétrique sur $\mathbb{F}_2$. De plus, cette borne permet d'établir que l'on peut remplacer la constante $C_2 = 54$ rappelée dans le théorème 2.1.5.4 par

$$C_2 = \frac{4824}{247} \approx 19.6.$$

4.1.1 Algorithme symétrique de type Chudnovsky adapté et rang de tenseur associé

Dans cette section, afin d'établir le résultat précédemment annoncé, on présente une spécialisation de l'algorithme énoncé dans le théorème 2.2.3.1 pour les places de degré un, deux et quatre, avec d'éventuelles évaluations d'ordre 2 (c'est-à-dire avec certains $l_i = 2$). On n'applique pas le théorème 2.2.3.2 car on n'arrive pas à prouver l'existence du diviseur non-spécial de degré $g - 1$ dans ce cas, mais on contourne le problème car on montre que l'existence (établie par le théorème 1.3.2.2) d'un diviseur de degré $g - 5$ suffit.

Proposition 4.1.1.1. *Soient*

- *q une puissance d'un nombre premier et $n \geq 2$ un entier,*
- *$F/\mathbb{F}_q$ un corps de fonctions algébriques,*
- *Q une place de degré n dans $F/\mathbb{F}_q$,*
- *$\mathcal{D}$ un diviseur dans $F/\mathbb{F}_q$,*

- $\mathscr{P} = \{P_1, \ldots, P_{N_1}, P_{N_1+1}, \ldots, P_{N_1+N_2}, P_{N_1+N_2+1}, \ldots, P_{N_1+N_2+N_4}\}$ *un ensemble de* N_1 *places de degré un,* N_2 *places de degré deux et* N_4 *places de degré quatre.*
- *trois entiers* n_1, n_2 *et* n_4 *tels que* $0 \leq n_1 \leq N_1$, $0 \leq n_2 \leq N_2$ *et* $0 \leq n_4 \leq N_4$.

Supposons que Q *et toutes les places de l'ensemble* $\mathscr{P}$ *n'appartiennent pas au support de* $\mathcal{D}$ *et que :*

(a) l'application

$$Ev_Q : \mathcal{L}(\mathcal{D}) \to \mathbb{F}_{q^n} \simeq F_Q$$

est surjective,

(b) l'application

$$\begin{array}{rccl} Ev_{\mathscr{P}} : & \mathcal{L}(2\mathcal{D}) & \to & \mathbb{F}_q^{N_1} \times \mathbb{F}_q^{n_1} \times \mathbb{F}_{q^2}^{N_2} \times \mathbb{F}_{q^2}^{n_2} \times \mathbb{F}_{q^4}^{N_4} \times \mathbb{F}_{q^4}^{n_4} \\ & f & \mapsto & \big(f(P_1), \ldots, f(P_{N_1}), f'(P_1), \ldots, f'(P_{n_1}), f(P_{N_1+1}), \ldots, \\ & & & \quad f(P_{N_1+N_2}), f'(P_{N_1+1}), \ldots, f'(P_{N_1+n_2}), f(P_{N_1+N_2+1}), \\ & & & \quad \ldots, f(P_{N_1+N_2+N_4}), f'(P_{N_1+N_2+1}), \ldots, f'(P_{N_1+N_2+n_4})\big) \end{array}$$

est injective.

Alors

$$\mu_q^{\mathrm{sym}}(n) \leq N_1 + 2n_1 + 3N_2 + 6n_2 + \mu_q^{\mathrm{sym}}(4)\big(N_4 + 2n_4\big).$$

Preuve. On utilise la version de l'algorithme présentée dans le théorème 2.2.3.1 avec $N = N_1 + N_2 + N_4$,

$$\deg P_i = \begin{cases} 1 & \text{pour } i = 1, \ldots, N_1, \\ 2 & \text{pour } i = N_1 + 1, \ldots, N_1 + N_2, \\ 4 & \text{pour } i = N_1 + N_2 + 1, \ldots, N, \end{cases}$$

et

$$l_i = \begin{cases} 2, & \text{si } 1 \leq i \leq n_1, \text{ ou } N_1 + 1 \leq i \leq N_1 + n_2, \\ & \quad \text{ou } N_1 + N_2 + 1 \leq i \leq N_1 + N_2 + n_4, \\ 1, & \text{sinon.} \end{cases}$$

Autrement dit, pour $i = 1, 2, 4$, on effectue N_i évaluations classiques sur des places de degré i et n_i évaluations d'ordre 2. Rappelons que pour tout q puissance d'un premier, on a $\mu_q^{\mathrm{sym}}(2) = 3$ et $\mu_q^{\mathrm{sym}}(1, 2) \leq 3$. La borne (2.6) donne alors

$$\begin{aligned} \mu_q^{\mathrm{sym}}(n) &\leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i) \mu_{q^{\deg P_i}}^{\mathrm{sym}}(1, l_i) \\ &\leq \sum_{i=1}^{n_1} \mu_q^{\mathrm{sym}}(1)\mu_q^{\mathrm{sym}}(1,2) + \sum_{i=n_1+1}^{N_1} \mu_q^{\mathrm{sym}}(1)\mu_q^{\mathrm{sym}}(1,1) + \sum_{i=N_1+1}^{N_1+n_2} \mu_q^{\mathrm{sym}}(2)\mu_{q^2}^{\mathrm{sym}}(1,2) \\ &\quad + \sum_{i=N_1+n_2+1}^{N_1+N_2} \mu_q^{\mathrm{sym}}(2)\mu_{q^2}^{\mathrm{sym}}(1,1) + \sum_{i=N_1+N_2+1}^{N_1+N_2+n_4} \mu_q^{\mathrm{sym}}(4)\mu_{q^4}^{\mathrm{sym}}(1,2) \\ &\quad + \sum_{i=N_1+N_2+n_4+1}^{N} \mu_q^{\mathrm{sym}}(4)\mu_{q^4}^{\mathrm{sym}}(1,1) \\ &\leq 3n_1 + N_1 - n_1 + 9n_2 + 3(N_2 - n_2) + 3\mu_q^{\mathrm{sym}}(4)n_4 + \mu_q^{\mathrm{sym}}(4)(N_4 - n_4) \\ &= N_1 + 2n_1 + 3N_2 + 6n_2 + \mu_q^{\mathrm{sym}}(4)(N_4 + 2n_4). \end{aligned}$$

□

Remarque. Si n_1, n_2 et n_4 sont des entiers tels que l'application $Ev_{\mathscr{P}}$ est injective, alors pour tous autres entiers m_1, m_2 et m_4 tels que $n_1 \leq m_1 \leq N_1$, $n_2 \leq m_2 \leq N_2$ et $n_4 \leq m_4 \leq N_4$, l'injectivité de l'application est encore vérifiée mais on obtient alors une borne moins bonne pour la complexité. Ainsi, on essayera d'utiliser des entiers n_1, n_2, n_4 « optimaux », c'est-à-dire les plus petit entiers possibles qui rendent l'application $Ev_{\mathscr{P}}$ injective. En particulier, si $n_1 = n_2 = n_4 = 0$ est un choix satisfaisant, alors on peut multiplier dans $\mathbb{F}_{q^n}$ en n'utilisant que des évaluations d'ordre 1.

Théorème 4.1.1.2. *Soit q une puissance d'un nombre premier et $n \geq 2$ un entier. Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g avec $B_i(F/\mathbb{F}_q)$ places de degré i. Soient $n_1, n_2, n_4, N_1, N_2, N_4$ des entiers tels que $0 \leq n_i \leq N_i \leq B_i(F/\mathbb{F}_q)$, pour $i = 1, 2, 4$. Si*

(i) il existe une place Q de degré n dans $F/\mathbb{F}_q$,

(ii) $N_1 + n_1 + 2(N_2 + n_2) + 4(N_4 + n_4) \geq 2n + 2g + 7$,

alors

$$\mu_q^{\mathrm{sym}}(n) \leq \frac{\mu_q^{\mathrm{sym}}(4)}{2}\big(n + g + 5\big) + \frac{\mu_q^{\mathrm{sym}}(4)}{4}(n_1 + 2n_2 + 4n_4).$$

En particulier, on a

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{9}{2}\big(n + g + 5\big) + \frac{9}{4}(n_1 + 2n_2 + 4n_4).$$

Preuve. On construit un diviseur $\mathcal{D}$ tel que l'application Ev_Q définie précédemment soit surjective. D'après le théorème 1.3.2.2 rappelé dans le chapitre 1, il existe un diviseur $\mathcal{R}$ de degré $g - 5$ et de dimension nulle. Soit $\mathcal{D}$ un diviseur équivalent à $\mathcal{K} + Q - \mathcal{R}$ (où $\mathcal{K}$ est un diviseur canonique) et tel que la place Q ne soit pas dans le support de $\mathcal{D}$ (on peut effectivement choisir $\mathcal{D}$ de la sorte d'après le lemme 1.1.4.11) ; un tel diviseur $\mathcal{D}$ est donc de degré $n + g + 3$. De plus, par le théorème de Riemann-Roch, on a d'une part $\dim \mathcal{D} \geq n + 4$, et d'autre part $\dim(\mathcal{D} - Q) = 4$ puisque $i(\mathcal{D} - Q) = \dim(\mathcal{K} - \mathcal{D} + Q) = \dim \mathcal{R} = 0$. Ainsi, Ev_Q est surjective, car la dimension de son image vérifie

$$\dim \mathrm{Im}(Ev_Q) = \dim \mathcal{D} - \dim(\mathcal{D} - Q) \geq n.$$

Posons $N := N_1 + n_1 + 2(N_2 + n_2) + 4(N_4 + n_4)$. D'après (ii), on a $N \geq 2n + 2g + 7$ donc, quitte à choisir de entiers N_i et n_i plus petits, on peut supposer que $N = 2n + 2g + 7 + \epsilon$ avec $\epsilon \in \{0, 1, 2, 3\}$. On considère un ensemble de places $\mathscr{P}$ contenant N_1 places de degré un, N_2 places de degré deux et N_4 places de degré quatre. D'après le lemme 1.1.4.11, on peut aussi supposer qu'aucune des places dans $\mathscr{P}$ n'appartient au support de $\mathcal{D}$. Ainsi, on peut appliquer la proposition 4.1.1.1 avec l'ensemble $\mathscr{P}$ en utilisant n_i evaluations d'ordre 2 sur les N_i places degré i, pour $i = 1, 2, 4$. En effet, si l'on note $\mathcal{A}$ le diviseur suivant

$$\mathcal{A} := \sum_{i=1}^{N_1+N_2+N_4} P_i + \sum_{i=1}^{n_1} P_i + \sum_{i=1}^{n_2} P_{N_1+i} + \sum_{i=1}^{n_4} P_{N_1+N_2+i},$$

alors on a $\deg \mathcal{A} = N$, donc $\deg(2\mathcal{D} - \mathcal{A}) < 0$ et $\ker Ev_{\mathcal{P}} = \mathcal{L}(2\mathcal{D} - \mathcal{A})$ est trivial. Ainsi, les deux conditions (a) et (b) de la proposition 4.1.1.1 sont vérifiées et on a :

$$\mu_q^{\mathrm{sym}}(n) \leq N_1 + 2n_1 + 3N_2 + 6n_2 + \mu_q^{\mathrm{sym}}(4)(N_4 + 2n_4).$$

Comme $\mu_q^{\mathrm{sym}}(4) \geq 8$, on a

$$\begin{aligned} \frac{\mu_q^{\mathrm{sym}}(4)}{4}\Big(\sum_{i|4} i(N_i + n_i) + \sum_{i|4} i n_i\Big) &\geq 2N_1 + 4n_1 + 4N_2 + 8n_2 + \mu_q^{\mathrm{sym}}(4)(N_4 + 2n_4) \\ &\geq N_1 + 2n_1 + 3N_2 + 6n_2 + \mu_q^{\mathrm{sym}}(4)(N_4 + 2n_4). \end{aligned}$$

Ainsi, on a

$$\begin{aligned} \mu_q^{\mathrm{sym}}(n) &\leq \frac{\mu_q^{\mathrm{sym}}(4)}{4}\Big(\sum_{i|4} i(N_i + n_i) + \sum_{i|4} i n_i\Big) \\ &\leq \frac{\mu_q^{\mathrm{sym}}(4)}{4} N + \frac{\mu_q^{\mathrm{sym}}(4)}{4} \sum_{i|4} i n_i, \end{aligned}$$

ce qui donne le résultat. Rappelons qu'en particulier, $\mu_2^{\mathrm{sym}}(4) = 9$, d'où la borne pour $\mu_2^{\mathrm{sym}}(n)$. □

Bien que les places de degré 4 ont un coût plus élevé, cela nous permet d'obtenir des améliorations des bornes uniformes de la complexité bilinéaire de $\mathbb{F}_{2^n}$ comme nous allons le voir dans la section suivante.

4.1.2 Rang de tenseur symétrique dans toute extension finie de $\mathbb{F}_2$

Dans cette section, on multiplie dans $\mathbb{F}_{2^n}$ avec l'algorithme présenté dans la section précédente appliqué sur la tour $\mathcal{T}_4/\mathbb{F}_2$. On présente deux résultats : une borne obtenue en utilisant des évaluations d'ordre 2 et une autre n'utilisant que les évaluations « classiques » (d'ordre 1). En effet, bien que la borne obtenue avec des évaluations d'ordre 2 soit meilleure, l'utilisation pratique de telles évaluations peut parfois être plus compliquée. Aussi, on s'intéresse également à l'efficacité de l'algorithme n'utilisant que des évaluations d'ordre 1 : la borne uniforme ainsi obtenue est tout de même meilleure que celles établies jusque-là.

Borne obtenue sans utiliser d'évaluations d'ordre > 1

Dans un premier temps, on applique la borne obtenue dans le théorème 4.1.1.2 sur la tour $\mathcal{T}_4/\mathbb{F}_2$ avec $n_1 = n_2 = n_4 = 0$.

Théorème 4.1.2.1. *Pour tout entier $n \geq 2$, on a*

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{45}{2} n + 85.5.$$

Preuve. Soit $q = p^2 = 4$. On considère la tour $\mathcal{T}_4 = \{H_{l,r}/\mathbb{F}_2\}$ et on pose

$$M_{l,r} := B_1(H_{l,r}/\mathbb{F}_2) + 2B_2(H_{l,r}/\mathbb{F}_2) + 4B_4(H_{l,r}/\mathbb{F}_2).$$

Pour tout entier n, le lemme 3.2.1.5 établit l'existence d'un étage de la tour $\mathcal{T}_4$ sur lequel on peut appliquer le théorème 4.1.1.2. Notons $H_{k,s}/\mathbb{F}_2$ le premier étage de la tour pour lequel les hypothèses du théorème 4.1.1.2 sont satisfaites avec $n_1 = n_2 = n_4 = 0$. D'après le lemme 3.2.1.5, cet étage est déterminé par le plus petit couple d'entiers k et s tels que $2n \leq M_{k,s} - 2g_{k,s} - 7$. En particulier, pour ce couple (k, s), on a $2n > M_{k,s-1} - 2g_{k,s-1} - 7$.
Pour tout entier $k \geq 1$ et tout entier $s = 0, 1, 2$, on a $g_{k,s} \leq q^{k-1}(q+1)p^s$ d'après le lemme 3.2.1.1 (iii). De plus, comme $M_{k,s-1} \geq (q^2-1)q^{k-1}p^{s-1}$ d'après la proposition 3.1.1.3, on obtient $2n > (q^2-2q-3)q^{k-1}p^{s-1} - 7$. Notons que l'on a $q^2 - 2q + 3 = (q+1)(q-3) = q+1$ car $q = 4$, ce qui entraîne que $2np > (q+1)q^{k-1}p^s - 7p \geq g_{k,s} - 7p$ et donc $g_{k,s} \leq 2np + 7p$. Finalement le théorème 4.1.1.2 donne

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{9}{2}\big(n + g_{k,s} + 5\big) \leq \frac{9}{2}n\,(1+2p) + \frac{9}{2}(7p+5)$$

d'où le résultat puisque $p = 2$. □

Borne obtenue avec des évaluations d'ordre 2

Ici, on applique la borne obtenue dans le théorème 4.1.1.2 sur la tour $\mathcal{T}_4/\mathbb{F}_2$ avec un nombre optimal d'évaluations d'ordre 2.

Théorème 4.1.2.2. *Pour tout entier $n \geq 2$, on a*

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{477}{26}n + \frac{45}{2}.$$

Preuve. Pour tout entier n fixé, le lemme 3.2.1.5 établit l'existence d'un étage de la tour $\mathcal{T}_4/\mathbb{F}_2$ sur lequel on peut appliquer le théorème 4.1.1.2 avec uniquement des évaluations d'ordre 1, c'est-à-dire avec $n_1 = n_2 = n_4 = 0$. Pour tout étage $H_{l,r}/\mathbb{F}_2$ de la tour, on pose

$$M_{l,r} := B_1(H_{l,r}/\mathbb{F}_2) + 2B_2(H_{l,r}/\mathbb{F}_2) + 4B_4(H_{l,r}/\mathbb{F}_2)$$

On note $H_{k,s+1}/\mathbb{F}_2$ le premier étage qui satisfait les hypothèses du théorème 4.1.1.2 avec $n_1 = n_2 = n_4 = 0$, c'est-à-dire que (k, s) est le couple d'entiers qui vérifie $M_{k,s+1} \geq 2n + 2g_{k,s+1} + 7$ et $M_{k,s} < 2n + 2g_{k,s} + 7$. On note $n_0^{k,s}$ le plus grand entier tel que $M_{k,s} \geq 2n_0^{k,s} + 2g_{k,s} + 7$ i.e.

$$n_0^{k,s} := \sup\Big\{m \in \mathbb{N} \;\Big|\; M_{k,s} \geq 2m + 2g_{k,s} + 7\Big\}$$

Pour multiplier dans $\mathbb{F}_{2^n}$, on a l'alternative suivante :

a) utiliser l'algorithme sur l'étage $H_{k,s+1}$. Dans ce cas, le théorème 4.1.1.2 appliqué avec $n_1 = n_2 = n_4 = 0$ donne la borne suivante pour la complexité bilinéaire :

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{9}{2}(n + g_{k,s+1} + 5) = \frac{9}{2}(n_0^{k,s} + g_{k,s} + 5) + \frac{9}{2}(n - n_0^{k,s} + \Delta g_{k,s}).$$

Rappelons que $\Delta g_{k,s} := g_{k,s+1} - g_{k,s}$.

b) utiliser l'algorithme sur l'étage $H_{k,s}$ avec, pour $i = 1, 2, 4$, n_i évaluations d'ordre 2 sur les places de degré i, où les entiers n_i satisfont $n_i \leq B_i(H_{k,s}/\mathbb{F}_2)$ et $M_{k,s} + \sum_{i|4} in_i \geq 2n + 2g_{k,s} + 7$. Pour cela, il suffit que la condition

$$\sum_{i|4} in_i \geq 2(n - n_0^{k,s}) \tag{4.1}$$

soit vérifiée avec $\sum_{i|4} in_i \leq \sum_{i|4} iB_i(H_{k,s}/\mathbb{F}_2)$. En effet, d'après la définition de l'entier $n_0^{k,s}$, (4.1) implique que la condition (ii) du théorème 4.1.1.2 est satisfaite, et $\sum_{i|4} in_i \leq \sum_{i|4} iB_i(H_{k,s}/\mathbb{F}_2)$ assure que l'on peut bien choisir les entiers $n_i \leq B_i(H_{k,s}/\mathbb{F}_2)$. Ainsi, le choix optimal (c'est-à-dire les plus petits entiers n_i que l'on puisse choisir pour appliquer l'algorithme) est $\sum_{i|4} in_i = 2(n - n_0^{k,s}) + \epsilon$ où $\epsilon \in \{0, 1, 2\}$. On obtient alors la borne suivante pour la complexité bilinéaire :

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{9}{2}(n+g+5) + \frac{9}{4}\big(2(n-n_0^{k,s}) + \epsilon\big) \leq \frac{9}{2}(n_0^{k,s} + g_{k,s} + 5) + 9(n - n_0^{k,s} + \frac{1}{2}).$$

Ainsi, sous réserve que l'on puisse choisir les entiers n_i comme dans le cas b), si $n - n_0^{k,s} < \Delta g_{k,s}$ alors la borne donnée par le cas b) est meilleure que celle donnée par le cas a). Or remarquons que d'après le lemme 3.2.1.2, si $n - n_0^{k,s} < D_{k,s}$ (où $D_{k,s} := p^{s+1}q^{k-1}$ est fixé comme dans ce dernier lemme) alors on a à la fois $n - n_0^{k,s} < \Delta g_{k,s}$ car $D_{k,s} \leq \Delta g_{k,s}$ mais aussi $\sum_{i|4} iB_i(H_{k,s}/\mathbb{F}_2) > 2D_{k,s} \geq 2(n - n_0^{k,s})$, donc on peut choisir les entiers n_i de sorte que $\sum_{i|4} in_i = 2(n - n_0^{k,s}) + \epsilon$ où $\epsilon \in \{0, 1, 2\}$. Autrement dit, si $n - n_0^{k,s} < D_{k,s}$ alors on peut choisir de procéder comme dans le cas b) et on obtient une meilleure borne pour la complexité bilinéaire.

Pour $x \in \mathbb{R}^+$ tel que $M_{k,s+1} \geq 2[x] + 2g_{k,s+1} + 7$ et $M_{k,s} < 2[x] + 2g_{k,s} + 7$, on définit la fonction $\Phi_{k,s}(x)$ comme suit :

$$\Phi_{k,s}(x) = \begin{cases} 9(x - n_0^{k,s}) + \frac{9}{2}(n_0^{k,s} + g_{k,s} + 6) & \text{si } x - n_0^{k,s} < D_{k,s} \\ \frac{9}{2}(x - n_0^{k,s}) + \frac{9}{2}(n_0^{k,s} + g_{k,s} + 5 + \Delta g_{k,s}) & \text{sinon.} \end{cases}$$

On définit ensuite la fonction Φ pour tout $x \geq 0$ comme le minimum des fonctions $\Phi_{k,s}$ pour lesquelles x est dans le domaine de définition de $\Phi_{k,s}$. Cette fonction est linéaire par morceau, avec deux sortes de morceaux : ceux de pente $\frac{9}{2}$ et ceux de pente 9. De plus, le graphe de Φ est situé en dessous des points de la forme $\big(n_0^{k,s} + D_{k,s}, \Phi(n_0^{k,s} + D_{k,s})\big)$, car ces points sont les sommets du graphe. Posons $X := n_0^{k,s} + D_{k,s}$, alors

$$\Phi(X) \leq \Phi_{k,s}(X) = \frac{9}{2}(X + g_{k,s+1} + 5) = \frac{9}{2}\left(1 + \frac{g_{k,s+1}}{X}\right)X + \frac{45}{2}.$$

D'après les lemmes 3.2.1.1 iii) et 3.2.1.3, on a

$$\begin{aligned}\frac{g_{k,s+1}}{X} &\leq \frac{q^{k-1}(q+1)p^{s+1}}{\frac{5}{2}q^{k-1}-\frac{7}{2}+p^{s+1}q^{k-1}-4}\\ &= \frac{q+1}{\frac{5}{2p^{s+1}}+1-\frac{15}{2q^{k-1}p^{s+1}}}\\ &\leq \frac{5}{\frac{13}{8}-\frac{15}{4\cdot 4^{k-1}}}\end{aligned}$$

Ainsi, le graphe de la fonction Φ est situé en dessous de la droite $y=\frac{9}{2}\left(1+\frac{5}{\frac{13}{8}-\frac{15}{4\cdot 4^{k-1}}}\right)x+\frac{45}{2}$ pour tout $k\geq 1$, d'où

$$\mu_2^{\mathrm{sym}}(n)\leq \Phi(n)\leq \frac{9}{2}\left(1+\frac{40}{13}\right)n+\frac{45}{2}.$$

□

En particulier, ce dernier théorème permet d'actualiser la constante $C_2=54$ dans le théorème 2.1.5.4. En effet, d'après le corollaire suivant, $C_2=\frac{4824}{247}\approx 19.6$ est une nouvelle constante qui convient :

Corollaire 4.1.2.3. *Pour tout $n\geq 2$, on a*

$$\mu_2^{\mathrm{sym}}(n)\leq \frac{4824}{247}n.$$

Preuve. D'après les valeurs de $\mu_2^{\mathrm{sym}}(n)$ données dans [CÖ10, Table1], pour tout $n\leq 18$, on a $\mu_2^{\mathrm{sym}}(n)\leq 19n$. D'autre part, pour tout $n\geq 19$, le théorème 4.1.2.2 donne

$$\mu_2^{\mathrm{sym}}(n)\leq \left(\frac{477}{26}+\frac{45}{2\times 19}\right)n=\frac{4824}{247}n$$

□

Remarque. Le théorème 4.1.2.2 donne la borne asymtotique suivante :

$$M_2^{\mathrm{sym}}\leq \frac{477}{26}\approx 18.35$$

qui est la meilleure borne symétrique asymptotique actuelle à être obtenue avec une tour explicite (et donc pour laquelle on peut disposer d'algorithmes explicites). Cependant, ce n'est plus la meilleure borne connue depuis les résultats établis par Cascudo, Cramer, Xing et Yang dans [CCXY12], puisqu'en utilisant des courbes de Shimura non-explicites, les auteurs obtiennent la borne purement asymptotique suivante, rappelée dans la section 2.1 : $M_2^{\mathrm{sym}}\leq 7.47$.

4.2 Amélioration des bornes d'Arnaud

Dans cette section, on présente une amélioration et une rectification de certaines bornes obtenues dans [Arn06]. Ces résultats font partie d'un article en cours.

4.2.1 Les bornes établies par N. Arnaud

Dans sa thèse [Arn06], Arnaud a établi les bornes suivantes :

Théorème 4.2.1.1. *Soit $q = p^r$ une puissance d'un nombre premier p.*

(i) Si $q \geq 4$, alors $\mu_{q^2}^{\mathrm{sym}}(n) \leq 2\left(1 + \frac{p}{q-3+(p-1)\left(1-\frac{1}{q+1}\right)}\right) n,$

(ii) Si $q \geq 16$, alors $\mu_{q}^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{2p}{q-3+2(p-1)\left(1-\frac{1}{q+1}\right)}\right) n.$

Notons que contrairement à ce qui est annoncé dans [Arn06, §2.3], la borne (ii) n'est pas établie pour tout $q \geq 4$ mais pour tout $q \geq 16$; on en donnera une version améliorée dans la section 4.2.3 qui sera, de plus, bien valable pour tout $q \geq 4$. On y prouvera aussi deux versions révisées de bornes données par Arnaud ; en effet, dans [Arn06], les deux bornes suivantes sont données sans détailler les calculs :

(iii) Pour tout premier $p \geq 5$, on a $\mu_{p^2}^{\mathrm{sym}}(n) \leq 2\left(1 + \frac{2}{p-2}\right) n,$

(iv) Pour tout premier $p \geq 5$, on a $\mu_{p}^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{4}{p-1}\right) n.$

En fait, il s'avère que les dénominateurs $p-1$ and $p-2$ sont légèrement surestimés sous les hypothèses d'Arnaud.

4.2.2 Algorithmes de type Chudnovsky adaptés

On établit les bornes générales pour le rang de tenseur symétrique de la multiplication qui seront utiles pour la section 4.2.3.

Ce premier résultat est dû à Arnaud [Arn06, Théorème 3.7].

Théorème 4.2.2.1. *Soient q une puissance d'un nombre premier et $n \geq 2$ un entier. Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques $F/\mathbb{F}_q$ de genre g avec $B_1(F/\mathbb{F}_q)$ places de degré 1. Soient a et N deux entiers tels que $0 \leq a \leq N \leq B_1(F/\mathbb{F}_q)$.*
Si

(i) il existe un diviseur $\mathcal{G}$ non-spécial de degré $g-1$ dans $F/\mathbb{F}_q$,

(ii) il existe une place Q de degré n dans $F/\mathbb{F}_q$,

(iii) $N + a \geq 2n + 2g - 1$.

Alors

$$\mu_q^{\mathrm{sym}}(n) \leq 2n + g - 1 + a.$$

Le théorème suivant est une amélioration de [Arn06, Théorème 3.8].

Théorème 4.2.2.2. *Soient q une puissance d'un nombre premier et $n \geq 2$ un entier. Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre g avec $B_i(F/\mathbb{F}_q)$ places de degré i. Soient a_1, a_2, N_1, N_2 des entiers tels que $0 \leq a_i \leq N_i \leq B_i(F/\mathbb{F}_q)$ pour $i = 1$ et 2.*
Si

(i) il existe un diviseur $\mathcal{G}$ non-spécial de degré $g-1$ dans $F/\mathbb{F}_q$,

(ii) il existe une place Q de degré n dans $F/\mathbb{F}_q$,

(iii) $N_1 + a_1 + 2(N_2 + a_2) \geq 2n + 2g - 1$.

Alors

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g + \frac{3}{2}(a_1 + 2a_2).$$

Preuve. Soient $\mathscr{P}_1 := \{P_1, \ldots, P_{N_1}\}$ un ensemble de N_1 places de degré 1 et $\mathscr{P}_1'$ un sous-ensemble de $\mathscr{P}_1$ de cardinal a_1. Soient $\mathscr{P}_2 := \{Q_1, \ldots, Q_{N_2}\}$ un ensemble de N_2 places de degré 2 et $\mathscr{P}_2'$ un sous-ensemble de $\mathscr{P}_2$ de cardinal a_2. D'après le lemme 2.2.1.2, on peut choisir un diviseur $\mathcal{D}$ (équivalent à $Q + \mathcal{G}$) non-spécial de degré $n + g - 1$ tel que la fonction d'évaluation Ev_Q est bijective. De plus, le lemme 1.1.4.11 assure que, quitte à considérer un diviseur équivalent, on peut supposer que le diviseur $\mathcal{D}$ est effectif et que son support ne contient ni Q, ni aucune des places des ensembles $\mathscr{P}_1$ et $\mathscr{P}_2$. On définit les applications Ev_Q et $Ev_{\mathscr{P}}$ comme dans la version de l'algorithme de la section 2.2.3 avec $l_P = 2$ si $P \in \mathscr{P}_1' \cup \mathscr{P}_2'$ et $l_P = 1$ si $P \in (\mathscr{P}_1 \backslash \mathscr{P}_1') \cup (\mathscr{P}_2 \backslash \mathscr{P}_2')$. Alors $Ev_{\mathscr{P}}$ est injective. En effet, son noyau est $\mathcal{L}(2\mathcal{D} - \sum_{P \in \mathscr{P}_1 \cup \mathscr{P}_2} l_P P)$, avec

$$\deg\big(2\mathcal{D} - \sum_{P \in \mathscr{P}_1 \cup \mathscr{P}_2} l_P P\big) = 2(n + g - 1) - (N_1 + a_1 + 2(N_2 + a_2)) < 0.$$

De plus, le rang $\operatorname{rk} Ev_{\mathscr{P}}$ de cette application $Ev_{\mathscr{P}}$ est $2n + g - 1$, car $\operatorname{rk} Ev_{\mathscr{P}} = \dim(2\mathcal{D}) = \deg(2\mathcal{D}) - g + 1 + i(2\mathcal{D})$, où $i(2\mathcal{D}) = 0$ puisque $2\mathcal{D} \geq \mathcal{D} \geq \mathcal{G}$ avec $i(\mathcal{G}) = 0$. Ainsi, on peut extraire des sous-ensembles $\tilde{\mathscr{P}}_1$ de $\mathscr{P}_1$, $\tilde{\mathscr{P}}_1{}'$ de $\mathscr{P}_1'$, $\tilde{\mathscr{P}}_2$ de $\mathscr{P}_2$ et $\tilde{\mathscr{P}}_2{}'$ de $\mathscr{P}_2'$, de cardinaux respectifs $\tilde{N}_1 \leq N_1$, $\tilde{a}_1 \leq a_1$, $\tilde{N}_2 \leq N_2$ et $\tilde{a}_2 \leq a_2$, tels que :

- $2n + g \geq \tilde{N}_1 + \tilde{a}_1 + 2(\tilde{N}_2 + \tilde{a}_2) \geq 2n + g - 1$,
- l'application $Ev_{\tilde{\mathscr{P}}}$ définie de la même façon que $Ev_{\mathscr{P}}$ avec $l_P = 2$ si $P \in \tilde{\mathscr{P}}_1{}' \cup \tilde{\mathscr{P}}_2'$ et $l_P = 1$ si $(\tilde{\mathscr{P}}_1 \backslash \tilde{\mathscr{P}}_1{}') \cup (\tilde{\mathscr{P}}_2 \backslash \tilde{\mathscr{P}}_2{}')$, est injective.

D'après la borne (2.6), on obtient $\mu_q^{\mathrm{sym}}(n) \leq \tilde{N}_1 + 2\tilde{a}_1 + 3(\tilde{N}_2 + 2\tilde{a}_2)$ car $\mu_q^{\mathrm{sym}}(1, 2) \leq 3$ pour tout q. Ainsi, comme $2n + g \geq \tilde{N}_1 + \tilde{a}_1 + 2(\tilde{N}_2 + \tilde{a}_2)$, on a

$$\begin{aligned} 3n + \frac{3}{2}g + \frac{3}{2}(\tilde{a}_1 + 2\tilde{a}_2) &\geq \frac{3}{2}\tilde{N}_1 + 3\tilde{N}_2 + 3\tilde{a}_1 + 6\tilde{a}_2 \\ &\geq \tilde{N}_1 + 2\tilde{a}_1 + 3(\tilde{N}_2 + 2\tilde{a}_2) \end{aligned}$$

d'où le résultat. □

4.2.3 Les bornes d'Arnaud améliorées

Ici, on donne une preuve détaillée de l'amélioration de la borne (ii) du théorème 4.2.1.1, sur un plus grand domaine de validité. De plus, on corrige la borne annoncée par Arnaud pour $\mu_{p^2}^{\mathrm{sym}}(n)$ et on améliore celle (non démontrée) pour $\mu_p^{\mathrm{sym}}(n)$. Plus précisément, on démontre le résultat suivant :

Théorème 4.2.3.1. *Soit p un nombre premier.*

(i) Si $q = p^r \geq 4$, alors $\mu_q^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{p}{q-3+(p-1)\left(1-\frac{1}{q+1}\right)}\right) n.$

(ii) Si $p \geq 5$, alors $\mu_{p^2}^{\mathrm{sym}}(n) \leq 2\left(1 + \frac{2}{p-\frac{33}{16}}\right) n.$

(iii) Si $p \geq 5$, alors $\mu_p^{\mathrm{sym}}(n) \leq 3\left(1 + \frac{2}{p-\frac{33}{16}}\right) n.$

Preuve. Le raisonnement général est le même que dans la preuve du théorème 4.1.2.2, mais pour les tours $\mathcal{T}_3/\mathbb{F}_q$, $\mathcal{T}_5/\mathbb{F}_{p^2}$ et $\mathcal{T}_5/\mathbb{F}_p$, avec les bornes des théorèmes 4.2.2.1 et 4.2.2.2. Les cas (i) et (iii) sont parfaitement analogues, car ils reposent sur l'algorithme du théorème 4.2.2.2 mais utilisé respectivement sur la tour $\mathcal{T}_3/\mathbb{F}_q$ et $\mathcal{T}_5/\mathbb{F}_p$. On démontre donc le résultat pour $\mu_q^{\mathrm{sym}}(n)$ en sachant que, *mutatis mutandis*, tout est également valable pour la démonstration de la borne pour $\mu_p^{\mathrm{sym}}(n)$. En particulier, les seules différences concernent les définitions des quantités suivantes qui se correspondent une à une :

(i) Pour chaque étage de la tour $\mathcal{T}_3/\mathbb{F}_q$, on note $g_{k,s} := g(G_{k,s}/\mathbb{F}_q)$ et on pose

$$M_{k,s} := B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_q),$$

$$n_0^{k,s} = \sup\left\{m \in \mathbb{N} \,|\, M_{k,s} \geq 2m + 2g_{k,s} - 1\right\}$$

$$\Delta g_{k,s} := g_{k,s+1} - g_{k,s}$$

$$D_{k,s} := (p-1)p^s q^k$$

(iii) Pour chaque étage de la tour $\mathcal{T}_5/\mathbb{F}_p$, on note $g_k := g(L_k/\mathbb{F}_p)$ et on pose

$$M_k := B_1(L_k/\mathbb{F}_p) + 2B_2(L_k/\mathbb{F}_p),$$

$$n_0^k = \sup\left\{m \in \mathbb{N} \,|\, M_k \geq 2m + 2g_k - 1\right\}$$

$$\Delta g_k := g_{k+1} - g_k$$

$$D_k := \Delta g_k$$

On suppose que $n \geq \frac{1}{2}(q + 1 + \epsilon(q))$ (resp. $n \geq \frac{1}{2}(p + 1 + \epsilon(p))$; sinon, on a déjà par les théorèmes 2.1.3.2 et 2.1.3.3 que $\mu_q^{\mathrm{sym}}(n) \leq 2n$ (resp. $\mu_p^{\mathrm{sym}}(n) \leq 2n$). D'après le lemme 3.2.1.10 (resp. 3.2.2.6), il existe un étage de la tour $\mathcal{T}_3/\mathbb{F}_q$ (resp. $\mathcal{T}_5/\mathbb{F}_p$) sur lequel on appliquer le théorème 4.2.2.2 avec $a_1 = a_2 = 0$. On note $G_{k,s+1}/\mathbb{F}_q$ le premier étage qui satisfait cette propriété. Pour multiplier dans $\mathbb{F}_{q^n}$, on a alors l'alternative suivante :

a) utiliser l'algorithme sur l'étage $G_{k,s+1}$. Dans ce cas, le théorème 4.2.2.2 appliqué avec $a_1 = a_2 = 0$ donne la borne suivante pour la complexité bilinéaire :

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g_{k,s+1} = 3n_0^{k,s} + \frac{3}{2}g_{k,s} + 3\Big(n - n_0^{k,s} + \frac{\Delta g_{k,s}}{2}\Big)$$

b) utiliser l'algorithme sur l'étage $G_{k,s}$ avec, pour $i = 1, 2$, a_i évaluations d'ordre 2 sur les places de degré i, où les entiers a_i satisfont $a_1 + 2a_2 \leq M_{k,s}$ et $M_{k,s} + a_1 + 2a_2 \geq 2n + 2g_{k,s} - 1$. Le choix optimal pour ces entiers est $a_1 + 2a_2 = 2(n - n_0^{k,s}) + \epsilon$ où $\epsilon \in \{0, 1\}$. On obtient alors la borne suivante pour la complexité bilinéaire :

$$\mu_q^{\mathrm{sym}}(n) \leq 3n + \frac{3}{2}g_{k,s} + \frac{3}{2}(a_1 + 2a_2) = 3n_0^{k,s} + \frac{3}{2}g_{k,s} + 6(n - n_0^{k,s}) + \frac{3}{2}.$$

Ainsi, sous réserve que l'on puisse choisir les entiers a_i comme dans le cas b), si $2(n - n_0^{k,s}) < \Delta g_{k,s}$ alors la borne donnée par le cas b) est meilleure que celle donnée par le cas a). Or remarquons que d'après le lemme 3.2.1.6 (resp 3.2.2.2), si $(n - n_0^{k,s}) < D_{k,s}$ alors on a à la fois $2(n - n_0^{k,s}) < \Delta g_{k,s}$ car $D_{k,s} \leq \Delta g_{k,s}$ mais aussi $M_{k,s} > D_{k,s} \geq 2(n - n_0^{k,s})$, donc on peut choisir les entiers a_i de sorte que $a_1 + 2a_2 = 2(n - n_0^{k,s}) + \epsilon$ où $\epsilon \in \{0, 1\}$. Autrement dit, si $2(n - n_0^{k,s}) < D_{k,s}$ alors on peut choisir de procéder comme dans le cas b) et on obtient une meilleure borne pour la complexité bilinéaire.

Pour $x \in \mathbb{R}^+$ tel que $M_{k,s+1} \geq 2\,[x] + 2g_{k,s+1} - 1$ et $M_{k,s} < 2\,[x] + 2g_{k,s} - 1$, on définit la fonction $\Phi_{k,s}(x)$ comme suit :

$$\Phi_{k,s}(x) = \begin{cases} 6(x - n_0^{k,s}) + 3(n_0^{k,s} + \frac{1}{2}g_{k,s} + \frac{1}{2}) & \text{si } 2(x - n_0^{k,s}) < D_{k,s} \\ 3(x - n_0^{k,s}) + 3(n_0^{k,s} + \frac{1}{2}g_{k,s} + \frac{1}{2}\Delta g_{k,s}) & \text{sinon.} \end{cases}$$

On définit ensuite la fonction Φ pour tout $x \geq 0$ comme le minimum des fonctions $\Phi_{k,s}$ pour lesquelles x est dans le domaine de définition de $\Phi_{k,s}$. Cette fonction est linéaire par morceau, avec deux sortes de morceaux : ceux de pente 6 et ceux de pente 3. De plus, le graphe de Φ est situé en dessous des points de la forme $\big(n_0^{k,s} + \frac{D_{k,s}}{2}, \Phi(n_0^{k,s} + \frac{D_{k,s}}{2})\big)$, car ces points sont les sommets du graphe. Posons $X := n_0^{k,s} + \frac{D_{k,s}}{2}$, alors

$$\Phi(X) \leq \Phi_{k,s}(X) = 3(X + \frac{g_{k,s+1}}{2}) = \frac{9}{2}\left(1 + \frac{g_{k,s+1}}{2X}\right)X.$$

On cherche alors une borne pour $\Phi(X)$ qui soit indépendante de k et s.
Pour le cas (i), on a

$$n_0^{k,s} \geq \frac{1}{2}q^{k-1}p^s(q+1)(q-3) \quad \text{d'après le lemme 3.2.1.7}$$

et

$$g_{k,s+1} \leq q^{k-1}(q+1)p^{s+1} \quad \text{d'après le lemme 3.2.1.1 iii).}$$

Ainsi,

$$\begin{aligned}\frac{g_{k,s+1}}{2X} &= \frac{g_{k,s+1}}{2(n_0^{k,s}+\frac{D_{k,s}}{2})}\\ &\leq \frac{q^{k-1}(q+1)p^{s+1}}{2(\frac{1}{2}q^{k-1}p^s(q+1)(q-3)+\frac{1}{2}(p-1)p^sq^k)}\\ &= \frac{q^{k-1}(q+1)p^sp}{q^{k-1}(q+1)p^s\left(q-3+(p-1)\frac{q}{q+1}\right)}\\ &= \frac{p}{(q-3)+(p-1)\frac{q}{q+1}}\end{aligned}$$

Finalement, le graphe de Φ est situé en dessous de la droite d'équation $y=3\left(1+\frac{p}{(q-3)+(p-1)\frac{q}{q+1}}\right)x$. En particulier, on obtient

$$\mu_q^{\mathrm{sym}}(n)\leq\Phi(n)\leq 3\left(1+\frac{p}{(q-3)+(p-1)\frac{q}{q+1}}\right)n.$$

Pour le cas (iii), les lemmes 3.2.2.1 ii), 3.2.2.2 et 3.2.2.3 donnent

$$\begin{aligned}\frac{g_{k+1}}{2X} &\leq \frac{2^{k+2}}{2^{k+1}(p-3)+4+2^{k+1}-2^{\frac{k+1}{2}}}\\ &= \frac{2^{k+2}}{2^{k+1}\left((p-3)+1+2^{-k+1}-2^{-\frac{k+1}{2}}\right)}\\ &= \frac{2}{p-2+2^{-k+1}-2^{-\frac{k+1}{2}}}\\ &\leq \frac{2}{p-\frac{33}{16}}\end{aligned}$$

la dernière inégalité provenant du fait que $-\frac{1}{16}$ est le minimum de la fonction $k\mapsto 2^{-k+1}-2^{-\frac{k+1}{2}}$.
Finalement, le graphe de Φ est situé en dessous de la droite d'équation $y=3\left(1+\frac{2}{p-\frac{33}{16}}\right)x$. En particulier, on obtient

$$\mu_p^{\mathrm{sym}}(n)\leq\Phi(n)\leq 3\left(1+\frac{2}{p-\frac{33}{16}}\right)n.$$

La démonstration de (ii) est similaire, mais en appliquant le théorème 4.2.2.1 sur la tour $\mathcal{T}_5/\mathbb{F}_{p^2}$. La fonction Φ_k alors définie est donnée par

$$\Phi_k(x)=\begin{cases}2x+g_k-1+2(x-n_0^k) & \text{si } 2(x-n_0^k)<\Delta g_k\\ 2x+g_{k+1}-1 & \text{sinon,}\end{cases}$$

avec $n_0^k:=\sup\left\{m\in\mathbb{N}\,|\,B_1(L_k/\mathbb{F}_{p^2})\geq 2n+2g_k-1\right\}$. Le graphe de la fonction Φ correspondante est situé en dessous des points de la forme $\left(n_0^k+\frac{\Delta g_k}{2},\Phi(n_0^k+\frac{\Delta g_k}{2})\right)$, car

ces points sont les sommets du graphe. Si on pose $X := n_0^{k,s} + \frac{\Delta g_k}{2}$, alors

$$\Phi(X) \quad \leq \quad 2X + g_{k+1} - 1 \leq 2\left(1 + \frac{g_{k+1}}{2X}\right) X.$$

De même que précédemment, on a $\frac{g_{k+1}}{2X} \leq \frac{2}{p-\frac{33}{16}}$, donc le graphe de Φ est situé en dessous de la droite d'équation $y = 2\left(1 + \frac{2}{p-\frac{33}{16}}\right) x$. En particulier, on obtient

$$\mu_p^{\mathrm{sym}}(n) \leq \Phi(n) \leq 2\left(1 + \frac{2}{p - \frac{33}{16}}\right) n.$$

□

Remarque. Bien qu'il soit théoriquement possible d'utiliser des évaluations d'ordre 3 lorsqu'il n'y a pas assez de places d'un certain degré (en particulier des places rationnelles) pour que la seconde fonction de l'algorithme soit injective en utilisant les évaluations d'ordre 1 et 2, cela n'est jamais le cas en pratique. Calculons en effet le coût de l'utilisation d'évaluations d'ordre 1, 2 et 3 : dans ce cas, l'hypothèse minimale pour avoir l'injectivité de la seconde fonction est $B_1 + 2a_1 = 3B_1 \approx 2n + g$ (en supposant que l'on effectue des évaluations d'ordre 1, 2 et 3 sur toutes les places rationnelles, c'est-à-dire que $a_1 = B_1$). La borne de complexité obtenue est alors

$$\mu_q^{\mathrm{sym}}(n) \leq B_1 + 5a_1 = 6B_1 \approx 4n + 2g.$$

Si, au contraire on décide, lorsque que les évaluations d'ordre 1 et 2 ne suffisent plus pour avoir l'injectivité de la seconde fonction de l'algorithme, d'utiliser les places de degré 2, alors sous l'hypothèse minimale $B_1 + a_1 + 2B_2 = 2(B_1 + B_2) \approx 2n + g$, on obtient la borne suivante :

$$\mu_q^{\mathrm{sym}}(n) \leq B_1 + 2a_1 + 3B_2 = 3(B_1 + B_2) \approx 3n + \frac{3}{2}g.$$

Cette borne est plus précise que celle obtenue dans le cas de l'utilisation d'évaluations d'ordre 3, c'est pourquoi il est préférable en général de ne pas utiliser de telles évaluations.

Chapitre 5

Bornes pour la complexité bilinéaire asymétrique

On utilise ici l'algorithme qui est présenté dans le théorème 2.2.5.1 ; les résultats de ce chapitre concernent donc la complexité bilinéaire non nécessairement symétrique. En particulier, on obtient les meilleures bornes uniformes actuelles pour la complexité asymétrique dans les extensions finies de $\mathbb{F}_2$, de $\mathbb{F}_p$ et $\mathbb{F}_{p^2}$ pour tout premier $p \geq 3$ et de $\mathbb{F}_q$ et $\mathbb{F}_{q^2}$ pour tout $q \geq 4$ (resp. $q > 5$). Certaines de ces bornes uniformes fournissent alors de nouvelles bornes asymptotiques.

Les résultats de ce chapitre sont l'objet d'un article en cours avec H. Randriambololona.

5.1 Algorithme de type Chudnovsky adapté

5.1.1 Spécialisation pour les places de degré divisant d

On détaille dans cette section une méthode générale permettant d'obtenir des bornes uniformes pour $\mu_q(n)$ en utilisant des places de degré i, pour i parcourant l'ensemble des diviseurs d'un entier d bien choisi. Pour cela, on commence par établir un lemme préliminaire, puis on spécialise l'algorithme sur les places de degré $i|d$.

Lemme 5.1.1.1. *Soit $d \in \mathbb{N}$. Pour tout entier $0 < j \leq d$ tel que $j < \frac{1}{2}(q+1+\epsilon(q))$ si $q \geq 4$, ou $j \leq \frac{1}{2}q+1$ si $q \in \{2,3\}$, on a*

$$\frac{\mu_q^{\mathrm{sym}}(j)}{j} \leq \frac{\mu_q^{\mathrm{sym}}(d)}{d}.$$

Preuve. Supposons que le lemme soit faux. Alors il existe un entier $0 < j < d$ tel que $j < \frac{1}{2}(q+1+\epsilon(q))$ si $q \geq 4$ (resp. $j \leq \frac{1}{2}q+1$ si $q \in \{2,3\}$) et $\mu_q^{\mathrm{sym}}(j) > \frac{j}{d}\mu_q^{\mathrm{sym}}(d)$. Deux cas se présentent :

- soit $j \leq \frac{1}{2}q+1$ (en particulier, c'est le cas si $q \in \{2,3\}$), et donc on a $\mu_q^{\mathrm{sym}}(j) > \frac{j}{d}\mu_q^{\mathrm{sym}}(d) \geq \frac{j}{d}(2d-1) > 2j-1$, ce contredit le théorème 2.1.3.2.
- soit $\frac{q}{2}+1 < j < \frac{1}{2}(q+1+\epsilon(q))$ et donc $\mu_q^{\mathrm{sym}}(d) \geq 2d$ entraîne que $\mu_q^{\mathrm{sym}}(j) > \frac{j}{d}\mu_q^{\mathrm{sym}}(d) \geq 2j$, ce qui contredit le théorème 2.1.3.3.

□

Proposition 5.1.1.2. *Soit q une puissance d'un premier et d un entier positif dont tout diviseur propre j soit tel que $j < \frac{1}{2}(q+1+\epsilon(q))$ si $q \geq 4$, ou $j \leq \frac{1}{2}q+1$ si $q \in \{2,3\}$. Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre $g \geq 2$ avec N_i places de degré i et soient l_i des entiers tels que $0 \leq l_i \leq N_i$, pour tout $i|d$. Supposons que :*

(i) il existe une place de degré n dans $F/\mathbb{F}_q$,

(ii) $\sum_{i|d} i(N_i + l_i) \geq 2n + g + \alpha_q$, où $\alpha_2 = 5$, $\alpha_3 = \alpha_4 = \alpha_5 = 2$ et $\alpha_q = -1$ pour $q > 5$.

Alors

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n + \frac{g}{2}\right) + \gamma_{q,d}\sum_{i|d} i l_i + \kappa_{q,d}, \tag{5.1}$$

où $\gamma_{q,d} := \max_{i|d}\left(\frac{\mu_q(i,2)}{i}\right) - \frac{2\mu_q^{\mathrm{sym}}(d)}{d}$ *et* $\kappa_{q,d} \leq \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1)$.

Preuve. On applique le théorème 2.2.5.2 avec $n_{i,1} = N_i - l_i$ et $n_{i,2} = l_i$ pour tout $i|d$, et $n_{j,u} = 0$ dans tous les autres cas. On choisit $l = 1$ et $m = n$ et on obtient

$$\begin{aligned}
\mu_q(n) &\leq \sum_{i|d}\Big(n_{i,1}\mu_q(i) + n_{i,2}\mu_q(i,2)\Big)\\
&= \sum_{i|d}\Big((N_i - l_i)\mu_q(i) + l_i\mu_q(i,2)\Big)\\
&\leq \sum_{i|d}\Big((N_i - l_i)\mu_q^{\mathrm{sym}}(i) + l_i\mu_q(i,2)\Big)\\
&= \sum_{i|d}\Big(\big(N_i + l_i\big)\mu_q^{\mathrm{sym}}(i) + l_i\big(\mu_q(i,2) - 2\mu_q^{\mathrm{sym}}(i)\big)\Big)\\
&= \sum_{i|d}\left(i\big(N_i + l_i\big)\frac{\mu_q^{\mathrm{sym}}(i)}{i} + il_i\left(\frac{\mu_q(i,2) - 2\mu_q^{\mathrm{sym}}(i)}{i}\right)\right)\\
&= \frac{\mu_q^{\mathrm{sym}}(d)}{d}\sum_{i|d} i\big(N_i + l_i\big) + \sum_{i|d}\left(i\big(N_i + l_i\big)\left(\frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d}\right)\right.\\
&\quad \left. + il_i\left(\frac{\mu_q(i,2) - 2\mu_q^{\mathrm{sym}}(i)}{i}\right)\right)\\
&= \frac{\mu_q^{\mathrm{sym}}(d)}{d}\sum_{i|d} i\big(N_i + l_i\big) + \sum_{i|d} il_i\left(\frac{\mu_q(i,2) - \mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d}\right)\\
&\quad + \sum_{i|d} iN_i\left(\frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d}\right)
\end{aligned}$$

D'après le lemme 5.1.1.1, on a $\frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d} \leq 0$, donc

$$\sum_{i|d} iN_i\left(\frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d}\right) \leq \sum_{i|d} il_i\left(\frac{\mu_q^{\mathrm{sym}}(i)}{i} - \frac{\mu_q^{\mathrm{sym}}(d)}{d}\right)$$

puisque $0 \leq l_i \leq N_i$ pour tout $i|d$. De plus, quitte à choisir des valeurs plus petites pour les l_i et/ou les N_i, on peut ramener la condition (ii) au cas où $\sum_{i|d} i(N_i + l_i) = 2n + g + \alpha_q + k_d$, avec $k_d \in \{0, \ldots, d-1\}$. On obtient alors

$$\mu_q(n) \quad \leq \quad \frac{\mu_q^{\mathrm{sym}}(d)}{d}(2n + g + \alpha_q + k_d) + \sum_{i|d} i l_i \left(\frac{\mu_q(i,2)}{i} - \frac{2\mu_q^{\mathrm{sym}}(d)}{d} \right)$$

d'où le résultat. □

Les deux corollaires suivants se déduisent de cette dernière proposition par application directe et donnent des valeurs explicites pour la borne (5.1), obtenues en appliquant la proposition précédente dans les cas où $d = 1$, 2 ou 4.

Corollaire 5.1.1.3. *Soient $q \geq 3$ une puissance d'un premier et $F/\mathbb{F}_q$ un corps de fonctions algébriques de genre $g \geq 2$ avec N_i places de degré i. Soient l_i des entiers tels que $0 \leq l_i \leq N_i$. Supposons que :*

(i) il existe une place de degré n dans $F/\mathbb{F}_q$,

(ii) $N_1 + l_1 + 2(N_2 + l_2) \geq 2n + g + \alpha_q$, où $\alpha_3 = \alpha_4 = \alpha_5 = 2$ et $\alpha_q = -1$ pour $q > 5$.

Alors on a

$$\mu_3(n) \leq 3n + \frac{3}{2}g + \frac{3}{2}(l_1 + 2l_2) + \frac{9}{2},$$

$$\text{pour } q = 4 \text{ ou } 5,\ \mu_q(n) \leq 3n + \frac{3}{2}g + l_1 + 2l_2 + \frac{9}{2},$$

et pour $q > 5$, on a les deux bornes suivantes :

$$\mu_q(n) \leq 3n + \frac{3}{2}g + \frac{1}{2}(l_1 + 2l_2),$$

ou dans le cas particulier où $N_2 = l_2 = 0$ (ce qui correspond à $d = 1$ dans la proposition 5.1.1.2)

$$\mu_q(n) \leq 2n + g + l_1 - 1.$$

Preuve. On applique la proposition 5.1.1.2 avec les bornes et valeurs suivantes, rappelées dans le chapitre 2, Section 2.1.5 : $\mu_q^{\mathrm{sym}}(2) = 3$ et $\mu_q(1,2) \leq 3$ pour tout q puissance d'un premier ; $\mu_3(2,2) \leq 9$; $\mu_q(2,2) \leq 8$ pour $q = 4$ ou 5 ; $\mu_q(2,2) \leq 7$ pour $q > 5$. On en déduit que $\gamma_{3,2} \leq \frac{9}{2} - 3 = \frac{3}{2}$, $\gamma_{q,2} \leq \frac{8}{2} - 3 = 1$ si $q = 4$ ou 5, et si $q > 5$, alors $\gamma_{q,2} \leq \frac{7}{2} - 3 = \frac{1}{2}$ et $\gamma_{q,1} \leq 1$. □

Corollaire 5.1.1.4. *Soit $F/\mathbb{F}_2$ un corps de fonctions algébriques de genre $g \geq 2$ avec N_i places de degré i et soient l_i des entiers tels que $0 \leq l_i \leq N_i$. Supposons que :*

(i) il existe une place de degré n dans $F/\mathbb{F}_2$,

(ii) $\sum_{i|4} i(N_i + l_i) \geq 2n + g + 5$.

Alors

$$\mu_2(n) \leq \frac{9}{2}\left(n + \frac{g}{2}\right) + \frac{3}{2}\sum_{i|4} i l_i + 18.$$

Preuve. On a rappelé dans le chapitre 2, Section 2.1.5, que $\mu_2^{\mathrm{sym}}(4) = 9$, $\mu_2(2,2) \leq 9$ et $\mu_2(4,2) \leq 24$, ce qui donne $\gamma_{2,4} \leq \frac{24}{4} - \frac{2 \cdot 9}{4} = \frac{3}{2}$ et le résultat se déduit de la proposition 5.1.1.2. □

5.1.2 Méthode générale pour l'obtention de bornes uniformes pour le rang de tenseur asymétrique

Considérons une tour $\mathcal{T}/\mathbb{F}_q$ de corps de fonctions $F_i/\mathbb{F}_q$ de genre $g(F_i)$ et avec $B_j(F_i)$ places de degré j. Soit d un entier dont tout diviseur propre j est tel que $j < \frac{1}{2}(q+1+\epsilon(q))$ si $q \geq 4$, ou $j \leq \frac{1}{2}q+1$ si $q \in \{2,3\}$.

Supposons qu'il existe un entier N tel que, pour tout $n \geq N$, il existe un entier $k(n)$ pour lequel les conditions suivantes sont vérifiées :

(A) $\sum_{j|d} jB_j(F_{k(n)+1}) \geq 2n + g(F_{k(n)+1}) + \alpha_q$ et $B_n(F_{k(n)+1}) > 0$,

(B) $\sum_{j|d} jB_j(F_{k(n)}) < 2n + g(F_{k(n)}) + \alpha_q$ mais $B_n(F_{k(n)}) > 0$,

(C) $g(F_{k(n)}) \geq 2$ (ce qui implique aussi que $g(F_{k(n)+1}) \geq 2$),

(D) $\Delta g_{k(n)} := g(F_{k(n)+1}) - g(F_{k(n)}) \geq \lambda D_{k(n)}$ où $\lambda := \frac{d\gamma_{q,d}}{\mu_q^{\mathrm{sym}}(d)}$,

(E) $\sum_{j|d} jB_j(F_{k(n)}) \geq D_{k(n)}$,

où α_q est l'entier défini dans la proposition 5.1.1.2 et $D_{k(n)}$ est fixé pour la tour $\mathcal{T}$ considérée et choisi de sorte à satisfaire (D) et (E).
On définit aussi

$$n_0^l := \sup\left\{ m \in \mathbb{N} \,\middle|\, \sum_{j|d} jB_j(F_l) \geq 2m + g(F_l) + \alpha_q \right\}.$$

Remarquons que pour l'entier $n_0^{k(n)}$, on a en particulier :

$$\sum_{j|d} jB_j(F_{k(n)}) + 2\left(n - n_0^{k(n)}\right) \geq 2n + g(F_{k(n)}) + \alpha_q. \tag{5.2}$$

Fixons désormais un entier $n \geq N$. Pour plus de concision, on note $k := k(n)$, l'entier satisfaisant les hypothèses (A) à (E).
Pour multiplier dans $\mathbb{F}_{q^n}$, on a l'alternative suivante :

(a) appliquer l'algorithme sur l'étage F_{k+1}, avec $B_j(F_{k+1})$ places de degré j pour tout $j|d$, toutes utilisées avec multiplicité 1 ; ceci est possible d'après les hypothèses (A) et (C). Dans ce cas, la proposition 5.1.1.2 donne la borne suivante pour $\mu_q(n)$:

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n + \frac{g(F_{k+1})}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1), \tag{5.3}$$

(b) appliquer l'algorithme sur l'étage F_k, avec pour tout $j|d$, $B_j(F_k)$ places de degré j parmi lesquelles l_j sont utilisées avec multiplicité 2 et le reste avec multiplicité 1, où les entiers $l_j \leq B_j(F_k)$ satisfont $\sum_{j|d} l_j \geq 2(n - n_0^k)$; pour de tels entiers l_j, on peut appliquer la proposition 5.1.1.2 d'après les conditions (B) et (5.2). En particulier, si $2(n-n_0^k) + d - 1 \leq \sum_{j|d} jB_j(F_k)$, alors on peut choisir les entiers l_j de sorte que $\sum_{j|d} jl_j = 2(n-n_0^k) + \epsilon$ pour un certain $\epsilon \in \{0, \ldots, d-1\}$, et ce choix convient. Dans ce cas, la proposition 5.1.1.2 donne :

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n + \frac{g(F_k)}{2}\right) + \gamma_{q,d}\sum_{j|d} jl_j + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1). \tag{5.4}$$

Notons que l'on peut réécrire (5.3) de la façon suivante :

$$\mu_q(n) \leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(n + \frac{g(F_k)}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}\Delta g_k$$

ce qui met en évidence que si $\gamma_{q,d}\sum_{j|d} jl_j < \frac{\mu_q^{\mathrm{sym}}(d)}{d}\Delta g_k$, alors la borne obtenue dans le cas (b) est meilleure que celle obtenue dans le cas (a).
Ainsi, lorsque $2(n - n_0^k) + d - 1 < D_k$, on peut procéder comme dans le cas (b) puisque d'après l'hypothèse (E), on peut choisir des entiers l_j et $\epsilon \in \{0, \ldots, d-1\}$ tels que $\sum_{j|d} jl_j = 2(n - n_0^k) + \epsilon$. De plus, on a

$$\frac{d\gamma_{q,d}}{\mu_q^{\mathrm{sym}}(d)}(2(n - n_0^k) + d - 1) < \Delta g_k$$

d'après l'hypothèse (D), donc $\gamma_{q,d}\left(2(n - n_0^k) + \epsilon\right) < \frac{\mu_q^{\mathrm{sym}}(d)}{d}\Delta g_k$ ce qui entraîne que la borne obtenue dans le cas (b) est plus précise.

Pour $x \in \mathbb{R}^+$, $x \geq N$, tel que $\sum_{j|d} jB_j(F_{k+1}) \geq 2\,[x] + g(F_{k+1}) + \alpha_q$ et $\sum_{j|d} jB_j(F_{k+1}) < 2\,[x] + g(F_k) + \alpha_q$, on définit la fonction Φ_k comme suit :

$$\Phi_k(x) = \begin{cases} \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(x + \frac{g(F_k)}{2}\right) + \gamma_{q,d}\big(2(x - n_0^k) + d - 1\big) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1), \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{si } 2(x - n_0^k) + d - 1 < D_k. \\ \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(x + \frac{g(F_{k+1})}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1), \text{ sinon.} \end{cases}$$

c'est-à-dire :

$$\Phi_k(x) = \begin{cases} \left(\frac{2\mu_q^{\mathrm{sym}}(d)}{d} + 2\gamma_{q,d}\right)(x - n_0^k) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}\left(2n_0^k + g(F_k) + \alpha_q + d - 1\right), \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{si } 2(x - n_0^k) + d - 1 < D_k. \\ \frac{2\mu_q^{\mathrm{sym}}(d)}{d}(x - n_0^k) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}\left(2n_0^k + g(F_{k+1}) + \alpha_q + d - 1\right), \text{ sinon.} \end{cases}$$

On définit alors la fonction Φ pour tout $x \geq N$ comme étant le minimum de toutes les fonctions Φ_i dont x est dans le domaine de définition. Cette fonction est linéaire par morceaux avec deux sortes de morceaux : ceux de pente $\frac{2\mu_q^{\mathrm{sym}}(d)}{d}$ et ceux de pente $\frac{2\mu_q^{\mathrm{sym}}(d)}{d} + 2\gamma_{q,d}$. De plus, le graphe de la fonction Φ est en dessous de toute droite passant au dessus des points de la forme $\big(n_0^i + \frac{1}{2}(D_i - d + 1), \Phi(n_0^i + \frac{1}{2}(D_i - d + 1))\big)$, car ces points constituent les sommets du graphe de Φ.
Posons $X := n_0^i + \frac{1}{2}(D_i - d + 1)$. Alors

$$\begin{aligned} \Phi(X) &\leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(X + \frac{g(F_{i+1})}{2}\right) + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1) \\ &\leq \frac{2\mu_q^{\mathrm{sym}}(d)}{d}\left(1 + \frac{g(F_{i+1})}{2X}\right)X + \frac{\mu_q^{\mathrm{sym}}(d)}{d}(\alpha_q + d - 1). \end{aligned}$$

Ainsi, si l'on peut donner une borne de $\Phi(X)$ qui est indépendante de i, alors cette borne est aussi valable pour $\mu_q(n)$ pour tout $n \geq N$, puisque $\mu_q(n) \leq \Phi(n)$.

5.2 Obtention des nouvelles bornes asymétriques

On applique la méthode générale décrite précédemment pour établir de nouvelles bornes uniformes asymétriques. Certaines d'entre elles permettent d'établir des bornes asymptotiques qui sont meilleures que les bornes asymptotiques symétriques obtenues dans [CCXY12]. De plus, nos nouvelles bornes asymptotiques proviennent de bornes uniformes et fournissent donc des algorithmes explicites pour cette complexité.

5.2.1 Bornes uniformes

Théorème 5.2.1.1. *Pour tout entier $n \geq 2$, on a*

$$\mu_2(n) \leq \frac{189}{22} n + 18.$$

Preuve. Soit $q := p^2 = 4$ et $n \geq 2$. On applique la méthode générale décrite dans la section 5.1.2 avec $d = 4$, sur la tour $\mathcal{T}_4/\mathbb{F}_2$ présentée au chapitre 3. On a donc $\gamma_{2,4} \leq \frac{3}{2}$, $\lambda := \frac{4\gamma_{2,4}}{\mu_2^{\mathrm{sym}}(4)} \leq \frac{2}{3}$, $X = n_0^{k,s} + \frac{1}{2}(D_{k,s} - 3)$ où $D_{k,s} = \frac{3}{2} p^{s+1} q^{k-1}$ (notons qu'en particulier, avec ces valeurs de $D_{k,s}$ et λ, le lemme 3.2.1.2 implique que les conditions (D) et (E) sont satisfaites). La condition (C) est vraie dès l'étage $H_{1,1}/\mathbb{F}_2$, et enfin le lemme 3.2.1.5 assure que les conditions (A) et (B) sont bien satisfaites (car on a toujours $2n + 2g_{k,s} + 7 \geq 2n + g_{k,s} + 5$ et que c'est toujours la condition (2) du lemme 3.2.1.5 qui est la dernière à être satisfaite, même en remplaçant $2n + 2g + 7$ par $2n + g + 5$). On a donc

$$\begin{aligned} \Phi(X) &= \frac{2\mu_q^{\mathrm{sym}}(d)}{d} \left(1 + \frac{g(H_{k,s+1})}{2X}\right) X + \frac{\mu_q^{\mathrm{sym}}(d)}{d} (\alpha_q + d - 1) \\ &= \frac{9}{2} \left(1 + \frac{g(H_{k,s+1})}{2X}\right) X + 18. \end{aligned}$$

D'après les lemmes 3.2.1.1 iii) et 3.2.1.4, on obtient :

$$\begin{aligned} \frac{g(H_{k,s+1})}{2X} &\leq \frac{q^{k-1}(q+1)p^{s+1}}{2n_0^{k,s} + D_{k,s} - 3} \\ &\leq \frac{q^{k-1}(q+1)p^{s+1}}{5p^{s+1}q^{k-1} - 5 + \frac{3}{2}p^{s+1}q^{k-1} - 3} \\ &= \frac{q+1}{\frac{13}{2} - \frac{8}{q^{k-1}p^{s+1}}}. \end{aligned}$$

Ainsi, si $k \geq 2$ (ce que l'on peut supposer, quitte à avoir une borne moins précise pour les petites valeurs de n), on a $\frac{g(H_{k,s+1})}{2X} \leq \frac{10}{11}$, ce qui donne $\mu_q(n) \leq \frac{9}{2}\left(1 + \frac{10}{11}\right) n + 18$ d'où le résultat annoncé. □

Remarque. La borne asymptotique correspondant à cette borne uniforme est

$$M_2 \leq \frac{189}{22} \simeq 8.6,$$

ce qui est moins bon que la borne purement asymptotique $M_2^{\mathrm{sym}} \leq 7.47$ obtenue dans [CCXY12] mais pour laquelle on ne dispose pas d'un algorithme explicite.

Théorème 5.2.1.2. *Soit p un nombre premier et $q := p^r$. Pour tout $n \geq 2$, on a :*

(i) si $q \geq 4$, alors

$$\mu_{q^2}(n) \leq 2\left(1 + \frac{p}{q-2+(p-1)\frac{q}{q+1}}\right) n - 1,$$

(ii) si $p \geq 3$, alors

$$\mu_{p^2}(n) \leq 2\left(1 + \frac{2}{p-1}\right) n - 1,$$

(iii) si $q > 5$, alors

$$\mu_q(n) \leq 3\left(1 + \frac{p}{q-2+(p-1)\frac{q}{q+1}}\right) n,$$

(iv) si $p > 5$, alors

$$\mu_p(n) \leq 3\left(1 + \frac{2}{p-1}\right) n.$$

Preuve.

(i) Soit $n \geq \frac{1}{2}\left(q^2 + 1 + \epsilon(q^2)\right)$. On applique la méthode générale décrite dans la section 5.1.2 avec $d = 1$, sur la tour $\mathcal{T}_2/\mathbb{F}_{q^2}$ présentée au chapitre 3, ce qui est possible d'après le lemme 3.2.1.9 (notons que la propriété (3) de ce lemme implique *a fortiori* que la condition (A) est bien satisfaite). On a alors $\gamma_{q^2,1} \leq 1$, $\lambda := \frac{\gamma_{q^2,1}}{\mu_{q^2}^{\mathrm{sym}}(1)} \leq 1$, $X = n_0^{k,s} + \frac{1}{2}D_{k,s}$ où $D_{k,s} = (p-1)p^s q^{k-1}$ et

$$\Phi(X) \;=\; 2\left(1 + \frac{g(F_{k,s+1})}{2X}\right) X - 1.$$

D'après les lemmes 3.2.1.1 iii) et 3.2.1.8, on obtient :

$$\begin{aligned}
\frac{g(F_{k,s+1})}{2X} &\leq \frac{q^{k-1}(q+1)p^{s+1}}{2n_0^{k,s} + D_{k,s}} \\
&\leq \frac{q^{k-1}(q+1)p^{s+1}}{(q+1)q^{k-1}p^s(q-2) + (p-1)p^s q^{k-1}} \\
&= \frac{p}{q-2+(p-1)\frac{q}{q+1}}
\end{aligned}$$

d'où le résultat.

(ii) Soit $n \geq \frac{1}{2}\left(p^2 + 1 + \epsilon(p^2)\right)$. On applique la méthode générale avec $d = 1$ sur la tour $\mathcal{T}_5/\mathbb{F}_{p^2}$, ce qui est possible d'après le lemme 3.2.2.7. On a $\gamma_{p^2,1} \leq 1$, $\lambda := \frac{\gamma_{p^2,1}}{\mu_{p^2}^{\mathrm{sym}}(1)} \leq 1$, $X = n_0^k + \frac{1}{2}D_k$ où $D_k = 2^{k+1} - 2^{\frac{k+1}{2}}$ et

$$\Phi(X) \;=\; 2\left(1 + \frac{g(L_{k+1})}{2X}\right) X - 1.$$

D'après les lemmes 3.2.2.1 ii) et 3.2.2.4, on obtient :

$$\begin{aligned}\frac{g(L_{k+1})}{2X} &\leq \frac{2^{k+2}}{2n_0^k + D_k} \\ &\leq \frac{2^{k+2}}{2^{k+1}(p-2) + 2^{\frac{k+3}{2}} + 2^{k+1} - 2^{\frac{k+1}{2}}} \\ &= \frac{2}{p - 1 + 2^{-\frac{k-1}{2}} - 2^{-\frac{k+1}{2}}}\end{aligned}$$

ce qui donne le résultat, puisque $2^{-\frac{k-1}{2}} - 2^{-\frac{k+1}{2}} \geq 0$.

(iii) Soit $n \geq \frac{1}{2}(q + 1 + \epsilon(q))$. On applique la méthode générale avec $d = 2$ sur la tour $\mathcal{T}_3/\mathbb{F}_q$, ce qui est possible d'après le lemme 3.2.1.10 (notons que la propriété (3) de ce lemme implique *a fortiori* que la condition (A) est bien satisfaite). On a $\gamma_{q,2} \leq \frac{1}{2}$, $\lambda := \frac{2\gamma_{q,2}}{\mu_q^{\mathrm{sym}}(2)} \leq \frac{1}{3}$, $X = n_0^{k,s} + \frac{1}{2}D_{k,s}$ où $D_{k,s} = (p-1)p^s q^{k-1}$ et

$$\Phi(X) = 3\left(1 + \frac{g(G_{k,s+1})}{2X}\right)X.$$

On procède comme pour (i) et on obtient $\frac{g(G_{k,s+1})}{2X} \leq \frac{p}{q-2+(p-1)\frac{q}{q+1}}$ ce qui donne le résultat. Notons que $\lambda \leq 1$ donc le lemme 3.2.1.6 implique que l'hypothèse (D) de la section 5.1.2 est bien vérifiée.

(iv) Soit $n \geq \frac{1}{2}(p + 1 + \epsilon(p))$. On applique la méthode générale avec $d = 2$ sur la tour $\mathcal{T}_5/\mathbb{F}_p$, ce qui est possible d'après le lemme 3.2.2.8 (notons que la propriété (2) de ce lemme implique *a fortiori* que la condition (A) est bien satisfaite dans le cas où $p > 5$, c'est-à-dire pour $\alpha_p = -1$). On a $\gamma_{p,2} \leq 1$, $\lambda := \frac{2\gamma_{p,2}}{3} \leq 1$, $X = n_0^k + \frac{1}{2}D_k$ où $D_k = 2^{k+1} - 2^{\frac{k+1}{2}}$ et

$$\Phi(X) = 3\left(1 + \frac{g(L_{k+1})}{2X}\right)X.$$

On procède comme pour (ii) et on obtient $\frac{g(L_{k+1})}{2X} \leq \frac{2}{p-1}$ ce qui donne le résultat. Encore une fois, $\lambda \leq 1$ donc le lemme 3.2.2.2 assure que l'hypothèse (D) de la section 5.1.2 est bien vérifiée.

□

Théorème 5.2.1.3. *Pour tout $n \geq 2$, on a*

$$\mu_3(n) \leq 6n$$

et

$$\mu_5(n) \leq \frac{9}{2}n.$$

Preuve. La preuve du théorème 5.2.1.2 (iv) est encore valable pour $p = 3$ ou 5, car $\gamma_{5,2} = 1$ et $\lambda := \frac{2\gamma_{5,2}}{3} \leq 1$; $\gamma_{3,2} \leq \frac{3}{2}$ et $\lambda := \frac{2\gamma_{3,2}}{3} \leq 1$. La même borne tient donc pour $p = 3$ ou 5. □

5.2.2 Bornes asymptotiques

Les bornes uniformes établies à la section précédente donnent les bornes asymptotiques suivantes, qui sont meilleures que les bornes symétriques obtenues dans [CCXY12] :

Théorème 5.2.2.1.

$$M_3 \leq 6, \qquad M_5 \leq 4.5, \qquad M_{11} \leq 3.6, \qquad M_{13} \leq 3.5.$$

Preuve. Les bornes pour M_3 et M_5 sont une conséquence du théorème 5.2.1.3 ; celles pour M_{11} et M_{13} sont obtenues par (iv) du théorème 5.2.1.2. □

Liste des notations

$\mathbb{F}_q$	corps fini à q éléments, 1
F/K	corps de fonctions algébriques sur le corps K, 5
$\tilde{K}$	corps des constantes de F/K, 5
$g_F = g(F/K)$	genre du corps de fonctions algébriques F/K, 11
$\mathbb{P}_F$	ensemble des places de F, 6
t_P	un paramètre local pour la place P, 6
$\mathcal{O}_P$	anneau de valuation de la place P, 6
v_P	valuation relative à la place P, 6
F_P	corps de classe résiduel de la place P, 7
$x(P)$	classe résiduelle de $x \in \mathcal{O}_P$ dans F_P, 7
$\deg P$	degré de la place P, 7
$\mathrm{Div}(F)$	groupe des diviseurs de F, 8
$\mathrm{supp}\,\mathcal{D}$	support du diviseur $\mathcal{D}$, 8
$(x)_0, (x)_\infty, (x)$	diviseur des zéros, des pôles, principal de x, 9
$\mathrm{Princ}(F)$	groupe des diviseurs principaux de F, 9
$\mathrm{Cl}(F)$	groupe des classes de diviseurs de F, 9
$\mathrm{Cl}^n(F)$	ensemble des classes de diviseurs de degré n de F, 10
$\mathcal{D} \sim \mathcal{D}'$	diviseurs équivalents, 9
$\deg \mathcal{D}$	degré du diviseur $\mathcal{D}$, 9
$\mathrm{Div}^0(F)$	groupe des diviseurs de degré zéro de F, 9
$\mathrm{Cl}^0(F/\mathbb{F}_q)$	groupe des classes de diviseurs de degré 0 de $F/\mathbb{F}_q$, 9
h_F	cardinal du groupe $\mathrm{Cl}^0(F/\mathbb{F}_q)$, 10
$\mathcal{L}(\mathcal{D})$	espace de Riemann-Roch associé au diviseur $\mathcal{D}$, 10
$\ell(\mathcal{D}) = \dim \mathcal{D}$	dimension du diviseur $\mathcal{D}$, 10
$i(\mathcal{D})$	indice de spécialité du diviseur $\mathcal{D}$, 11
$\mathbb{A}_k$	ensemble des diviseurs effectifs de degré k, 12
A_k	nombre de diviseurs effectifs de degré k, 13
$N = N(F/K)$	nombre de places de degré 1 dans F/K, 15
$N_r = N(F_r/\mathbb{F}_{q^r})$	nombre de places de degré 1 dans l'extension du corps des constantes de degré r de $F/\mathbb{F}_q$, 15
$B_k = B_k(F/K)$	nombre de places de degré k dans F/K, 16
$N_q(g)$	nombre maximal de places rationnelles pour un corps de fonctions de genre g, 17
$A(q)$	constante d'Ihara, 17
$\mu_F(\mathcal{A})$	complexité bilinéaire de la multiplication dans $\mathcal{A}$ sur F, 29
$\mu_F^{\mathrm{sym}}(\mathcal{A})$	complexité bilinéaire symétrique de la multiplication dans $\mathcal{A}$ sur F, 29

$\mu_q(n)$	complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, 29
$\mu_q^{\mathrm{sym}}(n)$	complexité bilinéaire symétrique de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, 29
$\mu_q(m,l)$	complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^m}[t]/(t^l)$ sur $\mathbb{F}_q$, 29
$\mu_q^{\mathrm{sym}}(m,l)$	complexité bilinéaire symétrique de la multiplication dans $\mathbb{F}_{q^m}[t]/(t^l)$ sur $\mathbb{F}_q$, 29
m_q	borne asymptotique inférieure de la complexité bilinéaire de la multiplication dans les extensions finies de $\mathbb{F}_q$, 33
m_q^{sym}	borne asymptotique inférieure de la complexité bilinéaire symétrique de la multiplication dans les extensions finies de $\mathbb{F}_q$, 32
M_q	borne asymptotique supérieure de la complexité bilinéaire de la multiplication dans les extensions finies de $\mathbb{F}_q$, 33
M_q^{sym}	borne asymptotique supérieure de la complexité bilinéaire symétrique de la multiplication dans les extensions finies de $\mathbb{F}_q$, 32
$\Delta g_{k,s}$ (resp. Δg_k)	différence $g_{k,s+1} - g_{k,s}$ (resp. $g_{k+1} - g_k$) entre les genres de deux étages consécutifs d'une tour, 50

Bibliographie

[Arn06] N. Arnaud – « Évaluations dérivées, multiplication dans les corps finis et codes correcteurs », Thèse, Université de la Méditerranée, Institut de Mathématiques de Luminy, 2006.

[Bal99] S. Ballet – « Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$ », *Finite Fields and Their Applications* **5** (1999), p. 364–377.

[Bal03] — , « Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of $\mathbb{F}_q$ », *Finite Fields and Their Applications* **9** (2003), p. 472–478.

[Bal08a] — , « A note on the tensor rank of the multiplication in certain finite fields », in *Algebraic geometry and its applications, Proceedings of the first SAGA conference* (Hackensack, NJ), Number theory and its applications, World Sci. Publ., 2008, p. 332–342.

[Bal08b] — , « On the tensor rank of the multiplication in the finite fields », *Journal of Number Theory* **128** (2008), p. 1795–1806.

[BC04] S. Ballet & J. Chaumine – « On the bounds of the bilinear complexity of multiplication in some finite fields », *Applicable Algebra in Engineering Communication and Computing* **15** (2004), p. 205–211.

[BCS97] P. Bürgisser, M. Clausen & A. Shokrollahi – *Algebraic complexity theory*, Grundlehren der mathematischen Wissenchaften, no. 315, Springer, 1997.

[BD78] R. W. Brockett & D. P. Dobkin – « On the optimal evaluation of a set of bilinear forms », *Linear Alg. Appl.* **19** (1978), p. 207–235.

[BD80] M. R. Brown & D. P. Dobkin – « An improved lower bound on polynomial multiplication », *IEEE Transactions on Computers* **29** (1980), no. 5, p. 337–340.

[BLB06] S. Ballet & D. Le Brigand – « On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$ », *Journal on Number Theory* **116** (2006), p. 293–310.

[BLBR09] S. Ballet, D. Le Brigand & R. Rolland – « On an application of the definition field descent of a tower of function fields », in *Proceedings of the Conference Arithmetic, Geometry and Coding Theory (AGCT 2005)*, vol. 21, Société Mathématique de France, sér. Séminaires et Congrès, 2009, p. 187–203.

[BP11] S. Ballet & J. Pieltant – « On the tensor rank of multiplication in any extension of $\mathbb{F}_2$ », *Journal of Complexity* **27** (2011), p. 230–245.

[BR04] S. Ballet & R. Rolland – « Multiplication algorithm in a finite field and tensor rank of the multiplication », *Journal of Algebra* **272** (2004), no. 1, p. 173–185.

[BR11] — , « Families of curves over any finite field attaining the generalized Drinfeld-Vladut bound », *Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. Nr.* (2011), p. 5–18.

[BRR10] S. Ballet, C. Ritzenthaler & R. Rolland – « On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$ », *Acta Arithmetica* **143** (2010), no. 4, p. 377–392.

[Cas10] I. Cascudo – « On asymptotically good strongly multiplicative linear secret sharing », Thèse, University of Oviedo, 2010.

[CC87] D. Chudnovsky & G. Chudnovsky – « Algebraic complexities and algebraic curves over finite fields », in *Proceedings of the National Academy of Sciences*, vol. 84, April 1987, p. 1739–1743.

[CC88] — , « Algebraic complexities and algebraic curves over finite fields », *Journal of Complexity* **4** (1988), p. 285–316.

[CCXY12] I. Cascudo, R. Cramer, C. Xing & A. Yang – « Asymptotic bounds for multiplication complexity in the extensions of small finite fields », *IEEE Transactions on Information Theory* (2012).

[Cha06] J. Chaumine – « On the bilinear complexity of multiplication in small finite fields », *Comptes Rendus de l'Académie des Sciences de Paris* **I** (2006), no. 343, p. 265–266.

[CÖ08] M. Cenk & F. Özbudak – « Efficient multiplication in $\mathbb{F}_{3^{lm}}$, $m \geq 1$ and $5 \leq l \leq 18$ », in *Progress in Cryptology – AFRICACRYPT 2008* (S. Vaudenay, éd.), Lecture Notes in Computer Science, vol. 5023, 2008, p. 406–414.

[CÖ10] — , « On multiplication in finite fields », *Journal of Complexity* **26** (2010), no. 2, p. 172–186.

[DFK+97] M. Daberkow, C. Fieker, J. Klüners, M. E. Pohst, R. Katherine & K. Wildanger – « KANT V4 », *Journal of Symbolic Computation* **24** (1997), p. 267–283.

[dG83] H. de Groote – « Characterization of division algebras of minimal rank and the structure of their algorithm varieties », *SIAM Journal on Computing* **12** (1983), no. 1, p. 101–117.

[FZ77] C. Fiduccia & Y. Zalcstein – « Algebras having linear multiplicative complexities », *Journal of the ACM* **24** (1977), no. 2, p. 311–331.

[GS95] A. Garcia & H. Stichtenoth – « A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound », *Inventiones Mathematicae* **121** (1995), p. 211–222.

[GSBB12] A. Garcia, H. Stichtenoth, A. Bassa & P. Beelen – « Towers of Function Fields over Non-prime Finite Fields », *http://arxiv.org/abs/1202.5922* (2012).

[GSR03] A. Garcia, H. Stichtenoth & H.-G. Rück – « On tame towers over finite fields », *Journal fur die reine und angewandte Mathematik* **557** (2003), p. 53–80.

[Iha81] Y. Ihara – « Some remarks on the number of rational points of algebraic curves over finite fields », *Journal of the Faculty of Science. University of Tokyo. Section IA. Mathematics* **28** (1981), p. 721–724.

[KO63] A. A. Karatsuba & Y. Ofman – « Multiplication of multidigit numbers on automata », *Soviet Physics Doklady* **7** (1963), p. 595.

[NX96] H. Niederreiter & C. Xing – « Low-discrepancy sequences and global function fields with many rational places », *Finite Fields and Their Applications* **2** (1996), p. 241–273.

[Ran12] H. Randriambololona – « Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method », *Journal of Complexity* **28** (2012), p. 489–517.

[Sho92] A. Shokrollahi – « Optimal algorithms for multiplication in certain finite fields using algebraic curves », *SIAM Journal on Computing* **21** (1992), no. 6, p. 1193–1198.

[Sti08] H. Stichtenoth – *Algebraic function fields and codes*, second éd., Graduate Texts in Mathematics, no. 254, Springer, 2008.

[STV92] I. Shparlinski, M. Tsfasman & S. Vlăduţ – « Curves with many points and multiplication in finite fields », in *Coding Theory and Algebraic Geometry* (Berlin) (H. Stichtenoth & M. Tsfasman, éds.), Lectures Notes in Mathematics, no. 1518, Springer-Verlag, 1992, Proceedings of AGCT-3 Conference, June 17-21, 1991, Luminy, p. 145–169.

[Too63] A. Toom – « The complexity of a scheme of functional elements realizing the multiplication of integers », *Soviet Mathematics Doklady* **3** (1963), p. 714–716, Translations of Doklady Akademie Nauk S.S.S.R.

[Wat69] W. C. Waterhouse – « Abelian Varieties over Finite Fields », *Ann. Scient. Éc. Norm. Sup.* **4** (1969), p. 521–560.

[Win77] S. Winograd – « Some bilinear forms whose multiplicative complexity depends on the field of constants », *Mathematical Systems Theory* **10** (1977), p. 169–180.

[Win79] — , « On multiplication in algebraic extension fields », *Theoretical Computer Science* **8** (1979), p. 359–377.

Résumé : On s'intéresse dans cette thèse à la détermination du rang de tenseur de la multiplication dans $\mathbb{F}_{q^n}$, l'extension de degré n du corps fini $\mathbb{F}_q$; ce rang de tenseur correspond en particulier à la complexité bilinéaire de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Dans cette optique, on présente les différentes évolutions de l'algorithme de type évaluation-interpolation introduit en 1987 par D.V. et G.V. Chudnovsky et qui a permis d'établir que le rang de tenseur de la multiplication dans $\mathbb{F}_{q^n}$ était linéaire en n. Cet algorithme en fournit désormais les meilleures bornes connues dans le cas d'extensions de degré grand relativement au cardinal du corps de base — le cas des petites extensions étant bien connu. Afin d'obtenir des bornes uniformes en le degré de l'extension, il est nécessaire, pour chaque n, de déterminer un corps de fonctions algébriques qui convienne pour appliquer l'algorithme pour $\mathbb{F}_{q^n}$, c'est-à-dire qui ait suffisamment de places de petit degré relativement à son genre g et pour lequel on puisse établir l'existence de diviseurs ayant certaines propriétés, notamment des diviseurs non-spéciaux de degré $g-1$ ou de dimension nulle et de degré aussi près de $g-1$ que possible ; c'est pourquoi les tours de corps de fonctions sont d'un intérêt considérable. En particulier, on s'intéresse ici à l'étude des tours de Garcia-Stichtenoth d'extensions d'Artin-Schreier et de Kummer qui atteignent la borne de Drinfeld-Vlăduţ. En dégageant des propriétés de ces tours, notamment par l'utilisation de techniques de descente du corps de définition associées à l'utilisation de développements locaux selon un élément primitif de places de petit degré, on obtient, à partir d'une méthode générale formalisée ici, de nouvelles bornes uniformes, symétriques et asymétriques, pour les extensions finies de $\mathbb{F}_{q^2}$, $\mathbb{F}_q$, $\mathbb{F}_{p^2}$, $\mathbb{F}_p$, et notamment les meilleures bornes actuellement connues pour le rang de tenseur de la multiplication dans $\mathbb{F}_{2^n}$. On déduit alors de certaines d'entre elles de bonnes bornes asymptotiques.

Mots-clés : Rang de tenseur de la multiplication, complexité bilinéaire, corps finis, tours de corps de fonctions algébriques, algorithme de type Chudnovsky.

Title: Towers of algebraic function fields and tensor rank of multiplication in finite fields.

Abstract: In this thesis, we focus on the determination of the tensor rank of multiplication in $\mathbb{F}_{q^n}$, the degree n extension of the finite field $\mathbb{F}_q$, which corresponds to the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. To this end, we describe the various successive improvements to the evaluation-interpolation algorithm introduced in 1987 by D.V. and G.V. Chudnovsky which shows the linearity of the tensor rank of multiplication in $\mathbb{F}_{q^n}$ with respect to n. This algorithm gives the best known bounds for large degree extensions relative to the cardinality of the base field (the case when the degree of the extension is small is well known). In order to obtain uniform bounds, we need to determine, for each n, a suitable algebraic function field for the algorithm on $\mathbb{F}_{q^n}$, namely a function field with sufficiently many places of small degree relative to its genus g and for which we can prove the existence of divisors with some good properties such as non-special divisors of degree $g-1$ or zero-dimensional divisors with degree as close to $g-1$ as possible; these conditions lead us to consider towers of algebraic function fields. In particular, we are interested in the study of Garcia-Stichtenoth towers of Artin-Schreier and Kummer extensions which attain the Drinfeld-Vlăduţ bound. By establishing some properties on these towers, and using field definition descent techniques and local expansion of functions at places of relatively small degree, we obtain, from a general method which is described here, new symmetric and asymmetric uniform bounds for finite extensions of $\mathbb{F}_{q^2}$, $\mathbb{F}_q$, $\mathbb{F}_{p^2}$, $\mathbb{F}_p$; in particular, we obtain the best actual known bounds for the tensor rank of multiplication in $\mathbb{F}_{2^n}$. We also deduce from this some good asymptotic bounds.

Keywords: Tensor rank of multiplication, bilinear complexity, finite fields, towers of algebraic function fields, Chudnovsky type algorithm.