Résidus de 2-formes différentielles sur les surfaces algébriques et applications aux codes correcteurs d'erreurs

Alain Couvreur

Thèse de l'Université de Toulouse

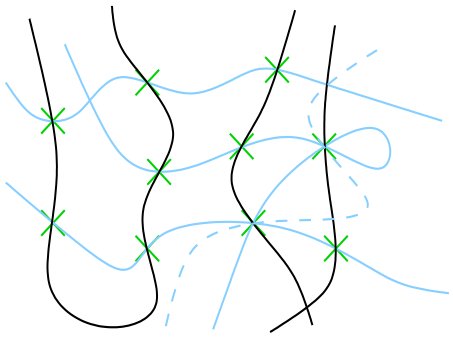
Résidus de 2-formes différentielles sur les surfaces algébriques et application aux codes correcteurs d'erreurs

par Alain Couvreur

Soutenue le lundi 8 décembre à 16h
dans l'amphithéâtre Schwartz

Jury

Emmanuel Hallouin	Université de Toulouse II	Examinateur
Gilles Lachaud	Université d'Aix-Marseille II	Examinateur
Marc Perret	Université de Toulouse II	Directeur
Marc Reversat	Université de Toulouse III	Directeur
Felipe Voloch	University of Texas	Rapporteur
Gilles Zemor	Université de Bordeaux I	Examinateur



Institut de Mathématiques de Toulouse, UMR 5219, UFR MIG
Laboratoire Émile Picard,
Université Paul Sabatier 31062 TOULOUSE Cédex 9

Ce qui nous rassure du sommeil, c'est qu'on en sort,
et qu'on en sort inchangé, puisqu'une interdiction bizarre
nous empêche de rapporter avec nous l'exact résidu de nos songes.

Marguerite Yourcenar
Mémoires d'Hadrien

Remerciements

Quelques mois avant de commencer ma thèse, une jeune chercheuse qui me vantait les mérites de la recherche avait formulé cette mise en garde : “une thèse, c'est difficile, on est très seul.” Je suis convaincu qu'une écrasante majorité de doctorant(e)s - dont je fais partie - a éprouvé ce sentiment au moins une fois. Pourtant, maintenant que la rédaction de ma thèse touche à sa fin, je réalise à quel point rien de tout ce que j'ai fait n'aurait été possible si j'avais réellement été seul.

Très souvent, les premières lignes d'un livre sont celles que l'auteur a écrit en dernier. Cette thèse n'échappe pas à la règle. De la même manière, mes premiers remerciements vont vers les acteurs du dénouement.

Ceux sans qui cette thèse ne pourrait se terminer. Je remercie les six personnes qui ont accepté de composer mon jury. Tout d'abord, Marc Reversat sans qui mon intégration dans l'ex-laboratoire Émile Picard n'aurait pas été possible. Ma gratitude va ensuite à Gilles Lachaud, directeur de mon directeur, pour son accueil chaleureux à l'IML au début de cette année. Un grand merci également à Gilles Zemor pour tout ce qu'il m'a appris lors de ma visite à Télécom Paris ainsi que pour les pertinentes corrections qu'il a suggéré pour ce manuscrit. Je remercie ensuite Felipe Voloch pour son accueil et son encadrement durant mon séjour à l'Université du Texas, je le remercie également d'avoir accepté de rapporter ma thèse. Je remercie bien sûr mon directeur Marc Perret, mais j'y reviendrai un peu plus loin... Enfin, je remercie Emmanuel Hallouin pour ses nombreux conseils tout au long de ma thèse. Je garderai un excellent souvenir des discussions de politique ou d'algèbre locale que nous avons eues ensemble.

Je remercie par ailleurs Dino Lorenzini pour toutes ses remarques et pertinentes suggestions sur mon manuscrit. Je lui suis également reconnaissant d'avoir accepté de rapporter ma thèse. Pour la même raison, je remercie sincèrement le troisième rapporteur de cette thèse Michael Tsfasman.

L'équipe de la dernière ligne droite. Merci à Matthieu et Aurélie qui ont sans aucune hésitation accepté que leur appartement soit envahi et leur cuisine dévastée, l'espace d'un week-end. Merci également à Tiphaine qui, durant la préparation du pot, n'a jamais rechigné à nettoyer tout couvert dégoulinant de chocolat fondu.

Ceux qui murmurent à l'oreille des processeurs. Face aux nombreux soucis dus à un ordinateur récalcitrant, j'ai toujours bénéficié d'une assistance mail ou téléphonique d'une efficacité remarquable. À ce titre, je remercie Maxime, grâce à qui ma version d'Emacs est si performante qu'elle serait presque capable de commander une pizza ou de cirer un parquet. Merci à Gâchette pour son objectivité dans le débat Ubuntu vs Madrake et enfin merci à Benjamin qui nous a démontré par l'exemple que son ordinateur cherchait à devenir le maître du monde.

Ceux qui font avancer à grands pas. Durant ces trois dernières années, un certain nombre de conversations orales ou écrites avec d'autres chercheurs m'ont indiscutablement aidé à avancer. Je remercie tout d'abord Julien Duval, Steven L. Kleiman et Gerhard Frey pour

leurs précieuses explications. Merci ensuite à Antoine Ducros pour son aptitude à dégainer un contre exemple plus vite que son ombre et à Joseph Tapia pour son excellente synthèse orale du *Residues and Duality* d'Hartshorne. Enfin, je tiens à remercier sincèrement Tom Høholdt pour sa gentillesse, son dévouement, son hospitalité ainsi ses indiscutables qualités de pédagogues qui ont fait de ma visite à la DTU (Université Technique du Danemark) un séjour aussi fructueux qu'agréable.

Ceux qui font la même chose... ou presque. Un grand merci à tous les doctorants (et docteurs) Toulousains que j'ai côtoyés durant ces trois années. Je remercie tout particulièrement Anne pour les "quatre heures" du mois d'août, Cécile pour sa maîtrise des blagues Carambar, Tony pour ses imitations du Schtroumpf grognon et Landry pour sa capacité à animer un débat en évitant systématiquement le consensus[1]. Merci également à Fred Protin pour ses mails aux jeux de mots décapants, à Fred Pitoun pour son dynamisme décontracté qui tonifiait nos jeudis, à Julien Roques qui partageait mon avis sur Bono et les performances de Randy Marsh. Je remercie enfin mes cobureaux, Charef, Ghada et Matthieu, leur présence me fut toujours des plus agréables.

Les uns et les hôtes. Lors de mes missions hors de Toulouse, j'ai fréquemment apprécié la qualité de mon accueil. Je remercie à ce titre Delphine Boucher de Rennes, Sylvain Duquesne et Louise Nyssen de Montpellier et Pierre-Louis Cayrel de Limoges. Je remercie également Frederic Edoukou, Adnen Sboui, leur ex-directeur de thèse François Rodier et Christophe Ritzenthaler de m'avoir acueilli durant une semaine à l'IML durant ma seconde année de thèse.

Je tiens également à remercier les membres de l'IML et du département de mathématiques de Luminy qui m'ont si bien accueilli et intégré dans leur équipe cette année. Remerciements particuliers à tous les membres de l'équipe ATI.

Parce qu'il n'y a pas que la recherche dans la thèse... Je remercie tous les enseignants et chercheurs du département de mathématiques de l'Université du Mirail. Mes trois années d'enseignement dans cette université furent un plaisir, tant pour le contact des étudiants que pour celui des collègues. Je tiens tout particulièrement à remercier Julien Labetaa pour qui j'ai donné des TD's et avec qui la collaboration fut des plus agréables.

... et qu'il n'y a pas que le travail dans la vie. Parmi les nombreux souvenirs que je garderai de ces trois années, il y aura les nombreuses fins d'après midi ensoleillées en terrasse. Merci à ceux avec qui j'ai partagé ces si agréables moments. Merci à Émilie, Gustavo, Romain, Seb, Solenn, Soazig, Tanguy et Perrine. Un grand merci également à Cécile qui m'a expliqué la différence entre un bus et un TUB, à Erwan parce qu'il comprend le 229^{e} degré et à Xavier pour son sens de l'orientation en situation critique.

Ceux qui simplifient la vie. Merci à Véronique Fabris, Agnès Requis et Jocelyne Picard pour leur disponibilité et leur patience en toute circonstance.

Celle que j'ai croisé. Merci à Lara pour tous les conseils qu'elle a pu me donner lors des nombreuses conversations que l'on a eues ensemble. C'est toujours un plaisir pour moi de trouver son nom sur la liste des participants d'une conférence à laquelle je me rends.

Ceux qui m'ont accueilli. Merci à tous les membres de l'ex-Grimm de m'avoir intégré parmi eux. Remerciements particuliers à Thierry Henocq et Christian Maire.

[1] Je sais, tu n'es pas d'accord avec ce que je viens de dire.

Ceux sans qui cette thèse n'aurait pas eu lieu. Je remercie Jean-Marc Couveignes qui fut mon premier contact à l'ex-Grimm et qui consacra une énergie particulière à la régularisation de ma complexe situation administrative. Merci également à Arnaud Debussche et Michel Pierre de m'avoir si bien conseillé en fin de Master.

Au chef. Merci à Marc Perret de m'avoir si bien encadré durant ces trois années. J'ai particulièrement apprécié son investissement, sa patience, sa capacité a expliquer en des termes simples les faits et objets mathématiques les plus complexes. Connaissant son extrême modestie, je préfère ne pas en dire plus de peur de le mettre mal à l'aise, mais si tout était à refaire, je lui conseillerais de ne rien changer.

Celles qui étaient là dès le début. Merci à mes sœurs Nadine et Sylvie.

Ceux sans qui je ne serais pas là. À mes parents, merci pour tout.

Celle qui est tout pour moi. Merci Gwenola.

Table des matières

I Résidus **23**

I Résidus de 2-formes sur une surface **25**
I.1 Notations . . . 25
I.2 Cadre . . . 25
I.3 Résidus en codimension 1 et 2 . . . 26
I.4 Complétions et séries de Laurent en deux variables . . . 28
I.4.1 Problématique . . . 28
I.4.2 Développements en séries de Laurent, première approche . . . 28
I.4.3 Développements en séries de Laurent, seconde approche . . . 30
I.4.4 Changement de variables . . . 32
I.4.5 Objets rationnels et formels . . . 34
I.5 Définition générale des résidus . . . 34
I.5.1 Invariance des 2-résidus . . . 34
I.5.2 Le cadre géométrique . . . 38
I.6 Propriétés des résidus . . . 41
I.6.1 Influence d'un éclatement sur les résidus . . . 42
I.6.2 Le cas des points singuliers d'une courbe . . . 42
I.7 Formules de sommation . . . 44

II Codes géométriques **53**

II Codes différentiels sur une surface **55**
II.1 Langage et Notations . . . 55
II.2 Rappels sur les codes construits à partir de courbes . . . 56
II.2.1 Codes fonctionnels et différentiels . . . 56
II.2.2 Paramètres de ces codes . . . 56
II.2.3 Relation d'orthogonalité et décodage . . . 57
II.2.4 Deux constructions distinctes mais une seule classe de codes . . . 57
II.3 Codes géométriques construits à partir de surfaces algébriques . . . 57
II.3.1 Cadre . . . 57
II.3.2 Codes fonctionnels . . . 58
II.3.3 Codes différentiels . . . 59
II.3.4 Paires de diviseurs Δ-convenables . . . 59
II.3.5 Exemples de diviseurs Δ-convenables. . . . 65
II.3.6 Discussion sur la Δ-convenance et le critère . . . 70
II.4 Relations entre codes fonctionnels et différentiels sur une surface . . . 70
II.4.1 Relation d'orthogonalité . . . 70
II.4.2 Un code différentiel est fonctionnel . . . 71
II.4.3 Réciproque, un code fonctionnel est différentiel . . . 73
II.5 Défaut d'inclusion réciproque pour le théorème d'orthogonalité . . . 74
II.5.1 Codes sur le plan projectif . . . 75
II.5.2 Codes sur un produit de deux droites projectives . . . 76

II.6 Heuristique, est-ce un problème de super abondance ? 79

III Théorème de réalisation **83**
III.1 Contexte 83
III.2 Sous-Δ-convenance 83
III.3 Sur les notions de réalisation 84
III.4 Construction de l'orthogonal d'un code fonctionnel 89
III.5 Discussion autour du théorème de réalisation 92
III.5.1 Un exemple de réalisation sans que les conditions du théorème de III.4.1 soient vérifiées 93
III.6 Une autre application possible des théorèmes "à la Bertini" 95
III.6.1 Les travaux de Pellikaan, Shen et Wee 95
III.6.2 Le cas des codes fonctionnels sur une surface 96

IV Orthogonal d'un code fonctionnel **99**
IV.1 Première approche 99
IV.1.1 Notion de m-généralité 99
IV.1.2 Systèmes linéaires de $\mathbf{P}^N$ 100
IV.1.3 Lien avec les notions de distance minimale 100
IV.1.4 Minorations de la distance minimale de l'orthogonal d'un code fonctionnel 101
IV.1.5 Applications 102
IV.2 Seconde approche, un problème ouvert 104

V Constructions de mots de faible poids et codes LDPC **109**
V.1 Introduction aux codes LDPC 109
V.1.1 Graphe de Tanner 109
V.1.2 Décodage itératif 111
V.1.3 L'algorithme min-somme 113
V.1.4 Discussion sur l'algorithme 115
V.2 Codes LDPC et surfaces de petit degré 117
V.2.1 Objectifs 117
V.3 Calcul explicite de mots de codes de petit poids 117
V.3.1 Mots provenant de droites non contenues dans S 118
V.3.2 Mots provenant de droites contenues dans S 122
V.4 Expérimentations avec Magma 123
V.4.1 Codes sur des surfaces cubiques 123
V.4.2 Implémentation 125
V.4.3 Codes sur des surfaces quartiques 126
V.4.4 Utilisation de l'algorithme min-somme pour le décodage de ces codes. 127

A Séries de Laurent **133**
A.1 Sur les modules de différentielles relatives 133
A.2 Démonstration du lemme I.5.8 134
A.3 Topologie de $k((u))[[v]]$ 135
A.4 Démonstration du théorème I.5.3 en caractéristique positive 137

B Indépendance des valuations **141**

C Complément d'algèbre linéaire **143**

D Construction de codes fonctionnels **147**
D.1 Construction 147
D.2 Essentiellement, c'est la même chose 148

E Points en position générale **149**

F Programmes Magma **153**
F.1 Diviseurs Δ-convenables 153
F.2 Calculs de matrices de parité de codes LDPC 162

Introduction

Cette thèse est composée de deux parties. La première porte sur les notions de résidus de 2-formes différentielles rationnelles sur une surface algébrique. La seconde partie utilise les résultats de la première en vue d'applications aux codes correcteurs d'erreurs. Ce travail de recherche est parti d'une constatation simple. En théorie des codes géométriques construits à partir de courbes algébriques, on distingue deux types de constructions. La construction *fonctionnelle* qui, comme son nom l'indique, utilise des fonctions et la construction *différentielle* qui utilise des formes différentielles. Cependant, tous les travaux de recherche abordant l'étude des codes géométriques construits à partir de variétés de dimension supérieure ou égale à 2 font systématiquement appel à une construction de type fonctionnelle. De cette observation est née une question : *peut-on généraliser la construction différentielle en dimension supérieure ou égale à 2 ?* Seule la généralisation aux surfaces sera abordée, nous justifierons ce choix un peu plus loin dans cette introduction.

Historique des codes géométriques

La première construction de codes correcteurs d'erreurs par des méthodes issues de la géométrie algébrique a été présentée par Goppa dans [Gop81]. Peu après, dans [TVZ82], Tsfasman, Vlăduţ et Zink, utilisaient cette approche géométrique pour construire des familles de codes dont les performances asymptotiques dépassaient celles de toutes les familles de codes connues jusque là. Ces résultats ont été la principale motivation du développement de la théorie des codes géométriques.

Codes sur les courbes algébriques

Dès la fin des années 80, la théorie des codes géométriques était devenue un thème de recherche extrêmement dynamique. Plusieurs centaines d'articles ont été publié sur l'étude de ces codes, que ce soit sur la recherche de bons codes, de bonnes familles de codes ou encode d'algorithmes de décodage. Il serait donc difficile de fournir une bibliographie complète sur le sujet. Signalons tout de même les quelques publications présentant un point de vue général sur la théorie. Le premier article de synthèse sur la question est dû à Lachaud [Lac86], il y est présenté toutes propriétés théoriques connues sur les codes géométriques. Pour des références plus détaillées, on peut consulter le livre de Goppa [Gop88] ou celui de Tsfasman et Vlăduţ [TV91]. Enfin, pour une synthèse sur les algorithmes de décodage de codes géométriques on pourra se référer à l'article de synthèse de Høholdt et Pellikaan [HP95] pour les travaux connus avant 1995 et au chapitre de [MMR08] écrit par Beelen et Høholdt pour les travaux plus récents.

Codes sur les variétés en dimension supérieure

Si le sujet des codes géométriques sur les courbes a été étudié de façon très approfondie, la recherche sur les codes construits à partir de variétés de dimension supérieure ou égale à 2 est restée nettement plus marginale. Historiquement, le premier à avoir donné une construction de codes correcteurs d'erreurs à partir de variétés de dimension quelconque est Manin dans [VM84]. Par la suite, un certain nombre d'articles est paru sur la question. La liste de références qui suit n'est pas exhaustive.

On dénombre au moins trois publications fournissant des résultats généraux sur les codes géométriques construits à partir de variétés algébriques de dimension supérieure ou égale à 2. Dans [Lac90] et [Lac96], Lachaud fournit une minoration de la distance minimale des codes construits sur une variété projective lisse quelconque. Dans [Han01], Søren Have Hansen étudie les paramètres des codes construits à partir de variétés algébriques lisses quelconques et propose des exemples issus des variétés de Deligne-Lustzig. Enfin, dans [Bou03], Bouganis étudie les codes construits sur des surfaces algébriques lisses quelconques puis étudie le comportement asymptotique de certaines familles de tels codes.

Pour le reste, la plupart des autres travaux publiés portent sur l'estimation des paramètres de codes construits à partir de variétés appartenant à une classe particulière. Les codes sur les surfaces toriques ont été étudiés par Hansen dans [Han00]. Ses résultats ont ensuite été généralisés en dimension quelconque par Ruano dans [Rua07]. Les codes construits sur des Grassmanniennes ont d'abord été étudiés par Nogin dans [Nog96], puis par Ghorpade et Lachaud dans [GL00]. Les codes construits à partir de variétés Hermitiennes ont été abordés pour la première fois par Chakravarti dans [Cha93], ensuite par Hirschfeld, Tsfasman et Vlăduţ dans [HTV94], puis par Sørensen dans sa thèse [Sør91] et enfin par Edoukou dans [Edo07]. Notons que les variétés Hermitiennes et Grassmaniennes peuvent être vues comme des variétés drapeaux. Ce point de vue unifié est discuté par Rodier dans [Rod03]. La distance minimale des codes sur les variétés quadriques de dimension quelconque est étudiée par Aubry dans [Aub92]. Le cas des surfaces quadriques est approché de façon pus détaillée par Edoukou dans [Edo08]. Enfin, Zarzar a traité le cas des surfaces dont le rang du Groupe de Néron-Sévéri arithmétique est petit dans [Zar07]. Il propose ensuite dans un travail commun avec F. Voloch [VZ05], une approche de décodage utilisant un algorithme de décodage itératif proposé par Luby et Mitzenmacher [LM05].

Enfin, signalons qu'une excellente synthèse sur les travaux connus sur les codes construits sur des variétés de dimension supérieure est présentée dans une prépublication de Little (voir [Lit08]).

À présent, rappelons que, comme indiqué au début de ce chapitre introductif, en théorie des codes sur les courbes on distingue deux méthodes de construction de codes respectivement appelées construction fonctionnelle et différentielle. Cependant, en dimension supérieure, on ne dispose que de la construction fournie par Manin dans [VM84]. Cette dernière est une généralisation naturelle de la construction fonctionnelle sur les courbes. Tous les travaux cités ci-dessus s'appuient sur cette construction et aucune généralisation de la construction différentielle n'a été proposée jusque là. Notons d'ailleurs que Little signale dans l'introduction de son article de synthèse [Lit08] une obstruction majeure à une telle généralisation.

"In a sense, the first major difference between higher dimensional varieties and curves is that points on X of dimension ≥ 2 are subvarieties of codimension ≥ 2, not divisors. This means that many familiar tools used for Goppa codes (e.g. Riemann-Roch theorems, the theory of differentials and residues etc.) do not apply exactly in the same way. "

En quelques mots, l'objectif de cette thèse est, après avoir mis en place le matériel théorique nécessaire, de fournir une construction différentielle de codes sur les surfaces, puis de l'appliquer à l'étude des codes géométriques.

Pourquoi des codes différentiels sur les surfaces ?

Outre la volonté de généralisation en vue d'une harmonisation des théories entre le cas des courbes et celui des variétés de dimension supérieure, plusieurs arguments motivent cette question.

Un intérêt historique. Les codes géométriques ont été introduits pour la première fois par V.D Goppa en 1981 [Gop81]. Dans cet article, la construction présentée était différentielle. Aussi, même si les codes fonctionnels sont plus populaires chez les spécialistes des codes géométriques, la construction historique est de type différentielle.

L'intérêt d'une nouvelle construction géométrique. Le second argument réside dans l'intérêt de disposer d'une construction géométrique de codes. Pour comprendre en quoi une telle construction est avantageuse, commençons par réfléchir aux différentes façons de décrire un code. La manière la plus simple est de s'en donner une base, c'est-à-dire une matrice génératrice. Cependant, une telle description n'est pas du tout adaptée à la résolution de problèmes tels que la minoration de la distance minimale ou la recherche d'un algorithme de décodage efficace. Par conséquent, on cherche en général à résoudre ces problèmes pour des classes de codes admettant une *réalisation* par des objets appartenant à une autre branche des mathématiques, comme l'arithmétique ou la géométrie. C'est par exemple le cas des codes de Reed-Solomon qui font appel à des polynômes en une variable, des codes de Reed-Müller qui se construisent à partir de polynômes à plusieurs variables ou encore des codes de résidus quadratiques dont la construction et l'étude font appel à de l'arithmétique des corps finis. Par ce biais, les problèmes de minoration de la distance minimale et de recherche d'algorithmes de décodage peuvent être traduits sous forme de problèmes d'algèbre ou de géométrie. On se ramène donc à un contexte comportant une *structure* (arithmétique ou géométrique par exemple) et dans lequel on dispose de davantage d'outils mathématiques pour résoudre un problème donné. En conclusion, **il est toujours intéressant de disposer d'une réalisation géométrique d'un code pour l'étudier**. À ce titre, la construction de codes correcteurs à partir de formes différentielles sur des surfaces est une voie que l'on se doit d'explorer.

Des codes en relation avec les codes fonctionnels. En théorie des codes géométriques construits à partir de courbes, on dispose de relations entre codes fonctionnels et codes différentiels.

(**R1**) Un code différentiel sur une courbe est toujours l'orthogonal d'un code fonctionnel construit à partir de la même courbe et associé aux mêmes diviseurs.

(**R2**) Tout code différentiel sur une courbe se réalise comme un code fonctionnel construit à partir de la même courbe mais associé à des diviseurs différents.

La relation (**R1**) est une conséquence de la formule des résidus et du théorème de Riemann-Roch. Cette propriété d'orthogonalité est de plus un ingrédient utilisé dans de nombreux algorithmes de décodage (voir [HP95]). D'une façon générale, disposer d'une réalisation géométrique de l'orthogonal ou d'un sous-code de l'orthogonal d'un code correcteur peut être fort utile pour le décodage. La relation (**R2**) est une conséquence du théorème d'approximation faible ([Sti93] I.3.1). Elle implique que les codes fonctionnels et les codes différentiels construits à partir de courbes algébriques, bien qu'obtenus par des constructions différentes, appartiennent à la même classe. On peut donc restreindre l'étude générale de ces codes à celle de codes provenant d'une seule des deux constructions. Le plus souvent, c'est la construction fonctionnelle qui est adoptée. Ce choix vient sans doute de ce que, pour beaucoup de mathématiciens, la notion d'évaluation d'une fonction en un point est plus intuitive et manipulable que celle d'évaluation du résidu d'une forme différentielle.

Ainsi, après s'être interrogé sur la possibilité d'étendre aux surfaces la construction différentielle de codes, il est naturel de réfléchir aux perspectives d'extension aux surfaces des

propriétés (**R1**) et (**R2**). De tels résultats contribueraient en effet à approfondir nos connaissances des codes géométriques construits à partir de surfaces. Nous détaillerons les résultats obtenus dans ce sens en page 18.

D'intéressants développements théoriques. Nous allons voir que la construction et l'étude des codes différentiels construits sur des surfaces a nécessité de nombreux résultats théoriques concernant les formes différentielles sur les surfaces. Les résultats énoncés dans le premier chapitre ne sont pas réellement nouveaux. En géométrie algébrique, la notion de résidu en dimension supérieure à 2 a été abordée par Grothendieck et Hartshorne dans [Har66] ainsi que par Lipman dans [Lip84]. Cependant, à la différence de ces références, la notion de résidu présentée dans le chapitre I provient d'une construction explicite ne faisant appel à aucun raisonnement de type fonctoriel. La volonté de construire des codes différentiels sur des surfaces algébriques a donc permis l'élaboration d'une introduction au résidus sur des surfaces par une approche plus explicite et constructive que celles qui existaient jusque-là[2].

Avant de passer à une présentation plus détaillée des différentes parties de la thèse. Signalons que le contenu des chapitres I et II en version *condensée* a donné lieu à la rédaction d'un article [Cou08].

Présentation de la première partie

Si la notion de résidu est bien connue dans le cas des 1-formes différentielles sur une courbe algébrique et qu'une unique définition de cet objet fait l'unanimité dans la littérature, en dimension supérieure la situation est nettement moins claire. Par exemple, en géométrie algébrique complexe, la définition énoncée dans l'ouvrage [GH78] de Griffiths et Harris diffère de celle du livre [BHPV] de Bath, Peters, Hulek et Van de Ven. Pour le premier, un résidu est un élément du corps de base (le corps des complexes) obtenu à partir de la donnée d'une n-forme méromorphe ω définie sur une variété complexe X de dimension n, d'un point P de X et d'une famille ordonnée de n diviseurs de cette variété s'intersectant en P. Pour le second, étant donnée une variété complexe X et une sous-variété Y de codimension un dans X, le résidu d'une r-forme méromorphe sur X le long de Y est la donnée d'une $(r-1)$-forme sur Y. Notons dès maintenant que ces ouvrages se placent dans le contexte des variétés complexes, contexte dans lequel on peut calculer les résidus avec l'aide de la formule de Cauchy. En d'autres termes, les résidus peuvent être obtenus en intégrant une forme différentielle sur une sous-variété réelle. Ce point de vue utilise le fait qu'une variété complexe de dimension n peut être vue comme une variété réelle de dimension $2n$. Un tel point de vue ne peut évidemment pas s'étendre à un autre cadre comme par exemple celui des variétés sur un corps fini.

Dans un contexte plus général, on trouve dans [Har66] un objet appelé *résidu de Grothendieck* qui ressemble à l'objet défini par Griffiths et Harris en ce sens qu'il associe à une forme différentielle de degré maximal un élément du corps (ou de l'anneau) de base. Cet objet est cependant plus fortement relié à un système de coordonnées locales et sa construction nécessite un important arsenal d'objets et de raisonnements fonctoriels.

Dans la première partie, qui est composée du seul chapitre I, on introduira les notions de 1-résidu qui correspondront à la définition de [BHPV] et de 2-résidu qui correspondront à la définition de [GH78]. Nous étudierons également les relations qui lient ces objets. Pour ce faire, nous étudierons les développements de fonctions et de 2-formes différentielles en séries de Laurent de deux variables. Le 2-résidu sera l'objet qui suscitera le plus notre attention. Il permet d'extraire un élément du corps de base à partir de la donnée d'une 2-forme rationnelle ω sur une surface, d'une courbe C plongée dans cette surface et d'un point rationnel P de

[2] Peu de temps après l'envoi de la seconde version de ce manuscrit, Oleg Osipov du Steklov Mathematical Institute, m'a contacté après avoir consulté une prépublication de mes résultats sur ArXiv (voir [Cou08]). Il m'a alors signalé qu'une approche similaire avait été donnée par Paršin dans [Par76]. J'ignorais l'existence de cet article peu connu et rarement cité lorsque j'ai travaillé sur ces questions.

C. On le notera

$$\mathrm{res}^2_{C,P}(\omega).$$

Présentation des résultats de la première partie

Les travaux effectués dans la première partie (donc le premier chapitre) aboutissent à deux types de résultats.

Invariance des 2-résidus

Le premier résultat majeur est le théorème I.5.3 qui assure que l'application $\mathrm{res}^2_{C,P}$ est bien définie. En d'autres termes, le 2-résidu en un point P le long d'une courbe C d'une 2-forme rationnelle ω ne dépend pas d'un choix de coordonnées locales.

Formules de sommation

L'objectif principal de ce travail est d'obtenir des formules du type : "*la somme des résidus de ω est nulle*", en vue de relations d'orthogonalité entre codes dans la seconde partie. Dans la section I.7 du chapitre I, on fournira trois formules de sommation[3].

Théorème I.7.1 (Première formule des résidus)**.** *Soit S une surface projective irréductible lisse définie sur un corps algébriquement clos. Soient C une courbe projective irréductible plongée dans S et ω une 2-forme rationnelle sur S. On a*

$$\sum_{P\in C} res^2_{C,P}(\omega) = 0.$$

Théorème I.7.4 (Deuxième formule des résidus)**.** *Soit S une surface quasi-projective irréductible lisse définie sur un corps algébriquement clos. Soient P un point de S et $\mathcal{C}_{\mathcal{S},\mathcal{P}}$ l'ensemble des germes de courbes irréductibles tracées sur S et contenant P. Pour toute 2-forme ω rationnelle sur S, on a*

$$\sum_{C\in\mathcal{C}_{S,P}} res^2_{C,P}(\omega) = 0.$$

La troisième formule de sommation nécessite la définition de 2-résidu en un point le long d'un diviseur. Nous renvoyons le lecteur à la définition I.7.10 page 50.

Théorème I.7.11 (Troisième formule des résidus, [Lip84] chap. 12)**.** *Soit S une surface projective irréductible lisse définie sur un corps algébriquement clos. Soient D_a et D_b deux diviseurs sur S dont l'intersection des supports est un ensemble fini Z. Soit $\Omega^2(-D_a - D_b)$ le faisceau de 2-formes rationnelles vérifiant localement*

$$(\omega) \geq -D_a - D_b.$$

Alors, pour toute section globale ω du faisceau $\Omega^2(-D_a - D_b)$, on a

$$\sum_{P\in S} res^2_{D_a,P}(\omega) = \sum_{P\in Z} res^2_{D_a,P}(\omega) = 0.$$

[3]Comme signalé dans la note au bas de la page 16, une partie des résultats présentés dans la première partie de cette thèse avaient en fait déjà été démontrées dans [Par76] par des méthodes similaires. C'est par exemple le cas des deux premières formules de sommation de résidus, à savoir les théorèmes I.7.1 et I.7.4

La troisième formule des résidus est le résultat que nous utiliserons dans le chapitre II pour obtenir un résultat d'orthogonalité entre codes. Elle se démontre à l'aide des deux autres formules de sommation énoncées (les théorèmes I.7.1 et I.7.4). Cette troisième formule des résidus n'est pas nouvelle, on en trouve un énoncé similaire dans le chapitre 12 de [Lip84] qui est valable en toute dimension et pas seulement sur les surfaces. Nous insistons une fois de plus sur le fait que la démonstration donnée dans cette thèse a l'intérêt de faire appel à des constructions plus explicites et plus constructives que celles utilisées dans les démonstrations connues de ce résultat. Achevons notre argumentation à ce sujet par une citation justement extraite de [Lip84], afin de légitimer ("*more or less*") le choix que nous avons fait de présenter et démontrer ces résultats de manière nouvelle et plus accessible.

"Statements 0.3A and 0.3B, are consequences (more or less) of ([Har66] page 383 corollary 3.4). However, one of our main purposes in this paper is to provide a proof of 0.3 for which loc. cit. is not a prerequisite. The other main purpuse is to describe the connection between local and global duality, via residues (c.f. [Har66] page 386 prop 3.5)."

Avant de passer à la présentation de la seconde partie, finissons par une remarque. Il peut sembler naturel de se demander pourquoi les résultats énoncés dans cette thèse ne portent principalement que sur les surfaces et non sur les variétés de dimension supérieure. Différentes raisons ont motivé ce choix. La première est que, même s'il est fort probable que les constructions et les résultats présentés dans la première partie admettent une généralisation en dimension supérieure à 2, tout travail dans cette direction aurait entraîné d'importantes lourdeurs dans les notations. Nous avons donc choisi de nous restreindre au cas déjà non trivial des surfaces, sachant que, pour ce type de problème de géométrie algébrique, le passage de la dimension 1 à 2 est l'étape difficile à franchir. Enfin, l'objectif étant de travailler sur les codes correcteurs, il semblait déjà fort intéressant de ne considérer que le cas des surfaces, ce dernier n'ayant été que rarement exploré. Il nous a donc semblé inutile de partir vers de telles généralités alors que le monde des surfaces algébriques offrait déjà de si nombreuses perspectives.

Présentation de la seconde partie

La seconde partie contient les chapitres II à V. Elle concerne les codes géométriques et plus précisément les codes différentiels construits sur des surfaces algébriques.

Présentation des résultats de la seconde partie

Les codes différentiels sur une surface algébrique sont définis dans le chapitre II (définition II.3.2 page 59). On se donne dans tout ce chapitre une surface projective lisse géométriquement intègre S sur $\mathbf{F}_q$, un diviseur G sur S et une famille de points rationnels $P_1, \ldots, P_n$ de S qui évitent le support de G. On note Δ le 0-cycle

$$\Delta := P_1 + \cdots + P_n.$$

Dans tout ce qui suit et jusqu'à la fin de cette introduction, les codes fonctionnels seront notés "C_L" et les codes différentiels "C_Ω". Les définitions respectives de ces codes sont données en sections II.3.2 et II.3.3.

Codes différentiels sur les surfaces

La construction de ces codes nécessite l'introduction d'une paire de diviseurs (D_a, D_b). Pour obtenir une relation d'orthogonalité on définit la notion de paires de diviseurs Δ-convenables (voir définition II.3.5 page 60). Il s'agit de paires de diviseurs qui sont en un certain sens *reliées* au 0-cycle Δ. Le premier résultat majeur de ce chapitre est une relation d'othogonalité qui est plus faible que la propriété (**R1**) dans le cas des courbes puisqu'il ne s'agit plus que d'une inclusion au lieu d'une égalité.

Théorème II.4.1 (Théorème d'orthogonalité). *Soient (D_a, D_b) une paire Δ-convenable de diviseurs et $D := D_a + D_b$. On a alors,*

$$C_{\Omega,S}(\Delta, D_a, D_b, G) \subseteq C_{L,S}(\Delta, G)^{\perp}.$$

L'inclusion réciproque est en général fausse, comme le montre le contre-exemple donné en section II.5.2. Plus précisément, on présente l'exemple d'une surface (le produit de deux droites projectives) sur laquelle l'orthogonal d'un code fonctionnel ne se réalise sous la forme d'un code différentiel pour aucun choix de paire de diviseurs Δ-convenable (D_a, D_b).

Nous étudions ensuite la possibilité d'étendre aux codes sur les surfaces la propriété (**R2**). À la différence de (**R1**), cette seconde relation s'étend parfaitement au cas des surfaces.

Théorème II.4.6. *Soient (D_a, D_b) une paire Δ-convenable de diviseurs et $D := D_a + D_b$, alors il existe un diviseur canonique K tel que*

$$C_{\Omega}(D_a, D_b, G) = C_L(\Delta, K - G + D).$$

Théorème II.4.9. *Étant donné un diviseur G sur S, il existe un diviseur canonique K et une paire Δ-convenable (D_a, D_b) telle que*

$$C_L(\Delta, G) = C_{\Omega}(D_a, D_b, K - G + D).$$

Le chapitre II se termine par une discussion en section II.6 autour des raisons du défaut d'inclusion réciproque dans le théorème d'othogonalité II.4.1. Cette discussion est consécutive à la présentation d'un contre-exemple à l'inclusion réciproque du théorème II.4.1 donnée en section II.5.2. Par ailleurs, ce contre-exemple permet de conclure le second chapitre sur une importante constatation. Il assure en effet que les codes fonctionnels construits sur une surface algébrique et leurs orthogonaux appartiennent en général à une classe différente. C'est un phénomène qui différencie fondamentalement le cas des courbes de celui des surfaces. Notons que cette asymétrie entre les codes fonctionnels et leurs orthogonaux avait déjà été signalée par Voloch et Zarzar dans [VZ05].

"It is interesting to note that Goppa codes coming from curves are seldom LDPC since their duals are also Goppa codes coming from curves and, as such, have a large minimal distance, whereas the dual of an LDPC has a small minimal distance by definition."

Pour le reste, cette observation ouvre un intéressant axe de recherche, celui de l'étude de l'orthogonal d'un code fonctionnel sur une surface. C'est ce qui donnera lieu au chapitre IV, nous y reviendrons plus loin.

Théorème de réalisation

Dans le chapitre III on montre comment, sous certaines conditions sur la surface S et le diviseur G, on peut réaliser l'orthogonal d'un code fonctionnel non pas comme un code différentiel mais comme une somme de codes différentiels. L'énoncé du théorème fait appel à la notion de sous-Δ-convenance définie en section III.2 (définition III.2.1 page 84).

Théorème III.4.1 (Théorème de réalisation). *Soient S une surface lisse géométriquement intègre et intersection complète dans un espace projectif $\mathbf{P}^r_{\mathbf{F}_q}$ et G un diviseur sur S linéairement équivalent à une section de S par une hypersurface de $\mathbf{P}^r$. On se donne également un 0-cycle Δ qui est la somme de n points rationnels de S évitant le support de G. Soit c un mot du code $C_{L,S}(\Delta, G)^{\perp}$. Alors, il existe une paire de diviseurs (D_a, D_b) et une 2-forme ω appartenant à l'espace des sections globales $\Gamma(S, \Omega^2(G - D_a - D_b))$, tels que*

$$c = res^2_{D_a,\Delta}(\omega).$$

Remarque. *Le théorème de réalisation dit en fait un peu plus que ça, il fournit également des informations sur les structures géométriques et les classes d'équivalence linéaires des diviseurs D_a et D_b (voir page 89).*

Corollaire III.4.2. *Sous les hypothèses du théorème de réalisation, il existe une famille finie $(D_a^{(1)}, D_b^{(1)}), \ldots, (D_a^{(s)}, D_b^{(s)})$ de paires de diviseurs sous-Δ-convenables telles que*

$$C_{L,S}(\Delta, G)^\perp = \sum_{i=1}^{s} C_{\Omega,S}(\Delta, D_a^{(i)}, D_b^{(i)}, G).$$

La démonstration du théorème de réalisation utilise un théorème "à la Bertini" sur les corps finis démontré par Poonen en 2004 dans [Poo04]. On termine le chapitre en montrant qu'un argument "à la Bertini" de type différent pourrait permettre d'obtenir d'intéressantes informations sur la distance minimale d'un code fonctionnel sur une surface. Ce problème reste ouvert, nous en discuterons de nouveau page 21.

Étude de l'orthogonal d'un code fonctionnel

Le chapitre IV explore la voie ouverte par le chapitre II, à savoir l'étude de cette nouvelle classe de codes que sont les orthogonaux de codes fonctionnels sur une surface. La première section de ce chapitre se place en fait dans un contexte plus général, celui des variétés de dimension quelconque. Son objectif est de minorer la distance minimale de l'orthogonal d'un code fonctionnel sur une telle variété à l'aide de méthodes d'algèbre linéaire. On obtient un résultat de minoration.

Théorème IV.1.7. *On suppose N supérieur ou égal à 2. Soit m un entier tel que $G \sim mL_X$, alors*

(1) la distance minimale $d^\perp$ du code $C_{L,X}(\Delta, G)^\perp$ vérifie

$$d^\perp \geq m + 2$$

et il y a égalité si et seulement si le support de Δ contient $m+2$ points alignés ;

(2) sinon, si le support de Δ ne contient pas $m+2$ points alignés, alors

$$d^\perp \geq 2m + 2$$

et il y a égalité si et seulement si le support de Δ contient $2m+2$ points sur une même conique plane.

On conclut cette première section en donnant quelques applications de ce résultat. On montre par exemple que si X est une courbe plane, alors pour certaines valeurs de m, la borne fournie par le théorème IV.1.7 (1) est meilleure que la distance construite[4] de Goppa ([Sti93] def II.2.4).

La deuxième section du chapitre IV présente une méthode de minoration de la distance minimale de l'orthogonal d'un code fonctionnel sur une surface, sous réserve de disposer d'un résultat "à la Bertini" que l'on énonce. Cette partie ne fournit donc pas de résultat à proprement parler mais motive un problème ouvert que l'on énoncera à la fin de cette introduction (voir question 5G page 21).

Codes LDPC et décodage itératif

Le chapitre V porte sur l'étude de certains codes fonctionnels construits sur des surfaces. Cette question a déjà été abordée par Voloch et Zarzar dans [VZ05].

[4] Le terme de "distance construite" a été choisi par l'auteur comme traduction de *designed minimal distance*.

Le chapitre commence par une série de prérequis concernant les codes LDPC (*Low Density Parity Check*, ce sont les codes admettant une matrice de parité *creuse*). On y rappelle les notions de graphe de Tanner et présente un algorithme de décodage itératif.

Dans un second temps on étudie la possibilité de construire une matrice de parité creuse pour certains codes fonctionnels sur des surfaces et on applique à ces codes l'algorithme de décodage itératif présenté en première partie de chapitre. Ce chapitre présente un volet plus expérimental de ce travail de thèse, en décrivant des calculs effectués avec le logiciel MAGMA.

Problèmes ouverts

Dans ce qui précède, nous avons signalé à plusieurs reprises l'existence de problèmes ouverts posés par ce travail de thèse. Nous concluons cette introduction en énonçant les plus importants.

Sur l'orthogonal d'un code fonctionnel

Dans le chapitre III, on montre que sous certaines hypothèses sur la surface S et le diviseur G, l'orthogonal du code fonctionnel se réalise comme somme de codes différentiels. On remarque ensuite par l'étude d'un exemple (page 93) que les conditions que doivent vérifier S et G dans l'énoncé du théorème de réalisation sont suffisantes mais pas nécessaires.

Question 3. *Le résultat du théorème de réalisation (théorème III.4.1) reste-t-il vrai si l'on élimine les hypothèses sur S et G dans l'énoncé ?*

Une autre question naturelle se pose concernant le théorème de réalisation, ou plutôt le corollaire III.4.2.

Question 4. *Sous les conditions du corollaire III.4.2, peut-on estimer le nombre minimal de codes différentiels dont la somme est égale à l'orthogonal d'un code fonctionnel en fonction d'invariants géométriques de la surface ?*

Sur les théorèmes "à la Bertini"

Une question majeure est posée à la fin du chapitre III et une variante de cette dernière est posée à la fin du chapitre IV. Une réponse à ce problème pourrait fournir des minorations de la distance minimale de codes fonctionnels construits sur des surfaces et d'orthogonaux de tels codes.

Question 5 (Arithmétique)**.** *Soient X une variété projective lisse géométriquement intègre sur un corps fini $\mathbf{F}_q$ et $P_1, \ldots, P_n$, une famille de points fermés de X. Peut-on évaluer explicitement ou majorer de façon précise le plus petit entier d tel qu'il existe au moins une hypersurface définie sur $\mathbf{F}_q$ de degré inférieur ou égal à d qui interpole tous les P_i et dont l'intersection schématique avec X soit une sous-variété lisse géométriquement intègre de codimension 1 ?*

Question 5 (Géométrique)**.** *Soit X une variété projective irréductible lisse définie sur $\overline{\mathbf{F}}_q$ et $P_1, \ldots, P_n$ une famille de points de X. Peut-on évaluer explicitement ou majorer de façon précise le plus petit entier d tel qu'il existe au moins une hypersurface H de degré inférieur ou égal à d contenant tous les P_i et telle que $H \cap X$ soit une sous-variété lisse de codimension un de X ?*

Une présentation plus complète des questions et problèmes ouverts posés par cette thèse sera faite dans la conclusion page 129.

Première partie

Résidus

Chapitre I

Résidus de 2-formes sur une surface

Résidu. n.m (lat. residuum). Matière qui subsiste après une opération physique ou chimique, un traitement industriel etc... Syn. Débris, déchet, rebut, reste.

Ce chapitre est relativement différent de ceux qui vont suivre. Il est en effet le seul dont le contenu ne soit pas directement relié à la théorie des codes correcteurs d'erreurs. L'objectif est de fournir le matériel théorique nécessaire à la construction et l'étude de codes différentiels construits sur des surfaces algébriques.

La notion centrale de ce premier chapitre est celle de résidu.

I.1 Notations

Soit X une variété algébrique définie sur un corps k, on note $k(X)$ le corps des fonctions rationnelles sur X. De même, on note $\Omega^i_{k(X)/k}$ le $k(X)$-espace vectoriel des i-formes différentielles rationnelles sur X. Soit Y une sous-variété irréductible de X, on dira qu'une fonction (resp. une forme différentielle) rationnelle sur X est *régulière au voisinage de* Y, si et seulement si elle est régulière sur un ouvert dont l'intersection avec Y est non vide[1]. L'anneau local des fonctions régulières au voisinage de Y et son idéal maximal sont respectivement notés $\mathcal{O}_{X,Y}$ et $\mathfrak{m}_{X,Y}$. On rappelle que le corps résiduel de cet anneau est le corps $k(Y)$ des fonctions rationnelles sur Y. Si u est un élément de $\mathcal{O}_{X,Y}$, on note $u_{|Y}$ sa restriction à Y. Si par ailleurs il n'y a pas d'ambiguïté concernant la sous-variété Y le long de laquelle on restreint notre fonction cette restriction pourra être notée $\bar{u}$. Enfin, le complété $\mathfrak{m}_{X,Y}$-adique de cet anneau est noté $\widehat{\mathcal{O}}_{X,Y}$

I.2 Cadre

Dans ce chapitre, sauf mention contraire, k désigne un corps quelconque (donc de caractéristique quelconque) et S une surface algébrique quasi-projective **lisse** géométriquement intègre[2] définie sur k. De plus, sauf mention contraire, C désigne une courbe irréductible absolument réduite définie sur k et plongée dans S et P un point rationnel lisse de C. Notons que, comme S est supposée lisse, C est non contenue dans le lieu singulier de cette surface. Par conséquent, l'anneau $\mathcal{O}_{S,C}$ est de valuation discrète. De plus, la valuation $\mathfrak{m}_{S,C}$-adique de cet anneau s'étend en une valuation discrète val_C sur $k(S)$.

[1] Dans le langage des schémas, cela revient à dire que la fonction (resp. la forme différentielle) est régulière au voisinage du point générique de Y.

[2] C'est-à-dire que sur tout ouvert affine U de S, l'anneau de coordonnées de $U \times_k \bar{k}$ est intègre. En d'autres termes, la surface S est absolument réduite et absolument irréductible.

Sur la notion de variété

Dans toute cette thèse, nous parlerons de *variétés*, or il s'avère que ce terme n'est pas réellement standard. Il est donc nécessaire de commencer par fixer une définition de cette notion.

Définition I.2.1. *Une variété X sur un corps k est un schéma noethérien de type fini sur k.*

Pour les définitions de schéma noethérien et de type fini voir [Har77] II.3.

I.3 Résidus en codimension 1 et 2

Il est signalé dans l'introduction, qu'en dimension supérieure à 1, différents objets portent le nom de *résidu* dans la littérature. Nous allons introduire ces objets et étudier les relations qui les relient. La définition de résidu la plus simple à introduire est celle de résidu en codimension 1. Rappelons que l'on se place sous les hypothèses énoncées en section I.2.

Proposition I.3.1. *Soit v une uniformisante[3] de l'anneau $\mathcal{O}_{S,C}$. Soit ω une 2-forme rationnelle de valuation supérieure ou égale à -1 le long de C. Alors, il existe $\eta_1 \in \Omega^1_{k(S)/k}$ et $\eta_2 \in \Omega^2_{k(S)/k}$, toutes deux régulières au voisinage de C et telles que*

$$\omega = \eta_1 \wedge \frac{dv}{v} + \eta_2. \tag{I.1}$$

De plus, la forme différentielle $\eta_{1|C} \in \Omega^1_{k(C)/k}$ est unique et ne dépend ni du choix de l'uniformisante v ni du choix de la décomposition (I.1).

Définition I.3.2. *On appelle cette 1-forme sur C le 1-résidu de ω le long de C et on la note*

$$res^1_C(\omega) := \eta_{1|C}.$$

Un analogue de la proposition I.3.1 est énoncé et démontré dans [BHPV] au début de la section II.4. Notons que ladite référence se place dans un cadre sensiblement différent, à savoir celui des formes holomorphes sur les variétés complexes. Toutefois, la preuve d'invariance ne fait en aucun cas appel à des propriétés spécifiques des variétés complexes. Elle s'étend de fait aisément au cadre dans lequel nous travaillons. Nous donnerons en section I.5.1 une preuve de cette proposition-définition dans un contexte plus général (voir lemme I.5.6).

Définition I.3.3. *Sous les hypothèses de la proposition I.3.1, soit P un point k-rationnel lisse de C. Le 2-résidu de ω en P le long de C est le résidu en P du 1-résidu de ω le long de C. On le note*

$$res^2_{C,P}(\omega) := res_P(res^1_C(\omega)).$$

Remarque I.3.4. *Étant donné que la 2-forme ω est k-rationnelle sur S, que la courbe C est définie sur k et que P est un point k-rationnel de C, ce 2-résidu est un élément de k.*

Notons que, comme le corps de base n'est pas supposé algébriquement clos, il peut sembler logique de se placer dans un cadre plus général, à savoir que P est un point fermé lisse de C. Cependant, la motivation de ce chapitre est d'aboutir à des formules de sommation de 2-résidus, dont l'une (le théorème I.7.11) peut être vue comme une version en dimension 2 de la formule des résidus bien connue en dimension 1. Pour parvenir à ces formules, nous avons trouvé plus confortable d'adopter une approche géométrique. Ainsi, dans la section I.7 qui concerne ces formules de sommation, le corps de base est supposé algébriquement clos.

D'un autre côté, nous aurons tout de même besoin dans les chapitres suivants d'un résultat de type arithmétique, à savoir la remarque I.3.4. En effet, l'objectif étant de construire des

[3] C'est à dire une fonction de valuation 1 le long de C.

codes par évaluation de résidus, il faut s'assurer que les mots de code construits sont bien à coefficients dans un corps fixé.

Ainsi, le compromis adopté est le suivant. Étant donné que tout point géométrique de S est un point rationnel de cette surface après une certaine extension des scalaires, on travaillera toujours avec des points rationnels. Dans un second temps lorsqu'il s'agira d'énoncer des résultats de sommation, on se placera dans $S \times_k \bar{k}$ de façon à pouvoir considérer sans distinction tous les points géométriques de S.

Avant de passer à la section suivante, donnons quelques exemples et remarques pour commencer à développer une certaine intuition des résidus.

Remarque I.3.5. *Dans les deux définitions précédentes on a supposé que ω n'avait pas de pôle multiple le long de C. Dans ce qui va suivre, nous verrons que les 2-résidus sont bien définis même si l'on retire cette hypothèse. Cependant, cette condition sur la valuation de ω le long de C est indispensable pour la bonne définition des 1-résidus le long de C. C'est ce que montre l'exemple I.3.6.*

Exemple I.3.6. Supposons que S est le plan affine complexe $\mathbf{A}^2_{\mathbf{C}}$ muni d'un système de coordonnées affines (x, y). Soient C la droite d'équation $y = 0$ et P l'origine du plan affine. Considérons la 2-forme

$$\omega := xdx \wedge \frac{dy}{y^2}.$$

Une généralisation naturelle de la notion de 1-résidu serait d'extraire de ω, la restriction à C du terme en dy/y. Dans l'expression ci-dessus on obtiendrait un 1-résidu nul. Effectuons maintenant le changement de variables, $x := u + y$. L'expression de ω devient

$$\omega = (u + y)du \wedge \frac{dy}{y^2} = udu \wedge \frac{dy}{y^2} + du \wedge \frac{dy}{y}$$

et on obtiendrait dans ce cas un 1-résidu égal à $d\bar{u}$.

Remarque I.3.7. *Il faut insister dès à présent sur le fait que l'on ne peut pas parler de résidu d'une 2-forme en un point mais de résidu d'une 2-forme,* ***le long d'une courbe*** *C en un point P. Cela peut sembler étrange, mais le calcul présenté dans l'exemple I.3.8 permet de se convaincre du fait que cette spécification est incontournable.*

Exemple I.3.8. On reprend $S = \mathbf{A}^2_{\mathbf{C}}$ et les mêmes C et P que dans l'exemple I.3.6. Soit

$$\omega := \frac{dx}{x} \wedge \frac{dy}{y}.$$

Ici nous sommes dans un cas sympathique, la 2-forme ω n'a que des pôles simples au voisinage de P. On a $\mathrm{res}^1_C(\omega) = \frac{d\bar{x}}{\bar{x}}$ et donc

$$\mathrm{res}^2_{C,P}(\omega) = 1.$$

À présent, posons $C' := \{x = 0\}$. L'anticommutativité du produit extérieur entraîne que $\mathrm{res}^1_{C'}(\omega) = -\frac{d\bar{y}}{\bar{y}}$. De fait,

$$\mathrm{res}^2_{C',P}(\omega) = -1.$$

Enfin, si on appelle C'' la droite d'équation $\{x = y\}$, en posant $v = y - x$, on obtient,

$$\omega = \frac{dx}{x} \wedge \frac{dv}{v + x}.$$

On développe alors en série de Laurent en la variable v,

$$\omega = \frac{dx}{x} \wedge \frac{dv}{x\left(1 + \frac{v}{x}\right)} = \left(1 - \frac{v}{x} + \frac{v^2}{x^2} - \cdots\right)\frac{dx}{x^2} \wedge dv.$$

Par conséquent, il n'y a pas de terme en $\frac{dv}{v}$, donc $\mathrm{res}^1_{C''}(\omega) = 0$ et

$$\mathrm{res}^2_{C'',P}(\omega) = 0.$$

Ce dernier exemple motive les constructions introduites dans la section suivante. En effet, le calcul effectué correspond à un développement du coefficient de cette 2-forme en une série de Laurent appartenant à $k((x))((v))$. Par ailleurs, les séries de Laurent étant l'objet utilisé en théorie des courbes algébriques pour calculer des résidus il semble naturel d'en introduire une généralisation en dimension 2.

I.4 Complétions et séries de Laurent en deux variables

I.4.1 Problématique

En un point k-rationnel lisse Q d'une courbe algébrique X, il est aisé de décrire le complété $\mathfrak{m}_{X,Q}$-adique de $k(X)$. Il s'identifie au corps des séries de Laurent $k((u))$, où u est un paramètre local en Q. Ici, le fait que $k(X)$ contienne le corps résiduel de $\widehat{k(X)}$, à savoir k, permet d'obtenir un unique plongement $k(X) \hookrightarrow k((T))$ envoyant u sur T. On dispose en particulier d'une méthode explicite pour décomposer une fonction en séries de Laurent en la variable u, et calculer le résidu d'une 1-forme en Q.

Dans le cas d'un corps de fonctions de dimension 2, la situation se complique lourdement. Si Y est une surface irréductible sur k, les anneaux de valuation discrète de $k(Y)$ sont ses sous-anneaux de la forme $\mathcal{O}_{Y,C}$, où C est une courbe irréductible absolument réduite contenue dans le complémentaire du lieu singulier de Y (ou d'une surface birationnelle à Y). Soit C une telle courbe et v une uniformisante de $\mathcal{O}_{S,C}$. Le corps résiduel de cet anneau local est le corps $k(C)$ des fonctions k-rationnelles sur C. De fait, l'anneau $\mathcal{O}_{S,C}$ est de valuation discrète, de même caractéristique que son corps résiduel (ils contiennent tous deux k) et contient un corps. D'après le théorème de structure de Cohen (voir [Eis95] théorème 7.7 ou [Coh46] théorème 9 pour une référence historique), l'anneau $\widehat{\mathcal{O}}_{S,C}$ est isomorphe à $k(C)[[v]]$ et le complété $\mathfrak{m}_{Y,C}$-adique de $k(Y)$ est isomorphe à $k(C)((v))$. Cette description peut sembler commode, elle a toutefois un défaut qui la rend difficile à exploiter : en général $k(Y)$ ne contient pas $k(C)$. L'exemple suivant illustre ce phénomène.

Exemple I.4.1. Soient $S = \mathbf{P}^2_k$ et $C \subset S$ une courbe elliptique. Alors, il existe $x \in k(S)$ telle que $k(C)$ est une extension quadratique de $k(x)$ et $k(S)$ une extension transcendante pure de $k(x)$. D'après le théorème de Lurröth, $k(S)$ ne peut pas contenir $k(C)$.

Une autre approche consiste à considérer l'anneau local $\mathcal{O}_{S,P}$ et à le compléter $\mathfrak{m}_{S,P}$-adiquement. Si l'on se donne un système de coordonnées locales (u, v) en P, l'anneau $\widehat{\mathcal{O}}_{S,P}$ est isomorphe à $k[[u, v]]$ et la décomposition en série de Taylor d'un élément de $\mathcal{O}_{S,P}$ est explicitement calculable (voir [Sha94] II.2.2). Malheureusement, si le corps des fractions de $k[[t]]$ est isomorphe à $k((t))$, on ne dispose pas d'une description aussi agréable du corps des fractions de $k[[u, v]]$. Ces constatations motivent le travail qui va être effectué dans cette section. Il s'agit de plonger les complétés $\mathfrak{m}_P$ et $\mathfrak{m}_C$-adiques de $k(S)$ dans un corps "plus gros". Deux approches vont être proposées. Moralement, la première utilise la structure de $\mathcal{O}_{S,P}$ et la seconde celle de $\mathcal{O}_{S,C}$.

I.4.2 Développements en séries de Laurent, première approche

Rappelons que C est supposée être une courbe irréductible sur k plongée dans S et P un point rationnel lisse de C. Dans la section I.3, nous avons vu que les 2-résidus d'une forme différentielle dépendaient d'une courbe et d'un point de celle-ci. De fait nous allons introduire un type de système de coordonnées locales *relié* à P et C.

Définition I.4.2 ((P,C)-paires fortes)**.** *On dit qu'une paire (u,v) d'éléments de $\mathcal{O}_{S,P}$ est une (P,C)-paire forte, si elle vérifie les deux conditions suivantes.*

(1) Le couple (u,v) est un système de coordonnées locales en P.

(2) La fonction v est une équation locale de C au voisinage de P.

Lemme I.4.3. *Soit (u,v) une (P,C)-paire forte, alors il existe un morphisme $\phi : k(S) \hookrightarrow k((u))((v))$ qui envoie u et v sur eux-mêmes et tel que l'image de $\mathcal{O}_{S,P}$ est contenue dans $k[[u,v]]$ et celle de $\mathcal{O}_{S,C}$ dans $k((u))[[v]]$.*

Remarque I.4.4. *La proposition I.4.12 de la section I.4.3 entraînera qu'un tel morphisme est unique.*

Preuve. Comme $k(S)$ est le corps des fractions de $\mathcal{O}_{S,C}$, il suffit de montrer l'existence d'un morphisme $\phi_0 : \mathcal{O}_{S,C} \hookrightarrow k((u))[[v]]$, qui envoie u et v sur eux-mêmes et injecte $\mathcal{O}_{S,P}$ dans $k[[u,v]]$. Le lemme s'en déduira en appliquant la propriété universelle des corps de fractions.

Commençons par montrer que $\mathcal{O}_{S,C}$ est isomorphe à $\mathcal{O}_{S,P_{(v)}}$. Soit U un voisinage affine de P tel que v soit une fonction régulière sur U dont le lieu d'annulation sur cet ouvert soit exactement $C \cap U$. Un tel ouvert existe étant donné que v est une équation locale de C au voisinage de P. Notons $k[U]$ l'anneau des fonctions régulières sur U.

Les anneaux $\mathcal{O}_{S,P}$ et $\mathcal{O}_{S,C}$ s'identifient respectivement aux localisés $k[U]_{\mathfrak{m}_P}$ et $k[U]_{\mathfrak{m}_C}$ où $\mathfrak{m}_P$ et $\mathfrak{m}_C$ correspondent respectivement à P et C. De plus, l'idéal $\mathfrak{m}_C$ est principal et engendré par v. De fait, comme $\mathfrak{m}_C \subset \mathfrak{m}_P$, on a

$$\mathcal{O}_{S,P_{(v)}} \cong \left(k[U]_{\mathfrak{m}_P}\right)_{\mathfrak{m}_C} \cong k[U]_{\mathfrak{m}_C} \cong \mathcal{O}_{S,C}.$$

Ensuite, la complétion $\mathfrak{m}_{S,P}$-adique de $\mathcal{O}_{S,P}$ fournit un morphisme injectif $\mathcal{O}_{S,P} \hookrightarrow k[[u,v]]$, qui à une fonction régulière au voisinage de P associe sa série de Taylor en les variables u et v. On considère alors le diagramme

$$\begin{array}{ccccc} \mathcal{O}_{S,P} & \xrightarrow[\text{loc}]{} & \mathcal{O}_{S,C} & \xrightarrow{\text{comp}} & \widehat{\mathcal{O}}_{S,C} \\ \downarrow & & \downarrow{\scriptstyle \exists !} & & \downarrow{\scriptstyle \exists !} \\ k[[u,v]] & \xrightarrow{\text{loc}} & k[[u,v]]_{(v)} & \xrightarrow{\text{comp}} & \widehat{k[[u,v]]}_{(v)}. \end{array} \tag{I.2}$$

Les deux premières flèches horizontales du carré de gauche sont des localisations. Celles du carré de droite sont des complétions (v)-adiques.

Pour finir il ne nous reste qu'à montrer que $\widehat{k[[u,v]]}_{(v)}$ est isomorphe à $k((u))[[v]]$. Pour ce faire, on commence par montrer que le corps résiduel de l'anneau $\widehat{k[[u,v]]}_{(v)}$ est $k((u))$. En effet,

$$\widehat{k[[u,v]]}_{(v)}/(v) \cong \text{Frac}\left(k[[u,v]]/(v)\right) \cong \text{Frac}\left(k[[u]]\right).$$

On invoque ensuite le théorème de structure de Cohen. L'anneau $\widehat{k[[u,v]]}_{(v)}$ est complet, de même caractéristique que son corps résiduel et contient un corps. Il est donc isomorphe à l'anneau $k((u))[[v]]$. □

Remarque I.4.5. *Noter que les variables u et v ne jouent pas un rôle symétrique, par exemple la série*

$$f := \sum_{n=0}^{\infty} \frac{v^n}{u^n}$$

est un élément de $k((u))((v))$ mais pas de $k((v))((u))$. Cette asymétrie n'a rien de choquant étant donné que, dans la définition de (P,C)-paire forte, les fonctions u et v elles-mêmes jouent des rôles asymétriques.

I.4.3 Développements en séries de Laurent, seconde approche

Dans ce paragraphe, nous allons introduire une autre approche du développement en série de Laurent. Pour cette nouvelle approche, nous nous placerons dans le contexte des (P, C)-paires faibles (voir définition I.4.9), moins restrictif que celui des (P, C)-paires fortes.

La principale motivation de cette seconde construction est que si l'on prend une fonction rationnelle f sur S, elle admet un développement en série de Laurent que l'on peut mettre sous la forme

$$f = \sum_{n \geq l} f_i(u) v^i,$$

où l'entier l désigne la valuation $\mathfrak{m}_{S,C}$-adique de f. Les coefficients f_i sont des éléments de $k((u))$. La série $f_l(\bar{u})$ est le développement $\bar{u}$-adique au voisinage de P de la restriction à C de la fonction $v^{-l} f$. Il s'agit donc du développement en série de Laurent en la variable $\bar{u}$ d'une fonction rationnelle sur C. Une question se pose : *en est-il de même pour les autres coefficients f_i ?*

Soit (u, v) une (P, C)-paire forte. Comme nous l'avons signalé dans l'introduction de cette section, d'après le théorème de structure de Cohen, l'anneau $\widehat{\mathcal{O}}_{S,C}$ est isomorphe à $k(C)[[v]]$. Malheureusement cet isomorphisme n'est en aucun cas unique. En effet, d'après [Coh46] théorème 10(c), si k est de caractéristique positive, il y a une infinité de sous-corps de $\widehat{\mathcal{O}}_{S,C}$ qui sont envoyés sur le corps résiduel $k(C)$ via le morphisme de réduction modulo $\mathfrak{m}_{S,C}$. Plus précisément, ce défaut d'unicité d'un représentant du corps résiduel est lié au fait que ce dernier n'est pas parfait. D'une certaine manière, le choix de u permet de contourner les éventuels problèmes d'inséparabilité. De ce fait, pour utiliser le théorème de Cohen, nous allons choisir un représentant du corps $k(C)$ qui sera en un certain sens *relié* à la fonction u.

Proposition I.4.6 (Le corps $\mathcal{K}_u$)**.** *Soit $u \in \mathcal{O}_{S,C}$ une fonction dont la restriction $\bar{u}$ à C est un élément séparant[4] de $k(C)$ au-dessus de k. Alors, il existe un unique sous-corps $\mathcal{K}_u$ de $\widehat{\mathcal{O}}_{S,C}$ contenant $k(u)$ et isomorphe à $k(C)$ via le morphisme de réduction modulo $\mathfrak{m}_{S,C}$. De plus, ce corps et une extension monogène de $k(u)$ engendrée par un élément y de $\widehat{\mathcal{O}}_{S,C}$.*

Preuve. **Existence.** Par hypothèse, l'extension de corps $k(C)/k(\bar{u})$ est une extension finie séparable. D'après le théorème de l'élément primitif, il existe une fonction $\bar{y}$ rationnelle sur C qui engendre $k(C)$ sur $k(\bar{u})$. D'après le lemme de Hensel, $\bar{y}$ se relève en un unique élément y de $\widehat{\mathcal{O}}_{S,C}$ dont le polynôme minimal sur $k(u)$ est celui de $\bar{y}$ sur $k(\bar{u})$. Soit $\mathcal{K}_u$, le sous-anneau de $\widehat{\mathcal{O}}_{S,C}$ engendré par $k(u)$ et y, c'est-à-dire

$$\mathcal{K}_u := k(u)[y].$$

On obtient ainsi une copie de $k(C)$ qui contient $k(u)$ et s'envoie isomorphiquement sur $k(C)$ via la réduction modulo $\mathfrak{m}_{S,C}$.

Unicité. Soit $\mathcal{K}'$ un corps distinct de $\mathcal{K}_u$ et vérifiant les mêmes propriétés. Il existe donc un élément de l'un de ces corps qui n'appartient pas à l'autre. Supposons par exemple qu'il existe $z \in \mathcal{K}'$ tel que $z \notin \mathcal{K}_u$. La classe de z modulo $\mathfrak{m}_{S,C}$ est une fonction $\bar{z} \in k(C)$. Cette dernière admet un unique relevé z' dans $\mathcal{K}_u$. De fait, soit $R \in k(\bar{u})[T]$ le polynôme minimal unitaire de $\bar{z}$ au dessus de $k(\bar{u})$. Alors les éléments z et z' de $\widehat{\mathcal{O}}_{S,C}$ sont tous deux solution du problème suivant,

$$\begin{cases} Z & \equiv & \bar{z} \mod \mathfrak{m}_{S,C} \\ R(u, Z) & = & 0. \end{cases}$$

Ce problème admet une solution unique d'après le lemme de Hensel ([Eis95] théorème 7.3) ce qui contredit l'hypothèse que z n'appartient pas à $\mathcal{K}_u$. □

Corollaire I.4.7. *Soit u une fonction rationnelle sur S régulière au voisinage de C dont la restriction $\bar{u}$ à C est un élément séparant de $k(C)/k$. Alors, toute fonction rationnelle f sur S admet un unique développement dans $\mathcal{K}_u((v))$.*

[4] Voir [Sti93] III.9 pour une définition d'*élément séparant*.

Remarque I.4.8. *En réalité, le résultat énoncé dans le corollaire I.4.7 est valable pour tout élément du complété $\mathfrak{m}_{S,C}$-adique du corps $k(S)$.*

Notons que, pour décrire ce corps $\mathcal{K}_u$ nous avons eu besoin de conditions plus faibles sur u que celles qui sont exigées dans la définition de (P,C)-paire forte. C'est ce qui motive la définition suivante.

Définition I.4.9 ((P,C)-paires faibles)**.** *Une (P,C)-paire faible est une paire (u,v) d'éléments de $\mathcal{O}_{S,C}$ vérifiant les conditions suivantes.*

(1) La restriction de u à C est une uniformisante de $\mathcal{O}_{C,P}$.

(2) La fonction v est une uniformisante de $\mathcal{O}_{S,C}$.

Remarque I.4.10. *Dans [Par76], le contexte décrit page 699 revient exactement à se donner une (P,C)-paire faible.*

Il va de soi qu'une (P,C)-paire forte est faible, mais la réciproque est fausse. En effet, en ce qui concerne u, le fait que sa restriction à C soit régulière au voisinage de P ne signifie pas que u l'est. Quant à v, la condition : *être une équation locale de C au voisinage de P* est plus forte que celle d'*être une uniformisante de $\mathcal{O}_{S,C}$*. L'exemple qui suit permet de s'en convaincre.

Exemple I.4.11. Supposons que S soit le plan affine complexe muni de coordonnées affines x et y. Soient C la droite d'équation $y=0$ et P l'origine du plan affine. Posons

$$u := \frac{(x+y)(x-y)}{x} \quad \text{et} \quad v := xy.$$

Alors, le couple (u,v) est une (P,C)-paire faible qui n'est pas forte. En effet, la fonction u n'est pas régulière en P et la fonction v est dans $\mathfrak{m}_{S,P}^2$, elle n'est donc pas une équation locale de C au voisinage de P.

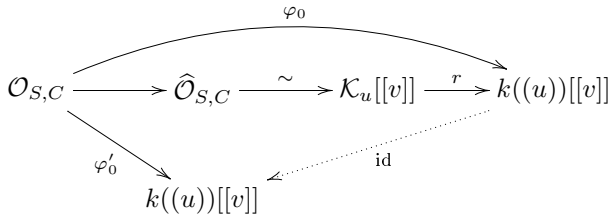
Nous pouvons maintenant présenter le second procédé de décomposition en séries de Laurent.

Proposition I.4.12. *Soit (u,v) une (P,C)-paire faible, il existe un unique morphisme $\varphi : k(S) \hookrightarrow k((u))((v))$ qui envoie $\mathcal{O}_{S,C}$ sur $k((u))[[v]]$ et envoie u,v sur eux-mêmes.*

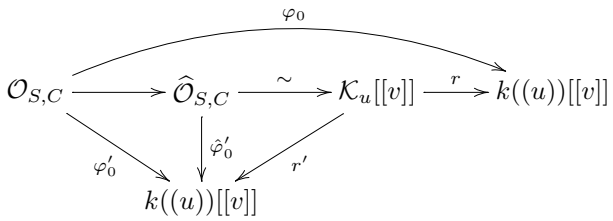
Preuve. **Existence.** Tout comme dans la preuve du lemme I.4.3, il suffit de prouver l'existence d'un morphisme $\varphi_0 : \mathcal{O}_{S,C} \hookrightarrow k((u))[[v]]$ envoyant u et v sur eux-mêmes, puis d'appliquer la propriété universelle des corps de fractions. La courbe C est supposée absolument réduite. Donc, d'après [Mum99] proposition II.4.4 (i), l'extension $k(C)/k$ est séparable, donc admet une base de transcendance séparante. Par ailleurs, la fonction $\bar{u}$ est une uniformisante de $\mathcal{O}_{C,P} \subset k(C)$, donc sa différentielle $d\bar{u} \in \Omega^1_{k(C)/k}$ est non nulle et d'après [Bou59] V.16.7 théorème 5, c'est un élément séparant de $k(C)/k$.

D'après le corollaire I.4.7, on dispose d'une injection $\mathcal{O}_{S,C} \hookrightarrow \mathcal{K}_u[[v]]$ et $\mathcal{K}_u$ est isomorphe à $k(C)$ via le morphisme de réduction modulo $\mathfrak{m}_{S,C}$. De plus, comme $\bar{u}$ est une uniformisante de $\mathcal{O}_{S,P}$, le complété $\mathfrak{m}_{C,P}$-adique de $k(C)$ est isomorphe à $k((\bar{u}))$. On dispose donc d'une injection $\mathcal{K}_u \hookrightarrow k((u))$ qui s'étend coefficient par coefficient en un morphisme $\mathcal{K}_u[[v]] \hookrightarrow k((u))[[v]]$. On en déduit l'existence de l'application $\varphi_0 : \mathcal{O}_{S,C} \hookrightarrow k((u))[[v]]$ recherchée.

Unicité. Soit $\varphi_0' : \mathcal{O}_{S,C} \to k((u))[[v]]$, un autre morphisme d'anneaux envoyant u et v sur eux-mêmes. Nous allons montrer que le diagramme suivant est commutatif.



Comme φ_0' envoie v sur lui-même, on en déduit que c'est un morphisme local non ramifié. La propriété universelle du complété, implique l'existence et l'unicité d'un morphisme $\hat{\varphi}_0'$ qui fait commuter le diagramme suivant.



Le morphisme r' est la composée du morphisme inverse de $\widehat{\mathcal{O}}_{S,C} \xrightarrow{\sim} \mathcal{K}_u((v))$ et de $\hat{\varphi}_0$. Il reste à montrer que $r = r'$. Un morphisme local de $\mathcal{K}_u[[v]]$ dans $k((u))[[v]]$ est entièrement déterminé par les images de u, v et y. Il suffit donc de montrer que $r(y) = r'(y)$. Remarquons dès à présent que, d'après la construction de φ_0 et donc de r, on a $r(y) = \psi(u)$, où $\psi(\bar{u})$ est le développement en série de Laurent en P de $\bar{y} \in k(C)$. Soit $F \in k(\bar{u})[T]$, le polynôme minimal unitaire de $\bar{y}$ sur $k(\bar{u})$. L'élément y de $\widehat{\mathcal{O}}_{S,C}$ vérifie $F(u, y) = 0$ et comme r et r' sont des morphismes d'anneau, on en déduit

$$F(u, r(y)) = 0 \quad \text{et} \quad F(u, r'(y)) = 0 \quad \text{dans } k((u))[[v]].$$

De plus, par passage au quotient modulo v, on a

$$r(\bar{y}) \equiv r'(\bar{y}) \equiv \psi(\bar{u}) \mod (v).$$

Ainsi $r(y)$ et $r'(y)$ sont tous deux solution du problème suivant.

$$\begin{cases} F(u, Z) & = & 0 \\ Z & \equiv & \psi(u) \mod (v). \end{cases}$$

D'après le lemme de Hensel, ce problème admet une unique solution qui est $\psi(u)$. Ce dernier étant égal à $r(y)$, cela conclut la preuve. □

Remarque I.4.13. *La principale différence entre les résultats de ce chapitre et ceux de la première partie de [Par76] est que ce dernier suppose que le corps de base est parfait, alors que nous ne nous sommes donnés aucune restriction sur k dans ce chapitre. On trouve dans cet article la démonstration d'un énoncé analogue à celui de la proposition I.4.12. Cette dernière se trouve de fait simplifiée grâce à cette hypothèse supplémentaire sur k.*

Ainsi, nous avons montré que si (u, v) est une (P, C)-paire forte, les deux approches fournissent les mêmes développements en série de Laurent. Par ailleurs nous avons obtenu une réponse à la question posée à la fin de la section I.4.2. Cela donne lieu au corollaire suivant.

Corollaire I.4.14. *Soit (u, v), une (P, C)-paire faible. Alors, toute fonction $f \in k(S)$ admet un unique développement en séries de Laurent*

$$f = \sum_{j \geq l} f_j(u) v^j \ \in k((u))((v)).$$

De plus, pour tout $j \geq l$, la série de Laurent $f_j(\bar{u})$ est une fonction rationnelle sur C.

I.4.4 Changement de variables

Les séries de Laurent ont été introduites de façon à montrer que l'on peut définir le 2-résidu d'une 2-forme $\omega \in \Omega^2_{k(S)/k}$ en P le long de C, sans aucune condition sur la valuation

de ω le long de C. Nous allons donc donner une définition générale des 2-résidus en utilisant les séries de Laurent. Ensuite, il faudra prouver que cet objet ne dépend pas du choix d'une (P,C)-paire. C'est la raison pour laquelle nous devons introduire les changements de (P,C)-paires.

Lemme I.4.15. *Soient (u,v) et (x,y) deux (P,C)-paires faibles. Les fonctions u et v se décomposent en séries de Laurent en les variables x et y et leurs développements sont de la forme suivante*

$$\left\{ \begin{array}{rcl} u & = & f(x,y) \quad avec \quad f(x,0) \in xk[[x]] \smallsetminus x^2k[[x]] \\ v & = & g(x,y) \quad avec \quad g(x,y) \in yk((x))[[y]] \smallsetminus y^2k((x))[[y]]. \end{array} \right. \tag{CV}$$

De plus, si (u,v) et (x,y) sont des (P,C)-paires fortes, alors f et g sont des séries de Taylor, c'est-à-dire des éléments de $k[[x,y]]$.

PREUVE. Les fonctions u et v sont des éléments de $\mathcal{O}_{S,C}$. D'après la proposition I.4.12, leurs développements respectifs en séries de Laurent $f(x,y)$ et $g(x,y)$ sont dans $k((x))[[x]]$. De plus, si (u,v) et (x,y) sont des (P,C)-paires fortes, alors ces fonctions sont des éléments de $\mathcal{O}_{S,P}$. Or, d'après le lemme I.4.3, les fonctions $\bar{u}$ et $\bar{x} \in k(C)$ sont toutes deux des uniformisantes de $\mathcal{O}_{C,P}$, donc $\bar{u} = f(\bar{x},0)$ est une série de Taylor de valuation $(\bar{x})$-adique 1. Les fonctions v et y sont de valuation $\mathfrak{m}_{S,C}$-adique 1 le long de C, donc leur quotient v/y est un inversible de $\mathcal{O}_{S,C}$. Par conséquent, $G(x,y) := v/y$ est un élément de $k((x))[[y]]$ est de valuation (y)-adique nulle. Ainsi, comme $g = yG$, on en déduit que g est de valuation (y)-adique 1. □

Avant de passer à la suite, faisons un courte remarque sur ce changement de variables. Soient (u,v) et (x,y) deux (P,C)-paires fortes, on dispose donc d'un changement de variables de la forme (CV),

$$\left\{ \begin{array}{rcl} u & = & f(x,y) \\ v & = & g(x,y). \end{array} \right.$$

De plus, les séries f et g sont des séries de Taylor et vérifient

$$f = \sum_{i,j \geq 0} f_{i,j} x^i y^j \quad \text{avec} \quad f_{0,0} = 0 \quad \text{et} \quad f_{1,0} \neq 0 \tag{I.3}$$

et

$$g = \sum_{i,j \geq 0} g_{i,j} x^i y^j \quad \text{avec} \quad \forall k \in \mathbf{N},\ g_{k,0} = 0 \quad \text{et} \quad g_{0,1} \neq 0. \tag{I.4}$$

De toutes la assertions ci-dessus seule "$g_{0,1} \neq 0$" n'est pas complètement évidente. Supposons que $g_{0,1} = 0$, alors, comme $g_{k,0}$ est nul pour tout entier naturel k, on en déduit que $g(x,y)$ est dans l'idéal $((x,y))^2$, ce qui contredit le fait que la paire (u,v) est une (P,C)-paire forte.

Regardons à présent la matrice jacobienne de ce changement de variables.

$$\mathrm{Jac}\left(\frac{f,g}{x,y}\right) = \begin{pmatrix} \frac{\partial f}{\partial x}(0,0) & \frac{\partial f}{\partial y}(0,0) \\ \frac{\partial g}{\partial x}(0,0) & \frac{\partial g}{\partial y}(0,0) \end{pmatrix} = \begin{pmatrix} f_{1,0} & f_{0,1} \\ g_{1,0} & g_{0,1} \end{pmatrix} = \begin{pmatrix} f_{1,0} & f_{0,1} \\ 0 & g_{0,1} \end{pmatrix}.$$

D'après (I.3) et (I.4), le produit $f_{1,0}g_{0,1}$ est non nul, donc que cette matrice est inversible, ce qui est normal puisque (u,v) est un système de coordonnées locales. On voit ainsi que les changement de (P,C)-paires fortes sont des changements de variables dont la jacobienne en P est triangulaire supérieure et inversible. On peut donner une interprétation géométrique à ce fait. Une matrice triangulaire supérieure est la matrice d'un endomorphisme qui préserve un drapeau. Le changement de variables (CV) préserve le *drapeau géométrique* (P,C).

I.4.5 Objets rationnels et formels

Dans la section I.5, nous manipulerons fréquemment des séries de Laurent. Cependant, l'objectif de ce travail n'est pas d'obtenir des résultats sur les séries formelles mais sur des objets géométriques, en l'occurrence les 2-formes rationnelles sur S. Aussi, les séries de Laurent ne sont qu'un outil pour arriver à nos fins. Elles nous permettront de traduire certains problèmes géométriques sous forme de problèmes purement combinatoires. Dans ce qui suit, outre les séries de Laurent nous allons manipuler de formes différentielles formelles, c'est à dire des éléments des espaces de différentielles relatives $\Omega^i_{k((u))((v))/k}$. On renvoie le lecteur au chapitre IX de [Mat86] pour une définition de ces espaces. Le lemme qui suit nous permet d'obtenir une description agréable des ces modules de différentielles relatives.

Lemme I.4.16. *Soit (u,v) une (P,C)-paire faible, on a les isomorphismes*

$$\Omega^i_{k((u))((v))/k} \cong \Omega^i_{k(S)/k} \otimes_{k(S)} k((u))((v)), \quad \textit{pour } i \in \{1,2\}$$

$$\textit{et} \qquad \Omega^1_{k((u))/k} \cong \Omega^1_{k(C)/k} \otimes_{k(C)} k((u)).$$

PREUVE. Voir annexe A.1. □

Lemme I.4.17. *Soient (u,v) deux éléments de $k((x))((y))$ liés aux variables (x,y) par un changement de variables de la forme[5] (CV). Alors, ce changement de variables induit un isomorphisme de corps locaux $k((u))((v)) \to k((x))((y))$. C'est-à-dire qu'il envoie un série de Laurent de valuation (v)-adique $m \in \mathbf{Z}$ sur une série de valuation (y)-adique m. De même, il induit un isomorphisme $\Omega^2_{k((u))((v))/k} \to \Omega^2_{k((x))((y))/k}$ qui préserve les valuations.*

PREUVE. Voir annexe A.3. □

I.5 Définition générale des résidus

En utilisant les notions introduites dans la section I.4, nous allons pouvoir donner une définition plus générale de résidus.

I.5.1 Invariance des 2-résidus

Dans ce qui suit nous allons travailler exclusivement avec des objets formels. Ensuite, en section I.5.2, on appliquera les résultats obtenus dans le cadre formel aux différentielles rationnelles. Noter que, le but étant d'obtenir des informations sur les 2-formes rationnelles, nous aurions pu énoncer un résultat géométrique. Cependant, la preuve du théorème I.5.3, qui est le point clé de cette section, consiste uniquement en des manipulations sur les coefficients de séries formelles. Surtout, nous aurons absolument besoin de la version formelle de ce résultat pour démontrer la proposition I.5.14 (voir section I.5.2). C'est pourquoi nous avons choisi de l'énoncer dans ce contexte.

Notation I.5.1. *Dans tout ce qui suit, lorsque nous aurons affaire à une série de Laurent $f \in k((u))((v))$ ou $k((x))((y))$, nous adopterons le système d'indices suivant. L'indice "i" sera lié à la première variable (u ou x) et l'indice "j" à la seconde (v ou y). De fait, f s'écrit,*

$$f = \sum_{j \geq l} f_j(u) v^j, \quad \textit{avec} \quad f_j(u) = \sum_{i \geq l_j} f_{i,j} u^i \ \in k((u)).$$

[5] Voir lemme I.4.15.

Définition I.5.2. *Soit $\omega = h(u,v)du \wedge dv$ avec $h = \sum_j h_j(u)v^i \in k((u))((v))$, une 2-forme formelle, on définit les objets suivants.*

(1) Le (u,v)-1-résidu de ω est défini par

$$(u,v)res^1(\omega) := h_{-1}(u)du \ \in \Omega^1_{k((u))/k}.$$

(2) Le (u,v)-2-résidu de ω en P le long de C est défini par

$$(u,v)res^2(\omega) := h_{-1,-1} \in k.$$

Le théorème qui suit est la clé de la définition des 2-résidus.

Théorème I.5.3. *Soit (x,y) une paire d'éléments du corps $k((u))((v))$ liée aux fonctions (u,v) par un changement de variables de la forme (CV). Alors, pour toute 2-forme formelle $\omega = h(u,v)du \wedge dv \in \Omega^2_{k((u))((v))/k}$, on a*

$$(u,v)res^2(\omega) = (x,y)res^2(\omega).$$

La preuve de ce théorème nécessite les lemmes I.5.4 et I.5.6 qui seront énoncés plus loin. Tout d'abord, considérons de nouveau le changement de variables (CV).

$$\left\{ \begin{array}{lcll} u & = & f(x,y) & \text{avec} \quad f(x,0) \in xk[[x]] \smallsetminus x^2k[[x]] \\ v & = & g(x,y) & \text{avec} \quad g \in yk((x))[[y]] \smallsetminus y^2k((x))[[y]]. \end{array} \right. \tag{CV}$$

Ce changement de variables peut être appliqué en deux étapes. On peut dans un premier temps passer de (u,v) à (u,y) puis de (u,y) à (v,y). C'est-à-dire,

$$\text{d'abord} \quad \text{(CV1)} \left\{ \begin{array}{lcl} u & = & u \\ v & = & \gamma(u,y) \end{array} \right. , \quad \text{ensuite} \quad \text{(CV2)} \left\{ \begin{array}{lcl} u & = & f(x,y) \\ y & = & y \end{array} \right. ,$$

où $\gamma(x,y)$ de valuation (y)-adique 1. Nous allons montrer successivement que les 2-résidus sont invariants sous l'action de (CV1), puis de (CV2).

Lemme I.5.4 (Invariance des 1-résidus sous l'action de (CV1))**.** *Soit $\omega = h(u,v)du \wedge dv$ une 2-forme formelle. Pour tout y lié à (u,v) par un changement de variables (CV1) : v=g(u,y), on a*

$$(u,v)res^1(\omega) = (u,y)res^1(\omega).$$

Preuve. En appliquant (CV1), on obtient

$$\omega = h(u,g(u,y))\frac{\partial g}{\partial y}du \wedge dy.$$

On peut voir le corps $k((u))((v))$ comme un corps de séries de Laurent à une variable au-dessus de $k((u))$. De ce point de vue, y est une autre uniformisante de ce corps. D'après [Sti93] proposition IV.2.9, le coefficient en v^{-1} de $h(u,v)$ est égal au coefficient en y^{-1} de $h(u,g(u,y))\partial g/\partial y$. □

Remarque I.5.5. *Dans tout le chapitre IV de [Sti93] , le corps de base est supposé parfait. Or si le corps k est de caractéristique positive, le corps $k((u))$ n'est pas parfait. Cependant la démonstration de la proposition IV.2.9 de cet ouvrage est purement formelle et ne nécessite en aucun cas un corps de base parfait.*

Nous avons donc vu que le changement de variables (CV1) n'avait pas d'influence sur les 1-résidus. Il n'en aura donc à fortiori pas sur les 2-résidus. En ce qui concerne le changement de variables (CV2), ce dernier peut avoir une influence sur les 1-résidus, c'est ce que montrait l'exemple I.3.6. Nous allons cependant montrer qu'il n'a pas d'influence sur les 2-résidus. Pour ce faire, nous aurons besoin du lemme qui suit.

Lemme I.5.6. *Pour toute 2-forme formelle $\omega = h(u,v)du\wedge dv \in \Omega^2_{k((u))((v))/k}$, de valuation (v)-adique supérieure ou égale à -1, on a*

$$(u,v)res^1(\omega) = (x,y)res^1(\omega).$$

Remarque I.5.7. *La proposition I.3.1 est une conséquence immédiate de ce lemme.*

PREUVE. D'après le lemme I.5.5, on a $(u,v)\mathrm{res}^1(\omega) = (u,y)\mathrm{res}^1(\omega)$. De fait, nous n'avons qu'à étudier le comportement de ω sous l'action de (CV2). Soit donc $u = f(x,y)$. Isolons dans ω le terme en y^{-1} :

$$\omega = \frac{h_{-1}(u)}{y}du\wedge dy + \left(\sum_{j\geq 0} h_j(u)y^j\right) du\wedge dy = \omega_{-1} + \omega_+.$$

La forme ω_+ a une valuation (y)-adique positive, donc d'après le lemme I.4.17, le changement de variables (CV2) n'a pas d'influence sur cette valuation. De fait, le (x,y)-1-résidu de ω est celui de ω_{-1} et

$$\omega_{-1} = \frac{h_{-1}(f(x,y))}{y}\frac{\partial f}{\partial x}dx\wedge dy.$$

D'après le lemme I.4.17, la valuation (y)-adique de $h_{-1}(f(x,y))$ est égale à la valuation (v)-adique de $h_{-1}(u)$, à savoir 0. Ainsi,

$$(x,y)\mathrm{res}^1(\omega) = h_{-1}(f_0(\bar{x}))f_0'(\bar{x})d\bar{x} = h_{-1}(f_0(\bar{x}))d(f_0(\bar{x})),$$

où $f_0(x) := f(x,0)$. Cette 1-forme formelle est égale à $(u,y)\mathrm{res}^1_{C,P}(\omega) = h_{-1}(\bar{u})d\bar{u}$. Il suffit pour s'en convaincre d'appliquer à $h_{-1}(\bar{u})d\bar{u}$ le changement de variables

$$\bar{u} = f(\bar{x},0).$$

□

Dans la preuve du théorème I.5.3 nous aurons besoin du lemme suivant dont la preuve est donnée en annexe.

Lemme I.5.8. *Soient A,B deux séries de Laurent appartenant à $k((u))((v))$. Pour toute paire de séries (x,y) liée à (u,v) par un changement de variables de la forme (CV), on a*

$$(x,y)res^2\,(dA\wedge dB) = 0.$$

PREUVE. Voir annexe A.2. □

Nous disposons à présent de tous les outils nécessaires à la démonstration du théorème I.5.3. Dans un premier temps, nous allons le démontrer dans le cas où la caractéristique du corps de base k est nulle.

PREUVE DU THÉORÈME I.5.3 SI k EST DE CARACTÉRISTIQUE NULLE. Dans l'intégralité de cette preuve, les (x,y)-1- et 2-résidus sont toujours en P le long de C. Aussi, pour alléger la rédaction, nous omettrons de signaler les "en P le long de C".

Commençons par décomposer $\omega = hdu\wedge dv$ en isolant les termes de valuation (y)-adique inférieure ou égale à -2.

$$\omega = \sum_{j=-l}^{-2} h_j(u)y^j du\wedge dy + \sum_{j\geq -1} h_j(u)y^j du\wedge dy = \omega_- + \omega_{\mathrm{inv}}.$$

Noter que l'extraction d'un 2-résidu est une application k-linéaire. Aussi, d'après les lemmes I.5.5 et I.5.6, il suffit d'étudier le comportement des 2-résidus de ω_- sous l'action de (CV2).

De plus, toujours pour des raisons de linéarité, on peut scinder le problème et restreindre notre étude aux 2-formes de la forme :

$$\omega = \phi(u)du \wedge \frac{dy}{y^n} \quad \text{avec} \quad \phi \in k((u)) \quad \text{et} \quad n \geq 2.$$

Le (u,y)-1-résidu de la 2-forme formelle ci-dessus est nul, il est en donc de même pour son (u,y)-2-résidu. Avant d'appliquer (CV2), nous allons continuer à travailler ω au corps. Isolons le terme en u^{-1} de la série de Laurent $\phi \in k((u))$.

$$\phi(u) = \widetilde{\phi}(u) + \frac{\phi_{-1}}{u}, \text{ où } \widetilde{\phi}_i = \begin{cases} \phi_i & \text{si} \quad i \neq -1 \\ 0 & \text{si} \quad i = -1. \end{cases}$$

Comme k est supposé de caractéristique nulle, la série $\widetilde{\phi}(u)$ a une primitive formelle $\widetilde{\Phi}(u)$. De même, posons $s := \frac{1}{(1-n)y^{n-1}}$. C'est une primitive formelle de $1/y^n$. On a alors

$$\omega = d\widetilde{\Phi} \wedge ds + \phi_{-1}\frac{du}{u} \wedge ds = \omega_r + \phi_{-1}\omega_{-1}.$$

D'après le lemme I.5.8, la forme ω_r a un 2-résidu nul et indépendant du choix de (u,y). Il reste à étudier la 2-forme

$$\omega_{-1} = \frac{du}{u} \wedge \frac{dy}{y^n}.$$

En lui appliquant (CV2), on obtient

$$\omega_{-1} = \frac{df(x,y)}{f(x,y)} \wedge \frac{dy}{y^n}.$$

Rappelons que f est de la forme : $\sum_{j\geq 0} f_j(x)y^j$ avec :

$$f_0(x) = f_{1,0}x + f_{2,0}x^2 + \cdots \quad \text{et} \quad f_{1,0} \neq 0.$$

On peut donc factoriser f_0 en

$$f_0(x) = f_{1,0}x\left(1 + \frac{f_{2,0}}{f_{1,0}}x + \cdots\right).$$

Posons

$$\begin{array}{rrcll} & r(x) & := & \frac{f_{2,0}}{f_{1,0}}x + \frac{f_{3,0}}{f_{1,0}}x^2 + \cdots & \in k[[x]] \\ \text{et} & \mu(x,y) & := & \frac{f_1(x)}{f_0(x)}y + \frac{f_2(x)}{f_0(x)}y^2 + \cdots & \in k((x))[[y]]. \end{array}$$

La série f se factorise donc en

$$f(x,y) = f_{1,0}x(1 + r(x))(1 + \mu(x,y)). \tag{I.5}$$

Par ailleurs, pour toute série S appartenant à $xk[[x]]$ (resp. à $yk((x))[[y]]$), on définit le logarithme formel de $1+S$ par

$$log(1+S) := \sum_{k=0}^{+\infty}(-1)^{k+1}\frac{S^k}{k}.$$

Cette définition a un sens puisque k est supposé de caractéristique nulle. De plus, cette série converge pour la topologie (x)-adique (resp. (y)-adique). Enfin, on a

$$d\log(1+S) = \frac{d(1+S)}{1+S}.$$

En utilisant la factorisation I.5, on obtient :

$$\omega_{-1} = \underbrace{\frac{dx}{x} \wedge \frac{dy}{y^n}}_{\mu_1} + \underbrace{d\log(1+r) \wedge ds}_{\mu_2} + \underbrace{d\log(1+\mu) \wedge ds}_{\mu_3}.$$

D'après le lemme I.5.8, les (x,y)-2-résidus des formes μ_2 et μ_3 sont nuls. La forme μ_1 a un (x,y)-1-résidu nul (elle n'a pas de terme en dy/y), son (x,y)-2-résidu est également nul. On en conclut que

$$(x,y)\mathrm{res}^2_{C,P}(\omega_{-1}) = 0.$$

□

Esquisse de preuve du théorème I.5.3 en caractéristique positive. La preuve est semblable à celle de l'invariance des résidus de 1-formes sur des courbes (c.f. [Sti93] IV.2.9 ou [Ser59] II.7 proposition 5). On montre que le (x,y)-2-résidu de ω est une expression polynomiale en certains coefficients de f. Ce polynôme ne dépend ni de f ni du corps de base. D'après le théorème de prolongement des identités algébriques ([Bou59] IV.3 proposition 9) et le travail effectué en caractéristique nulle, on conclut que ce polynôme est nul. Une preuve détaillée est donnée en annexe A.4. □

Ainsi, à partir de maintenant, lorsque nous parlerons de 2-résidus en un point le long d'un courbe, nous n'aurons plus à préciser la (P,C)-paire.

I.5.2 Le cadre géométrique

À présent nous allons introduire les notions de 1- et 2-résidus pour des 2-formes rationnelles. Tout comme en section I.3, les 2-résidus seront associés à un point P et une courbe C contenant P et les 1-résidus seront associés à une courbe C. Ces derniers, seront également associés à un autre paramètre si ω a un pôle multiple le long de C. Commençons par définir les 2-résidus qui sont *plus intrinsèques*.

Définition I.5.9. *Soient (u,v) une (P,C)-paire faible et ω une 2-forme rationnelle sur S. Il existe une fonction $h \in k(S)$ telle que $\omega = hdu \wedge dv$ et cette fonction admet un unique développement en série de Laurent $H(u,v)$. On appelle 2-résidu de ω en P le long de C le coefficient $H_{-1,-1}$ de $x^{-1}y^{-1}$ de H. On le note*

$$res^2_{C,P}(\omega) := H_{-1,-1}.$$

En d'autres termes et pour faire le lien avec ce qui précède, le 2-résidu en P le long de C de ω est le (u,v)-2-résidu de ω vue comme une forme formelle. Le travail effectué en section I.5.1 nous assure que l'objet est bien défini et ne dépend pas du choix de la paire (u,v).

Passons maintenant à la définition de résidus en codimension 1. Notre objectif est d'associer à une 2-forme différentielle rationnelle ω sur S une 1-forme rationnelle μ sur C.

Proposition I.5.10. *Soit u une fonction rationnelle sur S régulière au voisinage de C dont la restriction $\bar{u}$ à C est un élément séparant de $k(C)/k$. Soient ω une 2-forme rationnelle sur S et v une uniformisante de l'anneau $\mathcal{O}_{S,C}$. On rappelle que, d'après la proposition I.4.6 et son corollaire I.4.7, il existe une unique série de Laurent*

$$f = \sum_{j \geq -l} f_j v^j \in \mathcal{K}_u((v)) \quad \textit{telle que} \quad \omega = f du \wedge dv.$$

De plus, la 1-forme $\bar{f}_{-1} d\bar{u}$ est rationnelle sur C et ne dépend pas du choix de v.

Définition I.5.11. *Sous les hypothèses de la proposition I.5.10, on appelle (u)-1-résidu de ω le long de C la 1-forme rationnelle sur C définie par*

$$(u)res^1_C(\omega) := \bar{f}_{-1} d\bar{u}.$$

PREUVE DE LA PROPOSITION I.5.10. Rappelons que f_{-1} est un élément de $\mathcal{K}_u$. Ainsi, sa classe $\bar{f}_{-1}$ modulo $\mathfrak{m}_{S,C}$ est un élément de $k(C)$, la 1-forme $\bar{f}_{-1}d\bar{u}$ est donc rationnelle. L'indépendance de cette 1-forme par rapport au choix de v se démontre de la même façon que le lemme I.5.4. Si w est une autre uniformisante de $\mathcal{O}_{S,C}$, d'après [Sti93] IV.2.9, le coefficient en v^{-1} de la série de Laurent $f \in \mathcal{K}_u((v))$ est égal à celui en w^{-1} de $f\frac{\partial v}{\partial w}$. □

Remarque I.5.12. *L'exemple I.3.6 confirme la nécessité de faire intervenir la fonction u dans la définition. On ne peut espérer obtenir un objet qui ne dépende que de ω et de la courbe C.*

Maintenant que nous disposons d'une définition générale de 1-résidu, il serait souhaitable que cette dernière soit compatible avec la définition I.3.2. De plus, étant donné un point rationnel P de C, il serait intéressant de savoir quelle relation lie le (u)-1-résidu de ω le long de C et son 2-résidu en P le long de C. C'est le but du lemme I.5.13 et de la proposition I.5.14.

Lemme I.5.13. *Sous les conditions de la proposition I.5.10, soit ω une 2-forme rationnelle sur S de valuation supérieure ou égale à -1 le long de C. Alors le (u)-1-résidu de ω le long de C coïncide avec le résidu de ω le long de C de la définition I.3.1.*

PREUVE. Il existe une unique série de Laurent f appartenant à $\mathcal{K}_u((v))$ de valuation -1 telle que

$$\omega = f du \wedge dv = \sum_{j \geq -1} f_j v^j du \wedge dv.$$

Soit φ une fonction rationnelle sur S régulière au voisinage de C et dont la restriction à C est égale à $\bar{f}_{-1}$, on pose

$$\eta_1 := \varphi du \quad \text{et} \quad \eta_2 := \omega - \varphi du \wedge \frac{dv}{v}.$$

La 2-forme η_2 est régulière le long de C et ω se décompose en

$$\omega = \eta_1 \wedge \frac{dv}{v} + \eta_2.$$

D'après la définition I.3.2, la 1-forme $\eta_{1|C}$ sur C est le 1-résidu de ω le long de C. Or, $\eta_{1|C}$ est égale à $\bar{f}_{-1}d\bar{u}$. □

Proposition I.5.14. *Sous les conditions de la proposition I.5.10. Soient ω une 2-forme rationnelle sur S et P un point rationnel lisse de C, alors*

$$res_P((u)res^1_C(\omega)) = res^2_{C,P}(\omega).$$

Remarque I.5.15. *Si ω est de valuation supérieure ou égale à -1 le long de C, la proposition I.5.14 entraîne que le 2-résidu de ω en P le long de C défini dans cette section coïncide avec celui de la section I.3.*

Remarque I.5.16. *La condition "P est un point lisse de C" pourra être supprimée dès que l'on saura définir des 2-résidus le long de C en des points singuliers de cette courbe (voir section I.6.2).*

PREUVE DE LA PROPOSITION I.5.14. Soient P un point rationnel de C et v une uniformisante de $\mathcal{O}_{S,C}$. Commençons par noter que, si $\bar{u}$ est une uniformisante de $\mathcal{O}_{C,P}$, alors le résultat est évident d'après la définition du 2-résidu en P le long de C. En effet, dans cette situation, pour toute uniformisante v de $\mathcal{O}_{S,C}$, le couple (u,v) est une (P,C)-paire faible et

$$\mathrm{res}^2_{C,P}(\omega) = \mathrm{res}_P\left((u)\mathrm{res}^1_C(\omega)\right).$$

Si maintenant $\bar{u}$ n'est pas une uniformisante de $\mathcal{O}_{C,P}$, alors quatre situations peuvent survenir. Dans ce qui suit, t désigne la fonction $\frac{1}{u}$.

(1) La fonction $\bar{u}$ est régulière en P et $\bar{u}' := \bar{u} - \bar{u}(P)$ est une uniformisante de $\mathcal{O}_{C,P}$.
(2) La fonction $\bar{u}$ est régulière en P et $\bar{u}' := \bar{u} - \bar{u}(P)$ n'est pas une uniformisante de $\mathcal{O}_{C,P}$.
(3) La fonction $\bar{u}$ n'est pas régulière en P et $\bar{t}' := \bar{t} - \bar{t}(P)$ est une uniformisante de $\mathcal{O}_{C,P}$.
(4) La fonction $\bar{u}$ n'est pas régulière en P et $\bar{t}' := \bar{t} - \bar{t}(P)$ n'est pas une uniformisante de $\mathcal{O}_{C,P}$.

Remarquons que l'on peut donner une interprétation géométrique simple des deux premières situations si u est régulière[6] en P. La première situation signifie que la ligne de niveau $u = u(P)$ intersecte C transversalement en P. Dans la seconde situation, cette ligne de niveau est singulière en P ou tangente à C en P.

Nous allons à présent traiter successivement ces quatre situations. On rappelle qu'il existe une unique fonction rationnelle f sur S telle que $\omega = f du \wedge dv$ et que f se décompose de façon unique en série de Laurent

$$f = \sum_{j \geq -l} f_j v^j.$$

On pose également $\mu := (u)\mathrm{res}^1_C(\omega)$.

Situation 1. Le sous-corps $\mathcal{K}_u$ de $\widehat{\mathcal{O}}_{S,C}$ défini dans la proposition I.4.6 est l'unique sous-corps de $\widehat{\mathcal{O}}_{S,C}$ qui contienne $k(u)$ et soit isomorphe à $k(C)$ via le morphisme de réduction modulo $\mathfrak{m}_{S,C}$. La fonction $u_0 := u - \bar{u}(P)$ engendre le même sous-corps de $\mathcal{O}_{S,C}$. En d'autres termes, $k(u) = k(u_0)$. De ce fait, les sous-corps $\mathcal{K}_u$ et $\mathcal{K}_{u_0}$ de $\widehat{\mathcal{O}}_{S,C}$ sont égaux. De plus, $du = du_0$. Par conséquent,

$$\omega = f du \wedge dv = f du_0 \wedge dv$$

et le (u_0)-1-résidu de ω le long de C est $\bar{f}_{-1} d\bar{u}'$ qui est égal à μ. On déduit que

$$\mathrm{res}^2_{C,P}(\omega) = \mathrm{res}_P((u_0)\mathrm{res}^1_C(\omega)) = \mathrm{res}_P(\mu).$$

Situation 2. Soit x une fonction rationnelle sur S telle que (x, v) soit une (P, C)-paire faible. La fonction $\bar{x}$ est donc une uniformisante de $\mathcal{O}_{C,P}$. De fait, il existe une série formelle $\phi \in k[[T]]$ telle que $\bar{u}' = \phi(\bar{x})$. Soit σ le relevé de Hensel de $\bar{x}$ dans $\widehat{\mathcal{O}}_{S,C}$, alors c'est un élément de $\mathcal{K}_u$ et dans ce corps, on a la relation

$$u_0 = \phi(\sigma).$$

On en déduit la nouvelle expression de ω

$$\omega = \sum_{j \geq -l} f_j v^j \phi'(\sigma) d\sigma \wedge dv, \tag{I.6}$$

où ϕ' désigne la dérivée formelle de ϕ. Notons que σ n'est à priori pas une fonction. Le second membre de l'expression (I.6) est à priori une 2-forme formelle appartenant à $\Omega^2_{k((u))((v))/k}$ (voir section I.4.5). À présent, rappelons que σ est un élément de $\widehat{\mathcal{O}}_{S,C}$ qui est congru à x modulo $\mathfrak{m}_{S,C}$. Par conséquent, σ se décompose dans $k((x))[[v]]$ de la façon suivante

$$\sigma = x + \sigma_1(x)v + \sigma_2(x)v^2 + \cdots$$

La paire (σ, v) est liée à la paire (x, v) par un changement de variables de la forme (CV). D'après le théorème I.5.3, l'expression (I.6) fournit le même 2-résidu que la décomposition de ω dans $k((x))((v))$. On en conclut que

$$\mathrm{res}^2_{C,P}(\omega) = \mathrm{res}_P(\bar{f}_{-1}\phi'(\bar{\sigma})d\bar{\sigma}) = \mathrm{res}_P(\bar{f}_{-1}\phi'(\bar{x})d\bar{x}).$$

Or, $\phi'(\bar{x})d\bar{x}$ est égal à $d\phi(\bar{x}) = d\bar{u}'$, donc $\bar{f}_{-1}\phi'(\bar{x})d\bar{x}$ est égal à μ.

[6] Noter que le fait que $\bar{u}$ soit régulière en P ne signifie en rien que u l'est. Par exemple, sur $\mathbf{A}^2$, la fonction $u := (x+y)/(x-y)$ n'est pas régulière à l'origine. Par contre, sa restriction à la courbe $C := \{y = 0\}$ est la fonction constante et égale à 1 qui est régulière à l'origine.

Situation 3. Tout comme dans la situation 1, on remarque que, comme u est égal à $\frac{1}{t}$, on a

$$k(u) = k(t), \quad \text{ce qui implique} \quad \mathcal{K}_u = \mathcal{K}_t.$$

De fait, le développement de ω à coefficient dans $\mathcal{K}_t((v))$ s'écrit

$$\omega = \sum_{j \geq -l} f_j v^j \left(-\frac{dt}{t^2}\right) \wedge dv.$$

Par conséquent, on a

$$(t)\mathrm{res}^1_C(\omega) = -\bar{f}_{-1}\frac{d\bar{t}}{\bar{t}^2} = \bar{f}_{-1} d\bar{u} = (u)\mathrm{res}^1_C(\omega).$$

Comme $\bar{t}$ est par hypothèse une uniformisante de $\mathcal{O}_{C,P}$, le couple (t, v) est une (P, C)-paire faible et donc

$$\mathrm{res}^2_{C,P}(\omega) = \mathrm{res}_P((t)\mathrm{res}^1_C(\omega)) = \mathrm{res}_P((u)\mathrm{res}^1_C(\omega)).$$

Situation 4. D'après la situation 3, le (t)-1-résidu de ω le long de C est égal à son (u)-1-résidu. On reprend alors le travail effectué dans la situation 2 en remplaçant u par t et on en déduit le résultat. □

En conclusion, les objets définis dans cette section sont bien une généralisation de ceux introduits en section I.3.

I.6 Propriétés des résidus

Sur une courbe algébrique irréductible lisse X, une 1-forme régulière en un point P a un résidu nul en ce point. On dispose donc d'une condition nécessaire pour que le résidu d'une 1-forme en un point soit non nul. Le lemme qui suit fournit un énoncé analogue pour les 2-résidus. On rappelle que l'on se place toujours dans le cadre donné en section I.2.

Lemme I.6.1. *Soit ω une 2-forme rationnelle sur S admettant C comme pôle (éventuellement multiple) et P un point rationnel lisse de C. Si ω n'a pas d'autre pôle que C au voisinage de P, alors*

$$res^2_{C,P}(\omega) = 0.$$

Preuve. Soient (u, v) une (P, C)-paire forte et n un entier tel que la valuation de ω le long de C soit égale à $-n$. Par hypothèse, l'entier n est positif. Par ailleurs, il existe une fonction rationnelle h, régulière au voisinage de C, telle que

$$\omega = h du \wedge \frac{dv}{v^n}.$$

De plus, comme C est le seul pôle de ω au voisinage de P, on en déduit que h est régulière au voisinage de P, elle se développe donc en série de Taylor

$$h = \sum_{j \geq 0} h_j(u) v^j \quad \text{où } h_j \in k[[u]] \text{ pour tout entier } j.$$

Par conséquent,

$$(u)\mathrm{res}^1_C(\omega) = h_{n-1}(\bar{u}) d\bar{u}.$$

Cette 1-forme sur C est régulière au voisinage de P, son résidu en P est donc nul. □

Remarque I.6.2. *C'est pour démontrer ce type d'énoncé que la notion de (P, C)-paire forte est très utile.*

En d'autres termes, une 2-forme sur S admet un 2-résidu non nul en un point P le long d'une courbe C, seulement si plusieurs ω a des pôles autres que C au voisinage de P.

I.6.1 Influence d'un éclatement sur les résidus

Soient P un point rationnel lisse de C et (u,v) une (P,C)-paire faible. On note $\pi : \widetilde{S} \to S$ l'éclatement de S en P. On note E, le diviseur exceptionnel de $\widetilde{S}$. La transformation stricte par π d'une courbe X passant par P sera notée $\widetilde{X}$. On rappelle que la transformation stricte d'une courbe est l'adhérence de Zariski dans $\widetilde{S}$ de la courbe $\pi^{-1}(X) \smallsetminus E$.

Lemme I.6.3. *Soit ω une 2-forme rationnelle sur S, on a*

$$(\pi^* u) res^1_{\widetilde{C}}(\pi^*\omega) = \pi^* \left((u) res^1_C(\omega) \right).$$

PREUVE. L'application π induit un isomorphisme entre un ouvert de C et un ouvert de sa transformée stricte. Les 1-formes $(\pi^*u)\mathrm{res}^1_{\widetilde{C}}(\pi^*\omega)$ et $(u)\mathrm{res}^1_C(\omega)$ sont tirées en arrière l'une de l'autre par cet isomorphisme. □

Corollaire I.6.4. *Soit ω une 2-forme rationnelle sur U et Q le point d'intersection[7] de E avec $\widetilde{C}$. On a*

$$res^2_{\widetilde{C},Q}(\pi^*\omega) = res^2_{C,P}(\omega).$$

I.6.2 Le cas des points singuliers d'une courbe

Les deux énoncés qui précèdent permettent de généraliser la définition 2-résidu d'une 2-forme en P le long de C au cas où P est un point singulier de C. Dans ce qui suit, P désigne un point rationnel éventuellement singulier de C.

Proposition I.6.5. *Soit $\pi : \widetilde{S} \to S$ un morphisme birationnel provenant d'une suite finie d'éclatements de S induisant une résolution de la singularité de C en P. Soit $\widetilde{C}$ la transformée stricte de C par π, alors, la somme*

$$\sum_{Q \to P} res^2_{\widetilde{C},Q}(\pi^*\omega)$$

ne dépend pas de π. La notation "$Q \to P$" signifie que Q est un point de $\widetilde{C}$ envoyé sur P par π.

PREUVE. Soient $\pi_1 : \widetilde{S}_1 \to S$ et $\pi_2 : \widetilde{S}_2 \to S$ deux tels morphismes et notons $\widetilde{C}_1$ et $\widetilde{C}_2$ les transformées strictes respectives de C par ces applications. Comme les deux applications induisent un résolution de la singularité de C en P, le point P a le même nombre d'antécédents par $\pi_{1|\widetilde{C}_1}$ et $\pi_{2|\widetilde{C}_2}$. Notons respectivement $P_{1,1},\dots,P_{1,n}$ et $P_{2,1},\dots,P_{2,n}$ ces antécédents. Il existe alors deux ouverts $U_1 \subseteq \widetilde{C}_1$ et $U_2 \subseteq \widetilde{C}_2$ contenant respectivement $P_{1,1},\dots,P_{1,n}$ et $P_{2,1},\dots,P_{2,n}$ et un isomorphisme $\varphi : U_1 \to U_2$ tel que $\pi_{1|U_1} = \pi_{2|U_2} \circ \varphi$. De plus, quitte à ré ordonner les indices, φ envoie $P_{1,i}$ sur $P_{2,i}$ pour tout i appartenant à $\{1,\dots,n\}$.

On se donne alors une fonction $u \in \mathcal{O}_{S,C}$ dont la restriction à C est un élément séparent de $k(C)/k$. D'après le corollaire I.6.3, les 1-formes sont tirées en arrière l'une de l'autre par φ. Par conséquent, on a

$$\forall i \in \{1,\dots,n\}, \quad \mathrm{res}^2_{\widetilde{C}_1,P_{1,i}}(\pi_1^*\omega) = \mathrm{res}^2_{\widetilde{C}_2,P_{2,i}}(\pi_2^*\omega).$$

□

Définition I.6.6. *Soit P un point rationnel singulier de C et $\pi : \widetilde{S} \to S$ un morphisme birationnel défini par une séquence finie d'éclatements induisant une résolution de la singularité de C en P. Soit ω une 2-forme rationnelle sur S, on définit le 2-résidu de ω en P le long de C par*

$$res^2_{C,P}(\omega) := \sum_{Q \to P} res^2_{\widetilde{C},Q}(\pi^*\omega).$$

[7] La courbe C est supposée lisse en P. Par conséquent, elle intersecte E en un unique point.

Remarque I.6.7. *Les points Q au-dessus de P peuvent être définis sur une extension finie de k. Cependant, on peut facilement se convaincre du fait que la somme qui définit $res^2_{C,P}(\omega)$ est invariante sous l'action du groupe de Galois absolu de k. Le 2-résidu reste donc un élément de k.*

Remarque I.6.8. *Muni de cette définition on montre aisément que l'énoncé de la proposition I.5.14 reste valable dans le cas où le point P est un point singulier de la courbe C. Pour ce faire, il suffit de réaliser le même raisonnement que dans la preuve de cette proposition mais en l'appliquant à la courbe $\widetilde{C}$ de la définition ci-dessus.*

Une autre façon de définir et de calculer les 2-résidus d'une 2-forme le long d'une courbe C en un point singulier P de cette dernière est d'étendre à cette situation la définition de (P, C)-paire faible. Ce point de vue nous sera utile dans le chapitre III.

Définition I.6.9. *Soient donc C une courbe irréductible absolument réduite plongée dans S et P un point rationnel éventuellement singulier de S. On appelle $\pi : \widetilde{C} \to C$ la normalisation de C. Une (P, C)-paire faible est un couple de fonctions (u, v) appartenant à l'anneau local $\mathcal{O}_{S,C}$ et vérifiant les conditions suivantes.*

(*i*) *Pour tout point fermé Q de $\widetilde{C}$ au-dessus de P, la fonction $\pi^*\bar{u} \in k(\widetilde{C})$ est une uniformisante de $\mathcal{O}_{\widetilde{C},Q}$.*

(*ii*) *La fonction v est une uniformisante de $\mathcal{O}_{S,C}$.*

Remarque I.6.10. *Notons que cette définition est une généralisation naturelle de la définition I.4.9 de (P, C)-paires faibles.*

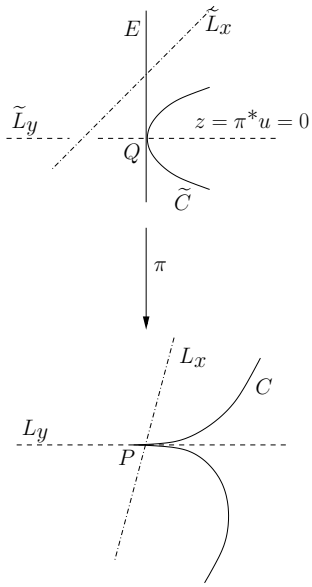
Remarque I.6.11. *Une (P, C)-paire faible existe toujours. En effet, d'après le théorème d'approximation faible ([Sti93] théorème I.3.1), il existe une fonction z dans $k(\widetilde{C})$ qui est une uniformisante de $\mathcal{O}_{\widetilde{C},Q}$ pour tout point fermé Q au-dessus de P. On descend z en une fonction $\bar{u}$ sur C que l'on relève ensuite en une fonction u dans $\mathcal{O}_{S,C}$.*

Exemple I.6.12. Prenons $S = \mathbf{A}^2_{\mathbf{C}}$ et C la cubique *cuspidale* d'équation affine $y^2 = x^3$ et P l'origine. On pose alors

$$u := \frac{y}{x} \quad \text{et} \quad v := y^2 - x^3.$$

On appelle L_x et L_y les droites d'équations respectives $x = 0$ et $y = 0$. Éclatons $\mathbf{A^2}$ en P. On considère dons la surface plongée dans $\mathbf{A}^2 \times \mathbf{P}^1$ définie par l'équation $xu = yv$ où $(u : v)$ est un système de coordonnées homogènes de $\mathbf{P}^1$. On pose $z := \frac{u}{v}$ et dans la carte affine $v \neq 0$ on obtient des équations pour $\widetilde{C}$,

$$\widetilde{C} = \{y = xz\} \cap \{z^2 = x\}.$$



On appelle Q le point de $\widetilde{C}$ au-dessus de P. La fonction $\pi^* u$ est égale à z et son lieu d'annulation au voisinage de Q est $\widetilde{L}_y$ qui intersecte $\widetilde{C}$ en Q avec multiplicité 1. De fait, $\pi^* \bar{u} = \bar{z}$ est une uniformisante de $\mathcal{O}_{\widetilde{C},Q}$. En conclusion, la couple (u, v) est bien une (P, C)-paire faible au sens de la définition I.6.9.

Terminons cette section sur un commentaire élémentaire. Soient C une courbe irréductible absolument réduite plongée dans S et P un point rationnel singulier de C. Soient alors (u, v) une (P, C)-paire faible et ω une 2-forme sur S. Comme $\bar{u}$ est un élément séparant de $k(C)/k$, on peut définir un (u)-1-résidu de ω le long de C qui s'identifie à une 1-forme sur la normalisée $\widetilde{C}$ de C. La somme des résidus de cette 1-forme sur $\widetilde{C}$ en tous les points au-dessus de P est évidemment égal au 2-résidu de ω en P le long de C de la définition I.6.6.

I.7 Formules de sommation

Les résultats énoncés dans cette section, en particulier le théorème I.7.11, sont ceux que nous utiliserons dans les chapitres suivants qui portent sur les codes correcteurs. On rappelle que notre objectif est de construire des codes à partir de 2-formes sur une surface et d'obtenir des relations d'orthogonalité entre ces codes et les codes fonctionnels. Dans le cas des courbes, une partie de la démonstration de cette relation d'othogonalité consiste à utiliser la formule des résidus. Aussi, il semble intéressant de pouvoir disposer de formules de sommation de 2-résidus d'une 2-forme sur une surface. Nous allons fournir trois relations de sommations. La troisième est celle qui nous sera la plus utile dans ce qui suit.

Attention ! Tout comme dans le cas des courbes, les formules de sommation qui suivent font intervenir tous des points géométriques de la surface. Aussi pour plus de confort, le corps de base k sera supposé **algébriquement clos** dans cette section.

Théorème I.7.1 (Première formule des résidus)**.** *Soit S une surface quasi-projective lisse géométriquement intègre définie sur k. Soient C une courbe projective irréductible plongée dans S et ω une 2-forme rationnelle sur S. On a*

$$\sum_{P \in C} res^2_{C,P}(\omega) = 0.$$

Remarque I.7.2. *D'après le lemme I.6.1, la somme ci-dessus a un support fini, l'énoncé a donc un sens.*

PREUVE. Commençons par supposer que C est lisse. Soit u une fonction rationnelle sur S, régulière au voisinage de C et dont la restriction $\bar{u}$ à C est un élément séparant de $k(C)/k$. Soit μ le (u)-1-résidu de ω le long de C. D'après la proposition I.5.14 et la remarque I.6.8, on a

$$\sum_{P\in C} \mathrm{res}^2_{C,P}(\omega) = \sum_{P\in C} \mathrm{res}_P(\mu)$$

et cette dernière somme est nulle d'après la formule des résidus sur une courbe. Si maintenant C est singulière, on considère un morphisme birationnel $\pi : \widetilde{S} \to S$ obtenu par une séquence finie d'éclatements et tel que la transformée stricte $\widetilde{C}$ de C soit lisse. D'après le lemme I.6.3 et son corollaire I.6.4, on a

$$\sum_{P\in C} \mathrm{res}^2_{C,P}(\omega) = \sum_{Q\in \widetilde{C}} \mathrm{res}^2_{\widetilde{C},Q}(\omega) = \sum_{Q\in \widetilde{C}} \mathrm{res}_Q(\pi^*\mu).$$

On conclut de nouveau en appliquant la formule des résidus à la courbe $\widetilde{C}$ et la 1-forme $\pi^*\mu$. □

Remarque I.7.3. *Noter que si la valuation de ω le long de C est supérieure ou égale à -1, alors le résultat est évident. En effet, il suffit d'appliquer la formule des résidus au 1-résidu de ω le long de C. La partie non évidente de la preuve ci-dessus est l'étude du cas où ω a un pôle multiple le long de C. Le travail sur les (u)-1-résidus effectué dans les sections I.5 et I.6 avait pour principal objectif de fournir les outils nécessaires à la preuve de ce résultat.*

Théorème I.7.4 (Deuxième formule des résidus)**.** *Soit S une surface quasi-projective lisse géométriquement intègre définie sur k. Soient P un point de S et $\mathcal{C}_{\mathcal{S},\mathcal{P}}$ l'ensemble des germes courbes irréductibles tracées sur S et contenant P. Pour toute 2-forme ω rationnelle sur S, on a*

$$\sum_{C\in\mathcal{C}_{S,P}} res^2_{C,P}(\omega) = 0.$$

Remarque I.7.5. *La somme ci-dessus a également un support fini (c.f. remarque I.7.2).*

PREUVE. Soient ω une 2-forme rationnelle sur S et $C_1, \ldots, C_n$ les composantes irréductibles du lieu des pôles de ω au voisinage de P.

Étape 1. Dans un premier temps, nous allons supposer que les pôles $C_1, \ldots, C_n$ de ω sont lisses en P et se croisent deux à deux transversalement en ce point.

- Si $n = 1$, d'après le lemme I.6.1, le 2-résidu de ω en P le long de C_1 est nul. Le résultat est donc immédiat.
- Si $n = 2$, soient u_1 et u_2 des équations locales respectives des courbes C_1 et C_2 au voisinage de P. Par hypothèse, C_1 et C_2 se croisent transversalement en P, donc (u_1, u_2) est un système de coordonnées locales en ce point. De fait, (u_1, u_2) est une (P, C_2)-paire forte et (u_2, u_1) une (P, C_1)-paire forte. Soient $-n_1$ et $-n_2$ les valuations respectives de ω le long de C_1 et C_2. Il existe une fonction h régulière au voisinage de P telle que

$$\omega = h\frac{du_1}{u_1^{n_1}} \wedge \frac{du_2}{u_2^{n_2}}.$$

  On développe h en série de Taylor

$$h = \sum_{i,j\neq 0} h_{i,j} u_1^i u_2^j.$$

  Le 2-résidu de ω en P le long de C est égal à h_{n_1-1,n_2-1} et, comme le produit extérieur est anticommutatif, le 2-résidu de ω le long de C_1 est égal à $-h_{n_1-1,n_2-1}$. Leur somme est donc nulle.

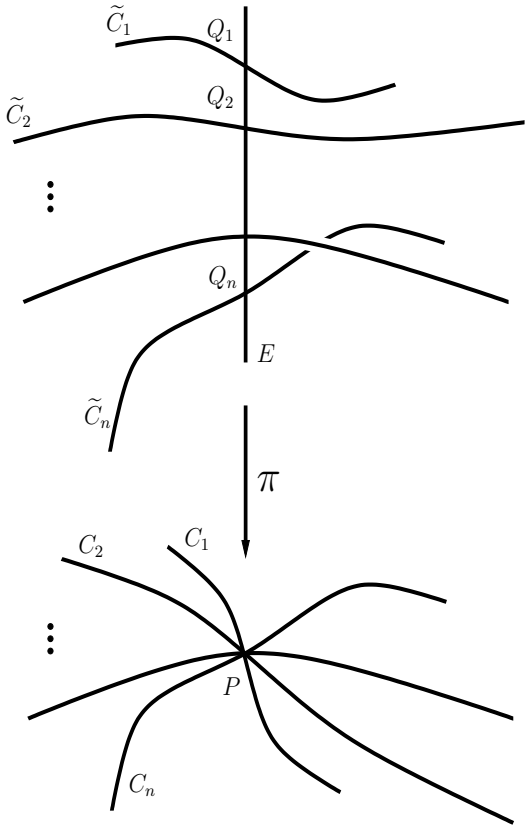


FIG. I.1 – Le cas $n \geq 2$ dans l'étape 1 de la preuve.

- Si $n \geq 2$, soit $\pi : \widetilde{S} \to S$ l'éclatement de S en P. Le diviseur exceptionnel est noté E, la transformée stricte d'une courbe C_i est notée $\widetilde{C}_i$. On rappelle que, par hypothèse les courbes C_i sont lisses en P et s'y croisent deux à deux transversalement. Donc, pour tout i, la courbe $\widetilde{C}_i$ intersecte E en un unique point que l'on appelle Q_i et les points $Q_1, \ldots, Q_n$ sont deux à deux distincts. La figure I.1 résume cette situation.
  La courbe E est projective et les $\widetilde{C}_i$ sont les seuls pôles de $\pi^*\omega$ qui intersectent E. Soit $i \in \{1, \ldots, n\}$, d'après le cas $n = 2$, on a

$$\mathrm{res}^2_{\widetilde{C}_i, Q_i}(\pi^*\omega) = -\mathrm{res}^2_{E, Q_i}(\pi^*\omega). \tag{I.7}$$

  Ainsi, en appliquant le lemme I.6.3 et la relation (I.7) ci-dessus, on en déduit que

$$\sum_{i=1}^{n} \mathrm{res}^2_{C_i, P}(\omega) = \sum_{i=1}^{n} \mathrm{res}^2_{\widetilde{C}_i, Q_i}(\pi^*\omega) = -\sum_{i=1}^{n} \mathrm{res}^2_{E, Q_i}(\pi^*\omega).$$

  Soit Q un point de E autre que $Q_1, \ldots, Q_n$, la courbe E est le seul pôle la 2-forme $\pi^*\omega$ au voisinage de ce point. Par conséquent, d'après le lemme I.6.1 le 2-résidu de $\pi^*\omega$ en Q le long de E est nul. En reprenant (I.7), on en déduit que

$$\sum_{i=1}^{n} \mathrm{res}^2_{C_i, P}(\omega) = -\sum_{i=1}^{n} \mathrm{res}^2_{E, Q_i}(\pi^*\omega) = -\sum_{Q \in E} \mathrm{res}^2_{E, Q}(\pi^*\omega)$$

  et cette somme est nulle d'après le théorème I.7.1.

Étape 2. Dans le cas général, les courbes $C_1, \ldots, C_n$ peuvent être singulières en P et la multiplicité d'intersection de deux d'entre elles peut être supérieure ou égale à 2. On réalise

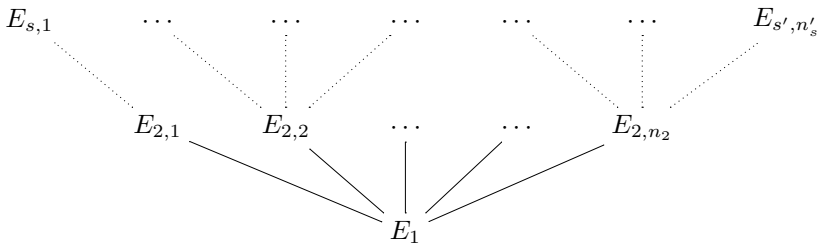
alors une désingularisation à **croisements normaux** de la courbe $C_1 \cup \ldots \cup C_n$. C'est-à-dire qu'à partir d'une séquence finie d'éclatements on obtient un morphisme birationnel $\pi : \widetilde{S} \to S$ tel que la surface $\widetilde{S}$ vérifie les propriétés suivantes.

(*i*) Les courbes $\widetilde{C}_1, \ldots, \widetilde{C}_n$ sont lisses en tout point Q tel que $\pi(Q) = P$.

(*ii*) Par un point Q tel que $\pi(Q) = P$ passe au plus une courbe $\widetilde{C}_i$.

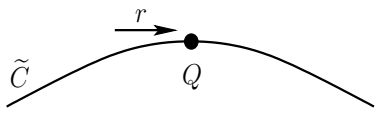
(*iii*) L'intersection d'une courbe $\widetilde{C}_i$ avec la courbe $\pi^{-1}(\{P\})$ est de multiplicité un.

On appelle arbre de résolution l'image réciproque par π du point P. Il s'agit d'une réunion de courbes projectives de genre nul. Les relations d'incidence entre ces diviseurs se représentent sous la forme d'un arbre que l'on notera $\mathcal{A}$.



Noter que les feuilles de cet arbre ne sont pas forcément toutes au même étage, même si le diagramme ci-dessus laisse supposer le contraire. C'est la raison pour laquelle les indices des deux feuilles (extrémités supérieures) représentées sont différents (s et s').

À présent, nous allons appliquer les résultats de l'étape précédente aux sommets l'arbre $\mathcal{A}$, en partant de ses feuilles et en remontant à sa racine. Dans ce qui suit, nous illustrerons notre travail de la façon suivante. Si $\widetilde{C}$ est un pôle de $\pi^*\omega$ et Q un point de $\widetilde{C}$, alors le 2-résidu r de $\pi^*\omega$ en Q le long de $\widetilde{C}$ apparaîtra dans un dessin sous la forme suivante.



Pour tout diviseur E correspondant à un sommet autre que la racine de l'arbre $\mathcal{A}$, on appelle T le point d'intersection de E avec son ascendant et $\mathcal{P}_E^j$ l'ensemble des points de $\widetilde{C}_j$ qui intersectent E ou un de ses ascendants dans l'arbre $\mathcal{A}$. On note

$$\sigma_E := \mathrm{res}^2_{E,T_E}(\pi^*\omega).$$

Commençons par montrer que pour tout diviseur E correspondant à un sommet de l'arbre autre que sa racine, on a

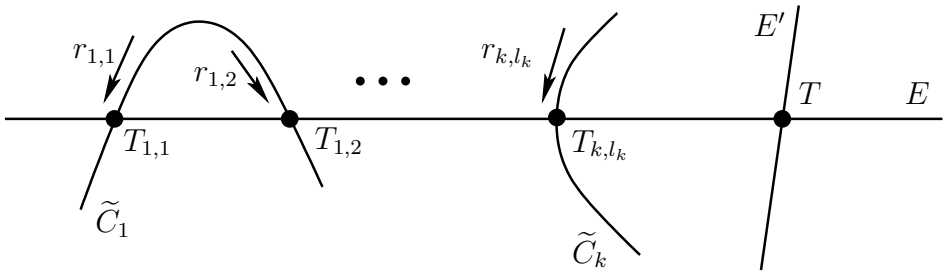
$$\sigma_E = \sum_{j=1}^{n} \sum_{Q \in \mathcal{P}_E^j} \mathrm{res}^2_{\widetilde{C}_j,Q}(\pi^*\omega). \tag{R}$$

Nous allons démontrer cette relation par récurrence sur les étages de l'arbre.

Étape 2.a. Soit E un diviseur correspondant à une feuille de l'arbre. Il admet un unique ascendant dans l'arbre que l'on note E' et qui intersecte E en un point T. Par ailleurs, quitte à réordonner les indices des courbes, ce diviseur E intersecte les courbes $\widetilde{C}_1, \ldots, \widetilde{C}_k$ en les points $T_{1,1}, \ldots, T_{1,l_1}, \ldots, T_{k,1}, \ldots, T_{k,l_k}$. On note enfin

$$r_{i,j} := \mathrm{res}^2_{\widetilde{C}_i,T_{i,j}}(\pi^*\omega).$$

La situation peut être représentée par la figure suivante.



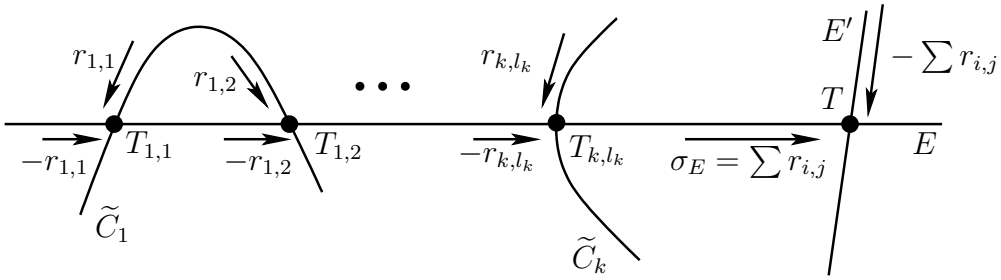
D'après le travail effectué dans l'étape 1, on sait que pour tout couple (i,j)

$$\mathrm{res}^2_{\widetilde{C}_i,T_{i,j}}(\pi^*\omega) = r_{i,j} = -\mathrm{res}^2_{E,T_{i,j}}(\pi^*\omega).$$

De plus, d'après le lemme I.6.1, la 2-forme $\pi^*\omega$ a des résidus non nuls seulement en les points $T_{i,j}$ et T. Donc, d'après la première formule des résidus (théorème I.7.1), on obtient

$$\sigma_E = \mathrm{res}^2_{E,T}(\pi^*\omega) = -\sum_{i,j} \mathrm{res}^2_{E,T_{i,j}}(\pi^*\omega) = \sum_{i,j} r_{i,j}.$$

C'est-à-dire la relation (R) pour une feuille de l'arbre $\mathcal{A}$. Le schéma suivant résume le travail qui vient d'être effectué.



Notons que, comme cela apparaît sur le dessin ci-dessus, en appliquant de nouveau le travail effectué dans l'étape 1, on obtient

$$\mathrm{res}^2_{E',T}(\pi^*\omega) = -\mathrm{res}^2_{E,T}(\pi^*\omega) = -\sum_{i,j} \mathrm{res}^2_{\widetilde{C}_i,T_{i,j}}(\pi^*\omega).$$

Étape 2.b. Soit E un diviseur correspondant à un sommet intermédiaire de l'arbre, c'est-à-dire un sommet qui n'est ni une feuille ni la racine. Par récurrence, supposons que la relation (R) est vérifiée par tous les descendants (directs ou indirects) de E dans $\mathcal{A}$. Notons E' l'ascendant direct de E dans $\mathcal{A}$ et $D_1,\dots,D_r$ ses descendants directs. Soient également $\widetilde{C}_1,\dots,\widetilde{C}_q$ les courbes[8] qui intersectent E. On désigne par T, le point d'intersection de E avec E'. Les points d'intersection de E avec $D_1,\dots,D_r$ sont notés $U_1,\dots,U_r$ et les points d'intersection de E avec $\widetilde{C}_1,\dots,\widetilde{C}_q$ sont notés $T_{1,1},\dots,T_{1,l_1},\dots,T_{q,1},\dots,T_{Q,l_q}$. On reprend la notation

$$r_{i,j} := \mathrm{res}^2_{\widetilde{C}_j,T_{i,j}}(\pi^*\omega).$$

D'après l'hypothèse de récurrence on a

$$\forall i \in \{1,\dots,r\}, \quad \mathrm{res}^2_{D_i,U_i}(\pi^*\omega) = \sigma_{D_i}.$$

Donc d'après le cas $n=2$ de l'étape 1, on a

$$\forall i \in \{1,\dots,r\}, \quad \mathrm{res}^2_{E,U_i}(\pi^*\omega) = -\sigma_{D_i}$$

[8] Quitte à ré indicer les courbes.

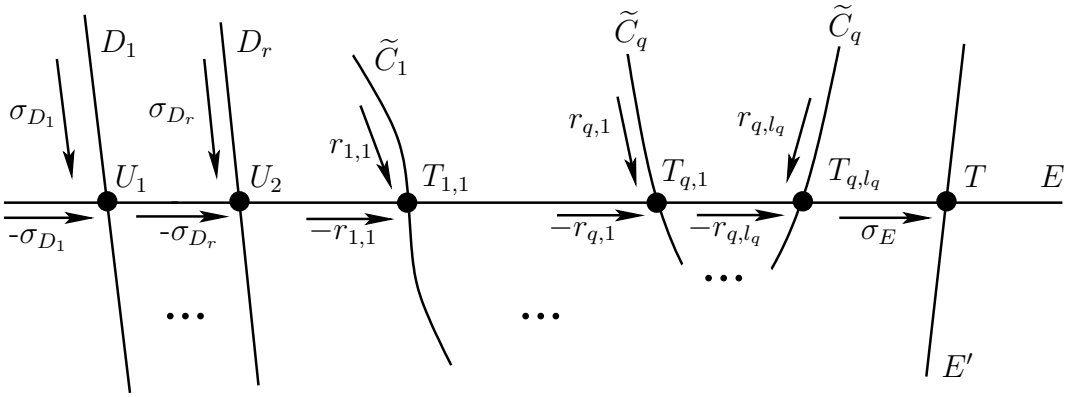
et

$$\forall j \in \{1, \dots, q\}, \forall i \in \{1, \dots, l_q\}, \quad \mathrm{res}^2_{E,T_{i,j}}(\pi^*\omega) = -r_{i,j}.$$

Ainsi, d'après le théorème I.7.1 appliqué à E et $\pi^*\omega$, on a

$$\sigma_E = \mathrm{res}^2_{E,T}(\pi^*\omega) = -\sum_{k=1}^{r} \mathrm{res}^2_{E,U_k}(\pi^*\omega) - \sum_{i,j} \mathrm{res}^2_{E,T_{i,j}}(\pi^*\omega) = \sum_{k=1}^{r} \sigma_{D_k} + \sum_{i,j} r_{i,j}$$

et cette dernière somme n'est autre que σ_E. La relation (R) est donc vérifiée par E. Le dessin suivant résume le travail effectué.



Étape 2.c. Considérons maintenant E_1 la racine de l'arbre $\mathcal{A}$. Ce dernier n'a pas d'ascendant. Reprenons les notations de l'étape précédente en ce qui concerne ses descendants directs et les courbes $\widetilde{C}_j$ qu'il intersecte. Par un raisonnement analogue à celui qui a été effectué dans l'étape précédente, en appliquant le théorème I.7.1 à E_1 et $\pi^*\omega$ on obtient

$$-\sum_{k=1}^{r} \sigma_{D_k} - \sum_{i,j} r_{i,j} = 0. \tag{I.8}$$

Or cette somme n'est autre que la somme

$$\sum_{i=1}^{n} \sum_{Q \in \mathcal{P}^i_{E_1}} \mathrm{res}^2_{\widetilde{C}_i,Q}(\pi^*\omega) = 0,$$

où l'on rappelle que $\mathcal{P}^i_{E_1}$ est l'ensemble des points de $\widetilde{C}_i$ qui intersecte E_1 ou l'un de ses antécédents. C'est donc l'ensemble des points des courbes $\widetilde{C}_i$ qui sont envoyés sur P par π. On conclut en rappelant que, d'après la définition I.6.6, on a

$$\sum_{Q \in \mathcal{P}^i_{E_1}} \mathrm{res}^2_{\widetilde{C}_i,Q}(\pi^*\omega) = \mathrm{res}^2_{C_i,P}(\omega).$$

En combinant cette relation avec l'équation (I.8) on obtient le résultat attendu, à savoir

$$\sum_{i=1}^{n} \mathrm{res}^2_{C_i,P}(\omega) = 0.$$

□

Remarque I.7.6. *Noter que, dans la démonstration du théorème I.7.4 qui précède, on n'a appliqué le théorème I.7.1 qu'à des diviseurs appartenant à l'image réciproque de P. Or, il a été signalé que la preuve du théorème I.7.1 est évidente si la valuation de ω le long de C est*

supérieure ou égale à -1. Aussi, il est important de signaler que, dans la preuve qui précède, la valuation de $\pi^*\omega$ le long d'un diviseur exceptionnel E provenant d'un éclatement peut être inférieure à -2. Le lemme suivant fournit une formule explicite de la valuation de $\pi^*\omega$ le long d'un tel diviseur exceptionnel.

Lemme I.7.7. *Soit ω une 2-forme rationnelle sur S et P un point de S. On note $\mathcal{C}_P$, l'ensemble de toutes les courbes irréductibles contenues dans S et contenant P. Soit $\pi : \widetilde{S} \to S$ l'éclatement de S en P, alors la valuation de $\pi^*\omega$ le long du diviseur exceptionnel E est donnée par la formule :*

$$val_E(\pi^*\omega) = 1 + \sum_{C \in \mathcal{C}_P} m_P(C) val_C(\omega),$$

où $m_P(C)$ est la multiplicité de C en P.

PREUVE. D'après [Har77] proposition V.3.3, on a l'égalité de diviseurs

$$(\pi^*\omega) = \pi^*(\omega) + E.$$

Ensuite, d'après [Har77] proposition V.3.6, la valuation du diviseur $\pi^*(\omega)$ le long de E est

$$\mathrm{val}_E(\pi^*(\omega)) = \sum_{C \in \mathcal{C}_P} m_P(C)\mathrm{val}_C(\omega).$$

□

Remarquons également que la théorème I.7.4 permet d'étendre le lemme I.6.1 au cas des courbes singulières voire même réductibles. C'est ce qui fera l'objet du corollaire I.7.9. Pour énoncer ce dernier, nous avons besoin de la convention et la définition ci-dessous.

Convention. Soit C une courbe quelconque plongée dans S et P un point de S n'appartenant pas à C, on dit alors que

$$\mathrm{res}^2_{C,P}(\omega) = 0.$$

Définition I.7.8 (2-résidu en un point d'une courbe réductible)**.** *Soit C une courbe réductible plongée dans S et $C_1, \ldots, C_d$ ses composantes irréductibles. Soit P un point de C et ω une 2-forme rationnelle sur S. On définit le 2-résidu de ω en P le long de C par*

$$res^2_{C,P}(\omega) := \sum_{i=1}^{d} res^2_{C_i,P}(\omega).$$

Corollaire I.7.9. *Soit C une courbe quelconque plongée dans S et P un point de C. Soit une 2-forme rationnelle ω dont le lieu des pôles au voisinage de P est contenu dans C, alors*

$$res^2_{C,P}(\omega) = 0.$$

PREUVE. On applique la deuxième formule des résidus (théorème I.7.4) à ω, ses pôles au voisinage de P faisant partie des composantes irréductibles de C. □

Pour finir ce chapitre, nous allons énoncer la troisième formule des résidus, qui est celle que nous appliquerons aux codes correcteurs dans le chapitre suivant. Noter que, dans le chapitre suivant nous manipulerons fréquemment des diviseurs. C'est ce qui motive la définition suivante.

Définition I.7.10 (2-Résidu en un point le long d'un diviseur)**.** *Soit D un diviseur sur S. Pour toute 2-forme rationnelle ω et tout point P de S, on appelle 2-résidu de ω en P le long de D et on notera $res^2_{D,P}(\omega)$ le 2-résidu de ω en P le long du **support** de D.*

Attention ! Noter qu'il ne s'agit pas exactement d'une extension de la définition par linéarité. D'une certaine façon, la définition I.7.10 ci-dessus autorise un abus de langage pour éviter d'avoir à parler de 2-*résidu en un point le long du support du diviseur* D. En particulier, il faut faire attention au fait que, selon cette définition, le résidu d'une 2-forme ω en un point P le long d'un diviseur D est par exemple égal à celui de ω en P le long du diviseur $2D$.

Théorème I.7.11 (Troisième formule des résidus, [Lip84] chap. 12)**.** *Soit S une surface projective lisse géométriquement intègre. Soient D_a et D_b deux diviseurs sur S dont l'intersection des supports est un ensemble fini Z. Soit $\Omega^2(-D_a - D_b)$ le faisceau de 2-formes vérifiant localement*

$$(\omega) \geq -D_a - D_b.$$

Alors, pour toute section globale ω du faisceau $\Omega^2(-D_a - D_b)$, on a

$$\sum_{P \in S} res^2_{D_a,P}(\omega) = \sum_{P \in Z} res^2_{D_a,P}(\omega) = 0.$$

PREUVE. La 2-forme ω n'a pas de pôles hors du support de $D_a + D_b$. Donc, d'après le corollaire I.7.9, les 2-résidus de ω le long de D_a sont nuls en tout point P n'appartenant pas à Z, ce qui nous donne la première égalité. La seconde égalité vient de la première formule des résidus (théorème I.7.1). En effet, soient $D_{a,1}, \ldots, D_{a,m_a}$ les composantes irréductibles du support de D_a. Le théorème I.7.1 entraîne

$$\forall i \in \{1, \ldots, m_a\}, \quad \sum_{P \in D_{a,i}} \mathrm{res}^2_{D_{a,i},P}(\omega) = 0.$$

De fait, en sommant ces m_a relations, on obtient

$$\sum_{P \in \mathrm{Supp} D_a} \mathrm{res}^2_{D_a,P}(\omega) = 0.$$

Et il revient au même de sommer sur tous les points de S puisque les 2-résidus de ω le long de D_a en un point hors du support de D_a sont nuls par convention. □

Remarque I.7.12. *Sous les conditions du théorème I.7.11, soit ω une section globale du faisceau $\Omega^2(-D_a - D_b)$. D'après la deuxième formule des résidus (thm I.7.4) on a*

$$\forall P \in S, \quad res^2_{D_a,P}(\omega) = -res^2_{D_b,P}(\omega).$$

Par conséquent l'énoncé du théorème I.7.11 est symétrique, c'est-à-dire qu'il reste vrai si l'on échange D_a et D_b.

Deuxième partie

Codes géométriques

Chapitre II

Codes différentiels sur une surface

"Je vous jure d'être décent et de ne pas dire un seul gros mot ni rien qui blesse les convenances."

Musset
Il ne faut jurer de rien

Dans ce chapitre, nous allons appliquer les résultats du chapitre I. Le but est de construire des codes correcteurs d'erreurs en évaluant les 2-résidus de 2-formes différentielles en des points rationnels d'une surface algébrique.

II.1 Langage et Notations

Soit X une variété géométriquement intègre de dimension n définie sur un corps k. On note $\mathcal{O}_X$ son faisceau structural. L'ensemble des diviseurs de Weil sur X sera noté $\mathrm{Div}_k(X)$. Étant donné un diviseur D sur S on note respectivement D^+ et D^- ses parties effectives et non effectives. Les diviseurs D^+ et D^- sont tous deux effectifs et D s'écrit

$$D = D^+ - D^-.$$

L'équivalence linéaire sera notée "$\sim$". Si X est lisse, le groupe $\mathrm{Div}_k(X)/\sim$ s'identifie au groupe de Picard de X que l'on notera $\mathrm{Pic}_k(X)$. Si X est une surface lisse et que les supports de deux diviseurs D et D' n'ont pas de composante irréductible commune, leur multiplicité d'intersection en un point P est notée $m_P(D, D')$. Étant donné un diviseur G sur X, on note $\mathcal{L}(G)$ (resp. $\Omega^n(G)$) le faisceau inversible des fonctions rationnelles (resp. des n-formes rationnelles) sur X qui vérifient localement

$$(f) \geq -G \quad (\text{resp. } (\omega) \geq G).$$

L'ensemble des sections globales d'un faisceau $\mathcal{F}$ sera noté $\Gamma(X, \mathcal{F})$ et $\mathcal{F}_P$ désignera sa fibre en un point P. En ce qui concerne les faisceaux $\mathcal{L}(G)$ (qui seront fréquemment utilisés), on utilisera la notation standard $L(G)$ pour $\Gamma(X, \mathcal{L}(G))$. Noter que, dans la littérature, le symbole $\Omega^n(G)$ peut désigner un faisceau inversible ou l'espace des sections globales du faisceau en question. Insistons donc sur le fait que, dans ce qui suit $\Omega^n(G)$ désignera toujours un faisceau de n-formes.

Pour finir, soit $\bar{k}$ la clôture algébrique de k, on note $\overline{X}$ la variété

$$\overline{X} := X \times_k \bar{k}$$

et, étant donné un faisceau $\mathcal{F}$ sur X, on note $\overline{\mathcal{F}}$ le tiré en arrière de $\mathcal{F}$ sur $\overline{X}$.

Important. Dans tout ce qui suit, sauf mention contraire, si D_1 et D_2 sont deux diviseurs sur une surface lisse S dont les supports n'ont pas de composante irréductible commune, alors "$D_a \cap D_b$" signifiera **intersection au sens de la théorie des schémas**. Il s'agit donc d'une intersection tenant compte des multiplicités et non d'une intersection ensembliste.

II.2 Rappels sur les codes construits à partir de courbes

Dans cette section, X désigne une courbe algébrique projective lisse au-dessus de $\mathbf{F}_q$. On se donne également un diviseur $\mathbf{F}_q$-rationnel G sur X et une famille de points $P_1, \ldots, P_n$ rationnels sur X et qui évitent le support de G. On note D le diviseur

$$D := P_1 + \cdots + P_n.$$

II.2.1 Codes fonctionnels et différentiels

La donnée des diviseurs G et D permet de construire deux codes différents. Ces codes sont respectivement appelés *codes fonctionnels* et *codes différentiels*. Les premiers sont construits par évaluation de fonctions en des points rationnels de X et les seconds par évaluation de résidus de formes différentielles en ces mêmes points.

Le code fonctionnel. Soit ev_D l'application,

$$\mathrm{ev}_D : \left\{ \begin{array}{ccc} L(G) & \to & \mathbf{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array} \right.$$

L'image de cette application est appelée code fonctionnel associé aux diviseurs D et G et notée $C_{L,X}(D, G)$.

Le code différentiel. Soit res_D l'application,

$$\mathrm{res}_D : \left\{ \begin{array}{ccc} \Gamma(X, \Omega^1(G - D)) & \to & \mathbf{F}_q^n \\ \omega & \mapsto & (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)). \end{array} \right.$$

L'image de cette application est appelée code différentiel associé aux diviseurs D et G et notée $C_{\Omega,X}(D, G)$.

Exemple II.2.1. Supposons que X soit la droite projective $\mathbf{P}^1_{\mathbf{F}_q}$ et que le diviseur G soit de la forme kP où P est un point rationnel de $\mathbf{P}^1_{\mathbf{F}_q}$. Alors, en prenant pour D une somme de points rationnels autres que P, le code fonctionnel est un code de Reed-Solomon et le code différentiel un code de Goppa classique (cf [HP95] exemples 3.3 et 3.4).

II.2.2 Paramètres de ces codes

L'un des intérêts de ces codes est que l'on dispose d'outils simples provenant de la théorie des courbes algébriques pour en évaluer les paramètres.

- Le théorème de Riemann-Roch permet de minorer, voire d'évaluer exactement la dimension de ces codes.
- Le fait que le degré d'un diviseur principal soit nul permet d'obtenir de façon élémentaire une borne inférieure pour la distance minimale d'un code fonctionnel. Un raisonnement analogue sur le degré d'un diviseur canonique fournit une méthode de minoration de la distance minimale d'un code différentiel. Nous renvoyons le lecteur aux références [Ste99], [Sti93] et[TV91] pour plus de détails sur ces propriétés (la liste n'est bien sûr pas exhaustive).

Concernant la distance minimale $d_{\min}$, on obtient pour les codes fonctionnels la minoration

$$n - k + 1 - g \leq d_{\min},$$

où k désigne la dimension du code et g le genre de la genre de la courbe. Ainsi on sait que ces codes sont toujours *à g de la borne de singleton*. C'est l'une des raisons qui a motivé les nombreux travaux effectués autour de l'étude des codes géométriques durant les 25 dernières années.

II.2.3 Relation d'orthogonalité et décodage

Un autre intérêt de ces codes est que l'on dispose d'une relation d'orthogonalité entre le code fonctionnel et le code différentiel, à savoir

$$C_{\Omega,X}(D,G) = C_{L,X}(D,G)^{\perp}.$$

La preuve de cette relation est une conséquence de la formule des résidus pour l'inclusion $\subseteq$ et du théorème de Riemann-Roch qui fournit une égalité de dimension entre ces codes entraînant l'inclusion réciproque. Nous renvoyons le lecteur à [TV91] théorème 3.1.44 ou [Sti93] théorème II.2.8 pour plus de détails sur ce résultat.

Noter que, cette relation d'orthogonalité est l'outil de base de la majorité des algorithmes de décodage (voir [HP95] ou [HVP98]).

II.2.4 Deux constructions distinctes mais une seule classe de codes

Un dernier résultat bien connu concernant ces codes est que tout code différentiel est un code fonctionnel associé à d'autres diviseurs et réciproquement. Plus précisément, étant donnés deux diviseurs D et G comme précédemment, il existe un diviseur canonique K tel que

$$C_{\Omega,X}(D,G) = C_{L,X}(D, K - G + D).$$

Le diviseur K est celui d'une forme différentielle dont les résidus en les points du support de D sont tous égaux à 1. L'existence d'un tel diviseur est une conséquence du théorème d'approximation faible dans les corps de fonctions ([Sti93] théorème I.3.1).

Aussi, si l'on souhaite étudier ces codes, on peut sans perte de généralité se restreindre à l'étude de codes issus d'une seule des deux constructions. Généralement, on se focalise sur les codes fonctionnels dont la construction semble plus accessible, les fonctions étant un objet plus intuitif que les formes différentielles.

Remarque II.2.2. *Il est toutefois intéressant de noter que la première construction de codes géométriques fut donnée par V.D. Goppa en 1981 dans l'article [Gop81]. Dans cet article, les codes introduits sont des codes différentiels. Sans doute parce qu'il sont une généralisation des codes de Goppa classiques.*

II.3 Codes géométriques construits à partir de surfaces algébriques

Si de telles constructions sont possibles sur les courbes, il est naturel de s'interroger sur les perspectives d'extension de ces constructions à des variétés de dimension supérieure.

II.3.1 Cadre

Dans ce qui suit et jusqu'à la fin de ce chapitre, S désignera une surface algébrique projective lisse définie au-dessus d'un corps fini $\mathbf{F}_q$. Sauf mention contraire, lorsque l'on parlera de courbe pongée dans S, il s'agira de courbe définie sur $\mathbf{F}_q$. On se donne également

un diviseur $\mathbf{F}_q$-rationnel G sur S et une famille de points rationnels $P_1, \ldots, P_n$ de S qui évitent le support de G. On appelle Δ le 0-cycle sur S défini par

$$\Delta := P_1 + \cdots + P_n.$$

Notons que Δ joue plus ou moins le rôle du diviseur D de la section précédente. Nous avons cependant choisi de le noter avec une lettre grecque car ce n'est plus un diviseur mais un 0-cycle. D'une façon générale, dans tout ce qui suit, les lettres latines majuscules désigneront des diviseurs et les lettres grecques majuscules des 0-cycles. Enfin, signalons dès à présent que la différence de dimension entre Δ et G sera à l'origine de la plupart des difficultés que posent la construction et l'étude des codes différentiels sur des surfaces.

II.3.2 Codes fonctionnels

Comme nous l'avons dit précédemment, la construction fonctionnelle présentée dans le cas des courbes se généralise à des variétés de dimension quelconque (voir [VM84] I.3.1). Pour ce faire, on définit l'application

$$\mathrm{ev}_\Delta : \left\{ \begin{array}{ccc} L(G) & \to & \mathbf{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array} \right.$$

L'image de cette application est appelée code fonctionnel sur S associé à Δ et G et est notée $C_{L,S}(\Delta, G)$. L'étude des paramètres de ce type de code est nettement plus ardue que dans le cas des courbes.

Sur la longueur du code. Si l'on veut étudier l'asymptotique des codes construits sur des surfaces algébriques, on doit disposer de moyens d'évaluer le nombre de points rationnels d'une surface sur un corps fini. La borne de Weil-Deligne (voir [Del74]) valable pour des variétés de dimension quelconque permet de majorer ce nombre de points. Lachaud et Tsfasman ont donné des estimations plus précises de ce nombre de points via des formules explicites dans [LT97].

Sur la dimension. En dimension supérieure ou égale à 2, le théorème de Riemann-Roch se complique. Aussi, l'évaluation de la dimension de ce type de code est en général plus ardue. Cependant, dans les exemples étudiés dans la littérature, le diviseur G est presque toujours un diviseur très ample obtenu par intersection de S avec une hypersurface. Dans ce cas, l'évaluation de la dimension du code se ramène au calcul élémentaire de la dimension d'espaces de polynômes en plusieurs variables et de degré total borné.

Sur la distance minimale. Alors que l'on disposait facilement de la distance minimale construite de Goppa (*designed minimal distance*) dans le cas des courbes (voir [Sti93] def II.2.4), dans le cas des variétés de dimension supérieure, la minoration de la distance minimale d'un code fonctionnel devient un problème infiniment plus complexe. Elle revient à majorer le nombre maximal de points rationnels du lieu d'annulation d'un élément de $L(G)$. Les références citées dans l'introduction (page 14) portent principalement sur la résolution de ce problème lorsque S appartient à une classe spécifique de surfaces.

Remarque II.3.1. *Notons que Lachaud propose dans [Lac88] une construction sensiblement différente du code fonctionnel. Cette approche a été reprise par un certain nombre des auteurs précédemment cités tels que Aubry, Edoukou et Sørensen. L'annexe D est consacrée à cette autre construction et au moyen de la relier à celle présentée ci-dessus.*

Passons maintenant à une première approche de la construction de codes différentiels sur une surface.

II.3.3 Codes différentiels

Pour réaliser une construction analogue à celle qui a été présentée en section II.2.1, il faut plus que la donnée de G et Δ. En effet, on souhaiterait évaluer les 2-résidus de 2-formes ayant des pôles prescrits. Il faut donc introduire un nouveau diviseur que l'on notera D et qui, d'une certaine manière, jouera le rôle[1] du diviseur du même nom dans la construction de codes différentiels sur une courbe. Il faut également que l'on évalue les 2-résidus le long de certains pôles de ω mais pas tous. En effet, d'après le théorème I.7.4 si l'on évalue le 2-résidu de ω en un point le long de tous ses pôles, on obtient zéro. Il faut donc décomposer le diviseur D en deux parties distinctes. C'est ce qui motive la définition suivante.

Définition II.3.2. *Soient D_a et D_b deux diviseurs sur S dont les supports n'ont pas de composante irréductible commune et soit D la somme de ces deux diviseurs. On définit l'application*

$$res^2_{D_a,\Delta} : \left\{ \begin{array}{ccc} \Gamma(S,\Omega^2(G-D)) & \rightarrow & \mathbf{F}_q^n \\ \omega & \mapsto & (res^2_{D_a,P_1}(\omega),\ldots,res^2_{D_a,P_n}(\omega)). \end{array} \right.$$

L'image de cette application est appelée code différentiel associé à Δ, D_a, D_b et G. On le note $C_{\Omega,S}(\Delta,D_a,D_b,G)$.

Remarque II.3.3. *On peut également construire une application $res^2_{D_b,\Delta}$ en échangeant D_a et D_b dans l'énoncé de la définition II.3.2. Le théorème I.7.4 entraîne*

$$res^2_{D_a,\Delta} = -res^2_{D_b,\Delta}.$$

De ce fait, les applications sont différentes mais ont même image. La construction du code ne dépend donc pas de l'ordre des éléments dans le couple (D_a,D_b).

Remarque II.3.4. *L'application $res^2_{D_a,\Delta}$ peut en fait être définie sur $\Omega^2_{\mathbf{F}_q(S)/\mathbf{F}_q}$ tout entier. Aussi, on s'autorisera à l'appliquer à des 2-formes quelconques de $\Omega^2_{\mathbf{F}_q(S)/\mathbf{F}_q}$ voire de $\Omega^2_{\overline{\mathbf{F}}_q(\overline{S})/\overline{\mathbf{F}}_q}$. Cet abus de notation sera par exemple utilisé dans la définition II.3.5.*

La définition II.3.2 n'est pas complètement satisfaisante, car il n'y a pas de lien entre le couple (D_a,D_b) et Δ. De fait, il se peut par exemple que les supports de D_a et D_b ne se croisent en aucun point du support de Δ, ce qui, d'après le corollaire I.7.9, donnerait un code nul. Nous allons donc introduire une nouvelle notion permettant de relier un 0-cycle sur S à une paire de diviseurs. Notons que cette définition (définition II.3.5) pourra sembler inutilement compliquée au premier abord. Cependant, les commentaires en section II.3.6 justifieront à posteriori la pertinence de ce choix.

II.3.4 Paires de diviseurs Δ-convenables

Commençons par se donner un cahier des charges. On souhaite disposer des propriétés suivantes.

(*a*) On aimerait que les codes différentiels construits à partir de Δ, G et du couple (D_a,D_b) n'aient pas une coordonnée systématiquement nulle. On souhaiterait donc que pour tout point P appartenant au support de Δ, il existe une section de $\Omega^2(G-D)$ qui n'annule pas l'application $\mathrm{res}^2_{D_a,P}$.

(*b*) Notre but est également d'obtenir une relation d'orthogonalité entre les codes $C_{L,S}(\Delta,G)$ et $C_{\Omega,S}(\Delta,D_a,D_b,G)$. Pour ce faire, nous allons utiliser la troisième formule des résidus (théorème I.7.11) et adopter une démarche proche de celle qui est utilisée dans le cas des courbes.

[1] On a signalé en section II.3.1 que Δ jouait le rôle du diviseur D dans le cas des courbes. En réalité, dans le cas des codes différentiels sur des surfaces deux objets de dimension différente endossent le rôle joué par le diviseur D dans le cas des courbes. Il y a d'un côté le 0-cycle Δ et d'un autre la paire de diviseurs (D_a,D_b).

La définition suivante répond à ce cahier des charges.

Définition II.3.5. *Soient D_a et D_b deux diviseurs sur S dont les supports n'ont pas de composante irréductible commune et soit D le diviseur $D := D_a + D_b$. La paire (D_a, D_b) est dite Δ-convenable si elle vérifie les conditions suivantes.*

(i) Pour tout point P de $\overline{S}$, l'application $res^2_{D_a,P} : \overline{\Omega^2(-D)}_P \to \overline{\mathbf{F}}_q$ est $\mathcal{O}_{\overline{S},P}$-linéaire. On rappelle que $\overline{\Omega^2(-D)}_P$ désigne la fibre en P du tiré en arrière sur $\overline{S}$ du faisceau $\Omega^2(-D)$

(ii) L'application $res^2_{D_a,P}$ définie ci-dessus est surjective pour tout point P appartenant au support de Δ et nulle pour tout autre point de $\overline{S}$.

Attention. Même si les propriétés requises dans la définition II.3.5 sont d'ordre géométriques, c'est-à-dire qu'elles concernent $\overline{S}$, les diviseurs D_a et D_b sont **rationnels**, c'est-à-dire définis sur $\mathbf{F}_q$.

Remarque II.3.6. *La structure de $\mathcal{O}_{\overline{S},P}$-module de $\overline{\mathbf{F}}_q$ est induite par l'application d'évaluation $f \to f(P)$. Aussi, la condition (i) signifie que pour toute fonction f régulière au voisinage de P et tout germe de 2-forme ω appartenant à $\overline{\Omega^2(-D)}_P$, on a*

$$res^2_{D_a,P}(f\omega) = f(P) res^2_{D_a,P}(\omega).$$

Notons également que si (D_a, D_b) vérifie (i), alors l'application $res^2_{D_a,P}$ s'annule sur $\mathfrak{m}_{\overline{S},P}\overline{\Omega^2(-D)}_P$.

Remarque II.3.7. *Par un raisonnement analogue à celui qui est utilisé dans la remarque II.3.3, on montre aisément que si (D_a, D_b) est Δ-convenable, alors l'application $res^2_{D_b,\Delta}$ vérifie les mêmes propriétés de $\mathcal{O}_{\overline{S}}$-linéarité que $res^2_{D_a,\Delta}$. Par conséquent la notion de Δ-convenance est symétrique.*

$$(D_a, D_b) \text{ est } \Delta\text{-convenable} \iff (D_b, D_a) \text{ est } \Delta\text{-convenable.}$$

Nous allons maintenant donner une critère de Δ-convenance faisant intervenir des propriétés d'intersection entre les composantes des diviseurs D_a et D_b.

Proposition II.3.8 (Critère de Δ-convenance)**.** *Soit (D_a, D_b) une paire de diviseurs dont les supports n'ont pas de composante irréductible commune et soit D la somme de ces deux diviseurs. Si D_a et D_b vérifient les conditions suivantes, alors la paire (D_a, D_b) est Δ-convenable.*

(1) Pour tout P appartenant au support de Δ, il existe une courbe irréductible C définie sur $\mathbf{F}_q$, lisse en P telle que, sur un voisinage U de P on ait

$$D_{a|U}^{+} = C \cap U \quad ou \quad D_{b|U}^{+} = C \cap U \quad et \quad m_P(C, D - C) = 1.$$

(2) Pour tout point géométrique P de $\overline{S}$ n'appartenant pas au support de Δ, alors l'un des diviseurs $D_* = D_a$ ou $D_* = D_b$ vérifie les conditions suivantes. Pour toute composante $\overline{\mathbf{F}}_q$-irréductible $\overline{C}$ de D_*^+ contenant P, on a :

(a) la courbe $\overline{C}$ est lisse en P ;

(b) la courbe $\overline{C}$ apparaît dans la décomposition de D_* en combinaison $\mathbf{Z}$-linéaire de composantes $\overline{\mathbf{F}}_q$-irréductibles avec le coefficient 1 ;

(c) $m_P(\overline{C}, D - \overline{C}) \leq 0$.

Remarque II.3.9. *Ce critère, quoique technique présente un avantage majeur, il permet de construire des paires de diviseurs Δ-convenables. La preuve de la proposition II.4.7 fournit un algorithme de construction d'une paire Δ-convenable étant donné un 0-cycle Δ (voir aussi remarque II.4.8).*

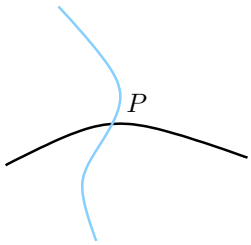
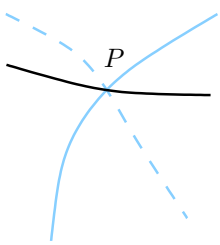
Avant de fournir une démonstration de cette proposition, nous allons faire quelques remarques. Nous donnerons ensuite quelques illustrations pour tenter de se développer une intuition des conditions exigées par le critère.

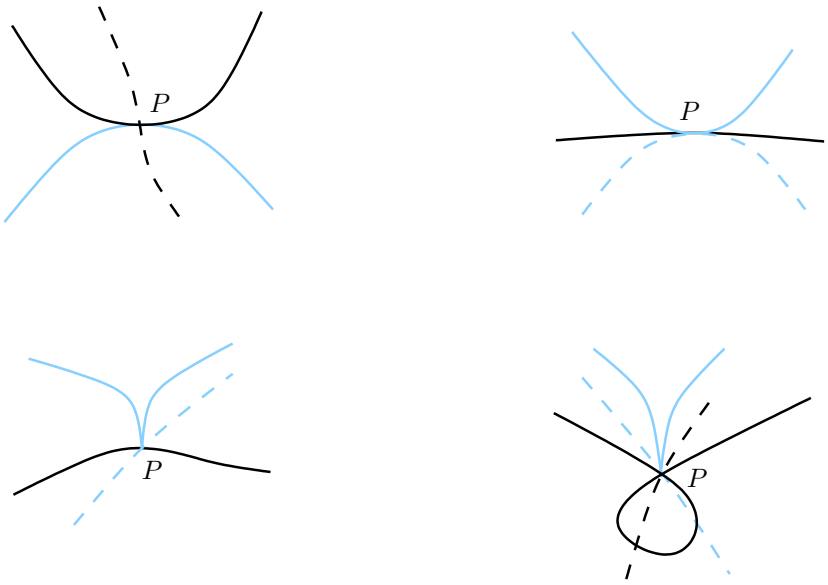
Remarque II.3.10. *Dans la condition (2) de la proposition II.3.8, le fait que D_* soit D_a ou D_b dépend du point P. En d'autres termes, en chaque point P de $\overline{S}$ évitant le support de Δ, les conditions (2a), (2b) et (2c) doivent être vérifiées soit par D_a, soit par D_b. Par ailleurs, le diviseur D_* peut-être nul au voisinage de P (c'est d'ailleurs ce qui arrive en presque tout point de $\overline{S}$). Dans ce cas, les conditions (2a), (2b) et (2c) sont trivialement vérifiées. De fait, si au voisinage d'un point P de $\overline{S}$, l'un des diviseurs D_a ou D_b est nul, c'est celui que l'on choisit pour jouer le rôle de D_*. Cela permet de se ramener à un nombre fini de vérifications.*

Dans tout ce qui suivra nous utiliserons le code de couleurs suivant.

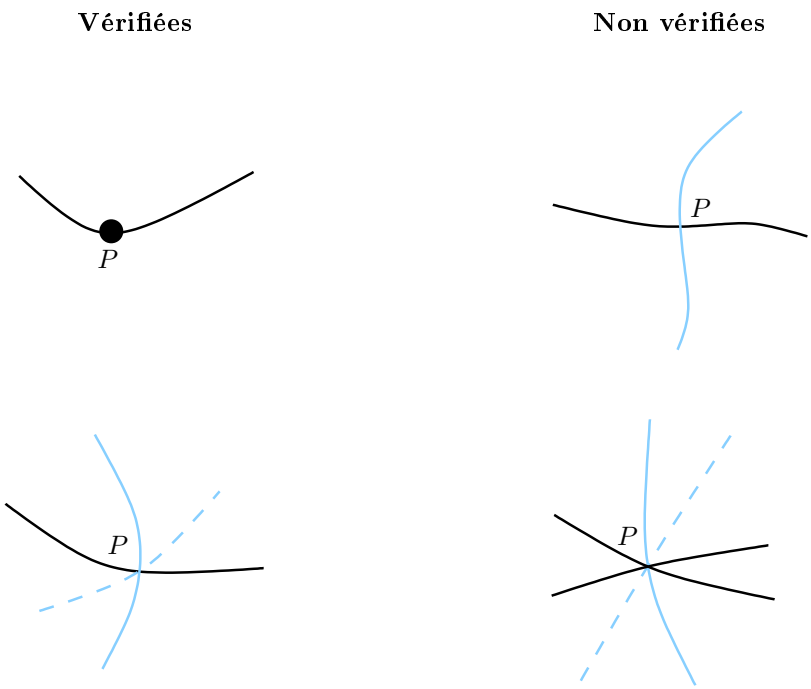
Nous allons illustrer les conditions du critère. Pour ce faire, nous allons représenter des situations dans lesquelles ces situations sont vérifiées et d'autres dans lesquelles elles ne le sont pas. Ces conditions sont locales. Nous allons donc présenter deux séries de figures. La première série correspond au voisinage d'un point du support de Δ et la seconde au voisinage d'un point géométrique de S non contenu dans le support de Δ.

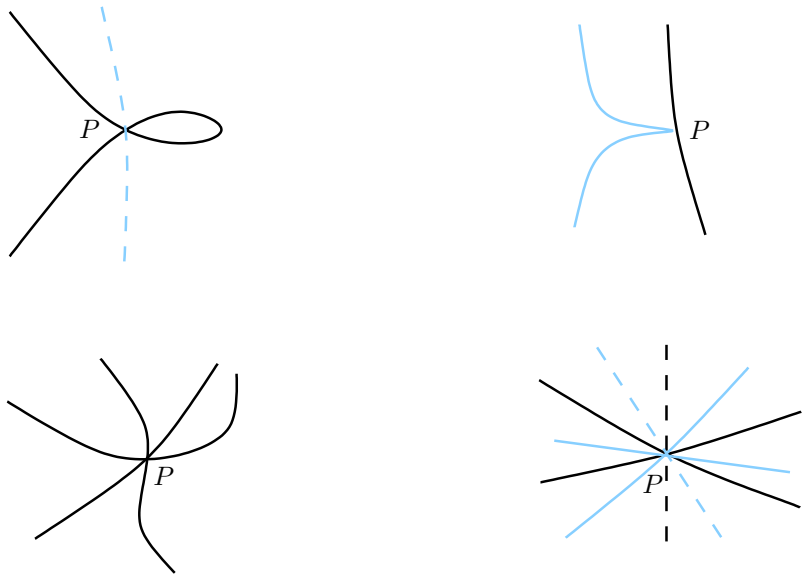
En un point P du support de Δ. Dans le tableau qui suit, les figures de la colonne de gauche représentent des situations où la condition (1) du critère est vérifiée. Dans ce tableau ainsi que dans celui qui suit, on suppose que les courbes représentées apparaissent dans l'expression de D_a (resp. de D_b) avec coefficient 1.

Vérifiées	**Non vérifiées**
	



En un point P n'appartenant pas au support de Δ. Les figures de la colonne de gauche représentent des situations ou les conditions (2a), (2b) et (2c) sont vérifiées. Dans la colonne de droite elle ne le sont pas.





Remarque II.3.11. *Le dernier exemple de la colonne de gauche peut surprendre. Pour le comprendre, on pourra se référer à la remarque II.3.10.*

La démonstration de la proposition II.3.8 nécessite le lemme et le corollaire qui suivent.

Lemme II.3.12. *Soient $\overline{C}$ une courbe $\overline{\mathbf{F}}_q$-irréductible plongée dans $\overline{S}$ et P un point lisse de $\overline{C}$. Soit ω une 2-forme sur $\overline{S}$ admettant un pôle simple le long de $\overline{C}$. Alors, le 1-résidu de ω le long de $\overline{C}$ vérifie*

$$val_P(res^1_{\overline{C}}(\omega)) = m_P(\overline{C}, (\omega) + \overline{C}).$$

Remarque II.3.13. *On déduit de ce lemme que le diviseur $(res^1_{\overline{C}}(\omega))$ sur $\overline{C}$ est égal à $i^*((\omega) + \overline{C})$, où i désigne l'injection naturelle $i : \overline{C} \hookrightarrow \overline{S}$. Cette relation est utilisée par Serre dans [Ser59] IV.8 lemme 2, pour démontrer la formule d'adjonction.*

Preuve du lemme II.3.12. Soient φ, ψ et v des équations locales respectives des diviseurs $\left((\omega) + \overline{C}\right)^+$, $\left((\omega) + \overline{C}\right)^-$ et $\overline{C}$ au voisinage de P. Soit u un élément de $\overline{\mathbf{F}}_q(\overline{S})$ tel que (u, v) soit une $(P, \overline{C})$-paire forte. Il existe une fonction h sur $\overline{S}$ régulière et inversible au voisinage de P telle que

$$\omega = h\frac{\varphi}{\psi} du \wedge \frac{dv}{v}.$$

Le 1-résidu de ω le long de $\overline{C}$ est $\bar{h}\bar{\varphi}\bar{\psi}^{-1}d\bar{u}$ et $\bar{h}$ est une fonction sur $\overline{C}$ régulière et inversible au voisinage de P. Par conséquent la valuation en P de $\bar{h}d\bar{u}$ est nulle et

$$\mathrm{val}_P(\mathrm{res}^1_{\overline{C}}(\omega)) = \mathrm{val}_P(\bar{\varphi}) - \mathrm{val}_P(\bar{\psi}).$$

De plus,

$$m_P(\overline{C}, (\omega) + \overline{C}) = m_P(\overline{C}, ((\omega) + \overline{C})^+) - m_P(\overline{C}, ((\omega) + \overline{C})^-). \tag{II.1}$$

On utilise ensuite la définition de la multiplicité d'intersection,

$$m_P(\overline{C}, ((\omega) + \overline{C})^+) = \dim_{\overline{\mathbf{F}}_q} \mathcal{O}_{\overline{S},P}/(\varphi, v) = \dim_{\overline{\mathbf{F}}_q} \mathcal{O}_{\overline{C},P}/(\bar{\varphi}) = \mathrm{val}_P(\bar{\varphi}). \tag{II.2}$$

De même,

$$m_P(\overline{C}, ((\omega) + \overline{C})^-) = \mathrm{val}_P(\bar{\psi}). \tag{II.3}$$

En injectant les résultats de (II.2) et (II.3) dans l'expression (II.1), on obtient le résultat recherché. □

Corollaire II.3.14. *Soient $\overline{C}$ une courbe $\overline{\mathbf{F}}_q$-irréductible plongée dans $\overline{S}$ et P un point lisse de C. Soit ω une 2-forme sur $\overline{S}$ telle que*

$$val_{\overline{C}}(\omega) \geq -1 \quad et \quad m_P(\overline{C}, (\omega) + \overline{C}) \geq -1.$$

Alors, pour toute fonction rationnelle f sur $\overline{S}$ régulière au voisinage de P, on a

$$res^2_{\overline{C},P}(f\omega) = f(P) res^2_{\overline{C},P}(\omega).$$

PREUVE. Soient (u, v) une $(P, \overline{C})$-paire forte et f une fonction rationnelle sur $\overline{S}$ régulière au voisinage de P. Il existe une fonction rationnelle ψ sur $\overline{S}$ régulière au voisinage de $\overline{C}$ telle que

$$\omega = \psi du \wedge \frac{dv}{v}.$$

Posons

$$\mu := \mathrm{res}^1_{\overline{C}}(\omega) = \bar{\psi} d\bar{u}.$$

Comme ω est de valuation supérieure à -1 et f de valuation positive le long de $\overline{C}$, on a

$$\mathrm{res}^1_{\overline{C}}(f\omega) = \bar{f}\mu.$$

D'après le lemme II.3.12, la valuation de μ en P est supérieure ou égale à -1, donc

$$\mathrm{res}_P(\bar{f}\mu) = \bar{f}(P)\mathrm{res}_P(\mu) \quad \Longrightarrow \quad \mathrm{res}^2_{\overline{C},P}(f\omega) = f(P)\mathrm{res}^2_{\overline{C},P}(\omega).$$

□

PREUVE DE LA PROPOSITION II.3.8. Soit (D_a, D_b) une paire de diviseurs vérifiant le critère, c'est-à-dire les conditions (1), (2a), (2b) et (2c) de la proposition II.3.8. Montrons qu'elle vérifie alors les conditions (i) et (ii) de la définition de Δ-convenance.

Condition (i)**.** Soient P un point appartenant au support de Δ et ω un germe de 2-forme appartenant à $\overline{\Omega^2(-D)}_P$. D'après la condition (1), il existe une courbe irréductible C qui est égale à D_a^+ ou D_b^+ au voisinage de P. D'après la remarque II.3.7, on peut supposer sans perte de généralité que C est égale à D_a^+ au voisinage de P. De fait,

$$\mathrm{res}^2_{D_a,P}(\omega) = \mathrm{res}^2_{C,P}(\omega).$$

De plus, la multiplicité d'intersection en P de C et D_b est inférieure à 1 donc

$$m_P(C, (\omega) + C) \geq -1.$$

Ainsi, comme la 2-forme ω est de valuation supérieure ou égale à -1 le long de C, d'après le corollaire II.3.14, l'application $\mathrm{res}^2_{C,P}$ (donc $\mathrm{res}^2_{D_a,P}$) restreinte à $\overline{\Omega^2(-D)}_P$ est $\mathcal{O}_{\overline{S},P}$-linéaire.

Condition (ii)**.** Soit P un point de $\overline{S}$ hors du support de Δ. Encore d'après la remarque II.3.7, on peut supposer que le D_a est le diviseur D_* de la condition (2) de la proposition II.3.8. Par conséquent, toute composante $\overline{\mathbf{F}}_q$-irréductible $\overline{C}$ du support de D_a^+ contenant P est lisse en ce point, apparaît dans D_a avec le coefficient 1 et vérifie

$$m_P(\overline{C}, D - \overline{C}) \leq 0. \tag{II.4}$$

Soient $\overline{C}$ une telle composante et ω un germe de 2-forme appartenant à $\overline{\Omega^2(-D)}_P$. D'après la condition (2b), ω est de valuation supérieure ou égale à -1 le long de $\overline{C}$. D'après le lemme II.3.12, l'inégalité (II.4) entraîne que le 1-résidu $\mathrm{res}^1_{\overline{C}}(\omega)$ de ω le long de $\overline{C}$ est de valuation positive en P. De fait, le 2-résidu de ω en P le long de $\overline{C}$ est nul. Cette assertion est valable pour toute composante $\overline{\mathbf{F}}_q$-irréductible de D_a^+ au voisinage de P, d'après la définition I.7.10, on en déduit que

$$\mathrm{res}^2_{D_a,P}(\omega) = 0.$$

□

II.3.5 Exemples de diviseurs Δ-convenables.

Le plan projectif

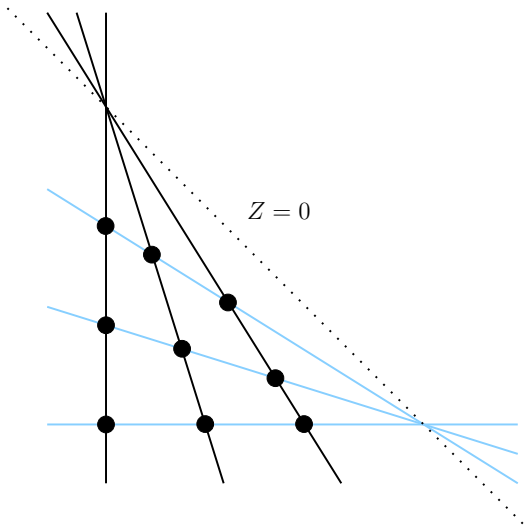
Si S est le plan projectif $\mathbf{P}^2_{\mathbf{F}_q}$ et X, Y, Z des coordonnées homogènes sur S. Soient U la carte affine $U := \{Z \neq 0\}$ et Δ la somme formelle de tous rationnels de U. Pour tout élément α appartenant à $\mathbf{F}_q$, on définit les droites

$$L_{a,\alpha} := \{X = \alpha\} \quad \text{et} \quad L_{b,\alpha} := \{Y = \alpha\},$$

puis les diviseurs

$$D_a := \sum_{\alpha \in \mathbf{F}_q} L_{a,\alpha} \quad \text{et} \quad D_b := \sum_{\alpha \in \mathbf{F}_q} L_{b,\alpha}.$$

La figure suivante représente cette paire de diviseurs dans le cas où le corps de base est $\mathbf{F}_3$. La droite en pointillés fins est la droite "à l'infini" et les $\bullet$ représentent les éléments du support de Δ.



La paire (D_a, D_b) vérifie le critère de la proposition II.3.8. En effet, soit P un point du support de Δ de coordonnées homogènes $(\alpha : \beta : 1)$, alors $L_{a,\alpha}$ (resp. $L_{b,\beta}$) est la seule composante de D_a (resp. D_b) passant par P, ces deux composantes sont lisses en P et s'intersectent avec multiplicité 1. En un point géométrique P de $\overline{S}$ n'appartenant pas au support de Δ, au moins l'un des diviseurs D_a ou D_b ne possède pas P dans son support, on lui fait donc jouer le rôle de D_* (voir remarque II.3.10).

Le produit de deux droites projectives

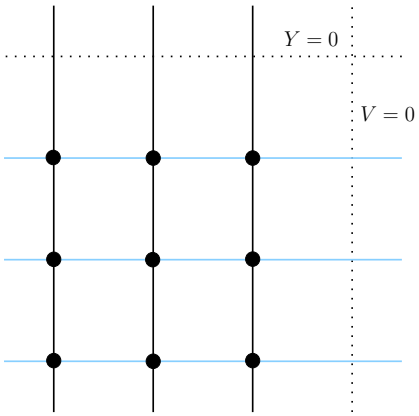
Supposons que S est la variété $\mathbf{P}^1_{\mathbf{F}_q} \times \mathbf{P}^1_{\mathbf{F}_q}$. Soit $((U, V), (X, Y))$ un système de coordonnées bihomogènes sur S. Soient W la carte affine $W := \{V \neq 0\} \cap \{Y \neq 0\}$ et Δ la somme des points rationnels de W. Pour tout α appartenant à $\mathbf{F}_q$, on introduit les droites

$$L_{a,\alpha} := \{U = \alpha\} \quad \text{et} \quad L_{b,\alpha} := \{X = \alpha\},$$

puis les diviseurs

$$D_a := \sum_{\alpha \in \mathbf{F}_q} L_{a,\alpha} \quad \text{et} \quad D_b := \sum_{\alpha \in \mathbf{F}_q} L_{b,\alpha}.$$

La figure suivante représente cette paire de diviseurs dans le cas où le corps de base est $\mathbf{F}_3$. Les droites en pointillés fins correspondent aux deux droites "à l'infini" et les $\bullet$ représentent les éléments du support de Δ.



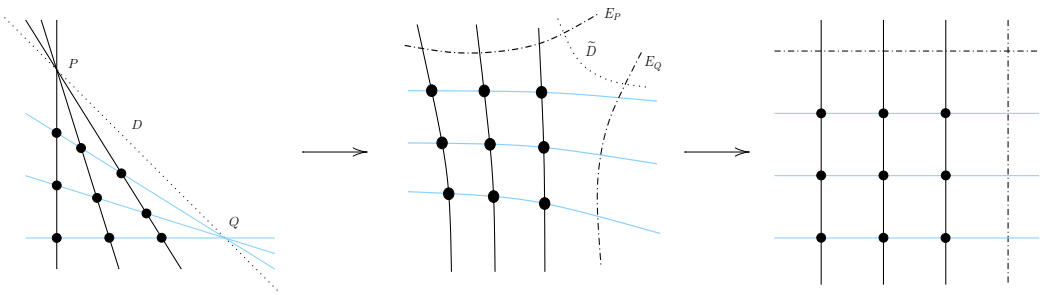
On montre aisément que le couple de diviseurs ainsi construit satisfait le critère de la proposition II.3.8, c'est donc un couple de diviseurs Δ-convenable.

Remarque II.3.15. *La construction ci-dessus s'étend aisément au cas où S est un produit de deux courbes admettant toutes deux des points rationnels.*

Quadriques lisses de $\mathbf{P}^3$

Sur un corps algébriquement clos, une quadrique lisse s'obtient à partir de $\mathbf{P}^2$ en éclatant deux points P et Q puis en contractant la transformée stricte l'unique droite contenant ces deux points. De fait, une quadrique lisse de $\mathbf{P}^3$ est toujours géométriquement isomorphe à un produit de deux droites projectives. Si le corps de base est un corps fini $\mathbf{F}_q$, on distingue deux classes d'isomorphisme de quadriques lisses dans $\mathbf{P}^3$. Les quadriques hyperboliques sont $\mathbf{F}_q$-isomorphes à $\mathbf{P}^1 \times \mathbf{P}^1$ et correspondent au cas où les points P et Q sont rationnels. Les quadriques elliptiques sont $\mathbf{F}_{q^2}$-isomorphes à $\mathbf{P}^1 \times \mathbf{P}^1$ et correspondent au cas où les points P et Q sont définis sur $\mathbf{F}_{q^2}$ et conjugués sous l'action de $\mathrm{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$.

De ce fait, on peut remarquer une relation entre les couples de diviseurs Δ-convenables des deux exemples précédents. Partons de l'exemple où S est le plan projectif. Appelons P et Q les points de concours respectifs des composantes de D_a et D_b et D la droite qui relie ces deux points. Alors, le processus d'éclatements et contractions décrit ci-dessus permet d'obtenir le couple de diviseurs Δ-convenables de l'exemple où S est $\mathbf{P}^1 \times \mathbf{P}^1$ à partir de celui où S est $\mathbf{P}^2$, par le procédé suivant



Les courbes E_P et E_Q de la figure centrale sont les diviseurs exceptionnels correspondant respectivement à P et Q. Dans la dernière figure, les courbes en pointillés sont les images de E_P et E_Q après contraction de $\widetilde{D}$.

Construction d'un diviseur Δ-convenable sur une quadrique elliptique de $\mathbf{P}^3$. Dans cet exemple, on suppose que le corps de base $\mathbf{F}_q$ est de **caractéristique différente de 2**. On considère une quadrique elliptique Q plongée dans $\mathbf{P}^3$. Soit P_∞ un point rationnel de Q et Δ, la somme de tous les points rationnels de Q sauf P_∞.

D'après les commentaires sur les quadriques donnés page 66, la surface Q se construit à partir de $\mathbf{P}^2$ en éclatant un point fermé de degré 2 puis en contractant la transformée stricte de l'unique droite rationnelle contenant ce point.

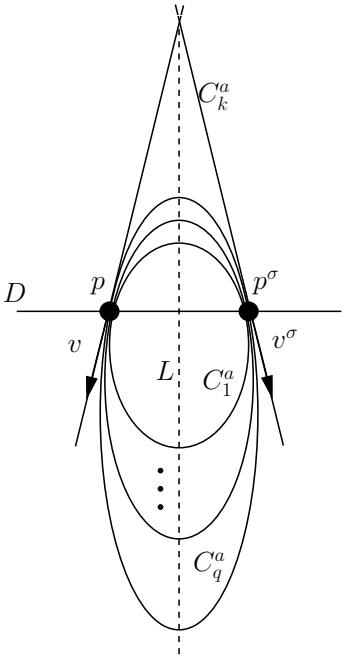
Nous allons construire notre paire de diviseurs Δ-convenable à partir de $\mathbf{P}^2$. On considère le plan projectif muni d'un système de coordonnées homogènes (X, Y, Z). Soit D, la droite d'équation $Z = 0$ et P un point fermé de D de degré 2. On notera p et p^σ les points correspondants après extension des scalaires de degré 2, l'exposant σ représente le conjugué sous l'action du Fröbenius. On pose Δ_1, la somme des points rationnels de $\mathbf{P}^2 \setminus D$. Après éclatement de P et contraction de la transformée stricte $\widetilde{D}$ de D, on obtient une quadrique elliptique, l'image de Δ_1 par cette opération est Δ.

Soient L la droite d'équation $X = 0$ et s la symétrie d'axe L définie par

$$s : (x : y : z) \mapsto (x : -y : z).$$

On rappelle que la caractéristique du corps $\mathbf{F}_q$ est supposée différente de deux dans cet exemple. De ce fait, l'application ci-dessus n'est pas l'identité.

Construction de $\mathbf{D_a}$. Soit $\alpha \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ dont la trace $\alpha + \alpha^q$ sur $\mathbf{F}_q$ est nulle. Soit $v \in \mathbf{F}_{q^2}^2$, le vecteur $v := (1, \alpha)$. Le conjugué v^σ de v est égal au symétrique de v par s. On considère l'ensemble de coniques rationnelles contenant P et admettant $\{v, v^\sigma\}$ comme vecteur tangent en ce point. Le système linéaire correspondant est de dimension 1, il y a donc $q+1$ coniques rationnelles satisfaisant ces contraintes. L'une d'entre elles est la droite double $2D$, les autres sont notées $C_1^a, \ldots, C_q^a$.



La figure est de plus invariante par s.

Remarque II.3.16. *Comme cela apparaît, l'une des coniques notée C_k^a dans la figure est dégénérée, elle est réunion de deux droites quadratiques conjuguées.*

On pose

$$D_a := \sum_{i=1}^{q} C_i^a.$$

Construction de $\mathbf{D_b^+}$. On se donne un autre vecteur $w \in \mathbf{F}_{q^2}^2 \setminus \mathbf{F}_q^2$ dont le conjugué coïncide avec son image par s et on construit une seconde famille de coniques $C_1^b, \ldots, C_q^b$ comme dans l'étape précédente. On pose

$$D_b^+ := \sum_{i=1}^{q} C_i^b.$$

Ce diviseur est également invariant sous l'action de la symétrie s.

Les diviseurs D_a et D_b^+ sont tous deux linéairement équivalents à $2qL$ où L est la classe d'équivalence linéaire d'une droite quelconque de $\mathbf{P}^2$. Le produit d'intersection de ces diviseurs est donc $4q^2$. Il va donc falloir éliminer des points en ajoutant à D_b une partie négative. Prenons le temps de décrire le 0-cycle d'intersection $D_a \cap D_b^+$.

(1) Tous les points du support de Δ y apparaissent. Les points doubles correspondent à une tangence entre un élément du support de D_a et un du support de D_b. L'invariance de ces deux diviseurs sous l'action de s entraîne que les points doubles sont sur l'axe de symétrie L. On a donc dans ce 0-cycle les q^2 points du support de Δ_1 dont q points de L qui apparaissent avec coefficient 2.

(2) La multiplicité d'intersection de D_a et D_b^+ en p (resp. p^σ) est q^2, donc le point P apparaît q^2 fois dans ce 0-cycle.

(3) Il reste donc $q^2 - q$ points géométriques à identifier dans ce 0-cycle. Ils s'agit en fait de $(q^2-q)/2$ points de degré 2 provenant de l'intersection d'un élément de $\mathrm{Supp}(D_a)$ et d'un élément de $\mathrm{Supp}(D_b)$.

Construction de $\mathbf{D_b^-}$. Pour construire D_b^-, nous allons avoir besoin de donner des équations explicites pour D_a et D_b^+. Soit $a \in \mathbf{F}_q^\times \setminus \mathbf{F}_q^{\times 2}$ et $\alpha \in \mathbf{F}_{q^2}$ une racine carrée de a. On peut supposer que le point p est de coordonnées $(1 : \alpha : 0)$. On peut alors se convaincre du fait que les deux équations suivantes fournissent de bons candidats pour D_a et D_b^+.

$$H_a = \prod_{t \in \mathbf{F}_q} (x^2 + y^2 + tz^2)$$

et

$$H_b = \prod_{t \in \mathbf{F}_q} ((x-z)^2 + y^2 + tz^2) = \prod_{t' \in \mathbf{F}_q} (x^2 + y^2 - 2xz + t'z^2).$$

Trouver un point d'intersection dans le plan affine de D_a et D_b^+ revient à trouver un point d'intersection entre une conique du support de D_a et une conique du support de D_b. Ce qui revient à résoudre le système :

$$\left\{ \begin{array}{rcl} x^2+y^2+t &=& 0 \\ x^2+y^2-2x+u &=& 0 \end{array} \right. \iff \left\{ \begin{array}{rcl} x^2+y^2+t &=& 0 \\ x &=& \frac{t-u}{2} \end{array} \right. \iff \left\{ \begin{array}{rcl} x &=& \frac{t-u}{2} \\ y^2 &=& t - (\frac{t-u}{2})^2. \end{array} \right.$$

On vérifie ensuite que l'application $(t,u) \to t - (t-u)^2/4$ est surjective de $\mathbf{F}_q \times \mathbf{F}_q$ dans $\mathbf{F}_q$. En d'autres termes les points d'intersections dans le plan affine de deux telles coniques sont soit des points $\mathbf{F}_q$-rationnels du plan affine soit des points de la forme (s, τ) où s est un élément de $\mathbf{F}_q$ et τ un élément de $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$ dont le carré est dans $\mathbf{F}_q$.

Rappelons que les points doubles dans l'intersection de D_a et D_b^+ sont tous sur l'axe de symétrie, à savoir la droite d'équation y. Aussi, le diviseur effectif d'équation

$$H_c := y \prod_{s \in \mathbf{F}_q^\times \setminus \mathbf{F}_q^{\times 2}} (y^2 - sz^2)$$

fournit un bon candidat pour le diviseur D_b^-.
On pose alors $D_b := D_b^+ - D_b^-$.

On définit enfin sur Q les diviseurs $\widetilde{D}_a$ et $\widetilde{D}_b$ construits comme étant les transformées strictes des diviseurs du même nom par l'opération d'éclatement/contraction. Le 0-cycle d'intersection de ces diviseurs est exactement Δ, car l'opération d'éclatement a "séparé" les diviseurs D_a et D_b en P. On vérifie alors que cette paire de diviseurs vérifie le critère de la proposition II.3.8, elle est donc Δ-convenable.

Remarque II.3.17. *Le groupe de Picard d'une quadrique elliptique est libre de rang* 1 *et engendré par la classe d'une section plane L_Q. On Peut aisément montrer que les diviseurs ainsi construits vérifient*

$$\widetilde{D}_a \sim \widetilde{D}_b^+ \sim \widetilde{D}_b^- \sim qL_Q.$$

Autres exemples

D'une façon générale le calcul de paires de diviseurs Δ-convenables est ardue. Toutefois, le lemme II.4.7 et la remarque II.4.8 stipulent que des paires de diviseurs Δ-convenables sont explicitement calculables via des méthodes d'interpolation implémentables sur ordinateur. Un programme appelé DeltaConv permettant de calculer des paires de diviseurs $\Delta - convenables$ à l'aide du logiciel MAGMA est proposé en annexe F.1. Avec l'aide de ce programme nous avons calculé des paires de diviseurs Δ-convenables pour quelques exemples moins triviaux que ceux qui précèdent.

Sur une surface Hermitienne. On considère la surface Hermitienne sur $\mathbf{F}_4$ plongée dans $\mathbf{P}^3$ d'équation $X^3+Y^3+Z^3+T^3=0$. On la munit du 0-cycle égal à la somme de ses points rationnels dans la carte affine $\{Z \neq 0\}$. Le programme nous retourne les résultats suivants.

```
>
> F<w>:=FiniteField(4);
> P3<x,y,z,t>:=ProjectiveSpace(F,3);
> Herm:=Scheme(P3,x^3+y^3+z^3+t^3);
>
>
> A:=DeltaConv(Herm,Points,1000,1000,10);
D_a a ete trouve de maniere deterministe.
D_b^+ a ete trouve de maniere deterministe.
D_b^- a ete trouve de maniere deterministe.


Le diviseur d'equation
x*y^3 + x*z^3 + y^4 + y*t^3 + z^4 + z*t^3
 convient pour D_a.

Le diviseur d'equation
w^2*x^4 + w^2*x*t^3 + w*y^4 + w*y*t^3 + z^4 + z*t^3
 convient pour D_b^+.

Le diviseur d'equation
x^2 + w^2*y^2 + w*z^2
 convient pour D_b^-.
```

Sur une surface quartique. On considère la surface d'équation $X^4+Y^4+Z^4+T^4=0$ définie sur $\mathbf{F}_3$. On prend comme 0-cycle Δ, la somme des points rationnels de la carte affine $\{Z=0\}$ de cette surface. On obtient le résultat suivant.

```
> S:=Scheme(P3,x^4+y^4+z^4+t^4);
> A:=DeltaConv(Herm,Points,1000,1000,10);

Le diviseur d'equation
x^2 + y^2 + z^2 + t^2
 convient pour D_a.

Le diviseur d'equation
z^3 + 2*z*t^2
 convient pour D_b^+.

Le diviseur d'equation
x^3*z + 2*x^3*t + 2*x^2*y^2 + x^2*y*z + x^2*y*t +
      x^2*z^2 + x^2*z*t + x^2*t^2 + x*y^2*z + 2*x*y^2*t +
      x*y*z^2 + 2*x*z^2*t + 2*x*z*t^2 + 2*x*t^3 + y^4 +
      y^3*z + y^3*t + y^2*z^2 + y^2*z*t + y*z^2*t +
      2*y*z*t^2 + y*t^3 + z^3*t + 2*z^2*t^2 + z*t^3 +
      2*t^4
 convient pour D_b^-.
```

II.3.6 Discussion sur la Δ-convenance et le critère

Au vu des exemples du plan projectif et du produit de deux droites projectives, on est tenté d'envisager une définition nettement plus simple. Un couple (D_a, D_b) serait Δ-convenable si et seulement si les diviseurs D_a et D_b étaient effectifs et le 0-cycle d'intersection $D_a \cap D_b$ vérifiait

$$D_a \cap D_b = \Delta.$$

On montre aisément qu'une telle définition implique en fait la Δ-convenance (il implique le critère de la proposition II.3.8). Cependant, elle n'est pas vraiment intéressante en ce sens où, étant donné un 0-cycle Δ sur S, une paire de diviseurs vérifiant de telles conditions n'existe pas en général. Par exemple, si S est le plan projectif et Δ la somme de trois points rationnels non alignés on ne peut construire une paire (D_a, D_b) vérifiant ces conditions. En effet, supposons qu'une telle paire existe et soit L une droite de $S = \mathbf{P}^2$, alors la classe de L engendre la groupe de Picard de S et il existe deux entiers positifs n_a et n_b tels que $D_a \sim n_a L$ et $D_b \sim n_b L$. De plus, le produit d'intersection de D_a et D_b est 3 par hypothèse. Donc, comme l'auto-intersection de L est égale à 1, on en déduit que n_a ou n_b est égal à 1, ce qui contredit le fait que les éléments du support de Δ sont non alignés.

II.4 Relations entre codes fonctionnels et différentiels sur une surface

Nous étudions dans cette section l'extension aux surfaces de relations connues en théorie des codes construits à partir de courbes. On rappelle que l'on se place toujours dans le cadre décrit en section II.3.1.

II.4.1 Relation d'orthogonalité

Le théorème qui suit est celui qui a motivé l'introduction de la notion de Δ-convenance.

Théorème II.4.1 (Théorème d'orthogonalité)**.** *Soient (D_a, D_b) une paire Δ-convenable de diviseurs et $D := D_a + D_b$. On a alors,*

$$C_{\Omega,S}(\Delta, D_a, D_b, G) \subseteq C_{L,S}(\Delta, G)^{\perp}.$$

PREUVE. Soient c un mot de $C_{L,S}(\Delta, G)$ et c' un mot de $C_{\Omega,S}(\Delta, D_a, D_b, G)$. Il existe respectivement une fonction f appartenant à $L(G)$ et une 2-forme ω appartenant à $\Gamma(S, \Omega^2(G-D))$ telles que

$$c = \mathrm{ev}_\Delta(f) \quad \text{et} \quad c' = \mathrm{res}^2_{D_a,\Delta}(\omega).$$

On note "$\langle\ ,\ \rangle$" la forme bilinéaire canonique sur $\mathbf{F}_q^n$. On a donc

$$\langle c, c' \rangle = \sum_{i=1}^{n} f(P_i)\mathrm{res}^2_{D_a,P_i}(\omega).$$

Comme le support diviseur G est supposé éviter celui du 0-cycle Δ, on en déduit que f est régulière au voisinage de tout point P_i appartenant au support de Δ. De plus, la 2-forme $f\omega$ appartient à $\Gamma(S, \Omega^2(-D))$. Donc, d'après la définition de Δ-convenance, on a

$$\forall P \in \overline{S},\ \mathrm{res}^2_{D_a,P}(f\omega) = \begin{cases} 0 & \text{si} \quad P \notin \mathrm{Supp}(\Delta) \\ f(P)\mathrm{res}^2_{D_a,P}(\omega) & \text{si} \quad P \in \mathrm{Supp}(\Delta). \end{cases}$$

Par conséquent,

$$\langle c, c' \rangle = \sum_{i=1}^{n} \mathrm{res}^2_{D_a,P_i}(f\omega) = \sum_{\mathbf{P}\in\overline{S}} \mathrm{res}^2_{D_a,P}(f\omega)$$

et cette dernière somme est nulle d'après la troisième formule des résidus (théorème I.7.11). □

En section II.5.2 l'étude d'un exemple simple nous montrera que l'inclusion réciproque est en général fausse. Elle peut d'ailleurs être fausse pour tout choix de paire Δ-convenable de diviseurs. Nous discuterons de ce défaut d'inclusion réciproque en section II.6.

Avant de passer à la suite faisons une courte remarque sur les notations adoptées.

Allègement des notations. Les notations de codes fonctionnels et différentiels sur S sont respectivement $C_{L,S}(\Delta, G)$ et $C_{\Omega,S}(\Delta, D_a, D_b, G)$. Dans ce qui suit, s'il n'y a pas d'ambiguïté sur la variété sur laquelle on travaille (en l'occurrence dans ce chapitre on travaille systématiquement sur S), on s'autorisera à ne pas la signaler en indice. On parlera alors de $C_L(\Delta, G)$ et $C_\Omega(\Delta, D_a, D_b, G)$.

II.4.2 Un code différentiel est fonctionnel

Nous avons vu en section II.2 qu'un code différentiel sur une courbe vérifiait deux propriétés intéressantes. La première est qu'il est l'orthogonal d'un code fonctionnel. La seconde est que ce code s'identifie à un code fonctionnel associé à d'autres diviseurs. Dans ce qui précède, nous avons cherché un analogue de la première propriété. Nous allons maintenant en chercher un pour la seconde et voir qu'à la différence de la première, cette seconde propriété s'étend parfaitement aux codes construits sur des surfaces.

Dans le cas des codes sur les courbes, ce résultat est une conséquence du théorème d'approximation faible aussi appelé théorème d'indépendance des valuations (voir [Sti93] I.3.1). De fait, nous allons avoir besoin d'un résultat analogue en dimension 2. La proposition qui suit est sensiblement différente d'un énoncé de théorème d'indépendance de valuations, mais elle va nous fournir exactement le résultat nécessaire pour la suite.

Proposition II.4.2. *Soit C une courbe irréductible plongée dans S. Soient $P_1, \ldots, P_r$ une famille de points fermés de $S \setminus C$ et $Q_1, \ldots, Q_S$ une famille de points fermés de C. Alors, il existe une uniformisante $v \in \mathcal{O}_{S,C}$ telle que le support du diviseur principal (v) évite les points $P_1, \ldots, P_r$ et celui du diviseur $(v) - C$ évite les points $Q_1, \ldots, Q_s$.*

Remarque II.4.3. *Une autre façon de formuler le résultat consiste à dire qu'il existe une fonction v qui est une équation locale de C au voisinage des points $Q_1, \ldots, Q_s$ et qui n'a ni zéro ni pôle en les points $P_1, \ldots, P_r$.*

PREUVE. Soit v_0 une uniformisante de $\mathcal{O}_{S,C}$. Alors, le diviseur de v_0 est de la forme

$$(v_0) = C + D,$$

où D est un diviseur dont le support ne contient pas C. D'après le *moving lemma* ([Sha94] III.1.3 théorème 1), il existe un diviseur D' linéairement équivalent à D dont le support évite les points $P_1, \ldots, P_r, Q_1, \ldots, Q_r$. Ainsi, il existe une fonction f rationnelle sur S telle que

$$D' = D + (f).$$

La fonction $v := fv_0$ est solution du problème. □

Remarque II.4.4. *Dans le premier volume du livre [Sha94] de Shafarevich, le corps de base est supposé algébriquement clos. Cependant, l'étude de la preuve du "moving lemma" permet de constater que cette hypothèse n'est pas utile pour prouver ce résultat. Une preuve directe de la proposition II.4.2 est donnée en annexe B. La logique de cette preuve est sensiblement la même que celle du moving lemma.*

Corollaire II.4.5. *Soit (D_a, D_b) une paire Δ-convenable de diviseurs et $D := D_a + D_b$. Alors, il existe une 2-forme ω_0 rationnelle sur S qui vérifie les propriétés suivantes.*

(1) Il existe un ouvert U contenant le support de Δ et tel que $(\omega_{0|U}) = -D_{|U}$.

(2) Pour tout point P appartenant au support de Δ, on a $res^2_{D_a,P}(\omega_0) = 1$.

(3) Pour tout point P appartenant au support de Δ et pour toute fonction f régulière au voisinage de P, on a $res^2_{D_a,P}(f\omega_0) = f(P)res^2_{D_a,P}(\omega_0)$.

PREUVE. Soient $X_1, \ldots, X_r$ et $Y_1, \ldots, Y_r$ les composantes irréductibles respectives des supports de D_a et D_b. Il existe des entiers $m_1, \ldots, m_r$ et $n_1, \ldots, n_s$ tels que

$$D_a = m_1X_1 + \cdots + m_rX_r \quad \text{et} \quad D_b = n_1Y_1 + \cdots + n_sY_s.$$

D'après la proposition II.4.2, il existe un voisinage U de $\mathrm{Supp}(\Delta)$ et des fonctions $u_1, \ldots, u_r$ et $v_1, \ldots, v_s$ régulières sur U telles que pour tout i (resp. tout j), la fonction $u_{i|U}$ est une équation de $X_i \cap U$ (resp. $v_{j|U}$ est une équation de $Y_j \cap U$).

Soit μ une 2-forme rationnelle sur S n'ayant ni zéro ni pôle au voisinage du support de Δ. Une telle 2-forme existe, car d'après le *moving lemma* (voir [Sha94] III.1.3 thm1 et remarque II.4.4), il existe un diviseur canonique dont le support évite celui de Δ. Quitte à remplacer U par un voisinage plus petit de $\mathrm{Supp}(\Delta)$ on peut supposer que la 2-forme μ restreinte à U n'a ni zéro ni pôle. On pose alors

$$\omega := \frac{\mu}{uv}.$$

On a donc

$$(\omega_{|U}) = -D_{|U}$$

et d'après la définition de Δ-convenance, pour tout P appartenant au support de Δ, on a

$$\mathrm{res}^2_{D_a,P}(\omega) = a_P \neq 0.$$

Par interpolation, on peut construire une fonction g régulière au voisinage du support de Δ et telle que pour tout P dans ce support,

$$g(P) = a_P^{-1}.$$

Quitte a réduire encore la taille de U, on peut supposer que g n'a ni zéro ni pôle sur U. On pose alors

$$\omega_0 := g\omega.$$

Comme g n'a ni zéro ni pôle sur U, les 2-formes ω et ω_0 restreintes à U ont même diviseur, c'est-à-dire

$$(\omega_{0|U}) = -D_{|U}.$$

La Δ-convenance du couple (D_a, D_b) permet de conclure que ω_0 vérifie les propriétés requises. □

Théorème II.4.6. *Soient (D_a, D_b) une paire Δ-convenable de diviseurs et $D := D_a + D_b$, alors il existe un diviseur canonique K tel que*

$$C_\Omega(\Delta, D_a, D_b, G) = C_L(\Delta, K - G + D).$$

PREUVE. Soit ω_0 une 2-forme rationnelle sur S vérifiant les propriétés du corollaire II.4.5 et soit K son diviseur. D'après la propriété 1 du corollaire II.4.5, le diviseur K est de la forme

$$K = -D + R,$$

où le support de R évite celui de Δ. Soit ω une 2-forme appartenant à $\Gamma(S, \Omega^2(G - D))$, il existe une unique fonction f dans $L(K - G + D)$ telle que

$$\omega = f\omega_0.$$

Notons que

$$K - G + D = -G + R.$$

Aussi, les éléments de $L(K - G + D)$ sont des fonctions régulières au voisinage de $\mathrm{Supp}(\Delta)$. Soit P un point du support de Δ, d'après les propriétés 2 et 3 du corollaire II.4.5, on a

$$\mathrm{res}^2_{D_a,P}(\omega) = \mathrm{res}^2_{D_a,P}(f\omega_0) = f(P)\underbrace{\mathrm{res}^2_{D_a,P}(\omega_0)}_{=1}.$$

On en déduit la relation

$$\mathrm{res}^2_{D_a,\Delta}(\omega) = \mathrm{ev}_\Delta(f).$$

□

Nous avons montré que tout code différentiel est en fait un code fonctionnel associé à d'autres diviseurs. Notons à ce stade que, dans le cas des courbes, la réciproque est élémentaire, à savoir : *tout code fonctionnel est différentiel*. Dans le cas des surfaces, cette réciproque est moins évidente. En effet, étant donné un code fonctionnel $C_L(\Delta, G)$, si l'on veut prouver que ce code se réalise sous la forme d'un code différentiel, il faut d'abord disposer d'une paire Δ-convenable de diviseurs.

II.4.3 Réciproque, un code fonctionnel est différentiel

Lemme II.4.7 (Existence d'une paire Δ-convenable pour tout Δ)**.** *Soient S une surface algébrique projective lisse géométriquement intègre et $Q_1, \ldots, Q_m$ une famille de points rationnels de S. Posons $\Delta := Q_1 + \cdots + Q_m$. Alors, il existe une infinité de paires Δ-convenables qui vérifient le critère de la proposition II.3.8.*

Remarque II.4.8. *La démonstration qui suit est constructive. De fait, elle accentue l'intérêt de la proposition II.3.8. En effet, même si le critère qui y est énoncé est extrêmement technique, les paires qui le vérifient peuvent être calculées explicitement.*

PREUVE. **Étape 1 : Construction de $\mathbf{D_a}$.** On choisit une courbe réduite C, éventuellement réductible qui contienne tout le support de Δ et qui soit régulière en chaque point de ce dernier. Assurons nous de l'existence d'une telle courbe. Soit U un voisinage affine du support de Δ, on note $\mathfrak{m}_{P_1}, \ldots, \mathfrak{m}_{P_n}$ les idéaux maximaux de $\mathbf{F}_q[U]$ correspondant aux points $P_1, \ldots, P_n$. Il s'agit de choisir un élément de l'idéal produit $\mathfrak{m}_{P_1} \cdots \mathfrak{m}_{P_n}$ qui n'appartienne à aucun des idéaux $\mathfrak{m}^2_{P_i}$. Les idéaux $\mathfrak{m}^2_{P_i}$ étant deux à deux étrangers, d'après le théorème chinois, on a l'isomorphisme

$$\mathbf{F}_q[U]/\mathfrak{m}^2_{P_1} \cdots \mathfrak{m}^2_{P_n} \xrightarrow{\sim} \prod_{i=1}^n \mathbf{F}_q[U]/\mathfrak{m}^2_{P_i}.$$

On choisit un élément $(\bar{a}_1, \ldots, \bar{a}_n)$ dans $\prod_i \mathfrak{m}_{P_i}/\mathfrak{m}^2_{P_i}$ dont aucune des coordonnées $\bar{a}_i$ n'est nulle. On relève cet élément en une fonction a de $\mathbf{F}_q[U]$ par le biais de l'isomorphisme ci-dessus. La fonction obtenue appartient bien à l'idéal produit $\mathfrak{m}_{P_1} \cdots \mathfrak{m}_{P_n}$ et n'est dans aucun

des $\mathfrak{m}_{P_i}^2$. La fermeture projective du lieu d'annulation de a est une courbe C vérifiant les conditions exigées. De plus, si l'on remplace a par $a+m$ où m est un élément de $\mathfrak{m}_{P_1}^2 \cdots \mathfrak{m}_{P_n}^2$ n'appartenant pas à l'idéal engendré par a, on obtient une courbe C' distincte de C et vérifiant les mêmes conditions. On en déduit l'existence d'une infinité de courbes interpolant le support de Δ et lisse en chaque point de ce dernier. Soit donc C une telle courbe, on pose alors

$$D_a := C_1 + \cdots + C_k,$$

où les C_i sont les composantes irréductibles de C.

Étape 2 : Construction de $\mathbf{D_b}$. On choisit, toujours par interpolation, un diviseur effectif D' interpolant tous les points de $\mathrm{Supp}(\Delta)$ et n'ayant pas de composante irréductible commune avec D_a. Soit Θ, le 0-cycle obtenu par l'intersection au sens de la théorie des schémas des diviseurs D_a et D'. On a donc

$$\Theta = \Delta + \Delta'$$

où Δ' est un 0-cycle effectif. On choisit alors un diviseur D'' tel que

$$D_a \cap D'' = \Delta' + \Delta''$$

où le support de Δ'' est disjoint de celui de Δ. Le diviseur D'' se construit également par interpolation. On pose enfin

$$D_b := D' - D''.$$

On montre aisément que la paire ainsi construite vérifie le critère de la proposition II.3.8. Elle est donc Δ-convenable. Comme il existe une infinité de façons de construire D_a (et D_b) on en déduit qu'il existe une infinité de paires Δ-convenables. □

Théorème II.4.9. *Étant donné un diviseur G sur S, il existe un diviseur canonique K et une paire Δ-convenable (D_a, D_b) telle que*

$$C_L(\Delta, G) = C_\Omega(\Delta, D_a, D_b, K - G + D).$$

Preuve. Le lemme II.4.7 assure l'existence d'une paire Δ-convenable (D_a, D_b). À partir de cette paire, on construit une 2-forme ω_0 en utilisant corollaire II.4.5. On pose

$$K := (\omega_0).$$

D'après le théorème II.4.6 on a

$$\begin{aligned} C_\Omega(\Delta, D_a, D_b, K - G + D) &= C_L(\Delta, K - (K - G + D) + D) \\ &= C_L(\Delta, G). \end{aligned}$$

Ce qui conclut la démonstration. □

II.5 Défaut d'inclusion réciproque pour le théorème d'orthogonalité

Nous allons présenter deux exemples de surfaces, qui sont en l'occurrence les exemples les plus simples que l'on connaisse, à savoir $\mathbf{P}^2$ et $\mathbf{P}^1 \times \mathbf{P}^1$. Nous allons voir que l'on dispose d'une inclusion réciproque systématique pour le premier exemple (le plan projectif) en choisissant une paire de diviseurs Δ-convenable extrêmement simple. Ensuite, nous observerons que dans le second exemple (le produit de deux droites projectives), l'inclusion réciproque pour le théorème d'orthogonalité n'a jamais lieu, et ce quel que soit la paire Δ-convenable choisie.

II.5.1 Codes sur le plan projectif

On reprend les notations de la section II.3.5. On rappelle que X, Y et Z désignent des coordonnées homogènes sur $\mathbf{P}^2$, que l'ouvert U est le complémentaire de la droite d'équation $Z = 0$ et que le 0-cycle Δ est la somme de tous les points rationnels de l'ouvert U. Pour construire des codes fonctionnels on doit également introduire un diviseur G. Soient m un entier positif et L_∞ la droite d'équation $Z = 0$, on pose

$$G_m := mL_\infty.$$

Notons que, comme la classe d'équivalence linéaire de la droite L_∞ engendre le groupe de Picard de $\mathbf{P}^2$, on peut sans perte de généralité considérer que le diviseur G est de la forme G_m.

Remarque II.5.1. *On a supposé que l'entier naturel m était positif, on aurait pu omettre cette hypothèse. Cependant, si $m < 0$, alors l'espace $L(G_m)$ est nul et le code fonctionnel le sera également. Nous avons donc choisi d'éviter cette situation totalement inintéressante.*

Codes fonctionnels

Commençons par rappeler que les codes fonctionnels $C_L(\Delta, G_m)$ ne sont autre que des codes de Reed-Müller affines. Posons

$$x := \frac{X}{Z} \quad \text{et} \quad y := \frac{Y}{Z}.$$

L'espace vectoriel $L(G_m)$ s'identifie à l'espace $\mathbf{F}_q[x, y]_{\leq m}$ des polynômes en x et y de degré total inférieur ou égal à m. On rappelle que, par convention, si l'entier m est strictement négatif, alors l'espace $\mathbf{F}_q[x, y]_{\leq m}$ est nul. Ainsi, le code $C_L(\Delta, G_m)$ s'obtient par évaluation en tous les points du plan affine U des éléments de l'espace vectoriel $\mathbf{F}_q[x, y]_{\leq m}$, c'est donc le code de Reed-Müller $RM_q(2, m)$. Pour plus d'informations sur les codes de Reed-Müller, voire [MS77a] chap 13 pour les codes binaires et [DGM70] pour le cas général.

Codes différentiels

On reprend la paire Δ-convenable (D_a, D_b) de la section II.3.5. C'est à dire que D_a (resp. D_b) est la somme de toutes les droites d'équations $x = \alpha$ (resp. $y = \alpha$) avec $\alpha \in \mathbf{F}_q$. Pour procéder à l'étude des codes différentiels de la forme $C_\Omega(\Delta, D_a, D_b, G_m)$, nous allons utiliser le théorème II.4.6 et chercher à quels codes fonctionnels ils s'identifient. Pour ce faire, nous allons introduire explicitement une 2-forme rationnelle ω_0 vérifiant les propriétés du corollaire II.4.5. Soit donc

$$\omega_0 := \frac{dx}{\prod_{\alpha \in \mathbf{F}_q}(x - \alpha)} \wedge \frac{dy}{\prod_{\beta \in \mathbf{F}_q}(y - \beta)}.$$

Calcul du diviseur de ω_0. D'après [Sha94] III.6.4, on sait qu'un diviseur canonique sur $\mathbf{P}^2$ est linéairement équivalent à $-3L_\infty$. De plus,

$$(\omega_{0|U}) = -D_{|U}.$$

De fait, le diviseur canonique (ω_0) est de la forme

$$(\omega_0) = kL_\infty - D$$

où k est un entier à déterminer. On sait également que, par construction, le diviseur D est linéairement équivalent à $2qL_\infty$. On en déduit la relation

$$-3L_\infty \sim (k - 2q)L_\infty, \quad \text{donc} \quad k = 2q - 3.$$

En conclusion,

$$(\omega_0) = (2q - 3)L_\infty - D = G_{2q-3} - D. \tag{II.5}$$

Propriétés vérifiées par ω_0. Maintenant que l'on connaît le diviseur (ω_0) et que l'on sait qu'il coïncide avec $-D$ sur le voisinage U du support de Δ, il reste à vérifier que ω_0 vérifie les deux autres propriétés du corollaire II.4.5. Soient P un point appartenant au support de Δ et x_P, y_P ses coordonnées affines dans U. On appelle C, la droite d'équation $y = y_P$ et on calcule le 1-résidu de ω_0 le long de cette droite. On obtient

$$\mathrm{res}^1_C(\omega_0) = \frac{1}{\prod_{\beta \neq y_P}(y_P - \beta)} \ \frac{d\bar{x}}{\prod_{\alpha \in \mathbf{F}_q}(\bar{x} - \alpha)}.$$

On remarque que le produit $\prod_{\beta \neq y_P}(y_P - \beta)$ est égal au produit de tous les éléments de $\mathbf{F}_q^\times$, il est donc égal à -1.
Calculons à présent le 2-résidu en P le long de C de ω_0, c'est à dire le résidu en P de la 1-forme sur C ci-dessus. On obtient

$$\mathrm{res}^2_{C,P}(\omega_0) = -\frac{1}{\prod_{\alpha \neq x_P}(x_P - \alpha)} = 1.$$

La propriété 3 est une conséquence immédiate de la Δ-convenance de (D_a, D_b).

Identification à des codes fonctionnels et orthogonalité. La 2-forme ω_0 vérifie les propriétés du corollaire II.4.5. On en déduit que pour tout entier m, le code $C_\Omega(\Delta, D_a, D_b, G_m)$ s'identifie au code $C_L(\Delta, (\omega_0) - G_m + D)$. D'après le calcul du diviseur (ω_0) en (II.5), on conclut que pour tout entier m, on a

$$C_\Omega(\Delta, D_a, D_b, G_m) = C_L(\Delta, G_{2q-3-m}).$$

D'après le théorème II.4.1, on a l'inclusion

$$C_\Omega(\Delta, D_a, D_b, G_m) \subseteq C_L(\Delta, G_m)^\perp.$$

On peut évaluer les dimensions de ces codes et montrer que l'inclusion réciproque est vérifiée. Ce résultat n'a absolument rien de nouveau. Il est en effet connu que l'orthogonal d'un code de Reed-Müller est encore un code de Reed-Müller (voir [MS77b] ch 13 et [DGM70] 3.2).

En conclusion, l'orthogonalité parfaite entre code fonctionnel et code différentiel est obtenue dans ce cas élémentaire et très particulier. Il ne s'agit malheureusement pas d'un fait général. L'exemple suivant, qui est pourtant presque aussi élémentaire, montre qu'en général on doit se contenter d'une inclusion stricte.

II.5.2 Codes sur un produit de deux droites projectives

On reprend les notations de la section II.3.5. On rappelle que $((U, V), (X, Y))$ est un système de coordonnées bihomogènes sur $\mathbf{P}^1 \times \mathbf{P}^1$. On note E et F les droites d'équations respectives $V = 0$ et $Y = 0$. On rappelle également que l'ouvert U est le complémentaire de $E \cup F$. Enfin, pour tout couple d'entiers (m, n) on définit le diviseur $G_{m,n}$ par

$$G_{m,n} := mE + nF.$$

Tout comme dans l'exemple précédent, on sait que l'on peut sans perte de généralité supposer que le diviseur G intervenant dans la construction du code fonctionnel est de la forme $G_{m,n}$. En effet, les classes d'équivalence linéaires de E et F engendrent le groupe de Picard de $\mathbf{P}^1 \times \mathbf{P}^1$.

Codes fonctionnels

Nous allons montrer tout d'abord que les codes fonctionnels de la forme $C_L(\Delta, G_{m,n})$ sont des produits tensoriels de codes de Reed-Solomon. Posons

$$u := \frac{U}{V} \quad \text{et} \quad x := \frac{X}{Y}.$$

L'espace vectoriel $L(G_{m,n})$ s'identifie au sous-espace de $\mathbf{F}_q[u,x]$ des polynômes de degré en u inférieur ou égal à m et de degré en x inférieur ou égal à n. En d'autres termes on a l'identification

$$L(G_{m,n}) \cong \mathbf{F}_q[u]_{\leq m} \otimes_{\mathbf{F}_q} \mathbf{F}_q[x]_{\leq n}.$$

On note $RS_q(n)$ le code de Reed-Solomon de longueur q obtenu par évaluation en tous les éléments de $\mathbf{F}_q$ des polynômes de $\mathbf{F}_q[t]_{\leq n}$. Le code fonctionnel sur $\mathbf{P}^1 \times \mathbf{P}^1$ est donc de la forme

$$C_L(\Delta, G_{m,n}) = RS_q(m) \otimes_{\mathbf{F}_q} RS_q(n).$$

L'orthogonal ne peut être différentiel. D'après le théorème II.4.6, il suffit de montrer que l'orthogonal du code fonctionnel $C_L(\Delta, G_{m,n})$ n'est pas un code fonctionnel sur $\mathbf{P}^1 \times \mathbf{P}^1$. Un tel résultat entraînerait, qu'il n'existe aucun couple Δ-convenable (D_a, D_b) tel que le code $C_L(\Delta, G_{m,n})^\perp$ soit égal à $C_\Omega(\Delta, D_a, D_b, G_{m,n})$. On a vu dans le paragraphe précédent que le code $C_L(\Delta, G_{m,n})$ était égal au produit tensoriel des codes $RS_q(m)$ et $RS_q(n)$. Ces codes de Reed-Solomon sont non triviaux, si et seulement si

$$0 \leq m \leq q-2 \quad \text{et} \quad 0 \leq n \leq q-2.$$

Si les entiers m et n vérifient les encadrements ci-dessus, alors l'orthogonal du code $C_L(\Delta, G_{m,n})$ ne peut être fonctionnel. En effet, si $C_L(\Delta, G_{m,n})^\perp$ était un code fonctionnel $C_L(\Delta, G)$, alors G serait linéairement équivalent à un certain $G_{a,b}$. De fait, le code fonctionnel $C_L(\Delta, G)$ serait isométrique[2] à $C_L(\Delta, G_{a,b})$ et cette isométrie serait représentée par une matrice diagonale dans la base canonique de $\mathbf{F}_q^{q^2}$. En regardant $\mathbf{F}_q^{q^2}$ comme le produit tensoriel de deux copies de $\mathbf{F}_q^q$, le code $C_L(\Delta, G_{a,b})$ est un produit tensoriel de deux codes et cette propriété est invariante sous l'action d'une isométrie diagonale. Ainsi, l'orthogonal $C_L(\Delta, G)$ de $C_L(\Delta, G_{m,n})$ serait un produit tensoriel de deux codes. Ce qui est impossible d'après le lemme C.0.5 énoncé en annexe C.

En conclusion, pour tout couple Δ-convenable (D_a, D_b) et tout couple d'entiers (m,n) tous deux compris entre 0 et $q-2$, on a

$$C_\Omega(\Delta, D_a, D_b, G) \subsetneq C_L(\Delta, G)^\perp.$$

Remarque II.5.2. *Par un raisonnement identique, on peut montrer que ce défaut d'inclusion réciproque a lieu pour toute surface S qui est un produit de deux courbes.*

Une réalisation de l'orthogonal. D'après le lemme C.0.4, l'orthogonal du code $C_L(\Delta, G_{m,n})$ est une somme de deux produits tensoriels. À savoir

$$C_L(\Delta, G_{m,n})^\perp = RS_q(m)^\perp \otimes \mathbf{F}_q^q + \mathbf{F}_q^q \otimes RS_q(n)^\perp. \tag{II.6}$$

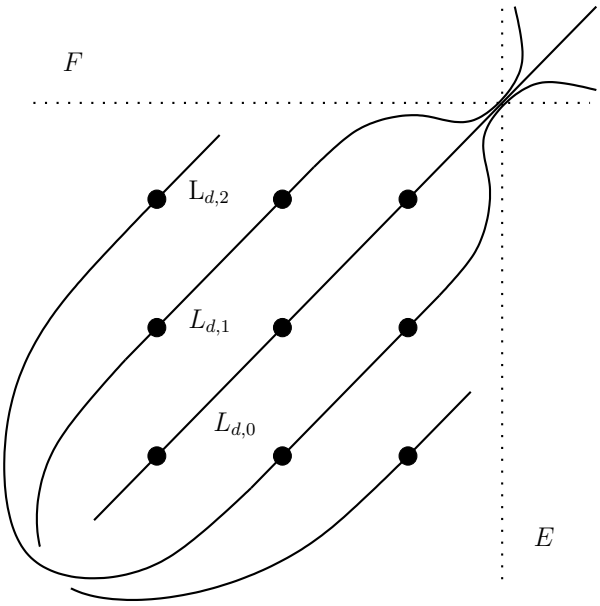
L'orthogonal d'un code de Reed-Solomon étant encore un code de Reed-Solomon, les deux termes de la somme ci-dessus ($RS_q(m)^\perp \otimes \mathbf{F}_q^q$ et $\mathbf{F}_q^q \otimes RS_q(n)^\perp$) sont des produits tensoriels de codes de Reed-Solomon. Ce sont donc des codes fonctionnels sur $\mathbf{P}^1 \times \mathbf{P}^1$. Nous allons tenter de les réaliser sous forme de codes différentiels.

Pour tout $\alpha \in \mathbf{F}_q$, on appelle $L_{d,\alpha}$ la droite d'équation $u - x - \alpha$. Les droites $(L_{d,\alpha})_{\alpha \in \mathbf{F}_q}$ forment un famille de droites *diagonales parallèles* dans l'ouvert U elles sont concourantes en le point Q d'intersection des droites à l'infini E et F. Elles sont également deux à deux tangentes en ce point. On définit le diviseur D_d par

$$D_d := \sum_{\alpha \in \mathbf{F}_q} L_{d,\alpha}.$$

La figure suivante est une tentative de représentation du support de D_d dans le cas où le corps de base est $\mathbf{F}_3$. Si les droites ne ressemblent plus à des droites, nous avons par contre cherché à représenter les points rationnels de U que ces *droites* interpolent.

[2] Au sens de la métrique de Hamming.



Remarque II.5.3. *Par le plongement de Segré, $\mathbf{P}^1 \times \mathbf{P}^1$ s'identifie à une quadrique hyperbolique de $\mathbf{P}^3$. Les droites $L_{d,\alpha}$ sont les tirés en arrière des éléments d'un pinceau de coniques rationnelles obtenues par des sections de cette quadrique par des plans rationnels contenant tous une même droite tangente à la quadrique en un point.*

Dans ce qui suit, les diviseurs D_a et D_b sont ceux qui ont été définis sur $\mathbf{P}^1 \times \mathbf{P}^1$ page 65.

Proposition II.5.4. *Si les entiers m et n sont tous deux compris entre 0 et $q-1$, on a alors les trois relations suivantes.*

$$\begin{array}{lll} (i) & C_\Omega(\Delta, D_a, D_d, G_{m,n}) & = \mathbf{F}_q^q \otimes RS_q(q-2-n). \\ (ii) & C_\Omega(\Delta, D_b, D_d, G_{m,n}) & = RS_q(q-2-m) \otimes \mathbf{F}_q^q. \\ (iii) & C_L(\Delta, G_{m,n})^\perp & = C_\Omega(\Delta, D_a, D_d, G_{m,n}) + C_\Omega(\Delta, D_b, D_d, G_{m,n}). \end{array}$$

Par conséquent, le code $C_L(\Delta, G_{m,n})^\perp$ est une somme de deux codes différentiels.

PREUVE. D'après la relation (II.6) page 77, si (i) et (ii) sont vérifiées, alors (iii) l'est également. De plus, par symétrie, (i) et (ii) sont équivalentes. Reste donc à prouver que (i) est vérifiée. Posons

$$\nu := \frac{dx}{\prod_{\alpha \in \mathbf{F}_q}(x-u-\alpha)} \wedge \frac{dy}{\prod_{\beta \in \mathbf{F}_q}(u-\beta)}.$$

Cette 2-forme vérifie les trois propriétés du corollaire II.4.5. Calculons le diviseur de ν. Sur U, on a

$$(\nu_{|U}) = -D_{a|U} - D_{d|U}.$$

De plus, pour tout élément α de $\mathbf{F}_q$, la droite $L_{d,\alpha}$ est linéairement équivalente à $E+F$, donc

$$D_d \sim q(E+F).$$

Par un calcul analogue à celui qui a été effectué dans l'exemple précédent, on montre que

$$(\nu) = (2q-2)E + (q-2)F - D_a - D_d.$$

De fait,

$$\begin{array}{rcl} C_\Omega(\Delta, D_a, D_d, mE+nF) & = & C_L(\Delta, (2q-2-m)E + (q-2-n)F) \\ & = & RS_q(2q-2-m) \otimes RS_q(q-2-n). \end{array}$$

Pour finir, il suffit de constater que si m est compris entre 0 et $q-1$, alors $2q-2-m$ est supérieur à $q-1$ et le code $RS_q(2q-2-m)$ est égal à $\mathbf{F}_q^q$. □

Cette stratégie de réalisation de l'orthogonal est celle qui va motiver le chapitre III, à savoir, si l'on ne peut réaliser l'orthogonal d'un code fonctionnel avec l'aide d'un seul code différentiel, il est peut-être possible de le réaliser comme somme de codes différentiels.

Remarque II.5.5. *Noter que le contre-exemple ci-dessus s'étend aisément en tout dimension supérieure ou égale à 2. En général, l'orthogonal d'un code fonctionnel sur un produit de droites projectives ne se réalise pas comme code fonctionnel sur cette variété.*

II.6 Heuristique, est-ce un problème de super abondance ?

Prenons le temps de commenter les phénomènes étudiés dans les exemples précédents. Pour ce faire, commençons par revenir provisoirement au cas des codes géométriques construits sur des courbes. Soient X une courbe algébrique projective lisse géométriquement intègre sur $\mathbf{F}_q$ munie d'un diviseur G et $D = P_1 + \cdots + P_n$ une somme de points rationnels de X. On sait que dans ce cas, on a systématiquement

$$C_L(D,G)^\perp = C_\Omega(D,G).$$

On démontre l'inclusion $\supseteq$ avec la formule des résidus comme l'inclusion réciproque par un argument d'égalité de dimension. Voyons comment s'obtient cette égalité de dimension. Considérons la suite exacte de faisceaux

$$0 \ \to \mathcal{L}(G-D) \ \to \mathcal{L}(G) \ \to \ \mathcal{L}(G)/\mathcal{L}(G-D) \ \to 0.$$

Le terme le plus à droite de cette suite exacte est un faisceau gratte-ciel. Il est donc flasque et son H^1 est trivial (cf [Har77] ch 3.5 théorème 5.1). On en déduit la suite exacte longue en cohomologie,

$$0 \ \to \ L(G-D) \ \to L(G) \ \to \mathbf{F}_q^n \ \to H^1(X, \mathcal{L}(G-D)) \ \to H^1(X, \mathcal{L}(G)) \ \to 0.$$

Si l'on note $E^\vee$ le dual d'un espace vectoriel E, alors par dualité de Serre, on a la suite exacte

$$0 \ \to \ L(G-D) \ \to L(G) \ \to \mathbf{F}_q^n \ \to \Gamma(X, \Omega^1(G-D))^\vee \ \to \Gamma(X, \Omega^1(G))^\vee \ \to 0.$$

La somme alternée des dimensions permet de conclure,

$$\underbrace{\dim L(G-D) - \dim L(G)}_{=\dim C_L(D,G)} + n - \underbrace{(\dim \Gamma(X, \Omega^1(G-D)) - \dim \Gamma(X, \Omega^1(G))}_{=\dim C_\Omega(D,G)} = 0.$$

Revenons à présent aux surfaces. L'étude des deux exemples triviaux que sont le plan projectif et le produit de deux droites projectives peut encourager le raisonnement heuristique suivant.

Si l'on arrive a avoir l'égalité de dimension dans le cas où $S = \mathbf{P}^2$ c'est parce que sur cette surface la super abondance[3] d'un faisceau inversible est nulle (cf [Har77] théorème III.5.1). Il est donc tentant de penser que l'écart de dimension entre le code différentiel et l'orthogonal du code fonctionnel est lié à la super abondance.

En réalité ce raisonnement est trop rapide. Pour s'en convaincre nous allons essayer de reproduire le raisonnement effectué ci-dessus, dans le cas des surfaces. Soit $\mathcal{I}_\Delta$ le faisceau d'idéaux associé à la sous-variété finie $\mathrm{Supp}(\Delta)$. Concernant la construction fonctionnelle il faut considérer la suite exacte courte de faisceaux suivante,

$$0 \to \ \mathcal{L}(G) \otimes \mathcal{I}_\Delta \to \ \mathcal{L}(G) \ \to \ \mathcal{L}(G)/\left(\mathcal{L}(G) \otimes \mathcal{I}_\Delta\right) \to 0.$$

[3] La dimension du H^1

En remarquant qu'ici encore le dernier faisceau est un faisceau gratte-ciel on en déduit la suite exacte longue

$$0 \to\ L(G)_\Delta\ \to\ L(G)\ \to\ \mathbf{F}_q^n\ \to\ H^1(S, \mathcal{L}(G) \otimes \mathcal{I}_\Delta)\ \to\ H^1(S, \mathcal{L}(G))\ \to 0,$$

où $L(G)_\Delta$ désigne l'ensemble des fonctions de $L(G)$ qui s'annulent en tous les points du support de Δ. Ici la dualité de Serre ne permet pas de traduire tous les H^1 sous formes d'espaces de 2-formes différentielles. Il faut donc considérer une seconde suite exacte de faisceaux, à savoir :

$$0 \to\ \Omega^2(G-D) \otimes \mathcal{I}_\Delta \to\ \Omega^2(G-D)\ \to\ \Omega^2(G-D)/\left(\Omega^2(G-D) \otimes \mathcal{I}_\Delta\right) \to 0.$$

On en déduit la suite exacte longue en cohomologie

$$\begin{array}{rcccl} 0 \to\ \Gamma(S, \Omega^2(G-D))_\Delta & \to & \Gamma(S, \Omega^2(G-D)) & \to & \mathbf{F}_q^n \\ & \to & H^1(S, \Omega^2(G-D) \otimes \mathcal{I}_\Delta) & \to & H^1(S, \Omega^2(G-D))\ \to\ 0, \end{array}$$

où $\Gamma(S, \Omega^2(G-D))_\Delta$ décrit l'ensemble des éléments de $\Gamma(S, \Omega^2(G-D))$ qui s'annulent en tous les éléments du support de Δ. Les faisceaux $\mathcal{L}(G)$ et $\Omega^2(G-D)$ sont inversibles. Donc, si la surface est $\mathbf{P}^2$, leurs H^1 sont nuls et les suites exactes longues donnent les égalités

$$\begin{array}{rcl} \dim H^1(\mathbf{P}^2, \mathcal{L}(G) \otimes \mathcal{I}_\Delta) & = & \operatorname{codim} C_L(\Delta, G) \\ \dim H^1(\mathbf{P}^2, \Omega^2(G-D) \otimes \mathcal{I}_\Delta) & = & \operatorname{codim} C_\Omega(D, G). \end{array}$$

Il faut ensuite réussir à prouver que la somme des dimensions de ces deux H^1 est égale à n. Dans tous les cas, le fait que les super abondances des faisceaux inversibles soient nulles ne suffit pas pour démontrer l'égalité de dimension espérée.

Ce qui semble réellement faire défaut à cette construction différentielle est moins la super abondance que l'asymétrie des constructions. Plus précisément, le fait qu'en dimension supérieure ou égale à 2, les points et les diviseurs sont des objets de dimension différente. Du fait de cette asymétrie, on doit introduire une paire de diviseur Δ-convenable pour construire des codes différentiels, cette dernière étant complètement absente dans la construction fonctionnelle.

Conclusion

Nous avons étendu la construction différentielle de codes correcteurs aux surfaces. Nous avons également montré que, tout comme dans la cas des courbes, les codes fonctionnels et différentiels sur les surfaces appartiennent à la même classe de codes. en d'autres termes, tout code fonctionnel sur une surface se réalise comme code différentiel sur cette même surface et réciproquement.

La différence majeure avec la théorie des courbes est que, à S et Δ fixés **l'orthogonal d'un code fonctionnel n'est pas fonctionnel (donc différentiel) en général**. Ces codes appartiennent à une "classe différente" de codes construits à partir de S. Voloch et Zarzar avaient d'ailleurs déjà constaté ce phénomène dans [VZ05]. Dans cet article, les auteurs remarquent en effet que les codes sur les surfaces qu'ils étudient sont LDPC[4]. De ce fait, ces codes sont très différents de leur orthogonal, ce qui n'est pas le cas des codes géométriques construits à partir de courbes algébriques.

Aussi, l'étude des codes différentiels sur les surfaces et des exemples que nous avons traités offrent des perspectives intéressantes. À ce titre, nous conclurons ce chapitre par deux questions.

Question 1. *Peut-on estimer les paramètres des codes qui sont l'orthogonal de codes fonctionnels ?*

[4] *Low Density Parity-Check*, c'est-à-dire admettant une matrice de parité creuse (voir chapitre V).

Question 2. *Si l'orthogonal d'un code fonctionnel ne peut se réaliser comme un code différentiel associé à une paire de diviseurs Δ-convenables, peut-on le réaliser comme somme de tels codes ?*

La question 1 donne lieu aux travaux présentés dans le chapitre IV. Concernant la question 2, une réponse partielle sera donnée dans le chapitre III.

Chapitre III

Théorème de réalisation

"Entre les désirs et leurs réalisations
s'écoule toute une vie humaine."

Schopenhauer

Dans ce chapitre, nous allons nous intéresser la question 2 posée à la fin du chapitre II. À savoir : *l'orthogonal $C_L(\Delta, G)^\perp$ d'un code fonctionnel sur une surface S se réalise-t-il comme somme de codes différentiels ?* Une réponse positive à cette question sera donnée sous certaines conditions sur la surface S et le diviseur G. Ces conditions sont décrites dans la section III.1 ci-dessous.

III.1 Contexte

Dans ce chapitre, S désigne une surface projective lisse géométriquement intègre au-dessus de $\mathbf{F}_q$. On se donne également un diviseur $\mathbf{F}_q$-rationnel G sur S et une famille $P_1, \ldots, P_n$ de points rationnels de S. On appelle Δ, le 0-cycle

$$\Delta := P_1 + \cdots + P_n.$$

Notation III.1.1. *Soit H un hyperplan de $\mathbf{P}^r$, pour toute sous-variété X de $\mathbf{P}^r$ non contenue dans H, on note L_X la classe d'équivalence linéaire du diviseur $\varphi^* H$ sur X, où φ désigne l'injection canonique $\varphi : X \hookrightarrow \mathbf{P}^r$. De même, la classe canonique sur X sera notée K_X.*

À partir de la section III.4, on supposera (hypothèse III.4) que S est intersection complète dans un espace projectif $\mathbf{P}^r$ et que G est linéairement équivalent à mL_S pour un certain entier naturel m.

III.2 Sous-Δ-convenance

Dans cette section, nous allons définir une notion très proche de celle de Δ-convenance et qui continue à vérifier le résultat du théorème d'orthogonalité (théorème II.4.1).

Commençons par justifier ce besoin d'introduire une nouvelle notion. La question 2 posée à la fin du chapitre II était en partie motivée par l'étude de la surface $\mathbf{P}^1 \times \mathbf{P}^1$. En effet, on a vu en section II.5.2 que l'orthogonal d'un code fonctionnel sur cette surface peut se réaliser comme somme de deux codes différentiels. Tout cela encourage à essayer de construire l'orthogonal d'un code fonctionnel en "plusieurs morceaux". Pour ce faire, on peut par exemple chercher des mots de code ou des sous-codes de $C_L(\Delta, G)^\perp$ dont le support est strictement contenu dans $\{1, \ldots, n\}$. De plus l'exemple des quadriques elliptiques du chapitre précédent

(section II.3.5) montre que la construction d'un diviseur Δ-convenable devient vite ardue, lorsque la surface S est plus compliquée que le plan projectif ou le produit de deux droites projectives. Ces deux arguments motivent la définition de paires de diviseurs sous-Δ-convenables qui suit.

Définition III.2.1 (Diviseurs sous-Δ-convenables)**.** *Une paire (D_a, D_b) est dite sous-Δ-convenable si elle est Λ-convenable pour un 0-cycle Λ vérifiant*

$$0 \leq \Lambda \leq \Delta.$$

Remarque III.2.2. *La sous-Δ-convenance peut également s'énoncer de la façon suivante. Soient D_a et D_b deux diviseurs dont l'intersection ensembliste des supports est finie et D le diviseur $D := D_a + D_b$. La paire (D_a, D_b) est sous-Δ-convenable si et seulement si elle vérifie les propriétés suivantes.*

(i) Pour tout point géométrique $P \in \overline{S}$, l'application $res^2_{D_a,P} : \overline{\Omega^2(-D)}_P \to \mathbf{F}_q$ est $\mathcal{O}_{\overline{S},P}$-linéaire.

(ii) L'application ci-dessus est nulle pour tout point géométrique P non contenu dans le support de Δ.

Rappelons que les diviseurs Δ-convenables ont été introduits pour obtenir une relation d'orthogonalité entre codes fonctionnels et codes différentiels (voir théorème II.4.1). Le lemme qui suit et dont la démonstration est immédiate montre que les paires de diviseurs sous-Δ-convenables sont en ce sens presque aussi intéressantes que les paires Δ-convenables.

Lemme III.2.3. *Soit S une surface lisse géométriquement intègre au-dessus de $\mathbf{F}_q$ et munie d'un diviseur G et d'un 0-cycle Δ qui est la somme formelle de points rationnels de S. Soit enfin (D_a, D_b) une paire sous-Δ-convenable de diviseurs, alors*

$$C_\Omega(\Delta, D_a, D_b, G) \subseteq C_L(\Delta, G)^\perp.$$

III.3 Sur les notions de réalisation

La question de la réalisation de l'orthogonal d'un code fonctionnel en utilisant des 2-formes rationnelles peut se poser de deux façons différentes. Il y a d'abord la question 2 posée à la fin du chapitre II que nous rappelons ici.

Question 2. *Si l'orthogonal d'un code fonctionnel ne peut se réaliser comme un code différentiel associé à une paire de diviseurs (sous-)Δ-convenable, peut-on le réaliser comme somme de tels codes ?*

On peut également se poser une question sensiblement différente, à savoir la question 2bis qui suit. Le théorème de réalisation énoncé en section III.4 y répondra sous certaines conditions.

Question 2bis. *Étant donné un mot de code c appartenant à $C_{L,S}(\Delta, G)^\perp$, existe-t-il une paire de diviseurs (sous-) Δ-convenable (D_a, D_b) et une 2-forme ω appartenant à $\Gamma(S, \Omega^2(G - D_a - D_b))$ et telle que*

$$c = res^2_{D_a,\Delta}(\omega) \ ?$$

Le fait qu'un code est un espace vectoriel de dimension finie permet de montrer aisément qu'une réponse positive à la question 2bis entraîne une réponse positive à la question 2. La réciproque de cette dernière assertion est également vraie, c'est ce que montre la proposition qui suit. Les problèmes posés par les questions 2 et 2bis sont donc équivalents.

Proposition III.3.1. *Soient c_D et c_E deux mots du code $C_L(\Delta, G)^\perp$. Supposons qu'il existe deux paires de diviseurs sous-Δ-convenables (D_a, D_b) et (E_a, E_b) et deux 2-formes*

rationnelles ω_D et ω_E appartenant respectivement aux espaces $\Gamma(S, \Omega^2(G - D_a - D_b))$ et $\Gamma(S, \Omega^2(G - E_a - E_b))$ et telles que

$$c_D = res^2_{D_a,\Delta}(\omega_D) \quad et \quad c_E = res^2_{E_a,\Delta}(\omega_E).$$

Alors, il existe une paire sous-Δ-convenable de diviseurs (F_a, F_b) et une 2-forme rationnelle ω_F appartenant à $\Gamma(S, \Omega^2(G - F_a - F_b))$ telle que

$$c_D + c_E = res^2_{F_a,\Delta}(\omega_F).$$

La preuve de proposition III.3.1 est une conséquence des lemmes III.3.2 et III.3.3 qui suivent.

Lemme III.3.2. *Soient (D_a, D_b) et (E_a, E_b) deux paires sous-Δ-convenables de diviseurs sur S telles que les supports des diviseurs $D := D_a + D_b$, $E := E_a + E_b$ et G n'ont pas de composante irréductible commune. Soient également ω_D et ω_E deux 2-formes rationnelles sur S appartenant respectivement à $\Gamma(S, \Omega^2(G - D))$ et $\Gamma(S, \Omega^2(G - E))$. Alors, il existe une paire sous-Δ-convenable de diviseurs (F_a, F_b) telle que la 2-forme $\omega_D + \omega_E$ appartienne à $\Gamma(S, \Omega^2(G - F))$ où F désigne le diviseur $F := F_a + F_b$. De plus,*

$$res^2_{F_a,\Delta}(\omega_D + \omega_E) = res^2_{D_a,\Delta}(\omega_D) + res^2_{E_a,\Delta}(\omega_E).$$

Lemme III.3.3. *Soit (D_a, D_b) une paire de diviseurs sous-Δ-convenable et ω un élément de $\Gamma(S, \Omega^2(G - D))$ où D désigne le diviseur $D := D_a + D_b$. Soient également $C_1, \ldots, C_s$ une famille de courbes irréductibles sur S deux à deux distinctes. Alors, il existe une paire sous-Δ-convenable (D'_a, D'_b) vérifiant les propriétés suivantes.*

(1) Les diviseurs D_a et D'_a (resp. D_b et D'_b) sont linéairement équivalents.

(2) Le support de $D' := D'_a + D'_b$ ne contient aucune des courbes $C_1, \ldots, C_s$.

(3) Pour toute 2-forme ω appartenant à $\Gamma(S, \Omega^2(G - D))$, il existe une 2-forme ω' appartenant à $\Gamma(S, \Omega^2(G - D'))$ telle que

$$res^2_{D_a,\Delta}(\omega) = res^2_{D'_a,\Delta}(\omega').$$

Preuve de la proposition III.3.1. Si les supports des diviseurs $D := D_a + D_b$ et $E := E_a + E_b$ sont sans composante commune, on applique le lemme III.3.2. Sinon on se ramène à cette situation grâce au lemme III.3.3. □

Preuve du lemme III.3.2. **Étape 1. Construction de $(\mathbf{F_a}, \mathbf{F_b})$.** Les diviseurs D_a^+, E_a^+, D_b^+, E_b^+ sont respectivement de la forme

$$\begin{array}{rclcrcl} D_a^+ & := & m_1V_1 + \cdots + m_kV_k & \qquad & E_a^+ & := & n_1W_1 + \cdots + n_lW_l \\ D_b^+ & := & r_1X_1 + \cdots + r_pX_p & & E_b^+ & := & s_1Y_1 + \cdots + s_qY_q, \end{array}$$

où les V_i, W_i, X_i, Y_i sont des courbes $\mathbf{F}_q$-irréductibles. Par hypothèse, ces courbes sont deux à deux disjointes. Nous allons construire une paire de diviseurs effectifs (F_a^+, F_b^+). Le diviseur F_a^+ fera apparaître tous les V_i (resp. W_j), pôles de ω_D (resp. ω_E) avec pour coefficient l'ordre de ce pôle. Le diviseur F_b^+ est construit exactement de la même manière en remplaçant les V_i par des X_i et les W_j par des Y_j. C'est-à-dire que l'on pose

$$F_a^+ := \sum_{i=1}^{k} \max(0, -\mathrm{val}_{V_i}(\omega_D))\, V_i + \sum_{j=1}^{l} \max(0, -\mathrm{val}_{W_j}(\omega_E))\, W_j \qquad \text{(III.1)}$$

et

$$F_b^+ := \sum_{i=1}^{p} \max(0, -\mathrm{val}_{X_i}(\omega_D))\, X_i + \sum_{j=1}^{q} \max(0, -\mathrm{val}_{Y_j}(\omega_E))\, Y_j. \qquad \text{(III.2)}$$

Soit ω_F, la 2-forme définie par $\omega_F := \omega_D + \omega_E$. On rappelle que les composantes irréductibles des supports des diviseurs D_a, D_b, E_a et E_b sont par hypothèse deux à deux disjointes. Par

conséquent, il existe un diviseur **effectif** R dont le support n'a aucune composante irréductible commune avec les supports de D_a^+, D_b^+, E_a^+ et E_b^+ et tel que

$$(\omega_F) = G + R - F_a^+ - F_b^+.$$

On pose enfin

$$F_b^- := R, \quad \text{et} \quad F_a^- := 0$$

et on a donc

$$F_a := F_a^+ \quad \text{et} \quad F_b := F_b^+ - F_b^-.$$

Le diviseur $F := F_a + F_b$ est donc construit de telle sorte que l'on ait exactement

$$(\omega_F) = G - F.$$

Le fait que ω_F est un élément de $\Gamma(S, \Omega^2(G-F))$ est immédiat. Il reste à montrer que la paire (F_a, F_b) est sous-Δ-convenable.

Étape 2. Sous-Δ-convenance de $(\mathbf{F_a}, \mathbf{F_b})$. Soit P un point de $\overline{S}$, il existe un germe de fonction f_P appartenant à $\overline{\mathcal{L}(G)}_P$ tel que le diviseur de la 2-forme $f_P\omega_F$ au voisinage de P soit égal à $-F$. Alors, le germe de 2-forme $f_P\omega_F$ au voisinage de P engendre la fibre $\overline{\Omega^2(-F)}_P$ comme $\mathcal{O}_{\overline{S},P}$-module. En effet, la 2-forme $f_P\omega_F$ est construite de telle sorte que pour tout germe de courbe C au voisinage de P on ait

$$\mathrm{val}_C(f_P\omega_F) = \min_{\mu_P \in \overline{\Omega^2(-F)}_P} \mathrm{val}_C(\mu_P).$$

Un germe de 2-forme $\mu_P \in \overline{\Omega^2(-F)}_P$ s'obtient donc par multiplication de $f_P\omega_F$ par une fonction régulière au voisinage de P.

Montrons que l'application $\mathrm{res}^2_{F_a,P}$ restreinte à $\overline{\Omega^2(-F)}_P$ est $\mathcal{O}_{\overline{S},P}$-linéaire. Soit $\varphi \in \mathcal{O}_{\overline{S},P}$. On a

$$\mathrm{res}^2_{F_a,P}(\varphi f_P\,\omega_F) = \underbrace{\mathrm{res}^2_{F_a,P}(\varphi f_P\,\omega_D)}_{I_D} + \underbrace{\mathrm{res}^2_{F_a,P}(\varphi f_P\,\omega_E)}_{I_E}. \tag{III.3}$$

Nous allons montrer que $I_D = \varphi(P)\mathrm{res}^2_{D_a,P}(f_P\omega_D)$. Commençons par faire deux remarques.

(1) D'après la construction de F_a^+ en (III.1), certaines des courbes V_i peuvent ne pas apparaître dans l'expression de ce diviseur. C'est ce qui arrive pour une courbe V_i donnée si la valuation de ω_D le long de V_i est positive. Dans ce cas, le 2-résidu de ω_D en P le long de V_i est nul. De plus, on rappelle que φ est régulière au voisinage de P et que, par hypothèse, le support de G n'a pas de composante commune avec ceux de D et E. Par conséquent, si ω_D n'a pas de pôle le long de V_i, alors le 2-résidu en P le long de V_i de $\varphi f_P\,\omega_D$ est nul.

(2) L'hypothèse "les supports des diviseurs D_a, D_b, E_a, E_b n'ont pas de composante irréductible commune" implique que pour tout i, les 2-formes ω_D et $\varphi f_P\,\omega_D$ n'ont pas de pôle le long de W_i, donc ont un 2-résidu nul en P le long de cette courbe.

On déduit de ces deux remarques que

$$I_D = \sum_{i=1}^{k} \mathrm{res}^2_{V_i,P}(\varphi f_P\,\omega_D). \tag{III.4}$$

Enfin, on rappelle que la définition de 2-résidu en un point le long d'un diviseur ne dépend que du support de ce dernier (voir définition I.7.10 et la mise en garde qui suit). Par conséquent,

$$I_D = \mathrm{res}^2_{D_a,P}(\varphi f_P\,\omega_D) = \varphi(P)\mathrm{res}^2_{D_a,P}(f_P\,\omega_D), \tag{III.5}$$

la seconde égalité étant une conséquence de la sous-Δ-convenance de (D_a, D_b) et du fait que $f_P\,\omega_D$ appartient à $\overline{\Omega^2(-D)}_P$ comme $\mathcal{O}_{\overline{S},P}$-module. Le cas de la quantité I_E de l'expression (III.3) se traite de façon rigoureusement identique. On obtient

$$I_E = \varphi(P)\mathrm{res}^2_{E_a,P}(f_P\,\omega_E). \tag{III.6}$$

En combinant les relations (III.3), (III.5) et (III.6), on aboutit à

$$\mathrm{res}^2_{F_a,P}(\varphi f_P\,\omega_F) = \varphi(P)\mathrm{res}^2_{F_a,P}(f_P\,\omega_F),$$

ce qui permet de conclure quant à l'$\mathcal{O}_{\overline{S},P}$-linéarité de l'application $\mathrm{res}^2_{F_a,P}$ restreinte à $\overline{\Omega^2(-F)}_P$.

Enfin, comme les paires (D_a, D_b) et (E_a, E_b) sont sous-Δ-convenables, pour tout point P de $\overline{S}$ n'appartenant pas au support de Δ, les applications $\mathrm{res}^2_{D_a,P}$ et $\mathrm{res}^2_{E_a,P}$ sont identiquement nulles respectivement sur $\overline{\Omega^2(-D)}_P$ et $\overline{\Omega^2(-E)}_P$. D'après (III.3), (III.5) et (III.6), on en déduit que l'application $\mathrm{res}^2_{F_a,P}$ est identiquement nulle sur $\overline{\Omega^2(-F)}_P$. D'après la remarque III.2.2, la paire (F_a, F_b) est sous-Δ-convenable. □

Pour finir, il nous reste à démontrer le lemme III.3.3.

Preuve du lemme III.3.3. **Étape 0. Mise en place.**

Quitte à réorganiser l'ordre des courbes $C_1, \ldots, C_s$, on peut supposer que $C_1, \ldots, C_l$ sont contenues dans le support de D_a, que $C_{l+1}, \ldots, C_m$ sont dans le support[1] de D_b et $C_{m+1}, \ldots, C_s$ ne sont contenues dans aucun des deux supports. Nous allons montrer comment *bouger* D_a afin d'éviter ces courbes. On pourra alors conclure d'après la remarque II.3.7 en appliquant un raisonnement identique à D_b.

Étape 1. Déplacement de $\mathbf{D_a}$.

Pour *déplacer* le support de D_a, nous allons utiliser la proposition B.0.2 énoncée en annexe B qui est un analogue du *moving lemma*. Commençons par établir une liste de points à éviter.

Soit $\mathcal{C}$, l'ensemble des courbes formé de la réunion des composantes irréductibles des supports de D_a, D_b et G et des courbes $C_1, \ldots, C_s$. L'ensemble $\mathcal{P}$ est un ensemble de points fermés de S formé de tous les points d'intersection (ensembliste) de deux éléments de $\mathcal{C}$. Si l'un des éléments C de $\mathcal{C}$ n'en intersecte aucun autre, on choisit arbitrairement un point de C que l'on ajoute dans $\mathcal{P}$, afin que ce dernier contienne au moins un point de chaque courbe appartenant à $\mathcal{C}$.

Soit i un entier appartenant à $\{1, \ldots, l\}$, on partitionne $\mathcal{P}$ en deux ensembles $\mathcal{P}_1^i$ et $\mathcal{P}_2^i$. L'ensemble $\mathcal{P}_1^i$ désigne l'ensemble des points P qui appartiennent à C_i et $\mathcal{P}_2^i$ désigne son complémentaire dans $\mathcal{P}$. D'après la proposition B.0.2, il existe une fonction f_i, vérifiant les propriétés suivantes.

(*i*) La fonction f_i est une équation locale de C_i au voisinage de tout point $P \in \mathcal{P}_1^i$.

(*ii*) Le support du diviseur de f_i évite tout point $P \in \mathcal{P}_2^i$.

On pose

$$m_i := \mathrm{val}_{C_i}(D_a),$$

et on définit la fonction rationnelle φ sur S par

$$\varphi := f_1^{m_1} \ldots f_l^{m_l}.$$

De la même manière, on pose

$$\widetilde{D} := D - (m_1 C_1 + \cdots + m_l C_l) + C_{m+1} + \cdots + C_s,$$

[1] On rappelle que par définition de la sous-Δ-convenance, les supports de D_a et D_b n'ont pas de composante irréductible commune. La courbe C_i ne peut donc pas être contenue dans l'intersection ensembliste des supports de D_a et D_b.

et on partitionne $\mathcal{P}$ en $\mathcal{P}_1$ et $\mathcal{P}_2$, formés respectivement des points de $\mathcal{P}$ contenus et non contenus dans le support de $\widetilde{D}$. D'après la proposition B.0.2, il existe une fonction rationnelle g qui est une équation locale de $\widetilde{D}$ au voisinage de tout élément de $\mathcal{P}_1$ et dont le support du diviseur évite tous les éléments de $\mathcal{P}_2$. Posons alors,

$$h := \frac{\varphi}{g+\varphi}, \quad \text{et} \quad D'_a := D_a - (h).$$

Montrons que le diviseur de la fonction h est de la forme

$$(h) = m_1 C_1 + \cdots + m_l C_l + R,$$

et que le support de R ne contient aucun élément de $\mathcal{C}$. Le diviseur (h) est la différence des diviseurs (φ) et $(\varphi+g)$. Par construction, le diviseur (φ) est de la forme

$$(\varphi) = m_1 C_1 + \cdots + m_l C_l + R_1,$$

où le support de R_1 évite tout élément de $\mathcal{P}$, donc ne contient aucun élément de $\mathcal{C}$. Quant à la fonction $\varphi+g$, elle est par construction régulière au voisinage de tout élément de $\mathcal{P}$. Elle l'est donc sur un ouvert admettant une intersection non vide avec tout élément de $\mathcal{C}$ et n'admet donc aucune de ces courbes comme pôle. De plus, pour toute courbe C appartenant à $\mathcal{C}$, l'une des fonctions φ ou g s'annule le long de C et l'autre ne s'annule pas. De fait, C ne peut être un zéro de $\varphi+g$. Par conséquent, le support du diviseur D'_a ne contient aucune des courbes $C_1, \ldots, C_s$ ni aucune composante des supports de D_b et G.

Étape 2. Sous-Delta-convenance de $(\mathbf{D'_a}, \mathbf{D_b})$.

Soit ω une section globale de $\Omega^2(G-D)$, on vérifie aisément que $h\omega$ est une section globale de $\Omega^2(G-D'_a-D_b)$. Nous allons montrer que pour toute 2-forme ω appartenant à $\Gamma(S, \Omega^2(G-D))$, on a

$$\mathrm{res}^2_{D_a,\Delta}(\omega) = \mathrm{res}^2_{D'_a,\Delta}(h\omega), \tag{III.7}$$

ce qui nous permettra de démontrer à la fois la propriété 3 de l'énoncé et le fait que la paire (D'_a, D_b) est sous-Δ-convenable. Commençons par noter que, d'après la remarque II.3.3 du chapitre II, la relation (III.7) et équivalente à

$$\mathrm{res}^2_{D_b,\Delta}(\omega) = \mathrm{res}^2_{D_b,\Delta}(h\omega). \tag{III.8}$$

Soient donc $\overline{C}$ une composante géométrique irréductible du support de D_b et u un élément de $\mathcal{O}_{\overline{S},\overline{C}}$ dont la restriction à $\overline{C}$ est un élément séparant de $\overline{\mathbf{F}}_q(\overline{C})/\overline{\mathbf{F}}_q$. Nous allons montrer que

$$(u)\mathrm{res}^1_{\overline{C}}(\omega) = (u)\mathrm{res}^1_{\overline{C}}(h\omega). \tag{III.9}$$

D'après la proposition I.5.14 du chapitre I, si l'on montre que la relation (III.9) ci-dessus est vérifiée par toute composante géométrique du support de D_b, alors la relation (III.8) sera vérifiée.

Soit v une uniformisante de l'anneau $\mathcal{O}_{\overline{S},\overline{C}}$. On rappelle que le complété $\mathfrak{m}_{\overline{S},\overline{C}}$-adique de $\overline{\mathbf{F}}_q(\overline{S})$ s'identifie au corps $\mathcal{K}_u((v))$, où $\mathcal{K}_u$ est une copie de $\overline{\mathbf{F}}_q(\overline{C})$ contenue dans $\widehat{\mathcal{O}}_{\overline{S},\overline{C}}$ (voir chapitre I section I.4.3). Posons

$$m := \mathrm{val}_{\overline{C}}(D_b).$$

Comme ω est un section globale de $\Omega^2(G-D)$, on sait que sa valuation le long de $\overline{C}$ est supérieure à $-m$. La construction des fonctions φ et g nous assure que ces dernières sont de valuations respectives 0 et m le long de $\overline{C}$. On en déduit donc

$$h\omega = \frac{\varphi}{\varphi+g}\omega = \frac{1}{1+g\varphi^{-1}}\omega = \left(1 - g\varphi^{-1} + \cdots\right)\omega.$$

La 2-forme ω étant de valuation supérieure à $-m$ le long de $\overline{C}$ et la fonction $g\varphi^{-1}$ de valuation m, on en déduit que les termes de la forme $(-1)^n(g\varphi^{-1})^n\omega$ de la série ci-dessus sont de valuation positive le long de $\overline{C}$. Leur contribution dans le calcul du (u)-1-résidu de ω le long de $\overline{C}$ est donc nulle. La relation (III.9) est bien vérifiée.

On conclut la preuve en appliquant un raisonnement identique à D_b. □

III.4 Construction de l'orthogonal d'un code fonctionnel

Le but de cette section est de démontrer le théorème suivant. On se place dans le contexte donné en section III.1 et on suppose de plus vérifiée l'hypothèse suivante.

Hypothèse III.4. *La surface S est plongée dans un espace projectif $\mathbf{P}^r_{\mathbf{F}_q}$ dans lequel elle est* ***intersection complète****. De plus ; le diviseur G est linéairement équivalent à l'intersection de S avec une hypersurface de $\mathbf{P}^r$. En d'autres termes et en utilisant la notation III.1.1, il existe un entier naturel m tel que $G \sim mL_S$.*

Théorème III.4.1 (Théorème de réalisation)**.** *Sous l'hypothèse III.4, soit c un mot du code $C_{L,S}(\Delta, G)^\perp$. Alors, il existe une paire de diviseurs (D_a, D_b) et une 2-forme ω appartenant à l'espace des sections globales $\Gamma(S, \Omega^2(G - D_a - D_b))$, tels que*

$$c = res^2_{D_a,\Delta}(\omega).$$

De plus, on peut choisir le couple (D_a, D_b) de telle sorte que

(1) la paire (D_a, D_b) vérifie le critère de la proposition II.3.8 ;

(2) D_a soit égal à une courbe lisse irréductible plongée dans S et $D_a \sim n_a L_S$ pour un certain entier strictement positif n_a ;

(3) $D_b \sim n_b L_S$ pour un certain entier n_b.

Avant de démontrer ce théorème, énonçons un corollaire immédiat de ce dernier.

Corollaire III.4.2. *Sous l'hypothèse III.4, il existe une famille finie $(D_a^{(1)}, D_b^{(1)}), \ldots, (D_a^{(s)}, D_b^{(s)})$ de paires de diviseurs sous-Δ-convenables telles que*

$$C_{L,S}(\Delta, G)^\perp = \sum_{i=1}^{s} C_{\Omega,S}(\Delta, D_a^{(i)}, D_b^{(i)}, G).$$

Preuve du corollaire III.4.2. L'inclusion vers la gauche est une conséquence immédiate du lemme III.2.3. Pour ce qui est de l'inclusion réciproque, le théorème III.4.1 implique que $C_{L,S}(\Delta, G)^\perp$ est égal à la somme de tous les codes de la forme $C_{\Omega,S}(\Delta, D_a, D_b, G)$ tels que (D_a, D_b) est sous-Δ-convenable. Comme un code est un espace de dimension finie, on peut extraire de cette somme une somme finie. □

Le lemme qui suit est la première étape de la preuve du théorème III.4.1.

Lemme III.4.3. *Sous l'hypothèse III.4, soit C une courbe lisse absolument irréductible plongée dans S obtenue par l'intersection de S avec une hypersurface de $\mathbf{P}^r$. On suppose également que C n'est pas contenue dans le support[2] de G. Soit G^* le tiré en arrière de G par l'inclusion canonique $C \hookrightarrow S$. Alors l'application de restriction à C*

$$r : \Gamma(S, \mathcal{L}(G)) \to \Gamma(C, \mathcal{L}(G^*))$$

est surjective.

Preuve. La courbe C est lisse donc normale. C'est de plus une intersection complète dans $\mathbf{P}^r$. Ainsi, d'après [Har77] II.8 ex 4, la courbe C est projectivement normale. Cela signifie par définition, que l'algèbre graduée des coordonnées homogènes de C pour le plongement i :

[2] Notons que si C est contenue dans le support de G, on peut remplacer ce dernier par un autre élément du système linéaire $|G|$, cette condition n'est donc pas vraiment problématique. D'une façon générale, on peut éviter ce type de restriction en adoptant un langage plus *faisceautique*. En effet, le tiré en arrière de G sur C n'a pas de sens quand C est contenue dans le support de G, le tiré en arrière de $\mathcal{L}(G)$ lui, est toujours bien défini (voir [Har77] II.5). Le défaut de ce point de vue est que dans ce cas, les sections de $i^*\mathcal{L}(G)$ ne peuvent plus être vues comme des restrictions à C de fonctions sur S. Nous avons donc préféré conserver une approche plus *fonctionnelle*.

$C \hookrightarrow \mathbf{P}^r$, est intégralement close. D'après [Har77] II.5 ex 14, cette algèbre graduée s'identifie à

$$\bigoplus_{m\in\mathbf{N}} \Gamma(C, i^*\mathcal{O}_{\mathbf{P}^r}(m))$$

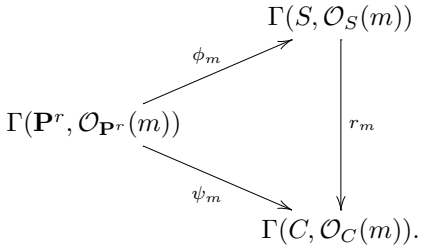
et sa clôture intégrale à

$$\bigoplus_{m\in\mathbf{N}} \Gamma(C, \mathcal{O}_C(m)).$$

La normalité projective de C entraîne que pour tout entier naturel m, l'application de restriction

$$\psi_m : \Gamma(\mathbf{P}^r, \mathcal{O}_{\mathbf{P}^r}(m)) \to \Gamma(C, \mathcal{O}_C(m))$$

est surjective (cf [Har77] II.5 ex 14 (d)). Par ailleurs, le diviseur G^* est linéairement équivalent à mL_C, donc le faisceau $\mathcal{L}(G^*)$ est isomorphe à $\mathcal{O}_C(m)$. Considérons le diagramme commutatif



La surjectivité de l'application ψ_m entraîne celle de l'application r_m. □

Le second ingrédient de la preuve du théorème III.4.1 est le théorème 3.3 de l'article [Poo04] de Poonen. Il s'agit d'un théorème "à la Bertini" pour des variétés sur des corps finis. Énonçons ce résultat.

Théorème III.4.4 (Poonen 2004)**.** *Soit X un sous-schéma quasi-projectif lisse de $\mathbf{P}^r$ de dimension $m \geq 1$ au-dessus de $\mathbf{F}_q$ et soit $F \subset X$ un ensemble fini de points fermés. Alors, il existe une hypersurface lisse et géométriquement intègre $H \subset \mathbf{P}^r$ telle que l'intersection $H \cap X$ est lisse, de dimension $m-1$ et contient F.*

Remarque III.4.5. *À la suite de ce théorème, l'auteur remarque que, si X est projective et géométriquement connexe, alors $H \cap X$ l'est également d'après [Har77] corollaire III.7.9.*

Démonstration du théorème III.4.1. **Étape 1. Construction de $\omega, \mathbf{D_a}$ et $\mathbf{D_b}$.** Soient $i_1, \ldots, i_s$ les indices du support du mot de code c. D'après le théorème III.4.4 et la remarque III.4.5, il existe une hypersurface H contenue dans $\mathbf{P}^r$ telle que l'intersection $C := H \cap S$ est une courbe projective lisse connexe contenant les points $P_{i_1}, \ldots, P_{i_s}$. On note G^* le tiré en arrière de G sur C par l'inclusion canonique $C \hookrightarrow S$ et Λ_C le diviseur

$$\Lambda_C := P_{i_1} + \cdots + P_{i_s} \ \in \mathrm{Div}_{\mathbf{F}_q}(C).$$

D'après le lemme III.4.3, l'application $\Gamma(S, \mathcal{L}(G)) \to \Gamma(C, \mathcal{L}(G^*))$ est surjective et induit donc une application surjective de codes

$$r : C_{L,S}(\Delta, G) \to C_{L,C}(\Lambda_C, G^*).$$

Soit à présent $c^* := (c_{i_1}, \ldots, c_{i_s})$ le mot de code poinçonné obtenu en ne conservant que les coordonnées du mot c d'indices $i_1, \ldots, i_s$. La surjectivité de l'application r entraîne que le mot c^* est un élément de $C_{L,C}(\Lambda_C, G^*)^\perp$. On sait également que

$$C_{L,C}(\Lambda_C, G^*)^\perp = C_{\Omega,C}(\Lambda_C, G^*).$$

Par conséquent, il existe une 1-forme μ sur C appartenant à $\Gamma(C, \Omega^1(G^* - \Lambda_C))$ et telle que $c^* = \mathrm{res}_{\Lambda_C}(\mu)$, où res_{Λ_C} désigne l'application

$$\mathrm{res}_{\Lambda_C} : \left\{ \begin{array}{ccc} \Gamma(C, \Omega^1(G^* - \Lambda_C)) & \to & \mathbf{F}_q^s \\ \omega & \mapsto & (\mathrm{res}_{P_{i_1}}(\omega), \ldots, \mathrm{res}_{P_{i_s}}(\omega)). \end{array} \right.$$

Notons que, par hypothèse, les coordonnées du mot de code poinçonné c^* sont toutes non nulles (il a été construit en éliminant les coordonnées nulles du mot c). De ce fait,

$$\forall k \in \{1, \ldots, s\}, \quad \mathrm{val}_{P_{i_k}}(\mu) = -1. \tag{III.10}$$

Soit à présent μ_* un relevé arbitraire de μ sur S, c'est-à-dire une 1-forme rationnelle sur S vérifiant $\mu_{*|C} = \mu$. Soit également v une uniformisante de l'anneau $\mathcal{O}_{S,C}$. Posons alors,

$$\omega := \mu_* \wedge \frac{dv}{v}.$$

Le diviseur de ω est de la forme $(\omega) = -C + R$, où R est un diviseur sur S dont le support ne contient pas la courbe C. Pour finir, on pose

$$D_a := C \quad \text{et} \quad D_b := G - R.$$

Ainsi ω est bien un élément de $\Gamma(S, \Omega^2(G - D_a - D_b))$. De plus, comme le 1-résidu de ω le long de C est μ, on en déduit

$$\mathrm{res}^2_{D_a,\Delta}(\omega) = \mathrm{res}^2_{C,\Delta}(\omega) = c.$$

Étape 2. Sous-Δ-convenance de $(\mathbf{D_a}, \mathbf{D_b})$. Soit Λ, le 0-cycle sur S défini par

$$\Lambda := P_{i_1} + \cdots + P_{i_s}.$$

Nous allons montrer que la paire (D_a, D_b) est Λ-convenable. Pour ce faire, nous allons utiliser le critère de la proposition II.3.8. Si l'on note i l'inclusion canonique $i : C \hookrightarrow S$, d'après le lemme II.3.12 on a l'égalité de diviseurs sur C :

$$(\mu) = i^*(G - D_b).$$

Comme μ est un élément de $\Gamma(C, \Omega^1(G - \Lambda_C))$, on en déduit que $i^* D_b \leq \Lambda$, ce qui implique l'inégalité de 0-cycles sur S suivante :

$$D_a \cap D_b \leq \Lambda. \tag{III.11}$$

Soit alors P, un point de $\overline{S}$ non contenu dans le support de Λ et n'appartenant pas à la courbe $\overline{C}$ (c'est-à-dire au support de D_a). Dans cette situation, D_a peut jouer le rôle[3] de D_* en P et comme D_a est nul au voisinage de ce point, le critère y est trivialement vérifié. Soit à présent un point P de $\overline{C}$ non contenu dans le support de Λ. Comme $\overline{C}$ est une courbe irréductible lisse, le diviseur $D_a = C$ peut encore jouer le rôle de D_*. D'après la relation (III.11), la multiplicité d'intersection de D_a avec D_b en P est négative, le critère est donc vérifié en ce point. En un point P du support de Λ, le diviseur D_a joue encore le rôle de D_* et l'inégalité (III.11) implique que la multiplicité d'intersection de D_a et D_b en P est inférieure ou égale à 1. D'après la relation (III.10) et le lemme II.3.12 l'inégalité est en fait un égalité. Le couple (D_a, D_b) vérifie donc bien le critère de Λ-convenance.

Étape 3. Classes d'équivalence linéaire de $\mathbf{D_a}$ et $\mathbf{D_b}$. D'après la construction de la courbe $C = D_a$ dans l'étape 1, on sait qu'il existe un entier naturel non nul n_a tel que

$$D_a \sim n_a L_S.$$

[3] Voir proposition II.3.8 pour une description de D^*.

D'après [Har77] II.8 ex 4(e), la classe canonique d'une sous-variété X intersection complète de $\mathbf{P}^r$ est de la forme $K_X \sim kL_X$ où k dépend du degré des hypersurfaces dont l'intersection est égale à X. Soit donc k l'entier tel que $K_S \sim kL_S$. Comme le diviseur de ω vérifie

$$(\omega) = G - D_a - D_b,$$

et que $G \sim mL_S$, on en déduit que

$$D_b \sim (m - k - n_a)L_S.$$

□

Remarque III.4.6. *La courbe C qui définit le diviseur D_a dans la preuve du théorème III.4.1 est construite de manière à interpoler les points correspondant au support du mot de code que l'on peut réaliser. Noter que l'on aurait pu tout aussi bien choisir une bonne fois pour toute une courbe interpolant tous les points du support de Δ et ne travailler que sur cette dernière.*

Notons au passage qu'une telle approche permet de démontrer qu'un code fonctionnel construit sur S à partir d'un diviseur $G \sim mL_S$ se réalise toujours comme code sur une courbe C contenue dans S. Ce fait n'a rien de nouveau, Pellikaan, Shen et Van Wee montrent dans [PSV91] que tout code correcteur se réalise comme code sur une courbe. L'exploitation potentielle de ce fait en vue d'une étude du code fonctionnel sera discutée en section III.6.

III.5 Discussion autour du théorème de réalisation

Quelques commentaires s'imposent au sujet du théorème III.4.1 et de sa démonstration. D'abord, il est important de noter que la preuve de ce théorème de réalisation n'est malheureusement pas constructive. En effet, cette dernière repose sur le théorème III.4.4 de Poonen qui n'est lui-même qu'un résultat d'existence. Ce dernier ne donne par exemple aucune information sur le degré minimal de l'hypersurface qui permet de construire le diviseur D_a.

Ensuite, on rappelle que le résultat n'est démontré que sous certaines conditions, à savoir que la surface S est intersection complète et que le diviseur G est linéairement équivalent à mL_S. En fait, ces conditions sont principalement là pour assurer la surjectivité de l'application

$$\Gamma(S, \mathcal{L}(G)) \to \Gamma(C, \mathcal{L}(G^*)).$$

Il s'avère que cette application est fréquemment surjective mais ce n'est pas systématique (un contre-exemple est donné en III.5.1). Les hypothèses du théorème assurent la surjectivité de l'application pour toute courbe lisse obtenue par intersection de S avec une hypersurface. En conclusion, il s'agit de conditions suffisantes, mais absolument pas nécessaires. Il est fort possible que le résultat reste vrai en omettant ces hypothèses, nous n'avons cependant pas été à même de le démontrer dans un cas plus général. L'exemple élémentaire présenté dans la section III.5.1 va confirmer l'aspect non nécessaire de ces hypothèses.

Cela nous amène à poser la question ouverte suivante.

Question 3. *Le résultat du théorème de réalisation reste-t-il vrai si l'on élimine les hypothèses que doivent vérifier S et G ?*

Notons également que le théorème de réalisation (plus exactement le corollaire III.4.2) répond à la question 2 posée page 81 sous certaines hypothèses sur S et G. Cependant, si l'on sait que sous ces hypothèses l'orthogonal d'un code fonctionnel se réalise comme une somme de codes différentiels, la question suivante reste ouverte.

Question 4. *Sous les conditions du corollaire III.4.2, peut-on estimer le nombre de minimal de codes différentiels dont la somme est égale à l'orthogonal d'un code fonctionnel en fonction d'invariants géométriques de la surface ?*

L'exemple qui suit a été suggéré par Antoine Ducros.

III.5.1 Un exemple de réalisation sans que les conditions du théorème de III.4.1 soient vérifiées

Soient S la surface obtenue par l'éclatement de $\mathbf{P}^2$ en un point O et

$$\pi : S \to \mathbf{P}^2,$$

l'éclatement de $\mathbf{P}^2$ en O. Le diviseur G est le diviseur exceptionnel de S et le 0-cycle Δ, la somme des points rationnels de S non contenus dans le support de G. La surface S peut être plongée dans $\mathbf{P}^5$ via le plongement de Segré ([Sha94] I.5.1). Pour ce plongement, S est un intersection complète. Cependant, le diviseur G ne peut s'identifier à une section hyperplane de S pour aucun plongement de cette surface. En effet, il est d'auto-intersection -1, donc ne vérifie pas le critère de Nakai-Moishezon ([Har77] théorème V.1.10). L'espace $\Gamma(S, \mathcal{L}(G))$ est de dimension 1 et ne contient que les fonctions constantes. En effet, comme G est d'auto-intersection négative, il est le seul élément du système linéaire $|G|$ qui est donc de dimension nulle. Par conséquent, la dimension de $\Gamma(S, \mathcal{L}(G))$ est égale à 1. On vérifie ensuite que les constantes sont bien des éléments de cet espace.

Soit à présent L la transformée stricte d'une droite de $\mathbf{P}^2$ passant par O. La courbe L intersecte G transversalement en un unique point Q. Le tiré en arrière G^* de G par l'inclusion canonique de L dans S est égal à Q. De fait, l'espace $\Gamma(L, \mathcal{L}(G^*))$ est de dimension 2 et donc l'application

$$\Gamma(S, \mathcal{L}(G)) \to \Gamma(L, \mathcal{L}(G^*))$$

n'est pas surjective. Montrons maintenant que l'on peut tout de même réaliser tous les mots de $C_L(\Delta, G)^\perp$ comme résidus de 2-formes sur S.

Approche non constructive.

Soit c un mot de $C_L(\Delta, G)^\perp$ et soit Λ le 0-cycle de S correspondant au support de c. Il existe une courbe irréductible lisse C de S qui contient tous les points du support de Λ et dont l'intersection avec G est vide. En effet, cela revient à construire une courbe lisse de $\mathbf{P}^2$ qui interpole une famille finie de points et évite le point O. Le tiré en arrière G^* de G sur C est nul et donc $\Gamma(C, \mathcal{L}(G^*))$ est l'ensemble des fonctions constantes sur C. Par conséquent, l'application

$$\Gamma(S, \mathcal{L}(G)) \to \Gamma(C, \mathcal{L}(G^*))$$

est surjective et on peut effectuer la construction effectuée dans la démonstration du théorème III.4.1.

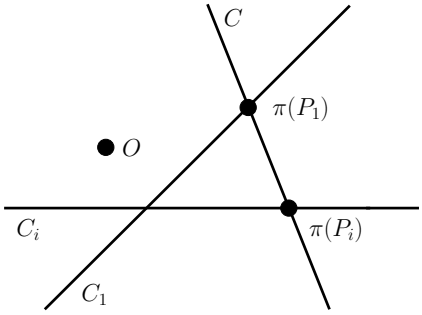
Approche constructive.

Le code $C_{L,S}(\Delta, G)$ est le code de répétition pure et de longueur $n = q^2+q$. Son orthogonal est donc un code de dimension $n-1$. On note $c_2, \ldots, c_n$ les mots de la forme

$$c_i := (1, 0, \ldots, 0, -1, 0, \ldots, 0),$$

le "-1" apparaissant en i-ème position. La famille $(c_2, \ldots, c_n)$ est une base de $C_L(\Delta, G)^\perp$. D'après la proposition III.3.1, il suffit de réaliser ces $n-1$ mots pour montrer que tout mot de C est réalisable.

Étape 1. Soit donc i un entier compris entre 2 et n et supposons que les points $\pi(P_1)$ et $\pi(P_i)$ ne sont pas alignés avec O dans $\mathbf{P}^2$. On appelle C, la droite de $\mathbf{P}^2$ reliant $\pi(P_1)$ et $\pi(P_i)$. On choisit deux droites C_1 et C_i dans $\mathbf{P}^2$ distinctes de C et contenant respectivement $\pi(P_1)$ et $\pi(P_i)$ et évitant le point O.



On rappelle que la classe canonique dans $\mathbf{P}^2$ est égale à $-3L$, où L désigne la classe d'équivalence linéaire des droites du plan projectif. De fait, le diviseur $-C-C_1-C_i$ est canonique, il existe donc une 2-forme ω sur $\mathbf{P}^2$ telle que

$$(\omega) := -C - C_1 - C_2.$$

D'après le lemme II.3.12, la 1-forme $\mathrm{res}^1_C(\omega)$ sur C n'a de pôles qu'en $\pi(P_1)$ et $\pi(P_i)$ et ces pôles sont simples. Elle a donc des résidus non nuls en ces points et d'après la formule des résidus, ils sont opposés. De ce fait, quitte à multiplier ω par un scalaire non nul, on a

$$\mathrm{res}^2_{C,P_1}(\omega) = 1 \quad \text{et} \quad \mathrm{res}^2_{C,P_i}(\omega) = -1.$$

De plus, la 2-forme ω n'a ni zéro ni pôle au voisinage de O. Donc, d'après le lemme I.7.7 la 2-forme $\pi^*\omega$ sur S est de valuation 1 le long du diviseur exceptionnel, on a donc

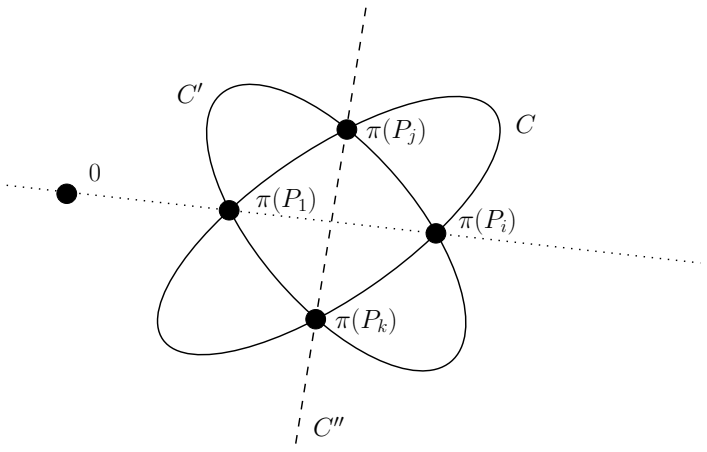
$$(\pi^*\omega) = G - \widetilde{C} - \widetilde{C}_1 - \widetilde{C}_2.$$

On pose

$$\Lambda_i := P_1 + P_i, \quad D_a := \widetilde{C} \quad \text{et} \quad D_b := \widetilde{C}_1 + \widetilde{C}_2$$

et on vérifie aisément que (D_a, D_b) est Λ_i-convenable (on peut par exemple voir qu'il satisfait le critère de la proposition II.3.8). De fait, le mot c_i est réalisé par la 2-forme $\pi^*\omega$.

Étape 2. Si maintenant les points $\pi(P_1)$ et $\pi(P_k)$ sont alignés avec O. On choisit deux autres points rationnels $\pi(P_j)$ et $\pi(P_k)$ de $\mathbf{P}^2$ tels que les points $\pi(P_1)$, $\pi(P_i)$, $\pi(P_j)$ et $\pi(P_k)$ soient en position générale (trois d'entre eux ne sont pas alignés). Il existe au moins deux coniques rationnelles C et C' distinctes interpolant ces quatre points et évitant le point O. En effet, le système linéaire des coniques interpolant ces points est de dimension 1, donc même si le corps de base est $\mathbf{F}_2$, il y a au moins 3 éléments dans ce système et un seul d'entre eux interpole 0. On appelle C'' la droite reliant $\pi(P_j)$ et $\pi(P_k)$.



Le diviseur $-C-C'+C''$ est linéairement équivalent à $-3L$, c'est donc un diviseur canonique et il existe une 2-forme ω sur $\mathbf{P}^2$ vérifiant

$$(\omega) = -C - C' + C''.$$

Avec le lemme II.3.12 on montre que $\pi(P_1)$ et $\pi(P_i)$ sont les seuls pôles de la 1-forme $\mathrm{res}^1_C(\omega)$ sur C. On en déduit que, quitte à multiplier ω par un scalaire inversible, on a

$$\mathrm{res}^2_{C,P_1}(\omega) = 1 \quad \text{et} \quad \mathrm{res}^2_{C,P_i}(\omega) = -1.$$

Par ailleurs, ω n'a ni zéro ni pôle au voisinage de O, donc $\pi^*\omega$ vérifie

$$(\pi^*\omega) = G - \widetilde{C} - \widetilde{C}' + \widetilde{C}''.$$

On finit en posant

$$\Lambda_i := P_1 + P_i, \quad D_a := \widetilde{C} \quad \text{et} \quad D_b := \widetilde{C}' + \widetilde{C}''$$

et en vérifiant (grâce au critère de la proposition II.3.8) que la paire (D_a, D_b) ainsi construite est bien Λ_i-convenable.

III.6 Une autre application possible des théorèmes "à la Bertini"

Cette section, qui conclut le chapitre III, a pour but de montrer qu'une réponse à une certaine question ouverte pourrait permettre dans certaines situations de minorer la distance minimale du code fonctionnel $C_L(\Delta, G)$. L'objectif est d'utiliser la constatation de la remarque III.4.6. Avant d'y arriver ouvrons une parenthèse historique sur la théorie des codes géométriques.

III.6.1 Les travaux de Pellikaan, Shen et Wee

Dans [PSV91], les auteurs classent les codes correcteurs en WAG (*Weakly Algebraic-Geometric*), AG (*Algebraic-Geometric*) et SAG (*Strongly Algebraic-Geometric*). Les codes WAG sont les codes Γ admettant une représentation géométrique, c'est-à-dire les codes pour lesquels il existe une courbe C, un diviseur G sur C et une famille $P_1, \ldots, P_n$ de points rationnels de X tels que

$$\Gamma = C_{L,C}(D, G) \quad \text{avec} \quad D := P_1 + \cdots + P_n.$$

Les codes AG sont les codes WAG qui admettent une représentation vérifiant $n > \deg(G)$. Quant aux SAG ce sont les WAG admettant une représentation telle que $n > \deg(G) > 2g_C - 2$.

L'un des résultats majeurs de l'article [PSV91] est le théorème 2 qui affirme que tout code est WAG. Dans la suite de l'article, les auteurs donnent des exemples de codes qui ne le sont pas. Ils signalent par exemple que les codes de Golay binaires ne sont pas AG ([PSV91] corollaire 9).

Le problème des codes est que toutes leurs réalisations comme codes sur des courbes donne une distance construite de Goppa nulle. Par conséquent, une représentation géométrique du code ne fournit aucune information sur sa distance minimale. En ce qui concerne les codes fonctionnels sur une surface algébrique, notre objectif va être de savoir si l'on peut disposer d'une représentation AG.

III.6.2 Le cas des codes fonctionnels sur une surface

Jusqu'à la fin du chapitre, nous nous plaçons sous l'hypothèse III.4 énoncée page 89. Reprenons la remarque III.4.6. Le théorème III.4.4 de Poonen nous assure l'existence d'une courbe lisse géométriquement intègre $C \subset S$ obtenue par intersection de S avec une hypersurface de $\mathbf{P}^r$ et qui interpole tous les points $P_1, \ldots, P_n$ du support de Δ. Puis, d'après le lemme III.4.3, l'application de restriction à C

$$\Gamma(S, \mathcal{L}(G)) \to \Gamma(C, \mathcal{L}(G^*))$$

est surjective. Si l'on note D le diviseur sur C défini par $D := P_1 + \cdots + P_n$, alors la surjectivité de l'application ci-dessus entraîne que les codes $C_{L,S}(\Delta, G)$ et $C_{L,C}(D, G^*)$ sont identiques. Le code $C_{L,S}(\Delta, G)$ s'identifie donc à un code sur une courbe algébrique. Si G est linéairement équivalent à mL_S, alors G^* es linéairement équivalent à mL_C. Le tout est de savoir quel est le degré de L_C. Ce degré est le nombre de points géométriques de l'intersection de C avec un hyperplan géométrique générique, c'est donc le degré de la courbe C pour son plongement dans $\mathbf{P}^r$. Enfin, au vu de la construction de C, son degré n'est autre que le degré de S multiplié par le degré de l'hypersurface H telle que $C = H \cap S$. Par conséquent, une estimation suffisamment fine du degré de l'hypersurface H permettrait de minorer la distance minimale du code $C_{L,S}(\Delta, G)$.

Question 5 (Arithmétique)**.** *Soient X une variété projective lisse géométriquement intègre sur un corps fini $\mathbf{F}_q$ et $P_1, \ldots, P_n$, une famille de points fermés de X. Peut-on évaluer explicitement ou majorer de façon précise le plus petit entier d tel qu'il existe au moins une hypersurface définie sur $\mathbf{F}_q$ de degré inférieur ou égal à d qui interpole tous les P_i et dont l'intersection schématique avec X soit une sous-variété lisse géométriquement intègre de codimension 1 ?*

Dans [Poo04], Poonen montre que de telles hypersurfaces existent et forment même un sous-ensemble de densité positive dans l'ensemble des hypersurfaces de $\mathbf{P}^r$, mais il ne donne aucune information sur le degré minimal d'une telle variété. On est de ce fait assurés de l'existence de l'entier d mais ne dispose d'aucun procédé d'estimation explicite.

Notons que la question 5A (Arithmétique) ne porte que sur les hypersurfaces définies sur $\mathbf{F}_q$. La remarque qui suit assure que l'on peut se poser la question pour les hypersurfaces définies sur $\overline{\mathbf{F}}_q$.

Remarque III.6.1. *Soit $\mathbf{F}_{q^m}$ une extension de $\mathbf{F}_q$ et S' la surface $S' := S \times_{\mathbf{F}_q} \mathbf{F}_{q^m}$. Notons Δ' et G' pour les tirés en arrière respectifs de Δ et G sur S'. On dispose alors de l'égalité de codes*

$$C_{L,S}(\Delta, G) \otimes_{\mathbf{F}_q} \mathbf{F}_{q^m} = C_{L,S'}(\Delta', G').$$

En particulier, ces codes ont la même distance minimale.

Par conséquent, on peut chercher une réalisation du code $C_{L,S}(\Delta, G) \otimes \mathbf{F}_{q^m}$ pour une extension quelconque de $\mathbf{F}_q$, ce qui ramène notre problème à la question suivante.

Question 5 (Géométrique)**.** *Soit X une variété projective irréductible lisse définie sur $\overline{\mathbf{F}}_q$ et $P_1, \ldots, P_n$ une famille de points de X. Peut-on évaluer explicitement ou majorer de façon précise le plus petit entier d tel qu'il existe au moins une hypersurface H de degré inférieur ou égal à d, qui contienne tous les P_i et telle que $H \cap X$ soit une sous-variété lisse de codimension 1 de X ?*

Cette dernière question ressemble fortement à un théorème "à la Bertini". En effet, si l'on note $\mathfrak{d}_d$ le système linéaire des sections hyperplanes de X de degré d et $\mathfrak{d}'_d$ le sous-système linéaire de $\mathfrak{d}_d$ des sections hyperplanes de X interpolant les P_i, alors la question 5G (Géométrique) se traduit par : *le système linéaire $\mathfrak{d}'_d$ possède-t-il un élément irréductible lisse ?*

Les questions 5A et 5G restent ouvertes. Notons que l'article [KA79] d'Altman et Kleiman donne une piste pour tenter d'y répondre. Les commentaires ci-dessous ont été suggérés par Steven L. Kleiman.

Théorème III.6.2 (Altman, Kleiman 1979)**.** *Soient k un corps infini, X un sous-schéma de l'espace projectif $\mathbf{P}^r_k$ et Z un sous-schéma de X. Soit $\mathcal{I}_{\overline{Z}}$ le faisceau d'idéaux de $\mathcal{O}_{\mathbf{P}^r}$ associé à l'adhérence de Z dans X. Soit d un entier tel que $\mathcal{I}_{\overline{Z}}(d)$ est engendré par ses sections globales. Supposons que $X \setminus \overline{Z}$ est lisse, alors l'intersection de X par des hypersurfaces génériques indépendantes de degré $d+1$ est lisse hors de $\overline{Z}$.*

Dans notre situation, soit Z la réunion des points $P_1, \ldots, P_n$. Supposons que l'on connaisse un entier d tel que $\mathcal{I}_Z(d)$ soit engendré par ses sections globales et que pour tout i, le faisceau $(\mathcal{I}_Z/\mathfrak{m}_{P_i}\mathcal{I}_Z)(d)$ soit engendré par les sections globales de $\mathcal{I}_Z(d)$. Alors, une section globale générique de $\mathcal{I}_Z(d)$ sera envoyée sur un élément non nul de $\mathfrak{m}_{P_i}/\mathfrak{m}_{P_i}^2$ et sera donc non singulière en ce point, elle sera également lisse hors de Z d'après le théorème ci-dessus. Le problème reste en tous les cas de trouver un tel entier d ou une borne supérieure pour celui-ci.

Chapitre IV

Orthogonal d'un code fonctionnel

Dans ce chapitre, nous allons travailler sur le problème de la minoration de la distance minimale de l'orthogonal d'un code fonctionnel. Nous allons présenter deux approches. La première s'applique aux codes fonctionnels construits à partir de variétés projectives de dimension quelconque et pas seulement aux surfaces. Elle est de plus indépendante de tous les résultats précédemment énoncés et ne fait pas intervenir la notion de formes différentielles. La seconde approche, elle, utilise les résultats obtenus dans le chapitre III.

Pour le reste, ce chapitre ne peut être considéré comme totalement abouti. Il ouvre cependant un certain nombre de problèmes de géométrie algébrique sur les systèmes linéaires dont la résolution permettrait d'obtenir des minorations de la distance minimale de l'orthogonal d'un code fonctionnel.

Notations

Nous allons reprendre dans ce chapitre un certain nombre de notations utilisées dans le chapitre III. En particulier, on rappelle que si X est une sous-variété fermée d'un espace projectif, on note L_X la classe d'équivalence linéaire d'une section hyperplane de X et K_X la classe canonique sur X.

IV.1 Première approche

Cette approche consiste en fait à n'utiliser que des méthodes d'algèbre linéaire relativement élémentaires. Dans cette section, N désigne un entier naturel non nul et k un corps quelconque. On se donne une variété projective lisse géométriquement intègre X intersection complète dans un espace projectif $\mathbf{P}^N$ et munie d'un diviseur G et d'un 0-cycle Δ. On suppose également qu'il existe un entier naturel m tel que $G \sim mL_X$ et que Δ est une somme de points rationnels de X qui évitent le support de G.

IV.1.1 Notion de m-généralité

Pour alléger les notations, on désignera l'espace $\Gamma(\mathbf{P}_k^N, \mathcal{O}_{\mathbf{P}_k^N}(m))$ des formes homogènes de degré m sur $\mathbf{P}_k^N$ par $\mathcal{F}_m^N$. Enfin, pour tout point rationnel P de $\mathbf{P}^N$, on note ev_P l'application d'*évaluation* décrite dans la définition D.1.1 (voir annexe D).

Définition IV.1.1. *On dit que les points $P_1, \ldots, P_r \in \mathbf{P}^N(k)$ sont liés en degré m ou m-liés si les formes linéaires $ev_{P_1}, \ldots, ev_{P_r}$ sont liées dans le dual $(\mathcal{F}_m^N)^\vee$ de $\mathcal{F}_m^N$. Dans le cas contraire, si ces formes linéaires forment une famille libre de $(\mathcal{F}_m^N)^\vee$, on dit que ces points sont en position m-générale.*

La définition ci-dessus peut s'interpréter de façon géométrique, comme le montre le lemme qui suit.

Lemme IV.1.2. *Une famille de r points $P_1, \ldots, P_r$ de $\mathbf{P}^N$ est en position m-générale, si et seulement si pour tout entier $i \in \{1, \ldots, r\}$, il existe une hypersurface de degré m qui contient les points $P_1, \ldots, \widehat{P_i}, \ldots, P_r$ et évite P_i.*

PREUVE. C'est un exercice élémentaire de dualité en algèbre linéaire. □

Remarque IV.1.3. *La notion de 1-généralité correspond à la définition classique de position générale. Le plus souvent, dans la littérature, une famille de points de $\mathbf{P}^N$ est dite en position générale si et seulement ces points forment un repère projectif de la variété linéaire projective qu'ils engendrent. Si l'on se donne un entier m, alors une famille de points de $\mathbf{P}^N$ sont en position m-générale si et seulement si leurs images par le m-ème plongement de Veronèse*[1] *sont en position générale au sens classique (décrit ci-dessus) dans $\mathbf{P}^M$ avec* $M = \begin{pmatrix} N+d \\ d \end{pmatrix} - 1$

Remarque IV.1.4. *On aurait pu donner une définition plus générale de ces notions en ne considérant plus seulement des points rationnels de $\mathbf{P}^N$, mais des points fermés et même des points infiniment près*[2] *de $\mathbf{P}^N$. Un tel point de vue étant totalement inutile dans ce qui suit, nous avons choisi de nous restreindre au cas des points rationnels de $\mathbf{P}^N$.*

Exemple IV.1.5. Supposons que $N = 1$, on travaille donc sur la droite projective. Dans ce cas, r points deux à deux distincts $P_1, \ldots, P_r$ sont en position m-générale si et seulement si $r \leq m + 1$. En effet, on peut construire une forme homogène de degré inférieur ou égal à m ayant exactement $r - 1$ racines données.

IV.1.2 Systèmes linéaires de $\mathbf{P}^N$

La notion de m-généralité peut se reformuler en termes de systèmes linéaires. Pour ce faire, on adoptera les notations de [Har77] V.4. Soient m un entier naturel, $\mathfrak{d}$ le système linéaire sur $\mathbf{P}^N$ des hypersurfaces de degré m et $P_1, \ldots, P_r$ une famille de points rationnels de $\mathbf{P}^N$. Pour tout entier naturel $1 \leq i \leq r$, on note $\mathfrak{d}_i$ le sous-système linéaire de $\mathfrak{d}$ des hypersurfaces de degré d contenant les points $P_1, \ldots, \widehat{P_i}, \ldots, P_r$. Selon les notations de [Har77] V.4,

$$\mathfrak{d}_i := \mathfrak{d} - P_1 - \cdots - \widehat{P_i} - \cdots - P_r.$$

En termes de systèmes linéaires, la m-généralité de $P_1, \ldots, P_r$ se formule de la façon suivante. Les points $P_1, \ldots, P_r$ sont en position d-générale si et seulement si pour tout i, le point P_i n'est pas un point base du système linéaire $\mathfrak{d}_i$.

IV.1.3 Lien avec les notions de distance minimale

Munis de ces définitions, la question de la minoration de la distance minimale du code $C_{L,X}(\Delta, G)^\perp$ peut se traduire sous forme d'un problème géométrique.

Proposition IV.1.6. *Soit m un entier tel que $G \sim mL_X$. La distance minimale $d^\perp$ du code $C_{L,X}(\Delta, G)^\perp$ est égale au nombre minimal s de points $P_1, \ldots, P_s$ du support de Δ qui sont m-liés.*

PREUVE. Soit $c = (c_1, \ldots, c_n)$ un mot de $C_L(\Delta, G)^\perp$. Cela signifie que l'application $\varphi_c := c_1 \mathrm{ev}_{P_1} + \cdots + c_n \mathrm{ev}_{P_n}$ est identiquement nulle sur $\Gamma(X, \mathcal{L}(G))$. Comme X est intersection

[1] Voir [Sha94] I.4.4.

[2] C'est-à-dire des points appartenant à une variété obtenue par une séquence d'éclatements de sous-variétés de X. Voir [Har77] V.3.

complète, d'après [Har77] II.8 ex 14, elle est projectivement normale et il y a donc une application surjective

$$f : \Gamma(\mathbf{P}^N, \mathcal{O}_{\mathbf{P}^N}(m)) \to \Gamma(X, \mathcal{L}(G)).$$

L'application $\varphi_c \circ f$ définie sur $\Gamma(\mathbf{P}^N, \mathcal{O}_{\mathbf{P}^N}(m))$ est donc nulle, or ce morphisme n'est autre que $c_1 \mathrm{ev}_{P_1} + \cdots + c_n \mathrm{ev}_{P_n}$ vu comme une forme linéaire sur $\Gamma(\mathbf{P}^N, \mathcal{O}_{\mathbf{P}^N}(m)) = \mathcal{F}_m^N$. □

Cette reformulation du problème de la distance minimale de $C_L(\Delta, G)^\perp$, nous ramène à un problème qui est loin d'être aussi élémentaire qu'il en a l'air. Autant il est aisé de savoir si une famille de points sont indépendants en dimension 1 (voir exemple IV.1.5), autant le problème se complique lourdement en dimension supérieure. En d'autres termes, il est très difficile en dimension supérieure à 2 de décider si une famille de points est en position d-générale ou, ce qui revient au même, de montrer qu'un système linéaire n'a pas d'autres points bases que ceux qu'on lui a assignés. Pour s'en convaincre on peut regarder les démonstrations du chapitre V.4 de [Har77].

IV.1.4 Minorations de la distance minimale de l'orthogonal d'un code fonctionnel

Nous allons utiliser la proposition IV.1.6 pour obtenir deux résultats de minoration de la distance minimale du code $C_L(\Delta, G)^\perp$.

Théorème IV.1.7. *On suppose N supérieur ou égal à 2. Soit m un entier tel que $G \sim mL_X$, alors*

(1) la distance minimale $d^\perp$ du code $C_{L,X}(\Delta, G)^\perp$ vérifie

$$d^\perp \geq m + 2$$

et il y a égalité si et seulement si le support de Δ contient $m+2$ points alignés ;

(2) sinon, si le support de Δ ne contient pas $m+2$ points alignés, alors

$$d^\perp \geq 2m + 2$$

et il y a égalité si et seulement si le support de Δ contient $2m+2$ points sur une même conique plane.

La démonstration du (1) de ce théorème fera appel aux lemmes IV.1.8 et IV.1.9 qui suivent et qui seront démontrés en annexe E.

Lemme IV.1.8. *Soient r et m deux entiers naturels avec $r \geq 1$, alors toute famille de $rm+2$ points rationnels distincts de $\mathbf{P}^N$ appartenant à une même courbe de degré r est m-liée.*

Lemme IV.1.9. *Soit m un entier naturel.*

(1) Si $m+2$ points rationnels distincts de $\mathbf{P}^N$ sont m-liés, alors ils sont alignés.

(2) Tout r-uplet de points rationnels deux à deux distincts de $\mathbf{P}^N$ avec $r \leq m+1$ est en position m-générale.

Démonstration du (1) du théorème IV.1.7. La proposition IV.1.6 et la propriété (2) du lemme IV.1.9 entraînent que la distance minimale du code $C_L(\Delta, G)^\perp$ est supérieure à $m+2$ et qu'une condition nécessaire pour qu'elle soit atteinte est que le support de Δ contienne $m+2$ points alignés. D'après le lemme IV.1.8, cette dernière condition est suffisante. □

Exemple IV.1.10. Si $G \sim L_X$, alors la distance minimale de $C_{L,X}(\Delta, G)^\perp$ est minorée par 3. Cette borne est atteinte dès que le support de Δ contient trois points alignés. Remarquons que la borne est par exemple atteinte dès que X contient une droite rationnelle.

Le point (2) du théorème IV.1.7 se démontre de la même façon que le point (1) en utilisant la proposition IV.1.6, le lemme IV.1.8 et le lemme IV.1.11 énoncé ci-dessous. Nous renvoyons le lecteur à l'annexe E pour une démonstration de ce dernier.

Lemme IV.1.11. *Soient m et r deux entiers naturels tels que $r \leq 2m+1$.*

(1) Une famille de r points distincts de $\mathbf{P}^N$ telle que $m+2$ d'entre eux sont non alignés est en position m-générale.

(2) Soit $P_1, \ldots, P_{2m+2}$ un $(2m+2)$-uplet de points rationnels distincts de $\mathbf{P}^N$ tels que $m+2$ d'entre eux ne sont pas alignés. Alors, ces points sont m-liés, si et seulement s'ils appartiennent à une même conique plane.

Peut-on aller plus loin ?

Une généralisation naturelle (mais fausse) du théorème IV.1.7 serait : *"soient m, s deux entiers naturels, supposons que pour tout $r < s$, un $(rm+2)$-uplet de points du support de Δ n'est jamais contenu dans une courbe de degré r, alors $d^\perp \geq sm+2$."*

Malheureusement, ce résultat est faux. En effet, d'après la proposition IV.1.6, un tel résultat impliquerait que $sm+1$ points de $\mathbf{P}^N$ tels que pour tout $r < s$, un $(rm+2)$-uplet d'entre eux n'est jamais contenu dans une courbe de degré r, sont en position m-générale. Or, si $s = 3$ et $m = 3$, cela signifierait que 10 points de $\mathbf{P}^2$ tels que 5 d'entre eux sont non alignés et 8 d'entre eux ne sont pas sur une même conique sont toujours en position 3-générale. Or d'après [Har77] corollaire V.4.5, on peut construire un 9-uplet de points 3-liés vérifiant ces propriétés. Un tel 9-uplet de points est construit en prenant les points d'intersection de deux cubiques réduites sans composante irréductible commune. Ces configurations de points provenant d'intersections de N hypersurfaces dans $\mathbf{P}^N$ sont difficiles à repérer et compliquent les démonstrations de m-généralité lorsque l'on veut améliorer les lemmes IV.1.9 et IV.1.11.

En conclusion, on sait que les deux premières configurations minimales de points rationnels m-liés dans $\mathbf{P}^N$ sont

(i) $m+2$ points alignés ;

(ii) $2m+2$ points sur une même conique plane.

Nous laissons une question ouverte.

Question 6. *Quelles sont les configurations minimales suivantes ?*

IV.1.5 Applications

Le théorème IV.1.7 permet d'obtenir des minorations assez fines de la distance minimale de l'orthogonal du code $C_{L,X}(\Delta, G)^\perp$ dans le cas où l'entier m tel que $G \sim mL_X$ est petit. Commençons par étudier le cas bien connu où X est une courbe.

Courbes algébriques planes, comparaison avec la distance minimale construite de Goppa

Soit X une courbe algébrique projective plane lisse de degré $d \geq 2$ et définie sur $\mathbf{F}_q$. Soient m un entier naturel et G un diviseur sur X linéairement équivalent à mL_X. Soient enfin $P_1, \ldots, P_n$ une famille de points rationnels de X qui évitent le support de G et D le diviseur $D := P_1 + \cdots + P_n$. On rappelle que le genre de X s'obtient par la formule

$$g_X = \frac{(d-1)(d-2)}{2}$$

et que l'orthogonal du code fonctionnel $C_L(D, G)$ est le code différentiel $C_\Omega(D, G)$. Par ailleurs, on rappelle également que la distance minimale $d^\perp$ du code $C_\Omega(D, G)$ (qui est égal à $C_L(D, G)^\perp$) vérifie

$$d^\perp \geq \deg(G) - (2g_X - 2).$$

La quantité $\deg(G) - (2g_X - 2)$ est appelée *distance construite de Goppa* et notée $\delta^\perp$.

La courbe X est supposée plane et lisse, elle est donc irréductible. Ainsi, comme $d \geq 2$, alors X ne contient pas plus de d points géométriques alignés. Par conséquent, nous allons distinguer les cas $0 \leq m \leq d-2$ et $m \geq d-1$.

- **Si $\mathbf{0 \leq m \leq d-2}$**, alors le théorème IV.1.7 (1) nous fournit la minoration

$$d^\perp \geq m+2.$$

  Quant à la distance construite de Goppa, on peut l'exprimer en fonction de m et d. En effet, comme $G \sim mL_X$, on en déduit que le degré de G est md et

$$\delta^\perp = md - (d-1)(d-2) + 2.$$

  Faisons la différence de ces deux minorants de $d^\perp$.

$$m+2-(md-(d-1)(d-2)+2) = m - md + (d-1)(d-2) = (d-1)(d-2-m).$$

  En conclusion, la minoration fournie par le théorème IV.1.7 (1) est meilleure que la distance construite de Goppa si $m < d-2$. Elle est en particulier nettement meilleure lorsque m est petit.
- **Si $\mathbf{m \geq d-1}$**, alors, d'après le théorème de Bezout, $m+2$ points de X ne sont jamais alignés. Le théorème IV.1.7 (2) fournit la minoration

$$d^\perp \geq 2m+2.$$

  La différence entre ce minorant de $d^\perp$ et la distance construite de Goppa est

$$2m+2-\delta^\perp = (d-2)(d-1-m).$$

  Comme m est supposée supérieure à $d-1$, la différence ci-dessus est toujours négative et donc la distance construite de Goppa fournit une meilleure minoration de $d^\perp$.

Conclusion. Dans ce contexte des courbes planes, les techniques développées en section IV.1.4 fournissent une meilleure minoration de la distance minimale de $C_L(D,G)^\perp = C_\Omega(D,G)$ que celle fournie par la distance construite de Goppa si et seulement si

$$m \leq d-2.$$

Surfaces de $\mathbf{P}^3$

Soit S une surface de $\mathbf{P}^3$ de degré d définie sur $\mathbf{F}_q$. Soient également m un entier naturel, G un diviseur sur S tel que $G \sim mL_S$ et Δ un 0-cycle de la forme $\Delta = P_1 + \cdots + P_n$ où les P_i sont des points rationnels de S qui évitent le support de G. On note de nouveau $d^\perp$, la distance minimale du code $C_{L,S}(\Delta, G)^\perp$. Tout comme dans le paragraphe précédent, le théorème IV.1.7 fournit les minorations suivantes.

(*i*) Pour tout m, on a $d^\perp \geq m+2$.

(*ii*) Si de plus $m \geq d-1$ et que S ne contient pas de droite rationnelle, alors $d^\perp \geq 2m+2$.

Exemple IV.1.12. Soit S, une surface cubique lisse de $\mathbf{P}^3$. Soit L un diviseur sur S donné par une section hyperplane de S et $G := mL$ avec $m \in \mathbf{N}$. On choisit enfin comme 0-cycle Δ, la somme des points rationnels de S qui évitent le support de G. On note $d^\perp(m)$ la distance minimale du code $C_{L,S}(\Delta, mL)^\perp$. Les résultats de la section IV.1.4 nous donnent

$$\begin{array}{rcl} d^\perp(1) & \geq & 3; \\ d^\perp(2) & \geq & \begin{cases} 4 & \text{si } S \text{ contient une droite rationnelle;} \\ 6 & \text{sinon.} \end{cases} \end{array}$$

Dans le premier cas la borne est atteinte seulement si le support de Δ contient trois points alignés. Nous verrons au chapitre V que ce phénomène est très fréquent et que ce code possède en général de nombreux mots de poids 3. Dans le dernier cas, la borne inférieure n'est atteinte que si le support de Δ contient 6 points appartenant à une même conique plane (éventuellement réductible).

Remarque IV.1.13. *Remarquons que la classification des surfaces cubiques lisses réalisée par Swinnerton-Dyer dans [SD67] assure l'existence de cubiques ne contenant pas de droites rationnelles. Cela fait d'ailleurs partie des exemples introduits par Zarzar et Voloch dans [VZ05].*

Exemple IV.1.14. On reprend les mêmes notations que dans l'exemple IV.1.12, mais cette fois, S est une surface lisse de degré 4. On obtient alors les minorations

$$\begin{array}{lllll} (i) & d^{\perp}(1) & \geq & 3; & \\ (ii) & d^{\perp}(2) & \geq & 4; & \\ (iii) & d^{\perp}(3) & \geq & \left\{ \begin{array}{ll} 5 & \text{si } S \text{ contient une droite rationnelle et } \sharp\, \mathbf{F}_q \geq 5; \\ 8 & \text{sinon.} \end{array} \right. \end{array}$$

Dans le cas (i) (resp. (ii)), la borne est atteinte seulement si S contient 3 (resp. 4) points alignés. Dans le dernier cas, la borne n'est atteinte que si le support de Δ contient 8 points appartenant à une même conique plane.

Remarque IV.1.15. *En ce qui concerne le cas (iii) de l'exemple précédent, dans [Sha94] théorème I.6.9, on montre qu'une surface cubique contient toujours au moins une droite géométrique (elle en contient même 27 quand elle est lisse) et qu'une surface générique de degré supérieur à 4 ne contient pas de droite géométrique. Ainsi, en général, si S est une surface de degré 4, la distance minimale de $C_{L,S}(\Delta, 3L)$ est supérieure ou égale à 8.*

IV.2 Seconde approche, un problème ouvert

Dans cette section nous revenons au contexte classique, à savoir celui des surfaces algébriques. Cette *seconde approche* ne fournira pas à proprement parler de minoration de la distance minimale de l'orthogonal d'un code fonctionnel. Il ne s'agit donc pas d'une section réellement aboutie, mais d'une ouverture vers des problèmes de géométrie algébrique qui auraient d'intéressantes applications à la théorie des codes correcteurs d'erreurs.

L'objectif étant d'utiliser les résultats du chapitre III, nous allons nous replacer dans le contexte de ce dernier. À savoir, S désigne une surface projective lisse géométriquement intègre, qui est intersection complète dans un espace projectif $\mathbf{P}^r$. On se donne également un entier naturel m et un diviseur G vérifiant $G \sim mL_S$, où L_S désigne la classe d'équivalence linéaire d'une section de S par un hyperplan de $\mathbf{P}^r$. Enfin, $P_1, \ldots, P_n$ désignent des points rationnels de S et Δ leur somme.

Exploitation du théorème de réalisation

D'après le théorème de réalisation (théorème III.4.1), pour tout mot de code $c \in C_L(\Delta, G)^{\perp}$, il existe un couple sous-Δ-convenable de diviseurs (D_a, D_b) et une 2-forme ω vérifiant

$$(\omega) = G - D_a - D_b \quad \text{et telle que} \quad c = \mathrm{res}^2_{D_a,\Delta}(\omega). \tag{IV.1}$$

De plus, le diviseur D_a est une courbe lisse géométriquement intègre provenant de l'intersection de S avec une hypersurface de $\mathbf{P}^r$. Il existe donc un entier naturel n_a tel que $D_a \sim n_a L_S$. Par conséquent, dans ce qui suit nous nous autoriserons l'abus de langage consistant à désigner par D_a à la fois le diviseur et la courbe irréductible sous-jacente. Enfin, le théorème de réalisation affirme qu'il existe un entier relatif n_b tel que $D_b \sim n_b L_S$.

La 2-forme ω est de valuation supérieure ou égale à -1 le long de la courbe D_a, le 1-résidu de ω le long de D_a est donc bien défini. On pose

$$\mu := \mathrm{res}^1_{D_a}(\omega) \in \Omega^1_{\mathbf{F}_q(D_a)/\mathbf{F}_q}$$

et d'après le lemme II.3.12, pour tout point géométrique P de D_a, on a

$$\mathrm{val}_P(\mu) = m_P(D_a, G - D_b).$$

Par conséquent, si l'on note D^* le tiré en arrière sur D_a d'un diviseur D sur S dont le support ne contient pas D_a, alors le diviseur de μ s'écrit

$$(\mu) = G^* - D_b^*. \tag{IV.2}$$

Soit Λ_c le diviseur sur la courbe D_a correspondant au support du mot de code c, on a

$$(\mu) \geq G^* - \Lambda_C$$

et on déduit de cette inégalité et de (IV.2) que $\Lambda_C \geq D_b^*$. On a de plus,

$$w(c) = \deg(\Lambda_C) \quad \text{et} \quad \deg(D_b^*) = D_a.D_b,$$

où $w(.)$ désigne le poids de Hamming d'un mot de code et $D.D'$ le produit d'intersection de deux diviseurs sur S. On en déduit la relation

$$w(c) \geq D_a.D_b = n_a n_b L_S^2. \tag{IV.3}$$

Soient k et m les entiers tels que

$$K_S \sim kL_S \quad \text{et} \quad G \sim mL_S,$$

où K_S désigne la classe canonique sur S. D'après la relation (IV.1) page 104, on a

$$n_b = m - n_a - k.$$

Si l'on injecte cette relation dans (IV.3), on obtient

$$w(c) \geq n_a(m - k - n_a)L_S^2. \tag{IV.4}$$

Le souci est que la quantité avec laquelle on minore le poids de Hamming de c est négative dès que $n_a \geq m - k$. Partant de la discussion ci-dessus, le théorème IV.2.1 qui suit n'est pas réellement exploitable en l'état. Il offre cependant des perspectives de minoration de la distance minimale de $C_{L,S}(\Delta, G)^\perp$ sous réserve d'obtenir des réponses à une question ouverte qui sera posée plus loin (question 7). La preuve de ce théorème est suivie d'une discussion sur l'énoncé.

Théorème IV.2.1. *Soit S une surface projective lisse intersection complète et géométriquement intègre. Soit m un entier et G un diviseur sur S vérifiant $G \sim mL_S$. Soit enfin Δ une somme formelle de points rationnels de S évitant le support de G. Supposons qu'il existe un entier naturel s vérifiant les conditions suivantes.*

- (*i*) *s est supérieur à la distance minimale $d^\perp$.*
- (*ii*) *Pour toute configuration $P_{i_1}, \ldots, P_{i_s}$ de points du support de Δ, il existe une hypersurface H de $\mathbf{P}^r$ **définie sur** $\overline{\mathbf{F}}_q$ de degré inférieur à $m - k - 1$ qui contient $P_{i_1}, \ldots, P_{i_s}$ et telle que $H \cap S$ est une courbe lisse. On rappelle que l'entier k est celui qui vérifie $K_S \sim kL_S$ où K_S désigne la classe canonique.*

Alors, la distance minimale $d^\perp$ du code $C_L(\Delta, G)^\perp$ vérifie

$$d^\perp \geq (m - k - 1)L_S^2.$$

PREUVE. D'après la remarque III.6.1 page 96, la distance minimale d'un code géométrique est invariante par extension des scalaires. Il suffit donc que l'on soit à même de réaliser géométriquement les mots de code de $C_{L,S}(\Delta, G)^\perp$ vus comme des mots de $C_{L,S'}(\Delta', G')$, où S' désigne $S \times_{\mathbf{F}_q} \mathbf{F}_{q^l}$ pour un certain entier naturel l et Δ' et G' les tirés en arrière respectifs de Δ et G sur S'. C'est ce qui justifie dans le (*ii*) le "*définie sur* $\overline{\mathbf{F}}_q$".

Soient s un entier vérifiant les condition (*i*) et (*ii*) de l'énoncé et E, l'ensemble des mots non nuls de $C_{L,S}(\Delta, G)^\perp$ de poids de Hamming inférieur ou égal à s. D'après (*ii*) et (IV.4), on a

$$\forall c \in E,\ w(c) \geq \min_{n_a=1}^{m-k-1} n_a(m - k - n_a)L_S^2.$$

La définition de E entraîne que l'inégalité ci-dessus est en fait vérifiée par tous les mots non nuls de $C_{L,S}(\Delta, G)^\perp$. Par ailleurs, l'étude de la fonction $x \mapsto x(m-k-x)$ sur l'intervalle $[1, m-k-1]$ permet de voir que le minimum de l'expression $n_a(m-k-n_a)L_S^2$ est atteint pour $n_a = 1$. On en déduit

$$d^\perp \geq (m-k-1)L_S^2.$$

□

Discussion au sujet du théorème IV.2.1. L'énoncé peut sembler troublant en ce sens où l'entier s doit être supérieur à la quantité $d^\perp$ sur laquelle on cherche à s'informer. Pour exploiter ce théorème il faut disposer d'une majoration *à priori* de $d^\perp$. Voici un certain nombre de pistes, pour obtenir une telle majoration.

(1) L'approche la plus naïve serait de majorer $d^\perp$ par la longueur du code.

(2) Si l'on connaît la dimension du code on peut utiliser la borne de singleton à savoir $d^\perp \leq n - \dim(C_{L,S}(\Delta, G)^\perp) + 1$.

(3) Sous réserve de disposer d'une évaluation de la distance minimale d'un code fonctionnel, le théorème d'orthogonalité (théorème II.4.1) fournit une majoration de la distance minimale de $C_L(\Delta, G)^\perp$. En effet, comme pour toute paire de diviseurs (sous-) Δ-convenable (D_a, D_b) on a

$$C_{\Omega,S}(\Delta, D_a, D_b, G) \subseteq C_{L,S}(\Delta, G)^\perp.$$

Par conséquent, la distance minimale du code $C_{L,S}(\Delta, G)^\perp$ est inférieure à celle du code $C_{\Omega,S}(\Delta, D_a, D_b, G)$. Ce dernier code est fonctionnel d'après le théorème II.4.6. Si l'on et capable d'estimer la distance minimale d'un code fonctionnel sur S on peut en déduire une bonne majoration à priori de $d^\perp$.

Il s'agit là d'un piste à explorer dans le futur. Notons tout de même que dans certaines situations, un tel entier s n'existe pas, il suffit par exemple que $m-k-1$ soit négatif. Avant de conclure, donnons deux exemples élémentaires. L'un assurant que l'entier s existe (au moins dans certaines situations élémentaires) et le second présentant un cas où l'entier s n'existe pas, bien que $m-k-1$ soit strictement positif.

Exemple IV.2.2 (Un exemple où s existe.). On reprend l'exemple présenté dans la section II.3.5 du chapitre II. Soit S le plan projectif sur un $\mathbf{F}_q$ de caractéristique différente de deux. Supposons par exemple que $m = 1$. On a $k = -3$ et le code $C_L(\Delta, G)$ avec $G \sim L_S$ est de dimension 3 et donc de longueur q^2. On en déduit que le code $C_L(\Delta, G)^\perp$ est de dimension $q^2 - 3$ et la borne de singleton nous assure que sa distance minimale vérifie

$$d^\perp \leq 4$$

On a $m-k-1 = 3$, l'objectif est donc de montrer que pour tout quadruplet de points rationnels de $\mathbf{P}^2$, il existe une courbe lisse de degré inférieur ou égal à trois qui contient ces points.

Soient donc P_1, P_2, P_3, P_4 quatre points de $\mathbf{P}^2$. S'ils sont alignés c'est terminé, une droite étant une courbe lisse de degré 3. Si P_1, P_2, P_3 appartiennent à une même droite L qui ne contient pas P_4, il existe un système de coordonnées homogènes (X, Y, Z) sur $\mathbf{P}^2$ et un élément $a \in \mathbf{F}_q \setminus \{0, 1\}$ tels que,

$$\begin{array}{lcllcl} P_1 & = & (0:0:1) & P_1 & = & (1:0:1) \\ P_3 & = & (a:0:1) & P_4 & = & (0:1:0). \end{array}$$

La courbe elliptique d'équation $Y^2Z = X(X-Z)(X-aZ)$ est lisse et interpole ces quatre points.

Enfin, supposons que trois de ces points ne soient pas alignés, alors il existe au moins une conique lisse qui les contient. L'entier $s = 4$ vérifie donc les conditions (i) et (ii) du

théorème IV.2.1, ce dernier nous fournit donc une minoration de la distance minimale du code $C_{L,S}(\Delta, G)^\perp$, à savoir

$$d^\perp \geq (m-k-1)L_S^2 = 3.$$

D'après le théorème IV.1.7 (1), le minorant obtenu est en fait exactement la distance minimale du code étudié.

Exemple IV.2.3 (Un exemple où $m-k-1 \geq 0$ mais s n'existe pas.). Soit S une surface cubique lisse de $\mathbf{P}^3_{\mathbf{F}_q}$ avec $q \geq 3$ et contenant au moins une droite rationnelle. Soit Δ la somme de tous les points rationnels de S et G un diviseur tel que $G \sim 2L_S$ et dont le support évite celui de Δ (un tel G existe, voir annexe D.2). On rappelle que les surfaces cubiques sont des surfaces de Del Pezzo. Donc $k = -1$ et $m-k-1 = 2$. Notons que, d'après le théorème IV.1.7 (2), on sait que $d^\perp = 4$, les mots de poids minimal étant ceux donc le support correspond à des points d'une droite rationnelle contenue dans S.

À présent, raisonnons par l'absurde, en supposant l'existence d'un entier s vérifiant les conditions du théorème IV.2.1. Alors, d'après ce théorème, la distance minimale de $C_{L,S}(\Delta, G)^\perp$ serait supérieure ou égale à 6, ce qui est faux d'après les remarques ci-dessus.

Conclusion. Le théorème IV.2.1 motive la question ouverte suivante.

Question 7. *Soient X une sous-variété irréductible lisse géométriquement intègre de $\mathbf{P}^r_{\overline{\mathbf{F}}_q}$ et d un entier naturel. Soient $P_1, \ldots, P_n$ une famille de points de X. Sous quelles conditions sur X et $P_1, \ldots, P_n$ a-t-on l'existence d'un entier s tel que pour tout s-uplet de points parmi $P_1, \ldots, P_n$, il existe une hypersurface H de degré d contenant ce s-uplet de points et telle que $H \cap X$ soit une sous-variété lisse de codimension 1 de X ?*

Notons qu'une réponse à la question 5G posée page 96, fournirait sans doute des éléments de réponse, voire même une réponse complète à la question ci-dessus. L'obtention d'un tel résultat "à la Bertini" nous donnerait de nombreuses informations, à la fois sur les codes fonctionnels et sur leurs orthogonaux. La question 5G est donc un problème ouvert ouvrant de nombreuses perspectives d'application.

Chapitre V

Constructions de mots de faible poids et codes LDPC

> Une idée reçue atteste que la creuse est le département le moins peuplé de France, ce qui est totalement faux.
>
> WIKIPEDIA

On signale dans la section III.5 du chapitre III que le théorème de réalisation n'est pas constructif. Aussi, ce chapitre est-il en partie consacré à la présentation de méthodes constructives de réalisation différentielle de mots de code appartenant à l'orthogonal d'un code fonctionnel. Les mots de l'orthogonal d'un code fonctionnel qui vont nous intéresser et qui s'avèreront être les plus simples à calculer seront ceux dont le poids de Hamming est *petit*. Si ces mots engendrent le code qui les contient, on dit que ce code est LDPC (*Low Density Parity Check*). La première section de ce chapitre est une introduction à la théorie de ces codes.

V.1 Introduction aux codes LDPC

Un code LDPC est un code admettant une matrice de parité *creuse*. En d'autres termes, c'est un code admettant une base duale composée de mots de petit poids de Hamming.

V.1.1 Graphe de Tanner

Définition V.1.1 (Graphe biparti)**.** *Un graphe biparti est la donnée de deux ensembles de sommets V_1 et V_2 et d'un ensemble d'arêtes E tels que toute arête $a \in E$ relie un unique élément de V_1 avec un unique élément de V_2.*

La définition qui suit a été introduite par R. Michael Tanner dans [Tan81].

Définition V.1.2 (Tanner 1981)**.** *Soient C un code binaire de longueur n et $H \in \mathfrak{M}_{r,n}(\mathbf{F}_2)$ une matrice de parité de C. On appelle graphe de Tanner de C, le graphe biparti dont la première famille de sommets V_1 est indexée par les colonnes de H et la seconde famille V_2 par les lignes. Une arête relie le i-ème sommet de la famille V_1 au j-ème de V_2 si et seulement si le coefficient $h_{i,j}$ de la matrice H est non nul.*

Remarque V.1.3. *Remarquer qu'un code n'admet pas un unique graphe de Tanner. Aussi, on devrait parler du graphe de Tanner de C associé à H et non du graphe de Tanner de C. Dans la pratique, cet abus de langage est toléré et même fréquemment pratiqué.*

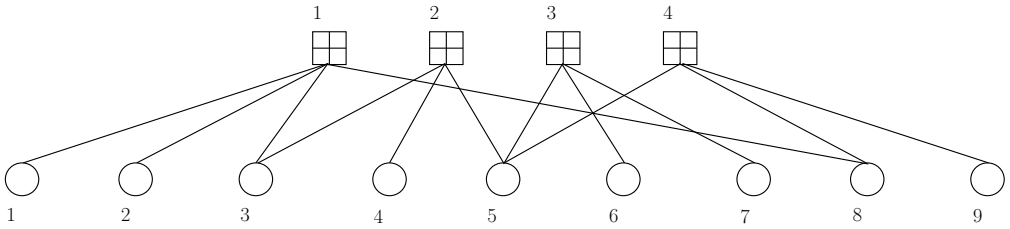
Dans ce qui suit, on représentera les sommets correspondant aux colonnes de la matrice par des $\bigcirc$ et on appellera ces sommets les *nœuds de données* ou tout simplement les *bits*.

Les sommets correspondant aux lignes seront représentés par des ⊞ et on les appellera les *nœuds de parité* ou les *relations*[1].

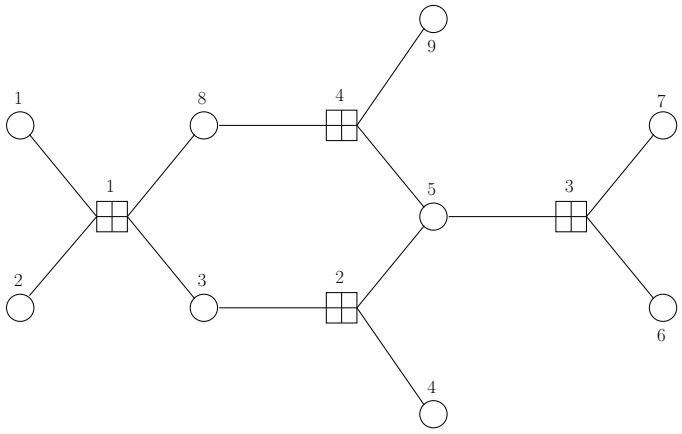
Exemple V.1.4. Soit C, le code de matrice de parité

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Le graphe de Tanner de C correspondant à la matrice H est de la forme suivante.



On peut également essayer de l'*étaler* afin d'y voir plus clair, sous réserve bien sûr que le graphe admette une représentation planaire.



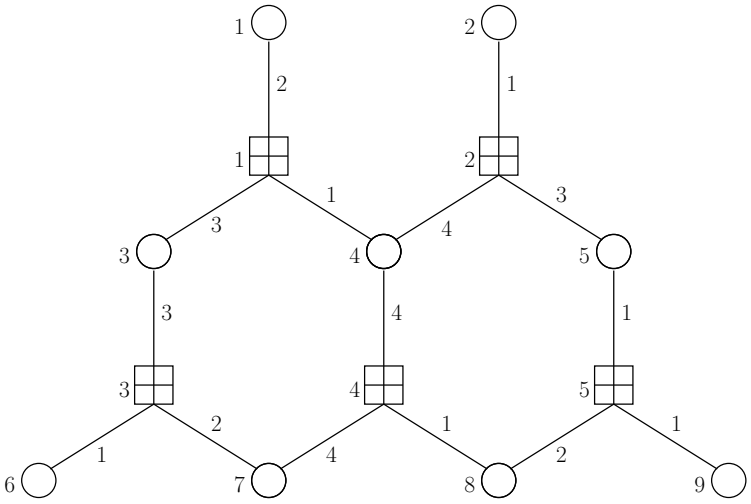
Si le code n'est pas binaire on peut réaliser une construction semblable mais avec des arêtes *pondérées*. Entre le bit i et la relation j on trace une arête pondérée par le coefficient $h_{i,j}$ de la matrice de parité si ce dernier est non nul et pas d'arête sinon.

Exemple V.1.5. Supposons que le corps de base soit $\mathbf{F}_5$ et considérons le code C de matrice de parité

$$H = \begin{pmatrix} 2 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 4 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 \end{pmatrix}.$$

Le graphe de Tanner de C associé à H se représente de la façon suivante.

[1] Dans la littérature anglophone, on parle de *check nodes*, c'est-à-dire nœud de contrôle. Nous avons préféré donner ce nom de *relation*, car ces nœuds symbolisent une équation, donc une relation entre les bits qui lui sont voisins dans le graphe.



V.1.2 Décodage itératif

L'intérêt majeur de la représentation d'un code par un graphe de Tanner est le décodage itératif. Le principe général consiste, étant donné un mot de code reçu y à évaluer les coûts locaux d'assignation de chaque bit à une valeur prescrite. Dans un second temps, par un principe de passage de messages dans le graphe, on actualise ces coûts en fonction du nombre de modifications qu'une assignation d'un bit à une valeur prescrite entraînerait sur les bits voisins dans le graphe. De façon schématique, la répétition de ce procédé permet (à de nombreux détails près) de passer de coûts locaux à des coûts globaux. On choisit alors comme sortie de l'algorithme, le mot de code correspondant aux coûts globaux minimaux.

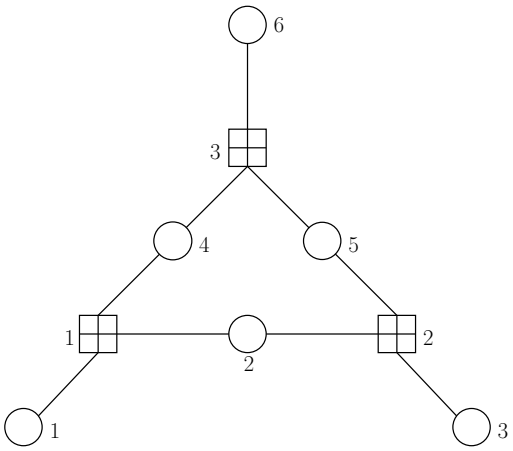
Il existe dans la littérature de nombreux algorithmes de décodage itératif. Celui que nous allons présenter porte en général le nom de *algorithme min-somme*. Notons que l'on peut trouver une excellente présentation de cet algorithme dans la thèse de Niclas Wiberg [Wib96].

Description à partir d'un exemple. Le mécanisme d'un algorithme de décodage itératif, sans être très complexe, est relativement technique. Nous allons commencer par le décrire à l'aide d'un exemple élémentaire.

Exemple V.1.6. Considérons le code binaire C de matrice de parité

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Son graphe de Tanner associé à H se présente sous la forme suivante.



Ce code est de distance minimale 3, on peut donc corriger une erreur.

Considérons ce code C et supposons que l'on ait reçu le mot

$$y = (1, 1, 0, 1, 0, 1).$$

Le second bit est erroné.

Étape 1. L'objectif de l'algorithme est d'évaluer le coût qu'aurait l'assignation d'un bit à une valeur prescrite dans $\mathbf{F}_2$. Pour ce faire, on commence par définir pour chaque bit une fonction de *coût local*. C'est une fonction $C^i_{\text{loc}} : \mathbf{F}_2 \to \mathbf{N}$ telle que $C^i_{\text{loc}}(\alpha)$ est nul si $y_i = \alpha$ et égal à 1 sinon. Par exemple $C^1_{\text{loc}}(0) = 1$ et $C^1_{\text{loc}}(1) = 0$.
Pour abréger, on note

$$C^1_{\text{loc}} = [1, 0].$$

Cette fonction quantifie le nombre de changements qu'impliquerait l'assignation du bit i à la valeur α sans chercher à vérifier les relations de parité. On voit facilement que

$$\begin{array}{lllllllll} C^1_{\text{loc}} & = & [1,0] & C^2_{\text{loc}} & = & [1,0] & C^3_{\text{loc}} & = & [0,1] \\ C^4_{\text{loc}} & = & [1,0] & C^5_{\text{loc}} & = & [0,1] & C^6_{\text{loc}} & = & [1,0]. \end{array}$$

Étape 2. Dans un second temps, on va évaluer le nombre de changements qu'impliquerait l'assignation d'un bit à une valeur prescrite avec la contrainte de respecter les relations de parité voisines de ce bit.

Étude locale. Focalisons nous sur le second bit. Il est voisin de deux relations de parité : la première et la seconde. Supposons que l'on lui assigne la valeur 0. Alors, pour respecter la première équation de parité, on a deux possibilités.

(1) Les bits 1 et 4 prennent tous deux la valeur 1.

(2) Les bits 1 et 4 prennent tous deux la valeur 0.

La première configuration est la moins coûteuse, elle n'implique aucun changement, c'est celle que l'on retient. On en déduit que l'assignation du second bit à la valeur 0 aura une répercussion de coût nul sur les autres bits voisins du premier nœud de relation. Si maintenant on assigne la valeur 1 à ce bit on a également deux possibilités.

(1) Le 1$^{\text{er}}$ bit prend la valeur 1 et le 4$^{\text{e}}$ la valeur 0.

(2) Le 1$^{\text{er}}$ bit prend la valeur 0 et le 4$^{\text{e}}$ la valeur 1.

Les deux configurations coûtent un changement. On en déduit que l'assignation du second bit à la valeur 0 a une répercussion de coût 1 sur le premier nœud de relation.

De la même manière, on montre que l'assignation du second bit à la valeur 0 (resp. 1) a une répercussion de coût 0 (resp. 1) sur les bits 3 et 5 voisins du second nœud de relation.

Étape 3. Au final l'assignation du second bit à la valeur 1 coûte deux changements (un sur le bit 1 ou 4 et un autre sur le 2 ou 5) comme le sixième. Par contre l'assignation de ce bit à 0 ne coûte qu'un seul changement, celui qui consiste à remplacer ce bit initialement à la valeur 1 par un 0. On est donc tentés d'assigner ce bit à 0 ce qui corrige l'erreur.

Remarque V.1.7. *Dans cet exemple, nous nous sommes focalisés sur un seul bit pour tenter de comprendre le mécanisme. En réalité, l'algorithme réalise en parallèle la même démarche pour chaque bit.*

Remarque V.1.8. *Il est important de remarquer que nous n'avons pas vérifié si l'assignation du second bit à une valeur donnée avait des répercussions sur les bits plus éloignés. On s'est limités au premier voisinage du second bit pour prendre notre décision. En général, on réitère le processus décrit dans l'étape 2 de façon à obtenir des informations sur les répercussions d'une assignation sur les bits éloignés.*

L'idée de l'algorithme min-somme peut se résumer de la façon suivante.

(1) On commence par compter le nombre de changements qu'impliquerait l'assignation du i-ème bit à une valeur donnée, sans tenir compte des relations de parité.

(2) On compte ensuite le nombre de changements que cela impliquerait pour les autres bits reliés à i par une relation de parité. C'est-à-dire le coût d'une telle assignation pour les bits étant dans le premier voisinage du i-ème bit.

(3) En réitérant ce procédé on peut compter le nombre de changements qu'implique une telle assignation pour les bits appartenant au second voisinage du i-ème bit.

(4) On réitère le processus...

(5) Lorsque l'on dispose du coût d'assignation du i-ème bit à une valeur donnée pour un voisinage *suffisamment grand* de ce dernier, on prend une décision sur la valeur à laquelle on l'assigne en choisissant bien sûr celle qui est la moins coûteuse.

Encore une fois, les opérations sont réalisées en parallèle pour tous les bits.

V.1.3 L'algorithme min-somme

Nous allons à présent donner une description générale et rigoureuse de l'algorithme min-somme.

Étape 1. Initialisation. À chaque bit, on associe une fonction de coût local $C^i_{\mathrm{loc}} : \mathbf{F}_q \to \mathbf{N}$. À l'état initial, la fonction de coût local du i-ème bit est extrêmement simple. Si la i-ème coordonnée du mot reçu y est égale à $\alpha \in \mathbf{F}_q$, alors la fonction f_i prend la valeur 0 en α et la valeur 1 en tous les autres éléments de $\mathbf{F}_q$. La valeur $C^i_{\mathrm{loc}}(\beta)$ quantifie le coût d'assignation du i-ème bit à la valeur β sans tenir compte des bits voisins.

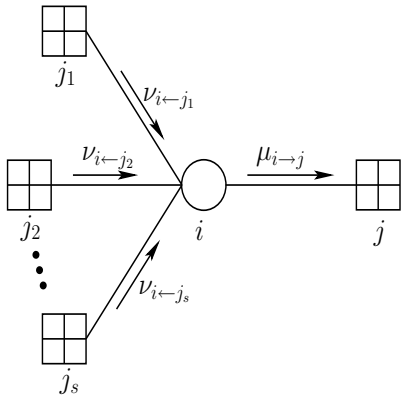
Pour toute arête (i, j) du graphe de Tanner, on définit les fonctions *messages* $\mu_{i\to j} : \mathbf{F}_q \to \mathbf{N}$ et $\nu_{i\leftarrow j} : \mathbf{F}_q \to \mathbf{N}$. Ces fonctions peuvent être vues respectivement comme un message allant du bit i vers la relation j et réciproquement. Ces fonctions sont des *variables locales* de l'algorithme, c'est-à-dire qu'elles sont actualisées à chaque itération de l'algorithme. Pour toute arrête (i, j), ces fonctions sont initialement assignées à la fonction nulle

$$\mu_{i\to j} := 0 \quad \text{et} \quad \nu_{i\leftarrow j} := 0.$$

Étape 2. Échanges de messages. Cette étape est itérée "autant de fois que nécessaire". Le nombre d'itérations sera discuté en section V.1.4.

Étape 2a. Messages données → relations. Dans cette étape, on actualise les messages $\mu_{i\to j}$ des données vers les relations en tenant compte des nouvelles informations fournies par les messages $\nu_{k\leftarrow l}$. Étant donnés un bit i et une relation j, on note $j_1, \ldots, j_s$ les relations voisines de i autres que j. Le nœud de données i centralise les informations transmises par les relations $j_1, \ldots, j_k$ et les envoie vers la relation j. Le message $\mu_{i\to j}$ devient alors

$$\mu_{i\to j} := C^i_{\mathrm{loc}} + \sum_{k=1}^{s} \nu_{i\leftarrow j_k}.$$

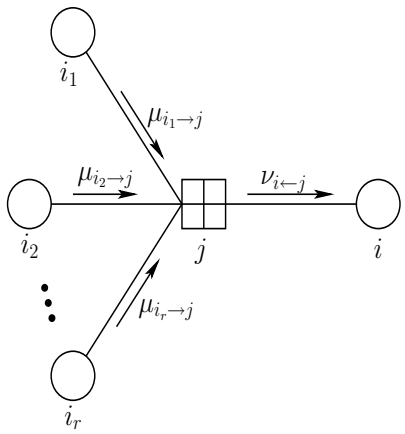


Remarque V.1.9. *Lors de la première itération de l'algorithme, la fonction $\mu_{i\rightarrow j}$ initialement assignée à la fonction nulle devient égale à la fonction C^i_{loc}.*

Étape 2b. Messages relations → données. Dans cette étape, on actualise les messages $\nu_{i\leftarrow j}$ en tenant compte des informations fournies par les messages $\mu_{i\rightarrow j}$. Un noeud de relation j centralise les informations fournies par les fonctions message $\mu_{i_k\rightarrow j}$ provenant des bits voisins autres que i et les redirige vers ce dernier. Soient donc $i_1,\dots,i_r$ les nœuds de donnée voisins du nœud de relation j autres que i. La fonction $\nu_{i\leftarrow j}$ est définie par

$$\forall \alpha \in \mathbf{F}_q, \quad \nu_{i\leftarrow j}(\alpha) := \min\left\{ \sum_{k=1}^{r} \mu_{i_k\rightarrow j}(\alpha_k) \;\middle|\; \begin{array}{c} (\alpha_1,\dots,\alpha_r)\in \mathbf{F}_q^r, \\ h_{i,j}\alpha + h_{i_1,j}\alpha_1 + \cdots + h_{i_r,j}\alpha_r = 0 \end{array} \right\}.$$

On calcule le coût minimal d'une configuration vérifiant la relation j et telle que le bit i vaille α. On rappelle que les coefficients $h_{i,j}$ sont les coefficients de la matrice de parité H qui pondèrent les arêtes du graphe de Tanner. Dans la figure qui suit, ils n'ont pas été indiqués de façon à alléger la représentation.



Remarque V.1.10. *Lors de la première itération de l'algorithme, l'entier $\nu_{i\leftarrow j}(\alpha)$ quantifie le nombre minimal de changements qu'entraînerait l'assignation du i-ème bit à la valeur α pour les autres bits intervenant dans la relation j.*

Exemple V.1.11. Dans l'exemple V.1.6 que nous avons étudié précédemment les fonctions $\nu_{2\leftarrow 1}$ et $\nu_{2\leftarrow 1}$ ont été calculées, on avait obtenu

$$\nu_{2\leftarrow 1} = [0,1] \quad \text{et} \quad \nu_{2\leftarrow 2} = [0,1].$$

Par le calcul on obtient également (la vérification est laissée au lecteur),

$$\begin{array}{llllllll} \nu_{1\leftarrow 1} & = & [0,1] & \nu_{3\leftarrow 2} & = & [1,0] & \nu_{4\leftarrow 1} & = & [0,1] & \nu_{4\leftarrow 3} & = & [1,0] \\ \nu_{5\leftarrow 2} & = & [1,0] & \nu_{5\leftarrow 3} & = & [0,1] & \nu_{6\leftarrow 3} & = & [1,0]. & & & \end{array}$$

Étape finale. Décision. Chaque nœud de donnée évalue ses coûts *globaux* d'assignation avec l'aide des fonctions $\nu_{i\leftarrow j}$. Soient i un noeud de données et $j_1, \ldots, j_t$ l'ensemble des nœuds de relation voisins de i. La fonction de coût *global* C^i_{glob} est définie par

$$\forall \alpha \in \mathbf{F}_q, \quad C^i_{\text{glob}}(\alpha) := C^i_{\text{loc}}(\alpha) + \sum_{k=1}^{t} \nu_{i\leftarrow j_k}(\alpha).$$

On regarde ensuite s'il existe un élément α qui minimise la fonction C^i_{glob}. Si oui, on assigne la valeur α au bit i.

Exemple V.1.12. Dans l'exemple V.1.6, si l'on prend une décision après une itération du processus d'échanges de messages, à partir des résultats de l'exemple V.1.11, on obtient

$$\begin{array}{llllllll} C^1_{\text{glob}} & = & [1,1] & C^2_{\text{glob}} & = & [1,2] & C^3_{\text{glob}} & = & [1,1] \\ C^4_{\text{glob}} & = & [2,1] & C^5_{\text{glob}} & = & [1,2] & C^6_{\text{glob}} & = & [2,0]. \end{array}$$

On ne peut donc pas prendre de décision quant à l'assignation finale des bits 1 et 3. Il ne fallait pas évaluer les fonctions de coûts globaux à cette étape mais réitérer le processus. À la seconde itération, l'actualisation des fonctions $\mu_{i\to j}$ donne

$$\begin{array}{llllllll} \mu_{1\to 1} & = & [1,0] & \mu_{2\to 1} & = & [1,1] & \mu_{2\to 2} & = & [1,1] \\ \mu_{3\to 2} & = & [0,1] & \mu_{4\to 1} & = & [2,0] & \mu_{4\to 3} & = & [1,1] \\ \mu_{5\to 2} & = & [0,2] & \mu_{5\to 3} & = & [1,1] & \mu_{6\to 3} & = & [1,0]. \end{array}$$

Après quoi, l'actualisation des fonctions $\nu_{i\leftarrow j}$ donne

$$\begin{array}{llllllll} \nu_{1\leftarrow 1} & = & [1,1] & \nu_{2\leftarrow 1} & = & [0,1] & \nu_{2\leftarrow 2} & = & [0,1] \\ \nu_{3\leftarrow 2} & = & [1,1] & \nu_{4\leftarrow 1} & = & [1,1] & \nu_{4\leftarrow 3} & = & [1,1] \\ \nu_{5\leftarrow 2} & = & [1,1] & \nu_{5\leftarrow 3} & = & [1,1] & \nu_{6\leftarrow 3} & = & [2,2]. \end{array}$$

Si l'on évalue les coûts globaux à la fin de cette seconde itération, on obtient

$$\begin{array}{llllllll} C^1_{\text{glob}} & = & [2,1] & C^2_{\text{glob}} & = & [1,2] & C^3_{\text{glob}} & = & [1,2] \\ C^4_{\text{glob}} & = & [3,2] & C^5_{\text{glob}} & = & [2,3] & C^6_{\text{glob}} & = & [3,2]. \end{array}$$

On peut donc prendre une décision, on choisit comme mot décodé le mot

$$c = (1,0,0,1,0,1),$$

qui est bien le mot le plus proche du mot reçu y pour la distance de Hamming.

V.1.4 Discussion sur l'algorithme

Avant de rentrer dans des considérations plus techniques, commençons par quelques remarques concernant cet algorithme.

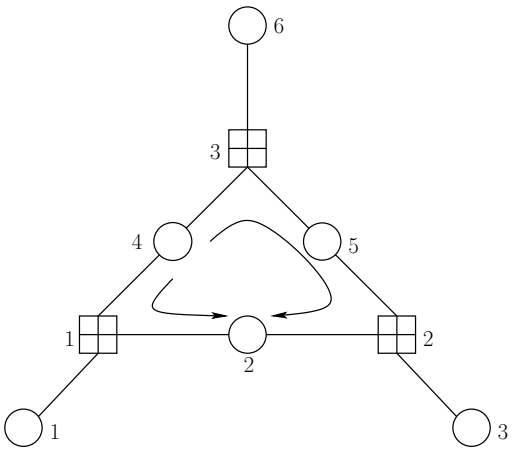
- Le nom de l'algorithme provient bien sûr de l'étape 2b et d'une façon plus générale, du fait que les seules opérations effectuées sont des sommes et des calculs de minima.
- Il existe également un algorithme appelé somme-produit dont le fonctionnement est assez comparable. Moralement le min-somme calcule des coûts, alors que le somme-produit évalue des probabilités.

Nombre d'itérations

Concrètement, au départ, chaque bit ne possède que l'information qui le concerne, à savoir son coût d'assignation à une valeur donnée, sans tenir compte de ses voisins. C'est l'information qu'il va transmettre à tous les nœuds de relation voisins sous la forme des fonctions $\mu_{i\to j}$ durant la première itération (voir remarque V.1.10). À la fin de la première itération on peut savoir le coût qu'aurait l'assignation d'un bit à une valeur prescrite pour ce bit et ses voisins (c'est-à-dire à une distance de deux arêtes). Si l'on réitère le processus p fois, on dispose de toutes les informations provenant des bits à une distance inférieure à p du i-ème bit. Aussi il semble raisonnable de choisir comme nombre d'itérations la distance maximale entre deux bits dans le graphe de Tanner.

Le problème des cycles

Le problème majeur de ces algorithmes est qu'ils agissent localement, sans tenir compte de la géométrie du graphe. Pour le comprendre reprenons l'exemple V.1.6 et supposons que l'on a effectué deux itérations de la phase d'échanges de messages (étape 2). Si l'on évalue la fonction de coût global C^2_{glob} après ces deux itérations, le coût évalué prend en compte la contribution de tous les bits qui sont à distance inférieure à 2 du 2^{e}. Le souci est que, en partant du 2^{e} bit, le 4^{e} (ainsi que le 5^{e}) peut être atteint par un chemin de longueur[2] deux de deux façons différentes, comme le montre la figure ci-dessous. De fait, dans le calcul du coût global C^2_{glob}, la contribution du quatrième et du cinquième bit est comptée deux fois, ce qui peut biaiser la décision finale.



Les résultats connus sur l'efficacité de l'algorithme sont que le coût global réel d'assignation d'un bit ne peut être calculé exactement par cet algorithme que si le graphe de Tanner est sans cycles. Cependant, les codes dont le graphe de Tanner est sans cycles sont peu intéressants (mauvais paramètres).

De fait, on ne dispose pas réellement de résultats sur l'efficacité d'un tel algorithme. On dispose cependant d'une constatation empirique, à savoir que si le graphe de Tanner n'a pas trop de "petits cycles", alors les algorithmes de décodage itératif sont extrêmement efficaces. Ils permettent en particulier de corriger un grand nombre d'erreurs en un temps relativement limité, **à condition que le code soit LDPC**.

Conclusion. L'étape réellement coûteuse est la seconde qui est exponentielle en la valence des nœuds de relation. C'est la raison pour laquelle, si l'on travaille sur un code pour lequel cette valence est bornée par une petite valeur, alors l'algorithme tournera rapidement.

[2]Il s'agit d'un graphe biparti, aussi on appelle *chemin de longueur* n un chemin de $2n$ arêtes.

V.2 Codes LDPC et surfaces de petit degré

Soient N un entier supérieur ou égal à 3 et X une hypersurface projective lisse géométriquement intègre de degré d de $\mathbf{P}^N$. Tout comme dans les chapitres précédents, on note L_X, la classe d'équivalence linéaire d'une section hyperplane de X. On se donne également G, un diviseur sur X tel que $G \sim mL_X$ pour un certain entier m et Δ, la somme formelle de tous les points rationnels de X qui évitent le support de G. Notons que si m est strictement négatif, le code $C_L(\Delta, G)$ est nul. On peut donc supposer m positif ou nul. D'après le théorème IV.1.7 (1) (chapitre IV), on sait l'orthogonal d'un code fonctionnel sur X a une distance minimale supérieure ou égale à $m+2$ et que cette borne est atteinte dès que le support de Δ contient $m+2$ points alignés. Cette borne inférieure ne peut donc être atteinte que dans deux situations.

(1) Le degré de X est supérieur ou égal à $m+2$ et il existe une droite de P^N dont l'intersection avec X contient au moins $m+2$ point rationnels.

(2) L'hypersurface X contient une droite rationnelle et toute droite contient au moins $m+2$ point rationnels, ce qui revient à dire que $\sharp\mathbf{F}_q \geq m+1$.

V.2.1 Objectifs

Dans ce qui suit, notre but est de chercher des codes construits sur des surfaces et dont l'orthogonal est engendré par des mots de petit poids, voire de poids minimal. Dans cette optique, la situation 1 ci-dessus est en fait la plus intéressante. En effet, la situation 2 est en général assez rare. Par exemple, dans le cas où X est une surface ($N = 3$), d'après [Sha94] théorème I.6.9, une surface générique de degré supérieur ou égal à 4 ne contient pas de droites et une surface générique de degré 3 n'en contient qu'un nombre fini (27 si elle est lisse). De plus, ce dernier résultat est géométrique, ce qui signifie que les droites sur une surface cubique peuvent ne pas être rationnelles. Les mots de code provenant de la situation 2, seront donc en général peu nombreux et engendreront un code dont le support sera souvent strictement contenu dans $\{1, \ldots, n\}$ où n désigne la longueur du code $C_L(\Delta, G)$. En effet, si P est un point de $\mathrm{Supp}(\Delta)$ qui n'est contenu dans aucune droite rationnelle contenue dans X, alors l'indice correspondant n'est dans le support d'aucun mot de code provenant de la situation 2.

Dans ce qui suit, nous allons nous intéresser aux surfaces fournissant un grand nombre de mots de codes provenant de la situation 1. N'ayant pas obtenu de résultat théorique permettant d'orienter cette recherche, nous avons fait appel à l'outil informatique (plus précisément le logiciel MAGMA). Dans la section V.4, nous allons présenter des résultats expérimentaux effectués sur des surfaces cubiques de $\mathbf{P}^3$. Auparavant, nous allons nous intéresser au calcul explicite de ces mots en utilisant des résidus.

V.3 Calcul explicite de mots de codes de petit poids

Dans ce qui suit, S désigne une surface projective lisse plongée dans $\mathbf{P}^3$ (elle est donc absolument irréductible). On note d le degré de la surface et on suppose que $d \geq 3$. L'espace projectif $\mathbf{P}^3$ est muni de coordonnée homogènes (X, Y, Z, T). Le plan d'équation $T = 0$ est appelé *plan à l'infini* et noté Π. La carte affine $\{T \neq 0\}$ de $\mathbf{P}^3$ est notée $\mathcal{U}_T$ et son intersection avec S est appelée U_t. On note x, y et z les fonction rationnelles sur $\mathbf{P}^3$ suivantes

$$x := \frac{X}{T}, \quad y := \frac{Y}{T}, \quad \text{et} \quad z := \frac{Z}{T}.$$

Ces trois fonctions forment un système de coordonnées affines dans la carte affine $\mathcal{U}_T$ de $\mathbf{P}^3$. Par ailleurs, on suppose que la surface S n'est contenue dans aucun plan de $\mathbf{P}^3$ et on note L_∞ le tiré en arrière du plan à l'infini Π sur S via l'injection canonique $S \hookrightarrow \mathbf{P}^3$. Pour finir, on se donne un entier naturel m, on pose

$$G := mL_\infty$$

et on appelle Δ la somme formelle des points rationnels de S qui évitent le support de G. En d'autres termes, Δ est la somme de tous les points rationnels de la carte affine U_t de S. Nous allons présenter une méthode de calcul explicite des mots de poids minimal du code $C_L(\Delta, G)^\perp$ provenant des situations 1 et 2 signalées page 117.

V.3.1 Mots provenant de droites non contenues dans S

Nous commençons par considérer un cas simple, à savoir $d = m + 2$. Pour des raisons que nous énoncerons plus loin c'est cette situation que nous traiterons plus en détail dans la section V.4. Plus précisément nous utiliserons l'outil informatique pour étudier spécifiquement les cas des surfaces cubiques avec $G = L_\infty$.

Le cas $\mathbf{d = m + 2}$

Soit F une droite non contenue dans S et contenant exactement d points $P_1, \ldots, P_d$ appartenant au support de Δ. D'après le théorème de Bezout, le schéma $F \cap S$ est réduit et son ensemble sous-jacent est égal à la réunion des points $P_1, \ldots, P_d$.

Fait V.3.1. *Étant donné que les points du support de Δ évitent le support de G, ils sont tous contenus dans la carte affine $\mathcal{U}_T$ de $\mathbf{P}^3$. La droite F n'est donc pas contenue dans l'hyperplan à l'infini.*

Quitte à faire un changement de coordonnées, on peut supposer que la droite F est définie dans la carte affine $\mathcal{U}_T$ par

$$F_{|\mathcal{U}_T} = \{x = 0,\ y = 0\}.$$

Fait V.3.2. *Soit $G(x, y, z)$ l'équation de S dans $\mathcal{U}_T$. D'après [Sha94] III.6.4, la 2-forme sur S*

$$\omega := \frac{1}{\left(\frac{\partial G}{\partial z}\right)}.dx \wedge dy$$

est régulière sur U_t et ne s'annule en aucun point de cet ouvert. Plus précisément, son diviseur est de la forme $(\omega) = (d-4)L_\infty$.

Soient D_a et D_b les diviseurs très amples définis respectivement par

$$D_a := i^*\{X = 0\} \quad \text{et} \quad D_b := i^*\{Y = 0\},$$

où i désigne l'injection canonique $i : S \hookrightarrow \mathbf{P}^3$. On a

$$(x) = D_a - L_\infty \quad \text{et} \quad (y) = D_b - L_\infty.$$

Fait V.3.3. *La 2-forme sur S*

$$\omega' := \frac{1}{\left(\frac{\partial G}{\partial z}\right)}.\frac{dx}{x} \wedge \frac{dy}{y} \tag{V.1}$$

vérifie $(\omega') = (d-2)L_\infty - D_a - D_b$. Or, on rappelle que l'on a supposé $d = m + 2$ (avec $G = mL_\infty$), donc

$$(\omega') = G - D_a - D_b.$$

Il reste à vérifier que la paire (D_a, D_b) est sous-Δ-convenable. Les supports de ces diviseurs s'intersectent seulement en les points $P_1, \ldots, P_d$ et, du fait que le schéma $F \cap S$ est réduit, on en déduit que D_a et D_b sont lisses et s'intersectent transversalement en chacun de ces points. Si l'on pose $\Lambda := P_1 + \cdots + P_d$, on a $0 \leq \Lambda \leq \Delta$ et (D_a, D_b) est Λ-convenable, donc sous-Δ-convenable.

Calcul explicite du mot de code correspondant. L'objectif est de calculer de façon explicite les 2-résidus

$$\mathrm{res}^2_{D_a,P_i}(\omega'), \quad \text{pour} \quad i \in \{1,\dots,d\},$$

où ω' est la 2-forme sur S définie dans l'expression (V.1).
On a vu qu'en tout point P_i pour $i \in \{1,\dots,d\}$, les diviseurs D_a et D_b se croisent transversalement. De plus, au voisinage de ces points, ces deux diviseurs sont respectivement définis par les équations locales $x=0$ et $y=0$. D'après le lemme II.3.12, on a pour tout $i \in \{1,\dots,d\}$

$$\mathrm{res}^2_{D_b,P_i}(\omega') = \frac{1}{\left(\frac{\partial G}{\partial z}\right)(P_i)} = -\mathrm{res}^2_{D_a,P_i}(\omega'). \tag{V.2}$$

En effet, soit C, la composante de D_b qui passe par P_i. La 2-forme ω' a un pôle simple le long de C, donc

$$\mathrm{res}^1_C(\omega') = \frac{1}{\left(\frac{\partial G}{\partial z}\right)_{|C}} . \frac{d\bar{x}}{\bar{x}}$$

et le calcul du résidu de cette 1-forme en P_i donne $\mathrm{res}^2_{C,P_i}(\omega')$ qui est en fait égal à $\mathrm{res}^2_{D_b,P_i}(\omega')$ (voir définition I.7.10). On en déduit donc la relation (V.2).

Remarque V.3.4. *Notons que sur la carte affine U_t de S, le lieu d'annulation de la fonction $\left(\frac{\partial G}{\partial z}\right)$ est le lieu des points de branchement du morphisme de projection de S sur le plan d'équation $z=0$. C'est également le lieu d'annulation de la 2-forme $dx \wedge dy$. Par conséquent, en un point P_i en lequel D_a et D_b s'intersectent transversalement, le couple (x,y) est un système de paramètres locaux et $dx \wedge dy$ ne s'annule pas. L'expression (V.2) est donc bien définie.*

Pour finir, remarquons que l'expression (V.2) s'obtient à condition d'avoir bien effectué un changement de coordonnées pour lequel la droite F est définie par les équations $x=0$ et $y=0$. Or, si l'on veut réaliser un programme calculant tous les mots de code de $C_L(\Delta,G)^\perp$ provenant de droites intersectant S en exactement d points, il sera malcommode de réaliser le changement de variables pour chaque droite. Une alternative à ce changement de variables, consiste à choisir des équations de F de la forme $L_{|\mathcal{U}_T}\{f(x,y,z)=0,\ g(x,y,z)=0\}$ et un vecteur directeur $\mathbf{v}$ de F. On considère alors la 2-forme sur S,

$$\omega'' := \frac{1}{\langle \mathbf{grad}(G), \mathbf{v}\rangle} . \frac{df}{f} \wedge \frac{dg}{g}. \tag{V.3}$$

Pour un changement de coordonnées affines de $\mathcal{U}_T$ adapté, la 2-forme ω'' ci-dessus coïncide avec la 2-forme ω' de l'expression (V.1). L'intérêt de l'expression (V.3) est qu'elle fournit une méthode de calcul explicite des mots de $C_L(\Delta,G)^\perp$ associés à des droites qui intersectent S en exactement d points rationnels distincts, sans avoir à effectuer de changement de coordonnées. On en déduit le lemme suivant.

Lemme V.3.5. *Soit G une équation de S dans la carte affine $\mathcal{U}_T$ et soit F une droite de $\mathbf{P}^3$ qui intersecte S en exactement d points $P_{i_1},\dots,P_{i_d}$. Alors le code $C_L(\Delta,G)^\perp$ contient le mot*

$$c := res^2_{D_b,\Delta}(\omega'') \quad \textit{tel que} \quad c_i = \begin{cases} 0 & \textit{si } i \notin \{i_1,\dots,i_d\}, \\ \langle \mathbf{grad}_{P_i}(G), \mathbf{v}\rangle^{-1} & \textit{sinon.} \end{cases}$$

Nous allons à présent considérer le cas $d < m+2$.

Le cas $\mathbf{d < m+2}$

Soient $P_1,\dots,P_{m+2}$ une famille de points alignés de $\mathrm{Supp}(\Delta)$ et soit F la droite les contenant. Tout comme dans le cas précédent, on va supposer que la droite F est définie par les équations $x=0$ et $y=0$ (ce qui sera toujours vrai après avoir effectué un changement

de coordonnées adapté). On note Λ, le 0-cycle défini par $\Lambda := P_1 + \cdots + P_{m+2}$. Comme $d < m+2$, le 0-cycle d'intersection $F \cap S$ vérifie

$$\Lambda \leq F \cap S.$$

Il peut y avoir dans le support de $F \cap S$ d'autres points que les P_i éventuellement de degré supérieur à 1, certains points peuvent également apparaître avec multiplicité supérieure ou égale à 1. Notre objectif est de construire une paire de diviseurs Λ-convenable (D_a, D_b) pour laquelle l'espace $\Gamma(S, \Omega^2(G - D_a - D_b))$ est non nul.

Soient Π_1 et Π_2 les plans d'équations respectives $x = 0$ et $y = 0$. On pose

$$D_a^+ := i^*\Pi_1 \quad \text{et} \quad D_b^+ := i^*\Pi_2,$$

où i désigne l'injection canonique $i : S \hookrightarrow \mathbf{P}^3$. Pour tout point géométrique P de S appartenant au support de $L \cap S$, on note $z_P \in \overline{\mathbf{F}}_q$, la coordonnée suivant z de ce point et on pose

$$r_P := m_P(F, S). \tag{V.4}$$

Remarque V.3.6. *Dans ce qui suit, afin d'éviter d'alourdir on notera indifféremment par "$m_P(.,.)$", la multiplicité d'intersection d'un diviseur et d'un 0-cycle de $\mathbf{P}^3$ et la multiplicité de deux diviseurs de S. L'expression (V.4) correspond à une multiplicité d'intersection dans $\mathbf{P}^3$. Quant à l'expression (V.5) qui suit elle correspond à une multiplicité d'intersection dans S.*

D'après les définitions de D_a^+ et D_b^+, on montre aisément que

$$m_P(D_a^+, D_b^+) = r_P. \tag{V.5}$$

On définit ensuite pour tout point géométrique P appartenant à $\mathrm{Supp}(F \cap S - \Lambda)$ le coefficient

$$s_p := \begin{cases} r_P & \text{si} \quad P \notin \mathrm{Supp}(\Lambda) \\ r_P - 1 & \text{sinon} \end{cases} \tag{V.6}$$

Notons que s_P n'est autre que le coefficient de P dans le 0-cycle $\overline{F} \cap \overline{S}$ sur $\overline{S} := S \times_{\mathbf{F}_q} \overline{\mathbf{F}}_q$. Comme $F \cap S - \Lambda$ est un 0-cycle $\mathbf{F}_q$-rationnel, on en déduit que l'ensemble $\{z_P \mid P \in \mathrm{Supp}(F \cap S - \Lambda)\}$ est invariant sous l'action de $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$. Par conséquent, la fonction

$$h := \prod_{P \in \mathrm{Supp}(F \cap S - \Lambda)} (z - z_P)^{s_P}$$

est définie sur $\mathbf{F}_q$ et son degré est égal à celui du 0-cycle $F \cap S - \Lambda$. On a donc

$$(h) \sim (d - m - 2)L_\infty. \tag{V.7}$$

Pour finir, posons

$$D_a := D_a^+, \quad D_b := D_b^+ - (h)^+ \quad \text{et} \quad D := D_a + D_b. \tag{V.8}$$

Lemme V.3.7. *La paire (D_a, D_b) décrite ci-dessus est Λ-convenable.*

Preuve. Nous allons utiliser le critère de la proposition II.3.8.

Étape 1. Soit P un point géométrique de S non contenu dans le support de Λ. Si l'un des diviseurs D_a ou D_b ne contient pas P dans son support, alors le critère est trivialement vérifié en ce point (voir remarque II.3.10). Sinon, si le point P fait partie des points géométriques de $\mathrm{Supp}(F \cap S)$ autres que $P_1, \ldots, P_{m+2}$. Comme les diviseurs D_a^+ et D_b^+ sont obtenus à partir de sections planes de S et que S est lisse, elle ne peut donc pas avoir deux plan tangents distincts en P. Ainsi, $\mathrm{Supp}(D_a^+)$ ou $\mathrm{Supp}(D_b^+)$ est lisse en P. Supposons que ce soit $\mathrm{Supp}(D_a^+)$, il faut

alors étudier la multiplicité d'intersection $m_P(D_a^+, D - D_a^+)$ qui n'est autre que $m_P(D_a, D_b)$. Or, d'après (V.8) et (V.5), on vérifie aisément que

$$\begin{aligned} m_P(D_a, D_b) &= m_P(D_a, D_b^+) - m_P(D_a, (h)^+) \\ &\leq r_P - s_P. \end{aligned}$$

Or, comme P n'est pas dans le support de Λ, d'après (V.6), on a $s_P = r_P$ et

$$m_P(D_a, D_b) \leq 0.$$

Si maintenant c'est $\mathrm{Supp}(D_b^+)$ qui est lisse en P, il faut étudier la multiplicité d'intersection $m_P(D_b^+, D_a^+ - (h)^+)$. Par un raisonnement identique on montre que cette multiplicité est négative ou nulle.

Étape 2. Supposons maintenant que P soit contenu dans le support de Λ. Par un raisonnement analogue à celui qui a été effectué dans l'étape précédente, on sait que $\mathrm{Supp}(D_a^+)$ ou $\mathrm{Supp}(D_b^+)$ est lisse en P. Supposons que $\mathrm{Supp}(D_a^+)$ soit lisse en P. Il faut calculer

$$m_P(D_a^+, D - D_a^+) = m_P(D_a^+, D_b) = m_P(D_a^+, D_b^+) - m_P(D_a^+, (h)^+). \tag{V.9}$$

D'après (V.5), le terme $m_P(D_a^+, D_b^+)$ est égal à r_P. Nous allons montrer que

$$m_P(D_a^+, (h)^+) = r_P - 1.$$

Étape 2a. Si $r_P = 1$, alors d'après la définition de h, le diviseur $(h)^+$ est nul au voisinage de P et

$$m_P(D_a^+, (h)^+) = 0 = r_P - 1.$$

Étape 2b. Si $r_P \geq 2$, alors sur un voisinage V de P, on a

$$(h)^+_{|V} = ((z - z_P)^{s_P})_{|V} = ((z - z_P)^{r_P - 1})_{|V}.$$

Comme le plan Π_0 d'équation $z = z_P$ ne contient pas la droite F et que cette dernière est par hypothèse tangente à S en P, on en déduit que le plan Π_0 est non tangent à S en P. Par conséquent, soit C le tiré en arrière de Π_0 sur S. Sur un voisinage de P, on a $C = \mathrm{Supp}((h)^+)$ et cette courbe est lisse au voisinage de P, de plus il intersecte $\mathrm{Supp}(D_a^+)$ transversalement en ce point. En conclusion, sur un voisinage V de P, on a

$$(h)^+_{|V} = s_P C_{|V}.$$

et

$$m_P(D_a^+, (h)^+) = s_P m_P(D_a^+, C) = s_P = r_P - 1.$$

Ainsi, quelle que soit la valeur de r_P, la relation (V.9) donne

$$m_P(D_a^+, D_b) = 1$$

Si maintenant, c'est $\mathrm{Supp}(D_b^+)$ qui est lisse en P, on effectue le même raisonnement en partant de la relation

$$m_P(D_b^+, D - D_b^+) = m_P(D_b^+, D_a^+) - m_P(D_b^+, (h)^+)$$

et en montrant que cette multiplicité d'intersection est égale à 1.

Conclusion. Le couple (D_a, D_b) vérifie le critère de la proposition II.3.8, il est donc Λ-convenable. □

Soit donc ω la 2-forme sur S définie par

$$\omega := \frac{h}{\left(\frac{\partial G}{\partial z}\right)}.\frac{dx}{x} \wedge \frac{dy}{y}.$$

Un bref calcul permet de montrer que cette 2-forme vérifie

$$(\omega) = G - D_a - D_b$$

et le mot $c := \mathrm{res}^2_{D_a,\Delta}(\omega)$ appartient à $C_L(\Delta, G)^\perp$ et a pour support $\{1, \ldots, d\}$.

Remarque V.3.8. *Il est plus délicat de donner une formule simple pour calculer le mot de code c comme dans le lemme V.3.5. La difficulté vient de ce que les fonctions h et $\langle \mathbf{grad}(G), \mathbf{v}\rangle$ s'annulent toutes deux en P. Cependant, si $Supp(D_a^+)$ (resp.$Supp(D_b^+)$) est lisse en P les fonctions $h_{|Supp(D_a^+)}$ et $\langle \mathbf{grad}(G), \mathbf{v}\rangle_{|Supp(D_a)^+}$ ont même valuation en P, on peut donc donner un sens à l'évaluation en P de leur rapport.*

V.3.2 Mots provenant de droites contenues dans S

On suppose dans cette sous-section que le cardinal du corps de base $\mathbf{F}_q$ est supérieur ou égal[3] à $m+2$. Soit F une droite contenue dans S et contenant une famille de points $P_1, \ldots, P_l$ appartenant au support de Δ. Une fois de plus, quitte à faire un changement de variables, on peut supposer que la droite F est définie sur l'ouvert affine[4] $\mathcal{U}_T$ de $\mathbf{P}^3$ par les équations $x = 0$ et $y = 0$.

Soit Π_0 le plan d'équation $x = 0$. La courbe C définie par l'intersection schématique $C := \Pi_0 \cap S$ est une courbe plane (car contenue dans Π_0). Elle est de plus réunion de F et d'une courbe C' de degré $d-1$. Soit $E(\bar{y}, \bar{z})$ une équation de la courbe C' dans le plan Π_0. On relève cette fonction en une fonction rationnelle $E(x, y, z)$ sur $\mathbf{P}^3$ qui ne dépend pas de x.

Soit enfin $P_1, \ldots, P_{m+2}$ une famille de points de $\mathrm{Supp}(\Delta)$ contenus dans F. On note $z_1, \ldots, z_{m+2}$ les coordonnées respectives de ces points suivant z. On pose

$$h := \prod_{i=1}^{m+2} (z - z_i)$$

et

$$D_a := F, \quad D_b := (h)_0.$$

Lemme V.3.9. *Soit Λ le 0-cycle défini par $\Lambda := P_1 + \cdots + P_{m+2}$. Alors, la paire (D_a, D_b) est Λ-convenable.*

Preuve. Le diviseur D_a est une droite, c'est donc une courbe lisse. Et le 0-cycle d'intersection de ces diviseurs est exactement Λ. De cette dernière assertion, on déduit aisément que cette paire vérifie le critère de la proposition II.3.8. Elle est donc Δ-convenable. □

Soit alors

$$\omega := \frac{E}{h}.\frac{1}{\left(\frac{\partial G}{\partial y}\right)}.\frac{dx}{x} \wedge dz.$$

Calculons le diviseur de cette 2-forme sur S.

[3] Dans l'introduction de cette section page 117, on demande que le cardinal du corps de base soit supérieur ou égal à $m+1$. En effet, dans cette introduction, la seule contrainte à laquelle on est soumis pour que le support de Δ puisse contenir $m+2$ points alignés est que le nombre de points rationnels d'une droite projective soit supérieur ou égal à $m+2$. Maintenant que l'on a précisé le contexte, il faut faire plus attention, car même si la droite projective sur $\mathbf{F}_q$ a $q+1$ points, les points de $\mathrm{Supp}(\Delta)$ sont tous par hypothèse contenus dans une carte affine de S. Par conséquent, le nombre maximal de points alignés de $\mathrm{Supp}(\Delta)$ est au plus égal à q. C'est ce qui explique cette hypothèse "q supérieur ou égal à $m+2$".

[4] Voir page 117 pour une définition de l'ouvert affine $\mathcal{U}_T$ ainsi que des fonctions x, y et z.

Étape 1. D'après [Sha94] III.6.4, on a

$$\left(\frac{1}{\left(\frac{\partial G}{\partial y}\right)}.du \wedge dz\right) = (d-4)L_\infty,$$

où l'on rappelle que L_∞ désigne la section plane à l'infini.

Étape 2. On rappelle que le plan Π_0 d'équation $x = 0$ intersecte S suivant une courbe $F \cup C'$ où C' est une courbe plane de degré $d-1$. De fait,

$$(u) = F + C' - L_\infty.$$

Étape 3. Par construction, la fonction E s'annule suivant la courbe C'. On rappelle également que E est un polynôme de degré $d-1$ en y et z. Il existe donc un diviseur effectif C'' sur S vérifiant

$$(E) = C' + C'' - (d-1)L_\infty.$$

Étape 4. La fonction h est un polynôme de degré $m+2$. On a donc

$$(h) = (h)_0 - (m+2)L_\infty.$$

Étape finale. On en déduit donc le calcul du diviseur de ω,

$$\begin{array}{rcl}(\omega) & = & (d-4)L_\infty - F - C + L_\infty + C' + C'' - (d-1)L_\infty - (h)_0 + (m+2)L_\infty \\ & = & mL_\infty + C'' - F - (h)_0 \\ & = & C'' + G - D_a - D_b \\ & \geq & G - D_a - D_b.\end{array}$$

Conclusion. Le mot de code

$$c := \mathrm{res}^2_{D_a,\Delta}(\omega)$$

appartient au code $C_L(\Delta, G)^\perp$. De plus, son support correspond exactement aux points $P_1, \ldots, P_{m+2}$.

V.4 Expérimentations avec Magma

V.4.1 Codes sur des surfaces cubiques

Dans cette section S est une surface cubique lisse de $\mathbf{P}^3$. On munit $\mathbf{P}^3$ d'un système de coordonnées homogènes (X, Y, Z, T). On note L_∞ le diviseur défini par l'intersection schématique de S avec le plan *à l'infini* d'équation $T = 0$. Soient $P_1, \ldots, P_n$ les points de S qui évitent le support de L_∞, on pose alors

$$\Delta := P_1 + \cdots + P_n \quad \text{et} \quad G := L_\infty.$$

On rappelle que U_t désigne la carte affine $\{T \neq 0\} \cap S$ de S.

Codes fonctionnels

Dans le contexte ci-dessus, l'espace $\Gamma(S, \mathcal{L}(G))$ s'identifie à l'espace des polynômes en x, y et z de degré inférieur ou égal à 1. Il est donc de dimension 4. Le code fonctionnel $C_L(\Delta, G)$ est donc un code de longueur n et de dimension 4. La distance minimale de ce type de code dépend du fait que S contienne ou non des droites rationnelles. En effet, la distance minimale de ce code est minorée par $n - l_S$, où l_S désigne le nombre maximal de points rationnels d'une section hyperplane de U_t. Pour minorer cette distance minimale, il faut majorer l_S. Or, l_S est le nombre maximal de points rationnels d'une courbe affine plane de degré 3. Les courbes de degré 3 ayant le plus grand nombre de points rationnels sont les réunions de trois droites rationnelles concourantes (Voir la lettre de Serre à M.Tsfasman [Ser91]).

Ainsi, si la surface S ne contient pas de droite rationnelle (ce qui est possible, voir [SD67]), alors la distance minimale du code fonctionnel est plus grande et le code fonctionnel est meilleur. C'est l'approche adoptée par Voloch et Zarzar dans [Zar07] et [VZ05][5].

Orthogonaux des codes fonctionnels

Dans [VZ05], les auteurs proposent une méthode pour construire de nombreux mots appartenant à l'orthogonal d'un code fonctionnel. Pour ce faire, ils se donnent un famille de courbes lisses $C_1, \ldots, C_r$ tracées sur S. Ensuite, ils considèrent les codes $C_{L,C_i}(D_i, G_i)$ où D_i est la somme des points de $\mathrm{Supp}(\Delta)$ qui appartiennent à C_i et G_i est le tiré en arrière de G sur C_i. Enfin, pour chacun de ces codes fonctionnels sur des courbes, ils en construisent l'orthogonal et en déduisent des mots dans le code $C_L(\Delta, G)^\perp$. Ces mots ont un support contenu dans l'ensemble des indices correspondant aux points de $\mathrm{Supp}(D_i)$. Ils ont donc un poids petit par rapport à la longueur du code. De cette manière, ils peuvent décoder le code $C_L(\Delta, G)$ par le biais d'un algorithme de décodage itératif du type de celui qui nous avons présenté en section V.1. L'algorithme qu'ils utilisent est présenté dans l'article [LM05] de Luby et Mitzenmacher.

Dans ce qui suit, nous allons utiliser les résultats théoriques présentés précédemment pour calculer un grand nombre de mots de poids minimal du code $C_L(\Delta, G)^\perp$. Nous chercherons ensuite à savoir si la famille de mots ainsi construite engendre le code $C_L(\Delta, G)^\perp$. Le cas échéant, l'algorithme min-somme pourra être utilisé pour décoder le code $C_L(\Delta, G)$.

Construction d'un graphe de Tanner

Notre objectif est de construire un graphe de Tanner en vue d'un décodage itératif. D'après ce qui a été vu en section en section V.1, le cahier des charges pour un bon graphe de Tanner repose sur deux contraintes.

(1) Éviter les noeuds de relation dont la valence est trop importante car ils augmentent lourdement la complexité de l'algorithme de décodage.

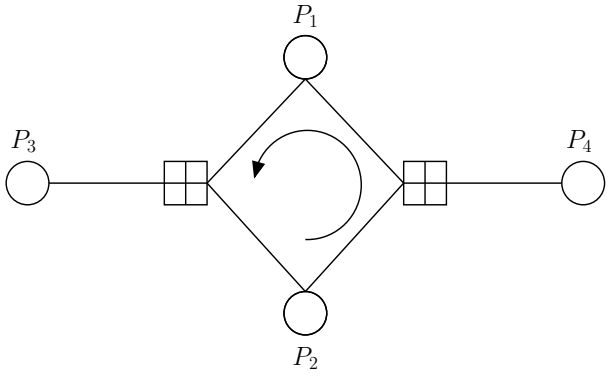
(2) Éviter les *petits cycles*.

Concernant la première contrainte, d'après le théorème IV.1.7 (1), la distance minimale de $C_L(\Delta, G)^\perp$ est supérieure ou égale à 3. De plus les mots de poids 3 de ce code ont pour support les indices de trois points alignés du support de Δ.

On dispose par ailleurs d'une formule explicite (lemme V.3.5) pour calculer les mots correspondant à des triplets de points appartenant à des droites non contenues dans S. Pour ce qui est des autres mots, il est préférable de les éviter afin de répondre à la seconde contrainte du cahier des charges. En effet, soit F une droite rationnelle contenue dans S. Alors, à tout triplet de points de F contenus dans $\mathrm{Supp}(\Delta)$, on associe un mot de poids 3 dans $C_L(\Delta, G)^\perp$. Si l'on note $P_1, \ldots, P_s$ les points de $F(\mathbf{F}_q) \cap \mathrm{Supp}(\Delta)$ et que l'on suppose de $s > 3$, alors les mots correspondant par exemple aux triplets (P_1, P_2, P_4) et (P_1, P_2, P_4) donneront un cycle de longueur[6] 2 dans le graphe de Tanner.

[5] Ces articles sont cités dans leur ordre d'écriture.

[6] On rappelle que la longueur d'un chemin dans un graphe biparti est la moitié du nombre d'arêtes composant ce chemin.



Il est donc préférable de ne pas choisir tous les mots construits à partir de cette droite. Nous avons fait le choix de n'en retenir aucun. Nous allons voir que dans la pratique, à condition que le corps $\mathbf{F}_q$ soit assez grand, les mots issus de triplets de points d'une droite non contenue dans S suffisent à engendrer le code $C_L(\Delta, G)^\perp$. Si de plus on ne considère que ces mots là, on évite les cycles de longueur 2. Les cycles minimaux seront alors de longueur 3 et correspondront à la donnée de trois droites coplanaires non contenues dans S, non concourantes et telles que les points d'intersection de deux d'entre elles sont dans $\mathrm{Supp}(\Delta)$.

V.4.2 Implémentation

Pour construire un graphe de Tanner, nous allons utiliser l'algorithme suivant.

Algorithme de construction d'équations de parité.
Entrées : Une surface cubique lisse de $\mathbf{P}^3$. *Sorties :* Une matrice.

(1) On se donne une liste de mots de codes M, initialement vide ($M := [\,]$).

(2) On crée l'ensemble $Points$ des points rationnels de la carte affine U_t de S.

(3) On crée un second ensemble PointsBis qui est initialisé à $PointsBis := Points$.

(4) Pour $P \in Points$
- Enlever P de $PointsBis$.
- Pour $Q \in PointsBis$,
  - Si la droite (PQ) n'est pas contenue dans S et contient exactement trois éléments de $Points$, alors on construit le mot de code c correspondant par la formule du lemme V.3.5 et on ajoute c dans la liste M.
  - Sinon, on ne fait rien.

(5) On construit une matrice dont les lignes sont les éléments de M.

Remarque V.4.1. *Un programme Magma de cet algorithme est donné en annexe F.2.*

Une question se pose ensuite, *La matrice ainsi construite est-elle une matrice génératrice de $C_L(\Delta, G)^\perp$?* Remarquons que le code $C_L(\Delta, G)$ est de dimension 4. Aussi, pour vérifier qu'une matrice obtenue par l'algorithme ci-dessus est bien génératrice de $C_L(\Delta, G)^\perp$, il suffit de vérifier qu'elle est de rang $n-4$. Les expérimentations présentées dans le tableau ci-dessous montrent qu'en général la matrice obtenue est bien une matrice génératrice de l'orthogonal. Nous ne sommes toutefois pas parvenus à fournir une preuve théorique de ce fait.

Dans le tableau qui suit, nous présentons une série d'expériences. Le test de base est le suivant. Pour une surface cubique lisse sur un corps $\mathbf{F}_q$ avec $q > 2$ on calcule une matrice en utilisant l'algorithme ci-dessus. Ensuite, on calcule le rang de cette matrice et le compare avec $n - 4$. S'il y a égalité le test est positif sinon il est négatif.

Voici les résultats de tests sur des surfaces choisies de façon aléatoire pour différents corps de base.

Corps de base	Nombre de tests effectués	Nombre de tests positifs	%	Écart moyen	Longueur moyenne
$\mathbf{F}_3$	10000	1139	$11,39\%$	$2,15$	$8,80$
$\mathbf{F}_4$	10000	6274	$62,64\%$	$1,96$	$15,88$
$\mathbf{F}_5$	10000	9763	$97,63\%$	$1,82$	$24,90$
$\mathbf{F}_7$	1000	1000	100%	–	$48,66$
$\mathbf{F}_8$	500	500	100%	–	$64,05$
$\mathbf{F}_9$	500	500	100%	–	$81,008$

Les deux dernières colonnes fournissent les quantités suivantes.

- **Écart moyen.** C'est la moyenne sur l'ensemble des tests négatifs de la quantité $n - 4 - \mathrm{Rang}(M)$, où M désigne la matrice construite grâce à l'algorithme ci-dessus.

$$\textbf{Écart moyen} = \frac{n - 4 - \mathrm{Rg}(M)}{\textbf{Nombre de tests négatifs}}.$$

- **Longueur moyenne.** C'est la longueur moyenne des codes construits, c'est-à-dire le nombre moyen de points rationnels des cartes affines U_t des surfaces cubiques testées.

$$\textbf{Longueur Moyenne} = \frac{\textbf{Longueur du code}}{\textbf{Nombre de tests effectués}}.$$

  On remarque dans le tableau ci-dessus que cette longueur moyenne est proche de q^2, ce qui est naturel puisque le nombre de points rationnels d'une surface cubique affine lisse est lui-même proche de q^2.

Remarque V.4.2. *Lorsque la taille du corps grandit, le nombre moyen de points rationnels d'une surface cubique augmente de façon quadratique en la taille du corps, ce qui contribue à augmenter lourdement la complexité de l'algorithme. C'est la raison pour laquelle le nombre de tests est moins important lorsque le corps de base est plus grand.*

Conclusion. Il semble très probable que pour $q \geq 7$, le code $C_L(\Delta, G)^\perp$ ainsi construit soit engendré par ses mots de poids 3. Il serait d'ailleurs intéressant d'obtenir une démonstration mathématique de ce résultat (si du moins il est vrai).

V.4.3 Codes sur des surfaces quartiques

Nous avons réalisé le même type d'expérience dans le cas où S est une surface de degré 4 et $G \sim 2L_S$. Voici les résultats de l'expérience.

Corps de base	Nombre de tests effectués	Nombre de tests positifs	%	Écart moyen	Longueur moyenne
$\mathbf{F}_4$	1000	40	4%	5.11	15.9
$\mathbf{F}_5$	1000	0	0%	9.66	24.57
$\mathbf{F}_7$	1000	204	$20,4\%$	8.87	48.71
$\mathbf{F}_8$	1000	633	$63,3\%$	$5,37$	$64,14$
$\mathbf{F}_9$	1000	894	$89,4\%$	$2,7$	$80,98$
$\mathbf{F}_{11}$	1000	999	$99,9\%$	1	$121,233$
$\mathbf{F}_{13}$	1000	1000	100%	–	$168,711$

La conclusion est sensiblement la même que pour l'expérience sur les cubiques. Il semble que l'orthogonal du code fonctionnel soit engendré par ses mots de poids 4 à condition que le cardinal du corps de base soit suffisamment grand.

V.4.4 Utilisation de l'algorithme min-somme pour le décodage de ces codes.

Le graphe de Tanner construit de cette manière offre de bonne perspectives de décodage. Reprenons par exemple la surface donnée par Voloch et Zarzar dans [VZ05], c'est-à-dire la surface S sur $\mathbf{F}_3$ d'équation

$$X^3 + Y^3 + Z^3 - ZX^2 - XY^2 - YZ^2 + XZ^2 + T^3.$$

Les auteurs montrent dans l'article cité ci-dessus que le code $C_{L,S}(\Delta, G)$, où G est la section plane à l'infini, est un code de longueur 13, de dimension 4 et de distance minimale 7.

Les points rationnels de cette surface sont

$$\begin{array}{lllllllll} P_1 &=& (2:0:0:1) & P_2 &=& (1:0:1:1) & P_3 &=& (0:0:2:1) \\ P_4 &=& (1:0:2:1) & P_5 &=& (2:1:1:1) & P_6 &=& (0:1:2:1) \\ P_7 &=& (2:1:2:1) & P_8 &=& (0:2:0:1) & P_9 &=& (1:2:0:1) \\ P_{10} &=& (2:2:0:1) & P_{11} &=& (2:2:1:1) & P_{12} &=& (0:2:2:1) \\ P_{13} &=& (2:2:2:1) & & & & & & \end{array}$$

et ils évitent tous le support de G. Si maintenant, on applique l'algorithme, les droites qui coupent S en exactement trois points rationnels sont les treize droites ci-dessous.

$$\begin{array}{lllll} L_1 &=& \{x+t=0,\ y+z=0\} & L_2 &=& \{x+t=0, y+2z=0\} \\ L_3 &=& \{x+z+t=0,\ y=0\} & L_4 &=& \{x+z+t=0, y+2z+t=0\} \\ L_5 &=& \{x+2z=0,\ y+2z+t=0\} & L_6 &=& \{x=0, z+t=0\} \\ L_7 &=& \{x+2z+2t=0,\ y+z+t=0\} & L_8 &=& \{x+2y+2t=0, z+t=0\} \\ L_9 &=& \{x+y+2t=0,\ z+t=0\} & L_{10} &=& \{x+z=0, y+z+t=0\} \\ L_{11} &=& \{y+t=0,\ z=0\} & L_{12} &=& \{x+2z+2t=0, y+t=0\} \\ L_{13} &=& \{x+t=0,\ y+t=0\} & & & \end{array}$$

Enfin, par la formule du lemme V.3.5, on obtient la matrice

$$M = \begin{pmatrix} 2&0&0&0&0&0&2&0&0&0&2&0&0 \\ 2&0&0&0&2&0&0&0&0&0&0&0&2 \\ 2&2&2&0&0&0&0&0&0&0&0&0&0 \\ 0&2&0&0&0&0&2&2&0&0&0&0&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&0&2&0&2&0&0&0&2&0&0&0&0 \\ 0&0&1&0&0&1&0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&1&0&0&0&0&1&0 \\ 0&0&0&1&0&1&0&0&0&0&0&0&1 \\ 0&0&0&1&1&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&2&2&2&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&1&1&0 \\ 0&0&0&0&0&0&0&0&0&2&2&0&2 \end{pmatrix}$$

On vérifie que la matrice M est de rang : $9 = 13 - 4$. Elle vérifie bien la relation $\mathrm{Rg}(M) = n - \dim C_L$, la matrice M est donc bien génératrice du code $C_L(\Delta, G)^\perp$. On peut l'utiliser pour implémenter un algorithme de décodage min-somme pour le code $C_L(\Delta, G)$.

Conclusion

Pour construire des codes différentiels à partir de surfaces algébriques, nous avons développé le matériel théorique nécessaire à l'obtention d'une formule de sommation de résidus en dimension 2. Ce résultat était déjà connu et dans un contexte plus général que celui des surfaces (voir [Har66], [Par76] et [Lip84]). Cependant, l'approche adoptée dans le premier chapitre fournit des constructions explicites et une démonstration plus accessible de cette formule.

Dans un second temps, on montre qu'un certain nombre de propriétés vérifiées par les codes différentiels construits sur les courbes s'étendent aux codes différentiels construits sur les surfaces. En fait, seule la relation d'orthogonalité ne s'étend pas parfaitement. Le théorème de réalisation est, en un certain sens, une manière de remédier à ce défaut d'inclusion réciproque dans la relation "$C_\Omega \subset C_L^\perp$".

Pour le reste, cette absence d'inclusion réciproque rend, d'une certaine manière, l'étude des codes géométriques construits sur des surfaces plus riche que celle des codes construits sur des courbes. En effet, dans le contexte des surfaces algébriques, les codes fonctionnels n'appartiennent plus en général à la même classe de codes que leurs orthogonaux.

Pour finir, rappelons que l'étude de ces deux classes de codes ouvre d'intéressants problèmes de théorie des codes et de géométrie algébrique que nous rappelons une dernière fois afin de conclure cette thèse. Commençons par énoncer les différentes questions posées tout au long de ce texte.

Question 1. *Peut-on estimer les paramètres des codes qui sont l'orthogonal de codes fonctionnels ?*

Question 2. *Si l'orthogonal d'un code fonctionnel ne peut se réaliser comme un code différentiel associé à une paire de diviseurs (sous-)Δ-convenables, peut-on le réaliser comme somme de tels codes ?*

Question 2bis. *Étant donné un mot de code c appartenant à $C_{L,S}(\Delta, G)^\perp$, existe-t-il une paire de diviseurs (sous-) Δ-convenable (D_a, D_b) et une 2-forme ω appartenant à $\Gamma(S, \Omega^2(G - D_a - D_b))$ et telle que*

$$c = res^2_{D_a,\Delta}(\omega) \ ?$$

Question 3. *Le résultat du théorème de réalisation(théorème III.4.1) reste-t-il vrai si l'on élimine l'hypothèse III.4 sur S et G (S est intersection complète et G est linéairement équivalent à l'intersection de G avec une hypersurface) ?*

Question 4. *Sous les conditions du corollaire III.4.2, peut-on estimer le nombre de minimal de codes différentiels dont la somme est égale à l'orthogonal d'un code fonctionnel en fonction d'invariants géométriques de la surface ?*

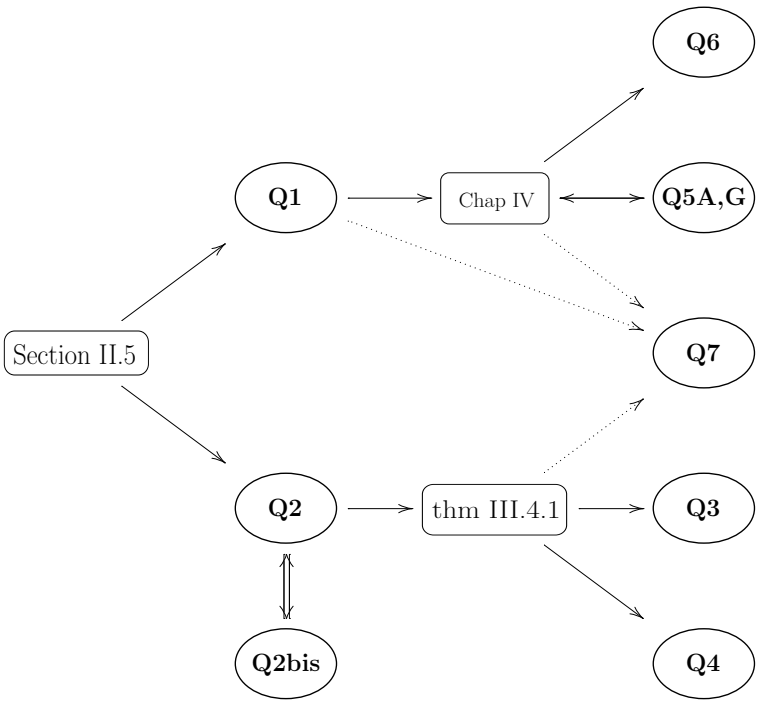
Question 5 (Arithmétique)**.** *Soient X une variété projective lisse géométriquement intègre sur un corps fini $\mathbf{F}_q$ et $P_1, \ldots, P_n$, une famille de points fermés de X. Peut-on évaluer explicitement ou majorer de façon précise le plus petit entier d tel qu'il existe au moins une hypersurface définie sur $\mathbf{F}_q$ de degré inférieur ou égal à d qui interpole tous les P_i et dont l'intersection schématique avec X soit une sous-variété lisse géométriquement intègre de codimension 1 ?*

Question 5 (Géométrique)**.** *Soit X une variété projective irréductible lisse définie sur $\overline{\mathbf{F}}_q$ et $P_1, \ldots, P_n$ une famille de points de X. Peut-on évaluer explicitement ou majorer de façon précise le plus petit entier d tel qu'il existe au moins une hypersurface H de degré inférieur ou égal à d, qui contienne tous les P_i et telle que $H \cap X$ soit une sous-variété lisse de codimension 1 de X ?*

Question 6. *Sachant que les deux premières configurations minimales de points rationnels m-liés dans $\mathbf{P}^N$ sont la donnée de $m+2$ points alignés et $2m+2$ points sur une même conique plane, quelles sont les configurations minimales suivantes.*

Question 7. *Soient X une sous-variété irréductible lisse géométriquement intègre de $\mathbf{P}^r_{\overline{\mathbf{F}}_q}$ et d un entier naturel. Soient $P_1, \ldots, P_n$ une famille de points de X. Sous quelles conditions sur X et $P_1, \ldots, P_n$ a-t-on l'existence d'un entier s tel que pour tout s-uplet de points parmi $P_1, \ldots, P_n$, il existe une hypersurface H de degré d contenant ce s-uplet de points et telle que $H \cap X$ soit une sous-variété lisse de codimension 1 de X ?*

Le diagramme suivant représente les relations entre ces questions ainsi que certaines parties ou résultat de cette thèse. Une flèche $A \to B$ doit se lire "A motive B" lorsque B est une question et "B répond à A" lorsque A est une question. les flèches pointillées signifient que les questions/résultats/parties ne sont qu'indirectement liés.



Nous conclurons en rappelant les perspectives qu'ouvriraient certaines questions ou problèmes ouverts. En particulier, une solution aux problèmes portant sur des systèmes linéaires de type Bertini posés par les questions 5 A et G fournirait une méthode d'estimation de la distance minimale de codes fonctionnels sur des surfaces ou même des variétés de dimension supérieures. Quant à la question 7 qui peut être vue comme une variante des 5 A et G, une réponse à cette dernière fournirait une élégante méthode d'estimation de la distance minimale de l'orthogonal d'un code fonctionnel sur une surface algébrique.

Annexes

Annexe A

Séries de Laurent

Les maths, ça s'écrit comme du français...
...les formules en plus.

Marc Perret

Cette première annexe contient toutes les démonstrations techniques relatives aux séries de Laurent et aux formes différentielles formelles.

A.1 Sur les modules de différentielles relatives

Le but est de démontrer le lemme I.4.16 sur les modules de différentielles relatives. Le résultat peut sembler assez élémentaire, cependant, les opérations de complétions et de passage au module des différentielles relatives ne commutent pas en général (voir [Eis95] ex 16.14). Nous avons donc choisi d'en donner une preuve détaillée faute de référence.

On se place dans le cadre décrit en I.2. On dispose de plus d'une (P,C)-paire faible sur S (voir définition I.4.9).

Étape 1. Commençons par montrer que

$$\Omega^1_{k((u))/k} \cong \Omega^1_{k(C)/k} \otimes_{k(C)} k((u)).$$

On sait que $\Omega^1_{k(C)/k}$ est un $k(C)$-espace vectoriel de dimension 1. De plus, $\bar{u}$ étant une uniformisante de $\mathcal{O}_{C,P}$, c'est un élément séparant de $k(C)/k$, donc la forme $d\bar{u}$ est non nulle sur C et engendre donc $\Omega^1_{k(C)/k}$ sur $k(C)$. Il suffit donc de montrer que du engendre $\Omega^1_{k((u))/k}$ sur $k((u))$. D'après [Mat86] ex 25.3, l'application $d : k((u)) \to \Omega^1_{k((u))/k}$ est continue pour la topologie (u)-adique. Cela implique que pour tout $f \in k((u))$, on a $df = f'(u)du$ où f' est la dérivée formelle de f par rapport à u. Par conséquent, tout élément de $\Omega^1_{k((u))/k}$ étant une somme finie d'éléments de la forme $fdg = fg'du$, on en déduit que $\Omega^1_{k((u))/k}$ est engendré par du sur $k((u))$.

Étape 2. Montrons maintenant que $\Omega^1_{k((u))((v))/k} \cong \Omega^1_{k(S)/k} \otimes_{k(S)} k((u))((u))$. Comme $\Omega^1_{k(S)/k}$ est librement engendré par du et dv sur $k(S)$, le module $\Omega^1_{k(S)/k} \otimes_{k(S)} k((u))((u))$ est librement engendré par du et dv sur $k((u))((v))$. Considérons l'application

$$\delta : \left\{ \begin{array}{ccc} k((u))((v)) & \to & \Omega^1_{k(S)/k} \otimes_{k(S)} k((u))((u)) \\ f & \mapsto & \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy \end{array} \right. .$$

Cette application est une dérivation. Donc, d'après la propriété universelle du module des différentielles, il existe un unique morphisme $\bar{\delta}$ qui fasse commuter le diagramme suivant

$$\begin{array}{ccc} k((u))((v)) & \xrightarrow{\delta} & \Omega^1_{k(S)/k} \otimes_{k(S)} k((u))((u)) \ . \\ \downarrow d & \nearrow_{\bar{\delta}} & \\ \Omega^1_{k((u))((v))/k} & & \end{array}$$

De fait, les différentielles du et dv appartenant à $\Omega^1_{k((u))((v))/k}$ sont respectivement envoyées par $\bar{\delta}$ sur du et dv appartenant à $\Omega^1_{k(S)/k} \otimes_{k(S)} k((u))((v))$. Par conséquent, ces deux formes différentielles sont linéairement indépendantes sur $k((u))((v))$ dans $\Omega^1_{k((u))((v))/k}$. Ce dernier est donc de dimension au moins 2 sur $k((u))((v))$, mais, d'après [Mat86] théorème 25.1, les injections successives

$$k \to k((u)) \to k((u))((v))$$

donnent une suite exacte

$$\Omega^1_{k((u))/k} \otimes_{k((u))} k((u))((v)) \longrightarrow \Omega^1_{k((u))((v))/k} \longrightarrow \Omega^1_{k((u))((v))/k((u))} \longrightarrow 0 \ .$$

Remarque A.1.1. *Cette suite exacte est en général appelée première suite exacte fondamentale ([Har77] proposition II.8.3.A).*

D'après l'étape 1, l'espace $\Omega^1_{k((u))((v))/k((u))}$ est de dimension 1 sur $k((u))((v))$ et engendré par dv. De même, $\Omega^1_{k((u))/k} \otimes_{k((u))} k((u))((v))$ est de dimension 1 et engendré sur $k((u))((v))$ par du. L'espace $\Omega^1_{k((u))((v))/k}$ est donc de dimension au plus 2. On conclut qu'il est de dimension 2 et librement engendré par du et dv.

Étape 3. Pour conclure quant à l'isomorphisme $\Omega^2_{k((u))((v))/k} \cong \Omega^2_{k(S)/k} \otimes_{k(S)} k((u))((v))$, il suffit de remarquer que

$$\Omega^2_{k((u))((v))/k} = \bigwedge^2 \Omega^1_{k((u))((v))/k}.$$

A.2 Démonstration du lemme I.5.8

Pour commencer nous allons introduire deux applications. La première est notée J (comme Jacobien), et est définie par

$$J : \left\{ \begin{array}{ccc} k((u))((v))^2 & \to & k((u))((v)) \\ (A,B) & \mapsto & \frac{\partial A}{\partial u}\frac{\partial B}{\partial v} - \frac{\partial A}{\partial v}\frac{\partial B}{\partial u} \end{array} \right. .$$

La seconde est notée ρ est définie par

$$\rho : \left\{ \begin{array}{ccc} k((u))((v)) & \to & k((u)) \\ \sum_{i \geq -n} h_i(u)v^i & \mapsto & h_{-1}(u) \end{array} \right. .$$

Lemme A.2.1. *Soient A, B deux éléments de $k((u))((v))$, alors il existe une série de Laurent $\phi \in k((u))$ telle que*

$$\rho \circ J(A,B) = \phi'(u),$$

où $\phi'(u)$ désigne la dérivée formelle d'une série de Laurent $\phi \in k((u))$.

Preuve. Comme les applications ρ et J sont respectivement k-linéaire et k-bilinéaire antisymétrique, on peut démontrer le lemme en ne considérant que les trois situations ci-dessous. Le résultat s'en déduira en utilisant ces propriétés de linéarité et d'antisymétrie.

(1) A et B sont éléments de $k((u))[[v]]$.

(2) $A \in k((u))[[v]]$ et B est de la forme $B = \frac{b(u)}{v^n}$ avec $n \in \mathbf{N}^*$ et $b(u) \in k((u))$.

(3) $A = \frac{a(u)}{v^m}$ et $B = \frac{b(u)}{v^n}$ avec $m, n \in \mathbf{N}^*$ et $a(u), b(u) \in k((u))$.

Traitons séparément ces trois situations.

Cas 1. Les séries A et B n'ont pas de pôle suivant la variable v, leurs dérivées partielles non plus, donc $\rho \circ J(A,B) = 0$.

Cas 2. La série A est de la forme, $A = \sum_{i\geq 0} a_i(u)v^i$. Le calcul de $J(A,B)$ donne

$$J(A,B) = \sum_{i\geq 0} a_i'(u)b(u)(-n)v^{i-n-1} - \sum_{i\geq 0} a_i(u)b'(u)iv^{i-n-1}.$$

On a donc

$$\rho(J(A,B)) = -n(a_n'(u)b(u) + a_n(u)b'(u)) = (-na_n(u)b(u))'.$$

Cas 3. On a,

$$J(A,B) = \left(-n\frac{a'(u)b(u)}{v^{m+n+1}} - (-m)\frac{a(u)b'(u)}{v^{m+n+1}}\right).$$

Comme m et n sont supposés strictement positifs, il n'y a pas de terme en v^{-1} et $\rho(J(A,B)) = 0$.

□

Par conséquent, soit (A,B) une paire d'éléments de $k((u))((v))$. Un calcul simple montre que $dA \wedge dB = J(A,B)$. De ce fait,

$$(u,v)\mathrm{res}^1(dA \wedge dB) = \rho(J(A,B))du.$$

D'après le lemme précédent, il existe $\phi \in k((u))$ tel que ce 1-résidu est égal à $\phi'(u)du$. Cette 1-forme n'a donc pas de terme en du/u et on a

$$(u,v)\mathrm{res}^2(dA \wedge dB) = 0.$$

Pour finir, noter que si une 2-forme formelle $\omega \in \Omega^2_{k((u))((v))/k}$ est de la forme $\omega = dA \wedge dB$ pour $A, B \in k((u))((v))$ et que (x,y) est un couple de séries lié à (u,v) par un changement de variables de le forme (CV)[1], alors ω est de la forme $dA' \wedge dB'$ pour $A', B' \in k((x))((y))$. Les séries A' et B' ne sont autres que $A(f(x,y),g(x,y))$ et $B(f(x,y),g(x,y))$. De fait le travail effectué ci-dessus permet de déduire que

$$(x,y)\mathrm{res}^2(\omega) = 0$$

et ce, pour tout couple (x,y) lié à (u,v)par un changement de variables de la forme (CV).

A.3 Topologie de $k((u))[[v]]$

Le but de cette section est de prouver le lemme I.4.17. Pour ce faire, nous allons introduire quelques notions de topologie sur $k((u))[[v]]$. La première question à se poser est : *de quelle topologie doit-on munir* $k((u))[[v]]$ *?* Il pourrait sembler logique de le munir de la topologie associée à la valuation (v)-adique, c'est-à-dire, la topologie rendant l'addition continue et telle que les idéaux $\{(v^n), n \in \mathbf{N}\}$ forment une base de voisinage de 0. Le défaut d'un tel choix est que pour cette topologie, la suite de terme général $(u^n)_{n\in\mathbf{N}}$ diverge. On souhaiterait donc munir $k((u))[[v]]$ d'une topologie qui tiendrait compte à la fois de la valuation (v)-adique mais également de la valuation (u)-adique sur $k((u))$. Pour ce faire, on rappelle que $k((u))[[v]]$ est une limite projective

$$k((u))[[v]] \cong \varprojlim k((u))[v]/(v^n).$$

De fait, si l'on munit $k((u))$ de sa topologie (u)-adique, on définit une topologie de limite projective sur $k((u))[[v]]$. Les ensembles suivants fournissent une base de voisinages de 0 pour cette topologie.

$$V_{i_0,\ldots,i_r} := \left\{ s = \sum_{j\geq 0} s_j(u)v^j \in k((u))[[v]], \quad \mathrm{val}_{(u)}(s_k) \geq i_k, \quad \forall k \in \{0,\ldots,r\} \right\}.$$

[1] Voir lemme I.4.15.

On rappelle que $\mathrm{val}_{(u)}$ désigne la valuation (u)-adique sur $k((u))$. Pour cette topologie, une suite $(s^{(n)})_{n\in\mathbf{N}}$ de séries converge vers 0 si et seulement si elle converge vers 0 *coordonnée par coordonnée*. C'est-à-dire :

$$\lim_{n\to+\infty} s^{(n)} = 0 \quad \Longleftrightarrow \quad \forall j \in \mathbf{N},\ \lim_{n\to+\infty} s_j^{(n)}(u) = 0.$$

Lemme A.3.1. *Pour cette topologie, une série est convergente si et seulement si son terme général tend vers* 0.

Preuve. Soit $(s^{(n)})_{n\in\mathbf{N}}$ une suite qui tend vers 0 pour la topologie de la limite projective. Cela signifie que pour tout entier naturel j, la suite $(s_j^{(n)})$ d'éléments de $k((u))$ converge vers 0 pour la topologie (u)-adique. La topologie (u)-adique provenant d'une norme ultramétrique, on en déduit que pour tout entier naturel j, la série de terme général $s_j^{(n)}$ converge. Donc la suite des sommes partielles $(\sum_{k=0}^{n} s^{(k)})_{n\in\mathbf{N}}$ converge coordonnée par coordonnée, elle converge donc pour la topologie de la limite projective. □

Remarque A.3.2. *La topologie de limite projective est moins fine que la topologie (v)-adique. On note par exemple que la topologie (v)-adique induit sur $k((u))$ une topologie discrète. De fait, une suite $(s^{(n)})_n$ qui converge (v)-adiquement vers une certaine limite s, converge vers cette même limite pour la topologie de la limite projective.*

Nous avons à présent les cartes en main pour démontrer le lemme I.4.17.

Démonstration du lemme I.4.17. Pour commencer, remarquons qu'il suffit de prouver que changement de variable est bien défini sur $k((u))[[v]]$ et induit un isomorphisme local $k((u))[[v]] \to k((x))[[y]]$. La propriété universelle des corps de fractions permettra ensuite de conclure.

Étape 1. Nous allons montrer que la suite $(f^n)_{n\in\mathbf{N}}$ converge vers 0 pour la topologie de limite projective. Rappelons que f est un élément de $k((x))[[y]]$ de la forme

$$f = f_0(x) + f_1(x)v + \cdots$$

et que la valuation (x)-adique de f_0 est égale à 1. Soient $n \in \mathbf{N}$ et $k \leq n$, on a

$$f^n = f_0^n + f_0^{n-1} f_1 y + f_0^{n-2}(f_1^2 + f_2)y^2 + \cdots + f_0^{n-k} P_k(f_1, \ldots, f_k)y^k + \cdots,$$

où P_k désigne un polynôme en les séries de Laurent $f_0, \ldots, f_k$. Ce polynôme ne dépend pas de n. Nous donnons ci-dessous, les premiers termes de cette suite de polynômes.

$$\begin{array}{lcllcl} P_0 &=& 1 & P_3 &=& f_1^3 + 2f_1f_2 + f_3 \\ P_1 &=& f_1 & P_4 &=& f_1^4 + 2f_1f_3 + f_2^2 + f_4 \\ P_2 &=& f_1^2 + f_2 & P_5 &=& f_1^5 + 2f_1f_4 + 2f_2f_3 + f_5. \end{array}$$

Ainsi, étant donné $i \in \mathbf{N}$, pour n assez grand, le coefficient de y^i dans f^n sera égal à $f_0^{n-i} P_i(f_0, \ldots, f_i)$. Comme f_0 est de valuation (x)-adique 1, le coefficient de y^i tend vers 0 quand n tend vers l'infini. La suite $(f^n)_n$ converge donc vers 0 pour la topologie de limite projective. Par conséquent, pour toute série $\varphi(u) \in k((u))$, la série $\varphi(f(x,y))$ converge dans $k((x))[[y]]$. Remarquons enfin que le coefficient en y^0 de la série $\varphi(f(x,y))$ est $\sum_i \varphi_i f_0^i$. Cette dernière série est non nulle, car f_0 est de valuation (x)-adique 1. De fait, la valuation (y)-adique de $\varphi(f(x,y))$ est nulle.

Étape 2. Soit $\psi(u,v) \in k((u))[[v]]$ de la forme $\psi = \sum_{j\geq 0} \psi_j(u)v^j$. D'après l'étape 1, pour tout $j \in \mathbf{N}$, la série $\psi_j(f(x,y))$ est bien définie. Ensuite, comme g est de valuation (y)-adique 1, la série $\psi_j(f)g^j$ est de valuation (y)-adique supérieure ou égale à j. Donc, d'après le lemme A.3.1 et la remarque A.3.2, la série de terme général $\psi_j(f)g^j$ converge dans $k((x))[[y]]$. Le changement de variables est donc bien défini. Par ailleurs, on a vu à la fin de l'étape 1 que la valuation (y)-adique d'un coefficient $\psi_j(f(x,y))$ est nulle. Donc, comme la série g est de valuation (y)-adique 1, on déduit que la valuation (y)-adique de $\psi(f(x,y), g(x,y))$ est égale à la valuation (v)-adique de $\psi(u,v)$.

Étape 3. Il nous reste à traiter le cas des 2-formes différentielles formelles. Soit donc une forme différentielle formelle $\omega = h(u,v)du \wedge dv$ de valuation (v)-adique n, montrons que la valuation (y)-adique de $h(f,g)df \wedge dg$ est également n. En utilisant les étapes précédentes, cela revient à montrer que $df \wedge dg$ est de valuation (y)-adique nulle. On a,

$$df \wedge dg = \left(\frac{\partial f}{\partial x}\frac{\partial g}{\partial y} - \frac{\partial f}{\partial y}\frac{\partial g}{\partial x}\right) dx \wedge dy.$$

Calculons les premiers termes de ces produits de dérivées partielles

$$\begin{aligned}\frac{\partial f}{\partial x}\frac{\partial g}{\partial y} &= f_0'(x)g_1(x) + (2f_0'(x)g_2(x) + g_1(x)f_1'(x))y + \cdots \\ \frac{\partial f}{\partial y}\frac{\partial g}{\partial x} &= f_1(x)g_1'(x)y + (2f_2(x)g_1'(x) + f_1(x)g_2'(y))y^2 + \cdots\end{aligned}$$

Par définition du changement de variables (CV), les séries f_0' et g_1 sont non nulles, on en déduit que le jacobien $\frac{\partial f}{\partial x}\frac{\partial g}{\partial y} - \frac{\partial f}{\partial y}\frac{\partial g}{\partial x}$ est de valuation (y)-adique nulle, ce qui achève cette démonstration. □

A.4 Démonstration du théorème I.5.3 en caractéristique positive

Cette section concerne les formes différentielles formelles. Les notations et définitions utilisées proviennent des sections I.4.5 et I.5.1.

Remarque A.4.1. *Dans cette section nous utilisons le système d'indexage de la notation I.5.1.*

Commençons par étudier quelles parties de la preuve du théorème I.5.3, nécessitent vraiment le fait que le corps k est de caractéristique nulle. Les lemmes I.5.4 et I.5.6 ainsi que la remarque I.5.5 sont valables en caractéristique quelconque. Seule la preuve à proprement parler du théorème, qui commence page 36 et se termine page 38 fait intervenir des primitives formelles qui n'existent pas toujours en caractéristique positive. Nous allons donc reprendre l'étude du comportement sous l'action de (CV2) de différentielles de la forme

$$\omega = \phi(u)du \wedge \frac{dy}{y^{n+1}} \quad \text{où} \phi \in k((u)) \quad \text{et} \quad n \geq 1.$$

Soit $N \in \mathbf{N}$, considérons un changement de variables de la forme (CV2) :

$$u = f(x,y) \quad \text{avec} \quad f = \sum_{j\geq 0} f_j(x)y^j$$

où f_0 est de valuation (x)-adique 1. On suppose de plus que

$$\min_{k=1\ldots n}\{\mathrm{val}_{(x)}(f_k)\} = -N, \tag{A.1}$$

où $\mathrm{val}_{(x)}$ désigne la valuation (x)-adique sur $k((x))$.

Étape 1. Si ω est de la forme $\omega = u^m du \wedge \frac{dy}{y^{n+1}}$ avec $m \in \mathbf{N}$. On a alors,

$$\omega = \underbrace{(f_0'(x) + f_1'(x)y + \cdots)}_{\frac{\partial f}{\partial x}}\underbrace{(f_0(x) + f_1(x)y + \cdots)^m}_{f^m} dx \wedge \frac{dy}{y^{n+1}}.$$

Le (x,y)-1-résidu de ω est le coefficient en y^{n-1} de la série $f^m \partial f/\partial x$. Ce résidu est de la forme

$$(x,y)\mathrm{res}^1_{C,P}(\omega) = P_{m,n}(f_0,\ldots,f_n,f_0',\ldots,f_n')dx, \tag{A.2}$$

où $P_{m,n} \in \mathbf{Z}[X_0, \dots X_n, Y_0, \dots, Y_n]$ est un polynôme qui ne dépend pas du corps de base, il ne dépend en fait que de m et n. Par un raisonnement analogue, le coefficient $p_{m,n}$ en x^{-1} de $P_{m,n}$ est une expression polynomiale en les $f_{i,j}$ avec

$$-N \leq i \leq N+1 \quad \text{et} \quad 0 \leq j \leq n.$$

En effet, $P_{m,n}$ est un polynôme en les f_j et f'_j pour $j \in \{0, \dots, n\}$ ce qui explique l'encadrement de j. Pour ce qui en de l'encadrement de i, on rappelle que, d'après (A.1), les séries de Laurent $f_0, \dots, f_n$ sont de valuation supérieure ou égale à $-N$. Leurs dérivées sont donc de valuation (x)-adique supérieure ou égale à $-N-1$ et donc les termes de degré en x maximal intervenant dans cette expression sont ceux de degré en x égal à N. Ces termes peuvent être des $f_{N,j}x^N$ provenant de $f_j(x)$ ou des $(N+1)f_{N+1,j}x^N$ provenant de $f'_j(x)$. Ainsi, l'indice i est donc toujours inférieur à $N+1$. Pour finir, d'après la preuve du théorème I.5.3 en caractéristique nulle, on sait que l'expression polynomiale $p_{m,n}$ s'annule sur l'ensemble $\{f_{1,0} \neq 0\}$. Ainsi, d'après le théorème de prolongement des identités algébriques ([Bou59] IV.2.3 théorème 2), ce polynôme est nul. Donc, le (x,y)-2-résidu de ω est nul.

Étape 2. Supposons à présent que ω soit de la forme $\omega = \phi(u)du \wedge \frac{dy}{y^{n+1}}$ où $\phi = \sum_{m\geq 0} \phi_i u^i$ est une série de Taylor (un élément de $k[[u]]$). D'après le travail effectué dans l'étape 1, on a

$$(x,y)\mathrm{res}^1(\omega) = \sum_{m\geq 0} \phi_m P_{m,n}(f_0, \dots, f_n, f'_0, \dots, f'_n)dx, \tag{A.3}$$

où les $P_{m,n}$ sont les polynômes définis dans la relation (A.2) de l'étape 1. Le (x,y)-1-résidu de ω est bien défini, donc la série apparaissant en (A.3) converge (x)-adiquement dans $k((x))$. Par conséquent, la valuation (x)-adique de ses termes tend vers l'infini quand m tend vers l'infini, elle est donc positive à partir d'un certain rang M. On a donc

$$(x,y)\mathrm{res}^1_{C,P}(\omega) = \sum_{m=0}^{M} \phi_m P_m dx + \underbrace{\sum_{m=M+1}^{+\infty} \phi_m P_m dx}_{\mathrm{val}_{(x)} \geq 0}.$$

Le reste de la série étant de valuation (x)-adique positive, son résidu est nul. Quant à la somme de 0 à M, son résidu est nul d'après le résultat obtenu dans l'étape 1 et étendu par linéarité. Ici encore, le (x,y)-2-résidu de ω est nul.

Étape 3. Supposons maintenant que ω est de la forme $\omega = \frac{du}{u^m} \wedge \frac{dy}{y^{n+1}}$, avec $m \in \mathbf{N}^*$. Après changement de variables, on obtient

$$\omega = \frac{1}{f^m}\frac{\partial f}{\partial x}dx \wedge \frac{dy}{y^{n+1}}.$$

Le (x,y)-1-résidu de ω est égal au coefficient en y^n de $\frac{1}{f^m}\frac{\partial f}{\partial x}$ multiplié par dx. Nous devons donc étudier la série $\frac{1}{f^m}\frac{\partial f}{\partial x}$. Commençons par travailler sur $\frac{1}{f^m}$. On a

$$\begin{aligned} \frac{1}{f^m} &= \frac{1}{f_0^m\left(1 + \frac{f_1}{f_0}y + \frac{f_2}{f_0}y^2 + \cdots\right)^m} \\ &= \frac{1}{f_0^m}\left(1 + \frac{U_1(f_0,f_1)}{f_0}y + \cdots + \frac{U_p(f_0,\dots,f_p)}{f_0^2}y^2 + \cdots\right)^m, \end{aligned}$$

où $U_p \in \mathbf{Z}[X_0, \dots, X_p]$ est un polynôme homogène de degré p qui ne dépend que de p. Voici les premiers termes de cette suite de polynômes

$$\begin{aligned} U_1(X_0,X_1) &= -X_1 \\ U_2(X_0,X_1,X_2) &= -X_0X_2 + X_1^2 \\ U_3(X_0,X_1,X_2,X_3) &= -X_0^2X_3 + 2X_0X_1X_2 - X_1^3 \\ U_4(X_0,X_1,X_2,X_3,X_4) &= -X_0^3X_4 + 2X_0^2X_1X_3 + X_0^2X_2^2 - 3X_0X_1^2X_2 + X_1^4. \end{aligned}$$

On développe ensuite le terme à la puissance m,

$$\frac{1}{f^m} = \frac{1}{f_0^m}\left(1 + \frac{mU_1(f_0,f_1)}{f_0} + \frac{\binom{m}{2}U_1(f_0,f_1)^2 + mU_2(f_0,f_1,f_2)}{f_0^2}y^2 + \cdots\right).$$

On introduit alors les notations suivantes

$$\frac{1}{f^m} = \frac{1}{f_0^m}\left(1 + \frac{V_{m,1}(f_1)}{f_0}y + \cdots + \frac{V_{m,p}(f_1,\ldots,f_p)}{f_0^p} + \cdots\right), \tag{A.4}$$

où les polynômes $V_{m,p} \in \mathbf{Z}[X_1,\ldots,X_p]$ sont des polynômes homogènes de degré p qui ne dépendent que de m et p. Le coefficient de y^n de $\frac{1}{f^m}\frac{\partial f}{\partial x}$ est donc

$$C_{m,n}(x) := \frac{1}{f_0^m}\left(f_n' + f_{n-1}'\frac{V_{m,1}(f_0,f_1)}{f_0} + \cdots + f_0'\frac{V_{m,n}(f_0,\ldots,f_n)}{f_0^n}\right).$$

Pour tout entier k appartenant à $\{1,\ldots,n\}$, on pose

$$S_{m,n,k}(f_0,\ldots,f_k) := f_0^{n-k}V_{m,k}(f_0,\ldots,f_k)$$

et $S_{m,n,0}(f_0) := f_0^n$. Les polynômes, $S_{m,n,k}$ sont homogènes de degré n et

$$C_{m,n}(x) := \underbrace{\frac{1}{f_0^{m+n}}}_{A_{m,n}(x)}\underbrace{\sum_{k=0}^{n} f_{n-k}'S_{m,n,k}(f_0,\ldots,f_k)}_{B_{m,n}(x)}. \tag{A.5}$$

Nous allons étudier $A_{m,n}$ séparément. On rappelle que f_0 était de valuation (x)-adique 1, c'est-à-dire que $f_0(x) = f_{1,0}x + f_{2,0}x^2 + \cdots$. En reprenant le calcul effectué précédemment pour $\frac{1}{f^m}$, on obtient

$$\begin{aligned} A_{m,n}(x) &= \frac{1}{f_{1,0}^{m+n}}\left(1 + \frac{V_{m+n,1}(f_{1,0},f_{2,0})}{f_{1,0}}x + \cdots\right. \\ &\qquad \left. \cdots + \frac{V_{m+n,p-1}(f_{1,0},\ldots,f_{p,0})}{f_{1,0}^{p-1}}x^{p-1} + \cdots\right), \end{aligned}$$

où les polynômes $V_{i,j}$ sont ceux introduits dans l'expression (A.4). Rappelons que l'objectif initial est de montrer le (x,y)-2-résidu, qui est le coefficient $c_{m,n,-1}$ de x^{-1} dans $C_{m,n}$, s'obtient comme une expression polynomiale en un nombre fini des coefficients $f_{i,j}$ de f. Nous allons voir quels coefficients interviennent.

Dans $A_{m,n}$. Comme les polynômes $S_{m,n,k}$ sont de degré n pour tout entier $k \in \{1,\ldots,n\}$, la valuation (x)-adique de $B_{m,n}$ vérifie

$$\mathrm{val}_{(x)}(B_{m,n}) \geq -nN - (N+1) = -(n+1)N - 1.$$

Le $-nN$ est la contribution de $S_{m,n,k}$ et le $-(N+1)$ celle de f_{n-k}'. Par conséquent, les termes de $A_{m,n}$ intervenant dans le calcul de $c_{m,n,-1}$ sont de degré au plus $N(n+1)$. En reprenant l'expression de $A_{m,n}$ ci-dessus, on voit que les termes de degré inférieur à $N(n+1)$ font intervenir les $f_{i,0}$ avec $-N \leq i \leq N(n+1)+1$.

Dans $B_{m,n}$. Comme la série de Laurent $A_{m,n}$ est de valuation $-m-n$, les termes de $B_{m,n}$ intervenant dans le calcul de ce 2-résidu $c_{m,n,-1}$ sont de degré au plus $m+n-1$. D'après l'expression de $B_{m,n}$, ces termes font intervenir les $f_{i,j}$ avec $i \leq m+n$ (on ajoute 1 du fait de la présence des dérivées f_i' dans l'expression).

Conclusion. Les coefficients $f_{i,j}$ intervenant dans le calcul de $c_{m,n,-1}$ sont ceux dont les indices vérifient

$$\begin{cases} -N & \leq & i & \leq & \max\{m+n, (n+1)N+1\} \\ 0 & \leq & j & \leq & n. \end{cases}$$

On note I cet ensemble de paires d'indices. Il existe donc un polynôme $Q_{m,n}(X_{i,j}) \in \mathbf{Z}[X_{i,j}|(i,j) \in I]$ et un entier M qui ne dépendent pas du corps de base k et tels que

$$c_{m,n,-1} = (x,y)\mathrm{res}^2(\omega) = \frac{1}{f_{1,0}^M} Q(f_{i,j}|(i,j) \in I).$$

Par un raisonnement analogue à celui effectué à la fin de l'étape 1 et faisant intervenir le théorème de prolongement des identités, on montre que ce résidu est nul.

Ainsi, nous avons montré l'invariance du 2-résidu d'une 2-forme formelle sous l'action d'un changement de variables de la forme $u = f(x,y)$ tel que les $n+1$ premiers coefficients $f_j(u)$ de f sont de valuation supérieure à $-N$. Ce résultat est valable pour tout entier N, donc pour tout changement de variables de la forme (CV2), ce qui conclut la démonstration.

Annexe B

Indépendance des valuations

L'objectif de ce chapitre est de donner une preuve de la proposition II.4.2. Nous allons en fait démontrer un résultat en dimension quelconque, ce qui n'augmente pas le niveau de difficulté de la preuve.

Proposition B.0.2. *Soient X une variété quasi-projective lisse irréductible de dimension supérieure ou égale à 2 au-dessus d'un corps quelconque k et Y une sous-variété de X de codimension 1. Soient $P_1, \ldots, P_n$ une famille de points fermés de $X \setminus Y$ et $Q_1, \ldots, Q_s$ une famille de points fermés de Y. Alors, il existe une uniformisante $v \in \mathcal{O}_{X,Y}$ telle que le support du diviseur principal (v) évite les points $P_1, \ldots, P_n$ et le support de $(v) - Y$ évite $Q_1, \ldots, Q_s$.*

La démonstration suivante a été suggérée par Gerhard Frey.

Preuve. Commençons par remarquer que l'on peut se contenter de démontrer le résultat dans le cas où Y est irréductible. Le cas général se déduira de ce cas particulier en raisonnant sur les composantes irréductibles de Y. On suppose donc désormais que Y est irréductible.

Dans un premier temps nous allons nous ramener au cas d'une variété affine. Il existe un ouvert affine de X contenant tous les points $P_1, \ldots, P_r, Q_1, \ldots, Q_s$. L'intersection de cet ouvert avec Y est non vide car contient les points Q_i. Aussi, quitte à se restreindre à cet ouvert, on peut supposer que X est affine. Dans ce qui suit, nous noterons I_Y l'idéal de $k[X]$ associé à Y et $\mathfrak{m}_{P_1}, \ldots, \mathfrak{m}_{P_r}, \mathfrak{m}_{Q_1}, \ldots, \mathfrak{m}_{Q_s}$ les idéaux maximaux correspondant respectivement aux points $P_1, \ldots, P_r$ et $Q_1, \ldots, Q_s$. On notera également $m_1, \ldots, m_s$ les multiplicités respectives de Y en $Q_1, \ldots, Q_s$. On rappelle que la multiplicité de Y en un point Q est le plus petit entier m tel que

$$I_Y \subset \mathfrak{m}_Q^m.$$

Reformulation du problème. On cherche une fonction $v \in k[X]$ vérifiant les propriétés suivantes.

(1) La fonction v appartient à $I_Y \setminus I_Y^2$.

(2) Pour tout entier i appartenant à $\{1, \ldots, r\}$, la fonction v n'appartient pas à $\mathfrak{m}_{P_i}$.

(3) Pour tout entier j appartenant à $\{1, \ldots, s\}$, la fonction v n'appartient pas à $\mathfrak{m}_{Q_j}^{m_j+1}$.

Le premier critère permet d'affirmer que v est bien une uniformisante de $\mathcal{O}_{X,Y}$, le second signifie que v ne s'annule en aucun des P_i, et le troisième équivaut au fait que Y soit l'unique zéro de v au voisinage de Q_i. Dans ce qui suit, lorsque P est un point fermé de X et $f \in \mathcal{O}_{X,P}$ on notera $f(P)$ l'image de f dans le corps résiduel $k(P)$.

Étape 0. Pour toute famille finie de points fermés deux à deux distincts $A_1, \ldots, A_n$ de X et toute famille d'entiers naturels $p_2, \ldots, p_n$, il existe une fonction g appartenant à l'idéal produit $\mathfrak{m}_{A_2}^{p_2} \cdots \mathfrak{m}_{A_n}^{p_n}$ telle que

$$g(A_1) = 1.$$

Pour le montrer, il suffit de constater que les idéaux $\mathfrak{m}_{A_1}$ et $\mathfrak{m}_{A_2}^{p_2} \cdots \mathfrak{m}_{A_n}^{p_n}$ sont étrangers, c'est-à-dire que

$$\mathfrak{m}_{A_1} + \mathfrak{m}_{A_2}^{p_2} \cdots \mathfrak{m}_{A_n}^{p_n} = k[X].$$

De fait, il existe une fonction f appartenant à $\mathfrak{m}_{A_1}$ et une fonction g appartenant à $\mathfrak{m}_{A_2}^{p_2} \cdots \mathfrak{m}_{A_n}^{p_n}$ telles que $f + g = 1$. Ainsi, on a bien $g(A_1) = 1$.

Étape 1. (*Construction d'une fonction qui vérifie 3*). Soit j_0 un entier appartenant à $\{1, \ldots, s\}$. Par définition de la multiplicité, il existe une fonction f appartenant à l'idéal I_Y et n'appartenant pas à $\mathfrak{m}_{Q_{j_0}}^{m_{j_0}+1}$. Soit f_{j_0} une telle fonction, d'après l'étape précédente il existe une fonction h_{j_0} régulière sur X telle que h_{j_0} est un élément de l'idéal produit $\mathfrak{m}_{Q_1}^{m_1} \cdots \widehat{\mathfrak{m}_{Q_{j_0}}} \cdots \mathfrak{m}_{Q_s}^{m_s}$ et h_{j_0} n'appartient pas à l'idéal $\mathfrak{m}_{Q_{j_0}}$. Posons alors

$$v_{j_0} := f_{j_0} h_{j_0} \quad \text{et} \quad v := \sum_{j=1}^{s} v_j.$$

La fonction v appartient à l'idéal I_Y, mais n'appartient à aucun $\mathfrak{m}_{Q_j}^{m_j+1}$. En effet, soit j_0 un entier appartenant à $\{1, \ldots, s\}$, alors

$$v_{j_0} \in \mathfrak{m}_{Q_{j_0}}^{m_{j_0}} \smallsetminus \mathfrak{m}_{Q_{j_0}}^{m_{j_0}+1} \quad \text{et} \quad \forall j \neq j_0,\ v_j \in \mathfrak{m}_{Q_{j_0}}^{m_{j_0}+1}.$$

Remarquons au passage que la fonction ainsi construite n'appartient pas à I_Y^2, car sinon elle appartiendrait à $\mathfrak{m}_{Q_j}^{2m_j}$ pour tout entier j appartenant à $\{1, \ldots, s\}$.

Étape 2. Nous allons montrer par récurrence sur r que, quitte à ajouter à v un élément de I_Y^2, ce qui n'aura aucune conséquence sur les propriétés acquises dans l'étape précédente, on peut faire en sorte que v ne s'annule en aucun des P_i.

Pour $\mathbf{r = 1}$, si $v(P_1)$ est non nul, c'est terminé. Sinon, comme P_1 n'est pas contenu dans Y, l'idéal I_Y ne contient pas $\mathfrak{m}_{P_1}$. De même, l'idéal I_Y^2 ne contient pas $\mathfrak{m}_{P_1}$, car $\mathfrak{m}_{P_1}$ est radical. De fait, les idéaux I_Y^2 et $\mathfrak{m}_{P_1}$ sont étrangers, il existe donc une fonction f appartenant à I_Y^2 et une fonction g appartenant à $\mathfrak{m}_{P_1}$ telles que $f + g = 1$. On remplace alors v par $v + f$ et cette nouvelle fonction ne s'annule plus en P_1.

Soit $\mathbf{r \geq 1}$, supposons la propriété vraie au rang r et montrons qu'elle est vérifiée au rang $r + 1$. Si $v(P_{r+1})$ est non nul, c'est terminé. Sinon, les idéaux $I_Y^2 \mathfrak{m}_{P_1} \cdots \mathfrak{m}_{P_r}$ et $\mathfrak{m}_{P_{r+1}}$ sont étrangers, on en déduit l'existence d'une fonction f appartenant à $I_Y^2 \mathfrak{m}_{P_1} \cdots \mathfrak{m}_{P_r}$ qui ne s'annule pas en P_{r+1} et on remplace v par $v + f$. □

Annexe C

Complément d'algèbre linéaire

Le but de cette annexe est de fournir quelques résultats d'algèbre linéaire utilisés à la fin du chapitre II. Ces résultats sont des exercices relativement élémentaires. Nous avons cependant choisi de les démontrer ici, faute de références.

Dans ce qui suit, E et F désignent des espaces vectoriels sur un corps quelconque k. On dispose de plus sur de formes bilinéaires E et F notées respectivement $\langle .\ ,\ .\rangle_E$ et $\langle .\ ,\ .\rangle_F$. On peut alors construire une forme bilinéaire sur $E \otimes_k F$ qui soit canoniquement associée à $\langle .\ ,\ .\rangle_E$ et $\langle .\ ,\ .\rangle_F$. Pour ce faire, on la définit sur les tenseurs élémentaires par

$$\langle .\ ,\ .\rangle_{E\otimes F} \ : \left\{ \begin{array}{ccc} E\otimes F \times E \otimes F & \rightarrow & k \\ (a\otimes b, a'\otimes b') & \mapsto & \langle a,a'\rangle_E.\langle b,b'\rangle_F \end{array} \right.$$

et on l'étend ensuite par linéarité. On constate immédiatement que si $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ sont des bases orthogonales respectives de E et F, alors $(e_i\otimes f_j)_{(i,j)\in I\times J}$ est une base orthogonale de $E\otimes F$.

Lemme C.0.3. *Si les formes bilinéaires $\langle .\ ,\ .\rangle_E$ et $\langle .\ ,\ .\rangle_F$ sont non dégénérées, alors il en est de même pour $\langle .\ ,\ .\rangle_{E\otimes F}$. De même, si $\langle .\ ,\ .\rangle_E$ et $\langle .\ ,\ .\rangle_F$ sont symétriques, alors $\langle .\ ,\ .\rangle_{E\otimes F}$ l'est également.*

PREUVE. Le fait que la symétrie de $\langle .\ ,\ .\rangle_E$ et $\langle .\ ,\ .\rangle_F$ entraîne celle de $\langle .\ ,\ .\rangle_{E\otimes F}$ est évident. Supposons que $\langle .\ ,\ .\rangle_E$ et $\langle .\ ,\ .\rangle_F$ soient non dégénérées. Soient $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ des bases orthogonales respectives de E et F et soit u un élément de $E\otimes F$ tel que la forme linéaire $\langle u,\ .\rangle_{E\otimes F}$ soit identiquement nulle. Le vecteur u est de la forme

$$u = \sum_{i,j} u_{i,j} e_i \otimes f_j.$$

Par ailleurs, pour tout couple (i,j), on a

$$\langle u, e_i\otimes f_j\rangle = 0, \quad \text{or} \quad \langle u, e_i\otimes f_j\rangle = u_{i,j}.$$

On en déduit que u est nul et que la forme bilinéaire $\langle .\ ,\ .\rangle_{E\otimes F}$ est non dégénérée. □

On suppose désormais que les formes bilinéaires $\langle .\ ,\ .\rangle_E$ et $\langle .\ ,\ .\rangle_E$ sont non dégénérées.

Lemme C.0.4. *Supposons que E et F soient de dimension finie. Soient A et B deux sous-espaces vectoriels respectifs de E et F, alors*

$$(A\otimes B)^\perp = A^\perp \otimes F + E\otimes B^\perp.$$

PREUVE. L'inclusion $\supseteq$ est élémentaire. En effet on prend a, a', b, f appartenant respectivement à $A, A^\perp, B$ et F. On a

$$\langle a\otimes b, a'\otimes f\rangle_{E\otimes F} = \underbrace{\langle a,a'\rangle}_{=0}\langle b,f\rangle = 0.$$

On en déduit que $A^\perp \otimes F$ est inclus dans $(A \otimes B)^\perp$. Par un raisonnement identique, on montre ensuite que $E \otimes B^\perp$ est inclus dans $(A \otimes B)^\perp$.

Pour l'inclusion réciproque, commençons par montrer que

$$A^\perp \otimes F \cap E \otimes B^\perp = A^\perp \otimes B^\perp.$$

L'inclusion $\supseteq$ est immédiate. Montrons donc l'inclusion réciproque. Soient $(e_i)_{i\in I_0}$ et $(f_j)_{j\in J_0}$ des bases respectives de $A^\perp$ et $B^\perp$ complétées en des bases $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ de E et F. Soit s un vecteur de $A^\perp \otimes F \cap E \otimes B^\perp$. Décomposons le dans la base $(e_i \otimes f_j)_{(i,j)\in I\times J}$.

$$s = \sum_{(i,j)\in I\times J} s_{ij}\, e_i \otimes f_j.$$

Comme $s \in A^\perp \otimes F$ (resp. $s \in E \otimes B^\perp$), les s_{ij} sont nuls pour $i \notin I_0$ (resp. pour $j \notin J_0$), ce qui prouve l'inclusion réciproque.

Pour finir, posons

$$\begin{array}{rclcrcl} m & := & \dim(E) & & a & := & \dim(A) \\ n & := & \dim(F) & & b & := & \dim(B), \end{array}$$

et calculons la dimension de $A^\perp \otimes F + E \otimes B^\perp$.

$$\begin{array}{rcl} \dim(A^\perp \otimes F + E \otimes B^\perp) & = & \dim(A^\perp \otimes F) + \dim(E \otimes B^\perp) - \dim(A^\perp \otimes B^\perp) \\ & = & n(m-a) + m(n-b) - (m-a)(n-b) \\ & = & mn - ab \\ & = & \dim(A^\perp \otimes B^\perp). \end{array}$$

□

Nous pouvons à présent énoncer un résultat fort utile dans le chapitre II, puisque c'est celui qui nous permet de prouver que l'orthogonal d'un code fonctionnel sur une surface n'est pas toujours fonctionnel. En particulier, il ne l'est jamais lorsque la surface est un produit de deux courbes.

Corollaire C.0.5. *Si A et B sont des sous-espaces non triviaux*[1] *respectifs de E et F, alors le sous-espace $(A \otimes B)^\perp$ de $E \otimes F$ n'est pas un produit tensoriel élémentaire $U \otimes V$ de sous-espaces de E et F.*

Preuve. C'est une conséquence immédiate du lemme C.0.4 et du lemme C.0.6 qui suit. □

Lemme C.0.6. *Soient E et F deux espaces vectoriels sur un corps k quelconque. Soient A et B des sous-espaces respectifs non triviaux de E et F. Alors, le sous-espace $A \otimes_k F + E \otimes_k B$ de $E \otimes_k F$ ne peut pas être écrit sous la forme d'un produit tensoriel élémentaire $U \otimes_k V$.*

Preuve. Raisonnons par l'absurde et supposons qu'il existe U et V, sous-espaces respectifs de E et F tels que

$$A \otimes_k F + E \otimes_k B = U \otimes_k V. \tag{C.1}$$

Supposons que U ne soit pas inclus dans A. Soient $(e_i)_{i\in I_0}$ et $(f_j)_{j\in J_0}$ des bases respectives de A et B complétées en des bases $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ de E et F. Soit également $u \in U \setminus A$. Pour tout vecteur $v \in V$, on a

$$u \otimes v = \sum_{(i,j)\in I\times J} u_i v_j\, e_i \otimes f_j.$$

D'après (C.1), le produit $u_i v_j$ est nul pour tout couple (i,j) tel que $i \notin I_0$ et $j \notin J_0$. Comme par hypothèse u n'est pas dans A, il existe au moins un $i_1 \notin I_0$ tel que u_{i_1} est non nul. Donc

[1] Par *non triviaux*, on entend que A (resp. B) est non nul et strictement inclus dans E (resp. F).

pour tout $j \notin J_0$, on a $u_{i_1} v_j = 0$, donc $v_j = 0$. Par conséquent, v appartient à B et ce pour tout $v \in V$. Donc

$$V \subseteq B, \quad \text{donc} \quad U \otimes V \subseteq E \otimes B. \tag{C.2}$$

Soient maintenant f un vecteur de F n'appartenant pas à B et a un vecteur non nul de A. Alors $a \otimes f$ appartient à $A \otimes F$ mais pas à $E \otimes B$ et d'après (C.2), il n'appartient pas à $U \otimes V$ ce qui contredit l'hypothèse de départ (C.1).

Si maintenant U est inclus dans A, alors $U \otimes V$ est inclus dans $A \otimes F$ et on aboutit à une contradiction en réalisant le raisonnement symétrique de celui qui vient d'être effectué. □

Annexe D

Construction de codes fonctionnels

Dans [Lac88], Lachaud présente une autre procédé de construction de codes fonctionnels sensiblement différent de celui qui est présenté dans le chapitre II. Les codes ainsi construits sont en général appelés codes de Reed-Müller projectifs.

D.1 Construction

On se place dans l'espace projectif $\mathbf{P}^r_{\mathbf{F}_q}$ muni d'un système de coordonnées homogènes $(X_0, \ldots, X_n)$. Pour tout entier naturel d on note $\mathcal{F}_d$, l'espace

$$\mathcal{F}_d := \{f \in \mathbf{F}_q[X_0, \ldots, X_n],\ f \text{ homogène de degré } d\} \cup \{0\}.$$

En d'autres termes, $\mathcal{F}_d$ est l'espace des sections globales du faisceau $\mathcal{O}_{\mathbf{P}^r}(d)$. Rappelons que, s'il est possible de définir le lieu d'annulation dans $\mathbf{P}^r$ d'un élément non nul de $\mathcal{F}_d$, l'évaluation d'un élément de $\mathcal{F}_d$ en un point de $\mathbf{P}^r$ n'a pas de sens. D'une certaine façon, la définition qui suit consiste à lui en donner un.

Définition D.1.1 (Lachaud 1988)**.** *Soit P un point rationnel de $\mathbf{P}^r$ de coordonnées homogènes $(x_0 : \cdots : x_n)$. Soit h le plus petit entier compris entre 0 et n tel que x_h soit non nul. Pour tout entier naturel d, on définit l'application d'évaluation en P par*

$$ev_P : \left\{ \begin{array}{ccc} \mathcal{F}_d & \rightarrow & \mathbf{F}_q \\ f & \rightarrow & \dfrac{f(x_0, \ldots, x_n)}{x_h^d}. \end{array} \right.$$

L'application est bien définie, mais n'est pas canonique, elle dépend du choix d'un système de coordonnés homogènes. À partir de cette application, on peut construire des codes correcteurs d'erreurs de la façon suivante.

Définition D.1.2. *Soient X une sous-variété fermée lisse absolument irréductible de $\mathbf{P}^r_{\mathbf{F}_q}$ et $P_1, \ldots, P_n$, l'ensemble des points rationnels de X. Pour tout entier naturel d, le code $C_d(X)$ est l'image de l'application*

$$c : \left\{ \begin{array}{ccc} \mathcal{F}_d & \rightarrow & \mathbf{F}_q^n \\ f & \mapsto & (ev_{P_1}(f), \ldots, ev_{P_n}(f)). \end{array} \right.$$

Bien que moins canonique que la construction présentée dans le chapitre II, cette approche présente de nombreux avantages. Tout d'abord, elle permet une évaluation en **tous les points de la variété**, sans avoir à se soucier des questions de définitions. Par rapport à la définition du chapitre II, on évite ici les restrictions du type "les points $P_1, \ldots, P_n$ évitent le support de

G". Ensuite, l'évaluation de la distance minimale et de la distribution des poids du code $C_d(X)$ se traduit sous la forme d'un problème de comptage explicite de tous les points rationnels de variétés projectives[1].

Toutefois, pour le cadre qui nous intéresse, à savoir celui de pouvoir construire l'orthogonal du code fonctionnel à partir de différentielles, cette construction n'est pas optimale. En effet, le défaut de canonicité des applications d'évaluation empêche toute possibilité de reproduction du raisonnement de la preuve du théorème II.4.1. L'obstruction est liée au fait que les éléments de $\mathcal{F}_d$ ne sont pas des fonctions. On peut localement les identifier à des fonctions rationnelles sur X, c'est ce qui est fait dans la définition de l'application ev_P, mais cette identification dépend du point P. D'une certaine façon, c'est comme si l'on évaluait en des points différents des fonctions différentes. On ne peut donc plus reproduire le raisonnement consistant à appliquer la formule des résidus à la 2-forme $f\omega$.

D.2 Essentiellement, c'est la même chose

Par la méthode de construction présentée dans le chapitre II, on peut construire un code fonctionnel isomorphe au code $C_d(X)$. Pour ce faire, on définit H_∞, l'hyperplan de $\mathbf{P}^r$ d'équation $X_0 = 0$. On appelle i l'inclusion canonique $i : X \hookrightarrow \mathbf{P}^r$ et on pose

$$L := i^* H_\infty \in \mathrm{Div}_{\mathbf{F}_q}(X).$$

Pour tout entier naturel d, les faisceaux $\mathcal{L}(dL)$ et $i^*\mathcal{O}_{\mathbf{P}^r}(d)$ sont isomorphes. Aussi, si les points $P_1, \ldots, P_n$ évitent le support de L, alors les codes $C_{L,X}(P_1 + \cdots + P_n, dL)$ et $C_d(X)$ sont isomorphes. Pour se défaire de la condition *évitent les point du support de* L, il suffit d'utiliser le *moving lemma* ([Sha94] III.1.3 théorème 1 et annexe B). En vertu de ce résultat, on sait qu'il existe $G \in \mathrm{Div}_{\mathbf{F}_q}(X)$ dont le support évite les points $P_1, \ldots, P_n$ et linéairement équivalent à dL. Cette fois-ci, on est assuré de la bonne définition du code $C_{L,X}(P_1 + \cdots + P_n, G)$ et le faisceau $\mathcal{L}(G)$ est isomorphe à $i^*\mathcal{O}_{\mathbf{P}^r}(d)$. On obtient donc l'isomorphisme de codes

$$C_{L,X}(P_1 + \cdots, P_n, G) \cong C_d(X).$$

On peut donc construire un code fonctionnel (provenant de la définition de [VM84] donnée dans le chapitre II) isomorphe à $C_d(X)$. Malheureusement la construction d'un diviseur G dont le support évite tous les points rationnels de X n'est pas toujours évidente. La définition D.1.2 reste donc commode car elle fournit une construction explicite simple.

Remarque D.2.1. *Notons que l'on a identifié les éléments de $\mathcal{F}_d$ restreints à X à des sections globales du faisceau $i^*\mathcal{O}_{\mathbf{P}^n}(d)$. Comme on l'a vu dans le chapitre III, si X est projectivement normale[2] en respect au plongement $X \hookrightarrow \mathbf{P}^r$, alors le faisceau $i^*\mathcal{O}_{\mathbf{P}^r}(d)$ s'identifie au faisceau $\mathcal{O}_X(d)$ (voir [Har77] II.5 ex 14).*

[1] Éventuellement réduites ou réductibles.
[2] Par exemple si c'est une intersection complète lisse de $\mathbf{P}^r$.

Annexe E

Points en position générale

Cette annexe contient les démonstrations de lemmes techniques utilisés dans la section IV.1 du chapitre III.

Lemme IV.1.8. *Soient r et m deux entiers naturels avec $r \geq 1$, alors toute famille de $rm+2$ points rationnels distincts de $\mathbf{P}^N$ appartenant à une même courbe de degré r est m-liée.*

PREUVE. Soient $P_1, \ldots, P_{rm+2}$ une telle famille de points et C la courbe de degré r qui les contient. D'après le théorème de Bezout, une hypersurface de degré m qui ne contient pas C l'intersecte en au plus rm points géométriques. Par conséquent, il n'existe pas d'hypersurface contenant tous ces points sauf un. □

Lemme IV.1.9. *Soit m un entier naturel.*

(1) Si $m+2$ points rationnels distincts de $\mathbf{P}^N$ sont m-liés, alors ils sont alignés.

(2) Tout r-uplet de points rationnels deux à deux distincts de $\mathbf{P}^N$ avec $r \leq m+1$ est en position m-générale.

PREUVE. **Preuve de (1).** Soient $P_1, \ldots, P_{m+2}$ des points distincts de $\mathbf{P}^N$ qui sont m-liés. Supposons qu'ils ne soient pas alignés. Il existe donc un hyperplan H qui évite P_{m+2} et contient au moins deux points parmi $P_1, \ldots, P_{m+1}$. Quitte à réordonner les indices des points on peut supposer qu'il existe $l \geq 2$ tel que $P_1, \ldots, P_l$ appartiennent à H.

- Si $l = m+1$, on dispose d'une hypersurface (en l'occurrence l'hyperplan H) qui contient tous les P_i sauf P_{2m+2}.
- Sinon, pour tout $l+1 \leq j \leq m+1$, il existe un hyperplan H_j qui contient P_j et évite P_{m+2}.

L'hypersurface $H \cup H_{l+1} \cup \cdots \cup H_{m+1}$ est de degré inférieur ou égal à m (car $l \geq 2$), contient tous les P_i sauf P_{m+2}. Par symétrie, on en déduit l'existence pour tout $i_0 \in \{1, \ldots, m+2\}$ d'une hypersurface de degré m qui contient tous les P_i sauf P_{i_0}.

Preuve de (2). Soient $P_1, \ldots, P_r$ des points distincts de $\mathbf{P}^N$ avec $r \leq m+1$. En réutilisant la technique présentée dans la preuve de (1), on peut construire à l'aide de réunions d'hyperplans, des hypersurfaces de degré m qui interpolent tous les points sauf un. On en déduit que ces points sont en position m-générale. □

Lemme IV.1.11. *Soient m et r deux entiers naturels.*

(1) Si $r \leq 2m+1$, alors une famille de r points distincts de $\mathbf{P}^N$ telle que $m+2$ d'entre eux sont non alignés est en position m-générale.

(2) Soient $P_1, \ldots, P_{2m+2}$ un $(2m+2)$-uplet de points rationnels distincts de $\mathbf{P}^N$ tels que $m+2$ d'entre eux ne sont pas alignés. Alors ces points sont m-liés, si et seulement s'ils appartiennent à une même conique plane.

PREUVE. **Preuve de (1).** Nous allons démontrer le résultat par récurrence sur m.

Pour $m = 0$, c'est évident car un point de $\mathbf{P}^N$ est toujours en position 0-générale.

Soit $m \geq 0$, supposons que la propriété soit vérifiée au rang m et montrons qu'elle l'est au rang $m+1$. Soit $P_1, \ldots, P_{2m+3}$ une famille de points rationnels de $\mathbf{P}^N$ telle que $m+3$ d'entre eux ne sont pas alignés. Soit $\mathfrak{L}$ l'ensemble des droites contenant P_{2m+3} et au moins un point parmi $P_1, \ldots, P_{2m+2}$. On choisit un élément L_1 de $\mathfrak{L}$ contenant un nombre maximal de points parmi les P_i. On choisit ensuite une droite L_2 de $\mathfrak{L} \smallsetminus L_1$ contenant un nombre maximal de points parmi les P_i. Les droites L_1 et L_2 sont distinctes et se croisent en P_{2m+3}. Quitte à réordonner les points P_i, on peut supposer que $P_1 \in L_1$ et $P_2 \in L_2$.

Ensuite, montrons que, par hypothèse, les droites L_1 et L_2 contiennent chacune au plus $m+2$ points parmi les P_i et que les autres droites de $\mathfrak{L}$ en contiennent au plus $m+1$. On distingue deux situations.

(1) Les droites L_1 et L_2 contiennent toutes deux $m+2$ points parmi les P_i. Comme par définition, ces droites contiennent toutes deux le point P_{2m+3}, l'ensemble des P_i contenus dans $L_1 \cup L_2$ est égal à l'ensemble $P_1, \ldots, P_n$. Aussi, dans cette situation l'ensemble $\mathfrak{L}$ est égal à $\{L_1, L_2\}$ et le résultat attendu est trivialement vérifié.

(2) La droite L_2 contient moins de $m+1$ points parmi les P_i et par définition de L_2, les éléments de $\mathfrak{L} \smallsetminus \{L_1, L_2\}$ contiennent tous moins de $m+1$ points parmi les P_i.

Par conséquent, d'après l'hypothèse de récurrence, les points $P_3, \ldots, P_{2m+3}$ sont en position m-générale, il existe donc une hypersurface H' de degré m qui interpole $P_3, \ldots, P_{2m+2}$ et évite le point P_{2m+3}. On choisit de plus un hyperplan H qui contient P_1, P_2 et évite P_{2m+3}. L'hypersurface $H \cup H'$ est de degré $m+1$ et interpole tous les P_i sauf P_{2m+3}. On en déduit que pour tout $i_0 \in \{1, \ldots, 2m+3\}$, il existe une hypersurface de degré $m+1$ qui interpole tous les P_i sauf P_{i_0}.

Preuve de (2).

Étape 2a. Si $m = 0$, alors deux points distincts sont toujours 0-liés et également tou–jours contenus dans une courbe de degré 2, la propriété est donc trivialement vérifiée dans ce cas. On supposera donc désormais que $m \geq 1$ et on se donne un $(2m+2)$-uplet de points $P_1, \ldots, P_{2m+2}$ m-liés et deux à deux distincts.

Étape 2b. Montrons que si les P_i ne sont pas coplanaires et que $m+1$ d'entre eux sont alignés, alors les $m+1$ restants ne le sont pas. Pour ce faire, on doit supposer que $\mathbf{P}^N$ est de dimension $N \geq 3$.

Raisonnons par l'absurde et supposons qu'il existe deux droites disjointes L_1 et L_2 contenant respectivement les points $P_1, \ldots, P_{m+1}$ et $P_{m+2}, \ldots, P_{2m+2}$. Il existe un unique plan contenant P_{m+2} et la droite L_1. Ce plan évite les points $P_{m+3}, \ldots, P_{2m+2}$. On en déduit l'existence d'un hyperplan H vérifiant les mêmes propriétés. D'après la propriété (2) du lemme IV.1.9, il existe une hypersurface H' de degré $m-1$ qui contient les points $P_{m+3}, \ldots, P_{2m+1}$ et l'hypersurface $H \cup H'$ est de degré m et contient tous les P_i sauf P_{2m+2}. De même, pour tout i_0, on peut construire une hypersurface contenant tous les P_i sauf P_{i_0}, ce qui contredit le fait que les P_i sont liés.

Étape 2c. Montrons que les P_i sont coplanaires. Ici encore, nous allons raisonner par l'absurde en supposant qu'ils ne le sont pas. Soit $\mathfrak{D}$, l'ensemble des droites de $\mathbf{P}^N$ contenant au moins deux points distincts parmi les P_i. Soit L_1 une droite de $\mathfrak{D}$ contenant un nombre maximal de ces points. Quitte à réorganiser les indices, on peut supposer que $P_1 \in L_1$. Par hypothèse, les P_i sont non coplanaires, on peut donc supposer que les points P_1, P_2, P_3 et P_{2m+2} sont non coplanaires.

De plus, comme P_1 est dans L_1, deux situations sont possibles.

- Soit L_1 contient moins de m points, moyennant quoi, par définition de L_1, il n'y a pas de $(m+1)$-uplet de P_i alignés.
- Soit L_1 contient $m+1$ points et d'après l'étape 2b, les $m+1$ points restants sont non alignés.

Ainsi, les points $P_4, \ldots, P_{2m+2}$ forment un $(2m-1)$-uplet de points tel que $m+1$ d'entre eux ne sont pas alignés. D'après la preuve la propriété 1, ces points sont en position $(m-1)$-générale, il existe donc une hypersurface H' de degré $m-1$ qui contient $P_4, \ldots, P_{2m+1}$ et évite P_{2m+2}. Il existe de plus un hyperplan H contenant P_1, P_2, P_3 et évitant P_{2m+2}. L'hypersurface $H \cup H'$ est donc de degré m et contient tous les P_i sauf P_{2m+2}.

En appliquant aux points $P_1, \ldots, P_{2m+1}$, le raisonnement que l'on vient d'appliquer à P_{2m+2}, on conclut que ces points sont en position m-générale. Il y a contradiction, les points $P_1, \ldots, P_{2m+2}$ sont donc coplanaires.

Étape 2d. Maintenant que l'on sait que les P_i sont coplanaires, montrons qu'un $(2m+2)$-uplet de points de $\mathbf{P}^2$ est m-lié seulement si ces points sont sur une même conique. Nous allons traiter séparément les cas $m = 1$ et $m = 2$.

Si $m = 1$, quatre points du plan sont toujours 1-liés et sont également toujours contenus dans une même conique. Si $m = 2$ et que les six points ne sont pas tous sur une même conique, alors pour tout $1 \leq i_0 \leq 6$, il existe une conique[1] contenant tous les P_i sauf P_{i_0}. Il y a contradiction avec le fait que les P_i sont 2-liés. Ils sont donc bien sur une même conique.

Supposons maintenant que $m \geq 3$ et $P_1, \ldots, P_{2m+2}$ soit un $(2m+2)$-uplet de points m-liés dans $\mathbf{P}^2$ tel que $m+2$ d'entre eux ne sont pas alignés. Supposons que ces points ne soient pas tous sur une même conique. On note de nouveau $\mathfrak{D}$ l'ensemble des droites de $\mathbf{P}^2$ contenant au moins deux points distincts parmi les P_i. Soit L_1 une droite contenant un nombre maximal de ces points. On peut supposer, quitte a changer l'ordre des indices, que $P_1 \in L_1$. Montrons qu'il existe quatre points $P_{i_1}, \ldots, P_{i_4}$ parmi $P_2, \ldots, P_{2m+1}$ tels qu'il existe une conique contenant $P_1, P_{i_1}, \ldots, P_{i_4}$ et évitant P_{2m+2}.

Dans le cas contraire, pour tout $i \in \{2, \ldots, 2m-2\}$ une conique C_i contenant P_1,P_i,P_{i+1}, P_{i+2} et P_{i+3} contiendrait P_{2m+2}. Soit alors $i \in \{2, \ldots, 2m-3\}$, les coniques C_i et C_{i+1} ont cinq points d'intersection, d'après le théorème de Bezout, elles ont donc une composante irréductible commune Γ qui est de degré un ou deux. Par récurrence, on montre que tous les P_i appartiennent à cette courbe Γ ce qui contredit le fait que les P_i ne sont pas tous sur une même conique.

Ainsi, quitte à réorganiser les indices, on peut supposer qu'il existe une conique C contenant les points $P_1, \ldots, P_5$ et évite P_{2m+2}. On rappelle que P_1 est un contenu dans une droite L_1 contenant un nombre maximal de points parmi les P_i. Par un raisonnement identique à celui qui a été effectué dans l'étape 2*c*, on montre que les points $P_6, \ldots, P_{2m+2}$ forment un $(2m-3)$-uplet de points tel que m d'entre eux ne sont pas alignés. D'après la propriété 1 appliquée à $m-2$ et $r = 2m-3 = 2(m-2)+1$, les points $P_6, \ldots, P_{2m+2}$ sont en position $(m-2)$-générale. Il existe donc une courbe C' de degré $m-2$ qui contient les points $P_6, \ldots, P_{2m+1}$ et qui évite P_{2m+2}. La courbe $C \cup C'$ est de degré m et contient tous les P_i sauf P_{2m+2}. On en déduit la m-généralité de ces points, il y a contradiction. Les points P_i sont donc bien tous sur une même conique plane. □

[1] On rappelle que par cinq points de $\mathbf{P}^2$ passe toujours au moins une conique. Il y a d'ailleurs unicité si et seulement si quatre d'entre eux ne sont pas alignés, c'est-à-dire s'ils sont en position 2-générale.

Annexe F

Programmes Magma

F.1 Diviseurs Δ-convenables

Dans cette section, nous allons présenter un programme magma qui permet de calculer une paire de diviseur Δ convenable sur une surface lisse S munie d'un 0-cycle Δ. La paire ainsi construite vérifie les propriétés suivantes :

- elle satisfait le critère de la proposition II.3.8 ;
- le diviseur D_a est effectif ;
- les diviseurs D_a et D_b sont tous deux linéairement équivalents à des sections de la surface S avec une hypersurface de son espace ambiant.

Pour ce faire on utilise essentiellement la méthode présentée dans la démonstration du lemme II.4.7. À savoir : les diviseurs D_a et D_b^+ sont construits par interpolation des points du support de Δ. Le diviseur D_b^- est construit en interpolant les points où les deux autres diviseurs ne doivent pas se croiser ou se croisent avec une multiplicité trop importante et en évitant les points où ces diviseurs se croisent bien.

Ce programme se décompose en trois grosses parties que sont le calcul de D_a, de D_b^+ et de D_b^-. Le principe est à chaque fois le même, on considère un système linéaire de courbes qui vérifient de bonnes propriétés et on cherche un candidat dans ce dernier. Suivant sa dimension (et donc son nombre d'éléments définis sur $\mathbf{F}_q$), la recherche se fera de façon exhaustive ou aléatoire.

Préliminaires. On a besoin d'un certain nombre de scripts pour y parvenir.

```
// Cette fonction est une variation de la fonction "IsReduced"
// de Magma qui a tendance a ramer dans le cas ou le schema
// considere n'est pas une hypersurface de son espace (affine
// ou projectif) ambiant.


function EstReduit(V)
d:=Dimension(V);
A:=SingularSubscheme(V);
dd:=Dimension(A);
delete A;
if dd eq d then return false;
   else return true;
end if;
end function;
```

```
// Ce programme permet d'evaluer l'entier n minimal pour lequel
// l'interpolation d'une famille finie de points par une
// hypersurface de degre n est possible.


function MinDim(V,Points)

// L'entier $n$ va designer un degre que l'on va
// incrementer au debut de chaque iteration.

n:=0;
d:=-1;

Proj:=AmbientSpace(V);
Liste:=[Proj!p: p in Points];

while d lt 0 do
      n+:=1;
      L:=LinearSystem(Proj,n);
      L1:=LinearSystem(L,Liste);
      L2:=LinearSystemTrace(L1,V);
      d:=Dimension(L2);
end while;

return [*n,d,L2,Proj,Liste*];

end function;
```

```
// Cette fonction permet de calculer un vecteur tangent
// en un point d'une courbe. Il est exprime dans le
// systeme de coordonnees de la carte affine
// AffinePatch(Proj,P).

function TangentVector(C,P)

assert P in C;
assert Dimension(C) eq 1;
assert IsNonSingular(C,P);

Proj:=AmbientSpace(C);
CAff:=AffinePatch(C,P);
Aff:=AmbientSpace(CAff);
d:=Dimension(Aff);
Q:=Aff!P;

T:=TangentSpace(CAff,Q);
TP:=RationalPoints(T);

if TP[1] eq Q then
   R:=TP[2];
    else R:=TP[1];
end if;
```

```
QQ:=Coordinates(Q);
RR:=Coordinates(R);
return [RR[i]-QQ[i]: i in {1..d}];

end function;
```

```
// Cette fonction permet de calculer un systeme lineaire
// ayant un vecteur tangent impose en un point base rationnel.

// ATTENTION: Le vecteur $v$ est un objet "affine".
// Il est defini dans la carte affine naturelle
// Choisie pour P dans "AffinePatch(Proj,P)";

function LinearSystemTangent(Proj,L,P,v)

// On commence par verifier que la longueur de $v$ est la bonne.

d:=Dimension(Proj);
F:=BaseField(Proj);
assert #v eq d;

// On se donne une carte affine naturellement adaptee a $P$.

Aff:=AffinePatch(Proj,P);
p:=Aff!P;
h:=ProjectiveClosureMap(Aff);
LL:=LinearSystem(L,P);
LLL:=Pullback(h,LL);
S:=Sections(LL);
T:=Sections(LLL);
m:=#S;
assert #T eq m;

// On commence par travailler localement, donc sur le systeme
// lineaire affine. Pour chaque section $f$ de notre systeme
// lineaire affine on evalue $\langle grad_p (f), v \rangle$.

Liste:=[&+[Evaluate(Derivative(f,j),p)*v[j]: j in {1..d}]: f in T];

M:=Matrix(F,m,1,Liste);
B:=Basis(NullSpace(M));
delete Liste;
delete M;
Liste2:=[ &+[B[i][j]*S[j]: j in {1..m}]: i in {1..#B}];
Lpv:=LinearSystem(LL,Liste2);
return Lpv;

end function;
```

Calcul de Da. Ce programme fait appel à eux sous-programmes "sectionreduite" et "randsectionreduite". Dont nous donnerons le code source plus loin.

```
// Pour des raisons de commodite, nous allons faire
// en sorte de choisir $D_a$ reduit.

function Da(V,Points,M,T,r)

R:=MinDim(V,Points);
n:=R[1];
d:=R[2];
L:=R[3];
Proj:=R[4];
Liste:=R[5];
Poly:=Random(L);
F:=BaseField(V);
q:=#F;

printf "Le degre minimal d'interpolation pour D_a est %o. ",R[1];

while q^d lt M do
      A:=SectionReduite(V,L);
      if A ne 0
         then printf "Le resultat obtenu pour
              D_a a ete trouve de maniere deterministe,
              avec une hypersurface de degre %o. ",n;
         return A;
      end if;

// En cas d'echec, on augmente le degre d'interpolation
// et on reinitialise notre syst\`eme lineaire.

      n+:=1;
      L:=LinearSystem(Proj,n);
      L:=LinearSystem(L,Liste);
      L:=LinearSystemTrace(L,V);
      d:=Dimension(L);
end while;


print "Passage en recherche aleatoire pour D_a. ";
delete d;


for i:=1 to r do
      printf "On demarre les recherches avec des
             hypersurfaces de degre %o pour D_a. ",n;
      A:=RandSectionReduite(V,L,T);
      if A ne 0
         then printf "On obtient une hypersurface de
              degre %o fournissant D_a. ",n;
         return A;
      end if;
      n+:=1;
```

```
      L:=LinearSystem(Proj,n);
      L:=LinearSystem(L,Liste);
      L:=LinearSystemTrace(L,V);
end for;

return "Echec";

end function;
```

```
// Cette fonction fait une recherche deterministe
// d'un element reduit d'un systeme lineaire.

function SectionReduite(V,L)

assert IsNonSingular(V);
assert IsIrreducible(V);
F:=BaseField(V);
d:=Dimension(L);

// On doit parametrer le systeme lineaire par
// un espace projectif de meme dimension.
// Le probleme est que MAGMA, ne comprend
// la notion d'espace projectif de dimension nulle.
// Il faut donc commencer par traiter le cas ou
// le systeme lineaire n'a qu'un seul element.

if d eq 0
   then Coeffts:=[[1]];
   else  Pd:=ProjectiveSpace(F,d);
   Coeffts:=RationalPoints(Pd);
end if;
Sec:=Sections(L);


// On teste tous les elements du systeme lineaire jusqu'a
// ce que l'on en trouve un reduit.

for i :=1 to #Coeffts do
    Poly:=&+[Coeffts[i][j]*Sec[j]: j in {1..d+1}];
    D:=Scheme(V,Poly);
    if EstReduit(D)
       then return Poly;
    end if;
end for;

print "Aucun element reduit trouve de maniere deterministe";
return 0;

end function;
```

```
// Cette fonction effecute une recherche aleatoire
// d'un element reduit d'un systeme lineaire.

function RandSectionReduite(V,L,m)

for i:=1 to m do

// Il faut eviter le diviseur nul dans notre systeme lineaire.
// Voila comment nous allons proceder.

    Poly:=Random(L);
    while Poly eq 0 do
          Poly:=Random(L);
    end while;

    D:=Scheme(V,Poly);
    if EstReduit(D) then return Poly;
    end if;
end for;

print "Aucun element reduit trouve de maniere aleatoire";
return 0;
end function;
```

Calcul de D_b. Nous donnons les deux programmes permettant de calculer respectivement D_b^+ et D_b^-. Tout comme le programme précédent, ces programmes appellent chacun deux sous-programmes effectuant des recherches exhaustives ou aléatoires. Ces sous-programmes ressemblant fortement aux programmes "sectionreduite" et "randsectionreduite", nous n'avons pas jugé nécessaire de les ajouter dans cette annexe.

De même, nous ne présenterons pas les programmes dans leur intégralité. Car certaines parties sont un copié/collé d'un des programme déjà présenté

```
// Cette fonction permet de calculer la partie
// effective d'un diviseur $D_b$ lorsque
// l'on a calcule $D_a$.

// Pour des raisons de simplicite, nous allons imposer
// a $D_b^+$ d'eviter le lieu singulier de $D_a$ hors
// du support de $\Delta$.

function Dbplus(V,Points,M,T,r,Ha)

// On doit se donner un degre minimal d'interpolation
// On se donne celui de $H_a$ qui est tout indique.

Proj:=AmbientSpace(V);
DA:=Scheme(Proj,Ha);
Da:=Scheme(V,Ha);
F:=BaseField(V);
q:=#F;
Liste:=[Proj!p: p in Points];
```

```
// Il faut ensuite construire le schema a eviter.
// C'est-a-dire tous les points geometriques singuliers
// de $D_a$ qui sont hors du support de $\Delta$.
// C'est pour cela que nous allons construire le schema
// "evite".

// Par ailleurs il faut memoriser les points du support
// de $\Delta$ qui sont singuliers pour $D_a$
// car en ces derniers, $D_b^+$ devra etre lisse!
// C'est pourquoi nous allons construire la liste DaSing,
// puis le schema "evite2".


UA:=SingularSubscheme(Da);
assert Dimension(UA) eq 0;
evite:=UA;

MultiA:=[];
DaSing:={@ @};
N:=#Points;

for i:=1 to N do
    mi:=Multi(UA,Liste[i]);
    Append(~MultiA,mi);

// Il faut enlever les points du support de $\Delta$
// que l'on ne doit bien sur pas eviter.

    if mi gt 0 then
        DaSing join:= {@Liste[i]@};
        evite:=DiffIter(evite,Liste[i],mi);
    end if;
end for;

// Il y a deux facons de programmer le schema vide.
// C'est le schema d'equation 1 et celui d'equations x,y,z,t.
// Le second se comporte mieux avec la fonction meet donc:

if IsEmpty(evite) then
   evite:=EmptySubscheme(Proj);
end if;


if IsEmpty(DaSing) then
   evite2:=EmptySubscheme(Proj);
   else evite2:=Cluster(DaSing);
end if;


// On construit ensuite notre systeme lineaire.

d:=-1;

// On initialise $n$ a degre de $H_a$ moins
```

```
// un car il sera incremente des le debut de la boucle.

deg:=TotalDegree(Ha);
n:=deg-1;


while d eq -1 do
      n+:=1;
      L:=LinearSystem(Proj,n);
      L:=LinearSystem(L,Liste);
      L:=Complement(L,DA);
      L:=LinearSystemTrace(L,V);

// Afin de gagner du temps,
// on verifie que le schema a eviter ne rencontre
// pas l'ensemble des points bases de $L$.
// On doit aussi verifier que las points de evite2
// ne sont pas generiquement de multiplicite
// superieure ou egale a $2$ dans $L$.

      R:=BaseScheme(L);
      if IsEmpty(DaSing) then
         z:=0;
         else z:=&+[Multiplicity(L,P)-1: P in DaSing];
      end if;

        if z eq 0 and IsEmpty(evite meet R) then
         d:=Dimension(L);
         else d:=-1;
      end if;

end while;

delete UA;
delete R;

printf "Le degre minimal d'interpolation pour D_b^+ est %o. ",n;

// Ensuite, on fait comme d'habitude...
```

```
// Cette fonction fournit $D_b^-$.

function Dbmoins(V,Points,M,T,r,Ha,Hb)

Proj:=AmbientSpace(V);
DA:=Scheme(Proj,Ha);
Da:=Scheme(V,Ha);
DB:=Scheme(Proj,Hb);
Db:=Scheme(V,Hb);
F:=BaseField(V);
q:=#F;
Liste:=[Proj!p: p in Points];
N:=#Liste;
```

```
// Il faut construire le schema des points
// bases.
// Nous allons par ailleurs lister trois types de
// Points:
// 1) les points que $D_b^-$ doit eviter;
// 2) les points que $D_b^-$ doit interpoler
// avec une multiplicite fixee;
// 3) ceux que $D_a^-$ doit interpoler
// avec un vecteur tangent fixe.

U:=Da meet Db;
SchemaBase:=U;
Base:=[];
NonBase:=[];
BaseSpe:=[];
mult:=[];


// Les elements de Base sont la donnee d'un point et de la
// multiplicite de $U$ en ce point. Les elements de baseSpe sont la
// donnee d'un point et d'un vecteur tangent en ce point.

for j:=1 to N do
    p:=Liste[j];
    mj:=Multi(U,p);
    Append(~mult,mj-1);

    if mj eq 0 then printf "ERREUR: D_a et D_b^+ ne se croisent
                    pas en %o. ",p;

    elif mj eq 1 then
       SchemaBase:=Difference(SchemaBase,Cluster(p));
       Append(~NonBase,p);

    elif mj eq 3 then
       SchemaBase:=DiffIter(SchemaBase,p,2);
       if IsNonSingular(Da,p)
          then Append(~BaseSpe,[*p,TangentVector(Da,p)*]);
          else Append(~BaseSpe,[*p,TangentVector(Db,p)*]);
       end if;

    else  SchemaBase:=DiffIter(SchemaBase,p,mj-1);
       Append(~Base,[*p,mj*]);

    end if;
end for;

print "D_b^-, premiere serie de calculs effecutee. ";

delete U;

// Il faut calculer le degre minimal du systeme lineaire.
```

```
n:=0;
d:=-1;

while d eq -1 do
      n+:=1;
      L:=LinearSystem(Proj,n);
      L:=LinearSystem(L,SchemaBase);
      for a in BaseSpe do
          L:=LinearSystemTangent(Proj,L,a[1],a[2]);
      end for;

      if IsEmpty(NonBase) then z:=0;
      else z:=&+[Multiplicity(L,p): p in NonBase];
      end if;

      if IsEmpty(Base) then z:=z;
      else z:=z+ &+[Multiplicity(L,a[1])-a[2]+1:a in Base];
      end if;

      t:=0;

      for a in BaseSpe do
          if Multiplicity(L,a[1]) gt 2 then t+:=1;
          end if;
      end for;

      if t eq 0 and z eq 0 then
         d:=Dimension(L);
      else d:=-1;
      end if;

end while;

printf "Le degre minimal d'interpolation pour D_b^- est %o. ",n;

// Ensuite c'est comme d'habitude...
```

F.2 Calculs de matrices de parité de codes LDPC

```
// Cette fonction permet de repertorier separement
// toutes les droites rationnelles de P3 qui sont contenues
// dans une cubique donnee et toutes celles qui l'intersectent
// en exactement trois points distincts. Elle compte egalement
// le nombre de droites de la seconde categorie qui est issue
// de chaque point.

function PickInc(F,Form)

Surf:=Scheme(P3,Form);
AffSurf:=AffinePatch(Surf,1);
Points:=RationalPoints(AffSurf,F);

A1<t>:=AffineSpace(F,1);
```

```
LP:=[{@Parent(AffSurf)| @}: i in {1..#Points}];
LD3:={@Parent(AffSurf)| @};
LDinc:={@Parent(AffSurf)| @};
PointsBis:=IndexedSetToSet(Points);


for p in Points do
L1:=Coordinates(p);
Exclude(~PointsBis,p);
        for q in PointsBis do
        L2:=Coordinates(q);

// On construit notre droite.

        h:=map<A1 -> A3 | [t*L1[k]+(1-t)*L2[k]:
                  k in {1..3}]>;
        D:=Image(h);
        Sec:=AffSurf meet D;
        PtSec:=RationalPoints(Sec,F);
                if D eq Sec then Include(~LDinc,D);
                elif #PtSec eq 3 then Include(~LD3,D);
                        Include(~LP[Index(Points,p)],D);
                        Include(~LP[Index(Points,q)],D);
                end if;
        end for;
end for;
LPcard:=[#LP[i]: i in {1..#LP}];
return [* LPcard, LP ,LD3,LDinc *];
end function;
```

Nous allons ensuite présenter la fonction qui permet de calculer une matrice de parité creuse. Cette dernière fait appel à une fonction dont nous ne donnerons pas le code source et qui à une droite affine associe un vecteur directeur.

```
// Cette fonction calcule une matrice de parite creuse.

function GenMatDiff(Form)

// On prend notre liste de droites interessantes.

L:=PickInc(F,Form)[3];
Surf:=Scheme(P3,Form);
AffSurf:=AffinePatch(Surf,1);
Points:=RationalPoints(AffSurf,F);
k:=#L;
n:=#Points;

// Il faut qu'on sache par quels points passe chaque droite:

IncidenceCtB:=[];
for i:=1 to k do
S:=[];
```

```
        for j:=1 to n do
                if Points[j] in Scheme(A3,Equations(L[i]))
                   then Append(~S,j);
                end if;
        end for;
Append(~IncidenceCtB,S);
end for;
UU:=[Equations(L[i]): i in {1..#L}];
U:=[];

// On calcule un vecteur directeur pour chaque droite.

for j :=1 to #UU do
Append(~U,DirVec(UU[j]));
end for;
delete UU;

// On calcule quelques derivees partielles...

AffForm:=UnHom(Form);
fx:=Derivative(AffForm,1,x);
fy:=Derivative(AffForm,1,y);
fz:=Derivative(AffForm,1,z);

// Et on va construire notre matrice.

MM:=[];
for j:=1 to k do
        ZZ:=[F| 0 : o in {1..n}];
        a:=IncidenceCtB[j];
        for i:=1 to 3 do
                p:=Coordinates(Points[a][i]);
                d:=1/(Evaluate(fx,p)*U[j][1]+Evaluate(fy,p)*U[j][2]
                + Evaluate(fz,p)*U[j][3] );
                ZZ[a[i]]:=d;
        end for;
        Append(~MM,ZZ);
end for;
Matmat:=Matrix(F,k,n,MM);
return Matmat;
end function;
```

Bibliographie

[Aub92] Yves Aubry. Reed-Muller codes associated to projective algebraic varieties. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 4–17. Springer, Berlin, 1992.

[BHPV] Wolf P. Barth, Klaus Hulek, Chris A. M. Peters, and Antonius Van de Ven. *Compact complex surfaces*, volume 4 of *Ergebnisse der Mathematik und ihrer Grenzgebiete.* Springer-Verlag, Berlin, second edition, 2004.

[Bou59] Nicolas Bourbaki. *Algèbre.* Hermann, Paris, 1959.

[Bou03] Thanasis Bouganis. Error correcting codes over algebraic surfaces. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*, volume 2643 of *Lecture Notes in Comput. Sci.*, pages 169–179. Springer, Berlin, 2003.

[Cha93] Indra M. Chakravarti. Geometric construction of some families of two-class and three-class association schemes and codes from nondegenerate and degenerate Hermitian varieties. *Discrete Math.*, 111(1-3) :95–103, 1993. Graph theory and combinatorics (Marseille-Luminy, 1990).

[Coh46] Irvin S. Cohen. On the structure and ideal theory of complete local rings. *Trans. Amer. Math. Soc.*, 59 :54–106, 1946.

[Cou08] Alain Couvreur. Sums of residues on algebraic surfaces and application to coding theory, 2008. Preprint. ArXiv :0810.4112v1.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43) :273–307, 1974.

[DGM70] Philippe Delsarte, Jean-Marie Goethals, and Florence J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16 :403–442, 1970.

[Edo07] Frédéric A. B. Edoukou. Codes defined by forms of degree 2 on Hermitian surfaces and Sørensen's conjecture. *Finite Fields Appl.*, 13(3) :616–627, 2007.

[Edo08] Frédéric A. B. Edoukou. Codes defined by forms of degree 2 on quadric surfaces. *IEEE Trans. Inform. Theory*, 54(2) :860–864, 2008.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995.

[GH78] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry.* Wiley-Interscience [John Wiley & Sons], New York, 1978. Pure and Applied Mathematics.

[GL00] Sudhir R. Ghorpade and Gilles Lachaud. Higher weights of Grassmann codes. In *Coding theory, cryptography and related areas (Guanajuato, 1998)*, pages 122–131. Springer, Berlin, 2000.

[Gop81] Valery D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6) :1289–1290, 1981.

[Gop88] Valery D. Goppa. *Geometry and codes*, volume 24 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1988. Translated from the Russian by N. G. Shartse.

[Han00] Johan P. Hansen. Toric surfaces and error-correcting codes. In *Coding theory, cryptography and related areas (Guanajuato, 1998)*, pages 132–142. Springer, Berlin, 2000.

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

[Har66] Robin Hartshorne. *Residues and duality*. Lecture Notes in Mathematics, No. 20. Springer-Verlag, Berlin, 1966.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[HP95] Tom Høholdt and Ruud Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 41(6, part 1) :1589–1614, 1995.

[HTV94] James W.P. Hirschfeld, Michael Tsfasman, and Sergei G. Vlăduţ. The weight hierarchy of higher dimensional hermitian codes. *IEEE Trans. Inform. Theory*, 40(1) :275–278, 1994.

[HVP98] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan. Algebraic geometry of codes. In *Handbook of coding theory, Vol. I, II*, pages 871–961. North-Holland, Amsterdam, 1998.

[KA79] Steven L. Kleiman and Allen B. Altman. Bertini theorems for hypersurface sections containing a subscheme. *Comm. Algebra*, 7(8) :775–790, 1979.

[Lac86] Gilles Lachaud. Les codes géométriques de Goppa. *Astérisque*, (133-134) :189–207, 1986. Seminar Bourbaki, Vol. 1984/85.

[Lac88] Gilles Lachaud. Projective Reed-Muller codes. In *Coding theory and applications (Cachan, 1986)*, volume 311 of *Lecture Notes in Comput. Sci.*, pages 125–129. Springer, Berlin, 1988.

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

[Lac96] Gilles Lachaud. Number of points of plane sections and linear codes defined on algebraic varieties. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 77–104. de Gruyter, Berlin, 1996.

[LT97] Gilles Lachaud and Michael A. Tsfasman. Formules explicites pour le nombre de points des variétés sur un corps fini. *J. Reine Angew. Math.*, 493 :1–60, 1997.

[Lip84] Joseph Lipman. Dualizing sheaves, differentials and residues on algebraic varieties. *Astérisque*, 117 :ii+138, 1984.

[Lit08] John B. Little. Algebraic geometry codes from higher dimensional varieties, 2008. Preprint, arXiv :math/0802.2349v1.

[LM05] Michael G. Luby and Michael Mitzenmacher. Verification-based decoding for packet-based low-density parity-check codes. *IEEE Trans. Inform. Theory*, 51(1) :120–127, 2005.

[Mat86] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[MMR08] Edgar Martinínez-Moro, Carlos Munuera, and Diego Ruano, editors. *Advances in algebraic codes*, volume 5 of *Series on coding theory and cryptology*. World Scientific, 2008.

[MS77a] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[MS77b] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error-correcting codes. II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[Mum99] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, second edition, 1999.

[Nog96] Dmitri Y. Nogin. Codes associated to Grassmannians. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 145–154. de Gruyter, Berlin, 1996.

[Par76] Aleksei N. Paršin. On the arithmetic of two-dimensional schemes. I. Distributions and residues. *Izv. Akad. Nauk SSSR Ser. Mat.*, 40(4) :736–773, 949, 1976.

[Poo04] Bjorn Poonen. Bertini theorems over finite fields. *Ann. of Math. (2)*, 160(3) :1099–1127, 2004.

[PSV91] Ruud Pellikaan, Ba-Zhong. Shen, and Gerhard J. M. van Wee. Which linear codes are algebraic-geometric ? *IEEE Trans. Inform. Theory*, 37(3, part 1) :583–602, 1991.

[Rod03] François Rodier. Codes from flag varieties over a finite field. *J. Pure Appl. Algebra*, 178(2) :203–214, 2003.

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

[SD67] Henry P. F. Swinnerton-Dyer. The zeta function of a cubic surface over a finite field. *Proc. Cambridge Philos. Soc.*, 63 :55–71, 1967.

[Ser59] Jean-Pierre Serre. *Groupes algébriques et corps de classes.* Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[Ser91] Jean-Pierre Serre. Lettre à M. Tsfasman. *Astérisque*, (198-200) :11, 351–353 (1992), 1991. Journées Arithmétiques, 1989 (Luminy, 1989).

[Sha94] Igor R. Shafarevich. *Basic algebraic geometry. 1.* Springer-Verlag, Berlin, second edition, 1994.

[Sør91] Anders B. Sørensen. *Rational points on algbraic surfaces, Reed-Müller codes and Algebraic-Geomatric codes.* PhD thesis, Aarhus, Denmark, 1991.

[Ste99] Serguei A. Stepanov. *Codes on algebraic curves.* Kluwer Academic/Plenum Publishers, New York, 1999.

[Sti93] Henning Stichtenoth. *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.

[Tan81] R. Michael Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inform. Theory*, 27(5) :533–547, 1981.

[TV91] Michael A. Tsfasman and Sergei G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series).* Kluwer Academic Publishers Group, Dordrecht, 1991.

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

[VM84] Sergei G. Vlăduts and Yuri I. Manin. Linear codes and modular curves. In *Current problems in mathematics, Vol. 25*, Itogi Nauki i Tekhniki, pages 209–257. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[VZ05] Felipe Voloch and Marcos Zarzar. Algebraic geometric codes on surfaces, 2005. Preprint. `http://www.ma.utexas.edu/users/voloch/Preprints/luminy.pdf`.

[Wib96] Niclas Wiberg. *Codes and Decoding on General Graphs.* PhD thesis, Department of Electrical Engeneering, Linköping University, Sweden, `http://citeseer.ist.psu.edu/wiberg96codes.html`, 1996.

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