UNIVERSITÉ DE LA MÉDITERRANÉE
AIX-MARSEILLE II
Faculté des Sciences de Luminy

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE E.D. 184

THÈSE

pour obtenir le grade de

DOCTEUR DE L' UNIVERSITÉ DE LA MÉDITERRANÉE

Discipline : Mathématiques

présentée et soutenue publiquement
par

Frédéric Aka Bilé EDOUKOU

Mardi 26 Juin 2007, à 10h30
Institut de Mathématiques de Luminy (Amphi Herbrand)

Titre

Codes Correcteurs d'Erreurs Construits à Partir des Variétés Algébriques

Directeur de Thèse : François RODIER

JURY

M. Yves Aubry	Maître de Conférences (H.D.R.), U.S.T.V, Toulon	Examinateur
M. Johan P. Hansen	Professeur, University of Aarhus, Danemark	Rapporteur
M. James W. P. Hirschfeld	Professeur, University of Sussex, Royaume Uni	Rapporteur
M. Gilles Lachaud	Directeur de Recherche, CNRS-I.M.L Marseille	Examinateur
M. François Rodier	Directeur de Recherche, CNRS-I.M.L Marseille	Directeur
M. Leo Storme	Professeur, Ghent University, Belgique	Examinateur

Remerciements

Je remercie vivement mon valeureux et dynamique directeur de Thèse, François Rodier, pour m'avoir proposé ce sujet de recherche assez passionnant et apporté son soutien ainsi que de nombreuses idées nécessaires à sa réalisation. Ses compétences scientifiques, son sens de l'orientation et ses qualités humaines notamment, sa patience et son organisation, m'ont permis de surmonter de nombreuses difficultés liées à ce travail.

Je tiens à remercier infiniment Gilles Lachaud, directeur de l'Institut de Mathématiques de Luminy (I.M.L) de s'être intéressé à mon travail et d'avoir accepté inconditionnellement d'être mon interlocuteur auprès du ministère de l'enseignement supérieur et de la recherche scientifique de Côte d'Ivoire pour toute affaire me concernant, en plus des avis favorables et de la bonne appréciation de mon directeur de thèse sur mon travail. J'ai été très touché par le fait qu'il me confia des responsabilités assez importantes au sein de ce laboratoire qu'il dirige et aussi par ces réponses à mes nombreuses questions en mathématiques. Je remercie le professeur Leo Storme (Department of Pure mathematics and computer algebra of Ghent University) de Belgique, pour sa participation au jury. Je remercie également Yves Aubry le plus jeune de tous (parmi les membres du Jury) pour ses nombreuses critiques très constructives, pour sa participation au jury, pour un travail qu'il a vu prendre forme et enrichi de ses idées depuis l'étape embryonnaire jusqu'à son éclosion et aussi pour sa sympathique amitié.

Je remercie très sincèrement le professeur Johan P. Hansen (University of Aarhus, D.K) président de la société de mathématiques du Danemark et le professeur James W. P. Hirschfeld (Emeritus Professor of Sussex University, Brighton, U.K), deux grands spécialistes de la géométrie algébrique sur des corps finis pour avoir accepté d'être rapporteurs de cette thèse et d'être membres du Jury malgré leur emploi du temps très chargé. Ce fut pour moi un grand honneur. Leurs nombreux conseils et suggestions concernant cette thèse m'ont été d'un grand secours.

Je remercie les membres de l'équipe A.T.I (Arithmétique et Théorie de l'Information) de l'I.M.L de Marseille, particulièrement Robert Rolland, Stéphane Louboutin, M. Laurent, nos deux russes S. Vladut et M. Tsfasman pour leur soutient et leur amitié. Je remercie le professeur David B. Leep (University of Kentucky, U.S.A) pour sa disponibilté et ses critiques qui m'ont permis d'améliorer mes articles, et le professeur Ladnor Geissinger (University of North Carolina - Chapell Hill, U.S.A) pour sa fructueuse correspondance.

Merci à Aurelia et Eric Lozingot pour leur gentillesse et leur efficacité pour toutes mes démarches administratives à l'I.M.L. Merci à Corinne Roux pour sa compréhension à la tête des relations internationnales à l'I.M.L. Merci également à Jean-Bruno Erismann pour le mal qu'il s'est donné en résolvant mes innombrables petits problèmes en informatique. Je remercie aussi Nathalie Granottier responsable de la bibliothèque du C.I.R.M qui était toujours à mes petits soins par rapport à ma documentation et aussi pour son amitié.

Je profite de ce moment pour saluer cette vision qu'ont eue tous ceux qui ont été à la base de la création du C.I.R.M (Centre International de Rencontres Mathématiques) situé sur le site de Luminy à Marseille, grand carrefour de la recherche en mathématique. En effet les travaux exposés dans ce centre par des conférenciers venus des quatre coins du monde, montrent bien qu'il y a une continuité dans les mathématiques et confirment non seulement le caractère universel des mathématiques "langage commun à toutes les sciences" mais aussi et surtout que les mathématiques dans leur ensemble constituent l'un des fondements d'une société de technologie avancée.

Merci aux amis du Groupe de Travail surfaces algébriques: Christophe Ritzenthaler, Anne Pichon, Adnen Sboui, Alexey Zykin, Karl Oeljeklaus, J.-P. Brasselet, Alain Couvreur, Philippe Lebacque. Merci aussi à tous les membres, thésards (Alain, Marc, J.B., Etienne, Anis, Zaid, Lionel, Anne, Héla, Amara, Nivaldo, Mohamed) post doctorants (Saabbouh, Nicolas, Arnaud, Redha, Idriss, Kaboré, Marion) de l'Institut de Mathématiques de Luminy.

Mes remerciements vont aux organisateurs et aux participants de la rencontre du 15 au 20 octobre 2006 à Eymoutiers (Haute Vienne) du groupe de travail C_2 (Codage et Crytographie) du GDR Informatique Mathématique, pour leurs remarques et suggestions. La bonne entente et la convivialité qui régnèrent sur les réunions du C_2 furent une clef de la réussite et de l'avancement de mes travaux. A un moment où il est légitime de s'interroger sur les débouchés offerts par un doctorat en mathématiques, il me paraît important de rappeler la conclusion de Franck Leprévost dans son article de survol [Les standards cryptographiques du XXIe sicle: AES et IEEE-P1363. Gaz. Math. No. 85 (2000), 9–23. 94 A60] qui signale que la sécurité des systèmes d'informations est un domaine riche d'opportunité pour notre discipline et notamment pour notre groupe de travail C_2 (Codage et Cryptographie) du GDR-IM.

Je rends un grand hommage au professeur Touré Saliou grande vedette des mathématiques en Côte d'Ivoire, ministre de l'enseignement supérieur et de la recherche scientifique de Côte d'Ivoire (1993-1996) qui a su redynamiser les mathématiques dans ce pays. Par son dévouement et son audace intellectuelle, la Côte d'Ivoire a pu se doter d'un institut de mathématiques (I.R.M.A), d'une société mathématiques (S.M.C.I), et bien d'autres structures contribuant au développement de ce pays aux potentiels énormes, qui malheureusement depuis le jeudi 19 septembre 2002 sombre dans de profondes ténèbres par la faute d'une machination très bien orchestrée !!! Notre devoir en tant que mathématiciens de la troisième génération serait de placer impérativement les mathématiques au coeur du développement de cette Côte d'Ivoire grâce à une collaboration intense avec les plus grandes institutions scientifiques mondiales, autrement notre Côte d'Ivoire restera éternellement dans le marasme du sous-développement!

Je pense également à Bamba Vamoussa ministre de l'éducation nationale de Côte d'Ivoire (1990-1993) évacué d'urgence sur Paris par manque d'un hôpital de haute qualité scientifique digne de notre pays (après plusieurs années de croissance économique en Côte d'Ivoire !!!) et décédé quelques jours plus tard dans un hôpital parisien le samedi 19 juin 1993 dans l'attente de nos résultats du Baccalauréat.

Je remercie également tous ces coopérants français, le professeur Edmond Fedida, le professeur Réné Gaudot, le professeur Boubakar Ba, Viry Guy, Alain Fouques, Bonhard Christian, Gérard Vinel, Durand, Jérôme Fehrenbach, Henri Dichi, Pitoun Frédéric et bien d'autres qui ont quitté leur pays la France pour venir nous transmettre le message des mathématiques avec enthousiasme et ferveur à l'Université d'Abidjan (Cocody) dans des conditions qui ne sont pas les leurs. Je pense aussi à ce coopérant belge le professeur Michel Duhoux qui a très bien professé l'analyse pendant plusieurs années au département de mathématiques de l'Université d'Abidjan (Cocody). Je pense également à tous ces missionnaires français Pierre-Yves Lagrée, le professeur Pierre Eymard, le directeur de recherche Jérôme Los, le professeur Aziz El Kacimir, ce missionnaire Luxembourgeois (qui a d'ailleurs fait sa thèse de doctorat en France en même temps que le professeur Touré Saliou avec le même directeur de thèse) le professeur Jean Paul Pier et bien d'autres venus tous à Abidjan pour des colloques, des conférences, des séminaires et des séances de travail, enrichir nos connaissances mathématiques.

Je ne saurais oublier Lê Dũng Tráng par qui je suis arrivé à Marseille et avec qui j'ai fait mes premiers pas dans la recherche en mathématiques, David Trotman le premier directeur de l' Ecole Doctorale de Mathématiques et Informatique que j'ai eu à Marseille et Hamish Short directeur très sympathique du LATP pendant mon sejour au CMI. Merci également à Nathalie Bonifay, Aline Blanc, Noëlle Tabarraci, Gerard Henry, tous du CMI.
Je remercie le directeur de l'U.F.R-M.I de l'Université d'Abidjan (Cocody) feu Donatien Niango et tout le personnel enseignant du Département de Mathématiques de l'Université d'Abidjan (Cocody) pour leur soutien notamment feu le professeur Pierre Nezit, le professeur Sangaré Daouda, le professeur N'Zi Modeste, Adjé A. Venance, Kangni Kinvi, Etienne Desquith, Koua Konin, Aballo Koffi, Berété, Fofana Ibrahim, Bamba Siaka, Ahoua Don Mello, Tchéré Seka, Danho Emile, Adou Kablan, Mobio, Kouakou Mathias, M. Guissé, Sohou Toussaint, Ayegnon P. Kodjo, Camara, Diallo Boubakar, Bla Toh Lambert, Kouadio Moya, Tanoé François, Koua Brou, Soumahoro, Arra Joseph, Mensah, Ligan Etienne, Diallo Hassimiou, Monsan Vincent, Kourouma, Florentin, Badara.
J'exprime aussi ma profonde reconnaissance à mes enseignants du département de physique pendant mon premier cycle universitaire à l'Université d'Abidjan (Cocody), les professeurs Ebby N'Dédé, Touré Siaka, Assamoi, Mohamed Charles, Mme Yao, Mme Koblavi Frédérica, Sylla, Kouadio, Aman, Sako, Monean. Je remercie également le professeur Claude Belorgeot coopérant français au departement de physique de l'Université d'Abidjan (Cocody).

Je tiens à remercier également mon directeur du C.S.P (Cours Secondaire Protestant) de Dabou Boni Koffi Amos, mon sous-directeur Boka Akré, mes éducateurs Dapleu et Mondé, et mes professeurs Koffi K. Pierre (mon pote), Béchehin Aboua, Zanouya Roger Camille, Edi, Gayé, Hibo G. Appolinaire, Kikibo Raphael, Bah Tierno B, Amoussou F. André, Ad-

joumani Y. Joseph, Amafon, Mr Ouattara, Mr Dialy, Yao, Diallo Dilane, Gnakpa Georges, Aminou, Migan, Herr Titiro, Herr Kouakou, Ourigou, Segui Michel, Fally, Dinguamio, feu Doungouss, le pasteur Boto, tantie Berthe, Mme Bourallima, Mme Ahuia née Don Loba Florence pour de très nombreuses et passionnantes discussions, et surtout pour ma formation dans leur établissement. Je remercie de façon très spéciale mon professeur de mathématiques des classes de prémière et terminale Bli Soignon Jean-Baptiste (qui fit de brillantes études de mathématiques dans une école d'ingénieur à Paris). Il fut celui qui me transmit la véritable passion pour les mathématiques, avec lui, j'appris beaucoup sur l'histoire des mathématiques et de la France mathématique. Je remercie également ces deux coopérants français et professeurs de mathématiques Bartoli et Thierry Foucauld au C.S.P de Dabou.

Je remercie mon directeur du C.E.G (Collège d'Enseignement Général) de Dabou Koutouan Noël, mon éducateur Agba Essis Athanase et mes professeurs Kidou Deni, Gbakayoro Celestin, Berthé, Kakou Gnangbo, Tro Miami, Adjelou J.B., N'Gô Ding Luong, Yapi A.C, Adjéhi Koffi, Desouza, Kahan Cristophe, Sina Ouattara, Kouamé, Kouassi Dominique, Diop, Barry Alpha, Jolissain Hubert, feu Zézé, feu Aka Tanoh Faustin, feu Mr N'Dja, feu Louess, feu Herr Niamblé Amon, Mr. Norbert, Nejmi Habib, Herr Cissé, Cissé, Gnakoua, Keïta, Sery, Ezoua Yves, Mr Zegri, Kouassi Celestin, Tiello Diallo, Mme Amessan, Herr Boya, Anoma, Guissé, Silué K., Vitou Thomas, M. et Mme Toffa. Je remercie également Monsieur Villette, coopérant français et professeur de mathématiques au C.E.G de Dabou.

Je remercie mon directeur de l'Ecole Primaire Publique Wrod de Dabou Etchien E. Jacob, mon conseiller pédagogique Ebbé, mes instituteurs Boli Bi, Tra Bi, Barou T. Lazare, Kouassi Pascal, Aka Georges, N'Da, feu Pascal, feu Kanda, feu Alberic, Kouassi, Goré, mes institutrices Aka Esther Amoi, Tantie Béa, et bien d'autres enseignants dont les noms m'echappent maintenant.

Je remercie également l'Etat de Côte d'Ivoire pour m'avoir octroyé une bourse couvrant toutes mes années d'étude en France. Je tiens également à remercier M. Diaby Seydou pour avoir mis un serieux indescriptible et étonnant dans son travail à la D.O.B-BHCI. Mes remerciements vont aussi à M. Anoma, M. Yohou, M. Ouézadé Parfait les directeurs successifs du service étudiant de l'ambassade de Côte d'Ivoire à Paris que j'ai connus, Mme M'Bra Wadja (que j'ai beaucoup fatiguée !), Morisson, Mme Hikpo et à tout le personnel du service étudiant de l'ambassade de Côte d'Ivoire à Paris.

Merci à mes nombreux frères et cousins Ed, Willy, Vier, Boris, Moses[3], Bejog, Kodjo[3], Joseph, J.B. Assogba, Pablo, Labbé Yves, Ahoua, Jacob Tegnan, Kouaho Clement, Yessoh, Asouan Amichia, Ebatchi, Bognini, Benjamin[2], Domi, Adjéhi, Mathieu, Popo, Roche, Koko, Douakpa, William, Marius, Adé N'Dakon Roger, Michel, Grand G, Aaron, Blin, feu Bouadi Kodjo Emmanuel, Señor Keshi, Dr Ehui Chambro et amis Yéo, feu Kaboré Aboudou, Assalé Modeste, Malan Emmanuel, Aristide Ouédraogo, Maroff Ouédraogo, Yobouet Olivier, Jonas, Meledje L. Hervé, Kabran Stéphane, Sam Kook, Edi Euloge, Kougba, Traoré Wilfried, Bamouni, Troukoula, Gnahor's, Mouho K. Pierre, Okou Abdul, Augustin, Christian, Adebissi, Assiongbon Ekwé Richard, Togbé T., Yod, Salé Cyril, Franck Goussanou, Marcelin,

Boli Tina, Agodio, Jean Pagnon, Romain Bondil, Estelle Souche, Fabien Pellegrini, Jean-Mars, Azoum, Kanga Kouassi Gérard, Edo S. Narcisse, Guizo, Kougbla Dominique, Tuo Navégué, Scotty, Labbé Kodji Bietch Armand, Angbonou Assalé, Djéhi Eric, Koné Aboudramane, Edri Sobou, Doté Arnaud, Faidol parade, Zoffou Aymard, Badé Arthur, pour leurs encouragements. J'adresse mes remerciements à mes nombreuses soeurs et cousines Adjoumani (ma nourrice dépuis ma tendre enfance), T.V, Nanetchi[2], Amah[2], Tenatchi, Annie[2], Sidonie, Asseytou[2], Cathy, Abrima Ackohi, feue Konan Aya Marie, Houéssou, Eboué, Ackohi A. Victoria, Sonia, Ferrima, Doudou, Ackah Sey Patricia, Adjouba, Magui, Joséphine, Sabine, Josie, Edith Lobognon, Marthe, Akou[2] (pour leur détermination à me sauver des difficultés indépendamment de ma volonté).

Je rends aussi un grand hommage à mon oncle feu Amouzou Kouamé Jacques, qui a su m'inculquer le goût du travail depuis mon plus bas âge et qui me parlait depuis tout petit du grand héritage et du potentiel scientifique de la France (pays qu'il connaissait très bien après y avoir passé une dizaine d'années) et aussi du transfert de technologies en Afrique via ces grandes puissances. Je remercie mon homonyme Miezan Aka-Bilé Frédéric pour sa profonde confiance en moi, papa Moise pour ces nombreuses prières, papa Akattia, feu Adjima Kouassi, feu Anodjo, tonton Daniel, tonton N'Drin Damas, Kèssi, Wadja, Gnammone Felix, Aka, Samson, Dominique, N'da, Richard, Edoukou, Akley, Aklompo, l'inspecteur Gnanzou, Colonel Aka Kodjo Marc, Dr John Beyebewon Anwomeah, feu Francis Kotokou, tonton Kouassi Bernard, feu papa Somia, feu Ackohi Paul, feu Gnuan Blaise, feu Kouaho, feu Mockey, feu Miezan Edoukou Vincent, feu Ackah Sey John, feu Adoulé Anthony pour m'avoir mis au point en anglais. Je remercie également feue Mamie Edoukou, mes tantes Gankou Cecile, Aka Odette, Awolê Monica, Affiba[2], Ahiza[2], Ahou[2], Attobla, Wawa, feue Magni, Adou Abba, Marceline, Abrima, Adjoubatchi, Echui-Bla, Pauline, feue Soma, Charlotte, maman Nando Françoise, Manza-Adjoba, Kangah Béatrice, Alima Joséphine, Mouchia[3], Beniè[3], Gnamekè-Amon, Tchètchè, Sorba, Caworma, Adjoua Agnès.

Je remercie le président du département de Mathématiques de la faculté de sciences de Luminy Arnaldo Nogueira et nos deux sympathiques secrétaires Sophie Realini, Haguenauer Catherine pour leur gentillesse. Je remercie le professeur Valent Galiano, Myriam Quatrini et Tomasz Stanislaw Miernowski qui m'ont permis aussi de profiter de leur expérience dans l'enseignement des mathématiques. Je remercie Christian Mauduit, Marie-Renée Fleury-Donnadieu et Dominique Barbolosi pour ma formation pendant mon stage Hyppocampe-Maths à l'I.R.E.M (Institut de Recherche sur l'Enseignement des Mathématiques) de Marseille. Je remercie mes étudiants de licence MASHS et MI de la faculté des sciences de Luminy pour leurs remarques et suggestions qui ont permis de m'améliorer dans les cours que je leur dispensais durant l'année universitaire 2006-2007.

Je dis également merci à tous ceux qui ont contribué à ma formation spirituelle afin de ne pas m'être égaré en me détournant un temps soit peu du vrai chemin de Dieu et emprunter le chemin de la vanité et de la perdition pendant cette longue traversée du désert. Je pense aussi aux fondateurs et aux membres de l'église d'action.

Je remercie Adjouba Marie-France que j'ai connue pendant 22 semaines 2 jours et Jin-Ah Maeva pour cette joie qu'elle m'a apportée dans la deuxième moitié de cette thèse. Je remercie également Adjoua Sylvia pour son soutien très considérable.

Je remercie mes médecins Dr Kouakou, Dr Yao Antoine en C.I., Dr Adamo Doumbia, Dr Vidal, Dr Brechard, Dr Sanchez, Dr Laplane, Dr Serratrice, Dr Billé-Turc, Mme Scott à Marseille, les Professeurs Cazenave, Claude Gras, Mansini, Pelissier, Raibaud à Marseille. Des gens qui m'ont aidé aussi dans ma vie, Vieux Allah, Essofo Ekoué, Essofo Aklou, neyan Koffi et monsieur Amon. Je remercie également les abbés Maestragi et Jean Lahondès de Marseille.

Je remercie également Mme Rocchi Jacqueline le propriétaire de mon appartement de Marseille et Mme Allasia Audrey ma conseillère à la banque populaire du prado à Marseille pour leur gentillesse et leur profonde confiance en moi. Je remercie Simone Ouattara, Niagne Jacqueline, Yédès Méliou. Je remercie Mel et Sofia Akpa, Arthur et Françoise Amani, Valentin et Elisa Gbeuly pour leur soutien.

Je remercie ma communauté chrétienne de Nice et principalement les familles Hur, Bliksas, Koyama, Parquet, Bortner, Hochster, Patricia, Chaillié, Curzi pour leur soutien.

Je rends aussi un grand hommage à notre ami Sylla Ibrahim étudiant africain en master première année de mathématiques au Département de Mathématiques de la Faculté des Sciences de Luminy assassiné le dimanche 1er avril 2007 à Marseille-Luminy dans la pire des atrocités !!! Nous avions partagé ensemble les mêmes passions pour les mathématiques et pour l'Afrique noire.

Je pense aussi à toutes ces personnes qui se sont battues comme de vaillants soldats pour améliorer mon avenir, fuyant la guerre pour certains, la souffrance et la misère pour d'autres, et dont mon arbre généalogique me fait remonter jusqu'à eux, feu neyan Yeboah, feu neyan N'Doua, feu neyan Johnson of Axim, feue nanan Awolê, feu nanan Bouzouma, Essofo Amon, feue nanan Allaba, feue nanan Kodjo Kanha Jeanne, feue nanan Gnamekè-Kwansima, feue Essofo Kakou Adjouba, la grande famille Bognini, feue nanan Adjéïba, feue nanan Wôma, neyan Ediémou, feue nanan Caworma, nanan N'Da, feu neyan Kodjo (black man), feu neyan Egnankou, feu neyan Essalli, feu neyan Allou, feu neyan Kouamè, feu neyan Edoukou, feu neyan Miezan, feu neyan Attobla, feu neyan Bediakon, feu neyan Adoulé, feu neyan Beyebewon, feu nanan Akoua, feu nanan Essi, nanan Amah, feu nanan Alba etc...

Je remercie tous ceux que j'ai certainement oubliés ici. La liste est longue vu que le chemin a été long !!!

Enfin, je tiens à louer mon père Miezan Edoukou Antoine pour sa bienveillance, sans laquelle cette thèse n'aurait jamais vu le jour. La préparation et l'achèvement de cette thèse n'auraient aucun goût sans le réconfort de ma mère Beyebewon N'Vidah Anne-Marie.

Table des matières

Introduction **10**
0.1 Rappels sur les Codes Correcteurs 10
0.2 Dénombrements dans l'espace projectif $\mathbb{P}^n(\mathbb{F}_q)$ 11
0.3 Introduction du code fonctionnel 12
0.4 Les variétés hermitiennes et quelques propriétés fondamentales 13
0.5 Le code $C_h(X)$ défini sur la surface hermitienne non-dégénérée 14
0.6 Etude du code $C_2(X)$ défini pour X une surface quadrique 18
0.6.1 X est une quadrique hyperbolique dans $\mathbb{P}^3(\mathbb{F}_q)$ 19
0.6.2 X est une quadrique elliptique dans $\mathbb{P}^3(\mathbb{F}_q)$ 20
0.6.3 X est une quadrique dégénérée de rang 3 dans $\mathbb{P}^3(\mathbb{F}_q)$ 21
0.7 Le code $C_2(X)$ défini sur les variétés quadriques dans $\mathbb{P}^4(\mathbb{F}_q)$ 22
0.8 Le code $C_2(X)$ défini sur les variétés hermitiennes non-dégénérées dans $\mathbb{P}^4(\mathbb{F}_q)$ 23
0.9 Questions ouvertes: deux conjectures à résoudre 25
0.9.1 Conjecture sur la distance minimale de $C_h(\mathcal{X})$ dans $\mathbb{P}^n(\mathbb{F}_q)$ 25
0.9.2 Conjecture sur les 5 premiers poids de $C_2(\mathcal{X})$ dans $\mathbb{P}^n(\mathbb{F}_q)$ 25

1 Codes defined by forms of degree 2 on hermitian surfaces and Sørensen's conjecture **28**

2 The weight distribution of the functional codes defined by forms of degree 2 on hermitian surfaces **45**

3 Codes defined by forms of degree 2 on quadric surfaces **59**

4 Codes defined by forms of degree 2 on quadric and non-degenerate hermitian varieties in $\mathbb{P}^4(\mathbb{F}_q)$ **65**

Introduction

0.1 Rappels sur les Codes Correcteurs

Soit p un nombre premier et $q = p^a$ une puissance de p. On note $\mathbb{F}_q$ le corps fini à q éléments. On appelle **code** (linéaire) de longueur n, de dimension k, un sous-espace vectoriel de ${\mathbb{F}_q}^n$. Les éléments de ce sous espace vectoriel C sont appelés les **mots** du code.
Soit $x = (x_1, x_2, \ldots, x_n)$ un mot du code C et $J = \{1, \ldots, n\}$. Le support de x est l'ensemble défini par $\text{supp}(x) = \{i \in J \mid x_i \neq 0\}$. Le poids de Hamming de x qu'on note $w(x)$ est le nombre de composantes non-nulles de x:

$$w(x) = \#\text{supp}(x).$$

Soient x et y deux éléments du code, on définit la **distance de Hamming** $d(x, y)$ entre x et y comme étant le nombre de composantes en lesquelles x et y diffèrent. Plus précisement si $x = (x_1, x_2, \ldots, x_n)$ et $y = (y_1, y_2, \ldots, y_n)$, alors

$$d(x, y) = \#\{x_i \neq y_i, 1 \leq i \leq n\}$$

Et on a la relation :

$$w(x) = d(x, O)$$

La **distance minimale** $d(C)$ d'un code C est la plus petite distance entre deux mots distincts. Comme $d(x, y) = w(x - y, O)$, on en déduit que la distance minimale est aussi le plus petit poids; on a:

$$d(C) = \min\{w(x), c \in C \text{ et } c \neq O\}$$

Un code C de longueur n, de dimension k et de distance minimale d est noté C=[n,k,d] et on dit que n,k, et d sont les **paramètres** du code C.

Deux des objectifs les plus recherchés dans la désignation d'un bon code sont:

Grande efficacité: dans le sens d'avoir un nombre relativement grand de mots du code pour une longueur donnée.

Grande distance minimale: pour une capacité de correction assez grande. En effet un code dont la distance minimale est d corrige exactement $e = [\frac{d-1}{2}]$ erreurs, et le nombre e est appelé la capacité de correction du code.

Un autre but aussi important dans la désignation d'un bon code est l'obtention d'un algorithme de codage-décodage susceptible d'être implémenté sur une machine de façon simple et de travailler pendant un temps court. Et pour ce troisième objectif, on peut faire appel à la **distribution des poids**.
Malheureusement, toutes ces exigences ne vont pas de pair, elles sont contradictoires. Et c'est pour cela que la désignation d'un bon code ou la recherche d'un bon code découle d'un processus difficile.
La théorie des codes correcteurs est née de par la nécessité de transmettre des messages à travers un canal bruité. Comme exemple nous avons, les conversations téléphoniques, les télécommunications par satellite, les faisceaux hertziens (la transmission d'image à la télévision), les radio-communications avec les mobiles, les techniques d'enregistrement. Les problèmes rencontrés sont à la base de nature de l'ingénierie, mais très souvent les solutions sont trouvées en utilisant, l'algèbre, la combinatoire, la géométrie finie et quelques fois d'autres branches des mathématiques.
Dans cette thèse, nous allons étudier une construction particulière de codes, et les propriétés qui en découlent.

0.2 Dénombrements dans l'espace projectif $\mathbb{P}^n(\mathbb{F}_q)$

On désigne par $\mathbb{P}^n(\mathbb{F}_q)$ l'espace projectif de dimension n sur le corps fini $\mathbb{F}_q$ à q éléments, où $q = p^a$ est une puissance d'un nombre premier.
Le nombre de points de $\mathbb{P}^n(\mathbb{F}_q)$ est:

$$\pi_n = \#\mathbb{P}^n(\mathbb{F}_q) = \#\Pi_n = q^n + q^{n-1} + ... + 1.$$

On note Π_r un sous-epace projectif linéaire de dimension r et $\Phi(r, n, q)$ le nombre de sous-espaces projectifs linéaires Π_r contenus dans $\mathbb{P}^n(\mathbb{F}_q)$. On a alors:

$$\Phi(r, n, q) = \prod_{i=n-r+1}^{n+1} (q^i - 1) / \prod_{i=1}^{r+1} (q^i - 1).$$

Soit $s \leq r$ et $\mathcal{X}(s, r; n, q)$ le nombre de sous-espaces projectifs Π_r passant par un Π_s fixé. Par le principe de dualité dans l'espace projectif, on montre que:

$$\mathcal{X}(s, r; n, q) = \Phi(n - r - 1, n - s - 1, q).$$

Soit W_i l'ensemble des points de cordonnées homogènes $(x_0 : ... : x_n) \in \mathbb{P}^n(\mathbb{F}_q)$ tel que $x_j = 0$ pour $j < i$ et $x_i \neq 0$. La famille $\{W_i\}_{0 \leq i \leq n}$ forme une partition de $\mathbb{P}^n(\mathbb{F}_q)$.
Soit $P = (x_0 : x_1 : ... : x_n) \in \mathbb{P}^n(\mathbb{F}_q)$ et $f(x_0, ..., x_n)$ un polynôme homogène en $n+1$ variables à coefficients dans $\mathbb{F}_q$ et de degré d. On a

$$f(P) = \frac{f(x_0, ..., x_n)}{{x_i}^d} \text{ avec } x = (x_0 : ... : x_n) \in W_i.$$

En 1989, aux 16 ième Journées Arithmétiques qui ont eu lieu à Marseille Luminy (17-21 juillet 1989) M. Tsfasman présenta une conjecture sur la meilleure borne pour le nombre de points d'une hypersurface dans $\mathbb{P}^n(\mathbb{F}_q)$. Elle fut résolue d'abord par J. P. Serre dans une lettre adressée à Tsfasman le 24 juillet 1989 ensuite par A. B. Sørensen un trimestre plus tard en utilisant une technique différente qui est en faite "duale" de celle de Serre.

Théorème 0.1. *(Tsfasman-Serre-Sørensen)([34, p.351], [36, chp.2, pp.7-10]) Soit $f(x_0, ..., x_n)$ un polynôme homogène en $n+1$ variables à coefficients dans $\mathbb{F}_q$ et de degré $d \leq q$. Alors le nombre de zéros de f dans $\mathbb{P}^n(\mathbb{F}_q)$ satisfait:*

$$\#Z_{(f)}(\mathbb{F}_q) \leq dq^{n-1} + \pi_{n-2}.$$

Cette borne supérieure est atteinte quand $Z_{(f)}$ est réunion de d hyperplans contenant une même variété linéaire de codimension 2.

Définition 0.1. *Soit $\mathcal{V}$ une variété projective, la dimension maximale $g(\mathcal{V})$ des sous espaces projectifs linéaires contenus dans $\mathcal{V}$, est appélée l'**indice projectif** de $\mathcal{V}$.*

Nous allons maintenant nous restreindre à l'espace projectif $\mathbb{P}^3(\mathbb{F}_q)$ et définir la notion de regulus qui se généralise dans tout espace projectif $\mathbb{P}^n(\mathbb{F}_q)$ de dimension impaire.

Lemme 0.1. *Dans $\mathbb{P}^3(\mathbb{F}_q)$ le nombre de droites rencontrant trois droites non concourantes deux à deux est $q+1$.*

On montre aussi que ces $q+1$ droites sont non concourantes deux à deux.

Définition 0.2. *L'ensemble des droites rencontrant trois droites non concourantes (deux à deux) est appelé un **regulus**. Ainsi donc, un regulus est constitué de $q+1$ droites non concourantes, et si l_1, l_2 et l_3 sont trois d'entre elles, le regulus est noté $\mathcal{R}(l_1, l_2, l_3)$.*

On montre également que les droites rencontrant l_1, l_2 et l_3 rencontrent toute droite de $\mathcal{R}(l_1, l_2, l_3)$ et forment un regulus appelé le regulus complémentaire.

0.3 Introduction du code fonctionnel

Soit X un ensemble fini, $X = \{P_1, \ldots, P_n\}$ et $\mathcal{F}(X, \mathbb{F}_q)$ l'espace vectoriel des applications définies sur X et à valeurs dans $\mathbb{F}_q$. Soit $\widetilde{F} \subset \mathcal{F}(X, \mathbb{F}_q)$ un sous-ensemble .
On définit l'application

$$\begin{aligned} c : \mathcal{F}(X, \mathbb{F}_q) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto c(f) = (f(P_1), \ldots, f(P_n)) \end{aligned}$$

Le code fonctionnel défini par $\widetilde{F}$ et X, et denoté $C(X, \widetilde{F})$ est l'image de l'application c restreinte à $\widetilde{F}$.

$$C(X, \widetilde{F}) = \mathrm{Im} c_{|\widetilde{F}}$$

Nous avons le résultat suivant:

Proposition 0.1. *Le code $C(X, \widetilde{F})$ a les paramètres suivants:*

$$\text{lengh}C(X, \widetilde{F}) = n, \qquad \dim C(X, \widetilde{F}) = \dim \widetilde{F} - \dim \ker C_{|\widetilde{F}}$$

$$\text{dist}C(X, \widetilde{F}) = n - \max_{\text{f}\in\widetilde{\text{F}}} cw(f).$$

Il est évident que pour avoir des codes avec un nombre relativement grand de mots de code, l'injectivité de l'application c s'impose.

Nous travaillerons plus particulièrement dans cette thèse, le cas où $X \subset \mathbb{P}^N(\mathbb{F}_q)$ est un ensemble algébrique et $\widetilde{F}$ est l'espace des formes de degré h sur X que nous notons $\mathcal{F}_h$. On note alors $C_h(X)$ le code $C(X, \widetilde{F})$. Dans ce cas particulier, on a :

$$\text{dist}C_h(X) = \#X(\mathbb{F}_q) - \max_{\text{f}\in\mathcal{F}_\text{h}} \#X_{Z(f)}(\mathbb{F}_q).$$

D'après cette formule, la distance minimale de $C_h(X)$ est determinée par le nombre de points $\#X_{Z(f)}(\mathbb{F}_q)$ de l'intersection de X avec les hypersurfaces f de degré h. Sous la condition de l'injectivité de l'application c, on obtient par des résultats d'analyse combinatoire que:

$$\dim C_h(X) = \binom{N+h}{h}.$$

Dans les chapitres 1, 2 et 4 (deuxième partie) X aura une structure de variété hermitienne.

0.4 Les variétés hermitiennes et quelques propriétés fondamentales

Les variétés hermitiennes sont définies dans des espaces projectifs sur des corps de Galois de la forme $\mathbb{F}_q$ où $q = t^2$ et t est une puissance d'un nombre premier.

Définition 0.3. *Soit $h \in \mathbb{F}_{t^2}$. On appelle **conjugué** de h et on note $\overline{h} = h^t$.*

Définition 0.4. *Soit $H = (h_{ij})_{0\leq i,j\leq N}$ une matrice carrée avec les $h_{ij} \in \mathbb{F}_{t^2}$. La matrice H est dite **hermitienne** si et seulement si $h_{ij} = \overline{h_{ji}}$ pour tout $0 \leq i, j \leq N$.*
Soit $x^T = (x_0, \ldots, x_N)$ un vecteur ligne et soit x le vecteur colonne correspondant où $x_0, x_1, \ldots, x_N$ sont des indeterminées, $x^T H x^{(t)}$ est un polynôme homogène en les variables $x_0, x_1, \ldots, x_N$ de degré $t + 1$.
*La forme $x^T H x^{(t)}$ est appelée une **forme hermitienne** si H est une matrice hermitienne et H est appelée la matrice de la forme. L'ordre et le rang d'une forme hermitienne sont définis comme étant l'ordre et le rang de H.*

Définition 0.5. *Soit $\tilde{\mathcal{X}}$ un ensemble de points dans $\mathbb{P}^N(\mathbb{F}_{t^2})$ dont les vecteurs lignes $x^T = (x_0, \ldots, x_N)$ satisfont l'équation: $x^T H x^{(t)} = 0$. On dit alors que $\tilde{\mathcal{X}}$ est une **variété hermitienne** ssi H est une matrice hermitienne. Elle est non-dégénérée si le rang de H est $N + 1$ et dégénérée dans le cas contraire (i.e. rang($\tilde{\mathcal{X}}$) $< N + 1$).*

R.C. Bose et I.M. Chakravarti ont donné en 1966 pour la première fois une formule permettant de déterminer exactement le nombre de points d'une variété hermitienne non-dégénérée. Ils déduisent de cette formule, le nombre de points d'une variété hermitienne dégénérée de rang r.

Théorème 0.2. *Soit $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ une variété hermitienne non-dégénérée. Alors,*

$$\#\tilde{\mathcal{X}}(\mathbb{F}_q) = \Upsilon(n, t^2) = [t^{n+1} - (-1)^{n+1}][t^n - (-1)^n]/(t^2 - 1) \tag{1}$$

Pour $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ une variété hermitienne dégénérée de rang $r < n+1$, nous avons:

$$\#\tilde{\mathcal{X}}(\mathbb{F}_q) = (t^2 - 1)\pi_{n-r}\Upsilon(r-1, t^2) + \pi_{n-r} + \Upsilon(r-1, t^2),$$

où $\Upsilon(n, t^2)$ est donnée par (1).

Ils ont aussi étudié la section d'une variété hermitienne non-dégénérée par un hyperplan tangent. Ils obtiennent le résultat suivant:

Théorème 0.3. *[6, p.1173] Soit $\tilde{\mathcal{X}}$ une variété hermitienne non-dégénérée dans $\mathbb{P}^n(\mathbb{F}_q)$ et H un hyperplan. Si H est tangent à $\tilde{\mathcal{X}}$ en P, alors $\tilde{\mathcal{X}} \cap H$ est une variété hermitienne dégénérée de rang $n-1$ dans $\mathbb{P}^{n-1}(\mathbb{F}_q)$. Le lieu singulier de $\tilde{\mathcal{X}} \cap H$ est constitué uniquement du point P.*

En 1971, I.M. Chakravarti achève tout seul l'étude de la section hyperplane d'une variété hermitienne non-dégénérée. Il obtient le résultat suivant:

Théorème 0.4. *[7, p.272] Soit $\tilde{\mathcal{X}}$ une variété hermitienne non-dégénérée dans $\mathbb{P}^n(\mathbb{F}_q)$ et H un hyperplan. Si H est non-tangent à $\tilde{\mathcal{X}}$, alors $\tilde{\mathcal{X}} \cap H$ est une variété hermitienne non-dégénérée dans $\mathbb{P}^{n-1}(\mathbb{F}_q)$.*

Dans leur article de 1966, Bose et Chakravarti ont également établi des propriétés sur des variétés hermitiennes dégénérées. Deux d'entre elles retiendront notre attention et auront une importance capitale dans la dernière partie du chapitre 4.

Théorème 0.5. *[6, p.1171] Soit $\tilde{\mathcal{X}}$ une variété hermitienne dégénérée de rang $r < n+1$ dans $\mathbb{P}^n(\mathbb{F}_q)$ et Π_{r-1} un sous-espace projectif linéaire de dimension $r-1$ disjoint du lieu singulier Π_{n-r} de $\tilde{\mathcal{X}}$. Alors $\Pi_{r-1} \cap \tilde{\mathcal{X}}$ est une variété hermitienne non-dégénérée dans Π_{r-1}.*

Théorème 0.6. *[6, p.1171] Soit $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ une variété hermitienne dégénérée de rang $r < n+1$. Si P est un point appartenant à l'espace singulier Π_{n-1} de $\tilde{\mathcal{X}}$ et D est un point arbitraire de $\tilde{\mathcal{X}}$, alors tout point de la droite (PD) appartient à $\tilde{\mathcal{X}}$.*

0.5 Le code $C_h(X)$ défini sur la surface hermitienne non-dégénérée

Ici $q = t^2$ et X est la surface hermitienne dans $\mathbb{P}^3(\mathbb{F}_q)$ non-dégénérée d'équation $X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$. D'après le théorème 0.2, on obtient $\#X(\mathbb{F}_q) = (t^2+1)(t^3+1)$.

Injectivité: L'injectivité de l'application c définissant le code $C_h(X)$ est vérifiée sous la

condition $h \leq t$. Et cette condition est elle-même obtenue grâce à la borne de Tsfasman-Serre-Sørensen pour les hypersurfaces.

Historique du code $C_h(X)$ sur la surface hermitienne:
En 1985, pour $h = 2$ et $t = 2$, R. Tobias un étudiant en thèse de I.M. Chakravarti à l'UNC-CH a étudié ce problème. Par un traitement à l'ordinateur, il donna d'abord la liste des 45 points de X. Il a ensuite évalué les 10 monônes quadratiques en chacun des 45 points de X, ce qui lui a permis de determiner la dimension de ce code. Il ne fut pas à mesure de déterminer la distance minimale de $C_2(X)$.
En 1986, pour $h = 2$ et $t = 2$, Paul P. Spurr dans sa thèse de master [38, p.28] à l'UNC-CH en Caroline du Nord sous la direction de Ladnor Geissinger détermina grâce à un programme informatique, non seulement la distance minimale mais aussi la distribution des poids du code $C_2(X)$. Tous les mots du code $C_2(X)$ sont de poids pairs. Il obtint d'ailleurs le prix du meilleur mémoire de master en sciences de son université.
En 1991, pour $h = 2$ et $t = 2$, A. B. Sørensen dans sa thèse de doctorat [36, pp.8-9] sous la direction du professeur J. P. Hansen à Aarhus, montra que l'utilisation d'un ordinateur n'était pas vraiment nécessaire pour déterminer la distance minimale de $C_2(X)$. Il a même décrit la structure géométrique des mots de poids minimaux et en a déduit leur nombre. Sørensen a généralisé son étude à la variété hermitienne non-dégénérée d'équation $X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$ et a formulé une conjecture

$$\text{pour} \quad h \leq t, \quad \#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1$$

qui une fois résolue, devrait donner exactement la distance minimale de $C_h(X)$.
En 1993, au colloque A.G.C.T-4 de Marseille-Luminy, G. Lachaud donna une borne supérieure du nombre de points d'un ensemble algébrique de dimension et de degré donnés. Le résultat de G. Lachaud appliqué aux hypothèses du problème ci-dessus, conduit à la borne suivante:

$$\text{pour} \quad h \leq t, \quad \#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 + t + 1)$$

qui est malheureusement plus large que celle de Sørensen.
En 2003, F. Rodier étudia également le code $C_h(X)$ défini sur la surface hermitienne non-dégénérée. Mais il n'apporta ni une amélioration à la borne de G. Lachaud, ni une information à la conjecture ci-dessus.

Résolution de la conjecture de Sørensen: On remarque que pour $h = 1$, la conjecture est vraie. Il suffit pour cela d'appliquer les théorèmes 0.3,0.4 et 0.2 pour s'en convaincre. Dans le cadre de cette thèse nous avons résolu dans le chapitre 1, la conjecture de Sørensen pour $h = 2$, en utilisant la classification projective des quadriques dans $\mathbb{P}^3(\mathbb{F}_q)$ et aussi les propriétés des variétés hermitiennes. De plus, les techniques développées à savoir:

- La structure de deux reguli, chacun engendrant la quadrique hyperbolique et la limite imposée au nombre de droites non-concourantes contenues dans un regulus pouvant appartenir à la surface hermitienne non-singulière,
- La section de la quadrique elliptique $\mathcal{E}_3$ par X, dans $\mathbb{P}^3(\mathbb{F}_q)$ vu comme une famille de $q + 1$ plans passant par une même droite définie par deux points distincts de $\mathcal{E}_3 \cap X$,

- La structure géométrique du cône quadrique de rang 3 qui est en fait une réunion de $q+1$ droites passant par un sommet et la limite imposée au nombre de droites du cône quadrique pouvant être contenues dans X,

nous permettent non seulement de répondre positivement à la conjecture ci-dessus pour les quadriques, mais aussi de préciser le premier, le second et le troisième poids, ainsi que la description géométrique des quadriques donnant ces poids et finalement le nombre des mots atteignant ces trois premiers poids. En clair, nous obtenons les résultats suivants:

Caractérisation du premier poids w_1 et sa multiplicité A_{w_1}

Théorème 0.7. *[12, pp.626-627] La distance minimale du code $C_2(X)$ est: $d = t^5 - t^3 - t^2 + t$. Les mots de poids minimaux correspondent aux quadriques qui sont réunion de plans, chacun tangent à la surface hermitienne (i.e. intersectant la surface hermitienne en $t+1$ droites passant par un point), et la droite d'intersection des deux plans intersectant X en $t+1$ points. Le nombre de mots de poids minimaux est:*

$$A_{w_1} = (t^2-1)[\frac{1}{2}(t^5+t^3+t^2+1)t^5].$$

Caractérisation du second poids w_2 et sa multiplicité A_{w_2}

Théorème 0.8. *[12, p.627 et 14, pp.4-5] Le second poids du code $C_2(X)$ est $w_2 = t^5 - t^3$. Les mots de code atteignant le second poids correspondent à trois types de quadriques:*
–quadriques hyperboliques contenant trois droites non-concourantes de X,
–quadriques qui sont réunion de deux plans tangents à la surface hermitienne X, se rencontrant en une droite contenue dans X,
–quadriques qui sont réunion de deux plans l'un tangent à X, le second non-tangent à X et la droite d'intersection des deux plans rencontrant X en un seul point.
Le nombre de mots atteignant le second poids est:

$$A_{w_2} = \frac{1}{2}(t^2-1)(t^5+t^3+t^2+1)(3t^2-t+1)t^2.$$

Caractérisation du troisième poids w_3 et sa multipicité A_{w_3}

Théorème 0.9. *[14, pp.8-9] Le troisième poids du code $C_2(X)$ est $w_3 = t^5 - t^3 + t$. Les mots de code atteignant le troisième poids correspondent aux quadriques qui sont réunion de deux plans l'un tangent à X, le second non-tangent à X et la droite d'intersection des deux plans intersectant la surface hermitienne X en $t+1$ points.*
Le nombre de mots atteignant le troisième poids est:

$$A_{w_3} = (t^2-1)(t^5+t^3+t^2+1)(t^6-t^5).$$

On remarque que pour $h=2$ et $t=2$, on retrouve les résultats de Sørensen et ceux de Spurr calculés par ordinateur: $w_1 = 22, A_{w_1} = 2160$; $w_2 = 24, A_{w_2} = 2970$; $w_3 = 26, A_{w_3} = 4320$.

Nous explicitons les quatrième et cinquième poids du code $C_2(\mathcal{X})$, et formulons une conjecture sur la structure géométrique des quadriques qui correspondent à ces poids.
Le mardi 27 février 2007, dans mon exposé au séminaire du G.R.I.M (Groupe de Recherche en Informatique et Mathématiques) de l'U.S.T.V à Toulon, Philippe Langevin (directeur du dit groupe) me fit remarquer que les cinq premiers poids du code $C_2(\mathcal{X})$ étaient divisibles par t et que cela pourrait peut être s'étendre à tous les autres poids (ce qui est d'ailleurs le cas pour $t = 2$). Nous allons prouver que cette remarque est bien fondée grâce au théorème de James Ax sur les zéros des polynômes à coefficients dans un corps fini.

Théorème 0.10. *[3, p.260] Soient r polynômes $F_i(x_1, ..., x_n)$ $(i = 1, ..., r)$ à n variables de degré d_i sur $\mathbb{F}_q$, alors le nombre de zéros communs des F_i est divisible par q^b si $n > b\sum_{i=1}^{r} d_i$.*

Théorème 0.11. *Tous les poids du code $C_2(\mathcal{X})$ défini sur la surface hermitienne non-dégénérée X sont divisibles par t.*

Preuve: Nous allons donner une démonstration plus générale dans $\mathbb{P}^n(\mathbb{F}_q)$.
Si ϕ est une forme hermitienne à $n+1$ variables avec $n \geq 3$ sur un corps $\mathbb{F}_q = \mathbb{F}_{t^2}$ et F une forme quadratique, on a

$$\phi(x_0, ..., x_n) = x_0^{t+1} + ... + x_n^{t+1}$$

Notons α un élément de $\mathbb{F}_q$ qui n'est pas dans $\mathbb{F}_t$. On a

$$\mathbb{F}_q = \mathbb{F}_t \oplus \alpha\mathbb{F}_t.$$

Décomposons les éléments x de $\mathbb{F}_q$

$$x = y + \alpha z.$$

La conjugaison est donnée par $x \longmapsto x^t$ et transforme α en $\overline{\alpha}$. Par conséquent $x^t = y + \overline{\alpha}z$, et par suite

$$x^{t+1} = (y + \alpha z)(y + \overline{\alpha}z) = y^2 + (\alpha + \overline{\alpha})yz + \alpha\overline{\alpha}z^2.$$

La forme ϕ est maintenant une forme de degré 2 en $2(n+1)$ variables. Et sa nouvelle équation devient

$$\phi(y_0, z_0, ..., y_n, z_n) = y_0^2 + (\alpha + \overline{\alpha})y_0z_0 + \alpha\overline{\alpha}z_0^2 + ... + y_n^2 + (\alpha + \overline{\alpha})y_nz_n + \alpha\overline{\alpha}z_n^2$$

Soient X et $\mathcal{Q}$ les variétés projectives associées aux formes ϕ et F. Les nouvelles équations donnant $X \cap \mathcal{Q}$ s'écrivent alors

$$\begin{cases} y_0^2 + (\alpha + \overline{\alpha})y_0z_0 + \alpha\overline{\alpha}z_0^2 + ... + y_n^2 + (\alpha + \overline{\alpha})y_nz_n + \alpha\overline{\alpha}z_n^2 = 0 \\ F(y_0, z_0, ..., y_n, z_n) = 0 \end{cases}$$

et sont des équations sur $\mathbb{F}_t$. Par le théorème d'Ax, le nombre de zéros communs N à ϕ et F (dans $\mathbb{F}_t^{2(n+1)}$) est divisible par t car $2(n+1) > 2+2$.
D'autre part F et ϕ sont homogènes, donc $N-1$ est divisible par $t-1$.
Etant donné que X et $\mathcal{Q}$ sont les variétés projectives associées aux formes ϕ et F, on a $\#(\mathcal{Q} \cap X) = \frac{N-1}{t-1}$. Soit $M = \frac{N-1}{t-1}$, on a $N \equiv (1 - M) \pmod{t}$. Et comme N est divisible par

t, on en déduit $M \equiv 1 \pmod{t}$
Le poids d'un mot de code associé à la variété quadrique $\mathcal{Q}$ sur X est égal à

$$w = \#X - \#(\mathcal{Q} \cap X) = \#X - M.$$

Or, par le théorème d' Ax encore, le nombre de zéros de ϕ (dans $\mathbb{F}_t^{2(n+1)}$) est divisible par t, donc $\#X \equiv 1 \pmod{t}$. Par conséquent,

$$w = \#X - M \equiv 0 (\text{mod. } t).$$

0.6 Etude du code $C_2(X)$ défini pour X une surface quadrique

Le code $C_2(X)$ défini sur X une variété quadrique de $\mathbb{P}^n(\mathbb{F}_q)$ a été étudié pour la première fois par Y. Aubry en 1993. Dans le but de déterminer la distance minimale, Aubry étudia l'intersection de deux quadriques dans $\mathbb{P}^n(\mathbb{F}_q)$.
Lorsque X est une quadrique qui est une réunion d'hyperplans ou un hyperplan répété, la détermination de $C_2(X)$ se ramène à l'étude de sections hyperplanes de quadriques. Ce problème a été étudié en plusieurs étapes, selon la dégénérescence de la quadrique.
En 1951, Primrose dans les presses de l'université de Cambridge étudia la section hyperplane d'une quadrique non-dégénérée. Dans le cas où l'hyperplan n'est pas tangent à X, son résultat affirme qu'on obtient une quadrique non-dégénérée dans $\mathbb{P}^{n-1}(\mathbb{F}_q)$, et une quadrique dégénérée de rang maximal dans $\mathbb{P}^{n-1}(\mathbb{F}_q)$ lorsque l'hyperplan est tangent à X. En 1975, J. Wolfmann achève l'étude de ce dernier cas, ce qui rend complète l'étude de la section hyperplane d'une quadrique non-dégénérée.
En ce qui concerne les quadriques dégénérées, il y a eu plusieurs approches:
–En 1986, R. Games a étudié les sections hyperplanes de quadriques dégénérées ayant la taille d'un hyperplan sans pour autant être des hyperplans.
–En 1990, I.M. Chakravarti étudia les sections hyperplanes de quadriques dégénérées de rang maximal.
–En 1993, la troisième et dernière approche est donnée par Y. Aubry. Il obtient des résultats très remarquables dans sa Thèse de Doctorat: il donne des résultats dans le cas général, i.e. pour des quadriques de rang quelconque. Il a retrouvé des résultats oubliés de H.P.F Swinnerton-Dyer de 1964. Lorsque j'ai présenté l'article de H.P.F. Swinnerton-Dyer à Y. Aubry le mercredi 18 janvier 2006, en discutant avec lui il m'expliqua qu'il ignorait l'existence de tels résultats. Autrement, des tentatives comme celles de Games et Chakravarti n'auraient pas eu lieu.
Lorsque les deux quadriques X et $\mathcal{Q}$ n'ont aucun facteur linéaire (hyperplan) en commun, Y. Aubry en considérant le résultant des deux polynômes définissant les quadriques et en appliquant la borne de Tsfasman-Serre-Sørensen pour les hypersufaces, donna une majoration de $\#(X \cap \mathcal{Q})$, le nombre de points dans l'intersection des deux quadriques X et $\mathcal{Q}$. Il obtint:

$$\#(X \cap \mathcal{Q}) \leq \pi_{n-2} + 7\frac{q^{n-1}}{q-1} - 6\frac{q^{n-2}}{q-1} \quad (q \geq 7).$$

En 1999, il y a eu une avancée dans la majoration du nombre de points dans l'intersection de deux quadriques. Cette avancée est venue de D. B. Leep et de son étudiante L. M. Schueller.

Ils ont amélioré les résultats d'Aubry sous l'hypothèse que les deux quadriques sont de "plein ordre", c'est à dire leur écriture simultanée nécessiterait la totalité des variables $x_0, \ldots, x_n$. On a le résultat suivant:

Théorème 0.12. *Soient $\mathcal{Q}_1$ et $\mathcal{Q}_2$ deux quadriques dans $\mathbb{P}^n(\mathbb{F}_q)$. Supposons que $w(\mathcal{Q}_1, \mathcal{Q}_2) = n+1$.*
Si $n+1 \geq 4$ et $n+1$ pair, alors

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq (2q^{n-1} - q^{n-2} + 2q^{\frac{n+1}{2}} - 3q^{\frac{n-1}{2}} + q^{\frac{n-3}{2}} - 1)/(q-1).$$

Si $n+1 \geq 5$ et $n+1$ impair, alors

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq (2q^{n-1} - q^{n-2} + q^{\frac{n+2}{2}} - q^{\frac{n}{2}} - 1)/(q-1).$$

Si $n+1 = 3$, alors

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq (q^2 + q - 2)/(q-1)$$

Et ces bornes sont les meilleures possibles.

L'hypothèse de D. B. Leep et L.M. Schueller est très restrictive. Nous donnons dans cette thèse un résultat similaire à la borne de Tsfasman-Serre-Sørensen tout en s'affranchissant de cette hypothèse, c'est à dire pour des paires de quadriques ayant un ordre quelconque.

Lemme 0.2. *[15, pp.5-6] Soient $\mathcal{Q}_1$ et $\mathcal{Q}_2$ deux quadriques dans $\mathbb{P}^n(\mathbb{F}_q)$ et l un entier tel que $1 \leq l \leq n-1$.*
Supposons que $w(\mathcal{Q}_1, \mathcal{Q}_2) = n - l + 1$ et $|\mathcal{Q}_1 \cap \mathcal{Q}_2 \cap \mathbb{E}_{n-l}(\mathbb{F}_q)| \leq m$ où $\mathbb{E}_{n-l}(\mathbb{F}_q) = \{x \in \mathbb{P}^n(\mathbb{F}_q) \ | x_{n-l+1} = ... = x_n = 0\}$. Alors

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq mq^l + \pi_{l-1}.$$

Cette borne est optimale dès que m l'est dans $\mathbb{E}_{n-l}(\mathbb{F}_q)$.

Rien que dans le cas de $\mathbb{P}^3(\mathbb{F}_q)$, qui est apparemment simple, quand X est une quadrique non-dégénérée (elliptique ou hyperbolique), ou dégénérée de rang maximal Aubry n'était pas en mesure de déterminer précisément la distance minimale de $C_2(X)$. Ses résultats conduisent à la borne:

$$|\mathcal{Q} \cap X| \leq 2(4q+1) + \frac{1}{q-1}$$

qui n'est d'ailleurs pas la meilleure possible.
L'amélioration faite par Leep et Schueller donne une borne certes interessante pour la distance minimale de $C_2(X)$ définie sur X, une quadrique non-dégénérée hyperbolique, cependant trop large lorsque X est une quadrique non-dégénérée elliptique.

0.6.1 X est une quadrique hyperbolique dans $\mathbb{P}^3(\mathbb{F}_q)$

Ici la borne de Leep stipule que le nombre de points dans l'intersection d'une quadrique hyperbolique X et toute autre quadrique différente de X, est plus petite que $4q$. En réalité il ne donne pas de façon explicite un exemple où celle-ci est optimale. En exploitant de façon particulière la structure géométrique de la quadrique hyperbolique, et aussi celle du cône quadrique de rang 3, nous obtenons les résultats suivants:

Proposition 0.2. *Soit $\mathcal{Q}'$ une quadrique dans $\mathbb{P}^3(\mathbb{F}_q)$ et X une quadrique hyperbolique. On a:*

$$\#X_{Z(\mathcal{Q}')}(\mathbb{F}_q) = 4q, 3q+1 \quad \text{or} \quad \#X_{Z(\mathcal{Q}')}(\mathbb{F}_q) \leq 3q$$

Théorème 0.13. *Le code $C_2(X)$ défini sur la quadrique hyperbolique X est un $[n,k,d]_q$- code avec:*

$$n = (q+1)^2, \quad k = 9, \quad d = (q-1)^2$$

Théorème 0.14. *Les mots de poids minimaux correspondent à deux types de quadriques:*
– les quadriques qui sont réunion de deux plans tangents à X et la droite d'intersection des deux plans intersecte la quadrique hyperbolique en deux points.
– les quadriques hyperboliques contenant exactement quatre droites de X reparties deux à deux dans chacun des deux reguli de X.

Théorème 0.15. *Le second et le troisième poids du code $C_2(X)$ défini sur la quadrique hyperbolique sont respectivement $w_2 = q(q-1)$, $w_3 = q^2 - q + 1$.*

Théorème 0.16. *Les mots du second poids correspondent à trois types de quadriques:*
– les quadriques qui sont réunion de deux plans tangents à X et la droite d'intersection des deux plans est un générateur X,
– les quadriques qui sont réunion de deux plans, l'un tangent à X, le second non-tangent à X, et la droite d'intersection des deux plans intersectant X en un seul point,
– les quadriques hyperboliques contenant exactement deux générateurs de X un dans chaque regulus et les q autres droites d'un regulus sont toutes des bisecantes à X.

0.6.2 X est une quadrique elliptique dans $\mathbb{P}^3(\mathbb{F}_q)$

Des intersections des quadriques de $\mathbb{P}^3(\mathbb{F}_q)$ avec la quadrique elliptique, l'intersection elliptique-elliptique est la plus complexe, en ce sens que nous avons à nous détacher de toutes les approches ayant servi précédemment et l'aborder avec une approche plus géométrique.
Ici plutôt que de regarder $\mathcal{Q}$ et $\mathcal{X}$ sur $\mathbb{F}_q$, nous regardons $\overline{\mathcal{Q}}$ et $\overline{\mathcal{X}}$ sur $\overline{\mathbb{F}_q}$. Nous considérons également $\mathcal{C} = \overline{\mathcal{Q}} \cap \overline{\mathcal{X}}$ qui définit une courbe que nous décomposons en composantes irréductibles $\mathcal{C} = \bigcup_{1 \leq i \leq t} \overline{\mathcal{C}}_i$. D'après la caractérisation d'une quadrique non-singulière donnée par I. Shafarevitch, à savoir que $\overline{\mathcal{Q}} \simeq \mathbb{P}^1(\overline{\mathbb{F}_q}) \times \mathbb{P}^1(\overline{\mathbb{F}_q})$ via le plongement de Segre, nous donnons une relation plus raffinée entre le genre arithmétique et le degré des courbes $\overline{\mathcal{C}}_i$.

Lemme 0.3. *[13, p.61] Soit $\mathcal{Q} \subset \mathbb{P}^3$ une surface quadrique non-singulière dans $\mathbb{P}^3$ et $\overline{C}_i$ une courbe irréductible sur $\overline{\mathcal{Q}}$.*
–Si deg $\overline{C}_i = 2l+2$ alors, $p_a(\overline{C}_i) \leq l^2$ $(\star)$
–Si deg $\overline{C}_i = 2l+1$ alors, $p_a(\overline{C}_i) \leq l(l-1)$ $(\star\star)$

En faisant agir le groupe de Galois $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ sur les composantes irréductibles , on arrive au résultat suivant:

Lemme 0.4. *Soit $\overline{\mathcal{C}} = \bigcup_{1 \leq i \leq t} \overline{C}_i$ la décomposition d'une courbe $\mathcal{C} \subset \mathbb{P}^n(\overline{\mathbb{F}}_q)$ en composantes irréductibles sur $\overline{\mathbb{F}}_q$ et $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Alors $\sigma(\overline{C}_i)$ et $\overline{C}_i$ ont le même degré. Si $\overline{C}_i$ est la seule composante de degré d_i, alors $\overline{C}_i$ est définie sur $\mathbb{F}_q$.*

En utilisant la borne de Weil et les améliorations qu'en ont faites Yves Aubry et Marc Perret pour le cas des courbes non-lisses, ainsi que les lemmes 0.3, 0.4 on obtient $|\mathcal{X} \cap \mathcal{Q}| \leq 2(q+1)$

Proposition 0.3. *Soit $\mathcal{Q}'$ une quadrique dans $\mathbb{P}^3(\mathbb{F}_q)$ et X une quadrique elliptique. Nous avons:*

$$\#X_{Z(\mathcal{Q}')}(\mathbb{F}_q) = 2(q+1), 2q+1 \quad \text{ou} \quad \#X_{Z(\mathcal{Q}')}(\mathbb{F}_q) \leq 2q$$

Théorème 0.17. *Le code $C_2(X)$ défini sur la quadrique elliptique X est un $[n,k,d]_q$- code avec:*

$$n = q^2+1, \quad k = 9, \quad d = q^2 - 2q - 1.$$

Remarque 0.1. *Ces codes fonctionnels $C_2(X)$ définis sur les quadriques elliptiques sont de bons codes selon les tables de Andries E. Brouwer* [4].

En fait pour, $q = 3, 4, 5, 7, 8, 9$ nous obtenons respectivement les codes suivants: $[10, 9, 2]_3$- code, $[17, 9, 7]_4$- code, $[26, 9, 14]_5$- code, $[50, 9, 34]_7$- code, $[65, 9, 47]_8$- code, $[82, 9, 62]_9$- code.

0.6.3 X est une quadrique dégénérée de rang 3 dans $\mathbb{P}^3(\mathbb{F}_q)$

Pour X une quadrique dégénérée de rang maximal, l'hypothèse de Leep pour la détermination du nombre de points de deux quadriques ne peut s'appliquer en ce sens qu'elle ne prendrait en compte aucune paire de quadriques dégénérées de rang maximal et d'ordre 3.
Par les trois considérations suivantes:

- En mettant à profit la structure géométrique du cône quadrique de rang 3,
- En déterminant le nombre de droites pouvant être contenues dans l'intersection du cône avec toute autre quadrique, autre que celle engendrée par deux plans
- En étudiant la section plane du cône par des quadriques qui sont réunion de deux plans et la description très précise de la droite d'intersection de ces deux plans vis à vis du cône,

nous obtenons les résultats suivants:

Proposition 0.4. *Soit $\mathcal{Q}'$ une quadrique dans $\mathbb{P}^3(\mathbb{F}_q)$ et X le cône quadrique de rang 3. Nous avons:*

$$\#X_{Z(\mathcal{Q}')}(\mathbb{F}_q) = 4q+1, 3q+1 \quad \text{ou} \quad \#X_{Z(\mathcal{Q}')}(\mathbb{F}_q) \leq 3q$$

Théorème 0.18. *Le code $C_2(X)$ défini sur le cône quadrique de rang 3 X est un $[n,k,d]_q$- code avec:*

$$n = q^2+q+1, \quad k = 9, \quad d = q(q-3)$$

Nous donnons aussi une description du premier, deuxième et du troisième poids de $C_2(X)$, ainsi que la description des mots atteignant ces poids respectifs.

0.7 Le code $C_2(X)$ défini sur les variétés quadriques dans $\mathbb{P}^4(\mathbb{F}_q)$

Cette partie est en fait, la première partie du chapitre 4 de cette thèse. Nous allons nous servir des résultats obtenus pour les surfaces quadriques dans $\mathbb{P}^3(\mathbb{F}_q)$ et aussi du lemme 0.2.
Lorsque $\mathcal{X}$ est une quadrique d'indice projectif g($\mathcal{X}$)=3, la détermination de la distance minimale de $C_2(X)$ découle directement des résultats de Swinnerton-Dyer, Primrose, Wolfmann pour le cas r($\mathcal{Q}$)=1, et de Boguslavsky pour le cas r($\mathcal{Q}$)=2.
De même pour g($\mathcal{X}$)=2=r($\mathcal{X}$), on déduit également la distance minimale de $C_2(X)$ des résultats de J.W.P. Hirschfeld.
Pour les quadriques $\mathcal{X}$ de rang r($\mathcal{X}$) ≥ 3, nous jouerons principalement sur leur structure géométrique combinée avec certaines considérations particulières pour déterminer la distance minimale de $C_2(X)$ ainsi que le second poids. Nous obtenons les résultats suivants:

Théorème 0.19. *Soit $\mathcal{Q}$ une quadrique dans $\mathbb{P}^4(\mathbb{F}_q)$ et $\mathcal{X}$ une quadrique non-dégénérée (parabolique) dans $\mathbb{P}^4(\mathbb{F}_q)$. Nous avons*

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 2q^2 + 3q + 1$$

et cette borne est la meilleure possible.
Le code $C_2(\mathcal{X})$ défini sur la quadrique parabolique $\mathcal{X}$ est un $[n, k, d]_q$-code où
$n = (q+1)(q^2+1)$, $k = 14$, $d = q^3 - q^2 - 2q$.

Théorème 0.20. *Les mots de poids minimaux du code $C_2(\mathcal{X})$ correspondent aux quadriques suivantes:*
–quadriques qui sont réunion de deux hyperplans non-tangents à X, chacun intersectant $\mathcal{X}$ en une surface quadrique hyperbolique telle que le plan d'intersection des deux hyperplans intersecte $\mathcal{X}$ en une conique plane non-singulière.
–quadriques avec $r(\mathcal{Q}) = 3$ (i.e. $q+1$ plans passant par une droite) et chaque plan contenant exactement deux droites de $\mathcal{X}$.
–quadriques non-dégénérées (i.e. paraboliques) contenant deux droites sécantes de $\mathcal{X}$ définissant un plan contenu dans les $q+1$ hyperplans où un des hyperplans est tangent à $\mathcal{X}$, les q autres sont non-tangents à $\mathcal{X}$ avec une section hyperplane maximale.

Théorème 0.21. *Soit $\mathcal{Q}$ une quadrique dans $\mathbb{P}^4(\mathbb{F}_q)$ et $\mathcal{X}$ une quadrique dégénérée dans $\mathbb{P}^4(\mathbb{F}_q)$. Nous avons:*
–Si $\mathcal{X}$ est dégénérée avec $r(\mathcal{X}) = 3$, alors

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 4q^2 + q + 1 \quad \text{ou} \qquad \#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

–Si $\mathcal{X}$ est dégénérée avec $r(\mathcal{X})$=4 et $g(\mathcal{X}) = 2$, alors

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 4q^2 + 1 \quad \text{ou} \qquad \#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

Théorème 0.22. *Le code $C_2(\mathcal{X})$ défini sur la quadrique dégénérée $\mathcal{X}$ dans $\mathbb{P}^4(\mathbb{F}_q)$ est un $[n, k, d]_q$-code tel que:*
–Si $\mathcal{X}$ est dégénérée avec $r(\mathcal{X})$=3, alors $n = q^3 + q^2 + q + 1$, $k = 14$, $d = q^3 - 3q^2$.
–Si $\mathcal{X}$ est dégénérée avec $r(\mathcal{X})$=4 et $g(\mathcal{X}) = 2$, alors $n = q^3 + 2q^2 + q + 1$, $k = 14$, $d = q^3 - 2q^2 + q$.

On détermine également les mots de poids minimaux du code $C_2(\mathcal{X})$ pour chacune des deux quadriques dégénérées du théorème ci-dessus et on se référera au théorème 4.2 du chapitre 4.

Théorème 0.23. *Soit $\mathcal{Q}$ une quadrique dans $\mathbb{P}^4(\mathbb{F}_q)$ et $\mathcal{X}$ une quadrique dégénérée dans $\mathbb{P}^4(\mathbb{F}_q)$ de rang $(\mathcal{X}) = 4$ et $g(\mathcal{X}) = 1$. Nous avons:*

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

Le code $C_2(\mathcal{X})$ défini sur la quadrique dégénérée $\mathcal{X}$ de rang r($\mathcal{X}$)=4 avec $g(\mathcal{X}) = 1$ est un $[n, k, d]_q$-code où $n = q^3 + q + 1$, $k = 14$, $d \geq q^3 - 3q^2$.

Notons ici que l'application du théorème de James Ax sur les zéros des polynômes à coefficients dans un corps fini permet de conclure à la divisibilité par q des poids du code $C_2(\mathcal{X})$ défini sur une variété quadrique dans $\mathbb{P}^4(\mathbb{F}_q)$.

0.8 Le code $C_2(X)$ défini sur les variétés hermitiennes non-dégénérées dans $\mathbb{P}^4(\mathbb{F}_q)$

Dans cette partie, nous considérons la variété hermitienne non-singulière $\mathcal{X}$ d'équation $\mathcal{X}$: $x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} + x_4^{t+1} = 0$.
D'après le théorème 0.2, on en déduit que

$$\#\mathcal{X}(\mathbb{F}_q) = (t^2 + 1)(t^5 + 1).$$

Bose et Chakravarti ont montré que g($\mathcal{X}$) = 1.
Pour étudier la section quadratique de $\mathcal{X}$, nous considérons trois cas différents, selon que l'indice projectif g($\mathcal{Q}$) est égal à 1, 2, ou 3.
Pour les quadriques $\mathcal{Q}$ telles que g($\mathcal{Q}$)=2, on sait qu'elles sont des réunions de plans et leur intersection avec la variété hermitienne $\mathcal{X}$ ne peut contenir de plans. On en déduit alors que $|\mathcal{X} \cap \mathcal{Q}| \leq t^5 + t^4 + t^3 + 2t^2 + 1$.
Pour les quadriques $\mathcal{Q}$ d'indice projectif g($\mathcal{Q}$)=3, on sait aussi qu'elles sont des quadriques de rang r(Q)=1 ou 2. Pour des quadriques de rang 1, les théorèmes 0.3, 0.4 donnent explicitement le nombre de points dans l'intersection de $\mathcal{X} \cap \mathcal{Q}$. Si r($\mathcal{Q}$) = 2 et $\mathcal{Q}$ est une réunion d'une paire d'hyperplans, on étudie $\mathcal{X} \cap \mathcal{Q}$ selon que les deux hyperplans sont de même nature ou de nature différente, et en utilisant les deux théorèmes (théorème 0.3 et 0.4) sur la section hyperplane d'une variété hermitienne non-dégénérée et aussi les théorèmes 0.5, 0.6, on trouve exactement les cinq valeurs prises par $|\mathcal{X} \cap \mathcal{Q}|$.
Pour les quadriques $\mathcal{Q}$ d'indice projectif g($\mathcal{Q}$)=1, $\mathcal{Q}$ est soit la quadrique non-dégénérée (i.e. parabolique), ou la quadrique dégénérée de rang 4 de type ellitique. Nous distinguons aussi deux cas, selon que l'intersection de $\mathcal{X} \cap \mathcal{Q}$ contient ou n'en contient pas de droites. Dans le cas où elle ne contiendrait pas de droite, on montre sans difficulté que $|\mathcal{X} \cap \mathcal{Q}| \leq t^5 + t^4 + t + 1$. Dans le cas où l'intersection contiendrait des droites, seul le cas $\mathcal{Q}$ non-dégénérée nécessite l'utilisation d'arguments plus complexes. On utilise les résultats de la section 0.5, et aussi le fait que $\mathbb{P}^4(\mathbb{F}_q)$ peut être engendré par $q + 1$ hyperplans passant par une même droite (définie par deux points de $\mathcal{X} \cap \mathcal{Q}$).

Finalement on montre le résultat suivant

Théorème 0.24. *Soit $\mathcal{Q}$ une quadrique dans $\mathbb{P}^4(\mathbb{F}_q)$ et $\mathcal{X}$ une variété hermitienne non-dégénérée $\mathcal{X} : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} + x_4^{t+1} = 0$, on a*

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2t^5 + t^3 + 2t^2 + 1,\ 2t^5 + t^3 + t^2 + 1$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2t^5 + 2t^2 + 1,\ 2t^5 + t^2 + 1,$$

$$\text{et pour } t \neq 2,3 \quad \#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = \begin{cases} 2t^5 - t^3 + 2t^2 + 1 \\ \quad \text{ou} \\ \leq 2t^5 - t^4 + 3t^3 - t + 1. \end{cases}$$

Nous explicitons les cinq premiers poids et donnons une description des mots correspondant à ces poids.

Théorème 0.25. *[15, p.26] Le premier poids du code $C_2(\mathcal{X})$ est $t^7 - t^5 - t^3 - t^2$.*
Les mots de poids minimaux correspondent aux quadriques qui sont réunion d'une paire d'hyperplans non-tangents à $\mathcal{X}$ tels que le plan d'intersection des deux hyperplans intersecte $\mathcal{X}$ en une courbe plane hermitienne non-singulière.

Théorème 0.26. *[15, p.26] Le second poids du code $C_2(\mathcal{X})$ est $t^7 - t^5 - t^3$.*
Les mots de code atteignant le second poids correspondent aux quadriques qui sont réunion d'une paire d'hyperplans non-tangents à $\mathcal{X}$ tels que le plan d'intersection des deux hyperplans intersecte $\mathcal{X}$ en une courbe plane hermitienne singulière de rang 2.

Théorème 0.27. *[15, p.27] Le troisième poids du code $C_2(\mathcal{X})$ est $t^7 - t^5 - t^2$.*
Les mots de code atteignant le troisième poids correspondent aux quadriques qui sont réunion d'une paire d'hyperplans, l'un tangent à $\mathcal{X}$, le second non-tangent à $\mathcal{X}$ et telle que le plan d'intersection des deux hyperplans intersecte $\mathcal{X}$ en une courbe plane hermitienne non-singulière.

Théorème 0.28. *[15, p.27] Le quatrième poids du code $C_2(\mathcal{X})$ est $t^7 - t^5$.*
Les mots de code atteignant le quatrième poids correspondent à deux types de quadriques:
–les quadriques qui sont réunion d'une paire d'hyperplans, l'un tangent à $\mathcal{X}$, le second non-tangent à $\mathcal{X}$ et le plan d' intersection des deux hyperplans est tangent à la surface hermitienne non-singulière obtenue du second hyperplan.
–les quadriques qui sont réunion d'une paire d'hyperplans tangents à $\mathcal{X}$ et le plan d' intersection des deux hyperplans intersecte $\mathcal{X}$ en une seule droite.

Théorème 0.29. *[15, p.27] Le cinquième poids (pour $t \neq 2,3$) du code $C_2(\mathcal{X})$ est $t^7 - t^5 + t^3 - t^2$.*
Les mots de code atteignant le cinquième poids correspondent (pour $t \neq 2,3$) aux quadriques qui sont réunion d'une paire d'hyperplans tangents et le plan d'intersection des deux hyperplans intersecte $\mathcal{X}$ en une courbe plane hermitienne non-singulière.

Remarquons que les cinq premiers poids du code $C_2(X)$ défini sur la variété hermitienne non-dégénérée dans $\mathbb{P}^4(\mathbb{F}_q)$ sont divisibles par t^2. Cette remarque n'est d'ailleurs pas fortuite. En fait par l'application du théorème de James Ax sur les zéros des polynômes à coefficients dans un corps fini tout comme dans le cas de la surface hermitienne au paragraphe §0.5, on montre la divisibilité par t^2 de tous les poids du code $C_2(\mathcal{X})$.

0.9 Questions ouvertes: deux conjectures à résoudre

Cette thèse se termine par la généralisation des résultats ci-dessus sous forme de conjectures pour des variétés hermitiennes de dimension supérieure dans $\mathbb{P}^n(\mathbb{F}_q)$.

0.9.1 Conjecture sur la distance minimale de $C_h(\mathcal{X})$ dans $\mathbb{P}^n(\mathbb{F}_q)$

Soit $\mathcal{X}$ la variété hermitienne non-singulière d'équation:

$$\mathcal{X} : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + ... + x_n^{t+1} = 0$$

Si $h \leq t$ on en déduit d'après le théorème 0.1 que l'application c définissant le code fonctionnel $C_h(\mathcal{X})$ est injective.

Conjecture.1

$\boxed{c(f) \text{ mot de poids minimum} \Leftrightarrow f \text{ est une hypersurface vérifiant les conditions 1, 2 et 3 suivantes}}$

1. hypersurfaces de Tsfasman-Serre-Sørensen (i.e. des hypersurfaces qui sont une réunion de h hyperplans passant par une sous-variété linéaire de codimension 2)

2. une condition de contact
   –si $n = 2l$, chacun des hyperplans H_i $i = 1, 2, ..., h$ est non-tangent à $\mathcal{X}$
   –si $n = 2l + 1$, chacun des hyperplans H_i $i = 1, 2, ..., h$ est tangent à $\mathcal{X}$.

3. la sous-variété projective linéaire $\mathcal{K} = \cap H_i$ de codimension 2 intersecte $\mathcal{X}$ en une variété hermitienne non-singulière dans $\mathbb{P}^{n-2}(\mathbb{F}_q)$.

Remarque 0.2. *La conjecture est vraie pour $h = 1$. On applique en fait les résultats* $\boxed{\textit{Bose+Char, 1966}}$+ $\boxed{\textit{Char, 1971}}$.
Elle est également vraie pour $h = 2$ et $n = 3, 4$ (voir § 0.5 et 0.6).

0.9.2 Conjecture sur les 5 premiers poids de $C_2(\mathcal{X})$ dans $\mathbb{P}^n(\mathbb{F}_q)$

Soit $\mathcal{X}$ la variété hermitienne non-singulière d'équation:

$$\mathcal{X} : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + ... + x_n^{t+1} = 0$$

Conjecture.2 Les mots atteignant les cinq premiers poids $(w_i)_{1 \leq i \leq 5}$ du code $C_2(\mathcal{X})$ correspondent à des quadriques ayant la configuration géométrique suivante:

1. $\boxed{w_1 \leq w \leq w_5}$ $\Rightarrow$ il existe une quadrique $\mathcal{Q}$ réunion de deux hyperplans distincts telle que $w(\mathcal{Q}) = w$.

2. $\boxed{w(\mathcal{Q}) = w_1}$ $\Leftrightarrow$ $\boxed{\mathcal{Q} = H_1 \cup H_2}$+$\boxed{\text{Condition de Contact}}$+$\boxed{\mathbb{P}^{n-2}}$
   –si $n = 2l$, H_1 et H_2 sont non-tangents à $\mathcal{X}$
   –si $n = 2l + 1$, H_1 et H_2 sont tangents à $\mathcal{X}$.
   –$(H_1 \cap H_2) \cap \mathcal{X}$ est une variété hermitienne non-singulière dans $\mathbb{P}^{n-2}(\mathbb{F}_q)$

3. $\boxed{w_5 < w} \Rightarrow$ aucun mot de code de poids w correspond à une quadrique $\mathcal{Q}$ réunion d'une paire d'hyperplans distincts.

Remarque 0.3. *Le point 2 de la conjecture est vraie pour $n = 3$. Pour $n = 3$, voir § 0.5. La conjecture est vraie pour $n = 4$ (voir § 0.8).*

Références

[1] Y. Aubry, Reed-Muller codes associated to projective algebraic varieties. In "Algebraic Geomertry and Coding Theory ". (Luminy, France, June 17-21, 1991). Lecture Notes in Math., Vol. 1518, Springer-Verlag, Berlin, (1992), 4-17.

[2] Y. Aubry and M. Perret, On the characteristic polynomials of the Frobenuis endomorphism for projective curves over finite fields, Finite Fields and Theirs Applications 10, (2004), 412-431

[3]J. Ax, Zeroes of polynomials over finite fields. Amer. J. Math., 86 (1964), 255-261.

[4] M. Boguslavsky, On the number of solutions of polynomial systems. Finite Fields and Their Applications 3 (1997), 287-299.

[5] A. E. Brouwer, Bounds on minimum distance of linear codes,
htpp://www.win.tue.nl/~aeb/voorlincod.html

[6] R. C. Bose and I. M. Chakravarti, Hermitian varieties in finite projective space $PG(N, q)$. Canadian J. of Math.18 (1966), 1161-1182.

[7] I. M. Chakravarti, Some properties and applications of Hermitian varieties in finite projective space PG(N,q^2) in the construction of strongly regular graphs (two-class association schemes) and block designs, Journal of Comb. Theory, Series B, 11(3) (1971), 268-283.

[8] I. M. Chakravarti, The generalized Goppa codes and related discrete designs from hermitian surfaces in $PG(3, s^2)$. Lecture Notes in computer Sci 311. (1986), 116-124.

[9] I. M. Chakravarti, Families of codes with few distinct weights from singular and nonsingular varieties and quadrics in projective geometries and Hadamard difference sets and designs associated with two-weight codes, in "Coding Theory and Design Theory ", Part I, IMA Vol. Math. Appl. 20, Springer, New York, (1990), 35-50.

[10] J. P. Cherdieu and R. Rolland, On the number of points of some hypersurface in $\mathbb{F}_q^n$, Finite Fields and Their Applications 2, (1996) 214-224.

[11] P. Dembowski, Finite Geometries, Springer-Verlag 1968.

[12] F. A. B. Edoukou, Codes defined by forms of degree 2 on hermitian surface and Sørensen conjecture, Finite Fields and Their Applications, Volume 13, Issue 3, (2007), 616-627.

[13] F. A. B. Edoukou, Codes defined by forms of degree 2 on quadric surfaces. arXiv:math. AG/0511679 v 1 28 Nov 2005. 5 pp., Submitted to IEEE. Trans. Inform. Theory (2005).

[14] F. A. B. Edoukou, The weight distribution of the functional codes defined by forms of degree 2 on hermitian surfaces. arXiv:math. AG/0512476 v 1 20 Dec 2005. 13 pp., Submitted to Finite Fields and Their Applications (2005).

[15] F. A. B. Edoukou, Codes defined by forms of degree 2 on quadric and non-degenerate hermitian varieties in $\mathbb{P}^4(\mathbb{F}_q)$. 29 pp., ArXiv : math.AG /0612229.

[16] F. A. B. Edoukou, Codes defined by forms of degree 2 on non-degenerate hermitian varieties in $\mathbb{P}^4(\mathbb{F}_q)$. 17 pp., Submitted to the Journal Designs, Codes and Cryptography, May 2007, ArXiv : math.AG /0612229.

[17] J. Harris, Algebraic Geometry (A first course), Graduate texts in mathematics 133, Springer-Verlag.

[18] R. Hartshorne, Algebraic geometry, Graduate texts in mathematics 52, Springer-Verlag, 1977.

[19] J. W. P. Hirschfeld, M. Tsfasman, S. Vladut, The weight hierarchy of higher dimensional hermitian codes, IEEE Trans. Inform. Theory 40 (1) (1994), 275-278.

[20] J. W. P. Hirschfeld, Projective Geometries Over Finite Fields (Second Edition) Clarendon Press. Oxford 1998.
[21] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Clarendon press. Oxford 1985.
[22] J. W. P. Hirschfeld, General Galois Geometies, Clarendon press. Oxford 1991.
[23] G. Lachaud, The parameters of projective Reed-Muller codes, Discrete Math, 81 (2) (1990) 217-221.
[24] G. Lachaud, La communication en équations, L'état des sciences et des techniques (Sous la direction de Nicolas Witkowski), Editions La Découverte Paris (1991), 341-344.
[25] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties; in " Arithmetic, Geometry, and Coding Theory ". (Luminy, France, 1993), Walter de Gruyter, Berlin-New York, (1996), 77-104.
[26] D. B. Leep and L. M. Schueller, Zeros of a pair of quadric forms defined over finite field. Finite Fields and Their Applications 5 (1999), 157-176.
[27] F. J. MacWilliams and N. J. Sloane, The theory of error-correctings codes, North-Holland Publishing C0., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.
[28] Y. I. Manin, S. Vladut, Linear codes and modular curves, Itogi Nauki i Tekhniki 25 (1984) 209-257 (English translation J. Soviet Math. 30 (1985) 2611-2643).
[29] O. Papini, J. Wolfmann, Algèbre discrète et codes correcteurs, Springer -Verlag, Berlin 1995.
[30] E. J. F. Primrose, Quadrics in finite geometries, Proc. Camb. Phil. Soc., 47 (1951), 299-304.
[31] D. K. Ray-Chaudhuri, Some results on quadrics in finite projective geometrie based on Galois fields, Can. J. Math. Vol. 14 (1962), 129-138.
[32] F. Rodier, Codes from flag varieties over a finite field, Journal of Pure and Applied Algebra 178 (2003), 203-214.
[33] P. Samuel, Géométrie projective, Presses Universitaires de France, 1986.
[34] J. P. Serre, Lettre à M. Tsfasman, In "Journées Arithmétiques de Luminy (1989)", Astérisque 198-199-200 (1991), 3511-353.
[35] I. R. Shafarevich, Basic algebraic geometry 1, Springer-Verlag, 1994.
[36] A. B. Sørensen, Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes. Ph. D. Thesis, Aarhus, Denmark, 1991.
[37] A. B. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inf. Theory Vol. 37 (6) (1991) 1567-1576.
[38] P. P. Spurr, Linear codes over $GF(4)$. Master's Thesis, University of North Carolina at Chapell Hill, USA, 1986.
[39] H. P. F. Swinnerton-Dyer, Rational zeros of two quadratics forms, Acta Arith. 9 (1964), 261-270.
[40] J. Wolfmann, Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie, Discrete Mathematics 13 (1975), 185-211.

Chapitre 1

Codes defined by forms of degree 2 on hermitian surfaces and Sørensen's conjecture

Codes defined by forms of degree 2 on hermitian surfaces and Sørensen's conjecture

Frédéric A. B. Edoukou

CNRS, Institut de Mathématiques de Luminy
Luminy case 907 - 13288 Marseille Cedex 9 - France
E.mail : edoukou@iml.univ-mrs.fr

Abstract

We study the functional codes $C_h(X)$ defined by G. Lachaud in [10] where $X \subset \mathbb{P}^N$ is an algebraic projective variety of degree d and dimension m.
When X is a hermitian surface in $PG(3,q)$, Sørensen in [15], has conjectured for $h \leq t$ (where $q = t^2$) the following result :

$$\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1$$

which should give the exact value of the minimum distance of the functional code $C_h(X)$.
In this paper we resolve the conjecture of Sørensen in the case of quadrics (i.e. $h = 2$), we show the geometrical structure of the minimum weight codewords and their number; we also estimate the second weight and the geometrical structure of the codewords reaching this second weight.

Keywords: functional codes, hermitian surface, hermitian curve, quadric, Sørensen's conjecture, weight.

Mathematics Subject Classification: 05B25, 11T71, 14J29

1 Introduction

After the works of Goppa, in coding theory, the construction of error-correcting codes from algebraic curves is now classical. From the works

of renowned scholars in algebraic geometry, such as Manin, Vladut [11], we are able to consider codes built from higher dimensional algebraic varieties. Some of such codes have already been studied. Among others, projective Reed-Muller codes have been studied by G. Lachaud [9], A. B. Sørensen [14] and Y. Aubry [1]; codes on hermitian varieties have also been studied by Chakravarti [4], and Hirschfeld, Vladut, Tsfasman [8].
In [10] G. Lachaud has also study the functional codes on a projective variety X of $\mathbb{P}^N$ of degree d and dimension m. Theses codes have similarities with the well known projective Reed-Muller codes defined over a projective variety X of $\mathbb{P}^N$.
In this paper, what we have in mind is to study the functional codes $C_h(X)$ introduced by G. Lachaud in [10] in the particular case where X is the non-degenerate hermitian surface $X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$ in $PG(3, q)$ and $q = t^2$. Indeed, the hermitian surfaces are interesting since they are maximal with respect to their number of rational points and they have also a beautiful geometry.
Even in the case of quadric surfaces, Y. Aubry [1] was not able to determine precisely the minimum distance of the functional codes $C_2(X)$, when the quadrics are non-degenerate (elliptic or hyperbolic) and 1-degenerate (cones).
Sørensen [15] has also tried to study the functional codes $C_h(X)$, on the hermitian surface X; but he was not able to find the minimum distance, even in the case $h = 2$. His work was motivated by the paper [3] (of Chakravarti) which undertake the study of the code $C_2(X)$ over $\mathbb{F}_4$ by a complete computer search. Thus, he conjectured a result, which will be the main purpose of our work.
The paper has been organized as follows. First of all, we recall somme notations and definitions of functional codes. Secondly, we state the conjecture of Sørensen:

$$\text{for } h \leq t, \quad \#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1.$$

Thirdly, by using the projective classification of quadrics in [7], the properties of the hermitian surface X and the projective classification of the hermitian plane curves in [7], we give a proof of the conjecture of Sørensen in the case $h = 2$. Finally we conclude our work by expressing more clearly the exact parameters of the functional codes $C_2(X)$, the geometrical structure of the minimum weight codewords and their number, the second weight and also the geometrical structure of codewords reaching this second weight.

2 Notations

We denote by $\mathbb{F}_q$ the field with q elements, where $q = p^a$ is a power of the prime number p. Let $V = \mathbb{A}^{N+1}$ be the affine space of dimension $N+1$ over $\mathbb{F}_q$. We denote also by $\mathbb{P} = \mathbb{P}(V) = PG(N,q) = \mathbb{P}^N$ the corrresponding projective space of dimension equal to N.
We denote also by $P_h(V, \mathbb{F}_q)$ the vector space of forms (that is, of homogeneous polynomials) of degree h in V with coefficients in $\mathbb{F}_q$. If $f \in P_h(V, \mathbb{F}_q)$, we denote by $Z(f)$, the set of zeros of f in the projective space. Let $X \subset \mathbb{P}$ be a subvariety of $\mathbb{P}$, $|X|$ denotes the number of its rational points over $\mathbb{F}_q$; we call $X \cap Z(f)$ a degree h section of X, and we denote by $X_{Z(f)}(\mathbb{F}_q)$, the the set of rational points over $\mathbb{F}_q$ of the algebraic set $X \cap Z(f)$.

3 Functional codes defined by forms on projective varieties

The subject of this section is to recall the construction of the functional codes defined by forms on projective varieties as it has been done by G. Lachaud in [10].

Definition 3.1 *Let X be a finite set, $X = (P_1, \ldots, P_n)$.*
Let $\mathcal{F}(X, \mathbb{F}_q)$ the space of all maps from X to $\mathbb{F}_q$. $\mathcal{F}(X, \mathbb{F}_q)$ is a vector space; let $\widetilde{F} \subset \mathcal{F}(X, \mathbb{F}_q)$ a subspace.
Let c be the map defined by

$$c : \mathcal{F}(X, \mathbb{F}_q) \longrightarrow \mathbb{F}_q^n$$

$$f \longmapsto c(f) = (f(P_1), \ldots, f(P_n))$$

We call functional code defined by $\widetilde{F}$ and X, and we denote it by $C(X, \widetilde{F})$, the image of the map c restricted to $\widetilde{F}$.

$$c_{|\widetilde{F}} : \widetilde{\mathrm{F}} \longrightarrow \mathbb{F}_q^n$$

$$f \longmapsto c_{|\widetilde{F}}(f) = (f(P_1), \ldots, f(P_n))$$

$$C(X, \widetilde{F}) = \mathrm{Im} c_{|\widetilde{F}}$$

The functional code we have defined has the following parameters

$$\mathrm{lengh} C(X, \widetilde{F}) = n, \qquad \dim C(X, \widetilde{F}) = \dim \widetilde{F} - \dim \ker C_{|\widetilde{F}}$$

Definition 3.2 *Let $c(f)$ be a codeword. We call coweight of the word $c(f)$, and we denote $cw(f)$, the number of zeros digits in $c(f)$.*

$$cw(f) = \#\{P \in X \quad | \quad f(P) = 0\} \qquad (3.2.1)$$

The weight of the word $c(f)$ which we denote by $w(c(f))$ is

$$w(c(f)) = n - cw(f)$$

The minimal distance of the functional code $C(X, \widetilde{F})$ is

$$\mathrm{dist}C(X, \widetilde{F}) = n - \max_{\mathrm{f}\in\widetilde{\mathrm{F}}} cw(f) \quad (3.2.2)$$

Definition 3.3 *We denote by $(x_0 : \ldots : x_N)$ the homogeneous coordinates in the projective space $\mathbb{P}^N$.*
Let W_i be the set of points with homogeneous coordinates $(x_0 : \ldots : x_N) \in \mathbb{P}^N$ such that $x_0 = x_1 = \ldots x_{i-1} = 0$ and $x_i \neq 0$.
The family $\{W_i\}_{0\leq i\leq N}$ is clearly a partition of $\mathbb{P}^N$.
Let ν be a map defined by:

$$\nu : \mathbb{P}^N \longrightarrow V - \{0\}$$

$$(x_0 : \ldots : x_N) \longmapsto (0, \ldots, 0, 1, x_{i+1}, \ldots, x_N)$$

for $(x_0 : \ldots : x_N) \in W_i$.

If $f \in P_h(V, \mathbb{F}_q)$ and $Q \in \mathbb{P}^N$, then

$$f(\nu Q) = \frac{f(x_0, \ldots, x_N)}{x_i^h} \qquad \text{with} \qquad \mathrm{Q} \in \mathrm{W_i}$$

Definition 3.4 *Let $X \subset \mathbb{P}^N$ be an algebraic set defined over $\mathbb{F}_q$ and $h \leq q$. The code defined by forms of degree h on X is the functional code $C_h(X) = C(X, \widetilde{F})$ obtained by taking $\widetilde{F}$ as the space of restrictions to X of forms in $P_h(V, \mathbb{F}_q)$.*

We have

$$\text{length } C_h(X) = \#X(\mathbb{F}_q) \quad (3.4.1)$$

When the map c is injective, we get

$$\dim C_h(X) = \binom{N+h}{h} \quad (3.4.2)$$

From (3.2.1), we deduce that

$$cw(f) = \#X_{Z(f)}(\mathbb{F}_q) \quad (3.4.3)$$

From (3.4.3), we can conclude that calculating the weights of the code $C_h(X)$, comes down to the computation of the number of points of degree h sections of X.

4 Codes defined by forms on hermitian varieties in $PG(3, q)$

We now restrict ourselves to functional codes defined in particular algebraic sets in $PG(3, q)$, where $q = t^2$ and t is a prime power. Thus, we consider the hermitian surface X defined by :

$$X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$$

We know from (3.4.1) that the length of this code is length $C_h(X) = \#X(\mathbb{F}_q)$. In [2](p.1179) Bose and Chakravarti showed that

$$\#X(\mathbb{F}_q) = (t^2 + 1)(t^3 + 1) \quad (4.1).$$

If $h \leq t$ the map c is injective and from (3.4.2), we can say that

$$\dim C_h(X) = \binom{3+h}{h} \quad (4.2).$$

For an estimate on the minimum distance of this code, as usually, a more careful analysis is necessary.

4.1 Codes defined by linear forms

In [2] we have the following result.

Theorem 4.1 *Let $H \subset \mathbb{P}^3$ be a plane*

$$\#X_H(\mathbb{F}_q) = \begin{cases} t^3 + 1 & \text{if } H \text{ is not tangent to } X, \\ t^3 + t^2 + 1 & \text{if } H \text{ is tangent to } X. \end{cases}$$

If H is tangent to X, $X \cap H$ is a singular hermitian curve of rank 2 in $PG(2, t^2)$. More precisely, $H \cap X$ is a set of t+1 lines passing through a common point. Thus we get $\#X_H(\mathbb{F}_q) = (t + 1)t^2 + 1 = t^3 + t^2 + 1$.
If H is not tangent to X, $X \cap H$ is a non-singular hermitian curve in $PG(2, t^2)$. Thus, we get $\#X_H(\mathbb{F}_q) = t^3 + 1$.

4.2 Codes defined by forms of degree two (quadrics)

In the case $h = 2$ and $t = 2$, the minimum distance of this code has been found by Paul P. Spurr in 1986 in his master's project by using a complete computer search; thus a $[45, 10, 22]$-code over $\mathbb{F}_4$ has been found.
In 1991, Anders B. Sørensen in [15], in his Ph. D. Thesis, without any computer programs, only with the geometric properties of quadrics and those of the non-singular cubic in [5], found the minimum distance of this code defined over $\mathbb{F}_4$.
Sørensen has tried to generalize the problem and conjectured that for $h \leq t$ (and t any prime power) we get

$$\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1$$

G. Lachaud has also proved in [10], with the help of proposition 2.3 [10] that

$$\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 + t + 1)$$

Unfortunately his bound is larger than that of Sørensen.

Remark 4.2 *From theorem 4.1 the conjecture is true in the case of codes defined by linear forms (h=1). In that case, the code $C_1(X)$ (noted $C(X)$) is a two-weight code of dimension 4 whose weights are t^5 and $t^5 + t^2$.*

We will now resolve the problem of Sorensen, in the case $h = 2$, and t any prime power.

5 Resolution of Sørensen's conjecture in the case $h = 2$ and t any prime power

We need to recall the notion of the rank of a quadric $\mathcal{Q} = Z(f)$.

Definition 5.1 *Let T be an inversible linear transformation defined over $\mathbb{P}^N$. Let $i(f)$ be the number of indeterminates appearing explicitly in F. The rank $r(\mathcal{Q})$ of the quadric $\mathcal{Q}$ is defined by*

$$r(Q) = \min_T i(f \circ T)$$

where T ranges over all inversible linear transformations over $\mathbb{F}_q$. A quadric $\mathcal{Q}$ is said to be degenerate if $r(\mathcal{Q}) < N + 1$. Otherwise the quadric is non-degenerate.

We have a particular property of quadric in [6] p.115.

Proposition 5.2 *A quadric $\mathcal{Q}$ is degenerate if and only it is singular.*

We recall also the classification of quadrics in $PG(3,q)$ under $PGL(4,q)$ given by J.W.P. Hirschfeld [7] in table 1; thus we will consider two cases depending on the degeneration of the quadrics.
In the whole paragraph we will note

$$s(t) = 2(t^3 + t^2 - t) + t + 1 \qquad s_2(t) = 2t^3 + t^2 + 1$$

Table.1 Quadrics in PG(3,q)

Rank	Description	$\lvert\mathcal{Q}\rvert$
1	repeated plane	$q^2 + q + 1$
2	pair of distinct planes	$2q^2 + q + 1$
2	line	$q + 1$
3	(quadric) cone	$q^2 + q + 1$
4	hyperbolic quadric	$(q + 1)^2$
4	elliptic quadric	$q^2 + 1$

5.1 $\mathcal{Q}$ is a degenerate quadric

Degenerate quadrics in $PG(3,q)$ are quadrics with rank stricly less than 4. So we need to distinguish four cases.

5.1.1 Rank $\mathcal{Q} = 1$

In this case $\mathcal{Q}$ is a repeated plane.
If $\mathcal{Q}$ is tangent to X, from theorem 4.1, $\mathcal{Q} \cap X$ is a singular hermitian curve of rang 2 in $PG(2,t^2)$, and $|\mathcal{Q} \cap X| = t^3 + t^2 + 1 < s_2(t)$.
If $\mathcal{Q}$ is not tangent to X, from [2], $\mathcal{Q} \cap X$ is a non-singular hermitian curve in $PG(2,t^2)$, and $|\mathcal{Q} \cap X| = t^3 + 1 < s_2(t)$.

5.1.2 Rank $\mathcal{Q} = 2$ and $\mathcal{Q}$ is a line

In this case we have $|\mathcal{Q}| = q + 1 = t^2 + 1$, so $|\mathcal{Q} \cap X| \leq t^2 + 1 < s_2(t)$.

5.1.3 Rank $\mathcal{Q} = 2$ and $\mathcal{Q}$ is a pair of distinct planes

(i) each plane is not tangent to X .
If we write $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$, then $\mathcal{P}_1 \cap X$ and $\mathcal{P}_2 \cap X$ are non-singular hermitian curves in $PG(2, t^2)$, such that $|\mathcal{P}_1 \cap X| = |\mathcal{P}_2 \cap X| = t^3 + 1$. Hence $|\mathcal{Q} \cap X| \leq 2(t^3 + 1) < s_2(t)$.

(ii) one plane is tangent and the second is not tangent to X .
Let us note $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$, with $\mathcal{P}_1$ tangent to X and $\mathcal{P}_2$ not tangent to X. The singular hermitian curve of rang 2, $\mathcal{P}_1 \cap X$ is in fact a set of $(t+1)$ lines passing through a point P, see theorem 4.1.
Let $l = \mathcal{P}_1 \cap \mathcal{P}_2$, then l is not contained in X from theorem 9.1 [3] p.1176. Since $l \subset \mathcal{P}_1$, we have $l \cap X = (l \cap \mathcal{P}_1) \cap X = l \cap (\mathcal{P}_1 \cap X)$, so that $l \cap X$ is a single point, or a set of $t + 1$ points since two distinct lines in the projective plane have exactly one common point. We know that

$$|\mathcal{Q} \cap X| = |\mathcal{P}_1 \cap X| + |\mathcal{P}_2 \cap X| - |\mathcal{P}_1 \cap \mathcal{P}_2 \cap X| \quad (5.1.3.\text{ii})$$

Since $|\mathcal{P}_1 \cap X| = t^3 + t^2 + 1$ and $|\mathcal{P}_2 \cap X| = t^3 + 1$, we get $|\mathcal{Q} \cap X| = 2t^3 + t^2 + 1 = s_2(t)$ in the case $l \cap X$ is a single point, or $|\mathcal{Q} \cap X| = 2t^3 + t^2 - t + 1 < s_2(t)$ in the case $l \cap X$ is a set of $t + 1$ points.

(iii) each plane is tangent to X .
Let us note $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$, with $\mathcal{P}_1$, and $\mathcal{P}_2$ tangent to X. We know that $\mathcal{P}_1 \cap X$ and $\mathcal{P}_2 \cap X$ as singular hermitian curves in $PG(2, t^2)$ are each one a set of $t + 1$ lines passing through respectively a point P_1 and a point P_2. Let $l = \mathcal{P}_1 \cap \mathcal{P}_2$, then $l \cap X$ is a set of $t + 1$ points or a line (in the case l is contained in X). Since $|\mathcal{P}_1 \cap X| = |\mathcal{P}_2 \cap X| = (t+1)t^2 + 1$, from the relation (5.1.3.ii) we conclude that either $|\mathcal{Q} \cap X| = s(t)$ when $l \cap X$ is a set of $t + 1$ points, or $|\mathcal{Q} \cap X| = 2t^3 + t^2 + 1 = s_2(t)$ when l is contained in X.

5.1.4 Rank $\mathcal{Q} = 3$ ($\mathcal{Q}$ is a cone)

Here, $|\mathcal{Q}| = q^2 + q + 1 = q(q + 1) + 1$ and $\mathcal{Q}$ consists of the points on $q + 1$ lines, passing through a vertex S. Thus we can consider two cases.

(i) no line in the cone is contained X .
Let us note $\mathcal{Q} = \bigcup_{i=1}^{q+1} \mathcal{L}_i$ where $\mathcal{L}_i$ is a line

$$\mathcal{Q} \cap X = \bigcup_{i=1}^{q+1} (X \cap \mathcal{L}_i) \quad (5.1.4.\text{i}.1)$$

We have also $|X \cap \mathcal{L}_i| \leq t+1$, so from the relation (5.1.4.i.1) $|\mathcal{Q} \cap X| \leq (t+1)(q+1)$. Hence $|\mathcal{Q} \cap X| \leq t^3 + t^2 + t + 1 < s_2(t)$.

(ii) at least one line of the cone is contained in X .
In $PG(3,q)$ the number of lines passing through a point is $q^2 + q + 1 = t^4 + t^2 + 1$.
From the study of the hermitian surface X in [2], we have the following result.

Proposition 5.3 *If C is any point in X, there pass exactly $t+1$ generators (i.e. lines lying in X) which constitute the intersection with X of the tangent plane at C. And through C, there pass t^2+1 lines lying in the tangent plane at C, among them $t+1$ are generators. The remaining $t^2 - t$ lines through C, which lie in the tangent plane meet X only in the single point C (there are called tangents to X). Each of the t^4 lines passing through C and not contained in the tangent plane at C intersect X in exactly $t+1$ points, one of which is C (such lines are called secants to X).*

From this proposition, on the hermitian surface X, we can assert first of all that the maximum number of generators the cone $\mathcal{Q}$ can contained is $t+1$. Secondly, if we suppose that the remaining $t^2 - t$ lines of the cone passing through the vertex S are all secants to X, we get

$$|\mathcal{Q} \cap X| \leq (t+1)t^2 + 1 + (t^2 - t)t.$$

And therefore, we have $|\mathcal{Q} \cap X| \leq 2t^3 + 1 < s_2(t)$.

5.2 $\mathcal{Q}$ is a non-degenerate quadric

Non-degenerate quadrics in $PG(3,q)$ are quadrics with rank equal to 4. Thus, from table 1, p. 7 there are two different types of such quadrics : hyperbolic quadrics and elliptic quadrics.

5.2.1 $\mathcal{Q}$ is a hyperbolic quadric

When $\mathcal{Q}$ is a hyperbolic quadric, we have $|\mathcal{Q}| = (q+1)^2$.
Before giving the proof of the conjecture of Sørensen when $\mathcal{Q}$ is a hyperbolic quadric, we need to recall some properties of lines, hermitian surfaces and hyperbolic quadrics in $PG(3,q)$.

Lemma 5.4 [7] *In PG(3,q), the number of lines meeting three skew lines is $q+1$.*

For a proof of this lemma see [7] p.3 .

Definition 5.5 *The set of transversals of three skew lines is called a regulus. So that a regulus consists of $q+1$ skew lines, and if l_1, l_2 and l_3 are any three of them, it is denoted by $\mathcal{R}(l_1, l_2, l_3)$.*

We have the following theorem, for the proof see [7] p.23 .

Theorem 5.6 *In PG(3,q), $q > 2$, let $\{l_1, l_2, l_3, l_4\}$ and $\{l'_1, l'_2, l'_3, l'_4\}$ be two sets of four lines such that any two of the same set are skew and such that 15 of the 16 pairs $\{l_i, l'_j\}$meet in a point. Then the last pair also does.*

The above theorem says that the lines meeting l_1, l_2 and l_3 meet all the lines of $\mathcal{R}(l_1, l_2, l_3) = \mathcal{R}$ and form a regulus, called the complementary regulus of $\mathcal{R}$.
From these results we have a good description of the hyperbolic quadric in $PG(3, q)$.

Theorem 5.7 *The hyperbolic quadric $\mathcal{Q}$ consists of $(q+1)^2$ points, which are all on a pair of complementary reguli. The two reguli are the two systems of generators of $\mathcal{Q}$. A hyperbolic quadric whose complementary reguli are $\mathcal{R}$ and $\mathcal{R}'$ is denoted by $\mathcal{H}(\mathcal{R}, \mathcal{R}')$.*

In [7] p.123, we also have an important property on the intersection of a hyperbolic quadric and the hermitian surface X, in the case the hyperbolic quadric contained at least three lines of a regulus.

Theorem 5.8 *If $\mathcal{Q} = \mathcal{H}(\mathcal{R}, \mathcal{R}')$ has three skew lines on X, then $X \cap \mathcal{Q}$ consists of $2(t+1)$ lines of $\mathcal{R}_0 \cup \mathcal{R}'_0$ where $\mathcal{R}_0 \subset \mathcal{R}$, $\mathcal{R}'_0 \subset \mathcal{R}'$ and $|\mathcal{R}'_0| = |\mathcal{R}_0| = t+1$.*

Remark 5.9 *Theorem 5.8 says that, if a hyperbolic quadric contains three skew lines on the non-degenerate hermition surface X, then it contains exactly $2(t+1)$ lines of the surface X, and $t+1$ lines in each of the two reguli.*

So that, if $X \cap \mathcal{Q} = \mathcal{C}$, then $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ where $\mathcal{C}_1$ and $\mathcal{C}_2$ are respectively the set of simple points, and double points, $\mathcal{C}_2 = \{l \cap l' | l \in \mathcal{R}_0,\ l' \in \mathcal{R}'_0\}$.
We get $|\mathcal{C}_1| = 2(t+1)(t^2+1-(t+1))$ and $|\mathcal{C}_2| = (t+1)^2$.
Hence $|\mathcal{Q} \cap X| = |\mathcal{C}| = 2t^3 + t^2 + 1$.

We can consider only one regulus instead of working in the whole hyperbolic quadric. Thus, we are now in position to say that the apparently difficult problem on the intersection of an hyperbolic quadric and the hermitian surface is reduced to the four following simple cases.

(i)A regulus of the hyperbolic quadric $\mathcal{H}(\mathcal{R},\mathcal{R}')$ contains at least three skew lines on the surface X In this case, from the above remark we have $|\mathcal{Q}\cap X| = s_2(t)$.

(ii)A regulus of the hyperbolic quadric $\mathcal{H}(\mathcal{R},\mathcal{R}')$ contains exactly two skew lines on the surface X We know that the hyperbolic quadric $\mathcal{Q}$ is generated by $q+1 = t^2+1$ lines of a regulus $\mathcal{R}$. The remaining t^2-1 lines of this regulus $\mathcal{R}$ which are not contained in the hermitian surface X, each of them, meets the hermitian surface X, in at most $t+1$ points. Therefore we have $|\mathcal{Q}\cap X| \leq 2(t^2+1)+(t^2-1)(t+1) = t^3+3t^2-t+1 < s_2(t)$.

(iii)A regulus of the hyperbolic quadric $\mathcal{H}(\mathcal{R},\mathcal{R}')$ contains exactly one line on the surface X We will suppose now that $\mathcal{R}$ is the regulus of the hyperbolic quadric which contains the only line of intersection. In this way, there are t^2 lines of $\mathcal{R}$ which are not contained in X. Each of them, meeting the hermitian surface in at most $t+1$ points, therefore $|\mathcal{Q}\cap X| \leq t^2+1+t^2(t+1) = t^3+2t^2+1 < s_2(t)$.

(iv) Each regulus of the hyperbolic quadric $\mathcal{H}(\mathcal{R},\mathcal{R}')$ does not contain any line on the surface X The hyperbolic quadric generated by one regulus for instance $\mathcal{R}$, and each line of the regulus meeting the hermitian surface X in at most $t+1$ points, implies that $|\mathcal{Q}\cap X| \leq (t^2+1)(t+1) = t^3+t^2+t+1 < s_2(t)$, as in the case 5.1.4.i).

5.2.2 $\mathcal{Q}$ is an elliptic quadric

When $\mathcal{Q}$ is an elliptic quadric, we have $|\mathcal{Q}| = q^2+1 = t^4+1$ and no line is contained in $\mathcal{Q}$ (that is the characterization of an elliptic quadric in $PG(3,q)$).
We need to distinguish two cases.

(i) $X\cap\mathcal{Q} = \emptyset$.
In this case the problem is resolved.

(ii) $X\cap\mathcal{Q} \neq \emptyset$.
Let us choose a point $P \in X\cap\mathcal{Q}$. We need the following proposition which can be found in [12].

Proposition 5.10 *Let $\mathcal{Q}_N$ be a non-degenerate quadric in $\mathbb{P}^N$ and H a hyperplane of $\mathbb{P}^N$. Then:*

If H is tangent to $\mathcal{Q}_N$, then $\mathcal{Q}_N \cap H$ is a degenerate quadric of rank $N-1$ in $\mathbb{P}^{N-1}$.
If H is not tangent to $\mathcal{Q}_N$, then $\mathcal{Q}_N \cap H$ is a non-degenerate quadric in $\mathbb{P}^{N-1}$.

Let H_1 be the tangent plane to the quadric at the point P. From the above proposition, we can deduce that $\mathcal{Q} \cap H_1$ is a degenerate quadric in $PG(2, t^2)$ of rank equal to 2. In [6] p.156, table 7.2, J.W.P. Hirschfeld gave the classification of quadrics in $PG(2, q)$. Thus, we get two cases: $\mathcal{Q} \cap H_1$ is either a pair of distinct lines or a point (a pair of conjuguate lines in $PG(2, q)$ which meet in $PG(2, t)$). Since the quadric $\mathcal{Q}$ does not contain any line, we can say that $\mathcal{Q} \cap H_1$ is a point, $\mathcal{Q} \cap H_1 = \{P\}$ and therefore

$$\mathcal{Q} \cap X \cap H_1 = \{P\} \quad (5.2.2.1)$$

Let us take a line D passing through P and contained in the plane H_1. We consider also all the planes $(H_i)_{i \in I}$ passing through the line D.
From the above proposition, if $H_i \neq H_1$, then $\mathcal{Q} \cap H_i$ is a non-degenerate quadric and therefore from proposition 5.2 a non-singular curve.
On the other hand $X \cap H_i$ is a hermitian curve (singular or not).
If H_i is not tangent to X, then $X \cap H_i$ is a non-singular hermitian curve. Thus, $X \cap H_i$ and $\mathcal{Q} \cap H_i$ are two non-singular projective plane curves, so they are irreducible. From the theorem of Bézout [13] chap.4, 2.1 p.236, we can say that

$$|X \cap \mathcal{Q} \cap H_i| \leq 2(t+1) \quad (5.2.2.2)$$

If H_i is tangent to X, then $X \cap H_i$ as a singular hermitian curve is from theorem 4.1 a set of $t+1$ lines passing through a common point; each line meeting $X \cap \mathcal{Q}$ in at most 2 points. Thus, we get

$$|X \cap \mathcal{Q} \cap H_i| \leq 2(t+1) \quad (5.2.2.3)$$

We can now conclude that

$$\text{if } H_i \neq H_1, \text{then} \qquad |X \cap \mathcal{Q} \cap H_i| \leq 2(t+1) \quad (5.2.2.4)$$

The point P belong to each $X \cap \mathcal{Q} \cap H_i$, and therefore from (5.2.2.4) we get

$$|X \cap \mathcal{Q} \cap H_i - \{P\}| \leq 2(t+1) - 1 \quad (5.2.2.5)$$

There are exactly $q+1$ planes passing through the line D, and their union generate the whole projective space $PG(3, q)$. Thus, we get

$$\mathcal{Q} \cap X = \{P\} \cup \bigcup_{i=2}^{q+1} (X \cap \mathcal{Q} \cap H_i - \{P\}) \quad (5.2.2.6)$$

From the relation (5.2.2.6) we get

$$|\mathcal{Q} \cap X| \leq 1 + \sum_{i=2}^{q+1} |X \cap \mathcal{Q} \cap H_i - \{P\}| \qquad (5.2.2.7)$$

And from the relations (5.2.2.5) and (5.2.2.7) we deduce that $|\mathcal{Q} \cap X| \leq 1 + q(2(t+1)-1)$.
Finally we get,

$$|\mathcal{Q} \cap X| \leq 2t^3 + t^2 + 1 = s_2(t).$$

It is now possible for us, to answer affirmatively to the conjecture of Sørensen in the case $h = 2$ and t any prime power.

5.3 Positive answer to Sørensen' s conjecture in the case of quadrics

Theorem 5.11 *Let $\mathcal{Q}$ be a quadric in PG(3,q) and X the non-degenerate hermitian surface $X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$, we have*

$$\#X_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2(t^3 + t^2 - t) + t + 1 \quad \text{or} \qquad \#X_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 2t^3 + t^2 + 1$$

We can now state the following results.

6 The parameters of the functional codes defined by forms of degree 2 in $PG(3, q)$ on the hermitian surface

Theorem 6.1 *The code $C_2(X)$ defined on the hermitian surface $X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$ is a $[n, k, d]_q$-code where*

$$n = (t^2+1)(t^3+1)$$
$$k = 10$$
$$d = t^5 - t^3 - t^2 + t = t(t-1)(t^3 + t^2 - 1)$$

Proof To find d we use the relations (3.2.2), (3.4.3) and the theorem 5.11.

Theorem 6.2 *The minimum weight codewords correspond now to the two planes each intersecting the hermitian surface X in $t+1$ lines passing trough a point and the line of intersection of the two planes intersects the hermitian surface in $t+1$ points.*

Lemma 6.3 *Let* $\{\mathcal{P}_1, \mathcal{P}_2\}$ *and* $\{\mathcal{P}_1, \mathcal{P}_3\}$ *be two distinct pairs of tangent planes to the hermitian surface* X. *Then* $(\mathcal{P}_1 \cap X) \cup (\mathcal{P}_2 \cap X) \neq (\mathcal{P}_1 \cap X) \cup (\mathcal{P}_3 \cap X)$.

Lemma 6.4 *Let* $\{\mathcal{P}_1, \mathcal{P}_2\}$ *and* $\{\mathcal{P}_3, \mathcal{P}_4\}$ *be two distinct pairs of tangent planes to the hermitian surface* X. *Then* $(\mathcal{P}_1 \cap X) \cup (\mathcal{P}_2 \cap X) \neq (\mathcal{P}_3 \cap X) \cup (\mathcal{P}_4 \cap X)$.

The proof of lemma 6.3 and lemma 6.4 are obvious. It is done by a simple calculation of intersection.

We come now to the computation of the codewords of minimum weight.

Theorem 6.5 *The number of codewords of minimum weight is :*

$$(t^2-1)[\frac{1}{2}(t^5+t^3+t^2+1)t^5]$$

Proof
We know that a codeword of minimum weight is given by a quadric $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$ where :
– $\mathcal{P}_1$ is a tangent plane to the hermitian surface X at a point P_1,
– $\mathcal{P}_2$ is a tangent plane to the hermitian surface X at a point P_2,
and P_2 doesn't belong in $\mathcal{P}_1$, (i.e. $\Delta = \mathcal{P}_1 \cap \mathcal{P}_2$ meets the hermitian surface in $t+1$ points).
We also know from [2], theorem 7.3 p.1172, that there are exactly $\#X(\mathbb{F}_q) = t^5+t^3+t^2+1$ tangent planes $\mathcal{P}$ to the surface X. Thus $\mathcal{P}_1 \cap X$ as a set of $t+1$ lines meeting in a common point, has t^3+t^2+1 points.
Given a tangent plane $\mathcal{P}_1$, if we wish that the quadric $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$ gives a codeword of minimum weight, we get exactly $\#X(\mathbb{F}_q) - (t^3+t^2+1) = t^5$ possibilities to choose the point P_2. Thus, we get $(t^5+t^3+t^2+1)t^5$ pairs $(\mathcal{P}_1,\ \mathcal{P}_2)$ of tangent planes to the hermitian surface X giving a codeword of minimum weight. Since the two pairs $(\mathcal{P}_1,\ \mathcal{P}_2)$, and $(\mathcal{P}_2,\ \mathcal{P}_1)$ are the same (they give the same quadric), we get from these tangent planes $\frac{1}{2}(t^5+t^3+t^2+1)t^5$ quadrics giving codewords of minimum weight. From lemmas 6.3 and 6.4, the codewords obtained from these quadrics are all distinct.
Given a quadric $\mathcal{Q}$, from which we get a codeword of minimum weight, the quadric $\mathcal{Q}' = \lambda\mathcal{Q}$ with $\lambda \in \mathbb{F}_q^\star$, gives a codeword of minimum weight. Thus, we get finally $(t^2-1)[\frac{1}{2}(t^5+t^3+t^2+1)t^5]$ codewords of minimum weight.

Observe that, in the case $t = 2$ there is exactly $3 \times \frac{1}{2} \times (45 \times 32) = 2160$ codewords of minimum weight. Thus, we recover the result of Paul P. Spurr [2] p.120 and the one of Sørensen [15] p.9.

Theorem 6.6 *The second weight of the code $C_2(X)$ is $t^5 - t^3$.*

Proof In fact when $\mathcal{Q}$ is not a pair of two tangent planes which intersection line meets X in $t+1$ points, we get $\#X_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq s_2(t) = 2t^3 + t^2 + 1$. And this upper bound is reached when $\mathcal{Q}$ is either a pair of two tangent planes meeting in a line contained in X, or a hyperbolic quadric containing three skew lines of X, or a pair of two planes, one tangent to X and the second not tangent to X, with the line of intersection of the two planes meting X at a single point.

Note that, in the case $t = 2$ we recover the second weight of the code $C_2(X)$ over $\mathbb{F}_4$ in agreement with [3] which is $2^5 - 2^3 = 24$.

Acknowledgments

The author would like to thank Mr F. Rodier. He is very grateful to him. His remarks and patience encouraged him to work on the problem.

References

[1] Y. Aubry, Reed-Muller codes associated to projective algebraic varieties. In "Algebraic Geomertry and Coding Theory ". (Luminy, France, June 17-21, 1991). Lecture Notes in Math., Vol. 1518, Springer-Verlag, Berlin, (1992), 4-17.

[2] R. C Bose and I. M Chakravarti, Hermitian varieties in finite projective space $PG(N, q)$. Canadian J.of Math.18 (1966), 1161-1182.

[3] I. M. Chakravarti, The generalized Goppa codes and related discrete designs from hermitian surfaces in $PG(3, s^2)$. Lecture Notes in computer Sci 311. (1986), 116-124.

[4] I. M. Chakravarti, Families of codes with few distinct weights from singular and nonsingular varieties and quadrics in projective geometries and Hadamard difference sets and designs associated with two-weight codes, in "Coding Theory and Design Theory ", Part I, IMA Vol. Math. Appl. 20, Springer, New York, (1990), 35-50.

[5] R. Hartshorne, Algebraic geometry, Graduate texts in mathematics 52, Springer-Verlag, 1977.

[6] J. W. P. Hirschfeld, Projective Geometries Over Finite Fields (Second Edition) Clarendon Press. Oxford 1998.

[7] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Clarendon press. Oxford 1985.

[8] J. W. P. Hirschfeld, M. Tsfasman, S. Vladut, The weight hierarchy of higher dimensional hermitian codes, IEEE Trans. Inform. Theory 40 (1) (1994), 275-278.

[9] G. Lachaud, The parameters of projective Reed-Muller codes, Discrete Math, 81 (2) (1990), 217-221.

[10] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties; in " Arithmetic, Geometry, and Coding Theory " . (Luminy, France, June 17-21, 1993), Walter de Gruyter, Berlin-New York (1996), 77-104.

[11] Y. I. Manin, S. Vladut, Linear codes and modular curves, Itogi Nauki i Tekhniki 25 (1984), 209-257 (English translation J. Soviet Math. 30 (1985), 2611-2643).

[12] E. J. F. Primrose, Quadrics in finite geometries, Proc. Camb. Phil. Soc., 47 (1951), 299-304.

[13] I. R. Shafarevich, Basic algebraic geometry 1, Springer-Verlag, 1994.

[14] A. B. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inf. Theory Vol. 37 (6) (1991), 1567-1576.

[15] A. B. Sørensen, Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes. Ph. D. Thesis, Aarhus, Denmark, 1991.

Chapitre 2

The weight distribution of the functional codes defined by forms of degree 2 on hermitian surfaces

The weight distribution of the functional codes defined by forms of degree 2 on hermitian surfaces

Frédéric A. B. Edoukou

CNRS, Institut de Mathématiques de Luminy
Luminy case 907 - 13288 Marseille Cedex 9 - France
E.mail : edoukou@iml.univ-mrs.fr

Abstract

We study the functional codes $C_2(X)$ defined on a projective variety X, in the case where $X \subset \mathbb{P}^3$ is a non-degenerate hermitian surface. We first give some bounds for $\#X_{Z(\mathcal{Q})}(\mathbb{F}_q)$, which are better than the ones known. We compute the number of codewords reaching the second weight. We also estimate the third weight, show the geometrical structure of the codewords reaching this third weight and compute their number. The paper ends with a conjecture on the fourth weight and the fifth weight of the code $C_2(X)$.

Keywords: arithmetical genus, functional codes, hermitian surface, hermitian curve, quadric, weight.

Mathematics Subject Classification: 05B25, 11T71, 14J29

1 Introduction

The code $C_h(X)$ over $\mathbb{F}_q$ ($q = t^2$, with t a prime power) has been studied by Sørensen [10] in his Ph.D Thesis in the case where X is a non-singular hermitian surface and also by G. Lachaud [8]. In fact, the code $C_2(X)$ has previously been studied over $\mathbb{F}_4$ by Paul P. Spurr [11] in his master thesis; by a complete computer search he found the weight distribution of this code. Sørensen was not able to find the minimum distance, even less the weight distribution. For f a form of degree h, he only conjectured the following

result:

$$\text{for } h \leq t \quad \#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1,$$

which should give the minimum distance. In [4] the author didn't only prove the conjecture for $h \leq 2$, but determined the second weight and three types of quadrics giving codewords of second weight.
The purpose of this paper is to express as possible the weight distribution of the code $C_2(X)$. Indeed, the study of the weights is important since they measure the efficiency of the code, and their notification is useful in the procedures of decoding.
The paper has been organized as follows. First of all, we give some bounds for the number of points of the section of the hermitian surfaces with quadrics of rank 2, quadrics cone, and the elliptic quadrics. These bounds are better than the ones obtained in [4]. Thus, codewords of second weight are obtained only from the three types of quadrics found in [4]; we compute their number. We determine the third weight, the geometrical structure of codewords reaching it and we compute their number. Finally, we conclude our work by a conjecture on the fourth and fifth weight of the code $C_2(X)$.
We now give a summary of notation and terminology. We denote by $\mathbb{F}_q$ the field with q elements and by $\mathbb{P}^n = \mathbb{P}^n(\mathbb{F}_q) = PG(n, q)$ the projective space of n dimension over $\mathbb{F}_q$. We use the term forms of degree h to describe homogeneous polynomials f of degree h; and we denote by $\mathcal{Q} = Z(f)$, the zeros of f in $\mathbb{P}^n(\mathbb{F}_q)$, which is a quadric when $h = 2$. Let $\mathcal{Q}$ be a quadric, the rank of $\mathcal{Q}$ denoted $r(\mathcal{Q})$ is the smallest number of indeterminates appearing in f under any change of coordinate system.
Let $\mathcal{F}$ be the vector space of forms of degree 2, $X \subset \mathbb{P}^3$ the non-degenerate hermitian surface $X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$ and $|X|$ the number of rational points of X over $\mathbb{F}_q$. We denote by W_i the set of points with homogeneous coordinates $(x_0 : ... : x_3) \in \mathbb{P}^3$ such that $x_j = 0$ for $j < i$ and $x_i = 1$. The family $\{W_i\}_{0 \leq i \leq 3}$ is a partition of $\mathbb{P}^3$. The code $C_2(X)$ is the image of the linear map $c : \mathcal{F} \longrightarrow \mathbb{F}_q^{|X|}$, defined by $c(\mathcal{Q}) = (c_x(\mathcal{Q}))_{x \in X}$, where $c_x(\mathcal{Q}) = \mathcal{Q}(x_0, ..., x_3)$ with $x = (x_0, ..., x_3) \in W_i$.

2 The number of intersection points of the hermitian surface with some quadrics

The subject of this section is to find some bounds for the number of intersection points of the hermitian surface and some quadrics which are better

than the ones of [4]. In what follows we will note:

$$s(t) = 2t^3 + 2t^2 - t + 1 \qquad s_2(t) = 2t^3 + t^2 + 1 \qquad s_3(t) = 2t^3 + t^2 - t + 1$$

$$s_4(t) = 2t^3 + 1 \qquad s_5(t) = 2t^3 - t + 1$$

2.1 Rank $(\mathcal{Q}) = 2$ and $\mathcal{Q}$ is a pair of distinct non-tangent planes

If we write $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$, then $\mathcal{P}_1 \cap X$ and $\mathcal{P}_2 \cap X$ are non-singular hermitian curves in $PG(2, t^2)$, such that $|\mathcal{P}_1 \cap X| = |\mathcal{P}_2 \cap X| = t^3 + 1$.
Let $l = \mathcal{P}_1 \cap \mathcal{P}_2$, then l is not contained in X from theorem 9.1 [2] p.1176. Thus, $l \cap X$ is either a single point or a set of $t+1$ points. Hence $|\mathcal{Q} \cap X| = s_4(t)$ when $l \cap X$ is a single point or $|\mathcal{Q} \cap X| = s_5(t)$ when l is a secant.

2.2 Rank $(\mathcal{Q}) = 3$ ($\mathcal{Q}$ is a cone)

Here $\mathcal{Q}$ consists of the points on $q+1$ lines passing through a vertex no three of which are coplanar. Thus, the intersection of the cone with the hermitian surface contains at most two generators. If no line of the cone is contained in X, we get $|\mathcal{Q} \cap X| \leq t^3 + t^2 + t + 1 < s_4(t)$. From proposition 5.3 [4], we conclude that, $|\mathcal{Q} \cap X| = t^3 + t^2 + 1$ or $|\mathcal{Q} \cap X| = t^3 + 2t^2 - t + 1$ according to the cone contains exactly one or two lines of X.

2.3 Rank $(\mathcal{Q}) = 4$ and $\mathcal{Q}$ is an elliptic quadric

When $\mathcal{Q}$ is an elliptic quadric, no line is contained in $\mathcal{Q}$. We get two cases: either $|X \cap \mathcal{Q}| \leq 1$ or $|X \cap \mathcal{Q}| \geq 2$.
In the case $|X \cap \mathcal{Q}| \geq 2$, we will use an analogous technique as the one used in [4] for the elliptic quadric.
Let us choose two distinct points $P_1, P_2 \in X \cap \mathcal{Q}$. Let H be a plane passing through the points P_1 and P_2. In [6] p.156, table 7.2, J.W.P. Hirschfeld gave the classification of quadrics in $PG(2, q)$. Thus, we get that $\mathcal{Q} \cap H$ is either a line or a pair of distinct lines or a point (a pair of conjuguate lines in $PG(2, q)$ which meet in $PG(2, t)$) or a conic (a non-degerate quadric). Since the quadric $\mathcal{Q}$ does not contain any line and contains two points, we can say that $\mathcal{Q} \cap H$ is a conic (a non-degerate quadric) and H is non-tangent to $\mathcal{Q}$. Let $(\mathcal{D})$ be the line passing through the two points P_1 and P_2. We consider also all the planes $(H_i)_{i \in I}$ passing through the line $(\mathcal{D})$. Then $\mathcal{Q} \cap H_i$ as a non-degenerate quadric is a non-singular curve. On the other hand $X \cap H_i$

is a hermitian curve (singular or not). Since H_i is non-tangent to $\mathcal{Q}$, as in [4] we conclude that:

$$\text{for each} \quad i \qquad |X \cap \mathcal{Q} \cap H_i| \leq 2(t+1) \quad (2.3.1)$$

The two points P_1 and P_2 belong to each $X \cap \mathcal{Q} \cap H_i$, and therefore from (2.3.1) we get: $\quad |X \cap \mathcal{Q} \cap H_i - \{P_1, P_2\}| \leq 2(t+1) - 2 \quad (2.3.2)$
There are exactly $q+1$ planes passing through the line $(\mathcal{D})$, and their union generate the whole projective space $PG(3,q)$. Thus, we get:

$$\mathcal{Q} \cap X = (X \cap \mathcal{Q} \cap H_1) \cup \bigcup_{i=2}^{q+1} (X \cap \mathcal{Q} \cap H_i - \{P_1, P_2\}) \quad (2.3.3)$$

And from the relations (2.3.1), (2.3.2) and (2.3.3) we deduce that $|\mathcal{Q} \cap X| \leq 2(t+1)+q(2(t+1)-2)$. Thus, we get finally $|\mathcal{Q} \cap X| \leq 2t^3+2t+2$. We have $2t^3+2t+2 < s_2(t)$ for $t \geq 3$ and for $t = 2$ we also have $|\mathcal{Q} \cap X| < |\mathcal{Q}| < s_2(2)$. Then when $\mathcal{Q}$ is an elliptic quadric we conclude that $|\mathcal{Q} \cap X| < s_2(t)$.

3 The second weight of the code $C_2(X)$

Theorem 3.1 [4] *The second weight of the code $C_2(X)$ is $t^5 - t^3$.*

Theorem 3.2 *The codewords of second weight correspond to:*
– hyperbolic quadrics containing three skew lines of X,
– quadrics which are union of two tangent planes meeting at a line contained in X,
– quadrics which are pair of two planes, one tangent to X and the second not tangent to X and the line of intersection of the two planes meeting X at a single point.

Proof From paragraph 2.3, we deduce that the codewords of second weight can not correspond to elliptic quadrics. Therefore the three types of quadrics found in [4] are the only ones which give codewords of second weight.

Lemma 3.3 *Let $\mathcal{P}_1$ and $\mathcal{P}'_1$ two tangent planes to X, $\mathcal{P}_2$ and $\mathcal{P}'_2$ two non-tangent planes with $\mathcal{P}_1 \cup \mathcal{P}_2 \neq \mathcal{P}'_1 \cup \mathcal{P}'_2$ and such that $|\mathcal{P}_1 \cap \mathcal{P}_2 \cap X| = |\mathcal{P}'_1 \cap \mathcal{P}'_2 \cap X| = 1$. Then $(\mathcal{P}_1 \cap X) \cup (\mathcal{P}_2 \cap X) \neq (\mathcal{P}'_1 \cap X) \cup (\mathcal{P}'_2 \cap X)$.*

Lemma 3.4 *Let $\mathcal{Q}'$ be a hyperbolic quadric containing three skew lines of X. Let $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$ be a pair of disctinct planes, one tangent to X. Then $\mathcal{Q}' \cap X \neq (\mathcal{P}_1 \cap X) \cup (\mathcal{P}_2 \cap X)$.*

Lemma 3.5 *Let $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$ be a pair of distinct tangent planes and $l = \mathcal{P}_1 \cap \mathcal{P}_2 \subset X$. Let $\mathcal{Q}' = \mathcal{P}'_1 \cup \mathcal{P}'_2$ be two planes, $\mathcal{P}'_1$ tangent to X, $\mathcal{P}'_2$ non-tangent to X and $l' = \mathcal{P}'_1 \cap \mathcal{P}'_2$ intersecting X at a single point. Then $(\mathcal{P}_1 \cap X) \cup (\mathcal{P}_2 \cap X) \neq (\mathcal{P}'_1 \cap X) \cup (\mathcal{P}'_2 \cap X)$.*

The proofs of these three lemmas are obvious. There are analogous to the proofs of lemma 6.3 and lemma 6.4 [4].

We come now to the computation of the codewords of second weight.

Theorem 3.6 *The number of codewords of second weight is:*

$$\frac{1}{2}(t^2-1)(t^5+t^3+t^2+1)(3t^2-t+1)t^2$$

Proof Since there are three types of codewords of second weight we will find the number of each of them.
(i) From J.W.P. Hirschfeld [7] p.124, there are exactly $n_q = \frac{1}{2}q^2(q\sqrt{q}+1)(q+1)$ hyperbolic quadrics containing three skew lines of the hermitian surface. Let $\mathcal{Q}$ and $\mathcal{Q}'$ be two distinct hyperbolic quadrics giving codewords of second weight, we have $\mathcal{Q} \cap X \neq \mathcal{Q}' \cap X$. Thus, there are exactly $(q-1)[\frac{1}{2}q^2(q\sqrt{q}+1)(q+1)]$ codewords of second weight obtained from the hyperbolic quadrics.
(ii) We also know from [2], theorem 7.3 p.1172, that there are exactly $\#X(\mathbb{F}_q) = t^5+t^3+t^2+1$ tangent planes to the hermitian surface X. We want now to determine the number of quadrics $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$ where $\mathcal{P}_1$ and $\mathcal{P}_2$ are two distinct tangent planes meeting at a line contained in X. Given a tangent plane $\mathcal{P}_1$, there are exactly $t^2(t+1) = t^3+t^2$ possibilities to choose the plane $\mathcal{P}_2$; so we get $(t^5+t^3+t^2+1)(t^3+t^2)$ couples $(\mathcal{P}_1,\ \mathcal{P}_2)$. Since the two couples $(\mathcal{P}_1,\ \mathcal{P}_2)$ and $(\mathcal{P}_2,\ \mathcal{P}_1)$ are the same (they give the same quadric), we get from these tangent planes $\frac{1}{2}(t^5+t^3+t^2+1)(t^3+t^2)$ quadrics giving codewords of second weight. And from lemma 6.3 and 6.4 [4], the codewords obtained from these quadrics are all distinct. Thus, we get $(t^2-1)[\frac{1}{2}(t^5+t^3+t^2+1)(t^3+t^2)]$ codewords of second weight.
(iii) Let $Q = \mathcal{P}_1 \cup \mathcal{P}_2$ be a quadric where $\mathcal{P}_1$ and $\mathcal{P}_2$ are respectively a tangent plane to X, a non-tangent plane to X, where $l = \mathcal{P}_1 \cap \mathcal{P}_2$ with $l \cap X = \{P_1\}$ $(l \not\subset X)$. Here, we need to find first of all the number of planes $(H_i)_{i\in I}$ for which we have $H_i \cap \mathcal{P}_1 = l$ where l is a line intersecting X in a single point P_1.
We know that there are (t^2-t) lines of such type (lines l).
Given a line l, there pass exactly $q+1$ planes through l ($\mathcal{P}_1$ is one of these

planes). Thus, we get at maximum $q(t^2-t)$ planes H_i, i.e. t^4-t^3 planes H_i. In fact, there are exactly t^4-t^3 planes H_i, since if H_1 and H_2 are respectively planes through l_1 and l_2 two distinct lines, then $H_1 \neq H_2$.
We also know that the number of tangent planes to X is $\#X((\mathbb{F}_q) = t^5+t^3+t^2+1$, so we deduce that there are exactly $(t^5+t^3+t^2+1)(t^4-t^3)$ quadrics $Q = \mathcal{P}_1 \cup \mathcal{P}_2$ (where $\mathcal{P}_1$ is a tangent plane to X, $\mathcal{P}_2$ is a non-tangent plane to X, and $l = \mathcal{P}_1 \cap \mathcal{P}_2$ intersecting X at a single point). And from lemma 3.3, the codewords obtained from these quadrics are all distinct. Thus, we get exactly $(t^2-1)(t^5+t^3+t^2+1)(t^4-t^3)$ codewords of second weight from these quadrics.
From lemmas 3.4 and 3.5, we deduce that the codewords obtained from **(i)**, **(ii)** and **(iii)** are all distinct.
Therefore we have exactly: $(t^2-1)[\frac{1}{2}t^4(t^3+1)(t^2+1)] + (t^2-1)[\frac{1}{2}(t^5+t^3+t^2+1)(t^3+t^2)] + (t^2-1)(t^5+t^3+t^2+1)(t^4-t^3) = \frac{1}{2}(t^2-1)(t^5+t^3+t^2+1)(3t^2-t+1)t^2$ codewords of second weight.

Observe that, in the case $t=2$, there are exactly $\frac{1}{2}\times 3\times 45\times 11\times 4 = 2970$ codewords of second weight. Thus, we recover the result of Paul P. Spurr [3] p.120 calculated by computer.

4 The Weight distribution of the code $C_2(X)$

In what follows $s(t)$, $s_2(t)$, $s_3(t)$, $s_4(t)$ and $s_5(t)$ have the same values as in section 2. It has been shown in [4] with the help of the relations (3.2.2) and (3.4.3) that $s(t)$ and $s_2(t)$ give respectively the first weight (minimum distance) and the second weight.
For $t>3$, $s_3(t) > 2t^3+2t+2$; and for $t=2$, the elliptic quadric $\mathcal{Q}$ over $\mathbb{F}_4$ has $|\mathcal{Q}| = 17$ points, and we have $17 < s_3(2) = 19$. Therefore, from table 4.2, the third weight is given by $s_3(t)$ for $t \neq 3$.

Theorem 4.1 *Let l be a line in $PG(3,\mathbb{F}_q)$ and X the hermitian surface then l meets X at a single point or $t+1$ points or is contained in X. This line is respectively called a tangent, a secant, or a generator.*

Proof: See [2], p.1179.

Definition 4.2 *A regulus (notion used by Hirschfeld [7] p.4) is the set of transversals of three skew lines. It consists of $q+1$ skew lines.*

Theorem 4.3 *[7] p.23 A hyperbolic quadric $\mathcal{Q}$ consists of $(q+1)^2$ points, which are all on a pair of complementary reguli. The two reguli are the*

two systems of generators of $\mathcal{Q}$. A hyperbolic quadric whose complementary reguli are $\mathcal{R}$ and $\mathcal{R}'$ is denoted by $\mathcal{H}(\mathcal{R}, \mathcal{R}')$.

Remark 4.4 *When $\mathcal{Q}$ is a hyperbolic quadric containing exactly two skew lines on the hermitian surface X (i.e. type 12 in table 4.2), we get:*
– for $t \geq 3$, $\#X_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq t^3 + 3t^2 - t + 1 < s_4(t)$,
– for $t = 2$, we get $\#X_{Z(\mathcal{Q})}(\mathbb{F}_4) \leq 2^3 + 3 \times 2^2 - 2 + 1 = 19 = s_3(2)$. Let us suppose in the case $(t = 2)$ that, $\#X_{Z(\mathcal{Q})}(\mathbb{F}_4) < 19$; therefore it exists a line l on the considered regulus of $\mathcal{Q}$ such that $l \cap X$ is a single point. Thus we get $\#X_{Z(\mathcal{Q})}(\mathbb{F}_4) \leq 2(t^2+1) + (t^2-2)(t+1) + 1 = 17 = s_4(2)$. Therefore we can assert that

$$\#X_{Z(\mathcal{Q})}(\mathbb{F}_4) = s_3(2) \quad \text{or} \quad \#X_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq s_4(t) \qquad (4.4.1)$$

Theorem 4.5 *Let $\mathcal{Q}$ be a hyperbolic quadric containing exactly two skew lines on the hermitian surface X. Then we have $\#X_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq s_4(t)$.*

Proof see appendix.

4.1 Table of the intersection of quadrics with the hermitian surface

Let us show in a table the geometrical structure of the intersection of quadrics with the hermitian surface.

Rank ($\mathcal{Q}$)	Description	Type
1	repeated plane	$1, 2$
2	line	$3, 4, 5$
2	pair of distinct planes	$6, 7, 8$
3	quadric cone	$9, 10$
4	hyperbolic quadric	$11, 12, 13, 14$
4	elliptic quadric	15

Type	Description
1	a tangent plane to X
2	a non-tangent plane to X
3	tangent to X
4	secant
5	a generator of X
6	two non-tangent planes to X
7	$\mathcal{P}_1$ is non-tangent to X and $\mathcal{P}_2$ is tangent to X

Type	Description
8	two tangent planes to X
9	no generartor in the cone
10	1 or 2 generators in the cone
11	3 skew generators in $\mathcal{R}$
12	2 skew generators $\mathcal{R}$
13	1 generator in $\mathcal{R}$
14	no generator in $\mathcal{R}$
15	elliptic quadric

4.2 Table of the weight distribution

Let us show in a table the quadrics (geometrical structure) with the corresponding weights associated to the codewords obtained from them. From the results of section 2 and those of section 5 [4], we have the following table.

Rank	Type	$\#X_{Z(\mathcal{Q})}(\mathbb{F}_q)$	$\#X_{Z(\mathcal{Q})}(\mathbb{F}_4)$	Weight over $\mathbb{F}_q$	Weight over $\mathbb{F}_4$
1	1	t^3+t^2+1	13	t^5	32
(repeated plane)	2	t^3+1	9	t^5+t^2	36
2	3	1	1	$t^5+t^3+t^2$	44
(line)	4	$t+1$	3	$t^5+t^3+t^2-t$	42
	5	t^2+1	5	t^5+t^3	40
2	6	$s_4(t)$	17	$t^5-t^3+t^2$	28
		$s_5(t)$	15	$t^5-t^3+t^2+t$	30
(pair of distinct planes)		$s_3(t)$	19	t^5-t^3+t	26
	7	$s_2(t)$	21	t^5-t^3	24
$\mathcal{Q}=\mathcal{P}_1\cup\mathcal{P}_2$		$s(t)$	23	$t^5-t^3-t^2+t$	22
	8	$s_2(t)$	21	t^5-t^3	24
3	9	$\leq t^3+t^2+t$ $+1<s_4(t)$	≤ 15	$\geq t^5-t$	$30\leq w\leq 44$
(cone)	10	t^3+t^2+1	13	t^5	32
		t^3+2t^2-t+1	15	t^5-t^2+t	30
	11	$s_2(t)$	21	t^5-t^3	24
4	12	$\leq t^3+3t^2-t$ $+1\leq s_3(t)$	≤ 19	$\geq t^5-t^3$	$26\leq w\leq 32$
(hyperbolic)	13	$\leq t^3+2t^2$ $+1\leq s_4(t)$	≤ 17	$\geq t^5-t^2$	$28\leq w\leq 36$
$\mathcal{H}(\mathcal{R},\mathcal{R}')$	14	$\leq t^3+t^2+$ $t+1<s_4(t)$	≤ 15	$\geq t^5-t$	$30\leq w\leq 40$
4		$\leq 2t^3+2t$		$\geq t^5-t^3+t^2$	
(elliptic)	15	$+2<s_2(t)$	≤ 17	$-2t-1$	$28\leq w\leq 45$

Note that, for the code $C_2(X)$ over $\mathbb{F}_4$, the codewords corresponding to quadrics of type.1 to type.14 have even weights. It has also been proved by Spurr (by a computer program) that $C_2(X)$ over $\mathbb{F}_4$ is an even weight code.

5 The third weight of the code $C_2(X)$

Theorem 5.1 *The third weight (for $t\neq 3$)of the code $C_2(X)$ is t^5-t^3+t*

Proof In fact when $\mathcal{Q}$ is a quadric not corresponding to the codewords of minimum weight and second weight, we get $\#X_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq s_3(t)$.

Note that in the case $t = 2$, we recover the third weight of the code $C_2(X)$ over $\mathbb{F}_4$ in agreement with [3] which is $2^5 - 2^3 + 2 = 26$.

Theorem 5.2 *The codewords of third weight (for $t \neq 3$) correspond to quadrics which are union of two planes, one tangent to the hermitian surface X, the second not tangent to X, and the line of intersection of the two planes intersects the hermitian surface in $t + 1$ points.*

Proof The codewords of third weight are not given by hyperbolic quadrics of type 12 in table 4.2 from theorem 4.5, nor by elliptic quadrics if $t \neq 3$.

We come now to the computation of the codewords of third weight.

Theorem 5.3 *The number of codewords of third weight (for $t \neq 3$) is:*

$$(t^2 - 1)(t^5 + t^3 + t^2 + 1)(t^6 - t^5)$$

Proof Let us write $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_2$, where:
– $\mathcal{P}_1$ is a tangent plane to the hermitian surface X at a point P_1,
– $\mathcal{P}_2$ is a non-tangent plane to the hermitian surface X ,
and $l = \mathcal{P}_1 \cap \mathcal{P}_2$ meets the hermitian surface in $t + 1$ points.
Given a fixed point P_1 in $\mathcal{P}_1$, there are exactly $q + 1$ lines passing through P_1 and contained in the same plane. We also know that in a plane, there pass exactly $q^2 + q + 1$ lines. We wish that the line l of intersection is not a generator, nor a tangent (the number of generators and tangent lines is $q + 1$). Thus, the remaining lines which number is $q^2 + q + 1 - (q + 1) = q^2$, is the number of possibilities we can choose the line l such that l intersects X at $t + 1$ points. For each line l, it pass exactly $q + 1$ planes $(\mathcal{P}_i)_{1 \leq i \leq q+1}$ (counting $\mathcal{P}_1$). Let us consider the q planes $(\mathcal{P}_i)_{2 \leq i \leq q+1}$; they are not all non-tangent to X (some of them are tangent to X). For a fixed point P_1, there are $q^2.q = q^3$ planes $\mathcal{P}_i$ constructed and these q^3 planes are all distinct. In total there are exactly $(t^5 + t^3 + t^2 + 1)q^3$ couples $(\mathcal{P}_1, \mathcal{P}_2)$, where $\mathcal{P}_1$ is a tangent plane to the hermitian surface X, $\mathcal{P}_2$ is a non-tangent plane to the hermitian surface X with $l = \mathcal{P}_1 \cap \mathcal{P}_2$ intersecting the hermitian surface at $t + 1$ points. We also know from the proof of theorem 6.5 [4] that $(t^5 + t^3 + t^2 + 1)t^5$ is the number of couples $(\mathcal{P}_1, \mathcal{P}_2)$ with $\mathcal{P}_1$ and $\mathcal{P}_2$ two tangent planes to the hermitian surface X, with the intersection line meeting X at $t + 1$ points. Thus, one deduces that $(t^5 + t^3 + t^2 + 1)(t^6 - t^5)$ is

the number of couples $(\mathcal{P}_1, \mathcal{P}_2)$ giving codewords of third weight. Therefore, there are $(t^2-1)(t^5+t^3+t^2+1)(t^6-t^5)$ codewords of third weight.

Observe that, for $t=2$, there are exactly $3 \times 45 \times 32 = 4320$ codewords of third weight in agreement with Spurr [3] p.120.

Remark 5.4 ***Conjecture on the fourth and fifth weight.***
The author has tried to study again $\#X_{Z(\mathcal{Q})}(\mathbb{F}_q)$ for $\mathcal{Q}$ an elliptic quadric and conjecture that $s_4(t)$, $s_5(t)$ should give respectively the fourth and the fifth weight. The codewords of fourth weight correspond now (for $t \geq 3$) to quadrics which are union of two non-tangent planes to X, and the line of intersection of the two planes meets X at a single point.
The codewords of fifth weight correspond (for $t > 3$) to quadrics which are union of two non-tangent planes to X, and the line of intersection of the two planes meets X in $t+1$ points.
Unfortunately no proof is found yet.

6 Appendix

Lemma 6.1 *Let $\bar{l}$ be a line defined over $\overline{\mathbb{F}}_q$ in $PG(3, \overline{\mathbb{F}}_q)$ and $l = \bar{l} \cap PG(3, \mathbb{F}_q)$. Then l is empty, or a single point or a line defined over $\mathbb{F}_q$.*

Proof It is a direct consequence of the equation of a line $PG(3,q)$.

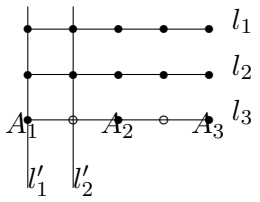
Let $\mathcal{Q}$ be a non-degenerate quadric over $\overline{\mathbb{F}}_q$. Note $d_i =$ degree of the curve $\mathcal{C}_i$ defined on $\mathcal{Q}$. From [9] (chap.4 example 2 p.241), we deduce an interesting relation between the arithmetical genus of a curve and its degree. Thus, we get the following result.

Proposition 6.2 *Let $\mathcal{Q} \subset \mathbb{P}^3$ be a non-singular quadric surface in $\mathbb{P}^3$ and $\mathcal{C}$ an irreducible curve on $\mathcal{Q}$.*
–If deg $\mathcal{C} = 2l+2$ then, $p_a(\mathcal{C}) \leq l^2 \quad (\star)$
–If deg $\mathcal{C} = 2l+1$ then, $p_a(\mathcal{C}) \leq l(l-1) \quad (\star\star)$

Let us recall the result of Yves Aubry and Marc Perret on the Weil theorem for singular curves, see [1]. With this result we get a bound for the number of rational points of any irreducible curve not necessary smooth.

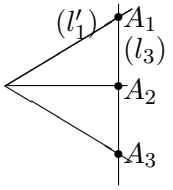
Proposition 6.3 *Let C be a reduced connected projective algebraic curve over a finite field $\mathbb{F}_q$, with r irreducible components and of arithmetical genus $p_a(C)$. Then $|\#C(\mathbb{F}_q) - (rq+1)| \leq 2p_a(C)\sqrt{q}$.*

Proof of theorem 4.5 From the relation 4.4.1 of remark 4.4, we need to prove that $\#X_{Z(\mathcal{Q})}(\mathbb{F}_4) \neq s_3(2)$. A hyperbolic quadric over $\mathbb{F}_4$ is a pair of two reguli, each regulus containing five skew lines. Let $\mathcal{R}$ be the regulus of $\mathcal{Q}$ containing the two skew lines l_1 and l_2 of the hermitian surface.

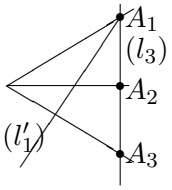


If each one of the remaining three lines of $\mathcal{R}$ is not secant to X (i.e. meets X at three points), then the problem is solved. Suppose now that there is a secant line. Let l_3 be a line of $\mathcal{R}$ secant to X; l_3 meets X at three points A_1, A_2 and A_3. Let us consider the five planes passing through l_3; each of them is tangent to the quadric $\mathcal{Q}$ (since $l_3 \cap X = \{A_1, A_2, A_3\} \subset H \cap \mathcal{Q}$). In fact, $H \cap \mathcal{Q}$ as a degenerate quadric of rank 2 in $PG(2, q)$, is a set of 2 lines from J.W.P.Hirschfeld [6] p.156. Thus, we can distinguish two cases: $H \cap \mathcal{Q} = \{l_3, l\}$ where l is a line of $\mathcal{Q}$ passing through one of the three points of $\{A_1, A_2, A_3\}$ or l does not meet any of the points A_1, A_2 and A_3. Without loss of generality, we may assume that $H \cap \mathcal{Q} = \{l_3, l'_1\}$ or $H \cap \mathcal{Q} = \{l_3, l'_2\}$.

First case: Suppose that $H \cap \mathcal{Q} = \{l_3, l'_1\}$
If H is tangent to X: In this case $H \cap X$ is a degenerate hermitian curve of rank 2 consisting of 13 points (a set of three lines meeting at a common point). But, two of the three points A_1, A_2 and A_3 can not be on a the same line of $H \cap X$, otherwise l_3 should be contained in X. So we get two eventualities:



(a) $l'_1 \subset H \cap X$



(b) $l'_1 \not\subset H \cap X$

(a) $l'_1 \subset H \cap X$: In this case, $\mathcal{Q}$ contains three lines of X among which two lines are in the same regulus and the third is in the complementary regulus. We can now write: $\mathcal{C} = \mathcal{Q} \cap X = l_1 \cup l_2 \cup l'_1 \cup \overline{C}$ (where $\overline{C}$ is a curve of degree 3 over $\overline{\mathbb{F}}_4$). If $\overline{C}$ is irreducible, it is defined on $\mathbb{F}_4$ and from proposition 6.2, we have $p_a(\overline{C}) = 0$ and therefore from proposition 6.3, we get $|\mathcal{Q} \cap X| \leq 18$. If $\overline{C}$ is not irreducible and since there is no plane conic on

X, we deduce that $\overline{C} = \overline{C}_1 \cup \overline{C}_2 \cup \overline{C}_2$ (union of three lines); at most one line among them should be defined over $\mathbb{F}_q$. Thus, from lemma 6.1 we deduce that $|\mathcal{Q} \cap X| \leq 18$.
(b) $l'_1 \not\subset H \cap X$: Here $l'_1 \cap H \cap X = 3$ points. So that $|H \cap X \cap \mathcal{Q}| \leq 5$.
If H is non-tangent to X: In this case, $H \cap X$ is a non-degenerate hermitian curve with $|H \cap X| = 9$. Here we need to distinguish two cases:
– If $l'_1 \subset H \cap X$, we recover the case which has been done previously.
– If $l'_1 \not\subset H \cap X$, then $|l \cap (H \cap X)| = 3$; so $|\mathcal{Q} \cap H \cap X| \leq 3 + 3 = 6$.

Second case: Suppose that $H \cap \mathcal{Q} = \{l_3, l'_2\}$
Similary, if H is tangent to X, then $H \cap X$ is a set of three lines meeting at a common point, thus $|\mathcal{Q} \cap H \cap X| \leq 6$. If H is non-tangent to X, then $H \cap X$ is a non-singular plane curve and therefore irreducible. Here $H \cap X$ does not contain the line l'_2, so l'_2 meets $H \cap X$ in exactly three points. Then $|\mathcal{Q} \cap H \cap X| \leq 6$.

Summary: *When $\mathcal{Q}$ is a hyperbolic quadric which regulus $\mathcal{R}$ contains exactly two skew lines of the hermitian surface X, $\mathcal{Q}$ should contains an other line l of X, in this case l is contained in the complementary regulus of $\mathcal{R}$ and then $|\mathcal{Q} \cap X| \leq 18$; or $|\mathcal{Q} \cap H_i \cap X| \leq 6$ for each one of the five planes $(H_i)_{1 \leq i \leq 5}$ passing through the line l_3, which leads to $|\mathcal{Q} \cap X| \leq 18$, therefore $|\mathcal{Q} \cap X| \in \{13, 15, 17\}$. This concludes the proof of theorem 4.5.*

Acknowledgment: The author would like to thank Mr F. Rodier whose remarks and patience encouraged him to work on the problem.

References

[1] Y. Aubry and M. Perret, On the characteristic polynomials of the Frobenuis endomorphism for projective curves over finite fields, Finite Fields and Theirs Applications 10, (2004), 412-431

[2] R. C. Bose and I. M Chakravarti, Hermitian varieties in finite projective space $PG(N, q)$. Canadian J. of Math.18 (1966), 1161-1182.

[3] I. M. Chakravarti, The generalized Goppa codes and related discrete designs from hermitian surfaces in $PG(3, s^2)$. Lecture Notes in computer Sci 311. (1986), 116-124.

[4] F. A. B. Edoukou, Codes defined by forms of degree 2 on hermitian surface and Sørensen conjecture. Finite Fields and Their Applications, Volume 13, Issue 3, (2007). 616-627.

[5] R. Hartshorne, Algebraic geometry, Graduate texts in mathematics 52, Springer-Verlag, 1977.

[6] J. W. P. Hirschfeld, Projective Geometries Over Finite Fields (Second Edition) Clarendon Press. Oxford 1998.

[7] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Clarendon press. Oxford 1985.
[8] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties; in "Arithmetic, Geometry, and Coding Theory". (Luminy, France, June 17-21, 1993), Walter de Gruyter, Berlin-New York (1996), 77-104.
[9] I. R. Shafarevich, Basic algebraic geometry 1, Springer-Verlag, 1994.
[10] A. B. Sørensen, Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes. Ph. D. Thesis, Aarhus, Denmark, 1991.
[11] P. P. Spurr, Linear codes over $GF(4)$. Master's Thesis, University of North Carolina at Chapell Hill, USA, 1986.

Chapitre 3

Codes defined by forms of degree 2 on quadric surfaces

Codes Defined By Forms Of Degree 2 On Quadric Surfaces

Frédéric A. B. Edoukou

***Abstract*—We study the functional codes $C_2(X)$ defined on projective varieties X, in the case where $X \subset \mathbb{P}^3(\mathbb{F}_q)$ is a 1-degenerate quadric or a non-degenerate quadric (hyperbolic or elliptic). We find the minimum distance of these codes, the second weight, and the third weight. We also show the geometrical structure of the first weight and second weight codewords. One result states that the codes $C_2(X)$ defined on the elliptic quadrics are good codes according to the table of A. E. Brouwer.**

***Index Terms*—Bézout's theorem, functional codes, quadrics, regulus, weight.**

I. Introduction

The code $C_2(X)$ over $\mathbb{F}_q$ where X is a quadric of $\mathbb{P}^n(\mathbb{F}_q)$ the projective space of dimension n has been studied by Y. Aubry [1]. In order to find the minimum distance of this code, Aubry determined some bounds for $N = |\mathcal{Q} \cap \mathcal{Q}'|$, the number of intersection points of two quadrics $\mathcal{Q}$ and $\mathcal{Q}'$ which are exactly known in the case where one of them is an hyperplane, the case both are proportionnal, and the case where the two quadrics have a common factor of degree 1. For the hyperplane section of a degenerate quadric, he rediscovered the earlier result of Swinnerton-Dyer [11] p.264. When the two quadrics have no common linear factor, he proved that:
$N \leq \pi_{n-2} + 7\frac{q^{n-1}}{q-1} - 6\frac{q^{n-2}}{q-1} \quad (q \geq 7)$. Thus, even in the case of $\mathbb{P}^3(\mathbb{F}_q)$, when the quadric surfaces X are 1-degenerate (cones), or non-degenerate (elliptic or hyperbolic) Aubry was not able to determine precisely the minimum distance of the code $C_2(X)$. His result leads to an upper bound:
$N \leq 2(4q+1) + \frac{1}{q-1}$ which is not the best possible. From the result of Lachaud [8] proposition 2.3, we deduce that this number of intersection points is bounded above by: $N \leq 4(q+1)$.
Aubry's result has been improved by D. B. Leep and L. M. Schueller [9] corollary 5.4 p.172 in the case, where the pair of quadrics cannot be written in a fewer number of variables: if $n+1 \geq 4$ and is even, then

$$N \leq (2q^{n-1} - q^{n-2} + 2q^{\frac{n+1}{2}} - 3q^{\frac{n-1}{2}} + q^{\frac{n-3}{2}} - 1)/(q-1).$$

Despite this improvement, the problem of the minimum distance of the code $C_2(X)$ in $\mathbb{P}^3(\mathbb{F}_q)$ is only solved for the hyperbolic quadric.
In this paper we find some bounds for the number of zeros of a pair of quadrics which are better than the ones known and we give the exact value of the minimum distance of the code $C_2(X)$ with X respectively a 1-degenerate quadric, or an elliptic quadric. For each one of the three types of quadrics mentioned above, we will determine the geometrical structure of the codewords reaching the first weight; we will compute the second and the third weight, and show the geometrical structure of codewords reaching the second weight. Let us note that the codes defined on the elliptic quadrics are good codes according to the table of Andries E. Brouwer [3].

Manuscript received November 25, 2005; revised

Frédéric A. B. Edoukou is with the Institut de Mathématiques de Luminy, CNRS, Luminy case 907 - 13288 Marseille Cedex 9 - France E.mail : edoukou@iml.univ-mrs.fr

TABLE I
Quadrics in $\mathbb{P}^3(\mathbb{F}_q)$

Rank	Description	$\lvert\mathcal{Q}\rvert$
1	repeated plane	q^2+q+1
2	pair of distinct planes	$2q^2+q+1$
2	line	$q+1$
3	quadric cone	q^2+q+1
4	hyperbolic quadric	$(q+1)^2$
4	elliptic quadric	q^2+1

II. Notations and terminology

We denote by $\mathbb{F}_q$ the field with q elements ($q \geq 3$). We use the term forms of degree two to describe homogeneous polynomials f of degree two, and $\mathcal{Q} = Z(f)$ the zeros of f in the projective space $\mathbb{P}^n(\mathbb{F}_q)$, is a quadric.
Let $\mathcal{Q}'$ be a quadric, the rank of $\mathcal{Q}'$ denoted $r(\mathcal{Q}')$, is the smallest number of indeterminates appearing in f' under any change of coordinate system. The quadric $\mathcal{Q}'$ is said to be degenerate if $r(\mathcal{Q}') < n+1$; otherwise it is non-degenerate. The quadrics of $\mathbb{P}^3(\mathbb{F}_q)$ fall into six orbits under $PGL(4,q)$ (see lemma 15.3.1 [6]). In [6] p.14 we have Table I of the quadrics in $\mathbb{P}^3(\mathbb{F}_q)$.
A regulus is the set of transversals of three skew lines in $\mathbb{P}^3(\mathbb{F}_q)$. It consists of $q+1$ skew lines. Thus, a hyperbolic quadric $\mathcal{Q}$ is a pair of complementary reguli ($\mathcal{Q} = \mathcal{R}_1 \cup \mathcal{R}_2$).
Let F be the vector space of forms of degree 2 with four variables, and $|X|$ the number of rational points over $\mathbb{F}_q$ of X. We denote by W_i the set of points with homogeneous coordinates $(x_0 : ... : x_3) \in \mathbb{P}^3(\mathbb{F}_q)$ such that $x_j = 0$ for $j < i$ and $x_i = 1$. The family $\{W_i\}_{0 \leq i \leq 3}$ is a partition of $\mathbb{P}^3(\mathbb{F}_q)$. The code $C_2(X)$ is the image of the linear map $c : F \longrightarrow \mathbb{F}_q^{|X|}$, defined by $c(\mathcal{Q}') = (c_x(\mathcal{Q}'))_{x \in X}$, where $c_x(\mathcal{Q}') = \mathcal{Q}'(x_0, ..., x_3)$ with $x = (x_0, ..., x_3) \in W_i$.

III. Some general theory

Now we will recall a general result on non-degenerate quadric surface which can be found in [10] pp.241-243.
Let $\mathcal{Q}$ be a non-degenerate quadric over $\mathbb{F}_q$ and $\mathcal{Q}'$ an other quadric. We denote by $\overline{\mathcal{Q}}$ the points on $\overline{\mathbb{F}}_q$ of the quadric $\mathcal{Q}$

defined over $\mathbb{F}_q$. Let us write $\mathcal{C} = \overline{\mathcal{Q}} \cap \overline{\mathcal{Q}}'$ and $\overline{\mathcal{C}} = \bigcup_{1 \leq i \leq t} \overline{C}_i$ the decomposition of $\mathcal{C}$ in irreducible components over $\overline{\mathbb{F}}_q$. Note d_i=degree of $\overline{C}_i$. Since $\overline{\mathcal{Q}}$ is non-degenerate, then $\overline{\mathcal{Q}}$ is isomorphic to $\mathbb{P}_1 \times \mathbb{P}_1$ on $\overline{\mathbb{F}}_q$ (see [10] chap.4 example 2 p.241). The curve $\overline{C}_i$ defines a divisor which we denote again $\overline{C}_i$ on the non-singular quadric $\overline{\mathcal{Q}}$. The divisor class group of $\overline{\mathcal{Q}}$, denoted by $Cl\overline{\mathcal{Q}}$ is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$. Note (m, n) the class of $\overline{C}_i$. The degree and the arithmetical genus of $\overline{C}_i$ are such that:

$$\deg \overline{C}_i = m + n \quad (3.1) \qquad p_a(\overline{C}_i) = (m-1)(n-1) \quad (3.2)$$

When $\overline{C}_i$ is a line, we get deg $\overline{C}_i = 1$ and $p_a(\overline{C}_i) = 0$. Except in the case $\overline{C}_i$ is a line, any irreducible curve has $m > 0$, $n > 0$. Using the two relations (3.1) and (3.2) we get an interesting relation between the arithmetical genus of a curve and its degree. Thus we get the following result.

Proposition 3.1: Let $\mathcal{Q} \subset \mathbb{P}^3(\mathbb{F}_q)$ be a non-singular quadric surface and $\overline{C}_i$ an irreducible curve on $\overline{\mathcal{Q}}$.
–If deg $\overline{C}_i = 2l + 2$ then, $p_a(\overline{C}_i) \leq l^2 \quad (\star)$
–If deg $\overline{C}_i = 2l + 1$ then, $p_a(\overline{C}_i) \leq l(l-1) \quad (\star\star)$

Lemma 3.2: Let $\bar{l}$ be a line defined over $\overline{\mathbb{F}}_q$ in $\mathbb{P}^3(\overline{\mathbb{F}}_q)$ and $l = \bar{l} \cap \mathbb{P}^3(\mathbb{F}_q)$. Then l is empty, or a single point or a line defined over $\mathbb{F}_q$.

Proof: It is obvious. ∎

Lemma 3.3: Let $\overline{\mathcal{C}} = \bigcup_{1 \leq i \leq t} \overline{C}_i$ be the decomposition of a curve $\mathcal{C} \subset \mathbb{P}^n(\overline{\mathbb{F}}_q)$ into irreducible components over $\overline{\mathbb{F}}_q$ and $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Then $\sigma(\overline{C}_i)$ and $\overline{C}_i$ have the same degree. If $\overline{C}_i$ is the only component of degree d_i, then $\overline{C}_i$ is defined over $\mathbb{F}_q$.

Proof: Let H and H' be hyperplanes of $\mathbb{P}^n(\overline{\mathbb{F}}_q)$; deg $\sigma(\overline{C}_i) = \max_{H' \not\supset \sigma(\overline{C}_i)} |\sigma(\overline{C}_i) \cap H'| = \max_{\sigma^{-1}(H') \not\supset \overline{C}_i} |\sigma(\overline{C}_i \cap \sigma^{-1}(H')| = \max_{H \not\supset \overline{C}_i} |\sigma(\overline{C}_i \cap H| = \max_{H \not\supset \overline{C}_i} |\overline{C}_i \cap H|$= deg $\overline{C}_i$. The second assertion of the lemma comes from the fact that $\{\overline{C}_i\}_{1 \leq i \leq t}$ are conjugate under Gal$(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. ∎

Let us recall the result of Yves Aubry and Marc Perret on the Weil theorem for singular curves, see [2] pp.415-418. With this result we get a bound for the number of rational points of any irreducible curve not necessary smooth.

Proposition 3.4: Let C be a reduced connected projective algebraic curve over a finite field $\mathbb{F}_q$, with r irreducible components and of arithmetical genus $p_a(C)$. Then

$$|\#C(\mathbb{F}_q) - (rq + 1)| \leq 2p_a(C)\sqrt{q}$$

In [5] p.229, we have the following result.

Proposition 3.5: Let $\overline{C} \subset \mathbb{P}^n(\overline{\mathbb{F}}_q)$ be an irreducible curve which does not lie in any hyperplane. Then deg $\overline{C} \geq n$.

IV. Intersection of two quadrics in $\mathbb{P}^3(\mathbb{F}_q)$

The quadrics of $\mathbb{P}^2(\mathbb{F}_q)$ fall in four orbits under $PGL(3, q)$ (see Theorem 7.4 [7]). In [7], we have the following table of quadrics in $\mathbb{P}^2(\mathbb{F}_q)$.

TABLE II
Quadrics $\mathcal{Q}$ in $\mathbb{P}^2(\mathbb{F}_q)$

Rank	Description	$\lvert\mathcal{Q}\rvert$
1	repeated line	$q+1$
2	pair of distinct lines	$2q+1$
2	point	1
3	conic	$q+1$

A. Plane Sections Of Quadrics

We have the following result which can be found in [1] p.7.

Proposition 4.1: Let $\mathcal{Q}$ be a non-degenerate quadric in $\mathbb{P}^3(\mathbb{F}_q)$ and H a plane. Then:
(i) If H is tangent to $\mathcal{Q}$, then $\mathcal{Q} \cap H$ is a degenerate quadric of rank 2 in $\mathbb{P}^2(\mathbb{F}_q)$.
(ii) If H is not tangent to $\mathcal{Q}$, then $\mathcal{Q} \cap H$ is a conic in $\mathbb{P}^2(\mathbb{F}_q)$.

From this proposition, we deduce that for any plane section of a non-degenerate quadric $\mathcal{Q}$ in $\mathbb{P}^3(\mathbb{F}_q)$, we get $|\mathcal{Q} \cap H| \leq 2q + 1$. We also have the same upper bound for a cone, since three of its $q + 1$ lines are not coplanar.

B. Intersection Of A Non-degenerate Quadric With A Pair Of Distinct Planes

Let $\mathcal{Q}$ be an hyperbolic quadric. The lines fall in four classes: the set of generators, tangents, bisecants, and lines skew to $\mathcal{Q}$. For $\mathcal{Q}$ elliptic, there is no generator. The two planes meet at a line denoted by l. There are two types of planes with respect to $\mathcal{Q}$: the tangent planes, and the non-tangent planes (those meeting $\mathcal{Q}$ in a conic). Thus the two planes have the three following configurations:

1) each plane is tangent to $\mathcal{Q}$: For $\mathcal{Q}$ hyperbolic, there is no line skew to $\mathcal{Q}$ in each tangent plane; there are only tangent lines, bisecants or generators. However for a fixed tangent line, there is only one tangent plane passing through it. Thus only bisecants and generators are intersection of two tangent planes. Therefore we get $|\mathcal{Q} \cap \mathcal{Q}'| = 4q$ or $|\mathcal{Q} \cap \mathcal{Q}'| = 3q + 1$ according to l is a bisecant or a generator. For $\mathcal{Q}$ elliptic, in each tangent plane there is no bisecant, there are only tangent lines and lines skew to $\mathcal{Q}$. However for any tangent line, there is only one tangent plane passing through it. Thus only lines skew to $\mathcal{Q}$ are intersection of two tangent planes. Therefore, we get $|\mathcal{Q} \cap \mathcal{Q}'| = 2$.

2) one of the plane is tangent and the second is non-tangent to $\mathcal{Q}$: For $\mathcal{Q}$ hyperbolic, l is either a tangent or a bisecant; and this gives respectively $|\mathcal{Q} \cap \mathcal{Q}'| = 3q + 1$, or $|\mathcal{Q} \cap \mathcal{Q}'| = 3q$. For $\mathcal{Q}$ elliptic, l is either a tangent line or skew to $\mathcal{Q}$; thus we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq q + 2$.

3) each one of the two planes is non-tangent to $\mathcal{Q}$: In this case the line l is not a generator; l is tangent, bisecant or skew to $\mathcal{Q}$, this give respectively $|\mathcal{Q} \cap \mathcal{Q}'| = 2q + 1$, $|\mathcal{Q} \cap \mathcal{Q}'| = 2q$ or $|\mathcal{Q} \cap \mathcal{Q}'| = 2(q + 1)$.

C. Intersection Of A Cone With A Pair Of Distinct Planes

Let $\mathcal{Q}$ be a quadric cone. We know from [6] p.14 that there are four types of planes with respect to $\mathcal{Q}$: the set of tangent planes, planes through a pair of generators, planes through the vertex S containing no generator, planes meeting $\mathcal{Q}$ in a conic. The lines fall in six classes:
$\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_1^+ \cup \mathcal{L}_1^- \cup \mathcal{L}_2^+ \cup \mathcal{L}_2^- \cup \mathcal{L}_3$ when q is odd.
$\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_1' \cup \mathcal{L}_1'' \cup \mathcal{L}_2^+ \cup \mathcal{L}_2^- \cup \mathcal{L}_3$ when q is even
and where $\mathcal{L}_3$, $\mathcal{L}_1$, $\mathcal{L}_1^+$, $\mathcal{L}_1^-$, $\mathcal{L}_2^+$, $\mathcal{L}_2^-$, $\mathcal{L}_1'$ and $\mathcal{L}_1''$ are respectively the set of generators, the set tangents at the simple points (excluding the generators), external vertex tangents which are intersection of pairs of tangent planes, internal vertex tangents which are the remaining lines of $\mathcal{Q}$ through S, the set of bisecants of $\mathcal{Q}$, the set of lines skew to $\mathcal{Q}$, the nuclear line, and the set of lines through S which are neither generators nor the nuclear line.
Let $\mathcal{Q}' = H_1 \cup H_2$, where H_1, H_2 are two distinct planes and $l = H_1 \cap H_2$. Thus, $|\mathcal{Q} \cap \mathcal{Q}'|$ takes the following values:
(i) $|\mathcal{Q} \cap \mathcal{Q}'| = 4q+1$, if each plane contains a pair of generators with $l \in \mathcal{L}_1''$ for q even, or $l \in \mathcal{L}_1^+$, $l \in \mathcal{L}_1^-$ for q odd. For example, for q odd, the cone defined by $f_1 = x_0^2 + x_1^2 - x_2^2$ and $f_2 = x_0 x_1$ have exactly $4q+1$ common points.
(ii) $|\mathcal{Q} \cap \mathcal{Q}'| = 3q+1$, if each plane contains a pair of generators with $l \in \mathcal{L}_3$, or one of the two planes is tangent to $\mathcal{Q}$ and the second plane contains a pair of generators with $l \in \mathcal{L}_1^+$ or $l \in \mathcal{L}_1''$
(iii) $|\mathcal{Q} \cap \mathcal{Q}'| \leq 3q$, otherwise.

D. Some Line Sections Of Quadrics

1) Section of Quadrics By A Quadric $\mathcal{Q}$ Of Rank 2 And $\mathcal{Q}$ Is A Line: It is obvious that $|\mathcal{Q} \cap \mathcal{Q}'| \leq |\mathcal{Q}|$, therefore $|\mathcal{Q} \cap \mathcal{Q}'| \leq q+1$.

2) Intersection Of An Elliptic Quadric With A Cone Or A Hyperbolic Quadric: Since there is no line in the elliptic quadric $\mathcal{Q}$, and each of the $q+1$ lines of the cone, or of one regulus meets $\mathcal{Q}$ in at most two points, we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq 2(q+1)$.

3) Intersection Of A Cone And A Hyperbolic Quadric: We will distinguish two cases according to this intersection contains a line or not.
–If $\mathcal{Q}$ and $\mathcal{Q}'$ have no common line: we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq 2(q+1)$.
–if $\mathcal{Q}$ and $\mathcal{Q}'$ have at least one common line: from the study of the hyperbolic quadric in [6] pp.23-26, we have the following result.

Proposition 4.2: If C is any point in $\mathcal{Q}'$, there pass exactly two generators (i.e. lines lying in $\mathcal{Q}'$) which constitute the intersection with $\mathcal{Q}'$ of the tangent plane at C. And through C, there pass $q+1$ lines lying in the tangent plane at C, among them 2 are generators. The remaining $q-1$ lines through C, which lie in the tangent plane meet $\mathcal{Q}'$ only in the single point C (there are called tangents to $\mathcal{Q}'$). Each of the q^2 lines passing through C and not contained in the tangent plane at C intersects $\mathcal{Q}'$ in exactly two points, one of which is C (such lines are called bisecants to $\mathcal{Q}'$).
From this proposition, on the hyperbolic quadric $\mathcal{Q}'$, we can assert first of all that the maximum number of generators the cone $\mathcal{Q}$ can contain is 2. Secondly, if we suppose that the remaining $q-1$ lines of the cone passing through the vertex S are all bisecants to $\mathcal{Q}'$, we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq 3q$.

4) Intersection of two cones: Let $\mathcal{C} = \mathcal{Q} \cap \mathcal{Q}'$; since the degrees of $\mathcal{Q}$ and $\mathcal{Q}'$ are 2 and 2, from the Bézout theorem [5] p.227, $\mathcal{C}$ contains at most 4 lines.
–if $\mathcal{Q}$ and $\mathcal{Q}'$ have no common line, each one of the $q+1$ lines of the cone $\mathcal{Q}'$ meeting $\mathcal{Q}$ in at most two points, we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq 2(q+1)$.
–if $\mathcal{Q}$ and $\mathcal{Q}'$ have exactly one common line, each one of the remaining q lines of $\mathcal{Q}'$ meets $\mathcal{Q}$ in at most two points (the vertex of the cone is one of the two points). Therefore, we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq (q+1) + q(2-1)$; thus $|\mathcal{Q} \cap \mathcal{Q}'| \leq 2q+1$.
–if $\mathcal{Q}$ and $\mathcal{Q}'$ have exactly two common lines, each one of the remaining $q-1$ lines of $\mathcal{Q}'$ meets $\mathcal{Q}$ in at most two points, we deduce that $|\mathcal{Q} \cap \mathcal{Q}'| \leq 3q$.
–if $\mathcal{Q}$ and $\mathcal{Q}'$ have at least three common lines: from lemma 3.3, we deduce that $\mathcal{Q}$ and $\mathcal{Q}'$ have exactly four common lines; thus we get $|\mathcal{Q} \cap \mathcal{Q}'| = 4q+1$.

E. Intersection Of Two Non-degenerate Quadrics Of The Same Type

From the result of D. B. Leep and L. M. Schueller [9] p.172 which gives an interesting upper bound for the number N of intersection points of a pair of quadrics in the affine space, we deduce the following consequence.

Proposition 4.3: Let $\{g, h\}$ be a pair of quadratic forms defined over $\mathbb{F}_q$ in $n+1$ variables with g non-degenerate, and $\mathcal{Q} = Z(g)$, $\mathcal{Q}' = Z(h)$ the corresponding quadrics in $\mathbb{P}^n(\mathbb{F}_q)$. If $n+1 \geq 4$ and is even, then:
$N \leq (2q^{n-1} - q^{n-2} + 2q^{\frac{n+1}{2}} - 3q^{\frac{n-1}{2}} + q^{\frac{n-3}{2}} - 1)/(q-1)$.

From this result, we deduce that in $\mathbb{P}^3(\mathbb{F}_q)$ the intersection of a non-degenerate quadric (hyperbolic, or elliptic) with any quadric is always less than $4q$. D. B. Leep and L. M. Schueller have found some pair of quadrics from which the upper bound is reached. Their example includes a case where one of the quadric is hyperbolic. Unfortunately for the elliptic quadric in $\mathbb{P}^3(\mathbb{F}_q)$ they didn't find an example; so the problem of the minimum distance of the code $C_2(X)$ defined on the elliptic quadric remains still unresolved. In what follows, we will study the section of two non-degenerate quadrics of the same type in order to improve the result of D. B. Leep and L. M. Schueller.

1) Intersection Of Two Hyperbolic Quadrics: Let $\mathcal{C} = \overline{\mathcal{Q}} \cap \overline{\mathcal{Q}}'$, $\mathcal{C}$ is a curve of degree less than 4 from the Bézout theorem [5] p.227. Therefore $\mathcal{C}$ contains at most 4 lines.
(i) If $\mathcal{Q}$ and $\mathcal{Q}'$ have at most one common line: Let us consider the regulus $\mathcal{R}_1$ which does not contain the common line. Each one of the $q+1$ lines of $\mathcal{R}_1$ meets $\mathcal{Q}$ in at most two points. Therefore, we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq 2(q+1)$.

(ii) If $\mathcal{Q}$ and $\mathcal{Q}'$ have exactly two common lines, we get two cases:
–the two lines are in the same regulus; since there is no intersection line in the complementary regulus, we deduce that $|\mathcal{Q} \cap \mathcal{Q}'| = 2(q+1)$.
–the two lines are in distinct regulus $\mathcal{R}_1$ and $\mathcal{R}_2$; we can consider only the regulus $\mathcal{R}_1$. Each one of the remaining q lines of the regulus $\mathcal{R}_1$ meets $\mathcal{Q}'$ in at most two points; we deduce that $|\mathcal{Q} \cap \mathcal{Q}'| \leq 3q+1$.
(iii) If $\mathcal{Q}$ and $\mathcal{Q}'$ have at least three common lines: From lemma 3.3, we deduce that $\mathcal{Q}$ and $\mathcal{Q}'$ have exactly four common lines. In this way we get the three following configurations:
–the four lines are in the same regulus,
–three lines on a regulus and the fourth in the complementary regulus,
–two lines in each regulus.
We know that in $\mathbb{P}^3(\mathbb{F}_q)$ the number of lines meeting 3 skew lines is $q+1$; and these $q+1$ lines are also skew. Since the hyperbolic quadric is a pair of complementary reguli, one concludes that if two hyperbolic quadrics have at least 3 skew lines in common, then they are identical. Therefore the last configuration is for interest. Let us note that the two first configurations can be eliminated from the result of D. B. Leep and L. M. Schueller. We deduce that $|\mathcal{Q} \cap \mathcal{Q}'| = 4q$. For example the two hyperbolic quadrics defined by the polynomials $f_1 = x_0x_1 + x_2x_3$ and $f_2 = x_3x_0 + x_1x_2$ have exactly four common lines for q odd.

2) Intersection Of Two Elliptic Quadrics: Let $\mathcal{C} = \overline{\mathcal{Q}} \cap \overline{\mathcal{Q}}'$, $\mathcal{C}$ is a curve of degree less than 4 from the Bézout theorem [5] p.227. Let $\overline{\mathcal{C}} = \bigcup_{1 \leq i \leq t} \overline{C}_i$ the decomposition of $\mathcal{C}$ in irreducible components, where $\overline{C}_i$ are defined over $\overline{\mathbb{F}}_q$ and $C_i = \overline{C}_i \cap \mathbb{P}^3(\mathbb{F}_q)$. Note d_i=degree of $\overline{C}_i$ then $\sum_{1 \leq i \leq t} d_i = d$. Without loss of generality we can assume that $d = 4$. Thus we get the five following configurations:

(i) $t = 1$: here $\overline{\mathcal{C}}$ is an irreductible curve of degree 4 defined over $\mathbb{F}_q$ from lemma 3.3, and from part ($\star$) of proposition 3.1 we get $p_a(\mathcal{C}) \leq 1$. Thus we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq 1 + q + 2\sqrt{q}$.

(ii) $t = 2$ with $d = 1 + 3$: this case is impossible; in fact from lemma 3.3 there is a common line defined over $\mathbb{F}_q$ in the two elliptic quadrics.

(iii) $t = 3$: here $\overline{\mathcal{C}} = \bar{l}_1 \cup \bar{l}_2 \cup \overline{C}_3$, where $\bar{l}_1$ and $\bar{l}_2$ are lines and $\overline{C}_3$ is a curve of degree 2 defined over $\overline{\mathbb{F}}_q$. From lemma 3.2, since there is no line on the elliptic quadric, we get that l_1 and l_2 contain each one at most one point over $\mathbb{F}_q$. The curve $\overline{C}_3$ is also defined over $\mathbb{F}_q$ and from part ($\star$) of proposition 3.1, $p_a(\overline{C}_3) = 0$ so that $|\overline{C}_3(\mathbb{F}_q)| \leq 1 + q$. Therefore we get $|\mathcal{Q} \cap \mathcal{Q}'| \leq q + 3$.

(iv) $t = 4$: here $\overline{\mathcal{C}} = \bar{l}_1 \cup \bar{l}_2 \cup \bar{l}_3 \cup \bar{l}_4$ with $\bar{l}_1$, $\bar{l}_2$, $\bar{l}_3$ and $\bar{l}_4$ lines defined over $\overline{\mathbb{F}}_q$. From lemma 3.2, we get that $|\mathcal{Q} \cap \mathcal{Q}'| \leq 4$.

(v) $t = 2$ with $d = 2 + 2$: here $\overline{\mathcal{C}} = \overline{C}_1 \cup \overline{C}_2$, where $\overline{C}_1$ and $\overline{C}_2$ are curves of degree 2. Let $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, then $\sigma(\overline{\mathcal{C}}) = \overline{\mathcal{C}}$; $\sigma(\overline{C}_1) \subset \overline{\mathcal{C}}$, therefore $\sigma(\overline{C}_1) = \overline{C}_1$ or $\sigma(\overline{C}_1) = \overline{C}_2$; thus we get two cases:
–(a) $\sigma(\overline{C}_1) = \overline{C}_1$ and $\sigma(\overline{C}_2) = \overline{C}_2$: in this case the two curves $\overline{C}_1$ and $\overline{C}_2$ are defined over $\mathbb{F}_q$. Therefore for $i = 1, 2$, we get $|C_i(\mathbb{F}_q)| \leq 1 + q + 2p_a(C_i)\sqrt{q}$ with $p_a(C_i) = 0$ from proposition 3.1. Hence $|\mathcal{Q} \cap \mathcal{Q}'| \leq 2(q+1)$.
–(b) $\sigma(\overline{C}_1) = \overline{C}_2$ and $\sigma(\overline{C}_2) = \overline{C}_1$: here we get $\sigma^2(\overline{C}_1) = \overline{C}_1$ and $\sigma^2(\overline{C}_2) = \overline{C}_2$; thus we can assert that $\overline{C}_1$ and $\overline{C}_2$ are defined over $\mathbb{F}_{q^2}$. We will use an analogous technique as the one used in [4] p.221. Let us remark that:

$$C_1 = \sigma(\overline{C}_1 \cap \mathbb{P}^3(\mathbb{F}_q)) = \sigma(\overline{C}_1) \cap \sigma(\mathbb{P}^3(\mathbb{F}_q)) = C_2$$
$$\text{and} \quad \overline{\mathcal{C}} \cap \mathbb{P}^3(\mathbb{F}_q) = C_1.$$

From proposition 3.5, $\overline{C}_1$ is a plane curve therefore it is defined by an irreductible form over $\mathbb{F}_{q^2}$. The curve $\overline{C}_1$ is defined by $f(x,y,z) = \sum f_{ijk}x^iy^jz^k$ with $f_{ijk} \in \mathbb{F}_{q^2}$. Let $\{1, \alpha\}$ be a $\mathbb{F}_q$-base of $\mathbb{F}_{q^2}$: $f_{ijk} = r_{ijk} + \alpha s_{ijk}$ where r_{ijk} and s_{ijk} belong in $\mathbb{F}_q$. We can now write $f(x,y,z) = R(x,y,z) + \alpha T(x,y,z)$ where $R(x,y,z) = \sum r_{ijk}x^iy^jz^k$ and $T(x,y,z) = \sum s_{ijk}x^iy^jz^k$. Let us denote by $Z_{\mathbb{F}_q}(G)$ the set of zeros of the polynomial G in the projective space $\mathbb{P}^2(\mathbb{F}_q)$. In this way we get: $C_1 = Z_{\mathbb{F}_q}(R) \cap Z_{\mathbb{F}_q}(T)$ which gives $|C_1| = |Z_{\mathbb{F}_q}(R) \cap Z_{\mathbb{F}_q}(T)|$. Since there is no line in the elliptic quadric, we deduce that there is no line in $Z_{\mathbb{F}_q}(R) \cap Z_{\mathbb{F}_q}(T)$ and finally $|C_1| \leq q + 1$.
Thus, in this case we have $|\mathcal{Q} \cap \mathcal{Q}'| \leq q + 1$.

V. Codes $C_2(X)$ defined on the quadric cones

Here X denotes a cone quadric. The additional hypothesis in [9] on the order of the pair of quadrics could not be satisfied. We apply the results of IV. (A, C, D) to determine the parameters of the functional code $C_2(X)$ defined on the cone quadric. Thus, we get the following results.

Proposition 5.1: Let $\mathcal{Q}'$ be a quadric in $\mathbb{P}^3(\mathbb{F}_q)$ and X the quadric cone. We have:

$$|X \cap \mathcal{Q}'| = 4q + 1, 3q + 1 \quad \text{or} \quad |X \cap \mathcal{Q}'| \leq 3q$$

Theorem 5.2: The code $C_2(X)$ defined on the quadric cone X is an $[n, k, d]_q$- code with:

$$n = q^2 + q + 1, \quad k = 9, \quad d = q(q-3)$$

The weight structure of the code $C_2(X)$ is as follows:
The minimum weight codewords correspond to:
– quadrics which are union of two planes passing through a pair of generators and the line of intersection of the two planes intersects the cone at a singhe point,
– quadrics cone containing exactly four lines of X.
The second weight is $w_2 = q(q-2)$ and the corresponding codewords are given by:
– quadrics which are union of two planes, each passing through a pair of generators and the line of intersection of the two planes is a generator,
– quadrics which are union of two planes, one tangent to the

cone and the second passing through a pair of generators and the line of intersection of the two planes $l \in \mathcal{L}_1^+$ or $l \in \mathcal{L}_1''$. The third weight is $w_3 = (q-1)^2$.

VI. Codes $C_2(X)$ defined on non-degenerate quadrics

Here X denotes a non-degenerate quadric. Since the parameters of the code $C_2(X)$ vary according to the type of the quadric X, we need to distinguish two cases: hyperbolic quadrics and elliptic quadrics.

A. The Parameters Of The Codes $C_2(X)$ Defined On Hyperbolic Quadrics

As previously indicated, the upper bound in [9] p.172 is optimal in this case; it gives the minimum distance. In the other hand it can not describe more than the first weight; this can be done by applying the results of IV. (A-B, D.1-3, E.1). Thus, we have the following results.

Proposition 6.1: Let $\mathcal{Q}'$ be a quadric in $\mathbb{P}^3(\mathbb{F}_q)$ and X a hyperbolic quadric. We have:

$$|X \cap \mathcal{Q}'| = 4q, 3q+1 \quad \text{or} \quad |X \cap \mathcal{Q}'| \leq 3q$$

Theorem 6.2: The code $C_2(X)$ defined on the hyperbolic quadric X is an $[n,k,d]_q$- code with:

$$n = (q+1)^2, \quad k = 9, \quad d = (q-1)^2$$

The weight structure of the code $C_2(X)$ is as follows:
The minimum weight codewords correspond to:
– quadrics which are union of two tangent planes to X and the line of intersection of the two planes intersects the hyperbolic quadric at two points,
– hyperbolic quadrics containing exactly four lines of X with two lines in each regulus of X.
The second weight is $w_2 = q^2 - q$ and the corresponding codewords are given by:
– quadrics which are union of two tangent planes to X and the line of intersection of the two planes is a generator of X,
– quadrics which are union of a tangent plane, and a non-tangent plane to X, and the line of intersection of the two planes is tangent to X,
– hyperbolic quadrics containing exactly two generators of X in distinct reguli and the remaining q lines of one regulus are all bisecants to X.
The third weight is $w_3 = q^2 - q + 1$.

B. The Parameters Of The Codes $C_2(X)$ Defined On Elliptic Quadrics

Here the upper bound from the result of D. B. Leep and L. M. Schueller is not the best possible; it cannot give the minimum distance. The minimum distance and the firsts weights of the code $C_2(X)$, can exactly be determined by a straight application of IV. (A-B, D.1-2 and E.2). Thus, we get the following results.

Proposition 6.3: Let $\mathcal{Q}'$ be a quadric in $\mathbb{P}^3(\mathbb{F}_q)$ and X an elliptic quadric. We have:

$$|X \cap \mathcal{Q}'| = 2(q+1), 2q+1 \quad \text{or} \quad |X \cap \mathcal{Q}'| \leq 2q$$

Theorem 6.4: The code $C_2(X)$ defined on the elliptic quadric X is an $[n,k,d]_q$- code with:

$$n = q^2+1, \quad k = 9, \quad d = q^2 - 2q - 1.$$

The weight structure of the code $C_2(X)$ is as follows:
The minimum codewords correspond to:
– quadrics which are union of two non-tangent planes to X and the line of intersection of the two planes is skew to X,
– quadrics cones which vertex doesn't lie on X, and all its $q+1$ lines are bisecants to X,
– hyperbolic quadrics with all the $q+1$ lines of a regulus are bisecants to X.
The second and third weights are respectively $w_2 = q(q-2)$, $w_3 = (q-1)^2$.

Remark 6.5: These functional codes $C_2(X)$ defined on the elliptic quadrics are good codes according to the table of Andries E. Brouwer [3].
In fact, for $q = 3, 4, 5, 7, 8, 9$ we get respectively the following codes: $[10, 9, 2]_3$- code, $[17, 9, 7]_4$- code, $[26, 9, 14]_5$- code, $[50, 9, 34]_7$- code, $[65, 9, 47]_8$- code, $[82, 9, 62]_9$- code.

Acknowledgment

The author would like to thank Mr F. Rodier and Mr. D. B. Leep. Theirs remarks and comments encouraged him to work on the problem.

References

[1] Y. Aubry, Reed-Muller codes associated to projective algebraic varieties. In "Coding Theory and Algebraic Geometry and Coding Theory ". (Luminy, France, June 17-21, 1991). Lecture Notes in Math., Vol. 1518 Springer-Verlag, Berlin, (1992), 4-17.

[2] Y. Aubry and M. Perret, On the characteristic polynomials of the Frobenuis endomorphism for projective curves over finite fields, Finite Fields and Theirs Applications 10, (2004), 412-431

[3] A. E. Brouwer, Bounds on minimum distance of linear codes, htpp://www.win.tue.nl/
˜aeb/voorlincod.html

[4] J. P. Cherdieu and R. Rolland, On the number of points of some hypersurface in $\mathbb{F}_q^n$, Finite Fields and Their Applications 2, (1996), 214-224.

[5] J. Harris, Algebraic Geometry (A first course), Graduate texts in mathematics 133, Springer-Verlag.

[6] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Clarendon press. Oxford 1985.

[7] J. W. P. Hirschfeld, Projective Geometries Over Finite Fields (Second Edition) Clarendon Press. Oxford 1998.

[8] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties; in " Arithmetic, Geometry, and Coding Theory " . (Luminy, France, 1993), Walter de Gruyter, Berlin-New York, (1996), 77-104.

[9] D. B. Leep and L. M. Schueller, Zeros of a pair of quadric forms defined over finite field. Finite Fields and Their Applications 5, (1999), 157-176.

[10] I. R. Shafarevich, Basic algebraic geometry 1, Springer-Verlag, 1994.

[11] H. P. F. Swinnerton-Dyer, Rational zeros of two quadratic forms, Acta Arithmetica 9 (1964), 261-270.

Chapitre 4

Codes defined by forms of degree 2 on quadric and non-degenerate hermitian varieties in $\mathbb{P}^4(\mathbb{F}_q)$

Codes defined by forms of degree 2 on quadric and non-degenerate hermitian varieties in $\mathbb{P}^4(\mathbb{F}_q)$

Frédéric A. B. Edoukou

CNRS, Institut de Mathématiques de Luminy
Luminy case 907 - 13288 Marseille Cedex 9 - France
E.mail : edoukou@iml.univ-mrs.fr

Abstract

We study the functional codes of second order defined by G. Lachaud on $\mathcal{X} \subset \mathbb{P}^4(\mathbb{F}_q)$ a quadric of rank($\mathcal{X}$)=3,4,5 or a non-degenerate hermitian variety. We give some bounds for the number of points of quadratic sections of $\mathcal{X}$, which are the best possible and show that codes defined on non-degenerate quadrics are better than those defined on degenerate quadrics. We also show the geometric structure of the minimum weight codewords and estimate the second weight of these codes. For $\mathcal{X}$ a non-degenerate hermitian variety, we list the first five weights and the corresponding codewords. The paper ends with two conjectures. One on the minimum distance for the functional codes of order h on $\mathcal{X} \subset \mathbb{P}^4(\mathbb{F}_q)$ a non-singular hermitian variety. The second conjecture on the distribution of the codewords of the first five weights of the functional codes of second order on $\mathcal{X} \subset \mathbb{P}^N(\mathbb{F}_q)$ the non-singular hermitian variety.

Keywords: functional codes, hermitian surface, hermitian variety, hermitian curve, quadric, weight.

Mathematics Subject Classification: 05B25, 11T71, 14J29

1 Introduction

We study the codes $C_2(\mathcal{X})$ defined on the quadric $\mathcal{X}$ and on the non-singular hermitian variety $\mathcal{X} : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} + x_4^{t+1} = 0$ in $\mathbb{P}^4(\mathbb{F}_q)$ with

$q = t^2$ (t is a prime power).
When $\mathcal{X}$ is a quadric, we will consider the cases where rank($\mathcal{X}$)= 3, 4, 5, since otherwise, the computation of the miminum distance of the codes $C_2(\mathcal{X})$ is reduced to the study of plane or hyperplane sections of quadrics which is well known.
The case where $\mathcal{X}$ is a non-degenerate quadric in $\mathbb{P}^4(\mathbb{F}_q)$ (i.e. rank($\mathcal{X}$) = 5, $\mathcal{X}$ is a parabolic quadric), a bound for the minimum distance is given by D. B. Leep and L. M. Schueller [11, p.172]:

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

It is not optimal. When $\mathcal{X}$ is a degenerate quadric of rank 3 or 4, the hypothesis of D. B. Leep and L. M. Schueller is too much restrictive and we cannot find the minimal distance. In this case, however, we have a bound given by G. Lachaud [10, proposition 2.3]:

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 4(q^2 + q + 1)$$

which is not the best possible.
In the case where $\mathcal{X}$ is a non-singular hermitian variety, the result of Lachaud gives an upper bound [14, p.208],

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 2(t+1)(q^2 + q + 1)$$

which is also not optimal.
In this paper we find some optimal bounds excepting the case where $\mathcal{X}$ is a degenerate quadric with rank($\mathcal{X}$) = 4 and projective index g($\mathcal{X}$)=1.
The paper is organized as follows. First of all we recall some generalities on quadrics and hermitian varieties. Secondly by using the projective classification of quadrics in [9, p.4] and their geometric structure, we find some interesting bounds on the number of rational points on the intersection of two quadrics. Thus, we show that for $\mathcal{X}$ a non-degenerate quadric:

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 2q^2 + 3q + 1$$

is the best possible. We also show that for $\mathcal{X}$ degenerate and rank ($\mathcal{X}$) = 3, we get

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 4q^2 + q + 1,$$

and this bound is optimal. Identically, for rank($\mathcal{X}$) = 4 and g($\mathcal{X}$)=2, we have the optimal bound:

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 4q^2 + 1.$$

For $\mathcal{X}$ of rank($\mathcal{X}$) = 4 and g($\mathcal{X}$)=1, we get the bound

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

Next, we express the exact parameters of the codes $C_2(\mathcal{X})$, the geometric structure of the minimum weight codewords and show that the performances of the codes $C_2(\mathcal{X})$ defined on the non-degenerate quadrics are better than the ones defined on the degenerate quadrics.
In the section 5, by using again the projective classification of quadrics in [9, p.4], those of hermitian surfaces in [8, p.112], some properties of hermitian varieties, we find the first five best upper bounds:

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2t^5 + t^3 + 2t^2 + 1, 2t^5 + t^3 + t^2 + 1, 2t^5 + 2t^2 + 1,$$

$2t^5 + t^2 + 1, 2t^5 - t^3 + 2t^2 + 1,$
on the number of rational points on the intersection of the non-singular hermitian variety $\mathcal{X}$ and any quadric $\mathcal{Q}$. In section 6, when $\mathcal{X}$ is a non-singular hermitian variety, we determine exactly the minimum distance of the code $C_2(\mathcal{X})$ and the minimum weight codewords. We also list the second, third, fourth, fifth weight, and describe the corresponding codewords reaching these weights.
The paper ends with two conjectures: the first, on the minimum distance for the code $C_h(\mathcal{X})$ where $\mathcal{X} \subset \mathbb{P}^4(\mathbb{F}_q)$ is the non-singular hermitian variety and the second, on the distribution of the codewords of the first five weights of $C_2(\mathcal{X})$ when $\mathcal{X} \subset \mathbb{P}^N(\mathbb{F}_q)$ is the non-singular hermitian variety.

2 Generalities

We denote by $\mathbb{F}_q$ the field with q elements. Let $V = A^{n+1}(\mathbb{F}_q)$ be the affine space of dimension $n+1$ over $\mathbb{F}_q$ and $\mathbb{P}^n(\mathbb{F}_q) = \Pi_n$ the corresponding projective space. Then

$$\pi_n = \#\mathbb{P}^n(\mathbb{F}_q) = q^n + q^{n-1} + ... + 1.$$

We use the term forms of degree two to describe homogeneous polynomials f of degree two, and $\mathcal{Q} = Z(f)$ (the zeros of f in the projective space $\mathbb{P}^n(\mathbb{F}_q)$) is a quadric.
Let $\mathcal{Q}$ be a quadric. The rank of $\mathcal{Q}$, denoted r($\mathcal{Q}$), is the smallest number of indeterminates appearing in f under any change of coordinate system. The quadric $\mathcal{Q}$ is said to be degenerate if r($\mathcal{Q}$) $< n+1$; otherwise it is non-degenerate. For $\mathcal{Q}$ a degenerate quadric and r($\mathcal{Q}$)=r, $\mathcal{Q}$ is a cone $\Pi_{n-r}\mathcal{Q}_{r-1}$

with vertex Π_{n-r} (the set of singular points of $\mathcal{Q}$) and base $\mathcal{Q}_{r-1}$ in a subspace Π_{r-1} skew to Π_{n-r}. For degenerate hermitian varieties we have an analogous decomposition as for quadrics.

Definition 2.1 *For $\mathcal{Q} = \Pi_{n-r}\mathcal{Q}_{r-1}$ a degenerate quadric with $r(\mathcal{Q}) = r$, $\mathcal{Q}_{r-1}$ is called the non-degenerate quadric associated to $\mathcal{Q}$. The degenerate quadric $\mathcal{Q}$ will said to be of type hyperbolic (resp. elliptic, parabolic) if its associated non-degenerate quadric is of the same type.*

Definition 2.2 *[11, p.158] Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two quadrics. The order $w(\mathcal{Q}_1, \mathcal{Q}_2)$ of the pair $(\mathcal{Q}_1, \mathcal{Q}_2)$, is the minimum number of variables, after invertible linear change of variables, necessary to write $\mathcal{Q}_1$ and $\mathcal{Q}_2$.*

Definition 2.3 *For any variety $\mathcal{V}$, the maximum dimension $g(\mathcal{V})$ of linear subspaces lying on $\mathcal{V}$, is called the projective index of $\mathcal{V}$.*

First of all, let us recall the classification of quadrics in $\mathbb{P}^4(\mathbb{F}_q)$. It can be found in the book of J. W. P. Hirschfeld [9, p.4].

r($\mathcal{Q}$)	Description	$\lvert\mathcal{Q}\rvert$	g($\mathcal{Q}$)
1	repeated hyperplane $\Pi_3\mathcal{P}_0$	q^3+q^2+q+1	3
2	pair of distinct hyperplanes $\Pi_2\mathcal{H}_1$	$2q^3+q^2+q+1$	3
2	the plane $\Pi_2\mathcal{E}_1$	q^2+q+1	2
3	the cone $\Pi_1\mathcal{P}_2$	$(q+1)(q^2+1)$	2
4	the cone $\Pi_0\mathcal{H}_3(\mathcal{R},\mathcal{R}')$	$q(q+1)^2+1$	2
4	the cone $\Pi_0\mathcal{E}_3$	$q(q^2+1)+1$	1
5	the parabolic quadric $\mathcal{P}_4$	$(q+1)(q^2+1)$	1

Table 1: Quadrics in $\mathbb{P}^4(\mathbb{F}_q)$

From the work of Ray-Chaudhuri [13, pp.132-136] we deduce that a non-degenerate quadric $\mathcal{P}_4$ in $\mathbb{P}^4(\mathbb{F}_q)$ contains exactly $\alpha_q = \pi_3$ lines and there are exactly $q+1$ lines contained in $\mathcal{P}_4$ through a given point in $\mathcal{P}_4$.
A regulus defined in the work of Hirschfeld [8, p.4], is the set of transversals of three skew lines in $\mathbb{P}^3(\mathbb{F}_q)$; it consists of $q+1$ skew lines. Thus, a hyperbolic quadric $\mathcal{Q}$ in $\mathbb{P}^3(\mathbb{F}_q)$ is a pair of complementary reguli (each one of the two reguli generates the whole hyperbolic quadric). It is denoted by $\mathcal{Q} = \mathcal{H}_3(\mathcal{R},\mathcal{R}')$ where $\mathcal{R}$ and $\mathcal{R}'$ are the two reguli.
Let $\mathcal{F}_h$ be the vector space of forms of degree h in $V = \mathbb{A}^{n+1}(\mathbb{F}_q)$, $X \subset \mathbb{P}^n(\mathbb{F}_q)$ a variety and $|X|$ the number of rational points of X over $\mathbb{F}_q$. We denote by

W_i the set of points with homogeneous coordinates $(x_0 : ... : x_n) \in \mathbb{P}^n(\mathbb{F}_q)$ such that $x_j = 0$ for $j < i$ and $x_i \neq 0$. The family $\{W_i\}_{0 \leq i \leq n}$ is a partition of $\mathbb{P}^n(\mathbb{F}_q)$. The code $C_h(X)$ is the image of the linear map $c : \mathcal{F}_h \longrightarrow \mathbb{F}_q^{|X|}$, defined by $c(f) = (c_x(f))_{x \in X}$, where $c_x(f) = f(x_0, ..., x_n)/{x_i}^h$ with $x = (x_0 : ... : x_n) \in W_i$. The length of $C_h(X)$ is equal to $\#X(\mathbb{F}_q)$. The dimension of $C_h(X)$ is equal to $\dim \mathcal{F}_h - \dim \ker c$. Therefore, when c is injective we get:

$$\dim\ C_h(\mathcal{X}) = \left(\begin{array}{c} n+h \\ h \end{array} \right). \tag{1}$$

The minimum distance of $C_h(X)$ is equal to the mimimum over all f of $\#X(\mathbb{F}_q) - \#X_{Z(f)}(\mathbb{F}_q)$.

3 Intersection of two quadrics

In this section, we will estimate the number of points in the intersection of two quadrics $\mathcal{X}$ and $\mathcal{Q}$ in $\mathbb{P}^4(\mathbb{F}_q)$. Some bounds in $\mathbb{P}^4(\mathbb{F}_q)$ have been given by Y. Aubry [1], G. Lachaud [10], D. B. Leep and L. M. Schueller [11]. These bounds are not the best possible even in the case of $\mathbb{P}^4(\mathbb{F}_q)$. Here $\mathcal{X}$ denotes a quadric of $\text{rank}(\mathcal{X}) = 3, 4, 5$ in $\mathbb{P}^4(\mathbb{F}_q)$.
Let us recall the result of D. B. Leep and L. M. Schueller [11, p.172] which gives an upper bound for the number of intersection of a pair of quadrics.

Theorem 3.1 *Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two quadrics in $\mathbb{P}^n(\mathbb{F}_q)$. Suppose that $w(\mathcal{Q}_1, \mathcal{Q}_2) = n + 1$. If $n + 1 \geq 5$ and $n + 1$ odd, then*

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq (2q^{n-1} - q^{n-2} + q^{\frac{n+2}{2}} - q^{\frac{n}{2}} - 1)/(q - 1).$$

From this theorem, we deduce the following result.

Corollary 3.2 *Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two quadrics in $\mathbb{P}^4(\mathbb{F}_q)$ with $w(\mathcal{Q}_1, \mathcal{Q}_2) = 5$. Then,*

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 3q^2 + q + 1.$$

In the theorem above the hypothesis on the order of the two quadrics $\mathcal{Q}_1$ and $\mathcal{Q}_2$ is too restrictive and does not work in general case. Let us state another property, free from this condition.

Lemma 3.3 *Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two quadrics in $\mathbb{P}^n(\mathbb{F}_q)$ and l an integer such that $1 \leq l \leq n - 1$.*
Suppose that $w(\mathcal{Q}_1, \mathcal{Q}_2) = n - l + 1$ (i.e. there exists a linear transformation such that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are defined with the indeterminates $x_0, x_1, ..., x_{n-l}$) and

$|\mathcal{Q}_1 \cap \mathcal{Q}_2 \cap \mathbb{E}_{n-l}(\mathbb{F}_q)| \leq m$ *where* $\mathbb{E}_{n-l}(\mathbb{F}_q) = \{x \in \mathbb{P}^n(\mathbb{F}_q) \ | x_{n-l+1} = ... = x_n = 0\}$. *Then*

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq mq^l + \pi_{l-1}.$$

This bound is optimal as soon as m *is optimal in* $\mathbb{E}_{n-l}(\mathbb{F}_q)$.

Proof If $w(\mathcal{Q}_1, \mathcal{Q}_2) = n - l + 1$, then there exists a linear transformation such that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are defined with the indeterminates $x_0, x_1, ..., x_{n-l}$. Let $m_0 \leq m$ such that $|\mathcal{Q}_1 \cap \mathcal{Q}_2 \cap \mathbb{E}_{n-l}(\mathbb{F}_q)| = m_0$. From the fact that $\mathcal{Q}_1 \cap \mathcal{Q}_2$ has exactly m_0 projective zeros in $\mathbb{E}_{n-l}(\mathbb{F}_q)$, we deduce that it has exactly $m(q-1)+1$ affine zeros in $\tilde{\mathbb{E}}(\mathbb{F}_q)$ (the corresponding affine space of dimension $n-l+1$).
Let $\tilde{y} = (y_0, y_1, ..., y_{n-l})$ be a zero of $\mathcal{Q}_1 \cap \mathcal{Q}_2$ in $\tilde{\mathbb{E}}(\mathbb{F}_q)$. We get that $y = (y_0, y_1, ..., y_{n-l}, x_{n-l+1}, ..., x_n)$ is a zero of $\mathcal{Q}_1 \cap \mathcal{Q}_2$ in $\mathbb{A}^{n+1}(\mathbb{F}_q)$ for any $(x_{n-l+1}, ..., x_n) \in \mathbb{F}_q^l$. And reciprocally every zero of $\mathcal{Q}_1 \cap \mathcal{Q}_2$ in $\mathbb{A}^{n+1}(\mathbb{F}_q)$ comes from a zero of $\mathcal{Q}_1 \cap \mathcal{Q}_2$ in $\tilde{\mathbb{E}}(\mathbb{F}_q)$. Therefore, we deduce that $\mathcal{Q}_1 \cap \mathcal{Q}_2$ contains exactly $\{m_0(q-1)+1\}q^l$ affine zeros in $\mathbb{A}^{n+1}(\mathbb{F}_q)$. Thus, in $\mathbb{P}^n(\mathbb{F}_q)$, we get $|\mathcal{Q}_1 \cap \mathcal{Q}_2| = (\{m_0(q-1)+1\}q^l - 1)/(q-1) = m_0 q^l + \pi_{l-1}$.

Lemma 3.4 *For* $\mathcal{Q}_1$ *and* $\mathcal{Q}_2$ *two quadrics in* $\mathbb{P}^n(\mathbb{F}_q)$, *we get*

$$w(\mathcal{Q}_1, \mathcal{Q}_2) \geq \sup\{\mathrm{r}(\mathcal{Q}_1), \mathrm{r}(\mathcal{Q}_2)\}.$$

Proof We have $\mathrm{r}(\mathcal{Q}_i) \leq w(\mathcal{Q}_1, \mathcal{Q}_2)$ for $i = 1, 2$.

3.1 Plane section of the quadric $\mathcal{X}$: g($\mathcal{Q}$)=2

Here we study the section of the quadric $\mathcal{X}$ by a quadric $\mathcal{Q}$ with g($\mathcal{Q}$)=2. We have three cases: $\mathcal{Q} = \Pi_2\mathcal{E}_1$, $\mathcal{Q} = \Pi_1\mathcal{P}_2$ and $\mathcal{Q} = \Pi_0\mathcal{H}_3(\mathcal{R}, \mathcal{R}')$. Here $\mathcal{Q} = \Pi_1\mathcal{P}_2$ and $\mathcal{Q} = \Pi_0\mathcal{H}_3(\mathcal{R}, \mathcal{R}')$ are respectively a set of $q+1$ planes through a common line or a common point.

3.1.1 $\mathcal{Q}$ is a quadric with r($\mathcal{Q}$)=2: $\mathcal{Q} = \Pi_2\mathcal{E}_1$

Here $\mathcal{Q}$ consists of one plane of $\mathbb{P}^4(\mathbb{F}_q)$. If this plane is not contained in $\mathcal{X}$, then $\mathcal{Q} \cap \mathcal{X}$ is a plane quadric. In the book of J. W. P. Hirschfeld [7, p.156], we have the following classsification of plane quadrics.

Therefore we deduce that if $\mathcal{Q}$ is a plane of $\mathbb{P}^4(\mathbb{F}_q)$:
– If it is contained in $\mathcal{X}$, we get $|\mathcal{X} \cap \mathcal{Q}| = q^2 + q + 1$.
– Otherwise, we get from the table above that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q + 1$.

r($\mathcal{Q}'$)	Description	$\lvert\mathcal{Q}'\rvert$	g($\mathcal{Q}'$)
1	repeated line $\Pi_1\mathcal{P}_0$	$q+1$	1
2	pair of lines $\Pi_0\mathcal{H}_1$	$2q+1$	1
2	point $\Pi_0\mathcal{E}_1$	1	0
3	parabolic $\mathcal{P}_2$	$q+1$	0

Table 2: Plane quadrics in $\mathbb{P}^2(\mathbb{F}_q)$

3.1.2 $\mathcal{Q}$ is a quadric with r($\mathcal{Q}$)=3,4: $\mathcal{Q} = \Pi_1\mathcal{P}_2$ and $\mathcal{Q} = \Pi_0\mathcal{H}_3$

For $\mathcal{X}$ a non-degenerate quadric, there is no plane in $\mathcal{X}$. Thus each of the $q+1$ planes of $\mathcal{Q}$ intersects $\mathcal{X}$ in at most $2q+1$ points. Therefore, we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 3q + 1$.

For $\mathcal{X}$ degenerate of $\mathrm{r}(\mathcal{X}) = 3, 4$, let us consider the order $w(\mathcal{X}, \mathcal{Q})$ of the pair $\{\mathcal{X}, \mathcal{Q}\}$. We have three possibilities $w(\mathcal{X}, \mathcal{Q}) = 3, 4, 5$:

(i) If $w(\mathcal{X}, \mathcal{Q}) = 5$, from the corollary 3.2 we get $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2 + q + 1$.

(ii) If $w(\mathcal{X}, \mathcal{Q}) = 4$, then there exists a linear transformation such that $\mathcal{X}$ and $\mathcal{Q}$ are defined with the indeterminates x_0, x_1, x_2, x_3.
Suppose rank($\mathcal{X}$)=3. From [5, IV-D-3,4], we get $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| = 4q+1$ or $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| \leq 3q$. From lemma 3.3 we deduce that either $|\mathcal{X} \cap \mathcal{Q}| = 4q^2 + q + 1$ in the case where $\mathcal{X}$ and $\mathcal{Q}$ have exactly four common planes through a line or $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2 + 1$ otherwise.
If rank($\mathcal{X}$)=4 and $g(\mathcal{X}) = 1$, from [5, IV-D-2] we get $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| \leq 2(q+1)$. Therefore lemma 3.3 gives $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 2q + 1$.
If rank($\mathcal{X}$)=4 and $g(\mathcal{X}) = 2$, [5, IV-D-3 and IV-E-1] give $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| = 4q$ or $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| \leq 3q + 1$. In fact, in the case $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| = 4q$, $\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)$ is exactly a set of four lines with two lines in each regulus of $\mathcal{H}_3$. Therefore, from lemma 3.3 and the geometric structure of $\mathcal{X}$ and $\mathcal{Q}$, we get $|\mathcal{X} \cap \mathcal{Q}| = 4q^2 + 1$ when $\mathcal{X}$ and $\mathcal{Q}$ have the same vertex Π_0 and contain four common planes with the following configuration:
(the first two planes ${\Pi_2}^{(1)}$ and ${\Pi_2}^{(2)}$ meet at the point Π_0, and the two others ${\Pi_2}^{(3)}$ and ${\Pi_2}^{(4)}$ also meet at the point Π_0,
the plane ${\Pi_2}^{(1)}$ meets ${\Pi_2}^{(3)}$ and ${\Pi_2}^{(4)}$ respectively at two distinct lines $\mathcal{D}_{1,3}$ and $\mathcal{D}_{1,4}$,
the plane ${\Pi_2}^{(2)}$ meets ${\Pi_2}^{(3)}$ and ${\Pi_2}^{(4)}$ respectively at two distinct lines $\mathcal{D}_{2,3}$ and $\mathcal{D}_{2,4}$,

each one of the four lines $\mathcal{D}_{1,3}$, $\mathcal{D}_{1,4}$, $\mathcal{D}_{2,3}$ and $\mathcal{D}_{2,4}$ passes through the point Π_0). For example, for the two quadrics defined by $f_{\mathcal{X}} = x_0x_1+x_2x_3$ and $f_{\mathcal{Q}} = x_3x_0+x_1x_2$ we have $|\mathcal{X}\cap\mathcal{Q}| = 4q^2+1$. Otherwise, we get $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2 + q + 1$.

(iii) If $w(\mathcal{X}, \mathcal{Q}) = 3$, necessary from lemma 3.4, we get r($\mathcal{X}$)=r($\mathcal{Q}$)=3. Here $\mathcal{Q} \cap \mathbb{E}_2(\mathbb{F}_q)$ and $\mathcal{X} \cap \mathbb{E}_2(\mathbb{F}_q)$ are two irreducible curves (conics). Therefore from the theorem of Bézout (the fact that two plane conics have exactly four common points or less than three points) and lemma 3.3, we deduce that $|\mathcal{X} \cap \mathcal{Q}| = 4q^2 + q + 1$, or otherwise $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2 + q + 1$.

3.2 Hyperplane section of the quadric $\mathcal{X}$: g ($\mathcal{Q}$)=3

This paragraph deals with the section of $\mathcal{X}$ by $\mathcal{Q}$ in the case g($\mathcal{Q}$)=3 i.e. $\mathcal{Q}$ contains a hyperplane. We have two cases: r($\mathcal{Q}$)=1 (i.e. $\mathcal{Q}$ is a repeated hyperplane), or r($\mathcal{Q}$)=2 with $\mathcal{Q}$ a pair of hyperplanes.

3.2.1 $\mathcal{Q}$ is a quadric with r($\mathcal{Q}$)=1: $\mathcal{Q} = \Pi_3\mathcal{P}_0$

Here $\mathcal{Q}$ is a repeated hyperplane H . Let us recall three general results on hyperplane section of quadrics in $\mathbb{P}^n(\mathbb{F}_q)$.

Lemma 3.5 *Swinnerton-Dyer [18, p.264], Let $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ be a degenerate quadric of rank r and H an hyperplane. Then $\tilde{\mathcal{X}}\cap H$ is a quadric in $\mathbb{P}^{n-1}(\mathbb{F}_q)$ of rank $r, r-1$, or $r-2$.*

Lemma 3.6 *Primrose [12, pp.299-300], Let $\tilde{\mathcal{X}}$ be a non-degenerate quadric in $\mathbb{P}^n(\mathbb{F}_q)$ and H a hyperplane. If H is tangent to $\tilde{\mathcal{X}}$, then $\tilde{\mathcal{X}} \cap H$ is a degenerate quadric of rank $n-1$ in $\mathbb{P}^{n-1}(\mathbb{F}_q)$. If H is not tangent to $\tilde{\mathcal{X}}$, then $\tilde{\mathcal{X}} \cap H$ is a non-degenerate quadric in $\mathbb{P}^{n-1}(\mathbb{F}_q)$.*

Let $H \subset \mathbb{P}^4(\mathbb{F}_q)$ be a hyperplane. If $\mathcal{X}$ is a non-degenerate quadric, from lemma 3.6, we get

$$(\star) \quad \#\mathcal{X}_H(\mathbb{F}_q) = \begin{cases} (q+1)^2, q^2+1 & \text{if H is not tangent to } \mathcal{X}, \\ q^2+q+1 & \text{if H is tangent to } \mathcal{X}. \end{cases}$$

If $\mathcal{X}$ is a degenerate quadric, from lemma 3.5, we get

$$\#\mathcal{X}_H(\mathbb{F}_q) \leq 2q^2 + q + 1. \tag{2}$$

The third important result on hyperplane section of a quadric is:

Lemma 3.7 *J. Wolfmann [19, pp.191-192], Let $\tilde{\mathcal{X}}$ be a non-degenerate quadric in $\mathbb{P}^n(\mathbb{F}_q)$ and H a hyperplane. If H is tangent to $\tilde{\mathcal{X}}$, then $\tilde{\mathcal{X}} \cap H$ is of the same type as $\tilde{\mathcal{X}}$ (in the sense of the definition 2.1).*

3.2.2 $\mathcal{Q}$ is a quadric with r($\mathcal{Q}$)=2 and $\mathcal{Q}$ is a pair of hyperplanes

Let H_1 and H_2 be the two distinct hyperplanes generating $\mathcal{Q}$. We have $\mathcal{Q} = H_1 \cup H_2$. Let $\mathcal{P} = H_1 \cap H_2$ be the plane of intersection of the two hyperplanes. We have

$$|\mathcal{Q} \cap \mathcal{X}| = |H_1 \cap \mathcal{X}| + |H_2 \cap \mathcal{X}| - |\mathcal{P} \cap \mathcal{X}|. \tag{3}$$

Let $\hat{\mathcal{X}}_1 = H_1 \cap \mathcal{X}$, and $\hat{\mathcal{X}}_2 = H_2 \cap \mathcal{X}$. We have

$$\mathcal{P} \cap \mathcal{X} = \mathcal{P} \cap \hat{\mathcal{X}}_1 = \mathcal{P} \cap \hat{\mathcal{X}}_2. \tag{4}$$

3.2.2.1 If $\mathcal{X}$ is non-degenerate (i.e. parabolic)

(i) In the case where each hyperplane is tangent to $\mathcal{X}$, we know that $\hat{\mathcal{X}}_1$, and $\hat{\mathcal{X}}_2$ are quadric cones of rank 3. We get that $|\hat{\mathcal{X}}_1| = |\hat{\mathcal{X}}_2| = q^2+q+1$. From lemma 3.5 and table 2, we deduce that $|\mathcal{P} \cap \hat{\mathcal{X}}_1| \geq 1$. Therefore, from relation 3, we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 2q + 1$.

(ii) In the case where one hyperplane H_2 is tangent to $\mathcal{X}$, and the second hyperplane H_1 is non-tangent to $\mathcal{X}$, $\hat{\mathcal{X}}_1$ is a non-degenerate quadric surface in $\mathbb{P}^3(\mathbb{F}_q)$: elliptic or hyperbolic.
–If $\hat{\mathcal{X}}_1$ is an elliptic quadric, from lemmas 3.6, 3.7 and table 2, we get that $\mathcal{P} \cap \hat{\mathcal{X}}_1$ is either a plane conic (parabolic), or a single point according to $\mathcal{P}$ being non-tangent or tangent to $\hat{\mathcal{X}}_1$. Therefore, from relations (4), (3) and table 2, we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + q + 1$.
–If $\hat{\mathcal{X}}_1$ is an hyperbolic quadric, from lemmas 3.6, 3.7 and table 2, we get that $\mathcal{P} \cap \hat{\mathcal{X}}_1$ is either a plane conic (parabolic), or a pair of two distinct lines according to $\mathcal{P}$ being non-tangent or tangent to $\hat{\mathcal{X}}_1$. Therefore, from (4) and (3), we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + q + 1$.

(iii) In the case where each hyperplane is non-tangent to $\mathcal{X}$, we know that $\hat{\mathcal{X}}_1$, and $\hat{\mathcal{X}}_2$ are non-singular quadric surfaces: elliptic or hyperbolic. They can be of the same type or of different types.
–If one of the two quadrics is elliptic, from lemma 3.6 and table 2, we deduce that $|\mathcal{P} \cap \hat{\mathcal{X}}_1| \geq 1$. Therefore from (3) and ($\star$) we get that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 2q + 1$.
–If the two quadrics are hyperbolic, from lemmas 3.6, 3.7 and table 2,

we deduce that $|\mathcal{P} \cap \hat{\mathcal{X}}_1| \geq q+1$. Therefore, from (4) and (3), we get $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2+3q+1$. And this upper bound is reached when $\mathcal{P}$ is non-tangent to $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$. For example, for the two quadrics defined by $f_{\mathcal{X}} = x_0x_1+x_2x_3+x_4^2$ and $f_{\mathcal{Q}} = (x_0+x_1)(x_2+x_3)$ with $\mathrm{car}(\mathbb{F}_q) \neq 2$

3.2.2.2 If $\mathcal{X}$ is degenerate (i.e. rank ($\mathcal{X}$)=3,4) .
Here we have $w(\mathcal{X}, \mathcal{Q}) = 3, 4, 5$:

(i) If $w(\mathcal{X}, \mathcal{Q}) = 5$, from corollary 3.2 we get $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2+q+1$.

(ii) If $w(\mathcal{X}, \mathcal{Q}) = 4$. Suppose rank($\mathcal{X}$)=3. From [5, IV-C] we get $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| = 4q+1$ or $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| \leq 3q+1$. From lemma 3.3 we deduce that either $|\mathcal{X} \cap \mathcal{Q}| = 4q^2+q+1$ in the case where $\mathcal{Q}$ is union of two hyperplanes (non-tangent) each through a pair of planes of $\mathcal{X}$ and the plane of intersection of the two hyperplanes intersecting $\mathcal{X}$ in a line or $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2+q+1$ otherwise.
If rank ($\mathcal{X}$)=4 and $g(\mathcal{X}) = 1$ from [5, IV-B] we get $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| \leq 2(q+1)$. Therefore lemma 3.3 gives $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2+2q+1$.
If rank ($\mathcal{X}$)=4 and $g(\mathcal{X}) = 2$, the result of [5, IV-B] gives $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| = 4q$ or $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| \leq 3q+1$. Therefore from lemma 3.3, we get either $|\mathcal{X} \cap \mathcal{Q}| = 4q^2+1$ when each hyperplane is tangent to $\mathcal{X}$ with the plane of intersection meeting $\mathcal{X}$ at two lines or $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2+q+1$ otherwise.

(iii) If $w(\mathcal{X}, \mathcal{Q}) = 3$, necessary from lemma 3.4, we get r($\mathcal{X}$)=3. Here, the quadric $\mathcal{Q}$ describes a pair of lines in $\mathbb{E}_2(\mathbb{F}_q)$. The number of points in the intersection of two secant lines with a conic (non-singular plane quadric) is exactly four or less than three. From table 2 and lemma 3.3 we get that either $|\mathcal{X} \cap \mathcal{Q}| = 4q^2+q+1$ or $|\mathcal{X} \cap \mathcal{Q}| \leq 3q^2+q+1$.

3.3 Line section of the quadric $\mathcal{X}$: g($\mathcal{Q}$)=1

In this section we estimate the number of points in the intersection of $\mathcal{X}$ and a quadric $\mathcal{Q}$ with g($\mathcal{Q}$) = 1. In this case $\mathcal{Q}$ is the degenerate quadric $\Pi_0\mathcal{E}_3$ or the non-degenerate quadric (i.e. parabolic) $\mathcal{P}_4$.

3.3.1 $\mathcal{Q}$ is a quadric with r($\mathcal{Q}$)=4: $\mathcal{Q} = \Pi_0\mathcal{E}_3$

(i) For $\mathcal{X}$ non-degenerate quadric, we get two possibilities:
– If there is a line of $\mathcal{X} \cap \mathcal{Q}$ through the vertex Π_0 of the cone $\mathcal{Q} = \Pi_0\mathcal{E}_3$, it is obvious that this vertex is a point of $\mathcal{X}$. Therefore there are

at most $q+1$ lines of the cone $\mathcal{Q}$ through Π_0 contained in $\mathcal{X}$; the other lines of $\mathcal{Q}$ meet $\mathcal{X}$ in at most two points each. Thus, we get $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 2q + 1$.
– If there is no line of $\mathcal{X} \cap \mathcal{Q}$ through the vertex of the cone $\mathcal{Q} = \Pi_0 \mathcal{E}_3$, each line of $\mathcal{Q}$ intersecting $\mathcal{X}$ in at most two points, we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq 2(q^2+1)$.

(ii) For $\mathcal{X}$ degenerate quadric (i.e. $\mathrm{r}(\mathcal{X}) = 3, 4$).
From lemma 3.4, we have $w(\mathcal{X}, \mathcal{Q}) = 4, 5$. The case $w(\mathcal{X}, \mathcal{Q}) = 5$ follows from corollary 3.2. Let us consider now that $w(\mathcal{X}, \mathcal{Q}) = 4$.
If r($\mathcal{X}$)=3,4 and g($\mathcal{X}$)=2, or r($\mathcal{X}$)=4 and g($\mathcal{X}$)=1, from [5, IV-D-2, IV-E-2] we get $|\mathcal{X} \cap \mathcal{Q} \cap \mathbb{E}_3(\mathbb{F}_q)| \leq 2(q+1)$. Thus, we deduce from lemma 3.3 that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 2q + 1$.

Remark 3.8 *Let $\mathcal{Q}$ be a non-degenerate quadric (i.e. $\mathcal{Q} = \mathcal{P}_4$) and r($\mathcal{X}$)=3,4. The cases r($\mathcal{X}$)=3,4 and g($\mathcal{X}$)=2, correspond to the first part of 3.1.2. with $\mathcal{Q}$ at the place of $\mathcal{X}$. In the same way r($\mathcal{X}$)=4 and g($\mathcal{X}$)=1, corresponds to 3.3.1.(i).*

3.3.2 Intersection of two non-degenerate quadrics

Here we study the number of points in the intersection of two non-degenerate quadrics $\mathcal{X}$ and $\mathcal{Q}$.

Proposition 3.9 *Let $\mathcal{X}$ and $\mathcal{Q}$ be two non-degenerate quadrics in $\mathbb{P}^4(\mathbb{F}_q)$. If there is no line in $\mathcal{X} \cap \mathcal{Q}$, then $|\mathcal{X} \cap \mathcal{Q}| \leq 2(q^2+1)$.*

Proof We use the fact that α_q is the number of lines of $\mathcal{X}$, each one of them meeting $\mathcal{Q}$ in at most two points. Moreover there pass exacly $q+1$ lines through each point contained in $\mathcal{X}$.

Now we will study the section of two non-degenerate quadrics containning a common line. Let us consider a line $\mathcal{D}$ contained in $\mathcal{X} \cap \mathcal{Q}$ and $\mathcal{P}$ a plane through $\mathcal{D}$. By the principle of duality in the projective space [15, pp.49-51], or [7, p.33, theorem 3.1 p.85], we deduce that there are exactly $q+1$ hyperplanes (H_i) through $\mathcal{P}$. These $q+1$ hyperplanes (H_i) generate $\mathbb{P}^4(\mathbb{F}_q)$. For $i = 1, ..., q+1$, we denote $\hat{\mathcal{X}}_i = H_i \cap \mathcal{X}$ and $\hat{\mathcal{Q}}_i = H_i \cap \mathcal{Q}$. Thus, we get:

$$|\mathcal{X} \cap \mathcal{Q}| \leq |\hat{\mathcal{X}}_1 \cap \hat{\mathcal{Q}}_1| + \sum_{i=2}^{q+1} |(\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i) - \mathcal{D}|. \tag{5}$$

From lemma 3.6, we deduce that $\hat{\mathcal{X}}_i$ and $\hat{\mathcal{Q}}_i$ are quadrics of rank 3 or 4 in $\mathbb{P}^3(\mathbb{F}_q)$. Since they contain the line $(\mathcal{D})$, they can not be elliptic. They are either hyperbolic or cone quadrics (of rank 3). Thus one has to study the three types of intersection in $\mathbb{P}^3(\mathbb{F}_q)$ given by the table 3.

Types	$\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$
1	(hyperbolic quadric) $\cap$ (quadric cone)
2	(quadric cone) $\cap$ (quadric cone)
3	(hyperbolic quadric) $\cap$ (hyperbolic quadric)

Table 3: Intersection of $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$ in $\mathbb{P}^3(\mathbb{F}_q)$

Lemma 3.10 *Let $\mathcal{X}$ and $\mathcal{Q}$ be two non-degenerate quadrics in $\mathbb{P}^n(\mathbb{F}_q)$, and $\mathcal{K}$ a linear space of codimension 2. Then there exists at most two hyperplanes H_i, $i = 1, 2$ through $\mathcal{K}$ such that $\hat{\mathcal{X}}_i = \hat{\mathcal{Q}}_i$.*

Proof Let

$$\mathcal{Q} = \sum_{0 \leq i \leq j \leq n} a_{ij} x_i x_j \text{ and } \mathcal{X} = \sum_{0 \leq i \leq j \leq n} a'_{ij} x_i x_j.$$

Without loss of generality, we can choose a system of coordinates, such that $H_1 = \{x_n = 0\}$, $H_2 = \{x_{n-1} = 0\}$. For $H_1 \cap \mathcal{X} = H_1 \cap \mathcal{Q}$, we get that $a_{ij} = a'_{ij}$ except may be for (i, n) with $i = 0, ..., n$. For $H_2 \cap \mathcal{X} = H_2 \cap \mathcal{Q}$, we get that $a_{ij} = a'_{ij}$ except may be for $(i, n-1)$ with $i = 0, ..., n-1$ and $(n-1, n)$. Therefore, we deduce that $a_{ij} = a'_{ij}$ except for $(i, j) = (n-1, n)$; and there exists $(\alpha, \beta) \in \mathbb{F}_q^2$ $(\alpha \neq \beta)$ such that:

$$\begin{cases} \mathcal{Q} = \mathcal{Q}_0(x_0, x_1, ..., x_{n-1}, x_n) + \alpha x_{n-1} x_n \\ \mathcal{X} = \mathcal{Q}_0(x_0, x_1, ..., x_{n-1}, x_n) + \beta x_{n-1} x_n. \end{cases}$$

Let us suppose that there is a third hyperplane H_3 through $\mathcal{K}$ such that $H_3 \cap \mathcal{X} = H_3 \cap \mathcal{Q}$. We can suppose that $H_3 = \{a x_{n-1} + b x_n = 0\}$ and $b \neq 0$, therefore $x_n = -\frac{a}{b} x_{n-1}$. From the above system and the fact that $H_3 \cap \mathcal{X} = H_3 \cap \mathcal{Q}$ we deduce that $-\alpha \frac{a}{b} x_{n-1}^2 = -\beta \frac{a}{b} x_{n-1}^2$. Since $\alpha \neq \beta$, we deduce that $a = 0$, which leads to $H_3 = H_2$.

Proposition 3.11 *Let $\mathcal{X}$ and $\mathcal{Q}$ be two non-degenerate quadrics in $\mathbb{P}^4(\mathbb{F}_q)$ containing a line $(\mathcal{D})$. There is a plane $(\mathcal{P})$ containing $(\mathcal{D})$ such that $\hat{\mathcal{X}}_i \neq \hat{\mathcal{Q}}_i$ for $i = 1, ..., q+1$.*

Proof We know from lemma 3.10 that there exists at most two hyperplanes H_i, $i = 1, 2$ such that $\hat{\mathcal{X}}_i = \hat{\mathcal{Q}}_i$. There are also at most $2(q+1)$ planes through $(\mathcal{D})$ contained in $H_1 \cup H_2$. Since there are exactly q^2+q+1 planes through $(\mathcal{D})$, we conclude that there are at least $q^2 - q - 1 > 0$ possibilities of choice for the plane $(\mathcal{P})$ such that $\hat{\mathcal{X}}_i \neq \hat{\mathcal{Q}}_i$ for $i = 1, ..., q+1$.

Lemma 3.12 *Let $\mathcal{D}_1$, $\mathcal{D}_2$ be two secant lines of the non-degenerate quadric $\mathcal{X} \subset \mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{P} =< \mathcal{D}_1, \mathcal{D}_2 >$ the plane defined by these two lines. Let (H_i) i=1,...,q+1 be the q+1 hyperlanes containing $\mathcal{P}$. If there exists a hyperplane H_1 tangent to $\mathcal{X}$, then it is unique (i.e. the remaining q hyperplanes are non-tangent to $\mathcal{X}$).*

Proof Let H_1 containing $\mathcal{P}$, be a hyperplane which is tangent to $\mathcal{X}$ at a point P_1. Then from lemma 3.6, $\hat{\mathcal{X}}_1$ is a quadric cone of rank 3 in $\mathbb{P}^3(\mathbb{F}_q)$: $\hat{\mathcal{X}}_1$ is a set of $q+1$ lines through P_1 ($\mathcal{D}_1$ and $\mathcal{D}_2$ are two of them).
Let H_2 containing $\mathcal{P}$ be another hyperplane which is tangent to $\mathcal{X}$ at a point P_2. Then $\hat{\mathcal{X}}_2$ is a set of $q+1$ lines through P_2 and ($\mathcal{D}_1$ and $\mathcal{D}_2$ are two of them). The lines $(\mathcal{D}_1)$ and $(\mathcal{D}_2)$ intersect at P_1 and P_2, therefore we deduce that $P_1 = P_2$. Thus, there exist a unique hyperplane H_1 tangent to $\mathcal{X}$ at the point $P = \mathcal{D}_1 \cap \mathcal{D}_2$.

Remark 3.13 *We also know from [5,§IV-D-4 and IV-E-1] that if the intersection of two quadrics cone (of rank 3) or two hyperbolic quadrics in $\mathbb{P}^3(\mathbb{F}_q)$ contains three lines, it contains exactly four common lines.*

From the results of [5, §IV] and table 3 above, we deduce the following table 4.

Let us explain the table 4. For the type 1, the intersection of a hyper-

Types	4 lines	2 lines	1 line
1		$3q$	$2q+1$
2	4q+1	$3q$	$2q+1$
3	$4q$	$3q+1$	$2(q+1)$

Table 4: Number of points and lines in $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$

bolic quadric and a quadric cone, contains at most two lines; therefore $3q$

and $2q+1$ are respectively the maximum number of this intersection when containing (exactly or) at most two lines or exactly one line. From the above remark, the types 2 and 3 are describe as before.

Now an estimation on the number of points in the intersection of the two non-degenerate quadrics $\mathcal{X}$ and $\mathcal{Q}$ containning a common line is reduced to the two following simple cases.

If $\mathcal{X} \cap \mathcal{Q}$ contains exactly one common line: Each $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$ contains exacly one line, and from the table 4, we get for $i = 1, ..., q+1$ $|\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i| \leq 2(q+1)$. Therefore from relation (5), we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq q^2 + 3q + 2$.

If $\mathcal{X} \cap \mathcal{Q}$ contains at least two common lines: We distinguish two following cases:

1. In the case where $\mathcal{X} \cap \mathcal{Q}$ contains only skew lines: from table 4, we get for $i = 1, ..., q+1$ $|\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i| \leq 2q+1$ for the types 1 and 2. Indeed, if $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$ contains more than one line, from the fact that one of the two quadrics $\hat{\mathcal{X}}_i$ or $\hat{\mathcal{Q}}_i$ is a quadric cone, they are secant. For type 3, if $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$ contains exactly four common lines, then it contains necessarily two secant lines. This is a contradiction. From remark 3.13, $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$ can only contain at most two lines. Thus, from table 4, $3q+1$ is an upper bound for the number of points in $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$. The lines of $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$ are skew; so they belong to the same regulus. From [5, IV-E-1] we get $|\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i| \leq 2(q+1)$. Finally, from relation (5) we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq q^2 + 3q + 2$.

2. In the case where there exist some secant lines in $\mathcal{X} \cap \mathcal{Q}$, let $\{\mathcal{D}_1, \mathcal{D}_2\}$ denote a pair of secant lines and $\mathcal{P}$ be the plane generated by this pair of secants. Let

$$\mathcal{Q} = \sum_{0 \leq i \leq j \leq 4} a_{ij} x_i x_j \text{ and } \mathcal{X} = \sum_{0 \leq i \leq j \leq 4} a'_{ij} x_i x_j.$$

(i) If there are exactly two hyperplanes H_i $i = 1, 2$ such that $\hat{\mathcal{X}}_i = \hat{\mathcal{Q}}_i$, then we can choose a system of coordinates, such that $H_1 = \{x_4 = 0\}$ and $H_2 = \{x_3 = 0\}$. From the proof of lemma 3.10, there exists $(\alpha, \beta) \in \mathbb{F}_q^2$ $(\alpha \neq \beta)$ such that:

$$\begin{cases} \mathcal{Q} = \mathcal{Q}_0(x_0, x_1, x_2, x_3, x_4) + \alpha x_3 x_4 \\ \mathcal{X} = \mathcal{Q}_0(x_0, x_1, x_2, x_3, x_4) + \beta x_3 x_4. \end{cases}$$

Thus, we have $\mathcal{X} \cap \mathcal{Q} = (H_1 \cap \mathcal{X}) \cup (H_2 \cap \mathcal{X})$ and from the relation (3) we get that $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 2q + 1$.

(ii) If there is exactly one hyperplane H_1 such that $\hat{\mathcal{X}}_1 = \hat{\mathcal{Q}}_1$, then by the same reasoning as above, we can choose two distinct linear forms $h_1(x_0, x_1, x_2, x_3, x_4)$ and $h_2(x_0, x_1, x_2, x_3, x_4)$ such that:

$$\begin{cases} \mathcal{Q} = \mathcal{X}_0(x_0, x_1, x_2, x_3) + x_4 h_1(x_1, x_2, x_3, x_4) \\ \mathcal{X} = \mathcal{X}_0(x_0, x_1, x_2, x_3) + x_4 h_2(x_1, x_2, x_3, x_4). \end{cases}$$

We have $\mathcal{X} \cap \mathcal{Q} = (H_1 \cap \mathcal{X}) \cup (H_2 \cap \mathcal{X} \cap \mathcal{Q})$ where H_2 is the hyperplane defined by the linear form $h_1 - h_2$. We also have $|H_2 \cap \mathcal{X} \cap \mathcal{Q}| \leq 4q+1$ from table 4 and $|H_1 \cap \mathcal{X}| \leq q^2 + 2q + 1$. Therefore we get that $|\mathcal{X} \cap \mathcal{Q}| \leq q^2 + 6q + 2$.

(iii) If for $i = 1, ..., q+1$ we get $\hat{\mathcal{X}}_i \neq \hat{\mathcal{Q}}_i$, one has two possibilities: If the $q+1$ hyperplanes H_i are all non-tangent to $\mathcal{X}$, $\hat{\mathcal{X}}_i$ are non-degenerate quadrics and only the types 1 and 3 of the table 3 can appear. From table 4 and remark 3.13, we deduce that $|\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i| \leq 4q$. If there exists a hyperplane H_i tangent to $\mathcal{X}$, then from lemma 3.12, it is unique. Let H_1 be this tangent hyperplane, $\hat{\mathcal{X}}_1$ is a quadric cone and $\hat{\mathcal{X}}_1 \cap \hat{\mathcal{Q}}_1$ is of type 1 or 2. Therefore we get $|\hat{\mathcal{X}}_1 \cap \hat{\mathcal{Q}}_1| \leq 4q + 1$. Finally from relation

$$|\mathcal{X} \cap \mathcal{Q}| \leq |\hat{\mathcal{X}}_1 \cap \hat{\mathcal{Q}}_1| + \sum_{i=2}^{q+1} |(\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i) - (\mathcal{D}_1 \cup \mathcal{D}_2)| \qquad (6)$$

we deduce that, $|\mathcal{X} \cap \mathcal{Q}| \leq 2q^2 + 3q + 1$.

4 The parameters of the code $C_2(\mathcal{X})$ defined on the quadric $\mathcal{X}$

When $\mathcal{X} = Z(f') \subset \mathbb{P}^n(\mathbb{F}_q)$ is a quadric, the linear map $c : \mathcal{F}_2 \longrightarrow \mathbb{F}_q^{|\mathcal{X}|}$ is not injective because $\ker c = \{\lambda f' | \lambda \in \mathbb{F}_q\}$. Therefore we deduce that:

$$\dim\ C_2(\mathcal{X}) = \begin{pmatrix} n+2 \\ 2 \end{pmatrix} - 1 = \frac{n(n+3)}{2}$$

From the results of section 3, we deduce the followings results.

Theorem 4.1 *Let $\mathcal{Q}$ be a quadric in $\mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{X}$ the non-degenerate (parabolic) quadric in $\mathbb{P}^4(\mathbb{F}_q)$. We get*

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 2q^2 + 3q + 1$$

and this bound is the best possible.
The code $C_2(\mathcal{X})$ defined on the parabolic quadric $\mathcal{X}$ is a $[n, k, d]_q$-code where $n = (q+1)(q^2+1)$, $k = 14$, $d = q^3 - q^2 - 2q$.

Theorem 4.2 *The minimum weight codewords of the code $C_2(\mathcal{X})$ correspond to:*
–either quadrics which are union of two (non-tangent) hyperplanes each intersecting $\mathcal{X}$ at a hyperbolic quadric such that the plane of intersection of the two hyperplanes intersects $\mathcal{X}$ at a plane conic.
–or quadrics with $r(\mathcal{Q}) = 3$ (i.e. $q+1$ planes through a line) and each plane containing exactly two lines of $\mathcal{X}$.
–or non-degenerate (i.e. parabolic) quadrics containing two secant lines of $\mathcal{X}$ defining a plane contained in the $q+1$ hyperplanes which has one tangent hyperplane, the q other non-tangent to $\mathcal{X}$, and with maximal hyperplane section.

Theorem 4.3 *Let $\mathcal{Q}$ be a quadric in $\mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{X}$ a degenerate quadric in $\mathbb{P}^4(\mathbb{F}_q)$. We get :*
–If $\mathcal{X}$ is degenerate with $r(\mathcal{X}) = 3$, then

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 4q^2 + q + 1 \quad \text{or} \qquad \#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

–If $\mathcal{X}$ is degenerate with $r(\mathcal{X})$=4 and $g(\mathcal{X}) = 2$, then

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 4q^2 + 1 \quad \text{or} \qquad \#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

Theorem 4.4 *The code $C_2(\mathcal{X})$ defined on the degenerate quadric $\mathcal{X}$ in PG(4,q) is a $[n, k, d]_q$-code where:*
–If $\mathcal{X}$ is degenerate with $r(\mathcal{X})$=3, then $n = q^3+q^2+q+1$, $k = 14$, $d = q^3-3q^2$.
–If $\mathcal{X}$ is degenerate with $r(\mathcal{X})$=4 and $g(\mathcal{X}) = 2$, then $n = q^3 + 2q^2 + q + 1$, $k = 14$, $d = q^3 - 2q^2 + q$.

Theorem 4.5 *The minimum weight codewords of the code $C_2(\mathcal{X})$ correspond :*
For $\mathcal{X}$ degenerate with $r(\mathcal{X})$=3 to:
–quadrics which are union of two hyperplanes (non-tangent) each through a

pair of planes and the plane of intersection of the two hyperplanes intersecting $\mathcal{X}$ in a line.
–quadrics with $r(\mathcal{Q}) = 3$ and a plane containing exactly four lines of $\mathcal{X}$.
For $\mathcal{X}$ degenerate quadric with $r(\mathcal{X}) = 4$ and $g(\mathcal{X}) = 2$:
–quadrics which are union of two tangent hyperplanes to $\mathcal{X}$ and the plane of intersection of the two hyperplanes meeting $\mathcal{X}$ at two secant lines.
–quadrics with $r(\mathcal{Q}) = 4$ and $g(\mathcal{Q}) = 2$ containning exactly four common planes of $\mathcal{X}$ with the following configuration: (the two first planes $\Pi_2^{(1)}$ and $\Pi_2^{(2)}$ meet at the point Π_0, and the two others planes $\Pi_2^{(3)}$ and $\Pi_2^{(4)}$ meet at the point Π_0,
the plane $\Pi_2^{(1)}$ meets $\Pi_2^{(3)}$ and $\Pi_2^{(4)}$ respectively at two distinct lines $\mathcal{D}_{1,3}$ and $\mathcal{D}_{1,4}$,
the plane $\Pi_2^{(2)}$ meets $\Pi_2^{(3)}$ and $\Pi_2^{(4)}$ respectively at two distinct lines $\mathcal{D}_{2,3}$ and $\mathcal{D}_{2,4}$,
each one of the four lines $\mathcal{D}_{1,3}$, $\mathcal{D}_{1,4}$, $\mathcal{D}_{2,3}$ and $\mathcal{D}_{2,4}$ pass through the point Π_0).

Theorem 4.6 *Let $\mathcal{Q}$ be a quadric in $\mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{X}$ a degenerate quadric in $\mathbb{P}^4(\mathbb{F}_q)$ of rank $(\mathcal{X}) = 4$ with $g(\mathcal{X}) = 1$. We get :*

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 3q^2 + q + 1.$$

The code $C_2(\mathcal{X})$ defined on the degenerate quadric $\mathcal{X}$ of rank($\mathcal{X}$)=4 with $g(\mathcal{X}) = 1$ is a $[n, k, d]_q$-code where $n = q^3 + q + 1$, $k = 14$, $d \geq q^3 - 3q^2$.

Remark 4.7 *From the study of the parameters of these codes, we can assert that the performances of the codes $C_2(\mathcal{X})$ defined on the non-degenerate quadrics are better than the ones defined on the degenerate quadrics.*

5 Quadratic section of the non-degenerate hermitian variety

In this section $\mathbb{F}_q$ denotes the field with q elements, where $q = t^2$ and $\mathcal{X}$ denotes the non-degenerate (i.e. non-singular) hermitian variety of $\mathbb{P}^4(\mathbb{F}_q)$ of equation $\mathcal{X} : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} + x_4^{t+1} = 0$.
In [3, p.1175] Bose and Chakravarti proved the following result:

Theorem 5.1 *Let $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ be a non-degenerate hermitian variety. Then,*

$$\#\tilde{\mathcal{X}}(\mathbb{F}_q) = \Upsilon(n, t^2) = [t^{n+1} - (-1)^{n+1}][t^n - (-1)^n]/(t^2 - 1) \qquad (7)$$

For $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ a degenerate hermitian variety of rank $r < n+1$, we have:

$$\#\tilde{\mathcal{X}}(\mathbb{F}_q) = (t^2-1)\pi_{n-r}\Upsilon(r-1,t^2) + \pi_{n-r} + \Upsilon(r-1,t^2),$$

where $\Upsilon(n,t^2)$ is given by (7).

From theorem 5.1 we get that

$$\#\mathcal{X}(\mathbb{F}_q) = (t^2+1)(t^5+1).$$

It has been shown by Bose et al. [3, p.1176] that $\mathrm{g}(\mathcal{X}) = 1$ (i.e. $\mathcal{X}$ contains lines and does not contain a plane). In the work of Hirschfeld [9, p.60] we get that there are t^3+1 lines contained in $\mathcal{X}$ through each point of $\mathcal{X}$.

We will study here the section of $\mathcal{X}$ by any quadric $\mathcal{Q}$ of $\mathbb{P}^4(\mathbb{F}_q)$. An approach to this problem has also been considered by F. Rodier in [14, pp.207-208]. He used the result of G. Lachaud [10, proposition 2.3] which gives an upper bound for the number of rational points of an algebraic set of a given degree. He found a bound which is not optimal.
We will use a different method depending mainly on the geometric structure of the quadric $\mathcal{Q}$ and the hermitian variety $\mathcal{X}$.
Let us recall the classification of hermitian varieties in $\mathbb{P}^3(\mathbb{F}_q)$, table.5, which can be found in the work of J.W.P. Hirschfeld [9, p.60].

$\mathrm{r}(\mathcal{V})$	Description	$\lvert\mathcal{V}\rvert$	$\mathrm{g}(\mathcal{V})$
1	repeated plane $\Pi_2\mathcal{U}_0$	t^4+t^2+1	2
2	$t+1$ collinear planes $\Pi_1\mathcal{U}_1$	$t^5+t^4+t^2+1$	2
3	a cone $\Pi_0\mathcal{U}_2$	t^5+t^2+1	1
4	non-singular hermitian surface $\mathcal{U}_3$	$t^5+t^3+t^2+1$	1

Table 5: Hermitian surfaces in $\mathbb{P}^3(\mathbb{F}_q)$

5.1 Plane section of the non-degenerate hermitian variety $\mathcal{X}$: $\mathrm{g}(\mathcal{Q})$=2

We are interested in the case where $\mathrm{g}(\mathcal{Q})$=2 for the quadric $\mathcal{Q}$. These are the cases where $\mathcal{Q} = \Pi_2\mathcal{E}_1$, $\mathcal{Q} = \Pi_1\mathcal{P}_2$ or $\mathcal{Q} = \Pi_0\mathcal{H}_3(\mathcal{R},\mathcal{R}')$. In the book of J. W. P. Hirschfeld [7, p.160], we have also the classification of plane hermitian curves.

r($\mathcal{V}$)	Description	$\lvert\mathcal{V}\rvert$	g($\mathcal{V}$)
1	repeated line $\Pi_1\mathcal{U}_0$	t^2+1	1
2	cone $\Pi_0\mathcal{U}_1$	t^3+t^2+1	1
3	non-singular hermitian curve $\mathcal{U}_2$	t^3+1	0

Table 6: Plane hermitian curves

From the table above, for the section of the non-singular hermitian variety $\mathcal{X}$ by a plane $\mathcal{Q}$ we get $|\mathcal{X}\cap\mathcal{Q}| \leq t^3+t^2+1$. In the case $\mathrm{r}(\mathcal{Q}) = 3$ or $\mathrm{r}(\mathcal{Q}) = 4$, ($\mathcal{Q}$ is a union of $q+1$ planes) we get $|\mathcal{X} \cap \mathcal{Q}| \leq t^5+t^4+t^3+2t^2+1$.

5.2 Hyperplane section of the non-degenerate hermitian variety $\mathcal{X}$: g($\mathcal{Q}$)=3

In the case g($\mathcal{Q}$)=3, i.e. when $\mathcal{Q}$ contains a hyperplane, we have two possibilities: r($\mathcal{Q}$)=1 ($\mathcal{Q}$ is a hyperplane), or r($\mathcal{Q}$)=2 and $\mathcal{Q}$ is a pair of distinct hyperplanes.

5.2.1 $\mathcal{Q}$ is a quadric with r($\mathcal{Q}$)=1: $\mathcal{Q} = \Pi_3\mathcal{P}_0$

Here $\mathcal{Q}$ is a repeated hyperplane H. Let us recall two general results of Bose and Chakravarti on hyperplane section of a non-degenerate hermitian variety.

Theorem 5.2 *[3, p.1173] Let $\tilde{\mathcal{X}}$ be a non-degenerate hermitian variety in $\mathbb{P}^n(\mathbb{F}_q)$ and H a hyperplane. If H is tangent to $\tilde{\mathcal{X}}$ at P, then $\tilde{\mathcal{X}} \cap H$ is a degenerate hermitian variety of rank $n-1$ in $\mathbb{P}^{n-1}(\mathbb{F}_q)$. The singular space of $\tilde{\mathcal{X}} \cap H$ consists of the single point P.*

Theorem 5.3 *[4, p.272] Let $\tilde{\mathcal{X}}$ be a non-degenerate hermitian variety in $\mathbb{P}^n(\mathbb{F}_q)$ and H a hyperplane. If H is not tangent to $\tilde{\mathcal{X}}$, then $\tilde{\mathcal{X}} \cap H$ is a non-degenerate variety in $\mathbb{P}^{n-1}(\mathbb{F}_q)$.*

From theorems 5.1, 5.2 and 5.3, we deduce the following result.

Theorem 5.4 *Let $H \subset \mathbb{P}^4(\mathbb{F}_q)$ be a hyperplane*

$$\#\mathcal{X}_H(\mathbb{F}_q) = \begin{cases} t^5+t^3+t^2+1 & \text{if } H \text{ is not tangent to } \mathcal{X}, \\ t^5+t^2+1 & \text{if } H \text{ is tangent to } \mathcal{X}. \end{cases}$$

If H is tangent to $\mathcal{X}$, then $\mathcal{X} \cap H$ is a singular hermitian surface of rank 3 in $\mathbb{P}^3(\mathbb{F}_q)$. More precisely, $\mathcal{X} \cap H$ is a set of t^3+1 lines passing through a common point P. If H is non-tangent to $\mathcal{X}$, then $\mathcal{X} \cap H$ is a non-singular hermitian surface in $\mathbb{P}^3(\mathbb{F}_q)$; thus we get $\#\mathcal{X}_H(\mathbb{F}_q) = t^5 + t^3 + t^2 + 1$.

5.2.2 $\mathcal{Q}$ is a quadric with r($\mathcal{Q}$)=2 and $\mathcal{Q}$ is a pair of hyperplanes

Here we will also use two important results of Bose and Charkravarti on degenerate hermitian varieties in $\mathbb{P}^n(\mathbb{F}_q)$.

Theorem 5.5 *[3, p.1171] Let $\tilde{\mathcal{X}}$ be a degenerate hermitian variety of rank $r < n+1$ in $\mathbb{P}^n(\mathbb{F}_q)$ and Π_{r-1} a linear projective space of dimension $r-1$ disjoint from the singular space Π_{n-r} of $\tilde{\mathcal{X}}$. Then $\Pi_{r-1} \cap \tilde{\mathcal{X}}$ is a non-degenerate hermitian variety in Π_{r-1}.*

Theorem 5.6 *[3, p.1171] Let $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ be a degenerate hermitian variety of rank $r < n+1$. If P is any point belonging to the singular space of $\tilde{\mathcal{X}}$ and D is an arbitrary point of $\tilde{\mathcal{X}}$, then any point of the line (PD) belongs to $\tilde{\mathcal{X}}$.*

Now let H_1 and H_2 be two distinct hyperplanes generating $\mathcal{Q}$. We have $\mathcal{Q} = H_1 \cup H_2$. Let $\mathcal{P} = H_1 \cap H_2$ be the plane of intersection of the two hyperplanes. Let $\hat{\mathcal{X}}_1 = H_1 \cap \mathcal{X}$, and $\hat{\mathcal{X}}_2 = H_2 \cap \mathcal{X}$.

(i) In the case where each hyperplane is tangent to $\mathcal{X}$, we know that $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$ as singular hermitian surfaces are sets of t^3+1 lines passing respectively through the point P_1 and P_2 ($P_1 \neq P_2$). From theorem 5.2, we deduce that P_1 and P_2 are the singular spaces of $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$.
–If the plane $\mathcal{P}$ does not pass through at least one of the two points P_1 and P_2, without loss of generality we can suppose that $\mathcal{P}$ does not pass through P_1. Since P_1 is the singular space of $\hat{\mathcal{X}}_1$, from theorem 5.5 we deduce that $\mathcal{P} \cap \hat{\mathcal{X}}_1$ is a non-singular curve in $\mathbb{P}^2(\mathbb{F}_q)$. Therefore, we get $|\mathcal{P} \cap \hat{\mathcal{X}}_1| = t^3+1$, which with the relations (3) and (4) give $|\mathcal{X} \cap \mathcal{Q}| = 2t^5 - t^3 + 2t^2 + 1$.
–If the plane $\mathcal{P}$ passes through P_1 and P_2, then it is obvious that P_1 and P_2 belong to $\mathcal{P} \cap \hat{\mathcal{X}}_1$ and $\mathcal{P} \cap \hat{\mathcal{X}}_2$ respectively. From the relation (4), we deduce that $P_2 \in \mathcal{P} \cap \hat{\mathcal{X}}_1$. Therefore $P_2 \in \hat{\mathcal{X}}_1$. Since P_1 is the singular space of $\hat{\mathcal{X}}_1$, from theorem 5.6 we deduce that the line (P_1P_2) is contained in $\hat{\mathcal{X}}_1$. The line (P_1P_2) is also contained in $\mathcal{P}$. Therefore (P_1P_2) is contained in $\mathcal{P} \cap \hat{\mathcal{X}}_1$ and from table 6, we get that $\mathcal{P} \cap \hat{\mathcal{X}}_1$ is a degenerate hermitian curve in $\mathbb{P}^2(\mathbb{F}_q)$. Here $\mathcal{P} \cap \hat{\mathcal{X}}_1$ cannot be a set of $t+1$ lines through a common point, because it would imply

$P_1 = P_2$. Thus, $\mathcal{P} \cap \hat{\mathcal{X}}_1$ is the line defined by the two points P_1 and P_2. Therefore, from the relations (3) and (4) we get $|\mathcal{X} \cap \mathcal{Q}| = 2t^5 + t^2 + 1$.

(ii) In the case where one hyperplane (H_2) is tangent to $\mathcal{X}$ and the second hyperplane (H_1) is non-tangent to $\mathcal{X}$, $\hat{\mathcal{X}}_2$ and $\hat{\mathcal{X}}_1$ are singular and non-singular hermitian surfaces respectively. From theorems 5.2, 5.5 and relation (4) we deduce that the following two conditions are equivalent:
–the plane $\mathcal{P}$ is non-tangent to $\hat{\mathcal{X}}_1$
–the plane $\mathcal{P}$ is disjoint from the singular space $\{P_2\}$ of $\hat{\mathcal{X}}_2$
Therefore, from the theorems above and relation (3) we get either $|\mathcal{X} \cap \mathcal{Q}| = 2t^5 + 2t^2 + 1$ when $\mathcal{P}$ is non-tangent to $\hat{\mathcal{X}}_1$ or $|\mathcal{X} \cap \mathcal{Q}| = 2t^5 + t^2 + 1$ when $\mathcal{P}$ is tangent to $\hat{\mathcal{X}}_1$.

(iii) In the case where both hyperplanes are non-tangent to $\mathcal{X}$, we know that $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$ are both non-singular hermitian surfaces. From the relation (4) and the fact that $\mathcal{P} \cap \hat{\mathcal{X}}_1$ (resp. $\mathcal{P} \cap \hat{\mathcal{X}}_2$) is singular if and only if $\mathcal{P}$ is tangent to $\hat{\mathcal{X}}_1$ (resp. $\hat{\mathcal{X}}_2$), we deduce that $\mathcal{P}$ is either tangent to $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$, or non-tangent to $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$.
–If the plane $\mathcal{P}$ is tangent to $\hat{\mathcal{X}}_1$ (i.e. it is also tangent to $\hat{\mathcal{X}}_2$), then from theorem 5.2, $\mathcal{P} \cap \hat{\mathcal{X}}_1$ is a singular hermitian curve of rank 2 in $\mathbb{P}^2(\mathbb{F}_q)$. Therefore, we get $|\mathcal{P} \cap \hat{\mathcal{X}}_1| = t^3 + t^2 + 1$, which with the relation (3) give $|\mathcal{X} \cap \mathcal{Q}| = 2t^5 + t^3 + t^2 + 1$
–If the plane $\mathcal{P}$ is non-tangent to $\hat{\mathcal{X}}_1$ (i.e. it is also non-tangent to $\hat{\mathcal{X}}_2$), $\mathcal{P} \cap \hat{\mathcal{X}}_1$ is a non-singular hermitian curve in $\mathbb{P}^2(\mathbb{F}_q)$. Therefore, we get $|\mathcal{P} \cap \hat{\mathcal{X}}_1| = t^3 + 1$, which with the relation (3) give $|\mathcal{X} \cap \mathcal{Q}| = 2t^5 + t^3 + 2t^2 + 1$.

5.3 Line section of the non-degenerate hermitian variety $\mathcal{X}$: g($\mathcal{Q}$)=1

We will now study the section of the non-degenerate hermitian variety $\mathcal{X}$ by $\mathcal{Q}$ with g($\mathcal{Q}$)=1. In this case $\mathcal{Q}$ is the non-degenerate quadric (parabolic) or the degenerate quadric $\Pi_0\mathcal{E}_3$.
For the section of $\mathcal{X}$ by $\mathcal{Q}$ we need to distinguish two cases.

5.3.1 $\mathcal{Q} \cap \mathcal{X}$ does not contain any line

When $\mathcal{Q}$ is degenerate (i.e. $\mathcal{Q} = \Pi_0\mathcal{E}_3$) and $\mathcal{Q} \cap \mathcal{X}$ does not contain any line, every line of $\mathcal{Q}$ intersects $\mathcal{X}$ in at most $t+1$ points. From the fact that $\mathcal{Q}$ consists of $q^2 + 1$ lines through the point Π_0, we deduce that $|\mathcal{Q} \cap \mathcal{X}| \leq t^5 + t^4 + t + 1$.

When $\mathcal{Q}$ is non-degenerate, it contains exactly α_q lines and there are $q+1$ lines of $\mathcal{Q}$ through any point of $\mathcal{Q}$. Therefore, we deduce that $|\mathcal{Q} \cap \mathcal{X}| \leq \alpha_q(t+1)/(q+1)$ i.e. $|\mathcal{Q} \cap \mathcal{X}| \leq t^5 + t^4 + t + 1$.

5.3.2 $\mathcal{Q} \cap \mathcal{X}$ contains a line

First, we will study the simple case of the section of $\mathcal{X}$ by the degenerate quadric. Next, we will treat the more technical case, section of $\mathcal{X}$ by the non-degenate quadric.

5.3.2.1 When $\mathcal{Q}$ is degenerate: We get two possibilities:
– If there is no line of $\mathcal{X} \cap \mathcal{Q}$ through the vertex Π_0 of the cone $\Pi_0\mathcal{E}_3$, as in 5.3.1 we deduce that $|\mathcal{X} \cap \mathcal{Q}| \leq t^5 + t^4 + t + 1$.
– If there is a line of $\mathcal{X} \cap \mathcal{Q}$ through the vertex Π_0 of the cone, it is obvious that Π_0 is a point of $\mathcal{X}$. Therefore, there are at most $t^3 + 1$ lines of $\mathcal{Q}$ contained in $\mathcal{X}$. Each one of the other $t^4 - t^3$ lines of $\mathcal{Q}$ intersects $\mathcal{X}$ in at most $t+1$ points. Thus, we deduce that $|\mathcal{Q} \cap \mathcal{X}| \leq 2t^5 - t^4 + t^2 + 1$.

5.3.2.2 When $\mathcal{Q}$ is non-degenerate: We will use the same technique as in §3.3.2 (intersection of two non-degenerate quadrics). Let us consider a line $\mathcal{D}$ contained in $\mathcal{Q} \cap \mathcal{X}$, $\mathcal{P}$ a plane through $\mathcal{D}$ and (H_i) the $q+1$ hyperplanes passing through $\mathcal{P}$ which generate $\mathbb{P}^4(\mathbb{F}_q)$. As in §3.3.2, for $i = 1, ..., q+1$ $\hat{\mathcal{Q}}_i = H_i \cap \mathcal{Q}$ are either hyperbolic quadrics or cone quadrics in $\mathbb{P}^3(\mathbb{F}_q)$. From theorems 5.2, 5.3 we get that for $i = 1, ..., q+1$, $\hat{\mathcal{X}}_i = H_i \cap \mathcal{X}$ are hermitian surfaces of rank 3 or 4 (non-singular hermitian surfaces) in $\mathbb{P}^3(\mathbb{F}_q)$.
Thus, one has to study the four types of intersection in $\mathbb{P}^3(\mathbb{F}_q)$ given by the table 7.

Type	$\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$
1	(hyperbolic quadric) $\cap$ (non − sing herm surf)
2	(quadric cone) $\cap$ (non − sing herm surf)
3	(hyperbolic quadric) $\cap$ (sing herm surface)
4	(quadric cone) $\cap$ (sing hermitian surface)

Table 7: Intersection of $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$ in $\mathbb{P}^3(\mathbb{F}_q)$

From the paragraphs 4.1 and 4.2 of [6], we can be more precise about

$\#\hat{\mathcal{X}}_{i_{Z(\hat{\mathcal{Q}}_i)}}(\mathbb{F}_q)$ for the types 1 and 2 of table 7 (section of the non-singular hermitian surface $\hat{\mathcal{X}}_i$ by a cone or hyperbolic quadric $\hat{\mathcal{Q}}_i$). Thus, we have the following table 8.

r($\hat{\mathcal{Q}}_i$)	Type	$L(\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i)$	$\#\hat{\mathcal{X}}_{i_{Z(\hat{\mathcal{Q}}_i)}}(\mathbb{F}_q)$
3 (cone)	2	2	t^3+2t^2-t+1
		1	t^3+t^2+1
4 (hyperbolic) $\mathcal{H}_3(\mathcal{R}_i,\mathcal{R}'_i)$	1	3	$2t^3+t^2+1$
		2	$\leq t^3+3t^2-t+1$
		1	$\leq t^3+2t^2+1$

Table 8: Number of points and lines in $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$

In table 8, $\hat{\mathcal{X}}_i$ and $L(\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i)$ denote respectively the non-degenerate hermitian surface and the number of lines contained in $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$. In the case where $\hat{\mathcal{Q}}_i$ is a hyperbolic, we consider $L(\hat{\mathcal{X}}_i \cap \mathcal{R}_i)$ (where $\mathcal{R}_i$ is a regulus of the hyperbolic quadric $\hat{\mathcal{Q}}_i$) instead of $L(\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i)$.

From the tables above, we deduce that an estimation on the number of points in the intersection of $\mathcal{X} \cap \mathcal{Q}$ where $\mathcal{X}$ and $\mathcal{Q}$ are respectively a non-degenerate hermitian variety and a non-degenerate quadric variety with a common line, is resolved by considering the two following simple cases.

(a) If $\mathcal{Q} \cap \mathcal{X}$ contains exactly one common line: From table 8, we get $|\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3+2t^2+1$ for the types 1 and 2 of table 7.
Likewise, for the type 3, if $\hat{\mathcal{Q}}_i$ and $\hat{\mathcal{X}}_i$ contain exactly the only common line $\mathcal{D}$, a fortiori there is a regulus $\mathcal{R}_i$ of the hyperbolic quadric $\hat{\mathcal{Q}}_i$ containing $\mathcal{D}$. Each one of the q other lines of $\mathcal{R}_i$ intersects $\hat{\mathcal{X}}_i$ in at most $t+1$ points. We deduce that $|\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3+2t^2+1$.
For the type 4, the quadric cone $\hat{\mathcal{Q}}_i$ consists of $q+1$ lines through a common point. The fact that there is only one line of $\hat{\mathcal{Q}}_i$ in $\hat{\mathcal{X}}_i$, implies that each one of the q other lines of $\hat{\mathcal{Q}}_i$ intersects $\hat{\mathcal{X}}_i$ in at most $t+1$ points (the vertex of the cone is one of them). We deduce that $|\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3+t^2+1$.
Finally, when $\mathcal{Q} \cap \mathcal{X}$ contains exactly one common line, we get:

$$\text{for} \quad i=1,2,...,q+1 \quad |\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3+2t^2+1. \tag{8}$$

In this way, by using the relations (5) and (8) we conclude that $|\mathcal{Q} \cap \mathcal{X}| \leq t^5+t^4+t^3+2t^2+1$.

(b) If $\mathcal{Q} \cap \mathcal{X}$ contains at least two common lines: We distinguish two cases: $\mathcal{Q} \cap \mathcal{X}$ containing only skew lines or some secant lines. We will use an important property on the intersection of a hyperbolic quadric and a non-singular hermitian surface in $\mathbb{P}^3(\mathbb{F}_q)$.

Lemma 5.7 *[8, pp.123-124] Let $\hat{\mathcal{Q}}_i = \mathcal{H}(\mathcal{R}_i, \mathcal{R}'_i)$ and $\hat{\mathcal{X}}_i$ denote respectively the hyperbolic quadric and the non-singular hermitian surface in $\mathbb{P}^3(\mathbb{F}_q)$. If $\hat{\mathcal{Q}}_i = \mathcal{H}(\mathcal{R}_i, \mathcal{R}'_i)$ has three skew lines on $\hat{\mathcal{X}}_i$, then $\hat{\mathcal{X}}_i \cap \hat{\mathcal{Q}}_i$ consists of $2(t+1)$ lines of $\mathcal{R}_0 \cup \mathcal{R}'_0$ where $\mathcal{R}_0 \subset \mathcal{R}_i$, $\mathcal{R}'_0 \subset \mathcal{R}'_i$ and $|\mathcal{R}'_0| = |\mathcal{R}_0| = t+1$.*

Remark 5.8 *Lemma 5.7 says that, if a hyperbolic quadric contains three skew lines on the non-singular hermitian surface $\hat{\mathcal{X}}_i$, then it contains exactly $2(t+1)$ lines of the surface $\hat{\mathcal{X}}_i$, and $t+1$ lines in each of the two reguli.*

We will also use the following result.

Lemma 5.9 *Let $\mathcal{D}_1$, $\mathcal{D}_2$ be two secant lines of the non-degenerate hermitian variety $\mathcal{X} \subset \mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{P} =< \mathcal{D}_1, \mathcal{D}_2 >$ the plane defined by these two lines. Let (H_i) i=1,...,q+1 be the $q+1$ hyperlanes containing $\mathcal{P}$. If there exists a hyperplane H_1 tangent to $\mathcal{X}$, then it is unique (i.e. the remaining q hyperplanes are non-tangent to $\mathcal{X}$).*

The proof of this lemma is analogous to the one of lemma 3.12.

(i) If $\mathcal{Q} \cap \mathcal{X}$ contains only skew lines.
For the types 2 and 4 of table 7, since the quadric cone consists of $q+1$ lines through a common point, we deduce that $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$ contains exactly one common line. And therefore from table 8, we get that $|\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3 + t^2 + 1$ for the type 2. For the type 4, we also have $|\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3 + t^2 + 1$ as in the subparagraph (a) above.
For the type 3, since the singular hermitian surface $\hat{\mathcal{X}}_i$ is a set of t^3+1 lines through a common point, we also deduce that $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$ contains exactly one common line. Thus, as in subparagraph (a), we get $|\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3 + 2t^2 + 1$.
For the type 1, from remark 5.8, we deduce that $\hat{\mathcal{Q}}_i$ as a hyperbolic quadric in $\mathbb{P}^3(\mathbb{F}_q)$, cannot contain three skew lines of $\hat{\mathcal{X}}_i$. Otherwise $\hat{\mathcal{Q}}_i$ would contain two secant lines of $\hat{\mathcal{X}}_i$. Thus, under the condition of the non-existence of secant lines in $\mathcal{Q} \cap \mathcal{X}$, any regulus of $\hat{\mathcal{Q}}_i$ contains at most two skew lines of $\hat{\mathcal{X}}_i$ and therefore from the table 8, we get $|\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3 + 3t^2 - t + 1$.
Finally, when $\mathcal{Q} \cap \mathcal{X}$ contains only skew lines, we get:

$$\text{for} \quad i = 1, 2, ..., q+1 \quad |\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq t^3 + 3t^2 - t + 1. \tag{9}$$

In this way, by using the relations (5) and (9) we conclude that $|\mathcal{Q} \cap \mathcal{X}| \leq t^5 + 2t^4 - 3t^2 + 1$.

(ii) If $\mathcal{Q} \cap \mathcal{X}$ contains some secant lines, let $(\mathcal{D}_1)$ and $(\mathcal{D}_2)$ be two of them (which are not skew) and $\mathcal{P}$ the plane generated by them. One has two cases:
– The $q+1$ hyperplanes H_i are all non-tangent to $\mathcal{X}$: in this case $\hat{\mathcal{X}}_i$ is a non-singular hermitian surface. From the four types of table 7, only the first two types appear in this case. From the table 8, we deduce that

$$\text{for} \quad i = 1, 2, ..., q+1 \quad |\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i| \leq 2t^3 + t^2 + 1. \tag{10}$$

Thus, from (6) and (10) we get $|\mathcal{Q} \cap \mathcal{X}| \leq 2t^5 - t^4 + 2t^3 + t^2 + 1$.
– If the $q+1$ hyperplanes are not all non-tangent to $\mathcal{X}$, from lemma 5.9, there is a unique tangent hyperplane to $\mathcal{X}$, say H_1. Now, $\hat{\mathcal{Q}}_1 \cap \hat{\mathcal{X}}_1$ can be of the types 3 and 4.
For the type 3, $\hat{\mathcal{Q}}_1$ and $\hat{\mathcal{X}}_1$ contain exactly two common lines. Each one of the remaining $t^3 - 1$ lines of $\hat{\mathcal{X}}_1$ intersects $\hat{\mathcal{Q}}_1$ in at most two points (the vertex of $\hat{\mathcal{X}}_1$ is one of them). We deduce that $|\hat{\mathcal{Q}}_1 \cap \hat{\mathcal{X}}_1| \leq t^3 + 2t^2$.
For the type 4, let $t \geq 3$, from the Bézout theorem, we deduce that $\deg(\hat{\mathcal{Q}}_1 \cap \hat{\mathcal{X}}_1) \leq 2(t+1)$. Therefore $\hat{\mathcal{Q}}_1 \cap \hat{\mathcal{X}}_1$ contains at most $2(t+1)$ lines. Without loss of generality we can assume that $\hat{\mathcal{Q}}_1 \cap \hat{\mathcal{X}}_1$ contains exactly $2(t+1)$ lines. If we suppose that each one of the remaining $t^2 - 2t - 1$ lines of the quadric cone $\hat{\mathcal{Q}}_1$ intersects $\hat{\mathcal{X}}_1$ at $t+1$ points, we get that $|\hat{\mathcal{Q}}_1 \cap \hat{\mathcal{X}}_1| \leq 3t^3 - t + 1$. For $t = 2$, we get obviously $|\hat{\mathcal{Q}}_1 \cap \hat{\mathcal{X}}_1| \leq |\hat{\mathcal{Q}}_1| = t^4 + t^2 + 1$.
Thus, when there is a unique hyperplane tangent to $\mathcal{X}$, from (6) we get that:

$$|\mathcal{X} \cap \mathcal{Q}| \leq \begin{cases} 2t^5 + t^2 + 1 & \text{if } t = 2, \\ 2t^5 - t^4 + 3t^3 - t + 1 & \text{if } t \geq 3. \end{cases}$$

6 The parameters of the code $C_2(\mathcal{X})$ defined on the non-degenerate hermitian variety $\mathcal{X}$

From the results of section 5, we deduce the following results.

Theorem 6.1 *Let $\mathcal{Q}$ be a quadric in $\mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{X}$ the non-degenerate hermitian variety $\mathcal{X} : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} + x_4^{t+1} = 0$, we get*

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2t^5 + t^3 + 2t^2 + 1,\ 2t^5 + t^3 + t^2 + 1$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2t^5 + 2t^2 + 1,\ 2t^5 + t^2 + 1,$$

$$\text{and for } t \neq 2,3 \quad \#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = \begin{cases} 2t^5 - t^3 + 2t^2 + 1 \\ \quad or \\ \leq 2t^5 - t^4 + 3t^3 - t + 1. \end{cases}$$

Theorem 6.2 *(Serre-Sørensen)([16, p.351], [17, chp.2, pp.7-10]) Let $f(x_0, ..., x_m)$ be a homogeneous polynomial in $m+1$ variables with coefficients in $\mathbb{F}_q$ and degree $h \leq q$. Then the number of zeros of f in $\mathbb{P}^m(\mathbb{F}_q)$ satisfies:*

$$\#Z_{(f)}(\mathbb{F}_q) \leq hq^{m-1} + \pi_{m-2}.$$

This upper bound is attained when $Z_{(f)}$ is a union of h hyperplanes passing through a common linear space of codimension 2.

Theorem 6.3 *The code $C_2(\mathcal{X})$ defined on the hermitian variety $\mathcal{X} : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} + x_4^{t+1} = 0$ is a $[n, k, d]_q$-code where $n = (t^2 + 1)(t^5 + 1)$, $k = 15$, $d = t^7 - t^5 - t^3 - t^2$.*

Proof: Here we need to prove that the linear map $c : \mathcal{F}_2 \longrightarrow \mathbb{F}_q^{|\mathcal{X}|}$ is injective. In general, when f is an homogeneous polynomial of degree h in the affine space $\mathbb{A}^5(\mathbb{F}_q)$, by the Serre-Sørensen's bound on hypersurfaces, we deduce that $\#Z_{(f)}(\mathbb{F}_q) \leq ht^6+t^4+t^2+1$. From the fact that $\#\mathcal{X}(\mathbb{F}_q) = t^7+t^5+t^2+1$ we deduce that for $h \leq t$, the map c is injective. From the relation (1), we get that $k = 15$. From theorem 6.1 and the defintion of d at the end of section 2, we deduce that $d = \#\mathcal{X}(\mathbb{F}_q) - (2t^5+t^3+2t^2+1) = t^7 - t^5 - t^3 - t^2$.

Observe that theorem 6.3 gives the exact parameters (i.e. the minimum distance) of the codes $C_2(\mathcal{X})$ which cannot be found by F. Rodier in [14, pp.207-208].

Theorem 6.4 *The minimum weight codewords correspond to quadrics which are pair of hyperplanes non-tangent to $\mathcal{X}$ such that the plane of intersection of the two hyperplanes intersects $\mathcal{X}$ at a non-singular hermitian plane curve.*

Theorem 6.5 *The second weight of the code $C_2(\mathcal{X})$ is $t^7 - t^5 - t^3$. The codewords of second weight correspond to quadrics which are pair of hyperplanes non-tangent to $\mathcal{X}$ and the plane of intersection of the two hyperplanes intersecting $\mathcal{X}$ at a singular hermitian plane curve of rank 2 (i.e. a set of $t + 1$ lines through a common point).*

Theorem 6.6 *The third weight of the code $C_2(\mathcal{X})$ is $t^7 - t^5 - t^2$.*
The codewords of third weight correspond to quadrics which are pair of hyperplanes, one tangent to $\mathcal{X}$, the second non-tangent to $\mathcal{X}$ and such that the plane of intersection of the two hyperplanes intersects $\mathcal{X}$ at a non-singular hermitian plane curve.

Theorem 6.7 *The fourth weight of the code $C_2(\mathcal{X})$ is $t^7 - t^5$.*
The codewords of fourth weight correspond to:
–quadrics which are pair of hyperplanes, one tangent to $\mathcal{X}$, the second non-tangent to $\mathcal{X}$ and the plane of intersection of the two hyperplanes is tangent at the non-singular hermitian surface obtained from the second hyperplane.
–quadrics which are pair of tangent hyperplanes and the plane of intersection of the two hyperplanes intersecting $\mathcal{X}$ at a single line.

Theorem 6.8 *The fifth weight (for $t \neq 2, 3$) of the code $C_2(\mathcal{X})$ is $t^7 - t^5 + t^3 - t^2$.*
The codewords of fifth weight (for $t \neq 2, 3$) correspond to quadrics which are pair of tangent hyperplanes and the plane of intersection of the two hyperplanes intersecting $\mathcal{X}$ at a non-singular hermitian plane curve.

7 Conjectures

7.1 Conjecture on the minimum distance of the code $C_h(\mathcal{X})$ in $\mathbb{P}^4(\mathbb{F}_q)$

The author has tried to generalize the study of the code $C_2(\mathcal{X})$ to $C_h(\mathcal{X})$ where $\mathcal{X}$ is the non-degenerate hermitian variety defined by $x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} + x_4^{t+1} = 0$ in $\mathbb{P}^4(\mathbb{F}_q)$ $(q = t^2)$ and conjecture that:

Conjecture 1

$$\text{For} \quad h \leq t \quad \#\mathcal{X}_{Z(f)}(\mathbb{F}_q) \leq h(t^5 + t^2) + t^3 + 1.$$

This upper bound is the best possible. The minimum weight codewords correspond to hypersufaces which have the following configuration:
–hypersurfaces reaching the Serre-Sørensen's upper bound for hypersurfaces (i.e. union of h hyperplanes H_i passing through a common plane $\mathcal{P}$)
–each hyperplane H_i is non-tangent to $\mathcal{X}$
–and the plane $\mathcal{P}$ of intersection of the h hyperplanes intersecting $\mathcal{X}$ at a non-singular hermitian plane curve.

Unfortunately no proof has been found yet. In general, it seems that when we use this strategy of code-construction, the combinatorical complexity of finding the minimum distance increases drastically with the degree h.

Remark 7.1 *The preceding conjecture is true for $h = 1$ (theorem 5.4) and for $h = 2$ (theorems 6.1, 6.4) .*

7.2 Conjecture on the first five weights of the code $C_2(\mathcal{X})$ in $\mathbb{P}^n(\mathbb{F}_q)$

The author has also tried to generalize the study of the code $C_2(\mathcal{X})$ to $\mathcal{X}$ the non-degenerate hermitian variety defined by $x_0^{t+1} + x_1^{t+1} + ... + x_N^{t+1} = 0$ in $\mathbb{P}^N(\mathbb{F}_q)$ $(q = t^2)$ and conjecture that:

Conjecture 2

1 *If w_i $(1 \leq i \leq 5)$ are the first five weights of the code $C_2(\mathcal{X})$, then there exist degenerate quadrics $\mathcal{Q}$ reaching the Serre-Sørensen's upper bound for hypersurfaces (i.e. $\mathcal{Q}$ is a pair of distinct hyperplanes $\mathcal{Q} = H_1 \cup H_2$), giving codewords of weight w_i.*

2 *The mimimum weight (i.e. w_1) codewords are only given by degenerate quadrics which are pair of distinct hyperplanes ($\mathcal{Q} = H_1 \cup H_2$) such that $(H_1 \cap H_2) \cap \mathcal{X}$ is a non-singular hermitian variety in $\mathbb{P}^{N-2}(\mathbb{F}_q)$ and:*
–If N is even, the two hyperplanes H_1 and H_2 are non-tangent to $\mathcal{X}$
–If N is odd, the two hyperplanes H_1 and H_2 are tangent to $\mathcal{X}$.

3 *For $i > 5$, there is no quadric which is a pair of distinct hyperplanes, giving codewords of weight w_i.*

Unfortunately no proof has been found yet.

Remark 7.2 *The second part of conjecture 2 is true for $N = 3$ (see [6, § 4.1-4.2]). The conjecture is also true for $N = 4$: theorem 6.1, theorems 6.3 to 6.8 give the result.*

Acknowlegment The author thanks Prof. F. Rodier. His remarks and patience encouraged him to work on the problem.

References

[1] Y. Aubry, Reed-Muller codes associated to projective algebraic varieties. In "Algebraic Geomertry and Coding Theory ". (Luminy, France, June 17-21, 1991). Lecture Notes in

Math., Vol. 1518, Springer-Verlag, Berlin, (1992), 4-17.
[2] M. Boguslavsky, On the number of solutions of polynomial systems. Finite Fields and Their Applications 3 (1997), 287-299.
[3] R. C. Bose and I. M. Chakravarti, Hermitian varieties in finite projective space $PG(N, q)$. Canadian J. of Math.18 (1966), 1161-1182.
[4] I. M. Chakravarti, Some properties and applications of Hermitian varieties in finite projective space PG(N,q^2) in the construction of strongly regular graphs (two-class association schemes) and block designs, Journal of Comb. Theory, Series B, 11(3) (1971), 268-283.
[5] F. A. B. Edoukou, Codes defined by forms of degree 2 on quadric surfaces. arXiv:math. AG/0511679 v 1 28 Nov 2005. 5 pp., Submitted to IEEE. Trans. Inform. Theory (2005).
[6] F. A. B. Edoukou, The weight distribution of the functional codes defined by forms of degree 2 on hermitian surfaces. arXiv:math. AG/0512476 v 1 20 Dec 2005. 13 pp., Submitted to Finite Fields and Their Applications (2005).
[7] J. W. P. Hirschfeld, Projective Geometries Over Finite Fields (Second Edition) Clarendon Press. Oxford 1998.
[8] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Clarendon press. Oxford 1985.
[9] J. W. P. Hirschfeld, General Galois Geometies, Clarendon press. Oxford 1991.
[10] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties; in " Arithmetic, Geometry, and Coding Theory ". (Luminy, France, 1993), Walter de Gruyter, Berlin-New York, (1996), 77-104.
[11] D. B. Leep and L. M. Schueller, Zeros of a pair of quadric forms defined over finite field. Finite Fields and Their Applications 5 (1999), 157-176.
[12] E. J. F. Primrose, Quadrics in finite geometries, Proc. Camb. Phil. Soc., 47 (1951), 299-304.
[13] D. K. Ray-Chaudhuri, Some results on quadrics in finite projective geometrie based on Galois fields, Canadian J. Math. Vol. 14 (1962), 129-138.
[14] F. Rodier, Codes from flag varieties over a finite field, Journal of Pure and Applied Algebra 178 (2003), 203-214.
[15] P. Samuel, Géométrie projective, Presses Universitaires de France, 1986.
[16] J. P. Serre, Lettre à M. Tsfasman, In "Journées Arithmétiques de Luminy (1989)", Astérisque 198-199-200 (1991), 3511-353.
[17] A. B. Sørensen, Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes. Ph. D. Thesis, Aarhus, Denmark, 1991.
[18] H. P. F. Swinnerton-Dyer, Rational zeros of two quadratics forms, Acta Arith. 9 (1964), 261-270.
[19] J. Wolfmann, Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie, Discrete Mathematics 13 (1975), 185-211.