Algorithme de Chudnovsky-Chudnovsky et diviseurs non-spéciaux de degré $g-1$

Julia Pieltant
LTCI – Paris
CNRS & Telecom ParisTech
Labex Mathématiques Hadamard

pieltant@enst.fr
http://www.lix.polytechnique.fr/∼pieltant

GT BaC, 7 juillet 2016

Plan

Complexité de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$:

Nombre minimal d'opérations élémentaires dans $\mathbb{F}_q$ nécessaires pour calculer le produit de deux éléments quelconques $x, y \in \mathbb{F}_{q^n}$.

Complexité de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$:

Nombre minimal d'opérations élémentaires dans $\mathbb{F}_q$ nécessaires pour calculer le produit de deux éléments quelconques $x, y \in \mathbb{F}_{q^n}$.

Types d'opérations :

- addition : $(a, b) \mapsto a + b$ où $a, b \in \mathbb{F}_q$,
- multiplication scalaire : $x_i \mapsto a \cdot x_i$ où $a, x_i \in \mathbb{F}_q$, et a est une constante,
- multiplication non-scalaire ou bilinéaire : $(x_i, y_j) \mapsto x_i \cdot y_j$ où $x_i, y_j \in \mathbb{F}_q$ dépendent des éléments x et y de $\mathbb{F}_{q^n}$ dont on effectue le produit.

Complexité de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$:

Nombre minimal d'opérations élémentaires dans $\mathbb{F}_q$ nécessaires pour calculer le produit de deux éléments quelconques $x, y \in \mathbb{F}_{q^n}$.

Types d'opérations :

- ✗ addition : $(a, b) \mapsto a + b$ où $a, b \in \mathbb{F}_q$,
- ✗ multiplication scalaire : $x_i \mapsto a \cdot x_i$ où $a, x_i \in \mathbb{F}_q$, et a est une constante,
- ✔ multiplication non-scalaire ou bilinéaire : $(x_i, y_j) \mapsto x_i \cdot y_j$ où $x_i, y_j \in \mathbb{F}_q$ dépendent des éléments x et y de $\mathbb{F}_{q^n}$ dont on effectue le produit.

Le nombre minimal 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 $\mathbb{F}_q$**, et notée $\mu_q(n)$.

Expression classique du produit d'éléments de $\mathbb{F}_{q^n}$

Soit $\mathcal{B} := (e_1, \ldots, e_n)$ une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.

On définit

$$e_i e_j := \sum_{k=1}^{n} a_{i,j,k} e_k \text{ pour tous } i, j \in \{1, \ldots, n\}.$$

Soient $x = \sum_{i=1}^{n} x_i e_i$ et $y = \sum_{i=1}^{n} y_i e_i$ deux éléments de $\mathbb{F}_{q^n}$, on a

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

Expression classique du produit d'éléments de $\mathbb{F}_{q^n}$

Soit $\mathcal{B} := (e_1, \ldots, e_n)$ une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.

On définit

$$e_i e_j := \sum_{k=1}^{n} a_{i,j,k} e_k \text{ pour tous } i, j \in \{1, \ldots, n\}.$$

Soient $x = \sum_{i=1}^{n} x_i e_i$ et $y = \sum_{i=1}^{n} y_i e_i$ deux éléments de $\mathbb{F}_{q^n}$, on a

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

Nombre d'opérations :

- n^2 multiplications bilinéaires,
- n^3 multiplications scalaires,
- $n(n-1)(n+1)$ additions d'éléments de $\mathbb{F}_q$.

Plus généralement...

On considère les coordonnées des éléments de $\mathbb{F}_{q^n}$ dans une base fixée :

$$x, y \in \mathbb{F}_{q^n} \quad \rightsquigarrow \quad (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{F}_q^n$$

- Les multiplications bilinéaires sont effectuées sur des C.L. des coordonnées :

$$\begin{cases} m_1 & := & A_1(x_1, \ldots, x_n) \times B_1(y_1, \ldots, y_n) \\ \vdots & & \\ m_\lambda & := & A_\lambda(x_1, \ldots, x_n) \times B_\lambda(y_1, \ldots, y_n) \end{cases}$$

avec $A_1, \ldots, A_\lambda, B_1, \ldots, B_\lambda \in \mathcal{L}(\mathbb{F}_q^n; \mathbb{F}_q)$.

- On retrouve les coordonnées du produit xy :

$$\big(C_1(m_1, \ldots, m_\lambda), \ldots, C_n(m_1, \ldots, m_\lambda)\big) \quad \text{où} \quad C_1, \ldots, C_n \in \mathcal{L}(\mathbb{F}_q^\lambda; \mathbb{F}_q)$$

Soit t le **tenseur de la multiplication** dans $\mathbb{F}_{q^n}$:

$$\forall\, x, y \in \mathbb{F}_{q^n},\ \ t(x \otimes y) = xy.$$

On considère une **décomposition de t en λ tenseurs élémentaires**, c-à-d on considère $a_i, b_i \in \mathbb{F}_{q^n}^{\star}$ et $c_i \in \mathbb{F}_{q^n}$ tels que tous $x, y \in \mathbb{F}_{q^n}$, on a

$$xy = t(x \otimes y) = \sum_{i=1}^{\lambda} a_i(x) b_i(y) c_i. \qquad (1)$$

Toute expression de type (1) est appelée **algorithme de multiplication bilinéaire** $\mathscr{A}$. Sa **complexité** λ est notée $\mu(\mathscr{A})$.

Soit t le **tenseur de la multiplication** dans $\mathbb{F}_{q^n}$:

$$\forall\, x, y \in \mathbb{F}_{q^n},\ \ t(x \otimes y) = xy.$$

On considère une **décomposition de t en λ tenseurs élémentaires**, c-à-d on considère $a_i, b_i \in \mathbb{F}_{q^n}^{\star}$ et $c_i \in \mathbb{F}_{q^n}$ tels que tous $x, y \in \mathbb{F}_{q^n}$, on a

$$xy = t(x \otimes y) = \sum_{i=1}^{\lambda} a_i(x) b_i(y) c_i. \qquad (1)$$

Toute expression de type (1) est appelée **algorithme de multiplication bilinéaire** $\mathscr{A}$. Sa **complexité** λ est notée $\mu(\mathscr{A})$.

Ainsi

$$\mu_q(n) := \min_{\mathscr{A}} \mu(\mathscr{A})$$

où $\mathscr{A}$ parcourt l'ensemble des algorithmes de multiplication bilinéaire dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.

Complexité bilinéaire symétrique

Définition

Un algorithme de multiplication bilinéaire est dit **symétrique** *s'il admet une expression de la forme :*

$$xy = \sum_{i=1}^{\lambda} a_i(x)a_i(y)c_i. \tag{2}$$

pour tous $x, y \in \mathbb{F}_{q^n}$, *avec* $a_i \in \mathbb{F}_{q^n}^{\star}$ *et* $c_i \in \mathbb{F}_{q^n}$

On définit la **complexité bilinéaire symétrique** de la multiplication dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ en posant :

$$\mu_q^{\text{sym}}(n) := \min_{\mathscr{A}^{\text{sym}}} \mu(\mathscr{A}^{\text{sym}})$$

où $\mathscr{A}^{\text{sym}}$ parcourt l'ensemble des algorithmes symétriques de multiplication bilinéaire dans $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.

Rq. $\mu_q(n) \leq \mu_q^{\text{sym}}(n)$

Algorithme de Karatsuba

Multiplication de deux polynômes de degré 1, à coefficients dans un corps K :

$$U(X) = a_0 + a_1 X \qquad V(X) = b_0 + b_1 X$$

Algorithme de Karatsuba

Multiplication de deux polynômes de degré 1, à coefficients dans un corps K :

$$U(X) = a_0 + a_1 X \qquad V(X) = b_0 + b_1 X$$

- Évaluations en $0, 1, \infty$:

$$\begin{array}{lll} U(0) = a_0 & U(1) = a_0 + a_1 & U(\infty) = a_1 \\ V(0) = b_0 & V(1) = b_0 + b_1 & V(\infty) = b_1 \end{array}$$

Algorithme de Karatsuba

Multiplication de deux polynômes de degré 1, à coefficients dans un corps K :

$$U(X) = a_0 + a_1 X \qquad V(X) = b_0 + b_1 X$$

- Évaluations en $0, 1, \infty$:

$$\begin{array}{lll} U(0) = a_0 & U(1) = a_0 + a_1 & U(\infty) = a_1 \\ V(0) = b_0 & V(1) = b_0 + b_1 & V(\infty) = b_1 \end{array}$$

- Multiplications bilinéaires :

$$m_1 = U(0)V(0) \qquad m_2 = U(1)V(1) \qquad m_3 = U(\infty)V(\infty)$$

Algorithme de Karatsuba

Multiplication de deux polynômes de degré 1, à coefficients dans un corps K :

$$U(X) = a_0 + a_1 X \qquad V(X) = b_0 + b_1 X$$

- Évaluations en $0, 1, \infty$:

$$\begin{array}{lcl} U(0) = a_0 & \quad & U(1) = a_0 + a_1 \\ V(0) = b_0 & & V(1) = b_0 + b_1 \end{array} \qquad U(\infty) = a_1 \quad V(\infty) = b_1$$

- Multiplications bilinéaires :

$$m_1 = U(0)V(0) \qquad m_2 = U(1)V(1) \qquad m_3 = U(\infty)V(\infty)$$

- Détermination des coeff. du produit $U(X)V(X) = p_0 + p_1 X + p_2 X^2$:

$$p_0 = m_1 \qquad p_1 = m_2 - m_1 - m_3 \qquad p_2 = m_3$$

Algorithme de Karatsuba

Multiplication de deux polynômes de degré 1, à coefficients dans un corps K :

$$U(X) = a_0 + a_1 X \qquad V(X) = b_0 + b_1 X$$

- Évaluations en $0, 1, \infty$:

$$\begin{array}{lll} U(0) = a_0 & U(1) = a_0 + a_1 & U(\infty) = a_1 \\ V(0) = b_0 & V(1) = b_0 + b_1 & V(\infty) = b_1 \end{array}$$

- Multiplications bilinéaires :

$$m_1 = U(0)V(0) \qquad m_2 = U(1)V(1) \qquad m_3 = U(\infty)V(\infty)$$

- Détermination des coeff. du produit $U(X)V(X) = p_0 + p_1 X + p_2 X^2$:

$$p_0 = m_1 \qquad p_1 = m_2 - m_1 - m_3 \qquad p_2 = m_3$$

Complexité : 3 multiplications bilinéaires et 4 additions.

Algorithme de Karatsuba

Multiplication de deux polynômes de degré 1, à coefficients dans un corps K :

$$U(X) = a_0 + a_1 X \qquad V(X) = b_0 + b_1 X$$

- Évaluations en $0, 1, \infty$:

$$\begin{array}{lll} U(0) = a_0 & U(1) = a_0 + a_1 & U(\infty) = a_1 \\ V(0) = b_0 & V(1) = b_0 + b_1 & V(\infty) = b_1 \end{array}$$

- Multiplications bilinéaires :

$$m_1 = U(0)V(0) \qquad m_2 = U(1)V(1) \qquad m_3 = U(\infty)V(\infty)$$

- Détermination des coeff. du produit $U(X)V(X) = p_0 + p_1 X + p_2 X^2$:

$$p_0 = m_1 \qquad p_1 = m_2 - m_1 - m_3 \qquad p_2 = m_3$$

Complexité : 3 multiplications bilinéaires et 4 additions.

Généralisation au produit de deux polynômes de degré n

Complexité : $O\left(n^{\log_2(3)}\right)$ multiplications bilinéaires et $O(n)$ additions.

Un premier pas vers l'algorithme de Chudnovsky-Chudnovsky

Algorithme de Karatsuba pour les polynômes de degré 1 $\leftrightsquigarrow$ Évaluations sur $\{0, 1, \infty\} \in \mathrm{P}^1(K)$

Un premier pas vers l'algorithme de Chudnovsky-Chudnovsky

Algorithme de Karatsuba pour les polynômes de degré 1 $\leftrightsquigarrow$ Évaluations sur $\{0, 1, \infty\} \in \mathrm{P}^1(K)$

Rappel.

- On note $\mathrm{P}^1(\overline{\mathbb{F}_q})$ la **droite projective** sur $\overline{\mathbb{F}_q}$:

$$\mathrm{P}^1(\overline{\mathbb{F}_q}) := \left\{(x, y) \in \mathbb{A}^2(\overline{\mathbb{F}_q}) \backslash \{(0,0)\}\right\} / \sim$$

où $\sim$ est la relation d'équivalence définie par la colinéarité.

- C'est une courbe algébrique de genre 0 avec $q+1$ points rationnels :

$$\mathrm{P}^1(\mathbb{F}_q) = \left\{(x:1) \;\middle|\; x \in \mathbb{F}_q\right\} \cup \{\infty\}.$$

Un premier pas vers l'algorithme de Chudnovsky-Chudnovsky

Algorithme de Karatsuba pour les polynômes de degré 1 $\leftrightsquigarrow$ Évaluations sur $\{0, 1, \infty\} \in \mathrm{P}^1(K)$

Rappel.

- On note $\mathrm{P}^1(\overline{\mathbb{F}_q})$ la **droite projective** sur $\overline{\mathbb{F}_q}$:

$$\mathrm{P}^1(\overline{\mathbb{F}_q}) := \left\{(x, y) \in \mathbb{A}^2(\overline{\mathbb{F}_q}) \backslash \{(0,0)\}\right\} / \sim$$

  où $\sim$ est la relation d'équivalence définie par la colinéarité.

- C'est une courbe algébrique de genre 0 avec $q+1$ points rationnels :

$$\mathrm{P}^1(\mathbb{F}_q) = \left\{(x:1) \;\middle|\; x \in \mathbb{F}_q\right\} \cup \{\infty\}.$$

Idée. **Généraliser** la méthode de Karatsuba en faisant **plus d'évaluations** sur $\mathrm{P}^1(\mathbb{F}_q)$ lorsque $q > 2$.

Multiplication de polynômes et multiplication dans $\mathbb{F}_{q^n}$ (I)

- Soit $P(X) \in \mathbb{F}_q[X]$ unitaire, de degré n, irréductible sur $\mathbb{F}_q$, alors :

$$\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/\big(P(X)\big)$$

et donc $\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\omega)$ avec ω une racine de $P(X)$.

Multiplication de polynômes et multiplication dans $\mathbb{F}_{q^n}$ (I)

- Soit $P(X) \in \mathbb{F}_q[X]$ unitaire, de degré n, irréductible sur $\mathbb{F}_q$, alors :

$$\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/\big(P(X)\big)$$

et donc $\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\omega)$ avec ω une racine de $P(X)$.

$\rightsquigarrow \mathcal{B} = (1, \omega, \omega^2, \ldots, \omega^{n-1})$ est une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$.

Multiplication de polynômes et multiplication dans $\mathbb{F}_{q^n}$ (I)

- Soit $P(X) \in \mathbb{F}_q[X]$ unitaire, de degré n, irréductible sur $\mathbb{F}_q$, alors :

$$\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/\big(P(X)\big)$$

et donc $\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\omega)$ avec ω une racine de $P(X)$.

$\rightsquigarrow \mathcal{B} = (1, \omega, \omega^2, \ldots, \omega^{n-1})$ est une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$.

- Pour connaître le produit deux éléments $x, y \in \mathbb{F}_{q^n}$ t.q.

$$x = \sum_{i=0}^{n-1} a_i \omega^i \qquad \text{et} \qquad y = \sum_{i=0}^{n-1} b_i \omega^i$$

Multiplication de polynômes et multiplication dans $\mathbb{F}_{q^n}$ (I)

- Soit $P(X) \in \mathbb{F}_q[X]$ unitaire, de degré n, irréductible sur $\mathbb{F}_q$, alors :

$$\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(P(X))$$

et donc $\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\omega)$ avec ω une racine de $P(X)$.

$\rightsquigarrow \mathcal{B} = (1, \omega, \omega^2, \ldots, \omega^{n-1})$ est une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$.

- Pour connaître le produit deux éléments $x, y \in \mathbb{F}_{q^n}$ t.q.

$$x = \sum_{i=0}^{n-1} a_i \omega^i \qquad \text{et} \qquad y = \sum_{i=0}^{n-1} b_i \omega^i$$

il suffit de déterminer les coefficients du produit des deux polynômes

$$A(X) = \sum_{i=0}^{n-1} a_i X^i \qquad \text{et} \qquad B(X) = \sum_{i=0}^{n-1} b_i X^i$$

car

$$xy = A(\omega)B(\omega) = (AB)(\omega).$$

Multiplication de polynômes et multiplication dans $\mathbb{F}_{q^n}$ (II)

Hypothèse. $|\mathrm{P}^1(\mathbb{F}_q)| \geq \deg\big(A(X)B(X)\big)+1$ i.e. $q+1 \geq 2n-1$

On choisit $\mathcal{S} := \{P_1, \ldots, P_{2n-1}\} \subseteq \mathrm{P}^1(\mathbb{F}_q)$.

Multiplication de polynômes et multiplication dans $\mathbb{F}_{q^n}$ (II)

Hypothèse. $|\mathrm{P}^1(\mathbb{F}_q)| \geq \deg\big(A(X)B(X)\big)+1$ i.e. $q+1 \geq 2n-1$

On choisit $\mathcal{S} := \{P_1, \ldots, P_{2n-1}\} \subseteq \mathrm{P}^1(\mathbb{F}_q)$.

1. On détermine les évaluations $A(P_i)$ et $B(P_i)$ en tous les points P_i de $\mathcal{S}$.
2. On calcule $(AB)(P_i) = A(P_i)B(P_i)$, pour tout $P_i \in \mathcal{S}$.
3. Par interpolation, on retrouve les coefficients de $(AB)(X)$, et donc le produit $xy = (AB)(\omega)$ dans la base $\mathcal{B}$.

Multiplication de polynômes et multiplication dans $\mathbb{F}_{q^n}$ (II)

Hypothèse. $|\mathrm{P}^1(\mathbb{F}_q)| \geq \deg\big(A(X)B(X)\big)+1$ i.e. $q+1 \geq 2n-1$

On choisit $\mathcal{S} := \{P_1, \ldots, P_{2n-1}\} \subseteq \mathrm{P}^1(\mathbb{F}_q)$.

1. On détermine les évaluations $A(P_i)$ et $B(P_i)$ en tous les points P_i de $\mathcal{S}$.
2. On calcule $(AB)(P_i) = A(P_i)B(P_i)$, pour tout $P_i \in \mathcal{S}$.
3. Par interpolation, on retrouve les coefficients de $(AB)(X)$, et donc le produit $xy = (AB)(\omega)$ dans la base $\mathcal{B}$.

Complexité bilinéaire : $|\mathcal{S}| = 2n-1$ multiplications.

Conséquence. Si $n \leq \dfrac{q}{2}+1$, alors $\mu_q^{\mathrm{sym}}(n) \leq 2n-1$.

Résultats connus pour les extensions de « petit » degré

Théorème (Winograd (1979) & de Groote (1983))

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

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

De plus,

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

Théorème (Shokrollahi (1992))

Si $n \leq \frac{1}{2}(q+1+\epsilon(q))$, alors

$$\mu_q^{\text{sym}}(n) \leq 2n$$

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

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

Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques défini sur $\mathbb{F}_q$ de genre g avec :

- Q une place de degré n,
- $\mathscr{P} := \{P_1, \ldots, P_N\}$ un ensemble de N places rationnelles,
- $\mathcal{D}$ un diviseur effectif tel que $\mathrm{supp}(\mathcal{D}) \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

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

Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques défini sur $\mathbb{F}_q$ de genre g avec :

- Q une place de degré n,
- $\mathscr{P} := \{P_1, \ldots, P_N\}$ un ensemble de N places rationnelles,
- $\mathcal{D}$ un diviseur effectif tel que $\mathrm{supp}(\mathcal{D}) \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

Si on a

(i) un morphisme de $\mathbb{F}_q$-espaces vectoriels **surjectif**

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

(ii) un morphisme de $\mathbb{F}_q$-espaces vectoriels **injectif**

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

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

Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques défini sur $\mathbb{F}_q$ de genre g avec :

- Q une place de degré n,
- $\mathscr{P} := \{P_1, \ldots, P_N\}$ un ensemble de N places rationnelles,
- $\mathcal{D}$ un diviseur effectif tel que $\mathrm{supp}(\mathcal{D}) \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

Si on a

(i) un morphisme de $\mathbb{F}_q$-espaces vectoriels **surjectif**

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

(ii) un morphisme de $\mathbb{F}_q$-espaces vectoriels **injectif**

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

alors

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

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

Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques défini sur $\mathbb{F}_q$ de genre g avec :

- Q une place de degré n,
- $\mathscr{P} := \{P_1, \ldots, P_N\}$ un ensemble de N places rationnelles,
- $\mathcal{D}$ un diviseur effectif tel que $\operatorname{supp}(\mathcal{D}) \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

Si on a

(i) un morphisme de $\mathbb{F}_q$-espaces vectoriels **surjectif**

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

(ii) un morphisme de $\mathbb{F}_q$-espaces vectoriels **injectif**

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

alors

$$\mu_q^{\mathrm{sym}}(n) \leq \operatorname{rk} \mathrm{Ev}_{\mathscr{P}} \leq N.$$

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

Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques défini sur $\mathbb{F}_q$ de genre g avec :

- Q une place de degré n,
- $\mathscr{P} := \{P_1, \ldots, P_N\}$ un ensemble de N places de degré quelconque,
- $\mathcal{D}$ un diviseur effectif tel que $\operatorname{supp}(\mathcal{D}) \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

Si on a

(i) un morphisme de $\mathbb{F}_q$-espaces vectoriels **surjectif**

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

(ii) un morphisme de $\mathbb{F}_q$-espaces vectoriels **injectif**

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

alors

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

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

Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques défini sur $\mathbb{F}_q$ de genre g avec :

- Q une place de degré n,
- $\mathscr{P} := \{P_1, \ldots, P_N\}$ un ensemble de N places de degré quelconque,
- $\mathcal{D}$ un diviseur effectif tel que $\mathrm{supp}(\mathcal{D}) \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

Si on a

(i) un morphisme de $\mathbb{F}_q$-espaces vectoriels **surjectif**

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

(ii) un morphisme de $\mathbb{F}_q$-espaces vectoriels **injectif**

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

alors

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

Une astuce avec des places de degré 2 :

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i) = 3N$$

$$\mathrm{Ev}_{\mathscr{P}}(f) = \big(f(P_1), f(P_2), \ldots, f(P_N)\big) = \big((a_{P_1}, b_{P_1}), (a_{P_2}, b_{P_2}), \ldots, (a_{P_N}, b_{P_N})\big)$$
$$\mathrm{Ev}_{\mathscr{P}}(g) = \big(g(P_1), g(P_2), \ldots, g(P_N)\big) = \big((\alpha_{P_1}, \beta_{P_1}), (\alpha_{P_2}, \beta_{P_2}), \ldots, (\alpha_{P_N}, \beta_{P_N})\big)$$

But : déterminer $\mathrm{Ev}_{\mathscr{P}}(fg) = \big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$

Une astuce avec des places de degré 2 :

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i) = 3N$$

$$\mathrm{Ev}_{\mathscr{P}}(f) = \big(f(P_1), f(P_2), \ldots, f(P_N)\big) = \big((a_{P_1}, b_{P_1}), (a_{P_2}, b_{P_2}), \ldots, (a_{P_N}, b_{P_N})\big)$$
$$\mathrm{Ev}_{\mathscr{P}}(g) = \big(g(P_1), g(P_2), \ldots, g(P_N)\big) = \big((\alpha_{P_1}, \beta_{P_1}), (\alpha_{P_2}, \beta_{P_2}), \ldots, (\alpha_{P_N}, \beta_{P_N})\big)$$

But : déterminer $\mathrm{Ev}_{\mathscr{P}}(fg) = \big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
. . . mais $\ell := \mathrm{rk}\,\mathrm{Ev}_{\mathscr{P}} < 2N$ coordonnées suffisent pour définir fg.

Problème : répartition parmis les couples (U_{P_i}, V_{P_i}) ?

Une astuce avec des places de degré 2 :

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i) = 3N$$

$$\mathrm{Ev}_{\mathscr{P}}(f) = \big(f(P_1), f(P_2), \ldots, f(P_N)\big) = \big((a_{P_1}, b_{P_1}), (a_{P_2}, b_{P_2}), \ldots, (a_{P_N}, b_{P_N})\big)$$
$$\mathrm{Ev}_{\mathscr{P}}(g) = \big(g(P_1), g(P_2), \ldots, g(P_N)\big) = \big((\alpha_{P_1}, \beta_{P_1}), (\alpha_{P_2}, \beta_{P_2}), \ldots, (\alpha_{P_N}, \beta_{P_N})\big)$$

But : déterminer $\mathrm{Ev}_{\mathscr{P}}(fg) = \big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
. . . mais $\ell := \mathrm{rk}\,\mathrm{Ev}_{\mathscr{P}} < 2N$ coordonnées suffisent pour définir fg.

Problème : répartition parmis les couples (U_{P_i}, V_{P_i}) ?

cas 1 : $\big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
complexité : 1, 5 mult. dans $\mathbb{F}_q$ par coord. $\quad\Longrightarrow\quad \mu_q^{\mathrm{sym}}(n) \leq \frac{3}{2}\ell < 3N$

Une astuce avec des places de degré 2 :

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i) = 3N$$

$$\mathrm{Ev}_{\mathscr{P}}(f) = \big(f(P_1), f(P_2), \ldots, f(P_N)\big) = \big((a_{P_1}, b_{P_1}), (a_{P_2}, b_{P_2}), \ldots, (a_{P_N}, b_{P_N})\big)$$
$$\mathrm{Ev}_{\mathscr{P}}(g) = \big(g(P_1), g(P_2), \ldots, g(P_N)\big) = \big((\alpha_{P_1}, \beta_{P_1}), (\alpha_{P_2}, \beta_{P_2}), \ldots, (\alpha_{P_N}, \beta_{P_N})\big)$$

But : déterminer $\mathrm{Ev}_{\mathscr{P}}(fg) = \big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
. . . mais $\ell := \mathrm{rk}\,\mathrm{Ev}_{\mathscr{P}} < 2N$ coordonnées suffisent pour définir fg.

Problème : répartition parmis les couples (U_{P_i}, V_{P_i}) ?

cas 1 : $\big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
complexité : 1, 5 mult. dans $\mathbb{F}_q$ par coord. $\Longrightarrow$ $\mu_q^{\mathrm{sym}}(n) \leq \frac{3}{2}\ell < 3N$

cas 2 : $\big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
complexité : 2 mult. dans $\mathbb{F}_q$ par coord. $\Longrightarrow$ $\mu_q^{\mathrm{sym}}(n) \leq 2N$

Une astuce avec des places de degré 2 :

$$\mu_q^{\mathrm{sym}}(n) \leq \sum_{i=1}^{N} \mu_q^{\mathrm{sym}}(\deg P_i) = 3N$$

$$\mathrm{Ev}_{\mathscr{P}}(f) = \big(f(P_1), f(P_2), \ldots, f(P_N)\big) = \big((a_{P_1}, b_{P_1}), (a_{P_2}, b_{P_2}), \ldots, (a_{P_N}, b_{P_N})\big)$$
$$\mathrm{Ev}_{\mathscr{P}}(g) = \big(g(P_1), g(P_2), \ldots, g(P_N)\big) = \big((\alpha_{P_1}, \beta_{P_1}), (\alpha_{P_2}, \beta_{P_2}), \ldots, (\alpha_{P_N}, \beta_{P_N})\big)$$

But : déterminer $\mathrm{Ev}_{\mathscr{P}}(fg) = \big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
. . . mais $\ell := \mathrm{rk}\,\mathrm{Ev}_{\mathscr{P}} < 2N$ coordonnées suffisent pour définir fg.

Problème : répartition parmis les couples (U_{P_i}, V_{P_i}) ?

cas 1 : $\big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
complexité : 1, 5 mult. dans $\mathbb{F}_q$ par coord. $\quad\Longrightarrow\quad \mu_q^{\mathrm{sym}}(n) \leq \frac{3}{2}\ell < 3N$

cas 2 : $\big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
complexité : 2 mult. dans $\mathbb{F}_q$ par coord. $\quad\Longrightarrow\quad \mu_q^{\mathrm{sym}}(n) \leq 2N$

cas 3 : $\big((U_{P_1}, V_{P_1}), (U_{P_2}, V_{P_2}), \ldots, (U_{P_N}, V_{P_N})\big)$
complexité : 2 mult. dans $\mathbb{F}_q$ par coord. isolée + 1.5 par coord. couplée
$\quad\Longrightarrow\quad \mu_q^{\mathrm{sym}}(n) \leq 2\widehat{N} + \frac{3}{2}\widehat{\ell}$ où $\widehat{N} + \frac{\widehat{\ell}}{2} < N$

$$\begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathscr{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

$$\begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathscr{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

(i) Ev_Q est surjectif **ssi** $\dim \mathcal{D} = n + \dim(\mathcal{D} - Q)$
ssi $\mathrm{i}(\mathcal{D}) = \mathrm{i}(\mathcal{D} - Q)$

$$\begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathscr{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

(i) Ev_Q est surjectif **ssi** $\dim \mathcal{D} = n + \dim(\mathcal{D} - Q)$
ssi $\mathrm{i}(\mathcal{D}) = \mathrm{i}(\mathcal{D} - Q)$

- on choisira $\mathcal{D}$ t.q. $\mathrm{i}(\mathcal{D} - Q) = 0$
- pour avoir $\dim \mathcal{D} = n$, il faut que $\deg(\mathcal{D} - Q) = g - 1$

$$\begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathscr{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

(i) Ev_Q est surjectif **ssi** $\dim \mathcal{D} = n + \dim(\mathcal{D} - Q)$
ssi $\mathrm{i}(\mathcal{D}) = \mathrm{i}(\mathcal{D} - Q)$

- on choisira $\mathcal{D}$ t.q. $\mathrm{i}(\mathcal{D} - Q) = 0$
- pour avoir $\dim \mathcal{D} = n$, il faut que $\deg(\mathcal{D} - Q) = g - 1$

Conséquence : $\deg \mathcal{D} = n + g - 1$

$$\begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathscr{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

(i) Ev_Q est surjectif **ssi** $\dim \mathcal{D} = n + \dim(\mathcal{D} - Q)$
ssi $\mathrm{i}(\mathcal{D}) = \mathrm{i}(\mathcal{D} - Q)$

- on choisira $\mathcal{D}$ t.q. $\mathrm{i}(\mathcal{D} - Q) = 0$
- pour avoir $\dim \mathcal{D} = n$, il faut que $\deg(\mathcal{D} - Q) = g - 1$

Conséquence : $\deg \mathcal{D} = n + g - 1$

(ii) $\mathrm{Ev}_{\mathscr{P}}$ est injectif **ssi** $\dim(2\mathcal{D} - \sum_{i=1}^{N} P_i) = 0$

$$\begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathscr{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

(i) Ev_Q est surjectif **ssi** $\dim \mathcal{D} = n + \dim(\mathcal{D} - Q)$
ssi $\mathrm{i}(\mathcal{D}) = \mathrm{i}(\mathcal{D} - Q)$

- on choisira $\mathcal{D}$ t.q. $\mathrm{i}(\mathcal{D} - Q) = 0$
- pour avoir $\dim \mathcal{D} = n$, il faut que $\deg(\mathcal{D} - Q) = g - 1$

Conséquence : $\deg \mathcal{D} = n + g - 1$

(ii) $\mathrm{Ev}_{\mathscr{P}}$ est injectif **ssi** $\dim(2\mathcal{D} - \sum_{i=1}^N P_i) = 0$

$\rightsquigarrow$ il suffit que $\sum_{i=1}^N \deg P_i > 2 \deg \mathcal{D}$

$$\begin{array}{ccc} \mathcal{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathcal{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

(i) Ev_Q est surjectif **ssi** $\dim \mathcal{D} = n + \dim(\mathcal{D} - Q)$
ssi $\mathrm{i}(\mathcal{D}) = \mathrm{i}(\mathcal{D} - Q)$

- on choisira $\mathcal{D}$ t.q. $\mathrm{i}(\mathcal{D} - Q) = 0$
- pour avoir $\dim \mathcal{D} = n$, il faut que $\deg(\mathcal{D} - Q) = g - 1$

Conséquence : $\deg \mathcal{D} = n + g - 1$

(ii) $\mathrm{Ev}_{\mathscr{P}}$ est injectif **ssi** $\dim(2\mathcal{D} - \sum_{i=1}^{N} P_i) = 0$

$\rightsquigarrow$ il suffit que $N \geq 2n + 2g - 1$

$$\begin{array}{ccc} \mathcal{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q} & \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array} \qquad \begin{array}{ccc} \mathcal{L}(2\mathcal{D}) & \xrightarrow{\mathrm{Ev}_{\mathscr{P}}} & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1),\ldots,f(P_N)\big) \end{array}$$

Théorème de Riemann-Roch : $\dim \mathcal{A} = \deg \mathcal{A} - g + 1 + \mathrm{i}(\mathcal{A})$

(i) Ev_Q est surjectif **ssi** $\dim \mathcal{D} = n + \dim(\mathcal{D} - Q)$
ssi $\mathrm{i}(\mathcal{D}) = \mathrm{i}(\mathcal{D} - Q)$

- on choisira $\mathcal{D}$ t.q. $\mathrm{i}(\mathcal{D} - Q) = 0$
- pour avoir $\dim \mathcal{D} = n$, il faut que $\deg(\mathcal{D} - Q) = g - 1$

Conséquence : $\deg \mathcal{D} = n + g - 1$

(ii) $\mathrm{Ev}_{\mathscr{P}}$ est injectif **ssi** $\dim(2\mathcal{D} - \sum_{i=1}^{N} P_i) = 0$

$\rightsquigarrow$ il suffit que $N \geq 2n + 2g - 1$

(i) + (ii) $\Longrightarrow$ $\mathrm{rk}\,\mathrm{Ev}_{\mathscr{P}} = \dim 2\mathcal{D} = 2n + g - 1$

Algorithme de Chudnovsky-Chudnovsky sur le corps de fonctions Hermitien

Soit $\mathrm{F}/\mathbb{F}_{q^2}$ le corps défini par : $\mathrm{F} := \mathbb{F}_{q^2}(x,y)$ où $y^q + y = x^{q+1}$.

Alors $g(\mathrm{F}) = \frac{q(q-1)}{2}$ et $N(\mathrm{F}) = q^2 + 1 + 2g(\mathrm{F})q = q^3 + 1$.

Algorithme de Chudnovsky-Chudnovsky sur le corps de fonctions Hermitien

Soit $\mathrm{F}/\mathbb{F}_{q^2}$ le corps défini par : $\mathrm{F} := \mathbb{F}_{q^2}(x,y)$ où $y^q + y = x^{q+1}$.

Alors $g(\mathrm{F}) = \frac{q(q-1)}{2}$ et $N(\mathrm{F}) = q^2 + 1 + 2g(\mathrm{F})q = q^3 + 1$.

Si $N(\mathrm{F}) \geq 2n + 2g(\mathrm{F}) - 1$ i.e. $n \leq \frac{1}{2}(q^3 - q^2 + q + 2)$

alors on peut appliquer l'algorithme de Chudnovsky-Chudnovsky sur le corps de fonctions $\mathrm{F}/\mathbb{F}_{q^2}$ pour multiplier dans $\mathbb{F}_{q^{2n}}$.

Algorithme de Chudnovsky-Chudnovsky sur le corps de fonctions Hermitien

Soit $\mathrm{F}/\mathbb{F}_{q^2}$ le corps défini par : $\mathrm{F} := \mathbb{F}_{q^2}(x,y)$ où $y^q + y = x^{q+1}$.

Alors $g(\mathrm{F}) = \frac{q(q-1)}{2}$ et $N(\mathrm{F}) = q^2 + 1 + 2g(\mathrm{F})q = q^3 + 1$.

Si $N(\mathrm{F}) \geq 2n + 2g(\mathrm{F}) - 1$ i.e. $n \leq \frac{1}{2}(q^3 - q^2 + q + 2)$

alors on peut appliquer l'algorithme de Chudnovsky-Chudnovsky sur le corps de fonctions $\mathrm{F}/\mathbb{F}_{q^2}$ pour multiplier dans $\mathbb{F}_{q^{2n}}$.

Pour $q = 4$: multiplication dans des extensions de degré n de $\mathbb{F}_{16}$.

$$\left.\begin{array}{l} g(\mathrm{F}/\mathbb{F}_{16}) = 6 \\ N(\mathrm{F}/\mathbb{F}_{16}) = 65 \end{array}\right\} \rightsquigarrow$$

si $n \leq 27$, on a un algorithme de multiplication dans $\mathbb{F}_{16^n}$ à partir de $\mathrm{F}/\mathbb{F}_{16}$ de complexité $\mu_q(n) \leq 2n + g(\mathrm{F}) - 1$.

Algorithme de Chudnovsky-Chudnovsky sur le corps de fonctions Hermitien

Soit $\mathrm{F}/\mathbb{F}_{q^2}$ le corps défini par : $\mathrm{F} := \mathbb{F}_{q^2}(x,y)$ où $y^q + y = x^{q+1}$.

Alors $g(\mathrm{F}) = \frac{q(q-1)}{2}$ et $N(\mathrm{F}) = q^2 + 1 + 2g(\mathrm{F})q = q^3 + 1$.

Si $N(\mathrm{F}) \geq 2n + 2g(\mathrm{F}) - 1$ i.e. $n \leq \frac{1}{2}(q^3 - q^2 + q + 2)$

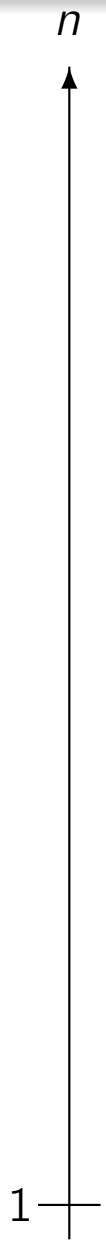
alors on peut appliquer l'algorithme de Chudnovsky-Chudnovsky sur le corps de fonctions $\mathrm{F}/\mathbb{F}_{q^2}$ pour multiplier dans $\mathbb{F}_{q^{2n}}$.

Pour $q = 4$: multiplication dans des extensions de degré n de $\mathbb{F}_{16}$.

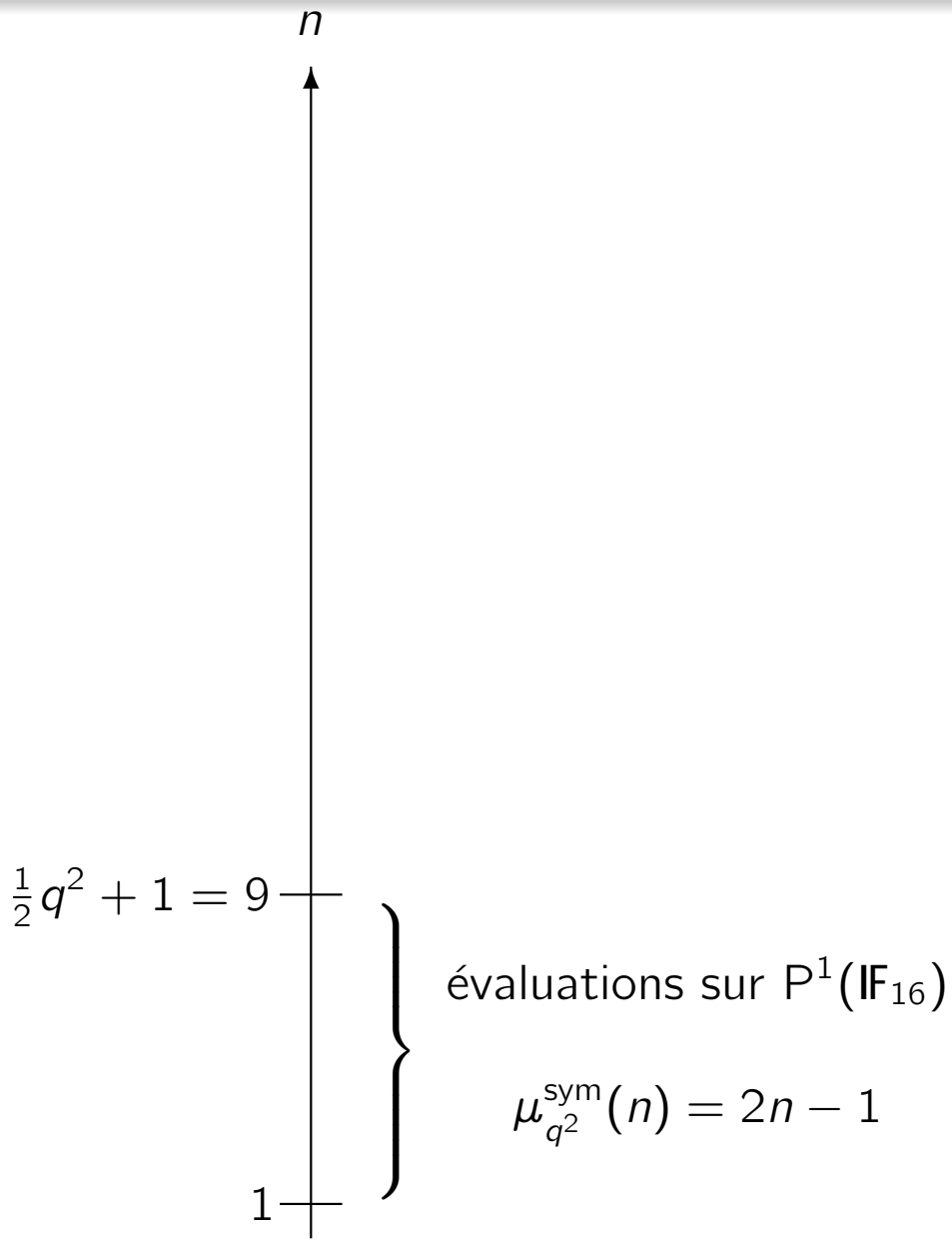
$$\left.\begin{array}{l} g(\mathrm{F}/\mathbb{F}_{16}) = 6 \\ N(\mathrm{F}/\mathbb{F}_{16}) = 65 \end{array}\right\} \rightsquigarrow$$

si $n \leq 27$, on a un algorithme de multiplication dans $\mathbb{F}_{16^n}$ à partir de $\mathrm{F}/\mathbb{F}_{16}$ de complexité $\mu_q(n) \leq 2n + 5$.

Cas des *petites* extensions $\mathbb{F}_{16^n}$ de $\mathbb{F}_{16}$

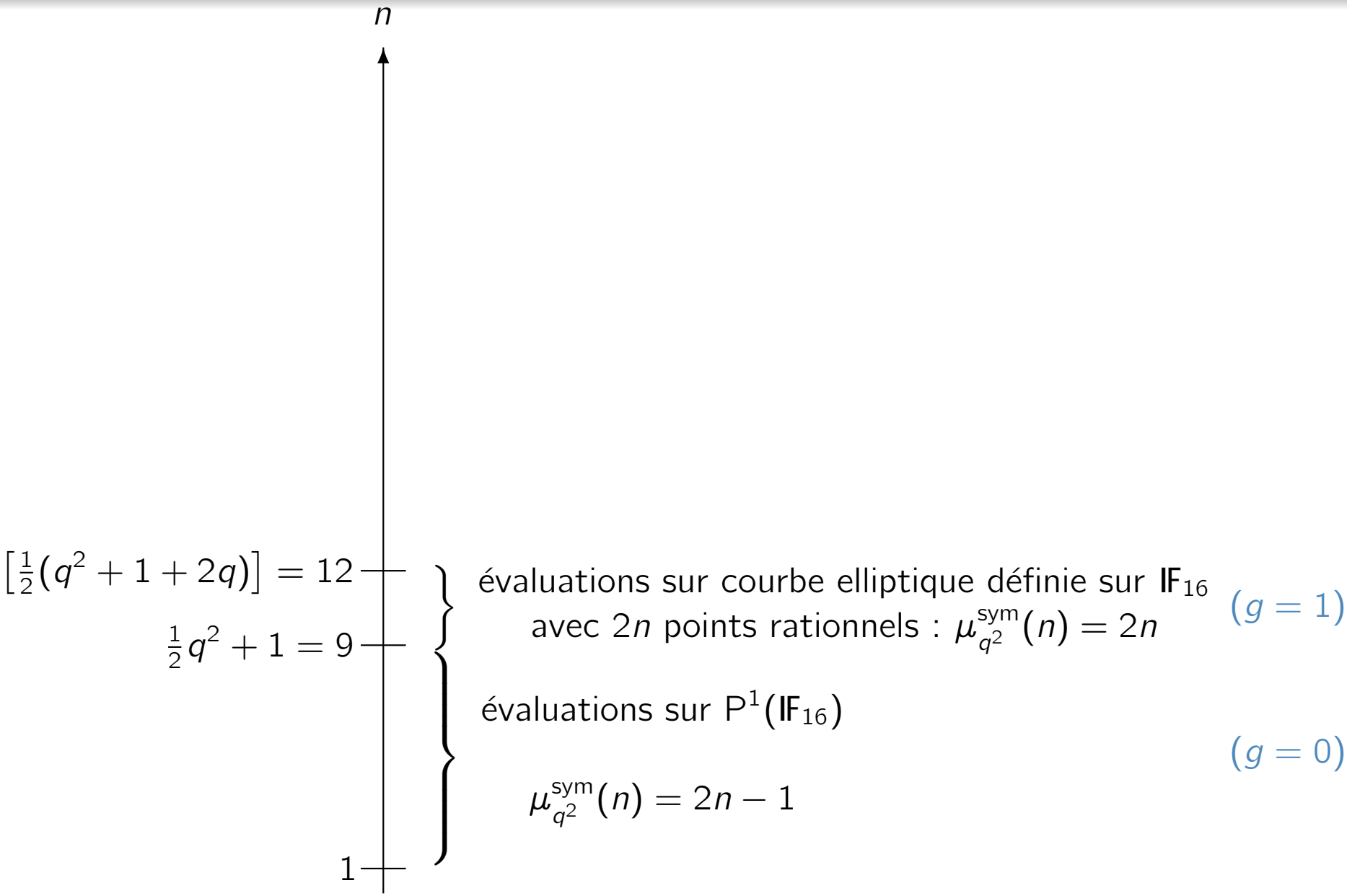


Cas des *petites* extensions $\mathbb{F}_{16^n}$ de $\mathbb{F}_{16}$

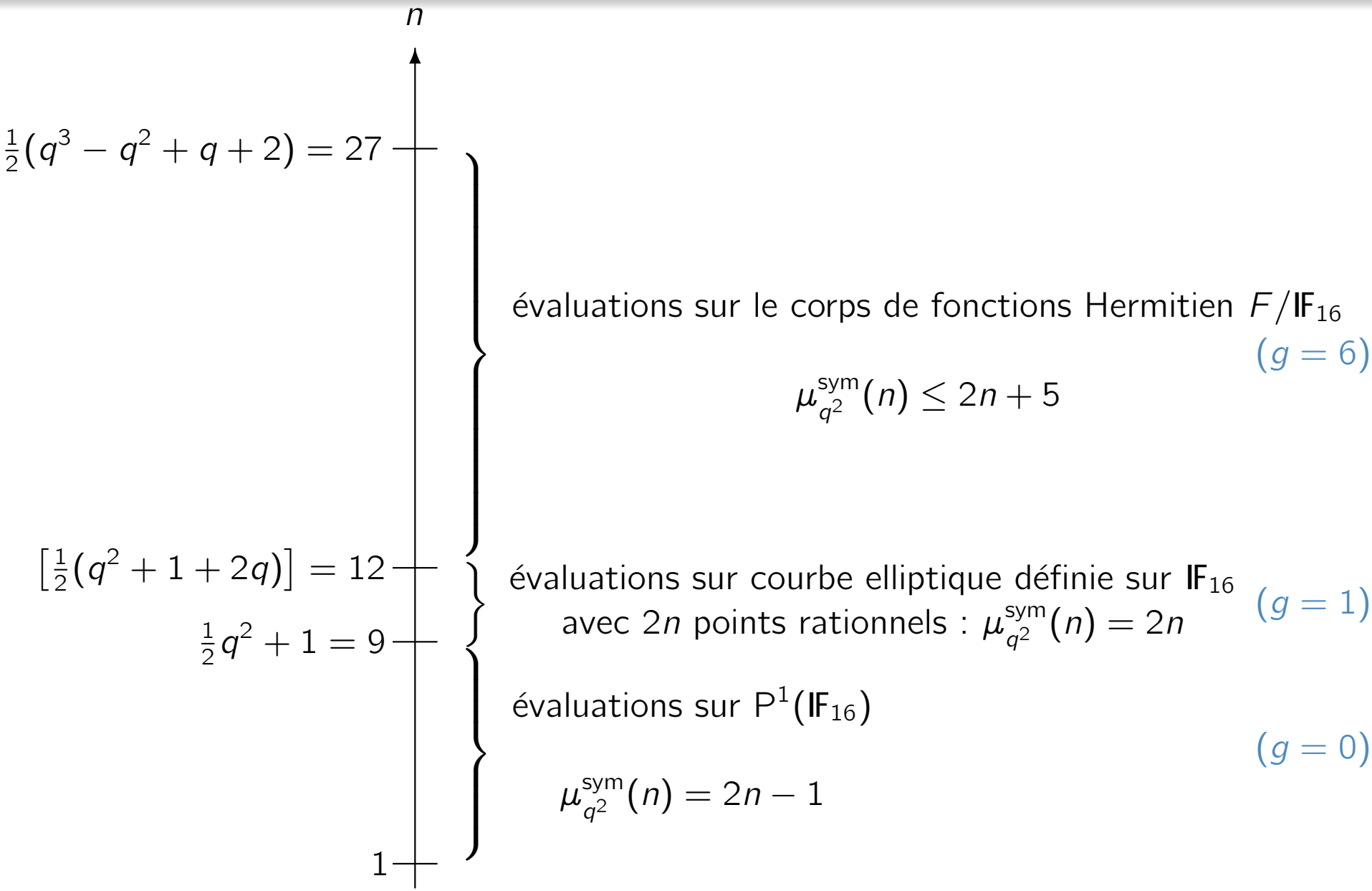


$(g=0)$

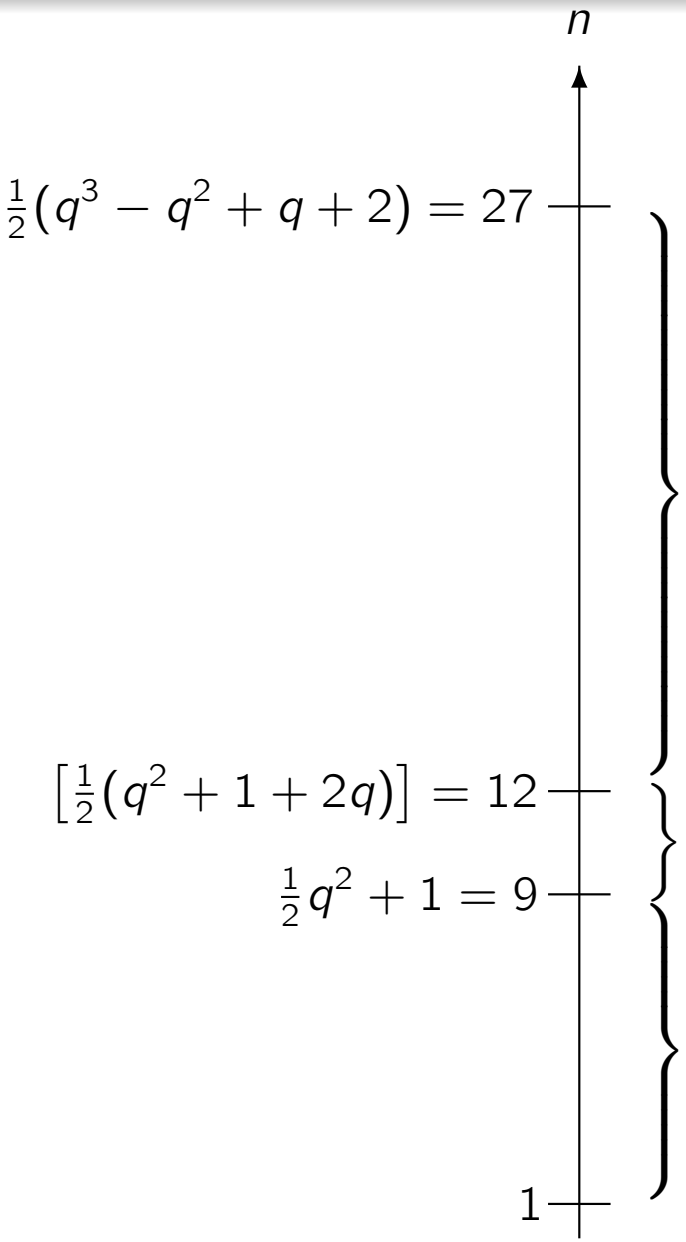
Cas des *petites* extensions $\mathbb{F}_{16^n}$ de $\mathbb{F}_{16}$



Cas des *petites* extensions $\mathbb{F}_{16^n}$ de $\mathbb{F}_{16}$



Cas des *petites* extensions $\mathbb{F}_{16^n}$ de $\mathbb{F}_{16}$



$$n \leq \tfrac{1}{2}(N-2g+1) \quad \Longrightarrow \quad \mu_q^{\mathrm{sym}}(n) \leq 2n+g-1$$

évaluations sur le corps de fonctions Hermitien $F/\mathbb{F}_{16}$ $(g=6)$

$$\mu_{q^2}^{\mathrm{sym}}(n) \leq 2n+5$$

évaluations sur courbe elliptique définie sur $\mathbb{F}_{16}$ avec $2n$ points rationnels : $\mu_{q^2}^{\mathrm{sym}}(n)=2n$ $(g=1)$

évaluations sur $\mathrm{P}^1(\mathbb{F}_{16})$ $(g=0)$

$$\mu_{q^2}^{\mathrm{sym}}(n)=2n-1$$

Application de l'algorithme sur une **suite asymptotiquement bonne de corps de fonctions** :

Théorème (Chudnovsky et Chudnovsky (1987))

Soit $q = p^r$ avec p premier, il existe une constante C_q telle que pour tout n,

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

Application de l'algorithme sur une **suite asymptotiquement bonne de corps de fonctions** :

Théorème (Chudnovsky et Chudnovsky (1987))

Soit $q = p^r$ avec p premier, il existe une constante C_q telle que pour tout n,

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

Objectifs.

- Établir des bornes théoriques :
  - améliorer l'algorithme (évaluations sur des places de degré supérieur, dissymétrisation...)
  - démontrer l'existence de corps de fonctions avec de meilleures propriétés
- Construire des algorithmes explicites pour la multiplication dans $\mathbb{F}_{q^n}$, pour n choisi.

Application de l'algorithme sur une **suite asymptotiquement bonne de corps de fonctions** :

Théorème (Chudnovsky et Chudnovsky (1987))

Soit $q = p^r$ avec p premier, il existe une constante C_q telle que pour tout n,

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

Objectifs.

- Établir des bornes théoriques :
  - améliorer l'algorithme (évaluations sur des places de degré supérieur, dissymétrisation...)
  - démontrer l'existence de corps de fonctions avec de meilleures propriétés
- Construire des algorithmes explicites pour la multiplication dans $\mathbb{F}_{q^n}$, pour n choisi.

Plan

Posons $\mathcal{G} := \sum_{i=1}^{N} P_i$.

On cherche $\mathcal{D}$ de degré $n+g-1$ tel que

(i) $\dim(\mathcal{D} - Q) = 0$

(ii) $\dim(2\mathcal{D} - \mathcal{G}) = 0$

Rappel. $\mathscr{L}(\mathcal{D}) := \left\{ f \in \mathrm{F}\backslash\{0\} \; ; \; (f) + \mathcal{D} \geq 0 \right\} \cup \left\{ 0 \right\}$

$\mathscr{L}(\mathcal{D})$ est un $\mathbb{F}_q$-ev de dimension finie : $\dim \mathcal{D} := \dim_{\mathbb{F}_q} \mathscr{L}(\mathcal{D})$.

Posons $\mathcal{G} := \sum_{i=1}^{N} P_i$.

On cherche $\mathcal{D}$ de degré $n+g-1$ tel que

(i) $\dim(\mathcal{D}-Q) = 0$

(ii) $\dim(2\mathcal{D}-\mathcal{G}) = 0$: il suffit que $\deg(2\mathcal{D}-\mathcal{G}) < 0$

Rappel. $\mathscr{L}(\mathcal{D}) := \{f \in \mathrm{F}\backslash\{0\} \,;\, (f)+\mathcal{D} \geq 0\} \cup \{0\}$

$\mathscr{L}(\mathcal{D})$ est un $\mathbb{F}_q$-ev de dimension finie : $\dim \mathcal{D} := \dim_{\mathbb{F}_q} \mathscr{L}(\mathcal{D})$.

Posons $\mathcal{G} := \sum_{i=1}^{N} P_i$. **But :** choisir N minimal !

On cherche $\mathcal{D}$ de degré $n+g-1$ tel que

(i) $\dim(\mathcal{D}-Q) = 0$

(ii) $\dim(2\mathcal{D}-\mathcal{G}) = 0$: il suffit que $\deg(2\mathcal{D}-\mathcal{G}) < 0$

Rappel. $\mathscr{L}(\mathcal{D}) := \{f \in \mathrm{F}\backslash\{0\} \,;\, (f)+\mathcal{D} \geq 0\} \cup \{0\}$

$\mathscr{L}(\mathcal{D})$ est un $\mathbb{F}_q$-ev de dimension finie : $\dim \mathcal{D} := \dim_{\mathbb{F}_q} \mathscr{L}(\mathcal{D})$.

Posons $\mathcal{G} := \sum_{i=1}^{N} P_i$. **But :** choisir N minimal !

On cherche $\mathcal{D}$ de degré $n+g-1$ tel que

(i) $\dim(\mathcal{D} - Q) = 0$

(ii) $\dim(2\mathcal{D} - \mathcal{G}) = 0$

Rappel. $\mathscr{L}(\mathcal{D}) := \{f \in \mathrm{F}\backslash\{0\} \,;\, (f) + \mathcal{D} \geq 0\} \cup \{0\}$

$\mathscr{L}(\mathcal{D})$ est un $\mathbb{F}_q$-ev de dimension finie : $\dim \mathcal{D} := \dim_{\mathbb{F}_q} \mathscr{L}(\mathcal{D})$.

Posons $\mathcal{G} := \sum_{i=1}^{N} P_i$. **But :** choisir N minimal !

On cherche $\mathcal{D}$ de degré $n+g-1$ tel que

(i) $\dim(\mathcal{D} - Q) = 0$

(ii) $\dim(2\mathcal{D} - \mathcal{G}) = 0$

$\rightsquigarrow$ Propriétés invariantes par **classe de diviseurs**

Stratégie. Soit $h_F := |\mathrm{Cl}^0(\mathrm{F})|$, montrer que

$$\left|\left\{\text{classes t.q. } \textbf{au moins une des deux conditions} \text{ n'est pas satisfaite}\right\}\right| < h_F$$

Caractérisation des diviseurs de dimension nulle

$$\dim \mathcal{A} = 0 \quad \Longleftrightarrow \quad \nexists\, \mathcal{A}' \in [\mathcal{A}] \ \text{ t.q. } \ \mathcal{A}' \geq 0$$

Notations.

- $\mathrm{A}_k := \left|\{\mathcal{A} \in \mathrm{Div}(\mathrm{F}) \ ; \ \mathcal{A} \geq 0 \ \text{ et } \ \deg \mathcal{A} = k\}\right|$
- $\mathrm{Cl}^0(\mathrm{F})[p] := \{[\mathcal{A}] \in \mathrm{Cl}^0(\mathrm{F}) \ ; \ p[\mathcal{A}] = 0\}$

Caractérisation des diviseurs de dimension nulle

$$\dim \mathcal{A} = 0 \quad \Longleftrightarrow \quad \nexists\, \mathcal{A}' \in [\mathcal{A}] \ \text{ t.q. } \ \mathcal{A}' \geq 0$$

Notations.

- $\mathrm{A}_k := \left|\{\mathcal{A} \in \mathrm{Div}(\mathrm{F}) \ ; \ \mathcal{A} \geq 0 \ \text{ et } \ \deg \mathcal{A} = k\}\right|$
- $\mathrm{Cl}^0(\mathrm{F})[p] := \{[\mathcal{A}] \in \mathrm{Cl}^0(\mathrm{F}) \ ; \ p[\mathcal{A}] = 0\}$

(i) $\dim(\mathcal{D} - Q) \neq 0$ pour au plus A_{g-1} classes de diviseurs

Caractérisation des diviseurs de dimension nulle

$$\dim \mathcal{A} = 0 \quad \Longleftrightarrow \quad \nexists\, \mathcal{A}' \in [\mathcal{A}] \ \text{ t.q. } \ \mathcal{A}' \geq 0$$

Notations.

- $\mathrm{A}_k := \left|\{\mathcal{A} \in \mathrm{Div}(\mathrm{F}) \ ; \ \mathcal{A} \geq 0 \ \text{ et } \ \deg \mathcal{A} = k\}\right|$
- $\mathrm{Cl}^0(\mathrm{F})[p] := \{[\mathcal{A}] \in \mathrm{Cl}^0(\mathrm{F}) \ ; \ p[\mathcal{A}] = 0\}$

(i) $\dim(\mathcal{D} - Q) \neq 0$ pour au plus A_{g-1} classes de diviseurs

(ii) $\dim(2\mathcal{D} - \mathcal{G}) \neq 0$ pour au plus $\mathrm{A}_{g-1} \cdot |\mathrm{Cl}^0(\mathrm{F})[2]|$ classes de diviseurs

car $\mathrm{Cl}^0(\mathrm{F})[2] = \ker \psi$ où $\psi : \begin{array}{ccc} \mathrm{Cl}(\mathrm{F}) & \to & \mathrm{Cl}(\mathrm{F}) \\ [\mathcal{A}] & \mapsto & 2[\mathcal{A}] \end{array}$

Caractérisation des diviseurs de dimension nulle

$$\dim \mathcal{A} = 0 \quad \Longleftrightarrow \quad \nexists\, \mathcal{A}' \in [\mathcal{A}] \text{ t.q. } \mathcal{A}' \geq 0$$

Notations.

- $\mathrm{A}_k := \left|\{\mathcal{A} \in \mathrm{Div}(\mathrm{F}) \ ; \ \mathcal{A} \geq 0 \text{ et } \deg \mathcal{A} = k\}\right|$
- $\mathrm{Cl}^0(\mathrm{F})[p] := \{[\mathcal{A}] \in \mathrm{Cl}^0(\mathrm{F}) \ ; \ p[\mathcal{A}] = 0\}$

(i) $\dim(\mathcal{D} - Q) \neq 0$ pour au plus A_{g-1} classes de diviseurs

(ii) $\dim(2\mathcal{D} - \mathcal{G}) \neq 0$ pour au plus $\mathrm{A}_{g-1} \cdot |\mathrm{Cl}^0(\mathrm{F})[2]|$ classes de diviseurs

car $\mathrm{Cl}^0(\mathrm{F})[2] = \ker \psi$ où $\psi : \begin{array}{ccc} \mathrm{Cl}(\mathrm{F}) & \to & \mathrm{Cl}(\mathrm{F}) \\ [\mathcal{A}] & \mapsto & 2[\mathcal{A}] \end{array}$

Conséquences

1. $\mathrm{A}_{g-1} < h_{\mathrm{F}} \quad \Rightarrow \quad \exists\, \mathcal{A}$ non-spécial de degré $g-1$ $\qquad \rightsquigarrow \mathcal{D} \sim \mathcal{A} + Q$
2. $\mathrm{A}_{g-1} + \mathrm{A}_{g-1} \cdot |\mathrm{Cl}^0(\mathrm{F})[2]| < h_{\mathrm{F}} \quad \Longrightarrow \quad \exists\, \mathcal{D}$ t.q. $\begin{cases} \dim(\mathcal{D} - Q) = 0 \\ \dim(2\mathcal{D} - \mathcal{G}) = 0 \end{cases}$

Caractérisation des diviseurs de dimension nulle

$$\dim \mathcal{A} = 0 \quad \Longleftrightarrow \quad \nexists\, \mathcal{A}' \in [\mathcal{A}] \ \text{ t.q. } \ \mathcal{A}' \geq 0$$

Notations.

- $\mathrm{A}_k := \left|\{\mathcal{A} \in \mathrm{Div}(\mathrm{F}) \ ; \ \mathcal{A} \geq 0 \ \text{ et } \ \deg \mathcal{A} = k\}\right|$
- $\mathrm{Cl}^0(\mathrm{F})[p] := \{[\mathcal{A}] \in \mathrm{Cl}^0(\mathrm{F}) \ ; \ p[\mathcal{A}] = 0\}$

(i) $\dim(\mathcal{D} - Q) \neq 0$ pour au plus A_{g-1} classes de diviseurs

(ii) $\dim(2\mathcal{D} - \mathcal{G}) \neq 0$ pour au plus $\mathrm{A}_{g-1} \cdot |\mathrm{Cl}^0(\mathrm{F})[2]|$ classes de diviseurs

car $\mathrm{Cl}^0(\mathrm{F})[2] = \ker \psi$ où $\psi : \begin{array}{ccc} \mathrm{Cl}(\mathrm{F}) & \to & \mathrm{Cl}(\mathrm{F}) \\ [\mathcal{A}] & \mapsto & 2[\mathcal{A}] \end{array}$

Conséquences

1. $\mathrm{A}_{g-1} < h_{\mathrm{F}} \quad \Rightarrow \quad \exists\, \mathcal{A}$ non-spécial de degré $g-1$ $\qquad \rightsquigarrow \mathcal{D} \sim \mathcal{A} + Q$
2. $\mathrm{A}_{g-1} + \mathrm{A}_{g-1} \cdot |\mathrm{Cl}^0(\mathrm{F})[2]| < h_{\mathrm{F}} \quad \Longrightarrow \quad \exists\, \mathcal{D}$ t.q. $\begin{cases} \dim(\mathcal{D} - Q) = 0 \\ \dim(2\mathcal{D} - \mathcal{G}) = 0 \end{cases}$

Fonction Zeta, L-polynôme et diviseurs effectifs... (I)

Soit $F/\mathbb{F}_q$ un corps de fonction de genre g.

- Fonction Zeta : $Z_F(T) := \sum_{n=0}^{\infty} A_n T^n \in \mathbb{C}[[T]]$
- L-polynôme : $L_F(T) := Z_F(T)(1-T)(1-qT)$

Propriétés

(a) $L_F(T) \in \mathbb{Z}[T]$ *et* $\deg L_F(T) = 2g$

(b) $L_F(T) = \sum_{i=0}^{2g} a_i T^i$ *avec*
$$\begin{cases} a_0 &= 1 \\ a_{2g} &= q^g \\ a_{2g-i} &= q^{g-i} a_i \quad \text{pour } 0 \le i \le g \\ a_1 &= N(F) - (q+1) \end{cases}$$

(c) $L_F(1) = \sum_{i=0}^{2g} a_i = h_F$

(d) *Dans* $\mathbb{C}[T]$, $L_F(T)$ *admet une factorisation de la forme :*
$$L_F(T) = \prod_{j=1}^{g} (1-\alpha_j T)(1-\overline{\alpha_j} T)$$

Si $g \geq 2$, alors :

$$2\sum_{n=0}^{g-2} q^{\frac{g-1-n}{2}} \mathrm{A}_n + \mathrm{A}_{g-1} \leq \frac{h_{\mathrm{F}}}{(q^{1/2}-1)^2}$$

Si $g \geq 2$, alors :

$$2\sum_{n=0}^{g-2} q^{\frac{g-1-n}{2}} \mathrm{A}_n + \mathrm{A}_{g-1} \leq \frac{h_{\mathrm{F}}}{(q^{1/2}-1)^2}$$

Théorème (Ballet–Le Brigand (2009))

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

Rq. $\mathrm{A}_0 = 1, \qquad \mathrm{A}_1 = N(\mathrm{F})$.

Si $g \geq 2$, alors :

$$2\sum_{n=0}^{g-2} q^{\frac{g-1-n}{2}} \mathrm{A}_n + \mathrm{A}_{g-1} \leq \frac{h_{\mathrm{F}}}{(q^{1/2}-1)^2}$$

Lemme (Lachaud – Martin-Deschamps (1990))

(i) *Si $n \geq 0$, alors :* $\mathrm{A}_n = q^{n+1-g}\mathrm{A}_{2g-2-n} + h_{\mathrm{F}}\dfrac{q^{n+1-g}-1}{q-1}$.

En particulier, si $n \geq 2g-1$ alors : $\mathrm{A}_n = h_{\mathrm{F}}\dfrac{q^{n+1-g}-1}{q-1}$.

(ii) *Pour $g \geq 2$, on a :* $\displaystyle\sum_{n=0}^{g-2} \mathrm{A}_n T^n + \sum_{n=0}^{g-1} \mathrm{A}_n T^{2g-2+n} = \frac{L_{\mathrm{F}}(T) - h_{\mathrm{F}} T^g}{(1-T)(1-qT)}$.

Fonction Zeta, L-polynôme et diviseurs effectifs... (II)

(i) Si $n \geq 0$, alors : $$\mathrm{A}_n = q^{n+1-g}\mathrm{A}_{2g-2-n} + h_{\mathrm{F}}\frac{q^{n+1-g}-1}{q-1}.$$

Preuve.

Fonction Zeta, L-polynôme et diviseurs effectifs... (II)

(i) Si $n \geq 0$, alors : $\mathrm{A}_n = q^{n+1-g}\mathrm{A}_{2g-2-n} + h_{\mathrm{F}}\dfrac{q^{n+1-g}-1}{q-1}$.

Preuve.

$$\begin{aligned}
\mathrm{A}_n &\overset{\text{def}}{=} \Big|\{\mathcal{A} \in \mathrm{Div}(\mathrm{F}/\mathbb{F}_q)\ ;\ \mathcal{A} \geq 0 \text{ et } \deg \mathcal{A} = n\}\Big| \\
&= \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \Big|\{\mathcal{A} \in [\mathcal{C}]\ ;\ \mathcal{A} \geq 0\}\Big| \\
&= \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \frac{q^{\dim[\mathcal{C}]}-1}{q-1} \\
&= \frac{1}{q-1} \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \left(q^{n+1-g+\mathrm{i}([\mathcal{C}])}-1\right) \\
&= \frac{1}{q-1} \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \left(q^{n+1-g}\left(q^{\mathrm{i}([\mathcal{C}])}-1\right) + q^{n+1-g}-1\right) \\
&= q^{n+1-g} \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \frac{q^{\dim[\mathcal{W}-\mathcal{C}]}-1}{q-1} + h_{\mathrm{F}}\frac{q^{n+1-g}-1}{q-1}
\end{aligned}$$

Fonction Zeta, L-polynôme et diviseurs effectifs... (II)

(i) Si $n \geq 0$, alors : $\mathrm{A}_n = q^{n+1-g}\mathrm{A}_{2g-2-n} + h_{\mathrm{F}}\dfrac{q^{n+1-g}-1}{q-1}$.

Preuve.

$$\begin{aligned}
\mathrm{A}_n &\overset{\text{def}}{=} \Big|\{\mathcal{A} \in \mathrm{Div}(\mathrm{F}/\mathbb{F}_q)\ ;\ \mathcal{A} \geq 0 \text{ et } \deg \mathcal{A} = n\}\Big| \\
&= \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \Big|\{\mathcal{A} \in [\mathcal{C}]\ ;\ \mathcal{A} \geq 0\}\Big| \\
&= \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \frac{q^{\dim[\mathcal{C}]}-1}{q-1} \\
&= \frac{1}{q-1} \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \Big(q^{n+1-g+\mathrm{i}([\mathcal{C}])}-1\Big) \\
&= \frac{1}{q-1} \sum_{[\mathcal{C}] \in \mathrm{Cl}^n(\mathrm{F}/\mathbb{F}_q)} \Big(q^{n+1-g}\big(q^{\mathrm{i}([\mathcal{C}])}-1\big) + q^{n+1-g}-1\Big) \\
&= q^{n+1-g} \sum_{[\mathcal{W}-\mathcal{C}] \in \mathrm{Cl}^{2g-2-n}(\mathrm{F}/\mathbb{F}_q)} \frac{q^{\dim[\mathcal{W}-\mathcal{C}]}-1}{q-1} + h_{\mathrm{F}}\frac{q^{n+1-g}-1}{q-1}
\end{aligned}$$

Fonction Zeta, L-polynôme et diviseurs effectifs... (III)

(ii) Pour $g \geq 2$, on a : $$\sum_{n=0}^{g-2} A_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} A_n T^{2g-2+n} = \frac{L_F(T) - h_F T^g}{(1-T)(1-qT)}$$

Preuve.

Fonction Zeta, L-polynôme et diviseurs effectifs... (III)

(ii) Pour $g \geq 2$, on a : $\displaystyle\sum_{n=0}^{g-2} A_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} A_n T^{2g-2+n} = \frac{L_F(T) - h_F T^g}{(1-T)(1-qT)}$

Preuve.

$$\begin{aligned}
Z_F(T) &= \sum_{n=0}^{g-2} A_n T^n + \sum_{n=g-1}^{2g-2} \left(q^{n+1-g} A_{2g-2-n} + h_F \frac{q^{n+1-g}-1}{q-1} \right) T^n \\
&\quad + \sum_{n=2g-1}^{\infty} h_F \frac{q^{n+1-g}-1}{q-1} T^n \\
&= \sum_{n=0}^{g-2} A_n T^n + \sum_{n=g-1}^{2g-2} q^{n+1-g} A_{2g-2-n} T^n + \sum_{n=g-1}^{\infty} h_F \frac{q^{n+1-g}-1}{q-1} T^n \\
&= \sum_{n=0}^{g-2} A_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} A_n T^{2g-2-n} + \frac{h_F T^{g-1}}{q-1} \sum_{n=0}^{\infty} (q^n - 1) T^n \\
&= \sum_{n=0}^{g-2} A_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} A_n T^{2g-2-n} + \frac{h_F T^{g-1}}{q-1} \left(\frac{1}{1-qT} - \frac{1}{1-T} \right)
\end{aligned}$$

□

Fonction Zeta, L-polynôme et diviseurs effectifs... (IV)

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

Preuve.

Fonction Zeta, L-polynôme et diviseurs effectifs... (IV)

Conséquence. Si $g \geq 2$, $\displaystyle 2\sum_{n=0}^{g-2} q^{\frac{g-1-n}{2}} A_n + A_{g-1} \leq \frac{h_F}{(q^{1/2}-1)^2}$

Preuve.

$$\sum_{n=0}^{g-2} A_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} A_n T^{2g-2+n} = \frac{L_F(T) - h_F T^g}{(1-T)(1-qT)}$$

$\rightsquigarrow$ on substitue $T = q^{-\frac{1}{2}}$:

$$\sum_{n=0}^{g-2} A_n q^{-n/2} + \sum_{n=0}^{g-1} q^{g-1-n} A_n q^{-g+1+n/2} = \frac{L_F(q^{-1/2}) - h_F q^{-g/2}}{(1-q^{-1/2})(1-q^{1/2})}$$

i.e. $$2\sum_{n=0}^{g-2} A_n q^{-n/2} + q^{-\frac{g-1}{2}} A_{g-1} = \frac{h_F q^{-g/2} - L_F(q^{-1/2})}{q^{-1/2}(q^{1/2}-1)^2}$$

avec $$L_F(q^{-1/2}) = \prod_{j=1}^{g} (1-\alpha_j q^{-1/2})(1-\overline{\alpha_j} q^{-1/2}) = \left|1-\alpha_j q^{-1/2}\right|^2 \geq 0.$$

□

Si $g \geq 2$, alors :

$$2\sum_{n=0}^{g-2} q^{\frac{g-1-n}{2}} \mathrm{A}_n + \mathrm{A}_{g-1} \leq \frac{h_{\mathrm{F}}}{(q^{1/2}-1)^2}$$

Théorème (Ballet–Le Brigand (2009))

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

Si $g \geq 2$, alors :

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

Théorème (Ballet–Le Brigand (2009))

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

Problème. Cas où $q = 2$ ou 3 ?

p-rang et ordinarité

- Si le corps des constantes de F est $\overline{\mathbb{F}_p}$, alors on définit le p-rang de F par :

$$\gamma(F) = \dim_{\mathbb{F}_p} \mathrm{Cl}_0(F)[p].$$

p-rang et ordinarité

- Si le corps des constantes de F est $\overline{\mathbb{F}_p}$, alors on définit le p-rang de F par :

$$\gamma(F) = \dim_{\mathbb{F}_p} \mathrm{Cl}_0(F)[p].$$

Si F est défini sur $\mathbb{F}_q$, on pose $\gamma(F) := \gamma(F\overline{\mathbb{F}_q})$.

p-rang et ordinarité

- Si le corps des constantes de F est $\overline{\mathbb{F}_p}$, alors on définit le p-rang de F par :

$$\gamma(\mathrm{F}) = \dim_{\mathbb{F}_p} \mathrm{Cl}_0(\mathrm{F})[p].$$

  Si F est défini sur $\mathbb{F}_q$, on pose $\gamma(\mathrm{F}) := \gamma(\mathrm{F}\overline{\mathbb{F}_q})$.

- Le p-rang vérifie : $\gamma(\mathrm{F}) = \deg\left(L_{\mathrm{F}}(T) \bmod p\right)$

p-rang et ordinarité

- Si le corps des constantes de F est $\overline{\mathbb{F}_p}$, alors on définit le p-rang de F par :

$$\gamma(\mathrm{F}) = \dim_{\mathbb{F}_p} \mathrm{Cl}_0(\mathrm{F})[p].$$

  Si F est défini sur $\mathbb{F}_q$, on pose $\gamma(\mathrm{F}) := \gamma(\mathrm{F}\overline{\mathbb{F}_q})$.

- Le p-rang vérifie : $\gamma(\mathrm{F}) = \deg\left(L_{\mathrm{F}}(T) \bmod p\right)$

$$0 \leq \gamma(\mathrm{F}) \leq g(\mathrm{F})$$

p-rang et ordinarité

- Si le corps des constantes de F est $\overline{\mathbb{F}_p}$, alors on définit le p-rang de F par :

$$\gamma(F) = \dim_{\mathbb{F}_p} \mathrm{Cl}_0(F)[p].$$

  Si F est défini sur $\mathbb{F}_q$, on pose $\gamma(F) := \gamma(F\overline{\mathbb{F}_q})$.

- Le p-rang vérifie : $\gamma(F) = \deg\left(L_F(T) \bmod p\right)$

$$0 \leq \gamma(F) \leq g(F)$$

- Si $\gamma(F) = g(F)$, F est dit **ordinaire**.

  Une tour $\mathcal{T} = (F_i/\mathbb{F}_q)_{i\geq 1}$ de corps de fonctions est dite **ordinaire** si les F_i sont **tous ordinaires**.

p-rang et ordinarité

- Si le corps des constantes de F est $\overline{\mathbb{F}_p}$, alors on définit le p-rang de F par :

$$\gamma(\mathrm{F}) = \dim_{\mathbb{F}_p} \mathrm{Cl}_0(\mathrm{F})[p].$$

  Si F est défini sur $\mathbb{F}_q$, on pose $\gamma(\mathrm{F}) := \gamma(\mathrm{F}\overline{\mathbb{F}_q})$.

- Le p-rang vérifie : $\gamma(\mathrm{F}) = \deg\left(L_{\mathrm{F}}(T) \bmod p\right)$

$$0 \leq \gamma(\mathrm{F}) \leq g(\mathrm{F})$$

- Si $\gamma(\mathrm{F}) = g(\mathrm{F})$, F est dit **ordinaire**.

  Une tour $\mathcal{T} = (\mathrm{F}_i/\mathbb{F}_q)_{i\geq 1}$ de corps de fonctions est dite **ordinaire** si les F_i sont **tous ordinaires**.

Proposition (Ballet–Ritzenthaler–Rolland (2010))

Si F *est un corps de fonctions défini sur* $\mathbb{F}_{p^r}$ *de genre* $g \geq 1$ *et de* p*-rang* γ*, alors il existe un diviseur de degré* $\gamma - 1$ *de dimension nulle.*

Tour ordinaire d'extensions d'Artin-Schreier

Definition (Garcia–Stichtenoth (1995))

Soit q une puissance d'un premier p. On définit la tour $\mathcal{T} = (\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2, \ldots)$ sur $\mathbb{F}_{q^2}$ en posant pour tout $\ell \geq 0$, $\mathrm{F}_\ell := \mathbb{F}_{q^2}(x_0, \ldots, x_\ell)$ avec

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1}+1} \quad \text{pour } i = 0, \ldots, \ell-1.$$

On a

$$g(\mathrm{F}_\ell) = \begin{cases} (q^{\frac{\ell}{2}+1}-1)(q^{\frac{\ell}{2}}-1) & \text{si } \ell \equiv 0 \pmod 2, \\ (q^{\frac{\ell+1}{2}}-1)^2 & \text{si } \ell \equiv 1 \pmod 2, \end{cases}$$

et pour $\ell > 2$, $\quad B_1(\mathrm{F}_\ell/\mathbb{F}_{q^2}) = \begin{cases} q^\ell(q^2-q)+2q^2 & \text{si } p = 2, \\ q^\ell(q^2-q)+2q & \text{si } p > 2. \end{cases}$

Tour ordinaire d'extensions d'Artin-Schreier

Definition (Garcia–Stichtenoth (1995))

Soit q une puissance d'un premier p. On définit la tour $\mathcal{T} = (\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2, \ldots)$ sur $\mathbb{F}_{q^2}$ en posant pour tout $\ell \geq 0$, $\mathrm{F}_\ell := \mathbb{F}_{q^2}(x_0, \ldots, x_\ell)$ avec

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1}+1} \quad \text{pour } i = 0, \ldots, \ell-1.$$

On a

$$g(\mathrm{F}_\ell) = \begin{cases} (q^{\frac{\ell}{2}+1}-1)(q^{\frac{\ell}{2}}-1) & \text{si } \ell \equiv 0 \pmod 2, \\ (q^{\frac{\ell+1}{2}}-1)^2 & \text{si } \ell \equiv 1 \pmod 2, \end{cases}$$

et pour $\ell > 2$, $\quad B_1(\mathrm{F}_\ell/\mathbb{F}_{q^2}) = \begin{cases} q^\ell(q^2-q)+2q^2 & \text{si } p = 2, \\ q^\ell(q^2-q)+2q & \text{si } p > 2. \end{cases}$

Théorème (Zaytsev–McGuire (2010))

La tour $\mathcal{T}/\mathbb{F}_{q^2}$ est ordinaire.

Cas de la caractéristique 2

On considère la tour $\mathcal{T}$ sur $\mathbb{F}_{16}$, i.e. pour $q = 4$.
Pour tout $\ell \geq 1$, $\mathrm{F}_{\ell+1} := \mathrm{F}_\ell(x_{\ell+1})$ avec

$$x_{\ell+1}^4 + x_{\ell+1} = \frac{x_\ell^4}{x_\ell^3 + 1}.$$

Cas de la caractéristique 2

On considère la tour $\mathcal{T}$ sur $\mathbb{F}_{16}$, i.e. pour $q = 4$.
Pour tout $\ell \geq 1$, $\mathrm{F}_{\ell+1} := \mathrm{F}_\ell(x_{\ell+1})$ avec

$$x_{\ell+1}^4 + x_{\ell+1} = \frac{x_\ell^4}{x_\ell^3 + 1}.$$

- **Densification :** pour tout $\ell \geq 1$, il existe un corps de fonctions $\mathrm{F}_{\ell,1}$ t.q.

$$\mathrm{F}_\ell \subset \mathrm{F}_{\ell,1} \subset \mathrm{F}_{\ell+1}$$

il est défini par : $\mathrm{F}_{\ell,1} := \mathrm{F}_\ell(t_{\ell+1})$ avec $t_{\ell+1}^2 + t_{\ell+1} = \frac{x_\ell^4}{x_\ell^3+1}$.

Cas de la caractéristique 2

On considère la tour $\mathcal{T}$ sur $\mathbb{F}_{16}$, i.e. pour $q = 4$.
Pour tout $\ell \geq 1$, $\mathrm{F}_{\ell+1} := \mathrm{F}_\ell(x_{\ell+1})$ avec

$$x_{\ell+1}^4 + x_{\ell+1} = \frac{x_\ell^4}{x_\ell^3 + 1}.$$

- **Densification :** pour tout $\ell \geq 1$, il existe un corps de fonctions $\mathrm{F}_{\ell,1}$ t.q.

$$\mathrm{F}_\ell \subset \mathrm{F}_{\ell,1} \subset \mathrm{F}_{\ell+1}$$

il est défini par : $\mathrm{F}_{\ell,1} := \mathrm{F}_\ell(t_{\ell+1})$ avec $t_{\ell+1}^2 + t_{\ell+1} = \frac{x_\ell^4}{x_\ell^3+1}$.

- **Descente du corps de définition de $\mathbb{F}_{q^2}$ à $\mathbb{F}_2$:** il existe une tour $\tilde{\mathcal{T}}/\mathbb{F}_2$

$$\mathrm{H}_0 \subset \mathrm{H}_{0,1} \subset \mathrm{H}_1 \subset \mathrm{H}_{1,1} \subset \mathrm{H}_2 \subset \ldots$$

définie sur $\mathbb{F}_2$ et t.q. pour tout $\ell \geq 0$:

$$\mathrm{F}_\ell = \mathbb{F}_{q^2}\mathrm{H}_\ell \quad \text{et} \quad \mathrm{F}_{\ell,1} = \mathbb{F}_{q^2}\mathrm{H}_{\ell,1}$$

Cas de la caractéristique 2

On considère la tour $\mathcal{T}$ sur $\mathbb{F}_{16}$, i.e. pour $q=4$.
Pour tout $\ell \geq 1$, $\mathrm{F}_{\ell+1} := \mathrm{F}_\ell(x_{\ell+1})$ avec

$$x_{\ell+1}^4 + x_{\ell+1} = \frac{x_\ell^4}{x_\ell^3+1}.$$

- **Densification :** pour tout $\ell \geq 1$, il existe un corps de fonctions $\mathrm{F}_{\ell,1}$ t.q.

$$\mathrm{F}_\ell \subset \mathrm{F}_{\ell,1} \subset \mathrm{F}_{\ell+1}$$

il est défini par : $\mathrm{F}_{\ell,1} := \mathrm{F}_\ell(t_{\ell+1})$ avec $t_{\ell+1}^2 + t_{\ell+1} = \frac{x_\ell^4}{x_\ell^3+1}$.

- **Descente du corps de définition de $\mathbb{F}_{q^2}$ à $\mathbb{F}_2$:** il existe une tour $\tilde{\mathcal{T}}/\mathbb{F}_2$

$$\mathrm{H}_0 \subset \mathrm{H}_{0,1} \subset \mathrm{H}_1 \subset \mathrm{H}_{1,1} \subset \mathrm{H}_2 \subset \ldots$$

définie sur $\mathbb{F}_2$ et t.q. pour tout $\ell \geq 0$:

$$\mathrm{F}_\ell = \mathbb{F}_{q^2}\mathrm{H}_\ell \quad \text{et} \quad \mathrm{F}_{\ell,1} = \mathbb{F}_{q^2}\mathrm{H}_{\ell,1}$$

$$\Longrightarrow \quad \begin{cases} B_1(\mathrm{F}_\ell/\mathbb{F}_{q^2}) = \sum_{i|4} iB_i(\mathrm{H}_\ell/\mathbb{F}_2) \\ g(\mathrm{F}_\ell/\mathbb{F}_{q^2}) = g(\mathrm{H}_\ell/\mathbb{F}_2) \end{cases}$$

Ordinarité de $\tilde{\mathcal{T}}/\mathbb{F}_2$

Propriété

Soit $F := \mathbb{F}_{q^r} H$.

$$H/\mathbb{F}_q \text{ ordinaire} \iff F/\mathbb{F}_{q^r} \text{ ordinaire.}$$

Conséquence. Pour tout $\ell \geq 0$, $H_{\ell,0} := H_\ell$ est ordinaire.

Ordinarité de $\tilde{\mathcal{T}}/\mathbb{F}_2$

Propriété

Soit $F := \mathbb{F}_{q^r} H$.

$$H/\mathbb{F}_q \text{ ordinaire} \quad \Longleftrightarrow \quad F/\mathbb{F}_{q^r} \text{ ordinaire.}$$

Conséquence. Pour tout $\ell \geq 0$, $H_{\ell,0} := H_\ell$ est ordinaire.

Proposition (Bassa–Beelen (2009))

Si E/F *est une extension de corps de fonctions, alors*

$$g(E) - \gamma(E) \geq g(F) - \gamma(F).$$

Conséquence. $H_{\ell+1}$ ordinaire $\Rightarrow$ $H_{\ell,1}$ ordinaire

Ordinarité de $\tilde{\mathcal{T}}/\mathbb{F}_2$

Propriété

Soit $F := \mathbb{F}_{q^r} H$.

$$H/\mathbb{F}_q \text{ ordinaire} \iff F/\mathbb{F}_{q^r} \text{ ordinaire.}$$

Conséquence. Pour tout $\ell \geq 0$, $H_{\ell,0} := H_\ell$ est ordinaire.

Proposition (Bassa–Beelen (2009))

Si E/F *est une extension de corps de fonctions, alors*

$$g(E) - \gamma(E) \geq g(F) - \gamma(F).$$

Conséquence. $H_{\ell+1}$ ordinaire $\Rightarrow$ $H_{\ell,1}$ ordinaire

Proposition

La tour $\tilde{\mathcal{T}}/\mathbb{F}_2$ *est ordinaire.*

Application pour $p=2$ et $q=p^2$

Proposition

Si $n \geq \frac{1}{2}(p+1+\epsilon(p))$, *alors il existe un étage* $\mathrm{H}_{\ell,s}$ *de la tour* $\tilde{\mathfrak{T}}/\mathbb{F}_2$ *t.q.*

(1) $B_n(\mathrm{H}_{\ell,s}/\mathbb{F}_2) > 0$

(2) $\sum_{i|4} i(B_i + b_i) \geq 2n + 2g(\mathrm{H}_{\ell,s}) - 1$, *avec* $0 \leq b_i \leq B_i(\mathrm{H}_{\ell,s}/\mathbb{F}_2)$.

Application pour $p=2$ et $q=p^2$

Proposition

Si $n \geq \frac{1}{2}(p+1+\epsilon(p))$, *alors il existe un étage* $\mathrm{H}_{\ell,s}$ *de la tour* $\tilde{\mathfrak{T}}/\mathbb{F}_2$ *t.q.*

(1) $B_n(\mathrm{H}_{\ell,s}/\mathbb{F}_2) > 0$

(2) $\sum_{i|4} i(B_i + b_i) \geq 2n + 2g(\mathrm{H}_{\ell,s}) - 1$, *avec* $0 \leq b_i \leq B_i(\mathrm{H}_{\ell,s}/\mathbb{F}_2)$.

On peut appliquer l'algorithme de Chudnovsky-Chudnovsky sur $\mathrm{H}_{\ell,s}/\mathbb{F}_2$ avec :

- des évaluations sur les places de degré 1, 2 et 4,
- b_i places de degré i utilisées pour des évaluations « doubles » : si f est régulière en $P = t\mathcal{O}_P$, alors

$$f = \underbrace{\alpha_0}_{f(P)} + \underbrace{\alpha_1}_{f'(P)} t + \alpha_2 t^2 + \cdots$$

Application pour $p=2$ et $q=p^2$

Proposition

Si $n \geq \frac{1}{2}(p+1+\epsilon(p))$, *alors il existe un étage* $\mathrm{H}_{\ell,s}$ *de la tour* $\tilde{\mathfrak{T}}/\mathbb{F}_2$ *t.q.*

(1) $B_n(\mathrm{H}_{\ell,s}/\mathbb{F}_2) > 0$

(2) $\sum_{i|4} i(B_i + b_i) \geq 2n + 2g(\mathrm{H}_{\ell,s}) - 1$, *avec* $0 \leq b_i \leq B_i(\mathrm{H}_{\ell,s}/\mathbb{F}_2)$.

On peut appliquer l'algorithme de Chudnovsky-Chudnovsky sur $\mathrm{H}_{\ell,s}/\mathbb{F}_2$.

La complexité de l'algorithme de multiplication dans $\mathbb{F}_{2^n}$ obtenu est

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{9}{2}\left(n + g(\mathrm{H}_{\ell,s}) + 1\right) + \frac{9}{4}\sum_{i|4} i b_i .$$

Nouvelles bornes uniformes sur $\mathbb{F}_2$ et $\mathbb{F}_3$ [Ballet, P. (2015)]

- Algorithme de Chudnovsky-Chudnovsky sur $\tilde{\mathcal{T}}/\mathbb{F}_2$:

$$\mu_2^{\mathrm{sym}}(n) \leq \frac{1035}{68}n + \frac{9}{2}.$$

Nouvelles bornes uniformes sur $\mathbb{F}_2$ et $\mathbb{F}_3$ [Ballet, P. (2015)]

- Algorithme de Chudnovsky-Chudnovsky sur $\tilde{\mathcal{T}}/\mathbb{F}_2$:

$$\mu_2^{\text{sym}}(n) \leq \frac{1035}{68}n + \frac{9}{2}.$$

- Algorithme de Chudnovsky-Chudnovsky sur la descente sur $\mathbb{F}_3$ de $\mathcal{T}/\mathbb{F}_9$ **sans étage intermédiaire** :

$$\mu_3^{\text{sym}}(n) \leq \frac{1933}{250}n.$$

Merci pour votre attention.