AG-codes repliables sur des tours de courbes

1 Introduction

Étant donnée une tour de corps de fonctions $(F_i)_{i\geq 0}$, notre objectif sera de construire une suite de codes géométriques $(\mathcal{C}_i)$ sur F_i $(i \geq 0)$; de tel sorte que l'on puisse réduire un test de proximité au "gros" code C_i à un test de proximité sur ses replies successifs (ie. les codes $\mathcal{C}_j$ construit sur les F_j, pour $j \leq i$.
Pour cela, on considérera différentes tours de corps de fonctions, qui vérifient de "bonnes propriétés", du type :

1. On est capable de décomposer un espace de Riemann-Roch sur F_i avec des espaces de Riemann-Roc sur les courbes quotients définies par les F_j, $j \leq i$;
2. On est en mesure de calculer de manière efficace les espaces de Riemann-Roch dans la tour;
3. On connaît la ramification dans la tour (F_i), ainsi qu'une formule du genre $g_i = g(F_i)$ pour tout i;
4. Les corps de fonctions successifs F_i possèdent "beaucoup" de points rationnels, ce qui nous permet de construire des codes géométriques assez longs.

2 La tour Hermitienne

2.1 Généralités

On considère la tour de courbes Hermitienne $(H_i)_{i\geq 0}$ sur $\mathbb{F}_{q^2}$ définie récursivement par l'équation

$$H_i = H_{i-1}(x_i) \ , \ avec \ \ x_i^q + x_i = x_{i-1}^{q+1},$$

et $H_0 = \mathbb{F}_{q^2}(x_0)$ le corps de fonctions rationnel.
Commençons par étudier la ramification dans la tour :

Lemme 1. *Notons $P_\infty^{(0)}$ le pôle de x_0 dans H_0. Alors $P_\infty^{(0)}$ est totalement ramifié dans chaque F_j, et son unique extension $P_\infty^{(j)}$ vérifie*

$$e(P_\infty^{(j)}|P_\infty^{(0)}) = [H_j : H_0] = q^j.$$

Proof. étude classique des extensions d'Artin-Schreier, cf. Stichtenoch. □

La même théorie des extensions d'Artin-Schreier nous permet de montrer que dans le corps de fonctions basique $H = \mathbb{F}_{q^2}(x, y)$, avec $y^q + y = x^{q+1}$ de la tour (H_i); on a

$$(x)^{\mathbb{F}_{q^2}} = P^{(0)} - P_\infty^{(0)},$$

et

$$(y)^H = (q+1)P^{(1)} - (q+1)P_\infty^{(1)};$$

où $P^{(1)}$ est l'unique extension de $P^{(0)}$ qui est un zéro commun de x et y. En appliquant ceci de manière récursive dans la tour, on obtient le lemme suivant :

Lemme 2. *1. $P_\infty^{(0)}$ est l'unique place qui se ramifie dans la tour;*

2. Pour $i \geq 1$, on a

$$(x_i)^{H_i} = (q+1)^i \left(P^{(i)} - P_\infty^{(i)}\right),$$

$P^{(i)}$ étant l'unique zéro commun de $x_0, ..., x_i$;

3. Pour $i \geq 1$, on a

$$(x_{i-1})^{H_i} = (q+1)^{i-1} S^{(i)} - q(q+1)^{i-1} P_\infty^{(i)},$$

où $S^{(i)} = \sum_{j=1}^{q} P_j^{(i)}$, avec $P_j^{(i)} \mid P^{(i-1)}$.

Ensuite, la formule du genre d'Hurwitz nous donne, pour $i \geq 1$:

$$g_i := g(H_i) = 1 - q^i + \frac{1}{2} \cdot \deg\left(\mathrm{Diff}(\mathrm{H_i}/\mathrm{H_0})\right).$$

À partir de ce stade, il n'est pas difficile de déterminer g_i, puisque le différente est uniquement supportée par les points qui se ramifient, et que l'on en a qu'un seul dans cette tour. En particulier, en utilisant la transitivité de la différente (cf. Stichtenoch), ainsi que le fait que pour tout $i \geq 0$, on a

$$d(P_\infty^{(i+1)}|P_\infty^{(i)}) = (q-1)(a_i+1),$$

avec $a_i := \nu_{P_\infty^{(i+1)}}(x_{i+1}) = q+1$, on obtient la formule :

Proposition 1. *On a $g_0 = 0$ et pour tout $i \geq 1$,*

$$\begin{aligned} g_i &= \frac{1}{2} \cdot ((q^2-1)((q+1)^i - q^i) + 1 - q^i) \\ &= \frac{1}{2} \cdot \left(\sum_{k=1}^{i} q^{i+1} \cdot \left(1 + \frac{1}{q}\right)^{k-1} + 1 - (1+q)^i \right) \end{aligned}$$

Concernant le nombre de places rationnelles sur chaque H_i, on peut montrer que pour tout $\alpha \in \mathbb{F}_{q^2}$, la place $P_{x_0-\alpha}$ de H_0 est totalement décomposée dans H_1. Elle possède donc q extensions P_j pour $1 \leq j \leq q$, et chauque P_j est le zéro commun de $x_0 - \alpha$ et $x_1 - \beta_j$ dans H_1, où les β_j sont précisément les racines du polynôme $T^q + T - \alpha^{q+1}$. De nouveaux pas récursivité, et sachant que le pôle de x_0 est totalement ramifié dans la tour, on obtient

Proposition 2. *Pour tout $i \geq 1$, on a*

$$N_i := \#H_i(\mathbb{F}_{q^2}) = q^{i+2} + 1.$$

Dans le but d'obtenir une suite de codes repliables, il nous faut décrire les espaces de Riemann-Roch à un certain étage à partir d'espaces de Riemann-Roch sur les étages inférieurs. Le problème est priori est que le théorème de Kani ne s'applique pas, donc il nous faudra trouver une décomposition à la main. En particulier, il est raisonnable de supposer que les diviseurs associés à nos codes sont seulement supportés par l'unique point ramifiés, ie. $P_\infty^{(i)}$. On se retrouve donc à devoir étudier le comportement des espaces de Riemann-Roch de la forme

$$L_{H_i}\left(rP_\infty^{(i)}\right), \text{ pour } i \geq 1.$$

Or, à un étage i fixé, $P_\infty^{(i)}$ est précisément l'unique pôles de $x_0, ..., x_i$; on a donc le lemme suivant :

Lemme 3. *Pour tout $i \leq 1$ et $r \leq 1$, on a*

$$L_{H_i}(rP_\infty^{(i)}) = \left\{ x_0^{a_0} \cdots x_i^{a_i} \mid a_0 \geq 0 \ , \ a_j \leq q-1 \text{ et } \sum_{j=0}^{i} a_j q^{i-j}(q+1)^j \leq r \right\}.$$

2.2 Construction de codes repliables

On fixe un étage $i_{\max} \geq 1$ dans notre tour Hermitienne. On considère un code géométrique sur $H_{i_{\max}}$ donné par

$$\mathcal{C}_{i_{\max}} := C_L(H_{i_{\max}}, \mathcal{P}_{i_{\max}}, G_{i_{\max}}),$$

où $G_{i_{\max}} = d_{i_{\max}} \cdot P_\infty^{(i_{\max})}$.

Soit $i \leq i_{\max}$. On note G_i le replié de $G_{i_{\max}}$ sur H_i (on verra plus tard comment ces repliés sont construits). Pour tout $0 \leq j \leq q-1$, notons

$$E_{i,j} := \left\lfloor \frac{1}{q} \pi_* \left(G_i - j(x_i)_\infty^{H_i} \right) \right\rfloor,$$

où $\pi : H_i \to H_{i-1}$ est indépendant de i.
À l'aide du lemme 3 utilisé à la fois à l'étage i et à l'étage $i-1$, on peut démontrer à la main la décomposition suivante :

Proposition 3. *On a*

$$L_{H_i}(G_i) = \bigoplus_{j=0}^{q-1} x_i^j \pi^* \left(L_{H_{i-1}}(E_{i,j}) \right).$$

D'après ce qui précède, on serait tenté de construire $G_{i-1} := E_{i,0} = \left\lfloor \frac{r_i}{q} \right\rfloor \cdot P_\infty^{(i-1)}$, où $r_i := deg(G_i)$. De cette manière, on obtient bien

$$G_{i-1} \geq E_{i,j} \ , \ \textit{pour tout } 0 \leq j \leq q-1,$$

ce qui est l'une des conditions demandées pour que G_{i-1} soit G_i-compatible (cf. S. Bordage, J. Nardi, *Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes* pour une définition précise). En revanche,

en construisant les diviseurs repliés de cette manière, on ne parvient pas à les équilibrer. En effet, l'autre condition de compatibilité est de pouvoir trouver des fonctions équilibrantes $\nu_{i-1,j} \in H_{i-1}$ (pour tout j) telles que

$$G_{i-1} - E_{i,j} = (\nu_{i-1,j})_\infty^{H_i}. \qquad (*)$$

Or, ceci n'est pas toujours possible. En effet, on remarque que pour tout $0 \leq j \leq q-1$:

$$G_{i-1} - E_{i,j} = \left\lfloor \frac{r_i - j(q+1)^i}{q} \right\rfloor \cdot P_\infty^{(i-1)}.$$

Pour équilibrer nos diviseurs, il nous faut donc étudier le semi-groupe de Weierstrass de $P_\infty^{(i-1)}$. Par définition, une fonction $\nu \in H_{i-1}$ vérifie $(*)$ si et seulement si ν est polynomiale en les variables $x_0, ..., x_{i-1}$. Par conséquent, on sait précisément quel est le semi-groupe de Weierstrass de $P_\infty^{(i-1)}$, ce qui est l'objet du lemme suivant :

Lemme 4. *Pour $i \geq 1$, on a*

$$\mathcal{H}\left(P_\infty^{(i-1)}\right) = \left\langle q^{i-k}(q+1)^k \ , \ 0 \leq k \leq i-1 \right\rangle_{\mathbb{N}}.$$

On en déduit que le diviseur G_{i-1} ainsi construit est G_i équilibré si et seulement si pour tout $1 \leq j \leq q-1$,

$$\left\lfloor \frac{r_i - j(q+1)^i}{q} \right\rfloor \in \mathcal{H}\left(P_\infty^{(i-1)}\right).$$

Cependant, en étudiant précisément les conditions ci-dessus, on se rend compte rapidement qu'elle n'est pratiquement jamais vérifiée; il nous faut donc construire autrement le diviseur G_{i-1}.

L'idée est la suivante : Pour s'assurer que les entiers $\deg(\mathrm{G_{i-1}} - \mathrm{E_{i,j}})$ ne soient pas des Gaps pour $P_\infty^{(i-1)}$ on augmente le degré du replié pour que ces écart soient automatiquement dans le semi-groupe de Weierstrass. De fait, on sait que

$$\max\left(\mathbb{N} \backslash \mathcal{H}\left(\mathrm{P_\infty^{(i-1)}}\right)\right) \leq 2\mathrm{g_{i-1}} - 1.$$

Ainsi, pour tout entier $i \leq i_{\max}$, on construit le replié G_{i-1} de $G_i := r_i \cdot P_\infty^{(i)}$ en posant

$$G_{i-1} := \left(\left\lfloor \frac{r_i}{q} \right\rfloor + 2g_{i-1} \right) \cdot P_\infty^{(i-1)}.$$

De cette manière, on est sur de pouvoir trouver des fonctions équilibrantes. La contrepartie est que les rendements successifs des codes repliés augmentent, et il faut s'assurer que le code sur $\mathbb{P}^1$ ne soit pas trivial, ie. de rendement > 1.
Dans la section suivante, on étudiera cette question. En particulier, on cherche à déterminer $i_{\max}$ en fonction de q, de sorte que le code $\mathcal{C}_0$ sur $\mathbb{P}^1$ soit non trivial.

2.3 Majoration du rendement sur $\mathbb{P}^1$ et recherche de $i_{\max}$

Afin de contrôler les rendements des différents code dans la tour, commençons par remarquer qu'ils forment une suite croissante, et que le plus gros rendement est celui du code $\mathcal{C}_0$. Afin de majorer ce rendement, on pourra majorer le degré r_0 du diviseur G_0 sur $\mathbb{P}^1$ (puisque ce de degré est pratiquement égal à la dimension du code).
Nos diviseurs repliés étant construit de manière récursive, on peut estimer tous les degrés des diviseurs repliés.

Lemme 5. *Pour $1 \leq j \leq i_{\max}$, on a*

$$d_{i_{\max}-j} \leq \left\lfloor \frac{d_{i_{\max}}}{q^j} \right\rfloor + \sum_{k=1}^{j} \left\lfloor \frac{2g_{i_{\max}-k}}{q^{j-k}} \right\rfloor + (j-1).$$

Proof. par récurrence sur j. □

Afin de donner des valeurs plus concrètes, il nous faut choisir les supports de nos codes. En l'occurrence, on le choisira maximal, ie. composé de toutes les places rationnelles (en dehors bien sur du pôle commun des x_j). En particulier, pour tout $i \leq i_{\max}$, on a dans ce cas :

$$n_i := \#\mathcal{P}_i = q^{i+2}.$$

Le seul élément qu'il nous manque pour majorer d_0 est une majoration sur les genre g_i dans la tour. On s'appuie sur le résultat suivant :

Proposition 4. *Pour $i \geq 1$, on a*

$$g_i \leq \frac{q^{i+1}}{2} \sum_{k=1}^{i} \binom{i}{k} \frac{1}{q^{k-1}} \leq \frac{iq^{i+1}}{2} \sum_{k=1}^{i} \left(\frac{i}{q}\right)^{k-1} \leq \frac{i}{2} q^{i+1} + \frac{i(i-1)}{4} q^i,$$

la dernière majoration utilisant le fait que $i - 1 \leq q$.

Proof. En repartant de la seconde expression de g_i de la proposition 1, on a

$$\begin{aligned}
g_i &= \frac{1}{2} \cdot \left(\sum_{k=1}^{i} q^{i+1} \cdot \left(1 + \frac{1}{q}\right)^{k-1} + \underbrace{1 - (1+q)^i}_{\leq 0} \right) \\
&\leq \frac{q^{i+1}}{2} \cdot \left(\frac{1 - (1+1/q)^i}{1 - (1+1/q)} \right) \\
&= \frac{q^{i+1}}{2} \cdot q \cdot ((1+1/q)^i - 1) \\
&= \frac{q^{i+1}}{2} \cdot \sum_{k=1}^{i} \binom{i}{k} \frac{1}{q^{k-1}}
\end{aligned}$$

À ce stade, remarquons si $kgeq2$, on a $\binom{i}{k} = \dfrac{i(i-1)\cdots(i-k+1)}{k(k-1)\cdots 2} \leq \dfrac{i(i-1)^{k-1}}{2}$, en minorant le dénominateur par 2 et les termes $i-1, i-2, ..., i-k+1$ par $i-1$. En réinjectant dans ce qui précède, on obtient

$$\begin{aligned}
g_i &\leq \frac{q^{i+1}}{2} \cdot \left(i + \frac{i}{2} \sum_{k=2}^{i} \left(\frac{i-1}{q}\right)^{k-1} \right) \\
&= \frac{iq^{i+1}}{2} \left(1 + \frac{1}{2} \cdot \left(\frac{i-1}{q}\right) \cdot \left(\frac{1 - (\frac{i-1}{q})^{i-1}}{1 - (\frac{i-1}{q})} \right) \right) \\
&= \frac{iq^{i+1}}{2} \left(1 + \frac{1}{2} \cdot \frac{i-1}{q-i+1} \cdot \left(\underbrace{1 - \left(\frac{i-1}{q}\right)^{i-1}}_{\leq 0 \ si \ i-1 \leq q} \right) \right) \\
&\leq \frac{iq^{i+1}}{2} \left(1 + \frac{i-1}{2q} \right),
\end{aligned}$$

d'où la majoration souhaitée. □

En utilisant cette majoration du genre et le lemme 5 pour estimer d_0, on a

Corollaire 1. *Avec les notations précédentes, le degré du diviseur G_0 du code replié sur $\mathbb{P}^1$ est majoré par*

$$d_0 \leq \left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor + \frac{i_{\max}(i_{\max}-1)}{2} \cdot \left(q - \frac{2}{3} + \frac{i_{\max}}{3} \right) + (i_{\max} - 1)$$

Proof. D'après le lemme 5 pour $j = i_{\max}$, on a

$$\begin{aligned}
d_0 &\leq \left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor + \sum_{k=1}^{i_{\max}} \left\lfloor \frac{2g_{i_{\max}-k}}{q^{i_{\max}-k}} \right\rfloor + (i_{\max} - 1) \\
&= \left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor + \sum_{k=0}^{i_{\max}-1} \left\lfloor \frac{2g_k}{q^k} \right\rfloor + (i_{\max} - 1) \\
&\leq \left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor + \sum_{k=0}^{i_{\max}-1} \left(kq + \frac{k(k-1)}{2} \right) + (i_{\max} - 1) \\
&= \left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor + (q - \frac{1}{2}) \cdot \frac{i_{\max}(i_{\max}-1)}{2} + \frac{i_{\max}(i_{\max}-1)(2i_{\max}-1)}{12} + (i_{\max} - 1) \\
&= \left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor + \frac{i_{\max}(i_{\max}-1)}{2} \cdot \left(q - \frac{2}{3} + \frac{i_{\max}}{3} \right) + (i_{\max} - 1)
\end{aligned}$$

□

On peut alors déterminer une condition sur $i_{\max}$ en fonction de q pour que le code sur $\mathbb{P}^1$ soit de rendement < 1. En effet, ce rendement ρ_0 peut être estimé par

$$\rho_0 = \frac{k_0}{n_0} = \frac{d_0 + 1}{n_0} \sim \frac{d_0}{n_0}.$$

Si le code à l'étage maximal est construit de longueur maximale, ie. $n_{i_{\max}} = q^{i_{\max}+2}$, on a $n_0 = q^2$. On obtient la condition suivante :

Corollaire 2. *On a l'équivalence :*

$$\rho_0 < 1 \iff \left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor + \frac{i_{\max}(i_{\max}-1)}{2} \cdot \left(q - \frac{2}{3} + \frac{i_{\max}}{3} \right) + (i_{\max} - 1) < q^2.$$

Pour conclure cette section et donner des valeurs concrètes, on supposera que le diviseur à l'étage maximal est de degré

$$d_{i_{\max}} = 2g_{i_{\max}} \leq i_{\max} q^{i_{\max}+1} + \frac{i_{\max}(i_{\max}-1)}{2} q^{i_{\max}}.$$

Notons que cette valeur du degré permet à la fois d'avoir égalité sur la dimension du code grâce à Riemann-Roch, et en même temps d'avoir un rendement "relativement faible" sur le code que l'on veut replier, puisque l'on sait que les repliement successifs vont l'augmenter.
Dans ce cas particulier, la condition du corollaire 2 devient

$$\rho_0 < 1 \iff i_{\max}(q+1) + \frac{i_{\max}(i_{\max}-1)}{2} \cdot \left(q - \frac{2}{3} + \frac{i_{\max}}{3} \right) - 1 < q^2.$$

Notons qu'il s'agit d'un polynôme de degré 3 en $i_{\max}$, et que pour déterminer la valeur de $i_{\max}$ en fonction de q, il nous faut prendre la partie entière de la plus grande racine de ce polynôme.
Le tableau ci-dessous donne différents paramètres sur notre suite de code pour différents choix de q.

Pour espérer avoir une famille de 'gros' codes à rendement constant, on va prendre un diviseur du haut avec un degré plus gros. la dépendance en le degré tant linéaire, ça devrait passer !

Proposition 5. *Let us assume that $i_{\max} = \sqrt{q}$ and that the divisor $G_{i_{\max}}$ has degre $d_{i_{\max}} = \kappa\sqrt{q} g_{i_{\max}}$ for some $\kappa \in (0,1)$. Then the last RS code is non trivial.*

Proof. Using Proposition 4 to bound the genus from above, we have

$$\left\lfloor \frac{d_{i_{\max}}}{q^{i_{\max}}} \right\rfloor \leq \frac{\kappa q}{2} \cdot \left(q + \frac{\sqrt{q}-1}{2} \right)$$

By Corollary 2, a sufficient condition to have $\rho_0 < 1$ is

$$\frac{\kappa q}{2} \cdot \left(q + \frac{\sqrt{q}-1}{2} \right) + \frac{\sqrt{q}(\sqrt{q}-1)}{2} \cdot \left(q - \frac{2}{3} + \frac{\sqrt{q}}{3} \right) + \sqrt{q} - 1 < q^2.$$

The right hand–side term is an increasing function of κ. Hence, if it is satisfied for $\kappa = 1$, it holds for every $\kappa \in (0, 1)$. Simplifying this inequation, we get

$$6(1 + \kappa - 2)q^2 + (3\kappa - 4)q\sqrt{q} - 3(\kappa + 2)q + 16\sqrt{q} - 12 < 0.$$

To prove that the above inequality is true for $\kappa = 1$, it enough to note that the 3-degree polynomial function $-x^3 - 6x^2 + 16x - 12$ takes negative value for any positive x. □

Take an integer r. Let us assume that $q = p^{2r}$ and take $\kappa = p^{-\ell}$ for an $0 < l < 2r$. Then the code $C_L \left(H_{p^r}, H_{p^r}(\mathbb{F}_{p^{4r}}) \setminus \{ {P_\infty}^{(p^r)} \}, \kappa p^3 r P_\infty^{(p^r)} \right)$ is foldable. When $p \to \infty$, the rate of $\mathcal{C}$ tends to $\frac{\kappa}{2}$ and its relative minimum distance is bounded from below by $1 - \frac{\kappa}{2} - \frac{\kappa}{4p^r}$. J'admets que c'est dégueulasse écrit comme ça mais on se comprend !

q	$i_{\max}$	$n_{i_{\max}}$	$k_{i_{\max}}$	n_0	k_0	ρ_0	majorant sur ρ_0
8	3	2^{15}	2^{12}	64	49	0,766	0,844
16	4	2^{24}	2^{21}	256	166	0,648	0,676
27	6	2^{38}	2^{34}	729	597	0,819	0,833
32	7	2^{45}	2^{41}	1024	947	0,925	0,936
64	10	2^{72}	2^{68}	4096	3680	0,898	0,902

3 Une tour récursive optimale

3.1 Définitions et propriétés

Dans cette section, on s'intéressera à une tour récursive, introduite et prouvée optimale par Garcia et Stichtenoch. Cette section s'appuie sur l'article de G. Oliveira et L. Quoos, *Bases for Riemann-Roc Spaces of One-Point Divisors on an Optimal Tower of Function Fields* .