

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par l'Université Toulouse 3 - Paul Sabatier

Présentée et soutenue par

Jade NARDI

Le 12 juin 2019

Quelques retombées de la géométrie des surfaces toriques sur un corps fini sur l'arithmétique et la théorie de l'information

---

Ecole doctorale : **EDMITT - Ecole Doctorale Mathématiques, Informatique et Télécommunications de Toulouse**

Spécialité : **Mathématiques et Applications**

Unité de recherche :

Thèse dirigée par
Marc PERRET et Emmanuel HALLOUIN

Jury

M. Peter BEELEN, Rapporteur
M. Jean-Marc COUVEIGNES, Rapporteur
M. Felipe VOLOCH, Rapporteur
Mme Christine BACHOC, Examinatrice
M. Christophe RITZENTHALER, Examinateur
M. Marc PERRET, Directeur de thèse
M. Emmanuel HALLOUIN, Co-directeur de thèse

Remerciements

Tout d'abord, je voudrais remercier Jean-Marc Couveignes, Peter Beelen et Felipe Voloch d'avoir accepté de relire cette thèse et d'en être rapporteurs.

I warmly thank Felipe Voloch for his welcome in its research team at Canterbury and his quick and accurate answers to my numerous questions.

En plus des rapporteurs qui m'ont fait l'honneur de faire partie du jury, je tiens à remercier les autres membres du jury : Christine Bachoc, Grégoire Lecerf et Christophe Ritzenthaler. Je glisse d'ailleurs un remerciement à ce dernier pour m'avoir fait découvrir la théorie des codes correcteurs en licence. Son cours m'a suffisamment marqué pour que je veuille faire de ce thème le cœur de ma thèse des années plus tard.

Evidemment, je remercie l'ANR *Manta* et tous ses membres. Les nombreuses rencontres organisées par Daniel Augot, Christine Bachoc et Marc Perret ont permis d'enrichissantes rencontres. Sans celles-ci, je n'aurais pas eu l'occasion de travailler à un papier commun avec Julien Lavauzelle, doctorant en informatique chez INRIA à l'époque. Je le remercie d'ailleurs chaleureusement pour cette coopération, qui s'est déroulée à merveille. J'ai pris grand plaisir à travailler sur ce projet qui m'a initiée à des problèmes pratiques de cryptographie. L'ANR *Manta* m'a aussi permis de travailler au sein d'un groupe de travail sur les codes sur les surfaces de Del Pezzo dont je remercie tous les membres pour leur tolérance à mes questions naïves : Régis Blache, Alain Couvreur, Emmanuel Hallouin, David Madore, Matthieu Rambaud, Hugues Randriam. Je remercie Gilles Zemor pour avoir relu l'introduction d'un de mes articles et m'avoir donné de précieux conseils de vocabulaire et de grammaire anglaise. En dehors de ces circonstances de travail, je n'oublie pas les autres participants aux fameuses retraites *Manta* avec lesquels j'ai beaucoup ri. La liste est longue et je préfère ne citer personne plutôt que de froisser les éventuels oubliés. Ils et elles se reconnaitront.

Je remercie également tous les doctorants et les autres membres de l'IMT, pour les bons moments partagés lors des séminaires étudiants.

Je remercie Stéphane Ballet pour l'organisation de la soutenance au CIRM à Luminy.

Naturellement, je remercie chaleureusement ma famille pour leur soutien et les moments de joie et de détente qu'ils ont partagés avec moi ces trois

dernières années, en dépit de la distance qui nous séparait. Un grand merci à ma maman qui a accepté de relire mon “chapeau” en français pour traquer les fautes dans un texte qui lui était presque incompréhensible. Je tiens aussi à remercier mon compagnon, Sebastian, pour sa patience au quotidien, son soutien et ses réponses, plus ou moins utiles, à mes interrogations sur la syntaxe anglaise. Aussi, je remercie mon chien, toujours enclin à faire une balade quand j'ai besoin de m'aérer l'esprit.

Enfin, et surtout, je tiens à remercier mes directeurs de thèse, Emmanuel Hallouin et Marc Perret, pour leur dédication et leur bienveillance. Ils ont eu le courage de supporter mes multiples questions et moi-même, avec le sourire et de nombreuses (bonnes ?) blagues, hebdomadairement pendant ces trois dernières années. Sans leur appui, ma thèse ne serait sans doute pas aussi bien déroulée.

Table des matières

1 Codes sur $\mathcal{H}_\eta$ et applications **5**
- 1.1 Qu'est-ce qu'un code correcteur ? . . . 6
- 1.2 Bornes sur les paramètres . . . 7
- 1.3 Codes de Goppa sur les courbes . . . 8
  - 1.3.1 Codes de Reed-Solomon . . . 8
  - 1.3.2 Codes de Goppa . . . 8
- 1.4 Codes de Goppa sur les variétés de dimension ≥ 2 . . . 9
  - 1.4.1 Codes de Reed-Muller affines et projectifs . . . 10
  - 1.4.2 Distance minimale et nombre de points de variétés . . . 10
  - 1.4.3 Estimation des paramètres . . . 10
- 1.5 Codes toriques . . . 13
- 1.6 Codes sur les surfaces de Hirzebruch . . . 13
  - 1.6.1 Qu'est-ce qu'une surface de Hirzebruch ? . . . 14
  - 1.6.2 Code d'évaluation . . . 16
- 1.7 Propriétés locales et applications . . . 19
  - 1.7.1 Applications au PIR . . . 20
- 1.8 Améliorer le taux de transmission grâce au *lift*. . . . 23
  - 1.8.1 Lifter par rapport aux droites . . . 23
  - 1.8.2 Lifter par rapport aux η-droites . . . 24

2 Majorer le nombre de points **27**
- 2.1 Motivation . . . 27
- 2.2 Stratégie . . . 27
  - 2.2.1 Borne de Hasse-Weil . . . 28
  - 2.2.2 Majorer le nombre de points rationnels . . . 28
  - 2.2.3 Choisir d'autres fibrés . . . 30

3 Codes sur les surfaces de Hirzebruch **37**

4 Bornes sur les courbes **77**

5 PIR et lift **97**

Chapitre 1

Codes correcteurs d'erreurs sur les surfaces de Hirzebruch et applications

L'émergence des technologies dans les années 50, telles que les réseaux téléphoniques, les communications par satellite, les disques optiques, soulève la question de l'amélioration et de la préservation de la qualité des systèmes de transmissions de données à travers l'espace et le temps. Une réponse a été apportée par la théorie de l'information développée par C.E. Shannon, en particulier à travers les codes correcteurs.

Concrètement, on veut transmettre un message m qui risque d'être détérioré lors de la transmission. On souhaite que le destinataire puisse détecter, voire corriger, les erreurs éventuelles. Pour ce faire, l'idée est d'utiliser de la redondance. C'est le rôle des *clés* des séries de chiffres qu'on utilise au quotidien, telles que le cryptogramme au dos de la carte bancaire ou encore les deux derniers chiffres du numéro de sécurité sociale en France.

Attardons-nous sur ce dernier exemple. Le numéro de sécurité sociale est formé de 15 chiffres. Les 13 premiers rassemblent des informations comme le sexe ainsi que l'année, le mois, le département et la commune de naissance. Les deux derniers chiffres, en revanche, forment un nombre compris entre 0 et 96 tel que la somme de ce nombre avec celui formé des 13 premiers chiffres est un multiple de 97. Ainsi, en ajoutant une clé de seulement 2 chiffres, si l'on se trompe d'un chiffre en remplissant notre numéro de sécurité sociale sur un formulaire, l'organisme récepteur est en mesure de savoir qu'il y a une erreur et peut nous redemander notre numéro. En revanche, il lui est impossible de corriger l'erreur.

Une idée naïve pour corriger une erreur de transmission est de renvoyer plusieurs fois le même message. Disons que je veuille envoyer deux bits, par

exemple 00. Si je double mon message en envoyant 0000, une erreur sur l'un des bits sera immédiatement détectée mais non corrigible. En revanche, si j'envoie 000000, le récepteur est en mesure de détecter et de corriger une éventuelle erreur de transmission. Cette méthode fonctionne mais n'a pas un bon taux de transmission : on triple la longueur du message pour corriger une seule erreur.

1.1 Qu'est-ce qu'un code correcteur ?

Soit p un nombre premier, $e \in \mathbb{N}^*$ et $q = p^e$. On suppose que le message à transmettre est un vecteur $m \in (\mathbb{F}_q)^k$. On détermine une fonction injective, dite d'encodage, $E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$. Le code correcteur C qui en résulte est l'image de l'application E. Le taux de transmission du code, noté κ, est le ratio de k par n. Lors de la transmission de $E(m) = x$ à travers le canal, le message a pu être altéré par une erreur $e \in \mathbb{F}_q^n$ et le récepteur reçoit le mot $y = x + e$. Idéalement, le but est de déterminer une fonction de décodage $D : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^k$ telle que $D \circ E = \mathrm{Id}$ et qui fait correspondre à tout vecteur reçu y un vecteur corrigé qui soit l'un des mots du code le plus vraisemblablement émis.

C. E. Shannon garantit qu'il existe des codes avec le meilleur taux de transmission souhaitable et une probabilité d'erreur aussi petite que l'on veut. Cependant son approche probabiliste présente l'inconvénient de ne pas être constructive. M. Golay et R. Hamming proposent donc une autre approche. Ils construisent explicitement des systèmes remplissant les conditions voulues, en considérant des codes linéaires, c'est-à-dire tels que l'application d'encodage E est une application linéaire de $\mathbb{F}_q$-espaces vectoriels. Un code linéaire est alors un sous-espace vectoriel C de $(\mathbb{F}_q)^n$ de dimension k.

A tout mot $x \in C$, on associe un poids

$$\omega(x) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}.$$

Pour déterminer le mot le plus vraisemblablement émis, on définit une distance entre les mots. Pour tout $(x, y) \in \mathbb{F}_q^n$, on pose

$$d(x, y) = \#\{i \in \{1, \dots, n\} \mid x_i \neq y_i\} = \omega(x - y)$$

Cela nous permet de définir un paramètre essentiel d'un code linéaire, sa distance minimale :

$$d(C) = \min\{d(x, y) \mid x, y \in C,\ x \neq y\} = \min_{x \in C} \omega(x).$$

La distance minimale est liée à la capacité de correction du code. Un code linéaire de distance minimale d est en mesure de décoder $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ erreurs.

Des méthodes récentes de détection d'erreurs améliore cette capacité de correction mais celle-ci n'excède pas la distance minimale.

Un code linéaire sur $\mathbb{F}_q$ de longueur n, de dimension k et de distance minimale d est dit $[n, k, d]_q$.

1.2 Bornes sur les paramètres des codes correcteurs

Le but est d'avoir un *bon code*, avec un taux de transmission $\kappa = \frac{k}{n}$ et une capacité de correction $\delta = \frac{d}{n}$ proches de 1. Évidemment, il existe un compromis entre ces deux quantités, qui ne peuvent pas être toutes deux aussi proches de 1 qu'on le souhaite. Plusieurs bornes, résumées par D. Augot [Aug10] par exemple, relient les paramètres d'un code linéaire.

La borne de Singleton affirme que tout code linéaire de paramètres $[n, k, d]$ vérifie $k + d \leq n + 1$. Autrement dit, $\kappa + \delta \leq 1 + \frac{1}{n}$. Un code qui atteint cette borne est dit MDS (*Maximum Distance Separable*). Les codes de Reed-Solomon (voir paragraphe 1.3.1) sont MDS.

Une autre borne, d'une nature tout à fait différente, dite de *Varshamov-Gilbert asymptotique*, considère la fonction d'entropie

$$H_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x).$$

Ce résultat assure que si $R \leq 1 - H_q(\delta)$, alors il existe une famille de codes linéaires $(C_i)_i$ de longueur n_i, de dimension k_i et de distance minimale d_i, telle que

$$\lim_{i \to +\infty} n_i = +\infty \lim_{i \to +\infty} \frac{k_i}{n_i} = \kappa \quad \text{et} \lim_{i \to +\infty} \frac{d_i}{n_i} = \delta.$$

En fait, on peut montrer que si l'on tire au hasard un code de longueur n et de dimension k, alors son taux de transmission et sa capacité de transmission ne sont pas loin de réaliser la borne de Varshamov-Gilbert asymptotique. Sa distance minimale sera telle que $\frac{k}{n} \simeq 1 - H_q(\frac{d}{n})$, avec probabilité tendant vers 1, quand n tend vers l'infini.

On a longtemps cru que la borne de Varshamov-Gilbert était une borne supérieure. M. A. Tsfasman, S. G. Vlăduţ and Th. Zink [TVZ82] montrent en 1982 que les codes de Goppa dépassent la borne de Varshamov-Gilbert dans le cas des corps de grand cardinal.

1.3 Codes de Goppa sur les courbes

1.3.1 Codes de Reed-Solomon

Soit $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$ et $k \leq n$. Le *code de Reed-Solomon* de degré $k-1$ sur $\mathbb{F}_q$, noté $\mathrm{RS}_q(k-1)$, est défini par

$$\mathrm{RS}_q(k-1) = \{(f(\alpha_1), \ldots, f(\alpha_n)),\ f \in \mathbb{F}_q[X]_{\leq k-1}\}.$$

On montre aisément que c'est un code de type $[n, k, n-k+1]$.

Ce code est facilement décodable. Intuitivement, on sent que la structure polynomiale permet d'utiliser des outils d'interpolation pour corriger les erreurs une fois que leur position est connue. Si le nombre d'erreurs est inférieur à t, on peut montrer que trouver les erreurs revient à résoudre un système linéaire. L'algorithme de Guruswami-Sudan [Gur05] utilise une interpolation avec "multiplicités" qui permet de décoder plus que la capacité de correction classique t du décodage unique.

Par ailleurs, ce code MDS est toujours de longueur plus petite que la taille de l'alphabet. Les codes de Goppa [Gop77], appelés aussi "codes algébriques" permettent un plus large choix de points d'évaluation.

1.3.2 Codes de Goppa

Soient X une courbe de genre g, un diviseur G de X et n points distincts $P_1, \ldots, P_n$ de X. On pose $D = P_1 + \cdots + P_n$. Le code de Goppa sur X associé à D et G est défini par l'ensemble des évaluations [1] des sections globales de G en les points P_i :

$$C_{\mathcal{L}}(D, G) = \{f(P_1), \ldots, f(P_n) \mid f \in \mathcal{L}(G)\} \subset \mathbb{F}_q^n.$$

On rappelle quelques propriétés de ces codes (voir [Sti09] pour les détails et les preuves).

Le code $C_{\mathcal{L}}(D, G)$ a pour paramètres $[n, k, d]$ avec

$$k = l(G) - L(G - D) \text{ et } d \geq n - \deg G.$$

Si G est de degré inférieur à n, alors $\deg(G - D) < 0$, donc $l(G - D) = 0$ et $k = l(G)$, c'est-à-dire que l'évaluation est injective. De plus, $l(G) \geq$

1. Si l'on veut être précis, l'évaluation telle quelle n'est pas bien définie, notamment si l'un des P_i est un pôle d'un $f \in L(G)$. Certains choisissent donc d'exiger aux points P_i de ne pas être supportés par G. Même si ce choix permet une définition simple de l'application d'évaluation, il se heurte à un autre problème : d'après le Moving Lemma, il existe un diviseur G' linéairement équivalent à G qui contient l'un des P_i. Néanmoins, deux codes linéaires associés à des diviseurs linéairement équivalents doivent être Hamming-équivalents et donc, aussi bien définis l'un que l'autre. La meilleure solution est donc de définir l'évaluation de f en un point P comme $f(P)t^e$ où t est une uniformisante autour de P et e est l'ordre du pôle de f en P.

$\deg G + 1 - g$. Par conséquent,

$$k + d \geq n + 1 - g \text{ c'est-à-dire } \kappa + \delta \geq 1 + \frac{1}{n} - \frac{g}{n}$$

Le théorème de Riemann-Roch assure que si $2g - 2 < \deg G < n$, alors $k = \deg G + 1 - g$.

Cette notion étend celle des codes de Reed-Solomon, qui sont des codes de Goppa sur $\mathbb{A}^1$.

Longueur d'un code de Goppa - La longueur d'un code de Goppa sur une courbe X est limitée par le nombre de points $\mathbb{F}_q$-rationnels. De plus, $\kappa + \delta$ grandit quand $\frac{n}{g}$ grandit.

Une *bonne famille de codes* sur $\mathbb{F}_q$ est une suite de codes (C_i) de paramètres $[n_i, k_i, d_i]$ tels que $\lim n_i = +\infty$, $\limsup \frac{d_i}{n_i} > 0$ et $\limsup \frac{k_i}{n_i} > 0$.

Ainsi, pour construire de bonnes familles de codes algébriques asymptotiques, on peut s'intéresser à la quantité

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

où $N_q(g)$ est le nombre maximal de $\mathbb{F}_q$-points sur une courbe de genre g. D'un point de vue asymptotique, les paramètres d'un code géométrique sur une courbe de grand genre ayant beaucoup de points vérifient

$$\kappa + \delta = 1 - \frac{1}{A(q)}.$$

Un résultat important de Drinfeld-Vladut affirme que $A(q) \leq \sqrt{q} - 1$. M. A. Tsfasman, S. G. Vlăduţ and Th. Zink [TVZ82] montrent qu'il y a égalité si q est un carré. Par ailleurs, on peut construire de manière explicite en temps polynomial une famille de codes géométriques avec $\kappa + \delta = 1 - \frac{1}{\sqrt{q}-1}$. Pour $q \geq 49$, cette borne est meilleure que la borne de Varshamov-Gilbert. En revanche, pour $q = 2$, on a $A(2) < 1$, et les codes construits via cette méthode n'ont aucun intérêt, puisqu'alors $\kappa + \delta < 0$.

Ainsi, pour avoir une bonne famille asymptotique de codes sur des petits corps, notamment sur $\mathbb{F}_2$ – cas qui intéresse majoritairement les codeurs –, il est naturel de généraliser la définition des codes de Goppa à des variétés de dimension plus grande.

1.4 Codes de Goppa généralisés aux variétés de dimension ≥ 2

Depuis les années 2000, le cadre d'étude suivant est posé : on fixe

— Une variété projective X définie sur $\mathbb{F}_q$,
— Un ensemble de n points $\mathbb{F}_q$-rationnels $\mathcal{P} = \{P_1, \ldots, P_n\} \subset X(\mathbb{F}_q)$,
— Un diviseur G de X,
et on définit le code linéaire $C(X, G, \mathcal{P})$ comme l'image de l'*application d'évaluation*

$$\alpha : \begin{cases} L(G) & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{cases}$$

où $L(G) = \{f \in \mathbb{F}_q(X) \mid (f) + G \geq 0\} \cup \{0\}$.

1.4.1 Codes de Reed-Muller affines et projectifs

Parmi les codes de Goppa généralisés les plus simples, on compte ceux de Reed-Muller. Ces codes de Goppa sur $X = \mathbb{A}^r$, ou $X = \mathbb{P}^r$ dans le cas projectif, associés à un diviseur de degré d sur $\mathbb{F}_q$ avec $\mathcal{P} = X(\mathbb{F}_q)$ sont notés $\mathrm{RM}_q(r, d)$, ou $\mathrm{PRM}_q(r, d)$ dans le cas projectif. Si $r = 1$, on retrouve le code de Reed-Solomon affine $\mathrm{RM}_q(1, d) = \mathrm{RS}_q(d)$ ou projectif $\mathrm{PRM}_q(1, d) = \mathrm{PRM}_q(d)$. Les paramètres des codes de Reed-Muller sont entièrement déterminés par A. B. Sørensen [Sør92].

1.4.2 Distance minimale et nombre de points de variétés

Un tel code a pour distance minimale

$$d = n - \max_{\substack{H \sim G \\ H \text{ effectif}}} \#H \cap \mathcal{P}$$

quand l'évaluation est injective, c'est-à-dire lorsque le terme de droite est strictement positif.

Ainsi, minorer [2] la distance minimale revient à majorer le nombre de points parmi ceux de $\mathcal{P}$ qui sont sur une hypersurface linéairement équivalente à G. La plupart des codes de Goppa étudiés choisissent $\mathcal{P} = X(\mathbb{F}_q)$. Dans ce cas, il faut majorer le nombre de points rationnels d'hypersurfaces de X de classe de Picard donnée. *Autrement dit, on s'intéresse au nombre de points de variétés avec deux contraintes : elles sont plongées dans un ambiant donné et ont toutes même classe de Picard.*

1.4.3 Estimation des paramètres

Généraliser à des dimensions plus grandes est une opération très naturelle mais n'est pas sans ajouter de difficultés à l'estimation des paramètres. En effet, dans le cas courbe, $P_1 + P_2 + \cdots + P_n$ est un diviseur de X, au même titre que G. Ainsi le théorème de Riemann-Roch donne à la fois une majoration de

2. Si on n'arrive pas à déterminer explicitement la distance minimale, les codeurs s'intéressent toujours à une minoration de celle-ci, puisqu'elle fournit une minoration de la capacité de correction. Une majoration n'a que très peu d'intérêt.

la dimension - voire la dimension exacte si α est injective – et une minoration de la distance minimale en considérant les diviseurs G et $G-P_1-P_2-\cdots-P_n$ (voir [Sti09]).

En dimension supérieure, on peut toujours utiliser le théorème de Riemann-Roch pour appréhender la dimension mais pas la distance minimale.

Dans un premier temps, on peut espérer des estimations sur la distance minimale qui dépendraient d'invariants de la surface, à la manière du genre pour le cas des courbes. Dans cette optique, S. H. Hansen [Han01] propose la constante de Seshadri.

Constante de Seshadri - Soit X une variété projective de dimension au moins 2, un ensemble $\mathcal{P} = \{P_1 \ldots, P_n\} \subset X(\mathbb{F}_q)$ et un diviseur G de X. On note $\mathcal{I}$ le faisceau d'idéaux de la variété formée par les P_i dans X.

Une solution pour rétablir la symétrie entre les points d'évaluation et le diviseur du code de Goppa est d'éclater la variété X en les points P_i pour en faire des diviseurs.

On pose donc $\pi : X' \to X$ le morphisme d'éclatement et E_i le diviseur exceptionnel au-dessus du point P_i pour $i \in \{1, \ldots, n\}$.

Ce contexte permet de définir la *constante de Seshadri* de G en D comme suit :

$$\epsilon(G, \mathcal{P}) = \sup\{\epsilon \in \mathbb{Q} \mid \pi^* G - \epsilon \sum_{i=1}^{n} E_i \text{ est nef}\}.$$

S. H. Hansen [Han01] montre que si G est ample et de constante de Seshadri $\epsilon(G, \mathcal{P}) \geq \epsilon$ avec $\epsilon \in \mathbb{N}$, alors la distance minimale du code $C(G, \mathcal{P})$ vérifie

$$d \geq n - \epsilon^{1-\dim X} G^{\dim X}.$$

Si, en plus, il existe $\zeta \in \mathbb{N}$ tel que $\mathcal{L}(G)^{\otimes \zeta} \otimes \mathcal{I}$ est engendré par ses sections globales, alors

$$d \geq n - \zeta^{\dim X - 1} G^{\dim X}.$$

La constante de Seshadri offre donc une formule agréable pour la minoration. Malheureusement, celle-ci est la plupart du temps incalculable en pratique.

Système $\mathcal{P}$-couvrant - S. H. Hansen [Han01] a aussi étudié le problème des codes sur les surfaces et a proposé une autre stratégie : celle des ensembles $\mathcal{P}$-couvrants.

Soit X une surface projective lisse. On cherche m courbes irréductibles $C_1, \ldots, C_m$ sur X telles que $\mathcal{P} = \bigcup_{i=1}^{m} C_i(\mathbb{F}_q)$. Un tel ensemble de courbes est dit $\mathcal{P}$-couvrant.

S. H. Hansen montre que si chaque C_i a au plus N points $\mathbb{F}_q$-rationnels et que $G.C_i \geq 0$, ce qui est toujours le cas si G est numériquement effectif,

alors en posant

$$l = \sup_{s \in L(G)} \#\{i \mid C_i \subseteq (s) + (G)\},$$

la distance minimale du code $C(G, \mathcal{P})$ vérifie $d \geq n - lN - \sum_{i=1}^{m} G.C_i$.

Si de plus, H est un diviseur nef de X tel que $H.C_i > 0$, alors

$$l \leq \frac{G.H}{\min_i\{C_i.H\}}.$$

Bons codes et rang de Picard - Un article de M. Zarzar [Zar07] met en évidence que les surfaces de faible rang de Picard arithmétique sont susceptibles de produire des bons codes.

A. Couvreur [Cou11] exploite cette idée pour trouver un fibré en droites dont les sections globales ont peu de points. D'après J.-P. Serre [Ser00], les courbes qui contiennent le plus de points dans le plan sont les réunions de droites. Pour éviter cette configuration, A. Couvreur considère le sous-système linéaire des sections globales qui s'annulent en un certain nombre de points irrationnels conjugués. Cela revient à considérer un code de Goppa associé à un système linéaire complet sur l'éclaté du plan projectif en ces points. De plus, quand on éclate $\mathbb{P}^2$ en un point, le rang de Picard géométrique augmente d'autant que du degré du point qu'on éclate mais le rang arithmétique n'augmente que de 1. En contractant une droite rationnelle, A. Couvreur se retrouve donc sur une surface au rang de Picard arithmétique égal à 1 sur laquelle il construit d'excellents codes qui battent même les meilleurs paramètres connus sur un corps fixé.

J. Little et H. Schenck [LS18] proposent par la suite une étude prospective des codes sur les surfaces de rang de Picard arithmétique égal à 1. En supposant que le groupe de Picard X est engendré par un diviseur ample H, ils montrent que le nombre maximal de composantes $\mathbb{F}_q$-irréductibles d'une section globale de $\mathcal{L}(mH)$ vaut au plus m. Ils en déduisent une minoration de la distance minimale pour le code $C(X, H, X(\mathbb{F}_q))$ dans le cas où H est la section hyperplane de X. Cette minoration, conséquence de la Borne de Hasse-Weil, dépend aussi du genre arithmétique de H : plus il est petit, meilleure est la distance minimale.

Après avoir cherché empiriquement des surfaces de rang de Picard arithmétique égal à 1 parmi les cubiques de $\mathbb{P}^3$, J. Little et H. Schenck suggèrent de s'intéresser aux surfaces munies d'un diviseur de genre nul, décrits par M. Andreatta et E. Ballico [AB90] : les droites et les coniques de $\mathbb{P}^2$, les sections hyperplanes d'une quadrique lisse de $\mathbb{P}^3$ et une famille de diviseurs sur les surfaces de Hirzebruch. Sur $\mathbb{P}^2$, ceci correspond aux codes de Reed-Muller $\mathrm{RM}_q(2,1)$ et $\mathrm{RM}_q(2,2)$. Les paramètres des codes sur la quadrique lisse sont aussi connus (voir [CD13] par exemple). Quant aux surfaces de Hirzebruch, des codes toriques (voir section 1.5) y ont été

considérés. Les paramètres d'un code de Goppa sur une surface de Hirzebruch dans le cas d'une évaluation sur la totalité des points rationnels sont établis dans cette thèse (Théorème 1).

À base d'éclatements et de contractions, R. Blache *et al* [BCH+19] construisent des surfaces de Del Pezzo de groupe Picard arithmétique est engendré par le diviseur anticanonique. Dans ce papier, les surfaces de Del Pezzo de rang 1 sont passées en revue et un modèle $\mathbb{F}_q$-birationnel est donné par chacune d'elles. Cela permet de construire explicitement les codes, qui s'avèrent dans certains cas avoir des paramètres aussi bons voire meilleurs que ceux connus jusqu'alors.

1.5 Codes toriques

Parmi les codes sur les surfaces considérés jusqu'à maintenant se distinguent les *codes toriques*. Introduits par J. P. Hansen [Han02] puis étudiés par D. Joyner [Joy04], J. Little and H. Schenck [LS06], D. Ruano [Rua07] ou encore I. Soprunov et J. Soprunova [SS09], ce sont des codes de Goppa sur des variétés toriques dont les points d'évaluation sont seulement ceux du tore. Ils présentent l'avantage de pouvoir être implémentés sans même savoir ce qu'est une variété torique. Pour construire un code sur une surface torique, il suffit de se donner un polygone [3] Δ dans $\mathbb{R}^2$ et on construit le code engendré par les $x^i y^j$ où $(i,j) \in \Delta \cap \mathbb{Z}^2$ et $(x,y) \in (\mathbb{F}_q^*)^2$.

Les paramètres d'un tel code sont étroitement liés à la combinatoire du polygone qui le définit. Le pont entre polynômes et polygones est réalisé par la notion de polygone de Newton [4] d'un polynôme. D. Ruano [Rua07] montre que le noyau de l'évaluation est engendré par des binômes $x^i y^j - x^{i'} y^{j'}$ tels que $q-1$ divise $i'-i$ et $j'-j$. Par conséquent, la dimension du code correspond au cardinal de Δ modulo $q-1$. I. Soprunov et J. Soprunova [SS09] donnent la forme des polynômes qui correspondent aux mots de poids minimal en fonction de la longueur de Minkowsky du polygone.

1.6 Codes sur les surfaces de Hirzebruch

Plutôt que de chercher à établir une estimation des paramètres d'un code sur une surface générale, j'ai donc préféré me concentrer sur une certaine catégorie de surfaces. En étudiant les travaux déjà réalisés à ce sujet, mon attention s'est portée sur un travail de C. Carvhalo et V. Neumann [CN16] sur les scrolls rationnels de dimension 2, autrement appelés *surfaces de Hirzebruch*.

3. On peut demander que le polygone soit entier, c'est-à-dire à sommets à coordonnées entières. Ceci est vrai si le diviseur choisi pour construire le code de Goppa est ample.

4. Si $f = \sum_{(i,j)\in\mathbb{Z}^2} a_{ij} x^i y^j$, le polygone de Newton de f, noté $\Delta(f)$, est défini comme l'enveloppe convexe de $\{(i,j) \in \mathbb{Z}^2 \mid a_{ij} \neq 0\}$.

1.6.1 Qu'est-ce qu'une surface de Hirzebruch ?

À chaque entier naturel $\eta \in \mathbb{N}$, on fait correspondre une surface de Hirzebruch, que l'on notera [5] $\mathcal{H}_\eta$. Plusieurs points de vue sont possibles pour la définir.

Quotient géométrique - La surface de Hirzebruch $\mathcal{H}_\eta$ peut-être décrite comme le quotient géométrique d'une variété affine par l'action d'un groupe algébrique ([CLS11] Théorème 5.1.11). Cette description est donnée par exemple par M. Reid [Rei97].

On définit une action de $\mathbb{G}_m \times \mathbb{G}_m$ sur $\left(\mathbb{A}^2 \setminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \setminus \{(0,0)\}\right)$: écrivons (t_1, t_2) pour le premier jeu de coordonnées sur $\mathbb{A}^2$, (x_1, x_2) pour le second et (λ, μ) pour les éléments de $\mathbb{G}_m \times \mathbb{G}_m$. On pose

$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu \lambda^{-\eta} x_1, \mu x_2).$$

La surface de Hirzebruch $\mathcal{H}_\eta$ est isomorphe à

$$\left(\mathbb{A}^2 \setminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \setminus \{(0,0)\}\right) / \mathbb{G}_m^2.$$

Cette description permet de se rendre compte de façon évidente que $\mathcal{H}_0$ n'est rien d'autre que $\mathbb{P}^1 \times \mathbb{P}^1$. Aussi, comme pour les espaces projectifs, on choisit des représentants des orbites sous l'action de $\mathbb{G}_m^2$ de la forme suivante : $(1, a, 1, b)$, $(0, 1, 1, b)$, $(1, a, 0, 1)$ ou $(0, 1, 0, 1)$ avec $(a, b) \in \overline{\mathbb{F}}$. Autrement dit, toute orbite de $\left(\mathbb{A}^2 \setminus \{(0,0)\}\right)^2$ contient un et un seul élément de cette forme, que l'on choisit être le représentant d'un point.

Sous-variété déterminantale de $\mathbb{P}^{\eta+3}$ - Ce point de vue permet d'appréhender cette surface en la plongeant dans un espace projectif. Posons

$$\iota : \left\{ \begin{array}{ccc} \mathcal{H}_\eta & \to & \mathbb{P}^{\eta+3} \\ (t_1, t_2, x_1, x_2) & \mapsto & [t_1^{\eta+1} x_1, t_1^\eta t_2 x_1, \ldots, t_2^{\eta+1} x_1, t_1 x_2, t_2 x_2] \end{array} \right. . \quad (1.1)$$

On montre facilement que ι une immersion fermée. L'image de ι est appelée un *scroll rationnel*.

Soient $(a_1, a_2) \in \mathbb{N}^2$. Grosso modo, pour construire le scroll rationnel $S(a_1, a_2)$ de dimension 2, on considère les deux courbes rationnelles C_1 et C_2 de degré respectif a_1 et a_2, c'est-à-dire des courbes isomorphes à $\mathbb{P}^1$ plongées dans $\mathbb{P}^{a_i}$ via le morphisme $\phi_i : (s, t) \mapsto (s^j t^{a_i - j})_{j \in \{0, \ldots, a_i\}}$ pour $i \in \{1, 2\}$. On fixe aussi un isomorphisme $\psi : \mathbb{P}^1 \to \mathbb{P}^1$. Dans l'espace projectif $\mathbb{P}^{a_1+a_2+1}$,

5. Dans la littérature, les surfaces de Hizerbuch sont paramétrées par un entier n. Néanmoins, cette lettre est déjà consacrée à la longueur d'un code linéaire. De plus, la surface de Hirzeburch associée à l'entier n est souvent notée $\mathbb{F}_n$ par les géomètres complexes, notation fort peu heureuse quand on fait de la géométrie sur les corps finis.

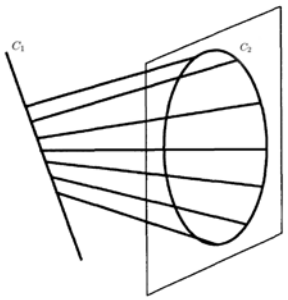


FIGURE 1.1 – Scroll $(1, 2)$ dans $\mathbb{P}^4$ [Har95]

deux copies de $\mathbb{P}^{a_1+1}$ et de $\mathbb{P}^{a_2+1}$ peuvent être supplémentaires. Le scroll se forme en reliant $\phi_1(P)$ à $\phi_2(\psi(P))$ pour tout $P \in \mathbb{P}^1$, comme illustré par la Figure 1.1. Notons que l'application ι a exactement pour image le scroll $S(1, \eta + 1)$.

Variété torique - La surface $\mathcal{H}_\eta$ est la variété torique associée à l'éventail Σ_η (see Figure 1.2) formé de 4 rayons $\rho_1, \ldots, \rho_4$ engendrés respectivement par $u_1 = (1, 0)$, $u_2 = (0, 1)$, $u_3 = (-1, \eta)$ et $u_4 = (0, -1)$.

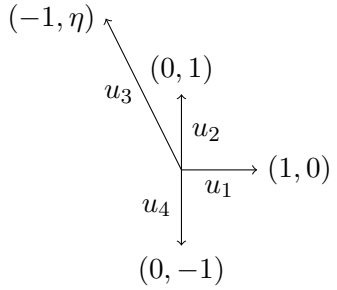


FIGURE 1.2 – Eventail Σ_η

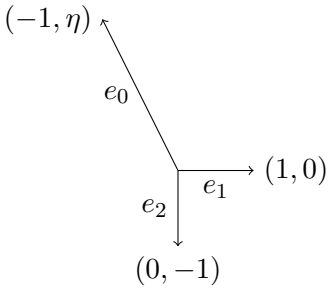


FIGURE 1.3 – Eventail de $\mathbb{P}(1, 1, \eta)$

Remarquons que l'éventail Σ met en évidence que la variété $\mathcal{H}_\eta$ est un éclatement de $\mathbb{P}(1, 1, \eta)$, puisque cet éventail est construit en ajoutant un rayon colinéaire à la somme de ses voisins à celui de $\mathbb{P}(1, 1, \eta)$ (voir Figure 1.3).

À chaque rayon, on associe une variable et donc un diviseur qui correspond au lieu où la variable associée s'annule. Ici, les variables sont appelées t_1, x_1, t_2, x_2 (dans le sens trigonométrique par rapport aux rayons). L'anneau $R = \mathbb{F}_q[t_1, t_2, x_1, x_2]$ est appelé l'*anneau de Cox* de $\mathcal{H}_\eta$.

La théorie des variétés toriques nous renseigne sur la théorie de l'intersection de cette surface. Le groupe de Picard de $\mathcal{H}_\eta$ est engendré par les diviseurs associés aux rayons de l'éventail. Plus précisément,

$\mathrm{Pic}(\mathcal{H}_\eta) = \mathbb{Z}D_{\rho_1} + \mathbb{Z}D_{\rho_2}$ avec

$$D_{\rho_3} \sim D_{\rho_1} \text{ et } D_{\rho_4} \sim D_{\rho_2} + \eta D_{\rho_1}.$$

On connaît aussi la forme d'intersection.

$$D_{\rho_1}^2 = 0, \quad D_{\rho_2}^2 = -\eta, \quad D_{\rho_1} \cdot D_{\rho_2} = 1. \tag{1.2}$$

L'anneau de Cox est muni d'une graduation indexée par le groupe de Picard $\mathrm{Pic}(\mathcal{H}_\eta)$ définie par l'éventail. Le lieu d'annulation du monôme $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$ de R est un diviseur

$$D_M = d_1 D_{\rho_2} + d_2 D_{\rho_4} + c_1 D_{\rho_1} + c_2 D_{\rho_3}. \tag{1.3}$$

Le degré de M est défini comme la classe de Picard du diviseur D_M.

À chaque base du groupe de Picard, on associe une définition du *bidegré*[6] d'un polynôme. Par exemple, dans la base $[D_{\rho_1}, D_{\rho_2}]$, on dit que le monôme M est de bidegré (α, β) si $D_M \sim \alpha D_{\rho_1} + \beta D_{\rho_2}$, c'est-à-dire si

$$\begin{cases} \alpha &= c_1 + c_2 + \eta d_2, \\ \beta &= d_1 + d_2. \end{cases} \tag{1.4}$$

On peut choisir une autre base, liée à la géométrie de la surface. La surface $\mathcal{H}_\eta$ est réglée : le morphisme qui à $(t_1, t_2, x_1, x_2) \in (\mathbb{A}^2 \setminus \{(0,0)\})^2$ associe $(t_1, t_2) \in \mathbb{A}^2 \setminus \{(0,0)\}$ est compatible avec l'action de $\mathbb{G}_m^2$ sur le domaine et celle de $\mathbb{G}_m$ sur le codomaine. On a donc une application régulière $\mathcal{H}_\eta \to \mathbb{P}^1$. On note $\mathcal{F}$ la classe d'une de ses fibres et σ celle d'une de ses sections. Alors $\mathcal{F} \sim D_{\rho_1}$ et $\sigma \sim D_{\rho_4} \sim D_{\rho_2} + \eta D_{\rho_1}$. Dans la base $[\mathcal{F}, \sigma]$, on dit que le monôme M est de bidegré (δ_T, δ_X) si $D_M \sim \delta_T \mathcal{F} + \delta_X \sigma$, c'est-à-dire si

$$\begin{cases} \delta_T &= c_1 + c_2 - \eta d_1, \\ \delta_X &= d_1 + d_2. \end{cases} \tag{1.5}$$

On utilise la seconde base dans le cadre des codes. Cela nous fournit une graduation de R comme suit :

$$R = \bigoplus_{(\delta_T, \delta_X) \in \mathbb{Z}^2} R(\delta_T, \delta_X)$$

où $R(\delta_T, \delta_X) \simeq H^0(\mathcal{H}_\eta, \mathcal{O}_{\mathcal{H}_\eta}(\delta_T \mathcal{F} + \delta_X \sigma))$.

1.6.2 Code d'évaluation

C. Carvalho et V. Neumann [CN16] étudient un code de Goppa sur $\mathbb{P}^{\eta+3}$ avec $\mathcal{P} = \iota(\mathcal{H})(\mathbb{F}_q)$. Ils se fixent un degré δ et considèrent l'évaluation de polynômes homogènes de degré δ dans $\mathbb{P}^{\eta+3}$ en les points rationnels de $\iota(\mathcal{H}_\eta)$.

6. On définit un **bi**degré car le groupe Picard de $\mathcal{H}_\eta$ est de rang **2**.

Cela revient à raccourcir un code projectif de Reed-Muller sur $\mathbb{P}^{\eta+3}$ en le restreignant aux points de $\iota(\mathcal{H}_\eta)(\mathbb{F}_q)$.

Pour appréhender ces codes, ils tirent en arrière les polynômes via le plongement ι pour obtenir des polynômes de l'anneau de Cox de $\mathcal{H}_\eta$ et montrent qu'évaluer les polynômes de $\mathbb{P}^{\eta+3}$ sur les points rationnels de l'image de ι est équivalent à évaluer leurs tirés en arrière en les $(q+1)^2$ représentants choisis dans le cadre du quotient géométrique.

Cependant, étudier de tels codes revient à considérer des codes de Goppa sur $\mathcal{H}_\eta$ seulement pour une certaine famille *unidimensionnelle* de diviseurs, alors que le rang de Picard de cette surface vaut 2. Ils passent donc à côté de nombreuses classes de Picard à étudier. Cela est probablement dû au fait que les auteurs ne tirent pas assez profit des propriétés toriques de ces surfaces. Pour pouvoir étudier tous les codes de Goppa sur les surfaces de Hirzebruch, je propose d'évaluer directement, *à la Lachaud* [Lac90], les polynômes d'un espace vectoriel $R(\delta_T, \delta_X)$, vus comme polynômes de 4 variables, en les points $(1, a, 1, b)$, $(0, 1, 1, b)$, $(1, a, 0, 1)$ et $(0, 1, 0, 1)$ avec $(a, b) \in \mathbb{F}_q^2$. Ce point de vue permet de plus une implémentation facile de ces codes, sans connaissance particulière de la surface.

En m'inspirant des méthodes mises en place par C. Carvalho et V. Neumann mais en tirant parti à la fois des propriétés toriques mais surtout des outils puissants de la théorie des bases de Gröbner, je parviens à exprimer les paramètres en termes combinatoires (voir Théorèmes A et B [Nar18]). Des calculs rébarbatifs, avec de nombreuses disjonctions de cas, mènent aux formules exactes des paramètres d'un code de Goppa sur $\mathcal{H}_\eta$ associé à un diviseur de classe de Picard quelconque.

Theorem 1 ([Nar18])**.** *Sur $\mathcal{H}_0$, le code $C_0(\delta_T, \delta_X)$ a pour dimension*

$$\dim C_0(\delta_T, \delta_X) = (\min(\delta_T, q) + 1)\,(\min(\delta_X, q) + 1)$$

et distance minimale

$$d_\eta(\delta_T, \delta_X) = \max(q - \delta_X + 1, 1)\max(q - \delta_T + 1, 1).$$

Si $\eta \geq 2$, on pose

$$m = \min(\lfloor A \rfloor, q-1),\ h = \begin{cases} \min(\delta_T, q) + 1 & \text{si } \delta_T \geq 0 \text{ and } q \leq \delta_X, \\ 0 & \text{sinon,} \end{cases}$$

$$s = \frac{\delta - q}{\eta} \text{ and } \tilde{s} = \begin{cases} \lfloor s \rfloor & \text{si } s \in [0, m], \\ -1 & \text{si } s < 0, \\ m & \text{si } s > m. \end{cases}$$

Alors le code $C_\eta(\delta_T, \delta_X)$ sur $\mathcal{H}_\eta$ a pour dimension

$$\dim C_\eta(\delta_T, \delta_X) = (q+1)(\tilde{s}+1) + (m - \tilde{s})\left(\delta + 1 - \eta\left(\frac{m + \tilde{s} + 1}{2}\right)\right) + h.$$

Sa distance minimale vaut

- $d_\eta(\delta_T, \delta_X) = (q + \mathbb{1}_{\delta_X=0})(q - \delta + 1)$ *si* $q > \delta$,
- $d_\eta(\delta_T, \delta_X) = q - \left\lfloor \frac{\delta - q}{\eta} \right\rfloor$ *si* $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$,
- $d_\eta(\delta_T, \delta_X) = \begin{cases} \max(q - \delta_X + 1, 1) & \text{if } \delta_T \geq 0, \\ 1 & \text{if } \delta_T < 0, \end{cases}$ *si* $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$.

Comparaison avec les résultats existants

Les valeurs des paramètres établies sur $\mathcal{H}_0$ dans le cas injectif sont compatibles ceux qu'a montrés S. H. Hansen [Han01]. Sa preuve est la suivante : il utilise un système $\mathcal{P}$-couvrant pour calculer les paramètres d'un code sur $\mathcal{H}_0 = \mathbb{P}^1 \times \mathbb{P}^1$. Soient $G = \delta_T \mathcal{F} + \delta_X \sigma$, $\mathcal{P} = X(\mathbb{F}_q)$, $H = \sigma$ et on recouvre X par $q + 1$ lignes L_i de type $(1, 0)$. Alors

$$C_i.H = 1,\ G.C_i = \delta_X,\ l = \delta_T,$$

et on en déduit que

$$n = (q+1)^2,\ k = (\delta_T + 1)(\delta_X + 1) \text{ et } d \geq n - (\delta_T + \delta_X)(q+1) + \delta_T \delta_X.$$

Mon approche permet aussi de montrer que la minoration de la distance minimale est atteinte, ce qui avait déjà été prouvé par A. Couvreur et I. Duursma [CD13] dans le cas particulier $\eta = 0$.

Pour $\eta \geq 1$, on peut comparer mes résultats à ceux sur les codes toriques sur ces surfaces (voir [Han02] par exemple). Notons cependant que les codes toriques ne considèrent l'évaluation qu'en les points du tore alors que j'étudie le code des évaluées en tous les points rationnels de $\mathcal{H}_\eta$.

Un polygone possible pour définir un code torique sur la surface de Hirzebruch $\mathcal{H}_\eta$ ($\eta \neq 0$) associé à un diviseur $\delta_T \mathcal{F} + \delta_X \sigma$ avec $\delta_T, \delta_X > 0$ est donné en figure 1.4. Si q est assez grand et que l'application d'évaluation est injective, la dimension n'est rien d'autre que le nombre de points entiers à l'intérieur et sur les côtés du polygone, et ce dans le cas torique ou dans le mien.

En revanche, une différence notable apparaît entre les deux contextes quand l'application n'est plus injective.

On rappelle que $\delta = \delta_T + \eta \delta_X$. Prenons $q = 4$. Dans le cas torique, d'après D. Ruano [Rua07], il suffit de considérer les coordonnées du polygone modulo $q - 1$. Or on exhibe $(q-1)^2 = 9$ points (dessinés en Figure 1.5) tous distincts modulo $q - 1$, ce qui montre que le code est plein – ou que l'application est surjective. Dans le cas projectif que j'étudie, un point (i, j) du polygone correspond à un monôme $T_1^{\delta - \eta i - j} T_2^j X_1^{\delta_X - i} X_2^i$. Un point sur un côté du polygone correspond donc à un monôme où l'une des variables n'apparaît pas. Évaluer non seulement en les points du tore mais aussi en

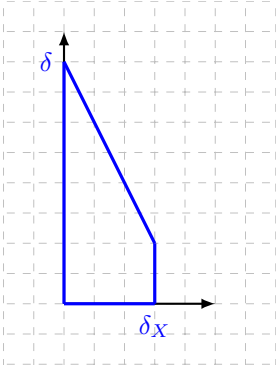


FIGURE 1.4 –

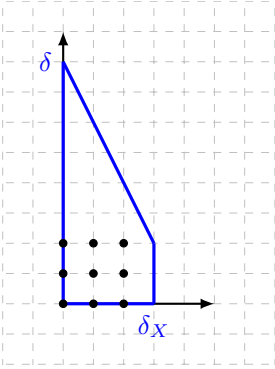


FIGURE 1.5 –

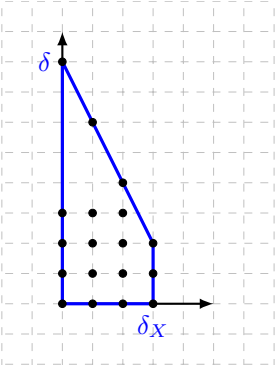


FIGURE 1.6 –

des points avec des coordonnées nulles impose qu'un monôme sur un côté du polygone ne peut avoir la même évaluation qu'un monôme hors de ce côté. Par conséquent, il ne suffit pas de regarder les coordonnées modulo $q-1$: il faut aussi traiter à part les points sur les côtés. Je montre que la dimension du code est égale au nombre de points dessinés en figure 1.6, c'est-à-dire 18. Puisque cette dimension est inférieure à $(q+1)^2 = 25$, ce code n'est pas plein.

Dans ce cas, je montre que le noyau de l'évaluation est formé de binômes, comme dans le cadre des codes toriques. En revanche, si δ_T est strictement négatif, le diviseur $\delta_T\mathcal{F} + \delta_X\sigma$ n'est plus ample je prouve qu'une base du noyau de l'évaluation est formée de différences de monômes et d'un polynôme à 4 termes. Cela prouve en particulier que l'idéal des points rationnels d'une surface de Hirzebruch n'est pas binomial.

1.7 Propriétés locales et applications

Pour améliorer les capacités de correction d'un code, on peut s'intéresser à ses propriétés de décodage local. Une propriété appréciée pour un code C est la suivante : l'ensemble des mots formés par restriction à un sous-ensemble donné de coordonnées des mots du code C forme un code connu. Par exemple, on vérifie aisément que tout mot d'un code de Reed-Muller restreint aux coordonnées correspondant aux points d'une même droite est un mot d'un code de Reed-Solomon de même degré. Puisqu'on sait décoder efficacement des codes de Reed-Solomon, un code de Reed-Muller est dit localement décodable [7]. Un code localement décodable donne naissance à un protocole de ***P**rivate **I**nformation **R**etrieval* (voir [KT00]), que l'on détaille ci-dessus dans le cadre des codes de Reed-Muller.

7. Définition précise par exemple dans [Lav17]

1.7.1 Applications au PIR

Les protocoles de PIR ont pour but d'assurer qu'un utilisateur puisse accéder à l'entrée D_i d'une base de données D sans révéler aucune information sur l'indice i au propriétaire de la base de données. Une solution simple mais brutale pour que le serveur n'ait aucune information sur i consiste pour l'utilisateur à télécharger la totalité de la base de données. Mais l'utilisateur se retrouve à télécharger beaucoup plus de données qu'il n'en veut véritablement. Pour proposer une solution efficace en termes de stockage, on peut supposer que la base de données est répartie entre plusieurs serveurs (voir [ALS14]) et utiliser des codes localement décodables.

Détaillons un protocole lié au code de Reed-Muller dans le plan affine. On suppose que la base de données est formée des mots de $\mathrm{RM}_q(d,2)$, qu'on dispose de q serveurs et on partitionne $\mathbb{A}^2(\mathbb{F}_q)$ en q droites parallèles $L_1, L_2, \ldots, L_q$. On attribue une droite à chaque serveur et on stocke sur ce serveur les coordonnées des mots du codes correspondant aux q points de la droite. En d'autres termes, chaque serveur contient les mots du code de Reed-Solomon, restriction du code $\mathrm{RM}_q(d,2)$ à une des L_i. La situation est illustrée en Figure 1.7.

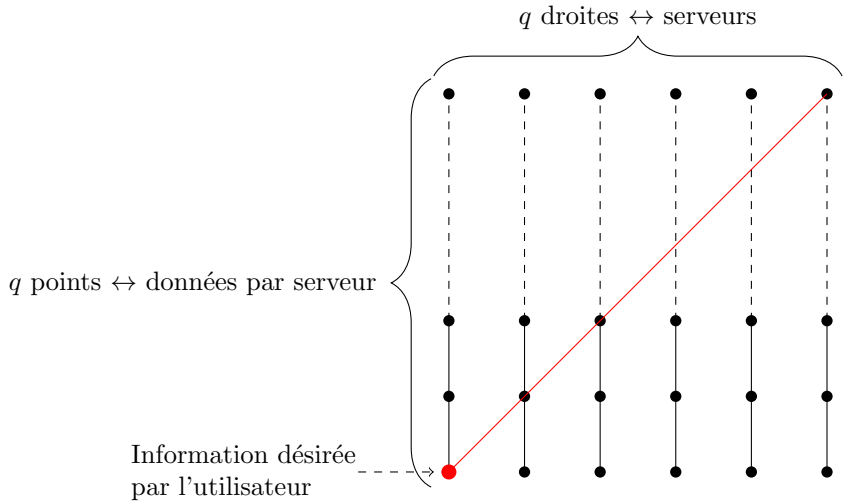


FIGURE 1.7 – Protocole de PIR lié à un Reed-Muller plan

Supposons maintenant que l'utilisateur désire accéder à la coordonnée associée à un point P_0 d'un mot de code $c \in \mathrm{RM}_q(d,2)$. L'utilisateur tire alors aléatoirement une droite rationnelle L (représentée en rouge sur la Figure 1.7) qui contient P_0 mais qui n'est pas l'une des L_i. Cette droite intersecte donc les droites L_i en un unique point. À chaque serveur associé à une droite

L_i telle que $P_0 \notin L_i$, l'utilisateur va demander $c_{L_i \cap L}$. Au serveur associé à la droite L_{i_0} qui contient P_0, l'utilisateur va demander une coordonnée c_P pour un point P tiré aléatoirement [8] sur la droite L_{i_0}. Si aucun serveur n'est défaillant ou malveillant, l'utilisateur récupère donc un mot de Reed-Solomon de degré d avec au plus une erreur qu'il est en mesure de corriger pour récupérer l'information voulue.

En fait, selon le degré d du code de Reed-Muller, et donc du code de Reed-Solomon, l'utilisateur peut quand même récupérer ce qu'il souhaite même s'il y a un certain nombre de serveurs défaillants ou malveillants. En revanche, si deux serveurs communiquent et comprennent le protocole, ils savent que l'information voulue par l'utilisateur est associée à un point de la droite reliant les deux points qu'on leur a demandés. Ce protocole n'est pas résistant aux collusions entre 2 serveurs.

Propriétés locales des codes sur les surfaces de Hirzebruch - L'étude des codes de Goppa sur les surfaces de Hirzebruch m'a permis de me familiariser avec la géométrie de ces surfaces. J. Lavauzelle, familier avec le protocole de PIR décrit au-dessus, m'a suggéré d'explorer les propriétés de décodage local de mon code.

Pour espérer des propriétés similaires pour les codes sur les surfaces de Hirzebruch, il nous faut d'abord définir des substituts potentiels aux droites du plan.

Naturellement, une surface de Hirzebruch étant une surface réglée, notre premier réflexe serait d'utiliser les droites du réglage. Néanmoins, par un point donné passe une et une seule droite du réglage. Les droites du réglage seront donc l'analogue des droites parallèles grâce auxquelles on répartit l'information sur les serveurs.

Qu'est-ce qui va jouer le rôle des autres droites ? Les droites du réglage sont les diviseurs d'équation $aT_1 + bT_2 = 0$, linéairement équivalents aux "axes de coordonnées" $T_i = 0$. La droite $X_1 = 0$ est d'auto-intersection $-\eta < 0$: elle donc seule dans sa classe d'équivalence. En revanche, la droite $X_2 = 0$ est linéairement équivalente à toute courbe définie par $X_2 = F(T_1, T_2)X_1$ où $F \in \mathbb{F}_q[X_0, X_1]$ est un polynôme homogène de degré η. On appelle ces courbes des *η-droites*. L'intersection d'une des ces η-droites avec l'une des droites du réglage consiste en un unique point. En dehors de la *directrice* $X_1 = 0$, tout point appartient à q^η η-droites. On a donc trouvé d'excellentes candidates pour remplacer les droites du protocole sur le Reed-Muller.

Reste à voir que la restriction d'un mot du code à l'une des ces η-droites se trouve dans un code connu.

8. Notons que ce point peut être P_0. Si on tire au hasard sur l'ensemble $L_{i_0} \setminus \{P_0\}$ et que la requête est fréquente, le serveur concerné pourrait remarquer que le point P_0 n'est jamais demandé et donc déterminer l'information souhaitée par l'utilisateur.

Prenons un monôme $T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \in R(\delta_T, \delta_X)$, c'est-à-dire tel que

$$\begin{cases} \delta_T &= c_1 + c_2 - \eta d_1, \\ \delta_X &= d_1 + d_2. \end{cases}$$

En remplaçant X_2 par $F(T_1, T_2)X_1$, on a $T_1^{c_1}T_2^{c_2}X_1^{d_1+d_2}F(T_1, T_2)^{d_2}$, ce qui est un polynôme homogène de degré $c_1+c_2+\eta d_2 = \delta$ en T_1 et T_2. Puisque que le choix des points d'évaluation force $x_1 \in \{0, 1\}$, le mot associé appartient au code de Reed-Muller projectif $\mathrm{PRM}_q(\delta)$.

Un protocole de PIR grâce aux codes sur $\mathcal{H}_\eta$. J. Lavauzelle et moi-même proposons un protocole résistant aux collusions, qui n'est pas publié [9].

On suppose que la base de données est formée des mots de $C_\eta(\delta_T, \delta_X)$ avec $\delta < q-2$ et qu'on dispose de $q+1$ serveurs. On partitionne $\mathcal{H}_\eta(\mathbb{F}_q)$ en les $q+1$ droites du réglage $L_1, L_2, \ldots, L_{q+1}$. Comme précédemment, on associe une droite à chaque serveur et on stocke sur ce serveur les coordonnées correspondant aux q points de la droite hors de la directrice. La situation est illustrée en Figure 1.8.

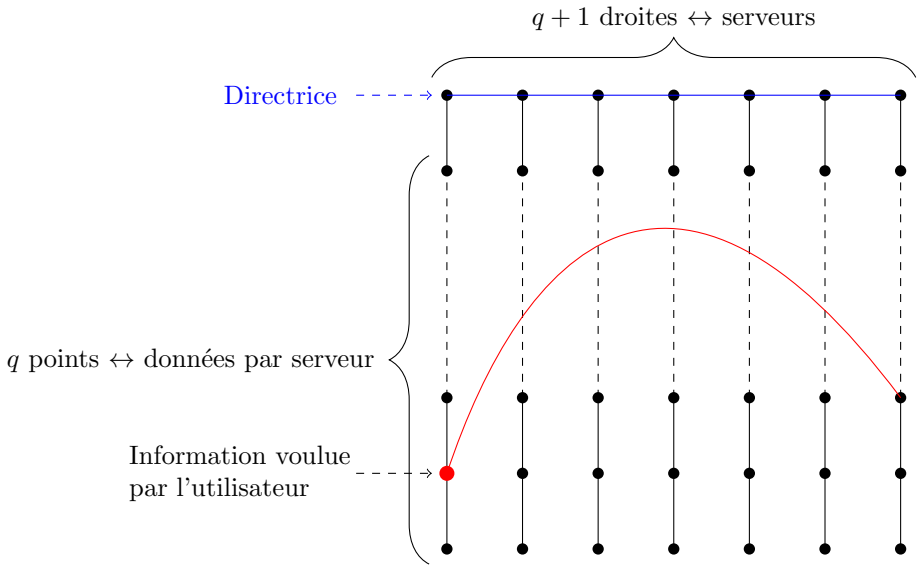


FIGURE 1.8 – Protocole de PIR lié à un code sur la surface de Hirzbruch $\mathcal{H}_\eta$

Comme précédemment, on suppose maintenant que l'utilisateur veut la coordonnée associée à un point P_0 d'un mot du code $C_\eta(\delta_T, \delta_X)$. L'utilisateur choisit aléatoirement une η-droite rationnelle L (représentée en rouge sur la Figure 1.8) qui passe par P_0. L'utilisateur récupère un mot erroné de $\mathrm{PRS}_q(\delta)$ en demandant à chaque serveur associé à une droite L_i telle que $P_0 \notin L_i$

9. Néanmoins, c'est ce qui a initié le travail sur les Reed-Muller pondérés [LN19].

la coordonnée $c_{L_i \cap L}$ et au serveur associé à la droite L_{i_0} une coordonnée quelconque.

On a un protocole très similaire à celui du Reed-Muller si $\eta = 1$. Néanmoins, si $\eta > 1$, on a un système résistant aux collusions. En effet, admettons que s serveurs qui ne correspondent pas à la droite contenant P_0 mettent en commun les s points que l'utilisateur a demandés. Alors ils peuvent chercher une η-droite qui contient ces s points par interpolation. Or, une telle η-droite est unique si et seulement si $\eta > s$. Par conséquent, si au plus η serveurs communiquent, ils ne sont pas en mesure de déterminer la vraie requête de l'utilisateur. On a donc construit un système qui résiste à η collusions. Malheureusement, cette amélioration vis-à-vis des collusions a un prix : la dimension d'un code $C_\eta(\delta_T, \delta_X)$ avec $\delta < q - 2$ est de l'ordre $\frac{\delta^2}{2\eta}$ alors qu'un code $\mathrm{RM}_q(2, d)$ est de dimension $\simeq \frac{d^2}{2}$.

1.8 Améliorer le taux de transmission grâce au *lift.*

1.8.1 Lifter par rapport aux droites

Revenons un instant sur les codes $\mathrm{RM}_q(2, d)$. La seule propriété dont on a besoin pour utiliser ces codes dans le protocole du PIR est le fait que les mots de ce code restreints aux points d'une même droite sont des mots d'un $\mathrm{RS}_q(d)$. Il est alors assez naturel de se demander s'il existe un code plus gros qui vérifie cette même propriété. Concrètement, on considère l'ensemble

$$\Phi = \{t \mapsto (at + b, ct + d) \mid (a, b, c, d) \in \mathbb{F}_q^4,\ ac \neq 0\}, \tag{1.6}$$

qui paramétrise les droites rationnelles de $\mathbb{A}^2$, et on cherche l'ensemble $\mathcal{F}$ défini par

$$\mathcal{F} = \{f \in \mathbb{F}_q[x, y] \mid \forall \phi \in \Phi,\ \mathrm{ev}(f \circ \phi) \in \mathrm{RS}_q(d)\}$$

pour définir un code d'évaluation qui aurait les propriétés voulues, noté $\mathrm{Lift}\,\mathrm{RS}_q(d)$.

On sait déjà que $\mathcal{F}$ contient les polynômes de degré d mais contient-il plus de polynômes ?

Par exemple, sur $\mathbb{F}_4$, prenons $f = x^2y^2$. Alors

$$\begin{aligned} f(at + b, ct + d) =& (a^2t^2 + 2abt + b^2)(c^2t^2 + 2cdt + d^2) \\ =& a^2c^2t^4 + (a^2cd + abc^2)t^3 + (a^2d^2 + b^2c^2)t^2 \\ &+ 2(abd^2 + b^2cd)t + b^2d^2 \end{aligned}$$

Or, modulo $t^4 - t$, ce polynôme est équivalent à un polynôme de degré 3. Par conséquent, $\mathrm{ev}(f) \in \mathrm{Lift}_\phi\,\mathrm{RS}_4(3) \setminus \mathrm{RM}_4(2, 3)$.

A. Guo, S. Kopparty, et M. Sudan [GKS13] ont montré que tout monôme apparaissant dans l'écriture d'un polynôme de $\mathcal{F}$ appartient lui-même à $\mathcal{F}$. Par conséquent, le code d'évaluation des polynômes de $\mathcal{F}$ est monomial : il est engendré par les évaluations de monômes. Il n'est pas très difficile de déterminer les monômes de $\mathcal{F}$.

J. Lavauzelle [Lav18] a adapté leur idée pour définir le *lift* du code de Reed-Solomon projectif. Le passage de l'affine au projectif permet un nouveau gain en dimension. Par exemple, J. Lavauzelle montre que $\dim \operatorname{Lift} \mathrm{RS}_4(3) = 7$ alors que $\dim \operatorname{Lift} \mathrm{PRS}_4(3) = 11$. Cependant, même si le code reste monomial dans le cas projectif, la caractérisation des monômes qui engendrent le code est légèrement plus complexe. Cela est essentiellement dû au noyau de l'évaluation. Dans le cas affine, le noyau est engendré par $x^q - x$ et $y^q - y$ alors que dans le cas projectif, il est engendré par les $X_i X_j^q - X_i^q X_j$ pour $(i, j) \in \{0, 1, 2\}^2$. Dans le premier cas, les générateurs ne dépendent que d'une variable, ce qui n'est pas le cas dans le second. Les calculs modulo le noyau en sont plus subtils. C'est le même phénomène qui explique le saut de dimension entre les codes toriques et les codes projectifs que j'ai considérés sur les surfaces de Hirzebruch (voir Figures 1.5 et 1.6).

1.8.2 Lifter par rapport aux η-droites

La propriété locale des codes sur la surface de Hirzebruch $\mathcal{H}_\eta$ nous indique qu'il peut être intéressant d'étudier une nouvelle façon de lifter les codes de Reed-Solomon, projectifs ou non. On s'intéresse ici seulement au cas affine.

Avec J. Lavauzelle [LN19], on propose, plutôt que de lifter par rapport à l'ensemble Φ (voir (1.6)), de le faire par rapport à

$$\Phi_\eta = \{t \mapsto (t, F(t)) \mid F \in \mathbb{F}_q[t],\ \deg F \leq \eta\}, \tag{1.7}$$

ce qui correspond à l'analogue affine des η-droites, et donc considérer le code d'évaluation $\operatorname{Lift}^\eta \mathrm{RS}_q(d)$ des polynômes de

$$\mathcal{F}_\eta = \{f \in \mathbb{F}_q[x, y] \mid \forall \phi \in \Phi_\eta,\ \mathrm{ev}(f \circ \phi) \in \mathrm{RS}_q(d)\}.$$

Il est clair que cet ensemble contient les polynômes de $\mathbb{F}_q[x, y]$ de degré pondéré d, où x est de poids 1 et y de poids η. On montre, avec J. Lavauzelle, que le code $\operatorname{Lift}^\eta \mathrm{RS}_q(d)$ est monomial et on caractérise les monômes qu'il contient. Bien qu'on ne fournisse pas de formule explicite pour la dimension, on a implémenté un programme Python qui calcule les monômes dans le lift et fournit une représentation graphique de ceux-ci, utilisée de nombreuses fois dans l'article. De plus, on exhibe deux familles de codes, dont la taille de l'alphabet tend vers l'infini et telles que le taux de transmission tend vers 1 dans un cas et vers une constante strictement positive dans l'autre. Plus précisément, on montre :

Theorem 2 ([LN19]). *Soit $\alpha \geq 2$, $\eta \geq 1$ et p un nombre premier. On pose $e_\alpha = \lfloor \log_p \alpha \rfloor$. Pour tout $e \geq e_\alpha$, on considère le code $\mathrm{Lift}^\eta \mathrm{RS}_{p^e}(p^e - \alpha)$ de taux de transmission R_e. Alors $\lim_{e\to+\infty} R_e = 1$.*

Theorem 3 ([LN19]). *Soit $c \geq 1$, $\eta \geq 1$ et p un nombre premier. On pose $\gamma = 1 - p^{-c}$. Pour tout $e \geq c+1$, on considère le code $\mathrm{Lift}^\eta \mathrm{RS}_{p^e}(\gamma p^e)$ de taux de transmission R_e. Alors il existe une constante $L = L(c, \eta, p)$ strictement positive qui ne dépend pas de e telle que $\lim_{e\to+\infty} R_e \geq L$.*

Dans le premier cas, cela nous permet de proposer des protocoles de PIR qui résistent à la collusions de η serveurs avec des bases de données aussi grandes que l'on le souhaite et dont le taux de transmission est d'autant meilleur que la base de données est grande. Dans le second, on construit une suite de codes asymptotiquement bonne qui corrigent une fraction constante d'erreurs.

Chapitre 2

Une stratégie globale pour majorer le nombre de points rationnels

2.1 Motivation

Soit X une surface projective, lisse et connexe sur le corps fini $\mathbb{F}_q$. La formule de Lefschetz exprime le cardinal de $X(\mathbb{F}_q^n)$ en fonction des nombres de Betti de X, invariants topologiques, et des valeurs propres des morphismes du Frobenius sur les groupes de cohomologie étale de la variété. En majorant le module des valeurs propres des morphismes du Frobenius, Deligne a montré :

$$X(\mathbb{F}_q) \leq 1 + q^2 + b_1(q^{1/2} + q^{3/2}) + b_2 q.$$

On connaît des surfaces qui atteignent la borne de Weil-Deligne, comme les surfaces hermitiennes. Ce résultat apparaît donc comme une solution définitive au problème du nombre de points $\mathbb{F}_q$-rationnels d'une variété.

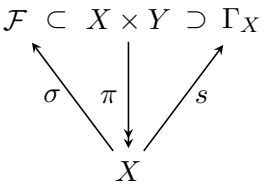
Mais qu'en est-il si l'on impose des contraintes à la variété X que l'on considère ? Par exemple, si l'on suppose qu'elle est plongée dans une autre variété Y ? Si cette question paraît anecdotique, elle prend tout son sens dans le cadre de la théorie des codes correcteurs (voir paragraphe 1.4.2).

2.2 Stratégie

Avant de s'attaquer au problème du dénombrement des points rationnels d'une variété, on étudie d'abord les résultats qui existent déjà à ce sujet et on essaie d'en retirer un principe commun.

Voici celui retenu. Admettons que l'on veuille étudier le nombre de points $\mathbb{F}_q$-rationnels d'une variété X. On suppose qu'elle est contenue dans une

autre variété Y, que l'on appellera l'*espace ambiant de* X. Pour la suite, on va considérer le fibré trivial $\pi : X \times Y \to X$, qui n'est rien d'autre que la projection sur la première coordonnée.

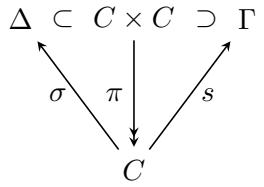


Pour tenir compte de la rationalité, il est raisonnable de faire intervenir le morphisme du Frobenius Φ. Pour ce faire, on pose la section $s : X \to X \times Y$ de π définie par $s(P) = (P, \Phi(P))$ et Γ_X son image dans $X \times Y$.

Trouver un majorant de $\#X(\mathbb{F}_q)$ dans ce cadre revient à déterminer une autre section, notée $\sigma : X \to X \times Y$, dont l'image $\mathcal{F} \subset X \times Y$ a l'agréable propriété d'intersecter Γ_X en un ensemble dans lequel s'injecte l'ensemble $X(\mathbb{F}_q)$.

Si Γ_X et $\mathcal{F}$ ont des dimensions complémentaires dans $X \times Y$, alors le cardinal de $X(\mathbb{F}_q)$ est majoré [1] par le nombre d'intersection $\mathcal{F} \cdot \Gamma_X$. Si l'on est en mesure de mener les calculs dans l'anneau de Chow de $X \times Y$ et que l'on est capable d'exprimer ce nombre d'intersection en fonction d'invariants des variétés X et Y, on peut obtenir une borne explicite.

2.2.1 Borne de Hasse-Weil



À titre de premier exemple, commençons par considérer la preuve de Weil sur le nombre de points d'une courbe. Prenons C une courbe projective lisse et considérons la surface $C \times C$.

Sur cette surface, les points (P, P) où $P \in C(\mathbb{F}_q)$ sont exactement les points d'intersection entre le graphe du Frobenius $\Gamma = \{(P, \Phi(P)) \mid P \in C\}$ et la diagonale $\Delta = \{(P, P) \mid P \in C\}$.

La théorie de l'intersection sur les surfaces nous permet de calculer le nombre exact de points, puisque cette intersection est transverse, comme le nombre d'intersection $\Gamma \cdot \Delta$. La borne de Hasse-Weil repose alors sur l'encadrement avec des arguments euclidiens de cette quantité en fonction de q et du genre de la courbe :

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}.$$

Cette situation rentre tout à fait dans le cadre décrit précédemment, en posant $X = Y = C$, $s = \mathrm{Id} \times \mathrm{Id}$ et donc $\mathcal{F} = \Delta$.

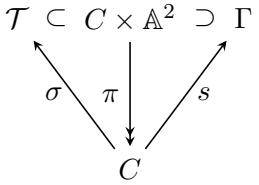
2.2.2 Majorer le nombre de points rationnels

On sait qu'il peut être intéressant d'avoir seulement un majorant du nombre de points rationnels, notamment pour la minoration de la distance

1. Cette majoration n'a de sens que si les points rationnels de X ne sont pas tous inclus dans une composante commune de Γ_X et $\mathcal{F}$.

minimale d'un code correcteur, comme expliqué au paragraphe 1.4.2. Contrairement à l'idée de la preuve de la borne de Hasse-Weil qui repose sur l'estimation du nombre exact de points rationnels, on peut déterminer une section s telle que son image $\mathcal{F}$ intersecte Γ_X en d'autres points que ceux de $X(\mathbb{F}_q)$, et ce de façon éventuellement non transverse. Pour éviter une majoration trop abrupte, on peut d'ailleurs demander en contrepartie une forte multiplicité d'intersection de $\mathcal{F}$ et Γ_X en les points rationnels de X.

Borne de Stöhr-Voloch sur les courbes planes



Un bon exemple illustrant ce principe est la borne sur les courbes planes de K. O. Sthör et F. J. Voloch [SV86].

Soit C une courbe plane définie par un polynôme f. K. O. Stöhr et F. J. Voloch ont compté les points dont l'image sous le morphisme du Frobebius est sur leur propre tangente, condition évidemment remplie par les points rationnels. Pour cela, ils comptent le nombre d'intersection entre C et la courbe définie par

$$(x^q - x)f_x + (y^q - y)f_y = 0.$$

Cela revient à poser $(X, Y) = (C, \mathbb{A}^2)$ et à considérer le fibré vectoriel $\mathcal{F} = \mathcal{T}$ défini par

$$\mathcal{T} = \{(P, Q) \in C \times \mathbb{A}^2 \mid Q \in T_P\, C\} = \mathcal{Z}\left((u - x)f_x(x, y) + (v - y)f_y(x, y)\right),$$

dont la fibre au-dessus d'un point P est l'espace tangent $T_P C$. Ce fibré est donc de codimension 1 dans $C \times \mathbb{A}^2$ et l'ensemble $\mathcal{T} \cap \Gamma$ est en bijection avec $\{P \in C \mid \Phi(P) \in T_P\, C\}$. Il est évident qu'un point dont le Frobenius est sur sa propre tangente n'est pas nécessairement rationnel. Mais, comme énoncé précédemment, les points rationnels se distinguent au sein de $\mathcal{T} \cap \Gamma$. Un calcul des espaces tangents de $\mathcal{T}$ et Γ prouve que ces deux variétés s'intersectent avec multiplicité au moins 2 en (P, P) si $P \in C(\mathbb{F}_q)$.

Par conséquent, si $\mathcal{T}$ and Γ n'ont pas de composante commune, ce qui est vrai si chaque composante irréductible de C contient au moins un point (sur la clôture algébrique) qui n'est pas d'inflexion, alors $2\#C(\mathbb{F}_q) \leq \mathcal{T} \cdot \Gamma$. Le calcul du produit d'intersection $\mathcal{T} \cdot \Gamma$ donne une borne qui dépend de q et du degré d de la courbe :

$$\#C(\mathbb{F}_q) \leq \frac{d}{2}(d + q - 1).$$

Bornes de Voloch pour les surfaces de $\mathbb{P}^3$

F. J. Voloch [Vol03] a étendu cette idée à une surface X incluse dans $Y = \mathbb{P}^3$, définie par $f = 0$ de degré d. Compter le nombre de points dont le Frobenius serait sur leur propre plan tangent mènerait à calculer l'intersection entre Γ_X et

$$\begin{aligned}\mathcal{T}_X &= \{(P,Q) \in X \times \mathbb{P}^3 \mid Q \in T_P X\} \\ &= \mathcal{Z}\left(\sum_{0\le i\le 3} u_i f_{x_i}(x_0,x_1,x_2,x_3), \sum_{0\le i,j\le 3} u_i u_j f_{x_i x_j}(x_0,x_1,x_2,x_3)\right).\end{aligned}$$

Dans ce cas, $\dim \Gamma_X + \dim \mathcal{T}_X = 2 + 4 \neq \dim S \times \mathbb{P}^3$. F. J. Voloch propose un fibré de dimension 3. Pour majorer le nombre de points $\mathbb{F}_q$-rationnels de X, il compte le nombre de points P de X dont l'image par le Frobenius est sur l'une de ses droites asymptotiques [2]. Cela revient à dénombrer les points de $X \times \mathbb{P}^3$ qui appartiennent à la fois à Γ_X et à

$$\begin{aligned}\mathcal{S} &= \{(P,Q) \in X \times \mathbb{P}^3 \mid \exists\, L \text{ droite de } \mathbb{P}^3 \text{ telle que } i(X,L;P) \ge 3 \text{ et } Q \in L\} \\ &= \mathcal{Z}\left(\sum_{0\le i\le 3} u_i f_{x_i}(x_0,x_1,x_2,x_3), \sum_{0\le i,j\le 3} u_i u_j f_{x_i x_j}(x_0,x_1,x_2,x_3)\right).\end{aligned}$$

Même si les dimensions de $\mathcal{S}$ et Γ_X sont complémentaires, ils ont une composante commune, qui est une courbe composée des points flecnodaux [3] de X. Cependant, une ancien résultat de G. Salmon [Sal65] donne le degré de cette courbe en fonction du degré de la surface, à savoir $d(11d-24)$. Hors de cette courbe, un $\mathbb{F}_q$-point de X a multiplicité 6 dans cette intersection. Si q est premier et $2 < d < q$, F. J. Voloch établit que

$$\#X(\mathbb{F}_q) \le \frac{1}{6}\mathcal{Z} \cdot \Gamma_X + (q+1)d(11d-24).$$

2.2.3 Choisir d'autres fibrés

Les bornes citées jusqu'à présent tiennent compte de l'inclusion de X dans un ambient Y *sympathique* et le choix du fibré $\mathcal{F}$ repose sur de plaisantes propriétés de Y, telles que la possibilité de voir l'espace tangent à X en un point comme une sous-variété de Y ou encore l'existence de droites asymptotiques dans un plan tangent à une surface de $\mathbb{P}^3$.

Il est naturel de penser qu'ajouter des contraintes de plongement à une variété va influer sur sa géométrie et donc sur son nombre de points rationnels. Ceci est bien illustré par la borne de K. O. Sthör et F. J. Voloch par rapport à celle de Hasse-Weil.

2. Une droite L est dite asymptotique en P sur X si la multiplicité d'intersection de L et X en P vaut au moins 3. Il est facile de montrer qu'en un point régulier, il y a au moins de deux droites asymptotiques, éventuellement confondues.

3. Un point P est dit flecnodal s'il existe une droite L telle que $m_p(L,X) \ge 4$.

Sur les surfaces toriques - L'étude des codes sur les surfaces de Hirzebruch m'a permis de me familiariser avec les surfaces toriques. Les variétés toriques présentent deux propriétés qui encouragent à y étendre le résultat de K. O. Sthör et F. J. Voloch. Primo, une variété torique de dimension n est un recollement d'espaces affines $\mathbb{A}^n$ dont les applications de transition entre cartes sont parfaitement connues. Ainsi, on donne aisément un sens local à la tangente et on est en mesure de lui donner un sens global via recollement. Secundo, les variétés toriques, tout comme les espaces projectifs, eux-mêmes variétés toriques, sont munies d'un anneau de coordonnés polynomial, appelé *Anneau de Cox* avec un processus d'homogénéisation. L'équation d'une sous-variété dans une carte affine peut-être homogénéisée pour obtenir une équation sur la variété torique tout entière.

Motivée par ces deux propriétés des surfaces toriques, j'ai généralisé l'idée de K. O. Sthör et F. J. Voloch à celles-ci. En pratique, on se donne une courbe absolument irréductible $X = C$ sur une surface torique $Y = S$. On peut alors définir autant de fibrés vectoriels "tangents" $\mathcal{T}_i$ qu'il y a de cartes affines sur S. L'intersection d'un fibré $\mathcal{T}_i$ avec Γ_C correspond exactement aux points de la carte affine considérée dont l'image par le Frobenius appartient à leur tangente. Sur une surface de Hirzeruch $Y = \mathcal{H}_\eta$, on montre qu'au moins un de ces fibrés n'a pas de composante commune avec Γ_C, et ce sans hypothèse de type inflexion comme dans le cas de K. O. Sthör et F. J. Voloch.

Theorem 4 ([Nar19])**.** *Soit $\mathcal{C}$ une courbe absolument irréductible sur $\mathcal{H}_\eta$ définie sur $\mathbb{F}_q$.*

— *Si $\eta = 0$ et $\mathcal{C}$ a bidegré $(\alpha, \beta) \in (\mathbb{N}^*)^2$, alors*

$$\#C(\mathbb{F}_q) \leq \alpha\beta + \frac{q}{2}(\alpha + \beta).$$

— *Si $\eta \neq 0$ et $\mathcal{C}$ a bidegré $(\alpha, \beta) \in (\mathbb{N}^*)^2$, alors*

$$\#\mathcal{C}(\mathbb{F}_q) \leq \frac{\beta}{2}(2\alpha - \eta\beta - \eta + 1) + \frac{q}{2}(\alpha + \beta).$$

Le théorème de K. O. Sthör et F. J. Voloch [SV86] peut dont être appliqué à une courbe sur une telle surface en considérant la courbe plongée dans $\mathbb{P}^{\eta+3}$. Néanmoins, le majorant obtenu via ma méthode est meilleur que celui de K. O. Sthör et F. J. Voloch si le degré de C est grand. Ceci n'est guère étonnant : contraindre une courbe de grand degré d'être sur une surface donnée impose des restrictions sur sa géométrie par rapport à une courbe quelconque et donc peut réduire le nombre maximal de points $\mathbb{F}_q$-rationnels qu'elle contient.

Perspective sur une surface de type général - Les surfaces de Hizebruch représentent une classe très réduite des surfaces et l'un des

objectifs en fin de thèse, qui n'est pas encore atteint, fut de dépasser ce type de contrainte.

Pour déterminer un fibré $\mathcal{F}$ qui mènerait à une borne intéressante sur $\#X(\mathbb{F}_q)$, pourquoi ne pas être plus spécifique sur l'ambiant Y ? Par exemple, si l'on considère une courbe, incluse dans une surface de $\mathbb{P}^n$, il est à nouveau possible de considérer une sorte de fibré tangent, à S ou à C (voir Figure 2.1).

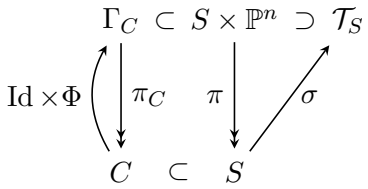


FIGURE 2.1 –

Concentrons-nous d'abord sur le cas $n = 3$. Soit Γ_C le graphe du Frobenius de $\mathbb{P}^3$ restreint à la courbe C et $\mathcal{T}_S$ le fibré tangent à S. Alors Γ_C est une courbe de $S \times \mathbb{P}^3$ et $\mathcal{T}_S$ est une hypersurface. Si leur intersection est de dimension 0, alors on sait que

$$2\#C(\mathbb{F}_q) \leq \Gamma_C \cdot \mathcal{T}_S = (\deg S + q - 1)\, C \cdot c_1(\mathcal{O}_S(1)),$$

puisqu'un point de type (P, P) avec $P \in C(\mathbb{F}_q)$ a multiplicité 2 dans $\Gamma_C \cap \mathcal{T}_S$. On a donc un majorant qui dépend du plongement de S dans $\mathbb{P}^3$, à travers son degré et sa section hyperplane, et de la classe de Picard de C.

L'un des points à préciser pour appliquer cette idée est la détermination d'une condition qui garantirait que Γ_C et $\mathcal{T}_S$ ne s'intersectent qu'en des points. Ce n'est évident pas toujours vrai : si S contient des droites et que l'une de ces droites figure parmi les composantes de C, cette droite est contenue dans l'intersection $\Gamma_C \cap \mathcal{T}_S$.

Bibliographie

[AB90] M. Andreatta and E. Ballico. Classification of projective surfaces with small sectional genus : char $p \geq 0$. *Rend. Sem. Mat. Univ. Padova*, 84 :175–193 (1991), 1990.

[ALS14] Daniel Augot, Françoise Levy-dit-Vehel, and Abdullatif Shikfa. A storage-efficient and robust private information retrieval scheme allowing few servers. In Dimitris Gritzalis, Aggelos Kiayias, and Ioannis G. Askoxylakis, editors, *Cryptology and Network Security - 13th International Conference, CANS 2014, Heraklion, Crete, Greece, October 22-24, 2014. Proceedings*, volume 8813 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2014.

[Aug10] Daniel Augot. Les codes algébriques principaux et leur décodage. In Jean-Guillaume Dumas, Grégoire Lecerf, Delphine Boucher ;, and Thomas Cluzeau, editors, *Journées Nationales de Calcul Formel*, volume 1 of *Les cours du CIRM*, pages 31–74, Luminy, France, May 2010. Jean-Guillaume Dumas, Grégoire Lecerf, Delphine Boucher et Thomas Cluzeau, CIRM.

[BCH+19] Régis Blache, Alain Couvreur, Emmanuel Hallouin, David Madore, Jade Nardi, Matthieu Rambaud, and Hugues Randriam. Anticanonical codes from del Pezzo surfaces with Picard rank one. working paper or preprint, March 2019.

[CD13] Alain Couvreur and Iwan Duursma. Evaluation codes from smooth quadric surfaces and twisted Segre varieties. *Des. Codes Cryptogr.*, 66(1-3) :291–303, 2013.

[CLS11] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.

[CN16] Cicero Carvalho and Victor G. L. Neumann. Projective Reed-Muller type codes on rational normal scrolls. *Finite Fields Appl.*, 37 :85–107, 2016.

[Cou11] Alain Couvreur. Construction of rational surfaces yielding good codes. *Finite Fields and Their Applications*, 17(5) :424–441, September 2011.

[GKS13] Alan Guo, Swastik Kopparty, and Madhu Sudan. New affine-invariant codes from lifting. In *ITCS'13—Proceedings of the 2013 ACM Conference on Innovations in Theoretical Computer Science*, pages 529–539. ACM, New York, 2013.

[Gop77] V. D. Goppa. Codes that are associated with divisors. *Problemy Peredači Informacii*, 13(1) :33–39, 1977.

[Gur05] Venkatesan Guruswami. List decoding of error-correcting codes. *Lecture Notes in Computer Science*, 3282, 08 2005.

[Han01] Søren Have Hansen. Error-correcting codes from higher-dimensional varieties. *Finite Fields Appl.*, 7(4) :531–552, 2001.

[Han02] Johan P. Hansen. Toric varieties Hirzebruch surfaces and error-correcting codes. *Appl. Algebra Engrg. Comm. Comput.*, 13(4) :289–300, 2002.

[Har95] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[Joy04] David Joyner. Toric codes over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 15(1) :63–79, 2004.

[KT00] Jonathan Katz and Luca Trevisan. On the Efficiency of Local Decoding Procedures for Error-Correcting Codes. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 80–86. ACM, 2000.

[Lac90] Gilles Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2) :217–221, 1990.

[Lav17] Julien Lavauzelle. Constructions for efficient Private Information Retrieval protocols. In *WCC 2017 - The Tenth International Workshop on Coding and Cryptography*, pages 1–12, Saint-Petersbourg, Russia, September 2017. INRIA and SUAI and Skoltech.

[Lav18] Julien Lavauzelle. Lifted projective Reed–Solomon codes. *Designs, Codes and Cryptography*, 2018.

[LN19] Julien Lavauzelle and Jade Nardi. Weighted lifted codes : Local correctabilities and application to robust private information retrieval. preprint, March 2019.

[LS06] John Little and Hal Schenck. Toric surface codes and Minkowski sums. *SIAM J. Discrete Math.*, 20(4) :999–1014, 2006.

[LS18] John Little and Hal Schenck. Codes from surfaces with small picard number. *CoRR*, abs/1803.00486, 2018.

[Nar18] Jade Nardi. Algebraic Geometric codes on minimal Hirzebruch surfaces. working paper or preprint, July 2018.

[Nar19] Jade Nardi. Bound on the number of rational points on curves on Hirzebruch surfaces over finite field. working paper or preprint, March 2019.

[Rei97] Miles Reid. Chapters on algebraic surfaces. In *Complex algebraic geometry (Park City, UT, 1993)*, volume 3 of *IAS/Park City Math. Ser.*, pages 3–159. Amer. Math. Soc., Providence, RI, 1997.

[Rua07] Diego Ruano. On the parameters of r-dimensional toric codes. *Finite Fields Appl.*, 13(4) :962–976, 2007.

[Sal65] George Salmon. *A treatise on the analytic geometry of three dimensions. Vol. II.* Fifth edition. Edited by Reginald A. P. Rogers. Chelsea Publishing Co., New York, 1965.

[Ser00] J.-P Serre. Lettre à m. tsfasman. *Astérisque*, 198 :351–353, 01 2000.

[Sør92] Anders Bjært Sørensen. Weighted Reed-Muller codes and algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 38(6) :1821–1826, 1992.

[SS09] Ivan Soprunov and Jenya Soprunova. Toric surface codes and Minkowski length of polygons. *SIAM J. Discrete Math.*, 23(1) :384–400, 2008/09.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[SV86] Karl-Otto Stöhr and José Felipe Voloch. Weierstrass points and curves over finite fields. *Proc. London Math. Soc. (3)*, 52(1) :1–19, 1986.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109 :21–28, 1982.

[Vol03] José Felipe Voloch. Surfaces in $\mathbf{P}^3$ over finite fields. In *Topics in algebraic and noncommutative geometry (Luminy/Annapolis, MD, 2001)*, volume 324 of *Contemp. Math.*, pages 219–226. Amer. Math. Soc., Providence, RI, 2003.

[Zar07] Marcos Zarzar. Error-correcting codes on low rank surfaces. *Finite Fields and Their Applications*, 13(4) :727 – 737, 2007.

Chapitre 3

Codes algébriques sur les surfaces de Hirzebruch minimales

Algebraic Geometric codes on minimal Hirzebruch surfaces

Jade Nardi *

May 27, 2019

Abstract

We define a linear code $C_\eta(\delta_T, \delta_X)$ by evaluating polynomials of bidegree (δ_T, δ_X) in the Cox ring on $\mathbb{F}_q$-rational points of a minimal Hirzebruch surface over the finite field $\mathbb{F}_q$. We give explicit parameters of the code, notably using Gröbner bases. The minimum distance provides an upper bound of the number of $\mathbb{F}_q$-rational points of a non-filling curve on a Hirzebruch surface.

AMS classification : 94B27, 14G50, 13P25, 14G15, 14M25
Keywords: Hirzebruch surface, Algebraic Geometric code, Gröbner basis, Rational scroll

Introduction

Until the 00's, most Goppa codes were associated to curves. In 2001 S.H. Hansen [Han01] estimated parameters of Goppa codes associated to normal projective varieties of dimension at least 2. As Hansen required very few assumptions on the varieties, the parameters he gave depended only on the Seshadri constant of the line bundle, which is hard to compute in practice. New classes of error correcting codes have thus been constructed, focusing on specific well-known families of varieties to better grasp the parameters. Among Goppa codes associated to a surface which have been studied so far, some toric and projective codes are based on Hirzebruch surfaces.

Toric codes, first introduced by J. P. Hansen [Han02] and further investigated by D. Joyner [Joy04], J. Little and H. Schenck [LS06], D. Ruano [Rua07] and I. Soprunov and J. Soprunova [SS09], are Goppa codes on toric varieties evaluating global sections of a line bundle at the $\mathbb{F}_q$-rational points of the torus. J. Little and H. Schenck [LS06] already computed the parameters of toric codes on Hirzeburch surfaces for some bidegrees and for q large enough to make the evaluation map injective.

Projective codes evaluate homogeneous polynomials on the rational points of a variety embedded in a projective space. A first example of projective codes is the family of projective Reed-Muller codes on $\mathbb{P}^n$ [Lac90]. A. Couvreur and

*Institut de Mathématiques de Toulouse ; UMR 5219, Université de Toulouse ; CNRS UPS IMT, F-31062 Toulouse Cedex 9, France jade.nardi@math.univ-toulouse.fr. Funded by ANR grant ANR-15-CE39-0013-01 "manta"

I. Duursma [CD13] studied codes on the biprojective space $\mathbb{P}^1 \times \mathbb{P}^1$ embedded in $\mathbb{P}^3$. The authors took advantage of the product structure of the variety, yielding a description of the code as a tensor product of two well understood Reed-Muller codes on $\mathbb{P}^1$. More recently C. Carvalho and V. G.L. Neumann [CN16] examined the case of rational surface scrolls $S(a_1, a_2)$ as subvarieties of $\mathbb{P}^{a_1+a_2+1}$, which extends the result on $\mathbb{P}^1 \times \mathbb{P}^1$, isomorphic to $S(1, 1)$.

In this paper we establish the parameters of Goppa codes corresponding to complete linear systems on minimal Hirzebruch surfaces $\mathcal{H}_\eta$, a family of projective toric surfaces indexed by $\eta \in \mathbb{N}$. This framework expands preceding works while taking advantage of both toric and projective features.

Regarding toric codes, we extend the evaluation map on the whole toric variety. This is analogous to the extension of affine Reed-Muller codes by projective ones introduced by G. Lachaud [Lac90], since we also evaluate at "points at infinity". In other words toric codes on Hirzebruch surfaces can be obtained by puncturing the codes studied here at the $4q$ points lying on the 4 torus-invariant divisors, that have at least one zero coordinate. As in the Reed-Muller case, through the extension process, the length turns to grow about twice as much as the minimum distance, as proved in Section 6.

Respecting the projective codes cited above, it turns out that rational surface scrolls are the image of some projective embeddings of a Hirzeburch surface, $\mathcal{H}_0$ for $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathcal{H}_{a_1-a_2}$ for $S(a_1, a_2)$. However no embedding of the Hirzebruch surface into a projective space is required for our study and the Cox ring replaces the usual $\mathbb{F}_q[X_0, \ldots, X_r]$ used in the projective context. Moreover, the embedded point of view forces to only evaluate polynomials of the Cox ring that are pullbacks of homogeneous polynomials of $\mathbb{F}_q[X_0, X_1, \ldots, X_r]$ under this embedding. No such constraint appears using the Cox ring and polynomials of any bidegree can be examined.

Toric codes have been mainly studied for q small enough to ensure the injectivity of the evaluation map. As in C. Carvalho and V. G.L. Neumann's work, no assumption of injectivity is needed here. In particular, the computation of the dimension of the code does not follow from Riemann-Roch theorem. For a given degree, this grants us a wider range of possible sizes for the alphabet, including the small ones.

Our study focuses on minimal Hirzeburch surfaces, putting aside $\mathcal{H}_1$, the blown-up of $\mathbb{P}^2$ at a point. Although most techniques can be used to tackle this case, some key arguments fail, especially when estimating the minimum distance.

The linear code $C_\eta(\delta_T, \delta_X)$ is defined as the evaluation code on $\mathbb{F}_q$-rational points of $\mathcal{H}_\eta$ of the set $R(\delta_T, \delta_X)$ of homogeneous polynomials of bidegree (δ_T, δ_X), defined in Section 1. The evaluation is naively not well-defined for a polynomial but a meaningful definition *à la* Lachaud [Lac90] is given in Paragraph 1.2.

Here the parameters of the code $C_\eta(\delta_T, \delta_X)$ are displayed as nice combinatoric quantities, from which quite intricate but explicit formulae can be deduced in Propositions 2.4.1 and 4.2.3. The rephrasing of the problem in combinatorial terms is already a key feature in Hansen's [Han02] and Carvalho and Neumann's works [CN16] that is readjusted here to fit a wider range of codes.

A natural way to handle the dimension of these codes is to calculate the number of classes under the equivalence relation $\equiv$ on the set $R(\delta_T, \delta_X)$ that identifies two polynomials if they have the same evaluation on every $\mathbb{F}_q$-rational point of the Hirzebruch surface. Our strategy is to first restrict the equivalence relation $\equiv$ on the set of monomials $\mathcal{M}(\delta_T, \delta_X)$ of $R(\delta_T, \delta_X)$ and a handy characterization for two monomials to be equivalent is given.

In most cases comprehending the equivalence relation over monomials is enough to compute the dimension. We have to distinguish a particular case:

$$\eta \geq 2, \quad \delta_T < 0, \quad \eta \mid \delta_T, \quad q \leq \delta_X + \tfrac{\delta_T}{\eta}. \tag{H}$$

Theorem A. *The dimension of the code $C_\eta(\delta_T, \delta_X)$ satisfies*

$$\dim C_\eta(\delta_T, \delta_X) = \#\left(\mathcal{M}(\delta_T, \delta_X)/\equiv\right) - \epsilon,$$

where ϵ is equal to 1 if the couple (δ_T, δ_X) satisfies (H) and 0 otherwise.

This quantity depends on the parameter η, the bidegree (δ_T, δ_X) and the size q of the finite field.

As for the dimension, the first step to determine the minimum distance is to bound it from below with a quantity that only depends on monomials. Again the strategy is similar to Carvalho and Neumann's one [CN16] but, even though they mentioned Gröbner bases, they did not fully benefit from the potential of the tools provided by Gröbner bases theory. Here, the approach to determine the minimum distance falls within the framework of *footprints bounds*, studied by O. Geil and T. Hoholdt [GH00] in the affine case and P. Beelen, M. Datta and S.R. Ghorpade [BDG19] in the projective one. These bounds on the number of points of a zero-dimensional set S are related to the footprint of the ideal I defining S, defined as the family of monomials which are not the leading monomial of any polynomial of I. Knowing a Gröbner basis of I gives a nice description of the foorprint of I. A similar strategy is used here with the homogeneous vanishing ideal $\mathcal{I}$ of the subvariety constituted by the $\mathbb{F}_q$-rational points in the Cox ring of $\mathcal{H}_\eta$. A good understanding of a Gröbner basis of $\mathcal{I}$, through Section 3, shortens the proof of the following theorem.

Theorem B. *Let us fix $(\epsilon_T, \epsilon_X) \in \mathbb{N}^2$ such that $\epsilon_T,\ \epsilon_X \geq q$. The minimum distance $d_\eta(\delta_T, \delta_X)$ satisfies*

$$d_\eta(\delta_T, \delta_X) \geq \min_{M \in \Delta^*(\delta_T, \delta_X)} \#\Delta^*(\epsilon_T, \epsilon_X)_M$$

where $\Delta^*(\epsilon_T, \epsilon_X)_M$ is defined in Notation 4.1.1. It is an equality for $\epsilon_T = \delta_T + \eta\delta_X + q$ and $\epsilon_X = \delta_X + q$.

This minimum depends on the parameter η, the bidegree (δ_T, δ_X) and the size q of the finite field.

The pullback of homogeneous polynomials of degree δ_X on $S(a_1, a_2) \subset \mathbb{P}^r$ studied by C. Carvalho and V. G.L. Neumann are polynomials of bidegree $(a_2\delta_X, \delta_X)$ on $\mathcal{H}_{a_1 - a_2}$. C. Carvalho and V. G.L. Neumann gave a lower bound of the minimum distance that we prove to be reached since it matches the parameters we establish here. The parameters also coincide with the one given by A. Couvreur and I. Duursma [CD13] in the case of the biprojective space $\mathbb{P}^1 \times \mathbb{P}^1$, isomorphic to Hirzebruch surface $\mathcal{H}_0$.

It is worth pointing out that the codes $C_\eta(\delta_T, \delta_X)$ with δ_T negative have never been studied until now. Although this case is intricate when the parameter η divides δ_T and the situation (H) occurs, it brings the ideal $\mathcal{I}$ to light as an example of a non binomial ideal on the toric variety $\mathcal{H}_\eta$.

The last section highlights an interesting feature of these codes which leads to a good puncturing. It results codes of length $q(q+1)$ but with identical dimension and minimum distance with the ones of the unpunctured codes.

1 Defining evaluation codes on Hirzebruch surfaces

1.1 Hirzebruch surfaces

We gather here some results about Hirzebruch surfaces over a field k, given in [CLS11] for instance.

Let η be a non negative integer. The *Hirzebruch surface* $\mathcal{H}_\eta$ can be considered from different points of view.

On one hand, the Hirzebruch surface $\mathcal{H}_\eta$ is the toric variety corresponding to the fan Σ_η (see Figure 1).

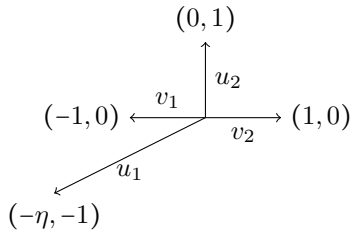


Figure 1: Fan Σ_η

The fan Σ_η being a refining of the one of $\mathbb{P}^1$, it yields a ruling $\mathcal{H}_\eta \to \mathbb{P}^1$ of fiber $\mathcal{F} \simeq \mathbb{P}^1$ and section σ. The torus-invariant divisors D_1, D_2, E_1 and E_2 corresponding to the rays spanned respectively by v_1, v_2, u_1, u_2 generate the Picard group of $\mathcal{H}_\eta$, described in the following proposition.

Proposition 1.1.1. *The Picard group of the Hirzebruch surface $\mathcal{H}_\eta$ is the free Abelian group*

$$\operatorname{Pic} \mathcal{H}_\eta = \mathbb{Z}\mathcal{F} + \mathbb{Z}\sigma$$

where

$$\mathcal{F} = E_1 \sim E_2 \text{ and } \sigma = D_2 \sim D_1 + \eta E_1. \tag{1}$$

We have the following intersection matrix.

	$\mathcal{F}$	σ
$\mathcal{F}$	0	1
σ	1	η

As a simplicial toric variety, the surface $\mathcal{H}_\eta$ considered over k carries a *Cox ring* $R = k[T_1, T_2, X_1, X_2]$. Each monomial $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$ of R is associated to a torus-invariant divisor

$$D_M = d_1 D_1 + d_2 D_2 + c_1 E_1 + c_2 E_2. \tag{2}$$

The *degree* of the monomial M is defined as the Picard class of the divisor D_M. The couple of coordinates (δ_T, δ_X) of D_M in the basis $(\mathcal{F}, \sigma)$ is called the *bidegree* of M and denoted by $\mathrm{bideg}(M)$. By (1) and (2),

$$\begin{cases} \delta_T &= c_1 + c_2 - \eta d_1, \\ \delta_X &= d_1 + d_2. \end{cases} \tag{3}$$

It is convenient to set

$$\delta = \delta_T + \eta \delta_X.$$

This gives the $\mathbb{Z}^2$-grading on R

$$R = \bigoplus_{(\delta_T, \delta_X) \in \mathbb{Z}^2} R(\delta_T, \delta_X)$$

where $R(\delta_T, \delta_X) \simeq H^0(\mathcal{H}_\eta, \mathcal{O}_{\mathcal{H}_\eta}(\delta_T \mathcal{F} + \delta_X \sigma))$ is the k-module of homogeneous polynomials of bidegree $(\delta_T, \delta_X) \in \mathbb{Z}^2$. Note that the $\mathbb{F}_q$-module $R(\delta_T, \delta_X)$ is non zero if and only if $\delta_X \in \mathbb{N}$ and $\delta \in \mathbb{N}$.

On the other hand, the Hirzebruch surface can be displayed as a geometric quotient of an affine variety under the action of an algebraic group ([CLS11] Theorem 5.1.11). This description is given for instance by M. Reid [Rei97].

Let us define an action of the product of multiplicative groups $\mathbb{G}_m \times \mathbb{G}_m$ over $\left(\mathbb{A}^2 \setminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \setminus \{(0,0)\}\right)$: write (t_1, t_2) for the first coordinates on $\mathbb{A}^2$, (x_1, x_2) on the second coordinates on $\mathbb{A}^2$ and (λ, μ) for elements of $\mathbb{G}_m \times \mathbb{G}_m$. The action is given as follows:

$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu \lambda^{-\eta} x_1, \mu x_2).$$

Then the Hirzebruch surface $\mathcal{H}_\eta$ is isomorphic to the geometric quotient

$$\left(\mathbb{A}^2 \setminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \setminus \{(0,0)\}\right) / \mathbb{G}_m^2.$$

This description enables us to describe a point of $\mathcal{H}_\eta$ by its homogeneous coordinates (t_1, t_2, x_1, x_2).

In this paper, we focus only on minimal Hirzebruch surfaces. A surface is minimal if it contains no -1 curve - *i.e.* a curve of genus 0 and self-intersection equal to 1. We recall the following well-known result about minimal Hirzebruch surface.

Theorem 1.1.2 ([LP10]). *The Hirzeburch surface $\mathcal{H}_\eta$ is minimal if and only if $\eta \neq 1$.*

1.2 Evaluation map

We consider now the case $k = \mathbb{F}_q$, q being a power of a prime integer.

From the ruling $\mathcal{H}_\eta \to \mathbb{P}^1$, the number of $\mathbb{F}_q$ rational points of the Hirzebruch surface $\mathcal{H}_\eta$ is

$$N = \#\mathcal{H}_\eta(\mathbb{F}_q) = (q+1)^2.$$

Let $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ such that $\delta \geq 0$. Given a polynomial $F \in R(\delta_T, \delta_X)$ and a point P of $\mathcal{H}_\eta$, *the evaluation of* F *at* P is defined by $F(P) = F(t_1, t_2, x_1, x_2)$, where (t_1, t_2, x_1, x_2) is the only tuple that belongs to the orbit of P under the action of $\mathbb{G}_m^2$ and has one of these forms:

- $(1, a, 1, b)$ with a, $b \in \mathbb{F}_q$,
- $(0, 1, 1, b)$ with $b \in \mathbb{F}_q$,
- $(1, a, 0, 1)$ with $a \in \mathbb{F}_q$,
- $(0, 1, 0, 1)$.

The *evaluation code* $C_\eta(\delta_T, \delta_X)$ is defined as the image of the evaluation map

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \begin{cases} R(\delta_T, \delta_X) & \to & \mathbb{F}_q^N \\ F & \mapsto & (F(P))_{P \in \mathcal{H}\eta(\mathbb{F}_q)}. \end{cases} \tag{4}$$

Note that this code is Hamming equivalent to the Goppa code $C(\mathcal{O}_{\mathcal{H}_\eta}(\delta_T \mathcal{F} + \delta_X \sigma), \mathcal{H}_\eta(\mathbb{F}_q))$, as defined by Hansen [Han01]. The *weight* $\omega(c)$ of a codeword $c \in C_\eta(\delta_T, \delta_X)$ is the number of non-zero coordinates. The minimum weight among all the non-zero codewords is called the *minimum distance* of the code $C_\eta(\delta_T, \delta_X)$ and is denoted by $d_\eta(\delta_T, \delta_X)$.

2 Dimension of the evaluation code $C_\eta(\delta_T, \delta_X)$ on the Hirzebruch surface $\mathcal{H}_\eta$

Let us consider $\eta \geq 0$ and $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ such that $\delta = \delta_T + \eta\delta_X \geq 0$.

Notation 2.0.1. The kernel of the map $\mathrm{ev}_{(\delta_T,\delta_X)}$ is denoted by $\mathcal{I}(\delta_T, \delta_X)$.

From the classical isomorphism

$$C_\eta(\delta_T, \delta_X) \simeq R(\delta_T, \delta_X) \diagup \mathcal{I}(\delta_T, \delta_X),$$

the dimension of the evaluation code $C_\eta(\delta_T, \delta_X)$ equals the dimension of any complementary vector space of $\mathcal{I}(\delta_T, \delta_X)$ in $R(\delta_T, \delta_X)$. This is tantamount to compute the image of a well-chosen projection map on $R(\delta_T, \delta_X)$ along $\mathcal{I}(\delta_T, \delta_X)$.

2.1 Focus on monomials

The aim of this section is to display a projection map, denoted by $\pi_{(\delta_T,\delta_X)}$, that would have the good property of mapping a monomial onto a monomial. The existence of such a projection is not true in full generality: given a vector subspace W of a vector space V and a basis $\mathcal{B}$ of V, it is not always possible to find a basis of W composed of differences of elements of $\mathcal{B}$ and a complementary space of W whose basis is a subset of $\mathcal{B}$. This will be possible here except if (H) holds.

With this goal in mind, our strategy is to focus first on monomials of $R(\delta_T,\delta_X)$. Let us define the following equivalence relation on the set of monomials of $R(\delta_T,\delta_X)$.

Definition 2.1.1. Let us define a binary relation $\equiv$ on the set $\mathcal{M}(\delta_T,\delta_X)$ of monomials of $R(\delta_T,\delta_X)$. Let $M_1, M_2 \in \mathcal{M}(\delta_T,\delta_X)$. We denote $M_1 \equiv M_2$ if they have the same evaluation at every $\mathbb{F}_q$-rational point of $\mathcal{H}_\eta$, i.e.

$$M_1 \equiv M_2 \Leftrightarrow \mathrm{ev}_{(\delta_T,\delta_X)}(M_1) = \mathrm{ev}_{(\delta_T,\delta_X)}(M_2) \Leftrightarrow M_1 - M_2 \in \mathcal{I}(\delta_T,\delta_X).$$

This section is intended to prove that, even if this equivalence relation can be defined over all $R(\delta_T,\delta_X)$, the number of equivalence classes when considering all polynomials is the same as when regarding only monomials, unless (H) holds. Thus the aim of this section is to prove Theorem A, stated in the introduction.

2.2 Combinatorial point of view of the equivalence relation on monomials

Throughout this article, the set $R(\delta_T,\delta_X)$ is pictured as a polygon in $\mathbb{N}\times\mathbb{N}$ of coordinates (d_2,c_2). This point of view, inherited directly from the toric structure, is common in the study of toric codes ([Han02], [Joy04], [Rua07], [LS06], [SS09]). It will be useful to handle the computation of the dimension and the minimum distance as a combinatorial problem.

Definition 2.2.1. Let $(\delta_T,\delta_X) \in \mathbb{Z}\times\mathbb{N}$. Let us define the polygon

$$P_D = \{(a,b) \in \mathbb{R}^2 \mid a \geq 0,\ b \geq 0,\ a \leq \delta_X \text{ and } \eta a + b \leq \delta\}$$

associated to the divisor $D = \delta E_1 + \delta_X D_1 \sim \delta_T \mathcal{F} + \delta_X \sigma$ and

$$\mathcal{P}(\delta_T,\delta_X) = P_D \cap \mathbb{Z}^2.$$

Being intersection of $\mathbb{Z}^2$ with half planes, it is easily seen that $\mathcal{P}(\delta_T,\delta_X)$ is the set of lattice points of the polygon P_D, whose vertices are

- $(0,0),(\delta_X,0),(\delta_X,\delta_T),(0,\delta)$ if $\delta_T > 0$,
- $(0,0),(\frac{\delta}{\eta},0),(0,\delta)$ if $\delta_T < 0$ and $\eta > 0$ or $\delta_T = 0$.

Note that P_D is a lattice polygone except if $\delta_T < 0$ and η does not divide δ_T.

Notation 2.2.2. Let us set

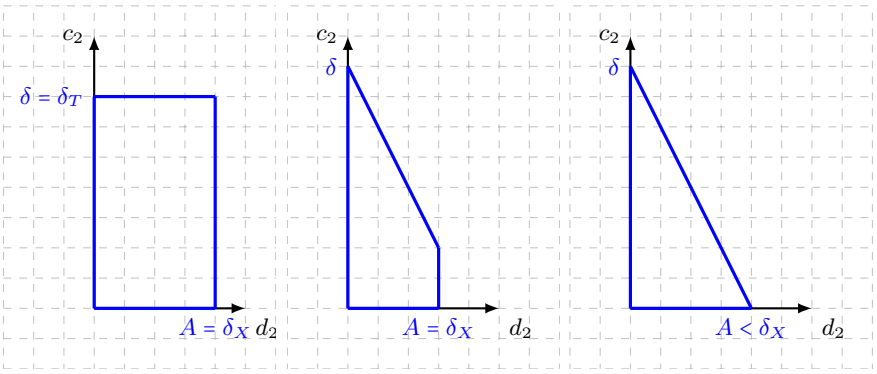
$$A = A(\eta,\delta_T,\delta_X) = \min\left(\delta_X, \frac{\delta}{\eta}\right) = \begin{cases} \delta_X & \text{if } \delta_T \geq 0, \\ \frac{\delta}{\eta} = \delta_X + \frac{\delta_T}{\eta} & \text{otherwise,} \end{cases}$$

the x-coordinate of the right-most vertices of the polygon P_D.

Let us highlight that A is not necessarily an integer if $\delta_T < 0$. Thus it does not always appear as the first coordinate of an element of $\mathcal{P}(\delta_T, \delta_X)$. It is the case if and only if $\eta \mid \delta_T$. If so, the only element of $\mathcal{P}(\delta_T, \delta_X)$ such that A is its first coordinate is $(A, 0)$.

We thus observe that

$$\mathcal{P}(\delta_T, \delta_X) = \{(a, b) \in \mathbb{N}^2 \mid a \in [\![0, \lfloor A \rfloor]\!] \text{ and } b \in [\![0, \delta_T + \eta(\delta_X - a)]\!]\}. \tag{5}$$



(a) $\eta = 0$ e.g. $\mathcal{P}(7, 4)$ (b) $\eta > 0$, $\delta_T > 0$ e.g. $\mathcal{P}(2, 3)$ in $\mathcal{H}_2$ (c) $\eta > 0$, $\delta_T \leq 0$ e.g. $\mathcal{P}(-2, 5)$ in $\mathcal{H}_2$

Figure 2: Different shapes of the polygon $\mathcal{P}(\delta_T, \delta_X)$

Example 2.2.3. *Figure 2 gives the three examples of possible shapes of the polygon $\mathcal{P}(\delta_T, \delta_X)$. The first one is the case $\eta = 0$, and the last two ones correspond to $\eta > 0$ and depend on the sign of δ_T, which determines the shape of P_D. All proofs of explicit formulae in Propositions 2.4.1 and 4.2.3 distinguish these cases.*

Thanks to (3), a monomial of $R(\delta_T, \delta_X)$ is entirely determined by the couple (d_2, c_2). Then each element of $\mathcal{P}(\delta_T, \delta_X)$ corresponds to a unique monomial. More accurately, for any couple $(d_2, c_2) \in \mathcal{P}(\delta_T, \delta_X)$, we define the monomial

$$M(d_2, c_2) = T_1^{\delta_T + \eta(\delta_X - d_2) - c_2} T_2^{c_2} X_1^{\delta_X - d_2} X_2^{d_2} \in \mathcal{M}(\delta_T, \delta_X). \tag{6}$$

Definition 2.2.4. The equivalence relation $\equiv$ on $\mathcal{M}(\delta_T, \delta_X)$ and the bijection

$$\begin{cases} \mathcal{P}(\delta_T, \delta_X) & \to & \mathcal{M}(\delta_T, \delta_X) \\ (d_2, c_2) & \mapsto & M(d_2, c_2) \end{cases} \tag{7}$$

endow $\mathcal{P}(\delta_T, \delta_X)$ with a equivalence relation, also denoted by $\equiv$, such that

$$(d_2, c_2) \equiv (d_2', c_2') \Leftrightarrow M(d_2, c_2) \equiv M(d_2', c_2').$$

Proposition 2.2.5. *Let two couples (d_2, c_2) and (d_2', c_2') be in $\mathcal{P}(\delta_T, \delta_X)$ and let us write*

$$M = M(d_2, c_2) = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \text{ and } M' = M(d_2', c_2') = T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_2^{d_2'}.$$

Then $(d_2, c_2) \equiv (d_2', c_2')$ *if and only if*

$$q-1 \mid d_i - d_i', \tag{C1}$$
$$q-1 \mid c_j - c_j', \tag{C2}$$
$$d_i = 0 \Leftrightarrow d_i' = 0, \tag{C3}$$
$$c_j = 0 \Leftrightarrow c_j' = 0. \tag{C4}$$

Proof. The conditions (C1), (C2), (C3) and (C4) clearly imply that $M(d_2, c_2) \equiv M(d_2', c_2')$, hence $(d_2, c_2) \equiv (d_2', c_2')$. To prove the converse, assume that $M \equiv M'$ and write

$$M = M(d_2, c_2) = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \text{ and } M' = M(d_2', c_2') = T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_n^{d_2'}.$$

Let $x \in \mathbb{F}_q$. Then $M(1, x, 1, 1) = M'(1, x, 1, 1)$, which means $x^{c_2} = x^{c_2'}$. But this equality is true for any element x of $\mathbb{F}_q$ if and only if $(T_2^q - T_2) \mid (T_2^{c_2} - T_2^{c_2'})$. This is equivalent to $c_2 = c_2' = 0$ or $c_2 c_2' \neq 0$ and $T_2^{q-1} - 1 \mid T_2^{c_2'-1}(T_2^{c_2 - c_2'} - 1)$, which proves (C2) and (C4) for $i = 2$.

Repeating this argument evaluating at $(1, 1, 1, x)$ for every $x \in \mathbb{F}_q$ gives $q - 1 \mid d_2 - d_2'$ and $d_2 = 0$ if and only if $d_2' = 0$, i.e. (C1) and (C3) for $i = 2$.

Moreover, we have $d_1 + d_2 = d_1' + d_2' = \delta_X$, which means that $q - 1 \mid d_2 - d_2'$ if and only if $q - 1 \mid d_1 - d_1'$. Evaluating at $(1, 1, 0, 1)$ gives $0^{d_1} = 0^{d_1'}$. Then $d_1 = 0$ if and only if $d_1' = 0$. This proves (C1) and (C3) for $i = 1$.

It remains the case of c_1 and c_1'. We have

$$c_1 - c_1' = c_2' - c_2 - \eta(d_1' - d_1)$$

and $q - 1$ divides $c_2 - c_2'$ and $d_1' - d_1$. Then it also divides $c_1 - c_1'$. Evaluating at $(0, 1, 1, 1)$ yields like previously $c_1 = 0$ of and only if $c_1' = 0$. □

Remark 2.2.6. The conditions of Lemma 2.2.5 also can be written

$$c_i = c_i' = 0 \text{ or } c_i c_i' \neq 0 \text{ and } q - 1 \mid c_i' - c_i, \tag{8}$$
$$d_i = d_i' = 0 \text{ or } d_i d_i' \neq 0 \text{ and } q - 1 \mid d_i' - d_i. \tag{9}$$

Besides, the conditions involving q are always satisfied for $q = 2$.

Observation 2.2.7. The conditions (C3) and (C4) mean that a point of $\mathcal{P}(\delta_T, \delta_X)$ lying on an edge of P_D can be equivalent only with a point lying on the same edge. Therefore the equivalence class of a vertex of P_D is a singleton.

To prove that the number of equivalence classes equals the dimension of the code $C_\eta(\delta_T, \delta_X)$ as stated in Theorem A (unless (H) holds), we will indicate a set $\mathcal{K}(\delta_T, \delta_X)$ of representatives of the equivalence classes of $\mathcal{P}(\delta_T, \delta_X)$ under the relation $\equiv$, which naturally gives a set of representatives $\Delta(\delta_T, \delta_X)$ for $\mathcal{M}(\delta_T, \delta_X)$ under the binary relation $\equiv$.

Notation 2.2.8. Let $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ and $q \geq 2$. Let us set

$$\mathcal{A}_X = \{\alpha \in \mathbb{N} \mid 0 \leq \alpha \leq \min(\lfloor A \rfloor, q-1)\} \cup \{A\} \cap \mathbb{N},$$
$$\mathcal{K}(\delta_T, \delta_X) = \left\{ (\alpha, \beta) \in \mathbb{N}^2 \;\middle|\; \begin{array}{c} \alpha \in \mathcal{A}_X \\ 0 \leq \beta \leq \min(\delta - \eta\alpha, q) - 1 \text{ or } \beta = \delta - \eta\alpha \end{array} \right\},$$
$$\Delta(\delta_T, \delta_X) = \{M(\alpha, \beta) \mid (\alpha, \beta) \in \mathcal{K}(\delta_T, \delta_X)\}.$$

Notice that $\mathcal{K}(\delta_T, \delta_X)$ is nothing but $\mathcal{P}(\delta_T, \delta_X)$ cut out by the set

$$(\{d_2 \leq q-1\} \cup \{d_2 = A\}) \cap (\{c_2 \leq q-1\} \cup \{c_2 = \delta - \eta d_2)\}) .$$

Example 2.2.9. *Let us set $\eta = 2$ and $q = 3$. Let us sort the monomials of $\mathcal{M}(-2,5)$, grouping the ones with the same image under $\mathrm{ev}_{(-2,5)}$, using Proposition 2.2.5.*

Figure 3 represents the set $\mathcal{K}(-2,5)$. Note that for each couple $(d_2, c_2) \in \mathcal{K}(-2,5)$, there is exactly one of these groups that contains the monomial $M(d_2, c_2)$.

Exponents (c_1, c_2, d_1, d_2) of $T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$	*Couple in $\mathcal{K}(-2,5)$*
$(8,0,5,0)$	$(0,0)$
$(7,1,5,0) \sim (5,3,5,0) \sim (3,5,5,0) \sim (1,7,5,0)$	$(0,1)$
$(6,2,5,0) \sim (4,4,5,0) \sim (2,6,5,0)$	$(0,2)$
$(0,8,5,0)$	$(0,8)$
$(6,0,4,1) \sim (2,0,2,3)$	$(1,0)$
$(5,1,4,1) \sim (3,3,4,1) \sim (1,5,4,1) \sim (1,1,2,3)$	$(1,1)$
$(4,2,4,1) \sim (2,4,4,1)$	$(1,2)$
$(0,6,4,1) \sim (0,2,2,3)$	$(1,6)$
$(4,0,3,2)$	$(0,2)$
$(3,1,3,2) \sim (1,3,3,2)$	$(2,1)$
$(2,2,3,2)$	$(2,2)$
$(0,4,3,2)$	$(2,4)$
$(0,0,1,4)$	$(4,0)$

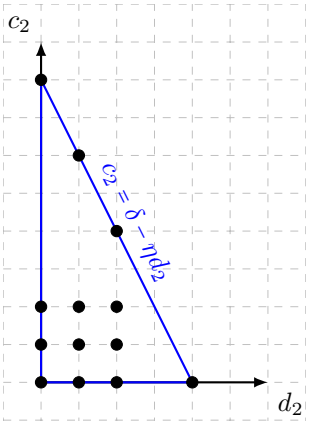


Figure 3: Dots in $\mathcal{P}(-2,5)$ correspond to elements of $\mathcal{K}(-2,5)$.

Motivated by Example 2.2.9, we give a map that displays $\mathcal{K}(\delta_T, \delta_X)$ as a set of representatives of $\mathcal{P}(\delta_T, \delta_X)$ under the equivalence relation $\equiv$.

Definition 2.2.10. Let us set the map $p_{(\delta_T, \delta_X)} : \mathcal{P}(\delta_T, \delta_X) \to \mathcal{P}(\delta_T, \delta_X)$ such that for every couple $(d_2, c_2) \in \mathcal{P}(\delta_T, \delta_X)$ its image $p_{(\delta_T, \delta_X)}(d_2, c_2) = (d_2', c_2')$ is defined as follows.

- If $d_2 = 0$ or $d_2 = A$, then $d_2' = d_2$,

- Otherwise, we choose $d_2' \equiv d_2 \mod q-1$ with $1 \leq d_2' \leq q-1$.

and

- If $c_2 = 0$, then $c_2' = 0$,
- If $c_2 = \delta - \eta d_2$, then $c_2' = \delta - \eta d_2'$,
- Otherwise, we choose $c_2' \equiv c_2 \mod q-1$ with $1 \leq c_2' \leq q-1$.

Proposition 2.2.11. *1. The map $p_{(\delta_T,\delta_X)}$ induces a bijection from the quotient set $\mathcal{P}(\delta_T,\delta_X)/\equiv$ to $\mathcal{K}(\delta_T,\delta_X)$.*

2. The set $\mathcal{K}(\delta_T,\delta_X)$ is a set of representatives of $\mathcal{P}(\delta_T,\delta_X)$ under the equivalence relation $\equiv$.

3. The set $\Delta(\delta_T,\delta_X)$ is a set of representatives of $\mathcal{M}(\delta_T,\delta_X)$ under the equivalence relation $\equiv$.

Proof. First notice that elements of $\mathcal{K}(\delta_T,\delta_X)$ are invariant under $p_{(\delta_T,\delta_X)}$.

The inclusion $p_{(\delta_T,\delta_X)}(\mathcal{P}(\delta_T,\delta_X)) \subset \mathcal{K}(\delta_T,\delta_X)$ is clear by definitions of $\mathcal{K}(\delta_T,\delta_X)$ (Not. 2.2.8) and $p_{(\delta_T,\delta_X)}$ (Def. 2.2.10). The equality follows from the invariance of $\mathcal{K}(\delta_T,\delta_X)$.

Last, we prove that $p_{(\delta_T,\delta_X)}(d_2,c_2) \equiv (d_2,c_2)$ for every couple $(d_2,c_2) \in \mathcal{P}(\delta_T,\delta_X)$. Take a couple $(d_2,c_2) \in \mathcal{P}(\delta_T,\delta_X)$ and denote by (d_2',c_2') its image under $p_{(\delta_T,\delta_X)}$. We have to prove that (d_2,c_2) and (d_2',c_2) satisfy all the conditions of Proposition 2.2.5.

By definition of $p_{(\delta_T,\delta_X)}$, it is clear that conditions (C1), (C2), (C3), as well as the the forward implication of (C4), are true. It remains to prove that $c_i' = 0 \Rightarrow c_i = 0$ for $i \in \{1,2\}$.

Let us prove only the case $i = 2$. So assume that $c_2' = 0$. Then $c_2 = 0$ or $c_2 = \delta - \eta d_2$. However,

$$c_2 = \delta - \eta d_2 \Leftrightarrow c_2' = \delta - \eta d_2' = 0 \Leftrightarrow d_2' = \frac{\delta}{\eta}.$$

This is only possible when $\delta_T \leq 0$ and then $d_2' = A$. By condition (C3), this implies that $d_2 = A$ and then $c_2 = 0$. This proves the first item.

The second assertion is a straightforward consequence of the first one.

Finally the third assertion yields from the definition of the equivalence relation $\equiv$ on $\mathcal{P}(\delta_T,\delta_X)$ via the bijection (7). □

Corollary 2.2.12. *The number of equivalence classes $\#\Delta(\delta_T,\delta_X)$ of $\mathcal{M}(\delta_T,\delta_X)$ under $\equiv$ is equal to the cardinality of $\mathcal{K}(\delta_T,\delta_X)$.*

Proof. This follows from Definition 2.2.4 and Proposition 2.2.11. □

2.3 Proof of Theorem A

The main idea of the proof is to define an endomorphism on the basis of monomials $\mathcal{M}(\delta_T,\delta_X)$ by conjugation of $p_{(\delta_T,\delta_X)}$ by the bijection (7) and prove it to be a projection along $\mathcal{I}(\delta_T,\delta_X)$ onto $\operatorname{Span}\Delta(\delta_T,\delta_X)$. However, when (H) occurs, there is a non trivial linear combination of elements of $\Delta(\delta_T,\delta_X)$ lying in $\mathcal{I}(\delta_T,\delta_X)$, as pointed out in the following lemma.

Lemma 2.3.1. *Let $(\delta_T, \delta_X) \in \mathbb{Z}^2$. Assume that $\eta \geq 2$, $\delta_T < 0$, $\eta \,|\, \delta_T$ and $q \leq \frac{\delta}{\eta}$, i.e. (H) holds. Let us set $k \in \mathbb{N}$ and $r \in [\![1, q-1]\!]$ such that*

$$A = \frac{\delta}{\eta} = k(q-1) + r.$$

The polynomial

$$\begin{aligned} F_0 =& M(A,0) - M(r,0) + M(r,q-1) - M(r,\eta k(q-1)) \\ & X_1^{-\frac{\delta_T}{\eta}} X_2^{\frac{\delta}{\eta}} - T_1^{\eta k(q-1)} X_1^{k(q-1)-\frac{\delta_T}{\eta}} X_2^r \\ & + T_1^{(\eta k-1)(q-1)} T_2^{q-1} X_1^{k(q-1)-\frac{\delta_T}{\eta}} X_2^r - T_2^{\eta k(q-1)} X_1^{k(q-1)-\frac{\delta_T}{\eta}} X_2^r \end{aligned}$$

belongs to $\mathcal{I}(\delta_T, \delta_X)$.

Proof. Let us prove that the polynomial F_0 vanishes at every $\mathbb{F}_q$-rational of $\mathcal{H}_\eta$.

For any $a \in \mathbb{F}_q$, we have $F_0(1,a,0,1) = 0$ and $F_0(0,1,0,1) = 0$ since every polynomial in $R(\delta_T, \delta_X)$ is divisible by X_1 when $\delta_T < 0$.

For $(a,b) \in \mathbb{F}_q^2$, $F_0(1,a,1,b) = b^{\frac{\delta}{\eta}} - b^r + a^{q-1}b^r - a^{\eta k(q-1)}b^r = 0$, as $q-1 \,|\, \frac{\delta}{\eta} - r \neq 0$.

For the same reason, $F_0(0,1,1,b) = b^{\delta_X + \frac{\delta_T}{\eta}} - 0 + 0 - b^r = 0$ for any $b \in \mathbb{F}_q$. □

The previous lemma displays a polynomial with 4 terms in the kernel when the couple (δ_T, δ_X) satisfies (H). We thus have to adjust the endomorphism in this case.

Definition 2.3.2. Let us set the linear map $\pi_{(\delta_T,\delta_X)} : R(\delta_T, \delta_X) \to R(\delta_T, \delta_X)$ such that for every $(d_2, c_2) \in P(\delta_T, \delta_X)$,

$$\pi_{(\delta_T,\delta_X)}(M(d_2,c_2)) = M(p_{(\delta_T,\delta_X)}(d_2,c_2))$$

except for $(d_2, c_2) = \left(\frac{\delta}{\eta}, 0\right)$ when the couple (δ_T, δ_X) satisfies (H). In this case, set (r,k) is the unique couple of integers such that $\frac{\delta}{\eta} = k(q-1)+r$ with $r \in [\![1, q-1]\!]$ and

$$\pi_{(\delta_T,\delta_X)}\left(M\left(\frac{\delta}{\eta}, 0\right)\right) = M(r,0) + M(r,\eta k(q-1)) - M(r,q-1).$$

Remark 2.3.3. The monomials $M(r,0)$, $M(r,\eta k(q-1))$ and $M(r,q-1)$, that appear in the definition above, belong to $\Delta(\delta_T, \delta_X)$.

Notation 2.3.4. Let $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ such that $\delta \geq 0$. If (H) holds, we set

$$\begin{aligned} \mathcal{K}^*(\delta_T,\delta_X) &= \mathcal{K}(\delta_T,\delta_X) \setminus \left\{\left(\frac{\delta}{\eta}, 0\right)\right\} \\ &= \left\{(\alpha,\beta) \in \mathbb{N}^2 \;\middle|\; \begin{array}{c} \alpha \in [\![0, q-1]\!] \\ 0 \leq \beta \leq \min(\delta - \eta\alpha, q) - 1 \text{ or } \beta = \delta - \eta\alpha \end{array} \right\}, \end{aligned}$$

and

$$\Delta^*(\delta_T,\delta_X) = \{M(\alpha,\beta) \,|\, (\alpha,\beta) \in \mathcal{K}^*(\delta_T,\delta_X)\}.$$

Otherwise, we set

$$\mathcal{K}^*(\delta_T,\delta_X) = \mathcal{K}(\delta_T,\delta_X) \text{ and } \Delta^*(\delta_T,\delta_X) = \Delta(\delta_T,\delta_X).$$

Lemma 2.3.5. *The only zero linear combination of elements of* $\Delta^*(\delta_T, \delta_X)$ *that belongs to* $\mathcal{I}(\delta_T, \delta_X)$ *is the trivial one.*

Proof. Let us assume that a linear combination of elements of $\Delta^*(\delta_T, \delta_X)$

$$H = \sum_{(\alpha,\beta)\in\mathcal{K}^*(\delta_T,\delta_X)} \lambda_{\alpha,\beta} M(\alpha,\beta)$$

satisfies $\mathrm{ev}_{(\delta_T,\delta_X)}(H) = 0$.

On one side, $H(1,0,1,0) = \lambda_{0,0}$, $H(1,0,0,1) = \lambda_{\delta_X,0}$, $H(0,1,0,1) = \lambda_{\delta_X,\delta_T}$ and $H(0,1,1,0) = \lambda_{0,\delta}$. Then $\lambda_{0,0} = \lambda_{\delta_X,0} = \lambda_{\delta_X,\delta_T} = \lambda_{0,\delta} = 0$. On the other side, evaluating at $(1,a,1,0)$ for any $a \in \mathbb{F}_q$ gives

$$H(1,a,1,0) = \sum_{\beta=1}^{\min(q-1,\delta-1)} \lambda_{0,\beta}\, a^\beta = 0.$$

Then the polynomial

$$\sum_{\beta=1}^{\min(q-1,\delta-1)} \lambda_{0,\beta}\, X^\beta$$

of degree less than $(q-1)$ has q zeros. This implies that $\lambda_{0,\beta} = 0$ for any β such that $(0,\beta) \in \mathcal{K}^*(\delta_T, \delta_X)$. Evaluating at $(1,a,0,1)$, we can deduce that $\lambda_{\delta_X,\beta} = 0$ for any β such that $(\delta_X, \beta) \in \mathcal{K}^*(\delta_T, \delta_X)$.

To evaluate at $(1,0,1,a)$, two cases are distinguished.

- If $\delta_T \geq 0$,
$$H = (1,0,1,a) = \sum_{\alpha=1}^{\min(\delta_X,q)-1)} \lambda_{\alpha,0}\, a^\alpha = 0,$$
which implies with the same argument that $\lambda_{\alpha,0} = 0$ for every α such that $(\alpha, B(\alpha)) \in \mathcal{K}^*(\delta_T, \delta_X)$.
- If $\delta_T < 0$,
$$H = (1,0,1,a) = \sum_{\alpha=1}^{\min(\lfloor A \rfloor,q-1)} \lambda_{\alpha,0}\, a^\alpha = 0$$
and we can repeat the same argument as before.

Similarly, by evaluating at $(0,1,1,a)$, we have $\lambda_{\alpha,B(\alpha)} = 0$ for any α such that $(\alpha, B(\alpha)) \in \mathcal{K}^*(\delta_T, \delta_X)$.

For any a, $b \in \mathbb{F}_q$, we then have

$$H(1,a,1,b) = \sum_{\alpha=1}^{\min(q-1,\delta_X-1)} \left(\sum_{\beta=1}^{\min(q-1,B(\alpha)-1)} \lambda_{\alpha,\beta}\, a^\beta \right) b^\alpha = 0$$

which implies that for any $a \in \mathbb{F}_q$, the polynomial

$$\sum_{\alpha=1}^{\min(q-1,\delta_X-1)} \left(\sum_{\beta=1}^{\min(q-1,B(\alpha)-1)} \lambda_{\alpha,\beta}\, a^\beta \right) X^\alpha$$

of degree lesser than $(q-1)$ has q zeros and, thus, is zero. By the same argument on each coefficient as polynomials of variable a, we then have proved that the linear combination H is zero. □

Theorem A follows from the following proposition.

Proposition 2.3.6. *The linear map $\pi_{(\delta_T,\delta_X)}$ is the projection along $\mathcal{I}(\delta_T,\delta_X)$ onto* $\operatorname{Span}\Delta^*(\delta_T,\delta_X)$. *Moreover the elements of $\Delta^*(\delta_T,\delta_X)$ are linearly independent.*

Proof. By construction of $\Delta^*(\delta_X,\delta_T)$, the definition of $\pi_{(\delta_T,\delta_X)}$ and Remark 2.3.3, it is clear that $\operatorname{range}\pi_{(\delta_T,\delta_X)} \subset \operatorname{Span}\Delta^*(\delta_T,\delta_X)$. Also, by Proposition 2.2.11 and the bijection (7), any monomial of $\Delta^*(\delta_T,\delta_X)$ is invariant under $\pi_{(\delta_T,\delta_X)}$, which ensures $\operatorname{range}\pi_{(\delta_T,\delta_X)} = \operatorname{Span}\Delta^*(\delta_T,\delta_X)$ and $\pi_{(\delta_T,\delta_X)}$ is a projection. Then

$$R(\delta_T,\delta_X) = \operatorname{range}\pi_{(\delta_T,\delta_X)} \oplus \ker\pi_{(\delta_T,\delta_X)} = \operatorname{Span}\Delta^*(\delta_T,\delta_X) \oplus \ker\pi_{(\delta_T,\delta_X)}. \quad (10)$$

By Proposition 2.2.11 and Lemma 2.3.1, we have

$$\forall\, M \in \mathcal{M}(\delta_T,\delta_X),\ M - \pi_{(\delta_T,\delta_X)}(M) \in \mathcal{I}(\delta_T,\delta_X),$$

which proves the inclusion $\ker\pi_{(\delta_T,\delta_X)} = \operatorname{range}(\mathrm{Id} - \pi_{(\delta_T,\delta_X)}) \subset \mathcal{I}(\delta_T,\delta_X)$.

The proof is completed by Lemma 2.3.5, which implies that the family $\Delta^*(\delta_T,\delta_X)$ is linearly independent modulo $\mathcal{I}(\delta_T,\delta_X)$. It also implies

$$\mathcal{I}(\delta_T,\delta_X) \cap \operatorname{Span}(\Delta^*(\delta_T,\delta_X) = \{0\},$$

which entails the equality $\ker\pi_{(\delta_T,\delta_X)} = \mathcal{I}(\delta_T,\delta_X)$. Indeed, $\ker\pi_{(\delta_T,\delta_X)}$ is a complementary space of $\operatorname{Span}(\Delta^*(\delta_T,\delta_X))$ in $R(\delta_T,\delta_X)$ by (10). Since $\ker\pi_{(\delta_T,\delta_X)}$ is included in $\mathcal{I}(\delta_T,\delta_X)$, if the intersection of $\mathcal{I}(\delta_T,\delta_X)$ and $\operatorname{Span}(\Delta^*(\delta_T,\delta_X))$ is the nullspace then $\ker\pi_{(\delta_T,\delta_X)} = \mathcal{I}(\delta_T,\delta_X)$. □

Proposition 2.3.6 displays $\Delta^*(\delta_T,\delta_X)$ as a set of representatives of $R(\delta_T,\delta_X)$ modulo $\mathcal{I}(\delta_T,\delta_X)$ and proves Theorem A, which can be rephrased as follows.

Corollary 2.3.7. *The dimension of the code $C_\eta(\delta_T,\delta_X)$ equals*

$$\dim C_\eta(\delta_T,\delta_X) = \#\mathcal{K}^*(\delta_T,\delta_X).$$

Proof. This is a straightforward consequence of Corollary 2.2.12 and Theorem A. □

Example 2.3.8. *We can easily deduce from Corollary 2.3.7 that the evaluation map $\mathrm{ev}_{(\delta_T,\delta_X)}$ is surjective if $\delta_T \geq q$ and $\delta_X \geq q$. Indeed, in this case,*

$$\mathcal{K}^*(\delta_T,\delta_X) = \mathcal{K}(\delta_T,\delta_X) = \left\{(\alpha,\beta) \in \mathbb{N}^2 \;\middle|\; \begin{array}{c} \alpha \in [\![0,q-1]\!] \cup \{\delta_X\} \\ \beta \in [\![0,q-1]\!] \cup \{\delta - \eta\alpha\} \end{array}\right\},$$

so that $\dim C_\eta(\delta_T,\delta_X) = \#\mathcal{K}^*(\delta_T,\delta_X) = (q+1)^2 = N$.

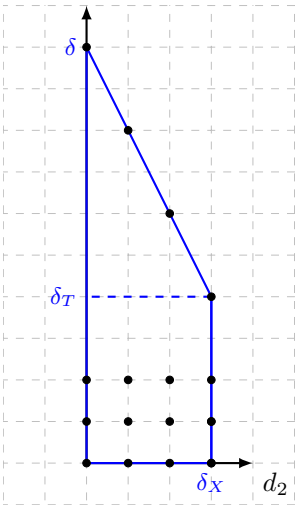


Figure 4: Example of $\mathcal{P}(\delta_T, \delta_X)$ when $\mathrm{ev}_{(\delta_T,\delta_X)}$ is surjective: $\mathcal{P}(4,3)$ with $q = 3$ in $\mathcal{H}_2$

2.4 Explicit formulae for the dimension of $C_\eta(\delta_T, \delta_X)$ and examples

By Corollary 2.3.7, computing the dimension is now reduced to the combinatorial question about the number of couples in $\mathcal{K}^*(\delta_T, \delta_X)$. The key of the proof of Proposition 2.4.1 below is to give a well-chosen partition of $\mathcal{K}^*(\delta_T, \delta_X)$ from which we can easily deduce its cardinality. Putting aside the very particular case of $\eta = 0$, two cases have to be distinguished according to the sign of δ_T, which determinates the shape of $\mathcal{P}(\delta_T, \delta_X)$ and the value of A. These two cases are themselves subdivided into several subcases, depending on the position of the preimage s of q under the function $x \mapsto \delta - \eta x$ with respect to $\mathcal{A}_X$, defined in Notation 2.2.8.

Proposition 2.4.1. *On $\mathcal{H}_0$, the dimension of the evaluation code $C_0(\delta_T, \delta_X)$ equals*

$$\dim C_0(\delta_T, \delta_X) = (\min(\delta_T, q) + 1)\,(\min(\delta_X, q) + 1)\,.$$

On $\mathcal{H}_\eta$ with $\eta \geq 2$, we set

$$m = \min(\lfloor A \rfloor, q-1),\ h = \begin{cases} \min(\delta_T, q) + 1 & \text{if } \delta_T \geq 0 \text{ and } q \leq \delta_X, \\ 0 & \text{otherwise,} \end{cases}$$

$$s = \frac{\delta - q}{\eta} \text{ and } \widetilde{s} = \begin{cases} \lfloor s \rfloor & \text{if } s \in [0, m], \\ -1 & \text{if } s < 0, \\ m & \text{if } s > m. \end{cases}$$

The evaluation code $C_\eta(\delta_T, \delta_X)$ on the Hirzebruch Surface $\mathcal{H}_\eta$ has dimension

$$\dim C_\eta(\delta_T, \delta_X) = (q+1)(\widetilde{s}+1) + (m - \widetilde{s})\left(\delta + 1 - \eta\left(\frac{m + \widetilde{s} + 1}{2}\right)\right) + h.$$

Remark 2.4.2. 1. For q large enough, the dimension is nothing but the number of points of $\mathcal{P}(\delta_T, \delta_X)$. This case was already studied by J. P. Hansen ([Han02] Theorem 1.5.)

2. The previous proposition generalizes the result of [CN16], in which the authors studied rational scrolls. For $a_1 \geq a_2 \geq 1$, the rational scroll $S(a_1, a_2)$ is isomorphic to the Hirzebruch surface $\mathcal{H}_{(a_1-a_2)}$ ([CLS11] Example 3.1.16.). This geometric isomorphism induces a Hamming isometry between the codes. We thus can compare our result with theirs for $\eta = a_1 - a_2$ and $\delta_T = a_2\delta_X$. Despite the appearing difference due to a different choice of monomial order (see Definition 3.0.3 and Remark 3.0.4), both formulae do coincide.

Proof. **To prove the case** $\eta = 0$, it is enough to write

$$\mathcal{K}^*(\delta_T, \delta_X) = \mathcal{K}(\delta_T, \delta_X) = \left\{ (\alpha, \beta) \in \mathbb{N}^2 \;\middle|\; \begin{array}{c} \alpha \in [\![0, \min(\delta_X, q) - 1]\!] \cup \{\delta_X\} \\ 0 \leq \beta \leq \min(\delta_T, q) - 1 \text{ or } \beta = \delta - \eta\alpha \end{array} \right\}.$$

Now, assume $\eta \geq 2$ **and** $\delta_T > 0$**.** Notice that the sets $\mathcal{K}^*(\delta_T, \delta_X)$ and $\mathcal{K}(\delta_T, \delta_X)$ always coincide in this case.

- Let us assume that $q > \delta_X$.
  - If $q > \delta$ also, then $s < 0$ and
  $$\mathcal{K}(\delta_T, \delta_X) = \bigcup_{\alpha=0}^{\delta_X} \{(\alpha, \beta) \mid \beta \in [\![0, \delta - \eta\alpha]\!]\}$$
  and thus $\#\mathcal{K}(\delta_T, \delta_X) = \sum_{\alpha=0}^{\delta_X} (\delta - \eta\alpha + 1) = (\delta_X + 1)\left(\delta_T + \eta\frac{\delta_X}{2} + 1\right)$.
  - If $\delta_T \leq q \leq \delta$, then $0 \leq s \leq \delta_X$ and one can write
  $$\begin{aligned} \mathcal{K}(\delta_T, \delta_X) = &\left(\bigcup_{\alpha=0}^{\lfloor s \rfloor} \{(\alpha, \beta) \mid \beta \in [\![0, q-1]\!] \cup \{\delta - \eta\alpha\}\} \right) \\ &\cup \left(\bigcup_{\alpha=\lfloor s \rfloor + 1}^{\delta_X} \{(\alpha, \beta) \mid \beta \in [\![0, \delta - \eta\alpha]\!]\} \right). \end{aligned}$$
  and thus $\begin{aligned} \#\mathcal{K}(\delta_T, \delta_X) &= \sum_{\alpha=0}^{\lfloor s \rfloor} (q+1) + \sum_{\alpha=\lfloor s \rfloor + 1}^{\delta_X} (\delta + 1 - \eta\alpha) \\ &= (q+1)(\lfloor s \rfloor + 1) + (\delta_X - \lfloor s \rfloor)\left(\delta + 1 - \eta\frac{\delta_X + \lfloor s \rfloor + 1}{2}\right). \end{aligned}$
  - If $\delta_X < q < \delta_T$, then $s > \delta_X$ and
  $$\mathcal{K}(\delta_T, \delta_X) = \left(\bigcup_{\alpha=0}^{\delta_X} \{(\alpha, \beta) \mid \beta \in [\![0, q-1]\!] \cup \{\delta - \eta\alpha\}\} \right)$$
  and then $\#\mathcal{K}(\delta_T, \delta_X) = (q+1)(\delta_X + 1)$.
- Let us assume that $q \leq \delta_X$.

– If $\frac{\delta}{\eta+1} < q$, then $0 \le s < q$ and $\lfloor s \rfloor \in \mathcal{A}_X$.

$$\begin{aligned}\mathcal{K}(\delta_T, \delta_X) = &\left(\bigcup_{\alpha=0}^{\lfloor s \rfloor} \{(\alpha, \beta) \mid \beta \in [\![0, q-1]\!] \cup \{\delta - \eta\alpha\}\} \right) \\ &\cup \left(\bigcup_{\alpha=\lfloor s \rfloor+1}^{q-1} \{(\alpha, \beta) \mid \beta \in [\![0, \delta - \eta\alpha]\!]\} \right) \\ &\cup \{(\delta_X, \beta) \mid \beta \in [\![0, h]\!]\}.\end{aligned}$$

Then

$$\begin{aligned}\#\mathcal{K}(\delta_T, \delta_X) &= \sum_{\alpha=0}^{\lfloor s \rfloor} (q+1) + \sum_{\alpha=\lfloor s \rfloor+1}^{q-1} (\delta + 1 - \eta\alpha) + h + 1. \\ &= (q+1)(\lfloor s \rfloor + 1) + (q - 1 - \lfloor s \rfloor) \left(\delta + 1 - \eta \frac{q + \lfloor s \rfloor}{2} \right) + h + 1\end{aligned}$$

– If $q \le \frac{\delta}{\eta+1}$, then $s \ge q$ and

$$\mathcal{K}(\delta_T, \delta_X) = \left(\bigcup_{\alpha=0}^{q-1} \{(\alpha, \beta) \mid \beta \in [\![0, q-1]\!] \cup \{\delta - \eta\alpha\}\} \right) \cup \{(\delta_X, \beta) | \beta \in [\![0, h]\!]\}.$$

Then $\#\mathcal{K}(\delta_T, \delta_X) = (q+1)q + h + 1$.

Finally assume $\eta \ge 2$ and $\delta_T \le 0$.

Let us rewrite $\mathcal{K}^*(\delta_T, \delta_X)$ to lead to formulae that coincide with the general one given above according to the position of q in the increasing sequence

$$\frac{\eta}{\eta+1} A < A \le \eta A,$$

with $A = \frac{\delta}{\eta}$. For any $\alpha \in \mathcal{A}_X$,

$$q \le \delta - \eta\alpha \Leftrightarrow \alpha \le \frac{\delta - q}{\eta} = s < A.$$

- If $q > \eta A$, then $\mathcal{K}^*(\delta_T, \delta_X) = \mathcal{K}(\delta_T, \delta_X)$, $s < 0$ and we can write

$$\mathcal{K}(\delta_T, \delta_X) = \bigcup_{\alpha=0}^{\lfloor A \rfloor} \{(\alpha, \beta) \mid \beta \in [\![0, \delta - \eta\alpha]\!]\}$$

and thus $\#\mathcal{K}(\delta_T, \delta_X) = \sum_{\alpha=0}^{\lfloor A \rfloor} (\delta - \eta\alpha + 1) = (\lfloor A \rfloor + 1) \left(\delta + 1 - \eta \frac{\lfloor A \rfloor}{2} \right)$.

- If $A < q \le \eta A$, we know that $\mathcal{K}^*(\delta_T, \delta_X) = \mathcal{K}(\delta_T, \delta_X)$ and we have

$$\mathcal{K}(\delta_T, \delta_X) = \left(\bigcup_{\alpha=0}^{\lfloor s \rfloor} \{(\alpha, \beta) \mid \beta \in [\![0, q-1]\!] \cup \{\delta - \eta\alpha\}\} \right) \cup \left(\bigcup_{\alpha=\lfloor s \rfloor+1}^{\lfloor A \rfloor} \{(\alpha, \beta) \mid \beta \in [\![0, \delta - \eta\alpha]\!]\} \right)$$

and then

$$\#\mathcal{K}(\delta_T,\delta_X) = \sum_{\alpha=0}^{\lfloor s\rfloor}(q+1) + \sum_{\alpha=\lfloor s\rfloor+1}^{\lfloor A\rfloor}(\delta-\eta\alpha+1)$$
$$= (q+1)(\lfloor s\rfloor+1) + (\lfloor A\rfloor-\lfloor s\rfloor)\left(\delta+1-\eta\frac{\lfloor A\rfloor+\lfloor s\rfloor+1}{2}\right).$$

- If $\frac{\eta}{\eta+1}A < q \le A$, then $q-1 < \lfloor A\rfloor$. Note that $\mathcal{K}^*(\delta_T,\delta_X) \neq \mathcal{K}(\delta_T,\delta_X)$ and

$$\mathcal{K}^*(\delta_T,\delta_X) = \left(\bigcup_{\alpha=0}^{\lfloor s\rfloor}\{(\alpha,\beta)\mid \beta\in[\![0,q-1]\!]\cup\{\delta-\eta\alpha\}\}\right)$$
$$\cup\left(\bigcup_{\alpha=\lfloor s\rfloor+1}^{q-1}\{(\alpha,\beta)\mid\beta\in[\![0,\delta-\eta\alpha]\!]\}\right)$$

Then

$$\#\mathcal{K}^*(\delta_T,\delta_X) = \sum_{\alpha=0}^{\lfloor s\rfloor}(q+1) + \sum_{\alpha=\lfloor s\rfloor+1}^{q-1}(\delta-\eta\alpha+1)$$
$$= (q+1)(\lfloor s\rfloor+1) + (q-1-\lfloor s\rfloor)\left(\delta+1-\eta\frac{q+\lfloor s\rfloor}{2}\right)$$

- If $q \le \frac{\eta}{\eta+1}A$, then $s \ge q$, $\mathcal{K}^*(\delta_T,\delta_X) \neq \mathcal{K}(\delta_T,\delta_X)$ and

$$\mathcal{K}^*(\delta_T,\delta_X) = \left(\bigcup_{\alpha=0}^{q-1}\{(\alpha,\beta)\mid\beta\in[\![0,q-1]\!]\cup\{\delta-\eta\alpha\}\}\right)$$

which gives $\#\mathcal{K}^*(\delta_T,\delta_X) = (q+1)q$.

□

2.5 Examples

Example 2.5.1. *Let us compute the dimension of the code $C_2(-2,5)$ using the previous formula on different finite fields. We have $A = 4 \in \mathbb{N}$. Beware that η divides δ_T, so (H) may hold. See Figure 5.*

- *On $\mathbb{F}_{11}$, $m = A$, $s < 0$, $\widetilde{s} = -1$,*

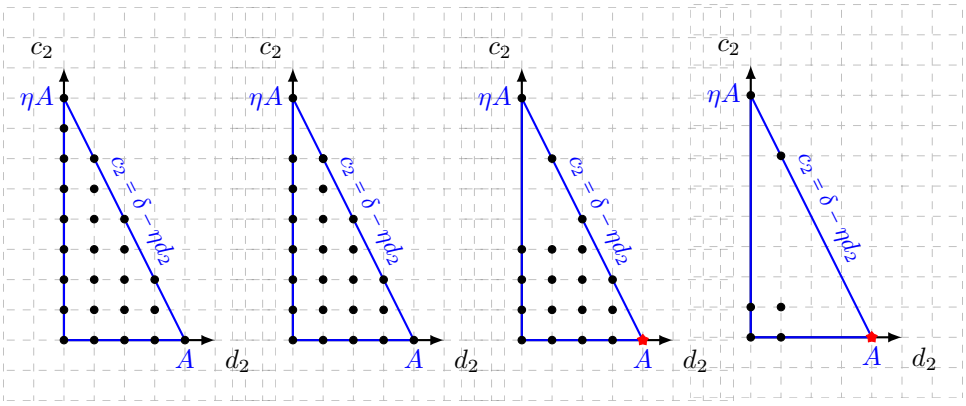
$$\dim C_2(-2,5) = (4+1)\left(-2+2\left(5-\frac{4}{2}\right)+1\right) = 25.$$

- *On $\mathbb{F}_7$, $m = A$, $s = \widetilde{s} = 0$,*

$$\dim C_2(-2,5) = (7+1)+4\left(-2+2\left(5-\frac{5}{2}\right)+1\right) = 8+16 = 24.$$

- *On $\mathbb{F}_4$, $m = 3$, $s = \widetilde{s} = 2$. Then (H) holds and*

$$\dim C_2(-2,5) = (4+1)(2+1)+\left(-2+2\left(5-\frac{6}{2}\right)+1\right) = 15+3 = 18.$$



(a) $\eta A \leq q = 11$ (b) $A < q = 7 \leq \eta A$ (c) $q = A = 4$ (d) $q = 2 \leq \frac{\eta}{\eta+1} A$

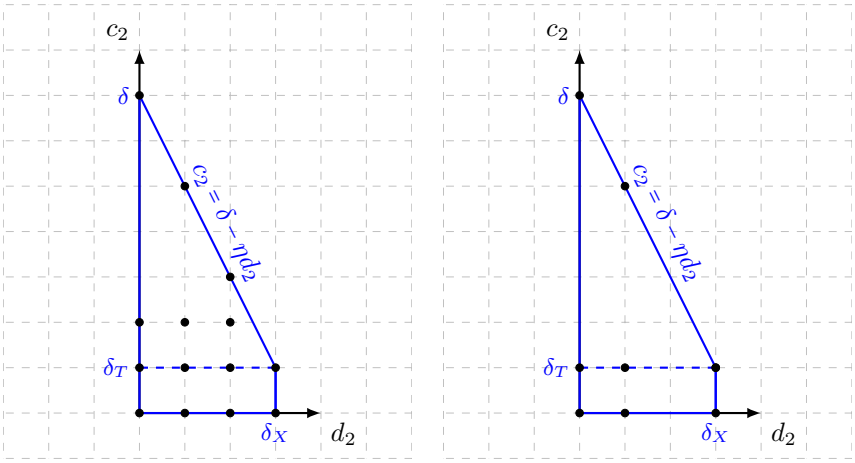
Figure 5: $\mathcal{P}(-2,5)$ in $\mathcal{H}_2$ for different values for q.

- *On* $\mathbb{F}_2$, $m = 1$, $s = \widetilde{s} = 1$. *Then (H) holds and*

$$\dim C_2(-2,5) = (2+1)(1+1) = 6.$$

Example 2.5.2. *To illustrate the cases* $q \leq \delta_X$, *let us compute the dimension of the code* $C_2(1,3)$ *using the previous formula on* $\mathbb{F}_3$ *and* $\mathbb{F}_2$. *See Figure 6.*

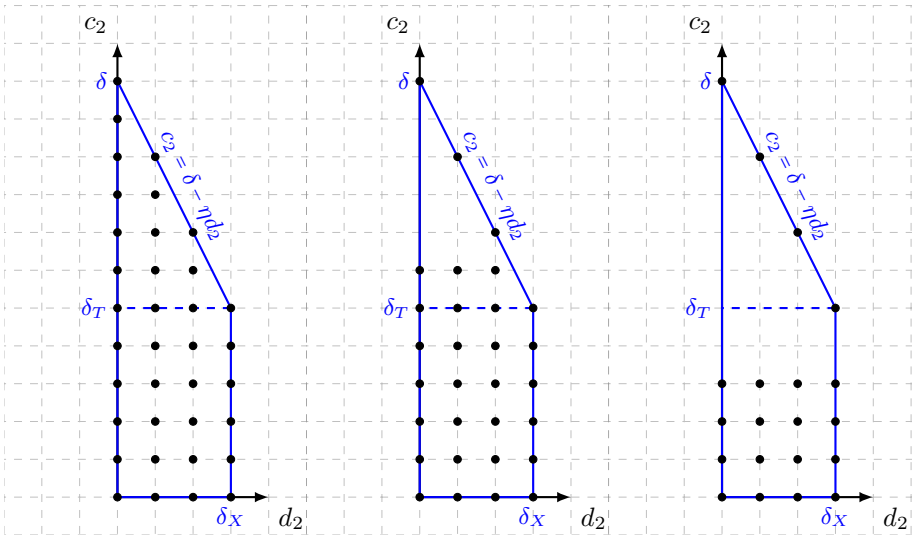
- *On* $\mathbb{F}_3$, $m = 2$, $s = \widetilde{s} = 2$, $h = 1$, $\dim C_2(1,3) = (3+1)(2+1) + 1 + 1 = 14$.
- *On* $\mathbb{F}_2$, $m = 1$, $s = 2.5 > m$, $\widetilde{s} = 1$, $h = 1$, $\dim C_2(-2,5) = (2+1)(1+1)+1+1 = 6+1 = 8$.



(a) $\frac{\delta}{\eta+1} < q = \delta_X = 3$ (b) $q = 2 \leq \frac{\delta}{\eta+1}$

Figure 6: $\mathcal{P}(1,3)$ in $\mathcal{H}_2$

Example 2.5.3. *On* $\mathcal{H}_2$, *let us compute the dimension of the code* $C_2(5,3)$ *on the finite fields* $\mathbb{F}_{13}$, $\mathbb{F}_7$ *and* $\mathbb{F}_4$. *See Figure 7. Since* $q > \delta_X$, *we have* $m = \delta_X = 3$.



(a) $\delta < q = 13$ (b) $\delta_T \leq q = 7 \leq \delta$ (c) $\delta_X < q = 4 < \delta_T$

Figure 7: $\mathcal{P}(5,3)$ in $\mathcal{H}_2$

- *On* $\mathbb{F}_{13}$, $s < 0$ *then* $\widetilde{s} = -1$.

$$\dim C_2(5,3) = (3+1)(5+3+1) = 36.$$

- *On* $\mathbb{F}_7$, $s = \widetilde{s} = 2$.

$$\dim C_2(5,3) = (7+1)(2+1) + (3-2)\left(5 + 2\left(3 - \frac{3+2+1}{2}\right) + 1\right) = 24+6 = 30.$$

- *On* $\mathbb{F}_4$, $s > m$ *then* $\widetilde{s} = m = 3$.

$$\dim C_2(5,3) = (4+1)(3+1) = 20.$$

3 Gröbner Basis

Our strategy to compute the dimension of the code highlights the key role of monomials in our study. Monomials remain crucial in the computation of the minimum distance, through the use of Gröbner bases. Until now, every technique we used has come from linear algebra, focusing on the finite dimensional vector spaces $R(\delta_T, \delta_X)$ and vector subspaces $\ker \mathrm{ev}_{(\delta_T,\delta_X)}$. However considering a convenient ideal of the ring R gives the possibility of using algebraic tools, Gröbner bases theory here, to handle the minimum distance problem.

Let us first recall classical facts about Gröbner bases. The reference for this section is [CLO15].

Let R be a polynomial ring. A *monomial order* is a total order on the monomials, denoted by $<$, satisfying the following compatibility property with multiplication: for all monomials M, N, P,

$$M < N \Rightarrow MP < NP \text{ and } M < MP.$$

For every polynomial $F \in R$, one can define the *leading monomial* of F, denoted by $\mathrm{LM}(F)$, to be the greatest monomial for this ordering that appears in F. The *leading term* of F is denoted by $\mathrm{LT}(F)$ and is defined as the leading monomial of F multiplied by its coefficient in F.

Let I be an ideal of the polynomial ring R, endowed with a monomial order $<$. The *monomial ideal* $\mathrm{LT}(I) \subset R$ associated to I is the ideal generated by the leading terms $\mathrm{LT}(F)$ of all polynomials $F \in I$. A finite subset G of an ideal I is a *Gröbner basis* of the ideal I if $\mathrm{LT}(I) = \langle \mathrm{LT}(g) \mid g \in G \rangle$.

The pleasing property of Gröbner bases (see [Stu96] Proposition 1.1) that will be used to compute the minimum distance of the code is the following.

Proposition 3.0.1. *Let I be an ideal of a polynomial ring R with Gröbner basis G. Then, setting π as the canonical projection of R onto ${}^{R}\!/_{I}$, the set*

$$\{\pi(M) \mid M \text{ monomials of } R \text{ such that for all } g \in G,\ \mathrm{LT}(g) \nmid M\}$$

is a basis of ${}^{R}\!/_{I}$ as a vector space.

Now that the necessary background is set up, let us define the ideal we shall use here.

Notation 3.0.2. Set $\mathcal{I} = \bigoplus_{(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}} \mathcal{I}(\delta_T, \delta_X)$.

Therefore, the ideal $\mathcal{I}$ is homogeneous : whenever it contains an element, it also contains all the homogeneous components of this element. This entails that $\mathcal{I}$ is the homogeneous vanishing ideal of the subvariety consisting of the $\mathbb{F}_q$-rational points of the Hirzebruch surface $\mathcal{H}_\eta$.

Another ingredient to benefit from Gröbner bases theory is a suitable monomial order over $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.

Definition 3.0.3. Let us define a order on monomials of R by stating that

$$T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_2^{d_2'} < T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$$

if and only if

$$d_1' + d_2' < d_1 + d_2 \text{ or } \left| \begin{array}{rl} d_1' + d_2' & = d_1 + d_2 \\ d_2' & < d_2 \end{array} \right. \text{ or } \left| \begin{array}{rl} d_1' & = d_1 \\ d_2' & = d_2 \\ c_2' & < c_2 \end{array} \right. \text{ or } \left| \begin{array}{rl} d_1' & = d_1 \\ d_2' & = d_2 \\ c_2' & = c_2 \\ c_1' & < c_1 \end{array} \right.$$

One can easily check that $<$ is a monomial order.

Remark 3.0.4. Notice that exchanging the role of d_1 and d_2 and the one of c_1 and c_2, we recover the monomial order chosen by Carvalho and Neumann [CN16].

The choice of this monomial order is motivated by the choice of representatives of monomials under $\equiv$, hence by the choice of the projection map $\pi_{(\delta_T, \delta_X)}$, as stated by the following lemma.

Lemma 3.0.5. *Any monomial $M \in \mathcal{M}(\delta_T, \delta_X)$ is greater than the leading term of its image under $\pi_{(\delta_T, \delta_X)}$.*

Proof. Since any $M \in \mathcal{M}(\delta_T, \delta_X)$ and its image under $\pi_{(\delta_T,\delta_X)}$ have the same bidegree, the first case of Definition 3.0.3 never occurs.

Except if (H) holds and $(d_2, c_2) = \left(\frac{\delta}{\eta}, 0\right)$, the image of a monomial $M(d_2, c_2) \in \mathcal{M}(\delta_T, \delta_X)$ under $\pi_{(\delta_T,\delta_X)}$ is the monomial $M(p_{(\delta_T,\delta_X)}(d_2, c_2))$, where $p_{(\delta_T,\delta_X)}$ is given in Definition 2.2.10.

Write $(d_2', c_2') = p_{(\delta_T,\delta_X)}(d_2, c_2)$. Then $d_2 \geq d_2'$. If $d_2 = d_2'$, then $c_2 \geq c_2'$, which means that $M \geq \pi_{(\delta_T,\delta_X)}(M)$.

It remains to check that it is also true for $M = M\left(\frac{\delta}{\eta}, 0\right)$ when (H) holds. In this case, according to Definition 2.3.2,

$$\pi_{(\delta_T,\delta_X)}\left(M\left(\frac{\delta}{\eta}, 0\right)\right) = M(r, 0) + M(r, \eta k(q-1)) - M(r, q-1).$$

with $r < \frac{\delta}{\eta}$. Then $\mathrm{LT}\left(\pi_{(\delta_T,\delta_X)}\left(M\left(\frac{\delta}{\eta}, 0\right)\right)\right) < M\left(\frac{\delta}{\eta}, 0\right)$, which concludes the proof. □

Notation 3.0.6. Let $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$. Let us set

$$\mathcal{G}(\delta_T, \delta_X) = \{M - \pi_{(\delta_T,\delta_X)}(M) \mid M \in \mathcal{M}(\delta_T, \delta_X) \setminus \Delta^\star(\delta_T, \delta_X)\}$$

and

$$\mathcal{G} = \bigcup_{(\delta_T,\delta_X)} \mathcal{G}(\delta_T, \delta_X).$$

Proposition 3.0.7. *There exists a finite subset $\mathcal{G}'$ of $\mathcal{G}$ that forms a Gröbner basis of the ideal $\mathcal{I}$.*

Proof. First, let us prove that the leading term of any polynomial of $\mathcal{I}$ is divisible by the leading term of an element of $\mathcal{G}$.

Fix $f \in \mathcal{I}$. We write $f_{(\delta_T,\delta_X)}$ the homogeneous component of f that has bidegree (δ_T, δ_X). The leading term of f is the leading term of one of its homogeneous component. Therefore, it is enough to prove that the leading term of any $f_{(\delta_T,\delta_X)}$ is divisible by the leading term of an element of $\mathcal{G}$.

By Proposition 2.3.6, the map $\pi_{(\delta_T,\delta_X)}$ is a projection along $\mathcal{I}(\delta_T, \delta_X)$ onto $\mathrm{Span}\,\Delta^*(\delta_T, \delta_X)$. Hence $\ker \pi_{(\delta_T,\delta_X)} = \mathcal{I}(\delta_T, \delta_X) = \mathrm{range}(\mathrm{Id} - \pi_{(\delta_T,\delta_X)})$. The set $\mathcal{G}(\delta_T, \delta_X)$ is thus a spanning family for the vector space $\mathcal{I}(\delta_T, \delta_X)$. Therefore any $f_{(\delta_T,\delta_X)}$ can be written as a linear combination of elements of $\mathcal{G}(\delta_T, \delta_X)$:

$$f_{(\delta_T,\delta_X)} = \sum_{\substack{M \in \mathcal{M}(\delta_T,\delta_X) \\ M \notin \Delta^\star(\delta_T,\delta_X)}} c_M \left(M - \pi_{(\delta_T,\delta_X)}(M)\right)$$

By Lemma 3.0.5, the leading monomial of $f_{(\delta_T,\delta_X)}$ is the maximum monomial M_{max} with respect to the monomial order $<$ among the monomials M in $\mathcal{M}(\delta_T, \delta_X) \setminus \Delta^\star(\delta_T, \delta_X)$ such that $c_M \neq 0$. It is thus clear that the leading term of f is divisible by the leading term of $M_{max} - \pi_{(\delta_T,\delta_X)}(M_{max})$, that belongs to $\mathcal{G}$.

To conclude, it is enough to apply Dickson's Lemma ([CLO15] §4 Theorem 4) to the monomial ideal $\mathrm{LT}(\mathcal{I})$. □

Let us highlight that the homogeneity of the ideal $\mathcal{I}$ gives a natural graduation of the quotient

$$R/I = \bigoplus_{(\delta_T,\delta_X)} \left(R(\delta_T,\delta_X)/\mathcal{I}(\delta_T,\delta_X) \right),$$

from which, with Propositions 3.0.1 and 3.0.7, the next corollary arises.

Corollary 3.0.8. *Let $(\delta_T,\delta_X) \in \mathbb{Z}\times\mathbb{N}$ such that $\delta \geq 0$. A basis of a complement space of $\mathcal{I}(\delta_T,\delta_X)$ in $R(\delta_T,\delta_X)$ is the set $\{M \in \mathcal{M}(\delta_T,\delta_X) | \forall g \in \mathcal{G}', \mathrm{LT}(g) \nmid M\}$.*

Proof. By Propositions 3.0.7 and 3.0.1, the set

$$\mathcal{B} = \left\{ M \in \bigcup_{(\delta_T,\delta_X)\in\mathbb{Z}\times\mathbb{N}} \mathcal{M}(\delta_T,\delta_X) \mid \forall\, g \in \mathcal{G}',\, \mathrm{LT}(g) \nmid M \right\}$$

is a basis of a complementary of $\mathcal{I}$, seen as $\mathbb{F}_q$-vector subspace of R. Every element of $\mathcal{B}$ is homogeneous. The result follows by restricting on a homogeneous component. □

In Proposition 2.3.6 we displayed $\Delta^*(\delta_T,\delta_X)$ as a basis of $R(\delta_T,\delta_X)$ modulo the subspace $\mathcal{I}(\delta_T,\delta_X)$ for each couple (δ_T,δ_X). Actually the image under the canonical projection of the union of the $\Delta^*(\delta_T,\delta_X)$ is exactly the basis given by the previous proposition, as stated in the following lemma.

Lemma 3.0.9. *Let us set $\Delta^* = \bigcup_{(\delta_T,\delta_X)} \Delta^*(\delta_T,\delta_X)$. Then Δ^* is the set of monomials of R that are not divisible by the leading term of any polynomial of $\mathcal{G}$.*

Proof. Fix $(\alpha,\beta) \in \mathcal{K}^*(\delta_T,\delta_X)$ and $M = M(\alpha,\beta) \in \Delta^*(\delta_T,\delta_X)$.

Let $G = N - \pi_{(\epsilon_T,\epsilon_X)}(N) \in \mathcal{G}(\epsilon_T,\epsilon_X)$ with

$$N = T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \in \mathcal{M}(\epsilon_T,\epsilon_X) \setminus \Delta^*(\epsilon_T,\epsilon_X).$$

By Lemma 3.0.5, $\mathrm{LT}(G) = N$.

Assume that N divides M, that is to say

$$d_2 \leq \alpha \tag{i}$$
$$d_1 = \epsilon_X - d_2 \leq \delta_X - \alpha \tag{ii}$$
$$c_2 \leq \beta \tag{iii}$$
$$c_1 = \epsilon_T + \eta(\epsilon_X - d_2) - c_2 \leq \delta - \eta\alpha - \beta \tag{iv}$$

We want to reach a contradiction.

First suppose that $\pi_{(\epsilon_T,\epsilon_X)}(N) = T_1^{c_1'}T_2^{c_2'}X_1^{d_1'}X_2^{d_2'}$ is a monomial. By Lemma 2.2.5, since $N \equiv \pi_{(\epsilon_T,\epsilon_X)}(N)$, there exist $k,\, l \in \mathbb{Z}$ such that

$$d_2 = d_2' + k(q-1),\ d_1 = d_1' - k(q-1),\ c_2 = c_2' + l(q-1) \text{ and } c_1 = c_1' - (l+\eta k)(q-1).$$

Since $\mathrm{LT}(G) = N$, either $d_2' > d_2$ or $d_2' = d_2$ and $c_2' > c_2$, i.e either $k \in \mathbb{N}^*$ or $k = 0$ and $l \in \mathbb{N}^*$.

- Let first assume that $k \in \mathbb{N}^*$. By condition (C1) for $i = 2$, this implies that $d_2' \geq 1$ and then $d_2 \geq q$. By (i), the only possible value for α is thus $\alpha = A$ if $A \geq q$.

  - If $\delta_T \geq 0$, then $\alpha = A = \delta_X$ and then, by (ii), $d_1 = 0$. By condition (C3) for $i = 1$, $d'_1 = 0$, which implies $k = 0$ and leads to a contradiction.
  - If $\delta_T < 0$, there is no integer $\alpha \geq q$ such that there exists $\beta \in \mathbb{N}$ satisfying $(\alpha, \beta) \in \mathcal{K}^*(\delta_T, \delta_X)$. This case never occurs.

- Now, let us assume that $k = 0$ and $l \in \mathbb{N}^*$, which implies $c_2 \geq q$. Since $c_2 \leq \beta$, by Notation 2.2.8, $\beta = \delta_T + \eta(\delta_X - \alpha)$. Then $c_1 = 0$ hence $c'_1 = 0$, which contradicts the hypothesis $l \neq 0$.

Now assume that (ϵ_T, ϵ_X) satisfies (H) and $N = X_1^{d_1} X_2^{d_2}$ with $d_1 = -\frac{\epsilon_T}{\eta} \neq 0$ and $d_2 = \epsilon_X + \frac{\epsilon_T}{\eta} \geq q$. As before, by (i), α can only be equal to A if $A \geq q$, which happens only if $\delta_T \geq 0$ and $A = \delta_X$. The same reasoning as previously leads to a contradiction.

We then have proved that Δ^* is a subset of the set of monomials non divisible by the leading term of any polynomial in $\mathcal{G}$. But these two sets are basis of two complementary spaces of a same vector space by Proposition 2.3.6 and Corollary 3.0.8. Therefore, these two sets coincide. □

4 Minimum distance of $C_\eta(\delta_T, \delta_X)$

4.1 Proof of the the lower bound of the minimum distance in Theorem B

Let us fix $(\epsilon_T, \epsilon_X) \in \mathbb{N}^2$ such that $\epsilon_T,\ \epsilon_X \geq q$.

Notation 4.1.1. Let us set

$$\Delta^*(\epsilon_T, \epsilon_X)_F = \{N \in \Delta^*(\epsilon_T, \epsilon_X) \mid \mathrm{LT}(F) \mid N\}$$

with $\Delta^*(\epsilon_T, \epsilon_X)$ defined in Notations 2.2.8 and 2.3.4.

Let $F \in R(\delta_T, \delta_X) \setminus \ker \mathrm{ev}_{(\delta_T, \delta_X)}$ and $\mathcal{Z}(F)$ its zero set in $\mathcal{H}_\eta$. We define

$$N_F = \#\mathcal{Z}(F)(\mathbb{F}_q).$$

We prove now the lower bound

$$d_\eta(\delta_T, \delta_X) \geq \min_{M \in \Delta^*(\delta_T, \delta_X)} \#\Delta^*(\epsilon_T, \epsilon_X)_M.$$

Proof of the lower bound. Recall that the minimum distance is defined by

$$d_\eta(\delta_T, \delta_X) = \min_{\substack{F \in R(\delta_T, \delta_X) \\ F \notin \ker \mathrm{ev}_{(\delta_T, \delta_X)}}} \omega(\mathrm{ev}_{(\delta_T, \delta_X)}(F)).$$

First, Proposition 2.3.6 gives $\mathrm{ev}_{(\delta_T, \delta_X)}(F) = \mathrm{ev}_{(\delta_T, \delta_X)}\left(\pi_{(\delta_T, \delta_X)}(F)\right)$ and then

$$d_\eta(\delta_T, \delta_X) = \min_{F \in \mathrm{Span}\, \Delta^*(\delta_T, \delta_X)} \omega(\mathrm{ev}_{(\delta_T, \delta_X)}(F)) = \min_{F \in \mathrm{Span}\, \Delta^*(\delta_T, \delta_X)} N - N_F,$$

so that we aim to bound from below $N - N_F$ uniformly in $F \in \mathrm{Span}\, \Delta^*(\delta_T, \delta_X)$.

Let us fix such a polynomial $F \in \operatorname{Span}\Delta^*(\delta_T, \delta_X)$.

Second, we aim to regard N_F as the dimension of some vector space. For this purpose, fix $(\epsilon_T, \epsilon_X) \in \mathbb{Z} \times \mathbb{N}$ and consider the map

$$\mathrm{ev}_{(\epsilon_T,\epsilon_X),F} : \begin{cases} R(\epsilon_T,\epsilon_X) & \to & \mathbb{F}_q^{N_F} \\ G & \mapsto & (G(Q))_{Q \in \mathcal{Z}(F)(\mathbb{F}_q)} \end{cases}.$$

For ϵ_T, $\epsilon_X \geq q$ the evaluation map $\mathrm{ev}_{(\epsilon_T,\epsilon_X)}$ is surjective by Example 2.3.8. The map $\mathrm{ev}_{(\epsilon_T,\epsilon_X),F}$ is thus also surjective for any $F \in R(\delta_T, \delta_X)$, as illustrated by the diagram

$$R(\epsilon_T,\epsilon_X) \xrightarrow[\mathrm{ev}_{(\epsilon_T,\epsilon_X)}]{} \mathbb{F}_q^{\mathcal{H}_\eta(\mathbb{F}_q)} \longrightarrow \mathbb{F}_q^{\mathcal{Z}(F)(\mathbb{F}_q)}, \qquad R(\epsilon_T,\epsilon_X) \xrightarrow{\mathrm{ev}_{(\epsilon_T,\epsilon_X),F}} \mathbb{F}_q^{\mathcal{Z}(F)(\mathbb{F}_q)}.$$

It follows that

$$N_F = \dim\left(R(\epsilon_T,\epsilon_X) \big/ \ker \mathrm{ev}_{(\epsilon_T,\epsilon_X),F}\right).$$

Third we aim to display an upper bound $\widetilde{N}_F$ of N_F such that $N - \widetilde{N}_F$ turns to be easier to handle. Let us denote by $\langle F \rangle$ the ideal of R generated by F and by $\langle F \rangle_{(\epsilon_T,\epsilon_X)}$ the subspace $FR(\epsilon_T - \delta_T, \epsilon_X - \delta_X) \subset R(\epsilon_T, \epsilon_X)$ spanned by F.

Observing that $\ker \mathrm{ev}_{(\epsilon_T,\epsilon_X)} + \langle F \rangle_{(\epsilon_T,\epsilon_X)} \subset \ker \mathrm{ev}_{(\epsilon_T,\epsilon_X),F}$, we get $\widetilde{N}_F \geq N_F$ with

$$\widetilde{N}_F = \dim\left(R(\epsilon_T,\epsilon_X) \big/ \ker \mathrm{ev}_{(\epsilon_T,\epsilon_X)} + \langle F \rangle_{(\epsilon_T,\epsilon_X)}\right).$$

Hence

$$d_\eta(\delta_T, \delta_X) \geq \min_{F \in \operatorname{Span}\Delta^*(\delta_T,\delta_X)} N - \widetilde{N}_F \tag{11}$$

and we are now reduced to bound from below $N - \widetilde{N}_F$ uniformly in $F \in \operatorname{Span}\Delta^*(\delta_T, \delta_X)$.

Fourth, we now prove that

$$N - \widetilde{N}_F \geq \#\Delta^*(\epsilon_T, \epsilon_X)_F. \tag{12}$$

In fact, we display $\Delta^*(\epsilon_T, \epsilon_X)_F$ as a subfamily of $\Delta^*(\epsilon_T, \epsilon_X)$ whose complement would be a spanning family of the vector space $R(\epsilon_T, \epsilon_X)$ modulo the vector subspace $\ker \mathrm{ev}_{(\epsilon_T,\epsilon_X)} + \langle F \rangle_{(\epsilon_T,\epsilon_X)}$.

By Corollary 3.0.8 and Lemma 3.0.9,

$$\Delta^*(\epsilon_T, \epsilon_X) = \{M,\ M \in \mathcal{M}(\epsilon_T, \epsilon_X) \text{ such that } \forall\, g \in \mathcal{G},\ LT(g) \nmid M\}$$

is a basis of $R(\epsilon_T, \epsilon_X)$ modulo $\mathcal{I}(\epsilon_T, \epsilon_X)$. By Example 2.3.8, its cardinality equals N.

As F is a homogeneous element, the ideal $\mathcal{I} + \langle F \rangle$ is homogeneous. Let $\widehat{\mathcal{G}}$ be a Gröbner basis of the ideal $\mathcal{I} + \langle F \rangle$ that contains $\mathcal{G} \cup \{F\}$. Using Proposition 3.0.1 and restricting on each homogeneous component as in Corollary 3.0.8, the set

$$\widetilde{\Delta}(\epsilon_T, \epsilon_X) = \{M,\ M \in \mathcal{M}(\epsilon_T, \epsilon_X) \text{ such that } \forall\, h \in \widehat{\mathcal{G}},\ LT(h) \nmid M\}$$

is a basis of $R(\epsilon_T, \epsilon_X)$ modulo $\mathcal{I}(\epsilon_T, \epsilon_X) + \langle F \rangle_{(\epsilon_T, \epsilon_X)}$ of cardinality $\widetilde{N}_F$.

Since $\mathcal{G} \subset \widehat{\mathcal{G}}$ and $F \in \widehat{\mathcal{G}}$, we have $\Delta^*(\epsilon_T, \epsilon_X)_F \subset \Delta^*(\epsilon_T, \epsilon_X) \setminus \widetilde{\Delta}(\epsilon_T, \epsilon_X)$, from which (12) follows.

We conclude the proof noticing that $\Delta^*(\epsilon_T, \epsilon_X)_F = \Delta^*(\epsilon_T, \epsilon_X)_{\mathrm{LT}(F)}$ for every polynomial F and using (11) and (12). □

4.2 Explicit formulae of the minimum distance

The previous paragraph gives a lower bound of the minimum distance for any couple $(\epsilon_T, \epsilon_X) \in \mathbb{N}^2$ such ϵ_T, $\epsilon_X \geq q$. We aim to maximize the quantity depending on this couple. **From now, we set**

$$\epsilon_X = q + \delta_X \text{ and } \epsilon_T = q + \delta$$

where as usual $\delta = \delta_T + \eta\delta_X$. The hypotheses for $R(\delta_T, \delta_X)$ not to be zero imply that ϵ_T and ϵ_X are greater than q. By Theorem B, one way to compute a lower bound of the minimum distance is to calculate $\#\Delta^*(\epsilon_T, \epsilon_X)_M$ for every monomial $M \in \Delta^*(\delta_T, \delta_X)$ and then minimize the quantity over $\Delta^*(\delta_T, \delta_X)$.

Proposition 4.2.1. *Let $(\alpha_0, \beta_0) \in \mathcal{K}^*(\delta_T, \delta_X)$, defined in Notations 2.2.8 and 2.3.4. Then*

$$\#\Delta(\epsilon_T, \epsilon_X)_{M(\alpha_0,\beta_0)} = \max(q - \alpha_0 + \mathbb{1}_{\{\alpha_0 = \delta_X\}}, 1) \max(q - B(\alpha_0) + \mathbb{1}_{\{\beta_0 = B(\alpha_0)\}}, 1)$$

with $B(\alpha_0) = \delta - \eta\alpha_0$.

Proof. Set $M = M(\alpha_0, \beta_0) = T_1^{\delta - \eta\alpha_0 - \beta_0} T_2^{\beta_0} X_1^{\delta_X - \alpha_0} X_2^{\alpha_0}$ with $(\alpha_0, \beta_0) \in \mathcal{K}^*(\delta_T, \delta_X)$, that is to say according to Notations 2.2.8 and 2.3.4

$$\begin{array}{rcl} 0 \leq \alpha_0 \leq \min(\lfloor A \rfloor, q-1) & \text{or} & (\alpha_0 = \delta_X \text{ if } \delta_T \geq 0), \\ 0 \leq \beta_0 \leq \min(\delta - \eta\alpha_0, q) - 1 & \text{or} & \beta_0 = \delta_T + \eta(\delta_X - \alpha_0). \end{array}$$

Let $N \in \Delta^*(\epsilon_T, \epsilon_X)$. Write

$$N = T_1^{\epsilon_T + \eta(\epsilon_X - \alpha) - \beta} T_2^{\beta} X_1^{\epsilon_X - \alpha} X_2^{\alpha}$$

with $(\alpha, \beta) \in \mathcal{K}^*(\epsilon_T, \epsilon_X)$. Since ϵ_T, $\epsilon_X \geq q$, then

$$\begin{array}{rcl} 0 \leq \alpha \leq q-1 & \text{or} & \alpha = \epsilon_X, \\ 0 \leq \beta \leq q-1 & \text{or} & \beta = \epsilon_T + \eta(\epsilon_X - \alpha). \end{array}$$

Suppose that M divides N. Then

$$\begin{array}{c} \alpha_0 \leq \alpha \\ \delta_X - \alpha_0 \leq \epsilon_X - \alpha \\ \beta_0 \leq \beta \\ \delta - \eta\alpha_0 - \beta_0 \leq \epsilon_T + \eta(\epsilon_X - \alpha) - \beta \end{array}$$

One can rewrite the previous conditions as

$$\alpha_0 \leq \alpha \leq q + \alpha_0 \quad \text{and} \quad \beta_0 \leq \beta \leq q + \eta(\epsilon_X - \alpha + \alpha_0) + \beta_0.$$

Since $\alpha \leq \epsilon_X$ and $\alpha_0, \beta_0 \in \mathbb{N}$, both upperbounds are greater than $q-1$. Moreover,

$$\begin{aligned} q + \alpha_0 = \epsilon_X &\Leftrightarrow \alpha_0 = \delta_X, \\ q + \eta(\epsilon_X - \alpha + \alpha_0) + \beta_0 = \epsilon_T + \eta(\epsilon_X - \alpha) &\Leftrightarrow \beta_0 = B(\alpha_0), \end{aligned}$$

which justifies the choice of ϵ_T and ϵ_X to maximize the quantity $\#\Delta^*(\epsilon_T, \epsilon_X)_{(M(\alpha_0,\beta_0)}$.

To sum up, determining $\#\Delta^*(\epsilon_T, \epsilon_X)_M$ is equivalent to compute the number of couples $(\alpha, \beta) \in \mathcal{K}^*(\epsilon_T, \epsilon_X)$ satisfying the following conditions.

$$\begin{cases} \alpha_0 \leq \alpha \leq q-1 \quad \text{or} \quad \{\alpha = \epsilon_X \text{ and } \alpha_0 = \delta_X\} \\ \beta_0 \leq \beta \leq q-1 \quad \text{or} \quad \{\beta = \epsilon_T + \eta(\epsilon_X - \alpha) \text{ and } \beta_0 = B(\alpha_0)\} \end{cases} \tag{$\star$}$$

Moreover,

- If $\delta_X \geq q$ and $\alpha_0 = \delta_X$, the only α that satifies $(\star)$ is $\alpha = \epsilon_X$.
- If $\delta_T + \eta\delta_T \geq q$ and $\beta_0 = \delta_T + \eta\delta_T$, the only β satifying $(\star)$ is $\beta = \epsilon_T + \eta\epsilon_X$.

Then, one can write

$$\#\Delta(\epsilon_T, \epsilon_X)_M = \begin{cases} (q-\alpha_0)(q-\beta_0) & \text{if } \alpha_0 < \delta_X \text{ and } \beta_0 < B(\alpha_0), \\ (q-\alpha_0)\max(q-B(\alpha_0)+1, 1) & \text{if } \alpha_0 < \delta_X \text{ and } \beta_0 = B(\alpha_0), \\ \max(q-\delta_X+1, 1)(q-\beta_0) & \text{if } \alpha_0 = \delta_X \text{ and } \beta_0 < B(\alpha_0), \\ \max(q-\delta_X+1, 1)\max(q-B(\alpha_0)+1, 1) & \text{if } \alpha_0 = \delta_X \text{ and } \beta_0 = B(\alpha_0). \end{cases}$$

Let us highlight that a couple $(\alpha_0, \beta_0) \in \mathcal{K}^*(\delta_T, \delta_X)$ is less than or equal to $q-1$ or equal to δ_X. Then either (α_0, β_0) or $(\alpha_0, \epsilon_T + \eta(\epsilon_X - \alpha_0))$ satisfies $(\star)$. Then the quantity $\#\Delta^*(\epsilon_T, \epsilon_X)_{M(\alpha_0,\beta_0)}$ can never be zero. □

To lowerbound the minimum distance, it remains to minimize

$$\max(q - \alpha_0 + \mathbb{1}_{\{\alpha_0=\delta_X\}}, 1)\max(q - \beta_0 + \mathbb{1}_{\{\beta_0=B(\alpha_0)\}}, 1)$$

over $(\alpha_0, \beta_0) \in \mathcal{K}^*(\delta_T, \delta_X)$. The problem can be reduced to minimize a univariate function, thanks to the following lemma.

Lemma 4.2.2. *Let $\eta \geq 0$ and $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ such that $\delta \geq 0$. Then*

$$d_\eta(\delta_T, \delta_X) \geq \min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0)$$

with

$$\mathcal{A}_X^* = \begin{cases} [\![0, \max(q, \delta_X) - 1]\!] \cup \{\delta_X\} & \text{if } \delta_T \geq 0, \\ \left[\!\left[0, \max\left(q-1, \left\lfloor \frac{\delta}{\eta} \right\rfloor\right)\right]\!\right] & \text{if } \delta_T < 0 \end{cases}$$

and

$$f(\alpha_0) = \max(q - \alpha_0 + \mathbb{1}_{\alpha_0=\delta_X}, 1)\max(q - \delta + \eta\alpha_0 + 1, 1)$$

Proof. By Theorem B, we have to minimize $\#\Delta^*(\delta_T, \delta_X)_{M_{(\alpha_0,\beta_0)}}$ for $(\alpha_0, \beta_0) \in \mathcal{K}^*(\delta_T, \delta_X)$. The only observation we need to prove this lemma is that for each $\alpha_0 \in \mathcal{A}_X^*$, for all $\beta \in [\![0, \min(B(\alpha_0), q) - 1]\!]$,

$$q - \beta_0 \geq q - B(\alpha_0) + 1.$$

Substituting in the formula of Proposition 4.2.1 gives the desired conclusion. □

In other words, Lemma 4.2.2 means that the minimum is reached by monomials of the form $M(\alpha_0, \delta - \eta\alpha_0)$ for $\alpha_0 \in \mathcal{A}_X^*$.

Proposition 4.2.3. *Let $\eta \geq 0$, $(\delta_T, \delta_X) \in \mathbb{Z}\times\mathbb{N}$ with $\delta \geq 0$. The code $C_\eta(\delta_T, \delta_X)$ on the Hirzebruch surface $\mathcal{H}_\eta$ has minimum distance that is given as follows:*

- *If $\eta \geq 2$,*
  - *If $q > \delta$, then*
$$d_\eta(\delta_T, \delta_X) = (q + \mathbb{1}_{\delta_X=0})(q - \delta + 1),$$
  - *If $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, then*
$$d_\eta(\delta_T, \delta_X) = q - \left\lfloor \frac{\delta - q}{\eta} \right\rfloor,$$
  - *If $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$,*
$$d_\eta(\delta_T, \delta_X) = \begin{cases} \max(q - \delta_X + 1, 1) & \text{if } \delta_T \geq 0, \\ 1 & \text{if } \delta_T < 0, \end{cases}$$
- *if $\eta = 0$,*
$$d_\eta(\delta_T, \delta_X) = \max(q - \delta_X + 1, 1)\max(q - \delta_T + 1, 1).$$

First we show that the mentioned values for the minimum distance provide lower bounds. Equality will follow from Proposition 3, exhibiting polynomials associated to words of minimum weight.

Proof. By Lemma 4.2.2, we aim to prove the lower bound by minimizing the function f on $\mathcal{A}_X^*$, the function and the set depending on parameters η, δ_T, δ_X and q.

Let us highlight that $\mathcal{A}_X^* \subset [0, \delta_X]$ regardless of parameters.

The form of the function f as a product of two maxima of a linear function with 1 implies that the real function $f : [0, \delta_X] \to \mathbb{R}$ is a concave piecewise function. The pieces depend on the size of q with respect to the parameters.

More precisely, note that

$$q - \delta + \eta\alpha_0 + 1 \leq 1 \Leftrightarrow \alpha_0 \leq s$$

where $s = \dfrac{\delta - q}{\eta}$ has already been defined in Section 2.4.

Then f is a piecewise function that has a decreasing linear polynomial on the interval $[0, s]$ and a concave quadratic function on the interval $[s, \delta_X[$ with negative dominant coefficient, provided that $s \in [0, \delta_X[$.

If $s \leq 0$, then the function f is quadratic and concave on $[0, \delta_X[$. Finally, if $s \geq \delta_X$, then f is decreasing on $[0, \delta_X[$.

Then the minimum point of f on $\mathcal{A}_X^*$ is the floor or the ceiling of one the bound of these intervals.

Let us first suppose that $\eta \geq 2$ and $\delta_T \geq 0$. Then

$$\mathcal{A}_X^* = \begin{cases} [\![0, \delta_X]\!] & \text{if } \delta_X \leq q \\ [\![0, q-1]\!] \cup \{\delta_X\} & \text{if } \delta_X \geq q \end{cases}$$

1. If $\delta < q$, then $s < 0$ and $q > \delta_X$. In this case

$$f(\alpha_0) = \begin{cases} (q-\alpha_0)(q-\delta+\eta\alpha_0+1) & \text{if } \alpha_0 \neq \delta_X, \\ (q-\delta_X+1)(q-\delta_T+1) & \text{if } \alpha_0 = \delta_X. \end{cases}$$

- If $\delta_X = 0$, then $\mathcal{A}_X^* = \{0\}$ and

$$\min_{\alpha_0 \in \mathcal{A}_X} f(\alpha_0) = f(\delta_X) = (q+1)(q-\delta_T+1).$$

- Otherwise, on the interval $[0, \delta_X - 1]$, the minimum is reached by one of the bounds of the interval, i.e. $\alpha_0 = 0$ or $\alpha_0 = \delta_X - 1$ (see Fig. 8).

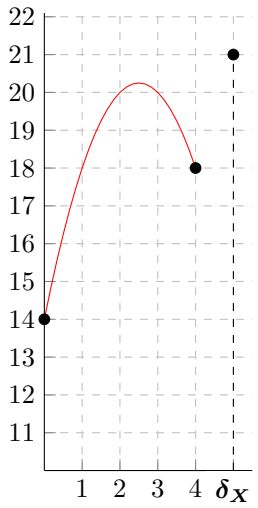


Figure 8: Graph of f when $q > \delta$
e.g. $(\eta, \delta_T, \delta_X, q) = (1, 1, 5, 7)$

In addition, one can notice that $f(\delta_X) = f(\delta_X - 1) + \eta(q - \delta_X - 1)$. Then

$$f(\delta_X) > f(\delta_X - 1).$$

The minimum of the function f on $\mathcal{A}_X^*$ is reached either by $\alpha_0 = 0$ or $\alpha_0 = \delta_X - 1$. It remains to compare both values.
We have $f(0) \leq f(\delta_X - 1)$ if and only if

$$q\eta\delta_X \geq (\delta_X - 1)(q - \delta_T - \eta + 1) + \eta q$$

which is equivalent to

$$q(\delta_X - 1)(\eta - 1) \geq -(\delta_X - 1)(\delta_T + \eta - 1) \tag{13}$$

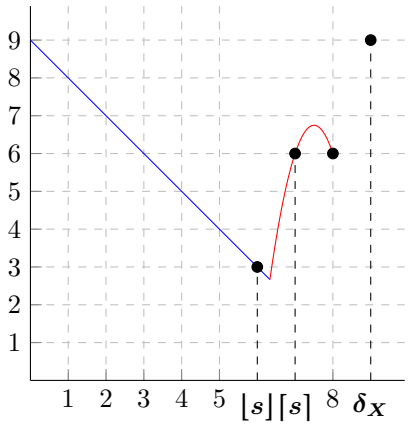
Since $\eta \geq 2$, $\delta_T \geq 0$, $\delta_X \geq 1$ and $q \geq 2$, the left hand side is non negative, whereas the the right hand side is non positive. The inequality (13) is thus always satisfied and

$$\min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0) = f(0) = q(q - \delta + 1)$$

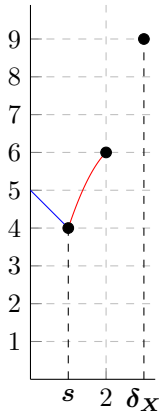
2. If $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, then $\delta_X \geq 1$ and $\lfloor s \rfloor \in [\![0, \min(\delta_X, q) - 1]\!]$. In this case

$$f(\alpha_0) = \begin{cases} (q-\alpha_0) & \text{if } \alpha_0 \leq s, \\ (q-\alpha_0)(\eta(\alpha_0 - s)+1) & \text{if } \alpha_0 \neq \delta_X \text{ and } \alpha_0 \geq s, \\ \max(q-\delta_X+1,1)(q-\delta_T+1) & \text{if } \alpha_0 = \delta_X. \end{cases}$$

See Figure 9 for examples of graph of the function f.



(a) $\delta_X \geq q$
e.g. $(\eta, \delta_T, \delta_X, q) = (3, 1, 9, 9)$



(b) $\delta_X < q$
e.g. $(\eta, \delta_T, \delta_X, q) = (1, 3, 3, 5)$

Figure 9: Examples of graph of the function f when $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$

The possible arguments for the minimum are $\lfloor s \rfloor$, $\lfloor s \rfloor + 1$, $\min(q, \delta_X) - 1$ and δ_X.

First notice that $\lfloor s \rfloor \leq q - 1$ and

$$\begin{aligned} f(\lfloor s \rfloor + 1) &= (q - \lfloor s \rfloor - 1)(\eta(\lfloor s \rfloor + 1 - s) + 1 \\ &= f(\lfloor s \rfloor) - 1 + (q - \lfloor s \rfloor)\eta(\lfloor s \rfloor + 1 - s). \end{aligned}$$

Therefore

$$f(\lfloor s \rfloor + 1) \geq f(\lfloor s \rfloor). \tag{14}$$

Second let us check that the minimum of f cannot be reached by $\alpha_0 = \delta_X$.

- If $\delta_X \leq q$, then $f(\delta_X) = f(\delta_X - 1) + \eta(q - \delta_X - 1)$ and $f(\delta_X) > f(\delta_X - 1)$.
- If $\delta_X \geq q$, then $f(\delta_X) = \eta(\delta_X - s) + 1 \geq \eta(q - 1 - s) + 1 = f(q-1)$.

Then the minimum of f is reached by either $\alpha_0 = \lfloor s \rfloor$ or $\alpha_0 = \min(\delta_X, q) - 1$.

- If $\delta_X \geq q$, we want to prove that $f(\lfloor s \rfloor) \leq f(q-1)$.

$$\begin{aligned} f(q-1) &= \eta(q - s - 1) + 1 \\ &\geq \eta(q - \lfloor s \rfloor - 1) + 1 \\ &\geq q - \lfloor s \rfloor + (\eta - 1)(q - \lfloor s \rfloor - 1) \quad \text{since } \lfloor s \rfloor \leq q - 1 \\ &\geq q - \lfloor s \rfloor = f(\lfloor s \rfloor) \end{aligned}$$

- If If $\delta_X \leq q$, we want to prove that $f(\lfloor s \rfloor) \leq f(\delta_X - 1)$.
  Let us assume $\lfloor s \rfloor \neq \delta_X - 1$ and $f(\lfloor s \rfloor) > f(\delta_X - 1)$ and let us display a contradiction.

  $$f(\lfloor s \rfloor) > f(\delta_X - 1) \Leftrightarrow \lfloor s \rfloor < \delta_X - 1 - \eta(\delta_X - 1 - s)(q - \delta_X + 1)$$

  Since the right hand side is an integer, we have

  $$f(\lfloor s \rfloor) > f(\delta_X - 1) \Rightarrow s < \delta_X - 1 - \eta(\delta_X - 1 - s)(q - \delta_X + 1)$$

  Replacing s by its value, we get

  $$\frac{\delta_T}{\eta} < -1 - \eta(\delta_X - 1 - s)(q - \delta_X + 1)$$

  But the assumption $\lfloor s \rfloor \neq \delta_X - 1$ ensures that $\delta_X - 1 > s$ and then $\eta(\delta_X - 1 - s)(q - \delta_X + 1) \geq 0$. The right handside being negative, it is a contradiction with $\delta_T \geq 0$.

Then, in both cases,

$$\min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0) = f(\lfloor s \rfloor) = q - \lfloor s \rfloor$$

3. if $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$, then $s \geq \min(\delta_X, q)$ and

   $$f(\alpha_0) = \max(q - \alpha_0 + \mathbb{1}_{\alpha_0 = \delta_X}, 1).$$

   This is a decreasing function on $[0, \delta_X]$, as $f(\delta_X - 1) = f(\delta_X)$. It follows easily that

   $$\min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0) = f(\delta_X) = \begin{cases} 1 & \text{if } q < \delta_X, \\ q - \delta_X + 1 & \text{if } q \geq \delta_X. \end{cases}$$

Now, let us focus on the case $\eta \geq 2$ and $\delta_T < 0$. Let us recall that $A = \frac{\delta}{\eta} < \delta_X$ does not belong to $\mathcal{A}_X^*$ if $A \geq q$ and

$$\mathcal{A}_X^* = \begin{cases} [\![0, \lfloor A \rfloor]\!] & \text{if } A < q, \\ [\![0, q-1]\!] & \text{if } A \geq q. \end{cases}$$

Moreover, $s = A - \frac{q}{\eta} < A$. . Since $\delta_X \notin \mathcal{A}_X^*$, one can rewrite

$$f(\alpha_0) = \begin{cases} (q - \alpha_0) & \text{if } \alpha_0 \leq s, \\ (q - \alpha_0)(q - \eta(A - \alpha_0) + 1) & \text{if } \alpha_0 \geq s \end{cases}$$

1. If $\delta = \eta A < q$, then $s < 0$ and $\mathcal{A}_X^* = [\![0, \lfloor A \rfloor]\!]$. Therefore the function f can be written

   $$f(\alpha_0) = (q - \alpha_0)(q + \eta(\alpha_0 - A) + 1)$$

   It is increasing then decreasing on $\mathcal{A}_X^*$ so its minimum is reached for either $\alpha_0 = 0$ or $\alpha_0 = \lfloor A \rfloor$. Let us compare $f(0)$ and $f(\lfloor A \rfloor)$.

   $$f(0) \leq f(\lfloor A \rfloor) \Leftrightarrow \lfloor A \rfloor(q + \eta(\lfloor A \rfloor - A) + 1) \leq q\eta\lfloor A \rfloor$$

If $\lfloor A \rfloor \neq 0$ we can simplify by $\lfloor A \rfloor$ and, writing $\{A\} = A - \lfloor A \rfloor$, we get

$$f(0) \leq f(\lfloor A \rfloor) \Leftrightarrow 1 - \eta\{A\} \leq q(\eta - 1)$$

However, $0 \leq \eta\{A\} \leq \eta - 1$, which implies that $1 - \eta\{A\} \leq 1$ whereas the right hand-side is a non negative integer. Then the right hand-side is greater than the left one if and only if it is non zero, which is equivalent to $\eta \geq 2$, which is always true[1].

Otherwise, it is obvious. Then

$$\min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0) = f(0) = q(q - \delta + 1).$$

2. If $\frac{\delta}{\eta+1} < q \leq \delta$, then

$$\lfloor s \rfloor \in \mathcal{A}_x^* = \begin{cases} [\![0, \lfloor A \rfloor]\!] & \text{if } q > A = \frac{\delta}{\eta}, \\ [\![0, q-1]\!] & \text{if } q \leq A. \end{cases}$$

The function f has a linear decreasing piece on $[0, s]$ and then it is concave on $[0, \min(\lfloor A \rfloor, q-1)]$, as illustrated in Figure 9.

Then it can be proved in a same way as in the second case for $\delta_T \geq 0$ (Equation (14)) that

$$f(\lfloor s \rfloor + 1) \geq f(\lfloor s \rfloor).$$

The minimum of f on $\mathcal{A}_X^*$ is thus either reached for $\alpha_0 = \lfloor s \rfloor$ or

- $\alpha_0 = \lfloor A \rfloor$ if $q > A$,
- $\alpha_0 = q - 1$ if $q \leq A$.

Let us prove that the minimum is reached at $\alpha_0 = \lfloor s \rfloor$ in both cases.

- If $q > A$, let us first notice that, since $s < A$, we have $\lfloor s \rfloor \leq \lfloor A \rfloor$.
  If they are equal, the problem is solved.
  Otherwise, one can write

  $$f(A) = (q - A)(q + 1) > f(\lfloor s \rfloor).$$

  As a fonction on $\mathbb{R}$, f is increasing on $[\lfloor s \rfloor + 1, A]$, then

  $$f(\lfloor A \rfloor) \geq f(\lfloor s + 1 \rfloor) \geq f(\lfloor s \rfloor).$$

- If $q \leq A$, we have

  $$f(q-1) = \eta(q - 1 - s) + 1 = q - s + (\eta - 1)(q - 1 - s).$$

  Since $\eta \geq 2$, we have

  $$\begin{aligned} f(q-1) &= q - s + (\eta - 1)(q - 1 - s), \\ &\geq q - s + (\eta - 1)\left(q\left(1 - \frac{1}{\eta}\right) + 1\right) && \text{since } \frac{\eta - 1}{\eta} q \leq s, \\ &\geq q - s + \left(\frac{q}{2} + 1\right) && \text{because } \eta \geq 2, \\ &\geq q - s + 1 && \text{because } q \geq 2, \\ &\geq f(\lfloor s \rfloor) = q - \lfloor s \rfloor && \text{because } s - 1 \leq \lfloor s \rfloor. \end{aligned}$$

[1] Here is one of the arguments that fail when $\eta = 1$.

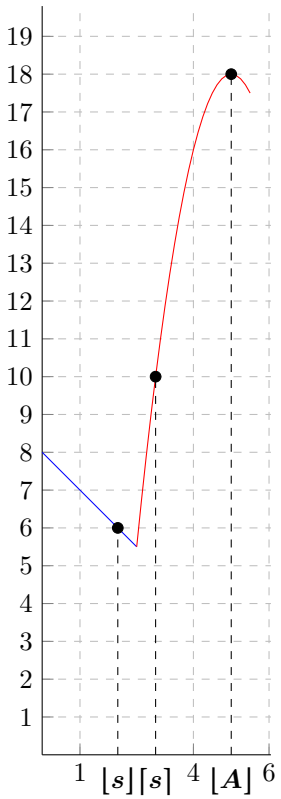


Figure 10: Graph of f for $\frac{\delta}{\eta} < q \leq \delta$ and $\eta \geq 2$
e.g. $(\eta, \delta_T, \delta_X, q) = (2, -5, 9, 8)$

Then, in both cases, $\min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0) = f(\lfloor s \rfloor) = q - \lfloor s \rfloor$.

3. If $q \leq \frac{\delta}{\eta+1}$, then $s \geq q$. For all $\alpha \in \mathcal{A}_X^* = [\![0, q-1]\!]$,

$$f(\alpha_0) = \max(q - \alpha_0, 1).$$

Since $q - 1 \in \mathcal{A}_X^*$, we have

$$\min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0) = f(q-1) = 1$$

Finally, for $\eta = 0$, the expression in the first maximum is a decreasing function of α_0 and the expression in the second maximum does not depend on α_0 anymore. Then

$$\min_{\alpha_0 \in \mathcal{A}_X^*} f(\alpha_0) = f(\delta_X) = \max(q - \delta_X + 1, 1) \max(q - \delta_T + 1, 1)$$

□

The following proposition displays some polynomials whose associated codewords has weight that reaches the lower bound given in Proposition 4.2.3.

Proposition 4.2.4. *Write* $\mathbb{F}_q = \{\xi_1, \xi_2, \ldots, \xi_q\}$.

- *If* $\eta \geq 2$,
  - *If* $q > \delta$, *set*

$$F(T_1, T_2, X_1, X_2) = X_1^{\delta_X} \prod_{i=1}^{\delta} (T_2 - \xi_i T_1),$$

  - *If* $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, *write* $s = \lfloor \frac{\delta - q}{\eta} \rfloor$. *Set*

$$F(T_1, T_2, X_1, X_2) = T_2^{\delta - \eta s - q}(T_2^q - T_2 T_1^{q-1}) X_1^{\delta_X - s} \prod_{i=1}^{s} (X_2 - \xi_i T_1^{\eta} X_1),$$

  - *If* $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$, *set*

$$F(T_1, T_2, X_1, X_2) = \begin{cases} T_2^{\delta_T - q}(T_2^q - T_2 T_1^{q-1}) \prod_{i=1}^{\delta_X} (X_2 - \xi_i X_1 T_1^{\eta}) & \text{if } \delta_X < q, \\ X_2^{\delta_X - q} T_2^{\delta - q}(T_2^q - T_2 T_1^{q-1}) \prod_{i=1}^{q} (X_2 - \xi_i X_1 T_1^{\eta}) & \text{if } \delta_X \geq q, \end{cases}$$

- *if* $\eta = 0$, *set* $m_T = \min(q, \delta_T)$ *and* $m_X = \min(q, \delta_X)$. *Set*

$$F(T_1, T_2, X_1, X_2) = X_2^{\delta_X - m_X} T_2^{\delta_T - m_T} \prod_{i=1}^{m_X} (X_2 - \xi_i X_1 T_1^{\eta}) \prod_{j=1}^{m_T} (T_2 - \xi_j T_1).$$

Then the weight of the codeword associated to F *in* $C_\eta(\delta_T, \delta_X)$ *reaches the minimum distance.*

Remark 4.2.5.

1. The minimum $\#\Delta^*(\delta_T, \delta_X)_M$ on $M \in \Delta^*(\delta_T, \delta_X)$ is reached for by the leading term of F in each case.
2. The previous proposition guarantees us than the choice of ϵ_T and ϵ_X in Paragraph 4.2 is adequate.
3. Focusing on the points lying on the torus, J. Little and H. Schenck [LS06] already proved that the polynomial with the most zero $\mathbb{F}_q$-points on a Hirzeburch surface have the form given in Proposition for q large enough to make the evaluation map injective. I. Soprunov and E. Soprunova [SS09] demonstrated that the number of $\mathbb{F}_q$ torus-points of a curve defined by $f = 0$ depends on the number L of absolutely irreducible factors of f:

$$\#C(\mathbb{F}_q^{\times}) \leq L(q-1) + \lfloor 2\sqrt{q} \rfloor - 1.$$

   Even though it seems natural to expect that maximal curves are union of "lines", a comprehensive computation of polynomials associated to minimum codewords highlights non linear factors among these polynomials, as stated by I. Soprunov and E. Soprunova.

Proof. First, suppose $\eta = 2$.

- If $q > \delta$, the polynomial $F(T_1, T_2, X_1, X_2) = X_1^{\delta_X} \prod_{i=1}^{\delta} (T_2 - \xi_i T_1)$ vanishes at every point of the form $(1, \xi_i, x_1, x_2)$ or $(t_1, t_2, 0, 1)$, that is to say at $(\delta)(q+1) + q + 1 - \delta$ points.

- If $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, note that $T_2^q - T_2 T_1^{q-1} = \prod_{a\in\mathbb{F}_q}(T_2 - aT_1)$. Then the polynomial

$$F(T_1, T_2, X_1, X_2) = T_2^{\delta-\eta s-q} \prod_{a\in\mathbb{F}_q} (T_2 - aT_1) X_1^{\delta_X - s} \prod_{i=1}^{s} (X_2 - \xi_i T_1^{\eta} X_1)$$

  vanishes at every point except at the ones of the form $(0, 1, 1, \xi)$ with $\xi \notin \{\xi_i, i \in \{1, \ldots, s\}\}$. The code word associated has weight equal to $q - s$.

- Assume $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$. If $q > \delta_X$, the polynomial

$$F(T_1, T_2, X_1, X_2) = T_2^{\delta_T - q}(T_2^q - T_2 T_1^{q-1}) \prod_{i=1}^{\delta_X} (X_2 - \xi_i X_1 T_1^{\eta})$$

  vanishes at the point with the form $(1, a, x_1, x_2)$ and $(0, 1, 1, \xi_i)$, that is to say $q(q+1) + \delta_X$.

  If $\delta_X \geq q$, the only point at which $F = X_2^{\delta_X - q} T_2^{\delta - q}(T_2^q - T_2 T_1^{q-1}) \prod_{i=1}^{q}(X_2 - \xi_i X_1 T_1^{\eta})$ is not zero is $(0, 1, 0, 1)$.

Finally, if $\eta = 0$, the polynomial

$$F(T_1, T_2, X_1, X_2) = X_2^{\delta_X - m_X} T_2^{\delta_T - m_T} \prod_{i=1}^{m_X} (X_2 - \xi_i X_1 T_1^{\eta}) \prod_{j=1}^{m_T} (T_2 - \xi_j T_1)$$

vanishes at every point of the form $(t_1, t_2, 1, \xi_i)$ and $(1, \xi_j, x_1, x_2)$, i.e. at $(m_T + m_X)(q+1) - m_T m_X$ points. Moreover, if $q < \delta_X$ (resp. $q < \delta_T$), it also vanishes at $(t_1, t_2, 1, 0)$ (resp. $(1, 0, x_1, x_2)$). □

Remark 4.2.6. The parameters for the code $C_0(\delta_T, \delta_X)$ on $\mathbb{P}^1 \times \mathbb{P}^1$, are the same as in [CD13] (see Theorem 2.1 and Remark 2.2).

5 Upperbound on the number of $\mathbb{F}_q$-rational points of curves on Hirzebruch surfaces

Proposition 4.2.3 gives an upper bound on the number of $\mathbb{F}_q$-rational points of a non-filling curve on a Hirzebruch surface $\mathcal{H}_\eta$. It is worth to highlight that there exists a filling curve of bidegree (δ_T, δ_X) if and only if $q < \delta$.

Corollary 5.0.1. *Let $\eta \geq 0$, $\eta \neq 1$ and $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ with $\delta = \delta_T + \eta\delta_X \geq 0$. Let $\mathcal{C}$ be a non-filling curve on the Hirzebruch surface $\mathcal{H}_\eta$ whose Picard class is $\delta_T\mathcal{F} + \delta_X\sigma$. Then the number of $\mathbb{F}_q$-rational point of the curve $\mathcal{C}$ is upper-bounded as follow.*

- *If $\eta \geq 2$,*
  - *If $q > \delta$, then*

$$\#\mathcal{C}(\mathbb{F}_q) \leq \begin{cases} (q+1)\delta_T & \text{if } \delta_X = 0 \text{ and } \delta_T \geq 0, \\ q(\delta+1)+1 & \text{otherwise.} \end{cases}$$

– *If* $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, *then*

$$\#\mathcal{C}(\mathbb{F}_q) \leq q^2 + q + 1 + \left\lfloor \frac{\delta - q}{\eta} \right\rfloor.$$

– *If* $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$ *and* $q \geq \delta_X$,

$$\#\mathcal{C}(\mathbb{F}_q) \leq q^2 + q + \delta_X.$$

- *if* $\eta = 0$,

$$\#\mathcal{C}(\mathbb{F}_q) \leq (q+1)^2 - \max(q - \delta_X + 1, 1)\max(q - \delta_T + 1, 1).$$

Moreover each upper bound is reached by Proposition 3.

These upper bounds cannot be compared to Hasse-Weil. Indeed the curves that reach these bounds can be highly reducible and singular, as displayed in Proposition 3. Such a phenomenon has already been observed on general toric surfaces by I. Soprunov and J. Soprunova [SS09].

6 Punctured codes

J. P. Hansen [Han02] and B. L. De La Rosa Navarro and M. Lahyane [DLRNL15] studied codes, only on $\mathbb{F}_q$ with q big enough so that the evaluation map is injective, that turn to be punctured codes of our evaluation code $C_\eta(\delta_T, \delta_X)$.

In [DLRNL15], the authors in fact considered a punctured code of $C_\eta(\delta_T, 0)$ at $q+1$ coordinates as the evaluation code of polynomials of bidegree $(\delta_T, 0)$ outside the fiber $\mathcal{F}$ for $q \geq \delta_T$. They obtained a quite bad puncturing since here the code $C_\eta(\delta_T, 0)$ has parameters $[N, k, d] = [(q+1)^2, \delta_T + 1, (q+1)(q - \delta_T + 1)]$ whereas theirs has parameters $[N - (q+1), k, d - (q+1)]$.

Among other toric surfaces, J.P. Hansen [Han02] and, more recently, J. Little and H. Schenck [LS06], studied toric codes on Hirzeburch surfaces that evaluate polynomials of $R(\delta_T, \delta_X)$ for δ_T and δ_X both positive and only on $\mathbb{F}_q$-rational points of the torus $\mathbb{G}_m^2$. They also assumed that $\delta = \delta_T + \eta\delta_X < q - 1$, which ensures the evaluation map to be injective. They proved the minimum distance to be equal to $(q-1)^2 - \delta(q-1)$.

Such a code is obtained from puncturing $C_\eta(\delta_T, \delta_X)$ at the $4q$ rational points of $\mathcal{Z}(T_1T_2X_1X_2) = D_1 + D_2 + E_1 + E_2$. They obtained a quite good puncturing since here the code $C_\eta(\delta_T, \delta_X)$ has parameters

$$[N, k', d'] = \left[(q+1)^2, (\delta_X + 1)\left(\delta_T + \eta\frac{\delta_X}{2} + 1\right), q(q - \delta_T + 1)\right],$$

whereas theirs has parameters $[N - 4q, k', d' - (3q - \delta - 1)]$. Note that, as stated in the introduction, the difference between minimum distances is at least $2q$, the half of the difference between the lengths. This feature was already observed by G. Lachaud when extending Reed-Muller codes to projective Reed-Muller codes [Lac90].

We highlight here an interesting puncturing of codes $C_\eta(\delta_T, \delta_X)$ when δ_T is negative, in the sense that all common zero coordinates of codewords and only them are punctured. Let us define the linear code $C^\star_\eta(\delta_T, \delta_X)$ over $\mathbb{F}_q$ obtained by punctuation of the code $C_\eta(\delta_T, \delta_X)$ at the points of $\mathcal{Z}(X_1) = D_1$.

Theorem 6.0.1. *Let $\eta \geq 1$, $\delta_T < 0$ and $\delta_X > 0$. The code $C^\star_\eta(\delta_T, \delta_X)$ has length $q(q+1)$ and has the same dimension and minimum distance as $C_\eta(\delta_T, \delta_X)$.*

Proof. Every monomial $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \in R(\delta_T, \delta_X)$ on $\mathcal{H}_\eta$ satisfies

$$0 \leq c_1 + c_2 = \delta_T + \eta d_1 < \eta d_1.$$

Hence $d_1 > 0$ and M is zero on $X_1 = 0$. □

Remark 6.0.2. The previous theorem is true even if $\eta = 1$.

Example 6.0.3. *Here are some examples of punctured code $\mathbb{F}_3$, of length 12 that reach the bounds given by code.tables [Gra07].*

η	δ_T	δ_X	*Parameters of* $C^\star_\eta(\delta_T, \delta_X)$
2	*-1*	*1*	*[12,2,9]*
2	*-1*	*3*	*[12,10,2]*
2	*-2*	*2*	*[12,4,6]*
2	*-2*	*3*	*[12,8,3]*

Acknowledgement

The author expresses his gratitude to the anonymous referee for his careful work and his helpful suggestions, especially for the third section.

References

[BDG19] Peter Beelen, Mrinmoy Datta, and Sudhir R. Ghorpade. Vanishing ideals of projective spaces over finite fields and a projective footprint bound. *Acta Mathematica Sinica, English Series*, 35(1):47–63, Jan 2019.

[CD13] Alain Couvreur and Iwan Duursma. Evaluation codes from smooth quadric surfaces and twisted Segre varieties. *Des. Codes Cryptogr.*, 66(1-3):291–303, 2013.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[CLS11] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.

[CN16] Cicero Carvalho and Victor G. L. Neumann. Projective Reed-Muller type codes on rational normal scrolls. *Finite Fields Appl.*, 37:85–107, 2016.

[DLRNL15] Brenda Leticia De La Rosa Navarro and Mustapha Lahyane. Algebraic-geometric codes from rational surfaces. In *Algebra for secure and reliable communication modeling*, volume 642 of *Contemp. Math.*, pages 173–180. Amer. Math. Soc., Providence, RI, 2015.

[GH00] O. Geil and T. Hoholdt. Footprints or generalized bezout's theorem. *IEEE Transactions on Information Theory*, 46(2):635–641, March 2000.

[Gra07] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2018-01-01.

[Han01] Søren Have Hansen. Error-correcting codes from higher-dimensional varieties. *Finite Fields Appl.*, 7(4):531–552, 2001.

[Han02] Johan P. Hansen. Toric varieties Hirzebruch surfaces and error-correcting codes. *Appl. Algebra Engrg. Comm. Comput.*, 13(4):289–300, 2002.

[Joy04] David Joyner. Toric codes over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 15(1):63–79, 2004.

[Lac90] Gilles Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2):217–221, 1990.

[LP10] Christian Liedtke and Stavros Argyrios Papadakis. Birational modifications of surfaces via unprojections. *J. Algebra*, 323(9):2510–2519, 2010.

[LS06] John Little and Hal Schenck. Toric surface codes and Minkowski sums. *SIAM J. Discrete Math.*, 20(4):999–1014, 2006.

[Rei97] Miles Reid. Chapters on algebraic surfaces. In *Complex algebraic geometry (Park City, UT, 1993)*, volume 3 of *IAS/Park City Math. Ser.*, pages 3–159. Amer. Math. Soc., Providence, RI, 1997.

[Rua07] Diego Ruano. On the parameters of r-dimensional toric codes. *Finite Fields Appl.*, 13(4):962–976, 2007.

[SS09] Ivan Soprunov and Jenya Soprunova. Toric surface codes and Minkowski length of polygons. *SIAM J. Discrete Math.*, 23(1):384–400, 2008/09.

[Stu96] Bernd Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

Chapitre 4

Bornes de sur le nombre de points rationnels des courbes irréductibles sur les surfaces de Hirzebruch

BOUND ON THE NUMBER OF RATIONAL POINTS ON CURVES ON HIRZEBRUCH SURFACES OVER FINITE FIELDS

JADE NARDI

ABSTRACT. This paper gives a bound on the number of rational points on an absolutely irreducible curve $\mathcal{C}$ lying on a minimal toric surface X. This upper bound improves pre-existing ones if $\mathcal{C}$ has large genus. The strategy consists in finding another curve that intersects $\mathcal{C}$ with good multiplicity at its rational points outside some well-handled closed set. Finding such a curve relies on an extension of K.O. Stöhr and F.J. Voloch's idea for plane curves to the toric framework based on homogenization.

INTRODUCTION

By the Hasse-Weil bound, the number of $\mathbb{F}_q$-points on a smooth, geometrically integral projective curve C defined over $\mathbb{F}_q$ of genus g is bounded from above by $q+1+2g\sqrt{q}$. K.O. Stöhr and F.J. Voloch [SV86] gave an upper bound on the number of $\mathbb{F}_q$-points on an irreducible non-singular projective curve. This bound depends on the Frobenius order-sequence and the genus of the curve. M. Homma and S. J. Kim [HK09] [HK10a] [HK10b] used Stöhr-Voloch theory to prove that a curve on $\mathbb{P}^2$ of degree d without $\mathbb{F}_q$-linear components has at most $(d-1)q+1$ $\mathbb{F}_q$-points, except for a certain curve over $\mathbb{F}_4$. Few years later, M. Homma managed to extend this result on $\mathbb{P}^r$ for $r \geq 3$ [Hom12].

These latter bounds are sharper than Weil's general one for projectively embedded curves for a certain range of parameters [see Figures 3 p16 and 4 p17]. Such bounds are interesting in themselves and also have applications in coding theory, for example the computation of the minimum distance of algebraic geometric codes introduced by V.D.Goppa in 1980. In this paper, we focus on curves embedded in a certain class of surfaces, namely toric smooth surfaces. One can expect that constraining a curve in a specific ambient space and taking advantage of its geometry enables one to enhance the upper bound. We concentrate on irreducible curves, as the reducible case has already been dealt with in the context of Hirzebruch surfaces via coding theory [see [CD13], [CN16], [Nar18]].

More precisely, our strategy is to adapt Stöhr and Voloch's idea [SV86] for plane curves to fit into the toric framework. They bounded the number of $\mathbb{F}_q$-points on a plane curve by computing the number of points whose image under the Frobenius map belongs to their tangent line. They put to good use the nice property of the tangent line to the curve $f = 0$ at a point $P = (x_P, y_P)$, namely that it has a global equation $(x-x_P)f_x(P) + (y-y_P)f_y(P) = 0$ on the affine plane. Their bound can thus easily be computed as half the intersection number of C and the curve defined by $(x^q - x)f_x + (y^q - y)f_y = 0$, since a $\mathbb{F}_q$-point has multiplicity 2 in this

2010 *Mathematics Subject Classification.* Primary 14M25, 14G05, 11G20, 11G25.

This work is partially funded by French ANR-15-CE39-0013 "manta". The author warmly thanks F.J. Voloch for his helpful remarks and the time he devoted to answer her questions.

intersection. To put it another way, the authors displayed a polynomial that vanishes with multiplicity at least 2 at the rational points of the curve. Their bound only depends on the size of the field q and the degree of the curve.

We aim to generalize this idea. Given a curve $\mathcal{C}$ on a toric surface, we want to find an interpolation curve that intersects $\mathcal{C}$ at its rational points with good multiplicity using the same "tangent trick" as K.O. Stöhr and F.J. Voloch. However, adapting their idea on toric surfaces other than $\mathbb{P}^2$ is not trivial since there is no notion of global tangent line of a curve. A naive idea to overcome this issue would be to consider the local tangent line at a point P on a curve $\mathcal{C}$ then take its Zariski closure in the whole surface. Unfortunately "tangents" constructed in this way at two points P_1 and P_2 on $\mathcal{C}$ would not have the pleasant property of always being linearly equivalent.

Happily we can benefit from handy geometric properties of toric varieties. First, toric varieties are endowed with a graded polynomial coordinate ring, named the Cox ring. In the same way that an affine polynomial can be made into a homogeneous one on $\mathbb{P}^n$, there exists a process of homogenization, detailed in Section 1.2, that turns a regular function on the dense torus $\mathbb{T}$ of the toric variety into a polynomial of the Cox ring [see [CLS11] [CD97]].

Moreover, on toric surfaces, a curve can be defined as the zero locus of a polynomial in this Cox ring. In dimension 2, this means that, given the equation of a curve on the dense torus of a toric surface, it is possible to get an equation of a curve on the whole toric surface containing the first one. The degree of the polynomial defining a curve corresponds to its Picard class.

In addition, a toric surface is covered by affine charts (U_σ) isomorphic to $\mathbb{A}^2$ with explicit transition maps. Modifying the regular fonction $g = (x^q - x)f_x + (y^q - y)f_y$ according to these maps, we are able for each toric affine patch U_σ to easily define a curve on the torus that intersects the curve $\mathcal{C} \cap \mathbb{T}^2$ at the set of points in $\mathbb{T}^2$ whose image under the Frobenius map belongs to their tangent. Homogenizing its equation, we thus get a curve on the toric surface, with explicit Picard class in terms of the one of $\mathcal{C}$. Repeating this process on each affine chart, we define as many curves as there are affine charts on the surface whose intersection with $\mathcal{C}$ contains the set of $\mathbb{F}_q$-points of $\mathcal{C}$ outside a well-handled closed set.

Finally the Picard group of a toric variety is well-understood: its generators and relations are completely determined by its fan. Therefore, the intersection number of $\mathcal{C}$ with one of these curves divided by 2 – the lowest intersection multiplicity at a $\mathbb{F}_q$-point of $\mathcal{C}$ – gives an effortlessly computable upper bound, provided that they have no common components. This yields several bounds according to the ambient surface:

Theorem 1. *Let $\mathcal{C}$ be an absolutely irreducible curve on a minimal toric surface X defined over a finite field $\mathbb{F}_q$.*

- *For $X = \mathbb{P}^2$ (Thm 1* [SV86]*) and $2 \nmid q$, if $\mathcal{C}$ has degree $d \geq 2$, then*
$$\#C(\mathbb{F}_q) \leq \frac{1}{2}d(d+q-1),$$
provided that $\mathcal{C}$ has a non flex point.
- *For $X = \mathbb{P}^1 \times \mathbb{P}^1$ (Thm 3), if $\mathcal{C}$ has bidegree $(\alpha, \beta) \in (\mathbb{N}^*)^2$, then*
$$\#C(\mathbb{F}_q) \leq \alpha\beta + \frac{q}{2}(\alpha+\beta).$$
- *For $X = \mathcal{H}_\eta$ with $\eta \neq 0$ (Thm 4), if $\mathcal{C}$ has bidegree $(\alpha, \beta) \in (\mathbb{N}^*)^2$, then*
$$\#\mathcal{C}(\mathbb{F}_q) \leq \frac{\beta}{2}(2\alpha - \eta\beta - \eta + 1) + \frac{q}{2}(\alpha+\beta).$$

Although the method we develop here can be applied to any toric surface, this paper solely focuses on the projective plane and Hirzeburch surfaces, which are the only minimal rational surfaces – except for $\mathcal{H}_1 \simeq \widetilde{\mathbb{P}^2}$. Also any smooth complete toric surface is obtained by toric blowups from either $\mathbb{P}^2$ or a Hirzebruch surface. It seems that we get a better upper bound using this fact than using the method elaborated here, as illustrated for $\mathcal{H}_1$ in Section 5.

It is worth to note that the bound on $\mathbb{A}^2$ or $\mathbb{P}^2$ requires the curve to have a least one non-flex point on each of its irreducible components whereas such kind of condition is not required on Hirzebruch surfaces, and thus on $\mathcal{H}_1$. On top of that, our method can doubtlessly be extended to higher dimensional toric varieties, notably to adapt F.J. Voloch's idea for surfaces in $\mathbb{P}^3$ [Vol03].

1 SOME TOOLS ON TORIC VARIETIES

1.1 COX RING AND CHARACTERS

General results about toric varieties are compiled here. The reader is invited to read [CLS11] for further details.

Fix an integer $n \in \mathbb{N}^*$. Set $N \simeq \mathbb{Z}^n$ a $\mathbb{Z}$-lattice and $M = \mathrm{Hom}(N, \mathbb{Z})$ its dual lattice. Let $\mathbb{T}^n$ be the *n-dimensional algebraic torus*, then $\mathbb{T}^n(\bar{k}) = (\bar{k}^\times)^n$. A *character* of $\mathbb{T}^n$ is a morhism $\chi : \mathbb{T}^n \to k^\times$ which is a group homomorphism. M is called the *character group*, forms the set of regular functions on $\mathbb{T}^n$ and is isomorphic to $\mathbb{Z}^n$ via the map

$$\begin{cases} \mathbb{Z}^n & \to & M \\ m & \mapsto & \chi^m : (t_1, \dots, t_n) \mapsto t_1^{m_1} \dots t_n^{m_n} \end{cases}$$

Let us set the dual pairing $\langle \cdot, \cdot \rangle : M \times N \to \mathbb{Z}$ which is $\mathbb{Z}$-bilinear. Let $N_\mathbb{R} = N \otimes \mathbb{R} \simeq \mathbb{R}^n$ and $M_\mathbb{R} = M \otimes \mathbb{R}$, its dual vector space. The dual pairing extends as a $\mathbb{R}$-bilinear pairing.

Let σ be a *strongly convex rational cone* in $N_\mathbb{R}$, i.e. $\sigma \cap (-\sigma) = \{0\}$ and σ is generated by vectors in N. From now, we assume any cone to be strongly convex rational. For any cone σ, we define its dual cone

$$\sigma^\vee := \{m \in M_\mathbb{R} \mid \forall\ u \in \sigma,\ \langle m, u \rangle \geq 0\}$$

and associate to σ the affine toric variety $U_\sigma = \mathrm{Spec}\, k[\sigma^\vee \cap M]$. A fan Σ in N is a finite set of cones in $N_\mathbb{R}$ such that each face of a cone in Σ is also a cone in Σ and the intersection of two cones in Σ is a face of each of both cones. The set of r-dimensional cones in Σ is denoted by $\Sigma(r)$. A 1-dimensional cone is called a ray. Any ray $\rho \in \Sigma(1)$ has a unique minimal generator $u_\rho \in \rho \cap \mathbb{Z}^n$. A n-dimensional cone is said to be *maximal*.

The toric variety X_Σ associated to the fan Σ is defined as the union of the affine toric varieties $(U_\sigma)_{\sigma \in \Sigma}$. If a cone τ is included in another cone σ, the variety U_σ contains U_τ, which means that

$$X_\Sigma = \bigcup_{\sigma \in \Sigma(n)} U_\sigma. \tag{1}$$

Moreover, the torus $\mathbb{T}^n$ is a dense open subset of X_Σ acting on X_Σ. The complement of $\mathbb{T}^n$ in X_σ is well-known. A $\rho \in \Sigma(1)$ corresponds to a codimension 1 orbit under $\mathbb{T}^n$, whose Zariski closure is a $\mathbb{T}^n$-invariant divisor, denoted by D_ρ. Then

$$X_\sigma = \mathbb{T}^n \sqcup \left(\bigcup_{\rho \in \Sigma(1)} D_\rho \right). \tag{2}$$

Assume that the set of minimal generators $\{u_\rho,\ \rho \in \Sigma(1)\}$ spans $\mathbb{R}^n$, i.e. X_Σ has *no torus factors*. Set $\mathrm{Div}_{\mathbb{T}^n}(X)$ the group of $\mathbb{T}^n$-invariant Weil divisors on X_Σ. Then we have a short exact sequence

$$0 \to M \to \mathrm{Div}_{\mathbb{T}^n}(X_\Sigma) \to \mathrm{Cl}(X_\Sigma) \to 0 \tag{3}$$

where the map $M \to \mathrm{Div}_{\mathbb{T}^n}(X_\Sigma)$ associates to a character χ^m the principal divisor

$$\mathrm{div}(\chi^m) = \sum_{\rho \in \Sigma(1)} \langle m, u_\rho \rangle D_\rho.$$

In other words, any divisor on X_Σ is linearly equivalent to a $\mathbb{T}^n$-invariant divisor, $\mathbb{Z}$-linear combination of the divisors D_ρ, and the divisors associated to characters are exactly the one linearly equivalent to 0. Thus, the Picard group has rank $\#\Sigma(1) - n$.

A variable x_ρ is associated to each ray $\rho \in \Sigma(1)$. The *Cox Ring* of X_Σ is defined by $S = k\left[x_\rho \,|\, \rho \in \Sigma(1)\right]$. The function field of X_Σ is $\mathrm{Frac}(S)$. The ring S can be endowed with a graduation, using the short exact sequence

$$0 \longrightarrow M \xrightarrow{a} \mathbb{Z}^{\Sigma(1)} \xrightarrow{b} \mathrm{Cl}(X_\Sigma) \longrightarrow 0,$$

with $a(m) = \left(\langle m, u_\rho \rangle\right)_{\rho \in \Sigma(1)}$ for $m \in M$ and $b(\alpha) = \left[\sum_\rho \alpha_\rho D_\rho\right]$ for $\alpha = (\alpha_\rho) \in \mathbb{Z}^{\Sigma(1)}$. The *degree* of a monomial $x^\alpha = \prod x_\rho^{\alpha_\rho}$ in S, where $\alpha \in \mathbb{N}^{\Sigma(1)}$, is defined as the Picard class of the divisor $\sum_\rho \alpha_\rho D_\rho$. Then

$$S = \bigoplus_{\beta \in \mathrm{Cl}(X_\Sigma)} S_\beta$$

where S_β is the vector k-space of homogeneous polynomials of degree β. As in projective spaces, we have some Euler relations. For any divisor class $\beta \in \mathrm{Cl}(X_\Sigma)$ and any group homomorphism $\phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Cl}(X_\Sigma), \mathbb{Z})$,

$$\forall F \in S_\beta,\ \sum_{\rho \in \Sigma(1)} \phi([D_\rho]) x_\rho \frac{\partial F}{\partial x_\rho} = \phi(\beta) F \tag{Eu}$$

Let $D = \sum a_\rho D_\rho$ be a $\mathbb{T}^n$-invariant Weil divisor on X_Σ. Let us set the polytope

$$P_D = \{m \in M_{\mathbb{R}} \,|\, \forall \rho \in \Sigma(1),\ \langle m, u_\rho \rangle \geq -a_\rho\}.$$

If D and D' are two linearly equivalent divisors, i.e. there exists $m \in M$ such that

$$D' = D + \sum_{\rho \in \Sigma(1)} \langle m, u_\rho \rangle D_\rho,$$

then P'_D is the translate of P_D by the translation of vector m.

The lattice points of this polytope give a description of the global sections of $\mathcal{O}_{X_\Sigma}(D)$:

$$\Gamma(X_\Sigma, \mathcal{O}_{X_\Sigma}(D)) = \bigoplus_{m \in P_D \cap M} k.\chi^m. \tag{4}$$

1.2 HOMOGENIZING A CHARACTER

Let $f \in k[t_1^{\pm 1}, \ldots, t_n^{\pm 1}]$ be a Laurent polynomial. It defines a regular function on the torus $\mathbb{T}^n$. We would like to give it a meaning on the whole variety X_Σ: we want to find a polynomial F in the Cox ring S of X_Σ such that the variety defined by $F = 0$ is – or at least contains –F the Zariski closure of the affine variety $f = 0$ on $\mathbb{T}^n$.

More practically, we aim to generalize the very natural operation of homogenization in the projective case.

Example 1. *On $\mathbb{P}^2$, the polynomial $f = x^m + x + y$ defines a regular function on $\mathbb{P}^2 \setminus \{Z = 0\}$ for $m \geq 1$. It can be homogenized as $F = X^m + XZ^{m-1} + YZ^{m-1}$ of degree m. It is also possible to homogenize this polynomial as $F' = Z^{d-m}(X^m + XZ^{m-1} + YZ^{m-1})$ of degree d, for any $d \geq m$. However, even if we can homogenize x and y by X and Y, of degree $d \geq 1$, we cannot homogenize the whole polynomial f by a polynomial of degree $d < m$, as it is not possible for x^m.*

As illustrated by Example 1, one have to choose a degree before homogenizing in the projective case. Since the Cox ring is graded by the Picard group, the analogous method in other toric varities will consist in choosing a Picard class.

Definition 1 (Homogenization of a character)**.** *Let $m \in M$ and D a $\mathbb{T}^n$-invariant divisor such that $m \in P_D$. The D-homogenization of the character χ^m is defined by*

$$x^{\langle m,D\rangle} = \prod_{\rho} x_\rho^{\langle m,u_\rho\rangle + a_\rho}.$$

Remark 1. *The assumption $m \in P_D$ in Definition 1 is analagous to the assumption $m \leq d$ in Example 1.*

It is thus possible to homogenize a Laurent monomial, using the method detailed in [CD97]. To homogenize a Laurent polynomial, we have to find a divisor D such that any character that appears in this polynomial can be D-homogenized. In order to find such a divisor, we use the Newton polytope of the Laurent polynomial. Set $f = \sum c_m \chi^m \in k[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$. The *Newton polytope* $\Delta(f)$ of f is defined as the convex hull of the set $\{m \in \mathbb{Z}^n,\ c_m \neq 0\}$ in $\mathbb{R}^n$.

Notation 1. *Let $f = \sum c_m \chi^m \in k[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$. For all $\rho \in \Sigma(1)$, set*

$$a_\rho^f = -\min_{\nu \in \Delta(f)} \langle \nu, u_\rho \rangle \tag{5}$$

and $D_f = \sum a_\rho^f D_\rho$.

On can easily check that the Newton polytope $\Delta(f)$ of the Laurent polynomial $f \in k[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$ is contained in the polytope P_{D_f}. Moreover any divisor $D = \sum b_\rho D_\rho$ such that $\Delta(f) \subset P_D$ satisfies $a_\rho^f \leq b_\rho$ for all $\rho \in \Sigma(1)$.

Definition 2. *Let $D = \sum a_\rho D_\rho$ be a $\mathbb{T}^n$-invariant divisor such that $\Delta(f) \subset P_D$. Then the D-homogenization of f is the polynomial*

$$F = \sum_{m \in \Delta(f)} c_m \prod_{\rho \in \Sigma(1)} x_\rho^{\langle m,u_\rho\rangle + a_\rho^f}$$

of degree $[D]$.

Remark 2. *The D-homogenization of a Laurent polynomial does not depend on the representative of $[D]$.*

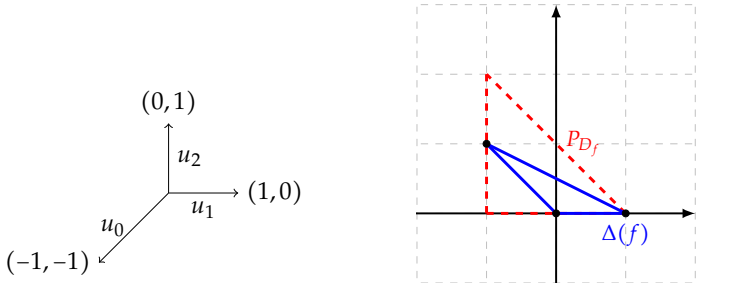
Example 2. *See Figure (1a) for the fan of the toric surface $\mathbb{P}^2$. As usual, we denote the variable associated to the ray spanned by u_i by x_i for $i \in \{0, 1, 2\}$.*

Let us consider the Laurent polynomial $f = t_1 + t_1^{-1} t_2 + 1$. Its Newton polygon $\Delta(f) = \mathrm{Conv}_{\mathbb{R}^2}\{(1,0), (-1,1), (0,0)\}$ is drawn in Figure (1b). In this case

$$-\min_{\nu \in \Delta(f)} \langle \nu, u_i \rangle = \begin{cases} 1 & \text{if } i = 0, \\ 1 & \text{if } i = 1, \\ 0 & \text{if } i = 2. \end{cases}$$

hence $D_f = D_0 + D_1$, where D_i is the $\mathbb{T}^2$-invariant divisor associated to the ray spanned by u_i. The D_f-homogenization of f is thus $F = x_1^2 + x_0 x_1 + x_0 x_2$, which is the same

polynomial as in Example 1. Two Laurent polynomials equal up to multiplication by a monomial have the same homogenization with respect to two linearly equivalent divisors.



(A) Fan of $\mathbb{P}^2$ (B) Newton polygon of f (Example 2)

FIGURE 1

2 PRINCIPLE

This section is dedicated to the implementation of the method used later. It essentially relies on Stöhr and Voloch's idea to bound the number of $\mathbb{F}_q$-points on a plane curve [SV86]. Given a plane curve $\mathcal{C}$ of equation $f = 0$, they display an interpolation polynomial h (see (6)) that vanishes at the $\mathbb{F}_q$-points of $\mathcal{C}$ with multiplicity at least 2, as proved in Lemma 1. This enables to give an upper bound for the cardinality of $\mathcal{C}(\mathbb{F}_q)$ by half the intersection number of $\mathcal{C}$ and the curve $\mathcal{D}$ defined by $h = 0$.

Our method aims to adapt this idea on another toric surface X. Given a curve $\mathcal{C}$ on X, we want to find an interpolation curve $\mathcal{D}$ that passes through the $\mathbb{F}_q$-points of $\mathcal{C}$ with mutliplicity at least 2. Since intersection multiplicity is a local property, we shall use the polynomial h in (6) and rewrite it in terms of the coordinates on each affine toric patch of X as displayed in (7). Next, it remains to homogenize this polynomial to get a global equation (9) on the whole surface X. Its results as many interpolation curves as there are affine toric patches.

2.1 STÖHR AND VOLOCH'S INTERPOLATION POLYNOMIAL ON $\mathbb{A}^2$

The following lemma by [SV86] exhibits a good interpolation polynomial of the $\mathbb{F}_q$-points of a given plane curve. Its proof is given here to make this paper comprehensive and understandable.

Lemma 1 ([SV86]). *Let $\mathcal{C}$ be a plane curve defined by a polynomial $f \in \mathbb{F}_q[x,y]$ on $\mathbb{A}^2$. The intersection multiplicity at a $\mathbb{F}_q$-points of $\mathcal{C}$ with the variety defined by $h = 0$, where*

$$h = (x^q - x)f_x + (y^q - y)f_y = 0, \tag{6}$$

is at least 2.

Proof. Take $P \in \mathcal{C}(\mathbb{F}_q)$. First, P is clearly a zero of h. Moreover, the multiplicity of P in $f = h = 0$ is greater than the product of the multiplicities on $f = 0$ and $h = 0$ with equality occurring if and only if the gradients of f and h are not collinear

at P [see [Ful89] section 3.3]. The case when P is a singular point of $\mathcal{C}$ is thus straightforward. Otherwise, if P is a simple $\mathbb{F}_q$-point on $\mathcal{C}$, then

$$dh_P = -f_x(P)dx_P - f_y(P)dy_P$$

and $\nabla h(P)$ and $\nabla f(P)$ are collinear, which concludes the proof. □

The polynomial h given in Lemma 1 has the advantage of interpolating $\mathbb{F}_q$-rational points of a given curve, with intersection multiplicity at least 2. We aim to generalize this idea. Given a polynomial F in the Cox ring, we want to display another polynomial G such that the intersection of the curves defined by $F = 0$ and $G = 0$ contains the $\mathbb{F}_q$-points of $F = 0$ and has multiplicity at least 2 at these points.

2.2 TORIC FRAMEWORK

Let X be a complete normal toric surface with fan Σ. Let us fix a polynomial $F \in S$ of degree $[D_F] = \left[\sum a_\rho D_\rho\right]$, defining a curve $\mathcal{C} \subset X$. Then

$$F = \sum_{m \in P_{D_F}} c_m \prod_{\rho \in \Sigma(1)} x_\rho^{\langle m, u_\rho \rangle + a_\rho}$$

and we set

$$f = \sum_{m \in P_{D_F}} c_m \chi^m.$$

the equation of $C \cap \mathbb{T}^2$. The toric surface X is covered by as many affines charts (U_σ) as there are maximal cones $\sigma \in \Sigma(2)$ in the fan Σ.

2.2.1 Interpolation polynomial on a toric affine patch

Let us consider a maximal cone $\sigma = \mathrm{Cone}(u_{\rho_1}, u_{\rho_2})$ in Σ. Set A_σ the square matrix created by juxtaposing the column vectors u_{ρ_1} and u_{ρ_2}. Set

$$\Delta_\sigma = \det A_\sigma.$$

Up to exchange ρ_1 and ρ_2, we assume $\Delta_\sigma > 0$. We denote by n_1^σ and n_2^σ the row vectors of $\Delta_\sigma \times A_\sigma^{-1}$, which entries are integers. Then the dual cone of σ is equal to $\sigma^\vee = \mathrm{Cone}(n_1^\sigma, n_2^\sigma)$, since $\left\langle n_i^\sigma, u_{\rho_j} \right\rangle = \Delta_\sigma \delta_{i,j}$ by construction . The affine toric variety U_σ associated to the cone σ corresponds to $\mathrm{Spec}\, k\left[\chi^{n_1^\sigma}, \chi^{n_1^\sigma}\right] \simeq \mathbb{A}^2$.

To adapt Stohr and Voloch's idea and take advantage of Lemma 1, we want to homogenize the polynomial

$$g_\sigma = (\chi^{(q-1)n_1^\sigma} - 1)\chi^{n_1^\sigma} \frac{\partial f}{\partial \chi^{n_1^\sigma}} + (\chi^{(q-1)n_2^\sigma} - 1)\chi^{n_2^\sigma} \frac{\partial f}{\partial \chi^{n_2^\sigma}}. \tag{7}$$

The points of $U_\sigma = \mathrm{Spec}\, k\left[\chi^{n_1^\sigma}, \chi^{n_1^\sigma}\right]$ lying on the curve $\mathcal{C}$ at which g_σ vanishes are exactly the points of $\mathcal{C} \cap U_\sigma$ whose image under the Frobenius map belongs to their tangent line in U_σ.

Remark 3. *For any $m \in M$ and $\lambda \in \mathbb{Z}$, one can write $(\chi^m)^\lambda$ or $\chi^{\lambda m}$ without ambiguity, as λm also belongs to the $\mathbb{Z}$-lattice M.*

2.2.2 Homogenization of the interpolation polynomial

In order to homogenize g_σ, we need to compute its Newton polygon. On this purpose, we shall express g in terms of the coefficients of f, which will enables to write the Newton polygon of g_σ depending on the one of f.

First let rewrite f with respect to $\chi^{n_1^\sigma}$ and $\chi^{n_2^\sigma}$. It is equivalent to find a_1 and a_2 such that $m = a_1 n_1^\sigma + a_2 n_2^\sigma$. Computing the scalar product of m with u_{ρ_1} and u_{ρ_2}, we have $a_i = \frac{1}{\Delta_\sigma}\langle m, u_{\rho_i}\rangle$ for $i \in \{1,2\}$. Then

$$\chi^m = \left(\chi^{n_1^\sigma}\right)^{\frac{1}{\Delta_\sigma}\langle m,u_{\rho_1}\rangle}\left(\chi^{n_2^\sigma}\right)^{\frac{1}{\Delta_\sigma}\langle m,u_{\rho_2}\rangle}$$

and the polynomial f can written

$$f = \sum_{m\in P_D} c_m \left(\chi^{n_1^\sigma}\right)^{\frac{1}{\Delta_\sigma}\langle m,u_{\rho_1}\rangle}\left(\chi^{n_2^\sigma}\right)^{\frac{1}{\Delta_\sigma}\langle m,u_{\rho_2}\rangle}.$$

Note that f is not a polynomial with respect to o $\chi^{n_1^\sigma}$ and $\chi^{n_2^\sigma}$ if $\Delta_\sigma \neq 1$, that is to say when the cone is not smooth. Anyway, for $i \in \{1,2\}$, we have

$$\chi^{n_i^\sigma}\frac{\partial f}{\partial \chi^{n_i^\sigma}} = \frac{1}{\Delta_\sigma}\sum c_m \langle m, u_{\rho_i}\rangle \chi^m, \tag{8}$$

which is a Laurent polynomial even if $\Delta_\sigma \neq 1$.

To determine in which degree we will homogenize the polynomial g_σ, we need to find a divisor E_σ such that the Newton polygon of g_σ is contained in P_{E_σ}. Using (8), we have

$$\Delta_\sigma g_\sigma = \sum c_m \left((\chi^{(q-1)n_1^\sigma}-1)\langle m, u_{\rho_1}\rangle + (\chi^{(q-1)n_2^\sigma}-1)\langle m, u_{\rho_2}\rangle\right)\chi^m.$$

We can deduce that

$$\Delta(g_\sigma) \subset \mathrm{Conv}\left(\left(\bigcup_{\substack{m\in\Delta(f)\\ \langle m,u_{\rho_1}\rangle\neq 0}} \{m, m+n_1^\sigma(q-1)\}\right)\cup\left(\bigcup_{\substack{m\in\Delta(f)\\ \langle m,u_{\rho_2}\rangle\neq 0}} \{m, m+n_2^\sigma(q-1)\}\right)\right).$$

Set $b_\rho^\sigma = -\min_{m\in\Delta(g_\sigma)}\langle m, u_\rho\rangle = a_\rho + (q-1)\epsilon_\rho^\sigma$ with

$$\epsilon_\rho^\sigma = -\min\left\{0, \langle n_1^\sigma, u_\rho\rangle, \langle n_2^\sigma, u_\rho\rangle\right\} \geq 0$$

and

$$E_\sigma = \sum_{\rho\in\Sigma(1)} b_\rho^\sigma D_\rho.$$

By construction, $\Delta(g_\sigma) \subset P_{E_\sigma}$.

The E_σ-homogenization of $\Delta_\sigma g_\sigma$ is the polynomial $G_\sigma \in S$ given by

$$G_\sigma = \left(\prod_{\rho\in\Sigma(1)} x_\rho^{(q-1)\epsilon_\rho^\sigma}\right)\sum_{j=1}^{2}\left(\prod_{\rho\in\Sigma(1)} x_\rho^{(q-1)\langle n_j^\sigma,u_\rho\rangle} - 1\right)x_{\rho_j}\frac{\partial F}{\partial x_{\rho_j}}. \tag{9}$$

3 APPLICATION TO THE PROJECTIVE PLANE: STÖHR AND VOLOCH'S BOUND

Employing the method above on $\mathbb{P}^2$, we recover the dimension 2 case of K.O. Stöhr and F.J. Voloch's general bound [SV86]. The proof of Theorem 1 uses our tools up to (10). From there, the proof, given here for the convenience of the reader, follows Stöhr and Voloch's one in the affine case.

Let us fix F a homogeneous polynomial of degree d. Set $\sigma_0 = \mathrm{Cone}(u_1, u_2)$, $\sigma_1 = \mathrm{Cone}(u_0, u_2)$ and $\sigma_2 = \mathrm{Cone}(u_0, u_1)$ [see Figure 1a].

Let us detail the computation on the cone σ_0. We have $\sigma_0^\vee = \mathrm{Cone}(n_1^0, n_2^0)$ with $n_1^0 = (1,0)$ and $n_2^0 = (0,1)$.

j	$\langle u_i, n_1^0\rangle$	$\langle u_i, n_2^0\rangle$	$\epsilon^0_{\rho_j}$
0	-1	-1	1
1	1	0	0
2	0	1	0

Therefore (9) gives

$$\begin{aligned} G_{\sigma_0} &= x_0^{q-1}\left[\left(x_0^{-(q-1)}x_1^{q-1}-1\right)x_1\frac{\partial F}{\partial x_1}+\left(x_0^{-(q-1)}x_2^{q-1}-1\right)x_2\frac{\partial F}{\partial x_2}\right] \\ &= \left(x_1^{q-1}-x_0^{q-1}\right)x_1\frac{\partial F}{\partial x_1}+\left(x_2^{q-1}-x_0^{q-1}\right)x_2\frac{\partial F}{\partial x_2}, \end{aligned}$$

that has degree $d+q-1$. By standard Euler Identity, it can be written as follow:

$$G_{\sigma_0} = x_0^q\frac{\partial F}{\partial x_0}+x_1^q\frac{\partial F}{\partial x_1}+x_2^q\frac{\partial F}{\partial x_2}-x_0^{q-1}dF.$$

One can easily check that for $i \in \{1,2\}$, we also have

$$G_{\sigma_i} = x_0^q\frac{\partial F}{\partial x_0}+x_1^q\frac{\partial F}{\partial x_1}+x_2^q\frac{\partial F}{\partial x_2}-x_i^{q-1}dF.$$

The three polynomials given by (9) are thus all equal modulo F to $G = x_0^q F_{x_0} + x_1^q F_{x_1} + x_2^q F_{x_2}$.

Proposition 1 ([SV86]). *Let $\mathcal{C}$ be an absolutely irreducible curve of degree d in $\mathbb{P}^2$ defined over a finite field with q elements of characteristic different from 2. If there exists at least a non flex point on $\mathcal{C}$, then*

$$\mathcal{C}(\mathbb{F}_q) \le \frac{1}{2}d(d+q-1).$$

Proof. Let $F \in k[x_0,x_1,x_2]$ be a polynomial defining the curve $\mathcal{C}$. Consider the homogeneous polynomial $G \in k[x_0,x_1,x_2]$ defined by $G = x_0^q F_{x_0} + x_1^q F_{x_1} + x_2^q F_{x_2}$ and let $\mathcal{D}$ the curve defined by $G = 0$.

Let us fix $P \in \mathcal{C}(\mathbb{F}_q)$. The symmetry of G with respect to the indeterminates allows us to assume without loss of generality that $P \notin (x_2 = 0)$. In the affine chart $(x_2 \neq 0)$, the equations of $\mathcal{C}$ and $\mathcal{D}$ are $f(x,y) = 0$ and

$$h(x,y) = (x^q - x)f_x + (y^q - y)f_y + df = 0, \tag{10}$$

where $f(x,y) = F(x,y,1)$. By Lemma 1, the multiplicity of P in $\mathcal{C}\cap\mathcal{D}$ is at least 2. If F does not divide G, then $2\#C(\mathbb{F}_q) \le \mathcal{C}\cdot\mathcal{D}$, which gives the expected bound.

Let us assume that F divides G. Therefore f divides h. Differentiating the equality $h = 0$ with respect to x and y modulo f, we get

$$-f_x + (x^q - x)f_{xx} + (y^q - y)f_{xy} = 0 \tag{11}$$

$$-f_y + (x^q - x)f_{xy} + (y^q - y)f_{yy} = 0 \tag{12}$$

Replacing f_x and f_y thanks to (11) and (12) in h gives

$$(x^q - x)^2 f_{xx} + 2(x^q - x)(y^q - y)f_{xy} + (y^q - y)^2 f_{yy} = 0 \tag{13}$$

On $\mathcal{C}\cap(f_x \neq 0)$, we have $(x^q - x) = -(y^q - q)\dfrac{f_y}{f_x}$, which gives by subtituting this expression in (13)

$$\frac{(y^q-y)^2}{(f_x)^2}\left[f_{xx}\left(f_y\right)^2 - 2f_{xy}\left(f_x\right)\left(f_y\right) + f_{yy}\left(f_x\right)^2\right] = 0$$

Therefore, $f_{xx}\left(f_y\right)^2 - 2f_{xy}\left(f_x\right)\left(f_y\right) + f_{yy}\left(f_x\right)^2 = 0$ on $\mathcal{C} \cap ((f_x)(y^q - y) \neq 0)$. This implies that f divides $f_{xx}\left(f_y\right)^2 - 2f_{xy}\left(f_x\right)\left(f_y\right) + f_{yy}\left(f_x\right)^2$. By homogenizing, it means that F divides $F_{x_0x_0}(F_{x_1})^2 - 2F_{x_0x_1}F_{x_0}F_{x_1} + F_{x_1x_1}(F_{x_0})^2$. This means exactly that every point is inflectional [see [HK96] Theorem 2.5].

□

4 APPLICATION TO HIRZEBRUCH SURFACES

4.1 BACKGROUND ON HIRZEBRUCH SURFACES

Let $\eta \in \mathbb{N}$. The Hirzebruch surface $\mathcal{H}_\eta$ is the toric variety associated to the fan Σ defined by 4 rays $\rho_1, \ldots, \rho_4$ respectively spanned by the vectors $u_1 = (1,0)$, $u_2 = (0,1)$, $u_3 = (-1,\eta)$ et $u_4 = (0,-1)$.

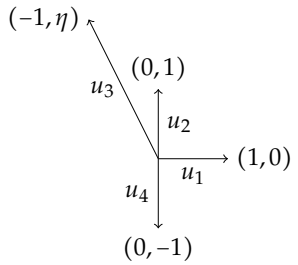


FIGURE 2. Fan Σ_η

According to the exact short sequence (3), a divisor D is principal if and only if there exists $m = (a,b) \in \mathbb{Z}^2$ such that

$$D = \sum_{i=1}^{4} \langle m, u_i \rangle D_{\rho_i} = a(D_{\rho_1} - D_{\rho_3}) + b(D_{\rho_2} + \eta D_{\rho_3} - D_{\rho_4}).$$

The divisors D_{ρ_1} and D_{ρ_2} thus form a $\mathbb{Z}$-basis of $\mathrm{Pic}(\mathcal{H}_\eta)$, with the intersection pairings

$$D_{\rho_1}^2 = 0, \quad D_{\rho_2}^2 = -\eta, \quad D_{\rho_1} \cdot D_{\rho_2} = 1. \tag{14}$$

A curve $\mathcal{C}$ is said to have *bidegree* (α,β) if $\mathcal{C}$ is linearly equivalent to $\alpha D_{\rho_1} + \beta D_{\rho_2}$. A non-zero polynomial $F \in S$ is said to have *bidegree* (α,β) if it belongs to $S_{[\alpha D_{\rho_1} + \beta D_{\rho_2}]}$, which also means that the curve defined by $F = 0$ has bidegree (α,β).

Notation 2. *The variables of S are chosen to be renamed to coincide with the Notations of Reid* [Rei97]*: $x_{\rho_1} = t_1$, $x_{\rho_2} = x_1$, $x_{\rho_3} = t_2$ and $x_{\rho_4} = x_2$.*

Let us take the group homomorphism $\phi_i : \mathrm{Cl}(X_\Sigma) \to \mathbb{Z}$ such that $\phi_i(D_{\rho_j}) = \delta_{i,j}$ for $(i,j) \in \{1,2\}^2$. Applying generalized Euler relation (Eu) with ϕ_1 and ϕ_2, for $F \in S$ of bidegree $(\alpha,\beta) \in \mathbb{Z}^2$, we have

$$t_1\frac{\partial F}{\partial t_1} + t_2\frac{\partial F}{\partial t_2} + \eta x_2\frac{\partial F}{\partial x_2} = \alpha F \tag{Eu1}$$

$$x_1\frac{\partial F}{\partial x_1} + x_2\frac{\partial F}{\partial x_2} = \beta F \tag{Eu2}$$

Finally, it is worth pointing out the essential role of Hirzeburch surfaces in the classification of rational surfaces. First, these surfaces for $\eta \neq 2$, together with $\mathbb{P}^2$ are minimal among smooth toric surfaces.

Theorem 2 ([CLS11]). *Every smooth complete toric surface is obtained from either $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1$, or $\mathcal{H}_\eta$ with $\eta \geq 2$ by a finite sequence of blowups at fixed points of the torus action.*

More generally, it is well-known that these particular surfaces are exactly the minimal rational surfaces.

4.2 COMPUTATION OF THE POLYNOMIALS G_σ

Let us fix a polynomial $F \in S$ of bidegree (α, β). Set $\sigma_i = \mathrm{Cone}(u_i, u_{i+1})$ for $i \in \{1,2,3\}$ and $\sigma_4 = \mathrm{Cone}(u_4, u_1)$. Let us compute G_{σ_i} for each $i \in \{1,\dots,4\}$. Let us denote G_{σ_i} by G_i to simplify notations. To this end, we have to compute the generating vectors n_1^i and n_2^i of the dual cone $\sigma_i^\vee$ and their scalar product with the vectors u_j in order the determine the value of ϵ_{ρ_j} for $j \in \{1,\dots,4\}$.

- Cone σ_1: $n_1^1 = (1,0)$ and $n_2^1 = (0,1)$.

j	$\langle u_i, n_1^1 \rangle$	$\langle u_i, n_2^1 \rangle$	$\epsilon_{\rho_j}^1$
1	1	0	0
2	0	1	0
3	−1	η	1
4	0	−1	1

  Then
$$\begin{aligned} E_{\sigma_1} &= \alpha D_{\rho_1} + \beta D_{\rho_2} + (q-1)(D_{\rho_3} + D_{\rho_4}) \\ &\sim (\alpha + (q-1)(\eta+1)) D_{\rho_1} + (\beta + q - 1) D_{\rho_2} \end{aligned}$$
$$G_1 = \left(t_1^{q-1} x_2^{q-1} - t_2^{q-1} x_2^{q-1}\right) t_1 F_{t_1} + \left(x_1^{q-1} t_2^{(\eta+1)(q-1)} - t_2^{q-1} x_2^{q-1}\right) x_1 F_{x_1}$$

- Cone σ_2: $n_1^2 = (\eta, 1)$ and $n_2^2 = (-1, 0)$.

j	$\langle u_i, n_1^2 \rangle$	$\langle u_i, n_2^2 \rangle$	$\epsilon_{\rho_j}^2$
1	η	−1	1
2	1	0	0
3	0	1	0
4	−1	0	1

  Then
$$E_{\sigma_2} = (\alpha + q - 1) D_{\rho_1} + \beta D_{\rho_2} + (q-1) D_{\rho_4} \sim E_{\sigma_1}$$
$$G_2 = \left(t_1^{(\eta+1)(q-1)} x_1^{q-1} - t_1^{q-1} x_2^{q-1}\right) x_1 F_{x_1} + \left(t_2^{q-1} x_2^{q-1} - t_1^{q-1} x_2^{q-1}\right) t_2 F_{t_2}$$

- Cone σ_3: $n_1^3 = (-1, 0)$ and $n_2^3 = (-\eta, -1)$.

j	$\langle u_i, n_1^3 \rangle$	$\langle u_i, n_2^3 \rangle$	$\epsilon_{\rho_j}^3$
1	−1	$-\eta$	$\begin{cases} 1 & \text{if } \eta = 0, \\ \eta & \text{if } \eta \geq 1. \end{cases}$
2	0	−1	1
3	1	0	0
4	0	1	0

  Then
$$E_{\sigma_3} = \begin{cases} (\alpha + q - 1) D_{\rho_1} + (\beta + q - 1) D_{\rho_2} \sim E_{\sigma_1} & \text{if } \eta = 0, \\ (\alpha + \eta(q-1)) D_{\rho_1} + (\beta + q - 1) D_{\rho_2} & \text{if } \eta \geq 1 \end{cases}$$

$$G_3 = \begin{cases} \left(x_1^{q-1}t_2^{q-1} - t_1^{q-1}x_1^{q-1}\right)t_2F_{t_2} + \left(t_1^{q-1}x_2^{q-1} - t_1^{q-1}x_1^{q-1}\right)x_2F_{x_2} & \text{if } \eta = 0 \\ \left(t_1^{(\eta-1)(q-1)}x_1^{q-1}t_2^{q-1} - t_1^{\eta(q-1)}x_1^{q-1}\right)t_2F_{t_2} + \left(x_2^{q-1} - t_1^{\eta(q-1)}x_1^{q-1}\right)x_2F_{x_2} & \text{if } \eta \geq 1 \end{cases}$$

- Cone σ_4: $n_1^4 = (0,-1)$ and $n_2^4 = (1,0)$.

i	$\langle u_i, n_1^4\rangle$	$\langle u_i, n_2^4\rangle$	$\epsilon^4_{\rho_i}$
1	0	1	0
2	-1	0	1
3	$-\eta$	-1	$\begin{cases} 1 & \text{if } \eta = 0, \\ \eta & \text{if } \eta \geq 1. \end{cases}$
4	1	0	0

$$E_{\sigma_4} = \begin{cases} \alpha D_{\rho_1} + (\beta+q-1)D_{\rho_2} + (q-1)D_{\rho_3} \sim E_{\sigma_1} & \text{if } \eta = 0, \\ \alpha D_{\rho_1} + (\beta+q-1)D_{\rho_2} + \eta(q-1)D_{\rho_3} \sim E_{\sigma_3} & \text{if } \eta \geq 1 \end{cases}$$

$$G_4 = \begin{cases} \left(t_2^{q-1}x_2^{q-1} - x_1^{q-1}t_2^{q-1}\right)x_2F_{x_2} + \left(t_1^{q-1}x_1^{q-1} - x_1^{q-1}t_2^{q-1}\right)t_1F_{t_1} & \text{if } \eta = 0 \\ \left(x_2^{q-1} - x_1^{q-1}t_2^{\eta(q-1)}\right)x_2F_{x_2} + \left(t_1^{q-1}x_1^{q-1}t_2^{(\eta-1)(q-1)} - x_1^{q-1}t_2^{\eta(q-1)}\right)t_1F_{t_1} & \text{if } \eta \geq 1 \end{cases}$$

In sum we have

$$G_1 = x_2^{q-1}(t_1^{q-1} - t_2^{q-1})t_1F_{t_1} + t_2^{q-1}\left(x_1^{q-1}t_2^{\eta(q-1)} - x_2^{q-1}\right)x_1F_{x_1}$$

$$G_2 = x_2^{q-1}\left(t_2^{q-1} - t_1^{q-1}\right)t_2F_{t_2} + t_1^{q-1}\left(t_1^{\eta(q-1)}x_1^{q-1} - x_2^{q-1}\right)x_1F_{x_1}$$

$$G_3 = \begin{cases} x_1^{q-1}\left(t_2^{q-1} - t_1^{q-1}\right)t_2F_{t_2} + t_1^{q-1}\left(x_2^{q-1} - x_1^{q-1}\right)x_2F_{x_2} & \text{if } \eta = 0 \\ t_1^{(\eta-1)(q-1)}x_1^{q-1}\left(t_2^{q-1} - t_1^{q-1}\right)t_2F_{t_2} + \left(x_2^{q-1} - t_1^{\eta(q-1)}x_1^{q-1}\right)x_2F_{x_2} & \text{if } \eta \geq 1 \end{cases}$$

$$G_4 = \begin{cases} x_1^{q-1}\left(t_1^{q-1} - t_2^{q-1}\right)t_1F_{t_1} + t_2^{q-1}\left(x_2^{q-1} - x_1^{q-1}\right)x_2F_{x_2} & \text{if } \eta = 0 \\ t_2^{(\eta-1)(q-1)}x_1^{q-1}\left(t_1^{q-1} - t_2^{q-1}\right)t_1F_{t_1} + \left(x_2^{q-1} - x_1^{q-1}t_2^{\eta(q-1)}\right)x_2F_{x_2} & \text{if } \eta \geq 1 \end{cases}$$

4.3 RESULT FOR $\mathcal{H}_0 \simeq \mathbb{P}^1 \times \mathbb{P}^1$

Theorem 3. *Let $\mathcal{C}$ be an absolutely irreducible curve on $\mathbb{P}^1 \times \mathbb{P}^1$ of bidegree $(\alpha,\beta) \in (\mathbb{N}^*)^2$ defined over $\mathbb{F}_q$. Then*

$$\#\mathcal{C}(\mathbb{F}_q) \leq \frac{1}{2}\mathcal{C}\cdot\left(\mathcal{C} - \frac{q}{2}K\right) = \alpha\beta + \frac{q}{2}(\alpha+\beta).$$

Proof. Let F be the equation of the curve $\mathcal{C}$. For every $i \in \{1,2\}$, set

$$H_1 = x_2^{q-1}(t_1^qF_{t_1} + t_2^qF_{t_2}) + t_2^{q-1}(x_1^qF_{x_1} + x_2^qF_{x_2}),$$
$$H_2 = x_2^{q-1}(t_1^qF_{t_1} + t_2^qF_{t_2}) + t_1^{q-1}(x_1^qF_{x_1} + x_2^qF_{x_2}).$$

Note that, using Euler relations (Eu1) and (Eu2), the difference between H_i and G_i is a multiple of F.

First let us prove that there exists $i \in \{1,2\}$ such that F does not divide H_i. On the contrary, assume that F divides H_1 and H_2. Then F divides

$$H_1 - H_2 = (t_2^{q-1} - t_1^q)(x_1^qF_{x_1} + x_2^qF_{x_2}) = \left(\prod_{\xi\in\mathbb{F}_q^\times}(t_2 - \xi t_1)\right)(x_1^qF_{x_1} + x_2^qF_{x_2}).$$

Since F is absolutely irreducible and α and β are larger than 1, this means using (Eu2) that F divides $(x_1^{q-1} - x_2^{q-1})x_1F_{x_1} = \left(\prod_{\xi\in\mathbb{F}_q}(x_1 - \xi x_2)\right)F_{x_1}$, which is impossible.

Let us assume that F does not divide H_1 and set $\mathcal{D} \subset \mathbb{P}^1 \times \mathbb{P}^1$ the curve defined by $H_1 = 0$. Using Euler relations (Eu1) and (Eu2), we clearly have $\mathcal{C}(\mathbb{F}_q) \subset \mathcal{C} \cap \mathcal{D}$. The calculations and the conclusion are the same if F does not divides H_2.

By Lemma 1, any $P \in \mathcal{C}(\mathbb{F}_q) \setminus (x_2t_2 = 0)$ the intersection multiplicity of $\mathcal{C}$ and $\mathcal{D}$ at P is at least 2. Indeed, on the affine chart $(t_2 \neq 0) \cap (x_2 \neq 0)$, setting $x = \frac{x_1}{x_2}$ and $t = \frac{t_1}{t_2}$, the curve $\mathcal{D}$ is defined by

$$h(x, y) = (t^q - t)f_t + (x^q - x)f_x,$$

where $f(x, y) = F(1, t, 1, x)$.

We thus have

$$\#\left(\mathcal{C}(\mathbb{F}_q) \cap (t_2x_2 = 0)\right) + 2\#\left(\mathcal{C}(\mathbb{F}_q) \setminus (t_2x_2 = 0)\right) \leq \mathcal{C} \cdot \mathcal{D}.$$

Note that $K \sim 2(t_2x_2 = 0)$ and $D \sim C + \frac{q-1}{2}K$. Therefore

$$2\#\mathcal{C}(\mathbb{F}_q) \leq \mathcal{C} \cdot \left(C + \frac{q}{2}K\right).$$

Since $\mathcal{C}$ et $\mathcal{D}$ do not have any common component, we get

$$2\#\mathcal{C}(\mathbb{F}_q) \leq \alpha(\beta + q - 1) + \beta(\alpha + q - 1) + (\alpha + \beta),$$

which establishes the excepted result.

□

Remark 4. *There is no geometrical reason that motivates the rewriting with respect to the canonical divisor K of $\mathcal{H}_0$. This is only possible because the sum of the two "lines" at infinity we consider happens to be equal to half of the canonical divisor. Such phemomenon does not hold on other Hirzeburch surfaces.*

4.4 Result on other Hirzebruch surfaces

As before, our study focuses on irreducible curves. Let us begin with a small observation about the bidegree and the irreducibility.

Lemma 2. *A polynomial of bidegree (α, β) such that $\alpha < \eta\beta$ is divisible by x_1.*

Proof. By definition of the bidegree, any monomial $t_1^{c_1}t_2^{c_2}x_1^{d_1}x_2^{d_2}$ of the polynomial satisfies

$$\begin{cases} c_1 + c_2 + \eta d_2 = \alpha, \\ d_1 + d_2 = \beta. \end{cases}$$

Then $c_1 + c_2 - \eta d_1 < 0$, which implies that $d_1 > 0$. □

This lemma enables us to concentrate on curves of bidegree (α, β) with $\alpha \geq \eta\beta$. Before establishing our upper bound on Hirzeburch surfaces, we need a preliminary result which guarantees that an absolutely irreducible polynomial F does not divide one of the interpolation polynomials given in Subsection 4.2.

Lemma 3. *Let $\eta \in \mathbb{N}^*$. The polynomial $A \in \mathbb{F}_q[t_1, t_2, x_1, x_2]$ defined by*

$$A(t_1, t_1, x_1, x_2) = (1 + \eta)x_2{}^{q-1} - \sum_{j=0}^{\eta} t_1{}^{(q-1)j}t_2{}^{(q-1)(\eta-j)}x_1{}^{q-1} \tag{15}$$

is a product of factors of bidegree $(1, 0)$ and $(0, 1)$ if the characteristic of the finite field $\mathbb{F}_q$ divides $\eta + 1$ and absolutely irreducible otherwise.

Proof. Let p be the characteristic of the finite field $\mathbb{F}_q$.

Assume that p divides $\eta+1$. Then $A(t_1,t_1,x_1,x_2) = -f(t_1,t_2)x_1^{q-1}$ with

$$f(t_1,t_2) = \sum_{j=0}^{\eta} t_1^{(q-1)j} t_2^{(q-1)(\eta-j)} = \frac{t_1^{(\eta+1)(q-1)} - t_2^{(\eta+1)(q-1)}}{t_1^{q-1} - t_2^{q-1}}$$

Let $N \in \mathbb{N}^*$ such that $\eta+1 = pN$. Then

$$t_1^{(\eta+1)(q-1)} - t_2^{(\eta+1)(q-1)} = \left(t_1^{N(q-1)} - t_2^{N(q-1)}\right)^p.$$

Take $\zeta \in \overline{\mathbb{F}_q}$ a primitive Nth root of unity. The polynomial f can be written as a product of factors of bidegree $(1,0)$:

$$f(t_1,t_2) = \prod_{\xi\in\mathbb{F}_q^*} \left((t_1 - \xi t_2)^{p-1} \prod_{j=1}^{N-1} (t_1 - \zeta^j \xi t_2)^p \right),$$

which proves that A is a product of factors of bidegree $(1,0)$ and $(0,1)$.

Assume that p does not divide $\eta+1$. The polynomial A is irreducible if and only if the polynomial $a \in k[t,x]$ defined by

$$a(t,x) = A(t,1,1,x) = (1+\eta)x^{q-1} - f(t), \text{ with } f(t) = \sum_{j=0}^{\eta} t^{(q-1)j},$$

is irreducible. Since $\gcd(\eta+1,p) = 1$, the polynomial f is separable:

$$f(t) = \prod_{\xi\in\mathbb{F}_q^*} \prod_{j=1}^{\eta} (t - \omega^j \xi)$$

where $\omega \in \overline{\mathbb{F}_q}$ is a primitive $(\eta+1)$th root of unity. Eisenstein's criterion applied with any of this linear factor to $a \in k[t][x]$ ensures that a is irreducible.

□

Remark 5. *Using that for any $\xi \in \mathbb{F}_q^*$, $\xi^{q-1} = 1$, the number of $\mathbb{F}_q$-points of the curve $\mathcal{C}_A$ defined by $A = 0$ is easily computed. The orbit of a rational point of the Hirzebruch surface $\mathcal{H}_\eta$ contains exactly one point of following form: $(a,1,b,1)$, $(a,1,1,0)$, $(1,0,b,1)$ with $(a,b) \in \mathbb{F}_q^2$ and $(1,0,1,0)$. Set p the characteristic of the finite field $\mathbb{F}_q$.*

One can effortless check that the polynomial vanishes at a point of type $(a,1,b,1)$ with $(a,b) \in (\mathbb{F}_q^*)^2$. If p divides $\eta+1$, it is true for $(a,b) \in \mathbb{F}_q^* \times \mathbb{F}_q$.

Concerning points of type $(a,1,1,0)$ with $a \in \mathbb{F}_q$, the polynomial A vanishes at every of them if p divides $\eta+1$. Otherwise, the polynomial A does not vanish at any of these point.

The polynomial is zero at points of type $(1,0,b,1)$ for $b \in \mathbb{F}_q^*$ if and only if p divides η. It is zero at $(1,0,0,1)$ if and only if $p \mid \eta+1$. Finally, the polynomial A never vanishes at $(1,0,1,0)$.

In sum, we have

$$\#\mathcal{C}_A(\mathbb{F}_q) = \begin{cases} q^2 & \text{if } p \nmid \eta+1, \\ q(q-1) & \text{if } p \nmid \eta, \\ (q-1)^2 & \text{otherwise.} \end{cases}$$

Theorem 4. *Let $\eta \in \mathbb{N}^*$. Let $\mathcal{C}$ be an absolutely irreducible curve of the Hirzebruch surface $\mathcal{H}_\eta$ of bidegree $(\alpha,\beta) \in (\mathbb{N}^*)^2$ defined over the finite field $\mathbb{F}_q$. Then*

$$\#\mathcal{C}(\mathbb{F}_q) \le \frac{\beta}{2}(2\alpha - \eta\beta - \eta + 1) + \frac{q}{2}(\alpha+\beta).$$

Proof. Let F be an equation of the curve $\mathcal{C}$. We consider the polynomials

$$G_1 = x_2^{q-1}(t_1^{q-1} - t_2^{q-1})t_1F_{t_1} + t_2^{q-1}\left(x_1^{q-1}t_2^{\eta(q-1)} - x_2^{q-1}\right)x_1F_{x_1},$$
$$G_2 = x_2^{q-1}\left(t_2^{q-1} - t_1^{q-1}\right)t_2F_{t_2} + t_1^{q-1}\left(t_1^{\eta(q-1)}x_1^{q-1} - x_2^{q-1}\right)x_1F_{x_1}.$$

We begin by proving that there exists $i \in \{1,2\}$, such that G_i is not divisible by F. Assume the contrary. Then, using F divides the polynomial

$$\begin{aligned} G_1 - G_2 =& x_2^{q-1}\left(t_1^{q-1} - t_2^{q-1}\right)\left(t_1F_{t_1} + t_2F_{t_2}\right) \\ &+ \left[\left(t_2^{(\eta+1)(q-1)} - t_1^{(\eta+1)(q-1)}\right)x_1^{q-1} + \left(t_1^{q-1} - t_2^{q-1}\right)x_2^{q-1}\right]x_1F_{x_1} \end{aligned}$$

and so, using Euler relations (Eu1) and (Eu2), it also divides

$$x_1F_{x_1}\left[(1+\eta)\left(t_1^{q-1} - t_2^{q-1}\right)x_2^{q-1} - \left(t_1^{(\eta+1)(q-1)} - t_2^{(\eta+1)(q-1)}\right)x_1^{q-1}\right],$$

which can be factorized as $x_1F_{x_1}\left(t_1^{q-1} - t_2^{q-1}\right)A(t_1,t_1,x_1,x_2)$ where A is defined in Equation 15.

Since the polynomial F is absolutely irreducible, it is coprime with its derivative F_{x_1}. By Lemma 2, we have $\alpha \geq \eta\beta \geq 1$, which implies F is coprime with x_1 and $\left(t_1^{q-1} - t_2^{q-1}\right)$ of bidegree $(q-1,0)$. Finally, unless $F = A$, Lemma 3 entails that F does not divide A, which arises a contradiction.

If $F = A$, one can easily verify that the bound we aim to prove is larger than the exact number of points of $\mathcal{C}_A$ given in Remark 5.

Now, let us assume that F does not divide

$$G_1 = x_2^{q-1}(t_1^{q-1} - t_2^{q-1})t_1F_{t_1} + t_2^{q-1}\left(x_1^{q-1}t_2^{\eta(q-1)} - x_2^{q-1}\right)x_1F_{x_1}.$$

Set $\mathcal{D} \sim (\alpha + (q-1)(\eta+1))D_{\rho_1} + (\beta + q - 1)D_{\rho_2}$ the curve defined by $G_1 = 0$.

First, let us check that $\mathcal{C}(\mathbb{F}_q) \setminus (t_2 = 0) \subset \mathcal{C} \cap \mathcal{D}$.

Any $\mathbb{F}_q$-point $p = (t_1(p), t_2(p), x_1(p), x_2(p))$ of $\mathcal{C}$ such that $t_2(p) \neq 0$ is obviously a zero of the first term of G_1. It is also clear that it is a zero of the second term if $x_2(p) \neq 0$. If $x_2(p) = 0$ then $x_1 \neq 0$ and, using (Eu2), we can deduce that $F_{x_1}(p) = 0$, which guarantees that the second term also vanishes at p.

Second, let us prove that for any point $p \in \mathcal{C}(\mathbb{F}_q) \setminus (t_2x_1 = 0)$, the intersection multiplicity of $\mathcal{C}$ and $\mathcal{D}$ at p is at least 2.

On the affine chart $(t_2 \neq 0) \cap (x_1 \neq 0)$, the curve $\mathcal{D}$ is defined by the polynomial

$$g(t,x) = (t^q - t)f_t + (x^q - x)f_x$$

where f is the equation of $\mathcal{C}$ in this affine open set. Using Lemma 1, we thus get

$$\#\left(\mathcal{C}(\mathbb{F}_q) \cap (x_1 = 0)\right) + 2\#\left(\mathcal{C}(\mathbb{F}_q) \setminus (t_2x_1 = 0)\right) \leq \mathcal{C} \cdot \mathcal{D},$$

which can be written

$$2\#\mathcal{C}(\mathbb{F}_q) \leq \mathcal{C} \cdot (\mathcal{D} + (x_1 = 0) + 2(t_2 = 0)).$$

It remains to compute the right handside. Knowing that $(x_1 = 0) = D_{\rho_2}$ and $(t_2 = 0) = D_{\rho_3} \sim D_{\rho_1}$, we get

$$\begin{aligned} 2\#\mathcal{C}(\mathbb{F}_q) &\leq \left(\alpha D_{\rho_1} + \beta D_{\rho_2}\right) \cdot \left((\alpha + (q-1)(\eta+1) + 2)D_{\rho_1} + (\beta + q)D_{\rho_2}\right) \\ &= \alpha(\beta + q) + \beta(\alpha + (q-1)(\eta+1) + 2) - \eta\beta(\beta + q) \\ &= \beta(2\alpha - \eta\beta - \eta + 1) + q(\alpha + \beta) \end{aligned}$$

□

4.5 COMPARISON WITH EXISTING BOUNDS

The linear system associated to the divisor $D = D_{\rho_3} + D_{\rho_4} \sim (\eta+1)D_{\rho_1} + D_{\rho_2}$ is very ample on the surface $\mathcal{H}_\eta$ of dimension $\#P_D \cap \mathbb{Z}^2$ by (4), where

$$P_D = \{(a,b) \in \mathbb{R}^2 \,|\, 0 \le a \le \eta b + 1 \text{ and } 0 \le b \le 1\}.$$

Then $\#P_D \cap \mathbb{Z}^2 = \eta + 3$. The linear system associated to the divisor $D = \big((\eta+1)D_{\rho_1} + D_{\rho_2}\big)$ is thus very ample on $\mathcal{H}_\eta$ and gives a closed immersion $\varphi_D : \mathcal{H}_\eta \to \mathbb{P}^{\eta+3}$. For $\eta = 0$, this immersion is nothing but the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ into $\mathbb{P}^3$.

Let C be a curve of bidegree (α, β) on $\mathcal{H}_\eta$. By the Adjunction formula, we have $2g(C) - 2 = C \cdot (K + C)$, where K is the canonical divisor of $\mathcal{H}_\eta$. Since $K = -\sum_{i=1}^4 D_{\rho_i} \sim -(2+\eta)D_{\rho_1} - 2D_{\rho_2}$, we have

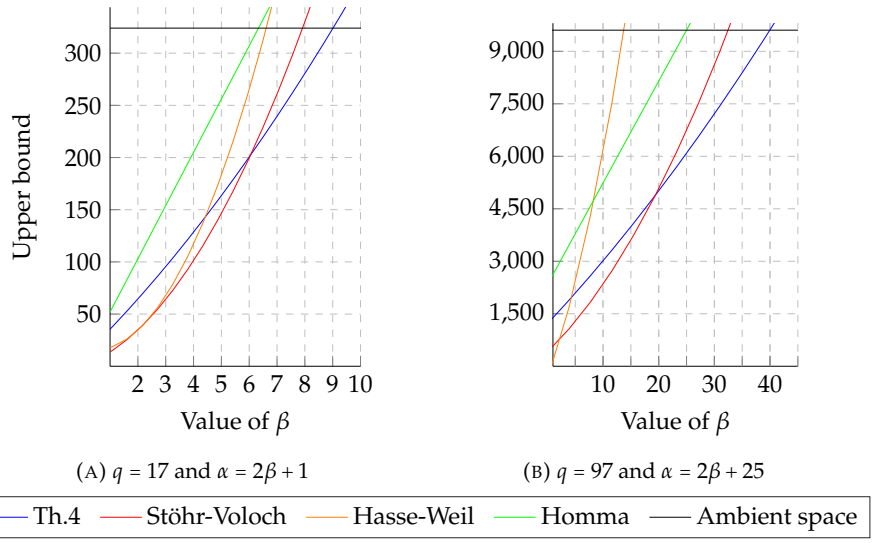
$$\begin{aligned} 2g(C) - 2 &= (\alpha D_{\rho_1} + \beta D_{\rho_2}) \cdot \big((\alpha - 2 - \eta)D_{\rho_1} + (\beta - 2)D_{\rho_2}\big) \\ &= \alpha(\beta - 2) + \beta(\alpha - 2 - \eta) - \eta\beta(\beta - 2) \\ &= 2(\alpha - 1)(\beta - 1) - \eta\beta(\beta - 1) - 2, \end{aligned}$$

which gives $g(C) = (\beta - 1)\left(\alpha - 1 - \dfrac{\eta\beta}{2}\right)$. Unless $\alpha \le \eta + 1$ and $\beta \le 1$, the curve $\varphi(C)$ does not lie on a hyperplane. Moreover it has degree $C \cdot D = \alpha + \beta$.

If the curve C is Frobenius-classical, K.O. Stöhr and F.J. Voloch [SV86] state that

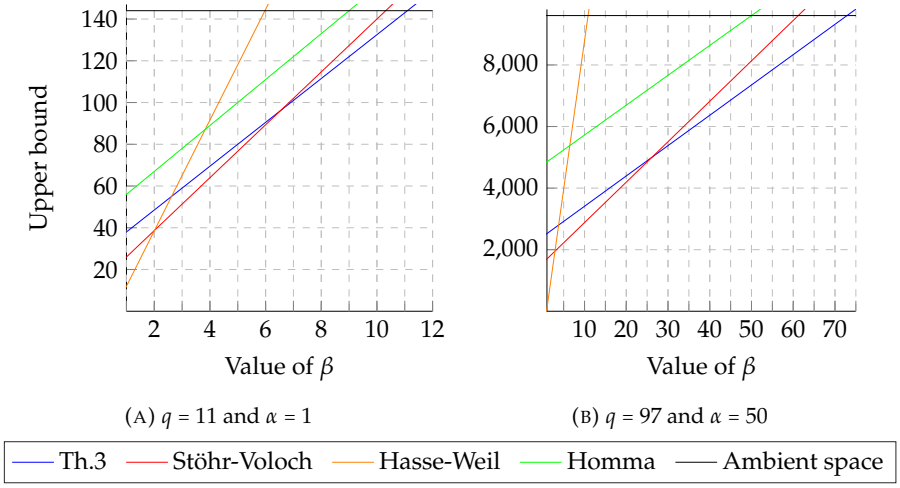
$$\#C(\mathbb{F}_q) \le (\eta+2)(g-1) + \frac{q+\eta+3}{\eta+3}(\alpha+\beta).$$

A sufficient condition for $\varphi(C)$ to be Frobenius-classical is $\deg(\phi(C)) = \alpha + \beta \le p$ where p is the characteristic of the finite field $\mathbb{F}_q$. If the curve is not Frobenius-classical, the coefficient of the genus g is greater than $\eta + 2$ and the upper bound grows.



(A) $q = 17$ and $\alpha = 2\beta + 1$ (B) $q = 97$ and $\alpha = 2\beta + 25$

FIGURE 3. Comparison of bounds on the number of $\mathbb{F}_q$-points on a curve on $\mathcal{H}_2$ of bidegree (α, β)



(A) $q = 11$ and $\alpha = 1$ (B) $q = 97$ and $\alpha = 50$

FIGURE 4. Comparison of bounds on the number of $\mathbb{F}_q$-points on a curve on $\mathbb{P}^1 \times \mathbb{P}^1$ of bidegree (α, β)

As displayed in Figures 3 and 4, the upper bounds given by Theorems 3 and 4 are sharper than the pre-existing ones for large bidegrees. It happens that previous bounds turn to be larger than the number of $\mathbb{F}_q$-points of $\mathcal{H}_\eta$, that equals to $(q+1)^2$ and is represented by the horizontal line labelled "Ambient space", whereas our bound is below this number.

5 WHAT'S NEXT?

The present work only studies curves on the projective plane or on a Hirzeburch surface. Although all the needed method to get a similar result on some other toric surfaces is detailed in Section 2, such idea does not seem to be fruitful, due to Theorem 2. The bound obtained from our method applied to a non minimal surface seems to be looser than the one deduced from the bound on the minimal surface it comes from and rough majorizations via multiplicities under blowups.

Let us take the example of the Hirzeburch surface $\mathcal{H}_1$, which is the blowup of $\mathbb{P}^2$. An irreducible curve on $\mathcal{H}_1$ is either the strict transform of an irreducible curve on $\mathbb{P}^2$ or the exceptional divisor D_{ρ_2}. The assumption on α and β forces a curve C to which Theorem 4 applies to be the strict transform of a plane projective curve C_0. More precisely, if C_0 has degree d and multiplicity m at the blown up point ($m < d$), then C has bidegree $(d, d-m)$.

Therefore, a naive upper bound from Proposition 1 is

$$\#C(\mathbb{F}_q) \leq \frac{d}{2}(d+q-1) + m - 1.$$

Proposition 4 gives $\#C(\mathbb{F}_q) \leq \frac{1}{2}(d^2 - m^2 + 2dq - mq)$. A simple computation shows that the latter quantity is lesser than the first one if $d + q + 2 \leq d - 1$, which never happens. Nevertheless, the bound given by Proposition 4 holds without assumption of the existence of a non-inflectional point.

On the bright side, our method can applied to singular toric surfaces. It also can easily be extended to higher-dimensional varieties. Given an hypersurface of a toric variety, we can compute an interpolation polynomial that vanishes on $\mathbb{F}_q$-points of the hypersurface on each toric affine open set. Our routine can also be adapted to homogenize higher-degree interpolation polynomials, as the ones used by F. Voloch to upperbond the number of $\mathbb{F}_q$-points lying on a surface in $\mathbb{P}^3$ [Vol03].

REFERENCES

[CD97] Eduardo Cattani and Alicia Dickenstein. A global view of residues in the torus. *J. Pure Appl. Algebra*, 117/118:119–144, 1997. Algorithms for algebra (Eindhoven, 1996).

[CD13] Alain Couvreur and Iwan Duursma. Evaluation codes from smooth quadric surfaces and twisted Segre varieties. *Des. Codes Cryptogr.*, 66(1-3):291–303, 2013.

[CLS11] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.

[CN16] Cicero Carvalho and Victor G. L. Neumann. Projective Reed-Muller type codes on rational normal scrolls. *Finite Fields Appl.*, 37:85–107, 2016.

[Ful89] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[HK96] Abramo Hefez and Neuza Kakuta. Polar curves. *J. Algebra*, 181(2):449–477, 1996.

[HK09] Masaaki Homma and Seon Jeong Kim. Around Sziklai's conjecture on the number of points of a plane curve over a finite field. *Finite Fields Appl.*, 15(4):468–474, 2009.

[HK10a] Masaaki Homma and Seon Jeong Kim. Sziklai's conjecture on the number of points of a plane curve over a finite field II. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, pages 225–234. Amer. Math. Soc., Providence, RI, 2010.

[HK10b] Masaaki Homma and Seon Jeong Kim. Sziklai's conjecture on the number of points of a plane curve over a finite field III. *Finite Fields Appl.*, 16(5):315–319, 2010.

[Hom12] Masaaki Homma. A bound on the number of points of a curve in a projective space over a finite field. In *Theory and applications of finite fields*, volume 579 of *Contemp. Math.*, pages 103–110. Amer. Math. Soc., Providence, RI, 2012.

[Nar18] Jade Nardi. Algebraic geometric codes on minimal hirzebruch surfaces. 2018. `https://arxiv.org/abs/1801.08407`.

[Rei97] Miles Reid. Chapters on algebraic surfaces. In *Complex algebraic geometry (Park City, UT, 1993)*, volume 3 of *IAS/Park City Math. Ser.*, pages 3–159. Amer. Math. Soc., Providence, RI, 1997.

[SV86] Karl-Otto Stöhr and José Felipe Voloch. Weierstrass points and curves over finite fields. *Proc. London Math. Soc. (3)*, 52(1):1–19, 1986.

[Vol03] José Felipe Voloch. Surfaces in $\mathbf{P}^3$ over finite fields. In *Topics in algebraic and noncommutative geometry (Luminy/Annapolis, MD, 2001)*, volume 324 of *Contemp. Math.*, pages 219–226. Amer. Math. Soc., Providence, RI, 2003.

E-mail address: `jade.nardi@math.univ-toulouse.fr`

INSTITUT DE MATHÉMATIQUES DE TOULOUSE ; UMR 5219, UNIVERSITÉ DE TOULOUSE ; CNRS UPS IMT, F-31062 TOULOUSE CEDEX 9, FRANCE

Chapitre 5

Codes liftés à poids : correctibilité locale et application à un protocole de PIR robuste

Weighted Lifted Codes: Local Correctabilities and Application to Robust Private Information Retrieval

Julien Lavauzelle* Jade Nardi†

May 27, 2019

Abstract

Low degree Reed-Muller codes are known to satisfy local decoding properties which find applications in private information retrieval (PIR) protocols, for instance. However, their practical instantiation encounters a first barrier due to their poor information rate in the low degree regime. This lead the community to design codes with similar local properties but larger dimension, namely the lifted Reed-Solomon codes.

However, a second practical barrier appears when one requires that the PIR protocol resists collusions of servers. In this paper, we propose a solution to this problem by considering *weighted* Reed-Muller codes. We prove that such codes allow us to build PIR protocols with optimal computation complexity and resisting to a small number of colluding servers.

In order to improve the dimension of the codes, we then introduce an analogue of the lifting process for weigthed degrees. With a careful analysis of their degree sets, we notably show that the weighted lifting of Reed-Solomon codes produces families of codes with remarkable asymptotic parameters.

1 Introduction

1.1 Weighted Reed-Muller codes

Weighted Reed-Muller codes were introduced by Sørensen in 1992, as a generalisation of Reed-Muller codes in the context of weighted polynomial rings [Sør92]. Formally, given a finite field $\mathbb{F}_q$, a *weight* $\omega = (\omega_1, \ldots, \omega_m) \in (\mathbb{N}^*)^m$ and a polynomial

$$P(X_1, \ldots, X_m) = \sum_{\boldsymbol{i}=(i_1,\ldots,i_m)\in I} p_{\boldsymbol{i}} X^{i_1} \ldots X^{i_m} \in \mathbb{F}_q[X_1, \ldots, X_m],$$

*IRMAR - UMR CNRS 6625, Université de Rennes 1, France. Email: julien.lavauzelle@univ-rennes1.fr

†Institut de Mathématiques de Toulouse ; UMR 5219, Université de Toulouse ; CNRS UPS IMT, F-31062 Toulouse Cedex 9, France. Email: jade.nardi@math.univ-toulouse.fr

the weighted degree of P with respect to ω is

$$\mathrm{wdeg}_\omega(P) := \max\left\{\sum_{j=1}^{m} \omega_j i_j \mid \boldsymbol{i} = (i_1, \ldots, i_m) \in I \text{ and } p_{\boldsymbol{i}} \neq 0\right\}.$$

In particular, if $\omega = (1, \ldots, 1)$, then we get the usual notion of total degree for multivariate polynomials.

In order to build codes from subspaces of polynomials, we consider the evaluation map

$$\begin{array}{rccc} \mathrm{ev}_{\mathbb{F}_q^m}: & \mathbb{F}_q[X_1, \ldots, X_m] & \to & \mathbb{F}_q^{q^m} \\ & P(x_1, \ldots, x_m) & \mapsto & (P(x_1, \ldots, x_m), \boldsymbol{x} = (x_1, \ldots, x_m) \in \mathbb{F}_q^m) \end{array}$$

Then, a weighted Reed-Muller code is defined as the image by $\mathrm{ev}_{\mathbb{F}_q^m}$ of a subspace of polynomials whose weighted degree is bounded by some integer d.

Definition 1.1 (Weighted Reed-Muller code)**.** Let $m \geq 1$, $\omega \in (\mathbb{N}^*)^m$ and $d \in \mathbb{N}$. The *weighted (affine) Reed-Muller code* of order m, degree d and weight ω is:

$$\mathrm{WRM}_q^\omega(d) = \{\mathrm{ev}_{\mathbb{F}_q^m}(P), P \in \mathbb{F}_q[X_1, \ldots, X_m], \mathrm{wdeg}_\omega(P) \leq d\}.$$

Note that weighted Reed-Muller codes are generalised Goppa codes on the weighted projective space $\mathbb{P}(1, \omega_1, \ldots, \omega_m)$ with evaluation points outside the line at infinity $X_0 = 0$.

The dimension of weighted Reed-Muller codes, as well as bounds on the minimum distance, are given by Sørensen in his seminal paper [Sør92]. Notice that these parameters are also analysed in a recent work [ACG+17] by Aubry, Castryck, Ghorpade, Lachaud, O'Sullivan, and Ram, who also describe minimum weight codewords with geometric techniques. Geil and Thomsen [GT13] finally proved that weighted Reed-Muller codes are efficiently decodable up to half their minimum distance, notably using an embedding of weighted Reed-Muller codes into Reed-Solomon codes.

1.2 Technical overview and organisation

In this work, we will only focus on the case where $m = 2$ and ω is of the form $\omega = (1, \eta)$ where $\eta \geq 1$. This setting seems very restrictive, but it is the most promising in terms of parameters (see for instance [Sør92, GT13]) and it also finds a practical application in private information retrieval protocols. For simplicity, we will use the shorter notation $\mathrm{WRM}_q^\eta(d)$ for $\mathrm{WRM}_q^{(1,\eta)}(d)$.

Our first observation is that, when $d \leq q - 1$, the evaluation map $\mathrm{ev}_{\mathbb{F}_q^2}$ is injective. This has two major consequences: (i) the code and its parameters are easier to describe and (ii) puncturing the code on "lines of weighted degree η" leads to highly-sound local correction. More precisely, in Section 2 we prove the following result.

Theorem 1.2 (informal)**.** *Let $\eta \geq 1$, q be a prime power and $\gamma \in (0, 1)$. For a fixed $\delta \in (0, 1)$ small enough, the family of weighted Reed-Muller codes $\mathrm{WRM}_q^\eta(\lfloor \gamma q \rfloor)$ are $(q - 1, \delta, \varepsilon)$-locally correctable, where $\varepsilon = O_\gamma(\delta)$.*

This result is obtained thanks to the following fact. Let $\phi(T) \in \mathbb{F}_q[T]$ be a univariate polynomial of (non-weighted) degree bounded by η, and let $L = ((t, \phi(t)), t \in \mathbb{F}_q) \subset \mathbb{F}_q^2$. Then for every $\boldsymbol{c} = \mathrm{ev}_{\mathbb{F}_q^2}(f(X,Y)) \in \mathrm{WRM}_q^\eta(d)$, the restriction $\boldsymbol{c}_{|L}$ of the vector $\boldsymbol{c}$ to the coordinates indexed by elements of L is a codeword of a Reed-Solomon code of degree d. Hence, if the codeword $\boldsymbol{c}$ is corrupted with a constant fraction of errors, picking ϕ at random and correcting $\boldsymbol{c}_{|L}$ succeeds with constant probability. As a consequence, it allows us to retrieve some symbols of the corrupted codeword in sublinear query complexity.

However, results described above do not improve the related "local decoding on curves" technique, described for instance by Yekhanin in his survey [Yek12]. Fortunately, local correctabilities of weighted Reed-Muller codes can be applied to private information retrieval protocols in order to resist collusion of servers. In particular, we prove that any weighted Reed-Muller code $\mathrm{WRM}_q^\eta(d)$ induces a private information retrieval protocol for databases of $\simeq q^2/2\eta$ entries, requiring a minimal computation complexity for the q servers, and remaining private against any collusion of η servers. We refer the reader to Section 3 for more details.

One should notice that the maximal number of entries in the database is directly given by the dimension of $\mathrm{WRM}_q^\eta(d)$. Unfortunately, the information rate of such codes remains bounded by $1/2\eta$ as long as $d \leq q-1$, a constraint which is necessary in our context. Therefore, following the seminal paper of Guo, Kopparty and Sudan [GKS13] and subsequent works [Guo16, Lav18b], we initiate the study of a *weighted lifting* of Reed-Solomon codes in order to produce codes with the same local properties as weighted Reed-Muller codes, but with a much larger dimension.

Definitions and essential properties of *weighted lifted codes* are given in Section 4. Similarly to the constructions of lifted (affine [GKS13] and projective [Lav18b]) Reed-Solomon codes and lifted Hermitian codes [Guo16], we also prove that for fixed η and $q \to \infty$, weighted lifts of Reed-Solomon codes are locally correctable with (i) a non-zero asymptotic information rate in the context of errors with constant relative weight, or (ii) an information rate arbitrary close to 1 when errors have smaller weight.

These two results are the main technical outcomes of the paper, and we present them in Section 5. They are obtained after a precise analysis of so-called *degree sets* of weighted Reed-Muller and lifted codes, which represent the sets of exponents of monomials spanning the codes. We finally provide numerical computations of dimensions of weighted lifted codes, which illustrate the improvement of weighted lifted codes over weighted Reed-Muller codes, and their practical useability in private information retrieval.

2 Local correction of weighted Reed-Muller codes

2.1 Restricting Reed-Muller codes to weighted lines

The local decoding properties of Reed-Muller codes come from the restriction of their codewords on a line being Reed-Solomon codewords. Expecting similar properties on weighted Reed-Muller codes, we have to find what will play the part of the lines in $\mathbb{P}(1,1,\eta)$.

Definition 2.1 (η-line on $\mathbb{P}(1,1,\eta)$)**.** Let $\eta \geq 1$. We call a (non-vertical) *η-line* on $\mathbb{P}(1,1,\eta)$ the set of zeroes of the polynomial $P(X_0,X_1,X_2) = X_2 - \phi(X_0,X_1)$ where $\phi \in \mathbb{F}_q[X_0,X_1]$ is homogeneous of degree η.

Since we evaluate polynomials only at points outside the line $X_0 = 0$, we shall define an η-line on the affine plane $\mathbb{A}^2$, viewed as the domain $X_0 \neq 0$, as the intersection of an η-line on $\mathbb{P}(1,1,\eta)$ and $X_0 \neq 0$.

Definition 2.2 (affine η-line)**.** Let $\eta \geq 1$. We call a (non-vertical) *η-line* on $\mathbb{A}^2$ the set of zeroes of a bivariate polynomial $P(X,Y) = Y - \phi(X)$, where $\phi \in \mathbb{F}_q[X]$ and $\deg\phi \leq \eta$.

Let us remark that if $P = Y - \phi(X)$ defines an η-line, then $\mathrm{wdeg}_\eta(P) \leq \eta$. The converse is not true, since we removed from the definition collections of "vertical lines" defined by $\phi(X) = 0$, $\deg\phi \leq \eta$.

An η-line can be parametrized by $t \mapsto (t,\phi(t))$. We thus define

$$\Phi_\eta = \{L_\phi : t \mapsto (t,\phi(t)) \mid \phi \in \mathbb{F}_q[T] \text{ and } \deg\phi \leq \eta\},$$

the set of embeddings of η-lines into the affine plane $\mathbb{A}^2 = \overline{\mathbb{F}_q}^2$. These embeddings are very useful when trying to characterise restrictions of weighted Reed-Muller codes to η-lines.

Proposition 2.3. *Any polynomial $f \in \mathbb{F}_q[X,Y]$ whose evaluation over $\mathbb{F}_q^2$ lies in $\mathrm{WRM}_q^\eta(d)$ satisfies $\mathrm{ev}_{\mathbb{F}_q}(f \circ L) \in \mathrm{RS}_q(d)$ for any $L \in \Phi_\eta$.*

Proof. It is sufficient to check the result on monomials. Let $f = X^iY^j$ where $i + \eta j \leq d$. For every $\phi \in \Phi_\eta$, the univariate polynomial $(f \circ L_\phi)(T) = T^i\phi(T)^j$ has degree less than d. □

2.2 Local correction

Local decoding was introduced by Katz and Trevisan [KT00] in order to characterise codes allowing to (probabistically) retrieve a message coordinate with a sublinear number of queries in the code length n. The difficulty comes from the fact that the retrieval must succeed with non-negligeable probability for *every* codeword which is corrupted by *any* possible error whose weight is bounded by a linear function in n. Local correction is very similar to local decoding, the only difference being that one requires that any coordinate of the *codeword* can be retrieved.

Before giving a formal definition of this notion, let us introduce some notation. We denote the Hamming distance between two vectors $\boldsymbol{x},\boldsymbol{y}$ by $d_H(\boldsymbol{x},\boldsymbol{y})$. The weight of $\boldsymbol{x}$ is $\mathrm{wt}(\boldsymbol{x}) \coloneqq d_H(\boldsymbol{x},\boldsymbol{0})$. An *erasure* is a symbol of a word that one knows to be erroneous. Finally, we denote[1] the full-length Reed-Solomon code by

$$\mathrm{RS}_q(d) \coloneqq \{\mathrm{ev}_{\mathbb{F}_q}(f), f \in \mathbb{F}_q[T], \deg(f) \leq d\},$$

and we recall that $\mathrm{RS}_q(d)$ can correct efficiently 1 erasure and up to $\lfloor \frac{n-d}{2} \rfloor$ errors.

[1] take care that this notation (with $\leq d$ instead of $< k$) is not the most currently used, but remains very convenient for our work

Definition 2.4 (locally correctable code)**.** Let $1 \leq \ell \leq k \leq n$, and $\delta, \varepsilon > 0$. A code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is said $(\ell, \delta, \varepsilon)$-locally correctable if there exists a probabilitic algorithm $\mathrm{Dec} : [1, n] \to \mathbb{F}_q$ such that the following holds. For every $1 \leq i \leq n$ and for every $\boldsymbol{y} \in \mathbb{F}_q^n$ such that $d_H(\boldsymbol{y}, \boldsymbol{c}) \leq \delta n$ for some $\boldsymbol{c} \in \mathcal{C}$, we have:

- the probability[2] that $\mathrm{Dec}(i)$ outputs c_i is larger than $1 - \varepsilon$;
- $\mathrm{Dec}(i)$ reads at most ℓ coordinates of $\boldsymbol{y}$.

Similarly to the case of classical Reed-Muller codes and codes derived from those, weighted Reed-Muller codes can be locally corrected using their restrictions to "lines". For simplicity, we see a vector $\boldsymbol{y} \in \mathbb{F}_q^{q^2}$ as a map $\mathbb{F}_q^2 \to \mathbb{F}_q$, using the bijection between $[1, q^2]$ and $\mathbb{F}_q^2$ given by the evaluation map. Similarly, $\boldsymbol{a} \in \mathbb{F}_q^q$ is seen as a map $\mathbb{F}_q \to \mathbb{F}_q$. One obtains the local correction procedure described in Algorithm 1.

Algorithm 1: A local correction algorithm Dec for the weighted Reed-Muller code $\mathrm{WRM}_q^\eta(d)$.

Input: A coordinate $\boldsymbol{x} = (x_1, x_2) \in \mathbb{F}_q^2$ where to decode, and a oracle access to a word $\boldsymbol{y} : \mathbb{F}_q^2 \to \mathbb{F}_q$, where $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$, $\boldsymbol{c} \in \mathcal{C}$, and $\mathrm{wt}(\boldsymbol{e}) \leq \delta q^2$.

Output: The symbol $c_{\boldsymbol{x}}$, with high probability.

1 Pick at random an η-line $L \in \Phi_\eta$ such that $L(t_0) = \boldsymbol{x}$ for some $t_0 \in \mathbb{F}_q$.
2 Define $S = L(\mathbb{F}_q)$ and $\boldsymbol{z} = \boldsymbol{y}_{|S} : \mathbb{F}_q \mapsto \mathbb{F}_q$.
3 Consider z_{t_0} as an erasure, and decode $\boldsymbol{z}$ in the Reed-Solomon code $\mathrm{RS}_q(d+1)$, giving a corrected codeword $\tilde{\boldsymbol{z}}$.
4 Output the corrected value $\tilde{z}_{t_0}$.

According to Katz and Trevisan's terminology [KT00], Algorithm 1 is not *perfectly smooth*, in the sense that the coordinate $y_{\boldsymbol{x}}$ is never queried. nevertheless, it can be made smooth following techniques described in [Lav18a, Chapter 2].

Theorem 2.5. *Let $\eta \geq 1$, q be a prime power, and $\gamma \in (0, 1)$ such that $q - \lfloor \gamma q \rfloor$ is even. For every $\delta \leq \frac{1-\gamma}{4}$, the weighted Reed-Muller code $\mathrm{WRM}_q^\eta(\lfloor \gamma q \rfloor)$ is $(q - 1, \delta, \varepsilon)$-locally correctable where $\varepsilon \leq \frac{2}{1-\gamma}\delta$.*

Proof. Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} : \mathbb{F}_q^2 \to \mathbb{F}_q$ be a corrupted codeword, where $\boldsymbol{c} \in \mathrm{WRM}_q^\eta(d)$ and $\mathrm{wt}(\boldsymbol{e}) \leq \delta q^2$. We define $E = \{\boldsymbol{x} \in \mathbb{F}_q^2 \mid e_{\boldsymbol{x}} \neq 0\}$ the support of $\boldsymbol{e}$. The random variable representing the set of queries addressed by the local decoder is denoted by $A_{\boldsymbol{x}}$. It is clear that the algorithm succeeds if $|A_{\boldsymbol{x}} \cap E| \leq w$, where $w = \frac{q - \lfloor \gamma q \rfloor}{2} - 1$, since a Reed-Solomon of dimension $\lfloor \gamma q \rfloor + 1$ can decode up to 1 erasure and w errors. Using Markov's inequality, the probability p of success of Algorithm 1 satisfies:

$$p \geq 1 - \mathbb{P}(|A_{\boldsymbol{x}} \cap E| \geq w + 1) \geq 1 - \frac{\mathbb{E}(|A_{\boldsymbol{x}} \cap E|)}{w + 1}.$$

[2] taken over the internal randomness of the decoder Dec

Moreover, for every $\boldsymbol{a} \in \mathbb{F}_q^2$, we have $\mathbb{P}(\boldsymbol{a} \in A_x) \leq \frac{q-1}{q^2-1}$. Hence,

$$\mathbb{E}(|A_x \cap E|) = \sum_{\boldsymbol{a} \in E} \mathbb{P}(\boldsymbol{a} \in A_x) \leq \delta q^2 \cdot \frac{q-1}{q^2-1} \leq \delta q \,.$$

Finally we get

$$p \geq 1 - \frac{4\delta q}{q - \lfloor \gamma q \rfloor} \geq 1 - \frac{2\delta}{1-\gamma} \,.$$

□

Remark 2.6. If $\eta \geq 2$, it is possible to get a sharper bound for the probability p of success of Algorithm 1. Using Chebyshev's inequality (quite similarly to [Lav18a, Proposition 2.36]), one can indeed prove that $p \geq 1 - \mathcal{O}\big(\frac{\delta(1-\delta)}{q}\big)$.

3 Application to private information retrieval

Private information retrieval (PIR) protocols are cryptographic protocols ensuring that a user can retrieve an entry D_i of a remote database $D = (D_1, \ldots, D_k)$, without revealing any information on the index $i \in [1, k]$ to the holder of the database. Additionally, it is also required that the communication cost (number of bits exchanged during the retrieval process) is sublinear in the size of the database.

Since its introduction by Chor, Goldreich, Kushilevitz and Sudan in 1995 [CGKS95], various kinds of PIR schemes have been designed according to the system constraints. In earliest PIR schemes, one assumes that the database is replicated over ℓ non-communicating honest-but-curious servers $S_1, \ldots, S_\ell$. In this context the seminal result of Katz and Trevisan [KT00] — which relates PIR protocols to the existence of so-called *smooth locally decodable codes* — induced many new constructions of PIR schemes, notably in [BIKR02, Yek08, Efr12, DG16]. These constructions eventually achieved $O(\exp(\sqrt{\log k \log\log k}))$ bits of communication for a k-entry database replicated on $\ell = 2$ servers.

Motivated by the use of storage codes in distributed storage systems, a large amount of recent works focused on the case where the database is *encoded* on the servers. In this context, entries of the database are usually very large (*e.g.* movies), so that we can assume that the *download* communication cost prevails over the upload one. Several works aimed at minimizing this cost depending on the storage system: Shah, Rashmi and Ramchandran [SRR14] considered the replication code as the storage code; Tajeddine, Gnilke and El Rouayheb [TGR18] MDS codes; Kumar, Rosnes and Graell i Amat [KRGiA17] arbitrary codes.

It is worth noticing that, following *e.g.* Beimel and Stahl [BS02], a few works also considered the more restrictive setting of colluding servers (*i.e.* servers communicating with each other so as to collect information about the required item), byzantine servers (*i.e.* servers able to produce wrong answers to user's queries) or unresponsive servers (servers unable to give ananswer to user's queries).

Finally, one should emphasise that families of PIR schemes referenced above mostly focus on decreasing the communication cost during the retrieval process. This is done at the expense of other crucial parameters, such as the computation complexity of the recovery, or the servers' storage overhead.

In this section, we show how the local properties of weighted Reed-Muller codes $\mathrm{WRM}_q^{\eta}(d)$ lead to very natural PIR protocols resisting to any set of b byzantine, u unresponsive and t colluding servers — provided that $2b + u + t \leq q - d - 1$ — with moderate communication complexity but optimal computation complexity.

3.1 Definitions

Definition 3.1 (private information retrieval)**.** Let $D \in \mathbb{F}_q^k$ be a remote database distributed on ℓ servers $S_1, \ldots, S_\ell$, in such a way[3] that we assume that each server S_j stores a vector $\boldsymbol{c}^{(j)} \in \mathbb{F}_q^m$. A *private information retrieval (PIR)* protocol for D is a tuple of algorithms $(\mathsf{Query}, \mathsf{Answer}, \mathsf{Recover})$ such that:

1. Query is a probabilistic algorithm taking as input a coordinate $i \in [1, k]$, and providing a random tuple of *queries* $\mathsf{Query}(i) = (q_1, \ldots, q_\ell) \in \mathcal{Q}^\ell$ for some finite set $\mathcal{Q}$;
2. Answer is a deterministic algorithm taking as input a server index $j \in [1, \ell]$, a query $q_j \in \mathcal{Q}$ and the vector $\boldsymbol{c}^{(j)}$ stored by server S_j, and outputs an *answer* $a_j \in \mathcal{A}$, where $\mathcal{A}$ is a finite set;
3. $\mathsf{Recover}$ is a deterministic algorithm taking as input a coordinate $i \in [1, k]$, a tuple of queries $\boldsymbol{q} = (q_1, \ldots, q_\ell) \in \mathcal{Q}^\ell$ and a tuple of answers $\boldsymbol{a} = (a_1, \ldots, a_\ell) \in \mathcal{A}^\ell$, and which outputs a symbol $r \in \mathbb{F}_q$ satisfying the following requirement. If $\boldsymbol{q} = \mathsf{Query}(i)$ and $\boldsymbol{a} = (\mathsf{Answer}(j, q_j, \boldsymbol{c}^{(j)}))_{1 \leq j \leq \ell}$, then:

$$D_i = \mathsf{Recover}(i, \boldsymbol{q}, \boldsymbol{a})\,. \tag{1}$$

We also say that a PIR protocol

- is *t-private* (or resists to any *collusion* of t servers) if for every $T \subset [1, \ell]$, $|T| = t$, we have
$$\mathrm{I}(\mathsf{Query}(i)_{|T}\,;\, i) = 0,$$
where $\mathrm{I}(\cdot\,;\,\cdot)$ denotes the mutual information between random variables;
- is *robust against b byzantine and u unresponsive servers* if (1) holds when up to b symbols of $\boldsymbol{a} = (\mathsf{Answer}(j, q_j, \boldsymbol{c}^{(j)}))_{1 \leq j \leq \ell} \in \mathcal{A}^\ell$ differ from the expected ones, and up to u symbols of $\boldsymbol{a}$ are missing.

Let us now define some of the most studied parameters of PIR protocols.

Definition 3.2. Let $(\mathsf{Query}, \mathsf{Answer}, \mathsf{Recover})$ be a PIR protocol. We define:

- its *communication complexity* as $C_{\mathrm{comm}} := \ell(\log(|\mathcal{Q}|) + \log(|\mathcal{A}|))$;

[3]Notice that we make no other assumption on the way (replication, encoding, etc.) the database is stored on the servers. We only require that the encoding map $D \mapsto (\boldsymbol{c}^{(1)}, \ldots, \boldsymbol{c}^{(\ell)})$ is injective.

- its *server computation complexity*, denoted C^s_{comp} as the maximal number of operations over $\mathbb{F}_q$ necessary to compute $\mathsf{Answer}(j, q_j, \boldsymbol{c}^{(j)})$;
- its *storage rate* as the ratio $\frac{k}{\ell m}$.

We finally say that a PIR protocol is *computationally optimal for the servers* if $C^s_{\text{comp}} \leq 1$.

3.2 The PIR protocol

We present in this section a PIR protocol based on weighted Reed-Muller codes. The protocol relies on a well-suited splitting of the encoded database over the servers, as it was originally done by Augot, Levy-dit-Vehel and Shikfa in [ALS14]

Protocol 3.3. Let $\mathcal{C} = \mathrm{WRM}^{\eta}_q(d)$, and denote its dimension by k. Recall that a codeword $\boldsymbol{c} \in \mathcal{C}$ can be seen as a map $\mathbb{F}_q^2 \to \mathbb{F}_q$. Let us also consider q servers $(S_t)_{t\in\mathbb{F}_q}$ indexed by elements of $\mathbb{F}_q$.

Initialisation. The database $D \in \mathbb{F}_q^k$ is encoded into a codeword $\boldsymbol{c} \in \mathcal{C}$. For every $t \in \mathbb{F}_q$, the server S_t receives the part $\boldsymbol{c}_{|\{t\}\times\mathbb{F}_q}$ of the codeword $\boldsymbol{c}$. Notice that $\boldsymbol{c}_{|\{t\}\times\mathbb{F}_q}$ consists in q symbols over $\mathbb{F}_q$.

Queries. Assume one wants to retrieve D_i, for $1 \leq i \leq k$. One can always assume that the encoding map is systematic, hence $D_i = c_{\boldsymbol{x}}$ for some $\boldsymbol{x} = (x_1, x_2) \in \mathbb{F}_q^2$. To define a vector of queries:

- Pick at random an η-line $L \in \Phi_\eta$ such that $L(t_0) = \boldsymbol{x}$ for some $t_0 \in \mathbb{F}_q$.
- The server S_{t_0} receives a random element $y_{t_0} \in \mathbb{F}_q$.
- Server $S_t, t \neq t_0$ receives $y_t \in \mathbb{F}_q$ such that $(t, y_t) = L(t)$.

Answers. Upon receipt of $y_t \in \mathbb{F}_q$, every server S_t reads the entry $c_{(t,y_t)} \in \mathbb{F}_q$ and sends it back to the user.

Recovery. The user collects $\boldsymbol{c}' = (c_{(t,y_t)})_{t\in\mathbb{F}_q}$ and runs an error-and-erasure correcting algorithm for $\mathrm{RS}_q(d)$ with input $\boldsymbol{c}'$. Then, the user returns the corrected symbol $c'_{(t_0,y_{t_0})}$.

Theorem 3.4. *Let q be a prime power, $\eta \geq 1$, and $b, u \geq 0$. Set $d = q - u - 2b - 2$. Then, Protocol 3.3 equipped with $\mathrm{WRM}^{\eta}_q(d)$ is η-private and robust against b byzantine and u unresponsive servers. Moreover, it is computationally optimal for the servers, its storage rate approaches $1/2\eta$ when $q \to \infty$, and its communication complexity is $2q \log q$.*

Proof. The correctness of the PIR scheme, under b byzantine and u unresponsive servers, comes from Proposition 2.3 and from the fact that $\mathrm{RS}_q(d)$ corrects b errors and $u + 1$ erasures if $d \geq q - u - 2b - 2$. Moreover, the scheme is η-private since any subset of η points of an η-line gives no information about the other points. Finally, the parameters of the scheme can be easily checked. □

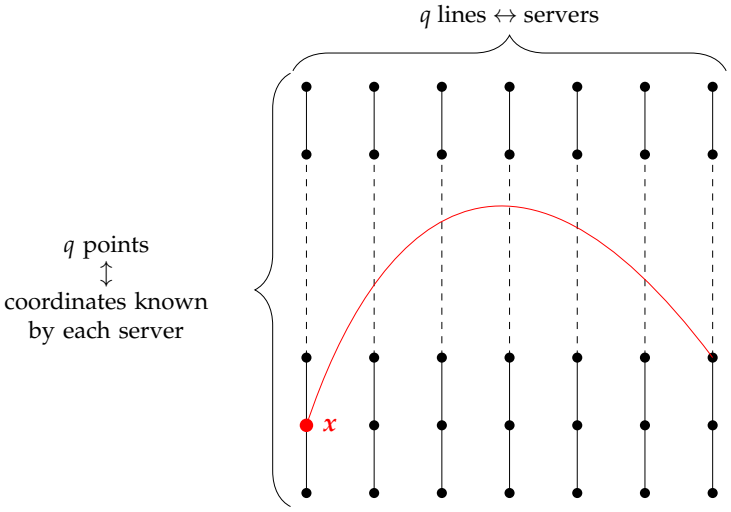


Figure 1: Illustration of the retrieval process. For a desired coordinate c_x, an η-line L (in red) containing x is picked at random.

4 Towards higher information rate: the lifting process

4.1 Definitions

In previous sections, we have proved that weighted Reed-Muller codes admit local properties that can be used in practical applications such as private information retrieval. However, such constuctions are moderately efficient in terms of storage, since the information rate of $\mathrm{WRM}_q^\eta(d)$ is bounded by $1/2\eta$ if $d \leq q-2$.

In this section, we show how to construct codes with the same local properties as weighted Reed-Muller codes, but admitting a much larger dimension. As a practical consequence, these new codes can replace weighted Reed-Muller codes in Protocol 3.3, leading to storage-efficient PIR schemes.

Techniques involved in the construction of these codes directly follow the lifting process initiated by Guo, Kopparty and Sudan [GKS13]. More precisely, the authors introduce so-called *lifted Reed-Solomon codes* as codes containing (classical) Reed-Muller codes, and satisfying that the restriction of any codeword to any affine line lies in a Reed-Solomon. The purpose of this section is to extend this notion to η-lines.

We thus naturally introduce the η-lifting of a Reed-Solomon code as follows.

Definition 4.1 (η-lifting of a Reed-Solomon code)**.** Let q be a prime power and $0 \leq d \leq q-1$. The *η-lifting of the Reed-Solomon code* $\mathrm{RS}_q(d)$ is the code of length $n = q^2$ defined as follows:

$$\mathrm{Lift}^\eta(\mathrm{RS}_q(d)) := \{\mathrm{ev}_{\mathbb{F}_q^2}(f) \mid f \in \mathbb{F}_q[X,Y], \forall L \in \Phi_\eta, \mathrm{ev}_{\mathbb{F}_q}(f \circ L) \in \mathrm{RS}_q(d)\}\,.$$

Notice that if $d = q-1$, the η-lifted code $\mathrm{Lift}^\eta(\mathrm{RS}_q(q-1))$ is the trivial full space $\mathbb{F}_q^{q^2}$. Hence, from now on we assume $d \leq q-2$.

It is clear that $\mathrm{WRM}_q^\eta(d) \subseteq \mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ since the constraints that define η-lifted codes are satisfied by each codeword of a comparable weighted Reed-Muller code. But quite surprisingly, the code $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ is sometimes much larger than $\mathrm{WRM}_q^\eta(d)$. Let us highlight this claim with an example.

Example 4.2. Let $q = 4$, $\eta = 2$ and $d = 2$. The associated weighted Reed-Muller code is generated by the evaluation vectors of monomials X^iY^j, where (i,j) lies in

$$\{(0,0),(0,1),(1,0),(2,0)\}.$$

Let us now consider the monomial $f(X,Y) = Y^2 \in \mathbb{F}_4[X,Y]$ and an η-line $L(T) = (T, aT^2 + bT + c) \in \Phi_2$, where $a,b,c \in \mathbb{F}_4$. We see that for every $t \in \mathbb{F}_4$, we have:

$$(f \circ L)(t) = (at^2 + bt + c)^2 = a^2t^4 + b^2t^2 + c^2 = b^2t^2 + a^2t + c\,.$$

Hence, $\mathrm{ev}_{\mathbb{F}_4}(f \circ L) \in \mathrm{RS}_4(2)$ for every $L \in \Phi_2$. Since $\mathrm{wdeg}_\eta(f) = 4 > 2$, we get

$$\mathrm{ev}_{\mathbb{F}_4^2}(f) \in \mathrm{Lift}^2(\mathrm{RS}_4(2)) \setminus \mathrm{WRM}_4^2(2)\,.$$

Given a polynomial $f(X,Y) = \sum_{i,j} f_{i,j}X^iY^j \in \mathbb{F}_q[X,Y]$, we define its *degree set* as

$$\mathrm{Deg}(f) \coloneqq \{(i,j) \in \mathbb{N}^2, f_{i,j} \neq 0\}\,.$$

By extension, the degree set $\mathrm{Deg}(S)$ of a subset $S \subseteq \mathbb{F}_q[X,Y]$ is the union of degree sets of polynomials lying in S. Similarly, if $\mathcal{C} = \{\mathrm{ev}_{\mathbb{F}_q^2}(f), f \in S\}$, then we set $\mathrm{Deg}(\mathcal{C}) \coloneqq \mathrm{Deg}(S)$.

Remark 4.3. Since $a^q = a$ for every $a \in \mathbb{F}_q$, one can consider degree sets as subsets of $[0, q-1]^2$. This precisely corresponds to considering polynomials modulo the ideal $I = \langle X^q - X, Y^q - Y\rangle = \ker \mathrm{ev}_{\mathbb{F}_q^2}$.

Lemma 4.4. *Let $f \in \mathbb{F}_q[X,Y]$ such that $\mathrm{Deg}(f) \subseteq [0,q-1]^2$, and let $(i,j) \in \mathrm{Deg}(f)$. Assume that for every $(a,b) \in \mathrm{Deg}(f)$, we have $i \geq a$ (respectively, $j \geq b$). Then, there exists an η-line $L \in \Phi_\eta$ such that $\deg(f \circ L) = i$ (respectively, $\deg(f \circ L) = j$).*

Proof. If $i \geq a$ for every $(a,b) \in \mathrm{Deg}(f)$, then $L(T) = (T,1)$ lies in Φ_η, and the degree of $f \circ L$ is thus i. The proof is similar for j. □

Proposition 4.5. *Let $d \leq q-2$. Then,*

$$\mathrm{Deg}(\mathrm{Lift}^\eta(\mathrm{RS}_q(d))) \subseteq [0,d]^2\,.$$

Proof. A pair $(i,j) \in \mathrm{Deg}(\mathrm{Lift}^\eta(\mathrm{RS}_q(d))) \setminus [0,d]^2$ would contradict Lemma 4.4. □

4.2 Monomiality

We say that a linear code $\mathcal{C}$ is *monomial* if there exists a set $S \subset \mathbb{F}_q[X,Y]$ of monomials, such that $\mathcal{C} = \mathrm{Span}\{\mathrm{ev}_{\mathbb{F}_q^2}(f), f \in S\}$. Monomial codes are convenient since they admit a simple description.

Let us define monomial transformations $m_{a,b} : (x,y) \mapsto (ax, by)$, for $(a,b) \in (\mathbb{F}_q^\times)^2$.

Lemma 4.6. *Let S be a subspace of $\mathbb{F}_q[X,Y]$ such that:*

(i) $\mathrm{Deg}(S) \subseteq [0, q-2]^2$, *and*
(ii) for every $f(X,Y) \in S$ and every $(a,b) \in (\mathbb{F}_q^\times)^2$, the polynomial $f \circ m_{a,b}$ also lies in S.

Then S is spanned by monomials.

Proof. Let $f(X,Y) = \sum_{(i,j)\in D} f_{i,j} X^i Y^j \in S$ where $D = \mathrm{Deg}(f) \subseteq [0,q-2]^2$. It is sufficient to prove that for all $(i,j) \in D$, the monomial X^iY^j lies in S.

For $(i,j) \in D$, let us define

$$Q_{i,j}(X,Y) \coloneqq \sum_{(a,b)\in(\mathbb{F}_q^\times)^2} \frac{1}{a^i b^j} f(aX, bY)\,.$$

Since S is a vector space invariant under $\{m_{a,b} \mid (a,b) \in (\mathbb{F}_q^\times)^2\}$, we have $Q_{i,j} \in S$. Moreover,

$$\begin{aligned}
Q_{i,j}(X,Y) &= \sum_{(a,b)\in(\mathbb{F}_q^\times)^2} \frac{1}{a^i b^j} \left(\sum_{(d,e)\in \mathrm{Deg}(f)} f_{d,e}\, a^d b^e X^d Y^e \right) \\
&= \sum_{(d,e)\in \mathrm{Deg}(f)} f_{d,e} \sum_{(a,b)\in(\mathbb{F}_q^\times)^2} a^{d-i} b^{e-j} X^d Y^e \\
&= \sum_{(d,e)\in \mathrm{Deg}(f)} f_{d,e} \cdot \underbrace{\Big(\sum_{a\in\mathbb{F}_q^\times} a^{d-i} \Big)}_{=0 \text{ if } d=i,\ -1 \text{ otherwise}} \cdot \underbrace{\Big(\sum_{b\in\mathbb{F}_q^\times} b^{e-j} \Big)}_{=0 \text{ if } e=j,\ -1 \text{ otherwise}} \cdot X^d Y^e \\
&= f_{i,j} \cdot (-1)^2 \cdot X^i Y^j\,.
\end{aligned}$$

Since $f_{i,j} \neq 0$, $X^iY^j \in S$. □

Proposition 4.7. *Let $d \leq q-1$. The linear code $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ is monomial.*

Proof. The code $\mathrm{Lift}^\eta(\mathrm{RS}_q(q-1))$ is the full space $\mathbb{F}_q^{q^2}$; hence it is trivially a monomial code. For $d \leq q-2$, let us define

$$S \coloneqq \{f \in \mathbb{F}_q[X,Y], \mathrm{Deg}(f) \subseteq [0,q-1]^2, \mathrm{ev}_{\mathbb{F}_q^2}(f) \in \mathrm{Lift}^\eta(\mathrm{RS}_q(d))\}\,.$$

Proposition 4.5 ensures that $\mathrm{Deg}(S) \subseteq [0,d]^2$. Let $f = \sum_{i,j} f_{i,j} X^i Y^j \in S$. For every $(a,b) \in (\mathbb{F}_q^\times)^2$ and every $L(T) = (T, \phi(T)) \in \Phi_\eta$ we have

$$f \circ m_{a,b} \circ L(T) = \sum_{i,j} f_{i,j} a^i T^i b^j \phi(T)^j\,.$$

Let us now define $Q(T) \coloneqq f(T, b\phi(a^{-1}T))$. One can easily check that $(T, b\phi(a^{-1}T))) \in \Phi_\eta$. Since $\mathrm{ev}_{\mathbb{F}_q^2}(f) \in \mathrm{Lift}^\eta(\mathrm{RS}_q(d))$, we also know that $\mathrm{ev}_{\mathbb{F}_q}(Q) \in \mathrm{RS}_q(d)$. Moreover, $\mathrm{RS}_q(d)$ is invariant under affine transformations, hence $\mathrm{ev}_{\mathbb{F}_q}(Q(aT)) \in \mathrm{RS}_q(d)$. Let us now remark that

$$Q(aT) = \sum_{i,j} f_{i,j} a^i T^i b^j \phi(T)^j = f \circ m_{a,b} \circ L(T)\,.$$

Consequently, $f \circ m_{a,b} \in S$. Therefore we can use Lemma 4.6, and our result follows immediately. □

4.3 The degree set of η-lifted Reed-Solomon codes

Previous discussions ensure that, given a tuple (η, d, q), the code $\mathcal{C}(q, d, \eta) \coloneqq \mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ is fully determined by its *degree set* $D(q, d, \eta) \coloneqq \mathrm{Deg}(\mathcal{C}(q, d, \eta)) \subseteq [0, d]^2$. Let us now seek for characterisations of $D(q, d, \eta)$.

For this purpose, we need to introduce some notation:

- $\langle \cdot, \cdot \rangle$ denotes the inner product between vectors, or tuples.
- We set $\boldsymbol{w} \coloneqq (1, 2, \ldots, \eta) \in \mathbb{N}^\eta$.
- Given $\alpha \in \mathbb{N}$ and a prime number p, we denote by $\alpha^{(r)}$ the rth digit in the representation of α in base p, *i.e.* $\alpha = \sum_{r \geq 0} \alpha^{(r)} p^r$.
- For $\alpha, \beta \in \mathbb{N}$, we write $\alpha \leq_p \beta$ if and only if $\alpha^{(r)} \leq \beta^{(r)}$ for every $r \geq 0$.
- For $\boldsymbol{k} \in \mathbb{N}^\eta$ and $r \in \mathbb{N}$, we also write $\boldsymbol{k}^{(r)} = \left(k_1^{(r)}, \ldots, k_\eta^{(r)}\right) \in \mathbb{N}^\eta$.

We will also make use of Lucas theorem [Luc78] which gives the reduction of binomial coefficients modulo primes.

Theorem 4.8 (Lucas theorem [Luc78])**.** *Let $a, b \in \mathbb{N}$ and p be a prime number. Recall that $a = \sum_{i \geq 0} a^{(i)} p^i$ is the representation of a in base p. Then,*

$$\binom{a}{b} = \prod_{i \geq 0} \binom{a^{(i)}}{b^{(i)}} \mod p\,.$$

In particular, in any field of characteristic p, the binomial coefficient $\binom{a}{b}$ is non-zero if and only if $b \leq_p a$.

In the next lemma, we characterise univariate polynomials arising from the restriction of Y^j to η-lines.

Lemma 4.9. *Let $j \geq 0$ and $\eta \geq 1$ and let us define $\Phi_\eta^j \coloneqq \{\phi(T)^j \mid \phi(T) \in \mathbb{F}_q[T], \deg \phi \leq \eta\} \subseteq \mathbb{F}_q[T]$. We have:*

$$\Phi_\eta^j = \mathrm{Span}\{T^\alpha \mid \alpha \in \Delta(j, \eta)\}\,,$$

where

$$\Delta(j, \eta) \coloneqq \left\{ \langle \boldsymbol{w}, \boldsymbol{k} \rangle \mid \boldsymbol{k} \in \mathbb{N}^\eta \text{ such that } \forall m \leq \eta,\ k_m \leq_p j - \sum_{\ell=1}^{m-1} k_\ell \right\}.$$

Proof. Given a polynomial $\phi(T) = \sum_{m=0}^{\eta} a_m T^m \in \mathbb{F}_q[T]$, the well-known multinomial theorem entails that:

$$\begin{aligned}\phi(T)^j &= (a_0 + a_1 T + \cdots + a_\eta T^\eta)^j \\ &= \sum_{k_1+\cdots+k_\eta \leq j} \binom{j}{k_1, \ldots, k_\eta} \lambda_{\boldsymbol{k}} x^{k_1+2k_2+\cdots+\eta k_\eta},\end{aligned}$$

where $\lambda_{\boldsymbol{k}} \coloneqq a_0^{j-|\boldsymbol{k}|} \times \prod_{\ell=1}^{\eta} a_\ell^{k_\ell} \in \mathbb{F}_q$ is a coefficient which only depends on $a_0, \ldots, a_\eta$ and $\boldsymbol{k}$, and where

$$\binom{j}{\boldsymbol{k}} \coloneqq \binom{j}{k_1, \ldots, k_\eta} = \frac{j!}{k_1! k_2! \ldots k_\eta! (j - \sum_{m=1}^{\eta} k_m)!}.$$

The coefficient of the term T^α in $\phi(T)^j$ is therefore:

$$c_\alpha = \sum_{\boldsymbol{k} \in K_\alpha} \binom{j}{\boldsymbol{k}} \lambda_{\boldsymbol{k}},$$

where $K_\alpha \coloneqq \{\boldsymbol{k} \in \mathbb{N}^\eta \mid |\boldsymbol{k}| \leq j \text{ and } \langle \boldsymbol{w}, \boldsymbol{k} \rangle = \alpha\}$. We claim that $c_\alpha = 0$ for every $\phi \in \Phi_\eta$ if and only if $\binom{j}{\boldsymbol{k}} = 0$ for every $\boldsymbol{k} \in K_\alpha$. Indeed, $c_\alpha \in \mathbb{F}_q$ can be seen as the evaluation of an homogeneous polynomial $C_\alpha \in \mathbb{F}_q[A_0, \ldots, A_\eta]$ of degree j at the point $(a_0, \ldots, a_\eta) \in \mathbb{F}_q^{\eta+1}$ corresponding to ϕ. Since $j \leq q-1$, the polynomial C_α vanishes over $\mathbb{F}_q^{\eta+1}$ if and only if it is the zero polynomial, which proves our claim.

Now, notice that

$$\binom{j}{\boldsymbol{k}} = \binom{j}{k_1} \binom{j-k_1}{k_2} \binom{j-k_1-k_2}{k_3} \cdots \binom{j-k_1-k_2-\cdots-k_{\eta-1}}{k_\eta}.$$

Hence, using Lucas theorem [Luc78] on every binomial coefficient in the above product, we see that $\binom{j}{\boldsymbol{k}} = 0$ if and only if there exists $m \in [1, \eta]$ such that $k_m \not\leq_p j - \sum_{\ell=1}^{m-1} k_\ell$.

In other words, the monomial T^α appears as a term of $\phi(T)^j$ if and only if there exists $\boldsymbol{k} \in \mathbb{N}^\eta$ such that $\alpha = \langle \boldsymbol{w}, \boldsymbol{k} \rangle = \sum_{\ell=1}^{\eta} \ell k_\ell$ and

$$\forall m \in [1, \eta], k_m \leq_p j - \sum_{\ell=1}^{m-1} k_\ell.$$

□

Let us now give some properties on the set $\Delta(j, \eta) \subseteq \mathbb{N}$ defined in Lemma 4.9.

Lemma 4.10. *We have $\Delta(j, \eta) \subseteq [0, j\eta]$. Moreover, an integer α belongs to $\Delta(j, \eta)$ if and only if*

$$\exists \boldsymbol{k} \in \mathbb{N}^\eta \text{ such that } \alpha = \langle \boldsymbol{w}, \boldsymbol{k} \rangle \text{ and } \forall r \geq 0, \sum_{\ell=1}^{m} k^{(r)} \leq j^{(r)}. \tag{2}$$

Proof. By definition, an integer α belongs to $\Delta(j, \eta)$ if and only if there exists $\boldsymbol{k} \in \mathbb{N}^\eta$ such that $\alpha = \sum_{\ell=1}^{\eta} \ell k_\ell$ and for all $m \leq \eta$, we have

$$k_m \leq_p j - \sum_{\ell=1}^{m-1} k_\ell. \tag{3}$$

We first prove by induction on m that, if $\alpha \in \Delta(j,\eta)$, then for all $m \leq \eta$ and for all $r \geq 0$,

$$\sum_{\ell=1}^{m} k_\ell^{(r)} \leq j^{(r)}\,.$$

Notice that it would prove the desired result for $m = \eta$. Moreover, the case $m = 1$ is a direct consequence of (3).

Let us fix $2 \leq m \leq \eta$ such that $\sum_{\ell=1}^{m-1} k_\ell^{(r)} \leq j^{(r)}$ for every $r \geq 0$. Then $\sum_{\ell=1}^{m-1} k_\ell^{(r)} \leq p-1$ and the uniqueness of the representation of the integer $\sum_{\ell=1}^{m-1} k_\ell$ in base p ensures that

$$\left(\sum_{\ell=1}^{m-1} k_\ell\right)^{(r)} = \sum_{\ell=1}^{m-1} k_\ell^{(r)} \leq j^{(r)}. \tag{4}$$

Using (3), we get $k_m^{(r)} \leq j^{(r)} - \sum_{\ell=1}^{m-1} k_\ell^{(r)}$, which implies that $\sum_{\ell=1}^{m} k_\ell^{(r)} \leq j^{(r)}$.

Conversely, assume that (2) holds, and let $1 \leq m \leq \eta$. We shall prove that (3) is satisfied. For every $r \geq 0$, we have

$$k_m^{(r)} \leq \sum_{\ell=m}^{\eta} k_\ell^{(r)} = \sum_{\ell=1}^{\eta} k_\ell^{(r)} - \sum_{\ell=1}^{m-1} k_\ell^{(r)}.$$

Equation (2) implies that $k_m^{(r)} \leq j^{(r)} - \sum_{\ell=1}^{m-1} k_\ell^{(r)}$. Moreover, $\sum_{\ell=1}^{m-1} k_\ell^{(r)} \leq j^{(r)}$, hence as we have seen in (4),

$$\left(\sum_{\ell=1}^{m-1} k_\ell\right)^{(r)} = \sum_{\ell=1}^{m-1} k_\ell^{(r)}\,.$$

This leads us to $k_m^{(r)} \leq \left(j - \sum_{\ell=1}^{m-1} k_\ell\right)^{(r)}$. Therefore, $k_m \leq_p j - \sum_{\ell=1}^{m-1} k_\ell$. □

As an easy corollary of Lemma 4.9 and Lemma 4.10, we see that

$$\mathrm{Deg}(\{(X^iY^j)\circ\phi, \phi \in \Phi_\eta\}) = \{i+u, u \in \Delta(j,\eta)\}\,.$$

Hence, $\mathrm{ev}_{\mathbb{F}_q^2}(X^iY^j)$ lies in $\mathrm{Lift}^\eta\,\mathrm{RS}_q(d)$ if, for all $u \in \Delta(j,\eta)$, every monomial T^{i+u} evaluates to a codeword of $\mathrm{RS}_q(d)$. Notice here that $i+u$ might be larger than q, therefore this is equivalent to say that $T^{i+u} \mod (T^q - T)$ is polynomial of degree bounded by d.

This remark leads us to introduce a relation of equivalence between integers. We write $a \equiv_q^\star b$ if and only if $T^a = T^b \mod (T^q - T)$. In other words, $a \equiv_q^\star b$ if and only if $(a,b) = (0,0)$, or $a > 0, b > 0$ and $(q-1) \mid (a-b)$. Finally, we denote[4] by $\mathrm{Red}_q^\star(a)$ the only integer in $[0, q-1]$ such that $\mathrm{Red}_q^\star(a) \equiv_q^\star a$.

From Lemma 4.9 and Lemma 4.10, and following the previous discussion, we deduce a characterisation of elements of $D(q,d,\eta)$.

Proposition 4.11. *Let $d \leq q-2$. A pair $(i,j) \in [0,d]^2$ belongs to $D(q,d,\eta)$ if and only if for every $\boldsymbol{k} \in \mathbb{N}^\eta$ such that for all $r \geq 0, |\boldsymbol{k}^{(r)}| \leq j^{(r)}$, we have*

$$\mathrm{Red}_q^\star(i + \langle \boldsymbol{w}, \boldsymbol{k}\rangle) \leq d.$$

[4] notation $\mod^* q$ is used in [GKS13], but we find it quite unconvenient

5 Analyses of sequences of degree sets

For a generic tuple (η, q, d), it seems difficult to give an explicit description of the degree set of $\mathrm{Lift}^\eta \mathrm{RS}_q(d)$. Our approach is to analyse *sequences* of degree sets $D(q, d, \eta)$ with varying parameters $q = p^e$, d, and η, in order to produce good asymptotic families of codes.

We will illustrate our analyses with graphical representations of degree sets. Our convention is the following. Assume one wants to represent a degree set $D \subseteq [q-1]^2$. If $(i, j) \in D$, then a black (or sometimes grey) unit square is represented at coordinate (i, j); otherwise, a white unit square is plotted. Such an illustration is proposed in Example 5.1.

Example 5.1. The degree set D of $\mathrm{Lift}^2(\mathrm{RS}_8(5))$, namely

$$D = \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(1,0),(1,1),(1,2),(1,3),(2,0),(2,1),(4,0),(4,1),(4,4)\}$$

is represented in Figure 2.

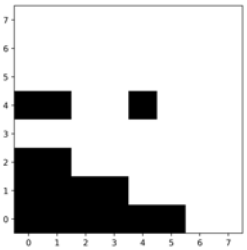


Figure 2: A representation of the degree set D of $\mathrm{Lift}^2 \mathrm{RS}_8(5)$.

Let us now provide generic relations between η-lifted codes of varying parameters.

5.1 Increasing and decreasing sequences of η-lifted codes

5.1.1 Sequence $(D(q, d, \eta))_{\eta \geq 1}$, with (q, d) fixed and varying η

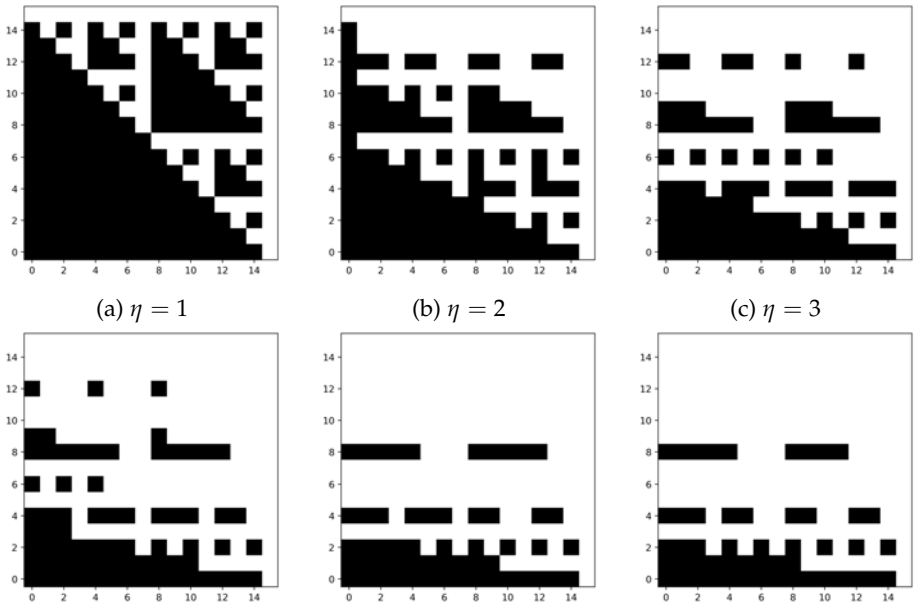
Lemma 5.2. *Let us fix a prime power q and $d \leq q-1$. The sequence of codes $(\mathrm{Lift}^\eta \mathrm{RS}_q(d))_{\eta \geq 1}$ is decreasing with respect to the inclusion of codes.*

Proof. It is enough to notice that an η-line is also an $(\eta+1)$-line, therefore every codeword of $\mathrm{Lift}^{\eta+1} \mathrm{RS}_q(d)$ fulfills the constraints defining $\mathrm{Lift}^\eta \mathrm{RS}_q(d)$. □

In Figure 3, we plot a sequence of degree sets which illustrates this result on $\mathbb{F}_{16}$.

5.1.2 Sequence $(D(q, d, \eta))_{0 \leq d \leq q-2}$ with (q, η) fixed and varying d

Lemma 5.3. *Let us fix a prime power q and $\eta \geq 1$. The sequence $(\mathrm{Lift}^\eta \mathrm{RS}_q(d))_{d \geq 0}$ is increasing.*



(a) $\eta = 1$ (b) $\eta = 2$ (c) $\eta = 3$

(d) $\eta = 4$ (e) $\eta = 5$ (f) $\eta = 6$

Figure 3: Representation of the degree set of $\mathrm{Lift}^{\eta}\,\mathrm{RS}_{16}(14)$ for different values of η

Proof. It is a straightforward consequence of the embedding of $\mathrm{RS}_q(d)$ into $\mathrm{RS}_q(d+1)$. □

In Figure 4, we plot a sequence of degree sets which illutrates this result on $\mathbb{F}_{16}$ with $\eta = 2$.

5.1.3 Sequence $(D(q, q-\alpha, \eta))_q$ with fixed (α, η), and varying q

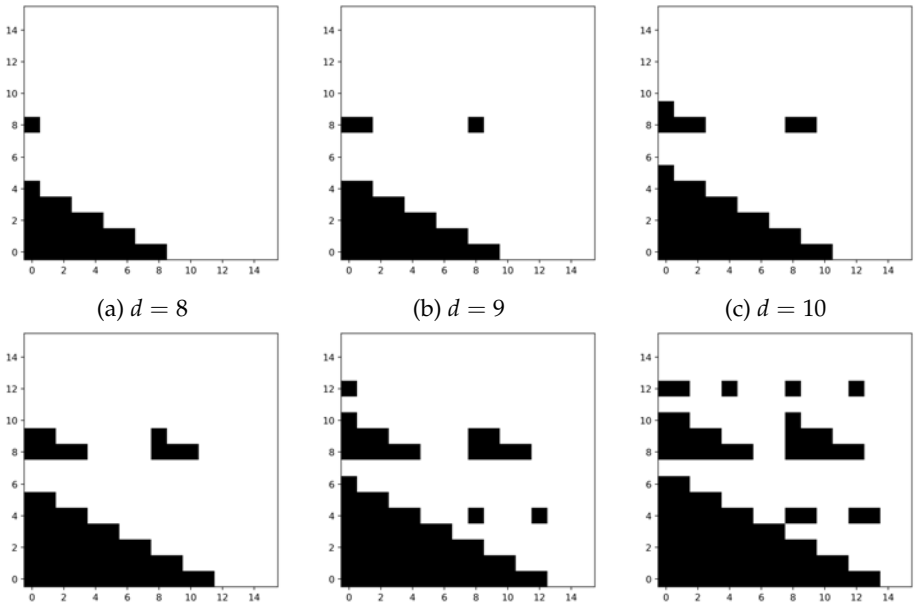
Let us fix a prime number p, and let us consider a sequence of degree sets $(D(p^e, p^e - \alpha, \eta))_{e \geq 1}$ with fixed (α, η), and varying e. Figure 5 represents such a sequence. In this figure, one can notice that $D(p^e, p^e - \alpha, \eta)$ is a subpattern (highlighted in grey) of the larger degree sets $D(p^{e+1}, p^{e+1} - \alpha, \eta)$.

This remark seems trivial at first, but it has a meaningful consequence in terms of codes. Indeed, it shows that the corresponding η-lifted codes are (up to isomophism) subcodes to each other when the field size $q = p^e$ grows. This property is formalized in the following lemma.

Lemma 5.4. *Let $\eta < q = p^e$ and $2 \leq \alpha \leq p^e$. If $(p^e - i, j) \in D(p^e, p^e - \alpha, \eta)$, then*

$$(p^{e+1} - i, j) \in D(p^{e+1}, p^{e+1} - \alpha, \eta)\,.$$

Proof. Let $(p^e - i, j) \in D(p^e, p^e - \alpha, \eta)$, and consider $\boldsymbol{k} \in \mathbb{N}$ such that $|\boldsymbol{k}^{(r)}| \leq j^{(r)}$ for every $r \geq 0$. Using Proposition 4.11, we know that $\mathrm{Red}^{\star}_{p^e}((p^e - i) + \langle \boldsymbol{w}, \boldsymbol{k} \rangle) \leq p^e - \alpha$, and we want to prove that $\mathrm{Red}^{\star}_{p^{e+1}}(p^{e+1} - i) \leq p^{e+1} - \alpha$.



(a) $d = 8$ (b) $d = 9$ (c) $d = 10$

(d) $d = 11$ (e) $d = 12$ (f) $d = 13$

Figure 4: Representation of the degree set of $\mathrm{Lift}^2 \mathrm{RS}_{16}(d)$ for different values of d

Notice that there exists $(Q_0, Q_1, R) \in \mathbb{N}^3$ satisfying:

$$(p^e - i) + \langle \boldsymbol{w}, \boldsymbol{k} \rangle = (Q_1 p + Q_0)(p^e - 1) + R$$

with $Q_0 \leq p - 1$ and $R \leq p^e - \alpha$. Since $\langle \boldsymbol{w}, \boldsymbol{k} \rangle \leq \eta |\boldsymbol{k}| \leq \eta j \leq \eta(p^e - 1)$, one can also check that $Q_1 p + Q_0 \leq \eta + 1$.

The case $R = 0$ must be handled at first. Notice that this implies that $(p^e - i) + \langle \boldsymbol{w}, \boldsymbol{k} \rangle = 0$, meaning that $(p^e - i, j) = (0, 0)$. Then one can check that $(p^{e+1} - p^e, 0) \in D(p^{e+1}, p^{e+1} - \alpha, \eta)$ since $\alpha \leq p^e$. Hence, from now on, we assume that $R \geq 1$, and we distinguish two cases.

First, assume that $Q_0 \geq 1$. Then we have

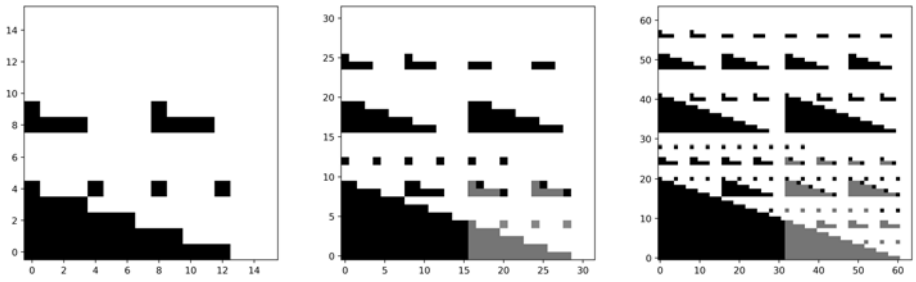
$$p^{e+1} - i + \langle \boldsymbol{w}, \boldsymbol{k} \rangle = p^{e+1} - p^e + (Q_1 p + Q_0)(p^e - 1) + R = (Q_1 + 1)(p^{e+1} - 1) + R'$$

where

$$R' \coloneqq Q_0(p^e - 1) + R - (Q_1 + 1)(p - 1)\,.$$

We see that $p^{e+1} - i + \langle \boldsymbol{w}, \boldsymbol{k} \rangle \equiv^{\star}_{p^{e+1}} R'$, hence it is sufficient to prove that $1 \leq R' \leq p^{e+1} - \alpha$. Using $R \leq p^e - \alpha$ and $Q_0 \leq p - 1$, we get $R' \leq p^{e+1} - \alpha$. Now, notice that $Q_1 \leq \frac{\eta + 1 - Q_0}{p} \leq \lfloor \frac{p^e - 1}{p} \rfloor = p^{e-1} - 1$. Hence,

$$R' \geq R + p^e - 1 - (p - 1)p^{e-1} \geq R + p^{e-1} - 1 \geq 1\,.$$



(a) $e = 4$ (b) $e = 5$ (c) $e = 6$

Figure 5: Representation of the degree set of $\mathrm{Lift}^3\,\mathrm{RS}_{2^e}(2^e - 4)$ for increasing values of e. In the degree set over $\mathbb{F}_{2^e}$, the grey part is an exact copy of the degree set over $\mathbb{F}_{2^{e-1}}$ which is represented on its left.

Now, assume that $Q_0 = 0$. We thus have

$$p^{e+1} - i + \langle \boldsymbol{w}, \boldsymbol{k} \rangle = Q_1(p^{e+1} - 1) + R'$$

where

$$R' \coloneqq p^{e+1} - p^e + R - Q_1(p-1).$$

Once again, let us prove that $1 \leq R' \leq p^{e+1} - \alpha$. It is straightforward to check that $R' \leq p^{e+1} - \alpha$. Moreover, $Q_1 \leq \frac{\eta+1}{p} \leq p^{e-1}$, leading to

$$R' \geq p^{e+1} - p^e + R - p^{e-1}(p-1) \geq R \geq 1\,.$$

□

5.2 On the asymptotic information rate of $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ when $q \to \infty$

In this section, we consider sequences of codes $\mathrm{Lift}^\eta\,\mathrm{RS}_q(d)$ where $q \geq 2$ varies exponentially (*i.e.* $q = p^e$ with increasing e), and where we see d as a function of q such that $d(q) \leq q - 2$. Recall that q represents simultaneously the size of the finite field and the square root of the code length. Throughout the section, we will write $q = p^e$.

To our opinion, two cases are of interest: $d = q - \alpha$ where $\alpha \geq 2$ is a fixed integer, and $d = \lfloor \gamma q \rfloor$ where $\gamma \in (0,1)$. In the first case ($d = q - \alpha$) we prove that we obtain η-lifted codes whose information rate grows to 1 when $q \to \infty$. In the second case ($d = \lfloor \gamma q \rfloor$) we prove that the sequence of η-lifted codes admits an asymptotic information rate $R_\gamma > 0$ when $q \to \infty$, meaning that this sequence of codes is asymptotically good and is locally correctable from a constant fraction of errors. In order to prove these results, we look for tight enough lower bounds on the dimension of η-lifted codes.

5.2.1 A lower bound for $|D(q, q-\alpha, \eta)|$.

We first highlight that, for a fixed $\alpha \geq 2$, the degree set $D(q, q-\alpha, \eta)$ of $\mathrm{Lift}^{\eta}\,\mathrm{RS}_q(q-\alpha)$ contains many copies of the degree set of $\mathrm{WRM}^{\eta}_{p^\varepsilon}(p^\varepsilon - \alpha - \eta)$, for $\varepsilon \leq e$. In terms of codes, it informally means that weighted Reed-Muller codes defined over several fields $\mathbb{F}_{p^\varepsilon}$ for $\varepsilon \leq e$, can be embedded in many different manners into η-lifted codes. This is formalized in the following proposition.

Proposition 5.5. *Let $0 \leq \varepsilon \leq e$, $\alpha \in [0, p^\varepsilon - 1]$ and $(i,j) \in \mathrm{Deg}(\mathrm{WRM}^{\eta}_{p^\varepsilon}(p^\varepsilon - \alpha - \eta))$. Then, for every $0 \leq a, b \leq p^{e-\varepsilon} - 1$, we have*

$$(i + ap^\varepsilon, j + bp^\varepsilon) \in D(p^e, p^e - \alpha, \eta)\,.$$

Proof. Assume that $(i,j) \in \mathrm{Deg}(\mathrm{WRM}^{\eta}_{p^\varepsilon}(p^\varepsilon - \alpha - \eta))$. Then $i + \eta j \leq p^\varepsilon - \alpha - \eta$. We use the characterisation of Proposition 4.11 to prove our result.

Take $\boldsymbol{k} \in \mathbb{N}^\eta$ such that for all $r \geq 0$, $\sum_{\ell=1}^{\eta} k_\ell^{(r)} \leq (j + bp^\varepsilon)^{(r)}$. Then

$$\sum_{\ell=1}^{\eta} k_\ell^{(r)} \leq \begin{cases} j^{(r)} & \text{if } r \in [0, \varepsilon - 1], \\ b^{(r-\varepsilon)} & \text{if } r \in [\varepsilon, e-1], \\ 0 & \text{if } r \geq e. \end{cases}$$

Our purpose is to bound $\mathrm{Red}^{\star}_{p^e}(i + ap^\varepsilon + \langle \boldsymbol{w}, \boldsymbol{k} \rangle)$. We see that

$$i + ap^\varepsilon + \langle \boldsymbol{w}, \boldsymbol{k} \rangle = i + ap^\varepsilon + \sum_{\ell=1}^{\eta} \ell \left(\sum_{r=0}^{\varepsilon-1} k_\ell^{(r)} p^r + \sum_{r=\varepsilon}^{e-1} k_\ell^{(r)} p^r \right) = R_1 + p^\varepsilon R_2$$

where $R_1 \coloneqq i + \sum_{\ell=0}^{\eta} \ell \sum_{r=0}^{\varepsilon-1} k_\ell^{(r)} p^r$ and $R_2 \coloneqq a + \sum_{\ell=0}^{\eta} \ell \sum_{r=\varepsilon}^{e-1} k_\ell^{(r)} p^{r-\varepsilon}$.

One can check that $R_1 \leq i + \eta j \leq p^\varepsilon - \alpha - \eta$. It remains to deal with R_2. Let us write $R_2 = \sum_{r=0}^{e-\varepsilon-1} R_2^{(r)} p^r + R_2' p^{e-\varepsilon}$ with $R_2' \leq \eta$. Then

$$p^\varepsilon R_2 = (p^e - 1) R_2' + R_2' + \sum_{r=0}^{e-\varepsilon-1} R_2^{(r)} p^{\varepsilon + r} \equiv^{\star}_{p^e} R_2' + \sum_{r=\varepsilon}^{e-1} R_2^{(r)} p^r\,.$$

Therefore,

$$i + ap^\varepsilon + \langle \boldsymbol{w}, \boldsymbol{k} \rangle \equiv^{\star}_{p^e} R_1 + R_2' + \sum_{r=0}^{\varepsilon-1} R_2^{(r)} p^{\varepsilon + r} \leq p^\varepsilon - \alpha - \eta + \eta + p^\varepsilon (p^{e-\varepsilon} - 1) \leq p^e - \alpha,$$

which proves that $(i + ap^\varepsilon, j + bp^\varepsilon)$ belongs to $D(p^e, p^e - \alpha, \eta)$. □

Notice that $\mathrm{WRM}^{\eta}_{p^\varepsilon}(p^\varepsilon - \alpha - \eta) = \{\boldsymbol{0}\}$ if $\alpha \geq p^\varepsilon$. Therefore let us set $e_\alpha = \lfloor \log_p \alpha \rfloor$ and define

$$\mathcal{W}(\varepsilon, a, b) \coloneqq \left\{ (i + ap^\varepsilon, j + bp^\varepsilon) \mid (i,j) \in \mathrm{Deg}\,\mathrm{WRM}^{\eta}_{p^\varepsilon}(p^\varepsilon - \alpha - \eta) \right\}$$

as the degree set of weighted Reed-Muller codes over $\mathbb{F}_{p^e}$, translated by $(ap^\varepsilon, bp^\varepsilon)$. Proposition 5.5 ensures that:

$$D(p^e, p^e - \alpha, \eta) \supset \bigcup_{\varepsilon=e_\alpha+1}^{e} \bigcup_{0\le a,b<p^{e-\varepsilon}} \mathcal{W}(\varepsilon, a, b). \tag{5}$$

Equation (5) helps us to obtain a first lower bound on the dimension of lifted codes. It is clear that $\mathcal{W}(\varepsilon, a, b) \cap \mathcal{W}(\varepsilon, a', b') = \varnothing$ if $(a', b') \neq (a, b)$. Unfortunately, the union given in (5) is not disjoint, as illustrated in Figure 6. The main reason is that $\mathcal{W}(\varepsilon, a, b)$ contains a certain number of degree sets of the form $\mathcal{W}(\varepsilon', a', b')$, for $\varepsilon' < \varepsilon$. We compute this precise number in Lemma 5.6.

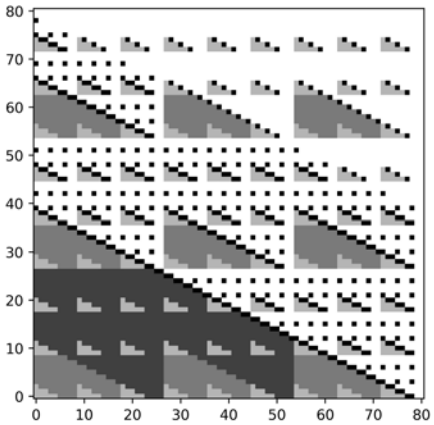


Figure 6: Embedding of $\mathcal{W}(\varepsilon, a, b) \subset D(3^5, 3^5 - 3, 2)$ with $\varepsilon \le 5$.

For $m \ge 0$, we set

$$T_m(p, \eta) = T_m := \left(\left\lfloor \frac{p^m - 1}{\eta} \right\rfloor + 1 \right) \left(p^m - \frac{\eta}{2} \left\lfloor \frac{p^m - 1}{\eta} \right\rfloor \right). \tag{6}$$

One can check that T_m is a positive integer which counts the number of pairs of non-negative integers (u, v) such that $u + \eta v \le p^m - 1$.

Lemma 5.6. *Fix $e_\alpha + 1 \le \varepsilon_1 \le \varepsilon_2 \le e$. Then, for all $0 \le a_2, b_2 < p^{e-\varepsilon_2}$, we have:*

$$\left| \{(a_1, b_1) \mid \mathcal{W}(\varepsilon_1, a_1, b_1) \subset \mathcal{W}(\varepsilon_2, a_2, b_2)\} \right| = T_{\varepsilon_2 - \varepsilon_1}.$$

Proof. We first notice that $\mathcal{W}(\varepsilon_1, a_1, b_1) \subseteq \mathcal{W}(\varepsilon_2, a_2, b_2)$ if and only if

$$\mathcal{W}(\varepsilon_1, a_1 - a_2 p^{\varepsilon_2 - \varepsilon_1}, b_1 - b_2 p^{\varepsilon_2 - \varepsilon_1}) \subseteq \mathcal{W}(\varepsilon_2, 0, 0).$$

Moreover, for $u, v \ge 0$, we see that $\mathcal{W}(\varepsilon_1, u, v) \subseteq \mathcal{W}(\varepsilon_2, 0, 0)$ if and only if for every $i, j \ge 0$, we have

$$i + \eta j \le p^{\varepsilon_1} - \alpha - \eta \implies i + u p^{\varepsilon_1} + \eta(j + v p^{\varepsilon_1}) \le p^{\varepsilon_2} - \alpha - \eta,$$

which is equivalent to $(u+\eta v)p^{\varepsilon_1} \leq p^{\varepsilon_2} - p^{\varepsilon_1}$. It remains to notice that $T_{\varepsilon_2-\varepsilon_1}$ counts the number of non-negative integers u, v such that

$$u + \eta v \leq \left\lfloor \frac{p^{\varepsilon_2} - p^{\varepsilon_1}}{p^{\varepsilon_1}} \right\rfloor = p^{\varepsilon_2-\varepsilon_1} - 1\,.$$

□

For any $m \in \mathbb{N}$, we set

$$\begin{aligned} W_m(\alpha) &\coloneqq |\operatorname{Deg} \mathrm{WRM}^{\eta}_{p^m}(p^m - \alpha - \eta)| = |\mathcal{W}(m,0,0)| \\ &= \left\lfloor \frac{p^m - \alpha}{\eta} \right\rfloor \left(p^m - \alpha + 1 - \frac{\eta}{2}\left(\left\lfloor \frac{p^m - \alpha}{\eta} + 1 \right\rfloor \right) \right)\,. \end{aligned} \tag{7}$$

Let us also define $N_0 \coloneqq 1$, and

$$N_m \coloneqq p^{2m} - \sum_{\nu=0}^{m-1} N_\nu T_{m-\nu} \tag{8}$$

as the number of triangles $\mathcal{W}(e-m, a, b)$ that are not included in any $\mathcal{W}(e-m', a', b')$ with $m' \leq m$. Notice that, equivalently, we have

$$p^{2m} = \sum_{\nu=0}^{m} N_\nu T_{m-\nu}\,. \tag{9}$$

Example 5.7. As displayed in Figure 6, for $p = 3$ and $\eta = 2$, the first terms of the sequence (N_m) are 1, 5, 36, 264.

The following theorem can be proven by a simple counting argument.

Theorem 5.8. *Fix $\alpha \geq 2$, $\eta \geq 1$ and a prime power $q = p^e$. Let $(W_m(\alpha))_{m \leq e}$ and $(N_m)_{m \leq e}$ be the sequences defined above. Then, the dimension $|D(q, q-\alpha, \eta)|$ of $\mathrm{Lift}^{\eta}\,\mathrm{RS}_q(q-\alpha)$ is lower bounded by*

$$\sum_{\varepsilon=0}^{e-e_\alpha-1} W_{e-\varepsilon}(\alpha) N_\varepsilon\,,$$

where $e_\alpha = \lfloor \log_p \alpha \rfloor$.

5.2.2 Asymptotical behaviour of the sequences (T_m), $(W_m(\alpha))$ and (N_m)

Let us sum up the asymptotics of the sequences introduced in the previous paragraph.

Lemma 5.9. *When $m \to +\infty$,*

1. $T_m \sim \frac{p^{2m}}{2\eta}$,
2. $W_m(\alpha) \sim T_m$ *for any* $\alpha \geq 2$.

The following technical lemma will be useful in the proof of Theorem 5.11.

Lemma 5.10. *Let (N_m) be the sequence defined in* (8)*. Then*

$$\lim_{m\to+\infty} \frac{1}{p^{2m}} \sum_{\ell=0}^{m} N_\ell = 0.$$

Proof. Let us first prove that the series $\sum_{\ell\geq 0} \frac{N_\ell}{p^{2\ell}}$ is convergent. Fix $\delta > 0$.

By Lemma 5.9, $T_m \sim \frac{p^{2m}}{2\eta}$. Hence there exists $L \in \mathbb{N}$ such that for any $\ell \geq L$, $p^{2\ell} \leq (2\eta+\delta)T_\ell$. Therefore, using (8), we get

$$\begin{aligned}
\sum_{\ell=0}^{m} \frac{N_\ell}{p^{2\ell}} &= \sum_{\ell=0}^{m-L} \frac{N_\ell}{p^{2\ell}} + \sum_{\ell=m-L+1}^{m} \frac{N_\ell}{p^{2\ell}} \\
&\leq \frac{1}{p^{2m}} \sum_{\ell=0}^{m-L} N_\ell p^{2(m-\ell)} + \sum_{\ell=m-L+1}^{m} \frac{N_\ell}{p^{2\ell}} \\
&\leq \frac{(2\eta+\delta)}{p^{2m}} \sum_{\ell=0}^{m-L} N_\ell T_{m-\ell} + \sum_{\ell=m-L+1}^{m} \frac{N_\ell}{p^{2\ell}},
\end{aligned}$$

since $m-\ell \geq L \iff \ell \leq m-L$.

Notice that all the terms of the first sum are non-negative. Hence by (9), we have $\sum_{\ell=0}^{m-L} N_\ell T_{m-\ell} \leq p^{2m}$, leading to

$$\sum_{\ell=0}^{m} \frac{N_\ell}{p^{2\ell}} \leq (2\eta+\delta) + \sum_{\ell=m-L+1}^{m} \frac{N_\ell}{p^{2\ell}}.$$

It remains to notice that the right handside sum is finite, and each summand $N_\ell/p^{2\ell}$ is trivially bounded by 1. Therefore $\sum_{\ell\geq 0} N_\ell/p^{2\ell}$ is convergent.

Denote by S its limit. We know there exists $M \in \mathbb{N}$ such that, for any $m \geq M$ it holds that

$$\left| S - \sum_{\ell=0}^{m} \frac{N_\ell}{p^{2\ell}} \right| \leq \delta\,.$$

As a consequence, $\sum_{\ell=M+1}^{m} N_\ell/p^{2\ell} \leq 2\delta$ and since $\sum_{\ell=0}^{M} N_\ell/p^{2\ell} \leq S$, we get

$$\frac{1}{p^{2m}} \sum_{\ell=0}^{m} N_\ell = \sum_{\ell=0}^{M} \frac{N_\ell}{p^{2\ell}} \frac{1}{p^{2(m-\ell)}} + \sum_{\ell=M+1}^{m} \frac{N_\ell}{p^{2\ell}} \leq \frac{S}{p^{2(m-M)}} + 2\delta,$$

which concludes the proof. □

5.2.3 Asymptotics of the rate of $\mathrm{Lift}^\eta \mathrm{RS}_q(q-\alpha)$ when $q \to \infty$ and α is fixed

Theorem 5.11. *Let $\alpha \geq 2$, $\eta \geq 1$ and p be a prime number. Define $e_\alpha = \lfloor \log_p \alpha \rfloor$, and consider the sequence of codes $\mathcal{C}_e = \mathrm{Lift}^\eta \mathrm{RS}_{p^e}(p^e - \alpha)$, for $e \geq e_\alpha$. Then, the information rate R_e of $\mathcal{C}_e$ approaches 1 when $e \to \infty$.*

Proof. By Lemma 5.9, $W_m(\alpha) \sim_{m\to+\infty} T_m$. Fix $\delta > 0$ and let $M \geq e_\alpha$ such that for every $m \geq M$, $W_m(\alpha) \geq (1-\delta)T_m$.

Using Theorem 5.8, we thus get

$$\begin{aligned}
|D(p^e, p^e-\alpha, \eta)| &\geq \sum_{\varepsilon=0}^{e-e_\alpha-1} W_{e-\varepsilon}(\alpha) N_\varepsilon \\
&\geq (1-\delta) \sum_{\varepsilon=0}^{e-M} T_{e-\varepsilon} N_\varepsilon + \sum_{\varepsilon=e-M+1}^{e-e_\alpha-1} W_{e-\varepsilon}(\alpha) N_\varepsilon \\
&\geq (1-\delta) \left(p^{2e} - \sum_{\varepsilon=e-M+1}^{e} T_{e-\varepsilon} N_\varepsilon \right) + \sum_{\varepsilon=e-M+1}^{e-e_\alpha-1} W_{e-\varepsilon}(\alpha) N_\varepsilon \\
&\geq (1-\delta) \left(p^{2e} - T_{M-1} \sum_{\varepsilon=e-M+1}^{e} N_\varepsilon \right) + W_{M-1}(\alpha) \sum_{\varepsilon=e-M+1}^{e-e_\alpha-1} N_\varepsilon \,.
\end{aligned}$$

Then, by Lemma 5.10, both terms $\sum_{\varepsilon=e-M+1}^{e} N_\varepsilon / p^{2e}$ and $\sum_{\varepsilon=e-M+1}^{e-e_\alpha-1} N_\varepsilon / p^{2e}$ vanish when $e \to \infty$. Hence we get

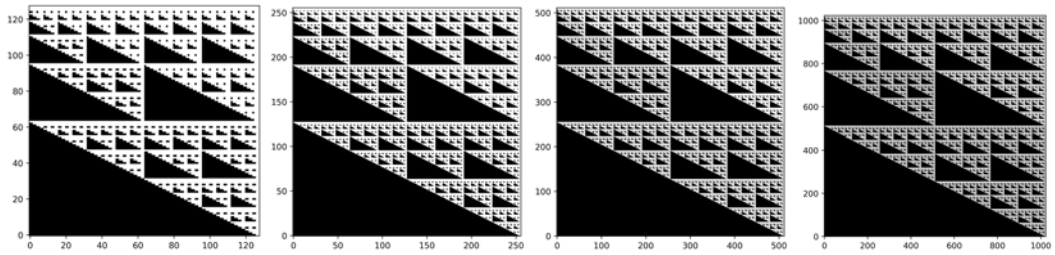
$$R_e = \frac{|D(q, q-\alpha, \eta)|}{p^{2e}} \to 1 \,.$$

□

Example 5.12. Let us give some numerical computations of the dimension and information rate of $\mathrm{Lift}^\eta \mathrm{RS}_{p^e}(p^e - \alpha)$ illustrating Theorem 5.11.

p	η	α	e	$n = p^{2e}$	$k = \lvert D(p^e, p^{e-c}, \eta)\rvert$	$R = k/n$
2	2	2	3	64	25	0.3906
			4	256	121	0.4727
			5	1024	561	0.5479
			6	4096	2513	0.6135
			7	16384	10977	0.6700
			8	65536	47073	0.7183
			9	262144	199105	0.7595
			10	1048576	833345	0.7947
2	2	16	6	4096	781	0.1907
			7	16384	4944	0.3018
			8	65536	26335	0.4018
			9	262144	128142	0.4888
			10	1048576	590885	0.5635
2	4	2	3	64	16	0.2500
			4	256	71	0.2773
			5	1024	331	0.3232
			6	4096	1506	0.3677
			7	16384	6749	0.4119

In Figure 7, we also represent the degree sets of $\mathrm{Lift}^2 \mathrm{RS}_{2^e}(2^e - \alpha)$ for $\alpha = 3$ and $e \in \{7, 8, 9, 10\}$.



(a) $e = 7$ (b) $e = 8$ (c) $e = 9$ (d) $e = 10$

Figure 7: Representation of the degree set of $\mathrm{Lift}^2 \mathrm{RS}_{2^e}(2^e - \alpha)$ for $\alpha = 3$ and different values of e.

5.2.4 Asymptotics of the rate of $\mathrm{Lift}^\eta \mathrm{RS}_q(\lfloor \gamma q \rfloor)$ when $q \to \infty$ and γ is fixed

Theorem 5.13. *Let $c \geq 1$, $\eta \geq 1$ and p be a prime number. Define $\gamma = 1 - p^{-c}$, and consider the sequence of codes $\mathcal{C}_e = \mathrm{Lift}^\eta \mathrm{RS}_{p^e}(\gamma p^e)$, for $e \geq c + 1$. Then, the information rate R_e of $\mathcal{C}_e$ satisfies:*

$$\lim_{e \to \infty} R_e \geq \frac{1}{2\eta} \sum_{\varepsilon=0}^{c-1} (p^{-\varepsilon} - p^{-c})^2 N_\varepsilon \,.$$

Proof. By Proposition 5.5,

$$|D(p^e, p^e - p^{e-c}, \eta)| \geq \sum_{\varepsilon=0}^{c-1} W_{e-\varepsilon}(p^{e-c}) N_\varepsilon \,.$$

Moreover, using (7), for every fixed $\varepsilon \leq c - 1$ we have

$$\lim_{e \to \infty} W_{e-\varepsilon}(p^{e-c}) = p^{2e} \frac{(p^{-\varepsilon} - p^{-c})^2}{2\eta} \,.$$

Then

$$\lim_{e \to \infty} R_e \geq \frac{1}{2\eta} \sum_{\varepsilon=0}^{c-1} (p^{-\varepsilon} - p^{-c})^2 N_\varepsilon \,.$$

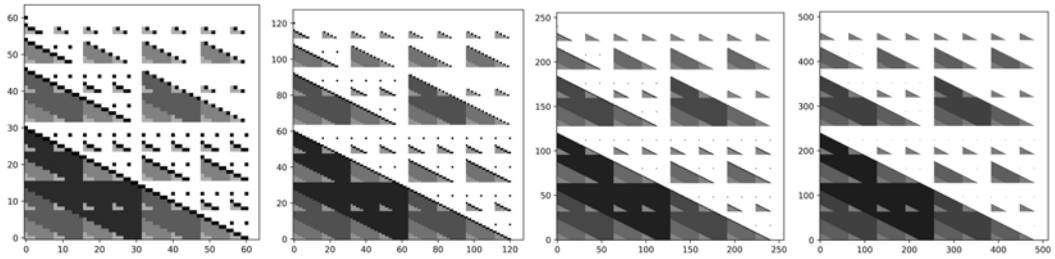
□

Example 5.14. Let us give some numerical computations, illustrating the tightness of the

bound given in Theorem 5.13.

p	η	c	e	$n = p^{2e}$	$k = \lvert D(p^e, p^{e-c}, \eta)\rvert$	$R = k/n$
2	2	4	5	1024	561	0.5479
			6	4096	1861	0.4543
			7	16384	6843	0.4177
			8	65536	26335	0.4018
			9	262144	103431	0.3946
			10	1048576	410071	0.3911
			lower bound on the asymptotic rate			0.3877
2	2	6	7	16384	10977	0.6700
			8	65536	39431	0.6017
			9	262144	150729	0.5750
			10	1048576	590885	0.5635
			lower bound on the asymptotic rate			0.5533
2	4	3	4	256	71	0.2773
			5	1024	205	0.2002
			6	4096	699	0.1707
			7	16384	2587	0.1579
			lower bound on the asymptotic rate			0.1465
5	2	2	3	15625	5789	0.3705
			4	390625	132109	0.3382
			5	9765625	3259709	0.3338
			lower bound on the asymptotic rate			0.3328

In Figure 8, we also represent the degree sets $D(2^e, 2^e - 2^{e-c}, \eta)$ for $p = 2$, $\eta = 2$, $c = 4$ and $e \in \{5, 6, 7, 8\}$.



(a) $e = 5$ (b) $e = 6$ (c) $e = 7$ (d) $e = 8$

Figure 8: Representation of the degree set of $\mathrm{Lift}^2\,\mathrm{RS}_{2^e}(2^e - 2^{e-c})$ for $c = 4$ and different values of e. Note that in each case, the number of differents shades of grey is constant and equal to c.

Acknowledgements

Part of this work was done while the first author was affiliated to LIX, École Polytechnique, Inria & CNRS UMR 7161, University Paris-Saclay, Palaiseau, France. The first author is now funded by the French *Direction Générale de l'Armement*, through the *Pôle d'excellence cyber*. This work was also funded in part by the grant ANR-15-CE39-0013-01 "Manta" from the French National Research Agency, which gave the authors the opportunity to work together.

References

[ACG+17] Yves Aubry, Wouter Castryck, Sudhir R. Ghorpade, Gilles Lachaud, Michael E. O'Sullivan, and Samrith Ram. Hypersurfaces in Weighted Projective Spaces Over Finite Fields with Applications to Coding Theory. In Everett W. Howe, Kristin E. Lauter, and Judy L. Walker, editors, *Algebraic Geometry for Coding Theory and Cryptography*, pages 25–61, Cham, 2017. Springer International Publishing.

[ALS14] Daniel Augot, Françoise Levy-dit-Vehel, and Abdullatif Shikfa. A storage-efficient and robust private information retrieval scheme allowing few servers. In Dimitris Gritzalis, Aggelos Kiayias, and Ioannis G. Askoxylakis, editors, *Cryptology and Network Security - 13th International Conference, CANS 2014, Heraklion, Crete, Greece, October 22-24, 2014. Proceedings*, volume 8813 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2014.

[BIKR02] Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and Jean-François Raymond. Breaking the $O(n^{1/(2k-1)})$ Barrier for Information-Theoretic Private Information Retrieval. In *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*, pages 261–270. IEEE Computer Society, 2002.

[BS02] Amos Beimel and Yoav Stahl. Robust information-theoretic private information retrieval. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers*, volume 2576 of *Lecture Notes in Computer Science*, pages 326–341. Springer, 2002.

[CGKS95] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private Information Retrieval. In *36th Annual Symposium on Foundations of Computer Science, Milwaukee, Wisconsin, 23-25 October 1995*, pages 41–50. IEEE Computer Society, 1995.

[DG16] Zeev Dvir and Sivakanth Gopi. 2-Server PIR with Subpolynomial Communication. *J. ACM*, 63(4):39:1–39:15, 2016.

[Efr12] Klim Efremenko. 3-Query Locally Decodable Codes of Subexponential Length. *SIAM J. Comput.*, 41(6):1694–1703, 2012.

[FHGHK17] Ragnar Freij-Hollanti, Oliver W. Gnilke, Camilla Hollanti, and David A. Karpuk. Private Information Retrieval from Coded Databases with Colluding Servers. *SIAM J. Appl. Algebra Geometry*, 1(1):647–664, 2017.

[GKS13] Alan Guo, Swastik Kopparty, and Madhu Sudan. New Affine-Invariant Codes from Lifting. In Robert D. Kleinberg, editor, *Innovations in Theoretical Computer Science, ITCS '13, Berkeley, CA, USA, January 9-12, 2013*, pages 529–540. ACM, 2013.

[GT13] Olav Geil and Casper Thomsen. Weighted Reed-Muller codes revisited. *Des. Codes Cryptogr.*, 66(1-3):195–220, 2013.

[Guo16] Alan Guo. High-Rate Locally Correctable Codes via Lifting. *IEEE Trans. Information Theory*, 62(12):6672–6682, 2016.

[KRGiA17] Siddhartha Kumar, Eirik Rosnes, and Alexander Graell i Amat. Private Information Retrieval in Distributed Storage Systems using an Arbitrary Linear Code. In *2017 IEEE International Symposium on Information Theory, ISIT 2017, Aachen, Germany, June 25-30, 2017*, pages 1421–1425. IEEE, 2017.

[KT00] Jonathan Katz and Luca Trevisan. On the Efficiency of Local Decoding Procedures for Error-Correcting Codes. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 80–86. ACM, 2000.

[Lav18a] Julien Lavauzelle. *Codes with locality: constructions and applications to cryptographic protocols*. Phd thesis, Université Paris-Saclay, 2018.

[Lav18b] Julien Lavauzelle. Lifted Projective Reed-Solomon Codes. *Designs, Codes and Cryptography*, 2018. To appear.

[Luc78] Édouard Lucas. Théorie des Fonctions Numériques Simplement Périodiques. *American Journal of Mathematics*, 1(3):197–240, 1878.

[Sør92] Anders Bjært Sørensen. Weighted Reed-Muller codes and algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 38(6):1821–1826, 1992.

[SRR14] Nihar B. Shah, K. V. Rashmi, and Kannan Ramchandran. One Extra Bit of Download Ensures Perfectly Private Information Retrieval. In *2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29 - July 4, 2014*, pages 856–860. IEEE, 2014.

[TGR18] Razan Tajeddine, Oliver W. Gnilke, and Salim El Rouayheb. Private information retrieval from MDS coded data in distributed storage systems. *IEEE Trans. Information Theory*, 64(11):7081–7093, 2018.

[Yek08] Sergey Yekhanin. Towards 3-query Locally Decodable Codes of Subexponential Length. *J. ACM*, 55(1):1:1–1:16, 2008.

[Yek12] Sergey Yekhanin. Locally Decodable Codes. *Foundations and Trends in Theoretical Computer Science*, 6(3):139–255, 2012.

Rémusé en français - Cette thèse, à la frontière entre les mathématiques et l'informatique, est consacrée en partie à l'étude des paramètres et des propriétés des codes de Goppa sur les surfaces de Hirzebruch.

D'un point de vue arithmétique, la théorie des codes correcteurs a ravivé la question du nombre de points rationnels d'une variété définie sur un corps fini, qui semblait résolue par la formule de Lefschetz. La distance minimale de codes géométriques donne un majorant du nombre de points rationnels d'une hypersurface d'une variété donnée et de classe de Picard fixée. Ce majorant étant le plus souvent atteint pour les courbes très réductibles, il est naturel de se concentrer sur les courbes irréductibles pour affiner les bornes. On présente une stratégie globale pour majorer le nombre de points d'une variété en fonction de son ambiant et d'invariants géométriques, notamment liés à la théorie de l'intersection. De plus, une méthode de ce type pour les courbe d'une surface torique est développée en adaptant l'idée de F.J Voloch et K.O. Sthör aux variétés toriques.

Enfin, on s'intéresse aux protocoles de *Private Information Retrivial*, qui visent à assurer qu'un utilisateur puisse accéder à une entrée d'une base de données sans révéler d'information sur l'entrée au propriétaire de la base de données. Un protocole basé sur des codes sur des plans projectifs pondérés est proposé ici. Il améliore les protocoles existants en résistant à la collusion de serveurs, au prix d'une grande perte de capacité de stockage. On pallie ce problème grâce à la méthode du lift qui permet la construction de familles de codes asymptotiquement bonnes, avec les mêmes propriétés locales.

English summary - A part of this thesis, at the interface between Computer Science and Mathematics, is dedicated to the study of the parameters ans properties of Goppa codes over Hirzebruch surfaces.

From an arithmetical perspective, the question about number of rational points of a variety defined over a finite field, which seemed dealt with by Lefchetz formula, regained interest thanks to error correcting codes. The minimum distance of an algebraic-geometric codes provides an upper bound of the number of rational points of a hypersurface of a given variety and with a fixed Picard class. Since reducible curves are most likely to reach this bound, one can focus on irreducible curves to get sharper bounds. A global strategy to bound the number of points on a variety depending on its ambient space and some of its geometric invariants is exhibited here. Moreover we develop a method for curves on toric surfaces by adapting F.J. Voloch et K.O. Sthör's idea on toric varieties.

Finally, we interest in *Private Information Retrivial* protocols, which aim to ensure that a user can access an entry of a database without revealing any information on it to the database owner. A PIR protocol based on codes over weighted projective planes is displayed here. It enhances other protocols by offering a resistance to servers collusions, at the expense of a loss of storage capacity. This issue is fixed by a lifting process, which leads to asymptotically good families of codes, with the same local properties.