THÈSE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR
DE L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE MATHÉMATIQUES ET

INFORMATIQUE

MATHÉMATIQUES FONDAMENTALES

Par **Fabrice DRAIN**

Algèbres cycliques non commutatives en théorie des codes : Applications à la dualité et au décodage

Noncommutative Cyclic Algebras in Coding Theory With Applications to Duality and Decoding

Sous la direction de : **Xavier CARUSO**
Co-directrice : **Elena BERARDINI**

Soutenue le 18 septembre 2026
Membres du jury :

M. Xavier CARUSO	Directeur de recherche	Université de Bordeaux	Directeur
Mme Elena BERARDINI	Chaire de Professeure Junior	Université de Bordeaux	Co-directrice
M. Emmanuel HALLOUIN	Maître de conférences	Université Toulouse	Rapporteur
M. Christian MAIRE	Professeur des universités	Université de Franche-Comté	Rapporteur
Mme Delphine BOUCHER	Maîtresse de conférences	Université de Rennes	Examinatrice
M. Yves AUBRY	Maître de conférences	Université de Toulon	Examinateur
M. Alin BOSTAN	Directeur de recherche	Inria Saclay	Examinateur
M. Jean-Marc COUVEIGNES	Professeur des universités	Université de Bordeaux	Examinateur et Président du jury

Algèbres cycliques non commutatives en théorie des codes : applications à la dualité et au décodage

Mots-clés : Courbes algébriques, codes en métrique somme-rang, décodage, algèbres à division
Résumé : En 2023, E. Berardini et X. Caruso ont introduit des codes en métrique somme-rang, appelés codes de géométrie algébrique linéarisés (LAG), obtenus par évaluation d'espaces de Riemann–Roch sur des algèbres à division définies sur des corps de fonctions. Ces codes généralisent à la fois les codes de géométrie algébrique et les codes de Reed–Solomon linéarisés, et combinent leurs avantages. Ils sont presque à distance maximale pour la métrique somme-rang : leur défaut par rapport à la borne de Singleton est égal au genre de l'ordre défini par une jauge de l'algèbre à division sous-jacente, tandis que leur longueur asymptotique n'est pas limitée par la taille de l'alphabet. L'objectif principal de cette thèse est de concevoir et prouver un algorithme de décodage polynomial pour ces codes LAG.

Plus généralement, nous nous intéressons aux algèbres cycliques non commutatives en théorie des codes. Notre approche repose sur les polynômes tordus. Notre première contribution consiste à compter et à énumérer les codes cycliques tordus autoduaux sur un corps fini à l'aide d'un algorithme de complexité cubique, dont nous fournissons une implémentation en SageMath.

Dans notre seconde et principale contribution, nous proposons un algorithme de décodage polynomial pour les codes LAG sous l'hypothèse de non-ramification aux places d'évaluation. Pour y parvenir, nous établissons un théorème de Riemann–Roch pour notre algèbre à division et montrons que les duaux des codes LAG sont eux-mêmes des codes LAG définis sur l'algèbre à division adjointe. Nous fournissons en outre une implémentation en SageMath de cet algorithme de décodage.

Nous montrons également que notre théorème de Riemann–Roch se déduit d'un théorème plus général de Tamagawa, grâce au calcul du discriminant de l'ordre associé à notre jauge. Nous appliquons ensuite cette même théorie de Tamagawa à la construction de codes LAG plus généraux, définis sur des algèbres abéliennes (ALAG), *i.e.*, des algèbres quotients d'anneaux de polynômes d'Ore multivariés à coefficients dans une extension abélienne de corps de fonctions. Enfin, nous fournissons une implémentation en SageMath d'un algorithme de décodage pour les codes ALAG, dont la preuve théorique reste inachevée.

Noncommutative Cyclic Algebras in Coding Theory: Applications to Duality and Decoding

Keywords: Algebraic curves, sum-rank metric codes, decoding, division algebras
Abstract: In 2023, E. Berardini and X. Caruso introduced sum-rank metric codes, called linearized algebraic geometry (LAG) codes, obtained by evaluating Riemann–Roch spaces on division algebras over function fields. These codes generalize both algebraic geometry codes and linearized Reed–Solomon codes, thereby combining their advantages. They have almost maximum sum-rank distance: their defect with respect to the Singleton bound is equal to the genus of the order defined by a gauge of the underlying division algebra, while their asymptotic length is not limited by the size of the alphabet. The main objective of this thesis is to design and prove the correctness of a polynomial-time decoding algorithm for these LAG codes.

More generally, we study noncommutative cyclic algebras in coding theory. Our approach is based on skew polynomials. Our first contribution is to count and enumerate self-dual skew cyclic codes over a finite field using an algorithm of cubic complexity, for which we provide a SageMath implementation.

Our second and main contribution is a polynomial-time decoding algorithm for LAG codes under the assumption that the algebra is unramified at the evaluation places. To achieve this, we establish a Riemann–Roch theorem for our division algebra and show that the duals of LAG codes are themselves LAG codes defined over the adjoint division algebra. We also provide a SageMath implementation of this decoding algorithm.

We further show that our Riemann–Roch theorem can be deduced from a more general theorem of Tamagawa by computing the discriminant of the order associated with our gauge. We then apply the same Tamagawa theory to construct more general LAG codes defined over abelian algebras (ALAG), *i.e.*, quotient algebras of multivariate Ore polynomial rings with coefficients in an abelian extension of function fields. Finally, we provide a SageMath implementation of a decoding algorithm for ALAG codes, whose theoretical proof remains incomplete.

Unité de recherche UMR 5251 Université, 33000 Bordeaux, France.

Remerciements

Avant tout, je tiens à remercier mon directeur de thèse Xavier Caruso pour m'avoir donné la chance de réaliser cette thèse enthousiasmante. Ce fut extrêmement enrichissant et instructif de travailler sous sa direction. Il m'a fait bénéficier de sa vision profonde de la recherche et m'en a appris la rigueur inhérente, tout en me laissant une entière autonomie. Je remercie également Elena Berardini, qui a eu la gentillesse de bien vouloir co-diriger ma thèse et qui m'a aussi beaucoup aidé dans mon effort de rigueur et de synthèse. Enfin, je remercie mes rapporteurs pour leurs très bon rapports de thèse ainsi que mon jury en général pour l'intérêt qu'il a porté à cette thèse.

Je repense avec beaucoup de gratitude à mon professeur de classes préparatoires au lycée Charlemagne, Monsieur Choquet, qui m'a initié aux fondamentaux des mathématiques ainsi qu'à Emmanuel Lecouturier, qui, plus tard, m'a fait découvrir la théorie algébrique des nombres alors que j'étais encore ingénieur dans les technologies financières de paiement. C'est grâce à la rencontre de ce dernier que je me suis inscrit à un cursus de M2 en formation continue à l'université Paris Cité en mathématiques fondamentales. Je tiens à remercier à ce propos Marco Maculan, mon directeur de mémoire de M2, pour son encadrement et pour m'avoir orienté.

J'ai beaucoup apprécié l'environnement de travail à l'institut mathématique de Bordeaux. Je remercie Cyril et les services informatiques pour leur disponibilité. Je remercie Bill Allombert et Sébastien Labbé pour leurs conseils avisés en calcul symbolique notamment lors des matinées SageMath. Je remercie chaleureusement Aurel Page pour nos discussions sur mon travail de thèse et son suivi au sein du comité de suivi individuel.

J'ai aussi eu la chance de pouvoir faire la connaissance enrichissante de nombreux camarades doctorants. Je remercie Nicolas pour son sens de l'improvisation et sa bonne humeur constante, Fabrice pour nos discussions politiques enflammées, Guilhelm pour ses concerts décoiffants, Pierrick pour son engagement sur les questions climatiques, Jean pour sa rigueur dans nos discussions mathématiques, et d'autres encore, merci à eux. Je remercie aussi toute la communauté de l'ANR Barracouda pour nos retraites amicales ainsi que l'équipe CANARI de l'Inria, notamment son responsable Damien Robert, dont les séminaires ont rythmé ces trois années de thèse.

Enfin, et surtout, je remercie Inna, mon épouse, qui m'a constamment soutenu et sans qui cette thèse n'aurait pas eu lieu.

Contents

Résumé étendu en français **11**

Introduction **25**

1 Historical Context 25
2 Motivation: Application of Skew Polynomials in Coding Theory 26
3 Contributions 28
3.1 Publications 28
3.2 Enumeration of Self-dual Skew Cyclic Codes 28
3.3 Duality and Decoding of LAG codes 29
3.3.1 Riemann–Roch and Duality Theorem for Cyclic Algebras 30
3.3.2 Duality and Decoding of LAG codes 32
3.4 Alternative Proof of our Riemann–Roch theorem 33
3.5 Decoding Shortened LAG and ALAG Codes 35
3.6 SageMath Implementations 36
4 Organization of the Thesis 37

I Self-dual Skew Cyclic Codes **39**

1 Witt's Decomposition Theorem 39
2 Article: Self-dual Skew Cyclic Codes 39
2.1 Abstract of the article [CD25] 39
2.2 Introduction 40
2.3 From skew cyclic codes to finite geometry 44
2.3.1 Definition of skew cyclic codes 44
2.3.2 The evaluation isomorphism 45
2.3.3 Adjunctions on $\mathbf{E}_k$ and related spaces 46
2.3.4 Vector space duality 50
2.4 Counting and generating self-dual skew cyclic codes 51
2.4.1 Existence criterion 52
2.4.2 Counting self-dual skew cyclic codes 54
2.4.3 Random generation of self-dual skew cyclic codes . . . 57
2.4.4 Enumeration of self-dual skew cyclic codes 65
2.5 Enumeration in the purely inseparable case 68

3 An implementation in SageMath 72
3.1 SageMath enumeration results in the separable case 72
3.2 SageMath enumeration results in the inseparable case 76

II Duality and Decoding of Linearized Algebraic Geometry Codes 77
1 Reminders on algebraic curves 77
1.1 Riemann–Roch Theorem and Serre duality 77
1.2 Different, Discriminant and Riemann–Hurwitz formula 78
2 Article: Duality and Decoding of Linearized Algebraic Geometry Codes 79
2.1 Abstract of the article [BCD26] 79
2.2 Introduction 79
2.3 Riemann–Roch theorem on division algebras 82
2.3.1 The case of numerical divisors 83
2.3.2 Riemann theorem for extended divisors 87
2.3.3 Differentials and residues 90
2.4 Application to linearized Algebraic Geometry codes 96
2.4.1 Duality 98
2.4.2 Decoding 99
2.5 Conclusion 104
3 Construction, Duality and Decoding of Shortened LAG codes 105
3.1 Construction of Shortened LAG codes 105
3.2 Duality of Shortened LAG codes 106
3.3 Parameters and Decoding of Shortened LAG codes 107
4 LAG Code Construction 107
4.1 Artin-Schreier LAG Code Construction 108
4.2 Artin–Schreier–Witt LAG Code Construction 110
5 Conjugacy with SageMath LAG codes 113
6 Implementation of the LAG decoding algorithm in SageMath 114
6.1 SageMath use case 114
6.2 SageMath benchmark 119

III Tamagawa's Theory 121
1 Theoretical Setting 121
1.1 Skolem–Noether and Wedderburn Theorem 121
1.2 Exponent and Index 122
1.3 Different, Discriminants and Maximal Orders 123
2 Gauge Order 126
2.1 Gauge Orders and Discriminant 126
2.2 Maximality Criterion for the Gauge Orders 129
3 Tamagawa's Theorem 130

3.1 Riemann Theorem for Parallelotopes 131
3.2 Riemann–Roch Theorem for parallelotopes 134
4 The Role of Tamagawa's Theorem in Our Riemann–Roch Proof 137
4.1 Our Riemann Theorem as a Corollary 139
4.2 Perspectives on Serre Duality 140
5 Construction and Decoding of Abelian LAG codes (ALAG) 141
5.1 Riemann Theorem for Abelian Algebras 141
5.2 Riemann–Roch Theorem for Abelian Algebras 147
5.3 ALAG Code Construction 150
5.4 SageMath Implementation of ALAG Decoding 151

IV Conclusion and Perspectives **155**
1 Conclusion 155
2 Perspectives 156

Bibliography **157**

Glossary

F The constant field of a function field extension. 80–83, 87–100, 102, 103, 118, 149

K A function field over F. 80–88, 90–98, 101, 118

L A function field extension over K. 80, 82–93, 95–97, 101, 118, 150

$\mathbb{D}$ A cyclic division algebra over K. 14, 16–19, 21, 22, 28–34, 36, 80–108, 110, 111, 113–115, 117, 118, 126, 127, 129, 130, 137–143, 146–149, 151, 152

$\mathbb{D}^\star$ The adjoint cyclic division algebra of $\mathbb{D}$. 18, 19, 32, 81, 82, 85, 86, 93, 94, 96, 98, 99, 101, 102, 105, 106, 141

$\mathbb{D}_{L,x_1,x_2}$ An abelian algebra over K defined by the abelian splitting field L and two elements x_1, x_2 of $K^\times$. 150, 153–155

$\mathbb{D}^\star_{L,x_1,x_2}$ The adjoint abelian algebra of $\mathbb{D}_{L,x_1,x_2}$. 150

$\mathcal{O}_P$ The valuation ring of K at P. 14, 20, 21, 27, 31, 33–35, 78, 79, 82, 91, 95, 123–129, 131–134, 137–139, 143, 145–148

$\mathcal{O}_{L,P}$ The integral closure of $\mathcal{O}_P$ in L. 14, 27, 28, 31, 78, 79, 127–129, 137, 138, 143–146

v_P The valuation of K at P. 83

w_Q The valuation of L at Q. 84, 91

ω_P The gauge of $\mathbb{D}$ at P. 84–86, 91, 92, 101, 127

Div The divisor group of an algebra. 77, 78, 83, 85–88, 91, 93, 94, 96, 97, 100, 101, 103, 131, 133–137, 139, 146–149, 151

$\mathcal{L}$ A Riemann–Roch space in K. 77, 86, 106, 136

$\Lambda_{\mathbb{D}}$ A Riemann–Roch space in $\mathbb{D}$. 16, 17, 19, 21, 22, 30–32, 34, 35, 80, 81, 85–89, 93, 98, 102, 104, 105, 112

$\Lambda_{\mathbb{D}^\star}$ A Riemann–Roch space in $\mathbb{D}^\star$. 32, 86, 98, 101–106

$\lambda_{\mathbb{D}}$ The dimension of a Riemann–Roch space in $\mathbb{D}$. 19, 31, 81, 85, 86, 88–90, 96, 99, 102, 106

$\lambda_{\mathbb{D}^\star}$ The dimension of a Riemann–Roch space in $\mathbb{D}^\star$. 81, 86, 96, 99

g_K The genus of K. 20, 33, 133–135, 140

g_L The genus of L. 18, 30, 107, 108, 110, 111, 147, 150

g_ω The genus corresponding to the gauge ω on $\mathbb{D}$. 18, 19, 23, 30–32, 36, 37, 106–108, 111, 113, 139, 141, 147, 150, 151

d_P The local different index of L/K . 21, 34, 35, 127, 129, 133, 140, 141, 143

$\delta(L/K)$ The different divisor of L/K. 78, 110, 137, 140, 141

Λ_P The gauge order of $\mathbb{D}$ at P. 21, 34, 35, 85, 104, 124–127, 129, 139, 141, 143, 147, 148

Δ The different divisor of the gauge order over L. 18, 19, 21, 22, 30–32, 34, 52, 53, 60, 64, 85, 86, 90, 93, 105, 107, 108, 110, 111, 129, 138–141, 150

$\mathcal{K}$ The canonical divisor of $\mathbb{D}$. 35, 81, 82, 85, 86, 93, 96, 98, 99, 102–106, 141

Res The residue map. 92, 95

$\mathcal{R}$es The endomorphic residue map. 91–93, 95, 98

Resrd The reduced residue map. 19, 32, 92, 94–96, 98

Ω_K The space of differentials of K. 19

$\Omega_{\mathbb{D}}$ The space of differentials of $\mathbb{D}$. 90–94

$\Omega_{\mathbb{D}^\star}$ The space of differentials of $\mathbb{D}^\star$. 19, 20, 31, 32, 93–95, 98

$\mathcal{A}_K$ The adele ring of K. 20, 33, 88, 131, 133–137, 139, 141, 147

$\mathcal{A}_L$ The adele ring of L. 87–89, 138, 150

$\mathcal{A}_{\mathbb{D}}$ The adele ring of $\mathbb{D}$. 18–21, 31, 32, 34, 87–90, 93–95, 137–142, 147

$\mathcal{A}_{\mathbb{D}^\star}$ The adele ring of $\mathbb{D}^\star$. 21, 34, 141

$\mathcal{A}_M$ The adelic space of a K-vector space M. 20, 21, 33, 131, 133–137

$\mathbb{P}_K$ The set of places of K. 18, 19, 21, 31–34, 77, 78, 105, 107, 110, 129–135, 137, 139–141, 143, 146–150

$\mathbb{P}_L$ The set of places of L. 18, 31, 77, 78, 108, 110, 130, 146

$d^\star$ The design distance of a code. 80, 81, 100, 103, 104, 119

End An endomorphism ring. 96, 97

Tr The trace map. 22, 35, 79, 91–98, 100, 102, 105, 124, 127, 144, 149

Nr The norm map. 14, 27, 87, 94, 110, 149

CoNr The conorm map. 19, 22, 32, 35, 78, 81, 82, 88, 90, 93, 96, 98, 99, 102–106, 137–139, 141, 148–150

Trd The reduced trace map. 19, 21, 32, 33, 91, 92, 95, 124, 125, 127, 137, 139, 143

Nrd The reduced norm map. 125

d_{srk} The sum-rank distance. 97

w_{srk} The sum-rank weight. 97, 102, 103

ρ_{algo} The decoding radius of the algorithm. 81, 100–104

AG Algebraic Geometry. 12, 13, 17, 20, 26, 29, 30, 32, 33, 80–83, 96–99

LAG Linearized Algebraic Geometry. 4–6, 11, 13–24, 26–30, 32–37, 79, 104–109, 111–113, 115, 117, 119, 130, 142, 143, 145, 147, 149, 151, 153, 155, 157, 158

LD Linearized Differential. 15, 18, 20, 28, 32, 98, 104, 130

ALAG Abelian Linearized Algebraic Geometry. 4, 6, 11, 20–24, 33–37, 130, 142, 143, 145, 147, 149, 151, 153, 155, 157, 158

MSRD Maximum Sum-Rank Distance. 13, 22, 26, 35, 99, 106, 113

Résumé étendu en français

Notre thèse s'inscrit dans le domaine de la théorie des codes et porte sur l'application des algèbres cycliques non commutatives à cette théorie.

Notre méthodologie consiste à utiliser la construction des anneaux de polynômes tordus de Ore pour représenter ces algèbres cycliques. Dans une première partie, nous appliquons cette construction à des extensions de corps finis K/F de degré arbitraire r, afin d'énumérer tous les codes cycliques tordus autoduaux, tels que définis dans [BU14], dans l'anneau quotient de Ore $K[X;\mathrm{Frob}]/(X^{rk}-1)$ pour tout entier positif k premier à la caractéristique p dans le cas séparable, ainsi que pour k, une puissance de p dans le cas purement inséparable, au prix de redondances dans ce cas. Enfin, nous présentons une implémentation en SageMath de cette énumération.

Dans un second temps, nous appliquons la même construction de Ore mais à des extensions cycliques de corps de fonctions et définissons ainsi des algèbres à division cycliques sur un corps de fonctions. Ces algèbres servent d'objet initial pour la construction des codes de géométrie algébrique linéarisés (codes LAG), une famille de codes d'évaluation en métrique somme-rang introduite dans [BC24]. Elles sont également essentielles à l'élaboration de notre algorithme de décodage polynomial pour ces codes LAG. Nous établissons d'abord un théorème de Riemann reliant la dimension de nos espaces de Riemann–Roch à celle d'un quotient d'adèles sur notre algèbre à division. Puis nous établissons une dualité de Serre pour ces algèbres. Ces théorèmes fondamentaux nous permettent ensuite de caractériser la dualité des codes LAG et de prouver notre algorithme de décodage. Pour finir, nous étendons la caractérisation de la dualité et l'algorithme de décodage aux sous-codes LAG raccourcis.

Dans la troisième partie, nous redémontrons notre théorème de Riemann–Roch comme corollaire d'un théorème de Tamagawa [Tam51]. Et enfin, nous généralisons les codes LAG et leur décodage aux codes LAG abéliens, les codes ALAG, définis sur des algèbres abéliennes. Nous fournissons également des implémentations en SageMath du décodage des codes LAG et ALAG.

Introduction

Dans son ouvrage fondateur de 1948 [Sha48], Claude Shannon a fondé le domaine de la théorie de l'information. Il y définit la capacité d'un canal comme le débit maximal, en bits par seconde, auquel l'information peut être transmise de manière fiable sur un canal de communication. Le compromis optimal entre le débit de transmission et le taux d'erreur est atteint grâce au principe de maximum de vraisemblance, qui garantit que l'algorithme de décodage associé au code corrige l'erreur la plus probable. Les codes les plus efficaces développés à ce jour sont linéaires. Ce sont des sous-espaces vectoriels d'un espace ambiant muni d'une métrique. La première métrique à avoir été étudiée est la métrique de Hamming, adaptée aux communications sur un canal unique. Plus récemment, la métrique rang, mieux adaptée aux communications sur des canaux multiples, a été introduite par Delsarte en 1978. En 2018, Umberto Martínez-Peñas a formellement défini la métrique somme-rang dans [MP18b] comme généralisation unificatrice de la métrique de Hamming et de la métrique rang. Pour tous les mots $\phi := (\phi_1, \ldots, \phi_s), \psi := (\psi_1, \ldots, \psi_s)$ dans l'espace ambiant $\prod_{i=1}^{s} \mathrm{Mat}_r(\mathbb{F}_q)$, la distance somme-rang est définie par

$$d_{\mathtt{sum-rank}}(\phi, \psi) := \sum_{i=1}^{s} \mathrm{rank}(\phi_i - \psi_i)$$

Cette distance dégénère en distance de Hamming pour $r = 1$ et se réduit à la distance rang pour $s = 1$.

Contexte Historique

En 1960, la première construction pratique de codes à distance maximale séparable (MDS) en métrique de Hamming sur $\mathbb{F}_q$, les codes de Reed–Solomon, paraît dans [RS60]. Ces codes atteignent la borne de Singleton, qui représente le compromis optimal entre la dimension k et la distance minimale d du code pour un code linéaire de longueur n, à savoir

$$k + d = n + 1.$$

Néanmoins, leur longueur n est limitée par la taille de leur alphabet q.

À partir de cette construction initiale, deux généralisations majeures sont apparues. La première, conduisant aux codes de géométrie algébrique (AG) de Goppa en 1982 dans [Gop81], visait à s'affranchir de la limitation en longueur, inhérente aux codes de Reed-Solomon. Les codes AG peuvent ainsi avoir une longueur asymptotiquement arbitraire pour un alphabet donné, au prix d'un défaut d'optimalité par rapport à la borne de Singleton égal à $\frac{1}{\sqrt{q}-1}$ pour une tour de courbes optimale sur le corps des constantes $\mathbb{F}_q$ avec q carré, comme montré dans [GS95].

La seconde généralisation a consisté en un passage de la métrique de Hamming à la métrique rang. Cela a conduit à la construction des codes de Gabidulin en 1985 dans [Gab85] qui sont à distance maximale séparable dans la métrique rang (MRD).

En outre, les codes de Gabidulin ont également été étudiés en métrique de Hamming en 2006 dans [BGU06], conduisant à la construction et à l'étude des codes cycliques tordus.

En 2018, Umberto Martínez-Peñas a étendu les codes de Gabidulin à la métrique somme-rang en introduisant les codes de Reed–Solomon linéarisés dans [MP18b], qui sont à distance maximale séparable en métrique somme-rang (MSRD).

Enfin, en 2024, X. Caruso et E. Berardini ont construit les codes de géométrie algébrique linéarisés (LAG) dans [BC24]. Cette famille de codes en métrique somme-rang généralise à la fois les codes de Reed–Solomon linéarisés et les codes AG. Elle combine ainsi leurs avantages. Ces codes sont quasi-MSRD, c'est-à-dire qu'ils atteignent la borne de Singleton en métrique somme-rang à un défaut près égal au genre associé à une jauge de l'algèbre à division sous-jacente, et leur longueur n'est pas limitée par la taille de leur alphabet.

L'objectif principal de cette thèse est d'établir un algorithme de décodage en temps polynomial pour cette dernière famille de codes d'évaluation, la plus générale, en métrique somme-rang.

Motivation : Polynômes tordus en théorie des codes

Dans cette thèse, nous utilisons les polynômes tordus comme outil principal pour construire, étudier et décoder des codes linéaires. Cette approche a été utilisée dans le développement de codes linéarisés, incluant les codes de Reed-Solomon linéarisés [MP18b], les codes de Reed-Muller linéarisés [BC25], et la famille la plus générale de codes d'évaluation connue à ce jour, les codes de géométrie algébrique linéarisés (LAG) [BC24].

Nous montrons maintenant comment ce changement de paradigme, des polynômes standards aux polynômes tordus, ouvre une nouvelle voie en géométrie non commutative effective. Donnons tout d'abord la définition d'un anneau de polynômes tordus à plusieurs variables, introduite par Ore dans [Ore33]. Soit L/K une extension abélienne d'un corps de base K, et soient θ_i des générateurs indépendants de son groupe de Galois. Nous définissons un anneau de polynômes tordus à plusieurs variables et à différentielles nulles comme l'anneau de polynômes $L[T_1;\theta_1,\ldots,T_n;\theta_n]$, où l'addition polynomiale est définie de manière usuelle, où les variables T_i commutent entre elles, mais où la multiplication scalaire est tordue par les automorphismes comme suit, pour tout $\lambda \in L$:

$$T_i\lambda = \theta_i(\lambda)T_i$$

Notamment, un anneau de polynômes tordus à une variable est un anneau euclidien à gauche et à droite, ce qui le rend particulièrement utile pour la conception d'algorithmes efficaces.

Contrairement aux polynômes standards, les polynômes tordus ne peuvent pas être évalués dans les scalaires L via un morphisme d'anneau. Cela s'explique par le fait que l'évaluation d'un produit de monômes, tels que T^i et τT^j, donnerait $\theta^i(\tau)\nu^{i+j}$ pour certains $\nu \in L$, alors que le produit de leurs évaluations donnerait $\tau\nu^{i+j}$. Une définition naturelle d'un morphisme d'évaluation sur les polynômes tordus est en revanche donnée pour $\lambda \in L^\times$ par:

$$\mathrm{ev}_\lambda : \begin{cases} L[T;\theta] & \to \mathrm{End}_K(L) \\ f(T) & \mapsto f(\lambda\theta) \end{cases}$$

ce qui entraîne :

$$\frac{L[T;\theta]}{T^r - \mathrm{Nr}(\lambda)} \simeq \mathrm{End}_K(L)$$

où r est l'ordre de θ et $\mathrm{Nr}(\lambda)$ est la norme de λ dans L/K. Ainsi, nous sommes naturellement amenés à étudier l'évaluation de fonctions dans des algèbres simples centrales cycliques, car elles peuvent toutes être localement et presque partout représentées sous cette forme. De plus, nous rappelons que toute algèbre simple centrale sur un corps de fonctions défini sur un corps de constantes fini est cyclique d'après [Rei75, Theorem 32.20].

Dans le cas où, L/K est une extension de corps finis, cette construction de Ore donne lieu à des codes cycliques tordus comme dans [CD25, Self-dual Skew Cyclic Codes]. D'autre part, dans le cas où L/K est une extension cyclique de corps de fonctions, il en résulte une algèbre à division $\frac{L[T;\theta]}{T^r-x}$ pour un choix approprié de l'élément $x \in K^\times$. La complétion $\frac{L[T;\theta]}{T^r-x} \otimes_K K_P$ en des places P telles que l'algèbre se décompose totalement, i.e., soit isomorphe à $\mathrm{End}_{K_P}(L \otimes_K K_P)$, conduit à la construction de codes LAG conformément à [BC24].

En notant $X(K)$ et $X(L)$ les schémas associés à K et L et $\pi : X(L) \to X(K)$ le morphisme surjectif de schémas associé à l'extension L/K, dans les deux cas, extension de corps finis ou extension de corps de fonctions, l'algèbre résiduelle de l'anneau quotient de Ore en un point P de $X(K)$ n'est pas le corps résiduel de K en P, $\mathcal{O}_P/P$, ni le corps résiduel de L en P, $\mathcal{O}_{L,P}/P$, où $\mathcal{O}_{L,P}$ désigne la clôture intégrale de $\mathcal{O}_P$ dans L_P, mais l'anneau d'endomorphismes $\mathrm{End}_{\mathcal{O}_P/P}(\mathcal{O}_{L,P}/P)$. L'application d'évaluation ev_λ conduit à la définition de diviseurs étendus où les zéros partiels des fonctions régulières en P sont pris en compte en tant que sous-espaces vectoriels sur $\mathcal{O}_P/P$ de l'espace vectoriel $\mathcal{O}_{L,P}/P$ de dimension r sur $\mathcal{O}_P/P$.

Si nous étendons la construction de l'anneau quotient de Ore aux polynômes de Ore à plusieurs variables, nous augmentons le niveau de généralité car nous pouvons alors évaluer n'importe quelle algèbre à division $\mathbb{D}$ sur K possédant un corps de décomposi-

tion abélien, i.e., un sous-corps commutatif (maximal) de degré $\sqrt{[\mathbb{D} : K]}$ qui est une extension abélienne du centre K.

Pour conclure, nous tenons à souligner que cette représentation des algèbres simples centrales en tant qu'algèbres quotients de Ore est un outil puissant qui permet des preuves explicites et des calculs effectifs dans les algèbres simples centrales. Par ailleurs, nous mentionnons un autre avantage de cette construction, à savoir que les codes issus de structures algébriques nouvelles et plus riches présentent un grand intérêt pour les schémas de cryptographie fondés sur les codes, tels que McEliece.

Contributions

Publications

Article: [CD25, Self-dual Skew Cyclic Codes]
Dans notre premier article, nous énumérons en temps cubique les codes cycliques tordus autoduaux en nous basant sur la construction de Ore. Cet article a été publié dans la revue Design Code and Cryptography par Springer Nature.

Article: [BCD26, Duality and Decoding of LAG codes]
Dans notre second article, nous caractérisons les codes différentiels linéarisés (LD) comme étant les duaux canoniques des codes LAG; nous montrons qu'ils sont isomorphes à ces derniers sur l'algèbre adjointe, et enfin nous les décodons en temps polynomial. Ce dernier article a été publié sur arXiv `https://arxiv.org/pdf/2603.11826`.

Énumération des codes cycliques tordus autoduaux

Les codes cycliques tordus autoduaux relatifs à une extension de corps fini $\mathbb{F}_{q^r}/\mathbb{F}_q$ et à un paramètre entier k peuvent être vus comme des idéaux à gauche autoduaux de l'algèbre quotient de polynômes tordus

$$\frac{\mathbb{F}_{q^r}[T; \mathrm{Frob}(\mathbb{F}_{q^r}/\mathbb{F}_q)]}{T^{kr} - 1}$$

dans lesquels les éléments sont deux à deux orthogonaux pour la forme bilinéaire canonique associée sur $\mathbb{F}_{q^r}^{kr}$.

Nous établissons des formules de comptage et fournissons un algorithme d'énumération en temps cubique pour les codes cycliques tordus autoduaux par rapport à la forme bilinéaire canonique, dans le cas séparable, où k est premier avec la caractéristique p. À cette fin, nous appliquons la décomposition des restes chinois aux idéaux à gauche $(f(T))$. Nous réduisons ensuite le problème d'énumération à un problème

d'algèbre bilinéaire par une équivalence de Morita entre les idéaux résultants $(f_i(T))$ et les noyaux de l'évaluation de leur générateur en 1, $\ker f_i(\theta)$. Enfin, nous résolvons un dernier problème d'algèbre bilinéaire consistant à trouver une base hyperbolique correspondant à deux sous-espaces maximaux isotropes pour les symétries euclidiennes ou hermitiennes. Les codes cycliques tordus autoduaux séparables, c'est-à-dire pour lesquels k est premier avec p, peuvent être énumérés en temps cubique en utilisant cette base hyperbolique.

Dans le cas inséparable, où p divise k, nous proposons un algorithme d'énumération exhaustif, bien que redondant. Pour ce faire, nous factorisons les polynômes tordus générateurs des codes cycliques tordus autoduaux inséparables en facteurs de polynômes tordus générateurs de codes cycliques séparables. L'énumération de ces facteurs séparables nécessite d'étendre l'énumération des espaces isotropes maximaux aux deux autres géométries classiques : les symétries anti-euclidiennes et anti-hermitiennes. Au total, nous obtenons les résultats suivants.

- **Énumération dans le cas séparable où k est premier avec p et $p \neq 2$**

  Nous avons établi une formule de comptage pour les codes cycliques tordus autoduaux et les avons produit de manière aléatoire selon une distribution uniforme. Et enfin, nous avons conçu et prouvé un algorithme d'énumération non redondant en temps cubique constant.

- **Énumération dans le cas inséparable où $p \mid k$ et $p \neq 2$**

  Nous avons conçu et prouvé un algorithme d'énumération exhaustif bien que redondant, en temps cubique constant.

Dualité et décodage des codes LAG

Nous rappelons la construction des codes LAG. Soit K un corps de fonctions correspondant à une courbe algébrique définie sur un corps de constantes quelconque F. Nous fixons une extension cyclique L/K de degré r et un générateur θ de son groupe de Galois. Nous notons $L[T;\theta]$ l'algèbre polynomiale de Ore correspondante. Nous définissons l'algèbre cyclique $\mathbb{D}$ comme le quotient de Ore suivant.

$$\mathbb{D} := \frac{L[T;\theta]}{T^r - x}$$

Nous choisissons l'élément $x \in K$ de sorte que $\mathbb{D}$ soit une algèbre à division, conformément à [BC24, Section IV A]. Dans [BC24], des fonctions Q ultramétriques sur $\mathbb{D}$, indexées par les places de L, sont introduites et utilisées pour définir des espaces de Riemann–Roch $\Lambda_{\mathbb{D}}(A) \subset \mathbb{D}$ associés à des diviseurs rationnels A de L. Ces fonctions

Q sur la L-base constituée des puissances de T de $\mathbb{D}$ sont définies par la formule

$$\omega_Q\left(\sum_{i=0}^{r-1} f_i T^i\right) := \min_{i=0}^{r-1}\left(w_Q(f_i) + i\frac{w_Q(x)}{r}\right) \quad \forall f_i \in L$$

De plus, pour toute place rationnelle P de K satisfaisant l'hypothèse **(H2-P_i)** décrite dans [BC24] et telle que les places Q au dessus de P soient disjointes du support de A, un morphisme d'évaluation $\bar{\varepsilon}_P : \Lambda_{\mathbb{D}}(A) \to \mathrm{End}_F(V_P)$ est construit, où V_P est l'algèbre résiduelle de L en P. Fixant un ensemble fini $\{P_1, \ldots, P_s\}$ de telles places et un diviseur d'évaluation $D = P_1 + \cdots + P_s$, nous concaténons les $\bar{\varepsilon}_{P_i}$ pour obtenir un morphisme d'évaluation

$$\bar{\varepsilon}_D : \Lambda_{\mathbb{D}}(A) \to \prod_{i=1}^{s} \mathrm{End}_F(V_{P_i}) \simeq \left(F^{r\times r}\right)^s$$

dont l'image est par définition le code AG linéarisé $\mathrm{LAG}_{\mathbb{D}}(A, D)$. Il est muni de la métrique somme-rang définie par la fonction poids suivante

$$(M_1, \ldots, M_s) \mapsto \sum_{i=1}^{s} \mathrm{rank}(M_i).$$

La construction des codes LAG repose sur les fonctions Q dont $\mathbb{D}$ est muni. Celles-ci sont liées à une présentation donnée de l'algèbre à division $\mathbb{D} := \frac{L[T;\theta]}{T^r - x}$. Afin de décoder les codes LAG, nous avons donc développé une théorie de Riemann–Roch sur $\mathbb{D}$ associée à ces fonctions Q. Notre première contribution consiste ainsi tout d'abord à établir un tel théorème de Riemann–Roch sur notre algèbre à division cyclique.

Théorème de Riemann–Roch et dualité de Serre pour les algèbres cycliques

Dans cette contribution, constituant le coeur de notre thèse, nous proposons un théorème de Riemann–Roch sur des algèbres à division cycliques $\mathbb{D}$ basé sur notre décomposition explicite

$$\mathbb{D} := \frac{L[T;\theta]}{T^r - x},$$

et pour une jauge (valuation surmultiplicative) définie localement par $\omega_P := e_P^{-1} \min_{Q|P} \omega_Q$.

Poursuivant les travaux de Witt dans sa thèse [Wit34], Tamagawa [Tam51], puis Mattson [Mat61] avaient déjà démontré un théorème de Riemann–Roch pour les parallélotopes d'ordres adéliques maximaux dans une algèbre simple centrale sur un corps de fonctions à une variable, indépendamment de sa représentation éventuelle comme quotient de Ore. En choisissant notre algèbre à division et sa représentation sous forme de quotient de Ore de telle sorte que les ordres des jauges correspondantes soient tous maximaux, notre théorème de Riemann–Roch devient une conséquence directe

du théorème de Tamagawa. Dans le cas général où nos ordres de jauge ne sont pas nécessairement maximaux, notre théorème de Riemann–Roch peut tout de même en être déduit par le calcul du discriminant des ordres de jauge.

Néanmoins, notre approche présente l'avantage d'être explicite concernant la dualité des codes LAG contrairement à la théorie de Tamagawa; elle nous permet de définir les duaux des codes LAG de manière canonique comme des codes différentiels linéarisés (LD), qui sont eux-mêmes isomorphes à des codes LAG sur l'algèbre adjointe $\mathbb{D}^\star$.

Notre théorème de Riemann–Roch est analogue au théorème classique de Riemann–Roch sur les corps de fonctions. Les fonctions Q ultramétriques jouent le rôle de valuations. Les diviseurs étendus (A, W) sur l'algèbre à division $\mathbb{D}$ quant à eux, ont une composante A à coefficients dans $\frac{\mathbb{Z}}{b_P}$ où

$$b_P = \frac{r}{\gcd(w_Q(x), r)}$$

pour $Q|P$ et prennent en compte des espaces vectoriels d'annulation W_i aux s places d'évaluation P_i. De plus, le genre g_ω de notre ordre de jauge adélique est donné par

$$g_\omega = g_L + \frac{\deg(\Delta)}{2}$$

où g_L est le genre du corps de fonctions L et où Δ est le diviseur différent de l'ordre de jauge par rapport à L donné par:

$$\Delta := \sum_{P \in \mathbb{P}_K} \sum_{Q|P} \frac{b_P - 1}{b_P} Q$$

.

Nous établissons tout d'abord le **Théorème de Riemann** qui caractérise la dimension des espaces de Riemann–Roch $\Lambda_{\mathbb{D}}(A, W)$ sur $\mathbb{D}$ définis de la manière suivante. Nous considérons un diviseur rationnel

$$A \in \bigoplus_{P \in \mathbb{P}_K} \bigoplus_{Q|P} \frac{\mathbb{Z}}{b_P} Q$$

et un produit de sous-espaces vectoriels $W = \prod_{i=1}^{s} W_i \subset V_D$ de l'algèbre résiduelle. Notant $[s] := \{1, \ldots, s\}$, nous posons

$$\Lambda_{\mathbb{D}}(A, W) := \{f \in \mathbb{D} \mid \omega_Q(f_P) + A_Q \geqslant 0 \, \forall P \in \mathbb{P}_K, \ \forall Q|P \text{ et } \bar{\varepsilon}_D(f)|_{W_i} = 0 \quad \forall i \in [s]\}$$

Nous définissons aussi l'espace des adeles correspondant par

$$\mathcal{A}_{\mathbb{D}}(A, W) := \left\{ f \in \prod_{P \in \mathbb{P}_K} \mathbb{D}_P \mid \omega_Q(f_P) + A_Q \geqslant 0 \, \forall P \in \mathbb{P}_K, \ \forall Q|P \text{ et } \bar{\varepsilon}_D(f)|_{W_i} = 0 \quad \forall i \in [s] \right\},$$

et l'anneau des adeles par

$$\mathcal{A}_{\mathbb{D}} := \left\{ f \in \prod_{P \in \mathbb{P}_K} \mathbb{D}_P \mid \omega_Q(f_P) \geqslant 0 \quad \forall Q|P, \text{ a.e. } P \right\}.$$

La formule de Riemann suivante relie la dimension $\lambda_{\mathbb{D}}(A, W)$ de l'espace de Riemann–Roch $\Lambda_{\mathbb{D}}(A, W)$ à celle du quotient d'adeles $\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D})$.

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) + r(1 - g_\omega) + \dim\left(\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D})\right)$$

Nous établissons enfin la **Dualité de Serre** qui correspond à la dualité suivante entre l'espace de Riemann–Roch dual de $\Lambda_{\mathbb{D}}(A, W)$ et l'espace des différentielles $\Omega_{\mathbb{D}^\star}(A, W) \subset \mathbb{D}^\star \otimes_K \Omega_K$ pour un choix d'uniformisante $t_D \in K$ à *toutes les places d'évaluation* et en notant $\mathrm{CoNr}(D) := \sum_{i=1}^{s} \mathrm{CoNr}(P_i) = \sum_{i=1}^{s} \sum_{Q|P_i} e_{P_i} Q$.

$$\begin{aligned} \Omega_{\mathbb{D}^\star}(A, W) &\simeq \Lambda_{\mathbb{D}^\star}\left(\left(\frac{dt_D}{t_D}\right)_L + \Delta + \mathrm{CoNr}(D) - A, W^\perp\right) \\ &\simeq \mathrm{Hom}_F\left(\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}), F\right) \end{aligned}$$

Cette dualité repose sur l'accouplement parfait donné par la somme des résidus réduits à toutes les places :

$$(\alpha, f \otimes \eta) \mapsto \sum_{P \in \mathbb{P}_K} \mathrm{Resrd}_P(\alpha_P f^\star \eta)$$

où, en notant $\kappa(P)$ le corps résiduel de K en la place P, les résidus réduits sont définis par

$$\mathrm{Resrd}_P(g\frac{dt_P}{t_P}) := \mathrm{Tr}_{\kappa(P)/F}(\,\mathrm{Res}_P(\,\mathrm{Trd}(g)\frac{dt_P}{t_P}))$$

pour une différentielle $g\frac{dt_P}{t_P} \in \Omega_{\mathbb{D}^\star}(A)$ et une uniformisante t_P de K en P. Nous rappelons que la trace réduite Trd est définie comme la trace de l'application L-linéaire de multiplication à droite dans $\mathbb{D}$. Nous obtenons finalement la formule de Riemann–Roch

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) + r(1 - g_\omega) + \lambda_{\mathbb{D}^\star}((A, W)^\star)$$

où le diviseur dual $(A, W)^\star$ est défini par

$$(A, W)^\star := \left(\left(\frac{dt_D}{t_D}\right)_L + \Delta + \mathrm{CoNr}(D) - A, W^\perp\right)$$

Dualité et décodage des codes LAG

Avant ces travaux, aucun algorithme de décodage en temps polynomial pour les codes LAG n'était connu, et leur dualité n'avait pas été caractérisée. En nous basant sur le

théorème des résidus appliqué aux résidus réduits et en invoquant notre théorème de Riemann–Roch, nous caractérisons la dualité des codes LAG.

Puis en utilisant à nouveau notre théorème de Riemann–Roch, nous prouvons notre algorithme de décodage, ce qui constituait l'objectif principal de notre thèse. Pour ce faire, nous avons adapté l'algorithme classique de décodage des codes AG de Stichtenoth [Sti93, Section 8.5]. En résumé, nous obtenons les résultats suivants.

- **Théorie de la dualité:**

  Les duaux canoniques des codes LAG sont les codes différentiels linéarisés (LD), définis comme l'image de l'espace de Riemann–Roch par les résidus endomorphiques suivants aux places d'évaluation.

$$(\mathcal{R}\mathrm{es}_{P_i})_i : \begin{cases} \Omega_{\mathbb{D}^\star}(A, V_D) & \to \prod_{i=1}^{s} \mathrm{End}(V_i) \\ f\frac{dt_D}{t_D} & \mapsto (\bar{\varepsilon}_{P_i}(f))_{i=1}^{s} \end{cases}.$$

  Moyennant le choix d'un diviseur canonique du corps de décomposition L, ils sont isomorphes aux codes LAG eux-mêmes sur l'algèbre adjointe.

- **Décodage polynomial:**

  Nous fournissons un algorithme de décodage en temps polynomial (de complexité inférieure à $O(s^3 r^6)$) pour les codes LAG. Il consiste à d'abord localiser l'espace des erreurs, i.e., l'image de l'erreur vue comme endomorphisme de l'algèbre résiduelle, pour ensuite résoudre le système d'équations restreint à cet espace de localisation.

Preuve du théorème de Riemann par la théorie de Tamagawa

Nous avons développé une théorie de Riemann–Roch à partir d'une représentation cyclique de notre algèbre à division. Cette théorie est bien adaptée aux codes LAG qui sont définis à partir de cette représentation mais pas à des codes plus généraux comme les codes LAG abéliens, ALAG, par exemple, qui ne possèdent pas de présentation cyclique en général. C'est pourquoi nous présentons une théorie alternative de Riemann–Roch publiée en 1951 par Tamagawa [Tam51]. Cette théorie ne met pas en jeu la présentation de l'algèbre à division. Soit $\mathcal{O}_P$ l'anneau de valuation du corps de fonctions local complet K_P. Elle s'applique en général à un espace vectoriel M de dimension n et de base $(e_i)_{i=1}^n$ sur un corps de fonctions K de degré de transcendance 1 et de corps des constantes quelconque ainsi qu'à un parallélotope Π, i.e., un $\mathcal{A}_K(0)$-module $\mathcal{A}_M := M \otimes_K \mathcal{A}_K$ presque partout trivial égal à $\oplus_{i=1}^n \mathcal{O}_P e_i$ et qui est localement un $\mathcal{O}_P$-réseau complet de $M \otimes_K K_P$. La formule de Riemann–Roch en résultant pour

une différentielle de Weil f_0 sur K est la suivante

$$\dim(\Pi \cap M) = V(\Pi) - n\,(g_K - 1) + \dim\left(\alpha_0^{-1}\Pi^\star \cap M\right)$$

où le diviseur (α_0) associé à l'idèle α_0 est donné par $(\alpha_0) = (f_0)$, où le parallélotope dual $\Pi^\star$ est donné par

$$\Pi^\star := \{\alpha \in \mathcal{A}_M \mid \mathrm{Trd}(\Pi\alpha_P) \subset \mathcal{O}_P \; \forall P\}$$

et où le volume du parallélotope $V(\Pi)$ est défini par

$$V(\Pi) := -\sum_{P \in \mathbb{P}_K} v_P\left(\det(\mathrm{mat}_e(a_P))\right) \deg P$$

pour une base fixe e de M sur K et une base a_P de Π_P représentée par la matrice $\mathrm{mat}_e(a_P)$ sur e.

Afin d'expliciter la formule de Tamagawa, nous calculons le discriminant des ordres de jauge de notre algèbre simple centrale complétée $\mathbb{D} \otimes_K K_P$. Incidemment, nous déterminons ainsi un critère de maximalité pour les ordres de jauge.

- **Calcul du discriminant** Soit Λ_P l'ordre de jauge de $\mathbb{D} \otimes_K K_P$

  $$\Lambda_P = \{f \in \mathbb{D} \otimes_K K_P \mid \omega_Q(f) \geqslant 0 \quad \forall Q|P\}.$$

  Nous démontrons la formule suivante pour le discriminant $\mathrm{disc}(\Lambda_P/\mathcal{O}_P)$ de l'ordre de jauge Λ_P sur l'anneau de valuation $\mathcal{O}_P$.

  $$\mathrm{disc}(\Lambda_P/\mathcal{O}_P) = P^{\frac{r^2}{e_P}d_P + \frac{r^2}{e_P}\frac{b_P - 1}{b_P}}$$

  où d_P est l'exposant de la différente et e_P l'indice de ramification en P.

- **Notre théorème de Riemann–Roch comme corollaire**

  Nous déduisons notre théorème de Riemann–Roch en injectant la formule du discriminant dans l'équation de Riemann–Roch par Tamagawa. En effet, posant $\Pi = \mathcal{A}_{\mathbb{D}}(A, U)$, nous obtenons $V(\Pi) = r\deg(A, U) - \frac{\deg(\mathrm{disc}(\mathcal{A}_{\mathbb{D}}(0)))}{2}$ et $\alpha_0^{-1}\Pi^\star = \mathcal{A}_{\mathbb{D}^\star}(\left(\frac{dt_D}{t_D}\right)_L + \mathrm{CoNr}(D) + \Delta - A, U^\perp)^\star$ où $(\alpha_0) = (\frac{dt_D}{t_D})$. Néanmoins, pour montrer cette dernière égalité, nous faisons appel à notre démonstration de la dualité de Serre. La formule de Hurwitz permet alors de déduire notre formule de Riemann–Roch de la formule de Tamagawa.

Décodage des codes LAG raccourcis et ALAG

Nous donnons deux généralisations des codes LAG.

- **Dualité entre les codes LAG raccourcis et les codes LAG poinçonnés**

  Pour une décomposition $V_i = U_i \oplus W_i$, le code LAG raccourci est défini par

  $$\bar{\varepsilon}_D(\Lambda_{\mathbb{D}}(A, U))|_W$$

  et le code LAG poinçonné correspondant par

  $$\pi_W^U \left(\bar{\varepsilon}_D \left(\Lambda_{\mathbb{D}^\star} \left((\frac{dt_D}{t_D})_L + \Delta + \mathrm{CoNr}(D) - A \right)^\star \right) \right)$$

  où π_W^U désigne la projection sur W le long de U.

  Nous montrons qu'ils sont duaux pour la forme bilinéaire non dégénérée:

  $$\begin{cases} \prod_{i=1}^s \mathrm{Hom}(W_i, V_i) \times \prod_{i=1}^s \mathrm{Hom}(V_i, W_i) & \to F \\ (u, v) & \mapsto \sum_{i=1}^s \mathrm{Tr}(u \circ v) \end{cases}$$

  que le code LAG raccourci est quasi-MSRD, i.e., qu'il atteint la borne de Singleton en métrique somme-rang à un défaut près égal au genre, comme le code LAG parent, et qu'en tant que sous-code d'un code LAG, il peut être décodé avec l'algorithme de décodage LAG.

- **Construction des codes ALAG**

  Nous définissons les codes ALAG comme une généralisation naturelle des codes LAG aux algèbres abéliennes, algèbres quotients de Ore multivariées ayant un corps de décomposition, i.e., sous-corps commutatif maximal de degré $\sqrt{[\mathbb{D} : K]}$, qui est une extension abélienne du corps de fonctions central. Soit $\mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$, son groupe de Galois. Nous définissons une nouvelle jauge naturelle $\omega_{x_1,\ldots,x_n}$ sur cette algèbre, par exemple, pour n variables $T_1, \ldots, T_n$,

  $$\omega_{x_1,\ldots,x_n,P}(f) = \frac{1}{e_P} \min_{Q|P, 0 \leqslant k_1 < r_1, \ldots, 0 \leqslant k_n < r_n} \left(w_Q(f_{k_1,\ldots,k_n}) + \frac{k_1}{r_1} w_Q(x_1) + \cdots + \frac{k_n}{r_n} w_Q(x_n) \right)$$

  Dans le cas d'une algèbre cyclique, où tous les r_i sont premiers deux à deux, cette jauge induit le même genre que celui du code LAG correspondant. Tout l'intérêt des codes ALAG réside donc dans le cas non cyclique, pour lequel nous démontrons également un théorème de Riemann–Roch, pourvu que $\mathbb{D}$ soit bien une algèbre à division; ce qui impose dans le cas non cyclique que le corps des constantes soit infini.

Implémentations en SageMath

- **Énumération des codes cycliques tordus autoduaux**

Dans le cas séparable où k est premier à la caractéristique p dans une algèbre cyclique semi-simple $\frac{\mathbb{F}_{q^r}[T;\mathrm{Frob}(\mathbb{F}_{q^r}/\mathbb{F}_q)]}{T^{kr}-1}$, l'algorithme fonctionne pour les quatre géométries finies (euclidienne, hermitienne, anti-euclidienne et anti-hermitienne). Il produit une solution en temps polynomial à chaque itération. Dans le cas purement inséparable où $k = p^n$ est une puissance de la caractéristique p , nous avons énuméré de façon exhaustive les codes cycliques tordus autoduaux dans l'algèbre $\frac{\mathbb{F}_{3^6}[T;\mathrm{Fr}]}{T^{18}-1}$. Nous avons obtenu 2360960 codes cycliques tordus autoduaux distincts, ce qui est en effet plus de trois fois plus petit que le nombre $80 \cdot 1120 \cdot 80$ d'énumérations (redondantes).

Le code source est disponible à l'emplacement suivant: `https://plmlab.math.cnrs.fr/caruso/selfdual-skew-cyclic-codes`

- **Algorithme de décodage LAG**

  Nous nous restreignons au cas où les places d'évaluation sont totalement décomposées. Nous obtenons un défaut de décodage par rapport au rayon de décodage théorique $\frac{d_{\mathrm{design}}-1}{2}$ égal à $\frac{g_\omega}{2}$ où g_ω est le genre associé à la jauge ω. La complexité du décodage à chaque itération est polynomiale et constante.

  Le code source du décodage des codes LAG est disponible à l'emplacement suivant: `https://plmlab.math.cnrs.fr/drain/lag-decoding`.

- **Algorithme de décodage ALAG**

  Nous décodons les codes ALAG dans le cas d'intérêt d'une algèbre abélienne matricielle de groupe de Galois non cyclique $\mathbb{Z}/(r_1) \times \mathbb{Z}/(r_2)$, donc avec r_1 non premier avec r_2. (Le cas cyclique fonctionne également mais le code associé ne présente pas d'intérêt par rapport à un code LAG classique.) Le code source du décodage des codes ALAG est disponible à l'emplacement suivant: `https://plmlab.math.cnrs.fr/drain/alag-decoding`.

Conclusion

Nos travaux tirent parti du fait que les anneaux de polynômes de Ore offrent un cadre efficace pour développer la théorie des codes en métrique somme-rang, notamment pour construire et étudier la dualité des codes cycliques tordus et, plus significativement, pour construire, caractériser la dualité et décoder les codes LAG ainsi que leurs généralisations ALAG. De plus, cet outil algébrique puissant que constitue les polynômes de Ore permet d'implémenter efficacement ces codes et de produire des preuves explicites de théorèmes fondamentaux tels que le théorème de Riemann–Roch et la dualité de Serre.

Perspectives

Concernant les codes cycliques tordus, nous voudrions explorer le cas inséparable avec des méthodes plus puissantes telles que l'équivalence de Morita et la décomposition d'Iwasawa en lieu et place de la factorisation des polynômes de Ore. Il serait alors permis d'espérer trouver une formule de comptage ainsi qu'un algorithme d'énumération non redondant possédant une complexité cubique.

Concernant les codes LAG, suivant les travaux de Tamagawa, il est naturel d'appliquer le théorème de Riemann–Roch à n'importe quelle algèbre semi-simple centrale abélienne (cas des codes ALAG) ou non abélienne pour tout diviseur étendu au sens large, c'est-à-dire correspondant à un parallélotope arbitraire, afin de donner une généralisation générique des codes LAG et de leur algorithme de décodage.

Enfin, de manière plus ambitieuse, nous aimerions établir à la fois un théorème de Riemann–Roch et une dualité de Serre pour des algèbres à division sur des corps de fonctions de dimension supérieure à 1, correspondant par exemple à des surfaces, et donner une construction et une caractérisation de la dualité des codes LAG associés ainsi qu'un algorithme de décodage polynomial.

Introduction

In his seminal work in 1948 [Sha48], Claude Shannon founded the field of information theory. He defined channel capacity as the maximum rate, in bits per second, at which information can be reliably transmitted over a communication channel. The optimal trade-off between transmission rate and error rate is achieved through the maximum likelihood principle, which ensures that the decoding algorithm associated with the code recovers the most likely error. The most efficient codes developed to this date are linear, meaning they are vector subspaces within an ambient space endowed with a metric.

The first metric to be studied was the Hamming metric, which is appropriate for single-channel communication. More recently, the rank metric, which is better suited to multichannel communication, was introduced by Delsarte in 1978. In 2018, Umberto Martínez-Peñas formally defined the sum-rank metric in [MP18b] as a unifying generalization of both Hamming and rank metrics. For any words $\phi := (\phi_1, \ldots, \phi_s), \psi := (\psi_1, \ldots, \psi_s)$ in the ambient space $\prod_{i=1}^{s} \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_q^r)$, the sum-rank distance is defined as follows:

$$d_{\mathtt{sum-rank}}(\phi, \psi) := \sum_{i=1}^{s} \mathrm{rank}(\phi_i - \psi_i)$$

This distance degenerates into the Hamming distance for $r = 1$ and reduces to the rank distance for $s = 1$. Furthermore, matrices with at most t nonzero columns have rank at most t, which means that the zero-centered Hamming ball of radius t is contained in the zero-centered sum-rank ball of radius t.

1 Historical Context

In 1960, Reed–Solomon codes emerged in [RS60] as the first practical construction of optimal codes in the Hamming metric over $\mathbb{F}_q$. These codes have maximum distance (MDS), which means that they meet the Singleton bound. This bound represents the optimal trade-off between the dimension k and the minimum distance d within an

ambient space of dimension n, namely

$$n + 1 = k + d.$$

Nevertheless, the length n of Reed–Solomon codes is limited by the size of their alphabet q.

From this initial construction, two main generalizations arose. The first sought to remove the constraint on the length, intrinsic to Reed-Solomon codes, leading to Goppa's algebraic geometry (AG) codes in 1982 in [Gop81]. These AG codes are almost MDS with a defect relative to the Singleton bound equal to the genus g of the curve and they are longer than Reed–Solomon codes for a given alphabet size q as the Hasse-Weil bound allows for up to $\lfloor 2g\sqrt{q} \rfloor$ additional evaluation places. These AG codes can be asymptotically of arbitrary length for a given alphabet at the cost of a defect relative to the asymptotic Singleton bound equal to $\frac{1}{\sqrt{q}-1}$ for a tower of optimal curves over the constant field $\mathbb{F}_q$, where q is a square, as shown in [GS95].

The second generalization involved a shift from the Hamming metric to the rank metric. This led to the development of Gabidulin codes in 1985 in [Gab85], which have maximal rank distance (MRD). Furthermore, Gabidulin codes were also studied in the Hamming metric in 2006 in [BGU06], leading to the construction and study of skew cyclic codes. In 2018, Umberto Martínez-Peñas extended these codes to the sum-rank metric by introducing linearized Reed–Solomon codes in [MP18b], which have maximum sum-rank distance (MSRD).

Finally, in 2024, E. Berardini and X. Caruso constructed linearized algebraic geometry (LAG) codes in [BC24]. This latter family of sum-rank codes generalizes both linearized Reed–Solomon codes and AG codes and combines their advantages. They are almost MSRD with a defect equal to the genus of a specific gauge defined over the underlying division algebra and their length is not limited by the size of the alphabet.

Our main objective in this thesis is to design and prove a polynomial-time decoding algorithm for this latter, most general family of evaluation codes in the sum-rank metric.

2 Motivation: Application of Skew Polynomials in Coding Theory

In this thesis, we make use of skew polynomials as a primary tool to construct, study, and decode linear codes. This approach has been used for the construction of linearized codes, including linearized Reed–Solomon codes [MP18b], linearized Reed-Muller codes [BC25], and the most general family of evaluation codes currently known, linearized algebraic geometry (LAG) codes [BC24]. We now show how this shift of

paradigm from standard polynomials to skew polynomials opens up a new avenue in effective non-commutative geometry.

Let us first give the definition of a multivariate skew polynomial ring introduced by Ore in [Ore33]. Let L/K be an abelian extension of a base field K, and let θ_i be independent generators of its Galois group. We define a multivariate skew polynomial ring with differentials set to zero as the polynomial ring $L[T_1;\theta_1,\dots,T_n;\theta_n]$, where the polynomial addition is defined as usual, where the variables T_i commute with each other, but where the scalar multiplication is twisted by the automorphisms as follows, for any $\lambda \in L$:

$$T_i\lambda = \theta_i(\lambda)T_i$$

In particular, a univariate skew polynomial ring is a left and right Euclidean domain, which makes it particularly useful for designing efficient algorithms.

In contrast to standard polynomials, skew polynomials $f \in L[T;\theta]$ cannot be evaluated in L via a ring morphism. This is because the evaluation of a product of monomials, such as T^i and τT^j, would result in $\theta^i(\tau)\nu^{i+j}$ for some $\nu \in L$, whereas the product of their evaluations would yield $\tau\nu^{i+j}$. Instead, a natural evaluation morphism on skew polynomials is given for $\lambda \in L^\times$ by:

$$\mathrm{ev}_\lambda : \begin{cases} L[T;\theta] & \to \mathrm{End}_K(L) \\ f(T) & \mapsto f(\lambda\theta) \end{cases}$$

yielding

$$\frac{L[T;\theta]}{T^r - \mathrm{Nr}(\lambda)} \simeq \mathrm{End}_K(L)$$

where r is the order of θ and $\mathrm{Nr}(\lambda)$ is the norm of λ in L/K. So, we are naturally led to study the evaluation of functions in cyclic central simple algebras as these algebras can be almost everywhere locally represented in this form. Moreover, we recall that every central simple algebra over a function field defined over a finite field of constants is cyclic by [Rei75, Theorem 32.20].

In the case where L/K is a finite field extension, this Ore construction gives rise to skew cyclic codes as ideals of the cyclic algebra, as defined in [BGU06] for the Hamming metric and in [MP18b] for the sum-rank metric. In the case where L/K is a cyclic extension of function fields, it can produce cyclic division algebras $\frac{L[T;\theta]}{T^r-x}$ for appropriate choices of x. Their completion $\frac{L[T;\theta]}{T^r-x} \otimes_K K_P$ at places P such that the algebra splits totally, i.e., is isomorphic to $\mathrm{End}_{K_P}(L \otimes_K K_P)$ leads to the construction of LAG codes as in [BC24].

In both cases, where L/K is a finite field extension or a function field extension, the residual algebra of the Ore quotient ring at a point P of K where the algebra splits totally, i.e., is isomorphic to $\mathrm{End}_{K_P}(L \otimes_K K_P)$, is not the residue field of K at P,

$\mathcal{O}_P/P$, nor the residue field of L at P, $\mathcal{O}_{L,P}/P$, where $\mathcal{O}_{L,P}$ denotes the integral closure of $\mathcal{O}_P$ in L_P, but the endomorphism ring $\mathrm{End}_{\mathcal{O}_P/P}(\mathcal{O}_{L,P}/P)$. The evaluation map ev_λ leads to the definition of extended divisors where partial zeros of regular functions f at P are taken into account as $\mathcal{O}_P/P$-vector subspaces of the r-dimensional $\mathcal{O}_P/P$ vector space $\mathcal{O}_{L,P}/P$ (see Definition 2.3.12). If we extend the Ore quotient ring construction to multivariate Ore polynomials, we increase the level of generality as we can then evaluate any division algebra $\mathbb{D}$ over K, which has an abelian splitting field.

To conclude this section, we would like to stress the fact that this representation of central simple algebras as an Ore quotient algebra allows for effective computations in the central simple algebras. Further developments of non-commutative algebraic geometry based on skew polynomials seem promising. Notably, a theory of skew residues has been built in 2021 in [Car21] and it was recently shown in 2024 in [PV24] that a Noether's normalization theorem holds for skew polynomials. Besides, we mention another advantage of this construction, namely, that codes stemming from new and richer algebraic structures are of interest for code-based cryptographic schemes such as McEliece.

3 Contributions

3.1 Publications

Article: [CD25, Self-dual Skew Cyclic Codes]
In our first article, based on this Ore construction, we enumerate self-dual skew cyclic codes in cubic time. This article has been published in the journal Design Code and Cryptography by Springer Nature.

Article: [BCD26, Duality and Decoding of LAG codes]
In our second article, we characterize Linearized Differential (LD) codes as being the canonical dual of LAG codes and as being isomorphic to LAG codes on the adjoint algebra. We then decode them in polynomial time (with complexity lower than $O(s^3r^6)$). This latter article has been posted as a preprint on arXiv `https://arxiv.org/pdf/2603.11826` and submitted to an international journal.

3.2 Enumeration of Self-dual Skew Cyclic Codes

Self-dual Skew Cyclic Codes relative to a finite field extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ and an integer parameter k can be viewed as self-dual left ideals of the semi-simple algebra, quotient of the skew polynomial ring

$$\frac{\mathbb{F}_{q^r}[T;\mathrm{Frob}(\mathbb{F}_{q^r}/\mathbb{F}_q)]}{T^{kr}-1}$$

in which elements are pairwise orthogonal with respect to the associated canonical (coordinate-wise) bilinear form on $\mathbb{F}_{q^r}^{kr}$.

We establish counting formulae and provide a cubic-time enumeration algorithm for self-dual skew cyclic codes with respect to the canonical (coordinate-wise) bilinear form, in the separable case, where k is coprime to the characteristic p. To this end, we apply the Chinese Remainder Decomposition to left ideals of the form $(f(T))$. We then reduce the enumeration problem to one of bilinear algebra by a Morita equivalence between the resulting ideals $(f_i(T))$ and the kernels of their generator evaluation at 1, $\ker f_i(\theta)$. Finally, we solve the bilinear algebra problem of finding hyperbolic bases corresponding to two supplementary maximal isotropic spaces in the Euclidean and Hermitian symmetries. Separable self-dual skew cyclic codes, for which k is coprime to p, can be enumerated effectively using these hyperbolic bases.

In the inseparable case, where p divides k, we propose an exhaustive, though redundant, enumeration algorithm. It consists of factoring skew polynomial generators of inseparable self-dual skew cyclic codes into skew polynomial generators of separable ones. Enumerating these separable factors requires enumerating maximal isotropic spaces in the two other classical geometries: skew Euclidean and skew Hermitian symmetries. In total, we provide the following results.

- **Enumeration in the separable case where k is coprime to p and $p \neq 2$**

  We have established counting formulae and a uniform random-generation procedure for self-dual skew cyclic codes. We have also designed and proved a non-redundant cubic enumeration algorithm.

- **Enumeration in the inseparable case where $p \mid k$ and $p \neq 2$**

  We have designed and proved an exhaustive though redundant cubic enumeration algorithm.

3.3 Duality and Decoding of LAG codes

We briefly outline the construction of linearized AG codes. Let K be the function field of an algebraic curve defined over a field F. We fix a cyclic extension L/K of degree r and a generator θ of its Galois group. We let $L[T;\theta]$ be the corresponding Ore polynomial ring. We set

$$\mathbb{D} := \frac{L[T;\theta]}{T^r - x},$$

where $x \in K$ is chosen so that $\mathbb{D}$ is a division algebra as in [BC24, Section IV A]. In [BC24], ultrametric Q functions on $\mathbb{D}$, indexed by the places of L, are introduced and used to define Riemann–Roch spaces $\Lambda_{\mathbb{D}}(A) \subset \mathbb{D}$ associated to certain rational divisors A of L. These Q-functions on the L-basis of $\mathbb{D}$ constituted by the powers of T

are defined by the following formula

$$\omega_Q\left(\sum_{i=0}^{r-1} f_i T^i\right) := \min_{i=0}^{r-1}\left(w_Q(f_i) + i\frac{w_Q(x)}{r}\right) \quad \forall f_i \in L.$$

Moreover, for any rational place P of K away from A, meaning that the support of A does not contain any place of L above P, and being totally split in $\mathbb{D}$, i.e., satisfying the hypothesis called **(H2-P_i)** in [BC24], an evaluation morphism $\bar{\varepsilon}_P : \Lambda_{\mathbb{D}}(A) \to \mathrm{End}_F(V_P)$ is constructed, where V_P is the residual algebra of L at P. Fixing a finite set $\{P_1, \ldots, P_s\}$ of such places and setting $D = P_1 + \cdots + P_s$, one can concatenate the $\bar{\varepsilon}_{P_i}$ to obtain a multievaluation morphism

$$\bar{\varepsilon}_D : \Lambda_{\mathbb{D}}(A) \to \prod_{i=1}^{s} \mathrm{End}_F\left(V_{P_i}\right) \simeq \left(F^{r\times r}\right)^s,$$

Its image is by definition the linearized AG code $\mathrm{LAG}_{\mathbb{D}}(A, D)$. The code is endowed with the sum-rank metric defined by the weight function

$$(M_1, \ldots, M_s) \mapsto \sum_{i=1}^{s} \mathrm{rank}(M_i).$$

LAG codes rely on the representation $\mathbb{D} := \frac{L[T;\theta]}{T^r - x}$ of our division algebra. In order to decode LAG codes, we thus have developed a theory of Riemann–Roch based on this representation. Our contributions consist in first establishing such a Riemann–Roch theorem with a Serre duality for our cyclic division algebras $\mathbb{D}$, and then in deriving from it a characterization of LAG code duality and a polynomial-time decoding algorithm for LAG codes.

3.3.1 Riemann–Roch and Duality Theorem for Cyclic Algebras

In this main contribution, we propose an explicit proof of the Riemann–Roch Theorem on cyclic division algebras $\mathbb{D}$ based on the explicit representation

$$\mathbb{D} := \frac{L[T;\theta]}{T^r - x}$$

This theorem is analogous to the classical Riemann–Roch theorem on function fields. The Q-functions play the role of valuations. Extended divisors (A, W) on the division algebra $\mathbb{D}$, have coefficients in $\frac{\mathbb{Z}}{b_P}$ where

$$b_P := \frac{r}{\gcd(w_Q(x), r)}$$

for $Q|P$ and take vanishing spaces W_i at the s evaluation places P_i into account. Also,

the genus g_ω of our adelic gauge order for the gauge ω is given by

$$g_\omega := g_L + \frac{\deg(\Delta)}{2}$$

where Δ is the different divisor of the gauge order relatively to L given by

$$\Delta := \sum_{P \in \mathbb{P}_K} \sum_{Q|P} \frac{b_P - 1}{b_P} Q$$

We first establish the **Riemann Theorem** characterizing the dimension of the Riemann–Roch spaces $\Lambda_{\mathbb{D}}(A, W)$ over $\mathbb{D}$ defined as follows. We consider a rational divisor

$$A \in \bigoplus_{P \in \mathbb{P}_K} \bigoplus_{Q|P} \frac{\mathbb{Z}}{b_P} Q, \text{ where } b_P = \frac{r}{\gcd(w_Q(x), r)},$$

and a product of vector subspaces $W = \prod_{i=1}^{s} W_i \subset \prod_{i=1}^{s} V_i =: V_D$ of the residual algebras $V_i := \mathcal{O}_{L,P_i}/P_i\mathcal{O}_{L,P_i}$, where $\mathcal{O}_{L,P}$ denotes the integral closure in L of the valuation ring $\mathcal{O}_P$ of K at P. Using the notation $[s] := \{1, \ldots, s\}$, we then set the corresponding Riemann–Roch space $\Lambda_{\mathbb{D}}(A, W)$ as follows.

$$\Lambda_{\mathbb{D}}(A, W) := \{f \in \mathbb{D} \mid \omega_Q(f) + A_Q \geqslant 0 \quad \forall Q \in \mathbb{P}_L \text{ and } \bar{\varepsilon}_D(f)|_{W_i} = 0 \quad \forall i \in [s]\}$$

We also define the corresponding adele space by

$$\mathcal{A}_{\mathbb{D}}(A, W) := \left\{ f \in \prod_{P \in \mathbb{P}_K} \mathbb{D}_P \;\middle|\; \omega_Q(f_P) + A_Q \geqslant 0 \quad \forall P \in \mathbb{P}_K,\ \forall Q|P \text{ and } \bar{\varepsilon}_D(f)|_{W_i} = 0 \quad \forall i \in [s] \right\}$$

and the adele ring by

$$\mathcal{A}_{\mathbb{D}} := \left\{ f \in \prod_{P \in \mathbb{P}_K} \mathbb{D}_P \;\middle|\; \omega_Q(f_P) \geqslant 0 \quad \forall Q|P,\ \text{a.e. } P \right\}$$

where a.e. stands for almost everywhere, i.e., almost at every place $P \in \mathbb{P}_K$. The following Riemann formula relates the dimension of the Riemann–Roch space $\Lambda_{\mathbb{D}}(A, W)$ to that of the adele quotient $\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D})$.

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) + r(1 - g_\omega) + \dim\left(\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D})\right)$$

We finally establish the **Serre Duality** which corresponds to the following duality between the Riemann–Roch space $\Lambda_{\mathbb{D}}(A, W)$ and the space of differentials $\Omega_{\mathbb{D}^\star}(A, W)$ for the choice of a uniformizer $t_D \in K$ at *all evaluation places* and set-

ting $\mathrm{CoNr}(D) := \sum_{i=1}^{s} \mathrm{CoNr}(P_i) = \sum_{i=1}^{s} \sum_{Q|P_i} e_{P_i} Q$.

$$\Omega_{\mathbb{D}^\star}(A, W) \simeq \Lambda_{\mathbb{D}^\star}((A, W)^\star) \simeq \mathrm{Hom}_F\left(\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}), F\right)$$

where

$$(A, W)^\star := \left(\left(\frac{dt_D}{t_D}\right)_L + \Delta + \mathrm{CoNr}(D) - A, W^\perp\right)$$

This duality relies on the perfect pairing given by the sum of the reduced residue as shown in Theorem 2.3.36.

$$\begin{aligned} \mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}) \times \Omega_{\mathbb{D}^\star}(A, W) &\to F \\ (\alpha, \nu) &\mapsto \sum_{P \in \mathbb{P}_K} \mathrm{Resrd}_P(\alpha_P \nu^\star) \end{aligned}$$

where $\nu = f\frac{dt_P}{t_P} \in \Omega_{\mathbb{D}^\star}(A)$ is a differential and $t_P \in K$ a uniformizer at P and where, denoting by $\kappa(P)$ the residual field of K at P,

$$\mathrm{Resrd}_P(f\frac{dt_P}{t_P}) := \mathrm{Tr}_{\kappa(P)/F}(\,\mathrm{Res}_P(\,\mathrm{Trd}(f)\frac{dt_P}{t_P}))$$

and the reduced trace Trd is defined as the trace of the L-linear right multiplication in $\mathbb{D}$. We obtain the Riemann–Roch formula relating the dimension $\lambda_{\mathbb{D}}(A, W)$ of the Riemann–Roch space $\Lambda_{\mathbb{D}}(A, W)$ to that of its dual $\Lambda_{\mathbb{D}^\star}((A, W)^\star)$, $\lambda_{\mathbb{D}^\star}((A, W)^\star)$.

$$\lambda_{\mathbb{D}}(A, W) = r\deg(A, W) + r(1 - g_\omega) + \lambda_{\mathbb{D}^\star}((A, W)^\star)$$

3.3.2 Duality and Decoding of LAG codes

Prior to this work, no polynomial-time decoding algorithm for LAG codes was known, and their duality was not characterized. Using the residue theorem and the Riemann–Roch Theorem, we characterize the duals of LAG codes. Then, based on the Riemann–Roch theorem again and on this duality, we decode them by adapting the classical AG decoding algorithm by Stichtenoth [Sti93, Section 8.5].

- **Duality theory:**

  The canonical dual of a LAG code is the Linearized Differential (LD) code, defined as the image of the dual Riemann–Roch space on the dual algebra by the following endomorphic residue map at the evaluation places.

$$(\mathcal{R}\mathrm{es}_{P_i})_i : \begin{cases} \Omega_{\mathbb{D}^\star}(A, V_D) & \to \prod_{i=1}^{s} \mathrm{End}(V_i) \\ f\frac{dt_D}{t_D} & \mapsto (\bar{\varepsilon}_{P_i}(f))_{i=1}^{s} \end{cases}.$$

By means of the choice of a canonical divisor of the splitting field L, they are isomorphic to LAG codes themselves over the adjoint algebra (See Theorem 2.4.3).

- **Polynomial decoding:**

  We provide a decoding algorithm for LAG codes that runs in polynomial time (See Theorem 2.4.18). Our approach is analogous to that of the classical AG code decoding algorithm presented in [Sti93, Section 8.5]. It consists of decoding the dual LAG codes by first localizing the image of the error seen as an endomorphism of the residual algebra V_D and then by solving the syndrome linear equation system restricted to this error localizing space.

3.4 Alternative Proof of our Riemann–Roch theorem

In the previous contribution, we have developed a Riemann–Roch theory depending on a representation of the cyclic division algebra $\mathbb{D}$ as $\frac{L[T;\theta]}{T^r-x}$. This theory is well suited for LAG codes which rely on this representation but not for more general families of codes as Abelian LAG (ALAG) Codes, for example, as abelian algebras do not necessarily have any cyclic representation. That is why we present in this thesis an alternative Riemann–Roch Theory published in 1951 by Tamagawa [Tam51]. Tamagawa's theory does not make use of a splitting field for the division algebra. Letting $\mathcal{O}_P$ be the valuation ring of the local complete function field K_P, Tamagawa's theory applies in general to a finite vector space M of dimension n and basis $(e_i)_{i=1}^n$ over the function field K of transcendence degree 1 over an arbitrary constant field F as well as to a parallelotope $\Pi \subset \mathcal{A}_M$, i.e., locally a $\mathcal{O}_P$-full lattice of $M \otimes_K K_P$, which is almost everywhere trivial equal to $\oplus_{i=1}^n \mathcal{O}_P e_i$. The resulting Riemann–Roch formula for a given Weil differential $f_0 \in \mathrm{Hom}(\mathcal{A}_K, F)$ is the following

$$\dim(\Pi \cap M) = V(\Pi) - n\,(g_K - 1) + \dim\left(\alpha_0^{-1}\Pi^\star \cap M\right)$$

where $\alpha_0 \in \mathcal{A}_K^\times$ is an idele, i.e., an invertible adele, such that its associated divisor satisfies $(\alpha_0) = (f_0)$, where the dual parallelotope $\Pi^\star$ is given by the formula

$$\Pi^\star := \{\alpha \in \mathcal{A}_M \mid \mathrm{Trd}(\Pi\alpha_P) \subset \mathcal{O}_P \ \forall P\}$$

and where the volume of the parallelotope $V(\Pi)$ is defined by

$$V(\Pi) := -\sum_{P \in \mathbb{P}_K} v_P\left(\det(\mathrm{mat}_e(a_P))\right) \deg P$$

for a fixed basis e of M over K and a basis a_P of Π_P represented by the matrix $\mathrm{mat}_e(a_P)$ over e. We define a gauge on $\mathbb{D}_P$, i.e., a surmultiplicative valuation extending the val-

uation of the central function field K_P, locally as $\omega_P := e_P^{-1} \min_{Q|P} \omega_Q$. If we choose our division algebra such that the gauge orders, i.e., the orders constituted of nonnegative elements for the gauge, are all maximal (See Corollary 2.2.5), our Riemann–Roch Theorem can be viewed as a direct consequence of Tamagawa's theorem. Also in the general case where our gauge orders may not be maximal, we can deduce our Riemann–Roch theorem from Tamagawa's Theorem by computing the discriminant of the gauge orders of our completed central simple algebra at $P \in \mathbb{P}_K$, $\mathbb{D} \otimes_K K_P$. As a byproduct, we so recover a maximality criterion for the gauge order of our cyclic division algebra in terms of the quantity $b_P = \frac{r}{\gcd(e_P v_P(x), r)}$ and of the local index ind_P at any place P, which is defined as the square root of the dimension of the underlying division algebra of $\mathbb{D} \otimes_K K_P$.

- **Discriminant Computation and Maximality Criterion of a Gauge Order**
  Let Λ_P be the gauge order of $\mathbb{D} \otimes_K K_P$.

  $$\Lambda_P = \{f \in \mathbb{D} \otimes_K K_P \mid \omega_Q(f) \geqslant 0 \quad \forall Q|P\}$$

  We show the following formula for the discriminant $\mathrm{disc}(\Lambda_P/\mathcal{O}_P)$ of the gauge order Λ_P over the valuation ring $\mathcal{O}_P$ (See Theorem 2.1.3).

  $$\mathrm{disc}(\Lambda_P/\mathcal{O}_P) = P^{\frac{r^2}{e_P} d_P + \frac{r^2}{e_P} \frac{b_P - 1}{b_P}}$$

  where $b_P := \frac{r}{\gcd(e_P v_P(x), r)}$, where d_P is the different exponent and e_P the ramification index at P. Whence, denoting by ind_P the local index of $\mathbb{D}$, the maximality criterion for the gauge order is as follows:

  $$r \frac{\mathrm{ind}_P - 1}{\mathrm{ind}_P} = \frac{r}{e_P} d_P + \frac{r}{e_P} \frac{b_P - 1}{b_P}$$

- **Our Riemann–Roch Theorem as a Corollary of Tamagawa's Theorem and our Serre Duality**

  We deduce our Riemann–Roch Theorem from Tamagawa's Theorem by injecting the discriminant formula in Tamagawa's equation 4.1.2. Indeed, letting $\Pi = \mathcal{A}_{\mathbb{D}}(A, U)$, we get $V(\Pi) = r \deg(A, U) - \frac{\deg(\mathrm{disc}(\mathcal{A}_{\mathbb{D}}(0)))}{2}$ and $\Pi^\star = \alpha_0^{-1} \mathcal{A}_{\mathbb{D}^\star} \left(\left(\frac{dt_D}{t_D} \right)_L + \Delta + \mathrm{CoNr}(D) - A, U^\perp \right)^\star$ où $(\alpha_0) = (\frac{dt_D}{t_D})$. However, in order to show the latter equality, we have made use, for simplicity, of our proof of Serre duality. Tamagawa's Theorem yields our Riemann–Roch formula by the Hurwitz formula.

3.5 Decoding Shortened LAG and ALAG Codes

- **Duality between Shortened LAG codes and Punctured LAG codes**

  For a decomposition $V_i = U_i \oplus W_i \quad \forall i \in \{1, \dots, s\}$, a shortened LAG code is defined as

  $$\bar{\varepsilon}_D(\Lambda_{\mathbb{D}}(A, U))|_W$$

  and the corresponding punctured LAG code as

  $$\pi_W^U \left(\bar{\varepsilon}_D \left(\Lambda_{\mathbb{D}^\star} \left(\mathcal{K} - A + \operatorname{CoNr}(D) \right)^\star \right) \right)$$

  where π_W^U denotes the projection onto W along U. We show that they are dual for the non-degenerate bilinear form:

  $$\begin{cases} \prod_{i=1}^s \operatorname{Hom}(W_i, V_i) \times \prod_{i=1}^s \operatorname{Hom}(V_i, W_i) & \to F \\ (u, v) & \mapsto \sum_{i=1}^s \operatorname{Tr}(u \circ v) \end{cases}$$

  We then show that shortened codes are almost MSRD, i.e., almost meeting the Singleton bound in sum-rank metric with a defect equal to the genus of the adelic order of our gauge on the underlying cyclic division algebra of the code. As a subcode of a LAG code, they can be decoded with the same design distance as for the parent LAG code, using the same LAG decoding algorithm.

- **Construction and Decoding of ALAG Codes**

  We define ALAG codes as LAG code generalizations on abelian algebra, i.e., multivariate Ore quotient algebra with abelian splitting fields. Let $\mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$ be its Galois group. We note that in the case of an infinite constant field, there exist non-cyclic abelian division algebras. We then pave the way for their decoding by applying Tamagawa's Theorem to the underlying abelian division algebra together with a computation of the discriminant of their gauge orders and by providing an experimental SageMath implementation of an ALAG decoding algorithm analogous to the LAG decoding algorithm. We compute the discriminant in the case of a splitting field of Galois group equal to the product of n cyclic groups and obtain the formula:

  $$\operatorname{disc}(\Lambda_P/\mathcal{O}_P) = P^{\frac{r^2}{e_P} d_P + \frac{r^2}{e_P} \frac{\operatorname{lcm}(b_{1P}, \dots, b_{nP}) - 1}{\operatorname{lcm}(b_{1P}, \dots, b_{nP})}}$$

  corresponding to the gauge:

  $$\omega_P(f) = \frac{1}{e_P} \min_{Q|P, 0 \leqslant i_1 < r_1, \dots, 0 \leqslant i_n < r_n} \left(w_Q(f_{i_1, \dots, i_n}) + \frac{i_1}{r_1} w_Q(x_1) + \cdots + \frac{i_n}{r_n} w_Q(x_n) \right)$$

for any $f = \sum_{0 \leqslant i_1 < r_1, \ldots, 0 \leqslant i_n < r_n} f_{i_1,\ldots,i_n} {T_1}^{i_1} \cdots {T_n}^{i_n}$ and where $b_{iP} := \frac{r_i}{\gcd(r_i, w_Q(x_i))}$ and $f_{i_1,\ldots,i_n} \in L$ for $i = 1, \ldots, n$. In the case of a cyclic algebra, where all the r_i are pairwise coprime, we check that this gauge induces the same genus as that of the corresponding LAG code. The whole point of ALAG codes therefore lies in the non-cyclic case.

Furthermore, as the subfields $L_i := L^{\theta_1, \cdots, \check{\theta_i} \cdots, \theta_n}$ (where $\check{\theta}_i$ means that we omit the i-th automorphism and where L^ϕ means the subfield of L fixed by ϕ) are linearly disjoint, we have

$$\frac{L[T_1; \theta_1, \ldots, T_n; \theta_n]}{{T_1}^{r_1} - x_1, \ldots, {T_n}^{r_n} - x_n} \simeq \frac{L_1[T_1; \theta_1]}{{T_1}^{r_1} - x_1} \otimes_K \cdots \otimes_K \frac{L_n[T_n; \theta_n]}{{T_n}^{r_n} - x_n}$$
$$\mathbb{D}_{x_1,\ldots,x_n} \simeq \mathbb{D}_{x_1} \otimes_K \cdots \otimes_K \mathbb{D}_{x_n}$$

As the unramified evaluation places P_i satisfy the splitting hypotheses **(H2-P_i)** for all $\mathbb{D}_{x_j}$ for $j = 1, \ldots, n$, we have:

$$\Lambda_{x_1,\ldots,x_n,P_i} \simeq \Lambda_{x_1,P_i} \otimes_{\mathcal{O}_{P_i}} \cdots \otimes_{\mathcal{O}_{P_i}} \Lambda_{x_n,P_i}$$

We can thus define the evaluation morphism as the tensor product of the evaluation morphisms on the gauge orders Λ_{x_j,P_i} for $j = 1, \ldots, n$ and define ALAG codes as the image of Riemann–Roch spaces under this evaluation morphism. We also prove the Riemann–Roch Theorem for extended evaluation divisors on these abelian division algebras, provided that $\mathbb{D}$ is a division algebra; which requires in the non-cyclic case that the constant field be infinite. We conjecture finally that ALAG codes can be decoded in polynomial time by using an algorithm analogous to the LAG decoding algorithm as it is corroborated by our SageMath implementation.

3.6 SageMath Implementations

- **Enumeration of self-dual skew cyclic codes**

  In the separable case where k is coprime to the characteristic p in a cyclic algebra $\frac{\mathbb{F}_{q^r}[T; \mathrm{Frob}(\mathbb{F}_{q^r}/\mathbb{F}_q)]}{T^{kr}-1}$, the algorithm works for the four finite geometries (Euclidean, Hermitian, skew-Euclidean and skew-Hermitian). It yields a solution in polynomial time at each iteration. In the purely inseparable case where $k = p^n$ is a power of the characteristic p, we computed the exhaustive enumeration of self-dual skew cyclic codes in the algebra $\frac{\mathbb{F}_{3^6}[T; \mathrm{Fr}]}{T^{18}-1}$. We obtained 2360960 distinct self-dual skew cyclic codes, which is indeed more than three times lower than the number $80 \cdot 1120 \cdot 80$ of (redundant) enumerations where 80 is the number of self-dual skew cyclic code in $\frac{\mathbb{F}_{3^6}[T; \mathrm{Fr}]}{T^6-1}$ for the Euclidean geometry and 1120 the

number of self-dual skew cyclic code in $\frac{\mathbb{F}_{3^6}[T;\mathrm{Fr}]}{T^6-\xi}$ where $\mathrm{Fr}^3(\xi) = -\xi$ for the skew Euclidean symmetry. The SageMath implementation location is the following. `https://plmlab.math.cnrs.fr/caruso/selfdual-skew-cyclic-codes`

- **LAG decoding algorithm**

  We restrict ourselves to the case of totally split evaluation places. We obtain a decoding defect relative to the theoretical decoding radius $\frac{d_{\mathrm{design}}-1}{2}$ of $\frac{g_\omega}{2}$, where g_ω is the genus of the gauge order given by the gauge ω. The SageMath implementation location is the following. `https://plmlab.math.cnrs.fr/drain/lag-decoding`

- **ALAG Decoding Algorithm**

  We provide without proof a SageMath implementation of ALAG decoding with a decoding defect of $\frac{g_\omega}{2}$ as for LAG decoding. We decode ALAG codes in the case of interest where r_1 and r_2 are not coprime, so that the splitting field is non-cyclic. (ALAG codes for r_1 coprime to r_2 are built upon a cyclic algebra and one easily checks that their associated genus is the same as the one of the corresponding LAG codes.) We thus obtain an ALAG code defined upon a matricial algebra with nonzero zero divisors. Nevertheless, by choosing x_1 and x_2 properly, we can still decode ALAG codes using the same decoding algorithm as for LAG codes. The SageMath implementation location is the following. `https://plmlab.math.cnrs.fr/drain/alag-decoding`

4 Organization of the Thesis

In a first section, we present our article on Self-dual Skew Cyclic Codes and the corresponding SageMath enumeration. Then, in the next section, we present our second and main article about LAG duality and decoding and its SageMath implementation. We also generalize LAG codes to shortened LAG codes and their dual punctured LAG codes. Further on, in a third and last section, we present Tamagawa's Theory and establish our Riemann–Roch Theorem as a corollary of Tamagawa's Theorem and our Serre Duality. Finally, we generalize LAG codes to abelian LAG (ALAG) codes. We sketch the proof of an analogous decoding algorithm for ALAG codes as for LAG codes and provide a SageMath implementation of this algorithm.

Chapter I

Self-dual Skew Cyclic Codes

1 Witt's Decomposition Theorem

We recall Witt's Decomposition Theorem over $\mathbb{F}_q$ in the Euclidean and in the Hermitian case in odd characteristic as it provides the theoretical foundation for solving the finite-geometry problem to which we reduced the self-dual skew cyclic code enumeration.

Theorem 1.0.1.
Let $(V, (_,_))$ be a non-degenerate Euclidean or Hermitian space of dimension $2s$ over a finite field of odd characteristic. We have an orthogonal direct sum of hyperbolic planes plus possibly an anisotropic plane in the Euclidean case.

$$V \simeq \overset{\perp}{\oplus}_{1\leqslant i\leqslant d} H_i \overset{\perp}{\oplus} W$$

The number of hyperbolic planes d in the decomposition is an invariant of V called the Witt index.

- *H_i is a hyperbolic plane $\langle u_i, v_i\rangle$ such that $(u_i, u_i) = (v_i, v_i) = 0$ and $(u_i, v_i) = 1$.*
- *W is either 0 or possibly an anisotropic plane in the Euclidean case, i.e., a plane containing no nonzero isotropic vectors.*

2 Article: Self-dual Skew Cyclic Codes

2.1 Abstract of the article [CD25]

Given a finite extension $\mathbf{K}/\mathbf{F}$ of degree r of a finite field $\mathbf{F}$, we enumerate all self-dual skew cyclic codes in the Ore quotient ring $\mathbf{E}_k := \mathbf{K}[X; \mathrm{Frob}]/(X^{rk} - 1)$ for any positive integer k coprime to the odd characteristic p (separable case). We also provide

an enumeration algorithm when k is a power of p (purely inseparable case), at the cost of some redundancies. Our approach is based on an explicit bijection between skew cyclic codes, on the one hand, and certain families of $\mathbf{F}$-linear subspaces of some extensions of $\mathbf{K}$. Finally, we report on an implementation in SageMath.

2.2 Introduction

Among linear codes, cyclic codes enjoy a rich algebraic structure as they are defined as ideals of quotient polynomial rings. This structure endows them with good properties (encoding, decoding, duality, dimension, distance, length). In the paper of Boucher, Geiselmann and Ulmer from 2006 [BGU06], cyclic codes are generalized by considering left ideals in Ore polynomial rings rather than in polynomial rings, thus obtaining a much larger class of linear codes called skew cyclic codes. In the present article, following their work, we study the self-dual property of these codes.

Let $\mathbf{K}/\mathbf{F}$ be a finite field extensions of degree r. Let $\theta : \mathbf{K} \to \mathbf{K}$ be the Frobenius $x \mapsto x^q$ where q denotes the cardinality of $\mathbf{F}$. We consider the Ore polynomial ring $\mathbf{K}[X;\theta]$, defined as the set of classical polynomials equipped with the standard addition and the twisted multiplication derived from the law $X\kappa = \theta(\kappa)X$ where κ is any element of K. Skew cyclic codes are by definition left ideals of a quotient of the form $\mathbf{E}_k := \mathbf{K}[X;\theta]/(X^{rk} - 1)$. We notice that cyclic codes correspond to the special case of skew cyclic codes when $r = 1$.

The ambient space $\mathbf{E}_k$ is equipped with a bilinear form coming from the coordinate-wise bilinear form on the vector space $\mathbf{K}^{rk}$, namely

$$\left(\sum_{i=0}^{kr-1} a_i X^i, \sum_{i=0}^{kr-1} b_i X^i\right) \mapsto \sum_{0 \leqslant i < rk} a_i b_i.$$

It thus makes sense to consider duality of skew cyclic codes. The topic was studied by Boucher among others [BU14, Bou15, Bou16, BBB20]. Notably, an existence criterion is given in [Bou15], while an enumeration of self-dual skew cyclic codes for $r = 2$ and a prime field $\mathbf{F}$ appears in [Bou16]. In the subsequent article [BBB20], the enumeration is extended to any positive integer r, for $k = 1$ and a prime field $\mathbf{F}$. In their conclusion, the authors suggest to further count and enumerate all self-dual skew cyclic codes for any values of the order r and of the degree k and for any finite base field $\mathbf{F}$. In the present paper, we give a complete answer to this question when the characteristic p of $\mathbf{F}$ is odd and k is coprime to it (separable case). We also study the case when k is a power of p (purely inseparable case) and obtain partial results in this case, our enumeration algorithm suffering from some redundancy.

As we will show in Subsection 2.3.1, r has to be even for self-dual skew cyclic codes to exist. We thus set $r = 2s$. We first consider the separable case, *i.e.,* we assume that

k is coprime with p. For the purpose of stating our main results, we write $\mathbf{F}[Y]/(Y^k-1)$ as a product of field extensions of $\mathbf{F}$, namely $\mathbf{F}[Y]/(Y^k-1) = \prod_{1\leqslant l\leqslant n} \mathbf{F}_l$ where each $\mathbf{F}_l$ corresponds to an irreducible factor of Y^k-1. We let y_l denote the image of Y in $\mathbf{F}_l$ and we set $\mathbf{K}_l := \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l$. We also consider the function τ acting on the indices l induced by the transformation $Y \mapsto \frac{1}{Y}$ on the irreducible factors of Y^k-1.

Let I be the subset of indexes $l \in \{1,\dots,n\}$ which are fixed by τ and let $I_{\mathtt{eucl}}$ (resp. $I_{\mathtt{herm}}$) be the subset of I consisting of indexes l such that $y_l = \pm 1$ (resp. $y_l \neq \pm 1$). Let also J be the set consisting of all the pairs $\{l, \tau(l)\}$ when l runs over the remaining indexes in $\{1,\dots,n\}\backslash I$. Finally, for each l, we denote by $\mathcal{V}(\mathbf{K}_l/\mathbf{F}_l)$ the set of $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$. When $l \in I_{\mathtt{eucl}}$ (resp. $l \in I_{\mathtt{herm}}$), we shall further equip $\mathbf{K}_l$ with a bilinear Euclidean (resp. sesquilinear Hermitian) form over $\mathbf{F}_l$; we let $\mathcal{S}_{\mathtt{eucl}}(\mathbf{K}_l/\mathbf{F}_l)$ (resp. $\mathcal{S}_{\mathtt{herm}}(\mathbf{K}_l/\mathbf{F}_l)$) denote the set of isotropic subspaces of $\mathbf{K}_l$ of dimension $s := r/2$. Our main theorem is as follows.

Theorem 2.1 There exists an explicit bijection between the set of self-dual skew cyclic codes in $\mathbf{E}_k$ and the Cartesian product of sets $W_{\mathtt{pal}} \times W_{\mathtt{nonpal}}$, where:

$$W_{\mathtt{pal}} = \prod_{l\in I_{\mathtt{eucl}}} \mathcal{S}_{\mathtt{eucl}}(\mathbf{K}_l/\mathbf{F}_l) \times \prod_{l\in I_{\mathtt{herm}}} \mathcal{S}_{\mathtt{herm}}(\mathbf{K}_l/\mathbf{F}_l)$$
$$W_{\mathtt{nonpal}} = \prod_{\{l,\tau(l)\}\in J} \mathcal{V}(\mathbf{K}_l/\mathbf{F}_l)$$

As a byproduct, we get the following counting of self-dual skew cyclic codes of $\mathbf{E}_k$.

Theorem 2.2 We assume that the characteristic of $\mathbf{F}$ is odd. Then there exist self-dual skew cyclic codes in $\mathbf{E}_k$ if and only if k is odd, s is odd and $q \equiv 3 \pmod 4$. Moreover, when self-dual codes exist, their number is given by

$$\prod_{l\in I_{\mathtt{eucl}}} \prod_{i=0}^{s-1} \left(q_l^i + 1\right) \times \prod_{l\in I_{\mathtt{herm}}} \prod_{i=0}^{s-1} \left(q_l^{i+1/2} + 1\right) \times \prod_{\{l,\tau(l)\}\in J} \sum_{k=0}^{r} \frac{\left(q_l^r - 1\right)\dots\left(q_l^{r-k+1} - 1\right)}{\left(q_l^k - 1\right)\dots\left(q_l - 1\right)}$$

where q_l denotes the cardinal of $\mathbf{F}_l$.

The existence criterion stated in the previous theorem was already known [Bou15]. Our approach, however, is new and allows for deriving other information, including the above counting formula and explicit methods for generating self-dual codes that we discuss now. First, we describe algorithms, with polynomial complexity in k and r, for generating randomly such a code, with uniform distribution. We then move to the question of complete enumeration. Since self-dual skew cyclic codes are quite numerous (their number grows exponentially with respect to r), it is not particularly useful to design an algorithm that outputs the complete list of such codes in one shot. Instead, we describe a routine that outputs a new code each time it is called with the

guarantee that all codes will show up–and show up only once–ultimately. The cost of each individual call to our algorithm is again polynomial in k and r.

Our method looks robust in the sense that we are confident that it could be adapted to other situations, *e.g.* even characteristic or negacyclic (or more generally, constacyclic) codes. However, addressing the inseparable case where k is not coprime to p using analogous methods seems more delicate (although probably doable). In the present paper, we outline a different method for enumerating all purely inseparable self-dual skew cyclic codes, for which k is a power of the characteristic p, by multiplying properly generators of some twisted separable self-dual skew cyclic codes as described and illustrated by means of SageMath computations in Section 2.5. This enumeration method could be used in combination with the enumeration method of the separable case to solve the general inseparable enumeration problem. However, it is not optimal as it comes with redundancies.

Organization of the paper

In Section 2.3, we define self-dual skew cyclic codes. Then, under the separability hypothesis that k is coprime to p, we relate the skew algebra $\mathbf{E}_k$ to a product of matrix algebras, and we transport the bilinear structure of $\mathbf{E}_k$ onto matrices. In Section 2.4, we use this reinterpretation to count self-dual skew cyclic codes and to generate them efficiently. In Section 3, we report on an implementation of our algorithms and provide some numerical experiments. The source code of the SageMath implementation is available at this location:

`https://plmlab.math.cnrs.fr/caruso/selfdual-skew-cyclic-codes`

In Section 2.5, we sketch an enumeration algorithm for purely inseparable self-dual skew cyclic codes, in the case where k is a power of p. Finally, we provide computation results for the enumeration of purely inseparable skew cyclic codes.

Conventions and notations

Throughout this paper, we will use the following notation:

- $\mathrm{End}_R(V)$ denotes, for any ring R and R-module V, the endomorphism ring of R-linear endomorphisms of V.
- $\mathrm{Mat}_{R,r\times r}$ denotes, for any ring R, the matrix ring of $r \times r$ square matrices with entries in R.
- M^{tr} denotes the transpose of the matrix M.
- id denotes the identity morphism.

- $\mathrm{GL}_n(F)$ denotes the general linear group of the vector space F^n over the finite field F.
- L^σ denotes the subfield of L fixed by the automorphism σ.
- $V^\perp$ denotes the orthogonal space of the subvector space V in some ambient space.

If F is a finite field, equipped with an involutive automorphism σ (*i.e.,* an automorphism of order 2), we recall that a *σ-sesquilinear form* $\mathcal{B}$ of an F-vector space V is an additive map $\mathcal{B} : V \times V \to F$ such that

$$\mathcal{B}(\lambda u, \mu v) = \lambda \cdot \sigma(\mu) \cdot \mathcal{B}(u, v) \qquad \forall u, v \in V, \quad \forall \lambda, \mu \in F$$

In this paper, we will consider four different types of sesquilinear forms:

- Euclidean case:

  $\sigma = \mathrm{id}$ and $\mathcal{B}$ is symmetric, *i.e.,* $\mathcal{B}(u, v) = \mathcal{B}(v, u)$ for all $u, v \in V$,

- skew-Euclidean case:

  $\sigma = \mathrm{id}$ and $\mathcal{B}$ is antisymmetric, *i.e.,* $\mathcal{B}(u, v) = -\mathcal{B}(v, u)$ for all $u, v \in V$,

- Hermitian case:

  $\sigma \neq \mathrm{id}$ and $\mathcal{B}$ is Hermitian, *i.e.,* $\mathcal{B}(u, v) = \sigma(\mathcal{B}(v, u))$ for all $u, v \in V$,

- skew-Hermitian case:

  $\sigma \neq \mathrm{id}$ and $\mathcal{B}$ is skew-Hermitian, *i.e.,* $\mathcal{B}(u, v) = -\sigma(\mathcal{B}(v, u))$ for all $u, v \in V$.

We recall that, when $\mathcal{B}$ is non-degenerate, the ring $\mathrm{End}_F(V)$ of F-linear endomorphisms of V is equipped with an involutive anti-automorphism $f \mapsto f^\star$ characterized by

$$\forall u, v \in V, \quad \mathcal{B}\big(u, f^\star(v)\big) = \mathcal{B}\big(f(u), v\big)$$

It is called the *adjunction* relative to $\mathcal{B}$. We recall that $(f + g)^\star = f^\star + g^\star$ and $(f \circ g)^\star = g^\star \circ f^\star$ for $f, g \in \mathrm{End}_F(V)$. Moreover, the adjoint of the scalar multiplication by an element $a \in F$ is the multiplication by $\sigma(a)$. The adjoint construction allows finally to endow $\mathrm{End}_F(V)$ itself with a sesquilinear pairing, defined by $\langle f, g \rangle = \mathrm{Trace}(f \circ g^\star)$.

Acknowledgments
We warmly thank Delphine Boucher and the anonymous referee for pointing out several inconsistencies in a former version of this article. This research was supported by the grant ANR-21-CE39-0009-BARRACUDA.

2.3 From skew cyclic codes to finite geometry

2.3.1 Definition of skew cyclic codes

Let $\mathbf{F}$ be a finite field of cardinality q and characteristic p. Let $\mathbf{K}$ be a finite extension of $\mathbf{F}$ of degree r. Let $\theta : x \mapsto x^q$ be the Frobenius automorphism of $\mathbf{K}$. We build the quotient of the free $\mathbf{K}$-algebra $\mathbf{K}\langle X\rangle$ by the noncommutative relation: $\forall \kappa \in \mathbf{K}$, $X\kappa = \theta(\kappa)X$. We then localize it at the powers of X. This results in the Ore Laurent polynomial ring $\mathbf{K}[X^{\pm 1};\theta]$. As shown in [Jac96, Theorem 1.1.22], its center is $\mathbf{F}[X^{\pm r}]$. For any $f \in \mathbf{F}[X^{\pm r}]$, we can thus form the quotient $\mathbf{K}[X^{\pm 1};\theta]/(f(X))$, which keeps a ring structure. We will call *skew quotient algebra* the algebra $\mathbf{K}[X^{\pm 1};\theta]/(f(X))$.

Remark 2.3 As a quotient ring of the left and right Euclidean domain of skew Laurent polynomials, $\mathbf{K}[X^{\pm 1};\theta]$, any skew quotient algebra is a left and right principal ideal ring.

We now move to the definition of self-dual skew cyclic codes. For any positive integer k, $X^{rk} - 1$ is in the center of $\mathbf{K}[X^{\pm 1};\theta]$. We can form the quotient ring $\mathbf{E}_k := \mathbf{K}[X^{\pm 1};\theta]/(X^{rk} - 1)$. Choosing for any element of $\mathbf{E}_k$ the unique lift in $\mathbf{K}[X;\theta] \subset \mathbf{K}[X^{\pm 1};\theta]$ of degree strictly less than kr defines an isomorphism of $\mathbf{K}$-vector spaces $\lambda : \mathbf{E}_k \to \mathbf{K}^{rk}$.

Using the classical Hamming distance d on the $\mathbf{K}$-vector space $\mathbf{K}^{rk}$, we define the *Hamming distance* D between two elements f and g of $\mathbf{E}_k$ by $D(f,g) = d(\lambda(f), \lambda(g))$.

Definition 2.4 Given $\alpha \in \mathbf{F}^*$, a *skew α-constacyclic code* is a left ideal of $\mathbf{K}[X^{\pm 1};\theta]/(X^{rk} - \alpha)$ endowed with the metric D. *Skew cyclic codes* (resp. *skew negacyclic codes*) are skew α-constacyclic codes for $\alpha = 1$ (resp. $\alpha = -1$).

We are interested in the skew cyclic code duality for the coordinate-wise bilinear form, defined on $\mathbf{K}^{rk}$ by

$$\big((x_i)_{0\leqslant i<rk}, (y_i)_{0\leqslant i<rk}\big) \mapsto \sum_{0\leqslant i<rk} x_i y_i$$

We note that this bilinear form is non-degenerate.

Definition 2.5 A skew cyclic code is said *self-orthogonal* (resp. *self-dual*) if $\lambda(I) \subset \lambda(I)^\perp$ (resp. if $\lambda(I) = \lambda(I)^\perp$).

As we have $\dim(\lambda(I)) + \dim(\lambda(I)^\perp) = rk$, a necessary condition for self-dual skew cyclic codes to exist is that rk is even.

2.3.2 The evaluation isomorphism $\mathcal{E}_l$

We now place ourselves in the separable case, where k is coprime to p. It is then known that $\mathbf{E}_k$ is a semisimple algebra (see [Wis91, Proposition 20.7]). As $\mathbf{E}_k$ is finite-dimensional over $\mathbf{F}$, classical results imply that it is a Cartesian product of matrix algebras over finite field extensions of $\mathbf{F}$. Below, we describe an explicit isomorphism realizing this decomposition.

We note $Y := X^r$ and decompose $Y^k - 1$ as a product of irreducible polynomials $P_l(Y)$ over $\mathbf{F}$. We set $\mathbf{F}_l := \mathbf{F}[Y]/P_l(Y)$, $\mathbf{K}_l := \mathbf{K}[Y]/P_l(Y)$ and let y_l denote the image of Y in $\mathbf{K}_l$. We extend θ to an automorphism of $\mathbf{K}_l$ by letting it act trivially on y_l. We have a first decomposition

$$\begin{aligned}\mathbf{E}_k &\simeq \mathbf{K}[Y, X; \theta]/(Y^k - 1, X^r - Y) \\ &\simeq \left(\frac{\mathbf{K}[Y, X; \theta]}{\prod\limits_{1 \leqslant l \leqslant n} P_l(Y)}\right)/(X^r - Y) = \prod_{1 \leqslant l \leqslant n} \mathbf{K}_l[X^{\pm 1}; \theta]/(X^r - y_l). \end{aligned} \tag{2.1}$$

We set $\tilde{\mathbf{E}}_k^{(l)} = \mathbf{K}_l[X^{\pm 1}; \theta]/(X^r - y_l)$ and now study each $\tilde{\mathbf{E}}_k^{(l)}$ separately. We observe that $\mathbf{K}_l$ is a finite étale extension of the finite field $\mathbf{F}_l$, *i.e.,* a finite product of finite extensions of $\mathbf{F}_l$. As such, the norm map $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}$ is surjective; hence, there exists an element x_l in $\mathbf{K}_l$ satisfying $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(x_l) = y_l$. The change of variables $X \mapsto x_l X$ defines an isomorphism

$$\mathrm{Eval}_{x_l X} : \tilde{\mathbf{E}}_k^{(l)} \xrightarrow{\sim} \mathbf{E}_k^{(l)} := \mathbf{K}_l[X^{\pm 1}; \theta]/(X^r - 1).$$

On the other hand, we have an evaluation morphism $X \mapsto \theta$:

$$\begin{array}{rccc} \mathrm{Eval}_\theta : & \mathbf{E}_k^{(l)} & \longrightarrow & \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l) \\ & P(X) & \mapsto & P(\theta) \end{array}$$

Composing both maps, we obtain a third morphism $\mathcal{E}_l : \tilde{\mathbf{E}}_k^{(l)} \to \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$. Applying it to each term $\tilde{\mathbf{E}}_k^{(l)}$ of the decomposition (2.1), we finally end up with a map relating $\mathbf{E}_k$ to a product of matrix algebras.

Proposition 2.6 The map

$$\left(\mathcal{E}_l\right)_{l \in \{1, \ldots, n\}} : \mathbf{E}_k \longrightarrow \prod_{1 \leqslant l \leqslant n} \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

is an $\mathbf{F}$-algebra isomorphism.

Proof. (See also [Jac96, Theorem 1.3.12].) By Artin's lemma, the family $(\theta^i)_{0 \leqslant i < r}$ is linearly independent. This proves the injectivity of $\mathcal{E}_l$. As the dimension (over $\mathbf{F}_l$) of

its domain and the codomain are both r^2, surjectivity follows. The final evaluation map resulting from the composition of the Chinese remainder isomorphism with the product of isomorphisms $\mathrm{Eval}_{x_l\theta}$ is thus an isomorphism. □

Remark 2.7 To compute the evaluation isomorphism $\mathcal{E}_l$, a fast computation of preimages by the norm is needed. One possible method consists of finding an irreducible factor of the skew polynomial $X^r - y_l$ in $\mathbf{K}_l[X;\theta]$. An algorithm for this task is described in [CB17].

Remark 2.8 By the Skolem–Noether theorem, the isomorphism $\mathcal{E}_l$ is uniquely defined up to conjugacy by an element of norm 1, *i.e.,* up to another choice of x_l as preimage of y_l by the norm map.

2.3.3 Adjunctions on $\mathbf{E}_k$ and related spaces

In this subsection, we construct an alternative bilinear pairing on $\mathbf{E}_k$ and show that it induces the same orthogonals as the coordinatewise bilinear form considered previously. Our variant is interesting because it will in turn induce a pairing on the simpler spaces $\mathbf{E}_k^{(l)}$.

We begin by defining an adjunction on $\mathbf{E}_k$. We start from the following $\mathbf{F}$-linear automorphism on $\mathbf{K}[X^{\pm 1};\theta]$

$$\begin{array}{ccc} \mathbf{K}[X^{\pm 1};\theta] & \xrightarrow{*} & \mathbf{K}[X^{\pm 1};\theta] \\ f = \sum_i f_i X^i & \mapsto & f^* = \sum_i X^{-i} f_i \end{array}$$

It is an involution, *i.e.,* $f^{**} = f$ for all f. One moreover checks that it is an anti-morphism, *i.e.,* it satisfies $(fg)^* = g^* f^*$ for all $f, g \in \mathbf{K}[X^{\pm 1};\theta]$. Indeed, by linearity, it is enough to check the desired property when f and g are monomials, which is a direct computation. We observe that the adjoint $(X^{rk}-1)^*$ is a multiple of $X^{rk}-1$ itself. The adjunction thus preserves the two-sided ideal generated by $X^{rk}-1$; therefore, it passes to the quotient to define an anti-automorphism of $\mathbf{E}_k$. In a slight abuse of notation, we continue to write f^* when $f \in \mathbf{E}_k$. Since the adjunction is an anti-automorphism, we underline that it maps left ideals of $\mathbf{E}_k$ to right ideals.

We now define a non-degenerate bilinear form corresponding to this adjunction. We introduce to this end the notion of *reduced trace* of a skew polynomial: given $f = \sum_i f_i X^i \in \mathbf{K}[X^{\pm 1};\theta]$, we set

$$T_{\mathrm{rd}}(f) = \sum_i \mathrm{Trace}_{\mathbf{K}/\mathbf{F}}(f_{ir}) \cdot Y^i \in \mathbf{F}[Y].$$

This definition passes to the quotient and defines a map $T_{\mathrm{rd}} : \mathbf{E}_k \to \mathbf{F}[Y]/(Y^k - 1)$.

For $f, g \in \mathbf{E}_k$, we define

$$\langle f, g \rangle := T_{\mathrm{rd}}(fg^*) \in \mathbf{F}[Y]/(Y^k - 1).$$

It is readily seen that $f \mapsto f^*$ satisfies the adjunction formula, in the sense that $\langle f, gh \rangle = \langle fh^*, g \rangle$ for any $f, g, h \in \mathbf{E}_k$. Denoting by $I^\perp$ the orthogonal space of $I \subset \mathbf{E}_k$, we have the following compatibility property.

Proposition 2.9 For any left ideal I of $\mathbf{E}_k$, we have $\lambda(I^\perp) = \lambda(I)^\perp$.

Proof. Let $f \in I$, $g \in I^\perp$ and set $u = \sum_{0 \leqslant i < kr} \lambda(f)_i \lambda(g)_i$. The condition $T_{\mathrm{rd}}(fg^*) = 0$ translates to $\mathrm{Trace}_{\mathbf{K}/\mathbf{F}}(u) = 0$. More generally, for all $\kappa \in \mathbf{K}$, we have $T_{\mathrm{rd}}(\kappa f g^*) = 0$ (since $\kappa f \in I$) and so $\mathrm{Trace}_{\mathbf{K}/\mathbf{F}}(\kappa u) = 0$. By non-degeneracy of $\mathrm{Trace}_{\mathbf{K}/\mathbf{F}}$, this implies that $u = 0$, *i.e.,* $\lambda(f)$ is orthogonal to $\lambda(g)$. The inclusion $\lambda(I^\perp) \subset \lambda(I)^\perp$ follows.

Conversely, we consider $g \in \mathbf{E}_k$ such that $\lambda(g) \in \lambda(I)^\perp$. Let also $f \in I$. The orthogonality condition between $\lambda(f)$ and $\lambda(g)$ implies the vanishing of the constant coefficient of fg^*. More generally, using that $X^{-ir} f \in I$, we deduce that the coefficient in X^{ir} of fg^* vanishes as well. Therefore $T_{\mathrm{rd}}(fg^*) = 0$ and we conclude that $g \in I^\perp$. $\square$

In what follows, we prefer working with the pairing $\langle -, - \rangle$ because it corresponds to sesquilinear trace forms on the $\mathbf{F}_l$-algebras $\mathbf{E}_k^{(l)}$. We now describe them.

Definition 2.10 We say that a polynomial is *palindromic* if the set of its roots in an algebraic closure of its base field does not contain zero and is stable under the inversion map $x \mapsto \frac{1}{x}$. Equivalently a polynomial $\sum_{i=0}^n p_i x^i$ (with $p_n \neq 0$) is *palindromic* if it is collinear to its reciprocal polynomial $\sum_{i=0}^n p_{n-i} x^i$.

We recall that we have the decomposition $F[Y]/(Y^k - 1) \simeq \prod_{1 \leqslant l \leqslant n} F[Y]/P_l(Y) \simeq \prod_{1 \leqslant l \leqslant n} \mathbf{F}_l$.

Definition 2.11 We define the map $\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$ by the relation $P_{\tau(l)}(\frac{1}{y_l}) = 0$.

As the polynomial $Y^k - 1$ is palindromic and separable, the index $\tau(l)$ exists, and τ is obviously involutive. Furthermore, we let σ be the endomorphism of F-algebras of $\mathbf{F}[Y]/(Y^k - 1)$ defined by $Y \mapsto \frac{1}{Y}$. It is also involutive, and it induces isomorphisms $\sigma_l : \mathbf{F}_l \to \mathbf{F}_{\tau(l)}$ such that $\sigma_l(y_l) = \frac{1}{y_{\tau(l)}}$. The tensor product $\mathrm{id} \otimes \sigma_l$ defines an involutive isomorphism $\mathbf{K}_l \to \mathbf{K}_{\tau(l)}$ extending σ_l. For simplicity, we will keep the notation σ_l for $\mathrm{id} \otimes \sigma_l$.

The next proposition shows that the adjunction behaves nicely with respect to the decomposition $\mathbf{E}_k = \prod_{l=1}^n \tilde{\mathbf{E}}_k^{(l)}$ we have established in Equation (2.1).

Proposition 2.12 The adjunction $f \mapsto f^*$ induces "partial" adjunctions $\tilde{\mathbf{E}}_k^{(l)} \to \tilde{\mathbf{E}}_k^{(\tau(l))}$, which are explicitly given by the formula

$$\sum_{i=0}^{r-1} f_i X^i \mapsto \sum_{i=0}^{r-1} X^{-i} \sigma_l(f_i), \quad \forall f_i \in \mathbf{K}_l. \tag{2.2}$$

Moreover, the "global" adjunction can be recovered by taking the product of the partial ones.

Proof. Let Q_l be the element of $F[Y]/(Y^k - 1) \subset \mathbf{E}_k$ corresponding to the factor $\mathbf{F}_l$, *i.e.,* the element defined by the congruences $Q_l \equiv 1 \pmod{P_l}$ and $Q_l \equiv 0 \pmod{P_{l'}}$ whenever $l' \neq l$. As automorphisms respect congruences, we have $Q_l^* = \sigma(Q_l) = Q_{\tau(l)}$. Besides $\tilde{\mathbf{E}}_k^{(l)} = Q_l \mathbf{E}_k = \mathbf{E}_k Q_l$. We thus have $\tilde{\mathbf{E}}_k^{(l)*} = (Q_l \mathbf{E}_k)^* = \mathbf{E}_k Q_l^* = \mathbf{E}_k Q_{\tau(l)} = \tilde{\mathbf{E}}_k^{(\tau(l))}$. The explicit formula (2.2) is derived after noticing that $f_i^* = \sigma_l(f_i)$ for $f_i \in \mathbf{K}_l$. Finally, the last statement of the proposition is clear. □

We now aim at describing how the adjunction is transformed by the evaluation isomorphisms $\mathcal{E}_l$. For this, the first step is to understand its effect on $\mathbf{E}_k^{(l)}$ (without the tilde) which, we recall, is defined as $\mathbf{E}_k^{(l)} = \mathbf{K}_l[X;\theta]/(X^r - 1)$. The adjunction $f \mapsto f^*$ again passes to the quotient and determines a well-defined adjunction $\mathbf{E}_k^{(l)} \to \mathbf{E}_k^{(\tau(l))}$, that we continue to denote $f \mapsto f^*$. Unfortunately, the latter is not exactly what we need; we are now going to fix this issue by defining a twisting version of it. For this, we first define $z_l := x_l \cdot \sigma_{\tau(l)}(x_{\tau(l)}) \in \mathbf{K}_l$.

Lemma 2.13 There exists a family of invertible elements $\zeta_l \in \mathbf{K}_l$ such that $\theta(\zeta_l) = z_l \zeta_l$ and $\sigma_l(\zeta_l) = \zeta_{\tau(l)}$ for all l.

Proof. Since $\sigma_l \circ \sigma_{\tau(l)} = \mathrm{id}$, we have $\sigma_l(x_l \cdot \sigma_{\tau(l)}(x_{\tau(l)})) = x_{\tau(l)} \sigma_l(x_l)$, which ensures that z_l is invariant under σ_l. Furthermore, we observe that $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(z_l) = y_l \cdot \sigma_{\tau(l)}(y_{\tau(l)}) = 1$. Hence, the Hilbert 90 Theorem guarantees the existence of an element ζ_l of $\mathbf{K}_l^*$ such that $\theta(\zeta_l) = z_l \zeta_l$ and hence $z_l X = \zeta_l^{-1} X \zeta_l$. Moreover, as automorphisms of finite fields commute, $\sigma_l(\zeta_l)$ satisfies $\theta(\sigma_l(\zeta_l)) = z_l \sigma_l(\zeta_l)$. Set $\zeta_l' := \zeta_l + \sigma_{\tau(l)}(\zeta_{\tau(l)})$, so that we have $\sigma_l(\zeta_l') = \zeta_{\tau(l)}'$. If ζ_l' is invertible, it satisfies $z_l X = {\zeta_l'}^{-1} X \zeta_l'$ as well. Conversely, if $\zeta_l' = 0$, we have $\sigma_{\tau(l)}(\zeta_{\tau(l)}) = -\zeta_l$. In this case, σ_l is nontrivial and so $y_{\tau(l)} \neq \pm 1$. As $\frac{\zeta_l}{y_l}$ satisfies also $\theta\big(\frac{\zeta_l}{y_l}\big) = z_l \frac{\zeta_l}{y_l}$, the element $\zeta_l'' := \frac{\zeta_l}{y_l} + \sigma_{\tau(l)}\big(\frac{\zeta_{\tau(l)}}{y_{\tau(l)}}\big)$ does not vanish and it satisfies moreover $\zeta_l'' z_l X = X \zeta_l''$ and $\sigma_l(\zeta_l'') = \zeta_{\tau(l)}''$. In full generality, we write $\mathbf{K}_l$ as a product of fields and apply the previous reasoning component by component. □

Remark 2.14 The element ζ_l can be efficiently computed using the following formula from the proof of the Hilbert 90 Theorem: it can be chosen as the multiplicative inverse of any nonzero element in the image of the endomorphism $\sum_{0 \leqslant i < r} \prod_{0 \leqslant j < i} \theta^j(z_l) \theta^i$.

Definition 2.15 For $f \in \mathbf{E}_k^{(l)}$, we set $f^\bullet := (\zeta_l f \zeta_l^{-1})^* = \zeta_{\tau(l)}^{-1} f^* \zeta_{\tau(l)} \in \mathbf{E}_k^{(\tau(l))}$.

Lemma 2.16 For all $f \in \tilde{\mathbf{E}}_k^{(l)}$, we have $f^*(x_{\tau(l)}X) = f(x_l X)^\bullet$.

Proof. By additivity, it is enough to check the formula when f is the monomial κX^i. We thus have $f^* = X^{-i}\sigma_l(\kappa)$ and so

$$f^*(x_{\tau(l)}X) = X^{-i}\sigma_l(\kappa)\left(\prod_{t=0}^{i-1}\theta^t(x_{\tau(l)})\right)^{-1}$$
$$f(x_lX)^\bullet = \left(\kappa\prod_{t=0}^{i-1}\theta^t(x_l)X^i\right)^\bullet = (z_{\tau(l)}X)^{-i}\sigma_l\left(\kappa\prod_{t=0}^{i-1}\theta^t(x_l)\right).$$

We conclude by noticing that $\prod_{t=0}^{i-1}\theta^t(z_{\tau(l)}) = \prod_{t=0}^{i-1}\theta^t(x_{\tau(l)})\sigma_l\left(\prod_{t=0}^{i-1}\theta^t(x_l)\right)$. □

Following the isomorphism $\mathbf{E}_k^{(l)} \simeq \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ and its counterpart for $\tau(l)$, we find that the adjunction $f \mapsto f^\bullet$ induces another anti-isomorphism $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l) \xrightarrow{\bullet} \mathrm{End}_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)})$. We are now going to prove that the latter is the adjunction map associated to some explicit sesquilinear map. Precisely, we introduce the twisted sesquilinear trace form

$$\begin{array}{rcl} \mathbf{K}_l \times \mathbf{K}_{\tau(l)} & \longrightarrow & \mathbf{F}_l \\ (\kappa,\rho) & \mapsto & (\kappa,\rho)_{\mathbf{F}_l} := \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l \cdot \kappa \cdot \sigma_{\tau(l)}(\rho)) \end{array} \tag{2.3}$$

In the palindromic case, we have $\mathbf{K}_{\tau(l)} = \mathbf{K}_l$, and we observe that the above pairing is Euclidean when $y_l = \pm 1$ and Hermitian otherwise. In all cases, the sesquilinear form $(-,-)_{\mathbf{F}_l}$ is non-degenerate and hence identifies $\mathbf{K}_l$ with the dual of $\mathbf{K}_{\tau(l)}$.

Proposition 2.17 The involutive isomorphism $\bullet$ is the adjunction relative to $(-,-)_{\mathbf{F}_l}$, *i.e.,*

$$(f(\kappa),\rho)_{\mathbf{F}_l} = (\kappa, f^\bullet(\rho))_{\mathbf{F}_l}, \qquad \forall f \in \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l), \quad \forall \kappa \in \mathbf{K}_l, \quad \forall \rho \in \mathbf{K}_{\tau(l)}.$$

Proof. We write $f = \sum_{0\leqslant i\leqslant r-1} f_i\theta^i$ with $f_i \in \mathbf{K}_l$ and compute

$$\begin{aligned}(f(\kappa),\rho)_{\mathbf{F}_l} &= \sum_{k=0}^{r-1}\theta^k\left(\zeta_l\cdot\sigma_{\tau(l)}(\rho)\cdot\sum_{i=0}^{r-1}f_i\theta^i(\kappa)\right)\\ &= \sum_{i=0}^{r-1}\sum_{k=0}^{r-1}\theta^{k+i}\left(\zeta_l\cdot\theta^{-i}(f_i)\cdot\frac{\theta^{-i}(\zeta_l)}{\zeta_l}\cdot\theta^{-i}(\sigma_{\tau(l)}(\rho))\cdot\kappa\right)\\ &= \sum_{k=0}^{r-1}\theta^k\left(\sum_{i=0}^{r-1}\zeta_l\cdot\theta^{-i}(f_i)\cdot\theta^{-i}(\zeta_l\sigma_{\tau(l)}(\rho))\cdot\zeta_l^{-1}\cdot\kappa\right)\\ &= \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l\cdot\sigma_{\tau(l)}(f^\bullet(\rho))\cdot\kappa) = (\kappa, f^\bullet(\rho))_{\mathbf{F}_l}\end{aligned}$$

which is exactly what we want. □

Finally, composing the morphisms $X \mapsto x_l X$ and $X \mapsto \theta$, we obtain the following commutative diagram:

$$\begin{array}{ccccc} \tilde{\mathbf{E}}_k^{(l)} & \xrightarrow{X\mapsto x_l X} & \mathbf{E}_k^{(l)} & \xrightarrow{X\mapsto\theta} & \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l) \\ \downarrow{\scriptstyle f\mapsto f^*} & & \downarrow{\scriptstyle f\mapsto f^\bullet} & & \downarrow{\scriptstyle \text{adjunction for } (-,-)_{\mathbf{F}_l}} \\ \tilde{\mathbf{E}}_k^{(\tau(l))} & \xrightarrow{X\mapsto x_{\tau(l)} X} & \mathbf{E}_k^{(\tau(l))} & \xrightarrow{X\mapsto\theta} & \mathrm{End}_{\mathbf{F}_{\tau(l)}}(\mathbf{K}_{\tau(l)}) \end{array} \tag{2.4}$$

where we note that the composite of the horizontal maps is $\mathcal{E}_l$ on the top, and $\mathcal{E}_{\tau(l)}$ on the bottom.

2.3.4 Vector space duality

In the previous subsections, we reduced the problem of finding self-dual skew cyclic codes in $\mathbf{E}_k$ to that of finding self-dual skew cyclic codes in the product of the $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$. We will now further reduce this problem to that of finding maximal isotropic $\mathbf{F}_l$-vector spaces of $\mathbf{K}_l$ in the palindromic case and of $\mathbf{K}_l \times \mathbf{K}_{\tau(l)}$ in the non-palindromic case.

To this end, we apply the classical duality between $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ and left ideals of $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$.Let us recall it briefly. Given a field F and a finite-dimensional F-vector space W, the *vector space duality* associates to every F-vector subspace V of W, the left ideal I_V of $\mathrm{End}_F(W)$ formed by the endomorphisms vanishing on V. Dually, it associates to every left ideal I of $\mathrm{End}_F(W)$, the intersection of the kernels of the morphisms in I. With formulas, it can be expressed as

$$\begin{aligned} I \mapsto V_I &= \bigcap_{f\in I} \ker(f), \\ V \mapsto I_V &= \big\{\, f \in \mathrm{End}_F(W) \,|\, V \subset \ker(f) \,\big\}. \end{aligned}$$

This duality defines an order-reversing one-to-one correspondence between the set of left ideals of $\mathrm{End}_F(W)$ and the set of F-vector subspaces of W. Moreover, for all $V \subset W$, we have $\dim_F I_V = (\dim_F W - \dim_F V) \cdot \dim_F W$.

We now assume in addition that we are given an involution $\sigma : F \to F$ and that W is endowed with a non-degenerate σ-sesquilinear form. We recall that this datum equips $\mathrm{End}_F(W)$ with a sesquilinear form as well. In particular, taking orthogonals over W and $\mathrm{End}_F(W)$ makes sense.

Proposition 2.18 For all subspaces V of W, we have $I_V^\perp = I_{V^\perp}$.

Proof. Given $f \in I_V$ and $g \in I_{V^\perp}$, we have $f \circ g^\star = 0$ since f vanishes on V and

im $g^\star = (\ker g)^\perp \subset V$. Therefore, f and g are orthogonal in $\mathrm{End}_F(W)$. It follows that $I_{V^\perp} \subset I_V^\perp$. The equality follows by comparing dimensions. □

We are now ready to apply what precedes to codes and prove the main theorem of this section.

Theorem 2.19 There exists an explicit bijection between the set of self-dual skew cyclic codes of $\mathbf{E}_k$ and the Cartesian product of sets $W_{\mathtt{pal}} \times W_{\mathtt{nonpal}}$, where:

- $W_{\mathtt{pal}}$ is the Cartesian product, over the set I of indexes invariant under τ, of the sets of isotropic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ of dimension $r/2$,
- $W_{\mathtt{nonpal}}$ is the Cartesian product, over the set J of all remaining nontrivial orbits of τ, of the sets of $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$.

Proof. By what we have done in previous subsections, self-dual codes in $\mathbf{E}_k$ are in bijection with left ideals of the Cartesian product

$$\prod_{l=1}^{n} \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

that are equal to their orthogonal. Besides, the orthogonal space of an ideal can be taken component by component, with the care that the orthogonal space of the l-th component lies in the $\tau(l)$-th component. Therefore, when $\tau(l) = l$, the l-th component must be self-dual itself whereas, when $\tau(l) \neq l$, the component at position l can be anything but it determines the component at position $\tau(l)$. Using now the vector space duality, we can further replace ideals of $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ by $\mathbf{F}_l$-subspaces of $\mathbf{K}_l$. This operation preserves the orthogonality condition as the vector space duality commutes with orthogonals.

We finally conclude by noticing that a subspace of $\mathbf{K}_l$ which is equal to its orthogonal is precisely a totally isotropic subspace of dimension $r/2$. Since $Y-1$ devides Y^k-1, no self-dual code exists in the separable case when r is odd. Henceforth we set $r = 2s$. □

2.4 Counting and generating self-dual skew cyclic codes

We keep the notation introduced before. In particular, we recall that $\mathbf{K}/\mathbf{F}$ is a finite field extensions of degree r and that $\mathbf{E}_k = \mathbf{K}[X;\theta]/(X^{kr}-1)$ (where $\theta : x \mapsto x^q$ with $q = \mathrm{Card}\ \mathbf{F}$). Besides, we set $Y = X^r$ and assume that k is coprime with p. Under this hypothesis, the polynomial $Y^k - 1$ is separable and we write down its decomposition as a product of irreducible factors $Y^k - 1 = P_1(Y) \cdots P_n(Y)$. We recall also that we have introduced an involution $\tau : \{1,\dots,n\} \to \{1,\dots,n\}$ defined by the condition that the roots of P_l are the inverses of the roots of $P_{\tau(l)}$. In Subsection 2.3.2, we proved that we

have an isomorphism of the form

$$\mathbf{E}_k \simeq \prod_{l=1}^{n} \mathbf{K}_l[X;\theta]/(X^r - y_l) \simeq \prod_{l=1}^{n} \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

where $\mathbf{F}_l = \mathbf{F}[Y]/P_l(Y)$, $\mathbf{K}_l = \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l = \mathbf{K}[Y]/P_l(Y)$ and y_l is the image of Y in $\mathbf{K}_l$. In Subsection 2.3.3, we showed that this decomposition preserves orthogonality in some precise sense. This allowed us to conclude (see Theorem 2.19) that enumerating self-dual skew cyclic codes sitting in $\mathbf{E}_k$ boils down to enumerating maximal isotropic $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ when $\tau(l) = l$ (palindromic case), and to enumerating $\mathbf{F}_l$-vector subspaces of $\mathbf{K}_l$ otherwise.

In this section, we rely on this theoretical result, first, to count skew cyclic codes and, second, to construct them explicitly. More precisely, we shall address two different problems: that of random generation and that of complete enumeration.

Throughout this section, we assume that the characteristic of $\mathbf{F}$ *is odd.*

2.4.1 Existence criterion

By Theorem 2.19, there exist self-dual codes in $\mathbf{E}_k$ if and only if for each l such that $\tau(l) = l$, the space $\mathbf{K}_l$ admits a totally isotropic subspace of dimension $s := r/2$. We then aim at providing simpler conditions for this property to hold. For this, we shall use Witt's decomposition theorem as a fundamental tool. Let us recall it briefly. Let F be a field of odd characteristic, and let $\sigma : F \to F$ be a ring homomorphism which is an involution (possibly the identity). Let V be a finite-dimensional vector space over F, endowed with a σ-sesquilinear form $\mathcal{B} : V \times V \to F$. We recall that a *hyperbolic pair* is a pair of vectors (u, v) of V satisfying $\mathcal{B}(u, u) = 0$, $\mathcal{B}(v, v) = 0$ and $\mathcal{B}(u, v) = 1$, and that the 2-dimensional subspace of V spanned by a hyperbolic pair (u, v) is called a *hyperbolic plane*.

Theorem 2.20 Keeping the previous notation, there exists an invariant d (called the Witt index of V) and hyperbolic planes $H_1, \ldots, H_d$ such that one has the orthogonal decomposition

$$V \simeq \left(\bigoplus_{1 \leqslant i \leqslant d} H_i \right) \oplus W$$

where W is a subspace that does not contain any nonzero isotropic vector.

Moreover, the dimension of any maximal isotropic space is equal to d.

Proof. See for instance [Art11, Theorem 3.11]. □

When F is a finite field, more can be said. For simplicity, we assume that $\dim V = 2s$. If $\sigma \neq \mathrm{id}$, the Witt index of V is always s. On the contrary, when $\sigma = \mathrm{id}$, it can be either s or $s-1$. But we can decide between those two values by

looking at the discriminant Δ_V of V (defined as the determinant of the matrix of $\mathcal{B}$ in some basis); precisely, the Witt index is s if and only if $(-1)^s\Delta_V$ is a square in $F^\times$. (See [Sch85, Theorem 3.3] for more details.)

In our case, Theorem 2.19 tells us that we are looking for isotropic subspaces of dimension s in $\mathbf{K}_l$; we recall from Equation (2.3) that the latter is endowed with the sesquilinear form

$$(\kappa, \rho)_{\mathbf{F}_l} = \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l \cdot \kappa \cdot \sigma_{\tau(l)}(\rho))$$

where $\sigma_{\tau(l)} : \mathbf{K}_{\tau(l)} \to \mathbf{K}_l$ is the map induced by $\sigma_{\tau(l)}(Y) = \frac{1}{Y}$ and ζ_l is an element of $\mathbf{K}_l$ defined in Lemma 2.13. We then need to compute the discriminant Δ_{ζ_l} of this sesquilinear form.

Lemma 2.21 We assume that $\sigma_l = \mathrm{id}$ and we let $\Delta_{\mathbf{K}_l/\mathbf{F}_l}$ be the discriminant of the extension $\mathbf{K}_l/\mathbf{F}_l$ (which is, by definition, the discriminant of the bilinear form $(\kappa, \rho) \mapsto \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\kappa\rho)$). Then

1. the discriminant Δ_{ζ_l} is equal to $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l) \cdot \Delta_{\mathbf{K}_l/\mathbf{F}_l}$,
2. the discriminant $\Delta_{\mathbf{K}_l/\mathbf{F}_l}$ is a square in $\mathbf{F}_l$ if and only if the degree of the extension $[\mathbf{F}_l : \mathbf{F}]$ is even,
3. if $y_l = 1$ (resp. $y_l = -1$), $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)$ is a square (resp. is not a square) in $\mathbf{F}_l$.

Proof. 1. We fix a basis of $\mathbf{K}_l$ over $\mathbf{F}_l$ and write $\mathrm{Mat}(\zeta_l)$ for the matrix representing the multiplication by ζ_l in this basis. Then $\Delta_{\zeta_l} = \det\left(\mathrm{Mat}(\zeta_l)^{\mathsf{tr}}\right) \cdot \Delta_{\mathbf{K}_l/\mathbf{F}_l} = \mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l) \cdot \Delta_{\mathbf{K}_l/\mathbf{F}_l}$.

2. From $\mathbf{K}_l = \mathbf{K} \otimes_{\mathbf{F}} \mathbf{F}_l$, we deduce that $\Delta_{\mathbf{K}_l/\mathbf{F}_l} = \Delta_{\mathbf{K}/\mathbf{F}} \in \mathbf{F}$. Moreover, we know that $\Delta_{\mathbf{K}/\mathbf{F}}$ is a square in $\mathbf{F}$ if and only if the Galois group of $\mathbf{K}/\mathbf{F}$ is a subgroup of the alternating group (see [Mil20, Corollary 4.2]), which never occurs in our situation given that $\mathrm{Gal}(\mathbf{K}/\mathbf{F})$ is a cyclic group of even cardinality. We conclude that $\Delta_{\mathbf{K}/\mathbf{F}}$ is a square in $\mathbf{F}_l$ if and only if the extension $\mathbf{F}_l/\mathbf{F}$ has even degree.

3. We assume that $y_l = \pm 1$ and compute

$$\begin{aligned}\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)^{\frac{q-1}{2}} &= \left(\zeta_l^{\sum_{0\leqslant i<2s} q^i}\right)^{\frac{q-1}{2}} \\ &= \left(\zeta_l^{q-1}\right)^{\frac{\sum_{0\leqslant i<2s} q^i}{2}} = \left(x_l\sigma_l(x_l)\right)^{\frac{\sum_{0\leqslant i<2s} q^i}{2}}\end{aligned}$$

As $y_l = \pm 1$, the automorphism σ_l is the identity and so $\mathrm{Norm}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta_l)^{\frac{q-1}{2}} = y_l$. We conclude by applying Euler's criterion. □

Corollary 2.22 We assume that the characteristic of $\mathbf{F}$ is odd.

1. If k is even, there are no self-dual skew cyclic codes in $\mathbf{E}_k$.

2. If k is odd, there exist self-dual skew cyclic codes in $\mathbf{E}_k$ if and only if $(-1)^s$ is not a square in $\mathbf{F}$, if and only if s is odd and $q \equiv 3 \pmod 4$.

Proof. We first notice that, whenever $y_l \neq \pm 1$, there is no obstruction to the existence of an isotropic subspace of half dimension. On the contrary, when $y_l = 1$ (resp. $y_l = -1$), it follows from Lemma 2.21 that an isotropic subspace of $\mathbf{K}$ of dimension s exists if and only if $(-1)^s$ is not a square (resp. is a square) in $\mathbf{F}$.

When k is even, the decomposition of $\mathbf{E}_k$ exhibits both factors $\mathbf{K}[X;\theta]/(X^r+1)$ and $\mathbf{K}[X;\theta]/(X^r-1)$. Since $(-1)^s$ cannot be simultaneously a square and a non-square, we conclude that self-dual skew cyclic codes cannot exist in this case. On the contrary, when k is odd, the factor $\mathbf{K}[X;\theta]/(X^r+1)$ does not show up and we are left to the condition corresponding to $y_l = 1$.

Finally, the fact that $(-1)^s$ is not a square in $\mathbf{F}$ if and only if s is odd and $q \equiv 3 \pmod 4$ is a direct application of Euler's criterion. □

2.4.2 Counting self-dual skew cyclic codes

We now aim at counting the number of self-dual codes sitting in $\mathbf{E}_k$, when they exist. In what follows, we then assume that the existence criterion of Corollary 2.22 is fulfilled. It follows from Theorem 2.19 that our task reduces to finding the cardinality of $W_{\mathtt{pal}}$ and $W_{\mathtt{nonpal}}$.

The non-palindromic case

We start by the non-palindromic case, which is by far the easiest. For this counting, we will use q-analogues of integers. We recall briefly that the q-analogue of $n \in \mathbf{N}$ is, by definition, $[n]_q := 1 + q + q^2 + \cdots + q^{n-1}$. The q-factorial of n is defined by $[n]_q! = [1]_q[2]_q \dots [n]_q$ and we set

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{[n]_q!}{[k]_q!\,[n-k]_q!} = \frac{(1-q^n)(1-q^{n-1})\dots(1-q^{n-k+1})}{(1-q)(1-q^2)\dots(1-q^k)}$$

where n and k are non-negative integers with $k \leqslant n$. It is a classical fact that the q-binomial coefficients count the number of $\mathbb{F}_q$-vector subspaces of dimension k in the ambient $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$.

Therefore, with the notation of Theorem 2.19, we have

$$\mathrm{Card}(W_{\mathtt{nonpal}}) = \prod_{\{l,\tau(l)\}\in J} \left(\sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix}_{q_l} \right). \tag{2.5}$$

The palindromic case

If V is a finite-dimensional vector space equipped with a sesquilinear form, we denote by $\textsc{Iso}(V)$ the number of isotropic subspaces of V of half dimension. It turns out that

the behavior of $\mathrm{Iso}(V)$ has been studied for a long time (see for instance [Seg59, Ple65, BBB20]) and that explicit formulas are known. Those are called Segre's formulas and are recalled in the following theorem.

Theorem 2.23 Let F be a finite field of odd characteristic and cardinality q_F and let $\sigma : F \to F$ be an involutive ring automorphism. Let V be an F-vector space of dimension $2s$ equipped with a non-degenerate σ-sesquilinear form, whose Witt index is s. Then:

1. if $\sigma = \mathrm{id}$ (Euclidean case), then $\mathrm{Iso}(V) = \prod_{i=0}^{s-1} (q_F^i + 1)$,
2. if $\sigma \neq \mathrm{id}$ (Hermitian case), then $\mathrm{Iso}(V) = \prod_{i=0}^{s-1} \left(q_F^{i+1/2} + 1\right)$.

Proof. We recall briefly the idea of the proof as it will be useful afterward. Let $\mathrm{iso}(W)$ be the number of isotropic vectors in a Euclidean or Hermitian vector space W over F. We claim that, if W has dimension $2d$ and Witt index d, then

1. if $\sigma = \mathrm{id}$ (Euclidean case), then $\mathrm{iso}(W) = (q_F^d - 1)(q_F^{d-1} + 1)$,
2. if $\sigma \neq \mathrm{id}$ (Hermitian case), then $\mathrm{iso}(W) = (q_F^d - 1)(q_F^{d-1/2} + 1)$

Indeed, let us fix an isotropic basis $((u_i)_{0\leqslant i<s}, (v_i)_{0\leqslant i<s})$ corresponding to the Witt's decomposition of W (see Theorem 2.20) and let $((a_i)_{0\leqslant i<s}, (b_i)_{0\leqslant i<s})$ be the coordinates in this basis of a vector. In the Euclidean case, the fact that this vector is isotropic reduces to the equation $\sum_{0\leqslant i<s} a_i b_i = 0$. Now, fixing a nonzero vector $(a_i)_{0\leqslant i<s}$ of $\mathbf{F}_l^s$, this occurs if and only if $(b_i)_{0\leqslant i<s}$ lies in some hyperplane. We thus have $(q_F^s - 1)q_F^{s-1}$ solutions corresponding to nonzero $(a_i)_{0\leqslant i<s}$, to which one should add $(q_F^s - 1)$ more solutions when all a_i vanish. Finally, we get $\mathrm{iso}(W) = (q_F^d - 1)(q_F^{d-1} + 1)$ as claimed.

The Hermitian case is similar, except that the equation to solve is now $\sum_{0\leqslant i<s} \sigma_l(a_i)b_i + \sum a_i\sigma_l(b_i) = 0$, which reduces to $\sum_{0\leqslant i<s} a_i\sigma_l(b_i) = \alpha$ where α satisfies $\sigma_l(\alpha) = -\alpha$. We conclude repeating the argument of the Euclidean case and using that there are exactly $q_F^{1/2}$ values for α.

We are now ready to prove Segre's formula. We start by taking $W_1 = V$ and by picking an isotropic vector u_1 in W. This corresponds to $\mathrm{iso}(W_1)$ possibilities. Once this is achieved, we set $W_2 := (Fu_1)^\perp/Fu_1$. This is a space of dimension $2(s-1)$, whose Witt index is $s-1$. Therefore, we can apply again our claim and find that there are exactly $\mathrm{iso}(W_2)$ isotropic vectors in W_2. We choose one of them, that we denote by u_2. Now we repeat the argument until we reach u_s. This corresponds to $\mathrm{iso}(W_1)\cdot\mathrm{iso}(W_2)\cdots\mathrm{iso}(W_s)$ choices. However, each of them corresponds $q_F \cdot q_F^2 \cdots q_F^{s-1} = q_F^{s(s-1)/2}$ choices of families of vectors of V since u_i has q^i preimages in V. We conclude that the number of bases of a maximal isotropic subspace of V is equal to $q_F^{s(s-1)/2} \cdot \mathrm{iso}(W_1) \cdot \mathrm{iso}(W_2) \cdots \mathrm{iso}(W_s)$. We finally obtain $\mathrm{Iso}(V)$ by dividing by the cardinality of $\mathrm{GL}_s(F)$. □

Remark 2.24 In the Euclidean case, one can alternatively prove Segre's formula by remarking that the orthogonal group of V acts transitively on the set of maximal isotropic subspaces and that the stabilizer of a given maximal isotropic subspace U can be presented as a semi-direct product of $\mathrm{GL}(U)$ and the group of antisymmetric linear applications from U to its dual $\mathrm{Hom}_F(U, F)$. From this description we find that the number of maximal isotropic subspaces is

$$\frac{\mathrm{Card}\big(O_{2s}(F)\big)}{q_F^{s(s-1)/2} \cdot \mathrm{Card}\big(\,\mathrm{GL}_s(F)\big)}$$

a formula from which one can eventually derive Segre's theorem. A similar approach also works in the Hermitian case.

Keeping the notation of Theorem 2.19, it follows from Theorem 2.23 that

$$\mathrm{Card}(W_{\mathtt{pal}}) = \prod_{\substack{l\in I\\ y_l=\pm 1}} \prod_{i=0}^{s-1} \left(q_l^i + 1\right) \times \prod_{\substack{l\in I\\ y_l\neq\pm 1}} \prod_{i=0}^{s-1} \left(q_l^{i+1/2} + 1\right). \tag{2.6}$$

We notice moreover that there is always exactly one index l for which $y_l = 1$, and there is at most one index l such that $y_l = -1$ (such an index actually exists if and only if k is even). In both cases, the corresponding field $\mathbf{F}_l$ is $\mathbf{F}$, and so $q_l = q$.

Now combining Equations (2.5) and (2.6), we get the number of self-dual skew cyclic codes sitting in $\mathbf{E}_k$, which proves Theorem 2.2.

Example 2.25 For $\mathbf{K} = \mathbb{F}_{q^{2s}}$ and $\theta : x \mapsto x^q$, the number of self-dual skew cyclic codes is equivalent to $q^{\frac{s(s-1)}{2}}$ as s grows to infinity, whereas the number of skew cyclic codes (number of s-dimensional $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^{2s}}$) is equivalent to q^{s^2} as s grows to infinity.

For example, for $\mathbf{K} = \mathbb{F}_{3^6}$ and $\theta : x \mapsto x^3$, the number of self-dual skew cyclic codes in $\mathbf{E}_1 = \mathbf{K}[X;\theta]/(X^6 - 1)$ is 80 among 33880 skew cyclic codes of dimension 3, whereas for $\mathbf{K} = \mathbb{F}_{3^{18}}$ and $\theta : x \mapsto x^3$, the number of self-dual skew cyclic codes in $\mathbf{E}_1 = \mathbf{K}[X;\theta]/(X^{18} - 1)$ is 469740602936729600 among 791614563787525746761491781638123230424 skew cyclic codes of dimension 9.

Remark 2.26 As we noticed at the end of subsection 2.3.1, there exist no self-dual skew cyclic codes at all in the case r odd. This is in particular the case for $r = 1$, when skew cyclic codes reduce to cyclic codes. On the contrary, for $s = 1$ and $q = 3$, we achieve the best ratio of self-dual skew cyclic codes over skew cyclic codes, which is $\frac{1}{2}$. Nevertheless, the proportion of self-dual skew cyclic codes over skew cyclic codes decreases as fast as $\mathcal{O}(q^{-\frac{s^2+s}{2}})$ as s grows larger.

2.4.3 Random generation of self-dual skew cyclic codes

Since the number of self-dual skew cyclic codes grows exponentially fast with respect to the dimension r, an algorithm outputting in one shot the complete list of these codes would be necessarily very inefficient (the best we can expect is exponential complexity) and hence, probably not quite useful. Instead, in what follows, we address a different question, which is that of random generation: we aim at finding a fast algorithm that outputs a unique code in this huge list with the guarantee that the returned code is *uniformly distributed* among all of them. Such an algorithm could be very useful to generate *typical* self-dual skew cyclic codes and to check their properties.

From skew cyclic codes to finite geometry: explicit methods

Before designing our algorithms, we need to explain how we represent the objects on the computer. We recall that a skew cyclic code is, by definition, a left ideal of $\mathbf{E}_k = \mathbf{K}[X;\theta]/(X^{kr}-1)$. Hence, it necessarily has the form $\mathbf{E}_k f$ for some $f \in \mathbf{K}[X;\theta]$. We can further normalize this generator by requiring that it is monic and has minimal degree; concretely, normalizing the generator f amounts to replacing it by $\mathrm{rgcd}(f, X^{kr}-1)$ (where rgcd denotes the right gcd). The same discussion applies similarly to all quotients of an Ore polynomial ring by a two-sided ideal and so, in particular, to $\mathbf{K}[X;\theta]/P_l(Y)$ and the algebras $\tilde{\mathbf{E}}_k^{(l)} = \mathbf{K}_l[X;\theta]/(X^r - y_l)$.

We recall further that we have the following sequence of isomorphisms:

$$\mathbf{E}_k \simeq \prod_{l=1}^{n} \mathbf{K}[X;\theta]/P_l(Y) \simeq \prod_{l=1}^{n} \tilde{\mathbf{E}}_k^{(l)} \simeq \prod_{l=1}^{n} \mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$$

and that the left ideals of $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ are in one-to-one correspondence with the $\mathbf{F}_l$-linear subspaces of $\mathbf{K}_l$ (see Subsection 2.3.4). We aim at making explicit all these identifications.

Going back and forth between $\mathbf{E}_k$ and $\prod_{l=1}^{n} \tilde{\mathbf{E}}_k$ is not difficult. Indeed, if a code sitting in $\mathbf{E}_k$ is generated by f, its image in $\mathbf{E}_k$ will be generated by f as well. Conversely, if one starts with a family of codes $\left(\tilde{\mathbf{E}}_k^{(l)} f_l\right)_{1 \leqslant l \leqslant n}$, its preimage in $\mathbf{E}_k$ is the code generated by an Ore polynomial f satisfying the set of congruences

$$f \equiv f_l \pmod{P_l(Y)} \qquad (1 \leqslant l \leqslant n). \tag{2.7}$$

We need to be careful however that f_l has *a priori* coefficients in $\mathbf{K}_l$; in order to view it as an Ore polynomial in $\mathbf{K}[X;\theta]$, we have to replace each occurrence of y_l by $Y = X^r$. The system of congruences (2.7) can then be solved using the Chinese Remainder Theorem; we underline that non-commutativity is not an issue here because all the moduli $P_l(Y)$ lie in the center. We also stress that the solution f to (2.7) is in general

not normalized, even if the f_l are; if one wants to normalize it, one needs to compute an additional rgcd.

We now explain how to navigate between $\tilde{\mathbf{E}}_k^{(l)}$ and $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$. We first recall that the isomorphism between those two rings is given by $X \mapsto x_i\theta$. Hence, the ideal of $\mathrm{End}_{\mathbf{F}_l}(\mathbf{K}_l)$ that corresponds to the ideal $\tilde{\mathbf{E}}_k^{(l)} f$ of $\tilde{\mathbf{E}}_k^{(l)}$ is the ideal consisting of linear maps vanishing on the kernel of $f(x_i\theta)$. The associated $\mathbf{F}_l$-linear subspace of $\mathbf{K}_l$ is then just $\ker f(x_l\theta)$. The correspondence in the other direction is also given by an explicit formula: if V is a $\mathbf{F}_l$-sub-vector space of $\mathbf{K}_l$ and $(v_1, \dots, v_d)$ is a basis of V, a generator of the ideal of $\tilde{\mathbf{E}}_k^{(l)}$ corresponding to V is

$$\mathrm{llcm}\left(X - \frac{x_l\theta(v_1)}{v_1}, \dots, X - \frac{x_l\theta(v_d)}{v_d}\right)$$

where llcm denotes the left lcm.

The discussion of this subsection is summarized by Algorithm 1 below which computes the normalized generator of the code sitting in $\mathbf{E}_k$ that corresponds to some element of $W_{\mathtt{nonpal}} \times W_{\mathtt{pal}}$ *via* the bijection of Theorem 2.19. The next subsections are devoted to explain how to produce a random element in (each component of) $W_{\mathtt{nonpal}} \times W_{\mathtt{pal}}$.

Algorithm 1: Explicit bijection with $W_{\mathtt{nonpal}} \times W_{\mathtt{pal}}$

Input: a family $\big((V_l)_{l\in I}, (V_l)_{\{l,\tau(l)\}\in J}\big) \in W_{\mathtt{nonpal}} \times W_{\mathtt{pal}}$
Output: the normalized generator of the corresponding self-dual skew cyclic code

1: **for** $l \in I$ **:**
2: pick a basis $(v_1, \dots, v_s)$ of V_l
3: $f_l \leftarrow \mathrm{llcm}\big(X - x_l\theta(v_i)/v_i,\ 1 \leqslant i \leqslant s\big)$
4: do the substitution $y_l \to X^r$ in f_l `//now` $f_l \in \mathbf{K}[X;\theta]$
5: $f_l \leftarrow \mathrm{rgcd}(f_l, P_l(Y))$
6: **for** $\{l, \tau(l)\} \in J$ **:**
7: pick a basis $(v_1, \dots, v_d)$ of V_l
8: $f_l \leftarrow \mathrm{llcm}\big(X - x_l\theta(v_i)/v_i,\ 1 \leqslant i \leqslant d\big)$
9: do the substitution $y_l \to X^r$ in f_l `//now` $f_l \in \mathbf{K}[X;\theta]$
10: $f_l \leftarrow \mathrm{rgcd}(f_l, P_l(Y))$
11: define $f_{\tau(l)}$ by the equality $f_l f^*_{\tau(l)} = P_l(Y)$
12: $f_{\tau(l)} \leftarrow \mathrm{rgcd}(f_{\tau(l)}, P_{\tau(l)}(Y))$
13: compute f such that $f \equiv f_l \pmod{P_l(Y)}$ for $1 \leqslant l \leqslant n$
14: **return** $\mathrm{rgcd}(f, X^{rk} - 1)$

To conclude, we record the following proposition which elucidates how duality acts on our representations.

Proposition 2.27 We set $E = E' = \mathbf{E}_k$ and $P = Y^k - 1$ (resp. $E = \mathbf{E}_k^{(l)}$, $E' = \mathbf{E}_k^{(\tau(l))}$ and $P = P_l$).

(a) Given $f, g \in K[X;\theta]$, the ideals Ef and $E'g$ are orthogonal if and only if $fg^* = 0$ in E.

(b) Given $f \in K[X,\theta]$ dividing P, the orthogonal space of Ef is the ideal $E'g^*$ where g is defined by $fg = P$.

Proof. (a) By non-degeneracy of sesquilinear form $\langle -,- \rangle$, the condition $fg^* = 0$ is equivalent to $gf^* = 0$ and then to $\langle E, gf^* \rangle = 0$. By adjunction relation, the condition becomes $\langle Ef, g \rangle = 0$. Since the adjunction is an isomorphism, the condition is further equivalent to $\langle (E')^* Ef, g \rangle = 0$ and finally to $\langle Ef, E'g \rangle = 0$.

(b) By what precedes, the ideals Ef and $E'g^*$ are orthogonal. We conclude by noticing that $\dim Ef + \dim E'g^* = (\deg P - \deg f) + (\deg P - \deg g) = \deg P$. □

Remark 2.28 As a corollary, Proposition 2.27 provides a simple criterion to check that the code $\mathbf{E}_k f$ is self-dual: assuming that f is normalized, it is the case if and only if $ff^* = 0$ in $\mathbf{E}_k$ and $\deg f = sk = rk/2$.

The non-palindromic case

We first consider the indices l such that $\tau(l) \neq l$. At those places, we simply need to generate a uniformly distributed random $\mathbf{F}_l$-subspace of $\mathbf{K}_l$. We proceed as follows. We first construct the dimension: we sample an integer $d \in \{0, \dots, r\}$ with distribution given by:

$$\text{Prob}[d = i] \quad \text{proportional to} \quad \begin{bmatrix} r \\ i \end{bmatrix}_{q_l}.$$

Once this is achieved, we sample d random elements in $\mathbf{K}_l$ with uniform distribution. If they are linearly independent over $\mathbf{F}_l$, we output the vector space they generate. Otherwise, we throw them and start again with d new elements. The probability of success is

$$\left(1 - \frac{1}{q_l^r}\right)\left(1 - \frac{1}{q_l^{r-1}}\right) \cdots \left(1 - \frac{1}{q_l^{r-d+1}}\right) \geqslant 1 - \left(\frac{1}{q_l^r} + \cdots + \frac{1}{q_l^{r-d+1}}\right) \geqslant 1 - \frac{1}{q_l - 1},$$

proving that, on average, we will need to repeat our process only $O(1)$ times.

Up to a multiplicative constant, the mean complexity of the algorithm is then equal to the complexity of checking linear independence of d vectors in a space of dimension r, which is within $O(r^3)$ by Gaussian elimination.

The Hermitian case

We now move to the Hermitian case, *i.e.,* we assume that $\tau(l) = l$ and $y_l \neq \pm 1$. We thus want to design an algorithm outputting a uniformly distributed random isotropic $\mathbf{F}_l$-subspace of $\mathbf{K}_l$ endowed with the Hermitian pairing $(-,-)_{\mathbf{K}_l}$ defined in (2.3), assuming that the existence criterion of Corollary 2.22 is fulfilled. Our construction is

inspired by the proof of Theorem 2.23, except that we will not work with the quotient $(Fu_1)^\perp/(Fu_1)$ but, instead, will embed u_1 in a hyperbolic plane H_1 and work with $H_1^\perp$.

We consider a finite field F of cardinality q_F equipped with a nontrivial involutive automorphism $\sigma : F \to F$. We also consider a Hermitian space V of dimension r and denote by $\langle -, - \rangle$ the bilinear form on it. We assume that V has Witt index s (*i.e.,* that V is isomorphic to the orthogonal direct sum of s hyperbolic planes) and aim at sampling a random isotropic subspace of V of dimension s.

For $u, v \in V$, we consider the following equation in λ:

$$(\mathcal{E}_{u,v}) : \quad \langle u + \lambda v, u + \lambda v \rangle = 0.$$

We briefly recall its resolution. If $\langle v, v \rangle = 0$, the equation reduces to $\mathrm{Trace}_{F/F^\sigma}(\lambda \cdot \langle v, u \rangle) = -\langle u, u \rangle$ which, by surjectivity of the trace, can be solved as soon as $\langle v, u \rangle \neq 0$.

On the contrary, when $\langle v, v \rangle \neq 0$, we consider the *discriminant* of $(\mathcal{E}_{u,v})$ defined by $\Delta := \langle u, v \rangle \cdot \langle v, u \rangle - \langle u, u \rangle \cdot \langle v, v \rangle$. One readily checks that Δ is invariant under σ and that the equation $(\mathcal{E}_{u,v})$ can be rewritten $\mathrm{Norm}_{F/F^\sigma}(\langle u, v \rangle + \lambda \cdot \langle v, v \rangle) = \Delta$. The solutions of $(\mathcal{E}_{u,v})$ are then the elements of the form

$$\lambda = \frac{\delta - \langle u, v \rangle}{\langle v, v \rangle}$$

where δ is a preimage of Δ by the norm map. Since the latter is surjective (because we are working over finite fields), a solution always exists.

We are now ready to present Algorithm 2: it computes a basis $(u_1, \ldots, u_s, v_1, \ldots, v_s)$ of V such that each pair (u_i, v_i) is hyperbolic and, writing $H_i \subset V$ for the hyperbolic plane they generate, we have the orthogonal decomposition $V = \bigoplus_{i=1}^s H_i$.

Proposition 2.29 Algorithm 2 is correct.

Proof. It follows from the construction that, after the first successful iteration of the loop, (u, v) is a hyperbolic pair in V. Indeed, we notice that the subspace H_1 generated by u and v does not change throughout the loop, and so it is still a plane at the end. Moreover, each update successively ensures that $\langle u, u \rangle = 0$, then $\langle v, v \rangle = 0$ and finally $\langle u, v \rangle = 1$. We observe that $\langle v, u \rangle$ does not vanish on line 10 because the substitution of line 9 leaves it unchanged. After this, we update W so that we continue to work in the orthogonal complement of H_1 which has dimension $2(s-1)$ and Witt index $s-1$ thanks to Witt's cancellation theorem. This completes the induction. □

Lemma 2.30 The tests of lines 4 and 7 are successful if and only if the vectors u, v picked on line 3 span a hyperbolic plane of $W^\perp$ and v is not isotropic.

Moreover, this happens with probability at least $\frac{\sqrt{q_F}-1}{\sqrt{q_F}+1} \cdot \frac{q_F-1}{q_F} \geqslant \frac{4}{9}$.

Algorithm 2: Decomposition as a direct sum of hyperbolic planes (Hermitian case)

Input: V: the ambient Hermitian vector space
Output: $\mathbf{u}, \mathbf{v}$: a basis of hyperbolic pairs

1: $\mathbf{u}, \mathbf{v}, W \leftarrow [\,], [\,], 0$
2: **while** $W \neq V$ **:**
3: $\quad u, v \leftarrow$ two random vectors in $W^\perp$
4: $\quad$ **if** (u, v) are linearly independent and $\langle v, v\rangle \neq 0$ **:**
5: $\quad\quad \lambda \leftarrow$ a random solution of the equation $(\mathcal{E}_{u,v})$
6: $\quad\quad u \leftarrow u + \lambda v$ `//now` $\langle u, u\rangle = 0$
7: $\quad\quad$ **if** $\langle u, v\rangle \neq 0$ **:**
8: $\quad\quad\quad \lambda \leftarrow$ a solution of the equation $(\mathcal{E}_{v,u})$
9: $\quad\quad\quad v \leftarrow v + \lambda u$ `//now` $\langle v, v\rangle = 0$
10: $\quad\quad\quad v \leftarrow v/\langle v, u\rangle$ `//now` (u, v) `is a hyperbolic pair`
11: $\quad\quad\quad \mathbf{u} \leftarrow \mathbf{u} + [u]$, $\mathbf{v} \leftarrow \mathbf{v} + [v]$
12: $\quad\quad\quad W \leftarrow W + Fu + Fv$
13: **return** $\mathbf{u}, \mathbf{v}$

Proof. It is clear that if u and v pass all tests, then they span a hyperbolic plane and that v is non-isotropic. Conversely, we need to prove if $H \subset W^\perp$ is a hyperbolic plane and u, v span H with $\langle v, v\rangle \neq 0$, then all tests pass. It is obvious for the test of line 4. If, on line 7, we had $\langle u, v\rangle = 0$, then u would be orthogonal to both u and v, implying that the Hermitian form would be degenerate on H. This is a contradiction.

We now count the number of hyperbolic planes in $W^\perp$. For this, we write $\dim_F W^\perp = 2d$ and we consider the map

$$\begin{array}{rccl} \mathcal{S}: & \left\{ \begin{array}{c}\text{pair of non-orthogonal}\\ \text{isotropic vectors in } W^\perp\end{array} \right\} & \longrightarrow & \left\{ \text{hyperbolic planes} \subset W^\perp \right\} \\ & (x, y) & \mapsto & Fx + Fy. \end{array}$$

The cardinality of the domain of $\mathcal{S}$ is $\mathrm{iso}(W^\perp) \cdot \mathrm{iso}^\star(W^\perp)$ where $\mathrm{iso}(W^\perp)$ denotes the number of isotropic vectors in $W^\perp$ (as in the proof of Theorem 2.23) and $\mathrm{iso}^\star(W^\perp)$ is the number of isotropic vectors in $W^\perp$ which are non-orthogonal to a given one. By the proof of Theorem 2.23, we know that $\mathrm{iso}(W^\perp) = (q_F^d - 1)(q_F^{d-1/2} + 1)$. The computation of $\mathrm{iso}^\star(W^\perp)$ can be handled similarly: reusing the notation of the proof of Theorem 2.23, it corresponds to count the tuples $((a_i)_{1\leqslant i\leqslant d}, (b_i)_{1\leqslant i\leqslant d}, \alpha)$ with $\sum_{i=1}^d a_i\sigma(b_i) = \alpha = -\sigma(\alpha)$ and $b_1 \neq 0$. There are then $\sqrt{q_F}$ choices for α, $(q_F - 1)q_F^{d-1}$ choices for the b_i and when all those are fixed, there remains q_F^{d-1} choices for the a_i. Therefore, $\mathrm{iso}^\star(W^\perp) = (q_F - 1)q_F^{2d-\frac{3}{2}}$ and we finally obtain:

$$\mathrm{Card}(\text{domain of } \mathcal{S}) = (q_F^d - 1) \cdot (q_F - 1) \cdot (q_F^{3d-2} + q_F^{2d-\frac{3}{2}}).$$

Similarly, given a hyperbolic plane $H \subset W^\perp$, we have:

$$\mathrm{Card}(\mathcal{S}^{-1}(H)) = \mathrm{iso}(H) \cdot \mathrm{iso}^\star(H) = (q_F - 1)^2 \cdot (q_F + \sqrt{q_F}).$$

We conclude that the number of hyperbolic planes in $W^\perp$ is

$$A = \frac{(q_F^d - 1) \cdot (q_F^{3d-2} + q_F^{2d-\frac{3}{2}})}{(q_F - 1) \cdot (q_F + \sqrt{q_F})}.$$

Now, once a hyperbolic plane H is fixed, the number of possibilities for v is

$$B = (q_F^2 - 1) - (1 + \sqrt{q_F})(q_F - 1) = (q_F - 1)(q_F - \sqrt{q_F})$$

while the number of options for u is $C = q_F^2 - q_F$. Finally, the probability we are looking for is $\frac{ABC}{q_F^{4d}}$ and calculus shows that it is always greater than $\frac{\sqrt{q_F}-1}{\sqrt{q_F}+1} \cdot \frac{q_F-1}{q_F}$ (which is the limit when d goes to infinity). The fact that the latter is bounded from below by $\frac{4}{9}$ follows from the observation that q_F is necessarily at least 9 because F has odd characteristic and admits a sub-field of index 2. □

Proposition 2.31 Algorithm 2 terminates almost surely and its average complexity is $O(r^3)$ operations in F^σ and $O(r)$ computations of inner products.

Proof. Termination follows directly for Lemma 2.30. Regarding complexity, we claim that each successful iteration of the loop costs at most $O(r^2)$ operations in F^σ and $O(1)$ computations of inner products. To achieve this, we first observe that solving the equation $(\mathcal{E}_{u,v})$ amounts to computing the attached discriminant (which corresponds to computing 4 inner products) and finding a uniformly distributed preimage of the discriminant by the norm map; the latter can be done using the algorithms of [CB17] for a constant cost. Similarly, solving $(\mathcal{E}_{v,u})$ reduces to a linear system, which can be attacked by simple linear algebra over F^σ for a constant cost again. Regarding the computation of W, we may process as follows: we maintain a matrix M in reduced row echelon form representing the subspace of $V^\star = \mathrm{Hom}_F(V, F)$ generated by the forms $\langle -, w \rangle$ with $w \in W$. At each update of W on line 11, we need to add two new lines to M and re-echelon it; this has a cost of $O(r^2)$ operations in F using standard Gaussian elimination. Moreover, knowing M, sampling u and v on line 3 amounts to finding two random solutions of the linear system $MX = 0$. Since M is already row-echeloned, this can be done for a cost of $O(r^2)$ operations in F as well. □

Finally, the link between Algorithm 2 and the question we are interested in is established in the next proposition.

Proposition 2.32 If $\mathbf{u}, \mathbf{v}$ is the output of Algorithm 2, then the space generated by $\mathbf{u}$ is a uniformly distributed random isotropic subspace of V of dimension s.

Proof. The fact that the span of $\mathbf{u}$ is an isotropic subspace of dimension s is clear. To prove that it is uniformly distributed, we notice that, after line 3, the plane $H := Fu + Fv$ is uniformly distributed among all planes in $W^\perp$. Since this plane stays unchained throughout the loop, the first part of Lemma 2.30 implies that, at the end of the loop, H is uniformly distributed among all hyperbolic planes in $W^\perp$.

We now fix a hyperbolic plane $H \subset W^\perp$, together with a non-isotropic vector $v \in H$. We claim that, when u varies in H, the vector u one obtains after the replacement of line 6 is uniformly distributed in the set $\mathcal{I}_H$ of isotropic vectors in H. In order to prove this, for $u \in H$, we define $L(u) \subset H$ as the affine line passing through u and directed by v. We also set $S(u) := L(u) \cap \mathcal{I}_H$. Clearly, for any fixed u noncollinear to v, the $L(\alpha u)$ form a partition of $H \backslash Fv$ when α varies in $F^\times$. Since v is itself non-isotropic, we conclude that

$$\mathcal{I}_H = \bigsqcup_{\alpha \in F^\times} S(\alpha u). \tag{2.8}$$

Moreover, the multiplication by α defines a bijection $S(u) \to S(\alpha u)$; hence, all the $S(\alpha u)$ have the same cardinality. Coming back now to the algorithm, we notice that the effect of lines 5 and 6 is to replace u by a uniformly distributed random vector in $S(u)$. The decomposition (2.8), combined with the fact that all $S(\alpha u)$ have the same cardinality, then implies that the vector u obtained after line 6 gets uniformly distributed in $\mathcal{I}_H$ when u varies on any given line of H that does not contain v. Since this holds for any line, our claim is proved.

Let $\mathcal{A}$ be the set of all $\big((H_1, u_1), \ldots, (H_s, u_s)\big)$ such that the H_i are pairwise orthogonal hyperbolic planes in V and, for all i, u_i is an isotropic vector in H_i. It follows for what precedes that, if $\mathbf{u} = (u_1, \ldots, v_s)$, $\mathbf{v} = (v_1, \ldots, v_s)$ is the output of Algorithm 2, the tuple $\big((H_1, u_1), \ldots, (H_s, u_s)\big)$ with $H_i := Fu_i + Fv_i$ is uniformly distributed in $\mathcal{A}$. To conclude, it is then enough to prove that all the fibers of the map

$$\begin{array}{rcl} \mathcal{A} & \longrightarrow & \mathcal{B} := \left\{ \begin{array}{c} s\text{-dimensional isotropic} \\ \text{subspaces of } V \end{array} \right\} \\ \big((H_1, u_1), \ldots, (H_s, u_s)\big) & \mapsto & Fu_1 + \cdots + Fu_s \end{array}$$

have the same cardinality. For this, we use the fact that the unitary group $\mathrm{U}(V)$ acts transitively on $\mathcal{B}$. In other words, given two s-dimensional isotropic subspaces $U, U' \subset V$, there exists a unitary transformation $f : V \to V$ such that $f(U) = U'$. Such an f induces a bijection between the fibers above U and U', then proving that the cardinalities are equal. □

Remark 2.33 Two important optimizations of Algorithm 2 need to be mentioned. Firstly, the lines 8–10 are in fact not needed if we are only interested in the span of $\mathbf{u}$ (as we are here). We kept them because computing a full hyperbolic basis can be interesting in its own right, and will be actually used afterward when we will come

to enumeration. Secondly, if the picked vector v is not isotropic on line 4, instead of giving up immediately, we may try to swap u and v and redo the test. On the one hand, this increases the probability of success and, on the other hand, one can prove that this does not affect the fact that the span of $\mathbf{u}$ is uniformly distributed at the end.

The Euclidean case

We move to the Euclidean case, *i.e.,* we consider the same setting as before, except that we now assume that σ is the identity. The equation $(\mathcal{E}_{u,v})$ continues to make sense but its resolution is a bit different. Precisely, expanding the scalar product, we find that it is equivalent to

$$\langle u, u\rangle + 2\lambda \cdot \langle u, v\rangle + \lambda^2 \cdot \langle v, v\rangle = 0.$$

If $\langle v, v\rangle = 0$, it is a linear equation that we can solve as soon as $\langle u, v\rangle \neq 0$. On the contrary, if $\langle v, v\rangle \neq 0$, it is a quadratic equation whose (reduced) discriminant is $\Delta := \langle u, v\rangle^2 - \langle u, u\rangle \cdot \langle v, v\rangle$ (this is in fact the same as before!). The equation $(\mathcal{E}_{u,v})$ has no solution when Δ is not a square, and it has one or two solutions otherwise: if $\delta^2 = \Delta$, they are given by $\lambda = \frac{\delta - \langle u,v\rangle}{\langle v,v\rangle}$.

From here, we can write down Algorithm 3 (which is a direct translation of Algorithm 2).

Algorithm 3: Direct sum decomposition of hyperbolic planes in the Euclidean case

Input: V: the ambient Euclidean vector space
Output: $\mathbf{u}, \mathbf{v}$: a basis of hyperbolic pairs

```
1:  u, v, W ← [ ], [ ], 0
2:  while W ≠ V :
3:      u, v ← two random vectors in W^⊥
4:      if (u, v) are linearly independent and ⟨v, v⟩ ≠ 0 :
5:          Δ ← ⟨u, v⟩^2 − ⟨u, u⟩ · ⟨v, v⟩
6:          if Δ is a square in F :
7:              λ ← a random solution of the equation (E_{u,v})
8:              u ← u + λv                                  //now ⟨u, u⟩ = 0
9:              if ⟨u, v⟩ ≠ 0 :
10:                 λ ← a solution of the equation (E_{v,u})
11:                 v ← v + λu                              //now ⟨v, v⟩ = 0
12:                 v ← v/⟨v, u⟩    //now (u, v) is a hyperbolic pair
13:                 u ← u + [u], v ← v + [v]
14:                 W ← W + Fu + Fv
15: return u, v
```

Proposition 2.34 Algorithm 3 is correct. It terminates almost surely and its average complexity is $O(r^3)$ operations in F and $O(r)$ computations of inner products. More-

over, if $\mathbf{u}, \mathbf{v}$ is the output of Algorithm 3, then the space generated by $\mathbf{u}$ is a uniformly distributed random isotropic subspace of V of dimension s.

Proof. It is a repetition of the proofs of Propositions 2.29, 2.31 and 2.32 (with the small difference that the probability of success in the analogue of Lemma 2.30 is now bounded from below by $\frac{(q_F-1)^2}{2q_F^2} \geqslant \frac{2}{9}$). □

2.4.4 Enumeration of self-dual skew cyclic codes

We finally address the question of enumeration. As we already said earlier, an algorithm that outputs in one shot the complete list of self-dual codes in $\mathbf{E}_k$ would only have a limited interest because the number of such codes grows exponentially with respect to r.

Instead, we will work with iterators, that are, roughly speaking, procedures that produce a new item each time they are called, without precomputing the entire list at the beginning. Concretely, we model iterators by importing the keywords **yield** and **next** from the Python syntax. When a procedure containing the keyword **yield** is called, it is not executed but instead returns an object called *iterator*, which can be understood as a pointer to the current state of execution of the procedure. Now, each time the iterator is called through the keyword **next**, the execution of the procedure continues until a statement **yield** is encountered; at that point, the execution is interrupted and the iterator outputs the attribute of the **yield** instruction.

In what follows, we assume[1] that we have at our disposal, for all integers $m \leqslant n$ and any finite field F, an iterator producing the list of all matrices in reduced row echelon form with m rows and n columns. We note that such matrices are in one-to-one correspondence with m-dimensional F-linear subspace of F^n (the subspace being the span of the rows of the matrix). Similarly, we also assume that, for any given linear system, we have at our disposal an iterator running over its solutions.

We now explain how to build iterators over each component of the product $W_{\texttt{nonpal}} \times W_{\texttt{pal}}$.

The non-palindromic case

In this case, we have to construct an iterator running over all $\mathbf{F}_l$-linear subspaces of $\mathbf{K}_l$. In order to reduce this task to a matrix enumeration, we first pick a basis of $\mathbf{K}_l$ over $\mathbf{F}_l$ (this can be done easily; for example, a basis of $\mathbf{K}$ over $\mathbf{F}$ does the job). Once this is achieved, we take an iterator that runs over all matrices over $\mathbf{F}_l$ in reduced row echelon form with r columns, which directly solves our problem.

[1] Such an iterator is available in many software, including SageMath. It is moreover easy to construct: we iterate over the subset of $I \subset \{1, \dots, n\}$ of cardinality m and, for each such I, we run over all the matrices in reduced row echelon form with pivots at positions in I.

The Euclidean case

As in Subsection 2.4.3, we work with a general r-dimensional Euclidean space V over a finite field F of cardinality q_F and assume that V has Witt index s. By the results of Subsection 2.4.3, we can further assume that we are given a hyperbolic basis of V, that is a basis $(u_1, \ldots, u_s, v_1, \ldots, v_s)$ such that $\langle u_i, v_i \rangle = 1$ and all other scalar products between elements in the basis vanish.

In order to take advantage of this basis, we will enumerate the s-dimensional subvector spaces of V in a slightly different manner. Those spaces are parameterized by the matrices M in reduced row echelon form of size $s \times (2s)$, but we shall further split M and write it as a block matrix as follows:

$$M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

Here A, B and C all have s columns and the horizontal separation is positioned is such a way that the last line of A is not identically zero. The matrices A and C are then reduced row echelon matrices of size $d \times s$ and $(s-d) \times s$ respectively (for some d). Besides, the columns of B in front of the pivots of C all vanish. Conversely, if we choose A, B and C satisfying the above conditions, the resulting block matrix M will be in reduced row echelon form. In other words, there is a bijection between the matrices M, on the one hand, and the triples (A, B, C), on the other hand; in the sequel, we will constantly rely on it to enumerate the M.

Remark 2.35 At the level of cardinalities, the above bijection leads to the (classical) formula

$$\begin{bmatrix} 2s \\ s \end{bmatrix}_{q_F} = \sum_{d=0}^{s} q_F^{d^2} \cdot \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}^2.$$

The (A, B, C)-presentation is quite interesting for our purpose because the isotropy condition translates to the equations:

$$AB^{\mathsf{tr}} + BA^{\mathsf{tr}} = 0 \tag{2.9}$$

$$AC^{\mathsf{tr}} = 0 \tag{2.10}$$

Equation (2.10) means that the row-span of A should be orthogonal to the row-span of C for the standard scalar product on F^s. Since those two spaces have complementary dimension, we conclude that $\mathrm{RowSpan}(C)$ must be the orthogonal space of $\mathrm{RowSpan}(A)$. Given that, in addition, C must also be in reduced row echelon form, we conclude that C is uniquely determined by A: it is the reduced row echelon basis of $\mathrm{RowSpan}(A)^{\perp}$.

Once C is known, one also knows its pivots and the shape of B is determined.

Equation (2.9) then appears as a linear equation on the entries of B, which can be easily solved using Gaussian elimination.

All of this leads to Algorithm 4.

Algorithm 4: Iterator over maximal isotropic spaces (Euclidean case)

```
A ← iterator over reduced row echelon matrices over F with s columns
while A ← next(A) :
    C ← reduced row echelon basis of RowSpan(A)^⊥
    B ← iterator over solutions of (2.9) with vanishing columns in front of
    pivots of C
    while B ← next(B) :
        yield ( A  B )
              ( 0  C )
```

Regarding complexity, it is clear that, in the worst case, an iteration of Algorithm 4 requires at most $O(r^6)$ operations in F since it only involves Gaussian elimination in dimension at most $O(r^2)$. However, in most cases, an iteration only consists of going from one solution B to the next one; once a basis of the space of solutions has been computed, this costs only $O(r^2)$ operations in F.

Remark 2.36 Denoting by d the number of rows of A, one can prove that the linear system (2.9) consists of $\frac{d(d+1)}{2}$ linearly independent equations. Therefore, the set of admissible B is an F-vector space of dimension $\frac{d(d-1)}{2} = \binom{d}{2}$; hence it has cardinality $q_F^{\binom{d}{2}}$. From this, we derive that the number of isotropic subspaces of V of dimension s is equal to

$$\sum_{d=0}^{s} q_F^{\binom{d}{2}} \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}.$$

Comparing with Segre's formula (see Theorem 2.23), we find the identity

$$\prod_{d=0}^{s-1}(1+q_F^d) = \sum_{d=0}^{s} q_F^{\binom{d}{2}} \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}$$

which is actually a special case of the well-known polynomial identity [PA71]:

$$\prod_{k=0}^{n-1}(1+q^k t) = \sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q t^k. \tag{2.11}$$

As a byproduct, our approach then provides a *bijective proof* of this identity when $t = 1$ and q is a power of a prime number.

The Hermitian case

We now equip F with a nontrivial involution $\sigma : F \to F$ and assume that the pairing

$\langle -, - \rangle$ on V is σ-sesquilinear. In this new situation, all the discussion of Subsection 2.4.4 applies, except that the Equations (2.9) and (2.10) have to be replaced by the following ones:

$$A\sigma(B^{\mathsf{tr}}) + B\sigma(A^{\mathsf{tr}}) = 0 \tag{2.12}$$

$$A\sigma(C^{\mathsf{tr}}) = 0 \tag{2.13}$$

As in the Euclidean case, it turns out that Equation (2.13) fully determines C; precisely C is the reduced row echelon basis of $\mathrm{RowSpan}(\sigma(A))^{\perp}$. Similarly, Equation (2.12) provides a linear system on the entries on B, but we need to be careful that it is F^{σ}-linearity and not F-linearity as before. Anyway, the system can equally be solved using Gaussian elimination.

Taking these remarks into account, we end up with Algorithm 5

Algorithm 5: Iterator over maximal isotropic spaces (Hermitian case)

```
1: A ← iterator over reduced row echelon matrices over F with s columns
2: while A ← next(A) :
3:     C ← reduced row echelon basis of RowSpan(σ(A))^⊥
4:     B ← iterator over solutions of (2.12) with vanishing columns in front of
       pivots of C
5:     while B ← next(B) :
6:         yield ( A  B )
                 ( 0  C )
```

Remark 2.37 Similarly to the Euclidean case, our approach gives a bijective proof of the numerical identity

$$\prod_{d=0}^{s-1}(1 + q_F^{d+1/2}) = \sum_{d=0}^{s} q_F^{d^2/2} \begin{bmatrix} s \\ d \end{bmatrix}_{q_F}$$

which is Equation (2.11) evaluated at $q = q_F$ and $t = \sqrt{q}$.

2.5 Enumeration in the purely inseparable case

We now address the case where k is not coprime to the characteristic p. We aim at finding an enumeration algorithm of self-dual skew cyclic codes in this case too. If k decomposes as $k'p^m$ with k' coprime with p, it follows easily from the chinese remainder

isomorphism

$$\begin{aligned}\mathbf{E}_k &\simeq \mathbf{K}[Y,X;\theta]/(Y^{k'}-1, X^{rp^m}-Y)\\ &\simeq (\mathbf{K}[Y,X;\theta]/(Y^{k'}-1))/(X^r - Y^{\frac{1}{p^m}})^{p^m}\\ &\simeq \left(\mathbf{K}[Y,X;\theta]/\prod_{1\leqslant l\leqslant n} P_l(Y)\right)/(X^r - Y^{\frac{1}{p^m}})^{p^m}\\ &\simeq \prod_{1\leqslant l\leqslant n} \left(\mathbf{K}[Y,X;\theta]/P_l(Y)\right)/(X^r - Y^{\frac{1}{p^m}})^{p^m}\end{aligned}$$

that we can recover an enumeration algorithm for any k by combining the separable case and the case where $k = p^m$ (purely inseparable case).

Enumeration of purely inseparable self-dual skew cyclic codes

In order to solve the purely inseparable case, we follow a factorization approach, inspired by but slightly different from that of article [BU14]. We introduce twisted skew separable codes $\mathbf{E}_{k,l}^{(\xi X^t)}$, that are slight generalizations of previously considered skew separable codes. They are defined as skew separable codes of $\mathbf{E}_k^{(l)}$ corresponding to the usual adjunction on $\mathbf{E}_k^{(l)}$ composed with the conjugation by ξX^t for $\xi \in \mathbf{K}_l$ and $t \in \{0, s\}$. We will then obtain all inseparable self-dual codes as products of twisted skew separable self-dual codes.

Definition 2.38 We fix parameters $t \in \{0, s\}$, $\xi \in \mathbf{K}_l$. We denote by $\mathbf{E}_{k,l}^{(\xi X^t)}$, the space $\mathbf{E}_k^{(l)}$ equipped with the ξX^t-twisted bilinear form $(\kappa, \rho) = \mathrm{Trace}_{\mathbf{K}_l/\mathbf{F}_l}(\zeta.\xi\kappa\theta^t(\sigma_l(\rho)))$.

The corresponding *adjunction* is $f^{\bullet_{X^t\xi^{-1}}} = X^t\xi^{-1}\zeta^{-1}\sum_i X^{-i}\sigma_l(f_i)\zeta\xi X^{-t}$; we have

$$(\kappa, f(\rho))_{\mathbf{F}_l}^{(\xi X^t)} = (f^{\bullet_{X^t\xi^{-1}}}(\kappa), \rho)_{\mathbf{F}_l}^{(\xi X^t)}.$$

In the sequel, we will take $\sigma_l(\xi) = \xi$, and if $t = s$ $\theta^t(\xi) = -\xi$, so that the ξX^t-twisted bilinear form enjoys the following symmetries:

- it is Euclidean if $y_l = \pm 1$ and $t = 0$,
- it is Hermitian if $y_l \neq \pm 1$ and $t = 0$,
- it is skew-Euclidean if $y_l = \pm 1$ and $t = s$,
- it is skew-Hermitian if $y_l \neq \pm 1$ and $t = s$.

Remark 2.39 Reusing the method of Remark 2.24, we can compute the number of twisted codes when $k = 1$. For example, in the skew-Euclidean case, it is given by

$$\frac{\mathrm{Card}\big(\mathrm{Sp}_{2s}(\mathbf{F}_l)\big)}{q_l^{s(s+1)/2}\cdot \mathrm{Card}\big(\mathrm{GL}_s(\mathbf{F}_l)\big)} = \prod_{d=1}^{s}(1+q_l^d)$$

where Sp_{2s} stands for the symplectic group. We refer to [Han05] for more details.

Lemma 2.40 The set of ξ-twisted self-dual skew cyclic codes is in bijection with the set of nontwisted self-dual skew cyclic codes and their intersection is empty if $\theta^s(\xi) \neq \xi$.

Proof. We have for any monic skew polynomial f of degree s generating a self-dual code C_f of $\mathbf{E}_k^{(l)}$:

$$f\xi f^{\bullet_{\xi^{-1}}}\xi^{-1} = \frac{ff^\bullet}{X^s(X^r-1)}X^s(X^r-1) = f(0)X^s(X^r-1)$$

where $f(0)$ denotes the constant term in f. As we assume ξ to be σ_l-invariant, by Hilbert-90, we can solve the equation $\gamma\sigma_l(\gamma) = \xi$ for γ in ${\mathbf{K}_l}^{\theta^s}$. Noting then $g = \sigma_l(\gamma)f\gamma^{-1}$, we get a bijection $f \mapsto g$ between nontwisted and ξ-twisted self-dual skew cyclic codes:

$$gg^{\bullet_\xi} = \sigma_l(\gamma)ff^\bullet\frac{1}{\sigma_l(\gamma)} = f(0)X^s(X^r-1)$$

Moreover, if we assume $\theta^s(\xi) \neq \xi$ and $ff^\bullet = ff^{\bullet_\xi} = f\xi^{-1}f^\bullet\xi = 0$ in $\mathbf{E}_k^{(l)}$, then by evaluating lifts at 0, we get $f(0) = f(0)\frac{\theta^s(\xi)}{\xi}$, and so $f(0) = 0$ and thus $f = 0$, which contradicts the hypothesis. □

Algorithm 6 is an iterator that enumerates self-dual skew cyclic codes sitting in $\mathbf{E}_k$. It is exhaustive, in the sense that it lists every self-dual code at least once, but it is slightly redundant.

Algorithm 6: Enumeration of purely inseparable self-dual skew cyclic codes

```
1: C ← array of length p^m of maps of iterators on all twisted codes indexed by all
   possible twists ξX^{s(deg(f)/s %2)} where ξ can be chosen among all representatives of
   P^r_{F_l} in K_l if deg(f)/s is even and otherwise among all representatives of P^r_{F_l} in K_l
   that are anti-symmetric relatively to θ^s.
2: procedure RunThroughRemainingCodes(f)
3:     i ← deg(f)/s
4:     if i = p^m :
5:         yield f
6:     else :
7:         while f_i ← next(C[i][f(0)X^{s(i%2)}]) :
8:             RunThroughRemainingCodes(f_i f)
9: RunThroughRemainingCodes(1)
```

Theorem 2.41 Algorithm 6 is correct and exhaustive

Proof. In order to enumerate all inseparable self-dual skew cyclic codes, at the cost of some redundancy, we can assume without loss of generality (See the last part of the proof, hereunder) that the general solution is a product of twisted self-dual skew cyclic

codes $f_1 \dots f_n$, where the f_i are left monic. We start by solving the equation $f_n f_n^\bullet \equiv 0 \mod (X^r - 1)$. This has been done in the preceding section. Now we obtain a scalar $\kappa_n = \frac{f_n f_n^\bullet}{X^s(X^r-1)}$ which is equal to $f_n(0)$. Let $\bullet_{\kappa_n}$ be defined by $f_i^{\bullet_{\kappa_n}} = \sigma_l(\kappa_n) f_i^\bullet {\kappa_n}^{-1}$. The equation becomes $f_{n-1} X^s f_{n-1}^{\bullet_{\kappa_n}} \equiv 0 \mod (X^r - 1)$. Solving it, we now obtain a scalar $\kappa_{n-1} = \frac{f_{n-1} X^s f_{n-1}^{\bullet_{\kappa_n}}}{X^{r+s}(X^r-1)}$. At the next step, the monomials X^s cancel, and we are back in the Hermitian case: $f_{n-2} f_{n-2}^{\bullet_{\kappa_{n-1}\kappa_n}} \equiv 0 \mod (X^r - 1)$. Continuing in this way, we obtain alternately a skew Hermitian (resp. skew Euclidean) and a Hermitian (resp. Euclidean) bilinear form. We have to check that the κ_i satisfy the required symmetry for the self-dual skew cyclic codes to exist. A monic polynomial f satisfying the product criterion: $f f^{\bullet_{\kappa X^t}} = 0$ in $\mathbf{E}_{k,l}^{(\kappa X^t)}$ has a constant term $f(0)$ satisfying:

$$\begin{aligned}(X^s + \cdots + f(0))\kappa X^t (X^r f(0) + \cdots + X^s) &= \theta^s(\kappa)\theta^{s+t}(f(0)) X^s X^t X^r + f(0)\kappa X^t X^s \\ &\propto X^{r+s+t} - X^{s+t}.\end{aligned}$$

Thus, we have:

$$\theta^s(f(0)) = -f(0) \quad \text{for } \theta^s(\kappa) = \kappa\,,\ t = 0 \tag{2.14}$$

$$\theta^s(\kappa) = -\kappa \quad \text{for } t = s \,(\text{symplectic case}) \tag{2.15}$$

$$-f(0)\kappa = \theta^s(\kappa f(0)) \quad \text{for } t = 0 \tag{2.16}$$

If we start with $\kappa = 1$, we get the symplectic case from (2.14) and (2.15) with κ satisfying $\theta^s(\kappa) = -\kappa$, at the next step. We have then an orthogonal case, then again alternatively a symplectic case with κ satisfying $\theta^s(\kappa) = -\kappa$ from (2.16), *etc.*

We now prove that the algorithm is exhaustive. We observe that the projection

$$\begin{array}{ccc} \mathbf{E}_k^{(l)} = \mathbf{K}_l[X^{\pm 1};\theta]/(X^r-1)^{p^m} & \longrightarrow & \mathbf{K}_l[X^{\pm 1};\theta]/(X^r-1) = \mathbf{E}_1^{(l)} \\ f & \mapsto & \bar{f} \end{array}$$

preserves the self-orthogonality property. Noting $f_{p^m} := \tilde{\bar{f}}$ the unique lift of $\bar{f}$ on the basis $(X^i)_{0 \leqslant i < r}$, we have a factorization $f_{p^m} = r_{p^m} g_{p^m}$ for a skew polynomial r_{p^m} of degree strictly less than s and a self-dual skew cyclic code g_{p^m} in E_1. Indeed, any self-orthogonal subspace of $\mathbf{E}_1^{(l)}$ of dimension strictly less than r, corresponding to a monic skew polynomial f can be extended, by Witt's decomposition, to a maximal isotropic space corresponding to a self-dual monic skew polynomial g of degree s. Now this vector space inclusion corresponds by duality to a factorization $\bar{f} = rg$ for a skew polynomial r of degree strictly less than s. Expressing $(X^r - 1)$ as a product of the self-dual codes g_{p^m}, $\frac{g_{p^m}^* g_{p^m}}{g_{p^m}(0) X^s}$ we get that any self-orthogonal skew cyclic code $f \in \mathbf{E}_k^{(l)}$

can be written in the form

$$f = h(X^r - 1) + f_{p^m} = \left(h \frac{g^*_{p^m}}{g_{p^m}(0) X^s} + r_{p^m} \right) g_{p^m}$$

where $\deg h = (p^m - 2)s$ and $\frac{1}{X^s g_{p^m}(0)} g^*_{p^m} \in \mathbf{K}_l[X;\theta]$ is of degree s. Let us note $f' = h \frac{1}{X^s g_{p^m}(0)} g^*_{p^m} + r_{p^m}$. We have $\deg f' = (p^m - 1)s$ and $f' g_{p^m} (f' g_{p^m})^* = f' g_{p^m}(0) X^s f'^* (X^r - 1) \equiv 0 \mod (X^r - 1)^{p^m}$ and hence $f' f'^{\bullet_{X^s g_{p^m}(0)}} \equiv 0 \mod (X^r - 1)^{p^m - 1}$. With the same reasoning, replacing f by f' and the adjunction $*$ by $\bullet_{X^s g_{p^m}(0)}$, we get yet another twisted separable self-dual skew cyclic code $g_{p^m - 1}$ and another skew polynomial f'' such that $f'' f''^{\bullet_{g_{p^m-1}(0) g_{p^m}(0)}} \equiv 0 \mod (X^r - 1)^{p^m - 2}$. In turn replacing f' by f'' and the adjunction $\bullet_{X^s g_{p^m}(0)}$ by $\bullet_{g_{p^m-1}(0) g_{p^m}(0)}$, we get yet another twisted separable self-dual skew cyclic code $g_{p^m - 2}$ and another skew polynomial f''' such that $f''' f'''^{\bullet_{X^s g_{p^m-2}(0) g_{p^m-1}(0) g_{p^m}(0)}} \equiv 0 \mod (X^r - 1)^{p^m - 3}$. By induction, we thus obtain a factorization $g_1 g_2 \cdots g_{p^m - 1} g_{p^m}$ of f into twisted separable self-dual skew cyclic codes as claimed. □

Remark 2.42 We notice the reason for the redundancy in the enumeration algorithm from the above proof of the exhaustiveness. Indeed, the many different factorizations $f_i = r_i g_i$ for self-orthogonal f_i at each step lead to as many redundant enumerations of the same inseparable self-dual skew cyclic code f.

3 An implementation in SageMath

3.1 SageMath enumeration results in the separable case

We implemented the algorithms of this section in SageMath. Our package is available at

`https://plmlab.math.cnrs.fr/caruso/selfdual-skew-cyclic-codes`

The package consists of a main class instantiated with the extension $\mathbf{K}/\mathbf{F}$ of order r and a palindromic polynomial of the center $P(X^r)$ in $\mathbf{F}(X^{\pm r})$ of $\mathbf{K}[X^{\pm 1};\theta]$ as constructor parameters. It provides an iterator on all self-dual codes for the Ore algebra $\mathbf{K}[X^{\pm 1};\theta]/P(X^r)$. Below, we present an example covering the palindromic Euclidean case.

We start by loading our package and defining the relevant base rings.

```
sage: load("selforthogonal_codes.sage")
None
sage: q = s = 3; F = GF(q); Fy.<y> = F[]
sage: Q = F['z'].irreducible_element(2*s, "adleman-lenstra")
sage: Q
z^6 + z^5 + z^4 + z^3 + z^2 + z + 1
```

Case 3.1 Palindromic Euclidean: $q = 3$, $s = 3$ and $P(Y) = Y - 1$

$P(Y)$	$q=3$	$q=5$	$q=7$	$q=3^2$
$Y-1$	no codes.	no codes.	no codes.	no codes.
Y^3-1	inseparable	no codes.	no codes.	inseparable
Y^5-1	no codes.	inseparable	no codes.	no codes.
Y^7-1	no codes.	no codes.	inseparable	no codes.
Y^9-1	inseparable	no codes.	no codes.	inseparable
$Y+1$	9 ms	9 ms	16 ms	21 ms
Y^2+1	16 ms	6 ms	15 ms	15 ms
Y^3+1	inseparable	26 ms	22 ms	inseparable
Y^4+1	18 ms	21 ms	35 ms	48 ms
Y^5+1	62 ms	inseparable	111 ms	128 ms
Y^6+1	inseparable	47 ms	59 ms	inseparable
Y^7+1	80 ms	300 ms	inseparable	250 ms
Y^8+1	463 ms	87 ms	113 ms .	108 ms
Y^9+1	inseparable	218 ms	125 ms	inseparable

Figure I.1: Timings for the generation of one single code when $s=2$

```
sage: A = SelfDualCodes(y - 1, Q)
sage: iter = A.enumerate_selfdual_codes()
sage: next(iter)
x^3 + (z^5 + 2*z^4 + z^2 + 1)*x^2 + (2*z^4 + z^3 + z^2 + z + 2)*x + z^3 + z^2 + z + 2
sage: next(iter)
x^3 + (2*z^3 + 2*z^2 + 2*z + 1)*x^2 + (2*z^5 + 2*z^4 + 2*z^3 + 2*z^2 + 1)*x + 2*z^4 +
    z^3
sage: next(iter)
x^3 + (2*z^5 + z^4 + 2*z^2 + 2)*x^2 + (2*z^4 + z^3 + z^2 + z + 2)*x + 2*z^3 + 2*z^2 +
    2*z + 1
```

Benchmarks for a larger set of inputs are reported in Figures II.2, II.3 and I.3; they were run on a computer with Intel(R) Core(TM) i7-9750H CPU 2.60GHz processor x64 and 16 GB of RAM.

We illustrate hereunder self-dual code enumeration in the non-palindromic case, and in the palindromic case for the four finite geometries: Euclidean, Hermitian, Skew Euclidean and Skew Hermitian.

Non-palindromic Case: $P(Y)=Y^2-2$ and $P(Y)=Y^2-3$

```
sage: load("selforthogonal_codes.sage")
None
sage: q =5; s=3; F = GF(q); Fy.<y> = F[]
sage: Q = F['z'].irreducible_element(2*s, "adleman-lenstra")
sage: A = SelfDualCodes(y^4 + 1, Q)
sage: iter = A.enumerate_selfdual_codes()
sage: next(iter)
x^12 + 3
sage: next(iter)
x^12 + (2*z^5 + 3*z^4 + z^2 + z + 2)*x^11 + (2*z^5 + 3*z^2 + 2*z + 2)*x^10 + (3*z^5 +
    4*z^2 + z + 3)*x^9 + (z^5 + 3*z^4 + z^3 + 4*z^2 + 3*z + 3)*x^8 + (4*z^5 + 2*z^4 +
```

$P(Y)$	$q=3$	$q=5$	$q=7$	$q=3^2$
$Y-1$	21 ms	no codes.	207 ms	no codes.
Y^3-1	inseparable	no codes.	42 ms	inseparable
Y^5-1	101 ms	inseparable	129 ms	no codes.
Y^7-1	195 ms	no codes.	inseparable	no codes.
Y^9-1	inseparable	no codes.	342 ms	inseparable
$Y+1$	no codes.	21 ms	no codes.	56 ms
Y^2+1	152 ms	12 ms	36 ms	32 ms
Y^3+1	inseparable	57 ms	no codes.	inseparable
Y^4+1	38 ms	47 ms	74 ms	141 ms
Y^5+1	no codes.	inseparable	no codes.	317 ms
Y^6+1	inseparable	101 ms	139 ms	inseparable
Y^7+1	no codes.	398 ms	inseparable	601 ms .
Y^8+1	209 ms	270 ms	270 ms	280 ms
Y^9+1	inseparable	450 ms	no codes.	inseparable

Figure I.2: Timings for the generation of one single code when $s=3$

$P(Y)$	$q=3$	$q=5$	$q=7$	$q=3^2$
$Y-1$	no codes.	no codes.	no codes.	no codes.
Y^3-1	inseparable	no codes.	no codes.	inseparable
Y^5-1	no codes.	inseparable	no codes.	no codes.
Y^7-1	no codes.	no codes.	inseparable	no codes.
Y^9-1	inseparable	no codes.	no codes.	inseparable
$Y+1$	59 ms	49 ms	58 ms	177 ms
Y^2+1	78 ms	29 ms	89 ms	69 ms
Y^3+1	inseparable	128 ms	90 ms	inseparable
Y^4+1	88 ms	108 ms	174 ms	412 ms
Y^5+1	220 ms	inseparable	336 ms	723 ms
Y^6+1	inseparable	200 ms	388 ms	inseparable
Y^7+1	286 ms	387 ms	inseparable	1367 ms
Y^8+1	406 ms .	551 ms	586 ms	2159 ms
Y^9+1	inseparable	691 ms	784 ms	inseparable

Figure I.3: Timings for the generation of one single code when $s=4$

```
    z^3 + 2*z^2 + 4*z + 4)*x^7 + (z^5 + 4*z^4 + 4*z^3 + 2*z^2 + 4*z + 1)*x^6 + (3*z^4
    + z^3 + 3*z + 1)*x^5 + (3*z^5 + z^4 + 4*z^3 + z^2 + 2*z + 2)*x^4 + (2*z^5 + 3*z^3
    + 2*z)*x^3 + (z^5 + 3*z^4 + z^3 + 4*z^2 + 4*z + 2)*x^2 + (3*z^5 + 4*z^4 + 2*z^3 +
    3*z^2 + 2)*x + z^4 + 4*z^3 + z^2 + 2*z
sage: next(iter)                                                                    25
x^12 + (3*z^5 + 2*z^4 + z^3 + 4*z^2 + 4*z + 2)*x^11 + (z^5 + 4*z^4 + z^3 + 3*z^2 + 1)*  26
    x^10 + (z^5 + 4*z^2 + 2)*x^9 + (z^5 + z^4 + 3*z^3 + z^2 + 3*z + 1)*x^8 + (z^3 + 4*
    z^2 + 2*z + 2)*x^7 + (4*z^5 + 4*z^4 + 3*z^3 + 3*z^2 + z)*x^6 + (4*z^5 + 4*z^4 + z
    ^3 + z + 2)*x^5 + (3*z^5 + 4*z^4 + 4*z^3 + 4)*x^4 + (4*z^4 + 3*z^3 + 4*z^2 + 4*z +
     2)*x^3 + (2*z^5 + 3*z^3 + 2*z^2 + 2)*x^2 + (2*z^5 + 4*z^4 + z^3 + z^2 + 2*z + 4)*
    x + 3*z^5 + 3*z^4 + 3*z^2 + 3*z + 1
```

Palindromic Euclidean Case: $P(Y) = Y - 1$

```
sage: load("selforthogonal_codes.sage")                                             27
None                                                                                28
sage: q = s = 3; F = GF(q); Fy.<y> = F[]                                            29
sage: Q = F['z'].irreducible_element(2*s, "adleman-lenstra")                        30
sage: A = SelfDualCodes(y - 1, Q)                                                   31
sage: iter = A.enumerate_selfdual_codes()                                           32
sage: next(iter)                                                                    33
x^3 + (z^5 + 2*z^2)*x^2 + x + 2*z^5 + 2*z^4 + z^3 + z^2                             34
sage: next(iter)                                                                    35
x^3 + (2*z^5 + 2*z^4 + 2*z^3 + z^2)*x^2 + (z^5 + z^4 + 2*z^2 + z + 2)*x + z^5 + z^4 +  36
    z + 2
sage: next(iter)                                                                    37
x^3 + (z^5 + 2*z^4 + z^2 + 2*z + 1)*x^2 + (z^5 + z^4 + z^3 + z^2 + 2)*x + z^5 + 2*z^4  38
    + z^3 + 2*z^2
```

Palindromic Euclidean Case: $P(Y) = Y - 1$ and Palindromic Hermitian Case: $P(Y) = 1 + Y + Y^2 + Y^3 + Y^4$

```
sage: load("selforthogonal_codes.sage")                                             39
None                                                                                40
sage: q = s = 3; F = GF(q); Fy.<y> = F[]                                            41
sage: Q = F['z'].irreducible_element(2*s, "adleman-lenstra")                        42
sage: A = SelfDualCodes(y^5- 1, Q)                                                  43
sage: iter = A.enumerate_selfdual_codes()                                           44
sage: next(iter)                                                                    45
x^15 + (2*z^5 + 2*z^4 + z^3 + z^2 + 2*z + 2)*x^14 + (z^4 + 2)*x^13 + (2*z^5 + 2*z^4 +  46
    z^2 + 2*z + 1)*x^12 + (2*z^5 + z^4 + 2*z^3 + z^2 + 2)*x^11 + (2*z^3 + 2*z^2 + z +
    2)*x^10 + (2*z^5 + 2*z^4 + 2*z^2 + 2*z)*x^9 + (z^4 + z^3 + 2*z^2 + 1)*x^8 + (2*z^5
     + 2*z^2 + z + 2)*x^7 + (2*z^5 + z^4 + z^2 + 2*z)*x^6 + (2*z^5 + 2*z^4 + 2*z + 1)*
    x^5 + (z^5 + 2*z^4 + z^3 + z^2 + 2)*x^4 + (2*z^5 + z^4 + z^3 + z^2)*x^3 + (2*z^5 +
     2*z^3 + 2*z^2 + 2*z + 2)*x^2 + (z^4 + 2*z^2)*x + z^5 + 2*z^4 + z^3 + 2*z^2
sage: next(iter)                                                                    47
x^15 + (2*z^5 + z^3 + z^2 + 2*z + 2)*x^14 + (z^5 + 2*z^2 + 2*z + 1)*x^13 + (z^5 + z^4  48
    + z^3 + 2*z^2 + z)*x^12 + (z^5 + z^4 + 2*z^3 + z^2 + z + 2)*x^11 + (z^5 + z^4 + z
    ^3)*x^10 + (z^5 + 2*z^4 + 2*z^3 + 2*z^2 + 1)*x^9 + (z^5 + 2*z^3 + z^2 + 1)*x^8 + (
    z^5 + z^4 + 2*z^3 + z + 2)*x^7 + (2*z^5 + 2*z^4 + 2*z)*x^6 + 2*z*x^5 + (2*z^4 + 2*
    z^2 + 2)*x^4 + (z^5 + 2*z^3 + z^2)*x^3 + (z^5 + z^4 + 2*z^3 + z)*x^2 + (z^5 + 2*z
    ^4 + z^3 + 2*z^2 + 2*z)*x + z^5 + 2*z^4 + z^2 + 2*z + 1
sage: next(iter)                                                                    49
x^15 + (z^5 + 2*z^2 + 1)*x^14 + (z^3 + z^2 + z + 1)*x^13 + (z^3 + z^2 + 2*z + 2)*x^12  50
    + (2*z^4 + z^3 + z^2 + 2*z + 1)*x^11 + (2*z^5 + z^4 + z^3 + z^2 + 2*z + 1)*x^10 +
    (z^3 + 2*z^2 + 2*z + 2)*x^9 + (2*z^5 + 2*z^3 + 1)*x^8 + (2*z^5 + 2*z^4 + z^3 + z +
     2)*x^7 + (2*z^5 + z^4 + 2)*x^6 + (2*z^5 + 2*z^4 + 2*z^3 + 2*z)*x^5 + (z^5 + z^4 +
     2*z^3 + z^2 + z + 2)*x^4 + (2*z^5 + z^3 + 2*z^2 + 2*z + 1)*x^3 + (z^3 + 2*z^2 +
    1)*x^2 + (z^4 + z^3 + 2*z)*x + 2*z^5 + 2*z^4 + 2*z^3 + 2*z^2 + z + 2
```

Palindromic Skew Euclidean Case: $P(Y) = Y - 1$

```
sage: load("selforthogonal_codes.sage")
None
sage: q =3; s=2; F = GF(q); Fy.<y> = F[];
sage: Q = F['z'].irreducible_element(2*s, "adleman-lenstra");K=Field.extension(F,Q)
sage: iota=K.frobenius_endomorphism(s)(K.gen())-K.gen()
sage: A = SelfDualCodes(y-1, Q,iota,True,True)
sage: iter = A.enumerate_selfdual_codes()
sage: next(iter)
x^2 + (2*z^3 + z)*x + 2*z^2 + z + 2
sage: next(iter)
x^2 + (2*z^3 + 1)*x + 2*z^3 + z^2 + 2*z
sage: next(iter)
x^2 + z^3 + z^2 + z + 1
```

Palindromic Skew Hermitian Case: $P(Y) = Y^2 + 1$

```
sage: load("selforthogonal_codes.sage")
None
sage: q =5; s=2; F = GF(q); Fy.<y> = F[];
sage: Q = F['z'].irreducible_element(2*s, "adleman-lenstra");K=Field.extension(F,Q)
sage: iota=K.frobenius_endomorphism(s)(K.gen())-K.gen()
sage: A = SelfDualCodes(y^2+1, Q,iota,True,True)
sage: iter = A.enumerate_selfdual_codes()
sage: next(iter)
x^4 + 3
sage: next(iter)
x^4 + (z^2 + 4*z + 2)*x^3 + (z^2 + 3*z + 3)*x^2 + (z^3 + 3*z^2 + z + 4)*x + 4*z^2 + 4
sage: next(iter)
x^4 + (3*z^2 + z + 3)*x^3 + (2*z^3 + 3*z^2)*x^2 + (3*z^3 + 2*z^2 + 2*z + 1)*x + 2*z^3
    + z^2 + 3*z
```

3.2 SageMath enumeration results in the inseparable case

For $F = GF(3)$, $K = GF(3^6)$ and $k = 3$, the upper bound on the number of generated inseparable self-dual skew cyclic codes is numerically equal to $80 \times 1120 \times 80$, where 80 is the number of orthogonal isotropic spaces and 1120 the number of symplectic isotropic spaces (see Remark 2.39). A SageMath enumeration based on this algorithm provides a number n of maximal isotropic codes equal to $n = 2360960$. There are relatively few redundancies since $80 \times 1120 \times 80 \approx 3 \times 2360960$. The computation runs in under 10 minutes on this computer.

Chapter II

Duality and Decoding of Linearized Algebraic Geometry Codes

1 Reminders on algebraic curves

We begin by recalling some definitions and theorems about algebraic curves.

1.1 Riemann–Roch Theorem and Serre duality

In this thesis, we primarily adopt the algebraic viewpoint, where places of a function field of one variable over a field F correspond to closed points on a nonsingular projective irreducible curve over F. This choice is justified by the anti-equivalence of categories between these curves equipped with non-constant F-morphisms on the one hand, and their algebraic counterparts equipped with F-embeddings inducing finite extensions on the other.

Let K be a function field of transcendence degree 1 over an arbitrary field F that is algebraically closed in K (i.e., F is the field of constants of K). Let L/K be a cyclic extension of K of degree r, of constant field also F. Let $\mathbb{P}_K$ (resp. $\mathbb{P}_L$) denote the places of K (resp. L). Let $\mathrm{Div}(L) := \oplus_{Q\in\mathbb{P}_L}\mathbb{Z}Q$ be the divisor group of L.

Definition 1.1.1.
Let $A = \sum_{Q\in\mathbb{P}_L} A_Q Q \in \mathrm{Div}(L)$ be a divisor of L. We define the Riemann–Roch space $\mathcal{L}(A)$ associated to A as

$$\mathcal{L}(A) := \{f \in L \mid w_Q(f) + A_Q \geqslant 0 \quad \forall Q \in \mathbb{P}_L\}$$

We denote by $l(A)$ its (finite) dimension.

Definition 1.1.2.
A canonical divisor W of L is a divisor $W := \sum_{Q\in\mathbb{P}_L} W_Q Q$ such that there exists a

differential on L, $\eta \in \Omega_L$ whose valuation is W_Q at every place $Q \in \mathbb{P}_L$, this valuation at Q being defined as the valuation of the coefficient $f \in L$ at Q for any decomposition $\eta = f dt$ where t is a uniformizer at Q.

We recall the classical Riemann–Roch Theorem and the Serre duality.

Theorem 1.1.3 (Classical Riemann–Roch)**.**
Let W be a canonical divisor of L. For any divisor $A \in \mathrm{Div}(L)$, the following Riemann–Roch formula holds:

$$l(A) = \deg A + 1 - g + l(W - A).$$

where g is an invariant non-negative integer called the genus of L.
Moreover, we have $l(A) = 0$ if $\deg(A) < 0$ and $\deg(W) = 2g-2$. So, if $\deg(A) > 2g-2$, then $l(W - A) = 0$.

1.2 Different, Discriminant and Riemann–Hurwitz formula

We recall the definition of the different divisor of a function field extension L/K. For $P \in \mathbb{P}_K$, let $\mathcal{O}_P$ be the (integrally closed) valuation ring of K_P, the completion of K at P, and let $\mathcal{O}_{L,P} = \prod_{Q|P} \mathcal{O}_Q$ denote the integral closure of $\mathcal{O}_P$ in the finite K_P-algebra $L_P = L \otimes_K K_P$.

Definition 1.2.1 (Different)**.**
Denoting by $L_P = L \otimes_K K_P$ the completion of L at P, the following set is called the complementary module of $\mathcal{O}_{L,P}$ over $\mathcal{O}_P$.

$$\mathcal{C}(\mathcal{O}_{L,P}) := \left\{ z \in L_P \mid \mathrm{Trace}_{L_P/K_P}(z \cdot \mathcal{O}_{L,P}) \subseteq \mathcal{O}_P \right\}$$

As we have $\mathcal{C}(\mathcal{O}_{L,P}) = t_P \cdot \mathcal{O}_{L,P}$ for some $t_P = (t_Q)_{Q|P} \in L_P \simeq \prod_{Q|P} L_Q$, we can define the different exponent at Q over P by;

$$d_Q := -w_Q(t_Q) \geqslant 0$$

This exponent d_Q does not depend on the place Q above a specific place P. Moreover, $d_Q = 0$ holds for almost all $Q \in \mathbb{P}_L$. We can therefore define the different divisor of L/K as:

$$\delta(L/K) := \sum_{P \in \mathbb{P}_K} \sum_{Q|P} d_Q \cdot Q$$

Theorem 1.2.2.
For any $t \in K \backslash \{0\}$ such that $dt \neq 0$, denoting by $\left(\frac{dt}{t}\right)_K$ resp. $\left(\frac{dt}{t}\right)_L$ the canonical divisor of K resp. L associated to the differential $\frac{dt}{t} \in \Omega_K$ resp. $\frac{dt}{t} \in \Omega_L$, we have

$$\left(\frac{dt}{t}\right)_L = \mathrm{CoNr}\left(\left(\frac{dt}{t}\right)_K\right) + \delta(L/K)$$

Proof. See [Sti93, Theorem 3.4.6] □

Finally, we define the discriminant $\mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)$.

Definition 1.2.3 (Discriminant)**.**
The discriminant is the following (principal) ideal of the discrete valuation ring $\mathcal{O}_P$

$$\mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P) = \det\left(\mathrm{Tr}(x_i x_j)\right)_{1\leqslant i,j\leqslant r}\mathcal{O}_P$$

where $r := \dim_{K_P} L_P = [L:K]$ *and* $(x_1,\ldots,x_r)$ *is a basis of* $\mathcal{O}_{L,P}$ *over* $\mathcal{O}_P$*.*

To relate the genus of L to that of K, one uses the Riemann–Hurwitz formula.

Theorem 1.2.4 (Riemann-Hurwitz formula)**.**
Let L/F *be an algebraic function field of genus* g *over the constant field* F *and let* L'/L *be a finite separable extension. Let* F' *denote the constant field of* L' *and* g' *the genus of* L'/F'*. Then we have*

$$2g' - 2 = \frac{[L':L]}{[F':F]}(2g-2) + \deg \mathrm{Diff}\,(L'/L)\,.$$

Proof. See [Sti93, Theorem 3.4.13]. □

2 Article: Duality and Decoding of Linearized Algebraic Geometry Codes

2.1 Abstract of the article [BCD26]

We design a polynomial-time decoding algorithm for linearized Algebraic Geometry codes with unramified evaluation places, a family of sum-rank metric evaluation codes on division algebras over function fields introduced in [BC24]. By establishing a Serre duality and a Riemann–Roch theorem for these algebras, we prove that the dual codes of such linearized Algebraic Geometry codes, that we term linearized Differential codes, coincide with the linearized Algebraic Geometry codes themselves over the adjoint algebra, and that our decoding algorithm is correct.

2.2 Introduction

Sum-rank metric codes have seen a resurgence of interest in recent decades due to their broad applications in areas like network coding, distributed data storage, and code-based cryptography as described in [MPSK22]. Recent code constructions, such as the linearized Reed–Solomon codes introduced in [MP18b], achieve the sum-rank

Singleton-type bound. Furthermore, linearized Algebraic Geometry (LAG) codes were introduced and studied by the first and second authors in [BC24], using Riemann–Roch spaces on some division algebras over function fields of curves. They generalize both Algebraic Geometry (AG) codes as described in [Sti93] and linearized Reed–Solomon codes. This lends them good properties in the sum-rank metric: they almost meet the sum-rank Singleton bound and their length is not limited by the size of the alphabet. We also mention that other algebraic constructions exist, such as linearized Reed–Muller codes, described in [BC25].

The main contributions of this paper are to study the duality properties of linearized AG codes and to design a decoding algorithm for them, under the hypothesis that the evaluation places used in their definition are unramified.

We briefly outline the construction of linearized AG codes (a more detailed presentation is given at the beginning of Section 2.4 of the present paper). Let K be the function field of an algebraic curve defined over a field F. We fix a cyclic extension L/K of degree r and a generator θ of its Galois group. We let $L[T;\theta]$ be the corresponding Ore polynomial ring. We set

$$\mathbb{D} := \frac{L[T;\theta]}{T^r - x},$$

where $x \in K$ is chosen so that $\mathbb{D}$ is a division algebra as in [BC24, Section IV A].

In [BC24], ultrametric value functions on $\mathbb{D}$ (indexed by the places of L) are introduced and used to define Riemann–Roch spaces $\Lambda_{\mathbb{D}}(A) \subset \mathbb{D}$ associated to certain rational divisors A of L. Moreover, for any rational place P of K away from A (meaning that the support of A does not contain any place of L above P) and satisfying a certain hypothesis called **(H2-P_i)** in [BC24], an evaluation morphism $\bar{\varepsilon}_P : \Lambda_{\mathbb{D}}(A) \to \mathrm{End}_F(V_P)$ is constructed, where V_P is the residual algebra of L at P. Fixing a finite set $\{P_1, \dots, P_s\}$ of such places and setting $D = P_1 + \cdots + P_s$, one can concatenate the $\bar{\varepsilon}_i$ to obtain a multie-valuation morphism

$$\bar{\varepsilon}_D : \Lambda_{\mathbb{D}}(A) \to \prod_{i=1}^{s} \mathrm{End}_F\left(V_{P_i}\right) \simeq \left(F^{r\times r}\right)^s,$$

whose image is by definition the linearized AG code $\mathrm{LAG}_{\mathbb{D}}(A, D)$. It is endowed with the sum-rank metric defined by the weight function $(M_1, \dots, M_s) \mapsto \sum_{i=1}^{s} \mathrm{rank}(M_i)$.

The theorem [BC24, Theorem 2] provides estimates on the parameters of the code $\mathrm{LAG}_{\mathbb{D}}(A, D)$: assuming $\deg(A) < sr$, its minimum distance is at least $d^\star(A) := sr - \deg A$, while its dimension is that of the Riemann–Roch space $\Lambda_{\mathbb{D}}(A)$, which is itself bounded below by $r\deg(A) - r(g-1)$, where g is given by an explicit formula (see Definition 2.3.8) and is called the *genus* of $\mathbb{D}$.

In this paper, we propose a decoding algorithm for linearized AG codes (see Algorithm 7) and prove the following theorem.

Theorem 1 (Theorem 2.4.18)**.**
Let A be a divisor as above, and satisfying $2g-2 < \deg A < sr$. We assume the existence of a non-evaluation rational place P of K satisfying $r|e_P b_P$ (see Hypothesis 2.4.12). Set

$$\rho_{\text{algo}} := \left\lfloor \frac{d^\star(A) - g - 1}{2} \right\rfloor .$$

Then, our algorithm decodes any error relative to the code $\mathrm{LAG}_{\mathbb{D}}(A, D)$ of sum-rank weight at most ρ_{algo}, with polynomial complexity in s and r.

Our decoding algorithm is the sum-rank analogue of the classical decoding algorithm for AG codes in the Hamming metric described in [Sti93, Section 8.5]. We express the received word m as the sum $m = c + e$ of the original codeword $c \in \mathrm{LAG}_{\mathbb{D}}(A, D)$ and an error e of sum-rank weight at most ρ_{algo}. We first determine a space U localizing the error e with sufficient precision, i.e., satisfying $\mathrm{im}(e) \subset U$ and $\dim(U) < d^\star(A)$. Then, we solve the syndrome equations for e restricted to the localizing space.

The fundamental theorem underlying our decoding algorithm is a Riemann–Roch Theorem on $\mathbb{D}$ for what we call *extended divisors*. Those are pairs composed of a divisor A away from D and a product of vector subspaces $W := \bigoplus_{i=1}^{s} W_i$, where $W_i \subset V_{P_i}$. To an extended divisor (A, W), we associate its degree $\deg(A, W) = \deg A - \dim_F W$ and the Riemann–Roch space

$$\Lambda_{\mathbb{D}}(A, W) := \left\{ f \in \Lambda_{\mathbb{D}}(A) \mid \bar{\varepsilon}_i(f)_{|W_i} = 0 \quad \forall i \in \{1, \dots, s\} \right\}.$$

We denote its dimension by $\lambda_{\mathbb{D}}(A, W)$. Besides, we define a canonical divisor K related to $\mathbb{D}$, whose degree is $2g-2$. Letting $\mathbb{D}^\star = \frac{L[T;\theta]}{T^r - x^{-1}}$, our Riemann–Roch Theorem reads as follows.

Theorem 2 (Theorem 2.3.38)**.**
Let (A, W) be an extended divisor. We have

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) + r(1-g) + \lambda_{\mathbb{D}^\star}\left(\mathcal{K} + \mathrm{CoNr}(D) - A, W^\perp\right)$$

where $\mathrm{CoNr}(D) = \sum_{i=1}^{s} \sum_{Q|P_i} Q$ and $W^\perp$ is the orthogonal of W with respect to the trace bilinear form (see Subsection 2.3.3).

Moreover, if $\deg(A, W) < 0$, then we have $\lambda_{\mathbb{D}}(A, W) = 0$.

We show this theorem by extending the proof of the classical Riemann–Roch Theorem as presented in [Sti93, Chapter 1] and in [Sha13, Chapter 7]. As an important ingredient of the proof, we define adelic spaces associated to $\mathbb{D}$ and differential spaces associated to $\mathbb{D}^\star$, and we show a Serre-type duality theorem, establishing a perfect pairing between them. As in the classical case, this theorem brings along a canonical

duality between linearized AG codes and some linearized Differential codes defined by means of residues (see Definition 2.4.2).

Theorem 3 (Theorem 2.4.3)**.**
For any divisor A away from D and a particular choice of K, we have the following equalities of codes:

$$\mathrm{LAG}_{\mathbb{D}}(A,D)^{\perp} = \mathrm{LD}_{\mathbb{D}^\star}(A,D) = \mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A, D).$$

We note that a similar theorem was proved in [CD23] for linearized Reed–Solomon codes, which correspond to the case where $K = \mathbb{F}_q(t)$, $L = \mathbb{F}_{q^r}(t)$ and A is a scalar multiple of the point at infinity. On the other hand, in this situation, the result of [CD23] encompasses a more general setting, as it includes Ore polynomials with derivations, and restrictions of the morphisms $\bar{\varepsilon}_D$ to subspaces.

Organization of the paper
The paper is structured as follows. In Section 2.3, we establish our Riemann–Roch Theorem. In Section 2.4, we move to applications to coding theory, establishing first the duality theory for linearized AG codes, and then designing their decoding algorithm. Besides, in Appendix 6, we provide some results from a SageMath implementation of our algorithm.

2.3 Riemann–Roch theorem on division algebras

We consider the setting of [BC24]. Let F be an arbitrary field. Let K be an algebraic function field in one variable over its constant field F. Let L/K be a cyclic extension of degree $r \geqslant 1$ with the same constant field F. We denote by θ a generator of its cyclic Galois group.

We denote by $\mathcal{P}_K$ and $\mathcal{P}_L$ the sets of places of K and L, respectively. For a place $P \in \mathcal{P}_K$ (resp. $Q \in \mathcal{P}_L$), we write K_P (resp. L_Q) for the completion of K (resp. L) at that place. We also use L_P (resp. $\mathbb{D}_P$) to denote the completion of L (resp. $\mathbb{D}$) at a place $P \in \mathcal{P}_K$. We denote by v_P (resp. w_Q) the normalized valuation of K (resp. of L) at a place P (resp. Q). We use the notation $Q|P$ to indicate that Q is a place of L above a place P of K. Writing e_P the ramification index of $Q|P$, we have $w_Q|_K = e_P v_P$. We also use the notation $\mathcal{O}_P$ (resp. $\mathcal{O}_Q$) for the valuation ring of K_P (resp. L_Q) and set

$$\mathcal{O}_{L,P} := \prod_{Q|P} \mathcal{O}_Q \subset L_P.$$

We consider the Ore polynomial ring $L[T;\theta]$, defined in [Ore33] as polynomials equipped with a twisted multiplication given by the rule $Ta = \theta(a)T$ for any $a \in L$.

We note that the ring $L[T;\theta]$ is left and right Euclidean as shown in [Ore33, Section 2]. Let $x \in K^\times$. We define as in [BC24] a cyclic algebra $\mathbb{D}$ by

$$\mathbb{D} := \frac{L[T;\theta]}{T^r - x}.$$

Throughout the paper, we assume that x is chosen in such a way that $\mathbb{D}$ is a division algebra (see Hypothesis **(H1)** in [BC24, Section IV]). For $P \in \mathcal{P}_K$, we set $\mathbb{D}_P = K_P \otimes_K \mathbb{D}$.

In the sequel, we will tacitly use the obvious isomorphisms

$$\begin{array}{rcl} \mathbb{D} & \xrightarrow{\sim} & L^r \\ \sum_{i=0}^{r-1} \alpha_i T^i & \mapsto & (\alpha_i)_{i=0}^{r-1} \end{array} \quad \text{and} \quad \begin{array}{rcl} L \otimes_K K_P & \xrightarrow{\sim} & \prod_{Q|P} L_Q \\ y & \mapsto & (y_Q)_{Q|P} \end{array}.$$

We will denote by $y_i \in L$ (resp. $y_i \in \prod_{P\in\mathcal{P}_K} L \otimes_K K_P$) the i-th component of $y \in \mathbb{D}$ (resp. $y \in \prod_{P\in\mathcal{P}_K} \mathbb{D} \otimes_K K_P$), induced by the first isomorphism, and by $y_Q \in L_Q$ the Q-th component of $y \in L \otimes_K K_P$ for $Q|P$, induced by the second isomorphism.

Remark 2.3.1.
As shown in [Rei75, Theorem 32.20], if F is a finite field, all finite-dimensional central simple algebras over the global function field K are cyclic and can be represented in the form $\frac{L[T;\theta]}{T^r-x}$. Therefore, in the context of application to linear codes over algebraic curves defined over a finite field of constants, our choice of $\mathbb{D}$ is general. However, for an arbitrary constant field F or for a higher dimensional function field K, the decomposition $\frac{L[T;\theta]}{T^r-x}$ need not represent all central simple algebras over K.

The goal of this section is to prove a Riemann–Roch Theorem on $\mathbb{D}$. Beyond its own interest, this result will be pivotal to design our decoding algorithm for linearized AG codes.

We mention that, following the Ph.D. thesis of Witt [Wit34], Tamagawa [Tam51] and later Mattson [Mat61] showed a Riemann–Roch Theorem in the more general setting of central simple algebras over a function field. However, our approach based on the decomposition $\mathbb{D} = \frac{L[T;\theta]}{T^r-x}$, is more explicit and allows for effective duality with differential forms. In particular, this will be pivotal, in Subsection 2.4.1, to canonically characterize the dual of a linearized AG code as a linearized Differential code.

2.3.1 The case of numerical divisors

For any place $P \in \mathcal{P}_K$, we define the positive integer

$$b_P := \frac{r}{\gcd(e_P v_P(x), r)}.$$

We note that we have $b_P = 1$ at all places where $v_P(x) = 0$, hence almost everywhere.

We define the group of *divisors* of $\mathbb{D}$

$$\mathrm{Div}(\mathbb{D}) := \bigoplus_{P\in\mathcal{P}_K} \bigoplus_{Q|P} \frac{\mathbb{Z}}{b_P} Q.$$

The *degree* of a divisor $A = \sum_Q A_Q Q$ is, by definition, $\deg A := \sum_Q A_Q \deg Q$.
We define the following Q-functions ω_Q

$$\begin{array}{rccl} \omega_Q : & \mathbb{D}_P \simeq \sum_{j=0}^{r-1} L_P T^j & \longrightarrow & \frac{\mathbb{Z}}{b_P} \\ & y = \sum_{j=0}^{r-1} (y_{jQ'})_{Q'|P} T^j & \mapsto & \min\limits_{0\leqslant j<r} \left(w_Q(y_{jQ}) + j\frac{w_Q(x)}{r} \right) \end{array}$$

and the gauge

$$\begin{array}{rccl} \omega_P : & \mathbb{D}_P & \longrightarrow & \frac{\mathbb{Z}}{b_P e_P} \\ & (\alpha_Q)_{Q|P} & \mapsto & \min\limits_{Q|P} \frac{\omega_Q(\alpha_Q)}{e_P} \end{array} .$$

Note that the definition ω_Q corresponds to the definition $e_P \cdot w_{j,x}$ from [BC24].

Lemma 2.3.2.
The gauge ω_P is surmultiplicative, that is, for every $f, g \in \mathbb{D}_P$ it holds

$$\omega_P(fg) \geqslant \omega_P(f) + \omega_P(g).$$

Proof. Let $P \in \mathcal{P}_K$. For $f, g \in \mathbb{D}_P$, we have

$$\omega_P(fg) = \omega_P\left(\sum_{i=0}^{r-1} f_i T^i \sum_{i=0}^{r-1} g_i T^i \right) = \omega_P\left(\sum_{i=0}^{r-1} \sum_{k=0}^{i} f_k \theta^k(g_{i-k}) T^i + \sum_{i=r}^{2r-2} \sum_{k=i-r+1}^{r-1} x f_k \theta^k(g_{i-k}) T^{i-r} \right).$$

Let i_0 be the index of a minimal summand. We let $Q_1, \ldots, Q_{m_P}$ be the places above P, indexed such that $\theta^{-1}(Q_j) = Q_{(j+1)\%m_P}$. We distinguish the two cases $i_0 \geqslant r$ and $0 \leqslant i_0 < r$. In the first case, we have

$$\begin{aligned} \omega_P(fg) &\geqslant \min_j \left(\frac{w_{Q_j}\left(x \sum_{i_0-r+1\leqslant k\leqslant r-1} f_k \theta^k(g_{i_0-k}) \right)}{e_P} + \frac{(i_0-r)v_P(x)}{r} \right) \\ &\geqslant \min_j \min_{i_0-r+1\leqslant k\leqslant r-1} \left(\frac{w_{Q_j}\left(x f_k \theta^k(g_{i_0-k}) \right)}{e_P} + \frac{(i_0-r)v_P(x)}{r} \right) \\ &\geqslant \min_j \min_{i_0-r+1\leqslant k\leqslant r-1} \left(\frac{w_{Q_j}(f_k)}{e_P} + \frac{k v_P(x)}{r} + \frac{w_{Q_{(j+k)\%m_P}}(g_{i_0-k})}{e_P} + \frac{(i_0-k)v_P(x)}{r} \right), \end{aligned}$$

which is greater than $\omega_P(f) + \omega_P(g)$. In the second case, we have

$$\begin{aligned}\omega_P(fg) &\geqslant \min_j \left(\frac{w_{Q_j}\left(\sum_{0\leqslant k\leqslant i_0} f_k \theta^k(g_{i_0-k})\right)}{e_P} + \frac{i_0 v_P(x)}{r} \right) \\ &\geqslant \min_j \min_{0\leqslant k\leqslant i_0} \left(\frac{w_{Q_j}\left(f_k \theta^k(g_{i_0-k})\right)}{e_P} + \frac{i_0 v_P(x)}{r} \right) \\ &\geqslant \min_j \min_{0\leqslant k\leqslant i_0} \left(\frac{w_{Q_j}(f_k)}{e_P} + \frac{k v_P(x)}{r} + \frac{w_{Q_{(j+k)\%m_P}}(g_{i_0-k})}{e_P} + \frac{(i_0-k) v_P(x)}{r} \right),\end{aligned}$$

which is also greater than $\omega_P(f) + \omega_P(g)$. □

Using the surmultiplicativity property of the gauge from Lemma 2.3.2, we can state the following definition.

Definition 2.3.3.
For any place $P \in \mathcal{P}_K$, we define the order Λ_P as

$$\Lambda_P := \{f \in \mathbb{D}_P \mid \omega_P(f) \geqslant 0\}.$$

Definition 2.3.4.
The principal divisor *of a function $f \in \mathbb{D}$ is $(f) = \sum_{Q\in\mathcal{P}_L} \omega_Q(f) Q$.*

Definition 2.3.5 ([BC24, Definition 2.3])**.**
For any $A \in \mathrm{Div}(\mathbb{D})$, the Riemann–Roch space *associated to A is*

$$\Lambda_{\mathbb{D}}(A) := \{f \in \mathbb{D} \mid \omega_Q(f) + A_Q \geqslant 0 \quad \forall Q \in \mathcal{P}_L\}.$$

We denote by $\lambda_{\mathbb{D}}(A)$ its dimension.

The aim of our Riemann–Roch Theorem is to relate $\lambda_{\mathbb{D}}(A)$ to the dimension of another Riemann–Roch space. We now introduce the necessary notions to define the parameters corresponding to this second Riemann–Roch space.

Definition 2.3.6.
The different divisor Δ *of $\mathbb{D}$ (relative to the gauges ω_P) is*

$$\Delta := \sum_{P\in\mathcal{P}_K} \sum_{Q|P} \frac{b_P - 1}{b_P} Q.$$

Definition 2.3.7.
A canonical divisor of $\mathbb{D}$ *is $\mathcal{K} := \mathcal{K}_L + \Delta$ where $\mathcal{K}_L$ is a canonical divisor of L.*

Definition 2.3.8.
The genus *of $\mathbb{D}$ (relative to the gauges ω_P) is the rational number g defined by* $2g - 2 = \deg(\mathcal{K})$.

The genus g does not depend on the choice of $\mathcal{K}$ as $\deg(\mathcal{K}_L)$ does not either.

Definition 2.3.9.
The adjoint algebra *of* $\mathbb{D}$ *is*

$$\mathbb{D}^\star := \frac{L[T;\theta]}{T^r - x^{-1}}.$$

Definition 2.3.10.
We define the adjunction *on* $\mathbb{D}$ *as the following involution:*

$$\begin{array}{ccc} \mathbb{D} & \longrightarrow & \mathbb{D}^\star \\ f = \sum_{i=0}^{r-1} \alpha_i T^i & \mapsto & f^\star = \sum_{i=0}^{r-1} T^{-i}\alpha_i \quad \textit{(with } \alpha_i \in L\textit{).} \end{array}$$

We readily check that $f \mapsto f^\star$ is an anti-isomorphism, i.e., it satisfies $(fg)^\star = g^\star f^\star$, and that $\omega_P(f) = \omega_P(f^\star)$ for any place $P \in \mathcal{P}_K$. We define the maps

$$\begin{array}{ccc} \mathrm{Div}(\mathbb{D}) & \xrightarrow{\pi_i} & \mathrm{Div}(L) \\ \sum_{Q\in\mathcal{P}_L} A_Q Q & \mapsto & \sum_{Q\in\mathcal{P}_L} \lfloor A_Q + i\frac{w_Q(x)}{r} \rfloor Q \end{array} \quad ; \quad \begin{array}{ccc} \mathrm{Div}(\mathbb{D}^\star) & \xrightarrow{\pi_i^\star} & \mathrm{Div}(L) \\ \sum_{Q\in\mathcal{P}_L} A_Q Q & \mapsto & \sum_{Q\in\mathcal{P}_L} \lfloor A_Q - i\frac{w_Q(x)}{r} \rfloor Q \end{array}$$

where $\mathrm{Div}(\mathbb{D}^\star) := \mathrm{Div}(\mathbb{D})$. In the sequel, we shall use π_i and $\pi_i^\star$ in combination with the isomorphisms below as in [BC24, Equation (5)], and write

$$\Lambda_{\mathbb{D}}(A) \simeq \oplus_{i=0}^{r-1} L(\pi_i(A)) \quad \text{and} \quad \Lambda_{\mathbb{D}^\star}(A) \simeq \oplus_{i=0}^{r-1} L(\pi_i^\star(A)), \tag{2.1}$$

where $L(-)$ denotes the classical Riemann–Roch space of L associated to the divisor in argument.

Theorem 2.3.11 (Riemann–Roch Theorem)**.**
For any $A \in \mathrm{Div}(\mathbb{D})$ *and any choice of a canonical divisor* $\mathcal{K}$*, we have*

$$\lambda_{\mathbb{D}}(A) = r \cdot \deg A + r(1-g) + \lambda_{\mathbb{D}^\star}(\mathcal{K} - A).$$

Proof. Applying the classical Riemann–Roch theorem on L [Sti93, Theorem 1.5.15], we have for any choice of $\mathcal{K}_L$ and for any $i \in \{0, \dots, r-1\}$

$$\dim \mathcal{L}\left(\pi_i(A)\right) = \deg \pi_i(A) + 1 - g_L + \dim \mathcal{L}\left(\mathcal{K}_L - \pi_i(A)\right). \tag{2.2}$$

We sum the Equations (2.2) over the indices i and consider each summand of the equation separately. First, using Equation (2.1), we get $\sum_{i=0}^{r-1} \dim \mathcal{L}(\pi_i(A)) = \lambda_{\mathbb{D}}(A)$. Secondly, from [BC24, Lemma 2.5], we have $\sum_{i=0}^{r-1} \deg(\pi_i(A)) = r \deg A - r\frac{\deg(\Delta)}{2}$. Thirdly, since $g_L = g - \frac{\deg \Delta}{2}$, we have $\sum_{i=0}^{r-1}(1-g_L) = r(1-g) + r\frac{\deg(\Delta)}{2}$. Finally, we set $a = A_Q + i\frac{w_Q(x)}{r}$. As a belongs to $\frac{\mathbb{Z}}{b_P}$, we get $\left\lfloor \frac{b_P-1}{b_P} - (a - \lfloor a \rfloor) \right\rfloor = 0$. Now, summing $-\lfloor a \rfloor = \left\lfloor \frac{b_P-1}{b_P} - a \right\rfloor$ over all places $Q \in \mathcal{P}_L$, we get $-\pi_i(A) = \pi_i^\star(\Delta - A)$.

Thus, we get $\mathcal{K}_L - \pi_i(A) = \mathcal{K}_L + \pi_i^\star(\Delta - A)$. As $\mathcal{K}_L$ belongs to $\mathrm{Div}(L) \subset \mathrm{Div}(\mathbb{D})$, we have $\mathcal{K}_L + \pi_i^\star(\Delta - A) = \pi_i^\star(\mathcal{K} - A)$. Hence, using Equation (2.1), we retrieve $\sum_{i=0}^{r-1} \dim \mathcal{L}(\mathcal{K}_L - \pi_i(A)) = \sum_{i=0}^{r-1} \dim \mathcal{L}(\pi_i^\star(\mathcal{K} - A)) = \lambda_{\mathbb{D}^\star}(\mathcal{K} - A)$.

Summing the four terms, we recover the statement. □

2.3.2 Riemann theorem for extended divisors

We now aim at proving an extension of Theorem 2.3.11 allowing for more general divisors, that we call "extended divisors" (see Definition 2.3.12 below).

For this, we fix $\{P_1, \dots, P_s\}$, a finite set of s rational *unramified places* of K indexed by $[s] := \{1, \dots, s\}$ and set $D := P_1 + \cdots + P_s \in \mathrm{Div}(K)$. We assume moreover that all P_i satisfy the hypothesis **(H2-P_i)** of [BC24, Section IV A], i.e., that there exist elements $u_Q \in L_Q^\times$ such that, for all $Q \in \mathcal{P}_L$ above P_i, we have

$$w_Q(u_Q) = \frac{w_Q(x)}{r} \quad \text{and} \quad x = \prod_{Q|P_i} \mathrm{Nr}_{L_Q/K_{P_i}}(u_Q) \in K_{P_i}. \tag{2.3}$$

If we assume F to be finite, a sufficient condition for this to hold is that r divides $v_{P_i}(x)$ (see [BC24, Lemma 6]).

We set $u_{P_i} := (u_Q)_{Q|P_i} \in L_{P_i}$ and recall from [BC24, Section IV A] that there is an isomorphism of K_{P_i}-algebras $\varepsilon_i : \mathbb{D}_{P_i} \to \mathrm{End}_{K_{P_i}}(L_{P_i})$, $f(T) \mapsto f(u_{P_i}\theta)$. Moreover, its restriction to Λ_{P_i} induces a second isomorphism

$$\varepsilon_{i|\Lambda_{P_i}} : \Lambda_{P_i} \xrightarrow{\sim} \mathrm{End}_{\mathcal{O}_{P_i}}(\mathcal{O}_{L,P_i}). \tag{2.4}$$

For $i \in [s]$, we define the *residual algebra* at P by $V_i := \mathcal{O}_{L,P_i}/P_i\mathcal{O}_{L,P_i}$ and set $V_D := \oplus_{i=1}^s V_i$. Since P_i is a rational place, we have $\dim_F V_i = r$ and so $\dim_F V_D = sr$.

We denote by $\mathrm{Div}(\mathbb{D}, D)$ the subgroup of divisors of $\mathbb{D}$ away from D, that is,

$$\mathrm{Div}(\mathbb{D}, D) := \{A \in \mathrm{Div}(\mathbb{D}) \mid A_Q = 0 \quad \forall Q|P_i \quad \forall i \in [s]\}.$$

Definition 2.3.12.
An extended divisor (A, W) *is a pair composed of a divisor* $A \in \mathrm{Div}(\mathbb{D}, D)$ *and a direct sum of* F*-vector subspaces* $W := \bigoplus_{i=1}^s W_i \subset V_D$*, where* $W_i \subset V_i$*.*

Its degree *is* $\deg(A, W) := \deg A - \dim_F(W)$.

We recall the definition of the space of adeles $\mathcal{A}_L(A)$ of L for a divisor $A = \sum_{Q \in \mathcal{P}_L} A_Q Q \in \mathrm{Div}(L)$ as in [Sti93, Definition 1.5.3]:

$$\mathcal{A}_L(A) := \left\{ (y_Q)_Q \in \prod_{Q \in \mathcal{P}_L} L_Q \;\middle|\; w_Q(y_Q) + A_Q \geqslant 0 \quad \forall Q \in \mathcal{P}_L \right\}.$$

We also let $\mathcal{A}_L$ be the union of all $\mathcal{A}_L(A)$. It is also the set of sequences $(y_Q)_Q$ such that $w_Q(y_Q) \geqslant 0$ for almost all Q.

Definition 2.3.13.
For a divisor $A = \sum_{Q \in \mathcal{P}_L} A_Q Q \in \mathrm{Div}(\mathbb{D})$, we define

$$\mathcal{A}_{\mathbb{D}}(A) := \left\{ (\alpha_P)_P \in \prod_{P \in \mathcal{P}_K} \mathbb{D}_P \;\middle|\; \omega_Q(\alpha_P) + A_Q \geqslant 0 \quad \forall P \quad \forall Q | P \right\}$$

and let $\mathcal{A}_{\mathbb{D}}$ be the union of all $\mathcal{A}_{\mathbb{D}}(A)$.

Note that by definition, we have $\Lambda_{\mathbb{D}}(A) = \mathcal{A}_{\mathbb{D}}(A) \cap \mathbb{D}$.

Lemma 2.3.14.
We have the following isomorphism of $\mathcal{A}_K$-algebras

$$\mathcal{A}_{\mathbb{D}} \simeq \bigoplus_{i=0}^{r-1} \mathcal{A}_L T^i.$$

Proof. The support of (x) in $\mathcal{P}_L$ being finite, we conclude using the isomorphism $L \otimes_K K_P \simeq \prod_{Q|P} L_Q$. □

In the sequel, we will use that L (resp. $\mathbb{D}$) injects diagonally in $\mathcal{A}_L$ (resp. $\mathcal{A}_{\mathbb{D}}$).

Lemma 2.3.15.
Let $A \in \mathrm{Div}(\mathbb{D})$. We have the following isomorphisms of F-vector spaces

$$\mathcal{A}_{\mathbb{D}}(A) \simeq \oplus_{i=0}^{r-1} \mathcal{A}_L(\pi_i(A)) \quad \textit{and} \quad \frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}} \simeq \oplus_{i=0}^{r-1} \frac{\mathcal{A}_L}{\mathcal{A}_L(\pi_i(A)) + L}.$$

Proof. The first isomorphism is analogous to the isomorphism of Equation (2.1). The isomorphism of Lemma 2.3.14 and the isomorphism $\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D} \simeq \oplus_{i=0}^{r-1} (\mathcal{A}_L(\pi_i(A)) + L)$ together with the natural injection $\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D} \hookrightarrow \mathcal{A}_{\mathbb{D}}$ induced by the diagonal embedding of $\mathbb{D}$ in $\mathcal{A}_{\mathbb{D}}$ allow us to build the quotients and prove the second isomorphism. □

We recall the definition of the evaluation map at $P_i \in \mathcal{P}_K$ for any divisor $A \in \mathrm{Div}(\mathbb{D}, D)$ as the following composition of morphisms according to [BC24, Definition 3.3]:

$$\bar{\varepsilon}_i : \Lambda_{\mathbb{D}}(A) \hookrightarrow \Lambda_{P_i} \xrightarrow{\varepsilon_i}_{\sim} \mathrm{End}_{\mathcal{O}_{P_i}}(\mathcal{O}_{L,P_i}) \twoheadrightarrow \mathrm{End}_F(V_i), \tag{2.5}$$

where the first map is the inclusion and the last one is the projection.

Definition 2.3.16.
Let (A, W) be an extended divisor. We define:

$$\mathcal{A}_{\mathbb{D}}(A, W) := \left\{ \alpha \in \mathcal{A}_{\mathbb{D}}(A) \mid \bar{\varepsilon}_i(\alpha_{P_i})_{|W_i} = 0 \quad \forall i \in [s] \right\},$$
$$\Lambda_{\mathbb{D}}(A, W) := \mathcal{A}_{\mathbb{D}}(A, W) \cap \mathbb{D}.$$

We denote by $\lambda_{\mathbb{D}}(A,W)$ *the dimension of* $\Lambda_{\mathbb{D}}(A,W)$.

We define the conorm of a divisor as follows:

$$\begin{array}{rccc} \mathrm{CoNr}: & \mathrm{Div}(K) & \to & \mathrm{Div}(L) \subset \mathrm{Div}(\mathbb{D}) \\ & P & \mapsto & e_P \sum_{Q|P} Q \end{array}.$$

Lemma 2.3.17.
For $A \in \mathrm{Div}(\mathbb{D}, D)$, *we have* $\mathcal{A}_{\mathbb{D}}(A, V_D) = \mathcal{A}_{\mathbb{D}}(A - \mathrm{CoNr}(D))$.

Proof. By definition, the kernel of $\varepsilon_i : \Lambda_{P_i} \xrightarrow{\varepsilon_i}{\sim} \mathrm{End}_{\mathcal{O}_{P_i}}(\mathcal{O}_{L,P_i}) \twoheadrightarrow \mathrm{End}_F(V_i)$ is the inverse image of $\mathrm{Hom}_{\mathcal{O}_{P_i}}(\mathcal{O}_{L,P_i}, P_i\mathcal{O}_{L,P_i})$ by ε_i, which is $\mathcal{A}_{\mathbb{D}}(A - \mathrm{CoNr}(D))_{P_i}$. □

Definition 2.3.18.
The index of speciality *of an extended divisor* (A,W) *is*

$$i(A,W) := \lambda_{\mathbb{D}}(A,W) - r\deg(A,W) - r(1-g).$$

Proposition 2.3.19.
For any extended divisor (A,W), *we have*

$$i(A,W) = \dim_F \left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A,W) + \mathbb{D}} \right).$$

Proof. We have an isomorphism

$$\begin{array}{rccc} \oplus_{i=0}^{r-1} \mathrm{Hom}\left(\frac{\mathcal{A}_L}{\mathcal{A}_L(\pi_i(A))+L}, F \right) & \tilde{\to} & \mathrm{Hom}\left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A)+\mathbb{D}}, F \right) \\ (\nu_0, \ldots, \nu_{r-1}) & \mapsto & (\alpha \mapsto \sum_{i=0}^{r-1} \nu_i(\alpha_i)) \end{array}.$$

Indeed, the map is obviously injective and it is also surjective, a preimage of $\nu \in \mathrm{Hom}\left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A)+\mathbb{D}}, F \right)$ being given by the linear forms $\nu_i : \alpha_i \mapsto \nu((0,\ldots,\alpha_i,\ldots,0))$. Now, using this isomorphism and the Riemann–Roch Theorem 2.3.11 applied to $\Lambda_{\mathbb{D}}(A)$, we get $i(A,0) = \dim\left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A)+\mathbb{D}} \right)$. Thus, we have

$$\dim\left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A,W) + \mathbb{D}} \right) = i(A,0) + \dim\left(\frac{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}}{\mathcal{A}_{\mathbb{D}}(A,W) + \mathbb{D}} \right). \tag{2.6}$$

In order to relate the dimension of the latter quotient to $i(A,W)$, we consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda_{\mathbb{D}}(A,W) & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A,W) & \longrightarrow & \frac{\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}}{\mathbb{D}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Lambda_{\mathbb{D}}(A) & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A) & \longrightarrow & \frac{\mathcal{A}_{\mathbb{D}}(A)+\mathbb{D}}{\mathbb{D}} & \longrightarrow & 0 \end{array}.$$

Applying the snake lemma to it, we get the following exact sequence of cokernels

$$0 \longrightarrow \frac{\Lambda_{\mathbb{D}}(A)}{\Lambda_{\mathbb{D}}(A,W)} \longrightarrow \frac{\mathcal{A}_{\mathbb{D}}(A)}{\mathcal{A}_{\mathbb{D}}(A,W)} \longrightarrow \frac{\mathcal{A}_{\mathbb{D}}(A)+\mathbb{D}}{\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}} \longrightarrow 0.$$

Hence

$$\dim\left(\frac{\mathcal{A}_{\mathbb{D}}(A)+\mathbb{D}}{\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}}\right) = \dim\left(\frac{\mathcal{A}_{\mathbb{D}}(A)}{\mathcal{A}_{\mathbb{D}}(A,W)}\right) - \lambda_{\mathbb{D}}(A) + \lambda_{\mathbb{D}}(A,W). \tag{2.7}$$

Finally, we observe that, for any $i \in [s]$, we have a second commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A,V_i)_{P_i} & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A)_{P_i} & \xrightarrow{\bar{\varepsilon}_i} & \mathrm{Hom}_F(V_i,V_i) & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A,V_i)_{P_i} & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A,W_i)_{P_i} & \xrightarrow{\bar{\varepsilon}_i} & \mathrm{Hom}_F(V_i/W_i,V_i) & \longrightarrow & 0
\end{array}$$

from which we derive that $\mathcal{A}_{\mathbb{D}}(A)_{P_i}/\mathcal{A}_{\mathbb{D}}(A,W_i)_{P_i} \simeq \mathrm{Hom}_F(W_i,V_i)$. Therefore $\mathcal{A}_{\mathbb{D}}(A)/\mathcal{A}_{\mathbb{D}}(A,W)$ is isomorphic to $\bigoplus_{i\in[s]} \mathrm{Hom}_F(W_i,V_i)$ and thus has dimension $r\dim(W)$. Combining with Equations (2.6) and (2.7), we get the desired result. □

Theorem 2.3.20.
For any extended divisor (A,W), we have

$$\lambda_{\mathbb{D}}(A,W) = r\deg(A,W) + r(1-g) + \dim\left(\mathcal{A}_{\mathbb{D}}/\left(\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}\right)\right).$$

Moreover, if $\deg(A,W) < 0$*, then* $\lambda_{\mathbb{D}}(A,W) = 0$.

Proof. The first equality results from Proposition 2.3.19. The second assertion is a consequence of [BC24, Theorem 3.5]. □

2.3.3 Differentials and residues

In order to prove the Riemann–Roch Theorem for extended divisors, we now need to relate the quotient $\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D})$ to an actual Riemann–Roch space. As in the classical case, we will use as an intermediate a certain space of differential forms over $\mathbb{D}$.

Definition
In the sequel, we denote by Ω_K (resp. Ω_L) the module of differentials of K (resp. L) as defined in [Sha13, Chapter 5]. For any differential $\eta \in \Omega_K$, we denote by $(\eta)_K$, (resp. $(\eta)_L$) the divisor of η viewed as a differential of Ω_K (resp. Ω_L). They satisfy the Riemann–Hurwitz relation $(\eta)_L = \mathrm{CoNr}((\eta)_K) + \mathrm{Diff}(L/K)$ as stated in [Sti93, Theorem 3.4.6], where $\mathrm{Diff}(L/K)$ is the different divisor of L/K as defined in [Sti93, Definition 3.4.3].

Definition 2.3.21.
The left module of differentials *of* $\mathbb{D}$ *is defined by* $\Omega_{\mathbb{D}} := \mathbb{D} \otimes_K \Omega_K$.

We recall that Ω_K is a one-dimensional vector space over K [Sti93, Proposition 1.5.9]. Henceforth, any element $\nu \in \Omega_{\mathbb{D}}$ is of the form $\nu = f \otimes \eta$ for $f \in \mathbb{D}$ and $\eta \in \Omega_K$.

Definition 2.3.22.
Let $\nu = f \otimes \eta \in \Omega_{\mathbb{D}}$ *with* $f \in \mathbb{D}$ *and* $\eta \in \Omega_K$. *The* principal divisor *of* ν *is*

$$(\nu)_{\mathbb{D}} := (f) + (\eta)_L + \Delta.$$

Proposition 2.3.23.
The divisor $(\nu)_{\mathbb{D}}$ *does not depend on the choice of the decomposition.*

Proof. Let $\nu = f' \otimes \eta'$ be another decomposition. Then $\eta' = u\eta$ and $f = uf'$ for some nonzero $u \in K$. As for any $v \in K$, $g \in \mathbb{D}$, and $Q \in \mathcal{P}_L$, we have $\omega_Q(vg) = \omega_Q(gv) = w_Q(v) + \omega_Q(g)$, we obtain $(f) + (\eta)_L = (f') + (u) + (\eta)_L = (f') + (\eta')_L$. □

Definition 2.3.24.
For any $A \in \mathrm{Div}(\mathbb{D})$, *we set* $\Omega_{\mathbb{D}}(A) := \big\{\nu \in \Omega_{\mathbb{D}} \mid (\nu)_{\mathbb{D}} \geqslant A\big\}$.

Definition 2.3.25.
Let $i \in [s]$ *and let* $t_i \in K$ *be a uniformizer at* P_i. *Let* $\nu \in \Omega_{\mathbb{D}}$ *and write* $\nu = f\frac{dt_i}{t_i}$ *with* $f \in \mathbb{D}$. *If* $\omega_{P_i}(f) \geqslant 0$, *we define the* residue endomorphism *of* ν *at* P_i *by*

$$\mathcal{R}\mathrm{es}_{P_i}(\nu) := \bar{\varepsilon}_i(f)$$

where $\bar{\varepsilon}_i$ *is defined in Equation* (2.5).

Proposition 2.3.26.
The residue endomorphism $\mathcal{R}\mathrm{es}_P(\nu)$ *does not depend on the choice of the decomposition of* ν.

Proof. Let t'_P be another uniformizer of K at P and write $\nu = f'\frac{dt'_P}{t'_P}$ with $f' \in \mathbb{D}$. We then have $f = f'\frac{dt'_P}{dt_P}\frac{t_P}{t'_P}$ and so $\omega_P(f') = \omega_P(f)$. Moreover $\varepsilon_P(f) = \varepsilon_P\left(f'\frac{dt'_P}{dt_P}\frac{t_P}{t'_P}\right) = \varepsilon_P(f')$. Indeed, writing $t'_P = \tau_0 t_P(1 + t_P(\tau_1 + t_P\rho))$ with $\rho \in \mathcal{O}_P$, $\tau_1 \in F$ and $\tau_0 \in F^\times$, we compute $\frac{dt'_P}{dt_P} \equiv \frac{t'_P}{t_P} \equiv \tau_0 \bmod P$. Finally, by definition, $v_P(t'_P) = v_P(t_P) = 1$. This ensures that $\tau_0 \neq 0 \bmod P$. □

The residue formula

We observe that the residue endomorphisms at different places do not live in the same ambient space. Therefore, adding them does not make sense and we then cannot hope

that their sum vanishes. However, this vanishing property does hold after taking traces, as we show now.

We first recall the notion of reduced trace on $\mathbb{D}$.

Definition 2.3.27.
The reduced trace *of an element f of $\mathbb{D}$ (resp. of $\mathbb{D}_P$), denoted by $\mathrm{Trd}(f)$, is the trace of left-L (resp. left-L_P) linear endomorphism of $\mathbb{D}$ (resp. $\mathbb{D}_P$) given by right multiplication by f.*

Lemma 2.3.28.
Let $P \in \mathcal{P}_K$ and let $f = f_0 + f_1 T + \cdots + f_{r-1}T^{r-1} \in \mathbb{D}_P$ with $f_j \in L_P$. Then $\mathrm{Trd}(f) = \mathrm{Tr}_{L_P/K_P}(f_0)$.

If moreover $P = P_i$ for some $i \in [s]$, then $\mathrm{Trd}(f) = \mathrm{Tr}_{K_{P_i}}(\varepsilon_i(f))$ (where we recall that ε_i is the morphism defined at the beginning of Subsection 2.3.2).

Proof. It is similar to the proof of [BC24, Lemma 2]. □

Lemma 2.3.29.
Let $P \in \mathcal{P}_K$, and $f \in \mathbb{D}_P$. We have $v_P(\mathrm{Trd}(f)) \geqslant \omega_P(f)$.

Proof. Let $f = f_0 + f_1 T + \cdots + f_{r-1}T^{r-1} \in \mathbb{D}_P$ with all $f_i \in L_P$. By Lemma 2.3.28 we have $\mathrm{Trd}(f) = \mathrm{Tr}_{L_P/K_P}(f_0)$. We conclude by the ultrametric inequality of ω_P that $v_P(\mathrm{Trd}(f)) = \omega_P\left(\mathrm{Tr}_{L_P/K_P}(f_0)\right) \geqslant \min_{0\leqslant i<r}(\omega_P(\theta^i(f_0))) = \omega_P(f_0) \geqslant \omega_P(f)$. □

Definition 2.3.30.
We define the reduced trace *on $\Omega_{\mathbb{D}}$ by*

$$\begin{array}{rccc} \mathrm{Trd}: & \Omega_{\mathbb{D}} & \longrightarrow & \Omega_K \\ & f \otimes \eta & \mapsto & \mathrm{Trd}(f)\cdot\eta \end{array}$$

For $\nu \in \Omega_{\mathbb{D}}$, we define the reduced residue *of ν at a place P by*

$$\mathrm{Resrd}_P(\nu) := \mathrm{Tr}_{\kappa(P)/F}(\mathrm{Res}_P(\mathrm{Trd}(\nu))),$$

where the right-hand side is the trace of the residual field $\kappa(P)$ of K at the place P of the classical residue of $\mathrm{Trd}(\nu) \in \Omega_K$ at the place P.

Proposition 2.3.31.
Let $i \in [s]$. Then, for any $\nu \in \Omega_{\mathbb{D}}$ such that $\mathcal{R}\mathrm{es}_{P_i}(\nu)$ is defined, we have $\mathrm{Resrd}_{P_i}(\nu) = \mathrm{Tr}_F(\mathcal{R}\mathrm{es}_{P_i}(\nu))$.

Proof. We write $\nu = f\frac{dt_i}{t_i}$ where t_i is a uniformizer at P_i, so that $\omega_{P_i}(f) \geqslant 0$ and $\mathcal{R}\mathrm{es}_{P_i}(\nu) = \bar{\varepsilon}_i(f)$. From Lemma 2.3.29, we deduce $v_{P_i}(\mathrm{Trd}(f)) \geqslant 0$ and then

$$\mathrm{Resrd}_{P_i}(\nu) = \mathrm{Res}_{P_i}\left(\mathrm{Trd}(f)\tfrac{dt_i}{t_i}\right) = \mathrm{Trd}(f) \bmod P_i.$$

On the other hand, Lemma 2.3.28 ensures that $\mathrm{Trd}(f) = \mathrm{Tr}_{K_{P_i}}(\varepsilon_i(f))$. Reducing modulo P_i, we obtain $\mathrm{Trd}(f) \bmod P_i = \mathrm{Tr}_F(\bar{\varepsilon}_i(f)) = \mathrm{Tr}_F(\mathcal{R}\mathrm{es}_{P_i}(\nu))$. □

Theorem 2.3.32 (Residue Theorem)**.**
For $\nu \in \Omega_{\mathbb{D}}$, we have

$$\sum_{P \in \mathcal{P}_K} \mathrm{Resrd}_P(\nu) = 0.$$

Proof. We apply the residue theorem as stated in [Sha13, Theorem 3.27] to $\mathrm{Trd}(\nu) \in \Omega_K$ and conclude. □

Riemann–Roch spaces

For all $i \in [s]$, we endow the space V_i with the bilinear form

$$\begin{array}{rccc} \langle -,- \rangle : & V_i \times V_i & \to & F \\ & (v_i, w_i) & \mapsto & \mathrm{Tr}_{V_i/F}(v_i w_i). \end{array}$$

It is nondegenerate given that the place P_i is supposed to be unramified in the extension L/K. If W_i is a vector subspace of V_i, we write $W_i^\perp$ for its orthogonal and, similarly, if $W = \bigoplus_{i=1}^s W_i$ is a subspace of V_D, we define $W^\perp = \bigoplus_{i=1}^s W_i^\perp$.

We now introduce Riemann–Roch spaces of differential forms: if (A, W) is an extended divisor, we set

$$\Omega_{\mathbb{D}}(A, W) := \big\{ \nu \in \Omega_{\mathbb{D}}(A - \mathrm{CoNr}(D)) \mid \mathcal{R}\mathrm{es}_{P_i}(\nu)_{|W_i^\perp} = 0,\ \forall i \in [s] \big\}.$$

It follows from Lemma 2.3.17 that $\Omega_{\mathbb{D}}(A, 0) = \Omega_{\mathbb{D}}(A)$ for any $A \in \mathrm{Div}(\mathbb{D}, D)$.

It turns out that Riemann–Roch spaces of differential forms are related to classical Riemann–Roch spaces. In order to make this relationship explicit, we choose $t_D \in K$ such that $v_{P_i}(t_D) = 1$ for all $i \in [s]$ and set

$$\mathcal{K} := \left(\tfrac{dt_D}{t_D}\right)_{\mathbb{D}} = \left(\tfrac{dt_D}{t_D}\right)_L + \Delta. \tag{2.8}$$

It is a canonical divisor of $\mathbb{D}$ in the sense of Definition 2.3.7.

Definition 2.3.33.
For an extended divisor (A, W), we set $(A, W)^\star := (\mathcal{K} + \mathrm{CoNr}(D) - A, W^\perp)$.

Theorem 2.3.34.
For any extended divisor (A, W), we have the isomorphism:

$$\begin{array}{rcl} \Lambda_{\mathbb{D}}((A, W)^\star) & \xrightarrow{\sim} & \Omega_{\mathbb{D}}(A, W) \\ f & \mapsto & f\frac{dt_D}{t_D} \end{array}$$

Proof. It follows directly from the definitions. □

Serre duality and Riemann–Roch Theorem

The last step of the proof of the Riemann–Roch Theorem consists of relating the adelic quotient $\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D})$ to the space of differential forms $\Omega_{\mathbb{D}^\star}(A,W)$, where $\mathbb{D}^\star$ is the adjoint algebra as introduced in Definition 2.3.9.

We recall from Definition 2.3.10 that we have already introduced an adjunction $\mathbb{D} \to \mathbb{D}^\star$, $f \mapsto f^\star$ at the level of Ore polynomials. It naturally extends to differential forms as follows:

$$\begin{array}{ccc} \Omega_{\mathbb{D}} & \longrightarrow & \Omega_{\mathbb{D}^\star} \\ \nu = f \otimes \eta & \mapsto & \nu^\star := f^\star \otimes \eta \end{array}$$

with, as usual, $f \in \mathbb{D}$ and $\eta \in \Omega_K$. Besides, for all $i \in [s]$, the algebra $\mathrm{End}_F(V_i)$ is also endowed with an adjunction $\varphi_i \mapsto \varphi_i^\star$ defined by the standard property

$$\langle \varphi_i(v_i), w_i \rangle = \langle v_i, \varphi_i^\star(w_i) \rangle \qquad (v_i, w_i \in V_i).$$

We recall the classical formulas $\ker(\varphi_i^\star) = \mathrm{im}(\varphi_i)^\perp$ and $\mathrm{im}(\varphi_i^\star) = \ker(\varphi_i)^\perp$.

If φ is a tuple $(\varphi_1, \ldots, \varphi_s)$, we will often write $\varphi^\star = (\varphi_1^\star, \ldots, \varphi_s^\star)$ for simplicity.

Lemma 2.3.35.
Let $A \in \mathrm{Div}(\mathbb{D}, D)$ and let $f \in \mathbb{D}$. If $i \in [s]$ is such that $\omega_{P_i}(f) \geqslant 0$, then

$$\bar{\varepsilon}_i(f)^\star = \bar{\varepsilon}_i(f^\star) \quad \textit{and} \quad \mathrm{Resrd}_{P_i}\left(f \tfrac{dt_D}{t_D}\right)^\star = \mathrm{Resrd}_{P_i}\left(f^\star \tfrac{dt_D}{t_D}\right)$$

where, in a slight abuse of notation, we continue to write $\bar{\varepsilon}_i$ for the evaluation morphism on $\mathbb{D}^\star$.

Proof. We reuse the notation u_{P_i} introduced in Equation (2.3). By linearity, it is enough to check that $\langle \bar{\varepsilon}_i(f^\star)(v_i), w_i \rangle = \langle v_i, \bar{\varepsilon}_i(f)(w_i) \rangle$ for $f = f_j T^j$ and $v_i, w_i \in V_i$. Setting $\mathrm{Nr}_{a,b}(u_P) := \prod_{k=a}^{b-1} \theta^k(u_P)$, we compute

$$\bar{\varepsilon}_i(f^\star) = \bar{\varepsilon}_i\left(\frac{T^{r-j}}{x^{-1}} f_j\right) = \frac{\mathrm{Nr}_{0,r-j}(u_P^{-1})\theta^{r-j}(f_j)}{\mathrm{Nr}_{0,r}(u_P^{-1})}\theta^{r-j} = \frac{\theta^{r-j}(f_j)}{\mathrm{Nr}_{r-j,r}(u_P^{-1})}\theta^{r-j}$$

as changing $x \mapsto x^{-1}$ in $\mathbb{D}^\star$ induces the change $u_{P_i} \mapsto u_{P_i}^{-1}$. Using $\theta^j(\mathrm{Nr}_{r-j,r}(u_{P_i})) = \mathrm{Nr}_{0,j}(u_{P_i})$, we get

$$\begin{aligned} \mathrm{Tr}_{V_i/F}\left(\frac{\theta^{r-j}(f_j)}{\mathrm{Nr}_{r-j,r}(u_{P_i}^{-1})}\theta^{r-j}(v_i)w_i\right) &= \sum_{k=0}^{r-1} \theta^k\left(\frac{\theta^{r-j}(f_j)}{\mathrm{Nr}_{r-j,r}(u_{P_i}^{-1})}\theta^{r-j}(v_i)w_i\right) \\ &= \mathrm{Tr}_{V_i/F}(v_i f_j \,\mathrm{Nr}_{0,j}(u_{P_i})\theta^j(w_i)), \end{aligned}$$

which concludes the proof. □

Theorem 2.3.36.
For any extended divisor (A, W), the F-bilinear form

$$\begin{array}{rccl} \Phi : \mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}) \times \Omega_{\mathbb{D}^\star}(A,W) & \longrightarrow & F \\ (\alpha,\nu) & \mapsto & \displaystyle\sum_{P\in\mathcal{P}_K} \operatorname{Resrd}_P(\alpha_P\nu^\star) \end{array}$$

is a perfect pairing.

Before diving into the proof, we show that this pairing is well-defined.

Lemma 2.3.37.
For $\nu \in \Omega_{\mathbb{D}^\star}(A,W)$, $\alpha \in \mathcal{A}_{\mathbb{D}}(A,W)$ and $a \in \mathbb{D}$, we have $\Phi(\alpha + a, \nu) = 0$.

Proof. As we have $a\nu^\star \in \Omega_{\mathbb{D}}$, we get $\Phi(a,\nu) = 0$ by applying Theorem 2.3.32 to $a\nu^\star$.

It remains to prove $\Phi(\alpha,\nu) = 0$. Let $P \in \mathcal{P}_K$. We first assume that P is one of the P_i, $i \in [s]$. Then $\mathcal{R}\mathrm{es}_{P_i}(\alpha_P\nu^\star)$ is defined and

$$\mathcal{R}\mathrm{es}_{P_i}(\alpha_P\nu^\star) = \bar{\varepsilon}_i(\alpha_P) \circ \mathcal{R}\mathrm{es}_{P_i}(\nu^\star) = \bar{\varepsilon}_i(\alpha_P) \circ \mathcal{R}\mathrm{es}_{P_i}(\nu)^\star.$$

Moreover, we know that $\bar{\varepsilon}_i(\alpha_P)$ and $\mathcal{R}\mathrm{es}_{P_i}(\nu)$ vanish on W_i and $W_i^\perp$ respectively. In other words $\operatorname{im} \mathcal{R}\mathrm{es}_{P_i}(\nu)^\star = \big(\ker \mathcal{R}\mathrm{es}_{P_i}(\nu)\big)^\perp \subset W_i \subset \ker \bar{\varepsilon}_i(\alpha_P)$. We deduce that $\mathcal{R}\mathrm{es}_{P_i}(\alpha_P\nu^\star)$ vanishes and so does its trace, i.e., $\operatorname{Resrd}_{P_i}(\alpha_P\nu^\star) = 0$.

We now consider the case where P is not an evaluation place. We write $\nu = f \otimes \eta$ where $f \in \mathbb{D}^\star$ and $\eta \in \Omega_K$ is chosen such that it has neither zero nor pole at P. We write $\alpha_P = \sum_{j=0}^{r-1} \alpha_j T^j$ (with $\alpha_j \in L_P$) and $f = \sum_{j=0}^{r-1} f_j T^j$ (with $f_j \in L$). It follows from Lemma 2.3.28 that

$$\operatorname{Resrd}_P(\alpha_P\nu^\star) = \operatorname{Tr}_{\kappa(P)/F}\big(\operatorname{Res}_P\big(\operatorname{Trd}(\alpha_P f^\star)\cdot\eta\big)\big) = \sum_{j=0}^{r-1} \operatorname{Tr}_{\kappa(P)/F}\big(\operatorname{Res}_P\big(\operatorname{Tr}_{L_P/K_P}(\alpha_j f_j)\cdot\eta\big)\big).$$

On the other hand, we deduce from the definition of the Riemann–Roch spaces that, for any place $Q \mid P$, we have the estimations

$$\begin{aligned} w_Q(\alpha_j) &\geqslant -A_Q - \tfrac{j}{r} w_Q(x) \\ w_Q(f_j) + w_Q(\mathrm{Diff}(L/K)) &\geqslant A_Q + \tfrac{j}{r} w_Q(x) - \tfrac{b_P-1}{b_P} \end{aligned}$$

where $\mathrm{Diff}(L/K)$ denotes the different of L/K. Adding the two inequalities and replacing the right hand sides by their ceilings, we find that $w_Q(\alpha_j f_j) \geqslant -w_Q(\mathrm{Diff}(L/K))$, as $\lceil -\frac{b_P-1}{b_P} \rceil \geqslant 0$. Hence, by definition of the different, $\operatorname{Tr}_{L_P/K_P}(\alpha_j f_j)$ has no pole at P. Therefore the residue at P of $\operatorname{Tr}_{L_P/K_P}(\alpha_j f_j)\cdot\eta$ vanishes, and we conclude that $\operatorname{Resrd}_P(\alpha_P\nu^\star) = 0$. □

Proof of Theorem 2.3.36. By Lemma 2.3.37 the pairing Φ is well-defined. The proof

of its non-degeneracy breaks down into two parts, proving the injectivity and then the surjectivity of the morphism

$$\begin{array}{rccl} \psi: & \Omega_{\mathbb{D}^\star}(A,W) & \to & \mathrm{Hom}\left(\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}),F\right) \\ & \nu & \mapsto & \big(\alpha \mapsto \Phi(\alpha,\nu)\big) \end{array}.$$

Injectivity. Let P be a fixed evaluation place. Since P is unramified, we can find an element $a \in \mathcal{O}_{L,P}$ such that $\mathrm{Tr}_{\mathcal{O}_{L,P}/\mathcal{O}_P}(a) \equiv 1 \pmod{P}$. We consider the adele $\beta \in \mathcal{A}_{\mathbb{D}}$ with coordinate a at P and 0 elsewhere. Let $\nu = f \otimes \frac{dt_P}{t_P} \in \Omega_{\mathbb{D}^\star}(A,W)$, $\nu \neq 0$. Since $\mathbb{D}^\star$ is a division algebra, f is invertible and we can form the adele $\alpha = \beta \cdot (f^{-1})^\star \in \mathcal{A}_{\mathbb{D}}$. Then

$$\Phi(\alpha,\nu) = \mathrm{Resrd}_P\left(a\tfrac{dt_P}{t_P}\right) = \mathrm{Tr}_{L_P/K_P}(a) \bmod P = 1$$

and injectivity follows.

Surjectivity. By injectivity of ψ and Theorem 2.3.34, we have

$$\lambda_{\mathbb{D}^\star}((A,W)^\star) \leqslant i(A,W) = \lambda_{\mathbb{D}}(A,W) - (r\deg(A,W) + r(1-g)).$$

Besides, since $\mathcal{K} + \mathrm{CoNr}(D) - A \in \mathrm{Div}(\mathbb{D}^\star, D)$, we can apply the previous inequality to the extended divisor $(A,W)^\star$. It yields

$$\begin{aligned} \lambda_{\mathbb{D}}(A,W) &\leqslant \lambda_{\mathbb{D}^\star}((A,W)^\star) - (r\deg((A,W)^\star) + r(1-g)) \\ &\leqslant \lambda_{\mathbb{D}}(A,W) - r\deg(A,W) - r\deg((A,W)^\star) + r(2g-2) = \lambda_{\mathbb{D}}(A,W) \end{aligned}$$

as $\deg(A,W) + \deg((A,W)^\star) = 2g-2$. Thus, all inequalities have to be equalities and we deduce $\lambda_{\mathbb{D}^\star}((A,W)^\star) = i(A,W)$. We conclude by invoking Theorem 2.3.34. □

Finally, we can state and prove our Riemann–Roch Theorem for extended divisors.

Theorem 2.3.38 (Riemann–Roch Theorem)**.**
For any extended divisor (A,W), we have

$$\lambda_{\mathbb{D}}(A,W) = r\deg(A,W) + r(1-g) + \lambda_{\mathbb{D}^\star}((A,W)^\star).$$

Proof. It results by combining Theorem 2.3.20, Theorem 2.3.34 and Theorem 2.3.36. □

2.4 Application to linearized Algebraic Geometry codes

In what follows, we consider the same setting as in Section 2.3 and refer to the introduction of that section for the notation. In particular, the field F can still be

arbitrary while, for applications to coding theory, the cases of most interest are finite fields $F = \mathbb{F}_q$.

To start with, we recall the construction of linearized AG codes as settled in [BC24]. As in Subsection 2.3.2, we fix a finite set of unramified places $\{P_1, \dots, P_s\} \subset \mathcal{P}_K$ satisfying the hypothesis **(H2-P_i)** and we let V_i denote the residue algebra of L at P_i. The ambient space in which our codes live is

$$\mathcal{H} := \operatorname{End}_F(V_1) \times \cdots \times \operatorname{End}_F(V_s).$$

By choosing F-bases of the V_i, $\mathcal{H}$ becomes isomorphic to the s-th power of a matrix algebra, namely $(F^{r\times r})^s$. However, in the algebraic context of this article, it will be convenient to work with endomorphisms, given that the evaluation morphisms $\bar{\varepsilon}_i$ (see Equation (2.5)) naturally produce endomorphisms. In any case, $\mathcal{H}$ is a vector space of dimension sr^2 over F and we endow it with the sum-rank metric defined by

$$d_{\mathrm{srk}}(\varphi, \psi) = w_{\mathrm{srk}}(\varphi - \psi) \quad \text{with} \quad w_{\mathrm{srk}}(\varphi_1, \dots, \varphi_s) = \sum_{i=1}^{s} \operatorname{rank}(\varphi_i).$$

We set $D := P_1 + \cdots + P_s \in \operatorname{Div}(K)$.

Definition 2.4.1.
Let $A \in \operatorname{Div}(\mathbb{D}, D)$. The linearized Algebraic Geometry *code associated to A and D is the image of*

$$\bar{\varepsilon}_D : \Lambda(A) \longrightarrow \mathcal{H}, \quad f \mapsto \big(\bar{\varepsilon}_1(f), \dots, \bar{\varepsilon}_s(f)\big).$$

It is denoted by $\mathrm{LAG}_{\mathbb{D}}(A, D)$.

The aim of this section is to apply the theory we developed previously to characterize the duals of linearized AG codes and to decode them. In the special case where $K = F(t)$, $L = F'(t)$ for a finite cyclic extension F'/F and A is a multiple of the point at infinity, removing the hypothesis on F being algebraically closed in L, would make of the code $\mathrm{LAG}_{\mathbb{D}}(A, D)$ a linearized Reed–Solomon code [MP18a], for which the duals have already been described in [CD23] and a decoding algorithm is known [MPK19]. Another corner case corresponds to the situation where the extension L/K is trivial: in this case, $\mathrm{LAG}_{\mathbb{D}}(A, D)$ is nothing but a classical AG code, and our results extend the classical ones.

We also mention that, as it was pointed out in [BC25, Section IV], linearized Reed–Muller codes [BC25] can be embedded in larger linearized AG codes and hence can be decoded using our decoding algorithm.

2.4.1 Duality

We recall that each V_i is endowed with a nondegenerate bilinear pairing (see Subsection 2.3.3), which allows us to define an adjunction $\varphi_i \mapsto \varphi_i^\star$ on $\mathrm{End}_F(V_i)$. We use it to endow $\mathcal{H}$ with another nondegenerate bilinear pairing defined by:

$$\begin{array}{ccc} \mathcal{H} \times \mathcal{H} & \longrightarrow & F \\ (\varphi, \psi) & \mapsto & \langle \varphi, \psi \rangle := \sum_{i=1}^{s} \mathrm{Tr}_F\left(\varphi_i \circ \psi_i^\star\right) \end{array},$$

where φ_i and ψ_i are the coordinates of φ and ψ respectively. We define the dual of a linearized AG code with respect to this pairing, as follows:

$$\mathrm{LAG}_{\mathbb{D}}(A, D)^\perp = \left\{\psi \in \mathcal{H} \;\middle|\; \langle \varphi, \psi \rangle = 0,\ \forall \varphi \in \mathrm{LAG}_{\mathbb{D}}(A, D)\right\}.$$

We will now apply the duality theory developed in Subsection 2.3.3 to define linearized Differential (LD) codes and subsequently show that they are the duals of linearized AG codes.

Definition 2.4.2.
The linearized Differential code *associated to the divisors A and D, denoted by $\mathrm{LD}_{\mathbb{D}^\star}(A, D)$, is the image of the following map:*

$$\begin{array}{ccc} \Omega_{\mathbb{D}^\star}(A, V_D) & \longrightarrow & \mathcal{H} \\ \nu & \mapsto & \left(\mathcal{R}\mathrm{es}_{P_1}(\nu), \ldots, \mathcal{R}\mathrm{es}_{P_s}(\nu)\right) \end{array}$$

where $\mathcal{R}$es is the endomorphism residue introduced in Definition 2.3.25.

Theorem 2.4.3.
Let $\mathcal{K}$ be the canonical divisor defined in Equation (2.8)*. Then, we have the following equalities of codes:*

$$\mathrm{LAG}_{\mathbb{D}}(A, D)^\perp = \mathrm{LD}_{\mathbb{D}^\star}(A, D) = \mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A, D).$$

Proof. We have the following commutative diagram

$$\begin{array}{ccc} \Lambda_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A) & \xrightarrow{f \mapsto f\frac{dt_D}{t_D}} & \Omega_{\mathbb{D}^\star}(A, V_D) \\ \downarrow{\scriptstyle (\bar{\varepsilon}_i)_i} & & \downarrow{\scriptstyle (\mathcal{R}\mathrm{es}_{P_i})_i} \\ \mathcal{H} & \xrightarrow{\quad\mathrm{Id}\quad} & \mathcal{H} \end{array}$$

whose top arrow is an isomorphism thanks to Theorem 2.3.34. The equality between $\mathrm{LD}_{\mathbb{D}^\star}(A, D)$ and $\mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A,\ D)$ follows.

Let $f \in \Lambda_{\mathbb{D}}(A)$ and $\nu \in \Omega_{\mathbb{D}^\star}(A, V_D)$. By the Residues Theorem (Theorem 2.3.32), we know that $\sum_{P \in \mathcal{P}_K} \mathrm{Resrd}_P(f\nu^\star) = 0$. Moreover, it follows from the proof of

Lemma 2.3.37 that

$$\mathrm{Resrd}_P(f\nu^\star) = \begin{cases} \mathrm{Tr}_F\left(\bar{\varepsilon}_i(f) \circ \mathcal{R}\mathrm{es}_{P_i}(\nu)^\star\right) & \text{if } P = P_i, \\ 0 & \text{if } P \notin \{P_1, \dots, P_s\}. \end{cases}$$

We deduce that the codewords attached to f, on the one hand, and ν, on the other hand, are orthogonal in $\mathcal{H}$, i.e., $\mathrm{LAG}_{\mathbb{D}}(A, D) \subset \mathrm{LD}_{\mathbb{D}^\star}(A, D)^\perp$. To show the reverse inclusion, we compare the dimensions. First of all, noticing that the kernel of $\bar{\varepsilon}_D$ is $\Lambda(A, V_D)$, we find

$$\dim_F \mathrm{LAG}_{\mathbb{D}}(A, D) = \lambda_{\mathbb{D}}(A) - \lambda_{\mathbb{D}}(A, V_D).$$

Then, using the first part of the theorem, we obtain similarly

$$\begin{aligned} \dim_F \mathrm{LD}_{\mathbb{D}^\star}(A, D) &= \lambda_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A) - \lambda_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A, V_D) \\ &= sr^2 - \lambda_{\mathbb{D}}(A) + \lambda_{\mathbb{D}}(A, V_D) \end{aligned}$$

the last equality coming from the Riemann–Roch Theorem (Theorem 2.3.38) and the fact that $\dim_F V_D = sr$. Observing that the two dimensions sum to $sr^2 = \dim_F \mathcal{H}$ concludes the proof. □

Corollary 2.4.4.
We assume $2g - 2 < \deg A < sr$. *Then the code* $\mathrm{LD}_{\mathbb{D}^\star}(A, D)$ *has length* sr^2, *dimension* $sr^2 - r \deg A + r(g-1)$ *over* F *and minimum distance at least* $\deg A - (2g-2)$.

Proof. This results from the estimates on the parameters of a linearized AG code given in [BC24, Theorem 2]. □

Remark 2.4.5.
As recalled in [MPSK22], a maximum sum-rank distance (MSRD) code in the sum-rank metric is a code achieving the sum-rank metric Singleton-type bound $rd + k = n + r$ *where* $[n, k, d]$ *are the code parameters: length, dimension, and minimum distance. In our situation, both* $\mathrm{LAG}_{\mathbb{D}}(A, D)$ *and its dual* $\mathrm{LD}_{\mathbb{D}^\star}(A, D)$ *meet the Singleton bound up to a defect of* rg, *i.e., they both satisfy* $rd + k \geqslant n + r(1 - g)$.

2.4.2 Decoding

In what follows we describe and prove a decoding algorithm for linearized AG codes with unramified evaluation places. Our algorithm can be seen as the sum-rank metric version of the one given in [Sti93, Section 8.5] for AG codes in the Hamming metric. We make the usual injectivity hypothesis on the evaluation maps giving the code and its dual, respectively, as follows.

Hypothesis 2.4.6.
From now on, we assume the following condition on A:

$$2g - 2 < \deg A < sr.$$

Remark 2.4.7.
The map $\bar{\varepsilon}_D$ defining the code $\mathrm{LAG}_{\mathbb{D}}(A, D)$ is injective if and only if $\lambda_{\mathbb{D}}(A, V_D) = 0$. This latter condition is fulfilled if $\deg A < sr$. Similarly, the defining morphism of the dual code $\mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A, D)$ is injective when $\deg A > 2g - 2$. The two inequalities of Hypothesis 2.4.6 thus imply the injectivity of both $\mathrm{LAG}_{\mathbb{D}}(A, D)$ and its dual.

We shall need the following consequence of the Riemann–Roch Theorem.

Theorem 2.4.8.
Let (A, W) be an extended divisor satisfying $2g - 2 < \deg(A, W)$. Then, the following short sequence is exact

$$0 \to \Lambda(A, W) \to \Lambda(A) \xrightarrow{\bar{\varepsilon}_{D|W}} \prod_{i=1}^{s} \mathrm{Hom}_F(W_i, V_i) \to 0$$

where, by definition, $\bar{\varepsilon}_{D|W}(f) = \big(\bar{\varepsilon}_1(f)_{|W_1}, \ldots, \bar{\varepsilon}_s(f)_{|W_s}\big)$.

Proof. The short sequence is left exact by definition. By applying Theorem 2.3.38 to $\Lambda(A)$ and $\Lambda(A, W)$, we check that the difference of their dimensions is $r \dim(W)$. We then conclude that $\bar{\varepsilon}_{D|W}$ is surjective. □

We will also need a variant of the pairing $\langle -, - \rangle$ relative to a subspace $W = \bigoplus_{i=1}^{s} W_i$ with $W_i \subset V_i$. Precisely, given such a subspace W, we consider the F-bilinear form

$$\begin{array}{rccl} \Phi_W : \prod_{i=1}^{s} \mathrm{Hom}_F(V_i, W_i) \times \prod_{i=1}^{s} \mathrm{Hom}_F(W_i, V_i) & \to & F \\ (\varphi, \psi) & \mapsto & \sum_{i=1}^{s} \mathrm{Tr}\,(\varphi_i \circ \psi_i) \end{array}$$

where φ_i and ψ_i stand for the coordinates of φ and ψ respectively.

Lemma 2.4.9.
The bilinear form Φ_W is nondegenerate.

Proof. If there existed a nonzero s-tuple of homomorphisms $(\varphi_1, \ldots, \varphi_s)$ with $\varphi_i \in \mathrm{Hom}_F(V_i, W_i)$, such that, say, $a_{i_0} \neq 0$ and $\sum_{i=1}^{s} \mathrm{Tr}\,(a_i \mathrm{Hom}_F(W_i, V_i)) = 0$, then taking $\psi_i = 0 \in \mathrm{Hom}_F(W_i, V_i)$ for $i \neq i_0$, we would have $\mathrm{Tr}\,(\varphi_{i_0} \mathrm{Hom}_F(W_{i_0}, V_{i_0})) = 0$. This contradicts [CD23, Lemma 4.2]. □

In what follows, we set

$$\rho_{\text{algo}} := \left\lfloor \frac{d^\star(A) - g - 1}{2} \right\rfloor = \left\lfloor \frac{sr - \deg A - g - 1}{2} \right\rfloor.$$

It is the maximal number of errors that we intend to decode with our algorithm.

An auxiliary divisor

Definition 2.4.10.
A divisor $A \in \mathrm{Div}(\mathbb{D})$ is called Galois *if $A_Q = A_{Q'}$ when Q and Q' are above the same place.*

Lemma 2.4.11.
Let $A_1, A_2 \in \mathrm{Div}(\mathbb{D})$. If A_2 is Galois then $\Lambda_{\mathbb{D}^\star}(A_1)\Lambda_{\mathbb{D}^\star}(A_2) \subset \Lambda_{\mathbb{D}^\star}(A_1 + A_2)$.

Proof. Let us denote by Q_j the m_P places above the place $P \in \mathcal{P}_K$. If we do not apply $\min_{Q_j|P}$ and thus replace ω_P by ω_{Q_j} in the proof of the surmultiplicativity of the gauge of Lemma 2.3.2, we get for any f in $\Lambda_{\mathbb{D}^\star}(A_1)$ and for any g in $\Lambda_{\mathbb{D}^\star}(A_2)$ that

$$\omega_{Q_j}(fg) \geqslant \min_{0 \leqslant k \leqslant i_0} \left(w_{Q_j}(f_k) + k\frac{w_Q(x^{-1})}{r} + w_{Q_{(j+k)\%m_P}}(g_{i_0-k}) + (i_0 - k)\frac{w_Q(x^{-1})}{r} \right).$$

Hence, for some $k_0 \in \{0, \ldots, i_0\}$, we have

$$\omega_{Q_j}(fg) \geqslant -(A_1)_{Q_j} - (A_2)_{Q_{(j+k_0)\%m_P}} = -(A_1)_{Q_j} - (A_2)_{Q_j} = -(A_1 + A_2)_{Q_j},$$

where the first equality holds since A_2 is a Galois divisor. □

We make the following assumption on L/K, which will be helpful to construct Galois divisors.

Hypothesis 2.4.12.
There exists a place $P \in \mathcal{P}_K \backslash \{P_1, \ldots, P_s\}$ such that $r \mid e_P b_P$ and $\deg P = 1$.

Lemma 2.4.13.
There exists a divisor $A_1 \in \mathrm{Div}(\mathbb{D}^\star, D)$ such that

(i) $A + A_1$ is Galois,

(ii) $\deg(A + A_1) < sr - \rho_{\text{algo}}$,

(iii) $\lambda_{\mathbb{D}^\star}(A_1) > r \cdot \rho_{\text{algo}}$.

Proof. Using Hypothesis 2.4.12, we can pick a Galois divisor G of degree $sr - \rho_{\text{algo}} - 1$ with support concentrated at the place P. We set $A_1 := G - A$. The first and second conditions are then clearly fulfilled. For the last one, we use the Riemann–Roch Theorem (Theorem 2.3.11), which implies

$$\frac{\lambda_{\mathbb{D}^\star}(A_1)}{r} \geqslant \deg(A_1) - g + 1 = \deg(G) - \deg(A) - g + 1 = sr - \deg(A) - g - \rho_{\text{algo}}.$$

Besides, it readily follows from the definition of ρ_{algo} that $sr - \deg(A) - g \geqslant 2\rho_{\text{algo}} + 1$ and the proposition follows. □

From now on, we fix a divisor A_1 satisfying the requirements of Lemma 2.4.13 (so, in particular, we assume Hypothesis 2.4.12).

Error localization

We denote by $m = c + e$ the received message as the sum of a codeword $c \in \mathrm{LAG}_{\mathbb{D}}(A, D)$ and an error $e = (e_1, \ldots, e_s)$ with $w_{\text{srk}}(e) \leqslant \rho_{\text{algo}}$. The first decoding step consists of finding a localizing function $f \in \mathbb{D}^\star$ in the following sense.

Definition 2.4.14.
An error localizing function *relative to the code* $\mathrm{LAG}_{\mathbb{D}}(A, D)$ *and an error* e *is a function* $f \in \mathbb{D}^\star$ *such that* $e_i^\star \circ \bar{\varepsilon}_i(f) = 0$ *for all* $i \in [s]$.

We note that the vanishing condition $e_i^\star \circ \bar{\varepsilon}_i(f) = 0$ is equivalent to the inclusion $\operatorname{im} e_i \subset \ker(\bar{\varepsilon}_i(f^\star))$, which justifies the terminology of "localizing function".

Proposition 2.4.15.
There exists a nonzero localizing function in $\Lambda_{\mathbb{D}^\star}(A_1)$.

Proof. We set $\Lambda_{\mathbb{D}}{}^\star(A_1) = \{f \in \mathbb{D} \mid w_{\theta^i(Q)}(f_i) + \frac{i w_Q(x)}{r} + A_{1Q} \geqslant 0 \quad \forall Q \in \mathbb{P}_L, \forall i \in \{0, \ldots, r-1\}\}$. It follows from the Riemann–Roch Theorem that

$$\dim_F \Lambda_{\mathbb{D}}{}^\star(A_1) - \dim_F \Lambda_{\mathbb{D}}{}^\star(A_1, \operatorname{im}(e)) \leqslant r \cdot w_{\text{srk}}(e).$$

As $\dim_F \Lambda_{\mathbb{D}}{}^\star(A_1) = \lambda_{\mathbb{D}^\star}(A_1) > r \cdot w_{\text{srk}}(e)$, we deduce that $\dim_F \Lambda_{\mathbb{D}}{}^\star(A_1, \operatorname{im}(e)) > 0$. We conclude by noticing that the adjoint of any function in $\Lambda_{\mathbb{D}}{}^\star(A_1, \operatorname{im}(e))$ is an error localizing function belonging to $\Lambda_{\mathbb{D}^\star}(A_1)$. □

Proposition 2.4.16.
A function $f \in \Lambda_{\mathbb{D}^\star}(A_1)$ *is an error localizing function if and only if*

$$\forall h \in \Lambda_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A - A_1), \quad \langle \bar{\varepsilon}_D(fh), m \rangle = 0. \tag{2.9}$$

Proof. Let $f \in \Lambda_{\mathbb{D}^\star}(A_1)$ and set $A_2 := \mathcal{K} + \operatorname{CoNr}(D) - A - A_1$ for simplicity. Noticing that $\mathcal{K}$ and $\operatorname{CoNr}(D)$ are both Galois divisors, we conclude that A_2 is Galois too. By Lemma 2.4.11, we thus have:

$$\Lambda_{\mathbb{D}^\star}(A_1) \cdot \Lambda_{\mathbb{D}^\star}(A_2) \subset \Lambda_{\mathbb{D}^\star}\big(\mathcal{K} + \operatorname{CoNr}(D) - A\big).$$

It then follows from Theorem 2.4.3 that $\langle \bar{\varepsilon}_D(fh), c\rangle = 0$ for all $h \in \Lambda_{\mathbb{D}^\star}(A_2)$. Thus

$$\langle \bar{\varepsilon}_D(fh), m\rangle = \langle \bar{\varepsilon}_D(fh), e\rangle = \sum_{i=1}^{s} \operatorname{Tr}_F\left(\bar{\varepsilon}_i(fh) \circ e_i^\star\right) = \sum_{i=1}^{s} \operatorname{Tr}_F\left(e_i^\star \circ \bar{\varepsilon}_i(f) \circ \bar{\varepsilon}_i(h)\right). \quad (2.10)$$

If f is a localizing function, then $e_i^\star \circ \bar{\varepsilon}_i(f) = 0$, so $\langle \bar{\varepsilon}_D(fh), m\rangle$ vanishes as well.

Conversely, let us assume that $\langle \bar{\varepsilon}_D(fh), m\rangle = 0$ for all $h \in \Lambda_{\mathbb{D}^\star}(A_2)$. We define $W_i := \operatorname{im} e_i^\star$ and set $W := \bigoplus_{i=1}^{s} W_i$ accordingly. We notice that the right hand side of Equation (2.10) can be rewritten as $\Phi_W\big((e_i^\star \circ \bar{\varepsilon}_i(f))_{i=1}^s, (\bar{\varepsilon}_i(h)_{|W_i})_{i=1}^s\big)$. Our assumption then reads

$$\forall h \in \Lambda_{\mathbb{D}^\star}(A_2), \quad \Phi_W\big((e_i^\star \circ \bar{\varepsilon}_i(f))_{i=1}^s, (\bar{\varepsilon}_i(h)_{|W_i})_{i=1}^s\big) = 0. \quad (2.11)$$

Observing moreover that

$$\begin{aligned}\deg(\mathcal{K} + \operatorname{CoNr}(D) - A - A_1, W) &= 2g - 2 + sr - \deg(A + A_1) - \dim_F W \\ &> 2g - 2 + \rho_{\text{algo}} - w_{\text{srk}}(e) \geqslant 2g - 2\end{aligned}$$

we can apply Theorem 2.4.8 to get the surjectivity of the map

$$\bar{\varepsilon}_{D|W} : \Lambda_{\mathbb{D}^\star}\big(\mathcal{K} + \operatorname{CoNr}(D) - A - A_1\big) \longrightarrow \prod_{i=1}^{s} \operatorname{Hom}_F(W_i, V_i).$$

Therefore Equation (2.11) shows that $\big(e_i^\star \circ \bar{\varepsilon}_i(f)\big)_{i=1}^s$ is orthogonal (for Φ_W) to the whole space $\prod_{i=1}^s \operatorname{Hom}_F(W_i, V_i)$. Thanks to Lemma 2.4.9, it then must vanish. □

Syndrome equation

It now only remains to solve the syndrome equation restricted to the localizing space previously determined.

Proposition 2.4.17.
Let $f \in \Lambda_{\mathbb{D}^\star}(A_1)$ be a nonzero localizing function and let $e' = (e'_1, \dots, e'_s) \in \prod_{i=1}^s \operatorname{End}_F(V_i)$ such that

1. *for all $i \in [s]$, we have $\operatorname{im}(e'_i) \subset \ker \bar{\varepsilon}_i(f^\star)$,*
2. *for all $h \in \Lambda_{\mathbb{D}^\star}\big(\mathcal{K} + \operatorname{CoNr}(D) - A\big)$, we have $\langle \bar{\varepsilon}_D(h), e'\rangle = \langle \bar{\varepsilon}_D(h), m\rangle$.*

Then $e' = e$.

Proof. From Theorem 2.4.3, we derive that the difference $e' - e$ lies in $\mathrm{LAG}_{\mathbb{D}}(A, D)$. Besides its image lies in $\bigoplus_{i=1}^{s} \ker \bar{\varepsilon}_i(f^\star)$ and thus $w_{\mathrm{srk}}(e' - e) \leqslant \dim_F \left(\bigoplus_{i=1}^{s} \ker \bar{\varepsilon}_i(f^\star)\right) \leqslant \deg A_1 < d^\star(A)$. We conclude that $e' = e$. □

Algorithm 7 summarizes our decoding algorithm.

Algorithm 7: Decoding algorithm for linearized Algebraic Geometry codes

Input: A message m with an error of weight at most $\rho_{\mathrm{algo}} = \left\lfloor \frac{d^\star(A) - g - 1}{2} \right\rfloor$.

Output: The error e corresponding to the maximum likelihood principle.

1: Pick a divisor $A_1 \in \mathrm{Div}(\mathbb{D}^\star, D)$ satisfying the requirements of Lemma 2.4.13.

2: Pick a nonzero solution $f \in \Lambda_{\mathbb{D}^\star}(A_1)$ of the linear system

$$\forall h \in \Lambda_{\mathbb{D}^\star}\big(\mathcal{K} + \mathrm{CoNr}(D) - A - A_1\big), \quad \langle \bar{\varepsilon}_D(fh), m \rangle = 0.$$

3: Solve the linear system with $e \in \prod_{i=1}^{s} \mathrm{Hom}_F(V_i, \ker \bar{\varepsilon}_i(f^\star))$:

$$\forall h \in \Lambda_{\mathbb{D}^\star}\big(\mathcal{K} + \mathrm{CoNr}(D) - A\big), \quad \langle \bar{\varepsilon}_D(h), e \rangle = \langle \bar{\varepsilon}_D(h), m \rangle.$$

4: Return e.

Theorem 2.4.18.
We assume Hypothesis 2.4.6 and 2.4.12. Then, Algorithm 7 can decode any error of weight at most

$$\rho_{\mathrm{algo}} = \left\lfloor \frac{d^\star(A) - g - 1}{2} \right\rfloor.$$

Moreover, its complexity is polynomial in s and r.

Proof. Correctness follows from Lemma 2.4.13 and Propositions 2.4.15, 2.4.16, 2.4.17. Indeed, we fix a divisor A_1 satisfying the conditions of Lemma 2.4.13. Then, Proposition 2.4.15 implies that there exists a nonzero localizing function f. Proposition 2.4.16 yields such a nonzero localizing function $f \in \Lambda_{\mathbb{D}^\star}(A_1)$. Obviously, we must have $\deg\left(A_1, \bigoplus_{i=1}^{s} \ker \bar{\varepsilon}_i(f^\star)\right) \geqslant 0$. Using the hypothesis $\deg(A + A_1) < sr - \rho_{\mathrm{algo}}$ from Lemma 2.4.13, we deduce $\dim_F \left(\bigoplus_{i=1}^{s} \ker \bar{\varepsilon}_i(f^\star)\right) \leqslant \deg A_1 < d^\star(A)$, so that Proposition 2.4.17 yields the error. All steps clearly have polynomial complexity in s and r, as the dimensions of both $\Lambda_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A)$ and $\Lambda_{\mathbb{D}^\star}(\mathcal{K} + \mathrm{CoNr}(D) - A - A_1)$ are in $O(sr^2)$. □

2.5 Conclusion

Following the Ph.D. thesis of Witt [Wit34], Tamagawa in [Tam51] and later Mattson in [Mat61] showed a Riemann–Roch theorem for parallelotopes on separable semisimple algebras over a function field. Our Riemann–Roch theorem can be viewed as a corollary

of this more general theorem by computing the discriminant of the gauge orders Λ_P and using our Serre Duality. However, our approach based on an explicit decomposition $\mathbb{D} := \frac{L[T;\theta]}{T^r - x}$ is more informative regarding the duality of LAG codes, as it allows us to define the Linearized Differential (LD) code $\mathcal{D}(A)$, dual of $\mathrm{LAG}_{\mathbb{D}}(A, D)$, as the image by the endomorphic residue map at the evaluation places of the differential space, dual of the Riemann–Roch space $\Lambda_{\mathbb{D}}(A)$ for the reduced residue sum pairing. In a future work, we intend to construct and decode a more general family of LAG codes using general parallelotopes as divisors of a (not necessarily cyclic) division algebra $\mathbb{D}$ based on Tamagawa's Theorem [Tam51].

3 Construction, Duality and Decoding of Shortened LAG codes

In this section we show how to construct Shortened LAG codes as subcodes of LAG Codes and we characterize their duals as the corresponding punctured code. Besides, it is straightforward that our LAG decoding algorithm can decode any shortened LAG code as a LAG subcode with the same design distance as its parent LAG code.

3.1 Construction of Shortened LAG codes

It is a general fact that the puncturing operation is dual to the shortening operation on codes as it is shown in the rank metric for matricial codes in [BR16]. Let $V_D = \prod_{i=1}^{s} V_i$ be the residual algebra. Let $U = \prod_{i=1}^{s} U_i$ be a product of vector subspaces $U_i \subset V_i$. Let W_i be a supplementary space of U_i in V_i and $W = \prod_{i=1}^{s} W_i$.

Definition 3.1.1.
The shortening operation relative to the decomposition $V_D = U \oplus W$ is given by:

$$\mathrm{LAG}_{\mathbb{D}}(A, D) \overset{\mathcal{S}_{U,W}}{\mapsto} \bar{\varepsilon}_D(\Lambda(A, U))|_W$$

in the ambient space $\prod_{i=1}^{s} \mathrm{Hom}(W_i, V_i)$.

Definition 3.1.2.
The puncturing operation relative to the decomposition $V_D = U \oplus W$ is given by:

$$\mathrm{LAG}_{\mathbb{D}}(A, D) \overset{\mathcal{P}_{U,W}}{\mapsto} \pi_W^U\left(\bar{\varepsilon}_D(\Lambda_{\mathbb{D}}(A)^\star)\right)$$

in the ambient space $\prod_{i=1}^{s} \mathrm{Hom}(V_i, W_i)$, where π_W^U denotes the projection onto W along U and $\Lambda_{\mathbb{D}}(A)^\star$ is the image of $\Lambda_{\mathbb{D}}(A)$ by the adjunction map.

3.2 Duality of Shortened LAG codes

Proposition 3.2.1 (Duality of Shortened LAG codes)**.**
The dual of the shortened code $\mathcal{S}_{U,W}(\mathrm{LAG}_{\mathbb{D}}(A,D))$ *for the trace bilinear form*

$$\begin{cases} \prod_{i=1}^{s} \mathrm{Hom}(W_i,V_i) & \times \prod_{i=1}^{s} \mathrm{Hom}(V_i,W_i) \to F \\ f,g & \mapsto \sum_{i=1}^{s} \mathrm{Tr}(fg) \end{cases}$$

is the punctured dual code

$$\mathcal{S}_{U,W}(\mathrm{LAG}_{\mathbb{D}}(A,D))^{\perp} = \mathcal{P}_{U,W}(\mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D),D))$$

where $\mathcal{K}$ *is a canonical divisor of* $\mathbb{D}^\star$ *given by* $\left(\frac{dt_D}{t_D}\right)_L + \Delta$ *for some uniformizer* t_D *at the evaluation places and where* $\Delta := \sum_{P\in\mathbb{P}_K}\sum_{Q|P}\frac{b_P-1}{b_P}Q$ *is the different of the gauge order.*

Proof. We first check the orthogonality of the codes. We compute

$$\begin{aligned} &\langle \mathcal{S}_{U,W}(\mathrm{LAG}_{\mathbb{D}}(A,D)), \mathcal{P}_{U,W}(\mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D),D))\rangle \\ &= \sum_{i=1}^{s} \mathrm{Tr}(\bar{\varepsilon}_D(\Lambda(A,U))|_W \pi_W^U\,(\bar{\varepsilon}_D(\Lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D))^\star))) \\ &= \sum_{i=1}^{s} \mathrm{Tr}\,(\bar{\varepsilon}_D(\Lambda(A,U))\bar{\varepsilon}_D(\Lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D))^\star)) \\ &\subset \sum_{i=1}^{s} \mathrm{Tr}\left(\bar{\varepsilon}_D(\Lambda(A))\bar{\varepsilon}_D(\Lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D)))^{tr}\right) \\ &= \{0\} \end{aligned}$$

Now, we check that the dimensions also coincide. We have

$$\dim(\mathcal{S}_{U,W}(\mathrm{LAG}_{\mathbb{D}}(A,D))) = \lambda_{\mathbb{D}}(A,U) - \lambda_{\mathbb{D}}(A,V_D)$$

and

$$\dim(\mathcal{P}_{U,W}(\mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D),D))) = \lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\mathrm{CoNr}(D))-\lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\mathrm{CoNr}(D),U^\perp),$$

where the second equality comes from the rank theorem applied to the morphism

$$\begin{cases} \mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D),D) & \to \mathcal{P}_{U,W}(\mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D),D)) \\ f & \mapsto \pi_W^U\,(f^\star) \end{cases}$$

as $\mathrm{im}(f^\star) = \ker(f)^\perp$ and $\dim(\Lambda_{\mathbb{D}^\star}(A)^\star) = \sum_{i=0}^{r-1}\dim(\theta^{-i}(\mathcal{L}(A_i))) = \sum_{i=0}^{r-1}\dim(\mathcal{L}(A_i)) = \lambda_{\mathbb{D}}(A)$

with the notations of the article II. Thus, by the Riemann–Roch theorem, we obtain:

$$\begin{aligned}
&\dim(\mathcal{S}_{U,W}(\mathrm{LAG}_{\mathbb{D}}(A,D))) + \dim(\mathcal{P}_{U,W}(\mathrm{LAG}_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D),D))) \\
&= \lambda_{\mathbb{D}}(A,U) - \lambda_{\mathbb{D}}(A,V_D) + \lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D)) - \lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D),U^\perp) \\
&= r\deg(A,U) + r(1-g_\omega) + \lambda_{\mathbb{D}^\star}(\mathcal{K}-A+\ \mathrm{CoNr}(D)) - \lambda_{\mathbb{D}}(A,V_D) \\
&= r\deg(A,U) + r(1-g_\omega) + r\deg(\mathcal{K}-A+\ \mathrm{CoNr}(D)) + r(1-g_\omega) \\
&= sr^2 - r\dim(U).
\end{aligned}$$

□

3.3 Parameters and Decoding of Shortened LAG codes

Being a subcode of a LAG code for the same design distance d_{design}, the shortened LAG code can be decoded with a decoding radius of $\lfloor \frac{d_{\mathrm{design}}-g_\omega-1}{2} \rfloor$ using the same decoding algorithm. Finally, we note that the shortened LAG code also inherits the MSRD property.

Corollary 3.3.1.
Assuming $2g_\omega - 2 < \deg(A) < sr$, *the MSRD defect* δ_{MSRD} *of the codes* $\mathcal{S}_{U,W}(\mathrm{LAG}_{\mathbb{D}}(A,D))$ *is upper bounded by* g_ω.

Proof. Using the Singleton bound in sum-rank metric as given in [MPSK22, Theorem 1.5], we check:

$$\delta_{\mathrm{MSRD}} \leqslant sr + 1 - \dim(U) - (\deg(A,U) + (1-g_\omega)) - (sr - \deg(A)) = g_\omega.$$

□

4 LAG Code Construction

To illustrate the LAG code construction, we now make it explicit for a given Artin–Schreier–Witt extension. We construct a cyclic function field L of order 4, which is totally wildly ramified at infinity over the rational function field $\mathbb{F}_{16}(t)$, defined by the recursive equations:

$$\begin{cases} y^2 + y &= t^3 \\ z^2 + z &= y^3 \end{cases}$$

We define the automorphism σ given by $\sigma(y) = y + 1$ and $\sigma(z) = z + y + \omega$ where $\omega \in \mathbb{F}_{16}$ is chosen such that $\omega^2 + \omega + 1 = 0$. We check that it is well defined as we have $(z+y+\omega)^2 + (z+y+\omega) = (y+1)^3$. We also check that it generates the cyclic Galois group $\mathbb{Z}/4\mathbb{Z}$ of $L/\mathbb{F}_{16}(t)$. Indeed, we compute $\sigma^2(z) = \sigma(z) + \sigma(y) + \omega = z + 1$

and deduce that the order of σ is 4. Moreover, the rational place at infinity of $\mathbb{F}_{16}(t)$ is totally wildly ramified in L because the equations defining L imply $4w_{Q_\infty}(z) = 6w_{Q_\infty}(y) = 9w_{Q_\infty}(t) = 9e_{P_\infty}v_{P_\infty}(t)$ and so $4|e_{P_\infty}$, as we will show in this section. We now make the construction of the LAG codes specified in [BC24] explicit for this wild extension.

4.1 Artin-Schreier LAG Code Construction

We first specify the Artin–Schreier wild subextension L_1 given by the following equation over $\mathbb{F}_{16}(t)$:

$$y^2 + y = t^3$$

We set $x = t + \xi$, where ξ is a primitive element of $\mathbb{F}_{16}$ over $\mathbb{F}_2$, so that $\mathbb{D} = \frac{L[T;\theta]}{T^2 - x}$ is a division algebra. Indeed, the rational place P_ξ associated to x in $\mathbb{F}_{16}(t)$ is inert as $y^2 + y = \xi^3$ is irreducible. We deduce that x, being of valuation 1 in the completed extension $L_{((x))}$ cannot be a norm in this extension. We compute $b_P = 1$ for all $P \in \mathbb{P}_K \backslash \{P_\xi\}$ and $b_{P_\xi} = 2$. So, denoting by Q_ξ, the single place above the inert place P_ξ, we get the degree of the different

$$\deg(\Delta) = \frac{b_{P_\xi} - 1}{b_{P_\xi}} \deg(Q_\xi) = \frac{2}{2} = 1$$

The genus corresponding to the gauge orders, g_ω, is given by the formula

$$g_\omega = g_L + \frac{\deg(\Delta)}{2}$$

where g_L is the genus of the elliptic curve corresponding to the function field L_1 which is 1 and $\deg(\Delta)$, the degree of the different divisor, which is 1 too. So, we get

$$g_\omega = \frac{3}{2}.$$

The rational places are given by the uniformizer $\frac{1}{t}$ at infinity for P_∞ and by the uniformizers $t - \alpha$ for $\alpha \in \mathbb{F}_{16}$, i.e., $\alpha \in \{0, 1, \xi, \ldots, \xi^{14}\}$ where ξ is a primitive element of $\mathbb{F}_{16}$ over $\mathbb{F}_2$ satisfying $\xi^4 + \xi + 1 = 0$ for the other rational places P_α. We set $D = P_0 + P_1 + \check{P}_\xi + P_{\xi^2} + \cdots + P_{\xi^{14}}$ (where $\check{P}_\xi$ means that P_ξ is removed from the sum) the evaluation divisor over $s = 14$ rational unramified places P_{ξ^i} of the code for which we readily check $b_{P_{\xi^i}} = 1$ for $i \neq 1$. Finally, we set $n \in \mathbb{Z}$ and $A = nQ_\infty \in \mathbb{P}_L$ for the defining divisor of the code. Its support is concentrated at the rational totally wildly ramified place at infinity over P_∞.

Assuming that the degree of A satisfies the usual hypothesis on LAG codes

$$2 = 2g_\omega - 1 \leqslant \deg(A) \leqslant sr - 1 = 29$$

the Riemann–Roch space $\Lambda(A)$ has dimension:

$$\lambda(A) = 2(n + 1 - g_\omega) = 2n - 1.$$

We compute from the equation $y^2 + y = t^3$,

$$2w_{Q_\infty}(y) = 3w_{Q_\infty}(t) = -3e_{P_\infty}.$$

Indeed, we have $3w_{Q_\infty}(t) = w_{Q_\infty}(y^2 + y) = w_{Q_\infty}(y) + w_{Q_\infty}(y + 1)$. Thus, if we had $w_{Q_\infty}(y) \geqslant 0$, then we would also have $w_{Q_\infty}(1 + y) \geqslant 0$ and so we would get $3w_{Q_\infty}(t) = -3e_{P_\infty} \geqslant 0$, which is absurd. Hence, we have $0 > w_{Q_\infty}(y) = w_{Q_\infty}(y + 1)$ and so $w_{Q_\infty}(y^2 + y) = 2w_{Q_\infty}(y)$. We thus get $2|e_{P_\infty}$. On the other hand, we have the fundamental relation for our Galois field extension at P.

$$e_{P_\infty} f_{P_\infty} m_{P_\infty} = [L : K] = 2$$

where e_{P_∞} is the ramification index at infinity, m_{P_∞}, the number of places above P_∞ in L and f_{P_∞} the inertial index equal to the degree of the extension of residual fields at P_∞. We deduce $w_{Q_\infty}(t) = e_{P_\infty} v_{P_\infty}(t) = -e_{P_\infty} = -2$. We get

$$\begin{cases} w_{Q_\infty}(t) & = -2 \\ w_{Q_\infty}(y) & = -3. \end{cases}$$

Setting $AB = \{ab | a \in A, b \in B\}$ for any subsets $A, B \subset \mathbb{D}$, we get the following Riemann–Roch basis by taking all monomials from the integral basis over $\mathbb{F}_{16}[t]$:

$$(1, y)$$

on which Q-functions are positive everywhere except at Q_∞ where they are greater than $-n$.

n	$\lambda(A)$	basis
2	3	$\{1\}\{1, T\} \cup \{t\}$
3	5	$\{1, t\}\{1, T\} \cup \{y\}$
4	7	$\{1, t, y\}\{1, T\} \cup \{t^2\}$
5	9	$\{1, y, t, t^2\}\{1, T\} \cup \{ty\}$

For example, we compute $\omega_{Q_\infty}(tT) = w_{Q_\infty}(t) + \frac{w_{Q_\infty}(x)}{2} = -2 - \frac{2}{2} = -3$, so that we have $tT \in \Lambda(3Q_\infty) \backslash \Lambda(2Q_\infty)$.

We consider split places characterized by the equations

$$\beta^2 + \beta = \alpha^3 \text{ for } \alpha, \beta \in \mathbb{F}_{16}.$$

Setting $u_P = (u_{P,1}, \ldots, u_{P,r})$, the images by $\bar{\varepsilon}_{P_\alpha}$ of the generators $1, y, t, T$ are given in the integral basis corresponding to the fiber $(Q_{\alpha,\beta}, Q_{\alpha,\beta+1})$ over P_α by

$$\bar{\varepsilon}_{P_\alpha}(y) = \begin{pmatrix} \beta & 0 \\ 0 & \beta+1 \end{pmatrix} \qquad \bar{\varepsilon}_{P_\alpha}(t) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$
$$\bar{\varepsilon}_{P_\alpha}(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \bar{\varepsilon}_{P_\alpha}(T) = \begin{pmatrix} 0 & u_{P,1} \\ u_{P,2} & 0 \end{pmatrix}$$

We check indeed $\bar{\varepsilon}_{P_\alpha}(T)^2 = x\,\mathrm{id}$ and $\bar{\varepsilon}_{P_\alpha}(T)\bar{\varepsilon}_{P_\alpha}(\lambda) = \bar{\varepsilon}_{P_\alpha}(\sigma(\lambda))\bar{\varepsilon}_{P_\alpha}(T)$ for $\lambda \in L$.

4.2 Artin–Schreier–Witt LAG Code Construction

We now consider the double cyclic Artin–Schreier–Witt extension L of degree 4. It is defined over $\mathbb{F}_{16}$ by the equation $y^2 + y = t^3$ and the additional equation

$$z^2 + z = y^3.$$

We check that the field $\mathbb{F}_{16}$ is still the constant field in this double extension. Proceeding as in Section 4.1, we compute from the equations defining L:

$$4w_{Q_\infty}(z) = 6w_{Q_\infty}(y) = 9w_{Q_\infty}(t) = 9e_{P_\infty}v_{P_\infty}(t).$$

We thus have $4|e_{P_\infty}$. On the other hand, we have the fundamental relation for our Galois field extension at P:

$$e_{P_\infty}f_{P_\infty}m_{P_\infty} = [L:K] = 4$$

We deduce $w_{Q_\infty}(t) = e_{P_\infty}v_{P_\infty}(t) = -e_{P_\infty} = -4$. We get

$$\begin{cases} w_{Q_\infty}(t) & = -4 \\ w_{Q_\infty}(y) & = -6 \\ w_{Q_\infty}(z) & = -9. \end{cases}$$

We set $A = nQ_\infty \in \mathbb{P}_L$ for $n \in \mathbb{Z}$ the defining divisor of the code. Its support is concentrated at the rational totally wildly ramified place at infinity and $D = \sum_{P_\alpha \in \mathbb{P}_K \setminus \{P_\infty, P_\xi\}} P_\alpha$ the evaluation divisor of the code over the $s = 14$ rational unramified places P_{ξ^i} of the

code satisfying $b_{P_{\xi^i}} = 1$ for $i \neq 1$. We check that

$$(1, y, z, yz)$$

is an integral basis over $\mathbb{F}_{16}[t]$, that is to say a basis of the order of all regular elements (having poles at infinity only) over $\mathbb{F}_{16}[t]$. In the general case this integral basis computation can be performed using the Zassenhaus's Round2 algorithm as described in [Coh10]. We developed an implementation of this algorithm in SageMath: `https://plmlab.math.cnrs.fr/drain/maximal-order`, as the desingularization algorithm for function fields currently available in the native SageMath library (function *maximal_order*) lacks efficiency. Furthermore, the genus g_L of the double function field extension $L/L_1/K$ is given by the Hurwitz formula

$$2g_L - 2 = 2(2g_{L_1} - 2) + \deg(\delta(L/L_1)) = 0 + (p-1)(-w_{Q_\infty}(y^3)/e_{L/L_1,P_\infty} + 1) = 10$$

by using the computation of the different exponent in an Artin–Schreier extension by [Sti93, Proposition 3.7.8 (c)]. So, we get $g_L = 6$ for the genus of L.

We set $x = t+\xi$ as before. We check that the order of x is $r = 4$ in the multiplicative group $\mathbb{F}_{16}(t)^\times/\operatorname{Nr}(L)^\times$ as the place associated to x is inert in L, so that $\mathbb{D} = \frac{L[T;\theta]}{T^4-x}$ is a division algebra. We compute $b_P = 1 \quad \forall P \in \mathbb{P}_K \backslash \{P_\xi\}$ and $b_{P_\xi} = 4$. So, denoting by Q_ξ the single place above P_ξ, we get the degree of the different

$$\deg(\Delta) = \frac{b_{P_\xi} - 1}{b_{P_\xi}} \deg(Q_\xi) = \frac{3}{4}4 = 3.$$

Again, we deduce the genus corresponding to the gauge orders from the formula

$$g_\omega = g_L + \frac{\deg(\Delta)}{2}.$$

We get

$$g_\omega = 6 + 3/2 = 15/2$$

Assuming that the degree of A satisfies the usual hypotheses on LAG codes

$$14 = 2g_\omega - 1 \leqslant n \leqslant sr - 1 = 55$$

the Riemann–Roch space $\Lambda(A)$ has dimension

$$\lambda(A) = 4(n + 1 - g_\omega) = 4n - 26.$$

Setting $AB = \{ab | a \in A, b \in B\}$ for any subsets $A, B \subset \mathbb{D}$, we get the following Riemann–Roch basis by taking all monomials from the integral basis $(1, y, z, yz)$ over

$\mathbb{F}_q[t]$ on which Q-functions are positive everywhere except at Q_∞ where they are greater than $-n$.

n	$\lambda(A)$	basis
14	30	$\{1,t,t^2,y,ty,z\}\{1,T,T^2,T^3\} \cup \{t^3\}\{1,T,T^2\} \cup \{tz\}\{1,T\} \cup \{t^2y\}\{1\}$
15	34	$\{1,t,t^2,y,ty,z,t^3\}\{1,T,T^2,T^3\} \cup \{tz\}\{1,T,T^2\} \cup \{t^2y\}\{1,T\} \cup \{yz\}\{1\}$
16	38	$\{1,t,t^2,y,ty,z,t^3,tz\}\{1,T,T^2,T^3\} \cup \{t^2y\}\{1,T,T^2\} \cup \{yz\}\{1,T\} \cup \{t^4\}\{1\}$
17	42	$\{1,t,t^2,y,ty,z,t^3,tz,t^2y\}\{1,T,T^2,T^3\} \cup \{yz\}\{1,T,T^2\} \cup \{t^4\}\{1,T\} \cup \{t^2z\}\{1\}$
18	46	$\{1,t,t^2,y,ty,z,t^3,tz,t^2y,yz\}\{1,T,T^2,T^3\} \cup \{t^4\}\{1,T,T^2\} \cup \{t^2z\}\{1,T\} \cup \{t^3y\}\{1\}$
...	...	...

For example, we compute $\omega_{Q_\infty}(t^2yT) = w_{Q_\infty}(t^2y) + \frac{w_{Q_\infty}(x)}{4} = -8-6-1 = -15$, so that we have $t^2yT \in \Lambda(15Q_\infty)\backslash\Lambda(14Q_\infty)$.

We assume

$$\begin{cases} \beta^2+\beta &= \alpha^3 \\ \gamma^2+\gamma &= \beta^3 \end{cases} \text{ for } \alpha,\beta,\gamma \in \mathbb{F}_{16}$$

so that P_α is totally split (This actually corresponds to the cases $\alpha = 0,1,\omega,\omega^2$ with $\omega^2+\omega+1=0$).

The images by the evaluation map underlying the LAG codes, $\bar{\varepsilon}_{P_\alpha}$, of the generators $1,t,y,z$ in the basis given by the fiber $(Q_{\beta,\gamma}, Q_{\beta+1,\gamma+\beta+\omega}, Q_{\beta,\gamma+1}, Q_{\beta+1,\gamma+\beta+\omega+1})$ over P_α are given by

$$\bar{\varepsilon}_{P_\alpha}(z) = \begin{pmatrix} \gamma & 0 & 0 & 0 \\ 0 & \gamma+\beta+\omega & 0 & 0 \\ 0 & 0 & \gamma+1 & 0 \\ 0 & 0 & 0 & \gamma+\beta+\omega+1 \end{pmatrix} \bar{\varepsilon}_{P_\alpha}(y) = \begin{pmatrix} \beta & 0 & 0 & 0 \\ 0 & \beta+1 & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta+1 \end{pmatrix}$$

$$\bar{\varepsilon}_{P_\alpha}(t) = \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix} \quad \bar{\varepsilon}_{P_\alpha}(1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\bar{\varepsilon}_{P_\alpha}(T) = \begin{pmatrix} 0 & 0 & 0 & u_{P,1} \\ u_{P,2} & 0 & 0 & 0 \\ 0 & u_{P,3} & 0 & 0 \\ 0 & 0 & u_{P,4} & 0 \end{pmatrix}$$

We check indeed $\bar{\varepsilon}_{P_\alpha}(T)^4 = x\,\mathrm{id}$ and $\bar{\varepsilon}_{P_\alpha}(T)\bar{\varepsilon}_{P_\alpha}(\lambda) = \bar{\varepsilon}_{P_\alpha}(\sigma(\lambda))\bar{\varepsilon}_{P_\alpha}(T)$ for $\lambda \in L$.

5 Conjugacy with SageMath LAG codes

For simplicity, we restrict ourselves to the case of totally split unramified rational evaluation places $Q_{i,j}|P_i$ in L/K. The evaluation morphism underlying the implementation of the LAG Code in SageMath is given by the concatenation of the following morphisms in the normal basis corresponding to the fiber $(Q_{i,0},\dots,Q_{i,r-1})$ over P_i satisfying $\sigma(Q_{i,j}) = Q_{i,(j+1 \mod r)}$.

$$\bar{\varepsilon}'_i \begin{cases} \Lambda_{\mathbb{D}}(A) & \to \mathrm{Mat}_r(\mathbb{F}_q) \\ \lambda & \mapsto \begin{bmatrix} \pi_{i,0}(\lambda) & 0 & \dots & 0 & 0 \\ 0 & \pi_{i,1}(\lambda) & \dots & 0 & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 0 & \pi_{i,r-1}(\lambda) \end{bmatrix} \\ T & \mapsto \begin{bmatrix} 0 & 0 & \dots & 0 & \pi_{i,0}(x) \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & & 0 \\ \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix} \end{cases}$$

where $\pi_{i,j}$ denotes the projection $\mathcal{O}_{Q_{i,j}} \to \mathcal{O}_{Q_{i,j}}/Q_{i,j}$.

These evaluation morphisms $\bar{\varepsilon}'_i$ are equal to the evaluation morphism underlying the standard LAG code $\mathrm{LAG}_{\mathbb{D}}(A,D)$ up to a conjugation. Indeed, setting $u_{P_i} = (u_{i,1},\dots,u_{i,r})$ a preimage of x by the norm map in $\mathbb{D}_{P_i}$ and

$$C_i := \begin{bmatrix} u_{i,1} & 0 & \dots & 0 & 0 \\ 0 & u_{i,1}u_{i,2} & \dots & 0 & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & \dots & \dots & u_{i,1}\cdots u_{i,r} \end{bmatrix},$$

we check the explicit conjugation on the generators λ and T:

$$\bar{\varepsilon}_i = C_i \bar{\varepsilon}'_i C_i^{-1}$$

6 Implementation of the LAG decoding algorithm in SageMath

We provide some results from a SageMath implementation of our decoding algorithm. Our source code is available at `https://plmlab.math.cnrs.fr/drain/lag-decoding`. Our program allows us to construct Kummer, Artin–Schreier, or Artin–Schreier–Witt extensions L/K and assumes the place(s) at infinity to be totally ramified in L/K. We also assume the evaluation places $Q_{i,j}|P_i$ to be totally split in L/K. By design, the maximal decodable error weight with our algorithm has a defect of $\frac{g_\omega}{2}$ relative to the theoretical one induced by the design distance. As LAG codes are almost MSRD with a defect of g_ω relative to their design distance, we obtain an overall gap to the Singleton bound of $2g_\omega$, as can be observed below.

6.1 SageMath use case

Kummer extension of degree 2 over an elliptic curve.

```
sage: load('LAG_decoding.sage')
None
sage: F = GF(81)
sage: DLx = DivisionAlgebra(F=F, rK=2, r=2, pol_K_arg=[0,2,1,1], pol_L_arg=[0,1],
    pol_x_arg=[F.gen(),1])
```

The division algebra $\mathbb{D}$ is given by the following presentation:

$$\mathbb{D} = \frac{\frac{\mathbb{F}_{81}(t)[y]}{y^2-(x)}[T;\theta]}{(T^2-(t+z4))}$$

```
sage: LAG = LinearizedAGCode(DLx=DLx, degA=7, s_eval=7)
sage: omega = LAG.maximal_decodable_error_weight()
sage: omega
1
sage: error = LAG.random_error(omega)
sage: error  # RANDOM ERROR
[                2,         z4^3] | [0, 0] | [0, 0]
[2*z4^3 + z4^2 + 2, z4^3 + z4^2] | [0, 0] | [0, 0]

[0, 0] | [0, 0] | [0, 0] | [0, 0]
[0, 0] | [0, 0] | [0, 0] | [0, 0]
sage: word = LAG.random_codeword()
sage: message = word + error
sage: message # RANDOM MESSAGE FOR THE ERROR
[           z4^2 + z4 + 2, 2*z4^2 + z4 + 1]
[2*z4^3 + 2*z4^2 + z4 + 2,          2*z4^2]

[z4^3 + 2*z4^2,                         0]
[z4^2 + z4 + 1, 2*z4^3 + z4^2 + 2*z4 + 2]
```

```
[2*z4^3 + 2*z4^2 + 1,   z4^3 + 2*z4^2]
[      z4^3 + z4 + 2, z4^2 + 2*z4 + 1]

[z4^3 + z4^2 + 1, z4^3 + 2*z4 + 2]
[             z4,         z4^3 + 2]

[                   2,     2*z4^2 + 1]
[2*z4^3 + 2*z4^2 + 1, z4^2 + z4 + 2]

[   2*z4^2 + 2, 2*z4^3 + 2*z4^2 + z4 + 1]
[2*z4^3 + 2*z4,             2*z4^3 + 2*z4]

[z4^2 + z4 + 2, 2*z4^3 + 2*z4 + 2]
[  2*z4^2 + z4,         z4^3 + z4]
sage: decoded_error = LAG.decode_msg(message) # DECODING ...
sage: decoded_error == error # CHECKING THE RESULT
True
sage: (LAG.parameters,DLx.gD,LAG.parameters['k']+DLx.r*LAG.parameters['d']==LAG.
    parameters['n']+DLx.r - DLx.gD*DLx.r) #PARAMETERS : ALMOST MSRD
({'n': 28, 'k': 8, 'd': 7}, 4, True)
sage: floor((LAG.parameters['d']-LAG.gD-1)/2) == omega # DECODING DEFECT G/2
True
```

Kummer extension of degree 4 over $\mathbb{P}^1$.

```
sage: load('LAG_decoding.sage')
None
sage: DLx = DivisionAlgebra(F=GF(25),r=4)
```

The division algebra $\mathbb{D}$ is given by the following presentation:

$$\frac{\frac{\mathbb{F}_{25}(t)[y]}{y^4-(t^3+t^2+t)}[T;\theta]}{(T^4-(t+z2))}$$

```
sage: LAG = LinearizedAGCode(DLx=DLx, degA=DLx.degAmean())
sage: omega = LAG.maximal_decodable_error_weight()
sage: omega
4
sage: error = LAG.random_error(omega)
sage: error  # RANDOM ERROR
[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]

[       4, 4*z2 + 1, 2*z2 + 2,   z2 + 3]
[4*z2 + 3, 3*z2 + 3,       z2, 3*z2 + 4]
[       1, 2*z2 + 2, 4*z2 + 1,     2*z2]
[4*z2 + 4,     2*z2, 2*z2 + 3, 2*z2 + 2]

[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
```

```
[    4*z2,   z2 + 3,     2*z2, 3*z2 + 3]
[  z2 + 1, 3*z2 + 2, 3*z2 + 3,       z2]
[4*z2 + 4, 2*z2 + 3, 2*z2 + 2,     4*z2]
[3*z2 + 2,        1, 4*z2 + 1, 4*z2 + 2]

[0, 0, 0, 0]
[0, 0, 0, 0]
[0, 0, 0, 0]
[0, 0, 0, 0]
sage: word = LAG.random_codeword()
sage: message = word + error
sage: decoded_error = LAG.decode_msg(message) # DECODING ...
sage: decoded_error == error # CHECKING THE RESULT
True
sage: (LAG.parameters,DLx.gD,LAG.parameters['k']+DLx.r*LAG.parameters['d']==LAG.
    parameters['n']+DLx.r - DLx.gD*DLx.r) #PARAMETERS : ALMOST MSRD
({'n': 112, 'k': 42, 'd': 14}, 9/2, True)
sage: floor((LAG.parameters['d']-LAG.gD-1)/2) == omega # DECODING DEFECT G/2
True
```

Artin–Schreier extension of degree 5 over $\mathbb{P}^1$.

```
sage: load('LAG_decoding.sage')
None
sage: DLx = DivisionAlgebra(r=5)
```

The division algebra $\mathbb{D}$ is given by the following presentation:

$$\mathbb{D} = \frac{\frac{\mathbb{F}_{25}(t)[y]}{y^5-y-(t^3+t^2+t)}[T;\theta]}{(T^5-(t+z2))}$$

```
sage: LAG = LinearizedAGCode(DLx=DLx, degA=DLx.degAmean())
sage: omega = LAG.maximal_decodable_error_weight()
sage: omega
5
sage: error = LAG.random_error(omega)
sage: error  # RANDOM ERROR
[0, 0, 0, 0, 0] | [0, 0, 0, 0, 0]
[0, 0, 0, 0, 0] | [0, 0, 0, 0, 0]
[0, 0, 0, 0, 0] | [0, 0, 0, 0, 0]
[0, 0, 0, 0, 0] | [0, 0, 0, 0, 0]
[0, 0, 0, 0, 0] | [0, 0, 0, 0, 0]

[    4*z2, 3*z2 + 4,       4, 4*z2 + 1, z2 + 3]
[2*z2 + 3,        2, z2 + 1,   z2 + 2,       4]
[2*z2 + 3,        2,       2, 2*z2 + 1,       4]
[       1,     2*z2,       2,         4,   4*z2]
[       3,       z2,   2*z2, 3*z2 + 3,   2*z2]

[0, 0, 0, 0, 0]
[0, 0, 0, 0, 0]
[0, 0, 0, 0, 0]
[0, 0, 0, 0, 0]
[0, 0, 0, 0, 0]
```

```
[2*z2 + 3, 0,       z2,     3*z2, 4*z2 + 1]
[3*z2 + 1, 0, 3*z2 + 2, 4*z2 + 1,   z2 + 2]
[2*z2 + 4, 0, 2*z2 + 3,   z2 + 4, 4*z2 + 3]
[4*z2 + 1, 0,     2*z2,       z2, 3*z2 + 2]
[    3*z2, 0, 2*z2 + 4,   z2 + 2,       z2]

[    2*z2, 2*z2 + 3,         4, 2*z2 + 1,       z2]
[4*z2 + 3,     3*z2, 2*z2 + 1, 2*z2 + 2, 2*z2 + 4]
[3*z2 + 4,        4,       z2, 2*z2 + 4, 4*z2 + 2]
[4*z2 + 1, 2*z2 + 4, 4*z2 + 4,         2, 2*z2 + 3]
[    3*z2, 3*z2 + 2,         1, 3*z2 + 4,     4*z2]

[2*z2 + 4,       z2, 3*z2 + 4,   3*z2,       z2]
[  z2 + 3,        2,       z2,      1,        2]
[    3*z2, 2*z2 + 3,         3, z2 + 4, 2*z2 + 3]
[2*z2 + 1,        4,     2*z2,      2,        4]
[  z2 + 3,        2,       z2,      1,        2]
sage: word = LAG.random_codeword()
sage: message = word + error
sage: decoded_error = LAG.decode_msg(message) # DECODING ...
sage: decoded_error == error # CHECKING THE RESULT
True
sage: (LAG.parameters,DLx.gD,LAG.parameters['k']+DLx.r*LAG.parameters['d']==LAG.
    parameters['n']+DLx.r - DLx.gD*DLx.r) #PARAMETERS : ALMOST MSRD
({'n': 175, 'k': 65, 'd': 17}, 6, True)
sage: floor((LAG.parameters['d']-LAG.gD-1)/2) == omega # DECODING DEFECT G/2
True
```

Kummer extension of degree 8 over $\mathbb{P}^1$.

```
sage: load('LAG_decoding.sage')
None
sage: DLx = DivisionAlgebra(F=GF(49),r=8)
```

The division algebra $\mathbb{D}$ is given by the following presentation:

$$\frac{\frac{\mathbb{F}_{49}(t)[y]}{y^8-(t^3+t^2+t)}[T;\theta]}{(T^8-(t+z2))}$$

```
sage: LAG = LinearizedAGCode(DLx=DLx, degA=DLx.degAmean(s_eval=6),s_eval=6)
sage: omega = LAG.maximal_decodable_error_weight()
sage: omega
4
sage: error = LAG.random_error(omega)
sage: error  # RANDOM ERROR

[  z2 + 1, 3*z2 + 5, 5*z2 + 5,        0,   z2 + 2, 4*z2 + 5, 6*z2 + 2, 2*z2 + 1]
[       3, 2*z2 + 1,   z2 + 1, 4*z2 + 3,        2,        1, 4*z2 + 6, 6*z2 + 3]
[3*z2 + 3, 3*z2 + 5, 5*z2 + 5, 5*z2 + 4, 6*z2 + 6, 5*z2 + 6, 6*z2 + 2, 2*z2 + 1]
[4*z2 + 2, 5*z2 + 2, 3*z2 + 5,        1, 5*z2 + 5, 5*z2 + 4,        1,   z2 + 6]
[4*z2 + 6, 5*z2 + 5,        4, 2*z2 + 6,   z2 + 6,   z2 + 5, 4*z2 + 1,   z2 + 1]
[6*z2 + 2, 2*z2 + 1,   z2 + 1, 5*z2 + 1,       z2, 3*z2 + 4, 4*z2 + 6, 6*z2 + 3]
[  z2 + 2,   z2 + 2,     6*z2,        2, 2*z2 + 3, 2*z2 + 2, 4*z2 + 3, 3*z2 + 6]
[       0, 4*z2 + 3,   z2 + 4,        2, 4*z2 + 1,   z2 + 1,        5, 5*z2 + 2]
```

```
                                                
```

	F	K	L	$x_{\mathbb{D}}$	g_K	g_L	$g_{\mathbb{D}}$	s
$C(2)$	$\mathbb{F}_{5^2}$	$\mathbb{F}_{5^2}(t)$	$\frac{\mathbb{F}_{5^2}(t)[y]}{y^2+4t^3+4t^2+4t}$	$t+z_2$	0	1	3/2	14
$C(3)$	$\mathbb{F}_{3^3}$	$\mathbb{F}_{3^3}(t)$	$\frac{\mathbb{F}_{3^3}(t)[y]}{y^3+2y+2t^3+2t^2+2t}$	$t+z_3$	0	1	2	9
$C(4)$	$\mathbb{F}_{5^2}$	$\mathbb{F}_{5^2}(t)$	$\frac{\mathbb{F}_{5^2}(t)[y]}{y^4+4t^3+4t^2+4t}$	$t+z_2$	0	3	9/2	7
$C(5)$	$\mathbb{F}_{5^2}$	$\mathbb{F}_{5^2}(t)$	$\frac{\mathbb{F}_{5^2}(t)[y]}{y^5+4y+4t^3+4t^2+4t}$	$t+z_2$	0	4	6	7
$C(8)$	$\mathbb{F}_{7^2}$	$\mathbb{F}_{7^2}(t)$	$\frac{\mathbb{F}_{7^2}(t)[y]}{y^8+6t^3+6t^2+6t}$	$t+z_2$	0	7	21/2	6
$C(2,2)$	$\mathbb{F}_{3^4}$	$\frac{\mathbb{F}_{3^4}(t)[x]}{x^2+2t^3+2t^2+t}$	$\frac{K(x)[y]}{y^2+2x}$	$t+z_4$	1	3	4	15

Figure II.1: Description of the tested codes, where z_n denotes a generator of $\mathbb{F}_{p^n}^{\times}$

	ω	$\deg A$	time	ω	$\deg A$	time	ω	$\deg A$	time
$C(2)$	1	23	1.985	6	12	2.978	11	2	4.003
$C(3)$	1	22	4.697	6	12	5.996	10	3	7.756
$C(4)$	1	20	7.023	4	14	7.682	7	8	8.793
$C(5)$	1	26	21.415	5	18	23.994	8	11	27.936
$C(8)$	1	34	142.395	4	27	153.397	8	20	164.652
$C(2,2)$	1	23	15.738	15	15	23.138	9	7	30.225

Figure II.2: CPU Timings in seconds for constructing a code.

6.2 SageMath benchmark

We tested the LAG decoding on different Kummer extensions and an Artin–Schreier–Witt extension. Benchmarks are reported in Figures II.2 and II.3, respectively, for the initial computation of the Riemann–Roch spaces and the iterative message decoding corresponding to the codes described in Figure II.1. There were run on a computer with AMD Ryzen 7 PRO 8840U (3,30 GHz up to 5,10 GHz) Processor and 16 GB DDR5-5 600MT/s (SODIMM).

Remark 6.2.1.
We also constructed generalized LAG codes (GLAG) as evaluations of Riemann–Roch spaces at places of arbitrary degree k. The implementation of their decoding is available at `https://plmlab.math.cnrs.fr/drain/glag-decoding`*. However, these codes yield very poor parameters ($[sr^2k, \lambda_{\mathbb{D}}(A), d^\star(A) := sr - \deg A]$), which is why we omitted them.*

	ω	$\deg A$	time	ω	$\deg A$	time	ω	$\deg A$	time
$C(2)$	1	23	0.009	6	12	0.026	11	2	0.052
$C(3)$	1	22	0.016	6	12	0.045	10	3	0.094
$C(4)$	1	20	0.032	4	14	0.065	7	8	0.137
$C(5)$	1	26	0.093	5	18	0.236	8	11	0.440
$C(8)$	1	34	1.386	4	27	2.394	8	20	4.741
$C(2,2)$	1	23	0.016	5	15	0.028	9	7	0.047

Figure II.3: CPU Timings in seconds for decoding a single random message in a code.

Chapter III

Tamagawa's Theory

1 Theoretical Setting

Following the thesis of Witt [Wit34], Tamagawa [Tam51], and later Mattson [Mat61] showed a Riemann–Roch Theorem for parallelotopes of maximal adelic orders in separable semisimple algebras over a function field of one variable, independently of its presentation as an Ore quotient algebra. In the case of an unramified splitting field and a defining element x such that $(x) = P - P'$ for two inert places P and P', our Riemann–Roch Theorem is a direct consequence of Tamagawa's Theorem [Tam51, Theorem 3] and of our Serre Duality because the gauge orders are all maximal in this case. It can still be viewed as a Corollary of Tamagawa's Theory [Tam51, Theorem 2] in the general case as well, as we will show by computing the discriminant of the gauge orders. We now review definitions and theorems underlying Tamagawa's theory.

1.1 Skolem–Noether and Wedderburn Theorem

In this section, we let K be a field. Finite dimensional central simple algebras over K are defined as simple algebras, i.e., algebras containing no non-trivial two-sided ideals, whose center is K and which are finite-dimensional over K. We need the following classical classification theorems on central simple algebras.

Theorem 1.1.1 (Skolem–Noether Theorem)**.**
Let A be a finite-dimensional central simple K-algebra. Let B be a simple K-algebra. Let $f, g : B \to A$ be two K-algebra homomorphisms. Then there exists an invertible element $x \in A$ such that $f(b) = xg(b)x^{-1}$ for all $b \in B$.

Proof. This follows from [For17, Theorem 3.2.6]. □

Theorem 1.1.2 (Wedderburn's Theorem)**.**
Let A be a finite-dimensional central simple K-algebra. Then A is isomorphic to a

matrix algebra over a finite-dimensional K-algebra D_A which is a division algebra:

$$A \simeq \mathrm{Mat}_{r/\mathrm{ind}_A}(D_A)$$

where r^2 is the dimension of A over K, where ind_A is an invariant integer (the index of A) dividing r and where D_A is unique up to isomorphism.

Proof. This follows from [Sta26, Section 074P]. □

1.2 Exponent and Index

Definition 1.2.1 (Index)**.**
As defined in [Rei75, Section 14], the index of a central simple algebra A over K is the square root of the dimension of D_A as K-vector space, where D_A is defined as in the Wedderburn Theorem 1.1.2.

$$\mathrm{ind}_A = \sqrt{[D_A : K]}$$

Definition 1.2.2 (Brauer group)**.**
Two finite-dimensional central simple algebras A, B over K are Brauer equivalent if they become isomorphic after tensoring each of them with a matricial algebra over K.

$$A \otimes_K \mathrm{Mat}_r(K) \simeq B \otimes_K \mathrm{Mat}_s(K)$$

for some positive integers r, s. As defined in [Rei75, Section 28], the Brauer group of K is defined as the set of equivalence classes of central simple algebras endowed with the tensor product as a group law.

Definition 1.2.3 (Exponent)**.**
As defined in [Rei75, Section 31], the exponent of a finite-dimensional central simple algebra A over K is its order in the Brauer group, that is to say the least positive integer k such that, for some integer n, one has an isomorphism of K-algebras

$$\overbrace{A \otimes_K \cdots \otimes_K A}^{k\text{-times}} \simeq \mathrm{Mat}_n(K)$$

Definition 1.2.4 (Cyclic algebra)**.**
A cyclic algebra A over a field K is a simple central algebra over K which is isomorphic to an Ore quotient ring

$$A := \frac{L[T;\theta]}{T^r - x}$$

for some cyclic splitting field extension L/K, i.e., a maximal commutative subfield of the algebra A containing K and of cyclic Galois group of order r generated by θ, and for some defining element $x \in K^\times$.

Theorem 1.2.5 (Exponent and Index)**.**
The local index at a place $P \in \mathbb{P}_K$, ind_P of a cyclic algebra (the index of the algebra completed at P) defined over a global function field, i.e., a function field with a finite constant field, is equal to its local exponent $\exp_P$ (the exponent of the algebra completed at P) in the Brauer group:

$$\exp_P = \mathrm{ind}_P$$

If the cyclic algebra is defined over an arbitrary function field, then we only know that the local exponent divides the local index:

$$\exp_P \mid \mathrm{ind}_P$$

Proof. This follows from [Rei75, Example 32.19] or [Rei75, Theorem 31.4] for the first part and from [Ker90, Satz 9.3] for the second part. □

Theorem 1.2.6 (Index Formula)**.**
The local index of the cyclic algebra of order r defined over a global function field K and given by the Ore quotient $\frac{L_Q[T;\theta^{m_P}]}{T^{r/m_P}-x}$, at an unramified place P for $Q|P$ is given by

$$\mathrm{ind}_P = \frac{r/m_P}{\gcd(r/m_P, v_P(x))}$$

where v_P is the valuation of K at P and m_P is the number of places of L above P.

Proof. This results from [Rei75, Example 32.20] using an unramified cyclic splitting field L at P. □

We recall the definition $b_P := \frac{r}{\gcd(w_Q(x),r)}$ and deduce the following Corollary from Theorem 1.2.6.

Corollary 1.2.7.
Let K be a global function field. At an unramified place P of K, ind_P divides b_P.

1.3 Different, Discriminants and Maximal Orders

We recall definitions and theorems about the different ideal and the discriminant of a cyclic algebra over a complete local function field as it plays a crucial role in the proof of Tamagawa's Theorem presented in Section 4. Let K be a function field of dimension one. Let A be a finite-dimensional central simple algebra over K, K_P be the completion of K at $P \in \mathbb{P}_K$ and $A_P := A \otimes K_P$ be the completion of A at P. We recall the definition of a maximal order in A_P as in [Rei75, Section 8].

Definition 1.3.1 ($\mathcal{O}_P$-lattice in A_P)**.**
Let $\mathcal{O}_P$ be the valuation ring of the local complete function field K_P. An $\mathcal{O}_P$-lattice in A_P is a finitely generated torsion-free $\mathcal{O}_P$-module of A_P.

Lemma 1.3.2.
An $\mathcal{O}_P$-lattice is a free $\mathcal{O}_P$-module of A_P.

Proof. By assumption, K is a function field of dimension one, $\mathcal{O}_P$ is a discrete valuation ring. In particular it is a principal ideal domain. Hence, the lemma follows from the structure theorem for finitely generated modules over a principal ideal domain. □

Definition 1.3.3 (Maximal Order of a Complete Local Cyclic Algebra)**.**
A full $\mathcal{O}_P$-lattice M in A_P is a $\mathcal{O}_P$-lattice in A_P such that its span over K_P is the whole central simple algebra:

$$K_P M = A_P$$

An $\mathcal{O}_P$-order is a full $\mathcal{O}_P$-lattice in A_P that is also a ring. A maximal order is an $\mathcal{O}_P$-order which is maximal for the inclusion.

The existence of a maximal order follows from [Rei75, Section 8.3]. Throughout this section, let Λ_P be an $\mathcal{O}_P$-order in A_P, and let $\mathrm{Trd} : A_P \to K_P$ be the reduced trace map, that is to say, the trace of the L_P linear map given by the left multiplication in A_P. Alternatively, the reduced trace is given by the formula $\mathrm{Trd}(a_0 + a_1 T + \cdots + a_{r-1}T^{r-1}) = \mathrm{Tr}_{L_P/K_P}(a_0)$ for $a_i \in L_P$. A left (resp. right, resp. two-sided) ideal of Λ_P refers to a left (resp. right, resp. two-sided) Λ_P-module of A_P.

Definition 1.3.4 (Different Ideal)**.**
Given a two-sided Λ_P-ideal J in A_P, its complementary ideal is defined in analogy with Definition (1.2.1) *as*

$$\mathcal{C}(J) = \{x \in A_P \mid \mathrm{Trd}(xJ) \subset \mathcal{O}_P\}$$

$\mathcal{C}(J)$ is clearly also a two-sided Λ_P-ideal in A_P. As defined in [Rei75, Section 4.d], we call $\mathcal{C}(\Lambda_P)$ the inverse different of Λ_P, and define the different ideal $\mathfrak{D}(\Lambda_P/\mathcal{O}_P)$ of Λ_P over $\mathcal{O}_P$ as

$$\mathfrak{D}(\Lambda_P/\mathcal{O}_P) = \mathcal{C}(\Lambda_P)^{-1} := \{x \in A_P \mid \mathcal{C}(\Lambda_P)x \subset \Lambda_P\}.$$

Since $\mathcal{C}(\Lambda_P) \supset \Lambda_P$, $\mathfrak{D}(\Lambda_P/\mathcal{O}_P)$ is clearly a right ideal of Λ_P. Also we note that the definition $\mathcal{C}(\Lambda_P)^{-1}$ could also be set as $\{x \in A_P \mid x\mathcal{C}(\Lambda_P) \subset \Lambda_P\}$. Indeed, as, the complementary ideal $\mathcal{C}(\Lambda_P)$ is generated by a (finite) dual basis of the free $\mathcal{O}_P$ module Λ_P for the reduced trace bilinear form, the element x belongs to $\mathcal{C}(\Lambda_P)^{-1}$ if and only if for all $c_1, c_2 \in \mathcal{C}(\Lambda_P)$ we have $\mathrm{Trd}(c_1 x c_2) \in \mathrm{Trd}(\Lambda_P \mathcal{C}(\Lambda_P)) = \mathcal{O}_P$, which is a symmetric criterion. So $\mathfrak{D}(\Lambda_P/\mathcal{O}_P)$ is a two-sided ideal of Λ_P.

Definition 1.3.5 (Discriminant Ideal)**.**
As in [Rei75, Section 4.d, Theorem 10.1], we define the discriminant $\mathrm{disc}(\Lambda_P/\mathcal{O}_P)$ *as the following (principal) ideal of the discrete valuation ring $\mathcal{O}_P$:*

$$\mathrm{disc}(\Lambda_P/\mathcal{O}_P) = \det\left(\left(\mathrm{Trd}(x_i x_j)\right)_{1 \leqslant i,j \leqslant r^2}\right)\mathcal{O}_P$$

where $r = \sqrt{[A_P : K_P]}$, $(x_1, \ldots, x_{r^2})$ *is a basis of* Λ_P *over* $\mathcal{O}_P$.

This definition does not depend on the choice of the basis $(x_1, \ldots, x_{r^2})$ as another choice $(y_1, \ldots, y_{r^2})$ would yield, denoting by $(a_{i,j})$ the base change matrix,

$$\begin{aligned}\det\left(\left(\operatorname{Trd}(x_i x_j)\right)_{1\leqslant i,j\leqslant r^2}\right)\mathcal{O}_P &= \det\left(\left(\sum_{k=1}^{r^2}\sum_{l=1}^{r^2} a_{i,k}a_{j,l}\operatorname{Trd}(y_k y_l)\right)_{1\leqslant i,j\leqslant r^2}\right)\mathcal{O}_P \\ &= \det((a_{i,j})_{1\leqslant i,j\leqslant r^2})^2 \det\left(\left(\operatorname{Trd}(y_i y_j)\right)_{1\leqslant i,j\leqslant r^2}\right)\mathcal{O}_P \\ &= \det\left(\left(\operatorname{Trd}(y_i y_j)\right)_{1\leqslant i,j\leqslant r^2}\right)\mathcal{O}_P\end{aligned}$$

Finally, we can also relate two discriminants of two $\mathcal{O}_P$-modules $M \subset M'$ in A_P by [NS13, Proposition 2.12] as follows.

Theorem 1.3.6 (Discriminant and Index of Orders)**.**
Let $M \subset M'$ *be two* $\mathcal{O}_P$*-modules included in each other. Then, we have*

$$\operatorname{disc}(M/\mathcal{O}_P) = [M' : M]^2 \operatorname{disc}(M'/\mathcal{O}_P)$$

where $[M' : M] := P^{\operatorname{length}_{\mathcal{O}_P}(M'/M)}$ *is the index ideal of* M *in* M'.

Theorem 1.3.7 (Maximal Order of a Division Algebra)**.**
We assume that D *is a division algebra over a local complete function field* K*. Then, there exists a unique valuation on* D *extending the discrete valuation on* K*. Its valuation ring is the unique maximal order of* D*.*

Proof. This results from [Wad00, Corollary 2.2]. The unique gauge is multiplicative in this case and its valuation ring, as it is integrally closed in D_P, is a maximal order of D_P. □

Theorem 1.3.8 (Maximal Order Principality [Rei75, Theorem 17.3])**.**
Let A_P *be the completion at* P *of a finite-dimensional central simple algebra* A *over a function field* K*. Assuming that* Λ_P *is a maximal order of* A_P/K_P*, every finitely generated left (resp. right)* Λ_P*-module* I *of* A_P *is a fractional left (resp. right) ideal*

$$I = \Lambda_P\delta \text{ for some } \delta \in A_P \tag{1.1}$$

resp.

$$I = \delta\Lambda_P \text{ for some } \delta \in A_P \tag{1.2}$$

Theorem 1.3.9 (Cyclicity of central simple algebras over a global function field [Rei75, Theorem 32.20])**.**
Over a global function field, i.e., a function field of transcendence degree one defined

over a finite field of constants, all finite-dimensional central simple algebras are cyclic algebras.

Finally, we have a formula giving the discriminant of a maximal order over a complete local function field over a finite constant field as a function of the index.

Theorem 1.3.10 (Maximal Order Discriminant)**.**
Let A_P be the completion at P of a finite-dimensional central simple algebra A over a global *function field K. The discriminant of a maximal $\mathcal{O}_P$-order $\mathcal{M}_P \subset A_P$ is given by*

$$\mathrm{disc}(\mathcal{M}_P/\mathcal{O}_P) = P^{r^2 \frac{\mathrm{ind}_P - 1}{\mathrm{ind}_P}}$$

Proof. This discriminant does not depend on the choice of a maximal order $\mathcal{M}_P$ by [Rei75, Theorem 25.3]. The formula results from [Rei75, Theorem 32.1]. □

2 Gauge Order

2.1 Gauge Orders and Discriminant

Definition 2.1.1 (Gauge)**.**
We recall that a gauge ω on a central simple algebra A defined over a local complete function field K is a surmultiplicative valuation extending the discrete valuation v on K, that is to say a function from $\mathbb{D}$ to $\mathbb{Q}$ satisfying:

$$\begin{cases} \forall x \in K, & \omega(x) = v(x) \\ \forall x, y \in \mathbb{D}, & \omega(x+y) \geqslant \min(\omega(x), \omega(y)) \text{ ultrametric property} \\ \forall x, y \in \mathbb{D}, & \omega(xy) \geqslant \omega(x) + \omega(y) \text{ surmultiplicative property} \end{cases}$$

Definition 2.1.2 (Gauge Order)**.**
Denoting by $\mathcal{O}$ the valuation ring of the local complete function field K, we define the $\mathcal{O}$-order $\Lambda \subset A$ with respect to the gauge ω as

$$\Lambda = \{f \in A \mid \omega(f) \geqslant 0\}$$

As the gauge ω is surmultiplicative, the $\mathcal{O}$-lattice Λ is well defined as an order.

Let $\mathbb{D} := L[T;\theta]/(T^r - x)$ be a cyclic algebra over a function field K and $\mathbb{D}_P := \mathbb{D} \otimes_K K_P$ be its completion at P. As in [BC24, section 1.2], we define a gauge on $\mathbb{D}_P$ by the following formula for any $\sum_{i=0}^{r-1} f_i T^i \in \mathbb{D}_P$ with $f_i \in L_P \simeq \prod_{Q|P} L_Q$.

$$\omega_P(\sum_{i=0}^{r-1} f_i T^i) := \frac{1}{e_P} \min_{Q|P} \min_{0 \leqslant i \leqslant r-1} \left(w_Q(f_{i,Q}) + \frac{i w_Q(x)}{r} \right)$$

Let Λ_P be the gauge order at P associated to ω_P. In this section, we compute the discriminant $\mathrm{disc}(\Lambda_P/\mathcal{O}_P)$ of the gauge order Λ_P over $\mathcal{O}_P$ and find that it is given by

$$\mathrm{disc}(\Lambda_P/\mathcal{O}_P) = P^{\frac{r^2}{e_P}d_P+\frac{r^2}{e_P}\frac{b_P-1}{b_P}}$$

where d_P is the different exponent of P in L/K, e_P is the ramification index of P in L/K, and $b_P := \frac{r}{\gcd(r,e_P v_P(x))}$. We then use this result together with Theorem 1.3.10 to give a maximality criterion for the gauge orders on a cyclic algebra $\mathbb{D}$ defined over a *global* function field.

Theorem 2.1.3 (Discriminant Formula)**.**
In our (Galois) cyclic extension L/K, we set $e_P = e_Q$ for $Q|P$ and set

$$b_P := \frac{r}{\gcd(r, w_Q(x))}$$

The discriminant of Λ_P over the discrete valuation ring $\mathcal{O}_P$ is given by

$$\mathrm{disc}(\Lambda_P/\mathcal{O}_P) = \mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^r P^{r^2\frac{b_P-1}{b_P e_P}}$$

Proof. We proceed in three steps: compute the discriminant of $A := \mathcal{O}_{L,P}[T;\theta]/(T^r - x)$, compute the index of A in Λ_P, and apply the formula [NS13, Proposition 2.12] relating the discriminants of A and Λ_P.

Replacing x by $\pi_P^{-mr}x$ and T by $\pi_P^{-m}T$ for a suitable $m \in \mathbb{Z}$, we may assume $0 \leqslant v_P(x) < r$ without changing b_P locally. Let $(a_0, \ldots, a_{r-1})$ be an $\mathcal{O}_P$-basis of $\mathcal{O}_{L,P}$. Then $(a_i T^n)_{0\leqslant i\leqslant r-1, 0\leqslant n\leqslant r-1}$ is an $\mathcal{O}_P$-basis of A. We evaluate the reduced trace of the product of any two basis elements:

$$\mathrm{Trd}(a_i T^n \cdot a_j T^m) = \mathrm{Trd}(a_i \theta^n(a_j) T^{n+m})$$

Therefore, the only nonzero values of the reduced trace are given by:

- Case $n = m = 0$: $\mathrm{Tr}_{L_P/K_P}(a_i a_j)$.
- Case $n + m = r$: $x \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta^n(a_j))$

In the first case, the determinant of the matricial $r \times r$ block $M_0 := (\mathrm{Tr}_{L_P/K_P}(a_i a_j))_{i,j}$ is $\mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)$. In the second case, we set the matrix $N_{i,j} = (\theta^i(a_j))_{i,j}$ and deduce that the determinant of the matricial $r \times r$ block $xM_n := \left(x \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta^n(a_j))\right)_{i,j}$ is $\det(x \cdot N \cdot \theta^n(N^{tr})) = \pm x^r \,\mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)$. Taking the determinant of the entire block

anti-diagonal matrix $\begin{pmatrix} M_0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & xM_{r-1} \\ 0 & 0 & \cdots & xM_{r-2} & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & xM_1 & \cdots & 0 & 0 \end{pmatrix}$ yields

$$\operatorname{disc}(A/\mathcal{O}_P) = \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P) \prod_{n=1}^{r-1} (x^r \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)) = \pm x^{r(r-1)} \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^r$$

We now compute the index of A in Λ_P. By definition, the gauge order Λ_P can be decomposed into a direct sum involving fractional ideals I_P:

$$\Lambda_P = \bigoplus_{i=0}^{r-1} I_P \left(- \left\lfloor \frac{i\, e_P v_P(x)}{r} \right\rfloor \right) \cdot T^i$$

where $I_P(w) = \{(z_Q) \in L_P \mid w_Q(z_Q) \geqslant w \ \forall Q|P\}$. We notice that each quotient $I_P(w)/I_P(w+1)$ has dimension $m_P \cdot f_P = \frac{r}{e_P}$ over the residue field $\mathcal{O}_P/P$. Therefore, the dimension of the quotient space Λ_P/A over $\mathcal{O}_P/P$ is:

$$\dim_{\mathcal{O}_P/P} (\Lambda_P/A) = \frac{r}{e_P} \sum_{i=0}^{r-1} \left\lfloor \frac{i\, v_P(x) e_P}{r} \right\rfloor$$

Using the same computation as in [BC24], we get:

$$\dim_{\mathcal{O}_P/P} (\Lambda_P/A) = \frac{r}{e_P} \left(\frac{r-1}{2} v_P(x) e_P - \frac{r(b_P-1)}{2b_P} \right)$$

We relate the discriminants using the standard formula [NS13, Proposition 2.12]:

$$\operatorname{disc}(\Lambda_P/\mathcal{O}_P) = \operatorname{disc}(A/\mathcal{O}_P) \cdot P^{-2\dim_{\mathcal{O}_P/P}(\Lambda_P/A)}$$

The term $x^{r(r-1)}$ generates the ideal $P^{r(r-1)v_P(x)}$, so we get

$$\operatorname{disc}(\Lambda_P/\mathcal{O}_P) = P^{r(r-1)v_P(x)} \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^r \cdot P^{-r(r-1)v_P(x) + \frac{r^2(b_P-1)}{e_P b_P}}$$

The terms involving $r(r-1)v_P(x)$ in the exponent cancel out, providing the result:

$$\operatorname{disc}(\Lambda_P/\mathcal{O}_P) = P^{\frac{r^2(b_P-1)}{e_P b_P}} \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^r$$

□

2.2 Maximality Criterion for the Gauge Orders

From the discriminant formula of the gauge order Λ_P, we deduce the following criterion for its maximality in the case of a *global* base function field K.

Corollary 2.2.1 (Maximality Criterion)**.**
We assume that K is a global *function field. Then, the gauge order Λ_P is a maximal order in $\mathbb{D}_P$ if and only if we have*

$$\frac{r}{e_P}d_P + \frac{r}{e_P}\frac{b_P - 1}{b_P} = r\frac{\mathrm{ind}_P - 1}{\mathrm{ind}_P}$$

Proof. The discriminant of a maximal order $\mathcal{M}_P$ in a cyclic algebra over a global function field is given by [Rei75, Theorem 32.1] by

$$\mathrm{disc}(\mathcal{M}_P/\mathcal{O}_P) = P^{r^2\frac{\mathrm{ind}_P - 1}{\mathrm{ind}_P}}$$

The gauge order coincides with a maximal order that contains it if and only if the discriminants agree, i.e., if and only if we have $\frac{r^2}{e_P}d_P + \frac{r^2}{e_P}\frac{b_P-1}{b_P} = r^2\frac{\mathrm{ind}_P-1}{\mathrm{ind}_P}$. □

Remark 2.2.2.
This always holds in the unramified case where $e_P = 1$ and $m_P = 1$, as in this case, we have $\mathrm{ind}_P = \frac{r/m_P}{\gcd(v_P(x), r/m_P)} = \frac{r}{\gcd(v_P(x),r)} = b_P$ by [Rei75, Example 32.20] and $d_P = 0$. We note that in the totally split case where $\mathrm{ind}_P = 1$, the maximality criterion boils down to the nonramification condition along with $b_P = 1$ as we must have $d_P = 0$ in this case.

We next exhibit a simple counterexample showing that there exist gauge orders that are not maximal. This is the case for complete local cyclic algebras that are split and whose splitting field is totally ramified for example.

Example 2.2.3.
Let $L = \mathbb{F}_q((\sqrt{t}))$ be our totally ramified splitting field over a constant field of odd characteristic. Let $x = t$ in $\mathbb{F}_q[[t]]$, so that $v(x) = 1$. Let $\mathbb{F}_q((\sqrt{t}))[T; \sqrt{t} \mapsto -\sqrt{t}]/(T^2 - x)$ be our complete local cyclic algebra. We assume $q = 1 \pmod 4$, so that -1 is a square in $\mathbb{F}_q$ and x is a norm. The cyclic algebra is thus totally split. We compute the discriminant $\mathrm{disc}(\Lambda_P/\mathcal{O}_P)$ on the integral basis $(1, \sqrt{t}, \sqrt{t}^{-1}T, T)$ of the gauge order at P. We get $\mathrm{disc}(\Lambda_P/\mathcal{O}_P) = \det\begin{pmatrix} \mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P) & 0 \\ 0 & \mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P) \end{pmatrix}$ as expected. Indeed, the general formula provides in this case $\mathrm{disc}(\Lambda_P/\mathcal{O}_P) = \mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^2 = (t\mathcal{O}_P)^2 = t^2\mathcal{O}_P$. As the discriminant of $\mathrm{Mat}_r(\mathcal{O}_P)$ is $\mathcal{O}_P$, the order Λ_P is not maximal; there exists $G \in \mathrm{GL}_r(K_P)$ such that $\Lambda_P \subsetneq G\,\mathrm{Mat}_r(\mathcal{O}_P)G^{-1}$ and $G\,\mathrm{Mat}_r(\mathcal{O}_P)G^{-1}$ is a maximal order.

Lemma 2.2.4.
We fix L/K a finite cyclic global function field extension. We can find $x \in K$ such that $(x) = P_1 - P_2$ for two inert places $P_1, P_2 \in \mathbb{P}_K$.

Proof. By the Chebotarev density Theorem, [NS13, Theorem 13.4], we can pick three inert places $P_0, P_1, P_2 \in \mathbb{P}_K$ of same degree k for k large enough, so that $P_1 - P_0$ and $P_2 - P_0$ have the same class in the (finite) divisor class group. □

Corollary 2.2.5.
We fix L/K an unramified cyclic global function field extension of order r. We pick x satisfying the condition of Lemma 2.2.4 and set $\mathbb{D} := L[T;\theta]/(T^r - x)$. In this case, our Riemann–Roch Theorem turns out to be a direct corollary of Tamagawa's Theorem [Tam51, Theorem 3] and of our Serre Duality.

Proof. At all places P except P_1 and P_2, we have $\gcd(v_P(x), r) = r$ and in virtue of the index formula corollary 1.2.7 for unramified extensions, we have $\mathrm{ind}_P \mid b_P = \frac{r}{\gcd(r, v_P(x))} = 1$. We deduce $\mathrm{ind}_P = b_P = 1$ at all places P except P_1 and P_2. Now, as the places P_1 and P_2 are both inert and as we have $v_{P_1}(x) = -v_{P_2}(x) = 1$, we get $\gcd(r, v_{P_1}(x)) = \gcd(r, v_{P_2}(x)) = 1$. By lemma [BC24, Lemma 3.1], we thus deduce that $\mathbb{D}_{P_1}$ and $\mathbb{D}_{P_2}$ are division algebras. We thus get $\mathrm{ind}_{P_1} = \mathrm{ind}_{P_2} = b_{P_1} = b_{P_2} = r$. So, the maximality criterion of Corollary 2.2.1 is fulfilled. We can thus apply Tamagawa's Theorem [Tam51, Theorem 3]. □

Remark 2.2.6.
The most efficient LAG codes for a given algebra $\mathbb{D}$ correspond to representations for which the genus is minimal or equivalently for which the adelic gauge order, i.e., the direct sum of the local gauge orders, has minimal discriminant. Unramified splitting fields L/K together with a defining element x of support concentrated in two inert places where it has valuation one are optimal in this sense. Such unramified cyclic extensions can be realized as Hilbert class field extensions of K by the global class field theory for function fields.

3 Tamagawa's Theorem

We present an adelic Riemann–Roch Theorem by Tamagawa published in 1951 in [Tam51], which applies to parallelotopes in adelic vector spaces. This theorem is thus more general than our Riemann–Roch Theorem but less explicit regarding the duality. Nevertheless, our approach is more explicit about LAG code duality than Tamagawa's theory. It allows us to define the duals of LAG codes canonically as Linearized Differential (LD) codes, which are themselves isomorphic to LAG codes over the adjoint algebra. We will use Tamagawa's Theorem as a foundation for the

design of our more general family of codes called ALAG codes, which are based on not necessarily cyclic abelian algebras.

3.1 Riemann Theorem for Parallelotopes

Let K be a function field defined over an arbitrary constant field F. Let $\mathcal{O}_P$ be the valuation ring of K at P. Let $\mathcal{A}_K(0) := \prod_{P\in\mathbb{P}_K} \mathcal{O}_P$ be the adelic maximal order of K. We set

$$M := \oplus_{i=1}^{n} K e_i$$

to be an n-dimensional K-vector space with basis $e = (e_i)_{i=1}^{n}$. We let $M_P := \oplus_{i=1}^{n} K_P e_i$ be its completion at P.

Definition 3.1.1.
We define the adele of M as the $\mathcal{A}_K(0)$-module given by

$$\mathcal{A}_M := \prod_{P\in\mathbb{P}_K}{}' M_P$$

where $\prod'$ denotes the restricted product for which almost every component is equal to $\oplus_{i=1}^{n} \mathcal{O}_P e_i$.

The following definition corresponds to the one given in Tamagawa's paper [Tam51, Section 3].

Definition 3.1.2 (Parallelotopes)**.**
A collection $\Pi := (\Pi_P)_{P\in\mathbb{P}_K}$ of finitely generated torsion-free $\mathcal{O}_P$-modules containing a K_P-basis of M_P, i.e., of full $\mathcal{O}_P$-lattices of M_P, that are almost everywhere equal to $\oplus_{i=1}^{n} \mathcal{O}_P e_i$ is called a parallelotope.

Lemma 3.1.3.
The $\mathcal{O}_P$-module Π_P is free of rank n.

Proof. This follows from the structure theorem for finitely generated modules over principal ideal domains as the $\mathcal{O}_P$-module Π_P is torsion free and finitely generated and as $\mathcal{O}_P$ is a principal ideal domain. □

Definition 3.1.4.
For any divisor $A \in \mathrm{Div}(K)$, we define the adele space of M associated to A by

$$\mathcal{A}_M(A) := \oplus_{i=1}^{n} \mathcal{A}_K(A) e_i \subset \mathcal{A}_M$$

We will use the following alternative definition.

Lemma 3.1.5 (Parallelotopes for Cyclic Algebras)**.**
A $\mathcal{A}_K(0)$-module $\Pi \subset \mathcal{A}_M$ is a parallelotope if and only if the following condition holds

$$\exists A, B \in \mathrm{Div}(K) \text{ such that } A \leqslant B \text{ and } \mathcal{A}_M(A) \subset \Pi \subset \mathcal{A}_M(B)$$

Proof. This condition is sufficient as it obviously implies $\Pi_P = \oplus_{i=1}^n \mathcal{O}_P e_i$ except for a finite number of places $P \in \mathbb{P}_K$ and also by tensoring by K_P over K that Π_P is a torsion-free $\mathcal{O}_P$-module containing a K_P-basis of M_P. Furthermore, setting π_P, a uniformizer of K_P, the condition implies that Π_P is generated by the finite family $(\pi_P^{-B_P+j_i} e_i)_{1\leqslant i\leqslant n, 0\leqslant j_i\leqslant B_P-A_P}$. Thus, Π_P is indeed an $\mathcal{O}_P$-lattice of M_P such that $K_P\Pi_P = M_P$. Conversely, as $\mathcal{O}_P$ is a principal ideal domain, Π_P is free as $\mathcal{O}_P$-module. We can take a $\mathcal{O}_P$-basis $(g_j)_j$ where $g_j = \sum_{i=1}^n g_{i,j} e_i$. Any element $f = \sum_{i=1}^n f_i e_i \in \Pi_P$ can be decomposed on this basis so that $f_i = \sum_j a_j g_{i,j}$ with $a_j \in \mathcal{O}_P$ has coordinate valuations satisfying

$$\min_j(v_P(g_{i,j})) \leqslant v_P(f_i)$$

Thus, setting $B_P = -\min_j(v_P(g_{i,j}))$ provides the upper bound of the condition. Moreover, setting $A_P = -\max_j(v_P(g_{i,j}))$, any $f \in \sum_{i=1}^n f_i e_i \in M_P$ such that

$$v_P(f_i) \geqslant -A_P \quad \forall i$$

can be written uniquely on the g_j basis with $f_i = \sum_j a_j g_{i,j}$ with $a_j = u_j \pi^{v_P(f_i) - \max_i(v_P(g_{i,j}))}$ for some element $u_j \in \mathcal{O}_P$ and so is in the $\mathcal{O}_P$ span of the g_j basis, i.e., in Π_P. □

Definition 3.1.6 (Volume of a Parallelotope)**.**
Denoting by $\mathrm{mat}_e(a_P)$ the matrix representing the basis a_P on the basis e, for $\mathcal{O}_P$-bases a_P of Π_P, the volume of the parallelotope Π is defined as

$$V(\Pi) := -\sum_{P\in\mathbb{P}_K} v_P(\det(\mathrm{mat}_e(a_P)))\deg(P)$$

The volume does not depend on the choice of the $\mathcal{O}_P$-basis a_P as another choice a'_P would result in a representative matrix $\mathrm{mat}_e(a'_P) = \mathrm{mat}_e(a_P)\,\mathrm{mat}_{a_P}(a'_P)$ with $\mathrm{mat}_{a_P}(a'_P)$ invertible in $\mathrm{Mat}_n(\mathcal{O}_P)$ and so of invertible determinant in ${\mathcal{O}_P}^\times$, so of valuation 0. Also, by definition, $\mathrm{mat}_e(a_P)$ is invertible almost everywhere. The following Lemma is taken from [Tam51, Lemma 2].

Lemma 3.1.7.
We assume $\Pi \supset \Pi'$. Then, we have

$$\dim(\Pi/\Pi') = V(\Pi) - V(\Pi')$$

Proof. By the structure theorem for finitely generated modules over principal ideal domains, for all places P of K, we can find a $\mathcal{O}_P$-basis a'_P of Π'_P and a $\mathcal{O}_P$-basis a_P of Π_P such that $a'_{Pi} = d_{Pi}a_{Pi}\ \forall i \in \{0, \cdots, n-1\}$ where the d_{Pi}'s denote the invariant factors of Π_P/Π'_P. For these bases, we have

$$\begin{aligned}\text{length}_{\mathcal{O}_P}(\Pi_P/\Pi'_P) = \sum_{i=0}^{n-1} \text{length}_{\mathcal{O}_P}(\mathcal{O}_P/(d_{Pi})) = \sum_{i=0}^{n-1} v_P(d_{Pi}) \\ = v_P(\prod_{i=0}^{n-1} d_{Pi}) = v_P(\det(\text{mat}_{a_P}(a'_P)))\end{aligned}$$

where $\text{mat}_{a_P}(a'_P)$, the matrix representing a'_P on the $\mathcal{O}_P$-basis a_P is the diagonal matrix with coefficients set to d_{Pi} on the diagonal. Thus, we get

$$\dim_F(\Pi/\Pi') = \sum_{P\in\mathbb{P}_K} v_P(\det(\text{mat}_{a_P}(a'_P)))\deg(P)$$

But, once again, we have $\text{mat}_e(a'_P) = \text{mat}_e(a_P)\,\text{mat}_{a_P}(a'_P)$. Whence, the formula. □

The following Theorem corresponds to [Tam51, Proposition 6].

Theorem 3.1.8 (Riemann Theorem for parallelotopes)**.**
The F-vector spaces $\Pi \cap M$ and $\mathcal{A}_M/(\Pi + M)$ are finite-dimensional and we have

$$\dim(\Pi \cap M) = V(\Pi) - n(g_K - 1) + \dim(\mathcal{A}_M/(\Pi + M))$$

Proof. By Riemann equality on K, there exists $A_1 \in \text{Div}(K)$ sufficiently large, such that the index of speciality $i(A_1) := \dim_F\left(\frac{\mathcal{A}_K}{\mathcal{A}_K(A_1)+K}\right)$ of K for the divisor A_1 is zero, $i(A_1) = 0$ so that $\Pi_1 = \oplus_{i=1}^n \mathcal{A}_K(A_1)e_i$ satisfies $\Pi_1 + M = \oplus_{i=1}^n(\mathcal{A}_K(A_1) + K)e_i = \oplus_{i=1}^n \mathcal{A}_K e_i = \mathcal{A}_M$. Thus, for such a divisor A_1, we have

$$i(\Pi) := \dim(\mathcal{A}_M/(\Pi + M)) = \dim((\Pi_1 + M)/(\Pi + M))$$

Now, by definition Π, being a parallelotope is contained in an adelic space $\oplus_{i=1}^n \mathcal{A}_K(A)e_i$ for some divisor A. We can assume $A_1 \geqslant A$ so that we have the inclusion $\Pi \subset \Pi_1$ and

apply the snake lemma to the following diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Pi \cap M & \longrightarrow & \Pi & \longrightarrow & (\Pi + M)/M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Pi_1 \cap M & \longrightarrow & \Pi_1 & \longrightarrow & (\Pi_1 + M)/M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \frac{\Pi_1 \cap M}{\Pi \cap M} & & \frac{\Pi_1}{\Pi} & & \frac{(\Pi_1+M)/M}{(\Pi+M)/M} & &
\end{array}$$

to obtain the exactness of the third row from that of the two first rows. We get

$$i(\Pi) = \dim((\Pi_1 + M)/(\Pi + M)) = \dim(\Pi_1/\Pi) - (\dim(\Pi_1 \cap M) - \dim(\Pi \cap M))$$

Now, we have $\dim(\Pi_1/\Pi) = V(\Pi_1) - V(\Pi)$ by Lemma 3.1.7. Let $\pi_P^{-A_{1P}} \operatorname{id}_{\mathrm{Mat}_n(K_P)}$ be the diagonal base change matrix from the basis $(e_i)_i$ to the basis $(\pi_P^{-A_{1P}} e_i)_i$, which is obviously an $\mathcal{O}_P$-basis of Π_{1P}. We first compute $V(\Pi_1) := -\sum_{P \in \mathbb{P}_K} v_P(\det(\pi_P^{-A_{1P}} \operatorname{id}_{\mathrm{Mat}_n(K_P)})) \deg(P) = \sum_{P \in \mathbb{P}_K} nA_{1P} \deg(P) = n \deg A_1$. We let $l(A_1)$ be the dimension of the Riemann–Roch space of K associated to the divisor A_1. We note that $\dim(\Pi_1 \cap M) = \sum_{i=1}^n \dim(\mathcal{A}_K(A_1) \cap K) = nl(A_1)$. So, replacing the terms in the formula for $i(\Pi)$, we conclude using the classical Riemann–Roch Theorem

$$n \deg(A_1) - nl(A_1) = n(g_K - 1).$$

□

3.2 Riemann–Roch Theorem for parallelotopes

Definition 3.2.1 (Dual Parallelotopes)**.**
Let $(_,_)$ be a non-degenerate K-bilinear form on M. It extends almost everywhere to a $\mathcal{O}_P$-bilinear form on $\oplus_{i=1}^n \mathcal{O}_P e_i$ and induces a non-degenerate bilinear form on $\mathcal{A}_M$ over $\mathcal{A}_K$ given by

$$\begin{cases} \mathcal{A}_M \times \mathcal{A}_M & \to \mathcal{A}_K \\ (\alpha_1, \alpha_2) & \mapsto ((\alpha_{1P}, \alpha_{2P}))_{P \in \mathbb{P}_K} \end{cases}$$

As α_1 and α_2 belong almost at every place P to $\oplus_{i=1}^n \mathcal{O}_P e_i$, we see that $(\alpha_{1P}, \alpha_{2P})$ belongs almost at every place P to $\mathcal{O}_P$. We denote by $\Pi^\star$ the dual parallelotope of Π with respect to this bilinear form. It is given by

$$\Pi^\star := \{\alpha \in \mathcal{A}_M | (\alpha, \Pi) \subset \mathcal{A}_K(0)\}$$

We recall the definition of Weil differentials on K

$$\mathcal{W}_K := \{f \in \mathrm{Hom}_F(\mathcal{A}_K, F) | \quad \exists A \in \mathrm{Div}(K) \text{ such that } f(\mathcal{A}_K(A) + K) = 0\}.$$

Definition 3.2.2.
We define Weil differentials on M by

$$\mathcal{W}_M := \{f \in \mathrm{Hom}_F(\mathcal{A}_M, F) | \quad \exists A \in \mathrm{Div}(K) \textit{ such that } f(\mathcal{A}_M(A) + M) = 0\}.$$

We define a morphism of vector spaces ϕ from M to $\mathcal{W}_M$.

Definition 3.2.3.
We fix $0 \neq f_0 \in \mathcal{W}_K$. We define the map $\phi : \begin{cases} M & \to \mathcal{W}_M \\ a & \mapsto a \cdot f_0 \end{cases}$ *by*

$$(a.f_0)(\beta) := f_0((a, \beta)) \quad \forall \beta \in \mathcal{A}_M.$$

Lemma 3.2.4.
The map ϕ is an isomorphism of K-vector spaces.

Proof. The map ϕ is injective. Indeed, taking $0 \neq a \in M$, the map $\begin{cases} \mathcal{A}_M & \to \mathcal{A}_K \\ \beta & \mapsto (a, \beta) \end{cases}$ is surjective, as the bilinear form is non-degenerate. Thus, as f_0 is nonzero, we can find $\beta \in \mathcal{A}_M$ such that $f_0((a, \beta)) \neq 0$. We claim that the map ϕ is also surjective. Let $e^\star$ be the dual basis of e. Let $0 \neq f_0 \in \mathcal{W}_K$. Let $a = \sum_{i=1}^n a_i e_i \in M$ with $a_i \in K$ and $\beta = \sum_{i=1}^n \beta_i e_i^\star \in \mathcal{A}_M$ with $\beta_i \in \mathcal{A}_K$. Then, we compute $a.f_0(\beta) = f_0((\sum_{i=1}^n a_i \beta_{i,P})_{P \in \mathbb{P}_K}) = \sum_{i=1}^n (a_i \cdot f_0)((\beta_{i,P})_{P \in \mathbb{P}_K})$. But, we know that $\mathcal{W}_K = K \cdot f_0$ as the Weil differentials of K build a one dimensional vector space over K by [Sti93, Proposition 1.5.9]. Thus, we get $M.f_0 = \oplus_{i=1}^n \mathcal{W}_K$. Finally, as $\mathcal{A}_M \simeq \oplus_{i=1}^n \mathcal{A}_K e_i^\star$, we obtain

$$M.f_0 = \oplus_{i=1}^n \mathcal{W}_K \simeq \mathcal{W}_M.$$

The map ϕ is thus surjective. □

The following Theorem corresponds to [Tam51, Theorem 2]. We give a more detailed proof though. We use the notation (f_0) to denote a canonical divisor of the Weil differential f_0, i.e., a maximal divisor $A \in \mathrm{Div}(K)$ for which f_0 vanishes on $\mathcal{A}_K(A)$ as defined in [Sti93, Definition 1.5.11].

Theorem 3.2.5 (Tamagawa's Theorem)**.**

For any invertible adele $\alpha_0 \in \mathcal{A}_K^\times$, such that $(\alpha_0) = (f_0)$ for some $f_0 \in \mathcal{W}_K$, we have

$$\dim(\Pi \cap M) = V(\Pi) - n(g_K - 1) + \dim(\alpha_0^{-1}\Pi^\star \cap M).$$

Proof. Invoking Theorem 3.1.8, it is enough to prove that $\dim(\mathcal{A}_M/(\Pi + M)) = \dim(\alpha_0^{-1}\Pi^\star \cap M)$ for $\alpha_0 \in \mathcal{A}_K^\times$ such that $(f_0) = (\alpha_0)$ according to Definition 3.2.3. Now pick $\omega \in \mathcal{W}_M$. We set $a \in M$ such that $\phi(a) = \omega \in \mathcal{W}_M$. By Lemma 3.2.4, this preimage exists and is unique. As $f_0(K) = 0$, ω vanishes on $\Pi + M$ if and only if if vanishes on Π. But we see using the definition of a canonical divisor (f_0) as in [Sti93, Definition 1.5.11], that this condition is equivalent to $(f_0) + ((a, \Pi)) \geqslant 0$, that is to say $(\alpha_0) + ((a, \Pi)) = (\alpha_0(a, \Pi)) \geqslant 0$. As α_0 is central, this condition amounts to $((\alpha_0 a, \Pi)) \geqslant 0$, and thus to $a \in \alpha_0^{-1}\Pi^\star \cap M$. We deduce that the following pairing is well defined and perfect

$$\begin{cases} \mathcal{A}_M/(\Pi + M) \times (\alpha_0^{-1}\Pi^\star \cap M) \cdot f_0 & \to F \\ (\alpha, \omega) & \mapsto \omega(\alpha) \end{cases}$$

We deduce that we have

$$\dim(\mathcal{A}_M/(\Pi + M)) = \dim(\alpha_0^{-1}\Pi^\star \cap M).$$

This concludes the proof. □

Remark 3.2.6.
The paper by Mattson, [Mat61], published later, provides essentially the same Riemann–Roch Theorem as Tamagawa's earlier article.

Remark 3.2.7.
In his paper [Gre88], Green develops a Riemann–Roch Theory for any order over any function field in one variable. He gives a hint at the end of his paper [Gre88] to apply his theorem to any semisimple central algebra as it is done in Mattson's paper [Mat61].

Remark 3.2.8.
In Van-Geel's theory [VDVGVO81], the Riemann–Roch Theorem is based on a completely different theoretical setting. The divisors are direct sums of local maximal orders and the algebraic theory is based on the notion of prime ideal in a non-commutative algebra in general instead of the valuation theory, which makes it slightly more general but also much more difficult to apprehend.

4 The Role of Tamagawa's Theorem in Our Riemann–Roch Proof

In this section, we deduce our Riemann Theorem as a corollary of Tamagawa's Theorem, and we outline the proof of our Riemann–Roch Theorem, which also follows from it using our Serre Duality. We set $\mathbb{D} = \frac{L[T;\theta]}{T^r - x}$ for a cyclic function field extension L/K of order r and Galois group generated by θ. We denote by $\delta(L/K)$ the different divisor of L/K, $\delta(L/K) := \sum\limits_{P \in \mathbb{P}_K} \sum_{Q|P} d_P Q \in \mathrm{Div}(L) \subset \mathrm{Div}(\mathbb{D})$ where d_P denotes the different index at Q above P. We will use Theorem 3.1.8 from the previous sections where we replace M (resp. $\mathcal{A}_M$) by $\mathbb{D}$ (resp. $\mathcal{A}_{\mathbb{D}}$), the fixed basis e of M by the K-basis of $\mathbb{D}$ given by $(\lambda_i T^j)_{0 \leqslant i \leqslant r-1, 0 \leqslant j \leqslant r-1}$ where λ_i denotes an integral basis of $\mathcal{O}_{L,P}$ over $\mathcal{O}_P$ and the bilinear form $(_,_)$ by $\mathrm{Trd}(_,_)$.

Lemma 4.0.1 (Adelic Spaces as Parallelotopes)**.**
The adelic space $\mathcal{A}_{\mathbb{D}}(A, W)$ defined in Definition 2.3.16 of Chapter II is a parallelotope in $\mathcal{A}_{\mathbb{D}}$.

Proof. First, $\mathcal{A}_{\mathbb{D}}(A, W)$ is a left $\mathcal{A}_K(0)$-module as the kernel condition is stable under addition and left multiplication by elements of $\mathcal{A}_K(0)$. The definition of a parallelotope is independent of the fixed basis e of $\mathbb{D}$ since for another basis e', we have $\oplus_{i=1}^{r^2} \mathcal{O}_P e_i = \oplus_{i=1}^{r^2} \mathcal{O}_P e'_i$ almost everywhere, since we have $v_P(\det(\mathrm{mat}_e(e'))) = 0$ almost everywhere. So we can use the K-basis $(\lambda_i T^j)_{0 \leqslant j < r, 0 \leqslant i < r}$ of $\mathbb{D}$ where λ_i denotes an integral basis of $\mathcal{O}_{L,P}$ over $\mathcal{O}_P$. By definition, for a decomposition of an element $a \in \mathbb{D}_P$ on that basis $a = \sum_{i,j=0}^{r-1,r-1} a_{i,j} \lambda_i T^j$, we get

$$\omega_Q(a) = \min_j \left(w_Q \left(\sum_i \lambda_i a_{i,j} \right) + j \frac{w_Q(x)}{r} \right)$$

We claim that decomposing (x) in zeros and poles as $(x) = (x)_0 - (x)_\infty$ where $(x)_0$ and $(x)_\infty$ are effective divisors of disjoint support, we have

$$\begin{aligned}
&\oplus_{i=0,j=0}^{r-1,r-1} \mathcal{A}_K \left(\sum_{P \in \mathbb{P}_K} \left\lfloor \frac{\min\limits_{Q|P}(A_Q - (x)_{\infty Q} - \mathrm{CoNr}(D)_Q)}{e_P} \right\rfloor P \right) \lambda_i T^j \\
&\subset \mathcal{A}_{\mathbb{D}}(A - \mathrm{CoNr}(D)) \subset \mathcal{A}_{\mathbb{D}}(A, W) \subset \mathcal{A}_{\mathbb{D}}(A) \\
&\subset \oplus_{i=0,j=0}^{r-1,r-1} \mathcal{A}_K \left(\sum_{P \in \mathbb{P}_K} \left\lceil \frac{\max_{Q|P}(A_Q + (x)_{0Q})}{e_P} \right\rceil P \right) \lambda_i T^j
\end{aligned}$$

We begin by demonstrating the first inclusion. For any $\alpha = \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} \alpha_{i,j} \lambda_j T^i \in \mathcal{A}_{\mathbb{D}}$ with $\alpha_{i,j} \in \mathcal{A}_K$, if we have $e_P v_P(\alpha_{P,i,j}) + (A - (x)_\infty - \mathrm{CoNr}(D))_{Q_0} \geqslant 0 \quad \forall i, j$ for some

$Q_0|P$, then it follows

$$\begin{aligned}\omega_{Q_0}(\alpha_P) + A_{Q_0} - \operatorname{CoNr}(D)_{Q_0} &= \min_{i=0}^{r-1}\left(w_{Q_0}\left(\sum_{j=0}^{r-1}\alpha_{P,i,j}\lambda_j\right) + i\frac{w_{Q_0}(x)}{r}\right) + A_{Q_0} - \operatorname{CoNr}(D)_{Q_0} \\ &\geqslant \min_{i=0,j=0}^{r-1,r-1}(w_{Q_0}(\alpha_{P,i,j})) - (x)_{\infty,Q_0} + A_{Q_0} - \operatorname{CoNr}(D)_{Q_0} \geqslant 0\end{aligned}$$

On the other hand, the second inclusion also holds because if we have for all $Q|P$, $\omega_Q(\alpha_P) + A_Q = \min_{i=0}^{r-1}\left(w_Q\left(\sum_{j=0}^{r-1}\alpha_{P,i,j}\lambda_j\right) + i\frac{w_Q(x)}{r}\right) + A_Q \geqslant 0$, then it follows

$$w_Q\left(\sum_{j=0}^{r-1}\alpha_{P,i,j}\lambda_j\right) + (A + (x)_0)_Q \geqslant 0 \quad \forall Q|P, \forall i \in \{0,\dots,r-1\}$$

Thus, for a uniformizer $\pi_P \in \mathcal{O}_P$ at P, we have

$$w_Q\left(\sum_{j=0}^{r-1}\alpha_{P,i,j}\lambda_j\pi_P^{\left\lceil\frac{\max_{Q|P}(A+(x)_0)_Q}{e_P}\right\rceil}\right) \geqslant 0 \quad \forall Q|P, \forall i \in \{0,\dots,r-1\}.$$

We deduce as λ_j is an integral basis of $\mathcal{O}_{L,P}$ over $\mathcal{O}_P$ and $\sum_{j=0}^{r-1}\alpha_{P,i,j}\lambda_j\pi_P^{\left\lceil\frac{\max_{Q|P}(A+(x)_0)_Q}{e_P}\right\rceil}$ is regular, that we have $v_P\left(\alpha_{P,i,j}\pi_P^{\left\lceil\frac{\max_{Q|P}(A+(x)_0)_Q}{e_P}\right\rceil}\right) \geqslant 0 \quad \forall i,j$ by uniqueness of the decomposition on the K_P vector space. This concludes the proof by Lemma 3.1.5. □

Corollary 4.0.2 (Volume Formula for Adelic Spaces)**.**
For $A, B \in \operatorname{Div}(\mathbb{D})$ and $W \subset V_D$, with $B \geqslant A$, we have

$$V(\mathcal{A}_{\mathbb{D}}(B)) - V(\mathcal{A}_{\mathbb{D}}(A,W)) = r\deg(B) - r\deg(A,W)$$

Proof. From Chapter II, we get $\dim(\mathcal{A}_{\mathbb{D}}(A)/\mathcal{A}_{\mathbb{D}}(A,W)) = r\dim W$. Moreover, we have by [BC24, Lemma 2.5], $\sum_{i=0}^{r-1}\deg(A_i) = r\deg(A) - \frac{r}{2}\deg(\Delta)$ where $A_{i,Q} = \left\lfloor A_Q + i\frac{w_Q(x)}{r}\right\rfloor$.

$$\begin{aligned}\dim(\mathcal{A}_{\mathbb{D}}(B)/\mathcal{A}_{\mathbb{D}}(A)) &= \sum_{i=0}^{r-1}\dim(\mathcal{A}_L(B_i)/\mathcal{A}_L(A_i)) \\ &= \sum_{i=0}^{r-1}(\deg(B_i) - \deg(A_i)) \\ &= r\deg(B) - r\frac{\deg(\Delta)}{2} - r\deg(A) + r\frac{\deg(\Delta)}{2}.\end{aligned}$$

□

4.1 Our Riemann Theorem as a Corollary

Let $A, B \in \mathrm{Div}(\mathbb{D})$, with $B \leqslant A - \mathrm{CoNr}(D)$. We set $M = \mathbb{D}$ and $\Pi = \mathcal{A}_{\mathbb{D}}(A, W)$. We take the non-degenerate bilinear form $\mathrm{Trd}(_,_)$ on $\mathbb{D}$ in place of the bilinear form $(_,_)$. We first compute the volume of our adelic gauge order $\mathcal{A}_{\mathbb{D}}(0) = \prod_{P \in \mathbb{P}_K} \Lambda_P$, where Λ_P is the gauge order of $\mathbb{D}_P$.

Theorem 4.1.1.
We set $v_P(I) := \min_{a \in I}(v_P(a))$ *for any set ideal* $I \subset K_P$ *and* $\deg(\alpha) := \sum_{P \in \mathbb{P}_K} v_P(\alpha_P) \deg P$ *for any* $\alpha \in \mathcal{A}_K$ *. We have*

$$V(\mathcal{A}_{\mathbb{D}}(0)) = -\frac{\deg(\mathrm{disc}(\mathcal{A}_{\mathbb{D}}(0)/\mathcal{A}_K(0)))}{2}$$

Proof. We set an integral basis $\eta^{(P)}$ of Λ_P over $\mathcal{O}_P$. We recall that we set $e = (\lambda_i T^j)_{0 \leqslant i \leqslant r-1, 0 \leqslant j \leqslant r-1}$. But, this choice does not play any role as the determinant of the base change matrix from e to another global basis e' is a principal adele, so that its degree is zero. We let $\mathrm{mat}_e(\eta^{(P)})$ be this base change matrix from $\eta^{(P)}$ to e. We can express the degree of the discriminant as:

$$\begin{aligned}
\deg(\mathrm{disc}(\mathcal{A}_{\mathbb{D}}(0)/\mathcal{A}_K(0))) &= \sum_{P \in \mathbb{P}_K} v_P\Bigg(\det\left(\mathrm{mat}_e(\eta^{(P)})\right) \det\left(\left(\mathrm{Trd}(e_i e_j)\right)_{i,j}\right) \\
&\qquad \cdot \det\left(\mathrm{mat}_e(\eta^{(P)})\right)\Bigg) \deg(P) \\
&= \sum_{P \in \mathbb{P}_K} v_P\left(\det\left(\mathrm{mat}_e(\eta^{(P)})\right)^2\right) \deg(P) \\
&= -2V(\mathcal{A}_{\mathbb{D}}(0))
\end{aligned}$$

The first equality follows from $\det\left(\mathrm{mat}_e(\eta^{(P)})\right) = \det\left(\mathrm{mat}_e(\eta^{(P)})^{tr}\right)$. The second equality follows from the fact that $\left(\det\left(\left(\mathrm{Trd}(e_i e_j)\right)_{i,j}\right)\right)$ being a principal divisor has degree zero. The third equality follows from the definition of the volume of a parallelotope. □

We now prove our Riemann Theorem as a Corollary of 3.1.8.

Theorem 4.1.2 (Riemann Theorem on Cyclic Algebras)**.**
Setting $g_\omega := g_L + \frac{\deg(\Delta)}{2}$*, where* $\Delta = \sum_{P \in \mathbb{P}_K} \sum_{Q|P} \frac{b_P - 1}{b_P} Q$*, we have*

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) - r(g_\omega - 1) + i(A, W)$$

Proof. We have by Theorem 3.1.8

$$\begin{aligned}\dim(\mathcal{A}_{\mathbb{D}}(A,W)\cap\mathbb{D}) =& V(\mathcal{A}_{\mathbb{D}}(A,W)) - V(\mathcal{A}_{\mathbb{D}}(0)) \\ &+ V(\mathcal{A}_{\mathbb{D}}(0)) - r^2(g_K-1) + \dim\left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}}\right)\end{aligned}$$

By Hurwitz's formula [Sti93, Theorem 3.4.13] we have $2g_L - 2 = r\cdot(2g_K-2) + \deg(\delta(L/K))$. It thus suffices to show

$$\lambda_{\mathbb{D}}(A,W) = r\deg(A,W) - \frac{r\deg(\Delta+\delta(L/K))}{2} - r^2(g_K-1) + i(A,W)$$

It is enough to show that all terms match the corresponding equalities.

- We have $\dim(\mathcal{A}_{\mathbb{D}}(A,W)\cap\mathbb{D}) = \lambda_{\mathbb{D}}(A,W)$.
- As shown in Corollary 4.0.2, we have

$$V(\mathcal{A}_{\mathbb{D}}(A,W)) - V(\mathcal{A}_{\mathbb{D}}(0)) = -r\dim W + r\deg(A) = r\deg(A,W)$$

- We get from Theorem 2.1.3 and Theorem 4.1.1, $V(\mathcal{A}_{\mathbb{D}}(0)) = -\frac{1}{2}\sum_{P\in\mathbb{P}_K}\left(\frac{r^2}{e_P}d_P + \frac{r^2}{e_P}\frac{b_P-1}{b_P}\right)\deg(P)$. We conclude using Hurwitz formula.

$$V(\mathcal{A}_{\mathbb{D}}(0)) - r^2(g_K-1) = -\frac{1}{2}\sum_{P\in\mathbb{P}_K}\left(\frac{r^2}{e_P}d_P + \frac{r^2}{e_P}\frac{b_P-1}{b_P}\right)\deg(P) - r^2(g_K-1) \tag{4.1}$$

$$= -\frac{1}{2}\sum_{P\in\mathbb{P}_K}\left(\frac{r^2}{e_P}d_P + \frac{r^2}{e_P}\frac{b_P-1}{b_P}\right)\deg(P) - r(g_L-1) \tag{4.2}$$

$$+ \frac{r}{2}\deg\delta(L/K) \tag{4.3}$$

$$= -\frac{1}{2}\sum_{P\in\mathbb{P}_K}\frac{r^2}{e_P}\frac{b_P-1}{b_P}\deg(P) - r(g_L-1) \tag{4.4}$$

- We have $i(A,W) = \dim\left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}}\right)$

□

4.2 Perspectives on Serre Duality

We deduce the following Corollary from the Theorem 2.3.36 of chapter II on Serre Duality over Cyclic Algebras.

Corollary 4.2.1.
We have

$$i(A,W) = \lambda_{\mathbb{D}^\star}((A,W)^\star)$$

Using this corollary 4.2.1, we recover our Riemann–Roch formula for the dual parallelotope of $\mathcal{A}_{\mathbb{D}}(A,W)$.

Theorem 4.2.2.
Setting $g_\omega := g_L + \frac{\deg(\Delta)}{2}$, *where* $\Delta = \sum_{P\in\mathbb{P}_K}\sum_{Q|P}\frac{b_P-1}{b_P}Q$ *and* $(A,W)^\star := (\mathcal{K} + \mathrm{CoNr}(D) - A, W^\perp)$, *we have*

$$\lambda_{\mathbb{D}}(A,W) = r\deg(A,W) - r(g_\omega - 1) + \lambda_{\mathbb{D}^\star}((A,W)^\star)$$

Proof. We have $\dim\left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A,W)+\mathbb{D}}\right) = \lambda_{\mathbb{D}^\star}((A,W)^\star)$ by Corollary 4.2.1. We conclude by Riemann Theorem 4.1.2. □

We would like to deduce our Riemann–Roch formula directly from the more general Theorem 3.2.5, bypassing Theorem 2.3.36 of Chapter II. To do so, it would suffice to prove that the dual parallelotope of $\mathcal{A}_{\mathbb{D}}(A,W)$ is $\mathcal{A}_{\mathbb{D}^\star}((\Delta + \delta(L/K) + \mathrm{CoNr}(D) - A, W^\perp))^\star$, where $*$ denotes the adjunction. This results from the vanishing lemma 2.3.17 at the evaluation places and from the dual parallelotope of $\mathcal{A}_{\mathbb{D}}(0)$ being $\mathcal{A}_{\mathbb{D}}(\Delta+\delta(L/K)) = \mathcal{A}_{\mathbb{D}^\star}(\Delta+\delta(L/K))^\star$. However, while we can easily show that $\mathcal{A}_{\mathbb{D}}(\Delta+\delta(L/K))$ is orthogonal to $\mathcal{A}_{\mathbb{D}}(0)$, we still have to invoke Theorem 2.3.36 of chapter II in order to prove the reverse inclusion at places P where Λ_P is not maximal.

5 Construction and Decoding of Abelian LAG codes (ALAG)

5.1 Riemann Theorem for Abelian Algebras

We propose a generalization of the construction of LAG codes that we call ALAG codes. It is built upon abelian algebras which we define as multivariate Ore quotient algebras with abelian splitting fields. We endow these abelian algebras with a gauge and compute the discriminant of the gauge order. We then show a Riemann–Roch Theorem for abelian algebras on extended divisors based on Tamagawa's Theorem and on our proof of Serre Duality.

Definition 5.1.1.
Let L/K be an abelian extension of function fields over an arbitrary constant field F.

We define an abelian algebra as the central simple algebra given by

$$\mathbb{D}_{L,x_1,\ldots,x_n} := \frac{L[T_1;\theta_1,\ldots,T_n;\theta_n]}{{T_1}^{r_1}-x_1,\ldots,{T_n}^{r_n}-x_n}$$

where $x_i \in K^\times$ for all i and the θ_i's are independent of order r_i and generate the Galois group of L/K: $\mathrm{Gal}(L/K) = \prod_{i=1}^n \mathbb{Z}/(r_i)$ and where the commuting variables T_i satisfy $T_i\lambda = \theta_i(\lambda)T_i \quad \forall \lambda \in L$.

Remark 5.1.2.
We notice that the orders r_i are pairwise coprime if and only if the abelian Galois group is cyclic. In this case, the abelian algebra $\mathbb{D}_{L,x_1,\ldots,x_n}$ is trivially isomorphic to the cyclic algebra $\mathbb{D}_{L,x}$, where $x = x_1^{r_2\cdots r_n}\cdots x_n^{r_1\cdots r_{n-1}}$. In this case, we also check that the gauge defined on $\mathbb{D}_{L,x_1,\ldots,x_n}$ induces the same genus as that of the corresponding cyclic algebra $\mathbb{D}_{L,x}$,. The whole point of ALAG codes therefore lies in the case of non-cyclic abelian Galois group. However, it can only give rise to a division algebra over an infinite field of constants and not over a finite field of constants.

We endow the abelian algebra $\mathbb{D}_{L,x_1,\ldots,x_n}$ with Q-functions where $Q \in \mathbb{P}_L$. For that, we fix an L-basis of the algebra $\mathbb{D}_{L,x_1,\ldots,x_n}$ given by the monomials $T_1^{k_1}\cdots T_n^{k_n}$. We decompose any element $f \in \mathbb{D}_{L,x_1,\ldots,x_n}$ on this L-basis $f = \sum\limits_{k_1\ldots,k_n} f_{k_1\ldots,k_n} T_1^{k_1}\cdots T_n^{k_n}$.

Definition 5.1.3.
We define the Q-function of f relative to the basis of monomials by

$$\omega_Q^{(x_1,\ldots,x_n)}(f) = \min_{\substack{0\leqslant k_1 < r_1 \\ \cdots \\ 0\leqslant k_n < r_n}} \left(w_Q(f_{k_1\ldots,k_n}) + \frac{k_1}{r_1}w_Q(x_1) + \cdots + \frac{k_n}{r_n}w_Q(x_n)\right)$$

for any $f = \sum_{0\leqslant k_1<r_1\ldots 0\leqslant k_n<r_n} f_{k_1\ldots,k_n} T_1^{k_1}\cdots T_n^{k_n}$ with $f_{k_1\ldots,k_n} \in L$.

Proposition 5.1.4.
Let P be a place of K. The minimum over all places Q above P of the Q-functions, divided by e_P, yields a gauge, i.e., a surmultiplicative valuation.

Proof. We proceed by induction on n. The base case $n = 1$ corresponds exactly to the cyclic case, which is proven in Lemma 2.3.2 of chapter II. For the inductive step, we note that the computation in Lemma 2.3.2 of chapter II relies solely on the ultrametric property and the surmultiplicativity of the underlying valuation w_Q, rather than its strict multiplicativity. Consequently, the exact same algebraic bounds apply when substituting w_Q with the gauge $\omega_P^{(x_1,\ldots,x_{n-1})}$. The surmultiplicativity is thus preserved for $\omega_P^{(x_1,\ldots,x_n)}$. □

Theorem 5.1.5 (Discriminant Formula)**.**
The discriminant of the gauge order Λ_P of $\mathbb{D}_{L,x_1,\ldots,x_n}$ over the discrete valuation ring $\mathcal{O}_P$ at $P \in \mathbb{P}_K$ is given by

$$v_P(\mathrm{disc}(\Lambda_P/\mathcal{O}_P)) = \frac{r^2}{e_P} d_P + \frac{r^2}{e_P} \frac{\mathrm{lcm}(b_{1P},\ldots,b_{nP}) - 1}{\mathrm{lcm}(b_{1P},\ldots,b_{nP})}$$

where b_{iP} is given by

$$b_{iP} := \frac{r_i}{\gcd(w_Q(x_i), r_i)}$$

for $Q|P$ in L, e_P is the ramification index at P, and d_P is the different of L over K at the place P.

Proof. For simplicity, we make the proof for $n = 2$. But it could easily be generalized to any positive integer n. We proceed as in the proof of Theorem 2.1.3. Replacing each x_j by $\pi_P^{-m_j r_j} x_j$ and T_j by $\pi_P^{-m_j} T_j$ for suitable $m_j \in \mathbb{Z}$, we may assume $0 \leqslant v_P(x_j) < r_j$ without changing the integers b_{jP}. Let $(a_0, \ldots, a_{r-1})$ be an $\mathcal{O}_P$-basis of $\mathcal{O}_{L,P}$. Then $(a_i T_1^{n_1} T_2^{n_2})_{0\leqslant i\leqslant r-1, 0\leqslant n_1\leqslant r_1-1, 0\leqslant n_2\leqslant r_2-1}$ is an $\mathcal{O}_P$-basis of $A := \mathcal{O}_{L,P}[T_1;\theta_1,T_2;\theta_2]/(T_1^{r_1} - x_1, T_2^{r_2} - x_2)$. We set the square matrix $N_{i_1,i_2,j} = (\theta_1^{i_1}\theta_2^{i_2}(a_j))_{i_1,i_2,j}$ indexed by $(\{0,\ldots,r_1-1\} \times \{0,\ldots,r_2-1\}) \times \{0,\ldots,r-1\}$ and we evaluate the reduced trace of the product of any two basis elements:

$$\mathrm{Trd}(a_i T_1^{n_1} T_2^{n_2} \cdot a_j T_1^{m_1} T_2^{m_2}) = \mathrm{Trd}(a_i \theta_1^{n_1}\theta_2^{n_2}(a_j) T_1^{n_1+m_1} T_2^{n_2+m_2})$$

Therefore, the only nonzero values of the reduced trace are given by:

- Case $n_1 = m_1 = 0$ and $n_2 = m_2 = 0$: $\mathrm{Tr}_{L_P/K_P}(a_i a_j)$.

  The determinant of the matricial $r \times r$ block $M_{0,0} := (\mathrm{Tr}_{L_P/K_P}(a_i a_j))_{i,j}$ is $\det(N \cdot N^{tr}) = \pm \mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)$.

- Case $n_1 + m_1 = r_1$ and $n_2 + m_2 = r_2$: $x_1 x_2 \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta_1^{n_1}\theta_2^{n_2}(a_j))$.

  The determinant of the matricial $r \times r$ block $x_1 x_2 M_{n_1,n_2} := \left(x_1 x_2 \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta_1^{n_1}\theta_2^{n_2}(a_j))\right)_{i,j}$ is $\det(x_1 x_2 N \cdot \theta_1^{n_1}\theta_2^{n_2}(N^{tr})) = \pm x_1^r x_2^r \,\mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)$.

- Case $n_1 + m_1 = r_1$ and $n_2 + m_2 = 0$: $x_1 \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta_1^{n_1}(a_j))$

  The determinant of the matricial $r \times r$ block $x_1 M_{n_1,0} := \left(x_1 \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta_1^{n_1}(a_j))\right)_{i,j}$ is $\det(x_1 N \cdot \theta_1^{n_1}(N^{tr})) = \pm x_1^r \,\mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)$.

- Case $n_1 + m_1 = 0$ and $n_2 + m_2 = r_2$: $x_2 \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta_2^{n_2}(a_j))$

  The determinant of the matricial $r \times r$ block $x_2 M_{0,n_2} := \left(x_2 \cdot \mathrm{Tr}_{L_P/K_P}(a_i \theta_2^{n_2}(a_j))\right)_{i,j}$ is $\det(x_2 N \cdot \theta_2^{n_2}(N^{tr})) = \pm x_2^r \,\mathrm{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)$.

As in the proof of Theorem 2.1.3, we compute the discriminant of the entire block anti-diagonal matrix $\begin{pmatrix} R_0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & x_2R_{r_2-1} \\ 0 & 0 & \cdots & x_2R_{r_2-2} & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & x_2R_1 & \cdots & 0 & 0 \end{pmatrix}$ where

$R_n := \begin{pmatrix} M_{0,n} & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & x_1M_{r_1-1,n} \\ 0 & 0 & \cdots & x_1M_{r_1-2,n} & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & x_1M_{1,n} & \cdots & 0 & 0 \end{pmatrix}$ for $n \in \{0, \ldots, r_2 - 1\}$.

We compute

$$\operatorname{disc}(R_0/\mathcal{O}_P) = \pm \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P) \cdot \prod_{m=1}^{r_1-1} (x_1^r \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)) = \pm x_1^{r(r_1-1)} \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^{r_1}$$

and for $n \in \{1, \ldots, r_2 - 1\}$,

$$\operatorname{disc}(x_2R_n/\mathcal{O}_P) = \pm x_2^r \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P) \cdot \prod_{m=1}^{r_1-1} (x_1^r x_2^r \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)) = \pm x_2^{rr_1} x_1^{r(r_1-1)} \cdot \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^{r_1}$$

This yields as R_n is a matrix of dimensions $rr_1 \times rr_1$ and as by definition $r = r_1r_2$:

$$\begin{aligned} \operatorname{disc}(A/\mathcal{O}_P) &= \operatorname{disc}(R_0/\mathcal{O}_P) \cdot \prod_{n=1}^{r_2-1} \operatorname{disc}(x_2R_n/\mathcal{O}_P) \\ &= \pm x_1^{r(r_1-1)} \cdot x_2^{rr_1(r_2-1)} x_1^{r(r_1-1)(r_2-1)} \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^{r_1} \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^{r_1(r_2-1)} \\ &= \pm x_2^{rr_1(r_2-1)} x_1^{rr_2(r_1-1)} \operatorname{disc}(\mathcal{O}_{L,P}/\mathcal{O}_P)^r \end{aligned}$$

We now compute the index of A in Λ_P. By definition, the gauge order Λ_P can be decomposed into a direct sum involving fractional ideals I_P:

$$\Lambda_P = \bigoplus_{i_1=0}^{r_1-1} \bigoplus_{i_2=0}^{r_2-1} I_P \left(- \left\lfloor \frac{i_1 e_P v_P(x_1)}{r_1} + \frac{i_2 e_P v_P(x_2)}{r_2} \right\rfloor \right) \cdot T_1^{i_1} T_2^{i_2}$$

where $I_P(w) = \{(z_Q) \in L_P \mid w_Q(z_Q) \geqslant w \ \forall Q|P\}$. We notice that each quotient $I_P(w)/I_P(w+1)$ has dimension $m_P \cdot f_P = \frac{r}{e_P}$ over the residue field $\mathcal{O}_P/P$. Therefore, the dimension of the quotient space Λ_P/A over $\mathcal{O}_P/P$ is:

$$\dim_{\mathcal{O}_P/P}(\Lambda_P/A) = \frac{r}{e_P} \sum_{i_1=0}^{r_1-1} \sum_{i_2=0}^{r_2-1} \left\lfloor \frac{i_1 e_P v_P(x_1)}{r_1} + \frac{i_2 e_P v_P(x_2)}{r_2} \right\rfloor$$

As for $Q|P$, the morphisms

$$\phi : \begin{cases} \mathbb{Z}/(r_1) \times \mathbb{Z}/(r_2) & \to \mathbb{Q}/\mathbb{Z} \\ (i_1, i_2) & \mapsto \frac{i_1 w_Q(x_1)}{r_1} + \frac{i_2 w_Q(x_2)}{r_2} \end{cases}$$

and

$$-\phi : \begin{cases} \mathbb{Z}/(r_1) \times \mathbb{Z}/(r_2) & \to \mathbb{Q}/\mathbb{Z} \\ (i_1, i_2) & \mapsto -\frac{i_1 w_Q(x_1)}{r_1} - \frac{i_2 w_Q(x_2)}{r_2} \end{cases}$$

have same image $(\mathbb{Z}/\operatorname{lcm}(b_{1P}, b_{2P}))/\mathbb{Z}$ of cardinality $\operatorname{lcm}(b_{1P}, b_{2P})$ and same kernel of cardinality $\frac{r}{\operatorname{lcm}(b_{1P}, b_{2P})}$, we deduce, for any $Q|P$, denoting by $\{a\} := a - \lfloor a \rfloor$ the fractional part of a rational number a and using the relation $\{a\} + \{-a\} = \delta_{a \neq 0 \pmod 1}$,

$$\begin{aligned}
&\sum_{i_1=0}^{r_1-1} \sum_{i_2=0}^{r_2-1} \left\{ \frac{w_Q(x_1) r_2 i_1 + w_Q(x_2) r_1 i_2}{r} \right\} \\
&= \frac{1}{2} \left(\sum_{i_1=0}^{r_1-1} \sum_{i_2=0}^{r_2-1} \left\{ \frac{w_Q(x_1) r_2 i_1 + w_Q(x_2) r_1 i_2}{r} \right\} + \sum_{i_1=0}^{r_1-1} \sum_{i_2=0}^{r_2-1} \left\{ \frac{-w_Q(x_1) r_2 i_1 - w_Q(x_2) r_1 i_2}{r} \right\} \right) \\
&= \frac{1}{2} \left(\sum_{i_1=0}^{r_1-1} \sum_{i_2=0}^{r_2-1} \delta_{(i_1,i_2) \notin \ker \phi} \right) = \frac{r(\operatorname{lcm}(b_{1P}, b_{2P}) - 1)}{2 \operatorname{lcm}(b_{1P}, b_{2P})}
\end{aligned}$$

This yields finally:

$$\begin{aligned}
&\dim_{\mathcal{O}_P/P} (\Lambda_P / A) \\
&= \frac{r}{e_P} \left(r_2 r_1 \frac{r_1 - 1}{2 r_1} w_Q(x_1) + r_1 r_2 \frac{r_2 - 1}{2 r_2} w_Q(x_2) - \sum_{i_1=0}^{r_1-1} \sum_{i_2=0}^{r_2-1} \left\{ \frac{w_Q(x_1) r_2 i_1 + w_Q(x_2) r_1 i_2}{r} \right\} \right) \\
&= \frac{r}{e_P} \left(\frac{r_2(r_1 - 1)}{2} v_P(x_1) e_P + \frac{r_1(r_2 - 1)}{2} v_P(x_2) e_P - \frac{r(\operatorname{lcm}(b_{1P}, b_{2P}) - 1)}{2 \operatorname{lcm}(b_{1P}, b_{2P})} \right)
\end{aligned}$$

As in the proof of Theorem 2.1.3, we relate the discriminants using the standard formula [NS13, Proposition 2.12].

$$\begin{aligned}
\operatorname{disc}(\Lambda_P / \mathcal{O}_P) &= \operatorname{disc}(A / \mathcal{O}_P) \cdot P^{-2 \dim_{\mathcal{O}_P/P}(\Lambda_P/A)} \\
&= P^{r r_1 (r_2 - 1) v_P(x_2) + r r_2 (r_1 - 1) v_P(x_1)} \operatorname{disc}(\mathcal{O}_{L,P} / \mathcal{O}_P)^r \\
&\quad \cdot P^{-2 \frac{r}{e_P} \left(\frac{r_2(r_1-1)}{2} v_P(x_1) e_P + \frac{r_1(r_2-1)}{2} v_P(x_2) e_P - \frac{r(\operatorname{lcm}(b_{1P}, b_{2P}) - 1)}{2 \operatorname{lcm}(b_{1P}, b_{2P})} \right)}
\end{aligned}$$

The terms involving $r r_1 (r_2 - 1) v_P(x_2) + r r_2 (r_1 - 1) v_P(x_1)$ in the exponent cancel out, providing the result:

$$\operatorname{disc}(\Lambda_P / \mathcal{O}_P) = P^{\frac{r^2 (\operatorname{lcm}(b_{1P}, b_{2P}) - 1)}{e_P \operatorname{lcm}(b_{1P}, b_{2P})}} \cdot \operatorname{disc}(\mathcal{O}_{L,P} / \mathcal{O}_P)^r$$

□

Definition 5.1.6.
We define the subgroup of divisors of $\mathbb{D}_{L,x_1,\dots,x_n}$ *by*

$$\mathrm{Div}(\mathbb{D}_{L,x_1,\dots,x_n}) := \oplus_{P\in\mathbb{P}_K} \oplus_{Q|P} \frac{\mathbb{Z}}{\mathrm{lcm}(b_{1P},\dots,b_{nP})} Q.$$

We define the subgroup of divisors of $\mathbb{D}_{L,x_1,\dots,x_n}$ *away from the evaluation places by*

$$\mathrm{Div}(\mathbb{D}_{L,x_1,\dots,x_n}, D) := \{A \in \mathrm{Div}(\mathbb{D}_{L,x_1,\dots,x_n}) \mid A_Q = 0 \quad \forall Q|P_i \quad \forall i \in [s]\}.$$

Definition 5.1.7.
For any $A \in \mathrm{Div}(\mathbb{D}_{L,x_1,\dots,x_n})$*, we define the Riemann–Roch space*

$$\Lambda_{\mathbb{D}_{L,x_1,\dots,x_n}}(A) := \{f \in \mathbb{D}_{L,x_1,\dots,x_n} \mid \omega_Q^{(x_1,\dots,x_n)}(f) + A_Q \geqslant 0 \quad \forall Q \in \mathbb{P}_L\}$$

We denote its dimension by $\lambda_{\mathbb{D}_{L,x_1,\dots,x_n}}(A)$*.*

In the same manner, we define the adelic space.

Definition 5.1.8.
We define the adelic space related to the divisor $A \in \mathrm{Div}(\mathbb{D}_{L,x_1,\dots,x_n})$ *as*

$$\mathcal{A}_{\mathbb{D}_{L,x_1,\dots,x_n}}(A) := \left\{(\alpha_P) \in \prod_{P\in\mathbb{P}_K} \mathbb{D}_P \mid \omega_Q^{(x_1,\dots,x_n)}(\alpha_P) + A_Q \geqslant 0 \quad \forall P \quad \forall Q|P\right\}$$

Proposition 5.1.9 (Adelic Spaces as Parallelotopes)**.**
The adelic spaces $\mathcal{A}_{\mathbb{D}_{L,x_1,\dots,x_n}}(A)$ *are parallelotopes in* $\mathcal{A}_{\mathbb{D}_{L,x_1,\dots,x_n}}$*.*

Proof. For simplicity, we prove the Proposition for $n = 2$, but it could easily be generalized to any positive integer n. Using an $\mathcal{O}_P$-basis $(\lambda_i T_1^{j_1} T_2^{j_2})_{0\leqslant i<r, 0\leqslant j_1<r_1, 0\leqslant j_2<r_2}$ of Λ_P over $\mathcal{O}_P$ as in the proof of Lemma 4.0.1, we get for $\alpha = \sum_{i=0}^{r-1}\sum_{j_1=0}^{r_1-1}\sum_{j_2=0}^{r_2-1} \alpha_{i,j_1,j_2}\lambda_i T_1^{j_1} T_2^{j_2}$:

$$\omega_Q^{(x_1,x_2)}(\alpha) = \min_{i,j_1,j_2}\left(w_Q(\lambda_i) + w_Q(\alpha_{i,j_1,j_2}) + j_1\frac{w_Q(x_1)}{r_1} + j_2\frac{w_Q(x_2)}{r_2}\right)$$

Thus, we get:

$$\oplus_{i=0,j_1=0,j_2=0}^{r-1,r_1-1,r_2-1} \mathcal{A}_K\left(\sum_{P\in\mathbb{P}_K}\left\lfloor\frac{\min_{Q|P}(A-(x)_\infty)_Q}{e_P}\right\rfloor P\right)\lambda_i T_1^{j_1}T_2^{j_2} \subset \mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(A)$$
$$\subset \oplus_{i=0,j_1=0,j_2=0}^{r-1,r_1-1,r_2-1} \mathcal{A}_K\left(\sum_{P\in\mathbb{P}_K}\left\lceil\frac{\max_{Q|P}(A+(x)_0)_Q}{e_P}\right\rceil P\right)\lambda_i T_1^{j_1}T_2^{j_2}$$

□

We deduce the following Riemann Theorem relative to our gauge orders.

Theorem 5.1.10 (Riemann Theorem)**.**
For any abelian division algebra, $\mathbb{D}_{L,x_1,\dots,x_n}$, and for any divisor A, we have

$$\lambda_{\mathbb{D}_{L,x_1,\dots,x_n}}(A) = r\deg(A) + r(1-g_\omega) + i(A)$$

where $i(A) := \dim(\frac{\mathcal{A}_{\mathbb{D}_{L,x_1,\dots,x_n}}}{\mathcal{A}_{\mathbb{D}_{L,x_1,\dots,x_n}}(A)+\mathbb{D}_{L,x_1,\dots,x_n}})$
and $g_\omega := g_L + \frac{1}{2}\sum_{P\in\mathbb{P}_K}\sum_{Q|P}\frac{\mathrm{lcm}(b_{1\,P},\dots,b_{n\,P})-1}{\mathrm{lcm}(b_{1\,P},\dots,b_{n\,P})}\deg Q$

Proof. It results from Tamagawa's Riemann Theorem 3.1.8 exposed in chapter 3, using the previous Proposition 5.1.9 and the computation of the discriminant of the gauge orders in 5.1.5 exactly as it was done in section 4. □

5.2 Riemann–Roch Theorem for Abelian Algebras

We now proceed to the definition of the evaluation map of the abelian code. We define $L_i = L^{\theta_1,\cdots,\check{\theta}_i\cdots,\theta_n}$ where $\check{\theta}_i$ means that we omit the i-th automorphism. We observe that the subfields L_i satisfy $\prod_{i=1}^n[L_i:K] = [L:K]$, meaning the extensions L_{iP} are linearly disjoint over K. This structural property allows us to decompose our abelian algebra as a tensor product.

Proposition 5.2.1.
Let $\mathcal{A}_{\mathbb{D}_{L,x_1,\dots,x_n}}$ be the abelian division algebra. We have a natural isomorphism of K-algebras:

$$\phi : \mathbb{D}_{L_1,x_1}\otimes\cdots\otimes_K\mathbb{D}_{L_n,x_n}\xrightarrow{\sim}\mathbb{D}_{L,x_1,\dots,x_n}$$

given by extending the map $a_1T_1^{i_1}\otimes\cdots\otimes a_nT_n^{i_n}\mapsto a_1T_1^{i_1}\cdots a_nT_n^{i_n}$. Furthermore, at any unramified place $P\in\mathbb{P}_K$ satisfying hypothesis **(H2-P)** *for all cyclic sub-algebras $\mathbb{D}_{L_i,x_i}$, (so that $\Lambda_{\mathbb{D}_{L_i,x_i\,P}}\simeq\mathrm{End}_{\mathcal{O}_P}(\mathcal{O}_{L_i,P})$,) the restriction of ϕ on the local gauge orders induces an isomorphism of maximal orders:*

$$\Lambda_{\mathbb{D}_{L_1,x_1\,P}}\otimes_{\mathcal{O}_P}\cdots\otimes_{\mathcal{O}_P}\Lambda_{\mathbb{D}_{L_n,x_n\,P}}\xrightarrow{\sim}\Lambda_{\mathbb{D}_{L,x_1,\dots,x_n\,P}}\simeq\mathrm{End}_{\mathcal{O}_P}(\mathcal{O}_{L,P})$$

Proof. For simplicity, we prove the Proposition for $n=2$, but it could easily be generalized to any positive integer n. The isomorphism of the global algebras follows directly from the linear disjointness of L_1 and L_2 ($L_1\otimes_K L_2\simeq L_1L_2=L$). From the obvious inequality $\omega_P^{(x_1,x_2)}(a_1T_1^ia_2T_2^j)\geqslant\omega_P^{(x_1)}(a_1T_1^i)+\omega_P^{(x_2)}(a_2T_2^j)$ follows that the restriction of ϕ is well defined. Locally, at an unramified and totally split place P, the hypothesis **(H2-P)** for both cyclic subalgebras ensures that $\Lambda_{\mathbb{D}_{L_i,x_i\,P}}$ are maximal

and isomorphic to $\mathrm{End}_{\mathcal{O}_P}(\mathcal{O}_{L_i,P})$ for $i = 1, 2$. The final isomorphism results from $\mathrm{End}_{\mathcal{O}_P}(\mathcal{O}_{L_1,P}) \otimes_{\mathcal{O}_P} \mathrm{End}_{\mathcal{O}_P}(\mathcal{O}_{L_2,P}) \simeq \mathrm{End}_{\mathcal{O}_P}(\mathcal{O}_{L_1,P} \otimes_{\mathcal{O}_P} \mathcal{O}_{L_2,P}) \simeq \mathrm{End}_{\mathcal{O}_P}(\mathcal{O}_{L,P})$. □

Definition 5.2.2.
Assuming the evaluation places P are rational, unramified, and satisfy hypothesis **(H2-P)** *in $\mathbb{D}_{L_i,x_i}$ for $i = 1, \ldots, n$, we define an evaluation morphism $\bar{\varepsilon}_P^{(x_1,\ldots,x_n)}$ at P by linearity on simple tensors as:*

$$\bar{\varepsilon}_P^{(x_1,\ldots,x_n)} : \begin{cases} \Lambda_P & \mapsto \mathrm{Mat}_r(\mathbb{F}_q) \\ a_1 \otimes \cdots \otimes a_n & \mapsto \bar{\varepsilon}_P(a_1) \otimes_{\mathbb{F}_q} \cdots \otimes_{\mathbb{F}_q} \bar{\varepsilon}_P(a_n) \end{cases}$$

Remark 5.2.3.
This definition is well defined by Proposition 5.2.1.

Lemma 5.2.4.
The vanishing Lemma 2.3.17 of chapter II still holds for the evaluation $\bar{\varepsilon}_P^{(x_1,\ldots,x_n)}$ on $\Lambda_{\mathbb{D}_{L,x_1,\ldots,x_n}P}$. For $A \in \mathrm{Div}(\mathbb{D}_{L,x_1,\ldots,x_n}, D)$, we have $\Lambda_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A, V_D) = \Lambda_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A - \mathrm{CoNr}(D))$.

Proof. The kernel of the evaluation map $\bar{\varepsilon}_P^{(x_1,\ldots,x_n)}$ is $\{f \in \Lambda_P \mid \omega_P^{(x_1,\ldots,x_n)}(f) \geqslant 1\}$. □

Lemma 5.2.5.
Let $A \in \mathrm{Div}(\mathbb{D}_{L,x_1,\ldots,x_n}, D)$ and let $f \in \mathbb{D}_{L,x_1,\ldots,x_n}$. If $i \in \{1, \ldots, s\}$ is such that $\omega_{P_i}(f) \geqslant 0$, then

$$\bar{\varepsilon}_{P_i}^{(x_1,\ldots,x_n)}(f^\star) = \bar{\varepsilon}_{P_i}^{(x_1,\ldots,x_n)}(f)^\star$$

Proof. For simplicity, we prove the Proposition for $n = 2$, but it could easily be generalized to any positive integer n. We reuse the notation u_{1,P_i} resp. u_{2,P_i} introduced in Equation (2.3). As in the proof of Lemma 2.3.35 of chapter II, by linearity, it is enough to check that $\langle \bar{\varepsilon}_i(f^\star)(v_i), w_i \rangle = \langle v_i, \bar{\varepsilon}_i(f)(w_i) \rangle$ for $f = f_{j_1,j_2} T_1^{j_1} T_2^{j_2}$ and $v_i, w_i \in V_i$. We compute

$$\bar{\varepsilon}_i(f^\star) = \bar{\varepsilon}_i\left(\frac{T_1^{r_1-j_1}}{x_1^{-1}} \frac{T_2^{r_2-j_2}}{x_2^{-1}} f_{j_1,j_2}\right) = \frac{\theta_1^{r_1-j_1} \circ \theta_2^{r_2-j_2}(f_{j_1,j_2})}{\mathrm{Nr}_{r_1-j_1,r_1}(u_{1,P_i}^{-1}) \mathrm{Nr}_{r_2-j_2,r_2}(u_{2,P_i}^{-1})} \theta_1^{r_1-j_1} \circ \theta_2^{r_2-j_2}$$

Finally, we check

$$\begin{aligned} &\mathrm{Tr}_{V_i/F}\left(\frac{\theta_1^{r_1-j_1} \circ \theta_2^{r_2-j_2}(f_{j_1,j_2})}{\mathrm{Nr}_{r_1-j_1,r_1}(u_{1,P_i}^{-1}) \mathrm{Nr}_{r_2-j_2,r_2}(u_{2,P_i}^{-1})} \theta_1^{r_1-j_1} \circ \theta_2^{r_2-j_2}(v_i) w_i\right) \\ &= \mathrm{Tr}_{V_i/F}(v_i f_{j_1,j_2} \mathrm{Nr}_{0,j_1}(u_{1,P_i}) \mathrm{Nr}_{0,j_2}(u_{2,P_i}) \theta_1^{j_1} \circ \theta_2^{j_2}(w_i)) \end{aligned}$$

□

Definition 5.2.6.
For any $A \in \mathrm{Div}(\mathbb{D}_{L,x_1,\ldots,x_n}, D)$, and any product W of s F-vector subspaces W_i of F^r, we define the Riemann–Roch space

$$\Lambda_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A,W) := \{f \in \mathbb{D}_{L,x_1,\ldots,x_n} \mid \omega_Q^{(x_1,\ldots,x_n)}(f) + A_Q \geqslant 0 \quad \forall P \in \mathbb{P}_K,\ \forall Q \in \mathbb{P}_L \ s.t.\ Q|P \\ \text{and} \quad \ker(\bar{\varepsilon}_{P_i}^{(x_1,\ldots,x_n)}(f)) \supset W_i \ \forall i \in \{1,\ldots,s\}\}$$

We denote its dimension by $\lambda_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A,W)$.

Definition 5.2.7.
We define the adelic space related to the extended divisor (A,W):

$$\mathcal{A}_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A,W) := \left\{ (\alpha_P)_P \in \prod_{P\in\mathbb{P}_K} \mathbb{D}_P \mid \omega_Q^{(x_1,\ldots,x_n)}(\alpha_P) + A_Q \geqslant 0 \quad \forall P, \forall Q|P \right. \\ \left. \text{and} \quad \ker(\bar{\varepsilon}_{P_i}^{(x_1,\ldots,x_n)}(\alpha_{P_i})) \supset W_i \quad \forall i \in \{1,\ldots,s\} \right\}$$

Proposition 5.2.8.
The adelic spaces $\mathcal{A}_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A,W)$ are parallelotopes in $\mathcal{A}_{\mathbb{D}_{L,x_1,\ldots,x_n}}$.

Proof. We obviously have stability by left multiplication and also $\mathcal{A}_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A - \mathrm{CoNr}(D)) \subset \mathcal{A}_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A,W) \subset \mathcal{A}_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A)$. □

We deduce our Riemann–Roch Theorem relative to our gauge orders by invoking our Serre Duality.

Theorem 5.2.9 (Riemann–Roch Theorem)**.**
For any abelian division algebra $\mathbb{D}_{L,x_1,\ldots,x_n}$, any set of totally split, unramified evaluation places, and any extended divisor (A,W), we have

$$\lambda_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A,W) = r\deg(A,W) + r(1-g_\omega) + \lambda_{\mathbb{D}_{L,x_1^{-1},\ldots,x_n^{-1}}}((A,W)^\star)$$

where $(A,W)^\star$ is defined similarly as in Definition 2.3.33 of chapter II by

$$(A,W)^\star := \left(\left(\frac{dt_D}{t_D} \right)_L + \Delta + \mathrm{CoNr}(D) - A, W^\perp \right)$$

where the different of the gauge order Δ is defined by

$$\Delta := \sum_{P\in\mathbb{P}_K} \sum_{Q|P} \frac{\mathrm{lcm}(b_{1P},\ldots,b_{nP}) - 1}{\mathrm{lcm}(b_{1P},\ldots,b_{nP})} Q$$

and where $g_\omega := g_L + \frac{1}{2}\deg\Delta$. Moreover, if $\deg(A,W) < 0$, then we have $\lambda_{\mathbb{D}_{L,x_1,\ldots,x_n}}(A,W) = 0$.

Proof. For simplicity, we prove the Proposition for $n = 2$, but it could easily be generalized to any positive integer n. It results from the Riemann Theorem 5.1.10 and Serre Duality Theorem 4.2.1. Proceeding as in Corollary 4.0.2, we get $\dim(\mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(A)/\mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(A,W)) = r\dim W$ and $\sum_{i_1=0}^{r_1-1}\sum_{i_2=0}^{r_2-1}\deg(A_{i_1,i_2}) = r\deg(A) - \frac{r}{2}\deg(\Delta)$ where $(A_{i_1,i_2})_Q = \left\lfloor A_Q + i_1\frac{w_Q(x_1)}{r_1} + i_2\frac{w_Q(x_2)}{r_2}\right\rfloor$. We deduce

$$\begin{aligned}\dim(\mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(B)/\mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(A)) &= \sum_{i_1=0}^{r_1-1}\sum_{i_2=0}^{r_2-1}\dim(\mathcal{A}_L(B_{i_1,i_2})/\mathcal{A}_L(A_{i_1,i_2}))\\ &= \sum_{i_1=0}^{r_1-1}\sum_{i_2=0}^{r_2-1}(\deg(B_{i_1,i_2})-\deg(A_{i_1,i_2}))\\ &= r\deg(B) - r\frac{\deg(\Delta)}{2} - r\deg(A) + r\frac{\deg(\Delta)}{2}.\end{aligned}$$

Thus, the parallelotope $\mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(A,W)$ has volume $V(\mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(0)) + r\deg(A,W)$. We now apply the Riemann Theorem to the parallelotope $\mathcal{A}_{\mathbb{D}_{L,x_1,x_2}}(A,W)$. In order to compute the remaining index of speciality, we establish the Serre Duality by reusing the proof of Theorem 2.3.36 in chapter II. The Serre Duality follows from the vanishing Lemma 5.2.4 and the fact that we only care about the monomial of zero degree in $hg^\star$ since the others vanish in the reduced trace. For $g = \sum_{i_1=0}^{r_1-1}\sum_{i_2=0}^{r_2-1} g_{i_1,i_2}\tilde{T_1}^{i_1}\tilde{T_2}^{i_2} \in \mathbb{D}^\star_{L,x_1,x_2} \simeq L[\tilde{T_1};\theta_1,\tilde{T_2};\theta_2]/(\tilde{T_1}^{r_1} - x_1^{-1}, \tilde{T_2}^{r_2} - x_2^{-1})$ such that $\omega_Q(g) \geqslant -A_Q\ \forall Q|P$ and $h = \sum_{i_1=0}^{r_1-1}\sum_{i_2=0}^{r_2-1} h_{i_1,i_2}T_1^{i_1}T_2^{i_2} \in \mathbb{D}_{L,x_1,x_2}$ such that $\omega_Q(h) \geqslant -A'_Q\ \forall Q|P$, we thus have:

$$\begin{aligned}\omega_Q(hg^\star) &= \omega_Q(\sum_{i_1=0}^{r_1-1}\sum_{i_2=0}^{r_2-1} h_{i_1,i_2}T_1{}^{i_1}T_2{}^{i_2}T_2{}^{-i_2}T_1{}^{-i_1}g_{i_1,i_2})\\ &\geqslant \omega_Q(h_{i_{1Q},i_{2Q}}g_{i_{1Q},i_{2Q}})\\ &= \omega_Q(h_{i_{1Q},i_{2Q}}T_1^{i_{1Q}}T_2^{i_{2Q}}) + \omega_Q(x_1^{-1}x_2^{-1}g_{i_{1Q},i_{2Q}}T_1^{r_1-i_{1Q}}T_2^{r_2-i_{2Q}})\\ &= \omega_Q(h_{i_{1Q},i_{2Q}}T_1^{i_{1Q}}T_2^{i_{2Q}}) + \omega_Q(g_{i_{1Q},i_{2Q}}\tilde{T_1}^{i_{1Q}}\tilde{T_2}^{i_{2Q}})\\ &\geqslant -A'_Q - A_Q\end{aligned}$$

for some indices i_{1Q}, i_{2Q} such that the Q-function is minimal on the summand $h_{i_{1Q},i_{2Q}}g_{i_{1Q},i_{2Q}}$. This inequality shows that the pairing is well defined. The rest of the proof remains identical to that of Theorem 4.2.1. □

5.3 ALAG Code Construction

We set an evaluation divisor $D = P_1 + \ldots + P_s$ where each evaluation place P_i is a rational unramified evaluation place that satisfies hypothesis **(H2-P_i)** in $\mathbb{D}_{L_i,x_i}$ for

$i = 1, \dots, n$. We pick a divisor $A \in \mathrm{Div}(\mathbb{D}_{L,x_1,\dots,x_n}, D)$ whose support is disjoint from the support of D and whose degree satisfies $\deg(A) < rs$ to ensure the injectivity of the evaluation map by the vanishing lemma 5.2.4.

Definition 5.3.1.
We define the ALAG code $\mathrm{ALAG}_{\mathbb{D}_{L,x_1,\dots,x_n}}(A, D)$ *as the image of* $\Lambda_{\mathbb{D}_{L,x_1,\dots,x_n}}(A)$ *by the evaluation map* $\bar{\varepsilon}_D^{(x_1,\dots,x_n)} : \begin{cases} \Lambda_{\mathbb{D}_{L,x_1,\dots,x_n}}(A) & \to \mathrm{Mat}_r(\mathbb{F}_q)^s \\ f & \mapsto (\bar{\varepsilon}_{P_i}^{(x_1,\dots,x_n)}(f))_{i\in\{1,\dots,s\}} \end{cases}$.

$$\mathrm{ALAG}_{\mathbb{D}_{L,x_1,\dots,x_n}}(A, D) := \bar{\varepsilon}_D^{(x_1,\dots,x_n)}(\Lambda_{\mathbb{D}_{L,x_1,\dots,x_n}}(A))$$

As a proof of concept, we apply the same decoding algorithm as in the LAG case and provide a SageMath implementation demonstrating a defect relative to the Singleton bound of $2g_\omega$, as for the LAG decoding algorithm.

5.4 SageMath Implementation of ALAG Decoding

We assume that the evaluation places split completely in L and illustrate the ALAG construction and decoding over a finite field of constants with a SageMath implementation available at `https://plmlab.math.cnrs.fr/drain/alag-decoding`. We also assume r_1 and r_2 are not coprime in order to treat the case of interest of a non-cyclic abelian algebra. As we moreover implement ALAG codes for a finite alphabet, i.e., over a finite field of constants, the algebra $\mathbb{D}_{L,x_1,x_2}$ cannot be a division algebra and necessarily contains nonzero zero divisors. Indeed, the algebra has torsion $\mathrm{lcm}(r_1, r_2)$ in the Brauer group and its exponent in the Brauer group is equal to its index over our global central function field by Theorem 1.2.5. Nevertheless, ALAG codes can still be decoded using the LAG decoding algorithm. Indeed, by properly choosing x_1 and x_2 with $x_1 \neq x_2$ and with (x_1) and (x_2) inert, we expect this choice to exclude the potential failures due to nonzero zero divisors. In the example below, we make such a choice in the case $r_1 = 2$ and $r_2 = 2$, so the abelian Galois group of the splitting field is $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ and the index of the algebra is 2.

We take L_1 and L to be defined by

$$\begin{cases} y^2 + y &= t + t^3 \text{ over } \mathbb{F}_{16}(t) \\ z^2 + z &= t + t^2 + t^3 \text{ over } L_1 \end{cases}$$

We set

$$\begin{cases} x_1 &= \alpha + t \\ x_2 &= \frac{\alpha+1+t}{\alpha+t} \end{cases} \quad \theta_1 : \begin{cases} L &\to L \\ y &\mapsto y + 1 \end{cases} \text{ and } \theta_2 : \begin{cases} L &\to L \\ z &\mapsto z + 1 \end{cases}$$

We define $L_2 := L^{\theta_1}$ (the subfield of L fixed by θ_1) and $L_1 := L^{\theta_2}$ (the subfield of L

fixed by θ_2). We obtain an abelian algebra of index 2:

$$\frac{L[T_1;\theta_1,T_2;\theta_2]}{{T_1}^2-x_1,{T_2}^2-x_2}$$

At an evaluation (unramified,splitting) place P, for $T_1 \in \frac{\mathcal{O}_{L_1,P}[T_1;\theta_1]}{{T_1}^2-x_1}$, $T_2 \in \frac{\mathcal{O}_{L_2,P}[T_2;\theta_2]}{{T_2}^2-x_2}$, and $\lambda_1\lambda_2 \in L_1L_2 = L$, we get the following representations in $\Lambda_{\mathbb{D}_{L_1,x_1}}$, $\Lambda_{\mathbb{D}_{L_2,x_2}}$, and $\Lambda_{\mathbb{D}_{L,x_1,x_2}}$:

$$\bar{\varepsilon}_P^{(1)}(T_1)=\begin{pmatrix}0 & \overline{x_1}\\ 1 & 0\end{pmatrix},\bar{\varepsilon}_P^{(1)}(\lambda_1)=\begin{pmatrix}\overline{\lambda_1} & 0\\ 0 & \overline{\theta_1(\lambda_1)}\end{pmatrix},\bar{\varepsilon}_P^{(2)}(T_2)=\begin{pmatrix}0 & \overline{x_2}\\ 1 & 0\end{pmatrix},\bar{\varepsilon}_P^{(2)}(\lambda_2)=\begin{pmatrix}\overline{\lambda_2} & 0\\ 0 & \overline{\theta_2(\lambda_2)}\end{pmatrix}$$

$$\bar{\varepsilon}_P^{(x_1,x_2)}(T_1)=\begin{pmatrix}0 & \overline{x_1} & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & \overline{x_1}\\ 0 & 0 & 1 & 0\end{pmatrix},$$

$$\bar{\varepsilon}_P^{(x_1,x_2)}(T_2)=\begin{pmatrix}0 & 0 & \overline{x_2} & 0\\ 0 & 0 & 0 & \overline{x_2}\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{pmatrix},$$

$$\bar{\varepsilon}_P^{(x_1,x_2)}(\lambda_1\lambda_2)=\begin{pmatrix}\overline{\lambda_1\lambda_2} & 0 & 0 & 0\\ 0 & \overline{\theta_1(\lambda_1)\lambda_2} & 0 & 0\\ 0 & 0 & \overline{\lambda_1\theta_2(\lambda_2)} & 0\\ 0 & 0 & 0 & \overline{\theta_1(\lambda_1)\theta_2(\lambda_2)}\end{pmatrix}.$$

The corresponding SageMath use case is computed below.

Biquadratic Artin–Schreier extension over $\mathbb{P}^1$.

```
sage: load('ALAG_decoding.sage')
None
sage: F = GF(16)
sage: DLx = DivisionAlgebra(F=F, r1=2, r2=2, pol_L1_arg = [0,1,0,1], pol_L2_arg =
    [0,1,1,1], pol_x1_arg=[F.gen(),1], pol_x1_denom_arg=[1], pol_x2_arg=[F.gen()+1,1],
    pol_x2_denom_arg=[F.gen(),1])
```

The abelian algebra $\mathbb{D}_{L,x_1,x_2}$ of genus 4 is given by the following presentation:

$$\mathbb{D}_{L,x_1,x_2}=\frac{\frac{\mathbb{F}_{16}(t)[y1]}{\frac{y1^2-y1-(t^3+t)}{y^2-y-(t^3+t^2+t)}}[y]}{(T_1^2-(t+z4),T_2^2-((t+z4+1)/(t+z4)))}[T_1;\theta_1,T_2;\theta_2].$$

```
sage: LAG = LinearizedAGCode(DLx=DLx, degA=DLx.degAmean())
sage: omega = LAG.maximal_decodable_error_weight()
sage: omega
1
sage: error = LAG.random_error(omega)
sage: word = LAG.random_codeword()
sage: message = word + error
sage: decoded_error = LAG.decode_msg(message) # DECODING ...
sage: decoded_error == error # CHECKING THE RESULT
True
sage: error  # RANDOM ERROR
[0, 0, 0, 0]
[0, 0, 0, 0]
[0, 0, 0, 0]
[0, 0, 0, 0]

[               z4^2,  z4^3 + 1,               z4,  z4^2 + 1]
[               z4^3,         1,            z4^2, z4^3 + z4]
[z4^3 + z4^2 + z4 + 1, z4^3 + z4, z4^3 + z4^2 + z4,      z4^3]
[                  0,         0,                0,         0]

[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
[0, 0, 0, 0] | [0, 0, 0, 0]
sage: (LAG.parameters,DLx.gD,LAG.parameters['k']+DLx.r1*DLx.r2*LAG.parameters['d']==
    LAG.parameters['n']+DLx.r1*DLx.r2 - DLx.gD*DLx.r1*DLx.r2) #PARAMETERS : ALMOST
    MSRD
({'n': 64, 'k': 20, 'd': 8}, 4, True)
sage: floor((LAG.parameters['d']-LAG.gD-1)/2) == omega # DECODING DEFECT G/2
True
```

Finally, the following test completed 10,000 iterations without failure for every admissible error weight tested. The abelian algebra $\mathbb{D}_{L,x_1,x_2}$ of genus 4 under test is given by the presentation:

$$\mathbb{D}_{L,x_1,x_2} = \frac{L[T_1;\theta_1,T_2;\theta_2]}{(T_1^2 - t, T_2^2 - (t + z_6))}$$

where $L = \frac{\frac{\mathbb{F}_{64}(t)[y_1]}{y_1^2 - y_1 - (t^3+t)}[y_2]}{y_2^2 - y_2 - (t^3+t^2+t)}$. The number of evaluation places is set to 8. The ranks of the matrices representing the random error follow the uniform discrete distribution.

Chapter IV

Conclusion and Perspectives

1 Conclusion

Skew polynomial rings provide a highly effective framework for advancing the theory of sum-rank metric codes. Our work exploits this framework to construct skew cyclic codes, enumerate self-dual skew cyclic codes, and, most significantly, construct Linearized Algebraic Geometry (LAG) codes, characterize their duality, and decode them along with their ALAG generalizations. Skew polynomials not only allow efficient implementations of these codes but also enable explicit proofs of fundamental theorems such as the Riemann–Roch theorem and Serre duality. The key contributions of this work are the following:

- **Coding Theory:** We established that skew polynomial rings enable efficient enumeration of skew cyclic codes and an efficient decoding algorithm for the sum-rank metric LAG codes as well as for their experimental/conjectural extensions to ALAG codes.
- **Theoretical Foundations:** We provide a Riemann–Roch theorem, which is less general but more explicit than Tamagawa's original Riemann–Roch Theorem on semisimple central algebras.
- **Implementation in SageMath:** Our theoretical findings were confirmed and illustrated by our SageMath implementations over finite fields. We were thus able to produce numerical evidence of the theoretical results and provide a powerful tool for further investigations and prospects. While our decoding algorithm remains unproven in the case of abelian algebras, our LAG decoding as well as our self-dual skew cyclic code enumeration work as designed and proved.

2 Perspectives

Regarding skew cyclic codes, the inseparable case could be investigated using more powerful tools such as Morita equivalence and Iwasawa decomposition instead of skew polynomial factorization. This may lead, also in the inseparable case, to a non-redundant cubic-time enumeration algorithm together with a counting formula.

Regarding LAG codes, building upon the work of Tamagawa, it would be natural to apply the Riemann–Roch Theorem on any central semisimple algebra, abelian (case of ALAG codes, the constant field being necessarily infinite in this non-cyclic case) or non-abelian for any extended divisor in a broader sense corresponding to arbitrary parallelotopes to give a more generic generalization of LAG Codes and their decoding algorithm.

Finally, in a more challenging way, for division algebras over function fields of dimension greater than 1, as surfaces, we would like to prove a Riemann–Roch Theorem and a Serre duality, in order to give a construction and a characterization of the duality of the associated LAG codes and to provide a polynomial decoding algorithm. However, the abelian Ore construction would not be general anymore in this case, even with a finite field of constants, as some division algebras over function fields of transcendence degree greater than 2 over a finite field of constants are not crossed product and cannot be a priori endowed with a gauge.

Bibliography

[Art11] M. Artin. *Algebra*. Pearson Education, 2011.

[BBB20] A. Batoul, D. Boucher, and R. Boulanouar. A construction of selfdual skew cyclic and negacyclic codes of length n over $\mathbb{F}_{p^n}$. In *WAIFI 2020: Arithmetic of Finite Fields*, volume 12542 of *Lecture Notes in Computer Science*, RENNES, France, July 2020.

[BC24] E. Berardini and X. Caruso. Algebraic geometry codes in the sum-rank metric. *IEEE Transactions on Information Theory*, 70(5):3345–3356, May 2024.

[BC25] E. Berardini and X. Caruso. Reed–Muller codes in the sum-rank metric. *Journal of Algebra and Its Applications*, April 2025.

[BCD26] E. Berardini, X. Caruso, and F. Drain. Duality and decoding of lag codes, 2026.

[BGU06] D. Boucher, W. Geiselmann, and F. Ulmer. Skew-cyclic codes, 2006.

[Bou15] D. Boucher. A note on the existence of self-dual skew codes over finite fields. In *Codes, cryptology, and information security. First international conference, C2SI 2015, Rabat, Morocco, May 26–28, 2015. Proceedings – in honor of Thierry Berger*, pages 228–239. Cham: Springer, 2015.

[Bou16] D. Boucher. Construction and number of selfdual skew codes over F_{p^2}. *Advances in Mathematics of Communications*, Volume 10(Issue 4):765 – 795, November 2016.

[BR16] E. Byrne and A. Ravagnani. Covering radius of matrix codes endowed with the rank metric, 2016.

[BU14] D. Boucher and F. Ulmer. Self-dual skew codes and factorization of skew polynomials. *Journal of Symbolic Computation*, 60:47–61, 01 2014.

[Car21] X. Caruso. A theory of residues for skew rational functions. *Journal de l'École polytechnique — Mathématiques*, 8:1159–1192, 2021.

[CB17] X. Caruso and J. Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *Journal of Symbolic Computation*, 79:411–443, 2017.

[CD23] X. Caruso and A. Durand. Duals of linearized Reed–Solomon codes. *Designs, Codes and Cryptography*, 91(1):241–271, 2023.

[CD25] X. Caruso and F. Drain. Selfdual skew cyclic codes: Selfdual skew cyclic codes. *Des. Codes Cryptography*, 93(12):5487–5516, September 2025.

[Coh10] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer Publishing Company, Incorporated, 2010.

[For17] T.J. Ford. *Separable Algebras*. Graduate Studies in Mathematics. American Mathematical Society, 2017.

[Gab85] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.

[Gop81] V. D. Goppa. Codes on algebraic curves. 1981.

[Gre88] B. Green. On the riemann-roch theorem for orders in the ring of valuation vectors of a function field. *manuscripta mathematica*, 60(3):259–276, 1988.

[GS95] A. Garcia and H. Stichtenoth. A tower of artin-schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Inventiones mathematicae*, 121(1):211–222, 1995.

[Han05] G. Hanlon. Counting points in sp(2n, fq) maximal parabolic subgroup. 04 2005.

[Jac96] N. Jacobson. Finite dimensional division algebras over fields. 1996.

[Ker90] I. Kersten. *Brauergruppen von Körpern*. Vieweg, 1990.

[Mat61] H. F. Mattson. A generalization of the Riemann-Roch theorem. *Illinois Journal of Mathematics*, 5(3):355–375, 1961.

[Mil20] J.S. Milne. *Fields and Galois theory*. 2020.

[MP18a] U. Martínez-Peñas. Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *J. Algebra*, 504:587–612, 2018.

[MP18b] U. Martínez-Peñas. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring, 2018.

[MPK19] U. Martínez-Peñas and F. R. Kschischang. Reliable and secure multishot network coding using linearized Reed–Solomon codes. *IEEE Transactions on Information Theory*, 65(8):4785–4803, 2019.

[MPSK22] U. Martínez-Peñas, M. Shehadeh, and F. R. Kschischang. Codes in the sum-rank metric: fundamentals and applications. *Foundations and Trends in Communications and Information Theory*, 19(5):814–1031, 2022.

[NS13] J. Neukirch and N. Schappacher. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[Ore33] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933.

[PA71] G. Pólya and G.L. Alexanderson. Gaussian binomial coefficients. *Elemente der Mathematik*, 26:102–109, 1971.

[Ple65] V. Pless. The number of isotropic subspaces in a finite geometry. *Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat.*, 39:418–421, 1965.

[PV24] Elad Paran and Thieu N Vo. Noether's normalization in skew polynomial rings. *arXiv preprint arXiv:2407.12686*, 2024.

[Rei75] I. Reiner. *Maximal Orders*. Institute for Research on Poverty Monograph Series. Academic Press, 1975.

[RS60] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[Sch85] W. Scharlau. *Quadratic and Hermitian Forms*. Grundlehren der mathematischen Wissenschaften. World Publishing Corporation, 1985.

[Seg59] B. Segre. Le geometrie di galois. *Annali di Matematica Pura ed Applicata*, 48:1–96, 1959.

[Sha48] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[Sha13] I. R. Shafarevich. *Basic algebraic geometry; 3rd ed.* Springer, Berlin, 2013.

[Sta26] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2026.

[Sti93] H. Stichtenoth. *Algebraic function fields and codes*. Universitext (Berlin. Print). Springer-Verlag, 1993.

[Tam51] T. Tamagawa. On the theorem of Riemann-Roch. *J. Fac. Sci., Univ. Tokyo, Sect. I*, 6:133–144, 1951.

[VDVGVO81] J. P. Van Deuren, J. Van Geel, and F. Van Oystaeyen. Genus and a riemann-roch theorem for non-commutative function fields in one variable. pages 295–318, 1981.

[Wad00] A. Wadsworth. Valuation theory on finite dimensional division algebras. *Fields Inst. Commun.*, 32, 12 2000.

[Wis91] R. Wisbauer. *Foundations of Module and Ring Theory: A Handbook for Study and Research (1st ed.)*. 1991.

[Wit34] E. Witt. *Riemann-Roch-Satz und Zeta-Funktion im hyperkomplexen*. Dissertation, University of Göttingen, 1934. Thesis directed by Emmy Noether.