Contributions to the theory of algebraic coding on finite fields and rings and their applications

Liqin Qian

UNIVERSITÉ PARIS 8
VINCENNES-SAINT-DENIS

THÈSE

en vue de l'obtention du grade de

Docteur de l'Université Paris 8,

délivré par UNIVERSITÉ PARIS 8

Discipline : **Mathématiques**

Laboratoire Analyse, Géométrie et Applications (LAGA), UMR 7539, équipe AGC3

École Doctorale (ED 224) Cognition, Langage, Interaction

Présentée et soutenue publiquement le 25 Juillet 2022 à 10h00

Liqin QIAN

dirigée par Sihem Mesnager

Contributions to the theory of algebraic coding on finite fields and rings and their applications

Devant le jury composé de :

Mme. Sihem MESNAGER, Université Paris 8, France. Maitre de conférence, HDR, Directrice

M. Xiwang CAO, Universié Nanjing, Chine, Professeur co-encadrant

M. Alexis BONNECAZE, Université de Marseille, France. Professeur, Rapporteur

M. Steven DOUGHERTY, Université de Scranton, USA. Professeur, Rapporteur

M. Ferruh Ozbudak, Université de Ankara, Turquie, Professeur, Examinateur

M. Wolfgang Schmid, Université Paris 8, France. Professeur, Examinateur

M. Patrick Solé, Université de Marseille, France. Directeur de recherche, Examinateur

Acknowledgements

I would like to express my gratitude to all those who helped me during my PhD.

My deepest gratitude goes first and foremost to Professor Sihem Mesnager and Professor Xiwang Cao, my two supervisors, for their constant encouragement and guidance. They have walked me through all the stages of the writing of this thesis. Through their patient instruction, I finally focused on the object studied in this thesis and obtained valuable advice on aspects ranging from framework construction and reference collection to elaborated analysis. This thesis could not have reached its present form without consistent and illuminating instruction. I will always fondly recall our moments of shared excitement at new results and the wise words of calm when things were becoming difficult.

I thank sincerely Professor Sihem Mesnager, who provided me with an opportunity to study in the Department of Mathematics of the University of Paris VIII in France and all-around help to study and live in Paris. I learned a lot of professional knowledge in the discussions and exchanges with her. She often told me about her experiences as a student to encourage me to work hard in scientific research and cherish the opportunity of learning. She always responded to my email rapidly and in time with many valuable suggestions and comments and encouraged me to complete the study. Once again, I would like to express my many thanks and best wishes to Professor Sihem Mesnager.

I am deeply grateful to Professor Xiwang Cao for his meticulous care and help in my life and scientific research over the past four years. He not only taught me knowledge but also provided me with opportunities to go out to study and communicate. My scientific research achievements at Nanjing University of Aeronautics and Astronautics are born from his insightful instructions and warm encouragement.

Secondly, I would like to thank the University of Paris VIII and Nanjing University of Aeronautics and Astronautics for providing a stimulating academic environment and support that promotes my growth here. I am also indebted to all the professors who have taught me in the Department of Mathematics at the University of Paris VIII and Nanjing University of Aeronautics and Astronautics, which significantly broadened my horizon and enriched my knowledge in my study. Their inspirational and conscientious teaching have provided me with a firm basis for composing this thesis and will always be of great value to my future academic research. As a student, I learned a lot from them, which is helpful to my scientific research.

My thanks also go to the scholars whose monographs and academic papers have enlightened me in the writing of this thesis. Moreover, I sincerely thank my fellow classmates and friends. We share joys and anxieties, which propels us forward together throughout the arduous journey.

And also, warm thanks to my family for their consistent support and concern and

all kinds of practical help. Their generous help has accompanied me for so long, yet I can only offer so little in return. I am much indebted to my parents for their loving consideration and great confidence in me throughout these years. I am most indebted to my husband for his love and understanding and his capability to manage all the matters when I feel helpless. His concern brings me warm encouragement and sweet joy when I feel frustrated at myself for my poor performance in organizing both my life and study.

Last but not least, I should give my hearty thanks to all jury members for their patient instructions in my thesis and their precious suggestions for my study here. I would like to thank all jury members for taking the time during their vacation to participate in my defense.

Liqin Qian
25/07/2022

Résumé

La théorie du codage algébrique sur les corps et les anneaux finis a une grande importance dans la théorie de l'information en raison de leurs diverses applications dans les schémas de partage de secrets, les graphes fortement réguliers, les codes d'authentification et de communication. Cette thèse aborde plusieurs sujets de recherche selon les orientations dans ce contexte, dont les méthodes de construction sont au cœur de nos préoccupations. Plus précisément, nous nous intéressons aux constructions de codes optimaux (ou codes asymptotiquement optimaux), aux constructions de codes linéaires à "hull" unidimensionnelle, aux constructions de codes minimaux et aux constructions de codes linéaires projectifs. Les principales contributions sont résumé comme suit. Cette thèse fournie une description explicite des caractères additifs et multiplicatifs sur les anneaux finis (précisément $\mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ et $\mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$), utilise des sommes Gaussiennes, hyper Eisenstein et Jacobi et fournit plusieurs classes de nouveaux codes optimaux (ou asymptotiquement optimaux) avec des paramètres flexibles, propose des codes linéaires (optimaux ou quasi-optimal) avec une "hull" unidimensionnelle sur des corps finis en utilisant des outils de la théorie de la somme Gaussienne. De plus, cette thèse explore plusieurs classes de codes linéaires binaires (optimaux pour la borne de Griesmer bien connue) sur des corps finis basés sur deux constructions génériques utilisant des fonctions. Aussi, elle détermine leurs paramètres et leurs distributions de poids et en déduit plusieurs familles infinies de codes linéaires minimaux. Enfin, elle étudie des constructions optimales de plusieurs classes de codes linéaires binaires projectifs avec peu de poids et leurs codes duaux correspondants.

Mots clés: Codebook, codes linéaires, codes minimaux, Hull, distributions de poids, partage de secrets.

Abstract

Algebraic coding theory over finite fields and rings has always been an important research topic in information theory thanks to their various applications in secret sharing schemes, strongly regular graphs, authentication and communication codes. This thesis addresses several research topics according to the orientations in this context, whose construction methods are at the heart of our concerns. Specifically, we are interested in the constructions of optimal codebooks (or asymptotically optimal codebooks), the constructions of linear codes with a one-dimensional hull, the constructions of minimal codes, and the constructions of projective linear codes. The main contributions are summarized as follows. This thesis gives an explicit description of additive and multiplicative characters on finite rings (precisely $\mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ and $\mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$), employees Gaussian, hyper Eisenstein and Jacobi sums and proposes several classes of optimal (or asymptotically optimal) new codebooks with flexible parameters. Next, it proposes(optimal or nearly optimal) linear codes with a one-dimensional hull over finite fields by employing tools from the theory of Gaussian sums. It develops an original method to construct these codes. It presents sufficient conditions for one-dimensional hull codes and a lower bound on its minimum distance. Besides, this thesis explores several classes of (optimal for the well-known Griesmer bound) binary linear codes over finite fields based on two generic constructions using functions. It determines their parameters and weight distributions and derives several infinite families of minimal linear codes. Finally, it studies (optimal for the sphere packing bound) constructions of several classes of projective binary linear codes with a few weight and their corresponding duals codes.

Keywords: Codebook, linear code, projective code, weight distribution, secret sharing scheme.

Introduction et aperçu de la thèse (en Français)

Avec le développement rapide de la communication et de la technologie informatique, Internet a été intégré dans la vie des gens. L'Internet a grandement facilité l'interaction de l'information des gens. Il a également favorisé le développement rapide de l'économie, de la culture, de l'armée, de l'éducation, de la production et d'autres domaines. En outre, il améliore également la qualité de vie des personnes modernes et apporte une grande commodité à la vie des gens. La technologie de la communication a également produit un développement sans précédent, et de nombreuses informations importantes sont transmises via le réseau. Le développement d'Internet étant global, ouvert, partagé et dynamique, tout utilisateur peut facilement y accéder, mais certains utilisateurs malveillants ne sont pas exclus. Par conséquent, la sécurité de l'information est devenue de plus en plus l'un des problèmes importants à résoudre de toute urgence. Parce que les informations dans le processus de transmission rencontreront diverses interférences, entraînant des erreurs de transmission d'informations. Le système de communication ne dispose toujours pas d'une capacité suffisante de correction d'erreurs; il est nécessaire d'effectuer une correction d'erreur et un codage des informations. Assurer la fiabilité de l'information dans les canaux de communication est également devenu l'un des enjeux majeurs auxquels les chercheurs s'intéressent.

En 1948, Shannon a proposé pour la première fois la très célèbre théorie du codage dans son article historique "A Mathematical Theory of Communication". Cet article a marqué le début de la théorie de l'information et de la théorie du codage. Depuis lors, la théorie du codage algébrique à été largement étudiée, y compris l'étude "codebooks", l'étude des codes linéaires, etc.

De nombreux d'éléments mathématiques, tels que les sommes de caractères sur des corps finis ou des anneaux, jouent un rôle crucial dans la théorie du codage algébrique, en particulier les sommes de caractères spéciaux sur des corps finis ou sont plus largement utilisés, par ex., sommes Gaussiennes, sommes de Jacobi, sommes d'Eisenstein et sommes de Kloosterman. Dans les systèmes de communication CDMA, les sommes de caractères peuvent être utilisées pour construire des "codebooks" et des séquences avec de meilleures propriétés de corrélation; en théorie du codage, les sommes de caractères peuvent être utilisées pour construire des codes linéaires spéciaux, tels que des codes LCD, des codes BCH, des codes linéaires à coque unidimensionnelle, des codes linéaires minimaux, des codes projectifs, etc.; en mathématiques combinatoires, des sommes de caractères peuvent être utilisées pour construire des ensembles de différences; dans les systèmes de communication quantique, les sommes de caractères peuvent être utilisées pour concevoir des codes quantiques (MDS) avec de meilleurs paramètres. En cryptographie, les sommes de caractères peuvent être aussi utilisées pour construire certaines fonctions booléennes ou vectorielles avec certaines propriétés cryptographiques

spéciales, telles que les fonctions courbes et les fonctions semi-courbes, etc.

Les corps finis ou anneaux finis sont un outil de recherche important dans la théarie du codage. Un "codebook" est un ensemble de signaux; en tant que forme de signal, il a de bonnes propriétés de corrélation et peut être utilisé comme signal pour un radar, la synchronisation et la mesure de système linéaire. Dans la transmission de signaux, la séquence de signaux sera interférée par elle-même et d'autres signaux associés dans une certaine mesure. La force du signal est affaiblie, ce qui apportera de nombreuses difficultés et problèmes à la communication réelle. En particulier, les "codebooks" MWBE ont été utilisés dans un large éventail d'applications, telles que le codage de description multiple sur des canaux d'effacement, les communications, la détection compressée, les codes spatio-temporels, la théarie du codage, l'informatique quantique, etc. Un "codebook" est appelé maximum-Welch-"codebooks" d'égalité liée (MWBE) s'il respecte une certaine limite, c'est-à-dire la limite de Welch ou la limite de Levenshtein, également appelée "codebook optimal". Cette classe de "codebooks" est utilisée pour distinguer les signaux de différents utilisateurs dans les systèmes à accès multiple par répartition en code (CDMA). Par conséquent, il est très important de construire un "codebook" optimal. Il est difficile de construire des "codebooks" optimaux pour atteindre la limite de Welch ou de Levenshtein. Par conséquent, de nombreux chercheurs ont essayé de construire des "codebooks" asymptotiquement optimaux; c'est-à-dire que la magnitude maximale atteint presque la borne de Welch ou la borne de Levenshtein. En tant que classe spéciale de codes de correction d'erreurs, les codes linéaires ont une structure algébrique spéciale qui les rend plus faciles à décrire, encoder et décoder que d'autres types de codes. Par conséquent, de nombreux chercheurs se sont largement préoccupés des codes linéaires. La plupart des codes correcteurs d'erreurs avec de bonnes performances sont des codes linéaires. Par exemple, les codes linéaires les plus étudiés sont les codes de Hamming, les codes BCH, les codes Reed-Solomon, les codes Golay, les codes Reed-Muller, les codes Goppa, les codes MDS, etc. La distance de Hamming minimale d'un code linéaire est une mesure de la capacité de correction d'erreur de ce code. Dans le même temps, la distribution de poids de Hamming des codes linéaires donne des informations importantes d'une importance à la fois pratique et théorique. En particulier, les codes linéaires avec peu de poids non nuls ont été largement étudiés en raison de leurs larges applications pratiques dans la communication, les schémas de partage de secrets, le calcul bipartite sécurisé les schémas d'association, les codes d'authentification et les graphes fortement réguliers. Par conséquent, la construction de codes linéaires pondérés avec de nouveaux paramètres est devenue un sujet de recherche brûlant en théarie du codage algébrique. De nombreux chercheurs construisent des codes linéaires optimaux en définissant des ensembles par rapport à certaines fonctions cryptographiques spéciales, telles que les fonctions courbes, les fonctions quadratiques, les fonctions courbes faiblement régulières, les fonctions plateaux, les fonctions APN ou PN, les fonctions deux vers un etc.

Ces dernières années, de nombreux chercheurs ont suscité un grand intérêt pour les codes linéaires à "hull" de faible dimension, principalement en raison des excellentes performances des codes linéaires à "hull" de faible dimension. Le "hull" d'un code linéaire sur des corps finis est l'intersection du code et de son dual, qui peut être vue comme une généralisation des codes auto-duaux, des codes auto-orthogonaux et des codes LCD. Il est clair que le "hull" des codes linéaires est également linéaire. A noter que les coquilles des codes linéaires jouent un rôle essentiel dans la détermination de

la complexité des algorithmes de vérification de l'équivalence de permutation de deux codes linéaires. Le "hull" est un indicateur de la complexité des algorithmes de calcul du groupe d'automorphismes du code linéaire. Ces algorithmes sont très efficaces en général si la taille du "hull" est petite. Par conséquent, les codes linéaires avec un "hull" de faible dimension sur des corps finis jouent un rôle important dans la théorie du codage algébrique. Un code linéaire avec la plus petite coque est un code LCD, qui peut être utilisé dans une technique de masquage de somme directe pour la prévention des attaques par canaux cachés. Un code linéaire avec la deuxième plus faible "hull" est un code linéaire avec un "hull" unidimensionnelle, ce qui peut améliorer l'efficacité de l'algorithme d'équivalence de permutation de deux codes linéaires. En général, ces algorithmes sont plus efficaces lorsque la dimension du "hull" d'un code linéaire est plus petite. Par conséquent, la construction de codes linéaires avec une coque de faible dimension est fascinante et a des applications pratiques bénéfiques dans le codage algébrique.

Cette thèse traite plusieurs sujets de recherche à la suite de directions existantes dans ce domaine dont les méthodes de constructions sont au coeur de nos préoccupations. Précisément, on s'intéresse aux constructions de codebooks optimaux (ou codebooks asymptotiquement optimaux), aux constructions de codes linéaires avec une coque ("hull" en anglais) unidimensionnelle, aux constructions de codes linéaires minimaux avec peu de poids, aux constructions de codes linéaires projectifs et leurs applications des les schémas de partage secret et ceux dit d'association.

En utilisant principalement les sommes de caractères sur des corps finis et des anneaux finis comme outils de recherche, cette thèse construit des codes optimaux ou asymptotiquement optimaux, des codes linéaires à coque unidimensionnelle et des codes linéaires optimaux à faible poids avec de nouveaux paramètres.

Pour comprendre nos réalisations techniques, nous introduisons brièvement quelques définitions de base et des résultats pertinents sur les codes linéaires que nous avons utilisés et rappelés en Chapitre 1 de le thèse.

Soit $\mathbb{F}_q$ le corps fini d'ordre q, et $\mathbb{F}_q^n$ désigne l'espace vectoriel de dimension n sur $\mathbb{F}_q$. Chaque sous-ensemble $\mathcal{C}$ non vide de $\mathbb{F}_q^n$ est appelé un *q-ary code*. Un élément de $\mathcal{C}$ est appelé un *mot de code* en $\mathcal{C}$. Le nombre de mots de code dans $\mathcal{C}$, noté $K = |\mathcal{C}|$, est appelé la *taille* de $\mathcal{C}$, où $1 \leq K \leq q^n$. Un code de longueur n et de taille K est appelé un code (n, K). Les "bit d'information" d'un code $\mathcal{C}$ de longueur n sont définis comme $k = \log_q K$. Le rendement d'un code $\mathcal{C}$ de longueur n est défini comme $\frac{k}{n}$. Lorsque le sous-ensemble non vide $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{F}_q^n$, le code $\mathcal{C}$ est appelé un code linéaire de paramètres $[n,k]$ sur le corps fini $\mathbb{F}_q$, où k est la dimension du code linéaire $\mathcal{C}$ et $|\mathcal{C}| = q^k$.

Dans ce qui suit, nous donnons la définition de base des codes duaux pour les codes linéaires sur des corps finis. Avant cela, rappelons d'abord la définition du produit scalaire euclidien. Soit $\mathbb{F}_q$ le corps fini d'ordre q, et q une puissance d'un nombre premier. Pour deux vecteurs quelconques $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ et $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in F_q^n$, leur Le produit scalaire euclidien $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ sur $\mathbb{F}_q$ est défini par

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i y_i.$$

Si $\mathcal{C}$ est un code linéaire de longueur n sur $\mathbb{F}_q$, alors le code dual de $\mathcal{C}$, noté $\mathcal{C}^{\perp}$, est

défini par

$$\mathcal{C}^{\perp} = \{\boldsymbol{x} \in \mathbb{F}_q^n : \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \forall\, \boldsymbol{y} \in \mathcal{C}\}.$$

Pour un code linéaire, sa distance minimale mesure la capacité de correction d'erreur de ce code. Dans cette thèse nous utilisons la distance de Hamming qui est directement liée aux poids de Hamming (dans le cas de traitement de codes linéaires, comme le cas de cette thèse).

Soient $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ et $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ deux vecteurs dans $\mathbb{F}_q^n$. Le *poids de Hamming* du vecteur $\boldsymbol{x}$, noté $w_H(\boldsymbol{x})$, est défini comme étant le nombre de coordonnées non nulles dans $\boldsymbol{x}$, c'est-à-dire ,

$$w_H(\boldsymbol{x}) = |\{i : 1 \leq i \leq n, x_i \neq 0\}|.$$

La *distance de Hamming* des vecteurs $\boldsymbol{x}$ et $\boldsymbol{y}$, noté $d_H(\boldsymbol{x}, \boldsymbol{y})$, est définie comme étant la nombre d'endroits où $\boldsymbol{x}$ et $\boldsymbol{y}$ diffèrent, c'est-à-dire,

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = |\{i : 1 \leq i \leq n, x_i \neq y_i\}| = w_H(\boldsymbol{x} - \boldsymbol{y}).$$

Soit $\mathcal{C}$ un code q-aire de longueur n. Le *poids de Hamming minimum* de $\mathcal{C}$, noté $w_H(\mathcal{C})$, est défini comme étant le plus petit des poids des mots de code non nuls de $\mathcal{C}$, c'est-à-dire,

$$w_H(\mathcal{C}) = \min\{w_H(\boldsymbol{c}) : \boldsymbol{0} \neq \boldsymbol{c} \in \mathcal{C}\}.$$

La *distance de Hamming minimale* de $\mathcal{C}$, désignée par $d_H(\mathcal{C})$, est définie comme étant la distance de Hamming minimale entre deux mots de code diffèrents dans $\mathcal{C}$, c'est-à-dire,

$$d = d_H(\mathcal{C}) = \min\{d_H(\boldsymbol{c}_1, \boldsymbol{c}_2) : \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C}, \boldsymbol{c}_1 \neq \boldsymbol{c}_2\}.$$

Soit A_i $(i = 1, 2, \ldots, n)$ le nombre de mots de code de poids de Hamming i dans $\mathcal{C}$. Le *énumérateur de poids* de $\mathcal{C}$ est défini par $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$ et la séquence $(1, A_1, A_2, \ldots, A_n)$ est appelée la *distribution des poids* de $\mathcal{C}$. Le code $\mathcal{C}$ est dit être un *t-poids code* si le nombre de A_i non nuls dans la séquence $(A_1, A_2, \ldots, A_n)$ est égal à t. Nous notons $(1, A_1^{\perp}, \ldots, A_n^{\perp})$ la distribution des poids du dual du code $\mathcal{C}$ de paramètres $[n, k, d]$. Les cinq premiers Pless les moments de puissance sont donnés dans [54](voir [Théorème 7.3.1]).

Un code linéaire $\mathcal{C}$ est dit *projectif* si son dual a le minimum distance d'au moins trois.

Soit $\mathcal{C}$ un code linéaire $[n, k, d]$ de longueur n sur $\mathbb{F}_q$ et son code dual noté $\mathcal{C}^{\perp}$ formé par tous les mots de $\mathbb{F}_q$ tels que le produit étoile avec les mots du code $\mathcal{C}$ soit nul (i.e. orthogonal aux mots du code $\mathcal{C}$). Le *hull* d'un code linéaire $\mathcal{C}$ sur un corps fini est défini comme

$$\mathrm{Hull}(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^{\perp}.$$

Il est clair que $\mathrm{Hull}(\mathcal{C})$ est également linéaire. La définition de $\mathrm{Hull}(\mathcal{C})$ a été introduite en 1990 par Assmus et Key [59] pour classer les plans projectifs finis. Supposons que la dimension de $\mathrm{Hull}(\mathcal{C})$ soit ℓ. Si $\ell = 0$, c'est-à-dire $\mathrm{Hull}(\mathcal{C}) = \{\boldsymbol{0}\}$, alors le code linéaire $\mathcal{C}$ est appelé linéaire Dual Complementary (LCD). Si $\ell = k$, c'est-à-dire $\mathrm{Hull}(\mathcal{C}) = \mathcal{C}$, alors on dit que le code linéaire $\mathcal{C}$ est un code auto-orthogonal. De plus, si $\ell = \frac{n}{2}$ pour n pair, alors $\mathcal{C}$ est appelé un code auto-dual.

Il est bien connu que les coquilles de codes linéaires jouent un rôle essentiel dans la détermination de la complexité des algorithmes de vérification d'équivalence de

permutation de deux codes linéaires. Par la suite, il a été montré que la coque est un indicateur de la complexité des algorithmes de calcul de l'automorphisme groupe d'un code linéaire dans [63, 94]. Plus précisément, la plupart des algorithmes ne fonctionnent pas si la taille du "hull" est grande.

Cependant, à l'inverse, ces algorithmes sont très efficaces en général si la taille de la coque est petite. donc l'étude de les codes linéaires avec une petite coquille sont utiles et intéressants pour ces calculs.

Pour mesurer l'optimalité des codes que nous construisons dans la thèse, nous nous référons à plusieurs bornes connues dans la literature.

Pour tout code linéaire $\mathcal{C}$ avec des paramètres $[n,k,d]$ sur $\mathbb{F}_q$.

La borne bien connue de Singleton est donnée par

$$d \leq n-k+1.$$

En particulier, si $d = n-k+1$, alors $\mathcal{C}$ est appelé un *code de distance maximale séparable (MDS)*. Un code est appelé *presque MDS* si sa distance minimale est un de moins que le cas MDS.

La borne de Griesmer, qui s'applique spécifiquement aux codes linéaires sur des corps finis est donnée par

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

où $\lceil \cdot \rceil$ est la fonction partie entière.

En particulier, le code $\mathcal{C}$ est appelé *code de Griesmer* s'il atteint la borne de Griesmer.

La borne appelée "Sphere Packing Bound" est donnée par

$$2^n \geq 2^k \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i},$$

où $\lfloor \frac{d-1}{2} \rfloor$ est le plus grand entier inférieur ou égal à $\frac{d-1}{2}$.

Un code $[n,k,d]$ sur $\mathbb{F}_q$ est dit alors *optimal-distance* s'il n'y a pas de code $[n,k,d']$ sur $\mathbb{F}_q$ avec $d' \geq d+1$ et *presque optimal en distance* si un code $[n,k,d+1]$ sur $\mathbb{F}_q$ est distance optimale.

Dans cette thèse, nous utilisons un certain nombre d'éléments de la théorie des corps finis et de la théorie des nombres. Soit $\mathbb{F}_q$ le corps fini avec $q = p^n$ éléments, où p est un nombre premier et n est un entier positif. Soit $m \mid n$ et m un entier positif. La fonction de trace de $\mathbb{F}_{p^n}$ à $\mathbb{F}_{p^m}$ est définie comme:

$$\mathrm{Tr}_{p^n/p^m}(x) := \sum_{i=0}^{\frac{n}{m}-1} x^{p^{im}} = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(\frac{n}{m}-1)m}}, x \in \mathbb{F}_q.$$

En particulier, si $m = 1$, alors la fonction de trace $\mathrm{Tr}_{q/p}(\cdot)$ est appelée *absolue fonction trace*. Nous rappellerons les définitions des caractères additifs et multiplicatifs de $\mathbb{F}_q$. Soit $q = p^n$, où p est un nombre premier et n est un entier positif. Pour chaque $a \in \mathbb{F}_q$, le *caractère additif* χ_a de $\mathbb{F}_q$ est défini par

$$\chi_a : \mathbb{F}_q \longrightarrow \mathbb{C}^*, \chi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)}, x \in \mathbb{F}_q,$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$, qui est une primitive p-ième racine de l'unité.

Si $a = 0$, alors $\chi_0(x)$ est appelé le *caractère additif trivial* de $\mathbb{F}_q$ et $\chi_0(x) = 1$ pour tout $x \in \mathbb{F}_q$; Si $a = 1$, alors $\chi_1(x) = \chi(x)$ est appelé le *caractère additif canonique* de $\mathbb{F}_q$; tous les autres caractères additifs de $\mathbb{F}_q$ sont dits non triviaux. De plus, le groupe constitué de tous les caractères additifs de $\mathbb{F}_q$ est désigné par $\widehat{\mathbb{F}}_q := \{\chi_a : a \in \mathbb{F}_q\}$. Le groupe de caractères est isomorphe à $(\mathbb{F}_q, +)$. A chaque caractère additif $\chi_a(x)$ de $\mathbb{F}_q$, il y a un conjugué associé caractère $\overline{\chi_a}(x)$ défini par $\overline{\chi_a}(x) = \overline{\chi_a(x)} = \chi_a(-x)$ pour tout $x \in \mathbb{F}_q$. De plus, $\chi_a(0) = 1$ pour tout $a \in \mathbb{F}_q$.

Pour tout $j = 0, 1, \ldots, q-2$, le *caractère multiplicatif* ψ_j de $\mathbb{F}_q$ est défini par

$$\psi_j : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*, \psi_j(g^k) = \zeta_{q-1}^{jk}, k = 0, 1, \ldots, q-2,$$

where $\zeta_{q-1} = e^{\frac{2\pi\sqrt{-1}}{q-1}}$, qui est une primitive $(q-1)$-ième racine de l'unité, et g est un élément primitif fixe de $\mathbb{F}_q$.

Si $j = 0$, alors ψ_0 est appelé le *caractère multiplicatif trivial* de $\mathbb{F}_q$; Si $j = 1$, alors ψ_1 est appelé le *caractère multiplicatif canonique* de $\mathbb{F}_q$; Si q est impair et $j = \frac{q-1}{2}$, alors $\psi_{\frac{q-1}{2}}$ est appelé le *caractère quadratique* de $\mathbb{F}_q$, noté η, c'est-à-dire $eta(g^k)$ vaut 1 si g^kest le carré d'un élément de $\mathbb{F}_q^*$ et -1 sinon. De plus, le groupe constitué de tous les caractères multiplicatifs de $\mathbb{F}_q$ est noté $\widehat{\mathbb{F}}_q^* = \{\psi_j : j = 0, 1, \ldots, q-2\}$. Le groupe de caractères est isomorphe à $(\mathbb{F}_q^*, \times)$. A chaque caractère multiplicatif ψ de $\mathbb{F}_q$, il y a un caractère conjugué associé $\overline{\psi}$ défini par $\overline{\psi}(x) = \overline{\psi(x)} = \psi^{-1}(x), x \in \mathbb{F}_q^*$. Si ψ est trivial, alors $\psi(0) = 1$; si ψ est non trivial, alors on définit $\psi(0) = 0$. Notons qu'il existent des relations d'orthogonalité pour les caractéres multiplicatifs de $\mathbb{F}_q$.

Dans cette thèse, nous utilisons plusieurs sommes que nous rappelons brièvement ci-dessous. A partir du caractère d'addition χ_a et du caractère multiplicatif ψ de $\mathbb{F}_q$, nous donnons la définition de la somme Gaussienne sur le corps fini $\mathbb{F}_q$ comme suit. Soit ψ un caractère multiplicatif et χ_a un caractère additif de $\mathbb{F}_q$, où $a \in \mathbb{F}_q$. Alors la *somme Gaussienne* $G(\psi, \chi_a)$ sur $\mathbb{F}_q$ est définie par

$$G(\psi, \chi_a) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi_a(x).$$

Si $a = 1$, on écrit généralement $G(\psi, \chi_1)$ comme $G(\psi)$.

Nous rappelons la définition des sommes hyper Eisenstein sur le corps fini $\mathbb{F}_q$. La somme hyper Eisenstein $E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1)$ est définie par

$$E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n) := E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1) = \sum_{x_1, \ldots, x_n \in \mathbb{F}_q^*, \mathrm{Tr}_{q/r}(x_1 + \cdots + x_n) = 1} \psi_1(x_1) \cdots \psi_n(x_n),$$

où $\psi_1, \psi_2, \ldots, \psi_n$ sont des caractères multiplicatifs de $\mathbb{F}_q$. Si $n = 1$, alors $E(\psi; 1) = \sum_{x \in \mathbb{F}_q^*, \mathrm{Tr}_{q/r}(x) = 1} \psi(x)$ s'appelle la *somme d'Eisenstein* sur $\mathbb{F}_q$. Si $q = r$, alors

$$\sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q^*, \\ x_1 + \cdots + x_n = 1}} \psi_1(x_1) \cdots \psi_n(x_n)$$

est appelé la *Jacobi somme* sur $\mathbb{F}_q$, nous l'écrivons généralement simplement comme $J_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;1)$.

De plus, on définit

$$E_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;s)=\sum_{\substack{x_1,\ldots,x_n\in\mathbb{F}_q^*,\\ \mathrm{Tr}_{q/r}(x_1+\cdots+x_n)=s}}\psi_1(x_1)\cdots\psi_n(x_n)$$

pour tout $s\in\mathbb{F}_r$, qui est appelée l'hyper-somme d'Eisenstein généralisée sur $\mathbb{F}_q$. Si $n=1$, alors $E(\psi;s)=\sum_{x\in\mathbb{F}_q^*,\mathrm{Tr}_{q/r}(x)=s}\psi(x)$ s'appelle la somme d'Eisenstein généralisée sur $\mathbb{F}_q$. A noter qu'il existe une relation entre les sommes hyper Eisenstein et Gaussiennes sur $\mathbb{F}_q$.

Les principaux apports se résume comme suit.

(1) Sur les "codebooks", cette thèse donne une description explicite des caractères additifs et des caractères multiplicatifs sur l'anneau à chaine fini $\mathbb{F}_q+u\mathbb{F}_q$ $(u^2=0)$, et l'anneau non chaîné fini $\mathbb{F}_q+u\mathbb{F}_q$ $(u^2=u)$, et présente des sommes Gaussiennes, des sommes hyper Eisenstein et des sommes de Jacobi sur ces deux anneaux. En termes d'application dans cet exe, cette thèse offre plusieurs classes de "codebooks" optimaux (ou asymptotiquement optimaux) par rapport à la borne de Welch (ou la borne de Levenshtein) à partir de ces sommes de caractères. Les paramètres de ces "codebooks" sont nouveaux et flexibles.

(2) Sur les codes linéaires à "hull" unidimensionnelle. Basée sur la théorie des sommes Gaussiennes sur des corps finis, cette thèse offre des codes linéaires avec une "hull" unidimensionnelle sur des corps finis. Certains d'entre eux sont des codes linéaires optimaux ou presque optimaux par rapport à la base de données en ligne de Grassl. Ces résultats généralisent les méthodes existantes de construction de codes linéaires à hull unidimensionnelle utilisant la somme Gaussienne quadratique et la somme Gaussienne dans le cas semi-primitif. De plus, cette thèse développe une méthode originale pour construire des codes linéaires avec "hull" unidimensionnelle en employant les analogues caractéristiques positives des sommes Gaussiennes. Certaines conditions suffisantes pour qu'un code linéaire soit un code linéaire ayant un "hull" unidimensionnelle sont présentées. Notamment, on y présente également une borne inférieure sur les distances minimales des codes linéaires construits.

(3) Sur les codes linéaires minimaux avec peu de poids qui ont diverses applications dans les schémas de partage de secrets, les graphes fortement réguliers, les codes d'authentification et la communication, cette thèse propose plusieurs classes de codes linéaires binaires avec peu de poids non nuls basée sur deux constructions génériques et une nouvelle construction et à partir de fonctions connues deux à un sur des corps finis et détermine leurs paramètres et distributions de poids. Ces codes ont de nouveaux paramètres, et certains sont optimaux par rapport à la borne bien connue appelé "borne de Griesmer". En particulier, cette thèse dérive plusieurs familles infinies de codes linéaires minimaux. Par ailleurs, on résout avec succès deux problèmes ouverts proposés par Qu et al.

(4) Enfin, sur les codes linéaires projectifs, on s'intéresse surtout à ceux de faible poids sont très précieux car ils sont étroitement liés aux espaces projectifs finis, aux schémas d'association, aux espaces normés fortement réguliers et aux conceptions combinatoires, etc. En sélectionnant deux restrictions différentes sur la définition des ensembles, cette thèse fourni des constructions de plusieurs classes de codes linéaires binaires projectifs avec peu de poids de fonctions deux à un sur des corps finis de caractéristique paire. On y détermine leurs distributions de poids en utilisant la transformée de Walsh des fonctions deux à un correspondantes. Les paramètres des duals des codes construits sont également déterminés. En particulier, certains duals sont optimaux en distance par rapport à la borne connue sous le nom de "the sphere packing bound". Outre, cette thèse montre que ces codes linéaires construits peuvent être utilisés pour construire des schémas d'association et de partage de secrets avec des structures d'accès intéressantes.

Dans la suite, nous décrivons brièvement le contenu de cette thèse.

- Le chapitre 1 présente l'historique du développement, la motivation de la recherche, le contexte de la recherche, le contenu de la recherche de la théorie du codage algébrique. Le chapitre 2 fournit quelques notations de base, des définitions et des résultats sur la théorie des caractères, les codes linéaires, la théorie algébrique des nombres et les fonctions booléennes et vectorielles.

- Dans le chapitre 3, on considère l'anneau $R_1 = \mathbb{F}_q + u\mathbb{F}_q = \{\alpha + \beta u : \alpha, \beta \in \mathbb{F}_q\}(u^2 = 0)$ ayant un unique idéal maximal $M = \langle u \rangle$. En fait, $R_1 = \mathbb{F}_q \oplus u\mathbb{F}_q \simeq \mathbb{F}_q^2$ est un espace vectoriel à deux dimensions sur $\mathbb{F}_q$ et $|R_1| = q^2$. Les éléments inversibles de R_1 sont

$$R_1^* = R_1 \backslash M = \mathbb{F}_q^* + u\mathbb{F}_q = \{\alpha + \beta u : \alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q\}.$$

Il est facile de savoir que $|R_1^*| = q(q-1)$. Nous introduisons alors la définition du caractère quadratique sur R_1 comme suit. Soit φ un caractère multiplicatif de R_1. Si $(\varphi(t))^2 = 1$ pour tout $t \in R_1^*$, alors φ est appelé le *caractère quadratique* de R_1, noté ρ . De plus, $G_{R_1}(\rho, \lambda)$ désigne la somme Gaussienne quadratique sur R_1, où λ est un caractère additif de R_1. Nous déterminons également la forme du caractère quadratique ρ de R_1. Soit η, ψ_0 et χ_0 respectivement le caractère quadratique, le caractère trivial multiplicatif et le caractère trivial additif du corps fini $\mathbb{F}_q$,. Nous utilisons la convention $\psi(0) = 0$ pour un caractère multiplicatif non trivial ψ de $\mathbb{F}_q$. Pour tout $t = t_0(1 + ut_1) \in R_1^*$, si le caractère multiplicatif φ de R_1 est un caractère quadratique, alors il faut $(\varphi(t))^2 = (\psi(t_0)\chi_a(t_1))^2 = 1$. Nous montrons un résultat très utile pour la suite de nos constructions de "codebooks".

Soient $\varphi_1, \varphi_2, \ldots, \varphi_n$ des caractères multiplicatifs de R_1 et $\varphi_i := \psi_i \star \chi_{a_i} (1 \leq i \leq n)$, où psi_i et χ_{a_i} sont des caractères multiplicatifs et additifs de $\mathbb{F}_q$, respectivement. Alors

(1) $E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;0)$

$$= \begin{cases} \frac{q^n}{r}E_{\mathbb{F}_q}(\psi_1,\psi_2,\ldots,\psi_n;0), & \text{if } a_1=\cdots=a_n=0; \\ \frac{q^n(r-1)}{r}\psi_1(a_1)\cdots\psi_n(a_n), & \text{if } a_1\cdots a_n\neq 0, \mathrm{Tr}_r^q(a_1+\cdots+a_n)=0 \text{ et} \\ & (\psi_1\cdots\psi_n)^* \text{ is trivial;} \\ 0, & \text{sinon,} \end{cases}$$

où $(\psi_1\cdots\psi_n)^*$ est la restriction de $\psi_1\cdots\psi_n$ à $\mathbb{F}_r$.

(2) $E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;1)$

$$= \begin{cases} \frac{q^n}{r}E_{\mathbb{F}_q}(\psi_1,\psi_2,\ldots,\psi_n;1), & \text{if } a_1=\cdots=a_n=0; \\ \frac{q^n}{r}\psi_1(\frac{a_1}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)})\cdots\psi_n(\frac{a_n}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)}), & \text{if } a_1\cdots a_n\neq 0 \text{ et} \\ & \mathrm{Tr}_r^q(a_1+\cdots+a_n)\neq 0; \\ 0, & \text{sinon,} \end{cases}$$

où $E_{\mathbb{F}_q}(\psi_1,\psi_2,\ldots,\psi_n;1)$ désigne l'hyper somme d'Eisenstein de $\mathbb{F}_q$.

(3) $E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;u)$

$$= \begin{cases} \frac{q^n}{r}E_{\mathbb{F}_q}(\psi_1,\psi_2,\ldots,\psi_n;0), & \text{if } a_1=\cdots=a_n=0; \\ \frac{q^n}{r}\psi_1(a_1)\cdots\psi_n(a_n)G_{\mathbb{F}_r}((\overline{\psi_1\cdots\psi_n})^*), & \text{if } a_1\cdots a_n\neq 0 \text{ et} \\ & \mathrm{Tr}_r^q(a_1+\cdots+a_n)=0; \\ 0, & \text{sinon,} \end{cases}$$

où $(\psi_1\cdots\psi_n)^*$ est la restriction de $\psi_1\cdots\psi_n$ à $\mathbb{F}_r$.

A l'aide de ces outils et d'autres sommes sur R_1 telle que la somme de Jacobi et d'autres some plus générale comme celle de la some Eisenstein, nous construisons des "codebooks" optimaux et asymptotiquement optimaux en étudiant la somme de Gauss la somme de Jacobi et la somme d'Eisenstein sur l'anneau à chaine fini $\mathbb{F}_q+u\mathbb{F}_q$ $(u^2=0)$.

Tout d'abord, nous construisons plusieurs familles de codes asymptotiquement optimaux à partir de la somme de Gauss sur R_1 comme suit.

Soit $\varphi := \psi\star\chi_a$ and $\lambda := \chi_b\star\chi_c$, où $a,b,c\in\mathbb{F}_q, \chi_a,\chi_b,\chi_c\in\widehat{\mathbb{F}}_q$ and $\psi\in\widehat{\mathbb{F}}_q^*$. Supposons que $t=t_0(1+ut_1)\in R_1^*$. Ensuite, nous définissons un ensemble $C_0(R_1^*,\widehat{R}_1^*\times\widehat{R}_1)$ comme

$$\begin{aligned} C_0(R_1^*,\widehat{R}_1^*\times\widehat{R}_1): &= \left\{\frac{1}{\sqrt{K}}(\varphi(t)\lambda(t))_{t\in R_1^*}, \varphi\in\widehat{R}_1^*, \lambda\in\widehat{R}_1\right\} \\ &= \left\{\frac{1}{\sqrt{K}}(\psi(t_0)\chi_a(t_1)\chi_b(t_0)\chi_c(t_0t_1))_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q}, \psi\in\widehat{\mathbb{F}}_q^*,\right. \\ &\qquad \left.\chi_a,\chi_b,\chi_c\in\widehat{\mathbb{F}}_q\right\}, \end{aligned}$$

où $K=|R_1^*|=q(q-1)$.

Selon la définition de l'ensemble $C_0(R_1^*, \widehat{R}_1^* \times \widehat{R}_1)$, nous donnerons deux constructions de codebooks sur R_1. La première construction de "codebook" est donnée comme suit.

Le "codebook" $C_1 := C_1(R_1^*, \widehat{R}_1^* \times \widehat{R}_1)$ de longueur $K_1 = |R_1^*| = q(q-1)$ sur R_1 est construit comme suit: $C_1 := \left\{ \frac{1}{\sqrt{K_1}} (\psi(t_0)\chi_a(t_1)\chi_b(t_0)\chi_c(t_0t_1))_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q} \right\}$ où ψ est un caractère multiplicatif fixe sur $\mathbb{F}_q$ et χ_a, χ_b, χ_c sont des éléments de $\widehat{\mathbb{F}}_q$.

A partir de cette construction du "codebook" C_1, nous montons le théorème suivant.

Soit C_1 "codebook" défini comme ci-dessus. Alors C_1 est un $(q^3, q(q-1))$ "codebook" ayant une amplitude de corrélation croisée maximale $I_{\max}(C_1) = \frac{1}{q-1}$. De plus, le "codebook C_1" satisfait asymptotiquement la borne de Welch.

La deuxième construction de "codebook" est présentée ci-dessous.

Le "codebook" $C_2 := C_2(R_1^*, \widehat{R}_1^* \times \widehat{R}_1)$ de longueur $K_2 = |R_1^*| = q(q-1)$ sur R_1 est défini par

$C_2 := \left\{ \frac{1}{\sqrt{K_2}} (\psi(t_0)\chi_a(t_1)\chi_b(t_0)\chi_c(t_0t_1))_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q} \right\}$ avec $\psi \in \widehat{\mathbb{F}}_q^*$, χ_b est un caractère additif fixé sur $\mathbb{F}_q$, χ_a,χ_c sont des éléments de $\widehat{\mathbb{F}}_q$.

Avec les notations ci-dessus, nous démontrons que C_2 est un $(q^2(q-1), q(q-1))$ codebook ayant un maximum amplitude de corrélation croisée $I_{\max}(C_2) = \frac{1}{q-1}$. De plus, le "codebook" C_2 satisfait asymptotiquement les bornes bien connues de Welch.

Ensuite, nous présentons des "codebooks" asymptotiquement optimaux qui sont construits par les sommes d'Eisenstein sur R_1. Précisément, nous montrerons d'abord que si $G := \{\phi_j : (r-1) \mid j, 0 \le j \le q-2\} \subseteq \widehat{\mathbb{F}}_q^*$, où $\phi_j = \phi_1^j$ et ϕ_1 est un générateur de $\widehat{\mathbb{F}}_q^*$ avec $0 \le j \le q-2$, alors G est un sous-groupe de $\mathbb{F}_q^*$ et $|G| = \frac{q-1}{r-1}$. De plus, pour tout $\psi \in \widehat{\mathbb{F}}_q^*$, ψ^* est trivial si et seulement si $\psi \in G$, où ψ^* désigne la restriction de ψ à $\mathbb{F}_r$.

Soit $D = \{t \in R_1^* : \mathrm{Tr}(t) = 1\}$ and $K_3 := |D|$. Ici, nous considérons le cas où $m = 2$ et $q = r^2$. Par conséquent, il est facile de vérifier que $K_3 = r^2$. Supposons que H est un sous-groupe de $G := \{\phi_j : (r-1) \mid j, 0 \le j \le q-2\} \subseteq \widehat{\mathbb{F}}_q^*$ et $k = |H|$. Alors $k \mid (r+1)$ puisque $|G| = \frac{q-1}{r-1} = r+1$.

Le "codebook" $C_3 := C_3(D, H \times \widehat{\mathbb{F}}_q)$ de longueur $K_3 = r^2$ sur R_1 est construit comme suit.

$C_3 := \left\{ \frac{1}{\sqrt{K_3}} ((\psi \star \chi_a)(t))_{t \in D}, \psi \in H, \chi_a \in \widehat{\mathbb{F}}_q \right\}$.

Nous montrons alors que C_3 est un "codebook" (kr^2, r^2) ayant amplitude de corrélation croisée maximale $I_{\max}(C_3) = \frac{1}{r}$. De plus, le codebook C_3 satisfait asymptotiquement la borne connue de Welch.

La quatrième construction de "codebook" utilise des sommes de Jacobi sur R_1. Nous considérons le cas où $n = 2$ et $m = 1$. Soit $t_1 = t_1'(1 + ut_1'')$ et $t_2 = t_2'(1 +$

$ut_2'') \in R_1^*$. Nous définissons $D' = \{t_1, t_2 \in R_1^* : t_1 + t_2 = 1\} = \{t_1', t_2' \in \mathbb{F}_q^*, t_1'', t_2'' \in \mathbb{F}_q : t_1' + t_2' = 1, t_1' t_1'' + t_2' t_2'' = 0\}$ et $K_4 := |D'|$.

Le "codebook" $C_4 := C_4(D', \widehat{R}_1^* \times \widehat{R}_1^*)$ de longueur K_4 sur R_1 est défini comme suit.

$C_4 = \left\{ \frac{1}{\sqrt{K_4}} (\varphi_1(t_1)\varphi_2(t_2))_{t_1,t_2 \in D'}, \varphi_1 = \psi_1 \star \chi_{a_1}, \varphi_2 = \psi_2 \star \chi_{a_2} \right\}$, où ψ_1 est un caractère multiplicatif fixé sur $\mathbb{F}_q$, $\psi_2 \in \widehat{\mathbb{F}}_q^*$,$\chi_{a_1}$, χ_{a_2} sont des éléments de $\widehat{\mathbb{F}}_q$.

Avec les notations ci-dessus, nous monterons que C_4 est un $(q^2(q-1), q(q-2))$ "codebook" ayant une amplitude de corrélation croisée maximale $I_{\max}(C_4) = \frac{1}{q-2}$. De plus, C_4 satisfait asymptotiquement la borne de Welch.

Ensuite, nous étudions une classe de "codebooks" vérifiant la borne de Welch qui peut être construit en utilisant des sommes Gaussiennes quadratiques sur $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$, où $q = 2^m$. Nous considérons le "codebook" $C_5 := C_5(D'', \widehat{R}_1)$ de longueur K_5 sur R_1 défini par

$C_5 := \left\{ \frac{1}{\sqrt{K_5}} (\lambda(t))_{t \in D''}, \lambda \in \widehat{R}_1 \right\}$. Et nous montrons que C_5 est un $(q^2, \frac{q(q-1)}{2})$ codebook ayant un maximum amplitude de corrélation croisée $I_{\max}(C_5) = \frac{1}{q-1}$. De plus, C_5 vérifie la borne de Welch.

Nous considérons également l'anneau non-chaîné fini $R_2 := \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$. Nous mettons en place une méthode pour construire des "codebook" ayant de nouveaux paramètres et satisfaisant asymptotiquement la borne de Welch et la borne de Levenstein. Nos constructions utilisent des sommes de Gauss, des sommes de Jacobi et des sommes d'Eisenstein sur l'anneau non-chaîné R_2. Pour cela, nous donnons d'abord une relation entre la somme Gauss sur l'anneauR_2 et la somme Gauss sur le corps fini $\mathbb{F}_q$. Plus précisément, si φ un caractère multiplicatif et λ un caractère additif de R_2, où $\varphi := \varphi' \star \varphi'', \lambda := \chi_a \star \chi_b, \varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*, \chi_a, \chi_b \in \widehat{\mathbb{F}}_q$ et $a, b \in \mathbb{F}_q$. Alors la somme Gauss $G_{R_2}(\varphi, \lambda)$ sur R_2 satisfait

$$G_{R_2}(\varphi, \lambda) = G_{\mathbb{F}_q}(\varphi', \chi_a) G_{\mathbb{F}_q}(\varphi'', \chi_b),$$

où $G_{\mathbb{F}_q}(\varphi', \chi_a)$ et $G_{\mathbb{F}_q}(\varphi'', \chi_b)$ sont des sommes de Gauss sur $\mathbb{F}_q$.

Ensuite, nous présentons la définition de l'hyper somme d'Eisenstein sur R_2. Précisément, si n un entier positif et $\varphi_1, \varphi_2, \ldots, \varphi_n$ des caractéres multiplicatifs de R_2. Alors la somme hyper Eisenstein pour $\varphi_1, \varphi_2, \ldots, \varphi_n$ sur R_2 est définie par

$$E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1) = \sum_{\substack{t_1, t_2, \ldots, t_n \in R_2^*, \\ \mathrm{Tr}(t_1 + t_2 + \cdots + t_n) = 1}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n). \qquad (1)$$

Comme extension, nous définissions $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r)$ comme suit:

$$E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) = \sum_{t_1, t_2, \ldots, t_n \in R_2^*, \mathrm{Tr}(t_1 + t_2 + \cdots + t_n) = r} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n)$$

pour chaque $r \in R_{(l)}$. Nous calculons la valeur de $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r)$:

$$E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) = E_{\mathbb{F}_q}(\varphi_1', \varphi_2', \ldots, \varphi_n'; r_1) E_{\mathbb{F}_q}(\varphi_1'', \varphi_2'', \ldots, \varphi_n''; r_2),$$

où $r = ur_1 + (1-u)r_2 \in R_{(l)}$.

Nous utilisons ces résultats et d'autres qui en découlent pour déduire des constructions spécifiques de trois "codebooks" asymptotiquement optimaux par rapport à la borne de Welch et une classe de "codebooks" optimaux par rapport à la borne de Levenshtein en utilisant des sommes de caractères sur l'anneau fini non chaîné $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$. Tout d'abord, nous construisons deux classes de "codebooks" asymptotiquement optimaux en utilisant la somme de Gauss sur R_2. Plus précisément, si $\varphi := \varphi' \star \varphi''$ $(\varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*)$ et $\lambda := \chi_a \star \chi_b$ $(\chi_a, \chi_b \in \widehat{\mathbb{F}_q}, a, b \in \mathbb{F}_q)$ est un caractère multiplicatif et un caractère additif de R_2, respectivement. En supposant que $t = ut' + (1-u)t'' \in R_2^*$, nous définissions un ensemble $C_0(R_2^*, \widehat{R}_2^* \times \widehat{R}_2)$ comme

$$\begin{aligned} C_0(R_2^*, \widehat{R}_2^* \times \widehat{R}_2) : &= \left\{ \frac{1}{\sqrt{K}} (\varphi(t)\lambda(t))_{t \in R_2^*}, \varphi \in \widehat{R}_2^*, \lambda \in \widehat{R}_2 \right\} \\ &= \left\{ \frac{1}{\sqrt{K}} (\varphi'(t')\varphi''(t'')\chi_a(t')\chi_b(t''))_{t',t'' \in \mathbb{F}_q^*}, \varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*, \right. \\ &\qquad \left. \chi_a, \chi_b \in \widehat{\mathbb{F}}_q \right\}, \end{aligned}$$

où $K = |R_2^*| = (q-1)^2$.

Nous présentons ensuite la première construction de "codebooks" $C_1 := C_1(R_2^*, \widehat{R}_2^* \times \widehat{R}_2)$ de longueur $K_1 = |R_2^*| = (q-1)^2$ sur R_2. C_1 est construit comme suit.

$$C_1 : = \left\{ \frac{1}{\sqrt{K_1}} (\psi(t')\psi(t'')\chi_a(t')\chi_b(t''))_{t',t'' \in \mathbb{F}_q^*}, \psi \in \widehat{\mathbb{F}}_q^*, \chi_a, \chi_b \in \widehat{\mathbb{F}}_q \right\}. \quad (2)$$

Nous prouvons que C_1 est un codebook de longueur $(q^2(q-1), (q-1)^2)$ ayant une corrélation croisée maximale d'amplitude $I_{\max}(C_1) = \frac{q}{(q-1)^2}$. De plus, le codebook C_1 satisfait asymptotiquement la borne de Welch.

Nous présentons également une deuxième construction de "codebook" $C_2 := C_2(R_2^*, \widehat{R}_2^* \times \widehat{R}_2^*)$ de longueur $K_2 = |R_2^*| = (q-1)^2$ sur R_2. C_2 est défini comme suit. $C_2 : \left\{ \frac{1}{\sqrt{K_2}} (\varphi'(t')\varphi''(t'')\chi_a(t')\chi_a(t''))_{t',t'' \in \mathbb{F}_q^*}, \varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*, \chi_a \in \widehat{\mathbb{F}}_q \right\}$.

Avec cette construction, nous déterminons la magnitude maximale $I_{\max}(C_2)$ et nous montrons que C_2 est un $(q(q-1)^2, (q-1)^2)$ codebook ayant une corrélation croisée maximale d'amplitude $I_{\max}(C_2) = \frac{q}{(q-1)^2}$. De plus, le codebook C_2 satisfait asymptotiquement la borne de Welch. Nous présentons également une troisième construction de "codebooks" optimaux qui sont construits par des sommes de Jacobi sur R_2. Précisément, on considère $t_1 = ut_1' + (1-u)t_1'', t_2 = ut_2' + (1-u)t_2'' \in R_2^*$ et on définit

$$\begin{aligned} D' &= \{(t_1, t_2) \in (R_2^*)^2 : t_1 + t_2 = 1\} \\ &= \{(t_1', t_2', t_1'', t_2'') \in (\mathbb{F}_q^*)^4 : t_1' + t_2' = 1, t_1'' + t_2'' = 1\}. \end{aligned} \quad (3)$$

Le "codebook" $C_3 := C_3(D', \widehat{R}_2^* \times \widehat{R}_2^*)$ de longueur $K_3 = |D'| = (q-2)^2$ sur R_2 est construit alors comme

$$C_3 : = \left\{ \frac{1}{\sqrt{K_3}} (\varphi_1(t_1)\varphi_2(t_2))_{t_1,t_2 \in D'}, \varphi_1 = \varphi_1' \star \varphi_1'', \varphi_2 = \psi \star \psi, \varphi_1', \varphi_1'', \psi \in \widehat{\mathbb{F}}_q^* \right\} \quad (4)$$

Et nous prouvons que C_3 est "codebook" de longueur $((q-1)^3, (q-2)^2)$ ayant un maximum corrélation croisée d'amplitude $I_{\max}(C_3) = \frac{q}{(q-2)^2}$. De plus, C_3 satisfait asymptotiquement la borne de Welch.

Enfin, nous présentons une quatrième construction des "codebook". Précisément, en supposant que $\lambda := \chi_1 \star \chi_1$ est le caractère additif canonique sur R_2 et $t = ut' + (1-u)t'' \in R_2$, où χ_1 est le caractère additif canonique de $\mathbb{F}_q$, nous définissons d'abord la relation d'équivalence "$\sim$" comme suit. sur l'anneau fini R_2 comme: pour tout $a = ua_1 + (1-u)a_2, b = ub_1 + (1-u)b_2 \in R_2$, *a simb* si et seulement si $a_1 + a_2 = b_1 + b_2$. $B := R_2/\sim$. Nous considérons alors l'ensemble B comme quotient de R_2 sous la relation d'équivalence "$\sim$" et nous définissons pour tout $x, y \in \mathbb{F}_q$, $C_4(B) = \{\boldsymbol{c}_{x,y} : x, y \in B\}$, où $\boldsymbol{c}_{x,y} = \frac{1}{\sqrt{q}}(\lambda((t+x)^3 + yt))_{t \in D}$. On notant $\widetilde{C}_4 := C_4(B) \cup \xi_q$, on montre que $\widetilde{C}_4$ un codebook de longueur (q^2+q, q) ayant une amplitude de corrélation croisée maximale $I_{\max}(\widetilde{C}_4) = \frac{1}{\sqrt{q}}$. De plus, $\widetilde{C}_4$ satisfait la borne de Welch.

Au final, nous présentons sept classes de "codebooks" asymptotiquement optimaux et deux classes de "codebooks" optimaux, qui ont été construits à partir de somme de caractères sur R_1 et R_2. Les résultats des calculs ont montré que l'amplitude maximale de corrélation de ces "codebooks" codes satisfont la borne de Welch ou la borne de Levenshtein (certains, seulement, asymptotiquement). Les paramètres des "codebooks" obtenus sont pertinents. En comparaison à la littérature, nos "codebooks" possédent de nouveaux paramètres, nous les avions répertoriés dans le tableauen fin de chapitre 3. Les paramètres de nos "codebooks" sont flexibles.

- Le chapitre 4 étudie une méthode de construction des codes linéaires avec un "hull" unidimensionnelle et généralise davantage la méthode de construction dans [16, 70]. Premièrement, les codes linéaires avec un "hull" unidimensionnelle de [16, 70] construits en utilisant certaines sommes de Gauss sont généralisés pour produire de tels codes linéaires en utilisant des sommes Gaussiennes générales sur des corps finis. Deuxièmement, certaines propriétés similaires aux sommes Gaussiennes sont obtenues en définissant deux applications homomorphes d'un corps fini à un autre corps fini. Dans ce chapitre, nous présentons principalement quelques méthodes de construction de codes linéaires avec un "hull" unidimensionnelle sur des corps finis et généralisons les méthodes de construction de [16, 70] à des méthodes plus générales. Précisément dans la Section 4.1, nous définissons deux homomorphismes d'un corps fini dans un corps fini puis étudions leurs propriétés, qui seront utiles pour construire des codes linéaires avec un "hull" unidimensionnelle. Dans la Section 4.2, nous construisons plusieurs classes de codes linéaires avec un "hull" unidimensionnelle en utilisant la somme Gaussienne générale sur des corps finis, puis nous obtenons des codes linéaires

optimaux ou presque optimaux. Ce résultat généralise les résultats de [16, 70]. Dans la Section 4.3, basées sur deux homomorphismes (4.12) et (4.13), des méthodes de construction de codes linéaires à "hull" unidimensionnelle sont présentées. Nous utlisons un lemme utile qui stipule que si $\mathcal{C}$ un code linéaire $[n,k]$ sur $\mathbb{F}_q$ de matrice génératrice $G=[I_k,P]$. Alors le code $\mathcal{C}$ a un "hull" unidimensionnelle si la matrice PP^T a une valeur propre -1 avec une multiplicité (algébrique) 1. Avec ce lemme qui avait été prouvé dans [70] (Lemme 1.2.4), nous donnons des conditions suffisantes sont données pour qu'un code linéaire sur des corps finis soit un code linéaire avec un "hull" à une dimension. Plusieurs classes de codes linéaires à "hull" unidimensionnelles ayant de nouveaux paramètres sont construites. Enfin, une borne inférieure sur les distances minimales des codes linéaires crées est présentée. Nous décrivons ci-dessous quelques résultats majeurs concernant les constructions de codes linéaires à "hull" unidimensionnelle à partir de Sommes Gaussiennes sur des corps finis. Soit q une puissance de p, où p est un nombre premier. Supposons que $\mathcal{G}=\mathbb{F}_{r^m}$, où r est un nombre premier et m est un entier positif. Soit ψ un caractère multiplicatif non trivial de $\mathbb{F}_{r^m}$ et $N>1$ l'ordre de ψ (c'est-à-dire que N est le plus petit entier positif tel que $\psi^N=\psi_0$). Soit $\rho:\mathcal{G}\longrightarrow\mathbb{C}$ une fonction. La fonction ρ satisfait $\rho|_{\mathbb{F}_{r^m}^*}=\psi$, c'est-à-dire pour tout $x\in\mathbb{F}_{r^m}^*$, $\rho(x)=\psi(x)$. Définissons la matrice $r^m\times r^m$ $P=(p_{ij})$ par $p_{ij}=\rho(x_j-x_i)$. Nous savons que le multi-ensemble

$$\left\{\lambda_a:=\sum_{x\in\mathbb{F}_{r^m}}\rho(x)\chi_a(x)\sum_{x\in\mathbb{F}_{r^m}}\rho(x)\overline{\chi}_a(x):a\in\mathbb{F}_{r^m}\right\}$$

présente toutes les valeurs propres de la matrice PP^T. Nous utilisons entre autre ce résultat clé pour caractériser et construire des codes de "hull" unidimensionnelle. Pour cela, nous nous plaçons en particulier dans $\mathbb{F}_{r^m}$ un corps fini, où r est un nombre premier et m est un entier positif. Soit ψ un caractère multiplicatif non trivial d'ordre N sur $\mathbb{F}_{r^m}^*$, où N est un entier positif. Supposons qu'il existe un corps de nombres K et un élément $\beta\in\mathbb{O}_K$ satisfaisant certaines conditions. Nous définissions $\rho:\mathbb{F}_{r^m}\longrightarrow\mathbb{C}$ par

$$\rho(x)=\begin{cases}\beta, & \text{si } x=0;\\ \psi(x), & \text{si } x\in\mathbb{F}_{r^m}^*.\end{cases}$$

Nous définissons également $P=(p_{ij})\in M_{r^m}(\mathbb{O}_K)$ par $p_{ij}=\rho(x_j-x_i)$. Aussi, $\bar{P}=(\bar{p}_{ij})$, où $\bar{p}_{ij}=p_{ij}+\mathcal{P}\in\mathbb{F}_{p^f}$, où f est le degré de $\mathcal{P}$.

Avec ces notations, nous considérons le code linéaire $\mathcal{C}$ sur $\mathbb{F}_{p^f}$ de matrice génératrice $[I_{r^m},\bar{P}]$. Soit $\psi(-1)=1$. Ensuite nous montrons le résultat suivant.

(1) Si $p=2$ et r est impair, alors $\mathcal{C}$ est un code linéaire $[2r^m,r^m]$ sur $\mathbb{F}_{p^f}$ avec "hull" unidimensionnelle.

(2) Si $p\geq 3$ est impair avec r et p premier entre eux et $2\beta+G(\psi,\chi_a)\not\equiv 0 \pmod{\mathcal{P}}$ pour tout $a\in\mathbb{F}_{r^m}^*$, alors $\mathcal{C}$ est un code linéaire $[2r^m,r^m]$ sur $\mathbb{F}_{p^f}$ avec "hull" unidimensionnelle.

Nous proposons aussi d'autres constructions de codes linéaires à "hull" unidimensionnelle. Nous présentons dans la suite d'un de nos résultats. Soit r un nombre premier et m un entier positif. $\mathbb{F}_{r^m}$ désigne le corps fini d'ordre r^m. Soit $\mathbb{F}_{r^m}^* = \mathbb{F}_{r^m} \backslash \{0\}$ et $\mathbb{F}_{r^m}^* = \langle \alpha \rangle$, où α est un élément primitif fixe de $\mathbb{F}_{r^m}^*$. Supposons que $N > 1$ est un entier positif et $N \mid (r^m - 1)$. Soit q une puissance de p, où p est un nombre premier. Supposons que $N \mid (q-1)$. Soit $\mathbb{F}_q^* = \langle \beta \rangle$, où β est un élément primitif fixe de $\mathbb{F}_q^*$. Par commodité on pose $u = \beta^{\frac{q-1}{N}}$. On définit la fonction

$$\varphi : \mathbb{F}_{r^m}^* \longrightarrow \mathbb{F}_q^*, \varphi(\alpha^k) = u^k,$$

où $0 \leq k \leq r^m - 2$. Il est facile de savoir que φ est un homomorphisme d'ordre N. Définissons le noyau de l'homomorphisme φ comme $\ker(\varphi) := \{\alpha^k, 0 \leq k \leq r^m - 2 : \varphi(\alpha^k) = 1\} = \langle \alpha^N \rangle$. On suppose que p et r sont premiers entre eux. Alors il existe un entier positif t tel que $r \mid (q^t - 1)$. Soit $\mathbb{F}_{q^t}^* = \langle \gamma \rangle$ et $\zeta = \gamma^{\frac{q^t-1}{r}}$, où γ est un élément primitif fixe de $\mathbb{F}_{q^t}^*$. Pour tout $a \in \mathbb{F}_{r^m}$, nous définissons

$$\chi_a : \mathbb{F}_{r^m} \longrightarrow \overline{\mathbb{F}}_q^*, \chi_a(x) = \zeta^{\mathrm{Tr}_r^{r^m}(ax)}, x \in \mathbb{F}_{r^m},$$

où $\mathrm{Tr}_r^{r^m}$ désigne la fonction de trace de $\mathbb{F}_{r^m}$ vers $\mathbb{F}_r$. Il est facile de savoir que χ_a est un homomorphisme. De plus, il découle de la définition de χ_a que $g(\varphi, \chi_{ab}) = \overline{\varphi}(b) g(\varphi, \chi_a)$, pour $a \in \mathbb{F}_{r^m}$ et $b \in \mathbb{F}_{r^m}^*$.

Fixons $v \in \mathbb{F}_q$. Soit $\mathbb{F}_{r^m} = \{x_i : 1 \leq i \leq r^m\}$. Définissons la matrice $r^m \times r^m$ $P = (p_{ij}) \in M_{r^m}(\mathbb{F}_q)$ en définissant $p_{ij} = \rho(x_j - x_i)$, où

$$\rho(x_j - x_i) = \begin{cases} \varphi(x_j - x_i), & \text{if } i \neq j; \\ v, & \text{if } i = j. \end{cases} \tag{5}$$

Pour tout $a \in \mathbb{F}_{r^m}$, on définit $\eta_a := (\chi_a(x_1), \chi_a(x_2), \ldots, \chi_a(x_{r^m}))^T$, où "$T$" désigne l'opérateur de transposition. Alors le $i$ème composant de $P\eta_a$ est $\sum_{j=1}^{r^m} \rho(x_j - x_i)\chi_a(x_j) = \sum_{x \in \mathbb{F}_{r^m}} \rho(x - x_i)\chi_a(x) \overset{y:=x-x_i}{=\!=\!=} \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y + x_i) = \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y)\chi_a(x_i)$.

Ainsi, $P\eta_a = \left(\sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y) \right) \eta_a$ et η_a est un vecteur propre de P.

De même, la $i$ème composante de $P^T\eta_a$ est $\sum_{j=1}^{r^m} \rho(x_i - x_j)\chi_a(x_j) = \sum_{x \in \mathbb{F}_{r^m}} \rho(x_i - x)\chi(x) \overset{y:=x_i-x}{=\!=\!=} \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(x_i - y) = \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(-y)\chi_a(x_i)$. Ainsi, $P^T\eta_a = \left(\sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(-y) \right) \eta_a$ et η_a est aussi un vecteur propre de P^T. Ensuite, nous prouvons que les r^m vecteurs $\{\eta_a := (\chi_a(x_1), \chi_a(x_2), \ldots, \chi_a(x_{r^m}))^T : a \in \mathbb{F}_{r^m}\}$ sont linéairement indépendants sur $\overline{\mathbb{F}}_q$. Par conséquent, les multi-ensembles $\left\{ \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y) : a \in \mathbb{F}_{r^m} \right\}$ and $\left\{ \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(-y) : a \in \mathbb{F}_{r^m} \right\}$ présente

respectivement toutes les valeurs propres de la matrice P et P^T. En conséquence,

$$PP^T\eta_a = P\left(\sum_{y\in\mathbb{F}_{r^m}}\rho(y)\chi_a(-y)\right)\eta_a = \left(\sum_{y\in\mathbb{F}_{r^m}}\rho(y)\chi_a(y)\sum_{y\in\mathbb{F}_{r^m}}\rho(y)\chi_a(-y)\right)\eta_a.$$

Alors le multi-ensemble $\left\{\lambda_a := \sum_{y\in\mathbb{F}_{r^m}}\rho(y)\chi_a(y)\sum_{y\ in\mathbb{F}_{r^m}}\rho(y)\chi_a(-y) : a\in\mathbb{F}_{r^m}\right\}$ présente toutes les valeurs propres de la matrice PP^T et $\{\eta_a : a\in\mathbb{F}_{r^m}\}$ présente tous les vecteurs propres de PP^T.

Nous enduisons que

$$\begin{aligned}
\lambda_a &= \sum_{y\in\mathbb{F}_{r^m}}\rho(y)\chi_a(y)\sum_{y\in\mathbb{F}_{r^m}}\rho(y)\chi_a(-y)\\
&= \left(v+\sum_{y\in\mathbb{F}^*_{r^m}}\varphi(y)\chi_a(y)\right)\left(v+\sum_{y\in\mathbb{F}^*_{r^m}}\varphi(y)\chi_a(-y)\right)\\
&= (v+g(\varphi,\chi_a))(v+g(\varphi,\overline{\chi}_a))\\
&= v^2+vg(\varphi,\chi_a)+vg(\varphi,\overline{\chi}_a)+g(\varphi,\chi_a)g(\varphi,\overline{\chi}_a)\\
&= v^2+vg(\varphi,\chi_a)+\varphi(-1)vg(\varphi,\chi_a)+\varphi(-1)(g(\varphi,\chi_a))^2\\
&= v^2+(1+\varphi(-1))vg(\varphi,\chi_a)+\varphi(-1)(g(\varphi,\chi_a))^2.
\end{aligned}$$

Ainsi, toutes les valeurs propres de PP^T sont données par le multiensemble

$$\{\lambda_a := v^2+(1+\varphi(-1))vg(\varphi,\chi_a)+\varphi(-1)(g(\varphi,\chi_a))^2 : a\in\mathbb{F}_{r^m}\}.$$

Enfin, nous considérons le code linéaire $\mathcal{C} := \mathcal{C}_{(\varphi,v)}$ sur le corps fini $\mathbb{F}_q$ de matrice génératrice $G = [I_{r^m}, P]$. Nous prouvons que $\mathcal{C}$ est un code linéaire $[2r^m, r^m]$ sur $\mathbb{F}_q$. Dans le cas particulier où $p = 2$, nous obtenons facilement des codes à "hull" unidimensionnelle. Plus précisément, si r un nombre premier impair et m un entier positif. Supposons que $N > 1$ est un entier positif et $N \mid (r^m-1)$. Soit q une puissance de $p = 2$ et $N \mid (q-1)$. Alors $\mathcal{C} := \mathcal{C}_{(\varphi,1)}$ est le code linéaire sur $\mathbb{F}_q$ de matrice génératrice $[I_{r^m}, P]$ est de paramètre $[2r^m, r^m]$ sur $\mathbb{F}_q$ avec un "hull" unidimensionnelle.

Nous avons étudié également le cas où $p > 3$. Nous démontrons dans ce cas l'existence d'un code de "hull" unidimensionnelle. Plus précisément, nous posons $\mathbb{F}_q^* = \langle\beta\rangle$, où β est un élément primitif fixe de $\mathbb{F}_q^*$. Supposons que $4 \mid (q-1)$.

Nous définissons $\rho(0) = v = \beta^{\frac{q-1}{4}}$. Alors $v^2 = (\beta^{\frac{q-1}{4}})^2 = \beta^{\frac{q-1}{2}} = -1$. On obtient alors une matrice $r^m \times r^m$ $P = (p_{ij})$ par $p_{ij} = \rho(x_j - x_i)$ definit par une certaine matrice. De plus, $\varphi(-1) = \varphi(\alpha^{\frac{r^m-1}{2}}) = u^{\frac{r^m-1}{2}} = (\beta^{\frac{q-1}{N}})^{\frac{r^m-1}{2}} = (\beta^{\frac{q-1}{2}})^{\frac{r^m-1}{N}} = (-1)^{\frac{r^m-1}{N}}$. Quand $\frac{r^m-1}{N}$ est impair, $\varphi(-1) = -1$; quand $\frac{r^m-1}{N}$ est pair, $\varphi(-1) = 1$.

Lorsque $\frac{r^m-1}{N}$ est impair, on a

$$\lambda_a = \begin{cases} -1, & \text{si } a = 0;\\ -1-(g(\varphi,\chi_a))^2, & \text{si } a\in\mathbb{F}^*_{r^m}; \end{cases} \tag{6}$$

quand $\frac{r^m-1}{N}$ est pair, on obtient

$$\lambda_a = \begin{cases} -1, & \text{si } a = 0; \\ -1 + (2v + g(\varphi, \chi_a))g(\varphi, \chi_a), & \text{si } a \in \mathbb{F}_{r^m}^*. \end{cases} \tag{7}$$

Ces résultas nous permettent de déduire d'abord des conditions suffisantes pour construire des codes linéaires avec "hull" unidimensionnelle lorsque $\frac{r^m-1}{N}$ est impair. Plus spécifiquement, si r un nombre premier et m un entier positif. Supposons que $N > 1$ est un entier positif et $N \mid (r^m - 1)$. Soit q une puissance d'un nombre p premier et r premier avec r. Supposons que $N \mid (q-1)$ et $4 \mid (q-1)$. Soit $\mathcal{C} := \mathcal{C}_{(\varphi, \beta^{\frac{q-1}{4}})}$ le code linéaire sur $\mathbb{F}_q$ avec matrice génératrice $[I_{r^m}, P]$. Lorsque $\frac{r^m-1}{N}$ est impair, $\mathcal{C}$ est un code linéaire $[2r^m, r^m]$ sur $\mathbb{F}_q$ avec "hull" unidimensionnelle.

Soit $\mathcal{C} := \mathcal{C}_{(\varphi,0)}$ un code linéaire sur $\mathbb{F}_q$ de matrice génératrice $G = [I_{r^m}, P]$. Soit A un entier positif. Supposons que tous les vecteurs A dans $\{\mu_{x_1}, \ldots, \mu_{x_{r^m}}\}$ sont linéairement indépendants et que tous les vecteurs A dans $\{\nu_{x_1}, \ldots, \nu_{x_{r^m}}\}$ sont également linéairement indépendants. Alors la distance minimale $d_{min}(\mathcal{C})$ du code vérifie $d_{min}(\mathcal{C}) \geq A + 1$.

En rémumé dans ce chapitre, nous avons d'abord généralisé les résultats de [16, 70] et utilisé des sommes Gaussiennes générales pour construire des codes linéaires de "hull" unidimensionnelle via des outils de la théorie des nombres. De plus, nous avons proposé une méthode générale pour construire des codes linéaires avec une "hull" unidimensionnelle en utilisant un analogue de sommes Gaussiennes où les caractères additif et multiplicatif correspondants prennent leurs valeurs dans un corps fini au lieu du des nombres complexes. De façon remarquable, les constructions de codes linéaires à "hull" unidimensionnelle ont été étudiées en caractérisant les valeurs propres de la matrice PP^T, et en les combinant avec le lemme énoncé ci-dessus. Nous avons présenté quelques conditions suffisantes pour qu'un code linéaire sur des corps finis de matrice génératrice $[I_{r^m}, P]$ soit un code linéaire avec une "hull" unidimensionnelle. En comparaison avec [16, 70], les résultats obtenus dans ce chapitre présentent des avantages en termes de généralisation et simplicité. En effet, les méthodes de constructions proposées dans la littérature sont spécifiques mais aussi assez complexes techniques, tandis que nos méthodes sont plus générales et directes. Elles se présentent principalement par trois aspects:

(1) Les méthodes de construction sont plus générales. Dans [16, 70], les auteurs avaient besoin que la matrice P ait des propriétés spéciales; par exemple, la plupart d'entre eux sont symétriques. Cependant, nous pouvons déterminer complètement toutes les valeurs propres de la matrice PP^T pour n'importe quelle matrice P. De plus, les auteurs ont construit des codes linéaires avec une coque unidimensionnelle en utilisant les sommes Gaussiennes spéciales (par exemple, les sommes Gaussiennes quadratiques et les sommes Gaussiennes dans le cas semi-primitif). Cependant, nous avons utilisé des sommes Gaussiennes générales pour construire des codes de coque linéaires avec des corps de nombres via unidimensionnels. Notre méthode de construction de ce chapitre généralise davantage la

methode de construction dans [16, 70], et les résultats pertinents dans [16, 70] sont des cas particuliers des résultats de ce chapitre.

(2) Les méthodes de construction sont plus directes. Dans [16, 70], les auteurs ont construit des codes linéaires avec une coque unidimensionnelle sur des corps finis en utilisant la matrice génératrice sur des corps de nombres quadratiques ou des corps cyclothymiques, tandis que nous les avons construits directement en utilisant la matrice génératrice sur des corps finis. De plus, cette approche simple peut conduire à des codes linéaires plus optimaux ou presque optimaux.

(3) Nous avons d'abord présenté une borne inférieure sur la distance minimale du code linéaire $\mathcal{C}$ sur $\mathbb{F}_q$ avec la matrice génératrice $G = [I_{r^m}, P]$ quand $N = 2$. Dériver de taille borne assez générale n'est pas une tache facile.

- Le chapitre 5 construit des codes linéaires binaires minimaux avec peu de poids (non nuls) en utilisant les fonctions 2-vers-1 connues sur le corps finis $\mathbb{F}_{2^n}$ à 2^n éléments. Inspirées des travaux de [72], plusieurs familles de codes linéaires à peu de poids sont construites à partir de deux constructions générales et d'une nouvelle construction impliquant des fonctions 2-vers-1, et ces codes ont de nouveaux paramètres. Les codes linéaires minimaux ont des applications importantes dans la construction de schémas de partage de secrets (SSS). Ensuite, nous donnons la définition des codes linéaires minimaux.

  Rappelons que le poids de Hamming, noté $wt(\boldsymbol{a})$, d'un mot de code $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ est la cardinalité de son *support* défini comme $\mathrm{Supp}(\boldsymbol{a}) = \{0 \leq i \leq n-1 : a_i \neq 0\}$. Soient $\boldsymbol{a}$ et $\boldsymbol{b}$ des mots de code de $\mathcal{C}$. Un mot de code $\boldsymbol{b}$ de $\mathcal{C}$ est couvert par un autre mot de code $\boldsymbol{a}$ de $\mathcal{C}$ si $\mathrm{Supp}(\boldsymbol{a})$ contient $\mathrm{Supp}(\boldsymbol{b})$. Un mot de code non nul $\boldsymbol{a} \in \mathcal{C}$ est appelé *minimal* s'il ne couvre que les mots de code $c\boldsymbol{a}$ pour tout $c \in \mathbb{F}_p$, mais pas d'autres mots de code non nuls de $\mathcal{C}$. Un code linéaire $\mathcal{C}$ est appelé *code linéaire minimal* si chaque mot de code non nul de $\mathcal{C}$ est minimal.

  Un résultat très connu due à Ashikhmin et Barg ([1]) donne une condition suffisante simple pour un code soit minimale. Plus précisément, ils montrent qu'un code linéaire $\mathcal{C}$ est minimal si ses poids sont suffisamment proches l'un de l'autre; précisément si $\mathcal{C}$ est un code linéaire sur $\mathbb{F}_p$, et $w_{\min}$ et $w_{\max}$ indiquent le minimum et le maximum Poids de Hamming des mots de code non nuls dans $\mathcal{C}$, respectivement. On a

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}},$$

  alors $\mathcal{C}$ est minimal. Dans chapitre nous proposons plusieurs constructions de codes linaires minimaux. Nous exploitons trois constructions génériques (ou plutôt deux et une variante d'une des deux).

  - La première construction générique de codes linéaires binaires $\mathcal{C}_F$ est basée sur la donnée d'une fonction booléenne vectorielle F. Le code $\mathcal{C}_F$ est alors définit par $\mathcal{C}_F := \{\boldsymbol{c}_{a,b} = (\mathrm{Tr}_n(ax + bF(x)))_{x \in \mathbb{F}_{2^n}^*} : a, b \in \mathbb{F}_{2^n}\}$, où Tr désigne la fonction trace (souvent la trace absolue). Il est clair que la longueur et

la dimension de $\mathcal{C}_F$sont respectivement 2^n-1 et au plus $2n$. Nous savons que la dimension de $\mathcal{C}_F$ est $2n-d_{K_1}$, où d_{K_1} est la dimension de $\mathbb{F}_2$-espace vectoriel.

– La deuxième construction générique des codes linéaires binaires $\mathcal{C}_D$ à partir d'un ensemble de définition donné $D := \{d_1, d_2, \ldots, d_l\}$ suggère de définir un code linéaire $\mathcal{C}_D = \{\boldsymbol{c}_b = (\mathrm{Tr}_n(bd_1), \mathrm{Tr}_n(bd_2), \ldots, \mathrm{Tr}_n(bd_l)) : b \in \mathbb{F}_{2^n}\}$. Pour établir une connexion avec les fonctions F (définies sur $\mathbb{F}_{2^n}$), nous pouvons choisir D (ou plus approprié D_F), par exemple, comme ensemble non nul de toutes les valeurs de F. Dans ce cas, nous notons le code résultant par $\mathcal{C}_{D_F}$, qui sera défini précisément comme suit: $\mathcal{C}_{D_F} = \{\boldsymbol{c}_b = (\mathrm{Tr}_n(bd_1), \mathrm{Tr}_n(bd_2), \ldots, \mathrm{Tr}_n(bd_l)) : b \in \mathbb{F}_{2^n}\}$, où $D_F := \{F(x), x \in \mathbb{F}_{2^n}\} \setminus \{0\} = \{d_1, d_2, \ldots, d_l\}$. Il est évident que la longueur et la dimension de $\mathcal{C}_{D_F}$ sont $l = |D_F|$ et au plus n, respectivement. De même, nous savons que la dimension de $\mathcal{C}_{D_F}$ est $n-d_{K_2}$, où d_{K_2} est la dimension de $\mathbb{F}_2$-espace vectoriel.

– La troisième construction générique de codes linéaires binaires est plutôt une variante de la deuxième. Les codes ainsi construits notés $\widetilde{\mathcal{C}}_{D_F}$ sont définis par $\widetilde{\mathcal{C}}_{D_F} = \{\widetilde{\boldsymbol{c}}_{a,b} = (\mathrm{Tr}_n(ad_i + bd_j))_{(d_i,d_j)\in D_F^2} : a, b \in \mathbb{F}_{2^n}\}$, où $D_F = \{F(x) : x \in \mathbb{F}_{2^n}\}\setminus\{0\} := \{d_1, d_2, \ldots, d_l\}$. De toute évidence, la longueur et la dimension de $\widetilde{\mathcal{C}}_{D_F}$ sont respectivement de l^2 et d'au plus $2n$. Pour déterminer la dimension de $\widetilde{\mathcal{C}}_{D_F}$, il suffit de calculer le nombre de $a, b \in \mathbb{F}_{2^n}$ tels que $\mathrm{Tr}_n(aF(x) + bF(y))) = 0$ pour tout $x, y \in \mathbb{F}_{2^n}$ puisque le code est linéaire. C'est-à-dire que la dimension de $\widetilde{\mathcal{C}}_{D_F}$ est $2n-d_{K_3}$, où d_{K_3} est la dimension de $\mathbb{F}_2$-espace vectoriel qui se calcule via $K_3 = \left\{(a,b) \in \mathbb{F}_{2^n}^2 : \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x)+bF(y))} = 2^{2n}\right\}$. Le poids de Hamming d'un mot de code $\widetilde{\boldsymbol{c}}_{a,b}$ dans $\widetilde{\mathcal{C}}_{D_F}$ est égal à

$$\begin{aligned}\mathrm{wt}(\widetilde{\boldsymbol{c}}_{a,b}) &= |\{1 \le i, j \le l : \mathrm{Tr}_n(ad_i + bd_j) = 1\}| \\ &= \frac{1}{2}\left(l^2 - \sum_{d_i,d_j\in D_F} (-1)^{\mathrm{Tr}_n(ad_i+bd_j)}\right).\end{aligned}$$

Posons $S_F(a,b) = \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x)+bF(y))}$. Notez que alors que

$$\begin{aligned}\sum_{d_i,d_j\in D_F} (-1)^{\mathrm{Tr}_n(ad_i+bd_j)} &= \frac{1}{4}\Bigg(\sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x)+bF(y))} - 2\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x))} \\ &\quad -2\sum_{y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bF(y))} + 4\Bigg) \\ &= \frac{1}{4}S_F(a,b) - \frac{1}{2}(W_F(0,a) + W_F(0,b)) + 1.\end{aligned}$$

où W_F désigne la transformée de Walsh de F.

Le chapitre 5 est organisé comme suit. La section 5.1 présente trois constructions de codes linéaires binaires par des fonctions 2-vers-1 sur $\mathbb{F}_{2^n}$. Nous proposons trois constructions de codes linéaires binaires (minimaux) en utilisant des fonctions 2-vers-1 sur des corps finis de caractéristique paire. Nos constructions sont basées sur des constructions génériques de codes linéaires binaires $\mathcal{C}_{D_F}$ via des foncions booléennes vectorielles F. En particulier quand la fonction F vaut 2-to-1 sur $\mathbb{F}_{2^n}$ avec $F(0)=0$, alors le poids de Hamming d'un mot de code se calcule comme suit: $\text{poids}(\widetilde{\boldsymbol{c}}_{a,b}) = 2^{2n-3} - 2^{n-1} - \frac{1}{8}S_F(a,b) + \frac{1}{4}(W_F(0,a) + W_F(0,b))$. On peut également calculer la distance minimale du code dual de $\widetilde{\mathcal{C}}_{D_F}$. Plus précisément, si F une fonction 2-vers-1 sur $\mathbb{F}_{2^n}$ avec $F(0)=0$ et si $\widetilde{\mathcal{C}}_{D_F}$ soit le code défini comme ci-dessus. De plus, soit $\widetilde{\mathcal{C}}^{\perp}_{D_F}$ le code dual de $\widetilde{\mathcal{C}}_{D_F}$ et d_{K_3} définis comme ci-dessus. Alors nous montrons que $\widetilde{\mathcal{C}}^{\perp}_{D_F}$ est un $[(2^{n-1}-1)^2, (2^{n-1}-1)^2 - (2n - d_{K_3})]$ code linéaire binaire avec la distance minimale $d^{\perp}$ satisfaisant $3 \leq d^{\perp} \leq 4$. De plus, le dual de $\widetilde{\mathcal{C}}_{D_F}$ est projectif. La section 5.2 détermine les paramètres et les distributions de poids des codes linéaires construits à la section 5.1 en utilisant le Walsh Hadamard transformée des fonctions correspondantes. Nous prouvons en particulier que si $n = 2m$ et $F(x) = x^{2^{m+1}+4} + x^{2^{m+2}+2} + \alpha x \in \mathbb{F}_{2^n}[x]$, où $m \geq 3$ est impair, et $\alpha \in \mathbb{F}_{2^n}$ tel que $\alpha^{2^m-1} = w$ avec $w \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$. Si nous définissons trois codes linéaires $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ et $\widetilde{\mathcal{C}}_{D_F}$ comme ci-dessus, respectivement. Alors,

(1) $\mathcal{C}_F$ est un code linéaire binaire à trois poids avec les paramètres $[2^n - 1.3m, 2^{n-1} - 2^m]$, et sa distribution de poids est donnée par le tableau (*);

(2) $\mathcal{C}_{D_F}$ est un code linéaire binaire à trois poids avec des paramètres $[2^{n-1} - 1, n, 2^{n-2} - 2^{m-1}]$, et sa distribution de poids est donnée par le tableau (**);

(3) $\widetilde{\mathcal{C}}_{D_F}$ est un code linéaire binaire à neuf poids avec des paramètres $[(2^{n-1} - 1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{m-1}(2^{n-1} - 1)]$, et sa distribution de poids est donnée par le tableau (***).

***Table 0.0.1**: La distribution de poids du code $\mathcal{C}_F$ (*)*

Poids	Fréquence
0	1
$2^{n-1} - 2^m$	$2^{3m-3} + 2^{n-3} - 2^{m-2}$
2^{n-1}	$3 \cdot 2^{3m-2} + 2^{n-2} - 1$
$2^{n-1} + 2^m$	$2^{3m-3} - 3 \cdot 2^{n-3} + 2^{m-2}$

De plus, certains des codes construits sont optimaux concernant la borne de Griesmer bien connue et optimale (ou presque optimale) pour la base de données de la base de Grassl. Certains des codes construits sont minimes et les structures d'accès des schémas de partage de secrets basés sur leurs codes sont décrits. En particulier, deux problèmes ouverts laissés dans [72] sont résolus. A noter que Dans le cas où $n = 2m+1$, les codes linéaires binaires $\mathcal{C}_F$ et $\mathcal{C}_{D_F}$ dérivés des codes connus fonction 2-vers-1 (exploités dans la thèse) et la fonction 2-vers-1 de la forme $(x^{2^t} + x)^e$ (avec t et n premiers entre eux) ont été étudiés dans [72]. Nous étudions le code $\widetilde{\mathcal{C}}_{D_F}$ avec quelques poids

***Table 0.0.2**: La distribution de poids du code $\mathcal{C}_{D_F}$ (**)*

Poids	Fréquence
0	1
$2^{n-2}-2^{m-1}$	$2^{n-3}+2^{m-2}$
2^{n-2}	$3\cdot 2^{n-2}-1$
$2^{n-2}+2^{m-1}$	$2^{n-3}-2^{m-2}$

***Table 0.0.3**: La distribution de poids du code $\widetilde{\mathcal{C}}_{D_F}$ (***)*

Poids	Fréquence
0	1
$2^{2n-3}-2^{n-2}-2^{m-1}(2^{n-1}-1)$	$2^{n-2}+2^{m-1}$
$2^{2n-3}-2^n-2^m$	$(2^{n-3}-2^{m-2})^2$
$2^{2n-3}-2^n+2^m$	$(2^{n-3}+2^{m-2})^2$
$2^{2n-3}-2^{n-1}-2^{m-1}$	$(3\cdot 2^{n-2}-1)(2^{n-2}-2^{m-1})$
$2^{2n-3}-2^{n-1}$	$(3\cdot 2^{n-2}-1)^2$
$2^{2n-3}-2^{n-1}+2^{m-1}$	$(3\cdot 2^{n-2}-1)(2^{n-2}+2^{m-1})$
$2^{2n-3}-2^{n-2}$	$3\cdot 2^{n-1}-2$
2^{2n-3}	$2^{2n-5}-2^{n-3}$
$2^{2n-3}-2^{n-2}+2^{m-1}(2^{n-1}-1))$	$2^{n-2}-2^{m-1}$

non nuls dérivés de ces fonctions 2-à-1. Nous montrons que si $n=2m+1$ et $F(x)=x^{2^{m+1}+2}+x^{2^{m+1}+1}+x^2+x$ ou $F(x)=x^{2^{m+1}+4}+x^{2^{m+1}+2}+x^2+x\in\mathbb{F}_{2^n}[x]$, où m est un entier positif. Alors le code linéaire $\widetilde{\mathcal{C}}_{D_F}$ est un code linéaire binaire à deux poids avec des paramètres $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$, et sa distribution de poids est donnée par le manuscrit. De plus, si $F(x)=x^{2^n-2^{m+1}+2}+x^{2^{m+1}}+x^2+x$ ou $F(x)=x^{2^{m+1}+2}+x^{2^{m+1}}+x^2+x$ ou $F(x)=(x^{2^t}+x)^e$ et e étant l'un des exposants presque courbe donnée dans la table (Table X dans [72]), où $m>1$ soit un entier positif. Alors le code $\widetilde{\mathcal{C}}_{D_F}$ est un code linéaire binaire à huit poids avec des paramètres $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n-3}{2}}(2^{n-1}-1)]$, et sa distribution de poids est donnée par le tableau ci-dessous Maintenant si $n=3m$ et $F(x)=x^{2^{2m+1}+1}+x^{2^{m+1}+1}+x^4+x^3$, où $m>1$ est un entier positif impair. Alors, nous prouvons que le code linéaire $\widetilde{\mathcal{C}}_{D_F}$ est un code linéaire binaire de paramètres $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n+2m-3}{2}}(2^{n-1}-1)]$, sa distribution de poids est donnée par le tableau ci-dessous. De plus quand $n=km$ et $F(x)=\mathrm{Tr}_m^n(x^{2^m+1})+x$, où $k>1$ est un entier positif impair et $m>1$ est un entier positif. Alors, nous prouvons que le code $\widetilde{\mathcal{C}}_{D_F}$ est un code linéaire binaire de paramètres $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n+m-4}{2}}(2^{n-1}-1)]$, sa distribution de poids est donnée par le tableau ci-dessous. D'autres codes des fonctions 2-à-1 sont également étudiés ce chapitre. Nous avons montré que les codes obtenus sont minimaux pour presque tous les cas. Prouver la propriété de minimalité de chaque code prendrait beaucoup de temps. Pour cette raison et pour éviter la redondance dans les preuves, nous présentons, à titre d'exemple, une preuve le

***Table 0.0.4**: La distribution de poids du code $\widetilde{\mathcal{C}}_{D_F}$ (*)*

Poids	Fréquence
0	1
$2^{2n-3}-2^{n-2}-2^{\frac{n-3}{2}}(2^{n-1}-1)$	$2^{n-1}+2^m$
$2^{2n-3}-3\cdot 2^{n-2}-2^{\frac{n-1}{2}}$	$(2^{n-2}-2^{m-1})^2$
$2^{2n-3}-3\cdot 2^{n-2}+2^{\frac{n-1}{2}}$	$(2^{n-2}+2^{m-1})^2$
$2^{2n-3}-2^{n-1}-2^{\frac{n-3}{2}}$	$(2^{n-1}-1)(2^{n-1}-2^m)$
$2^{2n-3}-2^{n-1}$	$(2^{n-1}-1)^2$
$2^{2n-3}-2^{n-1}+2^{\frac{n-3}{2}}$	$(2^{n-1}-1)(2^{n-1}+2^m)$
$2^{2n-3}-2^{n-2}$	$2^{2n-3}+3\cdot 2^{2m-1}-2$
$2^{2n-3}-2^{n-2}+2^{\frac{n-3}{2}}(2^{n-1}-1))$	$2^{n-1}-2^m$

***Table 0.0.5**: La distribution de poids du code $\widetilde{\mathcal{C}}_{D_F}$ (**)*

Poids	Fréquence
0	1
$2^{2n-3}-2^{n-2}-2^{\frac{n+2m-3}{2}}(2^{n-1}-1)$	$2^{m-1}+2^{\frac{m-1}{2}}$
$2^{2n-3}-2^{n-1}-2^{n+2m-2}-2^{\frac{n+2m-1}{2}}$	$(2^{m-2}-2^{\frac{m-3}{2}})^2$
$2^{2n-3}-2^{n-1}-2^{n+2m-2}+2^{\frac{n+2m-1}{2}}$	$(2^{m-2}+2^{\frac{m-3}{2}})^2$
$2^{2n-3}-2^{n-1}(2^{2m-1}-1)$	$2^{2m-3}-2^{m-2}$
$2^{2n-3}-2^{n-1}-2^{\frac{n+2m-3}{2}}$	$(2^n-2^{m-1}-1)(2^{m-1}-2^{\frac{m-1}{2}})$
$2^{2n-3}-2^{n-1}$	$(2^n-2^{m-1}-1)^2$
$2^{2n-3}-2^{n-1}+2^{\frac{n+2m-3}{2}}$	$(2^n-2^{m-1}-1)(2^{m-1}+2^{\frac{m-1}{2}})$
$2^{2n-3}-2^{n-2}$	$2^{n+1}-2^m-2$
$2^{2n-3}-2^{n-2}+2^{\frac{n+2m-3}{2}}(2^{n-1}-1)$	$2^{m-1}-2^{\frac{m-1}{2}}$

***Table 0.0.6**: La distribution de poids du code $\widetilde{\mathcal{C}}_{D_F}$ (***)*

Poids	Fréquence
0	1
$2^{2n-3}-2^{n-2}-2^{\frac{n+m-4}{2}}(2^{n-1}-1)$	$2^{n-m}+2^{\frac{n-m}{2}}$
$2^{2n-3}-2^{n-1}-2^{n+m-3}-2^{\frac{n+m-2}{2}}$	$(2^{n-m-1}-2^{\frac{n-m-2}{2}})^2$
$2^{2n-3}-2^{n-1}-2^{n+m-3}+2^{\frac{n+m-2}{2}}$	$(2^{n-m-1}+2^{\frac{n-m-2}{2}})^2$
$2^{2n-3}-2^{n-1}-2^{\frac{n+m-4}{2}}$	$(2^n-2^{n-m}-1)(2^{n-m}-2^{\frac{n-m}{2}})$
$2^{2n-3}-2^{n-1}$	$(2^n-2^{n-m}-1)^2$
$2^{2n-3}-2^{n-1}+2^{\frac{n+m-4}{2}}$	$(2^n-2^{n-m}-1)(2^{n-m}+2^{\frac{n-m}{2}})$
$2^{2n-3}-2^{n-2}$	$2^{n+1}-2^{n-m+1}-2$
$2^{2n-3}-2^{n-1}+2^{n+m-3}$	$2^{2n-2m-1}-2^{n-m-1}$
$2^{2n-3}-2^{n-2}+2^{\frac{n+m-4}{2}}(2^{n-1}-1))$	$2^{n-m}-2^{\frac{n-m}{2}}$

montrant que une famille de codes étudiés.

Nous décrivons donc les structures d'accès des systèmes de partage de secrets basés sur nos codes. La minimalité des autres codes peut être montrée de la même manière. Nous concluons que si $m \geq 3$ impair et $n = 2m$. Alors les affirmations suivantes sont vraies.

(1) Le code $\mathcal{C}_F$ (*) est un code linéaire minimal de paramètres $[2^n - 1, 3m, 2^{n-1} - 2^m]$;

(2) Le code $\mathcal{C}_{D_F}$ (**) est un code linéaire minimal de paramètres $[2^{n-1} - 1, n, 2^{n-2} - 2^{m-1}]$;

(3) Le code $\widetilde{\mathcal{C}}_{D_F}$ (***) est un code linéaire minimal de paramètres $[(2^{n-1} - 1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{m-1}(2^{n-1} - 1)]$.

Ensuite, nous étudions l'application des codes linéaires construits dans les schémas de partage de secrets. Nous avons décrit la structure d'accès d'un schéma de partage de secret basé sur le code dual d'un code linéaire minimal. Rappelons qu'un schéma de partage secret (SSS) consiste en un croupier, un groupe $\mathcal{P} = \{P_1, P_2, \ldots, P_\ell\}$ de participants ℓ, un espace secret S, ℓ partage des espaces $S_1, S_2 \ldots, S_\ell$, une procédure de partage de calcul et une procédure de récupération de secret. Le croupier choisit un secret s parmi S, calcule une part, qui appartient à S_i , de s (avec la procédure de partage de calcul) pour chaque participant P_i et puis donne la part à P_i , où $i = 1, \ldots, \ell$. Tout ensemble couvrant un ensemble de participants qui peut récupérer le secrèt s peut également récupérer s. La procédure informatique de partage et le secrèt s ne sont connus que du concessionnaire, tandis que la procédure de récupération secrète est connue de tous les participants en P.

Un ensemble de participants qui peuvent récupérer le secret s à partir de leurs partages est appelé *un accès Positionner*. L'ensemble de tous les ensembles d'accès est appelé *la structure d'accès* d'un schéma de partage de secret. An l'ensemble d'accès est appelé un *ensemble d'accès minimal* si l'un de ses sous-ensembles appropriés ne peut pas récupérer s de leurs actions. Par conséquent, nous ne nous intéressons qu'à l'ensemble de tous les ensembles d'accès minimaux, qui est dit être comme *bonne structure d'accès* d'un schéma de partage secret.

Généralement, la structure d'accès du schéma de partage de secret construit par des codes linéaires est difficile à déterminer, mais la structure d'accès du schéma de partage de secret construit par nos codes linéaires minimaux est plus facile. Nous pouvons savoir que les codes linéaires binaires construits dans ce chapitre sont des codes linéaires minimaux dans la plupart des cas. Nous suivons ensuite la méthode de construction de la structure d'accès du schéma de partage de secret basé sur les codes duaux de codes linéaires minimaux.

Soit $\mathcal{C}$ un code linéaire minimal $[N, k, d]_p$ sur $\mathbb{F}_p$ avec la matrice génératrice $G = [\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{N-1}]$. Ensuite, dans le schéma de partage de secrets basé sur $\mathcal{C}^\perp$, le nombre de participants est $N - 1$ et le nombre d'ensembles d'accès minimaux est p^{k-1}.

- Quand $d^{\perp}=2$, si $\boldsymbol{g}_i, 0 \leq i \leq N-1$, est un multiple de $\boldsymbol{g}_0$, alors participant P_i doit figurer dans tous les ensembles d'accès minimauxé sinon, dans $(p-1)p^{k-2}$ sur p^{k-1} accès minimal ensembles.
- Lorsque $d^{\perp} \geq 3$, pour tout $1 \leq t \leq \min\{k-1, d^{\perp}-2\}$, chaque ensemble de t participants est impliqué dans $(p-1)^t p^{k-(t+1)}$ sur p^{k-1} ensembles d'accès minimaux.

Dans le cas $d^{\perp}=2$, il y a des utilisateurs qui appartiennent à chaque coalition: les "*dictators*". Dans le cas $d^{\perp} \geq 3$, le schéma de partage secret est "*democratic*": chaque utilisateur appartient au même nombre de coalitions.

Nous savons que les codes duaux de $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ et $\widetilde{\mathcal{C}}_{D_F}$ ont une distance minimale $d^{\perp} \geq 3$. Cela implique que les schémas de partage de secrets des codes linéaires binaires obtenus dans nos résultats ont des structures d'accès décrites comme ci-dessus. Un tel système de partage secret est dit démocratique. A la fib du chapitre, nous décrivons les schémas de partage de secrets liés à nos codes minimaux que nous avons obtenu dans ce chapitre.

Finalement, dans ce chapitre, nous avons construit plusieurs classes de codes linéaires binaires (et, plus important encore, codes minimaux) avec des paramètres flexibles à partir de fonctions 2-vers-1 connues. Basé sur un article très récent (2021) dû à Li et al. [72], nous avons réussi (pour la deuxième fois) à construire plusieurs familles infinies de codes avec peu de poids (à savoir, les codes à poids 1, les codes à poids 3 et les codes à poids 5). Il convient de souligner que nous avons fourni une nouvelle construction dans ce chapitre, et sur la base de cette construction, nous avons également obtenu plusieurs familles de codes à 2 poids, de codes à poids 8 et de codes à poids 9, qui ont des paramètres différents de ceux existants dans la littérature. En outre, nous avons déterminé les distributions de poids de ces codes en utilisant la transformée de Walsh des fonctions deux à un correspondantes.

Les avantages des résultats de la recherche dans ce chapitre sont les suivants:

- Les codes linéaires binaires construits dans ce chapitre sont des codes linéaires minimaux dans la plupart des cas. Nos codes linéaires peuvent être appliqués aux schémas de partage de secrets.
- Les paramètres des codes linéaires binaires construits sont nouveaux (sauf un) et optimaux. Notamment, certains d'entre eux sont optimaux par rapport à la borne de Griesmer bien connue et optimale (ou presque optimale) par rapport à la base de données en ligne de Grassl.
- Deux problèmes ouverts de la littérature récente ont été résolus. Plus précisément, dans ce chapitre, le problème 2 dans [72] a été complètement résolu, et le problème 1 dans [72] a été partiellement résolu.

- Le chapitre 6 construit plusieurs familles de codes linéaires binaires projectifs et détermine leur distribution de poids. Certains des codes linéaires proposés sont optimaux ou presque optimaux, et plusieurs classes de codes autocomplémentaires sont obtenues. Dans ce chapitre, nous construisons plusieurs

familles de codes linéaires binaires projectifs avec peu de poids non nuls en utilisant des fonctions 2-vers-1 sur $\mathbb{F}_{2^n}$ et déterminons leurs distributions de poids. Ding et al. [33] a proposé une méthode générale pour construire des codes linéaires, c'est-à-dire construire des codes linéaires en choisissant des sous-ensembles non vides appropriés sur des corps finis. La sélection de l'ensemble de définition affecte directement les paramètres des codes linéaires. Ce chapitre, construit des codes linéaires binaires projectifs de certaines formes ayant différentes restrictions sur la définition d'ensembles à partir de fonctions deux-à-un sur $\mathbb{F}_{2^n}$. En utilisant des sommes exponentielles sur des corps finis comme outil de recherche, nous calculons la transformée de Walsh de la fonction deux à un, puis déterminons complémement les paramètres et les distributions de poids des codes linéaires construits. Enfin, nous étudions la distance minimale du dual des codes construits et obtenons que les duals sont optimaux en distance par rapport à la borne "sphere packing bound" lié La distance minimale du dual des codes construits est discutée, et leurs duals sont optimaux en distance pour la borne "sphere packing bound" . En tant qu'applications, certains des codes obtenus peuvent être utilisés pour construire des schémas d'association et des schémas de partage de secrets avec des structures d'accès intéressantes. Nous avons remarque que nos codes satisfont la condition que $w_{\min}/w_{\max} > \frac{1}{2}$ sous certaines conditions et peuvent donc être employés pour construire des structures d'acc`es intéressantes pour les secrets. régimes de partage.

Pour finir, comme présenté dans le chapitre 7, nous synthétisons ci-dessous les travaux réalisés et présentons des pistes de recherches futures. Dans cette thèse, nous avons principalement étudié la théorie du codage algébrique sur corps finis et anneaux finis et leurs applications, en particulier la construction de codes optimaux ou asymptotiquement optimaux, la construction de codes linéaires à "coque" unidimensionnelle, la codes linéaires avec peu de poids non nuls et plusieurs constructions de codes linéaires projectifs. Les principaux travaux de recherche et réalisations de cette thèse couvrent plusieurs axes dans ce contexte. Spécifiquement, la thèse a construit plusieurs familles de codes optimaux ou asymptotiquement optimaux en étudiant les sommes de caractères sur l'anneau fini $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ et l'anneau non-chaîne fini $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$. Sur la base de la méthode de recherche de sommes de caractères sur des corps finis, nous avons d'abord donné les définitions des sommes Gaussiennes, des sommes de Jacobi et des (hyper)sommes d'Eisenstein sur des anneaux finis et avons étudié certaines propriétés de ces sommes de caractères. De plus, nous avons établi la relation entre les sommes Gaussiennes et les sommes hyper Eisenstein sur les anneaux finis et les sommes Gaussiennes et les sommes hyper Eisenstein sur les corps finis, respectivement. Cette relation permet de donner la valeur absolue des sommes Gaussiennes et des hyper-sommes d'Eisenstein sur les anneaux finis. Pour leurs applications, nous avons construit plusieurs classes "codebooks" optimaux et asymptotiquement optimaux par rapport à la borne de Welch et une classe "codebooks" de codes optimaux. "codebooks" par rapport à la limite de Levenshtein en utilisant ces sommes de caractères sur R_1 et R_2. Notamment, les paramètres de certains de ces "codebooks" sont nouveaux et flexibles.

Sur la base de nos réalisations, d'autres travaux de recherche peuvent êtres menés

dans la suite. Ci-dessous quelques exemples.

(1) Déinir de nouvelles sommes de caractères sur des corps finis ou des anneaux finis, puis étudier leurs propriétés et discuter des valeurs des nouvelles sommes de caractères.

(2) Construire les codes linéaires de "hull" de faible dimension en étudiant la matrice génératrice spéciale (par exemple, matrice cyclique, matrice de symétrie, etc.) et caractèriser certaines conditions suffisantes pour qu'un code linéaire soit un code linéaire avec "hull" de faible dimension. Avec ces conditions, nous pouvons construire des codes linéaires optimaux et quasi optimaux avec une "hull" de faible dimension par Magma. En particulier, trouver de nouvelles applications des codes de "hull" unidimensionnels.

(3) Construire de nouvelles fonctions cryptographiques sur des corps finis. Par exemple, les nouvelles fonctions deux-vers-un, les fonctions n-vers-1, etc. A partir de deux constructions générales de codes linéaires, il serait intéressant de présenter de nouvelles constructions de codes linéaires utilisant de nouvelles fonctions cryptographiques puis de construire codes linéaires avec de nouveaux paramètres sur des corps finis.

(4) La méthode de construction de codes linéaires sur des corps finis est étendue aux anneaux finis, puis les codes linéaires optimaux avec de nouveaux paramètres sont construits par application de Gray sur des anneaux finis.

Contents

List of Tables

Chapter 1

Introduction

1.1 Motivation

With the rapid development of communication and computer technology, the Internet has been integrated into people's lives. The Internet has greatly facilitated people's information interaction. It has also promoted the rapid development of the economy, culture, military, education, production and other fields. In addition, it also improves the quality of life of modern people and brings great convenience to people's life. Communication technology has also produced unprecedented development, and much important information is transmitted through the network. Since the Internet development is global, open, shared and dynamic, any user can easily access it, but some malicious users are not excluded. Therefore, information security has increasingly become one of the significant problems to be solved urgently. Because the information in the transmission process will encounter various interference, resulting in information transmission errors. The communication system still lacks sufficient error-correcting capability; it is necessary to perform an error-correcting and encoding of the information. Ensuring the reliability of the information in the communication channels has also become one of the major issues that researchers pay attention to. Algebraic coding theory plays an essential role in ensuring the security and reliability of the information in communication channels, more and more researchers have devoted themselves to studying algebraic coding theory.

In 1948, Shannon firstly proposed the very famous coding theory in his landmark paper "A Mathematical Theory of Communication". This paper signified the beginning of both information theory and coding theory. Since then, algebraic coding theory has been extensively studied, including the study of codebooks, the study of linear codes, etc.

Character sums over finite fields or rings play a crucial role in algebraic coding theory, especially special character sums over finite fields or are more widely used, for example, Gaussian sums, Jacobi sums, Eisenstein sums and Kloosterman sums. In CDMA communication systems, character sums can be used to construct codebooks and sequences with better correlation properties; in coding theory, character sums can be used to construct special linear codes, such as LCD codes, BCH codes, linear codes with a one-dimensional hull, minimal linear codes, projective codes, etc.; in combinatorial mathematics, character sums can be used to construct some difference sets; in quantum communication systems, character sums can be used to design quantum (MD-

S) codes with better parameters; in cryptography theory, character sums can be used to construct some Boolean functions with some special cryptographic properties, such as bent functions and semi-bent functions, etc. Therefore, character sums over finite fields or finite rings are an important research tool in coding theory.

A codebook is a signal set; as a signal form, it has good correlation properties and can be used as a signal for radar ranging, synchronization and linear system measurement. In signal transmission, the signal sequence will be interfered with by itself and other related signals to some extent. The signal strength is weakened, which will bring many difficulties and problems to the actual communication. In particular, MWBE codebooks have been used in a wide range of applications, such as multiple description coding over erasure channels, communications, compressed sensing, space-time codes, coding theory, quantum computing, etc. A codebook is called a maximum-Welch-bound-equality (MWBE) codebook if it meets a certain bound, i.e., Welch bound, or Levenshtein bound, which is also called optimal codebooks. This class of codebooks is used to distinguish among the signals of different users in code-division multiple-access (CDMA) systems. Therefore, it is very meaningful to construct the optimal codebook. It is challenging to build optimal codebooks to achieve the Welch or Levenshtein bound. Hence, many scholars have tried to construct asymptotically optimal codebooks; namely, the maximum magnitude nearly achieves the Welch bound or Levenshtein bound.

As a special class of error-correcting codes, linear codes have a special algebraic structure that makes them easier to describe, encode and decode than other types of codes. Therefore, many researchers have been widely concerned with linear codes. Most error-correcting codes with good performance are linear codes. For example, the most studied linear codes are Hamming codes, BCH codes, Reed-Solomon codes, Golay codes, Reed-Muller codes, Goppa codes, MDS codes, etc. The main research contents include the minimum Hamming distance of linear codes, the Hamming weight distribution, etc. The minimum Hamming distance of a linear code is a measure of the error-correcting capability of this code. At the same time, the Hamming weight distribution of linear codes gives important information of both practical and theoretical significance. In particular, linear codes with few nonzero weights have been extensively studied because of their wide practical applications in communication, secret sharing schemes, secure two-party computation, association schemes, authentication codes and strongly regular graphs. Therefore, constructing a few weight linear codes with new parameters has become a hot research topic in algebraic coding theory. Many researchers construct optimal linear codes by defining sets with respect to some special cryptographic functions, such as bent functions, quadratic functions, weakly regular bent functions, plateaued functions, APN or PN functions, two-to-one functions, etc.

In recent years, many researchers have aroused great interest in linear codes with low-dimensional hulls, mainly because of the excellent performance of linear codes with low-dimensional hulls. The hull of a linear code over finite fields is the intersection of the code and its dual, which can be regarded as a generalization of self-dual codes, self-orthogonal codes and LCD codes. It is clear that the hull of linear codes is also linear. Note that the hulls of linear codes play a vital role in determining the complexity of algorithms for checking the permutation equivalence of two linear codes. The hull is an indicator of the complexity of algorithms for computing the automorphism group of linear code. These algorithms are very effective in general if the size of the hull

is small. Hence, linear codes with a low-dimensional hull over finite fields play an important role in algebraic coding theory. A linear code with the smallest hull is an LCD code, which can be used in a direct-sum-masking technique for the prevention of side-channel attacks. A linear code with the second smallest hull is a linear code with a one-dimensional hull, which can improve the efficiency of the permutation equivalence algorithm of two linear codes. In general, these algorithms are more efficient when the hull dimension of a linear code is smaller. Therefore, the construction of linear codes with a low-dimensional hull is fascinating and has beneficial practical applications in algebraic coding.

1.2 Background

Coding theory originated with the 1948 publication of the paper "A mathematical theory of communication" by Claude Shannon. After more than 70 years of development, algebraic coding theory has grown into a discipline intersecting mathematics and engineering with applications to almost every area of communication, such as information transmission and data storage. The research topics of this thesis mainly include codebooks, linear codes with a one-dimensional hull, minimal linear codes and projective codes, etc. The following is a detailed introduction of the research contents in these aspects.

1.2.1 The introduction of codebooks

Let $C = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}\}$ be a set of N unit-norm complex vectors $\mathbf{c}_l \in \mathbb{C}^K$ over an alphabet A, where $l = 0, 1, \ldots, N-1$. The size of A is called the alphabet size of C. Such a set C is called an (N, K) codebook (also called a signal set), where N is the number of elements of the codebook C and K is the length of the codebook C. The maximum cross-correlation amplitude, which is a performance measure of a codebook in practical applications, of the (N, K) codebook C is defined as

$$I_{\max}(C) = \max_{0 \le i < j \le N-1} |\mathbf{c}_i \mathbf{c}_j^H|,$$

where $\mathbf{c}_j^H$ denotes the conjugate transpose of the complex vector $\mathbf{c}_j$. For a certain length K, it is desirable to design a codebook such that the number N of codewords is as large as possible and the maximum cross-correlation amplitude $I_{\max}(C)$ is as small as possible. To evaluate a codebook C with parameters (N, K), it is important to find the minimum achievable $I_{\max}(C)$.

A codebook is a class of signal sets with low correlation, which has important applications in code-division multiple-access (CDMA) communication systems, quantum coding theory and compressed sensing. Hence, it is one of the important research topics in algebraic coding theory to construct the optimal codebook in which the parameters of the codebook reach a specific bound. The Welch bound [118], a well-known lower bound on $I_{\max}(C)$, is given as follows.

Lemma 1.2.1 *[118] For any (N,K) codebook C with $N \geq K$,*

$$I_{\max}(C) \;\geq\; I_W = \sqrt{\frac{N-K}{(N-1)K}}. \tag{1.1}$$

Furthermore, the equality in (1.1) is achieved if and only if

$$|\boldsymbol{c}_i \boldsymbol{c}_j^H| \;=\; \sqrt{\frac{N-K}{(N-1)K}} \tag{1.2}$$

for all pairs (i,j) with $i \neq j$.

Particularly, the codebook C is referred to as a maximum-Welch-bound-equality (MWBE) codebook [92] or an equiangular tight frame [61] if it meets the Welch bound equality in (1.2). As early as 1999, Sarwate [92] gave a comprehensive introduction to codebooks and pointed out that the construction of an MWBE codebook in an analytic way is known to be extremely difficult in general. In addition, Sarwate [92] successfully constructed a class of codebooks with parameters $(N,N-1)$ which meets the Welch bound by using m-sequence and discrete fourier transform. In 2005, Xia et al. [122] firstly constructed five families of optimal codebooks by utilizing Singer difference sets, quadratic difference sets, Octic difference sets and twin-primes difference sets. Because difference sets have a good structure in combinatorial design, it is helpful to construct optimal codebooks. In [27, 32], Ding and Feng further used (almost) difference sets to construct some optimal codebooks whose parameters reach the Welch bound. Based on Xia et al. [122] using cyclic difference sets to construct several classes of optimal codebooks, Ding proposed a new construction method of optimal codebooks in [27]. He not only obtained new optimal codebooks by using cyclic difference sets, but also obtained several families of optimal codebooks with new parameters reaching the Welch bound by utilizing acyclic difference sets.

In 2003, Strohmer and Heath [111] have pointed out that the Welch bound cannot be achieved when N is large compared with K. Specifically, there are no (N,K) real-valued codebook C can meeting the Welch bound if $N > \frac{K(K+1)}{2}$ and no (N,K) complex-valued codebook C can achieving the Welch bound if $N > K^2$. When N is large, the following Levenshtein bounds are better than the Welch bound.

Lemma 1.2.2 *[60, 65] For any real-valued codebook C with $N > \frac{K(K+1)}{2}$, we have*

$$I_{\max}(C) \;\geq\; I_L = \sqrt{\frac{3N-K^2-2K}{(K+2)(N-K)}}. \tag{1.3}$$

For any complex-valued codebook C with $N > K^2$, we have

$$I_{\max}(C) \;\geq\; I_L = \sqrt{\frac{2N-K^2-K}{(K+1)(N-K)}}. \tag{1.4}$$

Suppose the maximum cross-correlation amplitude of a codebook satisfies the Levenshtein bound. In that case, the codebook is said to be optimal. In [8, 119] and [131], the

authors obtained two classes of optimal real-valued codebooks $(2^{2m-1}+2^m, 2^m)$ with respect to the Levenstein bound, generated from Kerdock codes and bent functions, respectively. Moreover, Ding et al. [35], and Wootters et al. [119] constructed optimal codebooks with parameters (q^2+q, q) regarding the Levenshtein bound, which are derived from planar functions. Inspired by the work of [131], Heng and Yue [51] introduced a new construction of codebooks from generalized Boolean bent functions over $\mathbb{Z}_4$. In [123], Xiang et al. extended a few previous constructions. The proposed new constructions of codebooks meet the Levenshtein bound from binary codes.

It is challenging to construct codebooks to achieve the Welch bound or Levenshtein bound. Hence, many researchers began to construct asymptotically optimal codebooks; that is, the maximum cross-correlation amplitude of codebooks asymptotically reaches the Welch bound, or Levenshtein bound. In [27, 32], Ding and Feng constructed several families of asymptotically optimal codebooks with respect to the Welch bound by using almost difference sets. Since then, the method of constructing asymptotically optimal codebooks using almost difference sets has attracted the attention of many researchers. Zhang and Feng [129, 130] generalized the construction in [27, 32] and used almost difference sets to construct several families of new codebooks asymptotically reaching the Welch bound. In [133], Zhou and Tang designed several classes of asymptotically optimal codebooks with respect to the Welch bound by using the relative difference sets. Later, Li et al. [69] constructed a new class of almost difference sets using skew Hadamard difference sets and then utilized the constructed almost difference set to obtain a family of asymptotically optimal codebooks with new parameters. Furthermore, they presented a general construction of complex codebooks from partial differences sets. Several classes of nearly optimal codebooks with new parameters were obtained from the general construction. In [53], using difference sets and the product of abelian groups, Hu et al. proposed new constructions of codebooks nearly meeting the Welch bound with equality. Many researchers began to use binary sequences to construct codebooks in recent years because binary sequences have good cryptographic properties. In [125], Yu et al. studied the relationship between binary sequences and Φ-transform and then obtained that constructing a codebook with a small magnitude of inner products is equivalent to finding a binary sequence where the maximum magnitude of its Φ-transform is as small as possible. From the discovery, Yu et al. constructed several new classes of asymptotically optimal codebooks from binary Sidelnikov sequences [62, 104], binary Golay complementary sequences [43], multiplied binary m-sequences [47], and multiplied bent functions [47, 107]. In addition, Yu et al. also obtained a class of asymptotically optimal codebooks with the parameter $(N = K^2-1, K = 2^k)$ by using a partial Fourier matrix constructed from binary m-sequences. Based on binary row selection sequences, which are generated by quadratic residue mapping of p-ary m-sequences, Hong et al. [52] proposed new construction of codebooks from Hadamard matrices and then obtained a new class of near-optimal partial Hadamard codebooks. In 2017, Cao et al. [10] generalized the construction in [125] and used the general binary sequences to construct several families of asymptotically optimal codebooks having new parameters with respect to the Welch bound.

It is well-known that the character sums over finite fields or finite rings are a very useful mathematical tool in coding theory and have extremely wide applications. In recent years, character sums over finite fields or finite rings have played an important role

in calculating the maximum cross-correlation amplitude of codebooks. In 2012, Zhang and Feng [129] used the Jacobi sums over finite fields to construct a class of codebooks asymptotically reaching the Welch bound and solve the open problem proposed by Ding and Feng in [32]. Based on additive characters and multiplicative characters of finite fields, Tan and Zhou [112] proposed several classes of asymptotically optimal codebooks with respect to the Levenstein bound. In [49], Heng presented two new construction methods of codebooks by using multiplicative characters of finite fields and then obtained two families of asymptotically optimal codebooks with new parameters, asymptotically meeting the Welch and Levenstein bound, respectively. In 2018, Heng [48] also used the generalized Jacobi sum over finite fields to construct two classes of asymptotically optimal codebooks, which are asymptotically the Welch bound and Levenstein bound, respectively. Later, Luo and Cao firstly defined the hyper Eisenstein sum over finite fields in [81] and studied its properties. Then, they constructed two classes of asymptotically optimal codebooks concerning the Welch bound by the hyper Eisenstein sum. In addition, they also used the Gaussian sum and the Eisenstein sum over Galois rings to construct two classes of asymptotically optimal codebooks in [80].

1.2.2 The introduction of linear codes

Linear codes over finite fields have been studied extensively because of their linear structures and practical implementations. It is the basis of the research of various kinds of codes. Linear codes with few weights have diverse applications in communication [54], secret sharing schemes (see e.g., [23, 38, 89, 95, 99, 101, 127] and the references therein), secure two-party computation [21], association schemes [13], authentication codes [34], strongly regular graphs [7].

In recent years, the construction of new linear codes with few weights has been a fascinating research topic in error-correcting code theory. It is well-known that functions and linear codes are closely connected. Cryptographic functions have been used to construct linear codes for a long time ago. For instance, these two famous families of binary codes (namely, Reed-Muller codes and Kerdock codes) were obtained by Boolean functions from $\mathbb{F}_{2^m}$ (m is a positive integer) to $\mathbb{F}_2$. In the past two decades, the design of linear codes derived from (vectorial) Boolean functions has been a research topic of increasing importance. Designing linear codes from (cryptographic) functions has received much attention and success in the literature indisputably thanks to leading techniques and the novel ideas introduced, mainly by Ding, many years ago. It is still a hot and very attractive topic nowadays. A recent (2020) survey on results and problems devoted to constructions of linear codes from cryptographic functions is [75]. Also, a lengthy chapter on general linear codes from functions over finite fields published in the very recent (2021) book "A Concise Encyclopedia of Coding Theory" is [86]. For complete knowledge of (vectorial) Boolean functions in particular oriented coding theory, we refer to the excellent, very recent (2021) book [11] of Carlet on Boolean functions for cryptography and coding theory. Generally speaking, there are essentially two generic constructions of linear codes from (vectorial) Boolean functions (see, e.g., [86] and the references therein). The others are their generalizations and variations using various algebraic techniques. Let p be a prime and $q = p^m$ (m is a positive integer).

The first generic construction of linear codes is given by

$$\mathcal{C}_F = \{\boldsymbol{c}_{a,b} = (\mathrm{Tr}_m(ax + bF(x)))_{x\in\mathbb{F}_q} : a,b \in \mathbb{F}_q\}. \tag{1.5}$$

where $q = p^n, \mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ and Tr_m denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and F is a function (where $F(0) = 0$) from $\mathbb{F}_q$ to itself. It is clear that the resulting code $\mathcal{C}_F$ from F is a linear code over $\mathbb{F}_p$ of length q, and its dimension is upper bounded by $2m$. However, the research problems regarding this construction are how to select F such that $\mathcal{C}_F$ has suitable parameters and how to determine the weight distribution of this code. As proved by Mesnager in [85], the Hamming weight of a codeword of the code $\mathcal{C}_F$ can be directly expressed through the Walsh transform of some absolute trace functions over $\mathbb{F}_q$ involving the function F. The Walsh transform of the function F is generally difficult to settle. Subsequently, many researchers usually choose an appropriate function (or a special function) for which it is not too difficult to determine the weight distribution of $\mathcal{C}_F$, notably, (weakly regular) bent functions [85], weakly regular plateaued functions [87], quadratic functions [116], (almost) perfect nonlinear (APN or PN) functions [67, 115, 124], characteristic functions [88], almost bent (AB) functions [115, 116], two-to-one (shortly, 2-to-1) functions [72] and so on.

The second generic construction of linear codes (usually called the defining set construction) consists of considering codes by appropriately employing trace functions. Ding and Niederreiter first introduced it in [33]. Specifically, this construction is obtained firstly by fixing a set D over $\mathbb{F}_q^*$; precisely $D = \{d_1, d_2, \ldots, d_l\} \subset \mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ (where $q = p^m$). And next, by defining a linear code involving D over $\mathbb{F}_p$ as

$$\mathcal{C}_D = \{(\mathrm{Tr}_m(xd_1), \mathrm{Tr}_m(xd_2), \ldots, \mathrm{Tr}_m(xd_n)) : x \in \mathbb{F}_q\}, \tag{1.6}$$

where Tr_m denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. The set D is called the *defining set* of the code $\mathcal{C}_D$. Since the trace function is linear, the code $\mathcal{C}_D$ is linear. The resulting code $\mathcal{C}_D$ over $\mathbb{F}_p$ has length l and dimension at most m. It is easy to see that this approach can construct every p-ary linear code. This trace construction is equivalent to the generator matrix (where the generator matrix is made of distinct columns) construction, as every linear function from $\mathbb{F}_q$ to $\mathbb{F}_p$ must be of the form $\mathrm{Tr}_m(xd)$ (where x ranges over $\mathbb{F}_q$). However, the research problems regarding this construction are how to select $D \subset \mathbb{F}_q^*$ such that the code $\mathcal{C}_D$ has good parameters and how to determine the weight distribution of this code. Using the defining set construction, many linear codes over $\mathbb{F}_p$ with good parameters can be obtained by choosing the defining set D suitably (see e.g., [37, 38, 50, 72, 83, 89, 91, 105, 113, 114, 132]). Based on the second construction, Ding [30] set up a connection between the weight distributions of projective binary linear codes and the Walsh spectra of Boolean functions. A lot of progress has been made in this topic by selecting different defining sets with 2-designs [28], Boolean functions [29, 50, 72, 83] and p-ary functions [89, 105, 113, 114, 132], and then many linear codes over $\mathbb{F}_p$ with few weights could be produced.

Later, many researchers generalized the construction methods of (1.5) and (1.6) more generally, and obtained many linear codes with better parameters. In [68], Li et al. generalized the first construction method in (1.5), and defined the p-ary linear code by

$$\mathcal{C}_D \quad = \quad \{\boldsymbol{c}_{a,b} = (\mathrm{Tr}_m(ax + by))_{(x,y)\in D} : a,b \in \mathbb{F}_q\}, \tag{1.7}$$

where $D = \{(x,y) \in \mathbb{F}_q^2 \backslash \{(0,0)\} : \mathrm{Tr}_m(x^{N_1} + y^{N_2}) = 0\}$ (N_1, N_2 are positive integers). If $N_1, N_2 \in \{1, 2, p^{\frac{m}{2}} + 1\}$, then they obtained several classes of 2-weight and 3-weight p-ary linear codes in (1.7) and completely determined their weight distributions. In 2019, based on the construction method in [68], Jian et al. [56] defined the defining set $D_1 = \{(x,y) \in \mathbb{F}_q^2 \backslash \{(0,0)\} : \mathrm{Tr}_m(x + y^{p^u+1}) = 0\}$ and $D_2 = \{(x,y) \in \mathbb{F}_q^2 \backslash \{(0,0)\} : \mathrm{Tr}_m(x^2 + y^{p^u+1}) = 0\}$ (u is a positive integer) to construct several classes of 2-weight and 3-weight linear codes and some of them are optimal or almost optimal with respect to the Griesmer bound. In [121], Wu et al., inspired by [56, 68], selected two different defining sets, as follows: The first defining set is defined as $D = \{(x,y) \in \mathbb{F}_q^2 : x \in C_i, y \in C_j\}$, where C_i, C_j are any two cyclotomic classes of order e and e is a positive integer. By using the semiprimitive case of cyclotomic classes of order e, they showed that $\mathcal{C}_D$ is a five-weight linear code and determined its weight distribution according to Gaussian sums over finite fields; The second defining set is defined as $D = \{(x,y) \in \mathbb{F}_q^2 \backslash \{(0,0)\} : f(x) + g(x) = 0\}$, and the following two cases are considered to construct linear codes: (1) $f(x) = \mathrm{Tr}_m(x), g(x)$ is a weakly regular bent function; (2) $f(x), g(x)$ are weakly regular bent functions. By calculating Weil sums and using the properties of weakly regular bent functions, a class of three-weight linear codes can be obtained from the first case, and the second case will lead to both two-weight and three-weight linear codes. In 2021, motivated by the work in [56, 68, 121], Zheng et al. [117] constructed several classes of binary linear codes with few weights by choosing the following two defining sets $D = \{(x,y) \in \mathbb{F}_{2^m}^2 \backslash \{(0,0)\} : f(x) + g(x) = 0, \mathrm{Tr}_m(x+y) = \varepsilon\}$ and $D = \{(x,y) \in \mathbb{F}_{2^m}^2 \backslash \{(0,0)\} : f(x) + g(x) = 0, \mathrm{Tr}_m(x) = 0, \mathrm{Tr}_m(y) = \varepsilon\}$, where $\varepsilon \in \{0,1\}$, $f(x), g(x)$ are Boolean functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ with at most three Walsh transform values satisfying some additional conditions. Zhang et al. [116] generalized the second construction method in (1.5) and defined the linear code $\mathcal{C}(F)_D$ by

$$\mathcal{C}(F)_D \quad = \quad \{\boldsymbol{c}_{a,b} = (\mathrm{Tr}_m(ax + bF(x)))_{x \in D} : a, b \in \mathbb{F}_{2^m}\}, \tag{1.8}$$

where $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}_m(\lambda F(x)) = v\}$ or $D = \{x \in \mathbb{F}_{2^m}^* : \mathrm{Tr}_m(x) = 1\}$, $v \in \{0,1\}, \lambda \in \mathbb{F}_{2^m}^*$, $F(x)$ is an almost bent function from $\mathbb{F}_{2^m}$ to itself. Based on this construction, they obtained several families of binary linear codes with few weights, and their duals are distance-optimal with respect to the sphere packing bound.

Based on the construction method of trace codes over finite fields, many researchers extended the construction method in (1.6) from finite fields to finite rings. They obtained some linear codes with optimal parameters. In particular, Shi et al. have done a lot of research on trace codes over finite rings [78, 95–102]. By considering different defining sets and using the Gray map over finite rings, they determined the weight distribution of linear codes over finite rings using character sums and discussed their practical applications in secret sharing schemes.

1.2.3 The introduction of linear codes with low-dimensional hull

Let $\mathcal{C}$ be an $[n,k,d]$ linear code of length n over $\mathbb{F}_q$ and its dual code be denoted by $\mathcal{C}^\perp$. The *hull* of a linear code $\mathcal{C}$ over a finite field is defined to be

$$\mathrm{Hull}(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^\perp.$$

It is clear that Hull($\mathcal{C}$) is also linear. The definition of Hull($\mathcal{C}$) was introduced in 1990 by Assmus and Key [59] to classify finite projective planes. Suppose that the dimension of Hull($\mathcal{C}$) is ℓ. If $\ell = 0$, i.e., Hull($\mathcal{C}$) $= \{\mathbf{0}\}$, then the linear code $\mathcal{C}$ is termed as a linear complementary dual (LCD) code. If $\ell = k$, i.e., Hull($\mathcal{C}$) $= \mathcal{C}$, then the linear code $\mathcal{C}$ is said to be a self-orthogonal code. In addition, if $\ell = \frac{n}{2}$ for even n, then $\mathcal{C}$ is called a self-dual code.

It is well-known that the hulls of linear codes play a vital role in determining the complexity of algorithms for checking permutation equivalence of two linear codes in [64, 93]. Subsequently, it has been shown that the hull is an indicator for the complexity of algorithms for computing the automorphism group of a linear code in [63, 94]. Precisely, most of the algorithms do not work if the size of the hull is large. However, conversely, these algorithms are very effective in general if the size of the hull is small. Consequently, the study of linear codes with a small hull is useful and interesting for these computations. Hence, the construction of linear codes with low-dimensional hulls has aroused the interest of many researchers due to their wide applications. At present, a lot of research has been done on the construction of two types of linear codes with low-dimensional hulls: one is an LCD code, and the other is a linear code with a one-dimensional hull.

The linear codes with the smallest hull are LCD codes, which are widely studied. In 1992, Massey [84] first introduced LCD codes and showed the existence of asymptotically good LCD codes. In addition, a complete characterization of LCD codes via the nonsingularity of their generator matrices was employed in [13, 85], which provides a sufficient and necessary condition for a linear code to be an LCD code.

Lemma 1.2.3 *[13, 85] Let $\mathcal{C}$ be an $[n,k]$ linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k, P]$. Then the code $\mathcal{C}$ is LCD if and only if $I_k + PP^T$ is nonsingular, i.e., -1 is not an eigenvalue of the matrix PP^T, where P^T denotes the transpose of P.*

Inspired by the condition described in Lemma 1.2.3, Carlet et al. [16] constructed LCD codes by employing character sums in semi-primitive case from cyclotomic fields and multiplicative subgroups of finite fields. In 2014, Bringer et al. [4] and Carlet et al. [13] investigated an exciting application of binary LCD codes against side-channel attacks (SCA) and fault injection attacks (FIA) and presented several constructions of LCD codes. The study of LCD codes is thus becoming an interesting research topic. There is a lot of research work on the constructions of LCD codes. Mesnager et al. [90] gave a construction of algebraic geometry LCD codes, which could be good candidates to be resistant against SCA. In [18], Carlet et al. first presented a new characterization of binary LCD codes in terms of their orthogonal or symplectic basis and solved a conjecture proposed by Galvez et al. [42] on the minimum distance of binary LCD codes. It is worth noting that the equivalence of LCD codes has been extensively studied. Carlet et al. [17] showed that any MDS code is equivalent to an LCD code. Jin and Xing [58] proved that an algebraic geometry code over $\mathbb{F}_{2^m}$ $(m \geq 7)$ is equivalent to an LCD code. Whereafter, an outstanding result was presented in [20], which showed that any linear code over $\mathbb{F}_q$ $(q > 3)$ is equivalent to an LCD code. For more research on LCD codes, the reader is referred to [14, 15, 19, 22, 39, 40, 46, 57, 66, 76, 103, 126] for further understanding these codes.

We also have the following lemma on a linear code having one-dimensional hull, which provides an idea to construct linear codes with one-dimensional hull by using

the eigenvalues of the generator matrices.

Lemma 1.2.4 *[70] Let $\mathcal{C}$ be an $[n,k]$ linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k, P]$. Then the code $\mathcal{C}$ has one-dimensional hull if the matrix PP^T has an eigenvalue -1 with (algebraic) multiplicity* 1.

Inspired by the condition described in Lemma 1.2.4, Li et al. [70] constructed linear codes with one-dimensional hull by utilizing quadratic Gaussian sums from quadratic number fields and obtained that some of them are optimal. Later, Carlet et al. [16] employed the Gaussian sums in semi-primitive case and multiplicative subgroups of finite fields to construct some linear codes with one-dimensional hull from cyclotomic fields. Note that the value of the special Gaussian sum is known, which is helpful for studying linear codes with low-dimensional hull. Recently, many researchers are not limited to constructing linear codes low-dimensional hull by using special Gaussian sums. In 2020, Sok also provided two construction methods of linear codes with the one-dimensional hull in [108, 109]. The first method is to construct these codes by using algebraic geometry codes of genus-zero in [108]. The second method is to deduce these codes by using algebraic curves over finite fields with even characteristic, including elliptic curves, hyper-elliptic curves and Hermitian curves in [109]. In 2022, Sok [110] provided a new method to construct linear codes having a one-dimensional hull from self-orthogonal codes and then gave an application to EAQECCs. This new method improves the parameters of the codes given in the recent results of [108, 109]. Because the generalized Reed-Solomon codes are closely related to the hull of MDS codes [41, 82], Wu [120] constructed linear codes with a one-dimensional hull by using Reed-Solomon codes and showed that these codes are not monomial equivalent to Reed-Solomon codes. In 2022, motivated by the work in [120], Singh et al. [106] used multi-twisted Reed-Solomon codes to construct linear codes with a one-dimensional hull and presented some necessary conditions for the existence of multi-twisted Reed-Solomon codes with a one-dimensional hull.

1.3 Organization of the thesis

This thesis further studies the algebraic coding theory over finite fields and finite rings and gives some significant results. Mainly using the character sums over finite fields and finite rings as research tools, this thesis constructs optimal or asymptotically optimal codebooks, linear codes with one-dimensional hull and optimal few-weight linear codes with new parameters. We briefly describe the contents of this thesis as follows:

Chapter 1 introduces the development history, research motivation, research background, research contents of algebraic coding theory.

Chapter 2 provides some basic notation, definitions and results about character theory, linear codes, algebraic number theory and Boolean functions.

Chapter 3 constructs optimal and asymptotically optimal codebooks by studying the Gaussian sum, Jacobi sum and Eisenstein sum over finite chain ring $\mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ and finite non-chain ring $\mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$. These codebooks meet or asymptotically meet the Welch bound, and Levenstein bound. Some of the constructed codebooks have new parameters.

Chapter 4 investigates the construction method of linear codes with a one-dimensional hull and further generalizes the construction method in [16, 70]. Firstly, the linear codes with a one-dimensional hull of [16, 70] constructed by using certain Gaussian sums are generalized to produce such linear codes by using general Gaussian sums over finite fields. Secondly, some properties similar to Gaussian sums are obtained by defining two homomorphic mappings from a finite field to another finite field. In addition, sufficient conditions are given for a linear code over finite fields to be a linear code with a one-dimension hull. Several classes of linear codes with one-dimensional hulls having new parameters are constructed. Finally, a lower bound on the minimum distances of the created linear codes is presented.

Chapter 5 constructs minimal binary linear codes with few nonzero weights by using the known 2-to-1 functions over $\mathbb{F}_{2^n}$. Inspired by the work in [72], several families of linear codes with few weights are constructed from two general constructions and a new construction involving 2-to-1 functions, and these codes have new parameters. Some of the constructed codes are minimal and the access structures of the secret sharing schemes based on their dual codes are described. Particularly, two open problems left in [72] are solved.

Chapter 6 constructs several projective binary linear codes families and determines their weight distribution. Some of the proposed linear codes are optimal or almost optimal, and several classes of self-complementary codes are obtained. The minimum distance of the dual of the constructed codes is discussed, and their duals are distance-optimal for the sphere packing bound. As applications, some of the obtained codes can be used to construct association schemes and secret sharing schemes with interesting access structures.

Chapter 7 summarizes the findings and suggests directions for future research.

Chapter 2

Preliminaries

This chapter mainly introduces some basic concepts and results on characters over finite fields, linear codes over finite fields, algebraic number theory, Boolean functions, etc. This will be useful for our subsequent discussion. For more details, please refer to [1, 3, 6, 16, 24, 36, 48, 55, 59, 72–74, 77, 81, 128].

2.1 Character theory over finite fields

Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer. Let $m \mid n$ and m be a positive integer. The trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is defined as:

$$\mathrm{Tr}_{p^n/p^m}(x) := \sum_{i=0}^{\frac{n}{m}-1} x^{p^{im}} = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(\frac{n}{m}-1)m}}, x \in \mathbb{F}_q.$$

Particularly, if $m = 1$, then the trace function $\mathrm{Tr}_{q/p}(\cdot)$ is called the *absolute trace function*.

The following lemma gives some basic properties of the trace function.

Lemma 2.1.1 *[77, Theorem 2.23] Let $K = \mathbb{F}_{p^m}$ and $F = \mathbb{F}_{p^n}$, where m, n are positive integers and $m \mid n$. Let $\alpha, \beta \in F$ and $c \in K$. Then the trace function $\mathrm{Tr}_{F/K}(\cdot)$ satisfies the following properties:*

(1) $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$;

(2) $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$;

(3) $\mathrm{Tr}_{F/K}(\alpha^{p^m}) = \mathrm{Tr}_{F/K}(\alpha)$;

(4) Let $E = \mathbb{F}_{p^k}$. If $m \mid k$ and $k \mid n$, then $\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{F/E}(\alpha))$.

Next, we will recall the definitions of the additive and multiplicative characters of $\mathbb{F}_q$.

Definition 2.1.2 *[77] Let $q = p^n$, where p is a prime number and n is a positive integer. For each $a \in \mathbb{F}_q$, the* additive character χ_a *of $\mathbb{F}_q$ is defined by*

$$\chi_a : \mathbb{F}_q \longrightarrow \mathbb{C}^*, \chi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)}, x \in \mathbb{F}_q,$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$*, which is a primitive p-th root of unity.*

If $a = 0$, then $\chi_0(x)$ is called the *trivial additive character* of $\mathbb{F}_q$ and $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$; If $a = 1$, then $\chi_1(x) = \chi(x)$ is called the *canonical additive character* of $\mathbb{F}_q$; all other additive characters of $\mathbb{F}_q$ are called *nontrivial*. Moreover, the group that consists of all additive characters of $\mathbb{F}_q$ is denoted by $\widehat{\mathbb{F}}_q := \{\chi_a : a \in \mathbb{F}_q\}$. The group of characters is isomorphic to $(\mathbb{F}_q, +)$. With each additive character $\chi_a(x)$ of $\mathbb{F}_q$, there is an associated conjugate character $\overline{\chi_a}(x)$ defined by $\overline{\chi_a}(x) = \overline{\chi_a(x)} = \chi_a(-x)$ for all $x \in \mathbb{F}_q$. In addition, $\chi_a(0) = 1$ for all $a \in \mathbb{F}_q$.

The following lemma gives the orthogonality relations for the additive characters of $\mathbb{F}_q$.

Lemma 2.1.3 *[77] Let* χ_a *be the additive character of* $\mathbb{F}_q$*, where* $a \in \mathbb{F}_q$*. Then*

(1)

$$\sum_{x\in\mathbb{F}_q} \chi_a(x) = \begin{cases} q, & \text{if } a = 0; \\ 0, & \text{if } a \in \mathbb{F}_q^*. \end{cases}$$

(2)

$$\sum_{a\in\mathbb{F}_q} \chi_a(x) = \begin{cases} q, & \text{if } x = 0; \\ 0, & \text{if } x \in \mathbb{F}_q^*. \end{cases}$$

Definition 2.1.4 *[77] For any* $j = 0, 1, \ldots, q-2$*, the* multiplicative character ψ_j *of* $\mathbb{F}_q$ *is defined by*

$$\psi_j : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*, \psi_j(g^k) = \zeta_{q-1}^{jk}, k = 0, 1, \ldots, q-2,$$

where $\zeta_{q-1} = e^{\frac{2\pi\sqrt{-1}}{q-1}}$*, which is a primitive* $(q-1)$*-th root of unity, and g is a fixed primitive element of* $\mathbb{F}_q$*.*

If $j = 0$, then ψ_0 is called the *trivial multiplicative character* of $\mathbb{F}_q$; If $j = 1$, then ψ_1 is called the *canonical multiplicative character* of $\mathbb{F}_q$; If q is odd and $j = \frac{q-1}{2}$, then $\psi_{\frac{q-1}{2}}$ is called the *quadratic character* of $\mathbb{F}_q$, denoted by η, that is,

$$\eta(g^k) = \begin{cases} 1, & \text{if } g^k \text{ is the square of an elements of } \mathbb{F}_q^*; \\ -1, & \text{otherwise.} \end{cases}$$

Moreover, the group that consists of all multiplicative characters of $\mathbb{F}_q$ is denoted by $\widehat{\mathbb{F}}_q^* = \{\psi_j : j = 0, 1, \ldots, q-2\}$. The group of characters is isomorphic to $(\mathbb{F}_q^*, \times)$. With each multiplicative character ψ of $\mathbb{F}_q$, there is an associated conjugate character $\overline{\psi}$ defined by $\overline{\psi}(x) = \overline{\psi(x)} = \psi^{-1}(x), x \in \mathbb{F}_q^*$. If ψ is trivial, then $\psi(0) = 1$; if ψ is nontrivial, then we define $\psi(0) = 0$.

The following lemma gives the orthogonality relations for the multiplicative characters of $\mathbb{F}_q$.

Lemma 2.1.5 *[77] Let* ψ_j *be the multiplicative character of* $\mathbb{F}_q$*, where* $j = 0, 1, \ldots, q-2$*. Then*

(1)

$$\sum_{x\in\mathbb{F}_q^*}\psi_j(x)=\begin{cases} q-1, & \text{if } j=0;\\ 0, & \text{if } j\neq 0.\end{cases}$$

(2)

$$\sum_{j=0}^{q-2}\psi_j(x)=\begin{cases} q-1, & \text{if } x=1;\\ 0, & \text{if } x\in\mathbb{F}_q^* \text{ and } x\neq 1.\end{cases}$$

Based on the addition character χ_a and the multiplicative character ψ of $\mathbb{F}_q$, we give the definition of the Gaussian sum over the finite field $\mathbb{F}_q$ as follows.

Definition 2.1.6 *[77] Let ψ be a multiplicative and χ_a an additive character of $\mathbb{F}_q$, where $a\in\mathbb{F}_q$. Then the* Gaussian sum $G(\psi,\chi_a)$ *over $\mathbb{F}_q$ is defined by*

$$G(\psi,\chi_a)=\sum_{x\in\mathbb{F}_q^*}\psi(x)\chi_a(x).$$

If $a=1$, we usually write $G(\psi,\chi_1)$ simply as $G(\psi)$. The absolute value of $G(\psi,\chi_a)$ is at most $q-1$, but is in general much smaller, as the following lemma shows.

Lemma 2.1.7 *[77, Theorem 5.11] Let ψ be a multiplicative and χ_a an additive character of $\mathbb{F}_q$. Then the Gaussian sum $G(\psi,\chi)$ satisfies*

$$G(\psi,\chi)=\begin{cases} q-1, & \text{if } \psi=\psi_0 \text{ and } \chi_a=\chi_0;\\ -1, & \text{if } \psi=\psi_0 \text{ and } \chi_a\neq\chi_0;\\ 0, & \text{if } \psi\neq\psi_0 \text{ and } \chi_a=\chi_0.\end{cases}$$

If $\psi\neq\psi_0$ and $\chi_a\neq\chi_0$, then $|G(\psi,\chi_a)|=q^{\frac{1}{2}}$.

Lemma 2.1.8 *[77, Theorem 5.12] Gaussian sums for the finite field $\mathbb{F}_q$ have the following properties:*

(1) $G(\psi,\chi_{ab})=\overline{\psi(a)}G(\psi,\chi_b)$ *for $a\in\mathbb{F}_q^*, b\in\mathbb{F}_q$;*

(2) $G(\psi,\overline{\chi}_a)=\psi(-1)G(\psi,\chi_a)$ *for $a\in\mathbb{F}_q$.*

The following lemma, which is introduced in [77], gives a basic result about character sums.

Lemma 2.1.9 *[77, Theorem 5.33] Let χ be a nontrivial additive character of $\mathbb{F}_q$ with q odd, and $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$ with $a_2\neq 0$. Then*

$$\sum_{c\in\mathbb{F}_q}\chi(f(c))=\chi(a_0-a_1^2(4a_2)^{-1})\eta(a_2)G(\eta,\chi),$$

where η is the quadratic character of $\mathbb{F}_q$.

Let $r = p^l$, $q = r^m$, where $l(\geq 1)$ and $m(\geq 1)$ is a positive integer. $\mathbb{F}_p, \mathbb{F}_r$ and $\mathbb{F}_q$ denote the finite field with p, r and q elements, respectively, and $\mathbb{F}_p \subseteq \mathbb{F}_r \subseteq \mathbb{F}_q$. Let $\psi_1, \psi_2, \ldots, \psi_n$ be multiplicative characters of $\mathbb{F}_q$. For $1 \leq i \leq n$, the restriction of ψ_i to $\mathbb{F}_r$ will be denoted by ψ_i^*. In particular, if ψ_i is a trivial character on $\mathbb{F}_q$, then ψ_i^* is a trivial character on $\mathbb{F}_r$. Now, we give the definition of hyper Eisenstein sums over the finite field $\mathbb{F}_q$ as follows.

Definition 2.1.10 *[81] The* hyper Eisenstein sum $E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1)$ *is defined by*

$$E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n) := E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1) = \sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q^*, \\ \mathrm{Tr}_{q/r}(x_1 + \cdots + x_n) = 1}} \psi_1(x_1) \cdots \psi_n(x_n),$$

where $\psi_1, \psi_2, \ldots, \psi_n$ are multiplicative characters of $\mathbb{F}_q$. If $n = 1$, then $E(\psi; 1) = \sum_{x \in \mathbb{F}_q^*, \mathrm{Tr}_{q/r}(x) = 1} \psi(x)$ is called the Eisenstein sum over $\mathbb{F}_q$. If $q = r$, then $\sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q^*, \\ x_1 + \cdots + x_n = 1}} \psi_1(x_1) \cdots \psi_n(x_n)$ is called the Jacobi sum over $\mathbb{F}_q$, we usually write it simply as $J_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1)$.

Moreover, we define

$$E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; s) = \sum_{\substack{x_1, \ldots, x_n \in \mathbb{F}_q^*, \\ \mathrm{Tr}_{q/r}(x_1 + \cdots + x_n) = s}} \psi_1(x_1) \cdots \psi_n(x_n)$$

for all $s \in \mathbb{F}_r$, which is called the generalized hyper Eisenstein sum over $\mathbb{F}_q$. If $n = 1$, then $E(\psi; s) = \sum_{x \in \mathbb{F}_q^*, \mathrm{Tr}_{q/r}(x) = s} \psi(x)$ is called the generalized Eisenstein sum over $\mathbb{F}_q$.

It is easy to see that

$$E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; s) = (\psi_1 \cdots \psi_n)(s) E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1) \tag{2.1}$$

for each $s \in \mathbb{F}_r^*$. If $\psi_1, \ldots, \psi_n$ are all trivial, then

$$E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1) = \frac{(q-1)^n + (-1)^{n+1}}{r} \tag{2.2}$$

by [81, Lemma 5]. If some, but not all, of the ψ_i are trivial, without loss of generality, we assume that $\psi_1, \ldots, \psi_h$ are nontrivial and $\psi_{h+1}, \ldots, \psi_n$ are trivial, where $1 \leq h \leq n-1$. Then (see [81, Theorem 1])

$$E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1) = (-1)^{n-h} E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_h; 1). \tag{2.3}$$

In the following, we describe a relationship between hyper Eisenstein sums and Gaussian sums over $\mathbb{F}_q$.

Lemma 2.1.11 *[81, Theorem 3] Let $\psi_1, \psi_2, \ldots, \psi_n$ be nontrivial multiplicative characters on $\mathbb{F}_q$. Let $(\psi_1 \cdots \psi_n)^*$ be the restriction of $\psi_1 \cdots \psi_n$ to $\mathbb{F}_r$. Then*

$$E_{\mathbb{F}_q}(\psi_1, \ldots, \psi_n; 1) = \begin{cases} \frac{G_{\mathbb{F}_q}(\psi_1) \cdots G_{\mathbb{F}_q}(\psi_n)}{G_{\mathbb{F}_r}((\psi_1 \cdots \psi_n)^*)}, & \text{if } (\psi_1 \cdots \psi_n)^* \text{ is nontrivial;} \\ -\frac{G_{\mathbb{F}_q}(\psi_1) \cdots G_{\mathbb{F}_q}(\psi_n)}{r}, & \text{if } (\psi_1 \cdots \psi_n)^* \text{ is trivial.} \end{cases}$$

From Lemma 2.1.11 and Eq. (2.1), we can determine the absolute value of the sum $E_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;s)$ for each $s\in\mathbb{F}_r^*$.

Lemma 2.1.12 *[81, Corollary 1] Let $\psi_1,\psi_2,\ldots,\psi_n$ be nontrivial multiplicative characters on $\mathbb{F}_q$. Let $(\psi_1\cdots\psi_n)^*$ be the restriction of $\psi_1\cdots\psi_n$ to $\mathbb{F}_r$. Then*

$$|E_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;s)| = \begin{cases} r^{\frac{mn-1}{2}}, & \text{if } (\psi_1\cdots\psi_n)^* \text{ is nontrivial;} \\ r^{\frac{mn-2}{2}}, & \text{if } (\psi_1\cdots\psi_n)^* \text{ is trivial,} \end{cases}$$

for each $s\in\mathbb{F}_r^*$.

The following result relates $E_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;0)$ to the hyper Eisenstein sum $E_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;1)$.

Lemma 2.1.13 *[81, Theorem 2] Let $\psi_1,\psi_2,\ldots,\psi_n$ be multiplicative characters on $\mathbb{F}_q$. Let $(\psi_1\cdots\psi_n)^*$ be the restriction of $\psi_1\cdots\psi_n$ to $\mathbb{F}_r$. Then $E_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;0)$*

$$= \begin{cases} \frac{(q-1)^n+(-1)^n(r-1)}{r}, & \text{if } \psi_1,\ldots,\psi_n \text{ are all trivial;} \\ 0, & \text{if } (\psi_1\cdots\psi_n)^* \text{ is nontrivial;} \\ -(r-1)E_{\mathbb{F}_q}(\psi_1,\ldots,\psi_n;1), & \text{if } \psi_1,\ldots,\psi_n \text{ are not all trivial and } (\psi_1\cdots\psi_n)^* \text{ is trivial.} \end{cases}$$

2.2 Linear codes

In this section, we mainly introduces the basic definitions and relevant results about linear codes.

Definition 2.2.1 *[54] Let $\mathbb{F}_q$ be the finite field of order q, and $\mathbb{F}_q^n$ denote the n-dimensional vector space over $\mathbb{F}_q$. Each nonempty subset $\mathcal{C}$ of $\mathbb{F}_q^n$ is called a q-ary code. An element of $\mathcal{C}$ is called a codeword in $\mathcal{C}$. The number of codewords in $\mathcal{C}$, denoted by $K=|\mathcal{C}|$, is called the size of $\mathcal{C}$, where $1\le K\le q^n$. A code of length n and size K is called an (n,K)-code. The (information) bits of a code $\mathcal{C}$ of length n is defined to be $k=\log_q K$. The (information) rate of a code $\mathcal{C}$ of length n is defined to be $\frac{k}{n}$. When the nonempty subset $\mathcal{C}$ is a vector subspace of $\mathbb{F}_q^n$, the code $\mathcal{C}$ is called a linear code with parameters $[n,k]$ over the finite field $\mathbb{F}_q$, where k is the dimension of the linear code $\mathcal{C}$ and $|\mathcal{C}|=q^k$.*

In the following, we give the basic definition of dual codes for linear codes over finite fields. Before that, we first recall the definition of the Euclidean inner product.

Definition 2.2.2 *[54, 59] Let $\mathbb{F}_q$ be the finite field of order q, and q be a power of a prime number. For any two vectors $\boldsymbol{x}=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q^n$ and $\boldsymbol{y}=(y_1,y_2,\ldots,y_n)\in\mathbb{F}_q^n$, their Euclidean inner product $\langle\boldsymbol{x},\boldsymbol{y}\rangle$ on $\mathbb{F}_q$ is defined by*

$$\langle\boldsymbol{x},\boldsymbol{y}\rangle=\sum_{i=1}^{n}x_iy_i.$$

If $\mathcal{C}$ is a linear code of length n over $\mathbb{F}_q$, then the dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined by

$$\mathcal{C}^\perp=\{\boldsymbol{x}\in\mathbb{F}_q^n:\langle\boldsymbol{x},\boldsymbol{y}\rangle=0,\forall\,\boldsymbol{y}\in\mathcal{C}\}.$$

For a linear code, its minimum distance measures the error-correcting capability of this code. Next, we give the basic concept of the minimum distance of a linear code. Before that, we first introduce the Hamming weight and the Hamming distance concepts.

Definition 2.2.3 *[54] Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ be two vectors in $\mathbb{F}_q^n$. The Hamming weight of the vector $\boldsymbol{x}$, denoted by $w_H(\boldsymbol{x})$, is defined to be the number of nonzero coordinates in $\boldsymbol{x}$, i.e.,*

$$w_H(\boldsymbol{x}) = |\{i : 1 \le i \le n, x_i \neq 0\}|.$$

The Hamming distance of the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$, denoted by $d_H(\boldsymbol{x}, \boldsymbol{y})$, is defined to be the number of places at which $\boldsymbol{x}$ and $\boldsymbol{y}$ differ, i.e.,

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = |\{i : 1 \le i \le n, x_i \neq y_i\}| = w_H(\boldsymbol{x} - \boldsymbol{y}).$$

Definition 2.2.4 *[54] Let $\mathcal{C}$ be a q-ary code of length n. The minimum Hamming weight of $\mathcal{C}$, denoted by $w_H(\mathcal{C})$, is defined to be the smallest of the weights of the nonzero codewords of $\mathcal{C}$, i.e.,*

$$w_H(\mathcal{C}) = \min\{w_H(\boldsymbol{c}) : \boldsymbol{0} \neq \boldsymbol{c} \in \mathcal{C}\}.$$

The minimum Hamming distance of $\mathcal{C}$, denoted by $d_H(\mathcal{C})$, is defined to be the minimum Hamming distance between any two different codewords in $\mathcal{C}$, i.e.,

$$d = d_H(\mathcal{C}) = \min\{d_H(\boldsymbol{c}_1, \boldsymbol{c}_2) : \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C}, \boldsymbol{c}_1 \neq \boldsymbol{c}_2\}.$$

Let A_i $(i = 1, 2, \ldots, n)$ denote the number of codewords with Hamming weight i in $\mathcal{C}$. The *weight enumerator* of $\mathcal{C}$ is defined by $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$ and the sequence $(1, A_1, A_2, \ldots, A_n)$ is called the *weight distribution* of $\mathcal{C}$. The code $\mathcal{C}$ is said to be a *t-weight code* if the number of nonzero A_i in the sequence $(A_1, A_2, \ldots, A_n)$ is equal to t. We denote by $(1, A_1^{\perp}, \ldots, A_n^{\perp})$ the weight distribution of the dual of the code $\mathcal{C}$ with parameters $[n, k, d]$. Then the first five Pless power moments are given as follows [54, Theorem 7.3.1]:

$$\begin{aligned}
&\sum_{i=0}^{n} A_i = 2^k;\\
&\sum_{i=0}^{n} iA_i = 2^{k-1}(n - A_1^{\perp});\\
&\sum_{i=0}^{n} i^2 A_i = 2^{k-2}[n(n+1) - 2nA_1^{\perp} + 2A_2^{\perp}];\\
&\sum_{i=0}^{n} i^3 A_i = 2^{k-3}[n^2(n+3) - (3n^2 + 3n - 2)A_1^{\perp} + 6nA_2^{\perp} - 6A_3^{\perp}];\\
&\sum_{i=0}^{n} i^4 A_i = 2^{k-4}[n(n+1)(n^2 + 5n - 2) - 4n(n^2 + 3n - 2)A_1^{\perp} + 4(3n^2 + 3n - 4)A_2^{\perp}\\
&-24nA_3^{\perp} + 24A_4^{\perp}].
\end{aligned} \tag{2.4}$$

A linear code $\mathcal{C}$ is said to be *projective* if its dual has the minimum distance at least three.

Now, we have the following lemma, which presents the well-known Singleton bound for linear codes over finite fields.

Lemma 2.2.5 *[54, Singleton Bound] For any linear code $\mathcal{C}$ with parameters $[n,k,d]$ over $\mathbb{F}_q$ satisfy*

$$d \leq n-k+1.$$

In particular, if $d = n-k+1$, then $\mathcal{C}$ is called a *maximal distance separable (MDS) code*. A code is called *almost MDS* if its minimum distance is one less than the MDS case.

The next lemma introduces the Griesmer bound, which applies specifically to linear codes over finite fields.

Lemma 2.2.6 *[54, Griesmer Bound] Let $\mathcal{C}$ be a q-ary linear code with parameters $[N,k,d]$, where $k \geq 1$. Then*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil \cdot \rceil$ is the ceiling function.
In particular, the code $\mathcal{C}$ is called Griesmer code if it attains the Griesmer bound.

The following is a well-known Sphere packing bound for linear codes.

Lemma 2.2.7 *[54, Sphere Packing Bound] Let $\mathcal{C}$ be a binary $[n,k,d]$ code. Then*

$$2^n \geq 2^k \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i},$$

where $\lfloor \frac{d-1}{2} \rfloor$ is the largest integer less than or equal to $\frac{d-1}{2}$.

An $[n,k,d]$ code over $\mathbb{F}_q$ is said to be *distance-optimal* if there is no $[n,k,d']$ code over $\mathbb{F}_q$ with $d' \geq d+1$ and *almost distance-optimal* if an $[n,k,d+1]$ code over $\mathbb{F}_q$ is distance-optimal.

Minimal linear codes have important applications in building secret sharing schemes (SSS). Next, we gives the definition of minimal linear codes.

Definition 2.2.8 *[1, 36] The Hamming weight, denoted by $wt(\boldsymbol{a})$, of a codeword $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ is the cardinality of its* support *defined as $Supp(\boldsymbol{a}) = \{0 \leq i \leq n-1 : a_i \neq 0\}$. Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be codewords of $\mathcal{C}$. A codeword $\boldsymbol{b}$ of $\mathcal{C}$ is covered by another codeword $\boldsymbol{a}$ of $\mathcal{C}$ if $Supp(\boldsymbol{a})$ contains $Supp(\boldsymbol{b})$. A nonzero codeword $\boldsymbol{a} \in \mathcal{C}$ is called* minimal *if it only covers the codewords $c\boldsymbol{a}$ for all $c \in \mathbb{F}_p$, but no other nonzero codewords of $\mathcal{C}$. A linear code $\mathcal{C}$ is called* minimal linear code *if every nonzero codeword of $\mathcal{C}$ is minimal.*

The following lemma shows that a linear code $\mathcal{C}$ is minimal if its weights are close enough to each other, which was proved by Ashikhmin and Barg [1].

Lemma 2.2.9 *[1, Ashikhmin-Barg] Let $\mathcal{C}$ be a linear code over $\mathbb{F}_p$, and $w_{\min}$ and $w_{\max}$ denote the minimum and maximum Hamming weights of nonzero codewords in $\mathcal{C}$, respectively. If*

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}},$$

then $\mathcal{C}$ is minimal.

2.3 Some results in algebraic number theory

In this section, we recall some classical results in algebraic number theory. For more details on algebraic number theory, please refer to [55].

Let K be a finite extension over the rational numbers $\mathbb{Q}$ and $n = [K : \mathbb{Q}]$ the dimension of $K/\mathbb{Q}$. An element w in K is called an algebraic integer if it is a root of a polynomial $x^n + b_1 x^{n-1} + \cdots + b_n \in \mathbb{Z}[x]$, where $\mathbb{Z}$ denotes the ring of ordinary integers. It is clear that a rational number $w \in \mathbb{Q}$ is an algebraic integer if and only if $w \in \mathbb{Z}$.

The set of all algebraic integers in K forms a Dedekind domain, which is denoted by $\mathbb{O}_K$. It then follows that every nonzero ideal in $\mathbb{O}_K$ can be written as a product of nonzero prime ideals. It is easy to see that $\mathbb{Z} \subset \mathbb{O}_K$. For a prime p, $p\mathbb{O}_K$ generated by p is an ideal in $\mathbb{O}_K$. Then

$$p\mathbb{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_g^{e_g},$$

where $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_g$ are distinct nonzero prime ideals containing $p\mathbb{O}_K$ and $e_i \geq 1$ for $1 \leq i \leq g$ ($\mathcal{P}_i$ is also called the prime ideal in $\mathbb{O}_K$ over p); the $\mathcal{P}_i$ and the e_i are uniquely determined; e_i is called the ramification index of $\mathcal{P}_i$. Note that $\mathbb{O}_K$ is a Dedekind domain. Then every prime ideal $\mathcal{P}_i$ is maximal and thus $\mathbb{O}_K/\mathcal{P}_i$ is a field. In fact, it is a finite field containing $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Write $f_i := [\mathbb{O}_K/\mathcal{P}_i : \mathbb{F}_p]$. Then f_i is called the degree of $\mathcal{P}_i$. In addition, we have $\sum_{i=1}^{g} e_i f_i = n$.

Let $N \geq 3$ be an integer with $N \neq 2 \pmod 4$ and $\zeta_N = e^{\frac{2\pi\sqrt{-1}}{N}}$ an Nth primitive root of unity. Let $K = \mathbb{Q}(\zeta_N)$ be the cyclotomic field of Nth roots of unity. We then have $[K : \mathbb{Q}] = \phi(N)$ and $\mathbb{O}_K = \mathbb{Z}[\zeta_N]$, where ϕ is the Euler function. It is known that K is the splitting field of the polynomial $x^N - 1$ over $\mathbb{Q}$. Hence, $K/\mathbb{Q}$ is a Galois extension. In this case, we have $e_1 = e_2 = \cdots = e_g = e$ and $f_1 = f_2 = \cdots = f_g = f$ and then $\phi(N) = efg$.

For the cyclotomic field $K = \mathbb{Q}(\zeta_N)$, the following lemma shows how rational primes $p \in \mathbb{Z}$ split in $\mathbb{O}_K$, which will be useful in the next section.

Lemma 2.3.1 *[16, 55] Let $N \geq 3$ be an integer with $N \neq 2 \pmod 4$. Let $K = \mathbb{Q}(\zeta_N)$ be the cyclotomic field and $p \in \mathbb{Z}$ a prime.*

(1) Then we have $e = 1$ if and only if $p \nmid N$. In this case, let f be the smallest positive integer such that $p^f := 1 \pmod N$. Then

$$p\mathbb{O}_K = \mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_g,$$

where $\mathcal{P}_i$ has degree f and $g = \phi(N)/f$.

(2) When $p \mid N$, write $N = p^s N'$, where $p \nmid N'$. Let f be the smallest positive integer such that $p^f := 1 \pmod{N'}$. Then

$$p\mathbb{O}_K = (\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_g)^e,$$

where $e = \phi(p^s)$, each $\mathcal{P}_i$ has degree f and $g = \phi(N')/f$.

Next, we recall the definition of the Jacobi symbol, which is a generalization of the Legendre symbol.

Definition 2.3.2 *[3, 24] Let n be an odd positive integer with the prime factorization*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where the prime numbers $p_1, p_2, \ldots, p_k$ are distinct, and let x be an integer. The Jacobi symbol $\left(\frac{x}{n}\right)$ is defined as the product of the Legendre symbols corresponding to the prime factors of n:

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p_1}\right)^{a_1} \left(\frac{x}{p_2}\right)^{a_2} \cdots \left(\frac{x}{p_k}\right)^{a_k},$$

where each $\left(\frac{x}{p_i}\right)$ is a Legendre symbol. If n is prime, then the Jacobi symbol is the same as the Legendre symbol.

The Legendre symbol $\left(\frac{x}{p}\right)$ is defined for all integers x and all odd primes p by

$$\left(\frac{x}{p}\right) = \begin{cases} 0, & \text{if } x := 0 \ (mod\ p); \\ 1, & \text{if } x \neq 0 \ (mod\ p) \text{ and } x \text{ is a square, i.e., there is an element } y \\ & \text{such that } x := y^2 \ (mod\ p); \\ -1, & \text{if } x \neq 0 \ (mod\ p) \text{ and } x \text{ is a non-square.} \end{cases}$$

2.4 Boolean functions

Many cryptographic properties of cryptographic functions are characterized by their Walsh transform. Therefore, Walsh transform is a very important tool to study the properties of cryptographic functions. In the following, we recall the definition of Walsh transform.

Let $F(x)$ be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$, where n is a positive integer. The *Walsh transform* of $F(x)$ at $(a,b) \in \mathbb{F}_{2^n}^2$ is defined by

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bF(x))},$$

where $\mathrm{Tr}_n(\cdot)$ denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

If $W_F(a,b) = 0$ or $\pm 2^{\frac{n+1}{2}}$ for any pair $(a,b) \in \mathbb{F}_{2^n}^2$ with $b \neq 0$, then $F(x)$ is called an *almost bent (AB for short) function*. Almost bent functions exist only for odd n. Define

$$\delta_F = \max\{\delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\},$$

where $\delta_F(a,b) = |\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}|$. If $\delta_F = 2$, then $F(x)$ is called an *almost perfect nonlinear (APN for short) function*. It is well-known that AB functions and APN functions are special cryptographic functions that have important applications in coding theory. For instance, AB and APN functions have been employed to construct optimal linear codes over finite fields [12, 83].

Next, we give a lemma describing the relationship between AB functions and APN functions.

Lemma 2.4.1 *[6] Let $\mathbb{F}_{2^n}$ be a finite field with n a positive integer. If $F(x)$ is an almost bent function over $\mathbb{F}_{2^n}$, then $F(x)$ is an almost perfect nonlinear function over $\mathbb{F}_{2^n}$.*

The following lemma is from [72, Subsection B], which will be useful for determining the Walsh transform of quadratic functions.

Lemma 2.4.2 *[72] Let F be a quadratic function from $\mathbb{F}_{2^n}$ to itself. Let $\varphi_{a,b}(x) = \mathrm{Tr}_n(ax+bF(x))$. For the associated bilinear mapping $B_{\varphi_{a,b}}(x,y) = \varphi_{a,b}(x+y) + \varphi_{a,b}(x) + \varphi_{a,b}(y)$, its kernel $V_{\varphi_{a,b}}$ is given by $\{y \in \mathbb{F}_{2^n} : B_{\varphi_{a,b}}(x,y) = 0 \text{ for } \forall\ x \in \mathbb{F}_{2^n}\}$. Then the Walsh transform of F at $(a,b) \in \mathbb{F}_{2^n}^2$ is*

$$W_F(a,b) = \begin{cases} \pm 2^{\frac{n+d_b}{2}}, & \text{if } \mathrm{Tr}_n(ax+bF(x)) = 0 \text{ for all } x \in V_{\varphi_{a,b}}; \\ 0, & \text{otherwise,} \end{cases} \tag{2.5}$$

where d_b is the dimension of the kernel $V_{\varphi_{a,b}}$ of the bilinear mapping $B_{\varphi_{a,b}}$ over $\mathbb{F}_2$.

We recall some two-to-one functions over $\mathbb{F}_{2^n}$ recently obtained in [72–74, 128].

Lemma 2.4.3 *[73] Let $n = 2m$, $\alpha^{2^m-1} = w$ and $w \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$, where m is odd. Then $F(x) = x^{2^{m+1}+4} + x^{2^{m+2}+2} + \alpha x$ is 2-to-1 over $\mathbb{F}_{2^n}$.*

Lemma 2.4.4 *[128] Let $n = 2m$ and $\delta \in \mathbb{F}_{2^n}$, where m is even and $\mathrm{Tr}_n(\delta) = 1$. Then the following functions are all 2-to-1 over $\mathbb{F}_{2^n}$.*

(1) $F(x) = (x^2+x+\delta)^{2^m+1} + x$;

(2) $F(x) = (x^2+x+\delta)^{2^{2m-1}+2^{m-1}} + x$;

(3) $F(x) = (x^2+x+\delta)^{2^{2m-2}+2^{m-2}} + x$.

Lemma 2.4.5 *[128] Let $m, i \in \mathbb{N}$, $\delta \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_{2^m}^*$ with $n = 2m$, $\gcd(m,i) = 1$. Let $\mathrm{Tr}_m^n(\delta^2 + c^{2^m-i}\delta) \neq 0$. Then $F(x) = (x^{2^m}+x+\delta)^{2^i+1} + cx$ is 2-to-1 over $\mathbb{F}_{2^n}$.*

Lemma 2.4.6 *[128] Let $m, i \in \mathbb{N}$, $\delta \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_{2^m}$ with $n = 2m$. Let $\mathrm{Tr}_m^n(\delta)^{2^i+2} + \mathrm{Tr}_m^n(\delta) \neq 0$. Then $F(x) = (x^{2^m}+x+\delta)^{2^{m+2^i}+1} + cx$ is 2-to-1 over $\mathbb{F}_{2^n}$.*

Lemma 2.4.7 *[128] Let $m \in \mathbb{N}$, $\delta \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$ and $c \in \mathbb{F}_{2^m}^*$ with $n = 2m$. Let $\mathrm{Tr}_m(\frac{1}{c} + 1) \neq 0$. Then $F(x) = (x^{2^m}+x+\delta)^{2^{2m-2}+2^m-2^{m-2}} + cx$ is 2-to-1 over $\mathbb{F}_{2^n}$.*

Remark 2.4.8 *If $F(x)$ is a 2-to-1 function of the form $(x^{2^k}+x+\delta)^s$ under certain conditions, then $F(x)+\delta^s$ is still a 2-to-1 function over $\mathbb{F}_{2^n}$.*

Lemma 2.4.9 *[74] Let $n = 2m$ with m being an odd positive integer and $w \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$. Then $F(x) = x^{\frac{2^{n-1}+2^m-1}{3}} + x^{2^m} + wx$ is 2-to-1 over $\mathbb{F}_{2^n}$.*

Lemma 2.4.10 *[74] Let $n = 2m+1$ and m be a positive integer. Then the following quadrinomials are all 2-to-1 over $\mathbb{F}_{2^n}$.*

(1) $F(x) = x^{2^{m+1}+2} + x^{2^{m+1}+1} + x^2 + x$;

(2) $F(x) = x^{2^{m+2}+4} + x^{2^{m+1}+2} + x^2 + x$;

(3) $F(x) = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$;

(4) $F(x) = x^{2^n-2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$.

Lemma 2.4.11 *[74] Let $n = 3m$ with m being a positive integer. Then the following functions are all 2-to-1 over $\mathbb{F}_{2^n}$.*

(1) $F(x) = x^{2^{2m}+1} + x^{2^{m+1}} + x^{2^m+1} + x$ *with* $m \neq 1 \pmod 3$;

(2) $F(x) = x^{2^{2m+1}+1} + x^{2^{m+1}+1} + x^4 + x^3$ *with m being odd.*

Lemma 2.4.12 *[72] Let $n = km$, where k is an odd positive integer and m is a positive integer. Then $F(x) = \mathrm{Tr}_m^n(x^{2^m+1}) + x$ is 2-to-1 over $\mathbb{F}_{2^n}$.*

Chapter 3

Constructions of (asymptotically) optimal codebooks

In this chapter, we construct several classes of optimal or asymptotically optimal codebooks with respect to the Welch bound or the Levenshtein bound by studying the character sums over the finite chain ring $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ and the finite non-chain ring $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$. In Section 3.1, we first study the additive characters and multiplicative characters of R_1 and some properties of character sums, including Gaussian sums, hyper Eisenstein sums and Jacobi sums over R_1. Using these character sums over R_1, four classes of asymptotically optimal codebooks and a class of optimal codebooks with respect to Welch bound are obtained. In Section 3.2, we first investigate the additive characters and multiplicative characters of R_2 and some properties of Gaussian sums, hyper Eisenstein sums and Jacobi sums over R_2. Furthermore, we construct three classes of asymptotically optimal codebooks with respect to Welch bound and a class of optimal codebooks for Levenshtein bound from these character sums. The parameters of some codebooks constructed in this chapter are flexible and different from [9, 12, 27, 31, 32, 48, 49, 52, 53, 69, 71, 77, 79–82, 129, 130, 133].

3.1 Constructions of codebooks using character sums over $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$

Let q be a power of a prime, and $\mathbb{F}_q$ denote the finite field with q elements. We consider the chain ring $R_1 = \mathbb{F}_q + u\mathbb{F}_q = \{\alpha + \beta u : \alpha, \beta \in \mathbb{F}_q\}(u^2 = 0)$ having the unique maximal ideal $M = \langle u \rangle$. In fact, $R_1 = \mathbb{F}_q \oplus u\mathbb{F}_q \simeq \mathbb{F}_q^2$ is a two-dimensional vector space over $\mathbb{F}_q$ and $|R_1| = q^2$. The invertible elements of R_1 are

$$R_1^* = R_1 \backslash M = \mathbb{F}_q^* + u\mathbb{F}_q = \{\alpha + \beta u : \alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q\}.$$

It is easy to know that $|R_1^*| = q(q-1)$. R_1^* can also be represented as $\mathbb{F}_q^* \times (1 + M)$ (direct product).

3.1.1 Characters of R_1

In this subsection, we describe the additive and multiplicative characters of the finite chain ring $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$.

A. Additive characters of R_1

Define $\lambda : R_1 \longrightarrow \mathbb{C}^*$ as the additive character of finite chain R_1 satisfying $\lambda(\alpha+\beta) = \lambda(\alpha)\lambda(\beta)$ for any $\alpha,\beta \in R_1$. Then the group of additive characters of R_1 is $\widehat{R}_1 := \{\lambda : R_1 \longrightarrow \mathbb{C}^* \mid \lambda(\alpha+\beta) = \lambda(\alpha)\lambda(\beta), \alpha,\beta \in R_1\}$.

For any $a_0+ua_1 \in R_1$, we have $\lambda(a_0+ua_1) = \lambda(a_0)\lambda(ua_1)$. Define two mappings λ' and λ'' as follows: The mapping $\lambda' : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ is defined as

$$\lambda'(c) := \lambda(c)$$

for $c \in \mathbb{F}_q$; and the mapping $\lambda'' : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ is defined as

$$\lambda''(c) := \lambda(uc)$$

for $c \in \mathbb{F}_q$. It is easy to check that $\lambda'(c_1+c_2) = \lambda'(c_1)\lambda'(c_2)$ and $\lambda''(c_1+c_2) = \lambda''(c_1)\lambda''(c_2)$ for $c_1,c_2 \in \mathbb{F}_q$. We know that λ' and λ'' are both additive characters of $\mathbb{F}_q$. Hence, there exist $b,c \in \mathbb{F}_q$ such that

$$\lambda'(x) = \zeta_p^{\mathrm{Tr}_p^q(bx)} = \chi_b(x) \text{ and } \lambda''(x) = \zeta_p^{\mathrm{Tr}_p^q(cx)} = \chi_c(x)$$

for all $x \in \mathbb{F}_q$, where $\mathrm{Tr}_p^q(\cdot)$ denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity over $\mathbb{F}_q$. Therefore, we can express an additive character of R_1 as follows:

$$\begin{aligned} \lambda(a_0+ua_1) &= \lambda'(a_0)\lambda''(a_1) \\ &= \chi_b(a_0)\chi_c(a_1). \end{aligned}$$

Thus, there is an one-to-one correspondence:

$$\begin{aligned} \tau : (\widehat{R}_1,+) &\longrightarrow (\widehat{\mathbb{F}}_q,+)\times(\widehat{\mathbb{F}}_q,+), \\ \lambda &\longmapsto (\chi_b,\chi_c), \end{aligned}$$

where $\widehat{\mathbb{F}}_q$ denotes the group of additive characters of $\mathbb{F}_q$. It is easy to prove that the mapping τ is an isomorphism.

B. Multiplicative characters of R_1

The invertible elements of R_1 are can be represented as

$$\begin{aligned} R_1^* &= \{a_0+ua_1 : a_0 \in \mathbb{F}_q^*, a_1 \in \mathbb{F}_q\} \\ &= \{b_0(1+ub_1) : b_0 \in \mathbb{F}_q^*, b_1 \in \mathbb{F}_q\}. \end{aligned}$$

Define $\varphi : R_1^* \longrightarrow \mathbb{C}^*$ as the multiplicative character of finite chain R_1 satisfying $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ for any $\alpha,\beta \in R_1^*$. Then the group of multiplicative characters of R_1 is $\widehat{R}_1^* := \{\varphi : R_1^* \longrightarrow \mathbb{C}^* \mid \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta), \alpha,\beta \in R_1^*\}$.

For any $b_0(1+ub_1) \in R_1^*$, we have $\varphi(b_0(1+ub_1)) = \varphi(b_0)\varphi(1+ub_1)$. Define two mappings φ' and φ'' as follows: The mapping $\varphi' : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ is defined as

$$\varphi'(c) := \varphi(c),$$

for $c \in \mathbb{F}_q$; and the mapping $\varphi'' : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ is defined as

$$\varphi''(c) := \varphi(1+uc),$$

for $c \in \mathbb{F}_q$. It is easy to check that for any $c_1, c_2 \in \mathbb{F}_q^*$, we have $\varphi'(c_1c_2) = \varphi'(c_1)\varphi'(c_2)$ and

$$\begin{aligned} \varphi''(c_1+c_2) &= \varphi(1+u(c_1+c_2)) \\ &= \varphi((1+uc_1)(1+uc_2)) \\ &= \varphi(1+uc_1)\varphi(1+uc_2) \\ &= \varphi''(c_1)\varphi''(c_2). \end{aligned}$$

It follows that φ' is a multiplicative character of $\mathbb{F}_q$ and φ'' is an additive character of $\mathbb{F}_q$. Then there exists $a \in \mathbb{F}_q$ such that $\varphi'' = \chi_a$.

Hence, we can represent a multiplicative character of R_1 as a product

$$\varphi(b_0(1+ub_1)) = \varphi'(b_0)\chi_a(b_1),$$

where $\varphi' \in \widehat{\mathbb{F}}_q^*$ and $\chi_a \in \widehat{\mathbb{F}}_q$. Moreover, we have

$$\begin{aligned} \sigma : (\widehat{R}_1^*, \times) &\longrightarrow (\widehat{\mathbb{F}}_q^*, \times) \times (\widehat{\mathbb{F}}_q, +), \\ \varphi &\longmapsto (\psi, \chi_a), \end{aligned}$$

where $\widehat{\mathbb{F}}_q^*$ denotes the group of multiplicative characters of $\mathbb{F}_q$ and $\psi = \varphi'$ is the multiplicative character of $\mathbb{F}_q$. One can show that the mapping σ is an isomorphism.

3.1.2 Character sums over R_1

In this subsection, we introduce Gaussian sums, hyper Eisenstein sums and Jacobi sums over R_1 and present some fundamental properties of these character sums.

Let $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ and $R_{(r)} = \mathbb{F}_r + u\mathbb{F}_r$, where $u^2 = 0$, $q = r^m$, r is a power of a prime p, and m is a positive integer. Then $R_1/R_{(r)}$ is a Galois extension of rings and the Galois group $\mathrm{Gal}(R_1/R_{(r)}) = \langle \sigma_r \rangle$, where σ_r is the $R_{(r)}$-automorphism of R_1 defined by

$$\sigma_r(\alpha+u\beta) = \alpha^r + u\beta^r \ (\alpha, \beta \in \mathbb{F}_q).$$

Then, we can define the trace mapping from R_1 to $R_{(r)}$: $\mathrm{Tr}_{R_{(r)}}^{R_1} : R_1 \longrightarrow R_{(r)}$ satisfies $\mathrm{Tr}_{R_{(r)}}^{R_1}(\alpha+u\beta) = \mathrm{Tr}_r^q(\alpha) + u\mathrm{Tr}_r^q(\beta) = \sum_{i=0}^{m-1} \sigma_r^i(\alpha+u\beta)$, where $\mathrm{Tr}_r^q(\cdot)$ denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_r$. Moreover, it is easy to show that $\mathrm{Tr}_{R_{(r)}}^{R_1}(\mathfrak{s}t) = \mathfrak{s}\mathrm{Tr}_{R_{(r)}}^{R_1}(t)$ for each $\mathfrak{s} \in R_{(r)}$ and $t \in R_1$. For convenience, $\mathrm{Tr}_{R_{(r)}}^{R_1}$ is abbreviated as Tr.

From Subsection 3.1.1, for any $a, b, c \in \mathbb{F}_q, \chi_a, \chi_b, \chi_c \in \widehat{\mathbb{F}}_q$ and $\psi \in \widehat{\mathbb{F}}_q^*$, the additive and multiplicative characters of R_1 can be expressed as $\varphi := \psi \star \chi_a$, $\lambda := \chi_b \star \chi_c$. Then, for any $t = t_0(1+ut_1) \in R_1$, we have $\varphi(t) = (\psi \star \chi_a)(t) = \psi(t_0)\chi_a(t_1)$, and

$\lambda(t) = (\chi_b \star \chi_c)(t) = \chi_b(t_0)\chi_c(t_0 t_1)$.

A. Gaussian sums over R_1

Let λ and φ be an additive character and a multiplicative character of R_1, respectively. The Gaussian sum for λ and φ over $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ is defined by

$$G_{R_1}(\varphi, \lambda) = \sum_{t \in R_1^*} \varphi(t)\lambda(t).$$

The following theorem establishes the relation between the Gaussian sum over the finite chain R_1 and the Gaussian sum over the finite field $\mathbb{F}_q$.

Theorem 3.1.1 *Let φ be a multiplicative character and λ be an additive character of R_1, where $\varphi := \psi \star \chi_a, \lambda := \chi_b \star \chi_c$, $\psi \in \widehat{\mathbb{F}}_q^*$ and $a, b, c \in \mathbb{F}_q$. Then the Gaussian sum $G_{R_1}(\varphi, \lambda)$ satisfies*

$$G_{R_1}(\varphi, \lambda) = \begin{cases} qG_{\mathbb{F}_q}(\psi, \chi_b), & \text{if } a = 0, c = 0; \\ q\psi(-\frac{a}{c})\chi(-\frac{ab}{c}), & \text{if } a \neq 0, c \neq 0; \\ 0, & \text{otherwise,} \end{cases}$$

where $G_{\mathbb{F}_q}(\psi, \chi_b)$ denotes the Gaussian sum over $\mathbb{F}_q$.

Proof: Assume that $t = t_0(1 + ut_1)$, where $t_0 \in \mathbb{F}_q^*$ and $t_1 \in \mathbb{F}_q$.

$$\begin{aligned} G_{R_1}(\varphi, \lambda) &= \sum_{t \in R_1^*} \varphi(t)\lambda(t) \\ &= \sum_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q} \psi(t_0)\chi_a(t_1)\chi_b(t_0)\chi_c(t_0 t_1) \\ &= \sum_{t_0 \in \mathbb{F}_q^*} \psi(t_0)\chi_1(bt_0) \sum_{t_1 \in \mathbb{F}_q} \chi_1((a + ct_0)t_1) \\ &= q \sum_{t_0 \in \mathbb{F}_q^*, a + ct_0 = 0} \psi(t_0)\chi_1(bt_0) = \begin{cases} qG_{\mathbb{F}_q}(\psi, \chi_b), & \text{if } a = 0, c = 0; \\ q\psi(-\frac{a}{c})\chi_1(-\frac{ab}{c}), & \text{if } a \neq 0, c \neq 0; \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

This completes the proof. ■

Next, we introduce the definition of the quadratic character over R_1.

Definition 3.1.2 *Let φ be a multiplicative character of R_1. If $(\varphi(t))^2 = 1$ for any $t \in R_1^*$, then φ is called the* quadratic character *of R_1, denoted by ρ. Moreover, $G_{R_1}(\rho, \lambda)$ denotes the quadratic Gaussian sum over R_1, where λ is an additive character of R_1.*

In the following, we determine the form of the quadratic character ρ of R_1. Let η, ψ_0 and χ_0 denote the quadratic character, the trivial multiplicative character and the trivial additive character of the finite field $\mathbb{F}_q$, respectively. We use the convention that $\psi(0) = 0$ for a nontrivial multiplicative character ψ of $\mathbb{F}_q$. For any $t = t_0(1 + ut_1) \in R_1^*$,

if the multiplicative character φ of R_1 is a quadratic character, then we need $(\varphi(t))^2 = (\psi(t_0)\chi_a(t_1))^2 = 1$. However,

$$\begin{aligned}(\varphi(t))^2 &= (\psi(t_0)\chi_a(t_1))^2 \\ &= (\psi(t_0))^2\chi(2at_1) \\ &= (\psi(t_0))^2\zeta_p^{\mathrm{Tr}_p^q(2at_1)},\end{aligned}$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity over $\mathbb{F}_q$.

- If $p = 2$, there is no quadratic character η of $\mathbb{F}_q$ since $2 \nmid (q-1)$ and $\zeta_p^{\mathrm{Tr}_p^q(2at_1)} = 1$. Hence, when ψ is a trivial character and $a \neq 0$, we obtain that φ is a quadratic character ρ of R_1, denoted by $\rho := \psi_0 \star \chi_a$.
- If $p \neq 2$, then φ is a quadratic character ρ of R when $\psi = \eta$ and $a = 0$, denoted by $\rho := \eta \star \chi_0$.

Based on Theorem 3.1.1, we have the following corollary.

Corollary 3.1.3 *Let ρ be a quadratic character and λ be an additive character of R_1. Let $\chi_a, \chi_b, \chi_c \in \widehat{\mathbb{F}}_q$, η denote the quadratic character of $\mathbb{F}_q$ and χ_0 denote the trivial additive character of $\mathbb{F}_q$.*

(1) If $p = 2$, then

$$G_{R_1}(\rho, \lambda) = \begin{cases} q\chi(-\frac{ab}{c}), & \text{if } c \neq 0; \\ 0, & \text{if } c = 0, \end{cases}$$

where $\rho := \psi_0 \star \chi_a, \lambda := \chi_b \star \chi_c$ and $a \in \mathbb{F}_q^*, b, c \in \mathbb{F}_q$.

(2) If $p \neq 2$, then $|G_{R_1}(\rho, \lambda)| = q^{\frac{1}{2}}$ if $b \neq 0$ and $G_{R_1}(\rho, \lambda) = 0$ otherwise, where $\rho := \eta \star \chi_0$, $\lambda := \chi_b \star \chi_c$ and $b, c \in \mathbb{F}_q$.

B. Hyper Eisenstein sums over R_1

Now, we give the definition of hyper Eisenstein sums over $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$.

Definition 3.1.4 *Let n be a positive integer and $\varphi_1, \varphi_2, \ldots, \varphi_n$ multiplicative characters of R_1. Then the* hyper Eisenstein sum *for $\varphi_1, \varphi_2, \ldots, \varphi_n$ over R_1 is defined by*

$$E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1) = \sum_{\substack{t_1, t_2, \ldots, t_n \in R_1^*, \\ \mathrm{Tr}(t_1 + t_2 + \cdots + t_n) = 1}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n). \tag{3.1}$$

Moreover, we can define $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; \mathfrak{s})$ as follows: for each $\mathfrak{s} \in R_{(r)}$,

$$E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; \mathfrak{s}) = \sum_{t_1, t_2, \ldots, t_n \in R_1^*, \mathrm{Tr}(t_1 + t_2 + \cdots + t_n) = \mathfrak{s}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n).$$

If $\mathfrak{s} \in R_{(r)}^*$, then

$$\begin{aligned} E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;\mathfrak{s}) &= \sum_{t_1,t_2,\ldots,t_n\in R_1^*,\mathrm{Tr}(t_1+t_2+\cdots+t_n)=\mathfrak{s}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n) \\ &\overset{t_i\to\mathfrak{s}t_i}{=} \sum_{\substack{\mathfrak{s}t_1,\mathfrak{s}t_2,\ldots,\mathfrak{s}t_n\in R_1^*,\\ \mathrm{Tr}(\mathfrak{s}t_1+\mathfrak{s}t_2+\cdots+\mathfrak{s}t_n)=\mathfrak{s}}} \varphi_1(\mathfrak{s}t_1)\varphi_2(\mathfrak{s}t_2)\cdots\varphi_n(\mathfrak{s}t_n) \\ &= \varphi_1\cdots\varphi_n(\mathfrak{s}) \sum_{\substack{t_1,t_2,\ldots,t_n\in R_1^*,\\ \mathrm{Tr}(t_1+t_2+\cdots+t_n)=1}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n) \\ &= \varphi_1\cdots\varphi_n(\mathfrak{s})E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;1). \end{aligned}$$

If $\mathfrak{s} = ub \in u\mathbb{F}_r^*$ $(b \in \mathbb{F}_r^* \subset R_1^*)$, then

$$\begin{aligned} E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;\mathfrak{s}) &= \sum_{t_1,t_2,\ldots,t_n\in R_1^*,\mathrm{Tr}(t_1+t_2+\cdots+t_n)=\mathfrak{s}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n) \\ &\overset{t_i\to bt_i}{=} \sum_{\substack{bt_1,bt_2,\ldots,bt_n\in R_1^*,\\ \mathrm{Tr}(bt_1+bt_2+\cdots+bt_n)=ub}} \varphi_1(bt_1)\varphi_2(bt_2)\cdots\varphi_n(bt_n) \\ &= \varphi_1\cdots\varphi_n(b) \sum_{\substack{t_1,t_2,\ldots,t_n\in R_1^*,\\ \mathrm{Tr}(t_1+t_2+\cdots+t_n)=u}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n) \\ &= \varphi_1\cdots\varphi_n(b)E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;u). \end{aligned}$$

Thus, it is sufficient to compute

$$E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;0) = \sum_{t_1,t_2,\ldots,t_n\in R_1^*,\mathrm{Tr}(t_1+t_2+\cdots+t_n)=0} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n),$$

$$E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n) = E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;1) = \sum_{\substack{t_1,t_2,\ldots,t_n\in R_1^*,\\ \mathrm{Tr}(t_1+t_2+\cdots+t_n)=1}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n),$$

$$E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;u) = \sum_{t_1,t_2,\ldots,t_n\in R_1^*,\mathrm{Tr}(t_1+t_2+\cdots+t_n)=u} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n).$$

Before calculating the sums $E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;0), E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;1)$ and $E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;u)$, we need to establish some preliminary results.

Lemma 3.1.5 *Let $a \in \mathbb{F}_q$, $y \in \mathbb{F}_r$ and $t' \in \mathbb{F}_q^*$. Then*

$$\sum_{t''\in\mathbb{F}_q} \chi((a+yt')t'') = \begin{cases} q, & \text{if } a=0, t'\in\mathbb{F}_q^* \text{ and } y=0; \\ 0, & \text{if } a=0, t'\in\mathbb{F}_q^* \text{ and } y\neq 0; \\ q, & \text{if } a\neq 0, t'\in a\mathbb{F}_r^* \text{ and } y=-\frac{a}{t'}; \\ 0, & \text{if } a\neq 0, t'\in a\mathbb{F}_r^* \text{ and } y\neq -\frac{a}{t'}; \\ 0, & \text{if } a\neq 0, t'\notin a\mathbb{F}_r^* \text{ and } y\in\mathbb{F}_r. \end{cases}$$

Proof: The proof of the result is easy, so we omit it here. ■

Lemma 3.1.6 *Let $t'_1, t'_2, \ldots, t'_n \in \mathbb{F}_q^*$ and $a_1, a_2, \ldots, a_n \in \mathbb{F}_q$.*

(1) *If* $A := A(a_1, \ldots, a_n; t'_1, \ldots, t'_n) = \sum_{\substack{t''_1, \ldots, t''_n \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t'_1 t''_1 + \cdots + t'_n t''_n) = 0}} \chi_{a_1}(t''_1) \cdots \chi_{a_n}(t''_n)$, *then*

$$A = \begin{cases} \frac{q^n}{r}, & \text{if } a_1 = a_2 = \cdots = a_n = 0; \\ \frac{q^n}{r}, & \text{if } a_1 \cdots a_n \neq 0 \text{ and } \frac{a_1}{t'_1} = \cdots = \frac{a_n}{t'_n} \in \mathbb{F}_r^*; \\ 0, & \text{otherwise.} \end{cases}$$

(2) *If* $B := B(a_1, \ldots, a_n; t'_1, \ldots, t'_n) = \sum_{\substack{t''_1, \ldots, t''_n \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t'_1 t''_1 + \cdots + t'_n t''_n) = 1}} \chi_{a_1}(t''_1) \cdots \chi_{a_n}(t''_n)$, *then*

$$B = \begin{cases} \frac{q^n}{r}, & \text{if } a_1 = a_2 = \cdots = a_n = 0; \\ \frac{q^n}{r}\lambda(z), & \text{if } a_1 \cdots a_n \neq 0 \text{ and } \frac{a_1}{t'_1} = \cdots = \frac{a_n}{t'_n} = z \in \mathbb{F}_r^*; \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Let $t'_i \in \mathbb{F}_q^*, a_i \in \mathbb{F}_q$, where $1 \leq i \leq n$.

$$\begin{aligned}
(1)\, A &= \sum_{\substack{t''_1, \ldots, t''_n \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t'_1 t''_1 + \cdots + t'_n t''_n) = 0}} \chi_{a_1}(t''_1) \cdots \chi_{a_n}(t''_n) \\
&= \sum_{t''_1, \ldots, t''_n \in \mathbb{F}_q} \chi(a_1 t''_1 + \cdots + a_n t''_n) \frac{1}{r} \sum_{y \in \mathbb{F}_r} \mu(y \mathrm{Tr}_r^q(t'_1 t''_1 + \cdots + t'_n t''_n)) \\
&= \frac{1}{r} \sum_{y \in \mathbb{F}_r} \sum_{t''_1, \ldots, t''_n \in \mathbb{F}_q} \chi(a_1 t''_1 + \cdots + a_n t''_n + y(t'_1 t''_1 + \cdots + t'_n t''_n)) \\
&= \frac{1}{r} \sum_{y \in \mathbb{F}_r} \sum_{t''_1 \in \mathbb{F}_q} \chi((a_1 + y t'_1) t''_1) \cdots \sum_{t''_n \in \mathbb{F}_q} \chi((a_n + y t'_n) t''_n) \\
&= \frac{1}{r} \Bigg(\sum_{t''_1 \in \mathbb{F}_q} \chi(a_1 t''_1) \cdots \sum_{t''_n \in \mathbb{F}_q} \chi(a_n t''_n) + \sum_{y \in \mathbb{F}_r^*} \sum_{t''_1 \in \mathbb{F}_q} \chi((a_1 + y t'_1) t''_1) \cdots \\
&\qquad \sum_{t''_n \in \mathbb{F}_q} \chi((a_n + y t'_n) t''_n) \Bigg).
\end{aligned}$$

It is obvious that

$$\sum_{t''_1 \in \mathbb{F}_q} \chi(a_1 t''_1) \cdots \sum_{t''_n \in \mathbb{F}_q} \chi(a_n t''_n) = \begin{cases} q^n, & \text{if } a_1 = a_2 = \cdots = a_n = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Let $T = \sum_{y \in \mathbb{F}_r^*} \sum_{t''_1 \in \mathbb{F}_q} \chi((a_1 + y t'_1) t''_1) \cdots \sum_{t''_n \in \mathbb{F}_q} \chi((a_n + y t'_n) t''_n)$. We divide the rest of the proof into two cases according to Lemma 3.1.5.

1) Assume that $a_1 \cdots a_n = 0$. Then $T = 0$.

2) Assume that $a_1 \cdots a_n \neq 0$, such that $a_1 \neq 0, \ldots, a_n \neq 0$. The following is divided into two cases to discuss the value of T:

- If there exists t_i' such that $t_i' \notin a_i \mathbb{F}_r^*$, then $T = 0$.
- If $t_1' \in a_1 \mathbb{F}_r^*$ and $\cdots$ and $t_n' \in a_n \mathbb{F}_r^*$, such that $\frac{a_1}{t_1'}, \ldots, \frac{a_n}{t_n'} \in \mathbb{F}_r^*$, then

$$T = \begin{cases} q^n, & \text{if } \frac{a_1}{t_1'} = \cdots = \frac{a_n}{t_n'}; \\ 0, & \text{otherwise.} \end{cases}$$

To sum up, we can get the desired result.

$$\begin{aligned}
(2)\ B &= \sum_{\substack{t_1'', \ldots, t_n'' \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t_1' t_1'' + \cdots + t_n' t_n'') = 1}} \chi_{a_1}(t_1'') \cdots \chi_{a_n}(t_n'') \\
&= \sum_{t_1'', \ldots, t_n'' \in \mathbb{F}_q} \chi(a_1 t_1'' + \cdots + a_n t_n'') \frac{1}{r} \sum_{y \in \mathbb{F}_r} \mu(y(\mathrm{Tr}_r^q(t_1' t_1'' + \cdots + t_n' t_n'') - 1)) \\
&= \frac{1}{r} \sum_{y \in \mathbb{F}_r} \mu(-y) \sum_{t_1'', \ldots, t_n'' \in \mathbb{F}_q} \chi(a_1 t_1'' + \cdots + a_n t_n'' + y(t_1' t_1'' + \cdots + t_n' t_n'')) \\
&= \frac{1}{r} \sum_{y \in \mathbb{F}_r} \mu(-y) \sum_{t_1'' \in \mathbb{F}_q} \chi((a_1 + y t_1') t_1'') \cdots \sum_{t_n'' \in \mathbb{F}_q} \chi((a_n + y t_n') t_n'') \\
&= \frac{1}{r} \Bigg(\sum_{t_1'' \in \mathbb{F}_q} \chi(a_1 t_1'') \cdots \sum_{t_n'' \in \mathbb{F}_q} \chi(a_n t_n'') + \sum_{y \in \mathbb{F}_r^*} \mu(-y) \sum_{t_1'' \in \mathbb{F}_q} \chi((a_1 + y t_1') t_1'') \cdots \sum_{t_n'' \in \mathbb{F}_q} \chi((a_n \\
&\quad + y t_n') t_n'') \Bigg).
\end{aligned}$$

It is easy to check that

$$\sum_{t_1'' \in \mathbb{F}_q} \chi(a_1 t_1'') \cdots \sum_{t_n'' \in \mathbb{F}_q} \chi(a_n t_n'') = \begin{cases} q^n, & \text{if } a_1 = a_2 = \cdots = a_n = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Let $T = \sum_{y \in \mathbb{F}_r^*} \mu(-y) \sum_{t_1'' \in \mathbb{F}_q} \chi((a_1 + y t_1') t_1'') \cdots \sum_{t_n'' \in \mathbb{F}_q} \chi((a_n + y t_n') t_n'')$. We will calculate T in the following two cases according to Lemma 3.1.5.

1) Assume that $a_1 \cdots a_n = 0$. Then $T = 0$.

2) Assume that $a_1 \cdots a_n \neq 0$, such that $a_1 \neq 0, \ldots, a_n \neq 0$.

- If there exists t_i' such that $t_i' \notin a_i \mathbb{F}_r^*$, then $T = 0$.
- If $t_1' \in a_1 \mathbb{F}_r^*$ and $\cdots$ and $t_n' \in a_n \mathbb{F}_r^*$, such that $\frac{a_1}{t_1'}, \ldots, \frac{a_n}{t_n'} \in \mathbb{F}_r^*$, then

$$T = \begin{cases} q^n \mu(z), & \text{if } \frac{a_1}{t_1'} = \cdots = \frac{a_n}{t_n'} = z; \\ 0, & \text{otherwise.} \end{cases}$$

This completes the proof. ■

Our next result relates the sums $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 0), E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1)$ and $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; u)$ to the sums $E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 0)$ and $E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 1)$.

Theorem 3.1.7 *Let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be multiplicative characters of R_1 and $\varphi_i := \psi_i \star \chi_{a_i} (1 \le i \le n)$, where ψ_i and χ_{a_i} are multiplicative and additive characters of $\mathbb{F}_q$, respectively. Then*

(1) $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 0)$

$$= \begin{cases} \frac{q^n}{r} E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 0), & \text{if } a_1 = \cdots = a_n = 0; \\ \frac{q^{n(r-1)}}{r} \psi_1(a_1) \cdots \psi_n(a_n), & \text{if } a_1 \cdots a_n \neq 0, \mathrm{Tr}_r^q(a_1 + \cdots + a_n) = 0 \text{ and} \\ & (\psi_1 \cdots \psi_n)^* \text{ is trivial;} \\ 0, & \text{otherwise,} \end{cases}$$

where $(\psi_1 \cdots \psi_n)^*$ is the restriction of $\psi_1 \cdots \psi_n$ to $\mathbb{F}_r$.

(2) $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1)$

$$= \begin{cases} \frac{q^n}{r} E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 1), & \text{if } a_1 = \cdots = a_n = 0; \\ \frac{q^n}{r} \psi_1(\frac{a_1}{\mathrm{Tr}_r^q(a_1 + \cdots + a_n)}) \cdots \psi_n(\frac{a_n}{\mathrm{Tr}_r^q(a_1 + \cdots + a_n)}), & \text{if } a_1 \cdots a_n \neq 0 \text{ and } \mathrm{Tr}_r^q(a_1 + \cdots + a_n) \neq 0; \\ 0, & \text{otherwise,} \end{cases}$$

where $E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 1)$ denotes the hyper Eisenstein sum of $\mathbb{F}_q$.

(3) $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; u)$

$$= \begin{cases} \frac{q^n}{r} E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 0), & \text{if } a_1 = \cdots = a_n = 0; \\ \frac{q^n}{r} \psi_1(a_1) \cdots \psi_n(a_n) G_{\mathbb{F}_r}((\overline{\psi_1 \cdots \psi_n})^*), & \text{if } a_1 \cdots a_n \neq 0 \text{ and } \mathrm{Tr}_r^q(a_1 + \cdots + a_n) = 0; \\ 0, & \text{otherwise,} \end{cases}$$

where $(\psi_1 \cdots \psi_n)^*$ is the restriction of $\psi_1 \cdots \psi_n$ to $\mathbb{F}_r$.

Proof: Let $t_1, t_2, \ldots, t_n \in R_1^*$, where $t_i = t_i'(1 + ut_i'')$, $1 \le i \le n$. Then

$$\begin{aligned} (1)\ E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 0) &= \sum_{\substack{t_1, t_2, \ldots, t_n \in R_1^*, \\ \mathrm{Tr}(t_1 + t_2 + \cdots + t_n) = 0}} \varphi_1(t_1)\varphi_2(t_2) \cdots \varphi_n(t_n) \\ &= \sum_{\substack{t_1', \ldots, t_n' \in \mathbb{F}_q^*, t_1'', \ldots, t_n'' \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t_1' + \cdots + t_n') = 0, \mathrm{Tr}_r^q(t_1' t_1'' + \cdots + t_n' t_n'') = 0}} \psi_1(t_1') \chi_{a_1}(t_1'') \cdots \psi_n(t_n') \chi_{a_n}(t_n'') \\ &= \sum_{\substack{t_1', \ldots, t_n' \in \mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t_1' + \cdots + t_n') = 0}} \psi_1(t_1') \cdots \psi_n(t_n') \sum_{\substack{t_1'', \ldots, t_n'' \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t_1' t_1'' + \cdots + t_n' t_n'') = 0}} \chi_{a_1}(t_1'') \cdots \chi_{a_n}(t_n'') \\ &= \sum_{\substack{t_1', \ldots, t_n' \in \mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t_1' + \cdots + t_n') = 0}} \psi_1(t_1') \cdots \psi_n(t_n') A \text{ (By Lemma 3.1.6 (1)).} \end{aligned}$$

• If $a_1 = \cdots = a_n = 0$, then

$$\begin{aligned} E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 0) &= \frac{q^n}{r} \sum_{\substack{t_1', \ldots, t_n' \in \mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t_1' + \cdots + t_n') = 0}} \psi_1(t_1') \cdots \psi_n(t_n') \\ &= \frac{q^n}{r} E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 0). \end{aligned}$$

• If $a_1 \cdots a_n = 0$, but not all of them are zero, then $E_{R_1}(\psi_1, \psi_2, \ldots, \psi_n; 0) = 0$.
• If $a_1 \cdots a_n \neq 0$, then $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 0)$

$$
\begin{aligned}
&= \frac{q^n}{r} \sum_{\substack{t'_1,\ldots,t'_n \in \mathbb{F}_q^*, \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=0, \\ \frac{a_1}{t'_1}=\cdots=\frac{a_n}{t'_n} \in \mathbb{F}_r^*}} \psi_1(t'_1)\cdots\psi_n(t'_n) \\
&= \frac{q^n}{r} \sum_{\substack{z \in \mathbb{F}_r^*, \\ z\mathrm{Tr}_r^q(a_1+\cdots+a_n)=0}} \psi_1(a_1 z)\cdots\psi_n(a_n z) \quad \left(\text{Let } z = \frac{t'_1}{a_1} = \cdots = \frac{t'_n}{a_n}\right) \\
&= \frac{q^n}{r}\psi_1(a_1)\cdots\psi_n(a_n) \sum_{\substack{z \in \mathbb{F}_r^*, \\ z\mathrm{Tr}_r^q(a_1+\cdots+a_n)=0}} (\psi_1\cdots\psi_n)^*(z) \\
&= \begin{cases} 0, & \text{if } \mathrm{Tr}_r^q(a_1+\cdots+a_n) \neq 0; \\ \frac{q^n(r-1)}{r}\psi_1(a_1)\cdots\psi_n(a_n), & \text{if } \mathrm{Tr}_r^q(a_1+\cdots+a_n) = 0 \text{ and } (\psi_1\cdots\psi_n)^* \text{ is trivial}; \\ 0, & \text{if } \mathrm{Tr}_r^q(a_1+\cdots+a_n) = 0 \text{ and } (\psi_1\cdots\psi_n)^* \text{ is nontrivial}. \end{cases}
\end{aligned}
$$

$$
\begin{aligned}
(2)\ E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1) &= \sum_{t_1,t_2,\ldots,t_n \in R_1^*, \mathrm{Tr}(t_1+t_2+\cdots+t_n)=1} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n) \\
&= \sum_{\substack{t'_1,\ldots,t'_n \in \mathbb{F}_q^*, t''_1,\ldots,t''_n \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=1, \mathrm{Tr}_r^q(t'_1t''_1+\cdots+t'_nt''_n)=0}} \psi_1(t'_1)\chi_{a_1}(t''_1)\cdots\psi_n(t'_n)\chi_{a_n}(t''_n) \\
&= \sum_{\substack{t'_1,\ldots,t'_n \in \mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=1}} \psi_1(t'_1)\cdots\psi_n(t'_n) \sum_{\substack{t''_1,\ldots,t''_n \in \mathbb{F}_q, \\ \mathrm{Tr}_r^q(t'_1t''_1+\cdots+t'_nt''_n)=0}} \chi_{a_1}(t''_1)\cdots\chi_{a_n}(t''_n) \\
&= \sum_{\substack{t'_1,\ldots,t'_n \in \mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=1}} \psi_1(t'_1)\cdots\psi_n(t'_n)A \text{ (By Lemma 3.1.6 (1))}.
\end{aligned}
$$

• If $a_1 = \cdots = a_n = 0$, then

$$
\begin{aligned}
E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1) &= \frac{q^n}{r} \sum_{\substack{t'_1,\ldots,t'_n \in \mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=1}} \psi_1(t'_1)\cdots\psi_n(t'_n) \\
&= \frac{q^n}{r} E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 1).
\end{aligned}
$$

• If $a_1 \cdots a_n = 0$, but not all of them are zero, then $E_{R_1}(\psi_1, \psi_2, \ldots, \psi_n; 1) = 0$.

• If $a_1 \cdots a_n \neq 0$, then $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1)$

$$\begin{aligned}
&= \frac{q^n}{r} \sum_{\substack{t'_1,\ldots,t'_n \in \mathbb{F}_q^*, \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=1, \\ \frac{a_1}{t'_1}=\cdots=\frac{a_n}{t'_n}\in\mathbb{F}_r^*}} \psi_1(t'_1)\cdots\psi_n(t'_n) \\
&= \frac{q^n}{r} \sum_{\substack{z\in\mathbb{F}_r^*, \\ z\mathrm{Tr}_r^q(a_1+\cdots+a_n)=1}} \psi_1(a_1 z)\cdots\psi_n(a_n z) \quad \left(\text{Let } z = \frac{t'_1}{a_1} = \cdots = \frac{t'_n}{a_n}\right) \\
&= \frac{q^n}{r}\psi_1(a_1)\cdots\psi_n(a_n) \sum_{\substack{z\in\mathbb{F}_r^*, \\ z\mathrm{Tr}_r^q(a_1+\cdots+a_n)=1}} (\psi_1\cdots\psi_n)(z) \\
&= \begin{cases} 0, & \text{if } \mathrm{Tr}_r^q(a_1+\cdots+a_n) = 0; \\ \frac{q^n}{r}\psi_1\left(\frac{a_1}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)}\right)\cdots\psi_n\left(\frac{a_n}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)}\right), & \text{if } \mathrm{Tr}_r^q(a_1+\cdots+a_n) \neq 0. \end{cases}
\end{aligned}$$

$$\begin{aligned}
(3)\ E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; u) &= \sum_{t_1,t_2,\ldots,t_n\in R_1^*, \mathrm{Tr}(t_1+t_2+\cdots+t_n)=u} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n) \\
&= \sum_{\substack{t'_1,\ldots,t'_n\in\mathbb{F}_q^*, t''_1,\ldots,t''_n\in\mathbb{F}_q, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=0, \mathrm{Tr}_r^q(t'_1t''_1+\cdots+t'_nt''_n)=1}} \psi_1(t'_1)\chi_{a_1}(t''_1)\cdots\psi_n(t'_n)\chi_{a_n}(t''_n) \\
&= \sum_{\substack{t'_1,\ldots,t'_n\in\mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=0}} \psi_1(t'_1)\cdots\psi_n(t'_n) \sum_{\substack{t''_1,\ldots,t''_n\in\mathbb{F}_q, \\ \mathrm{Tr}_r^q(t'_1t''_1+\cdots+t'_nt''_n)=1}} \chi_{a_1}(t''_1)\cdots\chi_{a_n}(t''_n) \\
&= \sum_{\substack{t'_1,\ldots,t'_n\in\mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=1}} \psi_1(t'_1)\cdots\psi_n(t'_n)B \text{ (By Lemma 3.1.6 (2)).}
\end{aligned}$$

• If $a_1 = \cdots = a_n = 0$, then

$$\begin{aligned}
E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; u) &= \frac{q^n}{r} \sum_{\substack{t'_1,\ldots,t'_n\in\mathbb{F}_q^*, \\ \mathrm{Tr}_r^q(t'_1+\cdots+t'_n)=0}} \psi_1(t'_1)\cdots\psi_n(t'_n) \\
&= \frac{q^n}{r} E_{\mathbb{F}_q}(\psi_1, \psi_2, \ldots, \psi_n; 0).
\end{aligned}$$

• If $a_1 \cdots a_n = 0$, but not all of them are zero, then $E_{R_1}(\psi_1, \psi_2, \ldots, \psi_n; u) = 0$.

• If $a_1\cdots a_n\neq 0$, then $E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;u)$

$$\begin{aligned}
&= \frac{q^n}{r}\sum_{\substack{t_1',\ldots,t_n'\in\mathbb{F}_q^*,\mathrm{Tr}_r^q(t_1'+\cdots+t_n')=0,\\ z=\frac{a_1}{t_1'}=\cdots=\frac{a_n}{t_n'}\in\mathbb{F}_r^*}}\psi_1(t_1')\cdots\psi_n(t_n')\lambda(z)\\
&= \frac{q^n}{r}\sum_{\substack{z\in\mathbb{F}_r^*,\\ \frac{1}{z}\mathrm{Tr}_r^q(a_1+\cdots+a_n)=0}}\psi_1(\frac{a_1}{z})\cdots\psi_n(\frac{a_n}{z})\lambda(z)\\
&= \frac{q^n}{r}\psi_1(a_1)\cdots\psi_n(a_n)\sum_{\substack{z\in\mathbb{F}_r^*,\\ \frac{1}{z}\mathrm{Tr}_r^q(a_1+\cdots+a_n)=0}}(\overline{\psi_1\cdots\psi_n})^*(z)\lambda(z)\\
&= \begin{cases} 0, & \text{if } \mathrm{Tr}_r^q(a_1+\cdots+a_n)\neq 0;\\ \frac{q^n}{r}\psi_1(a_1)\cdots\psi_n(a_n)G_{\mathbb{F}_r}((\overline{\psi_1\cdots\psi_n})^*), & \text{if } \mathrm{Tr}_r^q(a_1+\cdots+a_n)=0.\end{cases}
\end{aligned}$$

This completes the proof of this theorem. ■

From the above theorem, we combine Eqs. (2.2), (2.3) with Lemma 2.1.11, then we can calculate the exact value of the hyper Eisenstein sum $E_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;1)$ over R_1. It is worth mentioning that we obtain a connection between hyper Eisenstein sums of R_1 and Gaussian sums of $\mathbb{F}_q$ when $\psi_1,\psi_2,\ldots,\psi_n$ are not all trivial by [81, Theorem 3]. Therefore, we obtain the following corollary.

Corollary 3.1.8 *Let $\varphi_1,\varphi_2,\ldots,\varphi_n$ be multiplicative characters of R_1 and $\varphi_i:=\psi_i\star\chi_{a_i}$ $(1\leq i\leq n)$, where ψ_i is a multiplicative character of $\mathbb{F}_q$ and χ_{a_i} is an additive character of $\mathbb{F}_q$ with $a_i\in\mathbb{F}_q$. We obtain the following three direct consequences.*

(1) If $\psi_1,\psi_2,\ldots,\psi_n$ are all trivial, then

$$E_{R_1}(\varphi_1,\ldots,\varphi_n;1)=\begin{cases}\frac{q^n((q-1)^n+(-1)^{n+1})}{r^2}, & \text{if } a_1=\cdots=a_n=0;\\ \frac{q^n}{r}, & \text{if } a_1\cdots a_n\neq 0 \text{ and } \mathrm{Tr}_r^q(a_1+\cdots+a_n)\neq 0;\\ 0, & \text{otherwise.}\end{cases}$$

(2) If $\psi_1,\ldots,\psi_h$ are all nontrivial and $\psi_{h+1},\ldots,\psi_n$ are all trivial for $1\leq h\leq n-1$, then $E_{R_1}(\varphi_1,\ldots,\varphi_n;1)$

$$=\begin{cases}\frac{(-1)^{n-h}q^nG_{\mathbb{F}_q}(\psi_1)\cdots G_{\mathbb{F}_q}(\psi_h)}{rG_{\mathbb{F}_r}((\psi_1\cdots\psi_h)^*)}, & \text{if } a_1=\cdots=a_n=0 \text{ and } (\psi_1\cdots\psi_h)^* \text{ is nontrivial;}\\ \frac{(-1)^{n-h+1}q^nG_{\mathbb{F}_q}(\psi_1)\cdots G_{\mathbb{F}_q}(\psi_h)}{r^2}, & \text{if } a_1=\cdots=a_n=0 \text{ and } (\psi_1\cdots\psi_h)^* \text{ is trivial;}\\ \frac{q^n}{r}\psi_1(\frac{a_1}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)})\cdots\psi_h(\frac{a_h}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)}), & \text{if } a_1\cdots a_n\neq 0 \text{ and } \mathrm{Tr}_r^q(a_1+\cdots+a_n)\neq 0;\\ 0, & \text{otherwise.}\end{cases}$$

(3) If $\psi_1, \psi_2, \ldots, \psi_n$ are all nontrivial, then $E_{R_1}(\varphi_1, \ldots, \varphi_n; 1)$

$$= \begin{cases} \frac{q^n G_{\mathbb{F}_q}(\psi_1)\cdots G_{\mathbb{F}_q}(\psi_n)}{r G_{\mathbb{F}_r}((\psi_1\cdots\psi_n)^*)}, & \text{if } a_1 = \cdots = a_n = 0 \text{ and} \\ & (\psi_1\cdots\psi_n)^* \text{ is nontrivial;} \\ -\frac{q^n G_{\mathbb{F}_q}(\psi_1)\cdots G_{\mathbb{F}_q}(\psi_n)}{r^2}, & \text{if } a_1 = \cdots = a_n = 0 \text{ and} \\ & (\psi_1\cdots\psi_n)^* \text{ is trivial;} \\ \frac{q^n}{r}\psi_1(\frac{a_1}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)})\cdots\psi_n(\frac{a_n}{\mathrm{Tr}_r^q(a_1+\cdots+a_n)}), & \text{if } a_1\cdots a_n \neq 0 \text{ and} \\ & \mathrm{Tr}_r^q(a_1+\cdots+a_n) \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

Remark 3.1.9 *Similarly, we can also calculate the exact value of the sums* $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; 0)$ *and* $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; u)$ *over* R_1 *using Lemma 2.1.13.*

In view of the fact that $E_{R_1}(\varphi_1, \ldots, \varphi_n; \mathfrak{s}) = \varphi_1\cdots\varphi_n(\mathfrak{s})E_{R_1}(\varphi_1, \ldots, \varphi_n; 1)$ and Corollary 3.1.8(3), we can determine the absolute value of $E_{R_1}(\varphi_1, \ldots, \varphi_n; \mathfrak{s})$ for all $\mathfrak{s} \in R_{(r)}^*$.

Corollary 3.1.10 *Let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be multiplicative characters of R_1 and $\varphi_i := \psi_i \star \chi_{a_i}$ $(1 \leq i \leq n)$, where ψ_i is a nontrivial multiplicative character of $\mathbb{F}_q$ and χ_{a_i} is an additive character of $\mathbb{F}_q$ with $a_i \in \mathbb{F}_q$. Assume that $(\psi_1\cdots\psi_n)^*$ is the restriction of $\psi_1\cdots\psi_n$ to $\mathbb{F}_r$. Then*

$$|E_{R_1}(\varphi_1, \ldots, \varphi_n; \mathfrak{s})| = \begin{cases} r^{\frac{3}{2}(mn-1)}, & \text{if } a_1 = \cdots = a_n = 0 \text{ and } (\psi_1\cdots\psi_n)^* \text{ is nontrivial;} \\ r^{\frac{3mn-4}{2}}, & \text{if } a_1 = \cdots = a_n = 0 \text{ and } (\psi_1\cdots\psi_n)^* \text{ is trivial;} \\ r^{mn-1}, & \text{if } a_1\cdots a_n \neq 0 \text{ and } \mathrm{Tr}_r^q(a_1+\cdots+a_n) \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

In fact, we can get the value of the sum $E_{R_1}(\varphi_1, \varphi_2, \ldots, \varphi_n; \mathfrak{s})$ when $n = 1$ in Theorem 3.1.7. If $\mathfrak{s} = 1$ and $n = 1$, then the sum $E_{R_1}(\varphi; 1)$ is usually called the Eisenstein sum over R_1, where φ is a multiplicative character of R_1. Hence, we have the following corollary as a special case of Theorem 3.1.7.

Corollary 3.1.11 *Let φ be a multiplicative character of R_1 and $\varphi := \psi \star \chi_a$, where ψ is a multiplicative character of $\mathbb{F}_q$ and χ_a is an additive character of $\mathbb{F}_q$ with $a \in \mathbb{F}_q$. Then*

(1)

$$E_{R_1}(\varphi; 0) = \begin{cases} \frac{q}{r}E_{\mathbb{F}_q}(\psi; 0), & \text{if } a = 0; \\ \frac{q(r-1)}{r}\psi(a), & \text{if } a \neq 0, \mathrm{Tr}_r^q(a) = 0 \text{ and } \psi^* \text{ is trivial;} \\ 0, & \text{otherwise,} \end{cases}$$

where $E_{\mathbb{F}_q}(\psi; 0)$ denotes the sum $E_{\mathbb{F}_q}(\psi; s)$ over $\mathbb{F}_q$ with $s = 0$.

(2)

$$E_{R_1}(\varphi; 1) = \begin{cases} \frac{q}{r}E_{\mathbb{F}_q}(\psi; 1), & \text{if } a = 0; \\ \frac{q}{r}\psi(\frac{a}{\mathrm{Tr}_r^q(a)}), & \text{if } a \neq 0 \text{ and } \mathrm{Tr}_r^q(a) \neq 0; \\ 0, & \text{if } a \neq 0 \text{ and } \mathrm{Tr}_r^q(a) = 0, \end{cases}$$

where $E_{\mathbb{F}_q}(\psi; 1)$ denotes the Eisenstein sum over $\mathbb{F}_q$.

(3)
$$E_{R_1}(\varphi;u)=\begin{cases}\frac{q}{r}E_{\mathbb{F}_q}(\psi;0), & \text{if } a=0;\\ 0, & \text{if } a\neq 0 \text{ and } \mathrm{Tr}_r^q(a)\neq 0;\\ \frac{q}{r}\psi(a)G_{\mathbb{F}_r}(\overline{\psi^*}), & \text{if } a\neq 0 \text{ and } \mathrm{Tr}_r^q(a)=0,\end{cases}$$

where $E_{\mathbb{F}_q}(\psi;0)$ is the sum $E_{\mathbb{F}_q}(\psi;s)$ over $\mathbb{F}_q$ with $s=0$ and $G_{\mathbb{F}_r}(\overline{\psi^*})$ is a Gaussian sum over $\mathbb{F}_r$.

Remark 3.1.12 *In view of the definition of Jacobi sum over $\mathbb{F}_q$ in [130], we have the Jacobi sums $J_{\mathbb{F}_q}(\varphi_1,\varphi_2,\ldots,\varphi_n;1)$ defined by*

$$J_{\mathbb{F}_q}(\varphi_1,\varphi_2,\ldots,\varphi_n;1)=\sum_{x_1,x_2,\ldots,x_n\in\mathbb{F}_q^*,x_1+x_2+\cdots+x_n=1}\varphi_1(x_1)\varphi_2(x_2)\cdots\varphi_n(x_n).$$

Similarly, we can define Jacobi sums over the ring R_1 as follows:

$$J_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;1)=\sum_{t_1,t_2,\ldots,t_n\in R_1^*,t_1+t_2+\cdots+t_n=1}\varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n).$$

Let $q=r^m$ and $r=p^l$. If $m=1$ in Definition 3.1.4, Jacobi sums over R_1 are special types of the hyper Eisenstein sums. Therefore, we have the following corollary, which relates the Jacobi sum $J_R(\varphi_1,\varphi_2,\ldots,\varphi_n;1)$ over the ring R_1.

Corollary 3.1.13 *Let $\varphi_1,\varphi_2,\ldots,\varphi_n$ be multiplicative characters of R_1 and $\varphi_i:=\psi_i\star\chi_{a_i}(1\leq i\leq n)$, where ψ_i and χ_{a_i} are multiplicative and additive characters of $\mathbb{F}_q$, respectively. Then $J_{R_1}(\varphi_1,\varphi_2,\ldots,\varphi_n;1)$*

$$=\begin{cases}q^{n-1}J_{\mathbb{F}_q}(\psi_1,\psi_2,\ldots,\psi_n;1), & \text{if } a_1=\cdots=a_n=0;\\ q^{n-1}\psi_1(\frac{a_1}{a_1+\cdots+a_n})\cdots\psi_n(\frac{a_n}{a_1+\cdots+a_n}), & \text{if } a_1\cdots a_n\neq 0 \text{ and } a_1+\cdots+a_n\neq 0;\\ 0, & \text{otherwise.}\end{cases}$$

where, the Jacobi sum $J_{\mathbb{F}_q}(\psi_1,\psi_2,\ldots,\psi_n;1)$

$$=\begin{cases}\frac{(q-1)^n+(-1)^{n+1}}{q}, & \text{if } \psi_1,\ldots,\psi_n \text{ are trivial;}\\ (-1)^{n-h}\frac{(q-1)^h+(-1)^{h+1}}{q}, & \text{if } \psi_1,\ldots,\psi_h \text{ are nontrivial and } \psi_{h+1},\ldots,\psi_n \text{ are trivial;}\\ \frac{G_{\mathbb{F}_q}(\psi_1)\cdots G_{\mathbb{F}_q}(\psi_n)}{G_{\mathbb{F}_q}(\psi_1\cdots\psi_n)}, & \text{if } \psi_1,\ldots,\psi_n \text{ and } \psi_1\cdots\psi_n \text{ are nontrivial;}\\ -\frac{G_{\mathbb{F}_q}(\psi_1)\cdots G_{\mathbb{F}_q}(\psi_n)}{q}, & \text{if } \psi_1,\ldots,\psi_n \text{ are nontrivial } \psi_1\cdots\psi_n \text{ is trivial.}\end{cases}$$

3.1.3 Constructions of several families of codebooks

In this subsection, we mainly study the applications of character sums over the local ring $R_1=\mathbb{F}_q+u\mathbb{F}_q$ $(u^2=0)$ to the construction of codebooks.

- **Constructions of asymptotically optimal codebooks**

Next, we present several families of asymptotically optimal codebooks constructed using Gaussian sums, hyper Eisenstein sums and Jacobi sums over R_1.

Firstly, we construct several families of asymptotically optimal codebooks from the Gaussian sum over R_1.

Let $\varphi := \psi \star \chi_a$ and $\lambda := \chi_b \star \chi_c$, where $a,b,c \in \mathbb{F}_q, \chi_a, \chi_b, \chi_c \in \widehat{\mathbb{F}}_q$ and $\psi \in \widehat{\mathbb{F}}_q^*$. Assume that $t = t_0(1+ut_1) \in R_1^*$. Then we can define a set $C_0(R_1^*, \widehat{R}_1^* \times \widehat{R}_1)$ as

$$\begin{aligned} C_0(R_1^*, \widehat{R}_1^* \times \widehat{R}_1) &= \left\{ \frac{1}{\sqrt{K}} (\varphi(t)\lambda(t))_{t \in R_1^*}, \varphi \in \widehat{R}_1^*, \lambda \in \widehat{R}_1 \right\} \\ &= \left\{ \frac{1}{\sqrt{K}} (\psi(t_0)\chi_a(t_1)\chi_b(t_0)\chi_c(t_0t_1))_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q}, \psi \in \widehat{\mathbb{F}}_q^*, \chi_a, \chi_b, \chi_c \in \widehat{\mathbb{F}}_q \right\}, \end{aligned}$$

where $K = |R_1^*| = q(q-1)$. According to the definition of the set $C_0(R_1^*, \widehat{R}_1^* \times \widehat{R}_1)$, we will give two constructions of codebooks over R_1.

A. The first construction of codebooks

The codebook $C_1 := C_1(R_1^*, \widehat{R}_1^* \times \widehat{R}_1)$ of length $K_1 = |R_1^*| = q(q-1)$ over R_1 is constructed as:

$$\begin{aligned} C_1 = \Bigg\{ & \frac{1}{\sqrt{K_1}} (\psi(t_0)\chi_a(t_1)\chi_b(t_0)\chi_c(t_0t_1))_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q}, \\ & \psi \text{ is a fixed multiplicative character over } \mathbb{F}_q, \chi_a, \chi_b, \chi_c \in \widehat{\mathbb{F}}_q \Bigg\}. \end{aligned} \tag{3.2}$$

Based on this construction of the codebook C_1, we have the following theorem.

Theorem 3.1.14 *Let C_1 be a codebook defined in (3.2). Then C_1 is a $(q^3, q(q-1))$ codebook having maximum cross-correlation amplitude $I_{\max}(C_1) = \frac{1}{q-1}$. Moreover, the codebook C_1 asymptotically meets the Welch bound.*

Proof: From Eq. (3.2), it is obvious that C_1 has $N_1 = q^3$ codewords of length $K_1 = q(q-1)$. Let $\mathbf{c}_1 = \frac{1}{\sqrt{K_1}} (\psi(t_0)\chi_{a_1}(t_1)\chi_{b_1}(t_0)\chi_{c_1}(t_0t_1))_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q}$, $\mathbf{c}_2 = \frac{1}{\sqrt{K_1}} (\psi(t_0)\chi_{a_2}(t_1)$ $\chi_{b_2}(t_0)\chi_{c_2}(t_0t_1))_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q}$ be any two distinct codewords in C_1. Denote the trivial multiplicative character of $\mathbb{F}_q$ by ψ_0. Let $a = a_1 - a_2, b = b_1 - b_2$ and $c = c_1 - c_2$. Set $\varphi := \psi_0 \star \chi_a$ and $\lambda := \chi_b \star \chi_c$. Then

$$\begin{aligned} K_1 \mathbf{c}_1 \mathbf{c}_2^H &= \sum_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q} \psi(t_0)\chi_{a_1}(t_1)\chi_{b_1}(t_0)\chi_{c_1}(t_0t_1)\overline{\psi(t_0)\chi_{a_2}(t_1)\chi_{b_2}(t_0)\chi_{c_2}(t_0t_1)} \\ &= \sum_{t_0 \in \mathbb{F}_q^*, t_1 \in \mathbb{F}_q} \psi_0(t_0)\chi((a_1-a_2)t_1 + (b_1-b_2)t_0 + (c_1-c_2)t_0t_1) \\ &= \sum_{t_0 \in \mathbb{F}_q^*} \psi_0(t_0)\chi((b_1-b_2)t_0) \sum_{t_1 \in \mathbb{F}_q} \chi((a_1-a_2)t_1 + (c_1-c_2)t_0t_1) \\ &= \sum_{t_0 \in \mathbb{F}_q^*} \psi_0(t_0)\chi(bt_0) \sum_{t_1 \in \mathbb{F}_q} \chi((a+ct_0)t_1) \\ &= \sum_{t_0 \in \mathbb{F}_q^*, a+ct_0=0} \psi_0(t_0)\chi_b(t_0) \\ &= G_{R_1}(\varphi, \lambda). \end{aligned}$$

Since $\mathbf{c}_1 \neq \mathbf{c}_2$, a,b and c are not all equal to 0. In view of Theorem 3.1.1, we have

$$K_1\mathbf{c}_1\mathbf{c}_2^H = \begin{cases} -q, & \text{if } a=0, c=0 \text{ and } b\neq 0; \\ q\chi(-\frac{ab}{c}), & \text{if } a\neq 0 \text{ and } c\neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

Consequently, we infer that $|\mathbf{c}_1\mathbf{c}_2^H| \in \left\{0, \frac{1}{q-1}\right\}$ for any two distinct codewords $\mathbf{c}_1, \mathbf{c}_2$ in C_1. Hence, $I_{\max}(C_1) = \frac{1}{q-1}$.

Next, we show that the codebook C_1 asymptotically meets the Welch bound. The corresponding Welch bound of the codebook C_1 is

$$I_W = \sqrt{\frac{N_1 - K_1}{(N_1-1)K_1}} = \sqrt{\frac{q^3-q(q-1)}{(q^3-1)q(q-1)}} = \sqrt{\frac{q^2-q+1}{q^4-q^3-q+1}}.$$

From $\frac{I_{\max}(C_1)}{I_W} = \sqrt{\frac{q^4-q^3-q+1}{(q^2-q+1)(q-1)^2}}$, we have $\lim\limits_{q\longrightarrow\infty} \frac{I_{\max}(C_1)}{I_W} = 1$, which implies that C_1 asymptotically meets the Welch bound. ■

B. The second construction of codebooks

The codebook $C_2 := C_2(R_1^*, \widehat{R}_1^* \times \widehat{R}_1)$ of length $K_2 = |R_1^*| = q(q-1)$ over R_1 is defined by

$$\begin{aligned} C_2 \;=\; & \Big\{ \frac{1}{\sqrt{K_2}} (\psi(t_0)\chi_a(t_1)\chi_b(t_0)\chi_c(t_0t_1))_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q}, \\ & \psi \in \widehat{\mathbb{F}}_q^*, \chi_b \text{ is a fixed additive character over } \mathbb{F}_q, \chi_a, \chi_c \in \widehat{\mathbb{F}}_q \Big\}. \end{aligned} \tag{3.3}$$

Theorem 3.1.15 *Let C_2 be a codebook defined in (3.3). Then C_2 is a $(q^2(q-1), q(q-1))$ codebook having maximum cross-correlation amplitude $I_{\max}(C_2) = \frac{1}{q-1}$. Moreover, the codebook C_2 asymptotically meets the Welch bound.*

Proof: According to Eq. (3.3), it is easy to see that C_2 has $N_2 = q^2(q-1)$ codewords of length $K_2 = q(q-1)$. Let $\mathbf{c}_1 = \frac{1}{\sqrt{K_2}}(\psi_1(t_0)\chi_{a_1}(t_1)\chi_b(t_0)\chi_{c_1}(t_0t_1))_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q}$ and $\mathbf{c}_2 = \frac{1}{\sqrt{K_2}}(\psi_2(t_0)\chi_{a_2}(t_1)\chi_b(t_0)\chi_{c_2}(t_0t_1))_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q}$ be any two distinct codewords in C_2. Set $\psi = \psi_1\overline{\psi}_2, a = a_1 - a_2$ and $c = c_1 - c_2$. Then

$$\begin{aligned} K_2\mathbf{c}_1\mathbf{c}_2^H &= \sum_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q} \psi_1(t_0)\chi_{a_1}(t_1)\chi_b(t_0)\chi_{c_1}(t_0t_1)\overline{\psi_2(t_0)\chi_{a_2}(t_1)\chi_b(t_0)\chi_{c_2}(t_0t_1)} \\ &= \sum_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q} \psi_1\overline{\psi}_2(t_0)\chi((a_1-a_2)t_1 + (c_1-c_2)t_0t_1) \\ &= \sum_{t_0\in\mathbb{F}_q^*} \psi(t_0) \sum_{t_1\in\mathbb{F}_q} \chi((a+ct_0)t_1) \\ &= q \sum_{t_0\in\mathbb{F}_q^*, a+ct_0=0} \psi(t_0). \end{aligned}$$

- If $a = c = 0$, since $\mathbf{c}_1 \neq \mathbf{c}_2$, it follows that ψ is nontrivial. Then we have
$$K_2 \mathbf{c}_1 \mathbf{c}_2^H = q \sum_{t_0 \in \mathbb{F}_q^*} \psi(t_0) = 0.$$
- If $a = 0, c \neq 0$ or $a \neq 0, c = 0$, then $K_2 \mathbf{c}_1 \mathbf{c}_2^H = 0$.
- If $a \neq 0$ and $c \neq 0$, then $K_2 \mathbf{c}_1 \mathbf{c}_2^H = q\psi(-\frac{a}{c})$.

$$\mathbf{c}_1 \mathbf{c}_2^H = \begin{cases} \frac{q}{K_2}\psi(-\frac{a}{c}), & \text{if } a \neq 0 \text{ and } c \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

Hence, we infer that $|\mathbf{c}_1 \mathbf{c}_2^H| \in \left\{0, \frac{1}{q-1}\right\}$ for any two distinct codewords $\mathbf{c}_1, \mathbf{c}_2$ in C_2. Therefore, $I_{\max}(C_2) = \frac{1}{q-1}$.

The proof is similar to the proof of Theorem 3.1.14, and by calculating, we have $I_W = \sqrt{\frac{q-1}{q^3-q^2-1}}$, and $\lim_{q \longrightarrow \infty} \frac{I_{\max}(C_2)}{I_W} = 1$, i.e., the codebook C_2 asymptotically meets the Welch bound. ■

C. The third construction of codebooks

Next, we present the asymptotically optimal codebooks which are constructed by Eisenstein sums over R_1. Based on this, we first give the following lemma.

Lemma 3.1.16 *Let $G := \{\phi_j : (r-1) \mid j, 0 \leq j \leq q-2\} \subseteq \widehat{\mathbb{F}}_q^*$, where $\phi_j = \phi_1^j$ and ϕ_1 is a generator of $\widehat{\mathbb{F}}_q^*$ with $0 \leq j \leq q-2$. Then G is a subgroup of $\mathbb{F}_q^*$ and $|G| = \frac{q-1}{r-1}$. Moreover, for every $\psi \in \widehat{\mathbb{F}}_q^*$, ψ^* is trivial if and only if $\psi \in G$, where ψ^* denotes the restriction of ψ to $\mathbb{F}_r$.*

Proof: Assume that $\mathbb{F}_q^* = \langle\theta\rangle$, i.e, let θ be a primitive element of $\mathbb{F}_q$. Then $\mathbb{F}_r^* = \langle\theta^{\frac{q-1}{r-1}}\rangle$. We can further assume that $\phi_1(\theta) = \zeta_{q-1}$. Then ψ^* is trivial $\Longleftrightarrow \psi(\theta^{\frac{q-1}{r-1}}) = 1 \Longleftrightarrow \psi(\theta)^{\frac{q-1}{r-1}} = 1 \Longleftrightarrow (\zeta_{q-1}^j)^{\frac{q-1}{r-1}} = 1, 0 \leq j \leq q-2 \Longleftrightarrow (q-1) \mid j\frac{q-1}{r-1} \Longleftrightarrow (r-1) \mid j$. ■

Let
$$D = \{t \in R_1^* : \mathrm{Tr}(t) = 1\} \text{ and } K_3 := |D|.$$
Here, we consider the case that $m = 2$ and $q = r^2$. Hence, it is easy to check that $K_3 = r^2$. Assume that H is a subgroup of $G := \{\phi_j : (r-1) \mid j, 0 \leq j \leq q-2\} \subseteq \widehat{\mathbb{F}}_q^*$ and $k = |H|$. Then $k \mid (r+1)$ since $|G| = \frac{q-1}{r-1} = r+1$.

The the codebook $C_3 := C_3(D, H \times \widehat{\mathbb{F}}_q)$ of length $K_3 = r^2$ over R_1 is built as

$$C_3 : \quad = \quad \left\{ \frac{1}{\sqrt{K_3}}((\psi \star \chi_a)(t))_{t \in D}, \psi \in H, \chi_a \in \widehat{\mathbb{F}}_q \right\}. \tag{3.4}$$

Theorem 3.1.17 *Let C_3 be the codebook defined in (3.4). Then C_3 is a (kr^2, r^2) codebook having maximum cross-correlation amplitude $I_{\max}(C_3) = \frac{1}{r}$. Moreover, the codebook C_3 asymptotically meets the Welch bound.*

Proof: From Eq. (3.4), it is obvious that C_3 has $N_3 = kr^2$ codewords of length $K_3 = r^2$. Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be any two distinct codewords in C_3, where $\mathbf{c}_1 = \frac{1}{\sqrt{K_3}}((\psi_1 \star \chi_{a_1})(t))_{t\in D}$ and $\mathbf{c}_2 = \frac{1}{\sqrt{K_3}}((\psi_2 \star \chi_{a_2})(t))_{t\in D}$. Let $\varphi_1 := \psi_1 \star \chi_{a_1}$ and $\varphi_2 := \psi_2 \star \chi_{a_2}$. Set $\varphi = \varphi_1\overline{\varphi_2}$ and $\varphi := \psi \star \chi_a$. Then

$$\begin{aligned} K_3\mathbf{c}_1\mathbf{c}_2^H &= \sum_{t\in D}(\psi_1 \star \chi_{a_1})(t)\overline{(\psi_2 \star \chi_{a_2})(t)} \\ &= \sum_{t\in R_1^*, \mathrm{Tr(t)}=1} \varphi_1(t)\overline{\varphi_2(t)} \\ &= E_{R_1}(\varphi;1) \\ &= \begin{cases} \frac{q}{p}E_{\mathbb{F}_q}(\psi;1), & \text{if } a = 0; \\ \frac{q}{p}\psi(\frac{a}{\mathrm{Tr}_r^q(a)}), & \text{if } a \neq 0 \text{ and } \mathrm{Tr}(a) \neq 0; \text{ (By Corollary 3.1.11 (2))} \\ 0, & \text{if } a \neq 0 \text{ and } \mathrm{Tr}(a) = 0. \end{cases} \end{aligned}$$

Since $\mathbf{c}_1 \neq \mathbf{c}_2$, it follows that ψ and χ_a are not all trivial. In view of Corollary 3.1.10 ($n = 1, m = 2$), we have

$$K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} r^{\frac{3}{2}}, & \text{if } a = 0, \psi \text{ and } \psi^* \text{ are nontrivial;} \\ 0, & \text{if } a \neq 0, \mathrm{Tr}_r^q(a) = 0 \text{ and } \psi \text{ is an arbitrary multiplicative character of } \mathbb{F}_q; \\ r, & \text{otherwise.} \end{cases}$$

Since $H \leq G$, which implies that ψ^* is trivial (by Lemma 3.1.16), we infer that $|\mathbf{c}_1\mathbf{c}_2^H| \in \left\{0, \frac{1}{r}\right\}$ for any $\mathbf{c}_1, \mathbf{c}_2 \in C_3$. Hence, $I_{\max}(C_3) = \frac{1}{r}$.

An argument analogous to the one given in the proof of Theorem 3.1.14 establishes that $I_W = \sqrt{\frac{k-1}{kr^2-1}}$, and then $\lim_{q\longrightarrow\infty} \frac{I_{\max}(C_3)}{I_W} = 1$. Hence, the codebook C_3 asymptotically meets the Welch bound. ■

D. The fourth construction of codebooks

In the following, we present the asymptotically optimal codebooks which are constructed using Jacobi sums over R_1. Now, we consider the case that $n = 2$ and $m = 1$. Let $t_1 = t_1'(1 + ut_1'')$ and $t_2 = t_2'(1 + ut_2'') \in R_1^*$. We define

$$\begin{aligned} D' &= \{t_1, t_2 \in R_1^* : t_1 + t_2 = 1\} \\ &= \{t_1', t_2' \in \mathbb{F}_q^*, t_1'', t_2'' \in \mathbb{F}_q : t_1' + t_2' = 1, t_1't_1'' + t_2't_2'' = 0\} \text{ and } K_4 := |D'|. \end{aligned}$$

The codebook $C_4 := C_4(D', \widehat{R}_1^* \times \widehat{R}_1^*)$ of length K_4 over R_1 is assembled as

$$\begin{aligned} C_4 = \Bigg\{ & \frac{1}{\sqrt{K_4}}(\varphi_1(t_1)\varphi_2(t_2))_{t_1,t_2\in D'}, \varphi_1 = \psi_1 \star \chi_{a_1}, \varphi_2 = \psi_2 \star \chi_{a_2}, \\ & \psi_1 \text{ is a fixed multiplicative character over } \mathbb{F}_q, \psi_2 \in \widehat{\mathbb{F}}_q^*, \chi_{a_1}, \chi_{a_2} \in \widehat{\mathbb{F}}_q \Bigg\} \end{aligned} \quad (3.5)$$

Theorem 3.1.18 *Let C_4 be the codebook defined in (3.5). Then C_4 is a $(q^2(q-1), q(q-2))$ codebook having maximum cross-correlation amplitude $I_{\max}(C_4) = \frac{1}{q-2}$. Moreover, the codebook C_4 asymptotically meets the Welch bound.*

Proof: According to Eq. (3.5), it is obvious that C_4 has $N_4 = q^2(q-1)$ codewords of length $K_4 = q(q-2)$. Let $\mathbf{c}_1 = \frac{1}{\sqrt{K_4}}(\psi_1(t_1')\chi_{a_1}(t_1'')\psi_2(t_2')\chi_{a_2}(t_2''))_{t_1',t_2' \in \mathbb{F}_q^*, t_1'', t_2'' \in \mathbb{F}_q}$ and $\mathbf{c}_2 = \frac{1}{\sqrt{K_4}}(\psi_1(t_1')\chi_{b_1}(t_1'')\psi_3(t_2')\chi_{b_2}(t_2''))_{t_1',t_2' \in \mathbb{F}_q^*, t_1'', t_2'' \in \mathbb{F}_q}$ be any two distinct codewords in C_4. Denote the trivial multiplicative character of $\mathbb{F}_q$ by ψ_0. Let $a = a_1 - b_1$ and $b = a_2 - b_2$. Set $\varphi_1 = \psi_0 \star \chi_a$ and $\varphi_2 = \psi_2\overline{\psi_3} \star \chi_b$. Then

$$\begin{aligned}
K_4\mathbf{c}_1\mathbf{c}_2^H &= \sum_{\substack{t_1',t_2' \in \mathbb{F}_q^*, t_1'', t_2'' \in \mathbb{F}_q, \\ t_1'+t_2'=1, t_1't_1''+t_2't_2''=0}} \psi_1(t_1')\chi_{a_1}(t_1'')\psi_2(t_2')\chi_{a_2}(t_2'')\overline{\psi_1(t_1')\chi_{b_1}(t_1'')\psi_3(t_2')\chi_{b_2}(t_2'')} \\
&= \sum_{\substack{t_1',t_2' \in \mathbb{F}_q^*, t_1'', t_2'' \in \mathbb{F}_q, \\ t_1'+t_2'=1, t_1't_1''+t_2't_2''=0}} \psi_0(t_1')\chi((a_1-b_1)t_1'')\psi_2\overline{\psi_3}(t_2')\chi((a_2-b_2)t_2'') \\
&= \sum_{\substack{t_1,t_2 \in R_1^*, \\ t_1+t_2=1}} \varphi_1(t_1)\varphi_2(t_2) \\
&= J_{R_1}(\varphi_1,\varphi_2).
\end{aligned}$$

According to Corollary 3.1.13 $(n = 2)$, we have

$$K_4\mathbf{c}_1\mathbf{c}_2^H = \begin{cases} -q, & \text{if } a = b = 0; (\text{since } \mathbf{c}_1 \neq \mathbf{c}_2, \psi_2\overline{\psi_3} \text{ is nontrivial}) \\ q\psi_2\overline{\psi_3}(\frac{a}{a+b}), & \text{if } a \neq 0, b \neq 0 \text{ and } a \neq -b; \\ 0, & \text{otherwise.} \end{cases}$$

Consequently, we infer that $|\mathbf{c}_1\mathbf{c}_2^H| \in \{0, \frac{1}{q-2}\}$ for any two distinct codewords $\mathbf{c}_1, \mathbf{c}_2$ in C_4. Hence, $I_{\max}(C_4) = \frac{1}{q-2}$.

The proof is similar to the proof of Theorem 3.1.14, and then obtain that the codebook C_4 asymptotically meets the Welch bound. ■

• Constructions of optimal codebooks

Next, we study a class of codebooks achieving the Welch bound that can be constructed using quadratic Gaussian sums over $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$, where $q = 2^m$.

From Subsection 3.1.2, when $p = 2$, we know that the quadratic character of R_1 is $\rho = \psi_0 \star \chi_a$ $(a \in \mathbb{F}_q^*)$. Assume that $\lambda := \chi_b \star \chi_c$, $t = t_0(1 + ut_1)$, where $b, c, t_1 \in \mathbb{F}_q$, $t_0 \in \mathbb{F}_q^*$. Let

$$D'' = \{t \in R_1^* : \rho(t) = -1\} \text{ and } K_5 = |D''|,$$

where $\rho := \psi_0 \star \chi_a$ is the quadratic multiplicative character of R_1 with $a \in \mathbb{F}_q^*$ and $\eta(0)$ is defined as 0 for convenience.

The codebook $C_5 := C_5(D'', \widehat{R}_1)$ of length K_5 over R_1 is defined by

$$C_5 = \left\{ \frac{1}{\sqrt{K_5}}(\lambda(t))_{t \in D''}, \lambda \in \widehat{R}_1 \right\}. \tag{3.6}$$

Theorem 3.1.19 *Let C_5 be a codebook defined in (3.6). Then C_5 is a $(q^2, \frac{q(q-1)}{2})$ codebook having maximum cross-correlation amplitude $I_{\max}(C_5) = \frac{1}{q-1}$. Moreover, the codebook C_5 meets the Welch bound.*

Proof: In the light of the definition of C_5, it is easy to see that C_5 has $N_5 = q^2$ codewords of length $K_5 = |D''| = \frac{q(q-1)}{2}$. Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be any two distinct codewords in C_5, where $\mathbf{c}_1 = \frac{1}{\sqrt{K_5}}(\lambda_1(t))_{t\in D''}$ and $\mathbf{c}_2 = \frac{1}{\sqrt{K_5}}(\lambda_2(t))_{t\in D''}$. Denote the trivial multiplicative character of $\mathbb{F}_q$ by ψ_0. Let $b = b_1 - b_2$ and $c = c_1 - c_2$. Set $\rho := \psi_0 \star \chi_a$ and $\lambda := \chi_b \star \chi_c$. Then

$$\begin{aligned}
K_5\mathbf{c}_1\mathbf{c}_2^H &= \sum_{t\in D''} \lambda_1(t)\overline{\lambda_2(t)} \\
&= \sum_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q} \chi_{b_1}(t_0)\chi_{c_1}(t_0t_1)\overline{\chi_{b_2}(t_0)\chi_{c_2}(t_0t_1)}\frac{1-\psi_0(t_0)\chi_a(t_1)}{2} \\
&= \sum_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q} \chi((b_1-b_2)t_0)\chi((c_1-c_2)t_0t_1)\frac{1-\psi_0(t_0)\chi_a(t_1)}{2} \\
&= \sum_{t_0\in\mathbb{F}_q^*, t_1\in\mathbb{F}_q} \chi_b(t_0)\chi_c(t_0t_1)\frac{1-\psi_0(t_0)\chi_a(t_1)}{2} \\
&= \frac{1}{2}\sum_{t_0\in\mathbb{F}_q^*}\chi_b(t_0)\sum_{t_1\in\mathbb{F}_q}\chi_c(t_0t_1) - \frac{1}{2}G_{R_1}(\rho,\lambda).
\end{aligned}$$

Since $\mathbf{c}_1 \neq \mathbf{c}_2$, b and c are not both equal to 0. Then we have

$$\sum_{t_0\in\mathbb{F}_q^*}\chi_b(t_0)\sum_{t_1\in\mathbb{F}_q}\chi_c(t_0t_1) = \begin{cases} -q, & \text{if } b\neq 0 \text{ and } c = 0; \\ 0, & \text{if } c\neq 0. \end{cases}$$

In view of Corollary 3.1.3, we have

$$G_{R_1}(\rho,\lambda) = \begin{cases} q\chi(-\frac{ab}{c}), & \text{if } c\neq 0; \\ 0, & \text{if } c = 0. \end{cases}$$

Hence,

$$K_5\mathbf{c}_1\mathbf{c}_2^H = \begin{cases} -\frac{1}{2}q, & \text{if } c = 0; \\ -\frac{1}{2}q\chi(-\frac{ab}{c}), & \text{if } c\neq 0. \end{cases}$$

Therefore, we get $|\mathbf{c}_1\mathbf{c}_2^H| = \frac{1}{q-1}$ for any two distinct codewords $\mathbf{c}_1, \mathbf{c}_2$ in C_5. Hence, $I_{\max}(C_5) = \frac{1}{q-1}$.

Next, we prove that the codebook C_5 meets the Welch bound. The corresponding Welch bound of the codebook C_5 is

$$I_W = \sqrt{\frac{N_5 - K_5}{(N_5-1)K_5}} = \sqrt{\frac{q^2 - \frac{1}{2}q(q-1)}{(q^2-1)\frac{1}{2}q(q-1)}} = \frac{1}{q-1}.$$

It follows that $\frac{I_{\max}(C_5)}{I_W} = 1$. Obviously, C_5 meets the Welch bound. ■

Remark 3.1.20 *(1) Let the set $\xi_{\mathfrak{n}}$ be the standard basis of the $\mathfrak{n}$-dimensional Hilbert space which is given by the rows of the identity matrix $I_{\mathfrak{n}}$. Let $\widetilde{C}_i = C_i \cup \xi_{K_i}$, where $i = 1,2,3,4$. Then the codebooks $\widetilde{C}_i$ are also asymptotically optimal and their parameters are as follows.*

(i) $\widetilde{N}_1 = N_1 + K_1 = q(q^2+q+1), \widetilde{K}_1 = K_1 = q(q-1)$ *and* $I_{\max}(\widetilde{C}_1) = I_{\max}(C_1) = \frac{1}{q-1}$.

(ii) $\widetilde{N}_2 = N_2 + K_2 = q(q^2-1), \widetilde{K}_2 = K_2 = q(q-1)$ *and* $I_{\max}(\widetilde{C}_2) = I_{\max}(C_2) = \frac{1}{q-1}$.

(iii) $\widetilde{N}_3 = N_3 + K_3 = kr^2 + r^2, \widetilde{K}_3 = K_3 = r^2$ *and* $I_{\max}(\widetilde{C}_3) = I_{\max}(C_3) = \frac{1}{r}$.

(iv) $\widetilde{N}_4 = N_4 + K_4 = q(q^2-2), \widetilde{K}_4 = K_4 = q(q-2)$ *and* $I_{\max}(\widetilde{C}_4) = I_{\max}(C_4) = \frac{1}{q-2}$.

The parameters of the codebooks $\widetilde{C}_1, \widetilde{C}_3, \widetilde{C}_4$ are new. The proof of this result is similar to the proof of [79, Theorem 4.1], so we omit the detail here.

(2) In Table 3.3.1, we list the parameters of some known classes of asymptotically optimal codebooks with respect to the Welch bound. By a comparison, we find that the parameters of codebooks obtained in Theorems 3.1.14, 3.1.17 and 3.1.18 are new.

3.2 Constructions of codebooks using character sums over $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$

Let $\mathbb{F}_q$ denote the finite field and $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, where q is a power of a prime p. Let the non-chain ring $R_2 = \mathbb{F}_q + u\mathbb{F}_q = \{\alpha + \beta u : \alpha, \beta \in \mathbb{F}_q\}(u^2 = u)$ having maximal ideals $\langle 1-u \rangle$ and $\langle u \rangle$. The ring R_2 is equivalent to the ring $\frac{\mathbb{F}_q[u]}{\langle u^2-u \rangle}$. In fact, $R_2 = u\mathbb{F}_q \oplus (1-u)\mathbb{F}_q \simeq \mathbb{F}_q^2$ is a two-dimensional vector space over $\mathbb{F}_q$ and $|R_2| = q^2$. The invertible elements of R_2 are

$$R_2^* = u\mathbb{F}_q^* \oplus (1-u)\mathbb{F}_q^* = \{u\alpha + (1-u)\beta : \alpha, \beta \in \mathbb{F}_q^*\}.$$

It is obvious that $|R_2^*| = (q-1)^2$.

3.2.1 Characters of R_2

In this subsection, we give the additive and multiplicative characters of R_2, which will be helpful for us to employ some character sums over the ring R_2 in the sequel.

A. Additive characters of R_2

Define $\lambda : R_2 \longrightarrow \mathbb{C}^*$ as the additive character of the finite non-chain R_2 satisfying $\lambda(r_1 + r_2) = \lambda(r_1)\lambda(r_2)$ for any $r_1, r_2 \in R_2$. Hence, the group of additive characters of R_2 is $\widehat{R}_2 := \{\lambda : R_2 \longrightarrow \mathbb{C}^* \mid \lambda(r_1 + r_2) = \lambda(r_1)\lambda(r_2), r_1, r_2 \in R_2\}$.

For any $ua_0 + (1-u)a_1 \in R_2$, we have $\lambda(ua_0 + (1-u)a_1) = \lambda(ua_0)\lambda((1-u)a_1)$. Define two mappings λ' and λ'' as follows: The mapping $\lambda' : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ is defined as

$$\lambda'(c) := \lambda(uc)$$

for $c \in \mathbb{F}_q$; and the mapping $\lambda'' : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ is defined as

$$\lambda''(c) := \lambda((1-u)c)$$

for $c \in \mathbb{F}_q$. Therefore, it is easy to prove that $\lambda'(c_1+c_2) = \lambda'(c_1)\lambda'(c_2)$ and $\lambda''(c_1+c_2) = \lambda''(c_1)\lambda''(c_2)$ for $c_1, c_2 \in \mathbb{F}_q$. It follows that λ' and λ'' are additive characters of $\mathbb{F}_q$. Thus, there exist $a, b \in \mathbb{F}_q$ such that

$$\lambda'(x) = \zeta_p^{\mathrm{Tr}_p^q(ax)} = \chi_a(x), \lambda''(x) = \zeta_p^{\mathrm{Tr}_p^q(bx)} = \chi_b(x),$$

where $\mathrm{Tr}_p^q(\cdot)$ denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$, and $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity over $\mathbb{F}_q$. Therefore, we can express an additive character of R_2 as follows:

$$\begin{aligned} \lambda(ua_0 + (1-u)a_1) &= \lambda'(a_0)\lambda''(a_1) \\ &= \chi_a(a_0)\chi_b(a_1). \end{aligned}$$

Thus, there is an one-to-one correspondence:

$$\begin{aligned} \tau : (\widehat{R}_2, +) &\longrightarrow (\widehat{\mathbb{F}}_q, +) \times (\widehat{\mathbb{F}}_q, +), \\ \lambda &\longmapsto (\chi_a, \chi_b), \end{aligned}$$

where $\widehat{\mathbb{F}}_q$ denotes the group of additive characters of $\mathbb{F}_q$. It is easy to check that the mapping τ is an isomorphism.

B. Multiplicative characters of R_2

The structure of the multiplicative group R_2^* is $R_2^* = u\mathbb{F}_q^* \oplus (1-u)\mathbb{F}_q^*$. Then the invertible elements of R_2 are can be represented as

$$\begin{aligned} R_2^* &= \{ua_0 + (1-u)a_1 : a_0, a_1 \in \mathbb{F}_q^*\} \\ &= \{(ua_0 + (1-u))(u + (1-u)a_1) : a_0, a_1 \in \mathbb{F}_q^*\}. \end{aligned}$$

Define $\varphi : R_2^* \longrightarrow \mathbb{C}^*$ as the additive character of the finite non-chain R_2 satisfying $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$ for any $r_1, r_2 \in R_2^*$. Therefore, the group of multiplicative characters of R_2 is $\widehat{R}_2^* := \{\varphi : R_2^* \longrightarrow \mathbb{C}^* \mid \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2), r_1, r_2 \in R_2^*\}$.

For any $(ua_0 + (1-u))(u + (1-u)a_1) \in R_2^*$, we have $\varphi((ua_0 + (1-u))(u + (1-u)a_1)) = \varphi(ua_0 + (1-u))\varphi(u + (1-u)a_1)$. Define two mappings φ' and φ'' as follows: The mapping $\varphi' : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ is defined as

$$\varphi'(c) := \varphi(uc + (1-u))$$

for $c \in \mathbb{F}_q^*$; and the mapping $\varphi'' : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ is defined as

$$\varphi''(c) := \varphi(u + (1-u)c)$$

for $c \in \mathbb{F}_q^*$.

For any $c_1, c_2 \in \mathbb{F}_q^*$, we have

$$\begin{aligned} \varphi'(c_1 c_2) &= \varphi(uc_1 c_2 + (1-u)) \\ &= \varphi(uc_1 + (1-u))\varphi(uc_2 + (1-u)) \\ &= \varphi'(c_1)\varphi'(c_2), \end{aligned}$$

and

$$\begin{aligned}\varphi''(c_1c_2) &= \varphi(u+(1-u)c_1c_2)\\ &= \varphi((u+(1-u)c_1)(u+(1-u)c_2))\\ &= \varphi(u+(1-u)c_1)\varphi(u+(1-u)c_2)\\ &= \varphi''(c_1)\varphi''(c_2).\end{aligned}$$

In view of these, we can obtain that φ' and φ'' are multiplicative characters of $\mathbb{F}_q$. Hence, we can describe a multiplicative character of R_2 as follows:

$$\varphi((ua_0+(1-u))(u+(1-u)a_1)) = \varphi'(a_0)\varphi''(a_1).$$

Moreover, we have

$$\begin{aligned}\sigma : (\widehat{R}_2^*, \times) &\longrightarrow (\widehat{\mathbb{F}}_q^*, \times) \times (\widehat{\mathbb{F}}_q^*, \times),\\ \varphi &\longmapsto (\varphi', \varphi''),\end{aligned}$$

where $\widehat{\mathbb{F}}_q^*$ denotes the group of multiplicative characters of $\mathbb{F}_q$. One can show that the mapping σ is an isomorphism.

3.2.2 Character sums over R_2

This subsection introduces Gaussian sums, Jacobi sums, and hyper Eisenstein sums over the finite non-chain ring R_2 and presents some fundamental properties of these character sums.

A. Gaussian sums over R_2

Let λ and φ be an additive character and a multiplicative character of $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$, respectively. The Gaussian sum for λ and φ of R_2 is defined by

$$G_{R_2}(\varphi, \lambda) = \sum_{t \in R_2^*} \varphi(t)\lambda(t).$$

Let $\varphi := \varphi' \star \varphi''$ and $\lambda := \chi_a \star \chi_b$. From Subsection 3.2.1, we denote $\varphi := \varphi' \star \varphi''$ and $\lambda := \chi_a \star \chi_b$, namely, for any $t = ut_0 + (1-u)t_1 \in R_2$, $\varphi(t) = \varphi'(t_0)\varphi''(t_1)$ and $\lambda(t) = \chi_a(t_0)\chi_b(t_1)$, where $\varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*, \chi_a, \chi_b \in \widehat{\mathbb{F}}_q$ and $a, b \in \mathbb{F}_q$. Moreover, we have $G_{R_2}(\varphi, \lambda) := G_{R_2}(\varphi' \star \varphi'', \chi_a \star \chi_b)$.

Next, we give the relationship between the Gaussian sum over the finite non-chain ring R_2 and the Gaussian sum over the finite filed $\mathbb{F}_q$.

Theorem 3.2.1 *Let φ be a multiplicative character and λ be an additive character of R_2, where $\varphi := \varphi' \star \varphi'', \lambda := \chi_a \star \chi_b, \varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*, \chi_a, \chi_b \in \widehat{\mathbb{F}}_q$ and $a, b \in \mathbb{F}_q$. Then the Gaussian sum $G_{R_2}(\varphi, \lambda)$ over R_2 satisfies*

$$G_{R_2}(\varphi, \lambda) = G_{\mathbb{F}_q}(\varphi', \chi_a) G_{\mathbb{F}_q}(\varphi'', \chi_b), \tag{3.7}$$

where $G_{\mathbb{F}_q}(\varphi', \chi_a)$ and $G_{\mathbb{F}_q}(\varphi'', \chi_b)$ are Gaussian sums over $\mathbb{F}_q$.

Proof: Assume that $t = ut_0 + (1-u)t_1$, where $t_0, t_1 \in \mathbb{F}_q^*$.

$$\begin{aligned} G_{R_2}(\varphi,\lambda) &= \sum_{t\in R_2^*} \varphi(t)\lambda(t) \\ &= \sum_{t_0\in\mathbb{F}_q^*} \varphi'(t_0)\chi_a(t_0) \sum_{t_1\in\mathbb{F}_q^*} \varphi''(t_1)\chi_b(t_1) \\ &= G_{\mathbb{F}_q}(\varphi',\chi_a)G_{\mathbb{F}_q}(\varphi'',\chi_b). \end{aligned}$$

This completes the proof. ■

Remark 3.2.2 *In Theorem 3.2.1, Eq. (3.7) establishes the relationship between the Gaussian sum over R_2 and the Gaussian sum over $\mathbb{F}_q$. From Lemma 2.1.7, we can determine the absolute value of the Gaussian sum $G_{R_2}(\varphi,\lambda) := G_{R_2}(\varphi'\star\varphi'', \chi_a\star\chi_b)$ over R_2. Based on the hypothesis in Theorem 3.2.1, we have*

$$|G_{R_2}(\varphi,\lambda)| = \begin{cases} (q-1)^2, & \text{if } \varphi',\varphi'',\chi_a \text{ and } \chi_b \text{ are all trivial;} \\ q-1, & \text{if } \varphi',\varphi'',\chi_a \text{ are all trivial and } \chi_b \text{ is nontrivial} \\ & \text{(or } \varphi',\varphi'',\chi_b \text{ are all trivial and } \chi_a \text{ is nontrivial);} \\ (q-1)\sqrt{q}, & \text{if } \varphi',\chi_a \text{ are all trivial and } \varphi'',\chi_b \text{ are all nontrivial} \\ & \text{(or } \varphi',\chi_a \text{ are all nontrivial and } \varphi'',\chi_b \text{ are all trivial);} \\ 1, & \text{if } \varphi',\varphi'' \text{ are all trivial and } \chi_a,\chi_b \text{ are all nontrivial;} \\ \sqrt{q}, & \text{if } \varphi' \text{ is trivial and } \varphi'',\chi_a,\chi_b \text{ are all nontrivial} \\ & \text{(or } \varphi'' \text{ is trivial and } \varphi',\chi_a,\chi_b \text{ are all nontrivial);} \\ q, & \text{if } \varphi',\varphi'',\chi_a \text{ and } \chi_b \text{ are all nontrivial;} \\ 0, & \text{otherwise.} \end{cases}$$

B. Hyper Eisenstein sums over R_2

Let $R_2 = \mathbb{F}_q + u\mathbb{F}_q$, $R_{(l)} = \mathbb{F}_l + u\mathbb{F}_l$ and $q = l^m (m \geq 1$ is a positive integer), where $u^2 = u$ and l is a power of a prime p. Any element $\alpha + u\beta$ in R_2 can be expressed in form $u\alpha + (1-u)\beta$, define the trace mapping:

$$\begin{aligned} \mathrm{Tr}_{R_{(l)}}^{R_2} : \ R_2 &\longrightarrow R_{(l)}, \\ \mathrm{Tr}_{R_{(l)}}^{R_2}(u\alpha+(1-u)\beta) &= u\mathrm{Tr}_l^q(\alpha) + (1-u)\mathrm{Tr}_l^q(\beta). \end{aligned}$$

For convenience, $\mathrm{Tr}_{R_{(l)}}^{R_2}$ is abbreviated as Tr.

Next, we present the definition of the hyper Eisenstein sum over R_2.

Definition 3.2.3 *Let n be a positive integer and $\varphi_1,\varphi_2,\ldots,\varphi_n$ be multiplicative characters of R_2. Then the hyper Eisenstein sum for $\varphi_1,\varphi_2,\ldots,\varphi_n$ over R_2 is defined by*

$$E_{R_2}(\varphi_1,\varphi_2,\ldots,\varphi_n;1) = \sum_{\substack{t_1,t_2,\ldots,t_n\in R_2^*, \\ \mathrm{Tr}(t_1+t_2+\cdots+t_n)=1}} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n). \tag{3.8}$$

As an extension, we can define $E_{R_2}(\varphi_1,\varphi_2,\ldots,\varphi_n;r)$ as follows:

$$E_{R_2}(\varphi_1,\varphi_2,\ldots,\varphi_n;r) = \sum_{t_1,t_2,\ldots,t_n\in R_2^*, \mathrm{Tr}(t_1+t_2+\cdots+t_n)=r} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n)$$

for each $r \in R_{(l)}$.

In the following, we calculate the value of $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r)$.

Theorem 3.2.4 *Let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be multiplicative characters of R_2 and $\varphi_i := \varphi_i' \star \varphi_i''(1 \le i \le n)$, where φ_i' and φ_i'' are multiplicative characters of $\mathbb{F}_q$. Then*

$$E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) = E_{\mathbb{F}_q}(\varphi_1', \varphi_2', \ldots, \varphi_n'; r_1) E_{\mathbb{F}_q}(\varphi_1'', \varphi_2'', \ldots, \varphi_n''; r_2),$$

where $r = ur_1 + (1-u)r_2 \in R_{(l)}$.

Proof: Let $t_1, t_2, \ldots, t_n \in R_2^*$, where $t_i = ut_i' + (1-u)t_i''$, $1 \le i \le n$. Then

$$\begin{aligned}
E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) &= \sum_{t_1, t_2, \ldots, t_n \in R_2^*, \mathrm{Tr}(t_1 + t_2 + \cdots + t_n) = r} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n) \\
&= \sum_{\substack{t_1', \ldots, t_n' \in \mathbb{F}_q^*, t_1'', \ldots, t_n'' \in \mathbb{F}_q^*, \\ \mathrm{Tr}_l^q(t_1' + \cdots + t_n') = r_1, \mathrm{Tr}_l^q(t_1'' + \cdots + t_n'') = r_2}} \varphi_1'(t_1')\varphi_1''(t_1'')\cdots\varphi_n'(t_n')\varphi_n''(t_n'') \\
&= \sum_{\substack{t_1', \ldots, t_n' \in \mathbb{F}_q^*, \\ \mathrm{Tr}_l^q(t_1' + \cdots + t_n') = r_1}} \varphi_1'(t_1')\cdots\varphi_n'(t_n') \sum_{\substack{t_1'', \ldots, t_n'' \in \mathbb{F}_q, \\ \mathrm{Tr}_l^q(t_1'' + \cdots + t_n'') = r_2}} \varphi_1''(t_1'')\cdots\varphi_n''(t_n'') \\
&= E_{\mathbb{F}_q}(\varphi_1', \varphi_2', \ldots, \varphi_n'; r_1) E_{\mathbb{F}_q}(\varphi_1'', \varphi_2'', \ldots, \varphi_n''; r_2).
\end{aligned}$$

Hence, the proof of this theorem is completed. ■

Remark 3.2.5 *In Theorem 3.2.4, it is easy to show the following four direct consequences.*

(1) *If $r \in R_{(l)}^*$, then $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) = (\varphi_1' \cdots \varphi_n')(r_1)(\varphi_1'' \cdots \varphi_n'')(r_2) E_{\mathbb{F}_q}(\varphi_1', \ldots, \varphi_n'; 1) E_{\mathbb{F}_q}(\varphi_1'', \ldots, \varphi_n''; 1)$;*

(2) *If $r = ur_1 \in u\mathbb{F}_l^*$, then $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) = (\varphi_1' \cdots \varphi_n')(r_1) E_{\mathbb{F}_q}(\varphi_1', \ldots, \varphi_n'; 1)$ $E_{\mathbb{F}_q}(\varphi_1'', \ldots, \varphi_n''; 0)$;*

(3) *If $r = (1-u)r_2 \in (1-u)\mathbb{F}_l^*$, then $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) = (\varphi_1'' \cdots \varphi_n'')(r_2) E_{\mathbb{F}_q}(\varphi_1', \ldots, \varphi_n'; 0) E_{\mathbb{F}_q}(\varphi_1'', \ldots, \varphi_n''; 1)$;*

(4) *If $r = 0$, then $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; r) = E_{\mathbb{F}_q}(\varphi_1', \ldots, \varphi_n'; 0) E_{\mathbb{F}_q}(\varphi_1'', \ldots, \varphi_n''; 0)$.*

Hence, according to Eqs. (2.2), (2.3) and Lemmas 2.1.11, 2.1.13, we can get the exact value of $E_{R_2}(\varphi_1, \varphi_2, \cdots, \varphi_n; r)$.

From Theorem 3.2.4, and combining Eqs. (2.2), (2.3) with Lemma 2.1.11, we can calculate the exact value of the hyper Eisenstein sum $E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1)$ over R_2.

Corollary 3.2.6 *Let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be multiplicative characters of R_2 and $\varphi_i := \varphi_i' \star \varphi_i''$ $(1 \le i \le n)$, where φ_i' and φ_i'' are multiplicative characters of $\mathbb{F}_q$. We obtain the following several direct consequences.*

(1) If $\varphi_1', \ldots, \varphi_n'$ and $\varphi_1'', \ldots, \varphi_n''$ are all trivial, then $E_{R_2}(\varphi_1, \ldots, \varphi_n; 1) = \frac{((q-1)^n + (-1)^{n+1})^2}{l^2}$.

(2) If $\varphi'_1,\ldots,\varphi'_n,\varphi''_{h+1},\ldots,\varphi''_n$ are all trivial and $\varphi''_1,\ldots,\varphi''_h$ are all nontrivial $(1\le h\le n-1)$*, then* $E_{R_2}(\varphi_1,\ldots,\varphi_n;1)=$

$$\begin{cases}\dfrac{(-1)^{n-h+1}((q-1)^n+(-1)^{n+1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_h)}{l^2}, & \text{if } (\varphi''_1\cdots\varphi''_h)^* \text{ is trivial;}\\ \dfrac{(-1)^{n-h}((q-1)^n+(-1)^{n+1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_h)}{lG_{\mathbb{F}_l}((\varphi''_1\cdots\varphi''_h)^*)}, & \text{if } (\varphi''_1\cdots\varphi''_h)^* \text{ is nontrivial.}\end{cases}$$

(3) If $\varphi'_1,\ldots,\varphi'_n$ are all trivial and $\varphi''_1,\ldots,\varphi''_n$ are all nontrivial, then

$$E_{R_2}(\varphi_1,\ldots,\varphi_n;1)=\begin{cases}-\dfrac{((q-1)^n+(-1)^{n+1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_n)}{l^2}, & \text{if } (\varphi''_1\cdots\varphi''_n)^* \text{ is trivial;}\\ \dfrac{((q-1)^n+(-1)^{n+1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_n)}{lG_{\mathbb{F}_l}((\varphi''_1\cdots\varphi''_n)^*)}, & \text{if } (\varphi''_1\cdots\varphi''_n)^* \text{ is nontrivial.}\end{cases}$$

(4) If $\varphi'_1,\ldots,\varphi'_h$ are all nontrivial and $\varphi'_{h+1},\ldots,\varphi'_n,\varphi''_1,\ldots,\varphi''_n$ are all trivial $(1\le h\le n-1)$*, then* $E_{R_2}(\varphi_1,\ldots,\varphi_n;1)=$

$$\begin{cases}\dfrac{(-1)^{n-h+1}((q-1)^n+(-1)^{n+1})G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_h)}{l^2}, & \text{if } (\varphi'_1\cdots\varphi'_h)^* \text{ is trivial;}\\ \dfrac{(-1)^{n-h}((q-1)^n+(-1)^{n+1})G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_h)}{lG_{\mathbb{F}_l}((\varphi'_1\cdots\varphi'_h)^*)}, & \text{if } (\varphi'_1\cdots\varphi'_h)^* \text{ is nontrivial.}\end{cases}$$

(5) If $\varphi'_1,\ldots,\varphi'_{h_1},\varphi''_1,\ldots,\varphi''_{h_2}$ are all nontrivial and $\varphi'_{h_1+1},\ldots,\varphi'_n,\varphi''_{h_2+1},\ldots,\varphi''_n$ are all trivial, then $E_{R_2}(\varphi_1,\ldots,\varphi_n;1)=$

$$\begin{cases}\dfrac{G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_{h_1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_{h_2})}{(-1)^{h_1+h_2}l^2}, & \text{if } (\varphi'_1\cdots\varphi'_{h_1})^* \text{ and } (\varphi''_1\cdots\varphi''_{h_2})^* \text{ are trivial;}\\ \dfrac{G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_{h_1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_{h_2})}{(-1)^{h_1+h_2-1}lG_{\mathbb{F}_l}((\varphi''_1\cdots\varphi''_{h_2})^*)}, & \text{if } (\varphi'_1\cdots\varphi'_{h_1})^* \text{ is trivial and } (\varphi''_1\cdots\varphi''_{h_2})^* \text{ is nontrivial;}\\ \dfrac{G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_{h_1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_{h_2})}{(-1)^{h_1+h_2-1}lG_{\mathbb{F}_l}((\varphi'_1\cdots\varphi'_{h_1})^*)}, & \text{if } (\varphi'_1\cdots\varphi'_{h_1})^* \text{ is nontrivial and } (\varphi''_1\cdots\varphi''_{h_2})^* \text{ is trivial;}\\ \dfrac{G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_{h_1})G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_{h_2})}{(-1)^{h_1+h_2}G_{\mathbb{F}_l}((\varphi'_1\cdots\varphi'_{h_1})^*)G_{\mathbb{F}_l}((\varphi''_1\cdots\varphi''_{h_2})^*)}, & \text{if } (\varphi'_1\cdots\varphi'_{h_1})^* \text{ and } (\varphi''_1\cdots\varphi''_{h_2})^* \text{ are nontrivial.}\end{cases}$$

(6) If $\varphi'_1,\ldots,\varphi'_h,\varphi''_1,\ldots,\varphi''_n$ are all nontrivial and $\varphi'_{h+1},\ldots,\varphi'_n$ are all trivial $(1\le h\le n-1)$*, then* $E_{R_2}(\varphi_1,\ldots,\varphi_n;1)=$

$$\begin{cases}\dfrac{(-1)^{n-h}G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_h)G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_n)}{l^2}, & \text{if } (\varphi'_1\cdots\varphi'_h)^* \text{ and } (\varphi''_1\cdots\varphi''_n)^* \text{ are trivial;}\\ \dfrac{(-1)^{n-h+1}G_{\mathbb{F}_q}(\varphi')\cdots G_{\mathbb{F}_q}(\varphi'_h)G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_n)}{lG_{\mathbb{F}_l}((\varphi''_1\cdots\varphi''_n)^*)}, & \text{if } (\varphi'_1\cdots\varphi'_h)^* \text{ is trivial and } (\varphi''_1\cdots\varphi''_n)^* \text{ is nontrivial;}\\ \dfrac{(-1)^{n-h+1}G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_h)G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_n)}{lG_{\mathbb{F}_l}((\varphi'_1\cdots\varphi'_h)^*)}, & \text{if } (\varphi'_1\cdots\varphi'_h)^* \text{ is nontrivial and } (\varphi''_1\cdots\varphi''_n)^* \text{ is trivial;}\\ \dfrac{(-1)^{n-h}G_{\mathbb{F}_q}(\varphi'_1)\cdots G_{\mathbb{F}_q}(\varphi'_h)G_{\mathbb{F}_q}(\varphi''_1)\cdots G_{\mathbb{F}_q}(\varphi''_n)}{G_{\mathbb{F}_l}((\varphi'_1\cdots\varphi'_h)^*)G_{\mathbb{F}_l}((\varphi''_1\cdots\varphi''_n)^*)}, & \text{if } (\varphi'_1\cdots\varphi'_h)^* \text{ and } (\varphi''_1\cdots\varphi''_n)^* \text{ are nontrivial.}\end{cases}$$

(7) If $\varphi'_1, \ldots, \varphi'_n$ are all nontrivial and $\varphi''_1, \ldots, \varphi''_n$ are all trivial, then

$$E_{R_2}(\varphi_1, \ldots, \varphi_n; 1) = \begin{cases} -\frac{((q-1)^n + (-1)^{n+1}) G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n)}{l^2}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ is trivial;} \\ \frac{((q-1)^n + (-1)^{n+1}) G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n)}{l G_{\mathbb{F}_l}((\varphi'_1 \cdots \varphi'_n)^*)}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ is nontrivial.} \end{cases}$$

(8) If $\varphi'_1, \ldots, \varphi'_n, \varphi''_1, \ldots, \varphi''_h$ are all nontrivial and $\varphi''_{h+1}, \ldots, \varphi''_n$ are all trivial $(1 \le h \le n-1)$*, then* $E_{R_2}(\varphi_1, \ldots, \varphi_n; 1) =$

$$\begin{cases} \frac{(-1)^{n-h} G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_h)}{l^2}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ and } (\varphi''_1 \cdots \varphi''_h)^* \text{ are trivial;} \\ \frac{(-1)^{n-h+1} G_{\mathbb{F}_q}(\varphi') \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_h)}{l G_{\mathbb{F}_l}((\varphi''_1 \cdots \varphi''_h)^*)}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ is trivial and } (\varphi''_1 \cdots \varphi''_h)^* \\ & \text{is nontrivial;} \\ \frac{(-1)^{n-h+1} G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_h)}{l G_{\mathbb{F}_l}((\varphi'_1 \cdots \varphi'_n)^*)}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ is nontrivial and } (\varphi''_1 \cdots \varphi''_h)^* \\ & \text{is trivial;} \\ \frac{(-1)^{n-h} G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_h)}{G_{\mathbb{F}_l}((\varphi'_1 \cdots \varphi'_n)^*) G_{\mathbb{F}_l}((\varphi''_1 \cdots \varphi''_h)^*)}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ and } (\varphi''_1 \cdots \varphi''_h)^* \text{ are nontrivial.} \end{cases}$$

(9) If $\varphi'_1, \ldots, \varphi'_n$ and $\varphi''_1, \ldots, \varphi''_n$ are all nontrivial, then $E_R(\varphi_1, \ldots, \varphi_n; 1) =$

$$\begin{cases} \frac{G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_n)}{l^2}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ and } (\varphi''_1 \cdots \varphi''_n)^* \text{ are trivial;} \\ -\frac{G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_n)}{l G_{\mathbb{F}_l}((\varphi''_1 \cdots \varphi''_n)^*)}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ is trivial and } (\varphi''_1 \cdots \varphi''_n)^* \text{ is nontrivial;} \\ -\frac{G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_n)}{l G_{\mathbb{F}_l}((\varphi'_1 \cdots \varphi'_n)^*)}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ is nontrivial and } (\varphi''_1 \cdots \varphi''_n)^* \text{ is trivial;} \\ \frac{G_{\mathbb{F}_q}(\varphi'_1) \cdots G_{\mathbb{F}_q}(\varphi'_n) G_{\mathbb{F}_q}(\varphi''_1) \cdots G_{\mathbb{F}_q}(\varphi''_n)}{G_{\mathbb{F}_l}((\varphi'_1 \cdots \varphi'_n)^*) G_{\mathbb{F}_l}((\varphi''_1 \cdots \varphi''_n)^*)}, & \text{if } (\varphi'_1 \cdots \varphi'_n)^* \text{ and } (\varphi''_1 \cdots \varphi''_n)^* \text{ are nontrivial.} \end{cases}$$

Combined the definition of hyper Eisenstein sums over R_2 with $n = 1$, we can get the sum $E_{R_2}(\varphi; 1)$ which is usually called the Eisenstein sum over R_2, where φ is a multiplicative character of R_2. From Corollary 3.2.6, we can determine the absolute value of the Eisenstein sum $E_{R_2}(\varphi; 1)$ as follows.

Corollary 3.2.7 *Let φ be a multiplicative character of R_2 and $\varphi := \varphi' \star \varphi''$, where φ' and φ'' are multiplicative characters of $\mathbb{F}_q$. Then*

$$|E_{R_2}(\varphi; 1)| = \begin{cases} (\frac{q}{l})^2, & \text{if } \varphi' \text{ and } \varphi'' \text{ are all trivial;} \\ \frac{q\sqrt{q}}{l^2}, & \text{if } \varphi' \text{ is trivial, } \varphi'' \text{ is nontrivial and } \varphi''^* \text{ is trivial} \\ & (\text{or } \varphi' \text{ is nontrivial, } \varphi'' \text{ is trivial and } \varphi'^* \text{ is trivial}); \\ \frac{q\sqrt{q}}{l\sqrt{l}}, & \text{if } \varphi' \text{ is trivial, } \varphi'' \text{ is nontrivial and } \varphi''^* \text{ is nontrivial} \\ & (\text{or } \varphi' \text{ is nontrivial, } \varphi'' \text{ is trivial and } \varphi'^* \text{ is nontrivial}); \\ \frac{q}{l^2}, & \text{if } \varphi', \varphi'' \text{ are all nontrivial and } \varphi'^*, \varphi''^* \text{ are all trivial;} \\ \frac{q}{l\sqrt{l}}, & \text{if } \varphi', \varphi'' \text{ are all nontrivial, } \varphi'^* \text{ is trivial and } \varphi''^* \text{ is nontrivial} \\ & (\text{or } \varphi', \varphi'' \text{ are all nontrivial, } \varphi'^* \text{ is nontrivial and } \varphi''^* \text{ is trivial}); \\ \frac{q}{l}, & \text{if } \varphi', \varphi'' \text{ are all trivial and } \varphi'^*, \varphi''^* \text{ are all nontrivial.} \end{cases}$$

Remark 3.2.8 *Let $q = l^m$ and l be a power of a prime p. If $q = l$ in Eq. (3.8), then the hyper Eisenstein sum over R_2*

$$E_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1) = \sum_{t_1,t_2,\ldots,t_n \in R_2^*, t_1+t_2+\cdots+t_n=1} \varphi_1(t_1)\varphi_2(t_2)\cdots\varphi_n(t_n). \quad (3.9)$$

According to the definition of Jacobi sums in [130], we call Eq. (3.9) a Jacobi sum over R_2. Combined with Theorem 3.2.4, we can get

$$J_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1) = J_{\mathbb{F}_q}(\varphi_1', \varphi_2', \ldots, \varphi_n'; 1) J_{\mathbb{F}_q}(\varphi_1'', \varphi_2'', \ldots, \varphi_n''; 1).$$

In Corollary 3.2.6, we have the exact value of the Jacobi sum $J_{R_2}(\varphi_1, \varphi_2, \ldots, \varphi_n; 1)$ over R_2. In the following corollary, we present the absolute value of the Jacobi sum $J_{R_2}(\varphi_1, \varphi_2; 1)$ over R_2 which is helpful to study asymptotically optimal codebooks in next section.

Corollary 3.2.9 *Let φ_1, φ_2 be multiplicative characters of R_2 and $\varphi_i := \varphi_i' \star \varphi_i''$ $(i = 1, 2)$, where φ_i' and φ_i'' are multiplicative characters of $\mathbb{F}_q$. Then*

(1) If φ_1', φ_2' and φ_1'', φ_2'' are all trivial, then $|J_{R_2}(\varphi_1, \varphi_2; 1)| = (q-2)^2$.

(2) If φ_1', φ_2' are all trivial, φ_1'' is trivial and φ_2'' is nontrivial (or φ_1' is trivial, φ_2' is nontrivial and φ_1'', φ_2'' are all trivial), then

$$|J_{R_2}(\varphi_1, \varphi_2; 1)| = \begin{cases} \frac{q-2}{\sqrt{q}}, & \text{if } \varphi_2''^* \text{ is trivial (or } \varphi_2'^* \text{ is trivial);} \\ q-2, & \text{if } \varphi_2''^* \text{ is nontrivial (or } \varphi_2'^* \text{ is nontrivial).} \end{cases}$$

(3) If φ_1', φ_2' are all trivial and φ_1'', φ_2'' are all nontrivial (or φ_1', φ_2' are all nontrivial and φ_1'', φ_2'' are all trivial), then

$$|J_{R_2}(\varphi_1, \varphi_2; 1)| = \begin{cases} q-2, & \text{if } (\varphi_1''\varphi_2'')^* \text{ is trivial (or } (\varphi_1'\varphi_2')^* \text{ is trivial);} \\ (q-2)\sqrt{q}, & \text{if } (\varphi_1''\varphi_2'')^* \text{ is nontrivial (or } (\varphi_1'\varphi_2')^* \text{ is nontrivial).} \end{cases}$$

(4) If φ_1', φ_1'' are all trivial and φ_2', φ_2'' are all nontrivial, then

$$|J_{R_2}(\varphi_1, \varphi_2; 1)| = \begin{cases} \frac{1}{q}, & \text{if } \varphi_2'^* \text{ and } \varphi_2''^* \text{ are all trivial;} \\ \frac{1}{\sqrt{q}}, & \text{if } \varphi_2'^* \text{ is trivial and } \varphi_2''^* \text{ is nontrivial} \\ & \text{(or } \varphi_2'^* \text{ is nontrivial and } \varphi_2''^* \text{ is trivial);} \\ 1, & \text{if } \varphi_2'^* \text{ and } \varphi_2''^* \text{ are all nontrivial.} \end{cases}$$

(5) If φ_1' is trivial and $\varphi_2', \varphi_1'', \varphi_2''$ are all nontrivial (or φ_1'' is trivial and $\varphi_1', \varphi_2', \varphi_2''$ are all nontrivial), then

$$|J_{R_2}(\varphi_1, \varphi_2; 1)| = \begin{cases} \frac{1}{\sqrt{q}}, & \text{if } \varphi_2'^* \text{ and } (\varphi_1''\varphi_2'')^* \text{ are all trivial (or } (\varphi_1'\varphi_2')^* \text{ and } \varphi_2''^* \text{ are all trivial);} \\ \sqrt{q}, & \text{if } \varphi_2'^* \text{ and } (\varphi_1''\varphi_2'')^* \text{ are all nontrivial (or } (\varphi_1'\varphi_2')^* \text{ and } \varphi_2''^* \text{ are all} \\ & \text{nontrivial);} \\ 1, & \text{otherwise.} \end{cases}$$

(6) If $\varphi_1', \varphi_2', \varphi_1''$ and φ_2'' are all nontrivial, then

$$|J_{R_2}(\varphi_1, \varphi_2; 1)| = \begin{cases} 1, & \text{if } (\varphi_1'\varphi_2')^* \text{ and } (\varphi_1''\varphi_2'')^* \text{ are all trivial;} \\ \sqrt{q}, & \text{if } (\varphi_1'\varphi_2')^* \text{ is trivial and } (\varphi_1''\varphi_2'')^* \text{ is nontrivial} \\ & \text{(or } (\varphi_1'\varphi_2')^* \text{ is nontrivial and } (\varphi_1''\varphi_2'')^* \text{ is trivial);} \\ q, & \text{if } (\varphi_1'\varphi_2')^* \text{ and } (\varphi_1''\varphi_2'')^* \text{ are all nontrivial.} \end{cases}$$

3.2.3 Constructions of several families of codebooks

This subsection presents specific constructions of three classes of asymptotically optimal codebooks with respect to the Welch bound and a class of optimal codebooks with respect to the Levenshtein bound by using character sums over the finite non-chain ring $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$.

• **Constructions of asymptotically optimal codebooks with respect to the Welch bound**

Firstly, we construct two classes of asymptotically optimal codebooks by using the Gaussian sum over R_2.

Let $\varphi := \varphi' \star \varphi''$ $(\varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*)$ and $\lambda := \chi_a \star \chi_b$ $(\chi_a, \chi_b \in \widehat{\mathbb{F}}_q, a, b \in \mathbb{F}_q)$ be a multiplicative character and an additive character of R_2, respectively. Assume that $t = ut' + (1-u)t'' \in R_2^*$. Define a set $C_0(R_2^*, \widehat{R}_2^* \times \widehat{R}_2)$ as

$$\begin{aligned} C_0(R_2^*, \widehat{R}_2^* \times \widehat{R}_2) : &= \left\{ \frac{1}{\sqrt{K}} (\varphi(t)\lambda(t))_{t \in R_2^*}, \varphi \in \widehat{R}_2^*, \lambda \in \widehat{R}_2 \right\} \\ &= \left\{ \frac{1}{\sqrt{K}} (\varphi'(t')\varphi''(t'')\chi_a(t')\chi_b(t''))_{t',t'' \in \mathbb{F}_q^*}, \varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*, \chi_a, \chi_b \in \widehat{\mathbb{F}}_q \right\}, \end{aligned}$$

where $K = |R_2^*| = (q-1)^2$.

A. The first construction of codebooks

The codebook $C_1 := C_1(R_2^*, \widehat{R}_2^* \times \widehat{R}_2)$ of length $K_1 = |R_2^*| = (q-1)^2$ over R_2 is constructed as

$$C_1 : = \left\{ \frac{1}{\sqrt{K_1}} (\psi(t')\psi(t'')\chi_a(t')\chi_b(t''))_{t',t'' \in \mathbb{F}_q^*}, \psi \in \widehat{\mathbb{F}}_q^*, \chi_a, \chi_b \in \widehat{\mathbb{F}}_q \right\}. \quad (3.10)$$

Theorem 3.2.10 *Let C_1 be a codebook defined in (3.10). Then C_1 is a $(q^2(q-1), (q-1)^2)$ codebook having maximum cross-correlation amplitude $I_{\max}(C_1) = \frac{q}{(q-1)^2}$. Moreover, the codebook C_1 asymptotically meets the Welch bound.*

Proof: From Eq. (3.10), it is easy to know that C_1 has $N_1 = q^2(q-1)$ codewords of length $K_1 = (q-1)^2$. Let $\mathbf{c}_1 = \frac{1}{\sqrt{K_1}} (\psi_1(t')\psi_1(t'')\ \chi_{a_1}(t')\chi_{b_1}(t''))_{t',t'' \in \mathbb{F}_q^*}$, $\mathbf{c}_2 = \frac{1}{\sqrt{K_1}} (\psi_2(t')\psi_2(t'')\chi_{a_2}(t')\chi_{b_2}(t''))_{t',t'' \in \mathbb{F}_q^*}$ be any two distinct vectors in C_1. Then

$$\begin{aligned} K_1 \mathbf{c}_1 \mathbf{c}_2^H &= \sum_{t',t'' \in \mathbb{F}_q^*} \psi_1(t')\psi_1(t'')\chi_{a_1}(t')\chi_{b_1}(t'')\overline{\psi_2(t')\psi_2(t'')\chi_{a_2}(t')\chi_{b_2}(t'')} \\ &= \sum_{t',t'' \in \mathbb{F}_q^*} \psi_1\psi_2^{-1}(t')\psi_1\psi_2^{-1}(t'')\chi((a_1-a_2)t' + (b_1-b_2)t'') \\ &= \sum_{t' \in \mathbb{F}_q^*} \psi(t')\chi(at') \sum_{t'' \in \mathbb{F}_q^*} \psi(t')\chi(bt'') \text{ (Let } \psi = \psi_1\psi_2^{-1}, a = a_1 - a_2, b = b_1 - b_2) \\ &= G_{\mathbb{F}_q}(\psi, \chi_a) G_{\mathbb{F}_q}(\psi, \chi_b) \\ &= G_{R_2}(\varphi, \lambda) \text{ (where } \varphi = \psi \star \psi, \lambda = \chi_a \star \chi_b) \text{ (By Theorem 3.2.1).} \end{aligned}$$

Since $\mathbf{c}_1 \neq \mathbf{c}_2$, ψ, χ_a, χ_b are not all trivial. From Remark 3.2.2, we have

$$K_1|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} q-1, & \text{if } \psi, \chi_a \text{ are all trivial and } \chi_b \text{ is nontrivial;} \\ 1, & \text{if } \psi \text{ is trivial and } \chi_a, \chi_b \text{ are all nontrivial;} \\ q, & \text{if } \psi, \chi_a \text{ and } \chi_b \text{ are all nontrivial;} \\ 0, & \text{otherwise.} \end{cases}$$

Consequently, we infer that $|\mathbf{c}_1\mathbf{c}_2^H| \in \left\{0, \frac{1}{q-1}, \frac{1}{(q-1)^2}, \frac{q}{(q-1)^2}\right\}$ for any two distinct vectors $\mathbf{c}_1, \mathbf{c}_2$ in C_1. Hence, $I_{\max}(C_1) = \frac{q}{(q-1)^2}$.

Next, we show that the codebook C_1 is asymptotically optimal. The corresponding Welch bound of the codebook C_1 is $I_W = \sqrt{\frac{N_1-K_1}{(N_1-1)K_1}} = \sqrt{\frac{q^2(q-1)-(q-1)^2}{(q^2(q-1)-1)(q-1)^2}} = \sqrt{\frac{q^2-q+1}{(q^3-q^2-1)(q-1)}}$. It follows from $I_{\max}(C_1) = \frac{q}{(q-1)^2}$ that

$$\frac{I_{\max}(C_1)}{I_W} = \sqrt{\frac{q^2(q^3-q^2-1)}{(q^2-q+1)(q-1)^3}}.$$

Obviously, $\lim_{q\longrightarrow\infty} \frac{I_{\max}(C_1)}{I_W} = 1$, which implies that C_1 asymptotically meets the Welch bound. ■

Remark 3.2.11 *In Table 3.2.1, we present some explicit values of the parameters of the codebook C_1 in Theorem 3.2.10 for some given q and a numerical comparison to the Welch bound for references. It is easy to see that the numerical results indicate the codebook C_1 asymptotically meets the Welch bound.*

***Table 3.2.1**: Parameters of the (N_1, K_1) codebook of Theorem 3.2.10*

q	(N_1, K_1)	$I_{\max}(C_1)$	I_W	$\frac{I_{\max}(C_1)}{I_W}$
13	$(2028, 144)$	0.0902778	0.0803401	1.123695
23	$(11638, 484)$	0.0475207	0.0445012	1.067852
5^2	$(15000, 576)$	0.0434028	0.0408602	1.062227
7^2	$(115248, 2304)$	0.0212674	0.0206241	1.031192
3^4	$(524880, 6400)$	0.0126563	0.0124236	1.018730
103	$(1082118, 10404)$	0.00990004	0.00975668	1.014694
151	$(3420150, 22500)$	0.00666667	0.00664470	1.003311
5^4	$(243750000, 389376)$	0.00160513	0.00160128	1.002404
7^5	$(4.747279e+12, 282441636)$	0.0000595061	0.0000595008	1.000089

e denotes the scientific notation

B. The second construction of codebooks

The codebook $C_2 := C_2(R_2^*, \widehat{R}_2^* \times \widehat{R}_2^*)$ of length $K_2 = |R_2^*| = (q-1)^2$ over R_2 is defined as

$$C_2 : \quad = \quad \left\{ \frac{1}{\sqrt{K_2}} (\varphi'(t')\varphi''(t'')\chi_a(t')\chi_a(t''))_{t',t''\in\mathbb{F}_q^*}, \varphi', \varphi'' \in \widehat{\mathbb{F}}_q^*, \chi_a \in \widehat{\mathbb{F}}_q \right\}. \quad (3.11)$$

With this construction, we will figure up the maximum magnitude $I_{\max}(C_2)$ as follows.

Theorem 3.2.12 *Let C_2 be a codebook defined in (3.11). Then C_2 is a $(q(q-1)^2,(q-1)^2)$ codebook having maximum cross-correlation amplitude $I_{\max}(C_2) = \frac{q}{(q-1)^2}$. Moreover, the codebook C_2 asymptotically meets the Welch bound.*

Proof: The proof of this theorem is similar to that of Theorem 3.2.10, then we omit it here. ■

Remark 3.2.13 *In Table 3.2.2, we list some examples of the codebook C_2 generated by Theorem 3.2.12 for some given q. As can be seen, the codebook C_2 asymptotically achieves the Welch bound.*

***Table 3.2.2**: Parameters of the (N_2,K_2) codebook of Theorem 3.2.12*

q	(N_2,K_2)	$I_{\max}(C_2)$	I_W	$\frac{I_{\max}(C_2)}{I_W}$
17	$(4352,256)$	0.0664062	0.0606409	1.095074
37	$(47952,1296)$	0.0285494	0.0274001	1.041944
83	$(558092,6724)$	0.0123438	0.0121214	1.018347
11^2	$(1742400,14400)$	0.00840278	0.00829883	1.012526
3^5	$(14231052,58564)$	0.00414931	0.00412372	1.006205
293	$(24982352,85264)$	0.00343639	0.00341881	1.005141
7^3	$(40118652,116964)$	0.00293253	0.00291971	1.004389
13^3	$(1.05948e+10,4822416)$	0.000455581	0.00045527	1.000683
5^5	$(3.0498e+10,9759376)$	0.000320205	0.000320051	1.000480

e denotes the scientific notation

C. The third construction of codebooks

Next, we present a class of asymptotically optimal codebooks which are constructed by Jacobi sums over R_2.

Let $t_1 = ut_1' + (1-u)t_1'', t_2 = ut_2' + (1-u)t_2'' \in R_2^*$. Define

$$\begin{aligned} D' &= \{(t_1,t_2) \in (R_2^*)^2 : t_1 + t_2 = 1\} \\ &= \{(t_1',t_2',t_1'',t_2'') \in (\mathbb{F}_q^*)^4 : t_1' + t_2' = 1, t_1'' + t_2'' = 1\}. \end{aligned} \tag{3.12}$$

The codebook $C_3 := C_3(D', \widehat{R}_2^* \times \widehat{R}_2^*)$ of length $K_3 = |D'| = (q-2)^2$ over R_2 is constructed as

$$C_3 : = \left\{ \frac{1}{\sqrt{K_3}} (\varphi_1(t_1)\varphi_2(t_2))_{t_1,t_2 \in D'}, \varphi_1 = \varphi_1' \star \varphi_1'', \varphi_2 = \psi \star \psi, \varphi_1', \varphi_1'', \psi \in \widehat{\mathbb{F}}_q^* \right\} \tag{3.13}$$

Theorem 3.2.14 *Let C_3 be a codebook defined in (3.13). Then C_3 is a $((q-1)^3,(q-2)^2)$ codebook having maximum cross-correlation amplitude $I_{\max}(C_3) = \frac{q}{(q-2)^2}$. Moreover, the codebook C_3 asymptotically meets the Welch bound.*

Proof: According to Eq. (3.13), it is obvious that C_3 has $N_3 = (q-1)^3$ codewords of length $K_3 = (q-2)^2$. Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be any two distinct vectors in C_3, where $\mathbf{c}_1 = \frac{1}{\sqrt{K_3}}(\varphi_1'(t_1')\varphi_1''(t_1'')\psi_1(t_2')\psi_1(t_2''))_{t_1',t_2',t_1'',t_2''\in\mathbb{F}_q^*}$, $\mathbf{c}_2 = \frac{1}{\sqrt{K_3}}(\varphi_2'(t_1')\varphi_2''(t_1'')\psi_2(t_2')\psi_2(t_2''))_{t_1',t_2',t_1'',t_2''\in\mathbb{F}_q^*}$. Set $\varphi_1 = \varphi_1'\overline{\varphi_2'} \star \varphi_1''\overline{\varphi_2''} = \phi_1 \star \phi_3$, $\varphi_2 = \psi_1\overline{\psi_2} \star \psi_1\overline{\psi_2} = \phi_2 \star \phi_2$. Then

$$\begin{aligned}
K_3\mathbf{c}_1\mathbf{c}_2^H &= \sum_{\substack{t_1',t_2',t_1'',t_2''\in\mathbb{F}_q^*,\\ t_1'+t_2'=1,t_1''+t_2''=1}} \varphi_1'(t_1')\varphi_1''(t_1'')\psi_1(t_2')\psi_1(t_2'')\overline{\varphi_2'(t_1')\varphi_2''(t_1'')\psi_2(t_2')\psi_2(t_2'')} \\
&= \sum_{\substack{t_1',t_2',t_1'',t_2''\in\mathbb{F}_q^*,\\ t_1'+t_2'=1,t_1''+t_2''=1}} \varphi_1'\overline{\varphi_2'}(t_1')\varphi_1''\overline{\varphi_2''}(t_1'')\psi_1\overline{\psi_2}(t_2')\psi_1\overline{\psi_2}(t_2'') \\
&= \sum_{\substack{t_1',t_2'\in\mathbb{F}_q^*,\\ t_1'+t_2'=1}} \varphi_1'\overline{\varphi_2'}(t_1')\psi_1\overline{\psi_2}(t_2') \sum_{\substack{t_1'',t_2''\in\mathbb{F}_q^*,\\ t_1''+t_2''=1}} \varphi_1''\overline{\varphi_2''}(t_1'')\psi_1\overline{\psi_2}(t_2'') \\
&= J_{R_2}(\varphi_1,\varphi_2).
\end{aligned}$$

Since $\mathbf{c}_1 \neq \mathbf{c}_2$, ϕ_1, ϕ_2 and ϕ_3 are not all trivial. In view of Corollary 3.2.9 ($n = 2$), we have the following results:

(1) If ϕ_1 is trivial, we divide the rest of the proof into three cases.

- If ϕ_2 is trivial and ϕ_3 is nontrivial, then $K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} \frac{q-2}{\sqrt{q}}, & \text{if } \phi_3^* \text{ is trivial;} \\ q-2, & \text{if } \phi_3^* \text{ is nontrivial.} \end{cases}$
- If ϕ_2 is nontrivial and ϕ_3 is trivial, then $K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} \frac{1}{q}, & \text{if } \phi_2^* \text{ is trivial;} \\ 1, & \text{if } \phi_2^* \text{ is nontrivial.} \end{cases}$
- If ϕ_2 and ϕ_3 are nontrivial, then

$$K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} \frac{1}{\sqrt{q}}, & \text{if } \phi_2^* \text{ and } (\phi_2\phi_3)^* \text{ are trivial;} \\ 1, & \text{if } \phi_2^* \text{ is trivial and } (\phi_2\phi_3)^* \text{ is nontrivial} \\ & \text{(or } \phi_2^* \text{ is nontrivial and } (\phi_2\phi_3)^* \text{ is trivial);} \\ \sqrt{q}, & \text{if } \phi_2^* \text{ and } (\phi_2\phi_3)^* \text{ are nontrivial.} \end{cases}$$

(2) If ϕ_1 is nontrivial, we divide the rest of the proof into four cases.

- If ϕ_2 and ϕ_3 are trivial, then $K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} \frac{q-2}{\sqrt{q}}, & \text{if } \phi_1^* \text{ is trivial;} \\ q-2, & \text{if } \phi_1^* \text{ is nontrivial.} \end{cases}$
- If ϕ_2 is trivial and ϕ_3 is nontrivial, then

$$K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} \frac{1}{q}, & \text{if } \phi_1^* \text{ and } \phi_3^* \text{ are trivial;} \\ \frac{1}{\sqrt{q}}, & \text{if } \phi_1^* \text{ is trivial and } \phi_3^* \text{ is nontrivial} \\ & \text{(or } \phi_1^* \text{ is nontrivial and } \phi_3^* \text{ is trivial);} \\ 1, & \text{if } \phi_1^* \text{ and } \phi_3^* \text{ are nontrivial.} \end{cases}$$

- If ϕ_2 is nontrivial and ϕ_3 is trivial, then

$$K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} \frac{1}{\sqrt{q}}, & \text{if } (\phi_1\phi_2)^* \text{ and } \phi_2^* \text{ are trivial;} \\ 1, & \text{if } (\phi_1\phi_2)^* \text{ is trivial and } \phi_2^* \text{ is nontrivial} \\ & \text{(or } (\phi_1\phi_2)^* \text{ is nontrivial and } \phi_2^* \text{ is trivial);} \\ \sqrt{q}, & \text{if } (\phi_1\phi_2)^* \text{ and } \phi_2^* \text{ are nontrivial.} \end{cases}$$

- If ϕ_2 and ϕ_3 are nontrivial, then

$$K_3|\mathbf{c}_1\mathbf{c}_2^H| = \begin{cases} 1, & \text{if } \phi_2^* \text{ and } (\phi_1\phi_3)^* \text{ are trivial;} \\ \sqrt{q}, & \text{if } \phi_2^* \text{ is trivial and } (\phi_1\phi_3)^* \text{ is nontrivial} \\ & \text{(or } \phi_2^* \text{ is nontrivial and } (\phi_1\phi_3)^* \text{ is trivial);} \\ q, & \text{if } \phi_2^* \text{ and } (\phi_1\phi_3)^* \text{ are nontrivial.} \end{cases}$$

Hence, $I_{\max}(C_3) = \frac{q}{(q-2)^2}$.

Similar to the proof of Theorem 3.2.10, we can prove that the codebook C_3 asymptotically meets the Welch bound. ■

Remark 3.2.15 *In Table 3.2.3, we provide some explicit examples of the codebook C_3 in Theorem 3.2.14 for some given q. It is indicated that the codebook C_3 is asymptotically optimal with respect to the Welch bound.*

***Table 3.2.3**: Parameters of the (N_3, K_3) codebook of Theorem 3.2.14*

q	(N_3, K_3)	$I_{\max}(C_3)$	I_W	$\frac{I_{\max}(C_3)}{I_W}$
19	$(5832, 324)$	0.0657439	0.0573525	1.146314
59	$(195112, 3364)$	0.0181594	0.0173972	1.043812
3^4	$(512000, 6400)$	0.0129787	0.0125809	1.031622
113	$(1404928, 12544)$	0.00917133	0.00896942	1.022511
211	$(9261000, 44100)$	0.00483048	0.00477339	1.011959
281	$(21952000, 78400)$	0.00360992	0.00357787	1.008959
5^4	$(242970624, 389376)$	0.00161029	0.00160385	1.004013
11^3	$(2.35264e+9, 1768900)$	0.000753578	0.000752163	1.001881
17^3	$(1.18515e+11, 24127744)$	0.000203707	0.000203604	1.000509

e denotes the scientific notation

• Constructions of optimal codebooks with respect to the Levenshtein bound

Assume that q is a power of an odd prime p and $q > 3$. Let the set $\xi_{\mathfrak{n}}$ be the standard basis of the $\mathfrak{n}$-dimensional Hilbert space which is given by the rows of the identity matrix $I_{\mathfrak{n}}$ and $\mathfrak{n}$ a positive integer. Next, we give the concrete construction as follows.

D. The fourth construction of codebooks

Suppose that $\lambda := \chi_1 \star \chi_1$ is the canonical additive character over R_2 and $t = ut' + (1-u)t'' \in R_2$, where χ_1 is the canonical additive character of $\mathbb{F}_q$. Before we give the construction, we first define the equivalence relation as follows.

Define an equivalence relation "$\sim$" on the finite ring R_2 as: For any $a = ua_1 + (1-u)a_2, b = ub_1 + (1-u)b_2 \in R_2$, $a \sim b$ if and only if $a_1 + a_2 = b_1 + b_2$. Let

$$B := = R_2/\sim . \tag{3.14}$$

In fact, the set B is the quotient set of R_2 under the equivalence relation "$\sim$". It is obvious that for every pair of two different elements $b_1 = ub_1' + (1-u)b_1'', b_2 = ub_2' + (1-u)b_2''$ in B, we have $b_1' + b_1'' \neq b_2' + b_2''$ and $|B| = q$. Let $D := \{t = ut' + (1-u)t'' \in R \mid t' = t''\}$ and then $|D| = q$. Define a set of vectors as follows:

$$C_4(B) = \{\boldsymbol{c}_{x,y} : x, y \in B\}, \tag{3.15}$$

where $\boldsymbol{c}_{x,y} = \frac{1}{\sqrt{q}}(\lambda((t+x)^3 + yt))_{t\in D}$. We denote $\widetilde{C}_4 := C_4(B) \cup \xi_q$. Then we have the following result.

Theorem 3.2.16 *Let q be a power of an odd prime, and $\widetilde{C}_4$ be a codebook defined in (3.15). Then $\widetilde{C}_4$ is a (q^2+q, q) codebook having maximum cross-correlation amplitude $I_{\max}(\widetilde{C}_4) = \frac{1}{\sqrt{q}}$. Moreover, the codebook $\widetilde{C}_4$ meets the Welch bound.*

Proof: It follows from the definition of $\widetilde{C}_4 = C_4(B) \cup \xi_q$ that the set $\widetilde{C}_4$ has $N_4 = q^2 + q$ codewords of length $K_4 = |D| = q$. We will divide the rest of the proof into three cases as follows.

Case 1: For any two distinct vectors $\boldsymbol{d}_1, \boldsymbol{d}_2 \in \xi_q$, it is obvious that $|\boldsymbol{d}_1 \boldsymbol{d}_2^H| = 0$.

Case 2: For any two distinct vectors $\boldsymbol{d}_1 \in C_4(B), \boldsymbol{d}_2 \in \xi_q$, it is easy to check that $|\boldsymbol{d}_1 \boldsymbol{d}_2^H| = \frac{1}{\sqrt{q}}$.

Case 3: For any two distinct vectors $\boldsymbol{d}_1, \boldsymbol{d}_2 \in C_4(B)$, then we write $\boldsymbol{d}_1 = \boldsymbol{c}_{x_1,y_1}$ and $\boldsymbol{d}_2 = \boldsymbol{c}_{x_2,y_2}$, where $x_i = ux_i' + (1-u)x_i'' \in B, y_i = uy_i' + (1-u)y_i'' \in B$ for $i = 1, 2$. Then we have

$$\begin{aligned}
q\boldsymbol{d}_1\boldsymbol{d}_2^H &= \sum_{t\in D} \lambda((t+x_1)^3 + y_1 t)\overline{\lambda((t+x_2)^3 + y_2 t)} \\
&= \sum_{t\in D} \lambda(u((t'+x_1')^3 + y_1' t') + (1-u)((t'+x_1'')^3 + y_1'' t')) \cdot \\
&\quad \overline{\lambda(u((t'+x_2')^3 + y_2' t') + (1-u)((t'+x_2'')^3 + y_2'' t'))} \\
&= \sum_{t'\in\mathbb{F}_q} \chi_1((t'+x_1')^3 + y_1' t')\chi_1((t'+x_1'')^3 + y_1'' t') \cdot \\
&\quad \overline{\chi_1((t'+x_2')^3 + y_2' t')\chi_1((t'+x_2'')^3 + y_2'' t')} \\
&= \sum_{t'\in\mathbb{F}_q} \chi_1(3(x_1' - x_2')t'^2 + (3x_1'^2 - 3x_2'^2 + y_1' - y_2')t' + x_1'^3 - x_2'^3) \cdot \\
&\quad \chi_1(3(x_1'' - x_2'')t'^2 + (3x_1''^2 - 3x_2''^2 + y_1'' - y_2'')t' + x_1''^3 - x_2''^3) \\
&= \sum_{t'\in\mathbb{F}_q} \chi_1(3(x_1' - x_2' + x_1'' - x_2'')t'^2 + (3(x_1'^2 - x_2'^2 + x_1''^2 - x_2''^2) \\
&\quad + y_1' - y_2' + y_1'' - y_2'')t' + x_1'^3 - x_2'^3 + x_1''^3 - x_2''^3).
\end{aligned}$$

Since $\boldsymbol{d}_1 \neq \boldsymbol{d}_2 \in C_4(B)$, we have $(x_1 - x_2, y_1 - y_2) = (u(x_1' - x_2') + (1-u)(x_1'' - x_2''), u(y_1' - y_2') + (1-u)(y_1'' - y_2'')) \neq (0,0)$, which implies that at least one of these four elements $x_1' - x_2', x_1'' - x_2'', y_1' - y_2'$ and $y_1'' - y_2''$ is nonzero.

- If $x_1' = x_2', x_1'' = x_2'', y_1' = y_2'$ and $y_1'' \neq y_2''$, then $q\boldsymbol{d}_1\boldsymbol{d}_2^H = \sum_{t' \in \mathbb{F}_q} \chi_1((y_1'' - y_2'')t') = 0$ by $y_1'' - y_2'' \neq 0$. Thus, $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = 0$. Because of the symmetry, it is the same thing for the case $x_1' = x_2', x_1'' = x_2'', y_1' \neq y_2'$ and $y_1'' = y_2''$.

- If $x_1' = x_2', x_1'' \neq x_2'', y_1' = y_2'$ and $y_1'' = y_2''$, then it follows from Lemma 2.1.9 that

$$\begin{aligned} q\boldsymbol{d}_1\boldsymbol{d}_2^H &= \sum_{t' \in \mathbb{F}_q} \chi_1(3(x_1'' - x_2'')t'^2 + (3x_1''^2 - 3x_2''^2)t' + x_1''^3 - x_2''^3) \\ &= \chi_1(x_1''^3 - x_2''^3 - (3x_1''^2 - 3x_2''^2)^2(12(x_1'' - x_2''))^{-1})\eta(3(x_1'' - x_2''))G(\eta, \chi_1). \end{aligned}$$

  Hence, we have $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = \frac{1}{q} \cdot \sqrt{q} = \frac{1}{\sqrt{q}}$ according to Lemma 2.1.7. In view of the symmetry, it is the same thing for the case $x_1' \neq x_2', x_1'' = x_2'', y_1' = y_2'$ and $y_1'' = y_2''$.

- If $x_1' = x_2', x_1'' = x_2'', y_1' \neq y_2'$ and $y_1'' \neq y_2''$, then $q\boldsymbol{d}_1\boldsymbol{d}_2^H = \sum_{t' \in \mathbb{F}_q} \chi_1((y_1' - y_2' + y_1'' - y_2'')t') = 0$ by the fact $y_i = uy_i' + (1-u)y_i'' \in B$ and $y_1' + y_1'' \neq y_2' + y_2''$. Hence, $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = 0$.

- If $x_1' = x_2', x_1'' \neq x_2'', y_1' = y_2'$ and $y_1'' \neq y_2''$, then it follows from Lemma 2.1.9 that

$$\begin{aligned} q\boldsymbol{d}_1\boldsymbol{d}_2^H &= \sum_{t' \in \mathbb{F}_q} \chi_1(3(x_1'' - x_2'')t'^2 + (3x_1''^2 - 3x_2''^2 + y_1'' - y_2'')t' + x_1''^3 - x_2''^3) \\ &= \chi_1(x_1''^3 - x_2''^3 - (3x_1''^2 - 3x_2''^2 + y_1'' - y_2'')^2(12(x_1'' - x_2''))^{-1}) \\ &\quad \eta(3(x_1'' - x_2''))G(\eta, \chi_1). \end{aligned}$$

  Therefore, we obtain that $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = \frac{1}{q} \cdot \sqrt{q} = \frac{1}{\sqrt{q}}$ according to Lemma 2.1.7. Due to the symmetry, it is the same thing for the case $x_1' \neq x_2', x_1'' = x_2'', y_1' \neq y_2'$ and $y_1'' = y_2''$.

- If $x_1' \neq x_2', x_1'' = x_2'', y_1' = y_2'$ and $y_1'' \neq y_2''$, then it follows from Lemma 2.1.9 that

$$\begin{aligned} q\boldsymbol{d}_1\boldsymbol{d}_2^H &= \sum_{t' \in \mathbb{F}_q} \chi_1(3(x_1' - x_2')t'^2 + (3x_1'^2 - 3x_2'^2 + y_1'' - y_2'')t' + x_1'^3 - x_2'^3) \\ &= \chi_1(x_1'^3 - x_2'^3 - (3x_1'^2 - 3x_2'^2 + y_1'' - y_2'')^2(12(x_1' - x_2'))^{-1}) \\ &\quad \eta(3(x_1' - x_2'))G(\eta, \chi_1). \end{aligned}$$

  Then $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = \frac{1}{q} \cdot \sqrt{q} = \frac{1}{\sqrt{q}}$ by Lemma 2.1.7. By the symmetry, it is the same thing for the case $x_1' = x_2', x_1'' \neq x_2'', y_1' \neq y_2'$ and $y_1'' = y_2''$.

- If $x_1' \neq x_2', x_1'' \neq x_2'', y_1' = y_2'$ and $y_1'' = y_2''$, then it follows from Lemma 2.1.9 and $x_i = ux_i' + (1-u)x_i'' \in B$ that

$$\begin{aligned} q\boldsymbol{d}_1\boldsymbol{d}_2^H &= \sum_{t' \in \mathbb{F}_q} \chi_1(3(x_1' - x_2' + x_1'' - x_2'')t'^2 + (3x_1'^2 - 3x_2'^2 + 3x_1''^2 - 3x_2''^2)t' \\ &\quad + x_1'^3 - x_2'^3 + x_1''^3 - x_2''^3) \\ &= \chi_1(x_1'^3 - x_2'^3 + x_1''^3 - x_2''^3 - (3x_1'^2 - 3x_2'^2 + 3x_1''^2 - 3x_2''^2)^2(12(x_1' - x_2' \\ &\quad + x_1'' - x_2''))^{-1})\eta(3(x_1' - x_2' + x_1'' - x_2''))G(\eta, \chi_1). \end{aligned}$$

  Hence, we obtain $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = \frac{1}{q} \cdot \sqrt{q} = \frac{1}{\sqrt{q}}$ by Lemma 2.1.7.

- If $x_1' = x_2', x_1'' \neq x_2'', y_1' \neq y_2'$ and $y_1'' \neq y_2''$, then it follows from Lemmas 2.1.7 and 2.1.9 that $q\boldsymbol{d}_1\boldsymbol{d}_2^H = \sum_{t' \in \mathbb{F}_q} \chi_1(3(x_1'' - x_2'')t'^2 + (3x_1''^2 - 3x_2''^2 + y_1' - y_2' + y_1'' - y_2'')t' + x_1''^3 - x_2''^3)$ and $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = \frac{1}{q} \cdot \sqrt{q} = \frac{1}{\sqrt{q}}$. Based on the symmetry, it is the same thing for the case $x_1' \neq x_2', x_1'' = x_2'', y_1' \neq y_2'$ and $y_1'' \neq y_2''$.
- If $x_1' \neq x_2', x_1'' \neq x_2'', y_1' \neq y_2'$ and $y_1'' = y_2''$, then $q\boldsymbol{d}_1\boldsymbol{d}_2^H = \sum_{t' \in \mathbb{F}_q} \chi_1(3(x_1' - x_2' + x_1'' - x_2'')t'^2 + (3x_1'^2 - 3x_2'^2 + 3x_1''^2 - 3x_2''^2 + y_1' - y_2')t' + x_1'^3 - x_2'^3 + x_1''^3 - x_2''^3)$. It follows from Lemma 2.1.9 and $x_i = ux_i' + (1-u)x_i'' \in B$ that $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = \frac{1}{q} \cdot \sqrt{q} = \frac{1}{\sqrt{q}}$. From the symmetry, it is the same thing for the case $x_1' \neq x_2', x_1'' \neq x_2'', y_1' = y_2'$ and $y_1'' \neq y_2''$.
- If $x_1' \neq x_2', x_1'' \neq x_2'', y_1' \neq y_2'$ and $y_1'' \neq y_2''$, then

$$\begin{aligned} q\boldsymbol{d}_1\boldsymbol{d}_2^H &= \sum_{t' \in \mathbb{F}_q} \chi_a(3(x_1' - x_2' + x_1'' - x_2'')t'^2 + (3x_1'^2 - 3x_2'^2 + 3x_1''^2 - 3x_2''^2 + \\ &\quad y_1' - y_2' + y_1'' - y_2'')t' + x_1'^3 - x_2'^3 + x_1''^3 - x_2''^3). \end{aligned}$$

  Hence, $|\boldsymbol{d}_1\boldsymbol{d}_2^H| = \frac{1}{q} \cdot \sqrt{q} = \frac{1}{\sqrt{q}}$ from Lemma 2.1.9 and $x_i = ux_i' + (1-u)x_i'' \in B$.

From what has been discussed above, we infer that $|\boldsymbol{d}_1\boldsymbol{d}_2^H| \in \left\{0, \frac{1}{\sqrt{q}}\right\}$ for any two distinct vectors $\boldsymbol{d}_1, \boldsymbol{d}_2 \in \widetilde{C}_4$. Hence, $I_{\max}(\widetilde{C}_4) = \frac{1}{\sqrt{q}}$.

For any complex valued (q^2+q, q) codebook $\widetilde{C}_4$, the Levenshtein bound in Lemma 1.2.2 is

$$\begin{aligned} I_L &= \sqrt{\frac{2N_4 - K_4^2 - K_4}{(N_4 - K_4)(K_4 + 1)}} \\ &= \sqrt{\frac{2(q^2+q) - q^2 - q}{(q^2+q-q)(q+1)}} \\ &= \frac{1}{\sqrt{q}}. \end{aligned}$$

In addition, we have $\frac{I_{\max}(\widetilde{C}_4)}{I_L} = 1$. Obviously, the codebook $\widetilde{C}_4$ meets the Levenshtein bound and then $\widetilde{C}_4$ is optimal.

This completes the proof. ■

3.3 Conclusions

In this chapter, we firstly studied the characters (including additive characters and multiplicative characters) and character sums (including Gaussian sums, Eisenstein sums and Jacobi sums) over the finite chain ring $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ and the finite non-chain ring $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$. The specific values and absolute values of these character sums were determined by studying their properties and establishing

***Table 3.3.1**: The parameters of codebooks asymptotically meet the Welch bound*

(N,K)	$I_{\max}$	References
$(N_1N_2, \frac{N_1N_2-1}{2})$, where $N_i := 3 \pmod 4$, $i = 1,2$	$\frac{\sqrt{(N_1+1)(N_2+1)}}{N_1N_2-1}$	[53]
$(N_1\cdots N_l, \frac{N_1\cdots N_l-1}{2})$, where $N_i := 3 \pmod 4$, $l > 1$	$\frac{\sqrt{(N_1+1)\cdots(N_l+1)}}{N_1\cdots N_l-1}$	[53]
$(p^n, \frac{p-1}{2p}(p^n + p^{\frac{n}{2}})+1)$, where p is an odd prime	$\frac{(p+1)p^{\frac{n}{2}}}{2pK}$	[52]
$((q-1)^k+q^{k-1}, q^{k-1})$, $k > 2$ and $q \geq 4$	$\frac{\sqrt{q^{k+1}}}{(q-1)^k+(-1)^{k+1}}$	[49]
$((q-1)^k+K, K)$, $k > 2$, where $K = \frac{(q-1)^k+(-1)^{k+1}}{q}$	$\frac{\sqrt{q^{k-1}}}{K}$	[49]
$(2K+1, K)$, where $K = \frac{(2^{s_1}-1)^n(2^{s_2}-1)^n-1}{2}, n \geq 1, s_1, s_2 > 1$	$\frac{2^{\frac{s_1n+s_2n}{2}}}{2K}$	[82]
$(2K+(-1)^{ln}, K)$, where $K = \frac{(2^{s_1}-1)^n\cdots(2^{s_l}-(-1)^{ln})^n-1}{2}, n \geq 1, l > 1, s_i > 1,\ 1 \leq i \leq l$	$\frac{2^{\frac{s_1n+s_2n+\cdots+s_ln}{2}}}{2K}$	[82]
$((q^s-1)^n+K, K)$, $s > 1$ and $n > 1$, where $K = \frac{(q^s-1)^n+(-1)^{n+1}}{q}$	$\frac{\sqrt{q^{sn+1}}}{(q^s-1)^n+(-1)^{n+1}}$	[81]
$((q^s-1)^n+q^{sn-1}, q^{sn-1})$, $s > 1$ and $n > 1$	$\frac{\sqrt{q}+1}{q-1}$	[81]
(q^3+q^2-q, q^2-q)	$\frac{1}{q-1}$	[80]
(kp^2+p^2, p^2), where $k \mid (p+1)$	$\frac{1}{p}$	[80]
$(q(q+4), \frac{q+1}{2})$	$\frac{\sqrt{q}+1}{q-1}$	[69]
$(q, \frac{(q+3)(q+1)}{2})$	$\frac{1}{q+1}$	[69]
(q^3, q^2),(q^3+q^2, q^2)	$\frac{1}{q}$	[79]
$((q-1)q^2, (q-1)q)$,$(q^2-1, (q-1)q)$	$\frac{1}{q-1}$	[79]
$((q-1)q^2, (q-1)^2)$,$(q^3-2q+1, (q-1)^2)$	$\frac{q}{(q-1)^2}$	[79]
$((q-1)^2q, (q-1)^2)$,$(q^3-q^2-q+1, (q-1)^2)$	$\frac{q}{(q-1)^2}$	[79]
$((q-1)^2q, (q-1)(q-2))$,$(q^3-q^2-2q+2, (q-1)(q-2))$	$\frac{q}{(q-1)(q-2)}$	[79]
$((q-1)^3, (q-2)^2)$,$(q^3-2q^2-q+3, (q-2)^2)$	$\frac{q}{(q-2)^2}$	[79]
$(p^n-1, \frac{p^n-1}{2})$, where p is an odd prime	$\frac{\sqrt{p^n}+1}{p^n-1}$	[125]
$(q^2, \frac{(q-1)^2}{2})$, where $q = p^s$ and p is an odd prime	$\frac{q+1}{(q-1)^2}$	[130]
$(q^l+q^{l-1}-1, q^{l-1})$, $l > 2$	$\frac{1}{\sqrt{q^l-1}}$	[133]
$(q^3, q(q-1))$	$\frac{1}{q-1}$	Theorem 3.1.14
$(q^2(q-1), q(q-1))$	$\frac{1}{q-1}$	Theorem 3.1.15
(kr^2, r^2), where $q = r^2, k \mid (r+1)$	$\frac{1}{r}$	Theorem 3.1.17
$(q^2(q-1), q(q-2))$	$\frac{1}{q-2}$	Theorem 3.1.18

the relationship between them. For their applications, we presented seven classes of asymptotically optimal codebooks and two classes of optimal codebooks, which were constructed from character sums over R_1 and R_2. The calculation results showed that the maximum cross-correlation amplitude of these codebooks meets or asymptotically meets the Welch bound or the Levenshtein bound. Compared with the parameters of the relevant codebooks in some references, some codebooks with new parameters constructed in this chapter were listed in Table 3.3.1, and the parameters of these codebooks are flexible. [1]

[1]The main content of this chapter has been published in Appl. Algebr. Eng. Comm. and Adv. Math. Commun..

Chapter 4

Constructions of linear codes with one-dimensional hull

In this chapter, we mainly present some methods for constructing linear codes with one-dimensional hull over finite fields and generalize the construction methods in [16, 70] to more general ones. In Section 4.1, we define two homomorphisms from a finite field into a finite field and then study their properties, which will be useful for constructing linear codes with one-dimensional hull. In Section 4.2, we construct several classes of linear codes with one-dimensional hull by using the general Gaussian sum over finite fields and then obtain some optimal or almost optimal linear codes. This result generalizes the results of [16, 70]. In Section 4.3, based on two homomorphisms (4.12) and (4.13), the construction methods of linear codes with one-dimensional hull are presented. Combined with Lemma 1.2.4, we give some sufficient conditions for a linear code to be a linear code with a one-dimensional hull. Finally, it is worth mentioning that we present a lower bound on the minimum distance of linear codes over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$.

4.1 Homomorphisms

Let $\mathbb{F}_{r^m}$ denote the finite field of order r^m, where r is a prime number and m is a positive integer. Let $\mathbb{F}_{r^m}^* = \mathbb{F}_{r^m} \backslash \{0\}$. Let $\overline{\mathbb{F}}_q$ be the algebraic closure of the finite field $\mathbb{F}_q$.

Let φ be a homomorphism from $\mathbb{F}_{r^m}^*$ into $\overline{\mathbb{F}}_q^*$, that is, a mapping from $\mathbb{F}_{r^m}^*$ into $\overline{\mathbb{F}}_q^*$ with $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in \mathbb{F}_{r^m}^*$. Define $\overline{\varphi}(x) := \varphi(x^{-1})$. Let φ_0 be the trivial homomorphism, which is defined by $\varphi_0(x) = 1$ for all $x \in \mathbb{F}_{r^m}^*$.

The following lemma gives the orthogonality relation of the homomorphism φ.

Lemma 4.1.1 *Let φ be defined as above. Then we have*

$$\sum_{x \in \mathbb{F}_{r^m}^*} \varphi(x) = \begin{cases} r^m - 1, & \text{if } \varphi = \varphi_0; \\ 0, & \text{if } \varphi \neq \varphi_0. \end{cases}$$

Proof: The proof is similar to that of [77, Theorem 5.4] and omitted here. ■

Let χ be a homomorphism from $\mathbb{F}_{r^m}$ into $\overline{\mathbb{F}}_q^*$, that is, a mapping from $\mathbb{F}_{r^m}$ into $\overline{\mathbb{F}}_q^*$ with $\chi(x+y)=\chi(x)\chi(y)$ for all $x,y\in\mathbb{F}_{r^m}$. Define $\overline{\chi}(x):=\chi(-x)$. Let χ_0 be the trivial homomorphism, which is defined by $\chi_0(x)=1$ for all $x\in\mathbb{F}_{r^m}$.

We also have the following lemma, which presents the orthogonality relation of the homomorphism χ.

Lemma 4.1.2 *Let χ be defined as above. Then we have*

$$\sum_{x\in\mathbb{F}_{r^m}}\chi(x)=\begin{cases} r^m, & \text{if } \chi=\chi_0;\\ 0, & \text{if } \chi\neq\chi_0.\end{cases}$$

Proof: The proof is similar to that of [77, Theorem 5.4] and omitted here. ■

According to the definition of φ and χ, we define the sums

$$g(\varphi,\chi)=\sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)\chi(x)$$

and

$$\overline{g(\varphi,\chi)}=g(\overline{\varphi},\overline{\chi})=\sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x^{-1})\chi(-x).$$

The following results show the value of the sum $g(\varphi,\chi)$.

Lemma 4.1.3 *Let φ and χ be defined as above. Then the sum $g(\varphi,\chi)$ satisfies*

$$g(\varphi,\chi)=\begin{cases} r^m-1, & \text{if } \varphi=\varphi_0 \text{ and } \chi=\chi_0;\\ -1, & \text{if } \varphi=\varphi_0 \text{ and } \chi\neq\chi_0;\\ 0, & \text{if } \varphi\neq\varphi_0 \text{ and } \chi=\chi_0.\end{cases}$$

Proof: The conclusion follows directly from Lemmas 4.1.1 and 4.1.2. ■

Lemma 4.1.4 *Let p be the characteristic of $\mathbb{F}_q$. Let φ and χ be defined as above. If $\varphi\neq\varphi_0$ and $\chi\neq\chi_0$, then*

$$g(\varphi,\chi)\overline{g(\varphi,\chi)}=r^m\in\mathbb{F}_p.$$

Proof: For $\varphi\neq\varphi_0$ and $\chi\neq\chi_0$, we get

$$\begin{aligned} g(\varphi,\chi)\overline{g(\varphi,\chi)} &= \sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)\chi(x)\sum_{y\in\mathbb{F}_{r^m}^*}\varphi(y^{-1})\chi(-y)\\ &= \sum_{x,y\in\mathbb{F}_{r^m}^*}\varphi(xy^{-1})\chi(x-y)\\ &\xrightarrow{x\longrightarrow xy} \sum_{x,y\in\mathbb{F}_{r^m}^*}\varphi(x)\chi(y(x-1))\\ &= \varphi(1)\sum_{y\in\mathbb{F}_{r^m}^*}\chi(0)+\sum_{x\in\mathbb{F}_{r^m}^*\setminus\{1\}}\varphi(x)\sum_{y\in\mathbb{F}_{r^m}^*}\chi(y(x-1))\\ &= r^m-1-\sum_{x\in\mathbb{F}_{r^m}^*\setminus\{1\}}\varphi(x)\\ &= r^m. \end{aligned}$$

This completes the proof of this lemma. ■

The study of the behavior of the sum $g(\varphi,\chi)$ under various transformations of the φ or χ leads to a number of useful identities.

Lemma 4.1.5 *Let φ and χ be defined as above. Then we have the following results.*

(1) $g(\varphi,\overline{\chi}) = \varphi(-1)g(\varphi,\chi)$;

(2) $g(\overline{\varphi},\chi) = \varphi(-1)\overline{g(\varphi,\chi)}$;

(3) $g(\varphi,\chi)g(\overline{\varphi},\chi) = \varphi(-1)r^m$ *for* $\varphi \neq \varphi_0$ *and* $\chi \neq \chi_0$;

(4) $(g(\varphi,\chi))^{p^s} = g(\varphi^{p^s},\chi^{p^s})$, *where p is the characteristic of $\mathbb{F}_q$ and s is a positive integer.*

Proof: The results of (1)-(3) are obvious by the definition $g(\varphi,\chi)$ and Lemma 4.1.4. Next, we prove the result of (4). Combined with the definitions of φ and χ, we have

$$(g(\varphi,\chi))^{p^s} = \left(\sum_{x\in\mathbb{F}_{r^m}^*} \varphi(x)\chi(x)\right)^{p^s} = \sum_{x\in\mathbb{F}_{r^m}^*} (\varphi(x))^{p^s}(\chi(x))^{p^s} = \sum_{x\in\mathbb{F}_{r^m}^*} \varphi^{p^s}(x)\chi^{p^s}(x) = g(\varphi^{p^s},\chi^{p^s}).$$ ■

4.2 Constructions of the first class of linear codes with one-dimensional hull

Let $\mathcal{G} = \{x_i : 1 \le i \le v\}$ be a finite abelian group of order v. Define a $v \times v$ matrix $P = (p_{ij})$ by

$$p_{ij} \;=\; \rho(x_j - x_i),$$

where $\rho : \mathcal{G} \longrightarrow \mathbb{C}$ is a function. Let $\chi : \mathcal{G} \longrightarrow \mathbb{C}^*$ be a character, i.e., a group homomorphism from $\mathcal{G} \longrightarrow \mathbb{C}^*$. Then one can check that (see [5, 16, 70]):

$$P\begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^v \rho(x_i - x_1)\chi(x_i) \\ \sum_{i=1}^v \rho(x_i - x_2)\chi(x_i) \\ \vdots \\ \sum_{i=1}^v \rho(x_i - x_v)\chi(x_i) \end{pmatrix} = \sum_{x\in\mathcal{G}} \rho(x)\chi(x) \begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix}. \qquad (4.1)$$

That is to say, $(\chi(x_1),\chi(x_2),\ldots,\chi(x_v))^T$ is an eigenvector of P with eigenvalue $\sum_{x\in\mathcal{G}} \rho(x)\chi(x)$, where "$T$" denotes the transpose operator. It is well known that $\mathcal{G}$ has v characters, each of which gives an eigenvector. In view of the orthogonality relations for characters, these eigenvectors are linearly independent. Let $\widehat{\mathcal{G}}$ be the group of characters of $\mathcal{G}$. Then the multiset

$$\left\{\sum_{x\in\mathcal{G}} \rho(x)\chi(x) : \chi \in \widehat{\mathcal{G}}\right\}$$

presents all eigenvalues of the matrix P.

Similarly, we can obtain the following result:

$$P^T \begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{v} \rho(x_1 - x_i)\chi(x_i) \\ \sum_{i=1}^{v} \rho(x_2 - x_i)\chi(x_i) \\ \vdots \\ \sum_{i=1}^{v} \rho(x_v - x_i)\chi(x_i) \end{pmatrix} = \sum_{x \in \mathcal{G}} \rho(x)\overline{\chi}(x) \begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix}. \quad (4.2)$$

That is to say, $(\chi(x_1), \chi(x_2), \ldots, \chi(x_v))^T$ is an eigenvector of P^T with eigenvalue $\sum_{x \in \mathcal{G}} \rho(x)\overline{\chi}(x)$. Then the multiset

$$\left\{ \sum_{x \in \mathcal{G}} \rho(x)\overline{\chi}(x) : \chi \in \widehat{\mathcal{G}} \right\}$$

presents all eigenvalues of the matrix P^T.

Combined Eq. (4.1) with Eq. (4.2), we have

$$PP^T \begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix} = P \sum_{x \in \mathcal{G}} \rho(x)\overline{\chi}(x) \begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix}$$

$$= \sum_{x \in \mathcal{G}} \rho(x)\overline{\chi}(x) P \begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix} = \sum_{x \in \mathcal{G}} \rho(x)\overline{\chi}(x) \sum_{x \in \mathcal{G}} \rho(x)\chi(x) \begin{pmatrix} \chi(x_1) \\ \chi(x_2) \\ \vdots \\ \chi(x_v) \end{pmatrix}.$$

Then the multiset

$$\left\{ \sum_{x \in \mathcal{G}} \rho(x)\chi(x) \sum_{x \in \mathcal{G}} \rho(x)\overline{\chi}(x) : \chi \in \widehat{\mathcal{G}} \right\} \quad (4.3)$$

presents all eigenvalues of the matrix PP^T.

Next, we describe constructions of linear codes with one-dimensional hull from Gaussian sums over finite fields.

Throughout this section, let q be a power of p, where p is a prime number. Suppose that $\mathcal{G} = \mathbb{F}_{r^m}$, where r is a prime number and m is a positive integer. Let ψ be a nontrivial multiplicative character of $\mathbb{F}_{r^m}$ and $N > 1$ the order of ψ (that is, N is the least positive integer such that $\psi^N = \psi_0$). Let $\rho : \mathcal{G} \longrightarrow \mathbb{C}$ be a function. The function ρ satisfies $\rho|_{\mathbb{F}_{r^m}^*} = \psi$, i.e., for any $x \in \mathbb{F}_{r^m}^*$, $\rho(x) = \psi(x)$. Define the $r^m \times r^m$ matrix $P = (p_{ij})$ by $p_{ij} = \rho(x_j - x_i)$. By (4.3), we know that the multiset

$$\left\{ \lambda_a := \sum_{x \in \mathbb{F}_{r^m}} \rho(x)\chi_a(x) \sum_{x \in \mathbb{F}_{r^m}} \rho(x)\overline{\chi}_a(x) : a \in \mathbb{F}_{r^m} \right\}$$

presents all eigenvalues of the matrix PP^T.

Based on the discussion above, and combine with Lemma 2.1.8(2), we have

$$\begin{aligned}
\lambda_a &:= \sum_{x\in\mathbb{F}_{r^m}} \rho(x)\chi_a(x) \sum_{x\in\mathbb{F}_{r^m}} \rho(x)\overline{\chi}_a(x) \\
&= \left(\rho(0)+\sum_{x\in\mathbb{F}_{r^m}^*} \psi(x)\chi_a(x)\right)\left(\rho(0)+\sum_{x\in\mathbb{F}_{r^m}^*} \psi(x)\overline{\chi}_a(x)\right) \\
&= \big(\rho(0)+G(\psi,\chi_a)\big)\big(\rho(0)+G(\psi,\overline{\chi}_a)\big) \\
&= \big(\rho(0)+G(\psi,\chi_a)\big)\big(\rho(0)+\psi(-1)G(\psi,\chi_a)\big) \\
&= \rho^2(0)+G(\psi,\chi_a)\big(\rho(0)+\psi(-1)\rho(0)+\psi(-1)G(\psi,\chi_a)\big).
\end{aligned}$$

Hence, we obtain

$$\lambda_a = \begin{cases} \rho^2(0), & \text{if } a=0; \\ \rho^2(0)+G(\psi,\chi_a)\big(\rho(0)+\psi(-1)\rho(0)+\psi(-1)G(\psi,\chi_a)\big), & \text{if } a\in\mathbb{F}_{r^m}^*. \end{cases} \tag{4.4}$$

4.2.1 The case $\psi(-1)=1$

Assume that $\psi(-1)=1$. Based on (4.4), for any $a\in\mathbb{F}_{r^m}^*$, we have

$$\begin{aligned}
\lambda_a &= \rho^2(0)+G(\psi,\chi_a)(2\rho(0)+G(\psi,\chi_a)) \\
&= \rho^2(0)+\overline{\psi}(a)G(\psi)(2\rho(0)+\overline{\psi}(a)G(\psi)).\text{(By Lemma 2.1.8(1))}
\end{aligned} \tag{4.5}$$

Assume that there exists a number field K and an element $\beta\in\mathbb{O}_K$ ($\mathbb{O}_K$ is the ring of algebraic integers in K) satisfying the following conditions:

$$\begin{aligned}
&(i)\ \zeta_N\in K \text{ (and then } \zeta_N\in\mathbb{O}_K); \\
&(ii)\ G(\psi)\in K \text{ (and then } G(\psi)\in\mathbb{O}_K); \\
&(iii)\ \text{there exists a prime ideal } \mathcal{P} \text{ in } \mathbb{O}_K \text{ over } p \text{ such that } \zeta_N+\mathcal{P}\in\mathbb{F}_q \text{ and} \\
&\quad G(\psi)+\mathcal{P}\in\mathbb{F}_q; \\
&(iv)\ \beta^2 := -1 \pmod{\mathcal{P}}.
\end{aligned} \tag{4.6}$$

Let $\bar{\beta}\in\mathbb{O}_K/\mathcal{P}$ be the image of β by the natural homomorphism $\mathbb{O}_K\longrightarrow\mathbb{O}_K/\mathcal{P}$, i.e., $\beta\longmapsto\bar{\beta}=\beta+\mathcal{P}$. Let $\rho(0)=\beta\in\mathbb{O}_K$. Define $\bar{P}=(\bar{p}_{ij})$, where $\bar{p}_{ij}=p_{ij}+\mathcal{P}$. By Conditions (i) and (iii), we have $\bar{p}_{ij}\in\mathbb{F}_q$. It then follows that $\bar{P}\in M_{r^m}(\mathbb{F}_q)$, where $M_{r^m}(\mathbb{F}_q)$ denotes the ring of all square matrices of order r^m over $\mathbb{F}_q$. According to the conditions (i), (ii) and (iv), we have $\lambda_a\in\mathbb{O}_K$. Define $\bar{\lambda}_a := \lambda_a+\mathcal{P}$. Then $\bar{\lambda}_a\in\mathbb{F}_q$. Hence, the multiset

$$\bar{\lambda}_a = \begin{cases} -1+\mathcal{P}, & \text{if } a=0; \\ -1+G(\psi,\chi_a)(2\beta+G(\psi,\chi_a))+\mathcal{P}, & \text{if } a\in\mathbb{F}_{r^m}^*. \end{cases} \tag{4.7}$$

presents all eigenvalues of the matrix $\bar{P}\bar{P}^T$.

Before giving the main conclusion, we first give the following lemma.

Lemma 4.2.1 *Let the symbols be the same as above. Let ψ be a nontrivial multiplicative character of order N over $\mathbb{F}_{r^m}$ and $(r,p)=1$. Then for any $a \in \mathbb{F}_{r^m}^*$, we have*

$$-1+G^2(\psi,\chi_a)+\mathcal{P} \neq -1+\mathcal{P},$$

i.e., $-1+G^2(\psi,\chi_a) \neq -1 \pmod{\mathcal{P}}$.

Proof: For any $a \in \mathbb{F}_{r^m}^*$, we have $|G(\psi,\chi_a)|^2 = r^m$ by Lemma 2.1.7. Since $(r,p)=1$, then

$$|G(\psi,\chi_a)|^2 = r^m \notin \mathcal{P}, \text{i.e.,} G(\psi,\chi_a)\overline{G(\psi,\chi_a)} = r^m \notin \mathcal{P}.$$

Hence, $G(\psi,\chi_a) \notin \mathcal{P}$ and $\overline{G(\psi,\chi_a)} \notin \mathcal{P}$. Based on this, we obtain that $G^2(\psi,\chi_a) \notin \mathcal{P}$.

Hence, we have $-1-G^2(\psi,\chi_a) \neq -1 \pmod{\mathcal{P}}$. ■

In summary, it is easy for us to draw the following theorem.

Theorem 4.2.2 *Let $\mathbb{F}_{r^m}$ be a finite field, where r is a prime number and m is a positive integer. Let ψ be a nontrivial multiplicative character of order N over $\mathbb{F}_{r^m}^*$, where N is a positive integer. Assume that there exist a number field K and an element $\beta \in \mathbb{O}_K$ satisfying the four conditions in (4.6). Define $\rho : \mathbb{F}_{r^m} \longrightarrow \mathbb{C}$ by*

$$\rho(x) = \begin{cases} \beta, & \text{if } x=0; \\ \psi(x), & \text{if } x \in \mathbb{F}_{r^m}^*. \end{cases}$$

Define $P=(p_{ij}) \in M_{r^m}(\mathbb{O}_K)$ by $p_{ij}=\rho(x_j-x_i)$. Define $\bar{P}=(\bar{p}_{ij})$, where $\bar{p}_{ij}=p_{ij}+\mathcal{P} \in \mathbb{F}_{p^f}$, where f is the degree of $\mathcal{P}$. Let $\mathcal{C}$ be the linear code over $\mathbb{F}_{p^f}$ with generator matrix $[I_{r^m},\bar{P}]$. Let $\psi(-1)=1$. Then we have the following.

(1) If $p=2$ and r is odd, then $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull.

(2) If $p \geq 3$ is odd, $(r,p)=1$ and $2\beta+G(\psi,\chi_a) \neq 0 \pmod{\mathcal{P}}$ for all $a \in \mathbb{F}_{r^m}^*$, then $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull.

Proof: Since $\psi(-1)=1$, it follows from (4.7) that all eigenvalues of the matrix $\bar{P}\bar{P}^T$ are

$$\bar{\lambda}_a = \begin{cases} -1+\mathcal{P}, & \text{if } a=0; \\ -1+G(\psi,\chi_a)(2\beta+G(\psi,\chi_a))+\mathcal{P}, & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases}$$

(1) If $p=2$ and r is odd, then $2 \in \mathcal{P}$. So we obtain that the eigenvalues of the matrix $\bar{P}\bar{P}^T$ are -1 and $-1+G^2(\psi,\chi_a)+\mathcal{P}$. By Lemma 4.2.1, we claim that $-1+G^2(\psi,\chi_a) \neq -1 \pmod{\mathcal{P}}$. Therefore, the matrix $\bar{P}\bar{P}^T$ has an eigenvalue -1 with multiplicity 1. It then follows from Lemma 1.2.4 that $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull.

(2) For $a=0$, we get $\lambda_a=\lambda_0:=-1 \pmod{\mathcal{P}}$. In view of $(r,p)=1$, we have $G(\psi,\chi_a) \notin \mathcal{P}$ by the proof of Lemma 4.2.1. Based on this and combined with $2\beta+G(\psi,\chi_a) \neq 0 \pmod{\mathcal{P}}$ for all $a \in \mathbb{F}_{r^m}^*$, we get $\bar{\lambda}_a \neq -1+\mathcal{P}$ for all $a \in \mathbb{F}_{r^m}^*$. Hence, the value distribution of eigenvalues of $\bar{P}\bar{P}^T$ is given as follows:

$$\bar{\lambda}_a = \begin{cases} -1+\mathcal{P}, & \text{occurs once;} \\ -1+G(\psi,\chi_a)(2\beta+G(\psi,\chi_a))+\mathcal{P} \neq -1+\mathcal{P}, & \text{others.} \end{cases}$$

Hence, -1 is an eigenvalue of the matrix $\bar{P}\bar{P}^T$ with (algebraic) multiplicity 1. By Lemma 1.2.4, $\mathcal{C}$ is a $[2r^m, r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull.

This completes the proof. ■

In the following, we present some concrete examples. In addition, the computations are carried out using Magma software [2].

Example 4.2.3 *Let $p=2, r=7, m=1$ and $N=3$. Then $K=\mathbb{Q}(\zeta_3)$. It is easy to see from Lemma 2.3.1(1) that the degree of $\mathcal{P}$ over p is equal to 2. Let $\mathbb{F}_4^* = \langle\alpha\rangle$, where α is a root of $x^2+x+1 \in \mathbb{F}_2[x]$. Then $\mathcal{C}$ is a $[14,7,6]$ linear code over $\mathbb{F}_4$ with one-dimensional hull and its generator matrix $[I_7, \bar{P}]$, where*

$$\bar{P} = \begin{pmatrix} 1 & 1 & \alpha & 1 & \alpha^2 & \alpha^2 & \alpha \\ 1 & 1 & \alpha & \alpha^2 & \alpha & 1 & \alpha^2 \\ \alpha & \alpha & 1 & \alpha^2 & 1 & \alpha^2 & 1 \\ 1 & \alpha^2 & \alpha^2 & 1 & 1 & \alpha & \alpha \\ \alpha^2 & \alpha & 1 & 1 & 1 & \alpha & \alpha^2 \\ \alpha^2 & 1 & \alpha^2 & \alpha & \alpha & 1 & 1 \\ \alpha & \alpha^2 & 1 & \alpha & \alpha^2 & 1 & 1 \end{pmatrix},$$

which is optimal according to the Database [45]. Its dual code $\mathcal{C}^\perp$ is also an optimal $[14,7,6]$ linear code over $\mathbb{F}_4$. Moreover, the hull of $\mathcal{C}$ is a $[14,1,14]$ cyclic code over $\mathbb{F}_4$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Example 4.2.4 *Let $p=3, r=17, m=1$ and $N=4$. Then $K=\mathbb{Q}(\zeta_4)$. It is easy to see from Lemma 2.3.1(1) that the degree of $\mathcal{P}$ over p is equal to 2. Let $\mathbb{F}_9^* = \langle\alpha\rangle$, where α is a root of $x^2+2x+2 \in \mathbb{F}_3[x]$. Then $\mathcal{C}$ is a $[34,17,11]$ linear code over $\mathbb{F}_9$ with one-dimensional hull, which is almost optimal in the sense that the minimal distance of the optimal linear code with length 34 and dimension 17 is 12 over $\mathbb{F}_9$ according to the Database [45]. Its dual code $\mathcal{C}^\perp$ is also an almost optimal $[34,17,11]$ linear code over $\mathbb{F}_9$. Moreover, the hull of $\mathcal{C}$ is a $[34,1,34]$ quasi-cyclic code of index 2 over $\mathbb{F}_9$.*

Taking the multiplicative character ψ with the semi-primitive case (see [16]) in Theorem 4.2.2, we obtain the result derived from [16, Theorem 2], which means that the result in [16, Theorem 2] is a special case of our results, details are as follows.

Corollary 4.2.5 *[16, Theorem 2] Let r be a prime number and N an odd positive integer. Assume that there exists a least positive integer s such that $r^s := -1 \pmod N$. Let $m = 2s\gamma$ for some positive integer γ. Suppose that ψ is a multiplicative character of order N over $\mathbb{F}_{r^m}^*$. Let p be a prime and $\mathcal{P}$ a prime ideal in $\mathbb{O}_K$ over p, where $K=\mathbb{Q}(\zeta_N)$. Assume that exists $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ satisfying that $\bar{\beta}^2 = -1$ and let $\beta \in \mathbb{O}_K$ be a preimage of $\bar{\beta}$ by the natural homomorphism $\mathbb{O}_K \longrightarrow \mathbb{O}_K/\mathcal{P}$, i.e., $\beta \longmapsto \bar{\beta} = \beta + \mathcal{P}$. Define ρ by*

$$\rho(x) = \begin{cases} \beta, & \text{if } x = 0; \\ \psi(x), & \text{if } x \in \mathbb{F}_{r^m}^*. \end{cases}$$

Define $P=(p_{ij})\in M_{r^m}(\mathbb{O}_K)$ *by* $p_{ij}=\rho(x_j-x_i)$. *Define* $\bar{P}=(\bar{p}_{ij})$, *where* $\bar{p}_{ij}=p_{ij}+\mathcal{P}\in\mathbb{F}_{p^f}$, *where* f *is the degree of* $\mathcal{P}$. *Let* $\mathcal{C}$ *be the linear code over* $\mathbb{F}_{p^f}$ *with generator matrix* $[I_{r^m},\bar{P}]$.

(1) When $p=2$ *and* r *is odd,* $\mathcal{C}$ *is a* $[2r^m,r^m]$ *linear code over* $\mathbb{F}_{p^f}$ *with one-dimensional hull.*

(2) When $p:=3 \pmod 4$ *and* $r^{\frac{m}{2}}:=1 \pmod p$, $\mathcal{C}$ *is a* $[2r^m,r^m]$ *linear code over* $\mathbb{F}_{p^f}$ *with one-dimensional hull.*

Proof: We claim that $K=\mathbb{Q}(\zeta_N)$ satisfies the four conditions in (4.6):

(i) $\zeta_N\in\mathbb{Q}(\zeta_N)=K$;

(ii) $G(\psi)=\pm r^{\frac{m}{2}}=\pm r^{\gamma_s}\in\mathbb{Z}\subseteq K$; (By Lemma 1 in [16])

(iii) $\zeta_N+\mathcal{P}\in\mathbb{O}_K/\mathcal{P}\cong\mathbb{F}_{p^f}$ and $G(\psi)+\mathcal{P}=\pm r^{\gamma_s}+\mathcal{P}\in\mathbb{F}_{p^f}$;

(iv) If $p=2$, we take $\bar{\beta}=1\in\mathbb{F}_{p^f}$. Taking $\beta\in\mathbb{O}_K$ such that $\bar{\beta}=\beta+\mathcal{P}$. If $p:=3 \pmod 4$, there exists an element $\beta\in\mathbb{O}_K$ satisfying that $\beta^2:=-1 \pmod{\mathcal{P}}$ by the assumed condition.

We first prove that $\psi(-1)=1$. If $r=2$, then we have $\psi(-1)=\psi(1)=1$. If r is an odd prime, one can check that $N\mid\frac{r^m-1}{2}$. Assume that α is a generator of $\mathbb{F}_{r^m}^*$. Then $\psi(-1)=\psi(\alpha^{\frac{r^m-1}{2}})=(\psi(\alpha))^{\frac{r^m-1}{2}}=(\psi(\alpha))^{N\cdot\frac{r^m-1}{2N}}=1$.

Secondly, it is easy to check that $(r,p)=1$.

When $p=2$ and r is odd, it then follows from Theorem 4.2.2(1) that $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull.

Suppose now that $p:=3 \pmod 4$ and $r^{\frac{m}{2}}:=1 \pmod p$. In this case, we check that $2\beta+G(\psi,\chi_a):\neq 0 \pmod{\mathcal{P}}$ for all $a\in\mathbb{F}_{r^m}^*$. Suppose on the contrary that $2\beta+G(\psi,\chi_a):=0 \pmod{\mathcal{P}}$ for some $a\in\mathbb{F}_{r^m}^*$. Then $2\beta\pm\bar{\psi}(a)r^{\frac{m}{2}}:=0 \pmod{\mathcal{P}}$. Since $r^{\frac{m}{2}}:=1 \pmod p$, we get

$$\begin{aligned}
2\beta\pm\bar{\psi}(a) &:= 0 \pmod{\mathcal{P}}\\
\Longrightarrow \bar{\psi}(a) &:= \pm 2\beta \pmod{\mathcal{P}}\\
\Longrightarrow \bar{\psi}(a)^{(p-1)} &:= (\pm 2\beta)^{(p-1)} \pmod{\mathcal{P}}\\
\Longrightarrow \bar{\psi}(a)^{(p-1)} &:= (-1)^{\frac{p-1}{2}} \pmod{\mathcal{P}}\\
\Longrightarrow \bar{\psi}(a)^{(p-1)N} &:= (-1)^{\frac{p-1}{2}N} \pmod{\mathcal{P}}\\
\Longrightarrow 1 &:= (-1)^{\frac{p-1}{2}N} \pmod{\mathcal{P}}.
\end{aligned}$$

Since $p:=3 \pmod 4$ and N is odd, we have $(-1)^{\frac{p-1}{2}N}:=-1 \pmod{\mathcal{P}}$. Hence, $1:=(-1)^{\frac{p-1}{2}N}=-1 \pmod{\mathcal{P}}$, a contradiction (since by the assumption that p is odd). From this, we obtain that $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull by Theorem 4.2.2(2). ■

Remark 4.2.6 *In [16, Theorem 2], N is an odd prime. In fact, if we only claim that N is an odd positive integer, the result is still true.*

When we take the multiplicative character $\psi = \eta$, where η is the quadratic multiplicative character of $\mathbb{F}_{r^m}^*$ (see [70]), we can check that the results in [70, Theorems 3 and 4] are a special case of our results, details as below.

Corollary 4.2.7 *[70, Theorem 3] Let $K = \mathbb{Q}(\sqrt{r})$ and m a integer, where $r := 1 \pmod 4$. Suppose that p is an odd prime such that $p \nmid (r^m + 4)$. Let $\mathbb{O}_K$ be the ring of algebraic integers in K and $\mathcal{P}$ a prime ideal in $\mathbb{O}_K$ over p. Assume that exists $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ satisfying $\bar{\beta}^2 = -1$ and let $\beta \in \mathbb{O}_K$ be a preimage of $\bar{\beta}$ by the natural homomorphism $\mathbb{O}_K \longrightarrow \mathbb{O}_K/\mathcal{P}$, i.e., $\beta \longmapsto \bar{\beta} = \beta + \mathcal{P}$. Define ρ by*

$$\rho(x) = \begin{cases} \beta, & \text{if } x = 0; \\ \eta(x), & \text{if } x \in \mathbb{F}_{r^m}^*, \end{cases}$$

where η is the quadratic multiplicative character of $\mathbb{F}_{r^m}^*$. Define $P = (p_{ij}) \in M_{r^m}(\mathbb{O}_K)$ by $p_{ij} = \rho(x_j - x_i)$. Define $\bar{P} = (\bar{p}_{ij})$, where $\bar{p}_{ij} = p_{ij} + \mathcal{P} \in \mathbb{F}_q$. Let $\mathcal{C}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, \bar{P}]$. Then we have the following.

(1) If $p := 1 \pmod 4$ and $p \neq r$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p-ary linear code with one-dimensional hull.

(2) If $\left(\frac{r}{p}\right) = -1$ and $p := 3 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p^2-ary linear code with one-dimensional hull.

Proof: We claim that $K = \mathbb{Q}(\sqrt{r})$ satisfies the four conditions in (4.6):

(i) Due to $\psi = \eta$, we get $\zeta_N = \zeta_2 = -1 \in \mathbb{Q} \subseteq K$;

(ii) $G(\psi) = G(\eta) = \pm\sqrt{r^m} \in K$;

(iii) $\zeta_N + \mathcal{P} \in \mathbb{O}_K/\mathcal{P}$ and $G(\psi) + \mathcal{P} = G(\eta) + \mathcal{P} \in \mathbb{O}_K/\mathcal{P}$;

(iv) If $p := 1 \pmod 4$, then there exists $\bar{\beta} \in \mathbb{F}_p$ such that $\bar{\beta}^2 = -1$. Taking $\beta \in \mathbb{O}_K$ such that $\bar{\beta} = \beta + \mathcal{P}$. If $\left(\frac{r}{p}\right) = -1$ and $p := 3 \pmod 4$, then $\mathbb{O}_K/\mathcal{P} = \mathbb{F}_{p^2}$ from [70, Lemma 3(2)] and there exists $\bar{\beta} \in \mathbb{F}_{p^2}$ such that $\bar{\beta}^2 = -1$. Taking $\beta \in \mathbb{O}_K$ such that $\bar{\beta} = \beta + \mathcal{P}$.

It is easy to check that $(r, p) = 1$. Since $r := 1 \pmod 4$, we have $r^m := 1 \pmod 4$ and $\psi(-1) = \eta(-1) = 1$.

Next, we need to check that $2\beta + G(\eta, \chi_a) \neq 0 \pmod{\mathcal{P}}$ for all $a \in \mathbb{F}_{r^m}^*$. Suppose on the contrary that $2\beta + G(\eta, \chi_a) := 0 \pmod{\mathcal{P}}$ for some $a \in \mathbb{F}_{r^m}^*$. Then

$$\begin{aligned} G^2(\eta, \chi_a) &:= 4\beta^2 \pmod{\mathcal{P}} \\ \Longrightarrow \bar{\eta}^2(a) G^2(\eta) &:= -4 \pmod{\mathcal{P}} \\ \Longrightarrow r^m &:= -4 \pmod p, \end{aligned}$$

which implies that $p \mid (r^m + 4)$, a contradiction (Since by assumption $p \nmid (r^m + 4)$). Hence, $2\beta + G(\eta, \chi_a) \neq 0 \pmod{\mathcal{P}}$ for all $a \in \mathbb{F}_{r^m}^*$.

Above all, then $\mathcal{C}$ is a $[2r^m, r^m]$ linear code with one-dimensional hull by Theorem 4.2.2. ■

Similarly, we can easily verify that [70, Theorem 4] is a special case of our results in Theorem 4.2.2.

Remark 4.2.8 *In [70, Theorem 3] and [70, Theorem 4], they need the condition "Assume that exists $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ satisfying that $\bar{\beta}^2 = -1$" and this condition was assumed at the beginning of the subsection.*

4.2.2 The case $\psi(-1) = -1$

In this subsection, we assume that $\psi(-1) = -1$. In this case, r must be odd. According to (4.4), for any $a \in \mathbb{F}_{r^m}^*$, we have

$$\begin{aligned} \lambda_a &= \rho^2(0) - G^2(\psi, \chi_a) \\ &= \rho^2(0) - \overline{\psi}^2(a) G^2(\psi) \text{ (By Lemma 2.1.8(1))}. \end{aligned} \tag{4.8}$$

Assume that there exist a number field K and an element $\beta \in \mathbb{O}_K$ ($\mathbb{O}_K$ is the ring of algebraic integers in K) satisfying the following conditions:

$$\begin{aligned} &(i)\ \zeta_N \in K \text{ (and then } \zeta_N \in \mathbb{O}_K); \\ &(ii)\ G^2(\psi) \in K \text{ (and then } G^2(\psi) \in \mathbb{O}_K); \\ &(iii)\ \text{there exists a prime ideal } \mathcal{P} \text{ in } \mathbb{O}_K \text{ over } p \text{ such that } \zeta_N + \mathcal{P} \in \mathbb{O}_K/\mathcal{P} \subseteq \mathbb{F}_q \\ &\quad \text{and} G^2(\psi) + \mathcal{P} \in \mathbb{O}_K/\mathcal{P} \subseteq \mathbb{F}_q; \\ &(iv)\ \beta^2 := -1 \pmod{\mathcal{P}}. \end{aligned} \tag{4.9}$$

Let $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ be the image of β by the natural homomorphism $\mathbb{O}_K \longrightarrow \mathbb{O}_K/\mathcal{P}$, i.e., $\beta \longmapsto \bar{\beta} = \beta + \mathcal{P}$. Let $\rho(0) = \beta \in \mathbb{O}_K$. Define $\bar{P} = (\bar{p}_{ij})$, where $\bar{p}_{ij} = p_{ij} + \mathcal{P}$. By Conditions (i) and (iii), we have $\bar{p}_{ij} \in \mathbb{F}_q$. It then follows that $\bar{P} \in M_{r^m}(\mathbb{F}_q)$, where $M_{r^m}(\mathbb{F}_q)$ denotes the ring of all square matrices of order r^m over $\mathbb{F}_q$. According to the conditions (i), (ii) and (iv), we have $\lambda_a \in \mathbb{O}_K$ and

$$\lambda_a = -1 - G^2(\psi, \chi_a) = -1 - \overline{\psi}^2(a) G^2(\psi). \tag{4.10}$$

Define $\bar{\lambda}_a := \lambda_a + \mathcal{P}$. Then $\bar{\lambda}_a \in \mathbb{F}_q$. Hence, the multiset

$$\bar{\lambda}_a = \begin{cases} -1 + \mathcal{P}, & \text{if } a = 0; \\ -1 - \overline{\psi}^2(a) G^2(\psi) + \mathcal{P}, & \text{if } a \in \mathbb{F}_{r^m}^*, \end{cases} \tag{4.11}$$

presents all eigenvalues of the matrix $\bar{P}\bar{P}^T$. In summary, it is easy for us to draw the following theorem.

Theorem 4.2.9 *Let $\mathbb{F}_{r^m}$ be a finite field, where r is a prime number and m is a positive integer. Let ψ be a nontrivial multiplicative character of order N over $\mathbb{F}_{r^m}^*$, where N is a positive integer. Assume that there exist a number field K and an element $\beta \in \mathbb{O}_K$ satisfying the four conditions in (4.9). Define $\rho : \mathbb{F}_{r^m} \longrightarrow \mathbb{C}$ by*

$$\rho(x) = \begin{cases} \beta, & \text{if } x = 0; \\ \psi(x), & \text{if } x \in \mathbb{F}_{r^m}^*. \end{cases}$$

Define $P = (p_{ij}) \in M_{r^m}(\mathbb{O}_K)$ by $p_{ij} = \rho(x_j - x_i)$. Define $\bar{P} = (\bar{p}_{ij})$, where $\bar{p}_{ij} = p_{ij} + \mathcal{P} \in \mathbb{F}_{p^f}$, where f is the degree of $\mathcal{P}$. Let $\mathcal{C}$ be the linear code over $\mathbb{F}_{p^f}$ with generator matrix $[I_{r^m}, \bar{P}]$. If $\psi(-1) = -1$ and $(r, p) = 1$, then $\mathcal{C}$ is a $[2r^m, r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull.

Proof: It follows from (4.11) that all eigenvalues of the matrix $\bar{P}\bar{P}^T$ are

$$\bar{\lambda}_a = \begin{cases} -1+\mathcal{P}, & \text{if } a=0; \\ -1-G^2(\psi,\chi_a)+\mathcal{P}, & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases}$$

For $a=0$, we get $\lambda_a = \lambda_0 := -1 \pmod{\mathcal{P}}$. For $a \in \mathbb{F}_{r^m}^*$, we obtain $\lambda_a \not\equiv -1 \pmod{\mathcal{P}}$ by Lemma 4.2.1. Hence, the value distribution of eigenvalues of $\bar{P}\bar{P}^T$ is given as follows:

$$\bar{\lambda}_a = \begin{cases} -1+\mathcal{P}, & \text{occurs once;} \\ -1-G^2(\rho,\chi_a)+\mathcal{P} \neq -1+\mathcal{P}, & \text{others.} \end{cases}$$

Hence, -1 is an eigenvalue of the matrix $\bar{P}\bar{P}^T$ with (algebraic) multiplicity 1. By Lemma 1.2.4, $\mathcal{C}$ is a $[2r^m, r^m]$ linear code over $\mathbb{F}_{p^f}$ with one-dimensional hull.

This completes the proof. ■

In the following, we give an example to illustrate Theorem 4.2.9. In addition, the computations are carried out using Magma software [2].

Example 4.2.10 *Let $p=3, r=5, m=1$ and $N=4$. Assume that $K=\mathbb{Q}(\zeta_{20}), \mathbb{O}_K = \mathbb{Z}[\zeta_{20}]$. Then $\mathbb{O}_K/\mathcal{P} = \mathbb{F}_{81}$ by Lemma 2.3.1, where $\mathcal{P}$ is the prime ideal in $\mathbb{O}_K$ over p. Let $\mathbb{F}_{81}^* = \langle\alpha\rangle$, where α is a root of $x^4+2x^3+2 \in \mathbb{F}_3[x]$. Then $\mathcal{C}$ is a $[10,5,4]$ linear code over $\mathbb{F}_{81}$ with one-dimensional hull and its generator matrix $[I_5, \bar{P}]$, where*

$$\bar{P} = \begin{pmatrix} \alpha^{20} & \alpha^{20} & -1 & -\alpha^{20} & 1 \\ -\alpha^{20} & \alpha^{20} & \alpha^{20} & 1 & -1 \\ 1 & -\alpha^{20} & \alpha^{20} & -1 & \alpha^{20} \\ \alpha^{20} & -1 & 1 & \alpha^{20} & -\alpha^{20} \\ -1 & 1 & -\alpha^{20} & \alpha^{20} & \alpha^{20} \end{pmatrix}.$$

Moreover, the hull of $\mathcal{C}$ is a $[10,1,10]$ quasi-cyclic code of index 2 over $\mathbb{F}_{81}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \alpha^{20} & \alpha^{20} & \alpha^{20} & \alpha^{20} & \alpha^{20} \end{pmatrix}.$$

In view of Theorem 4.2.9, we present a concrete result as corollary in the following. Before this, we first give a lemma as follows, which will be useful in the sequel.

Lemma 4.2.11 *Let φ be a generator of $\widehat{\mathbb{F}}_{r^m}^*$ and ψ a multiplicative character of order N over $\mathbb{F}_{r^m}^*$. If r and $\frac{r^m-1}{N}$ are odd, then $\psi(-1)=-1$.*

Proof: In view of $\widehat{\mathbb{F}}_{r^m}^* = \langle\varphi\rangle$, then all the multiplicative characters of order N have the form $\varphi^{\frac{r^m-1}{N}j}$, where $\gcd(j,N)=1$. Since r and $\frac{r^m-1}{N}$ are odd, then N is even. Because $\gcd(j,N)=1$, we obtain that j is odd. Hence, we have $\varphi^{\frac{r^m-1}{N}j}(-1) = (\varphi(-1))^{\frac{r^m-1}{N}j} = (-1)^{\frac{r^m-1}{N}j} = -1$ for all odd number j. Since ψ is a multiplicative character of order N over $\mathbb{F}_{r^m}^*$, we get $\psi(-1)=-1$. ■

Corollary 4.2.12 *Let r be an odd prime number and m a positive integer. Let $N \mid (r^m-1)$ and ψ be a multiplicative character of order N over $\mathbb{F}_{r^m}^*$, where N is a positive*

integer. Assume that $\frac{r^m-1}{N}$ *is odd. Let* p *be an odd prime and* $(r,p)=1$. *Assume that* q *is a power of* p *and* q *satisfies* $4 \mid (q-1)$ *and* $Nr \mid (q-1)$. *Let* $K=\mathbb{Q}(\zeta_{q-1})$ *and* $\mathbb{O}_K=\mathbb{Z}[\zeta_{q-1}]$. *Let* $\mathcal{P}$ *be a prime ideal in* $\mathbb{O}_K$ *over* p. *Assume that there exists* $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ *satisfying that* $\bar{\beta}^2=-1$ *and let* $\beta \in \mathbb{O}_K$ *be a preimage of* $\bar{\beta}$ *by the natural homomorphism* $\mathbb{O}_K \longrightarrow \mathbb{O}_K/\mathcal{P}$, *i.e.,* $\beta \longmapsto \bar{\beta}=\beta+\mathcal{P}$. *Let* $\rho : \mathbb{F}_{r^m} \longrightarrow \mathbb{C}$ *be the function defined by*

$$\rho(x)=\begin{cases} \beta, & \text{if } x=0; \\ \psi(x), & \text{if } x \in \mathbb{F}_{r^m}^*. \end{cases}$$

We obtain the $r^m \times r^m$ *matrix* $P=(p_{ij})$ *by* $p_{ij}=\rho(x_j-x_i)$. *Define* $\bar{P}=(\bar{p}_{ij})$, *where* $\bar{p}_{ij}=p_{ij}+\mathcal{P} \in \mathbb{O}_K/\mathcal{P}=\mathbb{F}_q$. *It then follows that* $\bar{P} \in M_{r^m}(\mathbb{F}_q)$. *Let* $\mathcal{C}$ *be the linear code over* $\mathbb{F}_q$ *with generator matrix* $[I_{r^m},\bar{P}]$. *Hence,* $\mathcal{C}$ *is a* $[2r^m,r^m]$ *linear code over* $\mathbb{F}_q$ *with one-dimensional hull.*

Proof: We claim that $K=\mathbb{Q}(\zeta_{q-1})$ satisfies the four conditions in (4.9):

(*i*) Since $N \mid (q-1)$, we get $\zeta_N \in \mathbb{Q}(\zeta_N) \subseteq \mathbb{Q}(\zeta_{q-1})=K$;

(*ii*) Due to $r \mid (q-1)$, we obtain $\zeta_r \in \mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_{q-1})=K$. Hence, $G^2(\psi) \in \mathbb{Q}(\zeta_N,\zeta_r)=\mathbb{Q}(\zeta_{Nr}) \subseteq \mathbb{Q}(\zeta_{q-1})=K$;

(*iii*) By the discussion in Section 2.3, we have $\mathbb{O}_K/\mathcal{P} \cong \mathbb{F}_q$. So $\zeta_N+\mathcal{P} \in \mathbb{F}_q$ and $G^2(\psi)+\mathcal{P} \in \mathbb{F}_q$;

(*iv*) Due to $4 \mid (q-1)$, there exists an element $\bar{\beta} \in \mathbb{F}_q$ such that $\bar{\beta}^2=-1$. Since $\mathbb{O}_K/\mathcal{P} \cong \mathbb{F}_q$, then there exists an element $\beta \in \mathbb{O}_K$ such that $\bar{\beta}=\beta+\mathcal{P}$ and $\beta^2 := -1 \pmod{\mathcal{P}}$.

Since r and $\frac{r^m-1}{N}$ are odd, we get $\psi(-1)=-1$ by Lemma 4.2.11. Combining with $(r,p)=1$ and by Theorem 4.2.9, we obtain that $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull. ■

Next, we give a concrete example of Corollary 4.2.12. In addition, the computations are carried out using Magma software [2].

Example 4.2.13 *Let* $p=5, q=5^2=25, r=3, m=2$ *and* $N=8$. *Then we get* q,r,N *satisfying the conditions in Corollary 4.2.12. Let* $K=\mathbb{Q}(\zeta_{24}), \mathbb{O}_K=\mathbb{Z}[\zeta_{24}]$ *and* $\mathbb{O}_K/\mathcal{P}=\mathbb{F}_{25}$, *where* $\mathcal{P}$ *is the prime ideal in* $\mathbb{O}_K$ *over* p. *Let* $\mathbb{F}_{25}^*=\langle\alpha\rangle$, *where* α *is a root of* $x^2+4x+2 \in \mathbb{F}_5[x]$. *Then* $\mathcal{C}$ *is a* $[18,9,8]$ *linear code over* $\mathbb{F}_{25}$ *with one-dimensional hull and its generator matrix* $[I_9,\bar{P}]$, *where*

$$\bar{P}=\begin{pmatrix} \alpha^6 & 1 & \alpha^6 & \alpha^{18} & \alpha^3 & \alpha^{21} & \alpha^{12} & \alpha^9 & \alpha^{15} \\ \alpha^{12} & \alpha^6 & \alpha^3 & \alpha^9 & \alpha^{21} & \alpha^6 & 1 & \alpha^{15} & \alpha^{18} \\ \alpha^{18} & \alpha^{15} & \alpha^6 & \alpha^6 & \alpha^{12} & 1 & \alpha^9 & \alpha^3 & \alpha^{21} \\ \alpha^6 & \alpha^{21} & \alpha^{18} & \alpha^6 & \alpha^9 & \alpha^{15} & \alpha^3 & \alpha^{12} & 1 \\ \alpha^{15} & \alpha^9 & 1 & \alpha^{21} & \alpha^6 & \alpha^{12} & \alpha^{18} & \alpha^6 & \alpha^3 \\ \alpha^9 & \alpha^{18} & \alpha^{12} & \alpha^3 & 1 & \alpha^6 & \alpha^{15} & \alpha^{21} & \alpha^6 \\ 1 & \alpha^{12} & \alpha^{21} & \alpha^{15} & \alpha^6 & \alpha^3 & \alpha^6 & \alpha^{18} & \alpha^9 \\ \alpha^{21} & \alpha^3 & \alpha^{15} & 1 & \alpha^{18} & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^{12} \\ \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} & 1 & \alpha^6 \end{pmatrix}.$$

Moreover, the hull of $\mathcal{C}$ is a $[18,1,18]$ quasi-cyclic code of index 2 over $\mathbb{F}_{25}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix}.$$

Comparing with the results in the reference [70], our results in Theorem 4.2.9 includes Theorem 5 in [70], specific as follows.

Corollary 4.2.14 *[70, Theorem 5] Let $K = \mathbb{Q}(\sqrt{r})$ and m an odd integer, where $r := 3 \pmod 4$. Let $\mathbb{O}_K$ be the ring of algebraic integers in K. Let p be an odd prime number and $\mathcal{P}$ a prime ideal in $\mathbb{O}_K$ over p. Assume that there exists $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ satisfying $\bar{\beta}^2 = -1$ and let $\beta \in \mathbb{O}_K$ be a preimage of $\bar{\beta}$ by the natural homomorphism $\mathbb{O}_K \longrightarrow \mathbb{O}_K/\mathcal{P}$, i.e., $\beta \longmapsto \bar{\beta} = \beta + \mathcal{P}$. Define ρ by*

$$\rho(x) = \begin{cases} \beta, & \text{if } x = 0; \\ \eta(x), & \text{if } x \in \mathbb{F}_{r^m}^*, \end{cases}$$

where η is the quadratic multiplicative character of $\mathbb{F}_{r^m}^*$. Define $P = (p_{ij}) \in M_{r^m}(\mathbb{O}_K)$ by $p_{ij} = \rho(x_j - x_i)$. Define $\bar{P} = (\bar{p}_{ij})$, where $\bar{p}_{ij} = p_{ij} + \mathcal{P} \in \mathbb{F}_q$. Let $\mathcal{C}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, \bar{P}]$. Then we have the following.

(1) If $p := 1 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p-ary linear code with one-dimensional hull.

(2) If $\left(\frac{r}{p}\right) = -1$ and $p := 3 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p^2-ary linear code with one-dimensional hull.

Proof: We claim that $K = \mathbb{Q}(\sqrt{r})$ satisfies the four conditions in (4.9):

(i) Due to $\psi = \eta$, we get $\zeta_N = \zeta_2 = -1 \in K$;

(ii) $G^2(\psi) = G^2(\eta) = -r^m \in \mathbb{Z} \subseteq K$;

(iii) $\zeta_N + \mathcal{P} \in \mathbb{F}_p \subseteq \mathbb{O}_K/\mathcal{P}$ and $G^2(\psi) + \mathcal{P} = G^2(\eta) + \mathcal{P} \in \mathbb{F}_p \subseteq \mathbb{O}_K/\mathcal{P}$;

(iv) If $p := 1 \pmod 4$, then there exists $\bar{\beta} \in \mathbb{F}_p \subseteq \mathbb{O}_K/\mathcal{P}$ such that $\bar{\beta}^2 = -1$. Taking $\beta \in \mathbb{O}_K$ such that $\bar{\beta} = \beta + \mathcal{P}$. If $\left(\frac{r}{p}\right) = -1$ and $p := 3 \pmod 4$, then $\mathbb{O}_K/\mathcal{P} = \mathbb{F}_{p^2}$ from [70, Lemma 3(2)] and there exists $\bar{\beta} \in \mathbb{F}_{p^2}$ such that $\bar{\beta}^2 = -1$. Taking $\beta \in \mathbb{O}_K$ such that $\bar{\beta} = \beta + \mathcal{P}$.

It is easy to check that $(r,p) = 1$. Since $r := 3 \pmod 4$ and m is an odd integer, we have $r^m := 3 \pmod 4$ and $\psi(-1) = \eta(-1) = -1$.

Above all, then $\mathcal{C}$ is a $[2r^m, r^m]$ linear code with one-dimensional hull by Theorem 4.2.9. ■

Remark 4.2.15 *In [70, Theorem 5], they need the condition "Assume that there exists $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ satisfying that $\bar{\beta}^2 = -1$" and this condition was assumed at the beginning of the subsection.*

Now, we take the multiplicative character $\psi = \eta$, where η is the quadratic multiplicative character of $\mathbb{F}_{r^m}^*$. Then we have the following corollary.

Corollary 4.2.16 *Let $K = \mathbb{Q}(\sqrt{r})$ and $p = 2$. Let $\mathbb{O}_K$ be the ring of algebraic integers in K and $\mathcal{P}$ a prime ideal in $\mathbb{O}_K$ over p. Assume that exists $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ satisfying that $\bar{\beta}^2 = -1$ and let $\beta \in \mathbb{O}_K$ be a preimage of $\bar{\beta}$ by the natural homomorphism $\mathbb{O}_K \longrightarrow \mathbb{O}_K/\mathcal{P}$, i.e., $\beta \longmapsto \bar{\beta} = \beta + \mathcal{P}$. Define ρ by*

$$\rho(x) = \begin{cases} \beta, & \text{if } x = 0; \\ \eta(x), & \text{if } x \in \mathbb{F}_{r^m}^*, \end{cases}$$

where η is the quadratic multiplicative character of $\mathbb{F}_{r^m}^*$. Define $P = (p_{ij}) \in M_{r^m}(\mathbb{O}_K)$ by $p_{ij} = \rho(x_j - x_i)$. Define $\bar{P} = (\bar{p}_{ij})$, where $\bar{p}_{ij} = p_{ij} + \mathcal{P} \in \mathbb{F}_q$.

(1) When $r := 5 \pmod 8$, then $\mathcal{C}$ is a $[2r^m, r^m]$ 4-ary linear code with one-dimensional hull.

(2) When $r := 1 \pmod 8$ or $r := 3 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ 2-ary linear code with one-dimensional hull.

Proof: Since $p = 2$, we can let $\beta = 1$ and thus $\bar{P}$ is a matrix with all entries 1. It is easy to compute that the eigenvalues of $\bar{P}\bar{P}^T$ are -1 with multiplicity 1 and 0 with multiplicity $r^m - 1$.

If $r := 1 \pmod 4$, we divide the rest of the proof into two cases.

When $r := 1 \pmod 8$, we have $2\mathbb{O}_K = \mathcal{P}_1\mathcal{P}_2$ and $\mathbb{O}_K/\mathcal{P}_1 = \mathbb{O}_K/\mathcal{P}_2 = \mathbb{F}_2$ according to [70, Lemma 4(1)]. Hence, $\mathbb{F}_q = \mathbb{O}_K/\mathcal{P} = \mathbb{F}_2$ and $\bar{P} \in M_{r^m}(\mathbb{F}_2)$. Therefore, $\mathcal{C}$ is a $[2r^m, r^m]$ 2-ary linear code with one-dimensional hull.

When $r := 5 \pmod 8$, we have $2\mathbb{O}_K = \mathcal{P}$ and $\mathbb{O}_K/\mathcal{P} \cong \mathbb{F}_4$ according to [70, Lemma 4(2)]. Hence, $\mathbb{F}_q = \mathbb{O}_K/\mathcal{P} = \mathbb{F}_4$ and $\bar{P} \in M_{r^m}(\mathbb{F}_4)$. Therefore, $\mathcal{C}$ is a $[2r^m, r^m]$ 4-ary linear code with one-dimensional hull.

If $r := 3 \pmod 4$, we get $2\mathbb{O}_K = \mathcal{P}^2$ and $\mathbb{O}_K/\mathcal{P} = \mathbb{F}_2$. Hence, $\mathbb{F}_q = \mathbb{O}_K/\mathcal{P} = \mathbb{F}_2$ and $\bar{P} \in M_{r^m}(\mathbb{F}_2)$ according to [70, Lemma 4(3)]. Therefore, $\mathcal{C}$ is a $[2r^m, r^m]$ 2-ary linear code with one-dimensional hull. ■

Remark 4.2.17 *In Corollary 4.2.16, when $r := 1 \pmod 4$ or $r := 3 \pmod 4$ and m is even, we get $\eta(-1) = 1$; when $r := 3 \pmod 4$ and m is odd, we have $\eta(-1) = -1$. Therefore, it is easy to prove that Corollary 4.2.16 is the special cases of Theorems 4.2.2 and 4.2.9 in two cases $\eta(-1) = -1$ and $\eta(-1) = 1$, respectively. Comparing with [70, Theorem 2], our results generalize their results.*

4.3 Constructions of the second class of linear codes with one-dimensional hull

Let r be a prime number and m a positive integer. $\mathbb{F}_{r^m}$ denotes the finite field of order r^m. Let $\mathbb{F}_{r^m}^* = \mathbb{F}_{r^m} \backslash \{0\}$ and $\mathbb{F}_{r^m}^* = \langle \alpha \rangle$, where α is a fixed primitive element of $\mathbb{F}_{r^m}^*$. Assume that $N > 1$ is a positive integer and $N \mid (r^m - 1)$. Let q be a power of p, where p is a prime number. Assume that $N \mid (q-1)$. Let $\mathbb{F}_q^* = \langle \beta \rangle$, where β is a fixed primitive element of $\mathbb{F}_q^*$. For the sake of convenience, we let $u = \beta^{\frac{q-1}{N}}$. Define the function

$$\varphi : \mathbb{F}_{r^m}^* \longrightarrow \mathbb{F}_q^*, \varphi(\alpha^k) = u^k, \tag{4.12}$$

where $0 \le k \le r^m - 2$. It is easy to know that φ is a homomorphism of order N. Define the kernel of the homomorphism φ as $\ker(\varphi) := \{\alpha^k, 0 \le k \le r^m - 2 : \varphi(\alpha^k) = 1\} = \langle \alpha^N \rangle$.

Assume that $(p,r) = 1$. Then there exists a positive integer t such that $r \mid (q^t - 1)$. Let $\mathbb{F}_{q^t}^* = \langle \gamma \rangle$ and $\zeta = \gamma^{\frac{q^t-1}{r}}$, where γ is a fixed primitive element of $\mathbb{F}_{q^t}^*$. For any $a \in \mathbb{F}_{r^m}$, we define

$$\chi_a : \mathbb{F}_{r^m} \longrightarrow \overline{\mathbb{F}}_q^*, \chi_a(x) = \zeta^{\mathrm{Tr}_r^{r^m}(ax)}, x \in \mathbb{F}_{r^m}, \tag{4.13}$$

where $\mathrm{Tr}_r^{r^m}$ denotes the trace function from $\mathbb{F}_{r^m}$ onto $\mathbb{F}_r$. It is easy to know that χ_a is a homomorphism. It follows from the definition of χ_a that

$$g(\varphi, \chi_{ab}) = \overline{\varphi}(b) g(\varphi, \chi_a), \tag{4.14}$$

for $a \in \mathbb{F}_{r^m}$ and $b \in \mathbb{F}_{r^m}^*$.

Fix $v \in \mathbb{F}_q$. Let $\mathbb{F}_{r^m} = \{x_i : 1 \le i \le r^m\}$. Define the $r^m \times r^m$ matrix $P = (p_{ij}) \in M_{r^m}(\mathbb{F}_q)$ by setting $p_{ij} = \rho(x_j - x_i)$, where

$$\rho(x_j - x_i) = \begin{cases} \varphi(x_j - x_i), & \text{if } i \ne j; \\ v, & \text{if } i = j. \end{cases} \tag{4.15}$$

For any $a \in \mathbb{F}_{r^m}$, set $\eta_a := (\chi_a(x_1), \chi_a(x_2), \ldots, \chi_a(x_{r^m}))^T$, where "$T$" denotes the transpose operator. Then the ith component of $P\eta_a$ is

$$\begin{aligned} \sum_{j=1}^{r^m} \rho(x_j - x_i)\chi_a(x_j) &= \sum_{x \in \mathbb{F}_{r^m}} \rho(x - x_i)\chi_a(x) \\ &\xlongequal{y := x - x_i} \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y + x_i) \\ &= \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y)\chi_a(x_i). \end{aligned}$$

Hence, $P\eta_a = \left(\sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y) \right) \eta_a$ and η_a is an eigenvector of P.

Similarly, the ith component of $P^T\eta_a$ is

$$\begin{aligned} \sum_{j=1}^{r^m} \rho(x_i - x_j)\chi_a(x_j) &= \sum_{x \in \mathbb{F}_{r^m}} \rho(x_i - x)\chi(x) \\ &\xlongequal{y := x_i - x} \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(x_i - y) \\ &= \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(-y)\chi_a(x_i). \end{aligned}$$

Hence, $P^T\eta_a = \left(\sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(-y) \right) \eta_a$ and η_a is also an eigenvector of P^T.

Next, we will prove that the r^m vectors $\{\eta_a := (\chi_a(x_1), \chi_a(x_2), \ldots, \chi_a(x_{r^m}))^T : a \in \mathbb{F}_{r^m}\}$ are linearly independent over $\overline{\mathbb{F}}_q$.

Suppose that $\sum_{a\in\mathbb{F}_{r^m}} k_a\eta_a = \mathbf{0}$, where $k_a \in \overline{\mathbb{F}}_q$. Then

$$\begin{aligned} &\sum_{a\in\mathbb{F}_{r^m}} k_a(\chi_a(x_1), \chi_a(x_2), \ldots, \chi_a(x_{r^m}))^T = \mathbf{0}, \\ \Longrightarrow \quad &\left(\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_1), \sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_2), \ldots, \sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_{r^m})\right)^T = \mathbf{0}. \end{aligned}$$

Hence, $\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_i) = 0$ for any $1 \le i \le r^m$.

Given an element $a_0 \in \mathbb{F}_{r^m}$, we have

$$\begin{aligned} &\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_i)\chi_{a_0}(-x_i) = 0, \\ \Longrightarrow \quad &\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_1((a-a_0)x_i) = 0, \\ \Longrightarrow \quad &\sum_{x\in\mathbb{F}_{r^m}} \sum_{a\in\mathbb{F}_{r^m}} k_a\chi_1((a-a_0)x) = 0, \\ \Longrightarrow \quad &\sum_{a\in\mathbb{F}_{r^m}} k_a \sum_{x\in\mathbb{F}_{r^m}} \chi_1((a-a_0)x) = 0. \end{aligned}$$

By Lemma 4.1.2, we obtain $k_{a_0}r^m = 0$ and then $k_{a_0} = 0$ by $(r,p) = 1$. Because a_0 is arbitrary, we have $k_a = 0$ for any $a \in \mathbb{F}_{r^m}$. Hence, the r^m vectors $\{\eta_a := (\chi_a(x_1), \chi_a(x_2), \ldots, \chi_a(x_{r^m}))^T : a \in \mathbb{F}_{r^m}\}$ are linearly independent over $\overline{\mathbb{F}}_q$.

Hence, the multisets $\left\{\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y) : a \in \mathbb{F}_{r^m}\right\}$ and $\left\{\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y) : a \in \mathbb{F}_{r^m}\right\}$ present all eigenvalues of the matrix P and P^T, respectively.

To sum up,

$$PP^T\eta_a = P\left(\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y)\right)\eta_a = \left(\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y) \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y)\right)\eta_a.$$

Then the multiset $\left\{\lambda_a := \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y) \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y) : a \in \mathbb{F}_{r^m}\right\}$ presents all eigenvalues of the matrix PP^T and $\{\eta_a : a \in \mathbb{F}_{r^m}\}$ presents all eigenvectors of PP^T.

Let the symbols be the same as above. According to Lemma 4.1.5(1), we obtain

$$\begin{aligned}
\lambda_a &= \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y) \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y) \\
&= \left(v+\sum_{y\in\mathbb{F}_{r^m}^*} \varphi(y)\chi_a(y)\right)\left(v+\sum_{y\in\mathbb{F}_{r^m}^*} \varphi(y)\chi_a(-y)\right) \\
&= (v+g(\varphi,\chi_a))(v+g(\varphi,\overline{\chi}_a)) \\
&= v^2+vg(\varphi,\chi_a)+vg(\varphi,\overline{\chi}_a)+g(\varphi,\chi_a)g(\varphi,\overline{\chi}_a) \\
&= v^2+vg(\varphi,\chi_a)+\varphi(-1)vg(\varphi,\chi_a)+\varphi(-1)(g(\varphi,\chi_a))^2 \\
&= v^2+(1+\varphi(-1))vg(\varphi,\chi_a)+\varphi(-1)(g(\varphi,\chi_a))^2.
\end{aligned}$$

Hence, all eigenvalues of PP^T are given by the multiset

$$\{\lambda_a := v^2+(1+\varphi(-1))vg(\varphi,\chi_a)+\varphi(-1)(g(\varphi,\chi_a))^2 : a\in\mathbb{F}_{r^m}\}. \quad (4.16)$$

Let $\mathcal{C} := \mathcal{C}_{(\varphi,v)}$ be a linear code over $\mathbb{F}_q$ with generator matrix $G=[I_{r^m},P]$. Then $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_q$.

4.3.1 The case $p=2$

Define $\rho(0)=v=1$. Then $v^2=1=-1$. We then obtain a $r^m\times r^m$ matrix $P=(p_{ij})$ by $p_{ij}=\rho(x_j-x_i)$, which is defined as (4.15). It follows from (4.16) that all eigenvalues of PP^T are given by

$$\lambda_a = \begin{cases} -1, & \text{if } a=0; \\ -1+(g(\varphi,\chi_a))^2, & \text{if } a\in\mathbb{F}_{r^m}^*. \end{cases} \quad (4.17)$$

Theorem 4.3.1 *Let r be an odd prime number and m be a positive integer. Assume that $N>1$ is a positive integer and $N\mid(r^m-1)$. Let q be a power of $p=2$ and $N\mid(q-1)$. Let $\mathcal{C}:=\mathcal{C}_{(\varphi,1)}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m},P]$. Then $\mathcal{C}$ is a $[2r^m,r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull.*

Proof: It follows from (4.17) that all eigenvalues of PP^T are -1 when $a=0$ and $-1+(g(\varphi,\chi_a))^2$ when $a\in\mathbb{F}_{r^m}^*$. By using Lemma 1.2.4, we just have to prove that $-1+(g(\varphi,\chi_a))^2\neq -1$ for any $a\in\mathbb{F}_{r^m}^*$. Note that the result $g(\varphi,\chi_a)\overline{g(\varphi,\chi_a)}=r^m$ for any $a\in\mathbb{F}_{r^m}^*$ from Lemma 4.1.4. Then $g(\varphi,\chi_a)\neq 0$ and $\overline{g(\varphi,\chi_a)}\neq 0$ for any $a\in\mathbb{F}_{r^m}^*$. Hence, $(g(\varphi,\chi_a))^2\neq 0$ and $-1+(g(\varphi,\chi_a))^2\neq -1$ for any $a\in\mathbb{F}_{r^m}^*$. The desired conclusion then follows. ■

Here, we give a concrete example as follows.

Example 4.3.2 *Let $r=13,m=1,N=3,p=2$ and $q=4$. Let $\mathbb{F}_4^*=\langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_4^*$. It is easy to check that q,r,N satisfy the conditions in*

Theorem 4.3.1. Then $\mathcal{C}$ is a $[26,13,8]$ linear code over $\mathbb{F}_4$ with one-dimensional hull and its generator matrix $[I_{13},P]$, where

$$P=\begin{pmatrix}
1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1\\
1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta\\
\beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta\\
\beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2\\
\beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1\\
1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2\\
\beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2\\
\beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1\\
1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2\\
\beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta\\
\beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta\\
\beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1\\
1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1
\end{pmatrix}.$$

Moreover, the hull of $\mathcal{C}$ is a $[26,1,26]$ cyclic code over $\mathbb{F}_4$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

4.3.2 The case $p \geq 3$

In this subsection, we let $\mathbb{F}_q^* = \langle \beta \rangle$, where β is a fixed primitive element of $\mathbb{F}_q^*$. Assume that $4 \mid (q-1)$.

Define $\rho(0) = v = \beta^{\frac{q-1}{4}}$. Then $v^2 = (\beta^{\frac{q-1}{4}})^2 = \beta^{\frac{q-1}{2}} = -1$. We then obtain a $r^m \times r^m$ matrix $P = (p_{ij})$ by $p_{ij} = \rho(x_j - x_i)$, which is defined as (4.15). In addition, $\varphi(-1) = \varphi(\alpha^{\frac{r^m-1}{2}}) = u^{\frac{r^m-1}{2}} = (\beta^{\frac{q-1}{N}})^{\frac{r^m-1}{2}} = (\beta^{\frac{q-1}{2}})^{\frac{r^m-1}{N}} = (-1)^{\frac{r^m-1}{N}}$. When $\frac{r^m-1}{N}$ is odd, $\varphi(-1) = -1$; when $\frac{r^m-1}{N}$ is even, $\varphi(-1) = 1$.

Combining with (4.16), when $\frac{r^m-1}{N}$ is odd, we have

$$\lambda_a = \begin{cases} -1, & \text{if } a = 0; \\ -1 - (g(\varphi,\chi_a))^2, & \text{if } a \in \mathbb{F}_{r^m}^*; \end{cases} \tag{4.18}$$

when $\frac{r^m-1}{N}$ is even, we get

$$\lambda_a = \begin{cases} -1, & \text{if } a = 0; \\ -1 + (2v + g(\varphi,\chi_a))g(\varphi,\chi_a), & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases} \tag{4.19}$$

Collecting all discussions above, we first present the sufficient conditions for constructing linear codes with one-dimensional hull when $\frac{r^m-1}{N}$ is odd.

Theorem 4.3.3 *Let r be a prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N \mid (r^m - 1)$. Let q be a power of prime p and $(p,r) = 1$.*

Assume that $N \mid (q-1)$ and $4 \mid (q-1)$. Let $\mathcal{C} := \mathcal{C}_{(\varphi,\beta^{\frac{q-1}{4}})}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. When $\frac{r^m-1}{N}$ is odd, $\mathcal{C}$ is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull.

Proof: The proof is similar to that of Theorem 4.3.1 and then we omit it here. ■

In the following, we present some concrete examples to explain Theorem 4.3.3.

Example 4.3.4 *Let $r = 3, m = 2, N = 8, p = 7$ and $q = 49$. Let $\mathbb{F}_{49}^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_{49}^*$. It is easy to check that q, r, N satisfy the conditions in Theorem 4.3.3. Then $\mathcal{C}$ is a $[18, 9, 8]$ linear code over $\mathbb{F}_{49}$ with one-dimensional hull and its generator matrix $[I_9, P]$, where*

$$P = \begin{pmatrix} \beta^{12} & \beta^{42} & \beta^{6} & \beta^{30} & 1 & \beta^{36} & \beta^{18} & \beta^{12} & 6 \\ \beta^{18} & \beta^{12} & 1 & \beta^{12} & \beta^{36} & \beta^{6} & \beta^{42} & 6 & \beta^{30} \\ \beta^{30} & 6 & \beta^{12} & \beta^{6} & \beta^{18} & \beta^{42} & \beta^{12} & 1 & \beta^{36} \\ \beta^{6} & \beta^{36} & \beta^{30} & \beta^{12} & \beta^{12} & 6 & 1 & \beta^{18} & \beta^{42} \\ 6 & \beta^{12} & \beta^{42} & \beta^{36} & \beta^{12} & \beta^{18} & \beta^{30} & \beta^{6} & 1 \\ \beta^{12} & \beta^{30} & \beta^{18} & 1 & \beta^{42} & \beta^{12} & 6 & \beta^{36} & \beta^{6} \\ \beta^{42} & \beta^{18} & \beta^{36} & 6 & \beta^{6} & 1 & \beta^{12} & \beta^{30} & \beta^{12} \\ \beta^{36} & 1 & 6 & \beta^{42} & \beta^{30} & \beta^{12} & \beta^{6} & \beta^{12} & \beta^{18} \\ 1 & \beta^{6} & \beta^{12} & \beta^{18} & 6 & \beta^{30} & \beta^{36} & \beta^{42} & \beta^{12} \end{pmatrix}.$$

Moreover, the hull of $\mathcal{C}$ is a $[18, 1, 18]$ quasi-cyclic code of index 2 over $\mathbb{F}_{49}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} \end{pmatrix}.$$

Comparing with Example 2(2) in [70], the linear code $\mathcal{C}$ over $\mathbb{F}_{49}$ with one-dimensional hull we obtained has better parameters than its parameters. In other words, the linear code $\mathcal{C}$ of the length 18 with the dimension 9 has the minimal distance 8, while the linear code $\mathcal{C}$ of the length 18 with the dimension 9 in [70, Example 2(2)] has the minimal distance 7. That is to say, the linear code $\mathcal{C}$ over $\mathbb{F}_{49}$ with one-dimensional hull we obtained is also considered new.

Example 4.3.5 *Let $r = 7, m = 1, N = 6, p = 5$ and $q = 25$. Let $\mathbb{F}_{25}^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_{25}^*$. It is easy to check that q, r, N satisfy the conditions in Theorem 4.3.3. Then $\mathcal{C}$ is a $[14, 7, 7]$ linear code over $\mathbb{F}_{25}$ with one-dimensional hull and its generator matrix $[I_7, P]$, where*

$$P = \begin{pmatrix} 2 & 1 & \beta^{8} & \beta^{4} & \beta^{16} & \beta^{20} & 4 \\ 4 & 2 & 1 & \beta^{8} & \beta^{4} & \beta^{16} & \beta^{20} \\ \beta^{20} & 4 & 2 & 1 & \beta^{8} & \beta^{4} & \beta^{16} \\ \beta^{16} & \beta^{20} & 4 & 2 & 1 & \beta^{8} & \beta^{4} \\ \beta^{4} & \beta^{16} & \beta^{20} & 4 & 2 & 1 & \beta^{8} \\ \beta^{8} & \beta^{4} & \beta^{16} & \beta^{20} & 4 & 2 & 1 \\ 1 & \beta^{8} & \beta^{4} & \beta^{16} & \beta^{20} & 4 & 2 \end{pmatrix},$$

which is an almost MDS code. Moreover, the hull of $\mathcal{C}$ *is a* $[14,1,14]$ *quasi-cyclic code of index* 2 *over* $\mathbb{F}_{25}$ *with generator matrix*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix}.$$

Next, we turn to the sufficient conditions for constructing linear codes with one-dimensional hull when $\frac{r^m-1}{N}$ is even.

Theorem 4.3.6 *Let* r *be a prime number and* m *be a positive integer. Assume that* $N>1$ *is a positive integer and* $N \mid (r^m-1)$. *Let* q *be a power of a prime* p *and* $(p,r)=1$. *Assume that* $N \mid (q-1)$ *and* $4 \mid (q-1)$. *Let* $\mathcal{C} := \mathcal{C}_{(\varphi,\beta^{\frac{q-1}{4}})}$ *be the linear code over* $\mathbb{F}_q$ *with generator matrix* $[I_{r^m}, P]$. *When* $\frac{r^m-1}{N}$ *is even and* $2v+g(\varphi,\chi_a)\neq 0$ *for all* $a \in \mathbb{F}_{r^m}^*$, $\mathcal{C}$ *is a* $[2r^m, r^m]$ *linear code over* $\mathbb{F}_q$ *with one-dimensional hull.*

Proof: It follows from (4.19) that all eigenvalues of PP^T are -1 when $a=0$ and $-1+(2v+g(\varphi,\chi_a))g(\varphi,\chi_a)$ when $a \in \mathbb{F}_{r^m}^*$. According to Lemma 1.2.4, we just have to prove that $-1+(2v+g(\varphi,\chi_a))g(\varphi,\chi_a) \neq -1$ for all $a \in \mathbb{F}_{r^m}^*$.

By utilizing Lemma 4.1.4 and the proof of Theorem 4.3.1, we obtain that $g(\varphi,\chi_a) \neq 0$ for any $a \in \mathbb{F}_{r^m}^*$. When $2v+g(\varphi,\chi_a)\neq 0$ for all $a \in \mathbb{F}_{r^m}^*$, we have $-1+(2v+g(\varphi,\chi_a))g(\varphi,\chi_a) \neq -1$ for all $a \in \mathbb{F}_{r^m}^*$.

Therefore, the matrix PP^T has an eigenvalue -1 with multiplicity 1. It then follows from Lemma 1.2.4 that $\mathcal{C}$ is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull. ■

In Theorem 4.3.6, the condition "$2v+g(\varphi,\chi_a)\neq 0$ for all $a \in \mathbb{F}_{r^m}^*$" is not very straightforward. Hence, we will present the following corollary as a concrete result.

Corollary 4.3.7 *Let* r *be a prime number and* m *be a positive integer. Assume that* $N>1$ *is a positive integer and* $N \mid (r^m-1)$. *Let* q *be a power of odd prime* p *and* $(p,r)=1$. *Assume that* $N \mid (q-1)$ *and* $4 \mid (q-1)$. *Let* $\mathcal{C} := \mathcal{C}_{(\varphi,\beta^{\frac{q-1}{4}})}$ *be the linear code over* $\mathbb{F}_q$ *with generator matrix* $[I_{r^m}, P]$. *Let* $\frac{r^m-1}{N}$ *be even. If* $\varphi(q)\neq 1$, *then* $\mathcal{C}$ *is a* $[2r^m, r^m]$ *linear code over* $\mathbb{F}_q$ *with one-dimensional hull.*

Proof: Since $\frac{r^m-1}{N}$ is even and it follows from (4.19) that all eigenvalues of PP^T are -1 when $a=0$ and $-1+(2v+g(\varphi,\chi_a))g(\varphi,\chi_a)$ when $a \in \mathbb{F}_{r^m}^*$. Suppose that $2v+g(\varphi,\chi_a)=0$ for some $a \in \mathbb{F}_{r^m}^*$. Then $g(\varphi,\chi_a)=-2v \in \mathbb{F}_p$ when $p := 1 \pmod 4$ and $g(\varphi,\chi_a)=-2v \in \mathbb{F}_{p^2}$ when $p := 3 \pmod 4$. In addition,

$$\begin{aligned}
(g(\varphi,\chi_a))^q &= \left(\sum_{x \in \mathbb{F}_{r^m}^*} \varphi(x)\chi_a(x)\right)^q \\
&= g(\varphi^q, \chi_{aq}) \\
&= g(\varphi, \chi_{aq}) \\
&= \varphi(q^{-1})g(\varphi,\chi_a) \\
&= \varphi(q)^{-1}g(\varphi,\chi_a)
\end{aligned}$$

by $N \mid (q-1)$ and (4.14). If $\varphi(q) \neq 1$, then $(g(\varphi,\chi_a))^q \neq g(\varphi,\chi_a)$, i.e., $g(\varphi,\chi_a) \notin \mathbb{F}_q$.

When $p := 1 \pmod 4$, $\mathbb{F}_p \subseteq \mathbb{F}_q$, which implies that $g(\varphi,\chi_a) \notin \mathbb{F}_p$. It is a contradiction.

When $p := 3 \pmod 4$, $\mathbb{F}_{p^2} \subseteq \mathbb{F}_q$ by $4 \mid (q-1)$, which implies that $g(\varphi,\chi_a) \notin \mathbb{F}_{p^2}$. It is a contradiction.

Hence, $2v + g(\varphi,\chi_a) \neq 0$. By using Lemma 4.1.4, we obtain that $g(\varphi,\chi_a) \neq 0$. Then $-1 + (2v + g(\varphi,\chi_a))g(\varphi,\chi_a) \neq -1$ for all $a \in \mathbb{F}_{r^m}^*$. Thus the matrix PP^T has an eigenvalue -1 with multiplicity 1. It then follows from Lemma 1.2.4 that the desired result then follows. ■

We now employ Corollary 4.3.7 to present an example as follows.

Example 4.3.8 *Let $r = 7, m = 1, N = 3, p = 5$ and $q = 25$. Let $\mathbb{F}_{25}^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_{25}^*$. It is easy to check that q, r, N satisfy the conditions in Corollary 4.3.7. Then $\mathcal{C}$ is a $[14,7,6]$ linear code over $\mathbb{F}_{25}$ with one-dimensional hull and its generator matrix $[I_7, P]$, where*

$$P = \begin{pmatrix} 2 & 1 & \beta^{16} & \beta^8 & \beta^8 & \beta^{16} & 1 \\ 1 & 2 & 1 & \beta^{16} & \beta^8 & \beta^8 & \beta^{16} \\ \beta^{16} & 1 & 2 & 1 & \beta^{16} & \beta^8 & \beta^8 \\ \beta^8 & \beta^{16} & 1 & 2 & 1 & \beta^{16} & \beta^8 \\ \beta^8 & \beta^8 & \beta^{16} & 1 & 2 & 1 & \beta^{16} \\ \beta^{16} & \beta^8 & \beta^8 & \beta^{16} & 1 & 2 & 1 \\ 1 & \beta^{16} & \beta^8 & \beta^8 & \beta^{16} & 1 & 2 \end{pmatrix}.$$

Moreover, the hull of $\mathcal{C}$ is a $[14,1,14]$ quasi-cyclic code of index 2 over $\mathbb{F}_{25}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix}.$$

Next, we discuss the lower bound on the minimum distance of linear code $\mathcal{C} := \mathcal{C}_{(\varphi,v)}$ with generator matrix $G = [I_{r^m}, P]$.

Assume that q is a power of odd prime p and $N = 2$. Let $\mathbb{F}_{r^m} = \{x_i : 1 \leq i \leq r^m\}$, where $x_1, \cdots, x_{\frac{r^m-1}{2}}$ are non-zero squares in $\mathbb{F}_{r^m}$, $x_{\frac{r^m+1}{2}}, \ldots, x_{r^m-1}$ are non-squares in $\mathbb{F}_{r^m}$ and $x_{r^m} = 0$. From Section 3, we have $P\eta_a = \theta_a\eta_a$ for any $a \in \mathbb{F}_{r^m}$, where $\theta_a := \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y)$ and $\eta_a := (\chi_a(x_1), \chi_a(x_2), \ldots, \chi_a(x_{r^m}))^T$. Let $Q := (\eta_{x_1}, \eta_{x_2}, \ldots, \eta_{x_{r^m}})$. Then

$$\begin{aligned} PQ &= (P\eta_{x_1}, P\eta_{x_2}, \ldots, P\eta_{x_{r^m}}) \\ &= (\theta_{x_1}\eta_{x_1}, \theta_{x_2}\eta_{x_2}, \ldots, \theta_{x_{r^m}}\eta_{x_{r^m}}) \\ &= (\eta_{x_1}, \eta_{x_2}, \ldots, \eta_{x_{r^m}})\Lambda \\ &= Q\Lambda, \end{aligned}$$

where

$$\Lambda = \begin{pmatrix} \theta_{x_1} & & & \\ & \theta_{x_2} & & \\ & & \ddots & \\ & & & \theta_{x_{r^m}} \end{pmatrix} \text{ is a diagonal matrix.}$$

Note that when $v=0$,

$$\theta_a = \begin{cases} 0, & \text{if } a=0; \\ \varphi(a^{-1})g(\varphi,\chi_1), & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases}$$

Let's just say $g := g(\varphi,\chi_1)$ for convenience.

It is easy to know that

$$\Lambda = g(\varphi,\chi_1)\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & & & & & 0 \end{pmatrix}. \tag{4.20}$$

It follows the definition of the linear code $\mathcal{C}$ that $\mathcal{C}$ can be expressed in the following form:

$$\mathcal{C} \;=\; \{c(\boldsymbol{k}) = \boldsymbol{k}G, \boldsymbol{k} \in \mathbb{F}_q^{r^m}\}, \text{where } \boldsymbol{k} = (k_1, k_2, \ldots, k_{r^m}).$$

For any codeword $c(\boldsymbol{k})$ in $\mathcal{C}$, we have

$$\begin{aligned} c(\boldsymbol{k}) &= \boldsymbol{k}G \\ &= \boldsymbol{k}(I_{r^m}, P) \\ &= (\boldsymbol{k}, \boldsymbol{k}P) \\ &= (\boldsymbol{k}, \boldsymbol{l}), \text{where } \boldsymbol{l} := \boldsymbol{l}(\boldsymbol{k}) = \boldsymbol{k}P \\ &= (k_1, k_2, \ldots, k_{r^m}, l_1, l_2, \ldots, l_{r^m}). \end{aligned}$$

Multiply both sides of the equation $\boldsymbol{l} = \boldsymbol{k}P$ by the matrix Q, we obtain

$$\boldsymbol{l}Q = \boldsymbol{k}PQ = \boldsymbol{k}Q\Lambda.$$

Based on the above discussion and combined with Eq. (4.20), we have the following three equations:

$$(l_1 - gk_1, \ldots, l_{r^m} - gk_{r^m})(\eta_{x_1}, \ldots, \eta_{x_{\frac{r^m-1}{2}}}) \;=\; \mathbf{0}; \tag{4.21}$$

$$\begin{aligned} (l_1 + gk_1, \ldots, l_{r^m} + gk_{r^m})(\eta_{x_{\frac{r^m+1}{2}}}, \ldots, \eta_{x_{r^m-1}}) &= \mathbf{0}; \\ l_1 + \cdots + l_{r^m} &= 0. \end{aligned} \tag{4.22}$$

In view of the above three equations, we present the following theorem. Before we do that, let's give some definitions. We define $\begin{pmatrix} \mu_{x_1} \\ \vdots \\ \mu_{x_{r^m}} \end{pmatrix} := (\eta_{x_1}, \ldots, \eta_{x_{\frac{r^m-1}{2}}})$ and $\begin{pmatrix} \nu_{x_1} \\ \vdots \\ \nu_{x_{r^m}} \end{pmatrix} := (\eta_{x_{\frac{r^m+1}{2}}}, \ldots, \eta_{x_{r^m-1}})$.

Theorem 4.3.9 *Let $\mathcal{C} := \mathcal{C}_{(\varphi,0)}$ be a linear code over $\mathbb{F}_q$ with generator matrix $G = [I_{r^m}, P]$. Let A be a positive integer. Assume that any A vectors in $\{\mu_{x_1}, \cdots, \mu_{x_{r^m}}\}$ are linearly independent and any A vectors in $\{\nu_{x_1}, \cdots, \nu_{x_{r^m}}\}$ are also linearly independent. Then $d_{min}(\mathcal{C}) \geq A+1$.*

Proof: Suppose that $c(\boldsymbol{k})$ is any codeword in $\mathcal{C}$ which satisfies that $\mathrm{wt}(c(\boldsymbol{k})) < A+1$. Note that $c(\boldsymbol{k}) = (\boldsymbol{k}, \boldsymbol{kP}) = (\boldsymbol{k}, \boldsymbol{l}) = (k_1, \ldots, k_{r^m}, l_1, \ldots, l_{r^m})$. Set $\Omega := \{(l_1, k_1), \ldots, (l_{r^m}, k_{r^m})\}$. Let $x = \#\{(l_i, k_i) \in \Omega \mid (l_i, k_i) = (0,0)\}$, $y = \#\{(l_i, k_i) \in \Omega \mid$ Only one of l_i and k_i is $0\}$ and $z = \#\{(l_i, k_i) \in \Omega \mid l_i \neq 0$ and $k_i \neq 0\}$. Then we have

$$\begin{cases} x+y+z = r^m; \\ 2x+y > 2r^m - A - 1. \end{cases} \tag{4.23}$$

From (4.23), we obtain

$$x \;>\; r^m - A - 1. \tag{4.24}$$

Let $u_i = l_i - gk_i$ and $w_i = l_i + gk_i$, where $1 \leq i \leq r^m$. It follows Eqs. (4.21) and (4.22) that

$$(u_1, \ldots, u_{r^m}) \begin{pmatrix} \mu_{x_1} \\ \vdots \\ \mu_{x_{r^m}} \end{pmatrix} = u_1\mu_{x_1} + \cdots + u_{r^m}\mu_{x_{r^m}} = \mathbf{0} \tag{4.25}$$

and

$$(w_1, \ldots, w_{r^m}) \begin{pmatrix} \nu_{x_1} \\ \vdots \\ \nu_{x_{r^m}} \end{pmatrix} = w_1\nu_{x_1} + \cdots + w_{r^m}\nu_{x_{r^m}} = \mathbf{0}. \tag{4.26}$$

According to (4.24), it is easy to know that there are at least $r^m - A$ zeros in $u_1, \ldots, u_{r^m}$. Similarly, there are also at least $r^m - A$ zeros in $w_1, \ldots, w_{r^m}$. Without loss of generality, let's assume that $u_{A+1} = \cdots = u_{r^m} = 0$. Since $\mu_{x_1}, \ldots, \mu_{x_A}$ are linearly independent, we have $u_1 = \cdots = u_A = 0$ according to Eq. (4.25). Hence, we obtain $u_1 = \cdots = u_{r^m} = 0$. Similarly, we also deduce $w_1 = \cdots = w_{r^m} = 0$. Therefore, we get $l_1 = \cdots = l_{r^m} = 0$ and $k_1 = \cdots = k_{r^m} = 0$. Then $c(\boldsymbol{k})$ is a zero codeword. That is to say, for any nonzero codeword c in $\mathcal{C}$, we have $\mathrm{wt}(c) \geq A+1$. So $d_{min}(\mathcal{C}) \geq A+1$.

This completes the proof. ■

4.4 Conclusions

In this chapter, we first generalized the results of [16, 70] and employed general Gaussian sums to construct linear codes with a one-dimensional hull via number fields. In addition, we proposed a general method to construct linear codes with a one-dimensional hull by using an analogue of Gaussian sums where both the corresponding additive and multiplicative character take their values in a finite field instead of the complex numbers. Remarkably, the constructions of linear codes with a one-dimensional hull were studied by characterizing the eigenvalues of the matrix PP^T, and combining them with Lemma 1.2.4,

we presented some sufficient conditions for a linear code over finite fields with generator matrix $[I_{r^m}, P]$ to be a linear code with a one-dimensional hull.

Compared with [16, 70], the results obtained in this chapter have clear advantages as follows:

(1) Construction methods are more general. In [16, 70], the authors needed the matrix P to have some special properties; for example, most of them are symmetric. However, we can completely determine all eigenvalues of the matrix PP^T for any matrix P. In addition, the authors constructed linear codes with a one-dimensional hull by using the special Gaussian sums (for example, quadratic Gaussian sums and Gaussian sums in the semi-primitive case). However, we employed general Gaussian sums to construct linear codes with a one-dimensional hull via number fields. The construction method in this chapter further generalizes the construction method in [16, 70], and the relevant results in [16, 70] are special cases of the results of this chapter.

(2) Construction methods are more direct. In [16, 70], the authors constructed linear codes with a one-dimensional hull over finite fields by using the generator matrix over quadratic number fields or cyclotomic fields, while we constructed them directly by utilizing the generator matrix over finite fields. Furthermore, this straightforward approach can lead to more optimal or almost optimal linear codes.

(3) We firstly presented a lower bound on the minimum distance of the linear code $\mathcal{C}$ over $\mathbb{F}_q$ with generator matrix $G = [I_{r^m}, P]$ when $N = 2$. [1]

[1] The main content of this chapter has been published in Des. Codes Cryptogr. and Cryptogr. Commun..

Chapter 5

Minimal binary linear codes and their applications

This chapter mainly constructs minimal binary linear codes with few nonzero weights by using two-to-one functions over finite fields with an even characteristic. Section 5.1 presents three constructions of binary linear codes by two-to-one functions over $\mathbb{F}_{2^n}$. Section 5.2 determines the parameters and weight distributions of linear codes constructed in Section 5.1 by utilizing the Walsh Hadamard transform of the corresponding functions. In addition, some of the constructed codes are optimal concerning the well-known Griesmer bound and optimal (or almost optimal) for the online Database of Grassl. In Section 5.3, we study the optimality of some binary linear codes obtained in Section 5.2 and describe the access structures of the secret sharing schemes based on their dual codes. Finally, two open problems in [72] are solved.

Throughout this chapter, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements and n be a positive integer. $\mathrm{Tr}_n(\cdot)$ denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and $\mathrm{Tr}_m^n(\cdot)$ denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, where $m \mid n$ and m is a positive integer.

5.1 Constructions of binary linear codes

In this section, we mainly present three constructions of binary linear codes by two-to-one functions over finite fields of even characteristic.

Let $F(x)$ be a two-to-one function from $\mathbb{F}_{2^n}$ to itself with $F(0) = 0$.

Construction 1:

The first generic construction of binary linear codes $\mathcal{C}_F$ is defined by

$$\mathcal{C}_F = \{\boldsymbol{c}_{a,b} = (\mathrm{Tr}_n(ax + bF(x)))_{x \in \mathbb{F}_{2^n}^*} : a, b \in \mathbb{F}_{2^n}\}. \tag{5.1}$$

It is obvious that the length and dimension of $\mathcal{C}_F$ in (5.1) is $2^n - 1$ and at most $2n$, respectively. From [72, Subsection A], we know that the dimension of $\mathcal{C}_F$ is $2n - d_{K_1}$, where d_{K_1} is the dimension of the $\mathbb{F}_2$-vector space

$$K_1 = \left\{(a,b) \in \mathbb{F}_{2^n}^2 : \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bF(x))} = 2^n\right\}. \tag{5.2}$$

The Hamming weight of a codeword $\boldsymbol{c}_{a,b}$ in $\mathcal{C}_F$ is

$$\mathrm{wt}(\boldsymbol{c}_{a,b}) = 2^{n-1} - \frac{1}{2}W_F(a,b). \tag{5.3}$$

When the Walsh transforms of F take three nontrivial values v_1, v_2, v_3 for $(a,b) \in \mathbb{F}_{2^n}^2$, the value distribution of $W_F(a,b)$ can be calculated by solving the following equations derived from the first three power moment identities [11]

$$\begin{cases} \sum_{i=0}^{3} X_i = 2^{2n}; \\ \sum_{i=0}^{3} v_i X_i = 2^{2n}; \\ \sum_{i=0}^{3} v_i^2 X_i = 2^{3n}, \end{cases} \tag{5.4}$$

where X_i is the occurrences of $W_F(a,b) = v_i$ $(i = 0,1,2,3)$ in the Walsh spectrum of F with $(X_0, v_0) = (2^{d_{K_1}}, 2^n)$. If a value of $W_F(a,b)$ occurs X_i times in the Walsh spectrum of F, then there are $X_i/2^{d_{K_1}}$ codewords in $\mathcal{C}_F$ with Hamming weight $2^{n-1} - \frac{1}{2}v_i$, and the weight distribution of $\mathcal{C}_F$ can be determined.

Construction 2:

The second generic construction of binary linear codes $\mathcal{C}_D$ from a given defining set $D := \{d_1, d_2, \ldots, d_l\}$ suggests defining a linear code $\mathcal{C}_D = \{\boldsymbol{c}_b = (\mathrm{Tr}_n(bd_1), \mathrm{Tr}_n(bd_2), \ldots, \mathrm{Tr}_n(bd_l)) : b \in \mathbb{F}_{2^n}\}$. To make a connection with functions F (defined over $\mathbb{F}_{2^n}$), we can choose D (or more appropriate D_F), for example, as the nonzero set of all the values of F. In this case, we denote the resulting code by $\mathcal{C}_{D_F}$, which will be defined precisely as follows:

$$\mathcal{C}_{D_F} = \{\boldsymbol{c}_b = (\mathrm{Tr}_n(bd_1), \mathrm{Tr}_n(bd_2), \ldots, \mathrm{Tr}_n(bd_l)) : b \in \mathbb{F}_{2^n}\}, \tag{5.5}$$

where $D_F := \{F(x), x \in \mathbb{F}_{2^n}\} \setminus \{0\} = \{d_1, d_2, \ldots, d_l\}$.

It is obvious that the length and dimension of $\mathcal{C}_{D_F}$ in (5.5) is $l = |D_F|$ and at most n, respectively. Similarly, from [72, Subsection A], we know that the dimension of $\mathcal{C}_{D_F}$ is $n - d_{K_2}$, where d_{K_2} is the dimension of the $\mathbb{F}_2$-vector space

$$K_2 = \left\{ b \in \mathbb{F}_{2^n} : \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bF(x))} = 2^n \right\}. \tag{5.6}$$

Now, if the function F is chosen to be 2-to-1 over $\mathbb{F}_{2^n}$ with $F(0) = 0$, then the length of $\mathcal{C}_{D_F}$ is $l = |D_F| = 2^{n-1} - 1$ and the Hamming weight of a codeword $\boldsymbol{c}_b$ in $\mathcal{C}_{D_F}$ is

$$\mathrm{wt}(\boldsymbol{c}_b) = 2^{n-2} - \frac{1}{4}W_F(0,b). \tag{5.7}$$

The following lemma is from [72], which gives the parameters of the dual code of $\mathcal{C}_{D_F}$ in (5.5).

Lemma 5.1.1 *[72, Theorem 1] Let F be a 2-to-1 mapping over $\mathbb{F}_{2^n}$ with $F(0) = 0$ and let $\mathcal{C}_{D_F}$ be defined as in (5.5). Moreover, let $\mathcal{C}_{D_F}^{\perp}$ be the dual code of $\mathcal{C}_{D_F}$ and d_{K_2} be defined as in (5.6). Then $\mathcal{C}_{D_F}^{\perp}$ is a $[2^{n-1} - 1, 2^{n-1} - 1 - n + d_{K_2})]$ binary linear code with the minimum distance $d^{\perp}$ satisfying $3 \le d^{\perp} \le 4$.*

Construction 3:

The third generic construction of binary linear codes $\widetilde{\mathcal{C}}_{D_F}$ is defined by

$$\widetilde{\mathcal{C}}_{D_F} = \{\widetilde{\boldsymbol{c}}_{a,b} = (\mathrm{Tr}_n(ad_i + bd_j))_{(d_i,d_j)\in D_F^2} : a,b \in \mathbb{F}_{2^n}\}, \tag{5.8}$$

where $D_F = \{F(x) : x \in \mathbb{F}_{2^n}\}\backslash\{0\} := \{d_1, d_2, \ldots, d_l\}$.

Clearly, the length and dimension of $\widetilde{\mathcal{C}}_{D_F}$ in (5.8) is l^2 and at most $2n$, respectively. To determine the dimension of $\widetilde{\mathcal{C}}_{D_F}$, it suffices to compute the number of $a,b \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_n(aF(x) + bF(y))) = 0$ for any $x,y \in \mathbb{F}_{2^n}$ since the code is linear. That is to say, the dimension of $\widetilde{\mathcal{C}}_{D_F}$ is $2n - d_{K_3}$, where d_{K_3} is the dimension of the $\mathbb{F}_2$-vector space

$$K_3 = \left\{(a,b) \in \mathbb{F}_{2^n}^2 : \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x)+bF(y))} = 2^{2n}\right\}. \tag{5.9}$$

The Hamming weight of a codeword $\widetilde{\boldsymbol{c}}_{a,b}$ in $\widetilde{\mathcal{C}}_{D_F}$ is

$$\begin{aligned}\mathrm{wt}(\widetilde{\boldsymbol{c}}_{a,b}) &= |\{1 \le i,j \le l : \mathrm{Tr}_n(ad_i + bd_j) = 1\}| \\ &= \frac{1}{2}\left(l^2 - \sum_{d_i,d_j\in D_F} (-1)^{\mathrm{Tr}_n(ad_i+bd_j)}\right).\end{aligned} \tag{5.10}$$

Set $S_F(a,b) = \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x)+bF(y))}$. Note that

$$\begin{aligned}\sum_{d_i,d_j\in D_F} (-1)^{\mathrm{Tr}_n(ad_i+bd_j)} &= \frac{1}{4}\Bigg(\sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x)+bF(y))} - 2\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x))} - \\ &\qquad 2\sum_{y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bF(y))} + 4\Bigg) \\ &= \frac{1}{4}S_F(a,b) - \frac{1}{2}(W_F(0,a) + W_F(0,b)) + 1.\end{aligned}$$

Since the function F is 2-to-1 over $\mathbb{F}_{2^n}$ with $F(0) = 0$, then

$$\mathrm{wt}(\widetilde{\boldsymbol{c}}_{a,b}) = 2^{2n-3} - 2^{n-1} - \frac{1}{8}S_F(a,b) + \frac{1}{4}(W_F(0,a) + W_F(0,b)). \tag{5.11}$$

The next theorem describes the minimum distance of the dual code of $\widetilde{\mathcal{C}}_{D_F}$ in (5.8).

Theorem 5.1.2 *Let F be a 2-to-1 mapping over $\mathbb{F}_{2^n}$ with $F(0) = 0$ and let $\widetilde{\mathcal{C}}_{D_F}$ be the code defined as in (5.8). Moreover, let $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ be the dual code of $\widetilde{\mathcal{C}}_{D_F}$ and d_{K_3} be defined as in (5.9). Then $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ is a $[(2^{n-1}-1)^2, (2^{n-1}-1)^2 - (2n - d_{K_3})]$ binary linear code with the minimum distance $d^{\perp}$ satisfying $3 \le d^{\perp} \le 4$. Moreover, the dual of $\widetilde{\mathcal{C}}_{D_F}$ is projective.*

Proof: Based on the above discussion, the code $\widetilde{\mathcal{C}}_{D_F}$ is a $[(2^{n-1}-1)^2, 2n-d_{K_3}]$ binary linear code. The length and dimension of $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ can be easily determined. Next, we discuss the minimum distance of $\widetilde{\mathcal{C}}_{D_F}^{\perp}$.

Clearly, $d^{\perp}$ cannot be 1 since $0 \notin D_F$. By the definition of $\widetilde{\mathcal{C}}_{D_F}$, $d^{\perp}=2$ if and only if there exist two distinct pairs $(d_i,d_j) \in D_f^2$ and $(d_i',d_j') \in D_f^2$ such that

$$\mathrm{Tr}_n(ad_i+bd_j)+\mathrm{Tr}_n(ad_i'+bd_j')=0,$$

for every $a,b \in \mathbb{F}_{2^n}$. That is, $\mathrm{Tr}_n(a(d_i+d_i')+b(d_j+d_j'))=0$ for every $a,b \in \mathbb{F}_{2^n}$, which implies that $d_i+d_i'=0$ and $d_j+d_j'=0$. That is, $(d_i,d_j)=(d_i',d_j')$ which is in contradiction with the assumption. This confirms that $d^{\perp} \geq 3$. Suppose that $d^{\perp} \geq 5$. Then

$$\sum_{i=0}^{2} \binom{(2^{n-1}-1)^2}{i} (2-1)^i = 2^{4n-5}-2^{3n-2}+7\cdot 2^{2n-3}-3\cdot 2^{n-1}+2 > 2^{2n-d_{K_3}},$$

which contradicts to the Sphere packing bound (see [54, Theorem 1.12.1]). Hence, $3 \leq d^{\perp} \leq 4$.

The proof is completed. ■

5.2 Weight distributions of binary linear codes

In this section, we investigate the weight distributions of binary linear codes $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ defined in (5.1), (5.5) and (5.8), respectively. We shall distinguish different cases depending on the value of n. The constraints come from the two-to-one property.

5.2.1 The case $n = 2m$

This subsection proposes several binary codes with few weights derived from the known 2-to-1 functions given in Lemmas 2.4.3-2.4.7. Firstly, we construct two classes of binary linear codes with 3-weight and a class of binary linear codes with 9-weight from the 2-to-1 function presented in Lemma 2.4.3.

Theorem 5.2.1 *Let $n=2m$ and $F(x)=x^{2^{m+1}+4}+x^{2^{m+2}+2}+\alpha x \in \mathbb{F}_{2^n}[x]$, where $m \geq 3$ is odd, and $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha^{2^m-1}=w$ with $w \in \mathbb{F}_{2^2}\backslash\mathbb{F}_2$. Define three linear codes $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ as in (5.1), (5.5) and (5.8), respectively. Then,*

(1) $\mathcal{C}_F$ is a three-weight binary linear code with parameters $[2^n-1, 3m, 2^{n-1}-2^m]$, and its weight distribution is given by Table 5.2.1;

(2) $\mathcal{C}_{D_F}$ is a three-weight binary linear code with parameters $[2^{n-1}-1, n, 2^{n-2}-2^{m-1}]$, and its weight distribution is given by Table 5.2.2;

(3) $\widetilde{\mathcal{C}}_{D_F}$ is a nine-weight binary linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{m-1}(2^{n-1}-1)]$, and its weight distribution is given by Table 5.2.3.

***Table 5.2.1**: The weight distribution of the code $\mathcal{C}_F$ in Theorem 5.2.1(1) (or Theorem 5.2.5(1))*

Weight	Frequency
0	1
$2^{n-1}-2^m$	$2^{3m-3}+2^{n-3}-2^{m-2}$
2^{n-1}	$3\cdot 2^{3m-2}+2^{n-2}-1$
$2^{n-1}+2^m$	$2^{3m-3}-3\cdot 2^{n-3}+2^{m-2}$

***Table 5.2.2**: The weight distribution of the code $\mathcal{C}_{D_F}$ in Theorem 5.2.1(2) (or Theorem 5.2.5(2))*

Weight	Frequency
0	1
$2^{n-2}-2^{m-1}$	$2^{n-3}+2^{m-2}$
2^{n-2}	$3\cdot 2^{n-2}-1$
$2^{n-2}+2^{m-1}$	$2^{n-3}-2^{m-2}$

Proof: First of all, we shall determine the values of the Walsh transform $W_F(a,b)$ (and, particularly $W_F(0,b), W_F(0,a)$). For any $a,b\in\mathbb{F}_{2^n}$, we have

$$\begin{aligned} W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bF(x))} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+b(x^{2^{m+1}+4}+x^{2^{m+2}+2}+\alpha x))} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n((a+b\alpha)x+(b^{2^m}+b)x^{2^{m+2}+2})}. \end{aligned}$$

If $b^{2^m}+b=0$, i.e., $b\in\mathbb{F}_{2^m}$, then

$$W_F(a,b)=\begin{cases} 2^n, & \text{if } a+b\alpha=0; \\ 0, & \text{otherwise.} \end{cases}$$

If $b^{2^m}+b\neq 0$, then $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. Set $\varphi_{a,b}(x)=\mathrm{Tr}_n(ax+bF(x))$. Then the bilinear form of $\varphi_{a,b}(x)$ is given by

$$\begin{aligned} B_{\varphi_{a,b}}(x,y) &= \varphi_{a,b}(x+y)+\varphi_{a,b}(x)+\varphi_{a,b}(y) \\ &= \mathrm{Tr}_n((b^{2^m}+b)(x^{2^{m+2}}y^2+x^2y^{2^{m+2}})) \\ &= \mathrm{Tr}_n(((b^{2^m}+b)y^2+(b^{2^m}+b)^2y^{2^3})x^{2^{m+2}}) \\ &= \mathrm{Tr}_n(L_b(y)x^{2^{m+2}}), \end{aligned}$$

where $L_b(y)=(b^{2^m}+b)y^2+(b^{2^m}+b)^2y^{2^3}$. Let $\ker(L_b)=\{y\in\mathbb{F}_{2^n}: L_b(y)=0\}$. By a computation, we have

$$\ker(L_b)=\{0,y_0,y_0w,y_0w^2\},$$

***Table 5.2.3**: The weight distribution of the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.1(3) (or Theorem 5.2.5(3))*

Weight	Frequency
0	1
$2^{2n-3}-2^{n-2}-2^{m-1}(2^{n-1}-1)$	$2^{n-2}+2^{m-1}$
$2^{2n-3}-2^n-2^m$	$(2^{n-3}-2^{m-2})^2$
$2^{2n-3}-2^n+2^m$	$(2^{n-3}+2^{m-2})^2$
$2^{2n-3}-2^{n-1}-2^{m-1}$	$(3\cdot 2^{n-2}-1)(2^{n-2}-2^{m-1})$
$2^{2n-3}-2^{n-1}$	$(3\cdot 2^{n-2}-1)^2$
$2^{2n-3}-2^{n-1}+2^{m-1}$	$(3\cdot 2^{n-2}-1)(2^{n-2}+2^{m-1})$
$2^{2n-3}-2^{n-2}$	$3\cdot 2^{n-1}-2$
2^{2n-3}	$2^{2n-5}-2^{n-3}$
$2^{2n-3}-2^{n-2}+2^{m-1}(2^{n-1}-1))$	$2^{n-2}-2^{m-1}$

where $y_0^3=\frac{1}{\sqrt{b+b^{2^m}}}$. Moreover,

$$\begin{aligned}\varphi_{a,b}(y_0)=\mathrm{Tr}_n(ay_0+bf(y_0)) &= \mathrm{Tr}_n((a+b\alpha)y_0+(b+b^{2^m})y_0^6)\\ &= \mathrm{Tr}_n((a+b\alpha)y_0+1)\\ &= \mathrm{Tr}_n((a+b\alpha)y_0) \text{ (Since } n \text{ is even)}.\end{aligned}$$

Similarly, we have

$$\begin{aligned}\varphi_{a,b}(y_0w)=\mathrm{Tr}_n(ay_0w+bf(y_0w)) &= \mathrm{Tr}_n((a+b\alpha)y_0w+w)\\ &= \mathrm{Tr}_n((a+b\alpha)y_0w)+\mathrm{Tr}_2(\mathrm{Tr}_2^n(1)w)\\ &= \mathrm{Tr}_n((a+b\alpha)y_0w)+\mathrm{Tr}_2(w) \text{ (Since } m \text{ is odd)}\\ &= \mathrm{Tr}_n((a+b\alpha)y_0w)+1,\end{aligned}$$

and $\varphi_{a,b}(y_0w^2)=\varphi_{a,b}(y_0)+\varphi_{a,b}(y_0w)$.

Hence, there must exist some $(a,b)\in\mathbb{F}_{2^n}\times(\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m})$ such that $\mathrm{Tr}_n(ax+bF(x))=0$ for all $x\in\ker(L_b)$. From Lemma 2.4.2, for any $a\in\mathbb{F}_{2^n}$ and $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, we have

$$W_F(a,b)=\begin{cases}\pm 2^{m+1}, & \mathrm{Tr}_n(ax+bF(x))=0 \text{ for all } x\in\ker(L_b),;\\ 0, & \text{otherwise.}\end{cases}$$

Having the above discussion regarding the values of $W_F(a,b)$, we determine the parameters and the weight distributions of $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$, respectively.

(1) For the linear code $\mathcal{C}_F$, $W_F(a,b)=2^n$ if and only if $b\in\mathbb{F}_{2^m}$ and $a+b\alpha=0$. Then, the dimension of $K_1=\{(a,b)\in\mathbb{F}_{2^n}^2 : W_F(a,b)=2^n\}$ is m according to Eq. (5.2). Thus, the dimension of $\mathcal{C}_F$ is $2n-m=3m$. Furthermore, for any $a,b\in\mathbb{F}_{2^n}$, $W_F(a,b)\in\{0,2^n,\pm 2^{m+1}\}$. Set $v_1=-2^{m+1},v_2=0,v_3=2^{m+1}$. According to Eq. (5.4), we obtain the occurrences X_i of $W_F(a,b)=v_i$ $(i=1,2,3)$ in the Walsh spectrum of F. Then there are $X_i/2^m$ codewords in $\mathcal{C}_F$ with Hamming weight $2^{n-1}-\frac{1}{2}v_i$, and the weight distribution of $\mathcal{C}_F$ can be determined.

(2) For the linear code $\mathcal{C}_{D_F}$, $W_F(0,b)=2^n$ if and only if $b=0$. Then, the dimension of $\mathcal{C}_{D_F}$ equals n by Eq. (5.6). If $b\in\mathbb{F}_{2^m}\backslash\{0\}$, then $W_F(0,b)=0$. If $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, from

the proof of (1), we have $\mathrm{Tr}_n(bF(y_0)) = \mathrm{Tr}_n(b\alpha y_0)$, $\mathrm{Tr}_n(bF(y_0w)) = \mathrm{Tr}_n(b\alpha y_0 w) + 1$ and $\mathrm{Tr}_n(bF(y_0w^2)) = \mathrm{Tr}_n(b\alpha y_0 w^2) + 1$. It is obvious that there exist some $b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$ such that $\mathrm{Tr}_n(bF(x)) = 0$, for all $x \in \ker(L_b)$. Hence, for any $b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$, we have $W_F(0,b) \in \{0, \pm 2^{m+1}\}$ by Lemma 2.4.2. According to Eq. (5.7), the Hamming weights of the codewords $\boldsymbol{c}_b$ in $\mathcal{C}_{D_F}$ satisfy $\mathrm{wt}(\boldsymbol{c}_b) \in \{2^{n-2}, 0, 2^{n-2} - 2^{m-1}, 2^{n-2} + 2^{m-1}\}$. Define $w_1 = 2^{n-2} - 2^{m-1}, w_2 = 2^{n-2}, w_3 = 2^{n-2} + 2^{m-1}$. By Lemma 5.1.1, the dual of $\mathcal{C}_{D_F}$ has Hamming weight no less than 3. From the Pless power moments in (2.4) lead to the following system of equations:

$$\begin{cases} \sum_{i=1}^{3} A_{w_i} = 2^n - 1; \\ \sum_{i=1}^{3} w_i A_{w_i} = 2^{n-1} \cdot (2^{n-1} - 1); \\ \sum_{i=1}^{3} w_i^2 A_{w_i} = 2^{n-2} \cdot (2^{n-1} - 1) \cdot 2^{n-1}. \end{cases} \tag{5.12}$$

By solving Eq. (5.12), it is easy to determine the weight distribution of $\mathcal{C}_{D_F}$.

(3) We first determine the weight of the codewords $\widetilde{\boldsymbol{c}}_{a,b}$ in $\widetilde{\mathcal{C}}_{D_F}$, that is, we need to calculate the values of $S_F(a,b), W_F(0,a)$ and $W_F(0,b)$ by Eq. (5.11). By the proof of (2), we have $W_F(0,a), W_F(0,b) \in \{0, 2^n, \pm 2^{m+1}\}$. Next, we only determine the values of $S_F(a,b)$.

$$\begin{aligned} S_F(a,b) &= \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x)+bF(y))} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(aF(x))} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bF(y))} \\ &= W_F(0,a) \cdot W_F(0,b) \\ &= \begin{cases} 2^{2n}, & \text{if } W_F(0,a) = W_F(0,b) = 2^n; \\ \pm 2^{n+m+1}, & \text{if } W_F(0,a) = 2^n \text{ and } W_F(0,b) = \pm 2^{m+1} \\ & (\text{or } W_F(0,a) = \pm 2^{m+1} \text{ and } W_F(0,b) = 2^n); \\ \pm 2^{n+2}, & \text{if } W_F(0,a) = \pm 2^{m+1} \text{ and } W_F(0,b) = \pm 2^{m+1}; \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

For the linear code $\widetilde{\mathcal{C}}_{D_F}$, $S_F(a,b) = 2^{2n}$ if and only if $a = 0$ and $b = 0$. Then, the dimension of $\widetilde{\mathcal{C}}_{D_F}$ equals $2n$ by Eq. (5.9). From Eq. (5.11) and by a simple calculation, we have

$$\mathrm{wt}(\widetilde{\boldsymbol{c}}_{a,b}) = \begin{cases} 2^{2n-3} - 2^{n-1}, & \text{if } W_F(0,a) = W_F(0,b) = 0; \\ 2^{2n-3} - 2^{n-2}, & \text{if } W_F(0,a) = 0 \text{ and } W_F(0,b) = 2^n \\ & (\text{or } W_F(0,a) = 2^n \text{ and } W_F(0,b) = 0); \\ 2^{2n-3} - 2^{n-1} \pm 2^{m-1}, & \text{if } W_F(0,a) = 0 \text{ and } W_F(0,b) = \pm 2^{m+1} \\ & (\text{or } W_F(0,a) = \pm 2^{m+1} \text{ and } W_F(0,b) = 0); \\ 0, & \text{if } W_F(0,a) = W_F(0,b) = 2^n; \\ 2^{2n-3} - 2^{n-2} \pm 2^{m-1}(2^{n-1} - 1), & \text{if } W_F(0,a) = 2^n \text{ and } W_F(0,b) = \pm 2^{m+1} \\ & (\text{or } W_F(0,a) = \pm 2^{m+1} \text{ and } W_F(0,b) = 2^n); \\ 2^{2n-3} - 2^n \pm 2^{\frac{n}{2}}, & \text{if } W_F(0,a) = \pm 2^{m+1} \text{ and } W_F(0,b) = \pm 2^{m+1}; \\ 2^{2n-3}, & \text{if } W_F(0,a) = \pm 2^{m+1} \text{ and } W_F(0,b) = \mp 2^{m+1}. \end{cases}$$

According to Table 5.2.2, we have

$$W_F(0,a) = W_F(0,b) \quad = \quad \begin{cases} 0, & \text{with } 3\cdot 2^{n-2}-1 \text{ times;} \\ 2^n, & \text{with 1 time;} \\ 2^{m+1}, & \text{with } 2^{n-3}+2^{m-2} \text{ times;} \\ -2^{m+1}, & \text{with } 2^{n-3}-2^{m-2} \text{ times.} \end{cases}$$

Hence, the value distribution of $\mathrm{wt}(\widetilde{\boldsymbol{c}}_{a,b})$ is obtained in Table 5.2.3.

This completes the proof. ■

Remark 5.2.2 *By comparing with [72], the linear code $\mathcal{C}_{D_F}$ in Theorem 5.2.1(2) has the same parameters as that in [72, Theorem 2(2)], but our linear code $\mathcal{C}_{D_F}$ is obtained by the different 2-to-1 function.*

Remark 5.2.3 *The binary linear codes $\mathcal{C}_F$ and $\mathcal{C}_{D_F}$ derived from the 2-to-1 function in Lemma 2.4.9 have been studied in [72, Theorem 2]. In a similar way to that of Theorem 5.2.1(3), the weight distributions of the linear code $\widetilde{\mathcal{C}}_{D_F}$ from the 2-to-1 function in Lemma 2.4.9 can be determined. The results show that the weight distribution and parameters of $\widetilde{\mathcal{C}}_{D_F}$ are the same as those of the linear code in Theorem 5.2.1. Therefore, its specification is omitted here.*

In the following, we give a concrete example of Theorem 5.2.1.

Example 5.2.4 *Let $m = 3$. The code $\mathcal{C}_F$ in Theorem 5.2.1(1) is a binary linear code with parameters $[63,9,24]$, and its weight enumerator is $1+70z^{24}+399z^{32}+42z^{40}$. The code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.1(3) is a binary linear code with parameters $[961,12,372]$, and its weight enumerator is $1+20z^{372}+36z^{440}+100z^{456}+564z^{476}+2209z^{480}+940z^{484}+94z^{496}+120z^{512}+12z^{620}$.*

Next, we present two families of 3-weight and a family of 9-weight binary linear codes from the 2-to-1 functions listed in Lemma 2.4.4(2).

Theorem 5.2.5 *Let $n = 2m$ and $F(x) = (x^2+x+\delta)^{2^{2m-1}+2^{m-1}}+x+\delta^{2^{2m-1}+2^{m-1}}$ with $\delta \in \mathbb{F}_{2^n}$, where m is even and $\mathrm{Tr}_n(\delta) = 1$. Define three linear codes $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ as in (5.1), (5.5) and (5.8), respectively. Then,*

(1) $\mathcal{C}_F$ is a three-weight binary linear code with parameters $[2^n-1, 3m, 2^{n-1}-2^m]$, its weight distribution is given by Table 5.2.1;

(2) $\mathcal{C}_{D_F}$ is a three-weight binary linear code with parameters $[2^{n-1}-1, n, 2^{n-2}-2^{m-1}]$, and its weight distribution is given by Table 5.2.2;

(3) $\widetilde{\mathcal{C}}_{D_F}$ is a nine-weight binary linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{m-1}(2^{n-1}-1)]$, and its weight distribution is given by Table 5.2.3.

Proof: Since $\mathrm{Tr}_n(b(x^2+x+\delta)^{2^{2m-1}+2^{m-1}}) = \mathrm{Tr}_n(b^{2^{2m}}((x^2+x+\delta)^{2^m+1})^{2^{m-1}}) = \mathrm{Tr}_n(b^{2^{m+1}}(x^2+x+\delta)^{2^m+1})$, we have

$$\begin{aligned} W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bF(x))} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+b^{2^{m+1}}(x^2+x+\delta)^{2^m+1}+bx-b^{2^{m+1}}\delta^{2^m+1}))} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n((a+b)x+b^{2^{m+1}}(x^{2^{m+1}+2}+x^{2^{m+1}+1}+\delta x^{2^{m+1}}+x^{2^m+2}+x^{2^m+1}+\delta x^{2^m}+\delta^{2^m}x^2+\delta^{2^m}x))}. \end{aligned}$$

Set $\varphi_{a,b}(x) = \mathrm{Tr}_n(ax+bF(x))$. Then, the bilinear form of $\varphi_{a,b}(x)$ is given by

$$\begin{aligned} B_{\varphi_{a,b}}(x,y) &= \varphi_{a,b}(x+y)+\varphi_{a,b}(x)+\varphi_{a,b}(y) \\ &= \mathrm{Tr}_n((b^{2^{m+1}}y^2+b^2y^2+b^{2^{m+1}}y+b^4y^4+b^{2^{m+2}}y^4+b^2y+b^{2^{m+2}}y^2+b^4y^2)x^{2^{m+1}}) \\ &= \mathrm{Tr}_n(((b^4+b^{2^{m+2}})y^4+(b^{2^{m+1}}+b^2+b^{2^{m+2}}+b^4)y^2+(b^{2^{m+1}}+b^2)y)x^{2^{m+1}}) \\ &= \mathrm{Tr}_n(((b+b^{2^m})^4y^4+((b^{2^m}+b)^2+(b^{2^m}+b)^4)y^2+(b^{2^m}+b)^2y)x^{2^{m+1}}) \\ &:= \mathrm{Tr}_n(L_b(y)x^{2^{m+1}}), \end{aligned}$$

where $L_b(y) = (b+b^{2^m})^4y^4+((b^{2^m}+b)^2+(b^{2^m}+b)^4)y^2+(b^{2^m}+b)^2y$.

If $b\in\mathbb{F}_{2^m}$, then we have $\mathrm{Tr}_n(ax+bF(x)) = \mathrm{Tr}_n((a+b)x+b^2(x^{2^{m+1}+2}+x^{2^m+1})) = \mathrm{Tr}_n((a+b)x)$ by $b^2(x^{2^{m+1}+2}+x^{2^m+1})\in\mathbb{F}_{2^m}$ and n is even. It is easy to check that

$$W_F(a,b) = \begin{cases} 2^n, & \text{if } a+b=0; \\ 0, & \text{otherwise.} \end{cases}$$

If $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, we let $\ker(L_b) = \{y\in\mathbb{F}_{2^n} : L_b(y)=0\}$. From Lemma 2.4.2, we have

$$W_F(a,b) = \begin{cases} \pm 2^{\frac{n+d_b}{2}}, & \text{if } \mathrm{Tr}_n(ax+bF(x)) = 0 \text{ for all } x\in\ker(L_b); \\ 0, & \text{otherwise,} \end{cases}$$

where d_b is the dimension of $\ker(L_b)$ over $\mathbb{F}_2$. From the expression of L_b, it is easy to see $d_b\le 2$. Moreover, since $n+d_b$ must be even and n is even, we have $d_b\in\{0,2\}$. Since $L_b(y) = (b+b^{2^m})^4y^4+((b^{2^m}+b)^2+(b^{2^m}+b)^4)y^2+(b^{2^m}+b)^2y$, it is obvious that $y=0,1$ are two solutions of $L_b(y)=0$ in $\mathbb{F}_{2^n}$. Then $d_b=2$ and the equation $L_b(y)=0$ has exactly four solutions in $\mathbb{F}_{2^n}$. Set $z = b^{2^m}+b$ and it is easy to check that $z\in\mathbb{F}_{2^m}^*$ by $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. Hence, we have

$$y^3+\frac{1+z^2}{z^2}y+\frac{1}{z^2} = 0.$$

Clearly, there exist the other two solutions A and B of $L_b(y)=0$ in $\mathbb{F}_{2^n}$ such that

$$(y-1)(y-A)(y-B) = 0,$$

and by comparing with the coefficient of y, we know that

$$\begin{cases} A+B+1=0; \\ A+B+AB=\frac{1+z^2}{z^2}; \\ AB=\frac{1}{z^2}. \end{cases}$$

Then it is clear that $A^2+A=\frac{1}{z^2}$ and $B^2+B=\frac{1}{z^2}$.

For $x=A$, we have

$$\begin{aligned} \mathrm{Tr}_n(ax+bF(x)) &= \mathrm{Tr}_n((a+b)A+b^{2^{m+1}}(A^{2^{m+1}}(A^2+A)+\delta A^{2^{m+1}}+A^{2^m}(A^2+A)+ \\ &\quad \delta A^{2^m}+\delta^{2^m}A^2+\delta^{2^m}A)) \\ &= \mathrm{Tr}_n((a+b)A+b^2(\frac{1}{z^2}+\delta)^{2^m}(A^2+A)+b^{2^{m+1}}\delta^{2^m}A^2+b^{2^{m+1}}\delta^{2^m}A) \\ &= \mathrm{Tr}_n((a^2+b^2+b^2(\frac{1}{z^2}+\delta^{2^m})+b^4(\frac{1}{z^2}+\delta)^{2^{m+1}}+b^{2^{m+1}}\delta^{2^m}+ \\ &\quad b^{2^{m+2}}\delta^{2^{m+1}})A^2). \end{aligned}$$

Hence, we have $\mathrm{Tr}_n(ax+bF(x))=0$ for $x=A$ if $a^2=b^2+b^2(\frac{1}{z^2}+\delta^{2^m})+b^4(\frac{1}{z^2}+\delta)^{2^{m+1}}+b^{2^{m+1}}\delta^{2^m}+b^{2^{m+2}}\delta^{2^{m+1}}$. Similarly, we can prove that there exist $(a,b)\in\mathbb{F}_{2^n}\times(\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m})$ such that $\mathrm{Tr}_n(ax+bF(x))=0$ for $x=B$. Thus, for any $a\in\mathbb{F}_{2^n}$ and $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$,

$$W_F(a,b) \in \{0,\pm 2^{m+1}\}.$$

The rest of the proof is similar to that of Theorem 5.2.1, and then we omit the details here. ■

Remark 5.2.6 *Although the linear codes in Theorem 5.2.1 and Theorem 5.2.5 have the same form of parameters and weight distributions, the derived codes from both statements are completely different (since $m\geq 3$ is odd in Theorem 5.2.1, whereas m is even in Theorem 5.2.5), leading to inequivalent codes.*

Remark 5.2.7 *Here, we only give the proof of the weight distributions of $\mathcal{C}_F,\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ derived from Lemma 2.4.4(2). The weight distributions of $\mathcal{C}_F,\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ from other 2-to-1 functions (i.e., Lemma 2.4.4(1)(3)) can be determined similarly and these linear codes have the same weight distributions and parameters as that of Theorem 5.2.5. Hence, we omit the details here.*

Example 5.2.8 *Let $m=2$. The code $\mathcal{C}_F$ in Theorem 5.2.5(1) is a binary linear code with parameters $[15,6,4]$, and its weight enumerator is $1+9z^4+51z^8+3z^{12}$. The code $\mathcal{C}_{D_F}$ in Theorem 5.2.5(2) is a binary linear code with parameters $[7,4,2]$, and its weight enumerator is $1+3z^2+11z^4+z^6$, which is almost optimal in the sense that the minimum distance of the optimal binary linear code with the length 7 and the dimension 4 is 3 by the online Database [44]. The code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.5(3) is a binary linear code with parameters $[49,8,12]$, its weight enumerator is $1+z^{12}+6z^{14}+9z^{20}+22z^{22}+121z^{24}+66z^{26}+22z^{28}+6z^{32}+2z^{42}$.*

Table 5.2.4*: The weight distribution of the code $\mathcal{C}_F$ in Theorem 5.2.10(1)*

Weight	Frequency
0	1
$2^{n-1}-2^{\frac{3m-1}{2}}$	$2^{2m-2}-2^{m-2}+2^{\frac{3m-5}{2}}-2^{\frac{m-3}{2}}$
2^{n-1}	$2^{3m}-2^{2m-1}-2^{m-1}-1$
$2^{n-1}+2^{\frac{3m-1}{2}}$	$2^{2m-2}-2^{m-2}-2^{\frac{3m-5}{2}}+2^{\frac{m-3}{2}}$

Now, we consider binary linear codes derived from the 2-to-1 functions in Lemmas 2.4.5, 2.4.6 and 2.4.7. Before giving the main results, we first present the following lemma, which is helpful for determining the Walsh coefficients.

Lemma 5.2.9 *[66, Theorem 3] Let $h \geq 1$ and let $a, l > 1$ be integers. Then*

$$\gcd(a^l+1, a^h-1) = \begin{cases} 1, & \text{if } \frac{h}{\gcd(l,h)} \text{ is odd and } a \text{ is even;} \\ 2, & \text{if } \frac{h}{\gcd(l,h)} \text{ is odd and } a \text{ is odd;} \\ a^{\gcd(l,h)}+1, & \text{if } \frac{h}{\gcd(l,h)} \text{ is even.} \end{cases}$$

By taking $c = 1$ in Lemma 2.4.5, we obtain four classes of binary linear codes specified below, which are 1-weight, 2-weight, 3-weight and 5-weight, respectively.

Theorem 5.2.10 *Let $n = 2m$ and $F(x) = (x^{2^m}+x+\delta)^{2^i+1}+x+\delta^{2^i+1}$ with $\gcd(m,i) = 1$, where $m, i \in \mathbb{N}$, $\delta \in \mathbb{F}_{2^n}$ and $\mathrm{Tr}_m^n(\delta^2+\delta) \neq 0$. Define three linear codes $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ as in (5.1), (5.5) and (5.8), respectively. Then,*

(1) $\mathcal{C}_F$ is a binary linear code with parameters $[2^n-1, 3m]$, and its weight distribution is given as follows:

- *(a) if $m \geq 3$ is odd, then $\mathcal{C}_F$ is a three-weight binary linear code with the minimal weight $2^{n-1}-2^{\frac{3m-1}{2}}$, and its weight distribution is given by Table 5.2.4.*
- *(b) if $m \geq 4$ is even, then $\mathcal{C}_F$ is a five-weight binary linear code with the minimal weight $2^{n-1}-2^{\frac{3m}{2}}$. Moreover, the weights of the codewords in $\mathcal{C}_F$ satisfy $\{2^{n-1}, 0, 2^{n-1}-2^{\frac{3m-2}{2}}, 2^{n-1}+2^{\frac{3m-2}{2}}, 2^{n-1}-2^{\frac{3m}{2}}, 2^{n-1}+2^{\frac{3m}{2}}\}$.*

(2) $\mathcal{C}_{D_F}$ is a one-weight binary linear code with parameters $[2^{n-1}-1, n-1, 2^{n-2}]$, and its weight enumerator is $1+(2^{n-1}-1)z^{2^{n-2}}$.

(3) $\widetilde{\mathcal{C}}_{D_F}$ is a two-weight binary linear code with parameters $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$, and its weight distribution is given by Table 5.2.5.

Table 5.2.5*: The weight distribution of the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.10(3) (or Theorems 5.2.13 or 5.2.17)*

Weight	Frequency
0	1
$2^{n-1}(2^{n-2}-1)$	$(2^{n-1}-1)^2$
$2^{n-2}(2^{n-1}-1)$	2^n-2

Proof: First of all, we shall determine the value of $W_F(a,b)$. For any $a,b \in \mathbb{F}_{2^n}$,

$$\begin{aligned}
W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bF(x))} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+b((x^{2^m}+x+\delta)^{2^i+1}+x-\delta^{2^i+1}))} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+b(x^{2^{m+i}+2^m}+x^{2^{m+i}+1}+\delta x^{2^{m+i}}+x^{2^i+2^m}+x^{2^i+1}+\delta x^{2^i}+\delta^{2^i}x^{2^m}+\delta^{2^i}x+x))} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n((a+b+b^{2^m}\delta^{2^{i+m}}+b\delta^{2^i})x+(b^{2^m}+b)x^{2^i+1}+(b^{2^m}+b)x^{2^m+2^i}+(b^{2^m}\delta^{2^m}+b\delta)x^{2^i})}.
\end{aligned}$$

If $b \in \mathbb{F}_{2^m}$, it follows from $\gcd(2^i, 2^n-1)=1$ that

$$\begin{aligned}
W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n((a+b+b\delta^{2^{i+m}}+b\delta^{2^i})x+(b\delta^{2^m}+b\delta)x^{2^i})} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n((a^{2^i}+b^{2^i}(1+\delta^{2^{2i}}+\delta^{2^{2i+m}})+b(\delta+\delta^{2^m}))x)} \\
&= \begin{cases} 2^n, & \text{if } a^{2^i}+b^{2^i}(1+\delta^{2^{2i}}+\delta^{2^{2i+m}})+b(\delta+\delta^{2^m})=0; \\ 0, & \text{otherwise.} \end{cases}
\end{aligned}$$

If $b \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, we let $\varphi_{a,b}(x) = \mathrm{Tr}_n((a+b+b^{2^m}\delta^{2^{i+m}}+b\delta^{2^i})x+(b^{2^m}+b)x^{2^i+1}+(b^{2^m}+b)x^{2^m+2^i}+(b^{2^m}\delta^{2^m}+b\delta)x^{2^i})$. Then the bilinear form of $\varphi_{a,b}(x)$ is given by

$$\begin{aligned}
B_{\varphi_{a,b}}(x,y) &= \varphi_{a,b}(x+y)+\varphi_{a,b}(x)+\varphi_{a,b}(y) \\
&= \mathrm{Tr}_n((b^{2^m}+b)(x^{2^i}y+xy^{2^i}+x^{2^m}y^{2^i}+x^{2^i}y^{2^m})) \\
&= \mathrm{Tr}_n(((b+b^{2^m})y^{2^m}+(b^{2^i}+b^{2^{m+i}})y^{2^{m+2i}}+(b^{2^{m+i}}+b^{2^i})y^{2^{2i}}+(b^{2^m}+b)y)x^{2^{m+i}}) \\
&:= \mathrm{Tr}_n(L_b(y)x^{2^{m+i}}),
\end{aligned}$$

where $L_b(y) = (b+b^{2^m})y^{2^m}+(b^{2^i}+b^{2^{m+i}})y^{2^{m+2i}}+(b^{2^{m+i}}+b^{2^i})y^{2^{2i}}+(b^{2^m}+b)y$. Let $\ker(L_b)=\{y\in\mathbb{F}_{2^n} : L_b(y)=0\}$. From Lemma 2.4.2, we have

$$W_F(a,b) = \begin{cases} \pm 2^{\frac{n+d_b}{2}}, & \text{if } \mathrm{Tr}_n(ax+bF(x))=0 \text{ for all } x\in\ker(L_b); \\ 0, & \text{otherwise,} \end{cases}$$

where d_b is the dimension of $\ker(L_b)$ over $\mathbb{F}_2$. From the expression of L_b, we have

$$(b+b^{2^m})(y+y^{2^m})+(b+b^{2^m})^{2^i}(y+y^{2^m})^{2^{2i}} = 0. \tag{5.13}$$

According to $b+b^{2^m} \in \mathbb{F}_{2^m}^*$ and Eq. (5.13), we obtain

$$\mathrm{Tr}_m^n(y) = 0 \text{ or } (\mathrm{Tr}_m^n(y))^{2^i+1} = \frac{1}{b+b^{2^m}}.$$

Set $T_1 := \{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^n(y) = 0\}$ and $T_2 := \{y \in \mathbb{F}_{2^n} : (\mathrm{Tr}_m^n(y))^{2^i+1} = \frac{1}{b+b^{2^m}}\}$. Then $\ker(L_b) = T_1 \cup T_2$. It is easy to know that $|T_1| = 2^m$. Next, we determine the number of elements in the set T_2. It follows from Lemma 5.2.9 and $\gcd(m,i) = 1$ that $\gcd(2^i+1, 2^m-1) = 1$ or 3. When m is odd, $|T_2| = 2^m$; when m is even, $|T_2| = 0$ if $\frac{1}{b+b^{2^m}} \notin (\mathbb{F}_{2^m})^{2^i+1}$, and $|T_2| = 3\cdot 2^m$ if $\frac{1}{b+b^{2^m}} \in (\mathbb{F}_{2^m})^{2^i+1}$. Hence, $|\ker(L_b)| = 2^m + 2^m = 2^{m+1}$ when m is odd, and $|\ker(L_b)| = 2^m + 0 = 2^m$ or $2^m + 3\cdot 2^m = 2^{m+2}$ when m is even. Namely,

$$d_b = \begin{cases} m+1, & \text{if } m \text{ is odd;} \\ m \text{ or } m+2, & \text{if } m \text{ is even.} \end{cases}$$

In the following, we show that there exist some $(a,b) \in \mathbb{F}_{2^n} \times (\mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m})$ such that $\mathrm{Tr}_n(ax+bF(x)) = 0$ for all $x \in \ker(L_b) = T_1 \cup T_2$.

For $\mathrm{Tr}_m^n(y) = 0$, i.e., $y \in \mathbb{F}_{2^m}$, it follows from $b^{2^m}+b, b^{2^m}\delta^{2^m}+b\delta, b^{2^m}\delta^{2^{i+m}}+b\delta^{2^i} \in \mathbb{F}_{2^m}$ and n is even that

$$\mathrm{Tr}_n(ax+bF(x)) = \mathrm{Tr}_n((a+b)x). \tag{5.14}$$

Obviously, $\mathrm{Tr}_n(ax+bF(x)) = 0$ for all $x \in T_1$ if $a = b$.

Now, we consider the equation

$$(\mathrm{Tr}_m^n(y))^{2^i+1} = \frac{1}{b+b^{2^m}}. \tag{5.15}$$

If $\frac{1}{b+b^{2^m}} \in (\mathbb{F}_{2^m})^{2^i+1}$, there are solutions to Eq. (5.15) over $\mathbb{F}_{2^n}$; otherwise there is no solution. Suppose that y_0 is a solution of Eq. (5.15). Then we have $y_0 + y_0^{2^m} = \alpha$, where α is a prescribed constant. Hence

$$\begin{aligned} \mathrm{Tr}_n(ax+bF(x)) &= \mathrm{Tr}_n((a+b+b^{2^m}\delta^{2^{i+m}}+b\delta^{2^i})y_0 + (b^{2^m}+b){y_0}^{2^i}\alpha + (b^{2^m}\delta^{2^m}+b\delta){y_0}^{2^i}) \\ &= \mathrm{Tr}_n((a^{2^i}+b^{2^i}+b^{2^{m+i}}\delta^{2^{2i+m}}+b^{2^i}\delta^{2^{2i}}+(b^{2^m}+b)\alpha+b^{2^m}\delta^{2^m}+b\delta){y_0}^{2^i}). \end{aligned}$$

Obviously, if $a^{2^i} = b^{2^i} + b^{2^{m+i}}\delta^{2^{2i+m}} + b^{2^i}\delta^{2^{2i}} + (b^{2^m}+b)\alpha + b^{2^m}\delta^{2^m} + b\delta$, then $\mathrm{Tr}_n(ax+bF(x)) = 0$ for all $x \in T_2$.

Thus, for any $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$,

$$W_F(a,b) \in \begin{cases} \{0, \pm 2^{\frac{3m+1}{2}}\}, & \text{if } m \text{ is odd;} \\ \{0, \pm 2^{\frac{3m}{2}}, \pm 2^{\frac{3m+2}{2}}\}, & \text{if } m \text{ is even.} \end{cases}$$

Next, we discuss the parameters of $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$, respectively.

(1) For the linear code $\mathcal{C}_F$, $W_F(a,b) = 2^n$ if and only if $b \in \mathbb{F}_{2^m}$ and $a^{2^i} + b^{2^i}(1 + \delta^{2^{2i}} + \delta^{2^{2i+m}}) + b(\delta + \delta^{2^m}) = 0$. Then, the dimension of $K_1 = \{(a,b) \in \mathbb{F}_{2^n}^2 : W_F(a,b) = 2^n\}$ is m according to Eq. (5.2). Thus, the dimension of $\mathcal{C}_F$ is $2n - m = 3m$. When m is odd, for any $a,b \in \mathbb{F}_{2^n}$, $W_F(a,b) \in \{0, 2^n, \pm 2^{\frac{3m+1}{2}}\}$. Set $v_1 = -2^{\frac{3m+1}{2}}, v_2 = 0, v_3 = 2^{\frac{3m+1}{2}}$. Similar to the proof of Theorem 5.2.1(1), we obtain the desired weight distribution of $\mathcal{C}_F$ in Table 5.2.4. When m is even, for any $a,b \in \mathbb{F}_{2^n}$, $W_F(a,b) \in \{0, 2^n, \pm 2^{\frac{3m}{2}}, \pm 2^{\frac{3m+2}{2}}\}$. By Eq. (5.3), the Hamming weights of the codewords $\boldsymbol{c}_{a,b}$ in $\mathcal{C}_F$ can be obtained.

(2) For linear code $\mathcal{C}_{D_F}$, $W_F(0,b) = 2^n$ if and only if

$$b^{2^i}(1 + \delta^{2^{2i}} + \delta^{2^{2i+m}}) + b(\delta + \delta^{2^m}) \;=\; 0. \tag{5.16}$$

It is obvious that 0 is a solution of Eq. (5.16). Since $\mathrm{Tr}_m^n(\delta^2 + \delta) \neq 0$, we have $\delta + \delta^{2^m} \neq 0$ and $\delta + \delta^{2^m} \neq 1$. Hence, from Eq. (5.16), we have $b^{2^i - 1} = \frac{\delta + \delta^{2^m}}{1 + \delta^{2^{2i}} + \delta^{2^{2i+m}}} \in \mathbb{F}_{2^m}^*$. Since $\gcd(2^i - 1, 2^m - 1) = 2^{\gcd(i,m)} - 1 = 1$, Eq. (5.16) has exactly one nonzero solution. Then, the dimension of $K_2 = \{b \in \mathbb{F}_{2^n} : W_F(0,b) = 2^n\}$ is 1 according to Eq. (5.6).

Next, we will show that the Walsh transform $W_F(0,b) = 0$ when $b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$, so we just need to prove that there exists $x \in \ker(L_b)$ such that $\mathrm{Tr}_n(bF(x)) \neq 0$. Note that $\{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^n(y) = 0\} \subseteq \ker(L_b)$. It follows from Eq. (5.14) that $\mathrm{Tr}_n(bF(x)) = \mathrm{Tr}_n(bx) = \mathrm{Tr}_m(\mathrm{Tr}_m^n(b)x)$. Since $\mathrm{Tr}_m^n(b) = b + b^{2^m} \neq 0$, there must be some $x \in \ker(L_b)$ such that $\mathrm{Tr}_n(bF(x)) \neq 0$. Hence, $W_F(0,b) = 0$ when $b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$. Consequently, for any $b \in \mathbb{F}_{2^n}$, $W_F(0,b) \in \{0, 2^n\}$. Moreover, by Eq. (5.7), we know that the Hamming weights of the codewords $\boldsymbol{c}_b$ in $\mathcal{C}_{D_F}$ satisfy

$$\mathrm{wt}(\boldsymbol{c}_b) \in \{0, 2^{n-2}\}.$$

The desired weight distribution of $\mathcal{C}_{D_F}$ is easy to obtain.

(3) The proof is similar to that of Theorem 5.2.1(3), and then we omit the details here. This completes the proof. ■

Example 5.2.11 *By taking $i = 1$ in Lemma 2.4.5. Let $m = 3$. The code $\mathcal{C}_F$ in Theorem 5.2.10(a) is a binary linear code with parameters $[63, 9, 16]$, and its weight enumerator is $1 + 21z^{16} + 483z^{32} + 7z^{48}$. The code $\mathcal{C}_{D_F}$ in Theorem 5.2.10(2) is a binary linear code with $[31, 5, 16]$, and its weight enumerator is $1 + 31z^{16}$, which is optimal by the online Database [44]. Let $m = 4$. The code $\mathcal{C}_F$ in Theorem 5.2.10(b) is a binary linear code with parameters $[255, 12, 64]$, and its weight enumerator is $1 + 15z^{64} + 100z^{96} + 3915z^{128} + 60x^{160} + 5x^{192}$. The code $\mathcal{C}_{D_F}$ in Theorem 5.2.10(2) is a binary linear code with parameters $[127, 7, 64]$, and its weight enumerator is $1 + 127z^{64}$, which is optimal by the online Database [44]. Let $m = 2$. The code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.10(3) is a binary linear code with parameters $[49, 6, 24]$, and its weight enumerator is $1 + 49z^{24} + 14z^{28}$, which is also optimal by the online Database [44].*

Remark 5.2.12 *In a similar discussion in the proof of Theorem 5.2.10, we can determine the weight distributions and parameters of $\mathcal{C}_F, \mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ from the 2-to-1*

functions in Lemmas 2.4.6 (taking $c = 1$) and 2.4.7, and then we omit it here. Furthermore, we obtain that these linear codes have the same weight distributions and parameters as that of Theorem 5.2.10.

5.2.2 The case $n = 2m+1$

The binary linear codes $\mathcal{C}_F$ and $\mathcal{C}_{D_F}$ derived from the known 2-to-1 function in Lemma 2.4.10 and the 2-to-1 function of the form $(x^{2^t}+x)^e$ with $\gcd(t,n) = 1$ have been investigated in [72]. In this subsection, we study the code $\widetilde{\mathcal{C}}_{D_F}$ with few nonzero weights derived from these 2-to-1 functions.

In the following, the binary linear code with 2-weight is derived from the 2-to-1 function in Lemma 2.4.10(1)(2).

Theorem 5.2.13 *Let $n = 2m+1$ and $F(x) = x^{2^{m+1}+2} + x^{2^{m+1}+1} + x^2 + x$ or $F(x) = x^{2^{m+1}+4} + x^{2^{m+1}+2} + x^2 + x \in \mathbb{F}_{2^n}[x]$, where m is a positive integer. Define the linear code $\widetilde{\mathcal{C}}_{D_F}$ as in (5.8). Then, $\widetilde{\mathcal{C}}_{D_F}$ is a two-weight binary linear code with parameters $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$, and its weight distribution is given by Table 5.2.5.*

Proof: In view of [72, Theorem 5] and by utilizing a proof similar to that of Theorem 5.2.10(3), we can obtain the desired result. Hence, we omit it here. ■

In the following, we present a concrete example, and the computations are carried out using Magma software [2].

Example 5.2.14 *By taking $m = 2$ in Theorem 5.2.13, the code $\widetilde{\mathcal{C}}_{D_F}$ is a binary linear code with parameters $[225, 8, 112]$, and its weight enumerator is $1 + 225z^{112} + 30z^{120}$, which is optimal by the online Database [44].*

Next, we obtain the binary linear code with 8-weight derived from the 2-to-1 function in Lemma 2.4.10(3)(4) and the 2-to-1 function of the form $(x^{2^t}+x)^e$.

Theorem 5.2.15 *Let $n = 2m+1$ and $F(x) = x^{2^n-2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$ or $F(x) = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + x$ or $F(x) = (x^{2^t}+x)^e$ with $\gcd(t,n) = 1$ and e being one of the almost bent exponents in [72, Table X], where $m > 1$ be a positive integer. Define the linear code $\widetilde{\mathcal{C}}_{D_F}$ as in (5.8). Then, $\widetilde{\mathcal{C}}_{D_F}$ is an eight-weight binary linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{\frac{n-3}{2}}(2^{n-1}-1)]$, and its weight distribution is given by Table 5.2.6.*

Proof: According to [72, Theorems 3 and 11] and by using a proof similar to that of Theorem 5.2.1(3), we can easily obtain the desired result. Therefore, we omit it here. ■

In the following, we present a concrete example to explain Theorem 5.2.15. In addition, the computations are carried out using Magma software [2].

Example 5.2.16 *By taking $m = 2$ in Theorem 5.2.15, the code $\widetilde{\mathcal{C}}_{D_F}$ is a binary linear code with parameters $[225, 10, 90]$, its weight enumerator is $1 + 20z^{90} + 36z^{100} + 100z^{108} + 180z^{110} + 225z^{112} + 300z^{114} + 150z^{120} + 12z^{150}$.*

***Table 5.2.6**: The weight distribution of the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.15*

Weight	Frequency
0	1
$2^{2n-3}-2^{n-2}-2^{\frac{n-3}{2}}(2^{n-1}-1)$	$2^{n-1}+2^m$
$2^{2n-3}-3\cdot 2^{n-2}-2^{\frac{n-1}{2}}$	$(2^{n-2}-2^{m-1})^2$
$2^{2n-3}-3\cdot 2^{n-2}+2^{\frac{n-1}{2}}$	$(2^{n-2}+2^{m-1})^2$
$2^{2n-3}-2^{n-1}-2^{\frac{n-3}{2}}$	$(2^{n-1}-1)(2^{n-1}-2^m)$
$2^{2n-3}-2^{n-1}$	$(2^{n-1}-1)^2$
$2^{2n-3}-2^{n-1}+2^{\frac{n-3}{2}}$	$(2^{n-1}-1)(2^{n-1}+2^m)$
$2^{2n-3}-2^{n-2}$	$2^{2n-3}+3\cdot 2^{2m-1}-2$
$2^{2n-3}-2^{n-2}+2^{\frac{n-3}{2}}(2^{n-1}-1))$	$2^{n-1}-2^m$

5.2.3 The case $n = 3m$

The binary linear codes $\mathcal{C}_F$ and $\mathcal{C}_{D_F}$ derived from the known 2-to-1 functions in Lemmas 2.4.11 and 2.4.12 have been studied in [72]. In this subsection, we investigate the binary code $\widetilde{\mathcal{C}}_{D_F}$ with few nonzero weights derived from these 2-to-1 functions.

In the following, the 2-weight and the 9-weight binary linear codes are derived from the 2-to-1 function in Lemma 2.4.11.

Theorem 5.2.17 *Let $n = 3m$ and $F(x) = x^{2^{2m}+1} + x^{2^{m+1}} + x^{2^m+1} + x$, where $m := 0 \pmod 3$ is a positive integer. Define the linear code $\widetilde{\mathcal{C}}_{D_F}$ as in (5.8). Then, $\widetilde{\mathcal{C}}_{D_F}$ is a two-weight binary linear code with parameters $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$, and its weight distribution is given by Table 5.2.5.*

Proof: According to [72, Theorem 6] and by using a proof similar to that of Theorem 5.2.10(3), we obtain the desired result. Therefore, we omit the proof here. ■

In the following, we give an example to illustrate Theorem 5.2.17. In addition, the computations are carried out using Magma software [2].

Example 5.2.18 *By taking $m = 3$ in Theorem 5.2.17, the code $\widetilde{\mathcal{C}}_{D_F}$ is a binary linear code with parameters $[65025, 16, 32512]$, its weight enumerator is $1 + 65025z^{32512} + 50z^{32640}$.*

Remark 5.2.19 *Although the linear codes in Theorems 5.2.10 (with $n = 2m$), 5.2.13 (with $n = 2m+1$) and 5.2.17 (with $n = 3m$ and $m := 0 \pmod 3$) have the same form of parameters and weight distributions. The codes derived from these three theorems are different and inequivalent. Note that n has not same parity in Theorem 5.2.10 and Theorem 5.2.13 and also, particularly, for $m = 3$ the corresponding codes from Theorem 5.2.17 cannot be obtained from Theorem 5.2.10.*

Theorem 5.2.20 *Let $n = 3m$ and $F(x) = x^{2^{2m+1}+1} + x^{2^{m+1}+1} + x^4 + x^3$, where $m > 1$ is an odd positive integer. Define the linear code $\widetilde{\mathcal{C}}_{D_F}$ as in (5.8). Then, $\widetilde{\mathcal{C}}_{D_F}$ is a binary linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n+2m-3}{2}}(2^{n-1}-1)]$, its weight distribution is given by Table 5.2.7.*

***Table 5.2.7**: The weight distribution of the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.20*

Weight	Frequency
0	1
$2^{2n-3}-2^{n-2}-2^{\frac{n+2m-3}{2}}(2^{n-1}-1)$	$2^{m-1}+2^{\frac{m-1}{2}}$
$2^{2n-3}-2^{n-1}-2^{n+2m-2}-2^{\frac{n+2m-1}{2}}$	$(2^{m-2}-2^{\frac{m-3}{2}})^2$
$2^{2n-3}-2^{n-1}-2^{n+2m-2}+2^{\frac{n+2m-1}{2}}$	$(2^{m-2}+2^{\frac{m-3}{2}})^2$
$2^{2n-3}-2^{n-1}(2^{2m-1}-1)$	$2^{2m-3}-2^{m-2}$
$2^{2n-3}-2^{n-1}-2^{\frac{n+2m-3}{2}}$	$(2^n-2^{m-1}-1)(2^{m-1}-2^{\frac{m-1}{2}})$
$2^{2n-3}-2^{n-1}$	$(2^n-2^{m-1}-1)^2$
$2^{2n-3}-2^{n-1}+2^{\frac{n+2m-3}{2}}$	$(2^n-2^{m-1}-1)(2^{m-1}+2^{\frac{m-1}{2}})$
$2^{2n-3}-2^{n-2}$	$2^{n+1}-2^m-2$
$2^{2n-3}-2^{n-2}+2^{\frac{n+2m-3}{2}}(2^{n-1}-1)$	$2^{m-1}-2^{\frac{m-1}{2}}$

Proof: The proof of this result is similar to that of Theorem 5.2.1(3), and then we omit the details here. ■

Next, we give an example to illustrate Theorem 5.2.20.

Example 5.2.21 *By taking $m=3$ in Theorem 5.2.20, the code $\widetilde{\mathcal{C}}_{D_F}$ is a binary linear code with parameters $[65025, 18, 16320]$, and its weight enumerator is $1+6z^{16320}+z^{24192}+9z^{24448}+6z^{24832}+1014z^{32448}+257049z^{32512}+3042z^{32576}+1014z^{32640}+2z^{48960}$.*

Next, we present a binary linear code with 9-weight derived from the 2-to-1 function in Lemma 2.4.12.

Theorem 5.2.22 *Let $n=km$ and $F(x)=\mathrm{Tr}_m^n(x^{2^m+1})+x$, where $k>1$ is an odd positive integer and $m>1$ is a positive integer. Define the linear code $\widetilde{\mathcal{C}}_{D_F}$ as in (5.8). Then, $\widetilde{\mathcal{C}}_{D_F}$ is a binary linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n+m-4}{2}}(2^{n-1}-1)]$, its weight distribution is given by Table 5.2.8.*

***Table 5.2.8**: The weight distribution of the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.22*

Weight	Frequency
0	1
$2^{2n-3}-2^{n-2}-2^{\frac{n+m-4}{2}}(2^{n-1}-1)$	$2^{n-m}+2^{\frac{n-m}{2}}$
$2^{2n-3}-2^{n-1}-2^{n+m-3}-2^{\frac{n+m-2}{2}}$	$(2^{n-m-1}-2^{\frac{n-m-2}{2}})^2$
$2^{2n-3}-2^{n-1}-2^{n+m-3}+2^{\frac{n+m-2}{2}}$	$(2^{n-m-1}+2^{\frac{n-m-2}{2}})^2$
$2^{2n-3}-2^{n-1}-2^{\frac{n+m-4}{2}}$	$(2^n-2^{n-m}-1)(2^{n-m}-2^{\frac{n-m}{2}})$
$2^{2n-3}-2^{n-1}$	$(2^n-2^{n-m}-1)^2$
$2^{2n-3}-2^{n-1}+2^{\frac{n+m-4}{2}}$	$(2^n-2^{n-m}-1)(2^{n-m}+2^{\frac{n-m}{2}})$
$2^{2n-3}-2^{n-2}$	$2^{n+1}-2^{n-m+1}-2$
$2^{2n-3}-2^{n-1}+2^{n+m-3}$	$2^{2n-2m-1}-2^{n-m-1}$
$2^{2n-3}-2^{n-2}+2^{\frac{n+m-4}{2}}(2^{n-1}-1))$	$2^{n-m}-2^{\frac{n-m}{2}}$

Proof: According to [72, Theorem 9] and by using a proof similar to that of Theorem 5.2.1(3), it is easy to obtain the desired result. ■

In the following, we give an example to illustrate Theorem 5.2.22, and the computations are carried out using Magma software [2].

Example 5.2.23 *By taking $k = 3, m = 2$ in Theorem 5.2.22, the code $\widetilde{\mathcal{C}}_{D_F}$ is a binary linear code with parameters $[961, 12, 372]$, and its weight enumerator is $1 + 20z^{372} + 36z^{440} + 100z^{456} + 564z^{476} + 2209z^{480} + 940z^{484} + 94z^{496} + 120z^{512} + 12z^{620}$.*

With the help of Lemma 2.2.6, we can obtain the following results. As an example, we only give a simple proof for the optimality of the code in Theorem 5.2.10, and similarly the others can be easily proved.

Theorem 5.2.24 *Let $n = 2m$ and m be a positive integer. Then both the code $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.10 are optimal codes.*

Proof: Thanks to Theorem 5.2.10(2), we know that $\mathcal{C}_{D_F}$ is a constant weight linear code, that is to say, $\mathcal{C}_{D_F}$ is a binary simplex code. Obviously, the code $\mathcal{C}_{D_F}$ is a Griesmer code (i.e., length-optimal).

From Theorem 5.2.10(3), we have $\widetilde{\mathcal{C}}_{D_F}$ is a $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$ binary linear code. We claim that $\sum_{i=0}^{k-1} \left\lceil \frac{d+1}{p^i} \right\rceil > N$, violating the Griesmer bound. Then we classify the range of i to determine the value of $\lceil \frac{d+1}{2^i} \rceil$.

- If $0 \le i \le n-1$, then $\left\lceil \frac{d+1}{2^i} \right\rceil = 2^{n-1-i}(2^{n-2}-1)+1$;
- If $n \le i \le 2n-3$, then $\left\lceil \frac{d+1}{2^i} \right\rceil = 2^{2n-3-i}$.

Hence,

$$\begin{aligned}
\sum_{i=0}^{k-1} \left\lceil \frac{d+1}{2^i} \right\rceil &= \sum_{i=0}^{n-1} \left\lceil \frac{d+1}{2^i} \right\rceil + \sum_{i=n}^{2n-3} \left\lceil \frac{d+1}{2^i} \right\rceil \\
&= \sum_{i=0}^{n-1} (2^{n-1-i}(2^{n-2}-1)+1) + \sum_{i=n}^{2n-3} 2^{2n-3-i} \\
&= 2^{2n-2} - 2^n + n.
\end{aligned}$$

Note that $\sum_{i=0}^{k-1} \left\lceil \frac{d+1}{2^i} \right\rceil - N = 2^{2n-2} - 2^n + n - (2^{n-1}-1)^2 = n-1 > 0$.

This completes the proof. ■

Theorem 5.2.25 *Let $n = 2m+1$ and m be a positive integer. Then the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.13 is optimal.*

Theorem 5.2.26 *Let $n = 3m$ and $m := 0 \pmod 3$ be a positive integer. Then the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.17 is optimal.*

5.3 Applications

In this section, we first observe that the obtained codes in Section 5.2 are in fact minimal. We, therefore, describe the access structures of the secret sharing schemes based on their dual codes.

Firstly, using Lemma 2.2.9, we emphasize that the binary linear codes constructed in this chapater are minimal for almost all cases. Proving the minimality property of each code would be pretty long. For this reason and to avoid redundancy in the proofs, we present, as an example, the proof showing that the codes from Theorem 5.2.1 are minimal (the minimality of the other codes can be shown similarly).

Theorem 5.3.1 *Let $m \geq 3$ be odd and $n = 2m$. Then the following statements hold.*

(1) The code $\mathcal{C}_F$ in Theorem 5.2.1(1) is a minimal linear code with parameters $[2^n - 1, 3m, 2^{n-1} - 2^m]$;

(2) The code $\mathcal{C}_{D_F}$ in Theorem 5.2.1(2) is a minimal linear code with parameters $[2^{n-1} - 1, n, 2^{n-2} - 2^{m-1}]$;

(3) The code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.1(3) is a minimal linear code with parameters $[(2^{n-1} - 1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{m-1}(2^{n-1} - 1)]$.

Proof: (1) By Theorem 5.2.1 (1) and Table 5.2.1, we know that the minimum nonzero weight $w_{\min} = 2^{n-1} - 2^m$ and the maximum nonzero weight $w_{\max} = 2^{n-1} + 2^m$. Then substituting these values into the inequality of Lemma 2.2.9, we get

$$\begin{aligned} 2w_{\min} - w_{\max} &= 2(2^{n-1} - 2^m) - (2^{n-1} + 2^m) \\ &= 2^m(2^{m-1} - 3) > 0, \end{aligned}$$

which is true for $m \geq 3$ odd.

(2) Note that $w_{\min} = 2^{n-2} - 2^{m-1}$ and $w_{\max} = 2^{n-2} + 2^{m-1}$ in Table 5.2.2. Similar to the proof of the case (1), the conclusion holds for $m \geq 3$ odd.

(3) From Table 5.2.3, we have $w_{\min} = 2^{2n-3} - 2^{n-2} - 2^{m-1}(2^{n-1} - 1)$ and $w_{\max} = 2^{2n-3} - 2^{n-2} + 2^{m-1}(2^{n-1} - 1)$. By using a proof similar to that of the case (1), we obtain the desired result. ■

As explained above, we shall present (successively without proof) the other minimal codes derived in Section 5.2.

Theorem 5.3.2 *Let $m \geq 4$ be even and $n = 2m$. Then the following statements hold.*

(1) The code $\mathcal{C}_F$ in Theorem 5.2.5(1) is a minimal linear code with parameters $[2^n - 1, 3m, 2^{n-1} - 2^m]$;

(2) The code $\mathcal{C}_{D_F}$ in Theorem 5.2.5(2) is a minimal linear code with parameters $[2^{n-1} - 1, n, 2^{n-2} - 2^{m-1}]$;

(3) The code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.5(3) is a minimal linear code with parameters $[(2^{n-1} - 1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{m-1}(2^{n-1} - 1)]$.

Theorem 5.3.3 *Let $n = 2m$ and m be a positive integer.*

(1) If $m \geq 5$ is odd, then the code $\mathcal{C}_F$ in Theorem 5.2.10(a) is a minimal linear code with parameters $[2^n - 1, 3m, 2^{n-1} - 2^{\frac{3m-1}{2}}]$;

(2) If $m \geq 6$ is even, then the code $\mathcal{C}_F$ in Theorem 5.2.10(b) is a minimal linear code with parameters $[2^n - 1, 3m, 2^{n-1} - 2^{\frac{3m}{2}}]$;

(3) If $m \geq 2$, then the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.10(3) is a minimal linear code with parameters $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$.

Theorem 5.3.4 *Let $n = 2m+1$ and $m \geq 2$ be a positive integer. Then the following statements hold.*

(1) The code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.13 is a minimal linear code with parameters $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$;

(2) The code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.15 is a minimal linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{\frac{n-3}{2}}(2^{n-1}-1)]$.

Theorem 5.3.5 *Let $n = 3m$ and m be a positive integer.*

(1) If $m := 0 \pmod 3$, then the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.17 is a minimal linear code with parameters $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$;

(2) If $m \geq 5$ is odd, then the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.20 is a minimal linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{\frac{n+2m-3}{2}}(2^{n-1}-1)]$.

Theorem 5.3.6 *Let $n = km$, and k be odd and m be a positive integer. If $k \geq 3$ and $m > 1$, then the code $\widetilde{\mathcal{C}}_{D_F}$ in Theorem 5.2.22 is a minimal linear code with parameters $[(2^{n-1}-1)^2, 2n, 2^{2n-3} - 2^{n-2} - 2^{\frac{n+m-4}{2}}(2^{n-1}-1)]$.*

Next, we investigate the application of the constructed linear codes in secret sharing schemes. The following proposition describes the access structure of a secret sharing scheme based on the dual code of a minimal linear code.

A secret sharing scheme (SSS) consists of a dealer, a group $\mathcal{P} = \{P_1, P_2, \ldots, P_\ell\}$ of ℓ participants, a secret space S, ℓ share spaces $S_1, S_2 \ldots, S_\ell$, a share computing procedure and a secret recovering procedure. The dealer chooses a secret s from S, computes a share, which belongs to S_i , of s (with the sharing computing procedure) for each participant P_i and then gives the share to P_i , where $i = 1, \ldots, \ell$. Any set covering a set of participants who can recover the secret s can also recover s. The sharing computing procedure and the secret s are known only by the dealer, while the secret recovering procedure is known by all the participants in P.

A set of participants who can recover the secret s from their shares is called *an access set*. The set of all access sets is called *the access structure* of a secret sharing scheme. An access set is called a *minimal access set* if any of its proper subsets cannot

recover s from their shares. Hence, we take only an interest in the set of all minimal access sets, which is said to be as *the nice access structure* of a secret sharing scheme

Generally, the access structure of the secret sharing scheme constructed by linear codes is difficult to determine, but the access structure of the secret sharing scheme constructed by dual codes of minimal linear codes is easier. From Theorems 5.3.1-5.3.6, we can know that the binary linear codes constructed in this chapter are minimal linear codes in most cases. Then the following proposition recalls the method of constructing access structure of the secret sharing scheme based on the dual codes of minimal linear codes.

Proposition 5.3.7 *Let $\mathcal{C}$ be a minimal linear $[N,k,d]_p$ code over $\mathbb{F}_p$ with the generator matrix $G = [\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{N-1}]$. Then, in the secret sharing scheme based on $\mathcal{C}^{\perp}$, the number of participants is $N-1$ and the number of minimal access sets is p^{k-1}.*

- *When $d^{\perp} = 2$, if $\boldsymbol{g}_i, 0 \le i \le N-1$, is a multiple of $\boldsymbol{g}_0$, then participant P_i must be in all minimal access sets; otherwise, in $(p-1)p^{k-2}$ out of p^{k-1} minimal access sets.*
- *When $d^{\perp} \ge 3$, for any fixed $1 \le t \le \min\{k-1, d^{\perp}-2\}$, every set of t participants is involved in $(p-1)^t p^{k-(t+1)}$ out of p^{k-1} minimal access sets.*

In the case $d^{\perp} = 2$, there are users who belong to every coalition: the "*dictators*"; In the case $d^{\perp} \ge 3$, the secret sharing scheme is "*democratic*": every user belongs to the same number of coalitions.

From [12, Theorem 5], Lemmas 5.1.1 and 5.1.2, we know that the dual codes of $\mathcal{C}_F$, $\mathcal{C}_{D_F}$ and $\widetilde{\mathcal{C}}_{D_F}$ have minimum distance $d^{\perp} \ge 3$. This implies that secret sharing schemes based on the dual codes of the obtained binary linear codes in Theorems 5.2.1, 5.2.5, 5.2.10, 5.2.13, 5.2.15, 5.2.17, 5.2.20 and 5.2.22 have access structures described in Proposition 5.3.7. Such a secret sharing scheme is said to be democratic.

In the subsequent corollaries, we describe the secret sharing schemes related to our minimal codes in this chapter.

Corollary 5.3.8 *Let $m \ge 3$ be odd (resp. $m \ge 3$ be even) and $n = 2m$.*

(1) Let $\mathcal{C}_F$ be the minimal $[2^n-1, 3m, 2^{n-1}-2^m]$ code in Theorem 5.2.1(1) (resp. Theorem 5.2.5(1)). Then, in the secret sharing scheme based on $\mathcal{C}_F^{\perp}$ with $d^{\perp} \ge 3$, the number of participants is equal to 2^n-2 and the number of minimal access sets is equal to 2^{3m-1}. For any fixed $1 \le t \le \min\{3m-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{3m-(t+1)}$ minimal access sets.

(2) Let $\mathcal{C}_{D_F}$ be the minimal $[2^{n-1}-1, n, 2^{n-2}-2^{m-1}]$ code in Theorem 5.2.1(2) (resp. Theorem 5.2.5(2)). Then, in the secret sharing scheme based on $\mathcal{C}_{D_F}^{\perp}$ with $d^{\perp} \ge 3$, the number of participants is equal to $2^{n-1}-2$ and the number of minimal access sets is equal to 2^{n-1}. For any fixed $1 \le t \le \min\{n-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{n-(t+1)}$ minimal access sets.

(3) Let $\widetilde{\mathcal{C}}_{D_F}$ be the minimal $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{m-1}(2^{n-1}-1)]$ code in Theorem 5.2.1(3) (resp. Theorem 5.2.5(3)). Then, in the secret sharing scheme

based on $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ with $d^{\perp} \geq 3$, the number of participants is equal to $(2^{n-1}-1)^2-1$ and the number of minimal access sets is equal to 2^{2n-1}. For any fixed $1 \leq t \leq \min\{2n-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{2n-(t+1)}$ minimal access sets.

Corollary 5.3.9 *Let $n = 2m$ and m be a positive integer.*

(1) Let $m \geq 5$ be odd and $\mathcal{C}_F$ be the minimal $[2^n-1, 3m, 2^{n-1}-2^{\frac{3m-1}{2}}]$ code in Theorem 5.2.10(a). Then, in the secret sharing scheme based on $\mathcal{C}_F^{\perp}$ with $d^{\perp} \geq 3$, the number of participants is equal to 2^n-2 and the number of minimal access sets is equal to 2^{3m-1}. For any fixed $1 \leq t \leq \min\{3m-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{3m-(t+1)}$ minimal access sets;

(2) Let $m \geq 6$ be even and $\mathcal{C}_F$ be the minimal $[2^n-1, 3m, 2^{n-1}-2^{\frac{3m}{2}}]$ code in Theorem 5.2.10(b). Then, in the secret sharing scheme based on $\mathcal{C}_F^{\perp}$ with $d^{\perp} \geq 3$, the number of participants is equal to 2^n-2 and the number of minimal access sets is equal to 2^{3m-1}. For any fixed $1 \leq t \leq \min\{3m-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{3m-(t+1)}$ minimal access sets;

(3) Let $m \geq 2$ and $\widetilde{\mathcal{C}}_{D_F}$ be the minimal $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$ code in Theorem 5.2.10(3). Then, in the secret sharing scheme based on $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ with $d^{\perp} \geq 3$, the number of participants is equal to $(2^{n-1}-1)^2-1$ and the number of minimal access sets is equal to 2^{2n-3}. For any fixed $1 \leq t \leq \min\{2n-3, d^{\perp}-2\}$, every set of t participants is involved in $2^{2n-1-(t+1)}$ minimal access sets.

Corollary 5.3.10 *Let $n = 2m+1$ and $m \geq 2$ be a positive integer.*

(1) Let $\widetilde{\mathcal{C}}_{D_F}$ be the minimal $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$ code in Theorem 5.2.13. Then, in the secret sharing scheme based on $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ with $d^{\perp} \geq 3$, the number of participants is equal to $(2^{n-1}-1)^2-1$ and the number of minimal access sets is equal to 2^{2n-3}. For any fixed $1 \leq t \leq \min\{2n-3, d^{\perp}-2\}$, every set of t participants is involved in $2^{2n-1-(t+1)}$ minimal access sets;

(2) Let $\widetilde{\mathcal{C}}_{D_F}$ be the minimal $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n-3}{2}}(2^{n-1}-1)]$ code in Theorem 5.2.15. Then, in the secret sharing scheme based on $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ with $d^{\perp} \geq 3$, the number of participants is equal to $(2^{n-1}-1)^2-1$ and the number of minimal access sets is equal to 2^{2n-1}. For any fixed $1 \leq t \leq \min\{2n-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{2n-(t+1)}$ minimal access sets.

Corollary 5.3.11 *Let $n = 3m$ and m be a positive integer.*

(1) Let $m := 0 \pmod 3$ and $\widetilde{\mathcal{C}}_{D_F}$ be the minimal $[(2^{n-1}-1)^2, 2n-2, 2^{n-1}(2^{n-2}-1)]$ code in Theorem 5.2.17. Then, in the secret sharing scheme based on $\widetilde{\mathcal{C}}_{D_F}^{\perp}$ with $d^{\perp} \geq 3$, the number of participants is equal to $(2^{n-1}-1)^2-1$ and the number of minimal access sets is equal to 2^{2n-3}. For any fixed $1 \leq t \leq \min\{2n-3, d^{\perp}-2\}$, every set of t participants is involved in $2^{2n-1-(t+1)}$ minimal access sets;

(2) Let $m \geq 5$ be odd and $\widetilde{\mathcal{C}}_{D_F}$ be the minimal $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n+2m-3}{2}}(2^{n-1}-1)]$ code in Theorem 5.2.20. Then, in the secret sharing scheme based on $\widetilde{\mathcal{C}}^{\perp}_{D_F}$ with $d^{\perp} \geq 3$, the number of participants is equal to $(2^{n-1}-1)^2-1$ and the number of minimal access sets is equal to 2^{2n-1}. For any fixed $1 \leq t \leq \min\{2n-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{2n-1-(t+1)}$ minimal access sets.

Corollary 5.3.12 *Let $n = km$, $k \geq 3$ be odd and $m > 1$ be a positive integer. Let $\widetilde{\mathcal{C}}_{D_F}$ be the minimal $[(2^{n-1}-1)^2, 2n, 2^{2n-3}-2^{n-2}-2^{\frac{n+m-4}{2}}(2^{n-1}-1)]$ code in Theorem 5.2.22. Then, in the secret sharing scheme based on $\widetilde{\mathcal{C}}^{\perp}_{D_F}$ with $d^{\perp} \geq 3$, the number of participants is equal to $(2^{n-1}-1)^2-1$ and the number of minimal access sets is equal to 2^{2n-1}. For any fixed $1 \leq t \leq \min\{2n-1, d^{\perp}-2\}$, every set of t participants is involved in $2^{2n-1-(t+1)}$ minimal access sets.*

5.4 Solving two open problems

In this section, we mainly solve two open problems presented in [72]: (1) Let n be odd. Prove that the exhibited function $F(x) = x^{3\cdot 2^{m+1}} + x^{2^{m+2}+1} + x^{2^{m+1}+1} + x$ is indeed 2-to-1 over $\mathbb{F}_{2^n}$; (2) Let $n = 3m$ and m is odd. Determine the weight distribution of the linear code $\mathcal{C}_F$ (defined in (5.1)) constructed from $F(x) = x^{2^{2m+1}+1} + x^{2^{m+1}+1} + x^4 + x^3$.

Next, we give the concrete proof of the open problem (1). Before doing that, we first recall the resultant of two polynomials over finite fields, which will be useful for proving the theorem later.

Definition 5.4.1 *[26, 77] Let $f(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{F}_q[x]$ and $g(x) = \sum_{i=0}^{m} b_i x^{m-i} \in \mathbb{F}_q[x]$ be two polynomials of formal degree n resp. m with $m, n \in \mathbb{N}$. The* resultant *$Res(f,g,x)$ of the two polynomials is defined by the determinant*

$$Res(f,g,x) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & & \cdots & a_n \\ b_0 & b_1 & \cdots & & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_m & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & & \cdots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

of order $m+n$.

Lemma 5.4.2 *[26] Under the assumption in Definition 5.4.1, $Res(f,g,x)$ has the following properties:*

(1) There are two polynomials $A, B \in \mathbb{F}_q[x]$ such that $Af + Bg = Res(f,g,x)$;

(2) $Res(f,g,x) = 0$ if and only if $f(x)$ and $g(x)$ have a common divisor in $\mathbb{F}_q[x]$ of positive degree;

(3) For two polynomials $F(x,y), G(x,y) \in \mathbb{F}_q[x,y]$ of positive degree in y, the resultant $Res(F,G,y)$ with respect to y is a polynomial in x, and is in the elimination ideal $\langle F,G\rangle \cap \mathbb{F}_q[x]$. So, $Res(F,G,y)$ vanishes at any common solution of $F = G = 0$.

Theorem 5.4.3 *[72, Problem 2] Let $n = 2m+1$ and F be the function defined by $F(x) = x^{3\cdot 2^{m+1}} + x^{2^{m+2}+1} + x^{2^{m+1}+1} + x$. Then F is 2-to-1 over $\mathbb{F}_{2^n}$.*

Proof: It is easy to verify that $F(x) = g(x^{2^{m+1}} + x)$, where $g(x) = x^{2^{m+1}+1} + x^{2^{m+1}} + x^3 + x^2 + x$. Since $L(x) := x^{2^{m+1}} + x$ is a 2-to-1 linearized function over $\mathbb{F}_{2^n}$, we now only need to prove that $g(x)$ is an injection from $T := \{L(x) \mid x \in \mathbb{F}_{2^n}\} = \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}_n(x) = 0\}$ to $\mathbb{F}_{2^n}$. Assume that there exist two elements x, X in T such that $g(x) + g(X) = 0$, i.e.,

$$x^{2^{m+1}+1} + x^{2^{m+1}} + x^3 + x^2 + x + X^{2^{m+1}+1} + X^{2^{m+1}} + X^3 + X^2 + X = 0. \tag{5.17}$$

Let $y = x^{2^{m+1}}$ and $Y = X^{2^{m+1}}$. Then Eq. (5.17) becomes

$$F(x,y,X,Y) := (X+1)Y + X^3 + x^3 + X^2 + x^2 + xy + X + x + y = 0. \tag{5.18}$$

Taking 2^{m+1}-power on both sides of Eq. (5.18) and simplifying it by $y^{2^{m+1}} = x^2$, $Y^{2^{m+1}} = X^2$, we have

$$G(x,y,X,Y) := Y^3 + Y^2 + \left(X^2+1\right)Y + yx^2 + y^3 + X^2 + x^2 + y^2 + y = 0. \tag{5.19}$$

From Eq. (5.18), we have

$$A(X,x,y) := Y = \frac{X^3 + x^3 + X^2 + x^2 + xy + X + x + y}{X+1}. \tag{5.20}$$

Plugging Eq. (5.20) into Eq. (5.19) and multiplying by $(X+1)^3$, we obtain

$$B(X,x,y) := (X+x)C(X,x,y)D(X,x,y) = 0,$$

where $C(X,x,y) := X^4 + \left(x^2+y\right)X^2 + (xy+x+y+1)X + x^4 + yx^2 + x^2 + xy + x + y + 1$; $D(X,x,y) := X^4 + (x+1)X^3 + (x+y)X^2 + \left(x^3 + x^2 + xy + y\right)X + x^4 + x^3 + x^2 + xy + y^2 + 1$. That is to say, we must have $C(X,x,y) = 0$ or $D(X,x,y) = 0$.

Case 1: If $C(X,x,y) = 0$. Taking 2^{m+1}-th power on both sides of it, we have

$$C'(Y,x,y) := Y^4 + \left(x^2+y^2\right)Y^2 + \left(yx^2 + x^2 + y + 1\right)Y + y^2x^2 + y^4 + yx^2 + x^2 + y^2 + y + 1 = 0,$$

and

$$C''(X,x,y) := (X+1)^4 C'(A(X,x,y),x,y) = D(X,x,y)E(X,x,y) = 0,$$

where

$$\begin{aligned}E(Y,x,y) := {} & X^8+(x+1)X^7+\left(x^2+x+y+1\right)X^6+(xy+x+y+1)X^5\\ & +\left(yx^2+x^2+xy+y^2+x+y+1\right)X^4+\left(x^3y+x^3+yx^2+x^2+xy+y\right)X^3\\ & +\left(x^6+x^4y+x^4+x^3y+y^2x^2+x^3+yx^2+xy+y^2+y\right)X^2\\ & +\left(x^7+x^6+x^5y+x^5+x^4y+x^4+x^3y+yx^2+xy+x+y+1\right)X\\ & +x^8+x^7+x^5y+x^4y^2+x^5+x^3y+y^2x^2+x^2+xy+y^2+x+1.\end{aligned}$$

Now, we have $D(X,x,y)=0$ or $E(X,x,y)=0$. If $D(X,x,y)=0$, we calculate the resultant of $C(X,x,y)$ and $D(X,x,y)$ in X,

$$Res(C(X,x,y),D(X,x,y),X)=(x+y+1)^4(x^2+y+1)^4=0,$$

which is a contradiction to $\mathrm{Tr}_n(x)=\mathrm{Tr}_n(y)=0$.

If $E(X,x,y)=0$, similarly, we have

$$Res(C(X,x,y),E(X,x,y),X)=(x+1)^8(x+y+1)^4(x^2+y+1)^4=0,$$

which is a contradiction, too.

Case 2: If $D(X,x,y)=0$, it also leads to a contradiction by a similar analysis to **Case 1**.

This completes the proof. ■

In the following, we present the proof of the open problem (2).

Theorem 5.4.4 *[72, Problem 1] Let $n=3m$ with m odd and $F(x)=x^{2^{2m+1}+1}+x^{2^{m+1}+1}+x^4+x^3$. Let $\mathcal{C}_F$ be the binary linear code defined as in (5.1). It is a $[2^n-1,2n]$ binary linear code with five weights $\{2^{n-1}-2^{\frac{n+2m-1}{2}},2^{n-1}+2^{\frac{n+2m-1}{2}},2^{n-1}-2^{\frac{n+m-2}{2}},2^{n-1}+2^{\frac{n+m-2}{2}},2^{n-1}\}$. Then the weight distribution of the linear code $\mathcal{C}_F$ is determined in Table 5.4.1.*

***Table 5.4.1**: The weight distribution of the code $\mathcal{C}_F$ in Theorem 5.4.4*

Weight	Frequency
0	1
$2^{n-1}\pm 2^{\frac{n+2m-1}{2}}$	$2^{m-1}(2^m-1)$
$2^{n-1}\pm 2^{\frac{n+m-2}{2}}$	$2^{n-m}(2^n-2^m)$
2^{n-1}	$2^{2n}-2^{n+2m}+2^n-2^{2m-1}+2^{m-1}-1$

Proof: For any $(a,b)\in\mathbb{F}_{2^n}^2$, we have

$$\begin{aligned}W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(ax+bF(x))}\\ &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(ax+bx^{2^{2m+1}+1}+bx^{2^{m+1}+1}+bx^4+bx^3)}.\end{aligned}$$

Let $\varphi_{a,b}(x) = \mathrm{Tr}_n(ax + bF(x))$. It is clear that $W_F(0,0) = 2^n$. Since F is quadratic, according to Lemma 2.4.2 and by a computation, we have

$$W_F(a,b) = \begin{cases} \pm 2^{\frac{n+d_b}{2}}, & \text{if } \varphi_{a,b}(x) = 0 \text{ for all } x \in \ker(L_b); \\ 0, & \text{otherwise,} \end{cases}$$

where d_b is the dimension of $\ker(L_b)$. From the proof of [72, Theorem 10], we have

$$\ker(L_b) = \begin{cases} \{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^n(y) = 0 \text{ or } \sqrt[3]{b^{-1}}\}, & \text{if } b \in \mathbb{F}_{2^m}^*; \\ \{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^n(y) = \mathrm{Tr}_m^n(by) = 0\}, & \text{if } b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}. \end{cases}$$

Case 1: $b \in \mathbb{F}_{2^m}^*$

If $\mathrm{Tr}_m^n(y) = 0$, then

$$\begin{aligned} \varphi_{a,b}(y) &= \mathrm{Tr}_n(ay + by^{2^{2m+1}+1} + by^{2^{m+1}+1} + by^4 + by^3) \\ &= \mathrm{Tr}_n(ay + b(y(\mathrm{Tr}_m^n(y))^2 + y^4)) \\ &= \mathrm{Tr}_n(ay + by^4)) \\ &= \mathrm{Tr}_n(ay) + \mathrm{Tr}_m(b(\mathrm{Tr}_m^n(y))^4) \\ &= \mathrm{Tr}_n(ay). \end{aligned}$$

Note that $\{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^n(y) = 0\} = \{x^{2^m} + x : x \in \mathbb{F}_{2^n}\}$. Then $\varphi_{a,b}(y) = \mathrm{Tr}_n(ay) = \mathrm{Tr}_n(a(x^{2^m} + x)) = \mathrm{Tr}_n((a + a^{2^m})x^{2^m}) = 0$ for all $x \in \mathbb{F}_{2^n}$ if and only if $a \in \mathbb{F}_{2^m}$.

If $\mathrm{Tr}_m^n(y) = \sqrt[3]{b^{-1}}$, then

$$\begin{aligned} \varphi_{a,b}(y) &= \mathrm{Tr}_n(ay + b(y(\mathrm{Tr}_m^n(y))^2 + y^4)) \\ &= \mathrm{Tr}_n(ay) + \mathrm{Tr}_m(b(\mathrm{Tr}_m^n(y))^3 + b(\mathrm{Tr}_m^n(y))^4) \\ &= \mathrm{Tr}_n(ay) + \mathrm{Tr}_m(1 + \mathrm{Tr}_m^n(y)) \\ &= \mathrm{Tr}_n((a+1)y) + 1. \end{aligned}$$

Note that $\{y \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^n(y) = \sqrt[3]{b^{-1}}\} = \{x^{2^m} + x + \alpha : x \in \mathbb{F}_{2^n}\}$, where $\mathrm{Tr}_m^n(\alpha) = \sqrt[3]{b^{-1}}$. Hence, we have

$$\begin{aligned} \varphi_{a,b}(y) &= \mathrm{Tr}_n((a+1)(x^{2^m} + x + \alpha)) + 1 \\ &= \mathrm{Tr}_n((a^{2^m} + a)x^{2^m} + (a+1)\alpha) + 1. \end{aligned}$$

Then $\varphi_{a,b}(y) = 0$, i.e., $\mathrm{Tr}_n((a^{2^m} + a)x^{2^m} + (a+1)\alpha) = 1$ if and only if $a \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_n((a+1)\alpha) = 1$. Since $\mathrm{Tr}_n((a+1)\alpha) = \mathrm{Tr}_m((a+1)\mathrm{Tr}_m^n(\alpha)) = \mathrm{Tr}_m((a+1)\sqrt[3]{b^{-1}})$, we have $\#\{a \in \mathbb{F}_{2^m} : \mathrm{Tr}_m((a+1)\sqrt[3]{b^{-1}}) = 1\} = 2^{m-1}$.

Therefore, the restriction of $\varphi_{a,b}(y) = \mathrm{Tr}_n(ay + bF(y))$ on $\ker(L_b)$ is the all-zero mapping if and only if $a \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_m((a+1)\sqrt[3]{b^{-1}}) = 1$. Thus,

$$W_F(a,b) = \begin{cases} \pm 2^{\frac{n+2m+1}{2}}, & \text{if } a \in \mathbb{F}_{2^m} \text{ and } \mathrm{Tr}_m((a+1)\sqrt[3]{b^{-1}}) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Hence, $|\{(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^* : \mathrm{Tr}_m((a+1)\sqrt[3]{b^{-1}}) = 1\}| = 2^{m-1}(2^m - 1)$.

Case 2: $b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$

It follows from the proof of [72, Theorem 10] that $\ker(L_b) = \{y \in \mathbb{F}_{2^n} | \mathrm{Tr}_m^n(y) = \mathrm{Tr}_m^n(by) = 0\} = \{(\beta + b)\eta : \eta \in \mathbb{F}_{2^m}\}$ with $\beta = \mathrm{Tr}_m^n(b)$. For $x \in \ker(L_b)$, $\varphi_{a,b}(y) = \mathrm{Tr}_n(ay + bF(y)) = \mathrm{Tr}_m((\mathrm{Tr}_m^n((b+a^4)(\beta+b)^4))\eta^4)$, where $\eta \in \mathbb{F}_{2^m}$.

Therefore, the restriction of $\varphi_{a,b}(y) = \mathrm{Tr}_n(ay + bF(y))$ on $\ker(L_b)$ is the all-zero mapping if and only if $\mathrm{Tr}_m^n((b+a^4)(b^{2^m}+b^{2^{2m}})^4) = 0$. Thus,

$$W_F(a,b) = \begin{cases} \pm 2^{\frac{n+m}{2}}, & \text{if } \mathrm{Tr}_m^n((b+a^4)(b^{2^m}+b^{2^{2m}})^4) = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Note that the number of the set $\{(a,b) \in \mathbb{F}_{2^n} \times (\mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}) : \mathrm{Tr}_m^n((b+a^4)(b^{2^m}+b^{2^{2m}})^4) = 0\}$ equals to $2^{n-m}(2^n - 2^m)$.

For the linear code $\mathcal{C}_F$, $W_F(a,b) = 2^n$ if and only if $(a,b) = (0,0)$. Then, the dimension of $K_1 = \{(a,b) \in \mathbb{F}_{2^n}^2 : W_F(a,b) = 2^n\}$ is 0 according to Eq. (5.2). Thus, the dimension of $\mathcal{C}_F$ is $2n$. Moreover, for any $a,b \in \mathbb{F}_{2^n}$, $W_F(a,b) \in \{0, 2^n, \pm 2^{\frac{n+2m+1}{2}}, \pm 2^{\frac{n+m}{2}}\}$. According to Eq. (5.3), the Hamming weights of the codewords $\boldsymbol{c}_{a,b}$ in $\mathcal{C}_F$ satisfy $\mathrm{wt}(\boldsymbol{c}_{a,b}) \in \{2^{n-1}, 0, 2^{n-1} \pm 2^{\frac{n+2m-1}{2}}, 2^{n-1} \pm 2^{\frac{n+m-2}{2}}\}$. Define $w_1 = 2^{n-1} - 2^{\frac{n+2m-1}{2}}, w_2 = 2^{n-1} + 2^{\frac{n+2m-1}{2}}, w_3 = 2^{n-1} - 2^{\frac{n+m-2}{2}}, w_4 = 2^{n-1} + 2^{\frac{n+m-2}{2}}, w_5 = 2^{n-1}$. We now determine the number A_{w_i} of codewords with weight w_i in $\mathcal{C}_F$. Based on the above discussion, we have $A_{w_1} + A_{w_2} = 2^{m-1}(2^m - 1)/2^{d_{K_1}} = 2^{m-1}(2^m - 1)$ and $A_{w_3} + A_{w_4} = 2^{n-m}(2^n - 2^m)/2^{d_{K_1}} = 2^{n-m}(2^n - 2^m)$. Hence, $A_{w_5} = 2^{2n} - 1 - (A_{w_1} + A_{w_2} + A_{w_3} + A_{w_4}) = 2^{2n} - 2^{2n-m} + 2^n - 2^{2m-1} + 2^{m-1} - 1$.

This completes the proof. ■

In the following, we give an example to illustrate Theorem 5.4.4. In addition, the computations are carried out using Magma software [2].

Example 5.4.5 *Let $m = 3$. The code $\mathcal{C}_F$ in Theorem 5.4.4 is a binary linear code with parameters $[511, 18, 128]$, and its weight enumerator is $1 + 21z^{128} + 18144z^{224} + 229859z^{256} + 14112z^{288} + 7z^{384}$.*

5.5 Conclusions

In this chapter, we constructed several classes of binary linear codes (and, more importantly, minimal codes) with flexible parameters from known 2-to-1 functions. Based on a very recent (2021) paper due to Li et al. [72], we succeeded (for the second time) in constructing several infinite families of codes with few weights (namely, 1-weight codes, 3-weight codes, and 5-weight codes) from 2-to-1 functions. It is worth emphasizing that we provided a new construction in this chapter, and based on this construction we also obtained several families of 2-weight codes, 8-weight codes, and 9-weight codes, which have different parameters from the existing literature. Meanwhile, we determined the weight distributions of these codes by using the Walsh transform of the corresponding two-to-one functions.

The advantages of the research results in this chapter are as follows:

(1) The binary linear codes constructed in this chapter are minimal linear codes in most cases. Based on their dual codes, these linear codes can be applied to the secret sharing schemes.

(2) The parameters of binary linear codes constructed are new (except Theorem 5.2.1(2)) and optimal. Notably, some of them are optimal with respect to the well-known Griesmer bound and optimal (or almost optimal) with respect to the online Database of Grassl.

(3) Two open problems from recent literature were solved. Specifically, in this chapter, Problem 2 in [72] was completely solved, and Problem 1 in [72] was partially solved.

Chapter 6

Two families of projective codes and their dual codes

In this chapter, we construct several families of projective binary linear codes with few nonzero weights by using two-to-one functions over $\mathbb{F}_{2^n}$ and determine their weight distributions. Ding et al. [33] proposed a general method to construct linear codes, that is, to construct linear codes by choosing suitable nonempty subsets over finite fields. The selection of the defining set directly affects the parameters of linear codes. This chapter construct projective binary linear codes of the form (1.6) and (1.8) having different restrictions on defining sets from two-to-one functions over $\mathbb{F}_{2^n}$. Using the exponential sum over finite fields as the research tool, we calculate the Walsh transform of the two-to-one function, and then completely determine the parameters and the weight distributions of the constructed linear codes. Finally, we study the minimum distance of the dual of the constructed codes and obtain that the duals are distance-optimal with respect to the sphere packing bound.

In Eqs. (1.6) and (1.8), we take $q = 2^n$ (n is a positive integer). Let $\mathcal{C}(F)_D$ and $\mathcal{C}_{D_F}$ denote the linear codes defined in Eqs. (1.8) and (1.6), respectively. Throughout this chapter, $\mathrm{Tr}_n(\cdot)$ denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and $\mathrm{Tr}_m^n(\cdot)$ denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, where $m \mid n$ and m is a positive integer.

6.1 The first family of projective codes

In this section, we introduce the binary linear codes $\mathcal{C}(F)_D$ from known two-to-one functions over and determine their weight distributions.

Let $F(x)$ be a 2-to-1 function over $\mathbb{F}_{2^n}$ with $F(0) = 0$. Let

$$D = \{x \in \mathbb{F}_{2^n}^* : \mathrm{Tr}_n(x) = v\}, \tag{6.1}$$

where $v \in \{0,1\}$. It is easy to know that $|D| = 2^{n-1} - 1 + v$. From the code $\mathcal{C}(F)_D$ defined in (1.8), we know that the length and dimension of $\mathcal{C}(F)_D$ is $2^{n-1} - 1 + v$ and at most $2n$, respectively.

Note that the dimension of the code $\mathcal{C}(F)_D$ is $2n - d_{V_1}$, where d_{V_1} is the dimension

of the $\mathbb{F}_2$-vector space

$$V_1 = \left\{ (a,b) \in \mathbb{F}_{2^n}^2 : \sum_{x \in D} (-1)^{\mathrm{Tr}_n(ax+bF(x))} = |D| \right\}.$$

We have

$$\begin{aligned}
\sum_{x \in D} (-1)^{\mathrm{Tr}_n(ax+bF(x))} &= \sum_{\substack{x \in \mathbb{F}_{2^n}^*, \\ \mathrm{Tr}_n(x)=v}} (-1)^{\mathrm{Tr}_n(ax+bF(x))} \\
&= \frac{1}{2} \sum_{z \in \mathbb{F}_2} \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{z(\mathrm{Tr}_n(x)-v)+\mathrm{Tr}_n(ax+bF(x))} \\
&= \frac{1}{2} \left(\sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_n(ax+bF(x))} + (-1)^v \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_n((1+a)x+bF(x))} \right) \\
&= \frac{1}{2}(W_F(a,b) + (-1)^v W_F(1+a,b)) - \frac{1+(-1)^v}{2}.
\end{aligned}$$

Thus,

$$V_1 = \left\{ (a,b) \in \mathbb{F}_{2^n}^2 : W_F(a,b) + (-1)^v W_F(1+a,b) = 2|D| + 1 + (-1)^v \right\}. \quad (6.2)$$

The Hamming weight of a codeword $\boldsymbol{c}_{a,b}$ in $\mathcal{C}(F)_D$ is

$$\begin{aligned}
wt(\boldsymbol{c}_{a,b}) &= |\{x \in D : \mathrm{Tr}_n(ax+bF(x)) = 1\}| \\
&= |D| - |\{x \in D : \mathrm{Tr}_n(ax+bF(x)) = 0\}| \\
&= \frac{1}{2} \left(|D| - \sum_{x \in D} (-1)^{\mathrm{Tr}_n(ax+bF(x))} \right) \\
&= \frac{|D|}{2} + \frac{1+(-1)^v}{4} - \frac{1}{4}(W_F(a,b) + (-1)^v W_F(1+a,b)). \quad (6.3)
\end{aligned}$$

For the linear code $\mathcal{C}(F)_D$, we present the main conclusions. We shall distinguish different cases depending on the value of n. The constraints come from the two-to-one property.

6.1.1 The case $n = 2m$

The following projective binary linear codes are derived from the two-to-one function given in Lemma 2.4.3.

Theorem 6.1.1 *Let $n = 2m$ and $F(x) = x^{2^{m+1}+4} + x^{2^{m+2}+2} + \alpha x \in \mathbb{F}_{2^n}[x]$, where m is odd, $\alpha^{2^m-1} = w$ and $w \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Let D be defined in (6.1). Then the following statements hold.*

(a) If $v = 0$, then $\mathcal{C}(F)_D$ is a five-weight binary code with parameters $[2^{n-1}-1, 3m-1, 2^{n-2}-2^m]$, and its weight distribution is given by Table 6.1.1.

***Table 6.1.1**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.1(a)*

Weight	Frequency
0	1
$2^{n-2}+2^m$	$2^{3m-5}-2^{2m-4}$
$2^{n-2}+2^{m-1}$	2^{3m-3}
2^{n-2}	$11\cdot 2^{3m-5}+2^{2m-4}-1$

***Table 6.1.2**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.1(b)*

Weight	Frequency
0	1
$2^{n-2}+2^m$	$2^{3m-4}-2^{2m-3}$
$2^{n-2}+2^{m-1}$	2^{3m-2}
2^{n-2}	$11\cdot 2^{3m-4}+2^{2m-3}-2$
2^{n-1}	1

(b) If $v=1$, then $\mathcal{C}(F)_D$ is a six-weight binary code with parameters $[2^{n-1},3m,2^{n-2}-2^m]$, and its weight distribution is given by Table 6.1.2.

Proof: In order to determine the weights of $\mathcal{C}(F)_D$, we first compute the Walsh transforms $W_F(a,b)$ and $W_F(1+a,b)$ for any $a,b\in\mathbb{F}_{2^n}$. From Theorem 5.2.1, we have

$$W_F(a,b)=\begin{cases}2^n, & \text{if } b\in\mathbb{F}_{2^m} \text{ and } a+b\alpha=0;\\ \pm 2^{m+1}, & \text{if } b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}, \mathrm{Tr}_n((a+b\alpha)y_0)=0 \text{ and } \mathrm{Tr}_n((a+b\alpha)y_0w)=1;\\ 0, & \text{otherwise,}\end{cases}$$

and

$$W_F(1+a,b)=\begin{cases}2^n, & \text{if } b\in\mathbb{F}_{2^m} \text{ and } 1+a+b\alpha=0;\\ \pm 2^{m+1}, & \text{if } b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}, \mathrm{Tr}_n((1+a+b\alpha)y_0)=0 \text{ and}\\ & \mathrm{Tr}_n((1+a+b\alpha)y_0w)=1;\\ 0, & \text{otherwise,}\end{cases}$$

where $y_0^3=\frac{1}{\sqrt{b+b^{2^m}}}\in\mathbb{F}_{2^m}^*$. It is not difficult to check that $\mathrm{Tr}_n(y_0)=0$ and $\mathrm{Tr}_n(y_0w)=\mathrm{Tr}_m(y_0)$. Hence, we have

$$W_F(a,b)+(-1)^vW_F(1+a,b)=\begin{cases}2^n, & \text{if } b\in\mathbb{F}_{2^m} \text{ and } a+b\alpha=0;\\ (-1)^v2^n, & \text{if } b\in\mathbb{F}_{2^m} \text{ and } 1+a+b\alpha=0;\\ 0 \text{ or } \pm 2^{m+2}, & \text{if } b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}, \mathrm{Tr}_n((a+b\alpha)y_0)=0,\\ & \mathrm{Tr}_n((a+b\alpha)y_0w)=1 \text{ and } \mathrm{Tr}_m(y_0)=0;\\ \pm 2^{m+1}, & \text{if } b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}, \mathrm{Tr}_n((a+b\alpha)y_0)=0\\ & \text{and } \mathrm{Tr}_m(y_0)=1;\\ 0, & \text{otherwise.}\end{cases}$$

(a) If $v=0$, it follows from Eq. (6.2) that $W_F(a,b)+W_F(1+a,b)=2(|D|+1)=2^n$ if and only if $b\in\mathbb{F}_{2^m}$ and $a+b\alpha=0$ or $b\in\mathbb{F}_{2^m}$ and $1+a+b\alpha=0$. Hence, the dimension of $\mathcal{C}(F)_D$ is $2n-(m+1)$.

It follows from Eq. (6.3) that the weight $\mathrm{wt}(\boldsymbol{c}_{a,b})$ of the codeword $\boldsymbol{c}_{a,b}$ in $\mathcal{C}(F)_D$ satisfies

$$\begin{aligned}\mathrm{wt}(\boldsymbol{c}_{a,b}) &= 2^{n-2}-\frac{1}{4}(W_F(a,b)+W_F(1+a,b))\\ &\in \{0,2^{n-2},2^{n-2}\pm 2^m,2^{n-2}\pm 2^{m-1}\}.\end{aligned}$$

It will be proved that the minimum weight of the dual code $\mathcal{C}(F)_D^{\perp}$ is at least 3 (see Theorem 6.3.1). Define $w_1=2^{n-2}-2^m, w_2=2^{n-2}-2^{m-1}, w_3=2^{n-2}, w_4=2^{n-2}+2^{m-1}, w_5=2^{n-2}+2^m$. We now determine the number A_{w_i} of codewords with weight w_i in $\mathcal{C}(F)_D$. Note that $|\{(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}: W_F(a,b)+W_F(1+a,b)=\pm 2^{m+1}\}|=|\{(a,b)\in\mathbb{F}_{2^n}\times(\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}): \mathrm{Tr}_n((a+b\alpha)y_0)=0, \text{ and } \mathrm{Tr}_m(y_0)=1\}|=2^{m-1}\cdot 2^m\cdot 2^{n-1}=2^{4m-2}$. Thus $A_{w_2}+A_{w_4}=2^{4m-2}/2^{d_{V_1}}=2^{4m-2}/2^{m+1}=2^{3m-3}$. The first three Pless power moments in (2.4) lead to the following system of equations:

$$\begin{cases}\sum_{i=1}^{5}A_{w_i}=2^{3m-1}-1;\\ \sum_{i=1}^{5}w_iA_{w_i}=2^{3m-2}(2^{n-1}-1);\\ \sum_{i=1}^{5}w_i^2A_{w_i}=2^{3m-3}(2^{n-1}-1)2^{n-1};\\ A_{w_2}+A_{w_4}=2^{3m-3}.\end{cases}\tag{6.4}$$

Solving the system of equations in (6.4) yields the weight distribution of Table 6.1.1.

(b) If $v=1$, then $W_F(a,b)-W_F(1+a,b)\in\{0,\pm 2^n,\pm 2^{m+1},\pm 2^{m+2}\}$. It follows from Eq. (6.2) that $W_F(a,b)-W_F(1+a,b)=2|D|=2^n$ if and only if $b\in\mathbb{F}_{2^m}$ and $a+b\alpha=0$. Hence, the dimension of $\mathcal{C}(F)_D$ is $2n-m$. It follows from Eq. (6.3), the weight $wt(\boldsymbol{c}_{a,b})$ of the codeword $\boldsymbol{c}_{a,b}$ in $\mathcal{C}(F)_D$ satisfies $\mathrm{wt}(\boldsymbol{c}_{a,b})\in\{0,2^{n-2},2^{n-1},2^{n-2}\pm 2^m,2^{n-2}\pm 2^{m-1}\}$. It will be proved that the minimum weight of the dual code $\mathcal{C}(F)_D^{\perp}$ is 4 (see Theorem 6.3.1). Define $w_1=2^{n-2}-2^m, w_2=2^{n-2}-2^{m-1}, w_3=2^{n-2}, w_4=2^{n-2}+2^{m-1}, w_5=2^{n-2}+2^m, w_6=2^{n-1}$. We now determine the number A_{w_i} of codewords with weight w_i in $\mathcal{C}(F)_D$. Note that $A_2+A_4=2^{4m-2}/2^{d_{V_1}}=2^{4m-2}/2^m=2^{3m-2}$ and $A_{w_6}=2^m/2^{d_{V_1}}=1$. The first four Pless power moments in (2.4) lead to the following system of equations:

$$\begin{cases}\sum_{i=1}^{6}A_{w_i}=2^{3m}-1;\\ \sum_{i=1}^{6}w_iA_{w_i}=2^{3m-1}\cdot 2^{n-1};\\ \sum_{i=1}^{6}w_i^2A_{w_i}=2^{3m-2}\cdot 2^{n-1}(2^{n-1}+1);\\ \sum_{i=1}^{6}w_i^3A_{w_i}=2^{3m-3}\cdot 2^{2n-2}(2^{n-1}+3);\\ A_{w_2}+A_{w_4}=2^{3m-3};\\ A_{w_6}=1.\end{cases}\tag{6.5}$$

Solving the system of equations in (6.5) yields the weight distribution of Table 6.1.2.

This completes the proof. ■

Next, we present a concrete example in Theorem 6.1.1. In addition, the computations are carried out using Magma software [2].

Example 6.1.2 *Let $m = 3$ in Theorem 6.1.1. If $v = 0$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[31, 8, 8]$ and weight enumerator $1 + 9z^8 + 40z^{12} + 179z^{16} + 24z^{20} + 3z^{24}$. If $v = 1$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[32, 9, 8]$ and weight enumerator $1 + 12z^8 + 64z^{12} + 358z^{16} + 64z^{20} + 12z^{24} + z^{32}$.*

6.1.2 The case $n = 2m + 1$

By utilizing the 2-to-1 function in Lemma 2.4.10, this subsection presents a class of 5-weight binary linear codes and a class of 6-weight binary linear codes.

Theorem 6.1.3 *Let $n = 2m+1$ and $F(x) = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + x \in \mathbb{F}_{2^n}[x]$. Let D be defined in (6.1). Then the following statements hold.*

(a) If $v = 0$, then $\mathcal{C}(F)_D$ is a five-weight binary code with parameters $[2^{n-1} - 1, 2n - 1, 2^{n-2} - 2^m]$, and its weight distribution is given by Table 6.1.3.

(b) If $v = 1$, then $\mathcal{C}(F)_D$ is a six-weight binary code with parameters $[2^{n-1}, 2n, 2^{n-2} - 2^m]$, and its weight distribution is given by Table 6.1.4.

***Table 6.1.3**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.3(a)*

Weight	Frequency
0	1
$2^{n-2} - 2^m$	$2^{4m-3} - 2^{2m-3} + 2^{3m-2} - 2^{m-2}$
$2^{n-2} - 2^{m-1}$	$2^{4m-1} + 2^{3m-1}$
2^{n-2}	$3 \cdot 2^{4m-2} + 2^{2m-2} - 1$
$2^{n-2} + 2^{m-1}$	$2^{4m-1} - 2^{3m-1}$
$2^{n-2} + 2^m$	$2^{4m-3} - 2^{3m-2} - 2^{2m-3} + 2^{m-2}$

***Table 6.1.4**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.3(b)*

Weight	Frequency
0	1
$2^{n-2} - 2^m$	$2^{4m-2} - 2^{2m-2}$
$2^{n-2} - 2^{m-1}$	2^{4m}
2^{n-2}	$3 \cdot 2^{4m-1} + 2^{2m-1} - 2$
$2^{n-2} + 2^{m-1}$	2^{4m}
$2^{n-2} + 2^m$	$2^{4m-2} - 2^{2m-2}$
2^{n-1}	1

Proof: We first determine the values of the Walsh transforms $W_F(a, b)$ and $W_F(1 + a, b)$.

For any $a,b \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax+bx^{2^{m+1}+2}+bx^{2^{m+1}}+bx^2+bx)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(b^{2^m}x^{2^{m+1}+1}+bx^2+(a+b+b^{2^m})x)}. \end{aligned}$$

- If $b=0$, then
$$W_F(a,b) = \begin{cases} 2^n, & \text{if } a=0; \\ 0, & \text{if } a\neq 0. \end{cases}$$

- If $b\neq 0$, we let $\varphi_{a,b}(x) = \mathrm{Tr}_n(b^{2^m}x^{2^{m+1}+1}+bx^2+(a+b+b^{2^m})x)$. Then the bilinear form of $\varphi_{a,b}(x)$ is given by
$$\begin{aligned} B_{\varphi_{a,b}}(x,y) &= \varphi_{a,b}(x)+\varphi_{a,b}(y)+\varphi_{a,b}(x+y) \\ &= \mathrm{Tr}_n(b^{2^m}(x^{2^{m+1}}y+xy^{2^{m+1}})) \\ &= \mathrm{Tr}_n((b^{2^m}y+by^2)x^{2^{m+1}}) \\ &= \mathrm{Tr}_n(L_b(y)x^{2^{m+1}}), \end{aligned}$$
where $L_b(y) = b^{2^m}y+by^2$. Let $\ker(L_b) = \{y\in\mathbb{F}_{2^n} : L_b(y)=0\}$. It is easy to know that $\ker(L_b) = \{0, b^{2^m-1}\}$. For $x = b^{2^m-1}, \mathrm{Tr}_n(ax+bF(x)) = \mathrm{Tr}_n(1+ab^{2^m-1}+b^{2^m}) = 0$ if and only if $\mathrm{Tr}_n(ab^{2^m-1}+b)=1$ since n is odd. According to Lemma 2.4.2, we have
$$W_F(a,b) = \begin{cases} \pm 2^{m+1}, & \text{if } \mathrm{Tr}_n(ab^{2^m-1}+b)=1; \\ 0, & \text{otherwise.} \end{cases}$$

In a similar way, we have

$$W_F(1+a,b) = \begin{cases} 2^n, & \text{if } a=1 \text{ and } b=0; \\ \pm 2^{m+1}, & \text{if } \mathrm{Tr}_n(ab^{2^m-1}+b+b^{2^m-1})=1 \text{ and } b\neq 0; \\ 0, & \text{oterwise.} \end{cases}$$

Therefore, by the above discussion and a simple calculation, we have $W_F(a,b) + (-1)^v W_F(1+a,b) =$

$$\begin{cases} 2^n, & \text{if } a=0, b=0; \\ (-1)^v 2^n, & \text{if } a=1, b=0; \\ 0 \text{ or } \pm 2^{m+2}, & \text{if } \mathrm{Tr}_n(ab^{2^m-1}+b)=1, \mathrm{Tr}_n(b^{2^m-1})=0 \text{ and } b\neq 0; \\ \pm 2^{m+1}, & \text{if } \mathrm{Tr}_n(ab^{2^m-1}+b)=1, \mathrm{Tr}_n(b^{2^m-1})\neq 0 \text{ and } b\neq 0 \\ & (\text{or } \mathrm{Tr}_n(ab^{2^m-1}+b)\neq 1, \mathrm{Tr}_n(b^{2^m-1})\neq 0 \text{ and } b\neq 0); \\ 0, & \text{otherwise.} \end{cases}$$

(a) If $v=0$, it follows from Eq. (6.2) that $W_F(a,b)+W_F(1+a,b) = 2(|D|+1) = 2^n$ if and only if $a=0, b=0$ or $a=1, b=0$. Hence, the dimension of $\mathcal{C}(F)_D$ is $2n-1$.

It follows from Eq. (6.3) that the weight $\mathrm{wt}(\boldsymbol{c}_{a,b})$ of the codeword $\boldsymbol{c}_{a,b}$ in $\mathcal{C}(F)_D$ satisfies

$$\mathrm{wt}(\boldsymbol{c}_{a,b}) \;=\; 2^{n-2}-\frac{1}{4}(W_F(a,b)+W_F(1+a,b)) \in \{0,2^{n-2},2^{n-2}\pm 2^m,2^{n-2}\pm 2^{m-1}\}.$$

Define $w_1=2^{n-2}, w_2=2^{n-2}-2^{m-1}, w_3=2^{n-2}+2^{m-1}, w_4=2^{n-2}-2^m, w_5=2^{n-2}+2^m$. Therefore, from Theorem 6.3.1 and the first five Pless power moments in (2.4),

$$\begin{cases} \sum\limits_{i=1}^{5} A_{w_i} = 2^{2n-1}-1; \\ \sum\limits_{i=1}^{5} w_i A_{w_i} = 2^{2n-2}(2^{n-1}-1); \\ \sum\limits_{i=1}^{5} w_i^2 A_{w_i} = 2^{2n-3}(2^{n-1}-1)2^{n-1}; \\ \sum\limits_{i=1}^{5} w_i^3 A_{w_i} = 2^{2n-4}(2^{n-1}-1)^2(2^{n-1}+2); \\ \sum\limits_{i=1}^{5} w_i^4 A_{w_i} = 2^{3n-6}(2^{n-1}-1)((2^{n-1}-1)^2+5\cdot 2^{n-1}-7), \end{cases}$$

we get the weight distribution in Table 6.1.3.

(b) If $v=1$, then $W_F(a,b)-W_F(1+a,b) \in \{0,\pm 2^n,\pm 2^{m+1},\pm 2^{m+2}\}$. It follows from Eq. (6.2) that $W_F(a,b)-W_F(1+a,b)=2|D|=2^n$ if and only if $a=0,b=0$. Hence, the dimension of $\mathcal{C}(F)_D$ is $2n$. It follows from Eq. (6.3), the weight $\mathrm{wt}(\boldsymbol{c}_{a,b})$ of the codeword $\boldsymbol{c}_{a,b}$ in $\mathcal{C}(F)_D$ satisfies $\mathrm{wt}(\boldsymbol{c}_{a,b}) \in \{0,2^{n-2},2^{n-1},2^{n-2}\pm 2^m,2^{n-2}\pm 2^{m-1}\}$. Define $w_1=2^{n-2}, w_2=2^{n-1}, w_3=2^{n-2}-2^{m-1}, w_4=2^{n-2}+2^{m-1}, w_5=2^{n-2}-2^m, w_6=2^{n-2}+2^m$. Therefore, from Theorem 6.3.1 and the first five Pless power moments in (2.4),

$$\begin{cases} \sum\limits_{i=1}^{6} A_{w_i} = 2^{2n}-1; \\ \sum\limits_{i=1}^{6} w_i A_{w_i} = 2^{2n-1}\cdot 2^{n-1}; \\ \sum\limits_{i=1}^{6} w_i^2 A_{w_i} = 2^{2n-2}\cdot 2^{n-1}(2^{n-1}+1); \\ \sum\limits_{i=1}^{6} w_i^3 A_{w_i} = 2^{2n-3}(2^{n-1})^2(2^{n-1}+3); \\ \sum\limits_{i=1}^{6} w_i^4 A_{w_i} = 2^{3n-5}(2^{n-1}+1)(2^{2n-2}+5\cdot 2^{n-1}-2); \\ A_{w_2}=1, \end{cases}$$

This completes the proof of Theorem 6.1.3. ■

Remark 6.1.4 *Comparing with some related references, we found that the binary linear codes in Theorem 6.1.3 have the same parameters as that of [115, Theorem 3] and [116, Corollary 12], but their weight distributions are different from that of the codes in [115, Theorem 3], and [116, Corollary 12].*

In the following, we give some examples to illustrate Theorem 6.1.3, and the computations are carried out using Magma software [2].

Example 6.1.5 *Let $m = 2$ in Theorem 6.1.3. If $v = 0$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[15,9,4]$ and weight enumerator $1+45z^4+160z^6+195z^8+96z^{10}+15z^{12}$. If $v = 1$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[16,10,4]$ and weight enumerator $1+60z^4+256z^6+390z^8+256z^{10}+60z^{12}+z^{16}$. These codes are optimal by the online Database [44].*

Example 6.1.6 *Let $m = 3$ in Theorem 6.1.3. If $v = 0$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[63,13,24]$ and weight enumerator $1+630z^{24}+2304z^{28}+3087z^{32}+1792z^{36}+378z^{40}$. If $v = 1$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[64,14,24]$ and weight enumerator $1+1008z^{24}+4096z^{28}+6174z^{32}+4096z^{36}+1008z^{40}+z^{64}$. These codes are optimal by the online Database [44].*

6.1.3 The case $n = 3m$

In this subsection, we consider binary linear codes from the 2-to-1 functions in Lemma 2.4.11, and then we obtain two families of 3-weight projective binary linear codes and two families of 4-weight projective binary linear codes.

Theorem 6.1.7 *Let $n = 3m$ and $F(x) = x^{2^{2m}+2^m}+x^{2^{2m}+1}+x^{2^m+1}+x \in \mathbb{F}_{2^n}[x]$. Let D be defined in (6.1).*

(a) If $v = 0$, then $\mathcal{C}(F)_D$ is a three-weight binary code with parameters $[2^{n-1}-1, n+m-1, 2^{n-2}-2^{2m-2}]$, and its weight distribution is given by Table 6.1.5.

(b) If $v = 1$, then $\mathcal{C}(F)_D$ is a four-weight binary code with parameters $[2^{n-1}, n+m, 2^{n-2}-2^{2m-2}]$, and its weight distribution is given by Table 6.1.6.

***Table 6.1.5**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.7(a)*

Weight	Frequency
0	1
$2^{n-2}-2^{2m-2}$	$2^{n-1}-2^{m-1}$
2^{n-2}	$2^{n+m-1}-2^n+2^{2m}-1$
$2^{n-2}+2^{2m-2}$	$2^{n-1}+2^{m-1}-2^{2m}$

Proof: To prove this theorem, we can proceed similarly as for Theorem 6.1.1. The proof is therefore omitted. ■

Next, we give some concrete examples in Theorem 6.1.7. In addition, the computations are carried out using Magma software [2].

Example 6.1.8 *Let $m = 2$ in Theorem 6.1.7. If $v = 0$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[31,7,12]$ and weight enumerator $1+30z^{12}+79z^{16}+18z^{20}$. If $v = 1$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[32,8,12]$ and weight enumerator $1+48z^{12}+158z^{16}+80z^{20}+z^{32}$. These codes are almost optimal. For example, the optimal one has parameters $[31,7,13]$ by the online Database [44].*

***Table 6.1.6**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.7(b)*

Weight	Frequency
0	1
$2^{n-2}-2^{2m-2}$	2^n-2^{2m}
2^{n-2}	$2^{n+m}-2^{n+1}+2^{2m+1}-2$
$2^{n-2}+2^{2m-2}$	2^n+2^{2m}
2^{n-1}	1

Example 6.1.9 *Let $m=3$ in Theorem 6.1.7. If $v=0$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[255,11,112]$ and weight enumerator $1+252z^{112}+1599z^{128}+196z^{144}$. If $v=1$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[256,12,112]$ and weight enumerator $1+448z^{112}+3198z^{128}+448z^{144}+z^{256}$.*

The following result is obtained by proceeding similarly to Theorem 6.1.1.

Theorem 6.1.10 *Let $n=3m$ $(m \not\equiv 1 \pmod 3)$ and $F(x)=x^{2^{2m}+1}+x^{2^{m+1}}+x^{2^m+1}+x \in \mathbb{F}_{2^n}[x]$. Let D be defined in (6.1).*

(a) If $v=0$, then $\mathcal{C}(F)_D$ is a three-weight binary code with parameters $[2^{n-1}-1, 2n-m-1, 2^{n-2}-2^{2m-1}]$, and its weight distribution is given by Table 6.1.7.

(b) If $v=1$, then $\mathcal{C}(F)_D$ is a four-weight binary code with parameters $[2^{n-1}, 2n-m, 2^{n-2}-2^{2m-1}]$, and its weight distribution is given by Table 6.1.8.

***Table 6.1.7**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.10(a)*

Weight	Frequency
0	1
$2^{n-2}-2^{2m-1}$	$2^{4m-3}-2^{2m-3}+2^{3m-2}-2^{m-2}$
2^{n-2}	$2^{5m-1}-2^{4m-2}+2^{2m-2}-1$
$2^{n-2}+2^{2m-1}$	$2^{4m-3}-2^{2m-3}-2^{3m-2}+2^{m-2}$

***Table 6.1.8**: The weight distribution of the code $\mathcal{C}(F)_D$ in Theorem 6.1.10(b)*

Weight	Frequency
0	1
$2^{n-2}-2^{2m-1}$	$2^{4m-2}-2^{2m-2}$
2^{n-2}	$2^{5m}-2^{4m-1}+2^{2m-1}-2$
$2^{n-2}+2^{2m-1}$	$2^{4m-2}-2^{2m-2}$
2^{n-1}	1

Remark 6.1.11 *Comparing with some related references, we found that the binary linear code in Theorem 6.1.10(b) has the same parameters as that of [116, Theorem 18], but our linear code $\mathcal{C}(F)_D$ is obtained by considering a different function.*

In the following, we give some examples in Theorem 6.1.10, and the computations are carried out using Magma software [2].

Example 6.1.12 *Let $m = 2$ in Theorem 6.1.10. If $v = 0$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[31,9,8]$ and weight enumerator $1+45z^8+451z^{16}+15z^{24}$. If $v = 1$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[32,10,8]$ and weight enumerator $1+60z^8+902z^{16}+60z^{24}+z^{32}$.*

Example 6.1.13 *Let $m = 3$ in Theorem 6.1.10. If $v = 0$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[255,14,96]$ and weight enumerator $1+630z^{96}+15375z^{128}+378z^{160}$. If $v = 1$, then the binary linear code $\mathcal{C}(F)_D$ has parameters $[256,15,96]$ and weight enumerator $1+1008z^{96}+30750z^{128}+1008z^{160}+z^{256}$.*

6.2 The second family of projective codes

In this section, we introduce the binary linear codes $\mathcal{C}_{D_F}$ from known two-to-one functions over $\mathbb{F}_{2^n}$ and determine their weight distributions.

Let $F(x)$ be a 2-to-1 function over $\mathbb{F}_{2^n}$ with $F(0) = 0$. Define

$$D_F = \{F(x) : \mathrm{Tr}_n(F(x)) = v, x \in \mathbb{F}_{2^n}\}\backslash\{0\} = \{d_1, d_2, \ldots, d_l\}. \tag{6.6}$$

From the code $\mathcal{C}_{D_F}$ defined in (1.6), it is evident that the length and dimension of $\mathcal{C}_{D_F}$ is $l = |D_F|$ and at most n, respectively. Set $n_0 = |\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_n(F(x)) = v\}|$. Since $F(x)$ is a 2-to-1 function over $\mathbb{F}_{2^n}$ with $F(0) = 0$, we have $l = |D_F| = \frac{1}{2}n_0 - 1 + v$. Note that

$$\begin{aligned} n_0 &= \frac{1}{2}\sum_{z\in\mathbb{F}_2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{z(\mathrm{Tr}_n(F(x))-v)} \\ &= 2^{n-1} + \frac{(-1)^v}{2}W_F(0,1). \end{aligned} \tag{6.7}$$

We know that the dimension of the code $\mathcal{C}_{D_F}$ is $n - d_{V_2}$, where d_{V_2} is the dimension of the $\mathbb{F}_2$-vector space

$$V_2 = \left\{ a \in \mathbb{F}_{2^n} : \sum_{d\in D_F}(-1)^{\mathrm{Tr}_n(ad)} = l \right\}.$$

Note that

$$\begin{aligned} \sum_{d\in D_F}(-1)^{\mathrm{Tr}_n(ad)} &= \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_{2^n},\\ \mathrm{Tr}_n(F(x))=v}}(-1)^{\mathrm{Tr}_n(aF(x))} - 1 + v \\ &= \frac{1}{4}\sum_{z\in\mathbb{F}_2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{z(\mathrm{Tr}_n(F(x))-v)+\mathrm{Tr}_n(aF(x))} - 1 + v \\ &= \frac{1}{4}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(aF(x))} + (-1)^v\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n((1+a)F(x))}\right) - 1 + v \\ &= \frac{1}{4}(W_F(0,a) + (-1)^v W_F(0,1+a)) - 1 + v. \end{aligned}$$

Hence,

$$V_2 = \{a \in \mathbb{F}_{2^n} : W_F(0,a) + (-1)^v W_F(0,1+a) = 4(l+1-v)\}. \quad (6.8)$$

The Hamming weight of a codeword $\boldsymbol{c}_a$ in $\mathcal{C}_{D_F}$ is

$$\begin{aligned} \mathrm{wt}(\boldsymbol{c}_a) &= |\{1 \le i \le l : \mathrm{Tr}_n(ad_i) = 1\}| \\ &= l - |\{1 \le i \le l : \mathrm{Tr}_n(ad_i) = 0\}| \\ &= \frac{1}{2}\left(l - \sum_{d \in D_F} (-1)^{\mathrm{Tr}_n(ad)}\right). \end{aligned} \quad (6.9)$$

According to the definition (1.6) of the linear code $\mathcal{C}_{D_F}$, we present several families of projective binary linear codes with few weights in the following sequel. We shall distinguish different cases depending on the value of n. The constraints come from the two-to-one property. Before that, let us recall a result about the exponential sum $S_h(a,b)$, which will help calculate the weight distribution of the constructed codes.

For any a and b in $\mathbb{F}_{2^n}$, we define the following exponential sum

$$S_h(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax^{2^h+1}+bx)}.$$

Lemma 6.2.1 *[25, Theorem 4.6] Let $t = \gcd(h,n)$ and n/t be odd. Then*

$$S_h(1,1) = \left(\frac{2}{n/t}\right)^t 2^{\frac{n+t}{2}},$$

where $(\cdot)$ is the Jacobi symbol.

6.2.1 The case $n = 2m+1$

Next, we present projective binary linear codes with 2-weight and 3-weight from the 2-to-1 function in Lemma 2.4.10.

Theorem 6.2.2 *Let $n = 2m+1$ and $F(x) = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + x \in \mathbb{F}_{2^n}[x]$. Let D_F be defined in (6.6).*

(a) If $v = 0$, then $\mathcal{C}_{D_F}$ is a two-weight binary code with parameters $[2^{n-2} + \left(\frac{2}{n}\right) 2^{m-1} - 1, n-1, 2^{n-3} + (\left(\frac{2}{n}\right) - 1)2^{m-2}]$, and its weight distribution is given by Table 6.2.1, where $\left(\frac{2}{n}\right)$ denotes the Jacobi symbol.

(b) If $v = 1$, then $\mathcal{C}_{D_F}$ is a three-weight binary code with parameters $[2^{n-2} - \left(\frac{2}{n}\right) 2^{m-1}, n, 2^{n-3} - (\left(\frac{2}{n}\right) + 1)2^{m-2}]$, and its weight distribution is given by Table 6.2.2, where $\left(\frac{2}{n}\right)$ denotes the Jacobi symbol.

***Table 6.2.1**: The weight distribution of the code $\mathcal{C}_{D_F}$ in Theorem 6.2.2(a)*

Weight	Frequency
0	1
$2^{n-3}+(\left(\frac{2}{n}\right)-1)2^{m-2}$	$2^{2m-1}+2^{m-1}-\frac{1}{2}(\left(\frac{2}{n}\right)+1)$
$2^{n-3}+(\left(\frac{2}{n}\right)+1)2^{m-2}$	$2^{2m-1}-2^{m-1}+\frac{1}{2}(\left(\frac{2}{n}\right)-1)$

***Table 6.2.2**: The weight distribution of the code $\mathcal{C}_{D_F}$ in Theorem 6.2.2(b)*

Weight	Frequency
0	1
$2^{n-3}-(\left(\frac{2}{n}\right)+1)2^{m-2}$	$2^{2m}-1$
$2^{n-3}-(\left(\frac{2}{n}\right)-1)2^{m-2}$	$2^{2m}-1$
$2^{n-2}-\left(\frac{2}{n}\right)2^{m-1}$	1

Proof: From Eq. (6.7) and Lemma 6.2.1,

$$\begin{aligned}
n_0 &= 2^{n-1}+\frac{(-1)^v}{2}W_F(0,1)\\
&= 2^{n-1}+\frac{(-1)^v}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(F(x))}\\
&= 2^{n-1}+\frac{(-1)^v}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(x^{2^{m+1}+2}+x^{2^{m+1}}+x^2+x)}\\
&= 2^{n-1}+\frac{(-1)^v}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(x^{2^m+1}+x)}\\
&= 2^{n-1}+\frac{(-1)^v}{2}S_m(1,1)\\
&= 2^{n-1}+(-1)^v\left(\frac{2}{n}\right)2^m,
\end{aligned}$$

where $\left(\frac{2}{n}\right)$ is the Jacobi symbol (see Definition 2.3.2). Then, the length l of the code $\mathcal{C}_{D_F}$ is $l=|D_F|=\frac{1}{2}n_0-1+v=2^{n-2}+(-1)^v\left(\frac{2}{n}\right)2^{m-1}-1+v$. For any $a\in\mathbb{F}_{2^n}$, we have

$$\begin{aligned}
W_F(0,a) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(aF(x))}\\
&= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(ax^{2^{m+1}+2}+ax^{2^{m+1}}+ax^2+ax)}\\
&= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_n(a^{2^m}x^{2^{m+1}+1}+ax^2+(a+a^{2^m})x)}.
\end{aligned}$$

- If $a=0$, it is obvious that $W_F(0,a)=2^n$.
- If $a=1$, it is easy to know $W_F(0,a)=\left(\frac{2}{n}\right)2^{m+1}$.

- If $a \neq 0,1$, we let $\varphi_a(x) = \mathrm{Tr}_n(a^{2^m} x^{2^{m+1}+1} + ax^2 + (a+a^{2^m})x)$, Then the bilinear form of $\varphi_a(x)$ is given by

$$\begin{aligned} B_{\varphi_a}(x,y) &= \varphi_a(x) + \varphi_a(y) + \varphi_a(x+y) \\ &= \mathrm{Tr}_n(a^{2^m}(x^{2^{m+1}}y + xy^{2^{m+1}})) \\ &= \mathrm{Tr}_n((a^{2^m}y + ay^2)x^{2^{m+1}}) \\ &= \mathrm{Tr}_n(L_a(y)x^{2^{m+1}}), \end{aligned}$$

where $L_a(y) = a^{2^m}y + ay^2$. Let $\ker(L_a) = \{y \in \mathbb{F}_{2^n} : L_a(y) = 0\}$. It is easy to know that $\ker(L_a) = \{0, a^{2^m-1}\}$. For $x = a^{2^m-1}$, $\mathrm{Tr}_n(aF(x)) = \mathrm{Tr}_n(1+a) = 0$ if and only if $\mathrm{Tr}_n(a) = 1$ since n is odd. According to Lemma 2.4.2, we have

$$W_F(0,a) = \begin{cases} \pm 2^{m+1}, & \text{if } \mathrm{Tr}_n(a) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Similarly, we can obtain

$$W_F(0,1+a) = \begin{cases} \left(\frac{2}{n}\right) 2^{m+1}, & \text{if } a = 0; \\ 2^n, & \text{if } a = 1; \\ \pm 2^{m+1}, & \text{if } \mathrm{Tr}_n(a) = 0 \text{ and } a \neq 0,1; \\ 0, & \text{otherwise.} \end{cases}$$

Then,

$$W_F(0,a) + (-1)^v W_F(0,1+a) = \begin{cases} 2^n + (-1)^v \left(\frac{2}{n}\right) 2^{m+1}, & \text{if } a = 0; \\ \left(\frac{2}{n}\right) 2^{m+1} + (-1)^v 2^n, & \text{if } a = 1; \\ \pm 2^{m+1}, & \text{otherwise.} \end{cases}$$

The rest of the proof is similar to that of Theorem 6.1.1, and then we omit the details here. ■

Next, we present some concrete examples in Theorem 6.2.2. In addition, the computations are carried out using Magma software [2].

Example 6.2.3 *Let $m = 2$ in Theorem 6.2.2. Then $\left(\frac{2}{n}\right) = \left(\frac{2}{5}\right) = -1$. If $v = 0$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[5,4,2]$ and weight enumerator $1 + 10z^2 + 5z^4$. If $v = 1$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[10,5,4]$ and weight enumerator $1 + 15z^4 + 15z^6 + z^{10}$. These codes are optimal by the online Database [44].*

Example 6.2.4 *Let $m = 3$ in Theorem 6.2.2. Then $\left(\frac{2}{n}\right) = \left(\frac{2}{7}\right) = 1$. If $v = 0$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[35,6,16]$ and weight enumerator $1 + 35z^{16} + 28z^{20}$. If $v = 1$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[28,7,12]$ and weight enumerator $1 + 63z^{12} + 63z^{16} + z^{18}$. These codes are optimal by the online Database [44].*

6.2.2 The case $n = 3m$

From the first 2-to-1 function in Lemma 2.4.11, this subsection presents a family of 3-weight projective binary linear codes and a family of 4-weight projective binary linear codes.

Theorem 6.2.5 *Let $n = 3m$ and $F(x) = x^{2^{2m}+2^m} + x^{2^{2m}+1} + x^{2^m+1} + x \in \mathbb{F}_{2^n}[x]$. Let D_F be defined in (6.6).*

(a) If $v = 0$, then $\mathcal{C}_{D_F}$ is a three-weight binary code with parameters $[2^{n-2} + (-1)^m 2^{2m-2} - 1, n-1, 2^{n-3} + ((-1)^m - 1)2^{2m-3}]$, and its weight distribution is given by Table 6.2.3.

(b) If $v = 1$, then $\mathcal{C}_{D_F}$ is a four-weight binary code with parameters $[2^{n-2} - (-1)^m 2^{2m-2}, n, 2^{n-3} - ((-1)^m + 1)2^{2m-3}]$, and its weight distribution is given by Table 6.2.4.

***Table 6.2.3**: The weight distribution of the code $\mathcal{C}_{D_F}$ in Theorem 6.2.5(a)*

Weight	Frequency
0	1
$2^{n-3} + ((-1)^m - 1)2^{2m-3}$	$2^{2m-1} + 2^{m-1} - \frac{1+(-1)^m}{2}$
$2^{n-3} + (-1)^m 2^{2m-3}$	$2^{3m-1} - 2^{2m}$
$2^{n-3} + ((-1)^m + 1)2^{2m-3}$	$2^{2m-1} - 2^{m-1} - \frac{1-(-1)^m}{2}$

***Table 6.2.4**: The weight distribution of the code $\mathcal{C}_{D_F}$ in Theorem 6.2.5(b)*

Weight	Frequency
0	1
$2^{n-3} - ((-1)^m + 1)2^{2m-3}$	$2^{2m} - 1$
$2^{n-3} - (-1)^m 2^{2m-3}$	$2^{3m} - 2^{2m+1}$
$2^{n-3} - ((-1)^m - 1)2^{2m-3}$	$2^{2m} - 1$
$2^{n-2} - (-1)^m 2^{2m-2}$	1

Proof: It follows from Eq. (6.7) and Lemma 6.2.1 that

$$\begin{aligned}
n_0 &= 2^{n-1} + \frac{(-1)^v}{2} W_F(0,1) \\
&= 2^{n-1} + \frac{(-1)^v}{2} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(x^{2^{2m}+2^m} + x^{2^{2m}+1} + x^{2^m+1} + x)} \\
&= 2^{n-1} + \frac{(-1)^v}{2} S_m(1,1) \\
&= 2^{n-1} + \frac{(-1)^v}{2} \left(\frac{2}{n/\gcd(m,n)} \right)^{\gcd(m,n)} 2^{\frac{n+\gcd(m,n)}{2}} \\
&= 2^{n-1} + (-1)^{m+v} 2^{2m-1}.
\end{aligned}$$

Hence, the length l of the code $\mathcal{C}_{D_F}$ is $l = |D_F| = \frac{1}{2}n_0 - 1 + v = 2^{n-2} + (-1)^{m+v}2^{2m-2} - 1 + v$.

Next, we shall determine the values of the Walsh transforms $W_F(0,a)$ and $W_F(0,1+a)$. For any $a \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} W_F(0,a) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax^{2^{2m}+2^m}+ax^{2^{2m}+1}+ax^{2^m+1}+ax)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n((a^{2^{2m}}+a^{2^m}+a)x^{2^m+1}+ax)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(\mathrm{Tr}_m^n(a)x^{2^m+1}+ax)}. \end{aligned}$$

- If $a = 0$, then $W_F(0,a) = 2^n$.
- If $a = 1$, then $W_F(0,a) = (-1)^m 2^{2m}$.
- If $\mathrm{Tr}_m^n(a) = 0$ and $a \neq 0$, then $W_F(0,a) = 0$.
- If $\mathrm{Tr}_m^n(a) \neq 0$ and $a \neq 0,1$. Let $\varphi_a(x) = \mathrm{Tr}_n(\mathrm{Tr}_m^n(a)x^{2^m+1} + ax)$. Then the bilinear form of $\varphi_a(x)$ is given by

$$\begin{aligned} B_{\varphi_a}(x,y) &= \varphi_a(x) + \varphi_a(y) + \varphi_a(x+y) \\ &= \mathrm{Tr}_n(\mathrm{Tr}_m^n(a)(x^{2^m}y + xy^{2^m})) \\ &= \mathrm{Tr}_n((\mathrm{Tr}_m^n(a)(y^{2^m} + y))x^{2^{2m}}) \\ &= \mathrm{Tr}_n(L_a(y)x^{2^{2m}}), \end{aligned}$$

  where $L_a(y) = \mathrm{Tr}_m^n(a)(y^{2^m} + y)$. Let $\ker(L_a) = \{y \in \mathbb{F}_{2^n} : L_a(y) = 0\}$. It is easy to know that $\ker(L_a) = \{\eta : \eta \in \mathbb{F}_{2^m}\}$. For any $x = \eta \in \ker(L_a)$, $\mathrm{Tr}_n(aF(x)) = \mathrm{Tr}_n(a\eta^2 + a\eta) = \mathrm{Tr}_n((a+a^2)\eta^2) = \mathrm{Tr}_m((\mathrm{Tr}_m^n(a+a^2))\eta^2) = 0$ if and only if $\mathrm{Tr}_m^n(a+a^2) = 0$, i.e, $\mathrm{Tr}_m^n(a) = 1$ (since the assumption $\mathrm{Tr}_m^n(a) \neq 0$). From Lemma 2.4.2, we have

$$W_F(0,a) = \begin{cases} \pm 2^{2m}, & \text{if } \mathrm{Tr}_m^n(a) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Similarly, we can obtain,

$$W_F(0,1+a) = \begin{cases} (-1)^m 2^{2m}, & \text{if } a = 0; \\ 2^n, & \text{if } a = 1; \\ \pm 2^{2m}, & \text{if } \mathrm{Tr}_m^n(a) = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, by a simple calculation, we have

$$W_F(0,a) + (-1)^v W_F(0,1+a) = \begin{cases} 2^n + (-1)^{m+v}2^{2m}, & \text{if } a = 0; \\ (-1)^v 2^n + (-1)^m 2^{2m}, & \text{if } a = 1; \\ \pm 2^{2m}, & \text{if } a \neq 0,1 \text{ and } \mathrm{Tr}_m^n(a) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

The rest of the proof is similar to that of Theorem 6.1.1, and then we omit it here. ■

Next, we give some concrete examples in Theorem 6.2.5, and the computations are carried out using Magma software [2].

Example 6.2.6 *Let $m = 2$ in Theorem 6.2.5. If $v = 0$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[19,5,8]$ and weight enumerator $1+9z^8+16z^{10}+6z^{12}$. If $v = 1$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[12,6,4]$ and weight enumerator $1+15z^4+32z^6+15z^8+z^{12}$. These codes are optimal by the online Database [44].*

Example 6.2.7 *Let $m = 3$ in Theorem 6.2.5. If $v = 0$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[111,8,48]$ and weight enumerator $1+36z^{48}+192z^{56}+27z^{64}$. If $v = 1$, then the binary linear code $\mathcal{C}_{D_F}$ has parameters $[144,9,64]$ and weight enumerator $1+63z^{64}+384z^{72}+63z^{80}+z^{144}$.*

6.3 Dual codes

In this section, we will determine the parameters of the duals $\mathcal{C}(F)_D^{\perp}$ and $\mathcal{C}_{D_F}^{\perp}$ of the binary linear codes $\mathcal{C}(F)_D$ and $\mathcal{C}_{D_F}$.

Firstly, we consider the parameters of the dual code of $\mathcal{C}(F)_D$ in (1.8).

Theorem 6.3.1 *Let F be a 2-to-1 mapping over $\mathbb{F}_{2^n}$ with $F(0) = 0$ and the code $\mathcal{C}(F)_D$ be defined as in (1.8). Let $\mathcal{C}(F)_D^{\perp}$ be the dual code of $\mathcal{C}(F)_D$ and d_{V_1} be defined as in (6.2). Then $\mathcal{C}(F)_D^{\perp}$ is a $[2^{n-1}-1+v, 2^{n-1}-1+v-(2n-d_{V_1}), d^{\perp}]$ binary linear code with the minimum distance $d^{\perp}$ satisfying*

- *if $v = 0$, then $3 \le d^{\perp} \le 6$.*
- *if $v = 1$, then $4 \le d^{\perp} \le 6$.*

In particular, if F is APN, then the minimum distance $d^{\perp}$ satisfies

- *if $v = 0$, then $5 \le d^{\perp} \le 6$.*
- *if $v = 1$, then $d^{\perp} = 6$.*

Proof: According to the first construction in Section 6.1, the linear code $\mathcal{C}(F)_D$ has length $2^{n-1}-1+v$ and dimension $2n-d_{V_1}$. Then it is easy to obtain the length and dimension of its dual. Next, it suffices to consider the minimum distance.

Since D does not contain the zero element of $\mathbb{F}_{2^n}$, the minimum distance $d^{\perp}$ of $\mathcal{C}(F)_D^{\perp}$ cannot be one. If $d^{\perp} = 2$, then there exist two distinct elements $x_1, x_2 \in D$ such that $\mathrm{Tr}_n(a(x_1+x_2)+b(F(x_1)+F(x_2))) = 0$ for any $a, b \in \mathbb{F}_{2^n}$, i.e., $x_1+x_2 = 0$ and $F(x_1)+F(x_2) = 0$, which is a contradiction. Hence, the minimum distance of $\mathcal{C}(F)_D^{\perp}$ cannot be 2. Thus, $d^{\perp} \ge 3$. Suppose that $d^{\perp} \ge 7$. Then we have $\sum_{i=0}^{2} \binom{2^{n-1}-1+v}{i}(2-1)^i = 1+2^{n-1}-1+v+\frac{1}{2}(2^{n-1}-1+v)(2^{n-1}-2+v)+\frac{1}{6}(2^{n-1}-1+v)(2^{n-1}-2+v)(2^{n-1}-3+v) > 2^{2n-d_{V_1}}$, which contradicts the sphere packing bound. Therefore, $3 \le d^{\perp} \le 6$. If $v = 1$, we can easily prove that $d^{\perp} \ne 3$ and then $4 \le d^{\perp} \le 6$.

In particular, if F is APN, we obtain that the dual of $\mathcal{C}_F$ (defined in (1.5)) has minimum distance 5 by [12, Theorem 5]. Note that $\mathcal{C}(F)_D$ is a punctured code. Therefore, the dual of $\mathcal{C}(F)_D$ has minimum distance $d^\perp \geq 5$.

Next, we show that $d^\perp \neq 5$ when $v = 1$.

If $d^\perp = 5$, then there are five pairwise-distinct elements x_1, x_2, x_3, x_4 and x_5 in D such that

$$\begin{cases} \mathrm{Tr}_n(x_1) = \mathrm{Tr}_n(x_2) = \mathrm{Tr}_n(x_3) = \mathrm{Tr}_n(x_4) = \mathrm{Tr}_n(x_5) = 1; \\ \mathrm{Tr}_n(a\sum_{i=1}^5 x_i + b\sum_{i=1}^5 F(x_i)) = 0, \end{cases}$$

for any $a, b \in \mathbb{F}_{2^n}$. Then

$$\begin{cases} \mathrm{Tr}_n(\sum_{i=1}^5 x_i) = 1; \\ \sum_{i=1}^5 x_i = 0, \end{cases}$$

leading to a contradiction. Thus $d^\perp \neq 5$ and then $d^\perp \geq 6$.

This completes the proof. ■

Remark 6.3.2 *In view of the proof of Theorem 6.3.1, we notice that the dual code $\mathcal{C}(F)_D^\perp$ is distance-optimal with respect to the sphere packing bound when $v = 1$ and F is APN.*

In the following, we present the parameters of the duals of the binary linear codes defined in (1.8) obtained in Section 6.1.

Corollary 6.3.3 *Let the code $\mathcal{C}(F)_D$ be defined as in (1.8). We have the following results.*

(1) For the binary linear code in Theorem 6.1.1, if $v = 1$, its dual has parameters $[2^{n-1}, 2^{n-1} - 3m, 4]$, and is distance-optimal with respect to the sphere packing bound.

(2) For the binary linear code in Theorem 6.1.3, if $v = 0$, its dual has parameters $[2^{n-1} - 1, 2^{n-1} - 2n, 5]$; if $v = 1$, its dual has parameters $[2^{n-1}, 2^{n-1} - 2n, 6]$, and is distance-optimal with respect to the sphere packing bound.

(3) For the binary linear code in Theorem 6.1.7, if $v = 0$, its dual has parameters $[2^{n-1} - 1, 2^{n-1} - n - m, 3]$; if $v = 1$, its dual has parameters $[2^{n-1}, 2^{n-1} - n - m, 4]$, and is distance-optimal with respect to the sphere packing bound.

(4) For the binary linear code in Theorem 6.1.10, if $v = 0$, its dual has parameters $[2^{n-1} - 1, 2^{n-1} - 2n + m, 3]$; if $v = 1$, its dual has parameters $[2^{n-1}, 2^{n-1} - 2n + m, 4]$, and is distance-optimal with respect to the sphere packing bound.

Proof: We prove the desired results for Cases (1) and (2) only. The results in Cases (3) and (4) can be proved in a similar way.

(1) It follows from Theorem 6.1.1(b) that the linear code $\mathcal{C}(F)_D$ has length 2^{n-1} and dimension $3m$. Then the length and dimension of the dual of $\mathcal{C}(F)_D$ can be trivially determined. Next, we consider the minimum distance. In view of Theorem 6.3.1, we

know that the minimal distance of the dual of $\mathcal{C}(F)_D$ is $d^\perp \geq 4$. Suppose $d^\perp \geq 5$, then we have $\sum_{i=0}^{2} \binom{2^{n-1}}{i}(2-1)^i = 1+2^{n-1}+2^{n-2}(2^{n-1}-1) > 2^{3m}$, which contradicts the sphere packing bound. Thus $d^\perp = 4$.

(2) If $v=0$, from Theorem 6.3.1, we have $A_1^\perp = A_2^\perp = A_3^\perp = A_4^\perp = 0$. By the sixth Pless power moment in (2.4), we get $A_5^\perp = (2^{6m-1} - 11\cdot 2^{4m-2} + 11\cdot 2^{2m+1} - 16)/120 \neq 0$. Hence, the dual of $\mathcal{C}(F)_D$ has parameters $[2^{n-1}-1, 2^{n-1}-2n, 5]$ by Theorem 6.3.1. If $v=1$, since $W_F(a,b) = 0$ or $\pm 2^{\frac{n+1}{2}} = \pm 2^{m+1}$ for any pair $(a,b) \in \mathbb{F}_{2^n}^2$ with $b \neq 0$, and then F is APN, it is easy to determine the parameters of the dual of $\mathcal{C}(F)_D$ by Theorem 6.3.1.

This completes the proof. ■

In the following, we give some concrete examples of Corollary 6.3.3, and the computation is verified by Magma [2].

Example 6.3.4 *Let $m=3$. For the binary linear code in Theorem 6.1.1, if $v=0$, its dual has parameters $[31,23,3]$ and is almost optimal, while the optimal binary code has parameters $[32,23,4]$; if $v=1$, its dual has parameters $[32,23,4]$ and is optimal.*

Example 6.3.5 *Let $m=2$. For the binary linear code in Theorem 6.1.3, if $v=0$, its dual has parameters $[15,6,5]$ and is almost optimal, while the optimal binary code has parameters $[15,6,6]$; if $v=1$, its dual has parameters $[16,6,6]$ and is optimal.*

Example 6.3.6 *Let $m=2$. For the binary linear code in Theorem 6.1.7, if $v=0$, its dual has parameters $[31,24,3]$ and is almost optimal, while the optimal binary code has parameters $[31,24,4]$; if $v=1$, its dual has parameters $[32,24,4]$ and is optimal.*

Example 6.3.7 *Let $m=3$. For the binary linear code in Theorem 6.1.10, if $v=0$, its dual has parameters $[255,241,3]$ and is almost optimal, while the optimal binary code has parameters $[255,241,4]$; if $v=1$, its dual has parameters $[256,241,4]$ and is optimal.*

Next, we consider the dual code of $\mathcal{C}_{D_F}$ in (1.6) and investigate its parameters.

Theorem 6.3.8 *Let F be a 2-to-1 mapping over $\mathbb{F}_{2^n}$ with $F(0)=0$ and the code $\mathcal{C}_{D_F}$ be defined as in (1.6). Let $\mathcal{C}_{D_F}^\perp$ be the dual code of $\mathcal{C}_{D_F}$ and d_{V_2} be defined as in (6.8). Then $\mathcal{C}_{D_F}^\perp$ is a $[2^{n-2} + \frac{(-1)^v}{4}W_F(0,1) - 1 + v, 2^{n-2} + \frac{(-1)^v}{4}W_F(0,1) - 1 + v - (n-d_{V_2}), d^\perp]$ binary linear code with the minimum distance $d^\perp$ satisfying*

- *if $v=0$, then $3 \leq d^\perp \leq 4$*
- *if $v=1$, then $d^\perp = 4$.*

Proof: By the second construction in Section 6.2, the linear code $\mathcal{C}_{D_F}$ has length $2^{n-2} + \frac{(-1)^v}{4}W_F(0,1) - 1 + v$ and dimension $n - d_{V_2}$, and it, therefore, suffices to consider the minimum distance. It is obvious that $d^\perp \neq 1$. If $d^\perp = 2$, then there exist two distinct elements $d_1 = F(x_1), d_2 = F(x_2) \in D_F$ such that $\mathrm{Tr}_n(aF(x_1)) + \mathrm{Tr}_n(aF(x_2)) = 0$

for any $a \in \mathbb{F}_{2^n}$, i.e., $F(x_1)+F(x_2)=0$, which is a contradiction. Hence, $d^{\perp} \geq 3$. Furthermore, suppose that $d^{\perp} \geq 5$. Then we have $\sum_{i=0}^{2} \binom{2^{n-2}+\frac{(-1)^v}{4}W_F(0,1)-1+v}{i}(2-1)^i = 1+2^{n-2}+\frac{(-1)^v}{4}W_F(0,1)-1+v+\frac{1}{2}(2^{n-2}+\frac{(-1)^v}{4}W_F(0,1)-1+v)(2^{n-2}+\frac{(-1)^v}{4}W_F(0,1)-2+v) > 2^{n-d_{V_2}}$, which contradicts the sphere packing bound. Therefore, $3 \leq d^{\perp} \leq 4$.

In the following, we will show that $d^{\perp}=4$ when $v=1$. According to the above discussion, it suffices to prove that $d^{\perp} \neq 3$. Suppose that $d^{\perp}=3$. Then there are three pairwise-distinct elements $d_1=F(x_1), d_2=F(x_2)$ and $d_3=F(x_3)$ in D_F such that

$$\begin{cases} \mathrm{Tr}_n(F(x_1))=\mathrm{Tr}_n(F(x_2))=\mathrm{Tr}_n(F(x_3))=1; \\ \mathrm{Tr}_n(a(F(x_1)+F(x_2)+F(x_3)))=0, \end{cases}$$

for any $a \in \mathbb{F}_{2^n}$. Then

$$\begin{cases} \mathrm{Tr}_n(F(x_1)+F(x_2)+F(x_3))=1; \\ F(x_1)+F(x_2)+F(x_3)=0, \end{cases}$$

which is a contradiction. Hence, $d^{\perp}=4$ when $v=1$. ■

Remark 6.3.9 *In view of the proof of Theorem 6.3.8, we remark that the dual code $\mathcal{C}_{D_F}^{\perp}$ is distance-optimal with respect to the sphere packing bound when $v=1$.*

Next, we give the parameters of the duals of the binary linear codes defined in (1.6) obtained in Section 6.2.

Corollary 6.3.10 *Let the code $\mathcal{C}_{D_F}$ be defined as in (1.6). We have the following results.*

(1) For the binary linear code in Theorem 6.2.2, if $v=0$, its dual has parameters $[2^{n-2}+\binom{2}{n}2^{m-1}-1, 2^{n-2}+\binom{2}{n}2^{m-1}-n, 3]$; if $v=1$, its dual has parameters $[2^{n-2}-\binom{2}{n}2^{m-1}, 2^{n-2}-\binom{2}{n}2^{m-1}-n, 4]$, and is distance-optimal with respect to the sphere packing bound.

(2) For the binary linear code in Theorem 6.2.5, if $v=0$, its dual has parameters $[2^{n-2}+(-1)^m 2^{2m-2}-1, 2^{n-2}+(-1)^m 2^{2m-2}-n, 3]$; if $v=1$, its dual has parameters $[2^{n-2}-(-1)^m 2^{2m-2}, 2^{n-2}-(-1)^m 2^{2m-2}-n, 4]$, and is distance-optimal with respect to the sphere packing bound.

Proof: Using Lemma 2.2.7 and Theorem 6.3.8 and similar discussions in the proof of Corollary 6.3.3, one can prove this corollary. ■

In the following, we give some concrete examples of Corollary 6.3.10, and the computation is verified by Magma [2].

Example 6.3.11 *Let $m=2$. For the binary linear code in Theorem 6.2.2, if $v=0$, its dual has parameters $[5,1,5]$ and is optimal; if $v=1$, its dual has parameters $[10,5,4]$ and is optimal.*

Example 6.3.12 *Let $m = 3$. For the binary linear code in Theorem 6.2.5, if $v = 0$, its dual has parameters $[111, 103, 3]$ and is almost optimal, while the optimal binary code has parameters $[111, 103, 4]$; if $v = 1$, its dual has parameters $[144, 135, 4]$ and is optimal.*

Note that if the dual of a linear code has the minimum Hamming distance of at least 3, then the linear code is called a projective linear code. From Theorems 6.3.1 and 6.3.8, we obtain the following result.

Theorem 6.3.13 *The binary linear codes $\mathcal{C}(F)_D$ and $\mathcal{C}_{D_F}$ constructed in Sections 6.1 and 6.2, respectively, are projective linear codes.*

6.4 Conclusions

In this chapter, based on the constructions in (1.6) and (1.8), we succeeded in this chapter in constructing large families of projective binary linear codes with few weights (namely, 1-weight, 2-weight, 3-weight, 4-weight, 5-weight, and 6-weight) from 2-to-1 functions by selecting two different defining sets. Using the Walsh transform of the corresponding 2-to-1 functions over $\mathbb{F}_{2^n}$, we determined the weight distributions of these codes. The results show that the parameters of these linear codes are novel and flexible. Notably, the minimum distance of the duals of the constructed codes was discussed, and the dual codes of some linear codes are distance-optimal with respect to the sphere packing bound. In addition, the linear codes constructed in this chapter have two applications: Firstly, the projective binary linear codes with three-weight in Theorems 6.1.7(a), 6.1.10(a), 6.2.2(b) and 6.2.5(a) may be used to construct association scheme with three classes. As another application, some binary linear codes of this paper may yield secret sharing schemes with interesting access structures:

• Let m be odd and $n = 2m$. Then for the linear code in Theorem 6.1.1(a), if $m \geq 5$, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{n-2} - 2^m}{2^{n-2} + 2^m} > \frac{1}{2}.$$

• Let m be a positive integer and $n = 2m + 1$. Then for the linear code in Theorem 6.1.3(a), if $m \geq 3$, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{n-2} - 2^m}{2^{n-2} + 2^m} > \frac{1}{2}.$$

For the linear code in Theorem 6.2.2(a), if $m \geq 3$, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{n-3} + (\binom{2}{n} - 1)2^{m-2}}{2^{n-3} + (\binom{2}{n} + 1)2^{m-2}} > \frac{1}{2}.$$

• Let m be a positive integer and $n = 3m$. Then for the linear code in Theorem 6.1.7(a), if $m \geq 2$, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{n-2} - 2^{2m-2}}{2^{n-2} + 2^{2m-2}} > \frac{1}{2}.$$

For the linear code in Theorem 6.1.10(a), if $m \geq 3$ and $m \not\equiv 1 \pmod 3$, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{n-2} - 2^{2m-1}}{2^{n-2} + 2^{2m-1}} > \frac{1}{2}.$$

For the linear code in Theorem 6.2.5(a), if $m \geq 3$, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{n-3} + ((-1)^m - 1)2^{2m-3}}{2^{n-3} + ((-1)^m + 1)2^{2m-3}} > \frac{1}{2}.$$

Consequently, the linear codes presented in this chapter satisfy the condition that $w_{\min}/w_{\max} > \frac{1}{2}$ under certain conditions and can therefore be employed to construct interesting access structures for secret sharing schemes.

Chapter 7

Conclusions and Future Work

This chapter summarizes the completed work and presents the directions of further research in the future.

7.1 Conclusions

In this thesis, we have mainly studied the theory of algebraic coding over finite fields and finite rings and their applications, including the construction of optimal or asymptotically optimal codebooks, the construction of linear codes with a one-dimensional hull, minimal linear codes with few nonzero weights, and the construction of projective linear codes. The main research work and achievements of this thesis are as follows:

(1) This thesis constructed several families of optimal or asymptotically optimal codebooks by studying the character sums over the finite chain ring $R_1 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 0)$ and the finite non-chain ring $R_2 = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = u)$. Based on the research method of character sums over finite fields, we first gave the definitions of Gaussian sums, Jacobi sums and (hyper) Eisenstein sums over finite rings and investigated some properties of these character sums. Moreover, we established the relationship between Gaussian sums and hyper Eisenstein sums over finite rings and Gaussian sums and hyper Eisenstein sums over finite fields, respectively. This relationship allows us to give the absolute value of Gaussian sums and hyper Eisenstein sums over finite rings. For their applications, we constructed several classes of optimal and asymptotically optimal codebooks with respect to the Welch bound and a class of optimal codebooks with respect to the Levenshtein bound by using these character sums over R_1 and R_2. Notably, the parameters of some of these codebooks are new and flexible.

(2) This thesis constructed linear codes with one-dimensional hull by further extending the existing construction method and exploring new methods. Firstly, we constructed several classes of linear codes with one-dimensional hull by using general Gaussian sums over finite fields. In addition, sufficient conditions were given for a linear code over finite fields to be a linear code with one-dimension hull and several classes of linear codes with one-dimensional hull having new parameters were constructed by exploring two homomorphic mappings over finite fields. Furthermore, we presented a lower bound on the minimum distances of the constructed linear codes.

(3) This thesis studied few-weight binary linear codes by using the known two-to-

one functions over finite fields. Based on three constructions, we constructed several families of linear codes with few weights and completely determined their weight distributions by using the Walsh transform of the corresponding two-to-one functions. Besides, some of them are optimal with respect to the well-known Griesmer bound. We also showed that the derived binary linear codes were minimal for most cases, and described the access structures of the secret sharing schemes based on their dual codes. In particular, we solved two open problems in [72].

(4) Based on the construction method of linear codes given by Qu et al. [72, 116], we proposed two new construction methods and then obtained several classes of projective binary linear codes with new parameters. In addition, we showed that the duals of the constructed codes were distance-optimal with respect to the sphere packing bound. As applications, some of the obtained codes can be used to construct association schemes and secret sharing schemes with interesting access structures.

7.2 Future work

Based on the research on this thesis, further research work is given as follows:

(1) Define new character sums over finite fields or finite rings, and then study their properties and discuss the values of the new character sums.

(2) Construct the linear codes with low-dimensional hull by studying the special generator matrix (for example, cyclic matrix, symmetry matrix and so on) and characterize some sufficient conditions for a linear code to be a linear code with low-dimensional hull. With these conditions, we can construct some optimal and almost optimal linear codes with low-dimensional hull by Magma. Particularly, finding new applications of codes with one-dimensional hull.

(3) Construct new cryptographic functions over finite fields. For example, new two-to-one functions, n-to-one functions and so on. Based on two general constructions of linear codes, it would be interesting to present new construction of linear codes by using new cryptographic functions and then construct linear codes with new parameters over finite fields.

(4) The construction method of linear codes over finite fields is extended to finite rings, and then the optimal linear codes with new parameters are constructed by the Gray mapping over finite rings.

Bibliography

[1] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inf. Theory*, 44(5):2010–2017, 1998. (document), 2, 2.2.8, 2.2, 2.2.9

[2] W. Bosma, J. Cannon, C. Fieker, and A. Steel. *Handbook of Magma functions*. Edition 2.22 5669 pages. http://magma.maths.usyd.edu.au/magma/, 2016. 4.2.1, 4.2.2, 4.2.2, 5.2.2, 5.2.2, 5.2.3, 5.2.3, 5.4, 6.1.1, 6.1.2, 6.1.3, 6.1.3, 6.2.1, 6.2.2, 6.3, 6.3

[3] D. Bressoud and S. Wagon. *A Course in Computational Number Theory*. Springer, 2000. 2, 2.3.2

[4] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi. Orthogonal direct sum masking-a smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks. In D. Naccache and D. Sauveron, editors, *Information Security Theory and Practice. Securing the Internet of Things-8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30-July 2, 2014. Proceedings*, volume 8501 of *Lecture Notes in Computer Science*, pages 40–56. Springer, 2014. 1.2.3

[5] A. Brouwer and W. Haemers. *Spectra of Graphs*. New York, NY, USA: Springer-Verlag, 2012. 4.2

[6] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Trans. Inf. Theory*, 52(3):1141–1152, 2006. 2, 2.4.1

[7] A. Calderbank and W. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 18(2):97–122, 1986. 1.2.2

[8] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. $\mathbb{Z}_4$-kerdock codes, orthogonal spreads, and extremal euclidean linesets. *Proc. London Math. Soc.*, 75(3):436–480, 1997. 1.2.1

[9] E. J. Candès and M. B. Wakin. An introduction to compressive sampling. *IEEE Signal Process. Mag.*, 25(2):21–30, 2008. 3

[10] X. Cao, W. Chou, and X. Zhang. More constructions of near optimal codebooks associated with binary sequences. *Adv. Math. Commun.*, 11(1):187–202, 2017. 1.2.1

[11] C. Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press. Cambridge, U.K., 2021. 1.2.2, 5.1

[12] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998. 2.4, 3, 5.3, 6.3

[13] C. Carlet and S. Guilley. Complementary dual codes for countermeasures to side-channel attacks. *In Coding Theory and Applications (CIM Series in Mathematical Sciences), 3, E. R. Pinto, Ed. Cham, Switzerland: Springer-Verlag*, pages 97–105, 2014. 1.2.2, 1.2.3, 1.2.3

[14] C. Carlet, C. Güneri, S. Mesnager, and F. Özbudak. Construction of some codes suitable for both side channel and fault injection attacks. In Lilya Budaghyan and Francisco Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields - 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14-16, 2018, Revised Selected Papers*, volume 11321 of *Lecture Notes in Computer Science*, pages 95–107. Springer, 2018. 1.2.3

[15] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, and P. Solé. On linear complementary pairs of codes. *IEEE Trans. Inf. Theory*, 64(10):6583–6589, 2018. 1.2.3

[16] C. Carlet, C. Li, and S. Mesnager. Linear codes with small hulls in semi-primitive case. *Des. Codes Cryptogr.*, 87(12):3063–3075, 2019. (document), 1.2.3, 1.2.3, 1.3, 2, 2.3.1, 4, 4.2, 4.2.1, 4.2.5, 4.2.1, 4.2.6, 4.4

[17] C. Carlet, S. Mesnager, C. Tang, and Y. Qi. Euclidean and hermitian LCD MDS codes. *Des. Codes Cryptogr.*, 86(11):2605–2618, 2018. 1.2.3

[18] C. Carlet, S. Mesnager, C. Tang, and Y. Qi. New characterization and parametrization of LCD codes. *IEEE Trans. Inf. Theory*, 65(1):39–49, 2019. 1.2.3

[19] C. Carlet, S. Mesnager, C. Tang, and Y. Qi. On σ-lcd codes. *IEEE Trans. Inf. Theory*, 65(3):1694–1704, 2019. 1.2.3

[20] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and Ruud Pellikaan. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. *IEEE Trans. Inf. Theory*, 64(4):3010–3017, 2018. 1.2.3

[21] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In Hyang-Sook Lee and Dong-Guk Han, editors, *Information Security and Cryptology-ICISC 2013-16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, volume 8565 of *Lecture Notes in Computer Science*, pages 34–46. Springer, 2013. 1.2.2

[22] B. Chen and H. Liu. New constructions of MDS codes with complementary duals. *IEEE Trans. Inf. Theory*, 64(8):5776–5782, 2018. 1.2.3

[23] G. Cohen, S. Mesnager, and A. Patey. On minimal and quasiminimal linear codes. In *In Proc. IMA Int. Conf. Cryptogr. Coding. Berlin, Germany*, volume 8308, pages 85–98. Springer, 2013. 1.2.2

[24] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate texts in mathematics*. Springer, 1993. 2, 2.3.2

[25] R. S. Coulter. On the evaluation of a class of weil sums in characteristic 2. *New Zealand J. of Math.*, 28:171–184, 1999. 6.2.1

[26] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms - an introduction to computational algebraic geometry and commutative algebra (2. ed.)*. Undergraduate texts in mathematics. Springer, 1997. 5.4.1, 5.4.2

[27] C. Ding. Complex codebooks from combinatorial designs. *IEEE Trans. Inf. Theory*, 52(9):4229–4235, 2006. 1.2.1, 1.2.1, 3

[28] C. Ding. Linear codes from some 2-designs. *IEEE Trans. Inf. Theory*, 61(6):3265–3275, 2015. 1.2.2

[29] C. Ding. A construction of binary linear codes from boolean functions. *Discret. Math.*, 339(9):2288–2303, 2016. 1.2.2

[30] C. Ding. The construction and weight distributions of all projective binary linear codes. *CoRR*, abs/2010.03184, 2020. 1.2.2

[31] C. Ding and T. Feng. A generic construction of complex codebooks meeting the welch bound. *IEEE Trans. Inf. Theory*, 53(11):4245–4250, 2007. 3

[32] C. Ding and T. Feng. Codebooks from almost difference sets. *Des. Codes Cryptogr.*, 46(1):113–126, 2008. 1.2.1, 1.2.1, 3

[33] C. Ding and H. Niederreiter. Cyclotomic linear codes of order 3. *IEEE Trans. Inf. Theory*, 53(6):2274–2277, 2007. (document), 1.2.2, 6

[34] C. Ding and X. Wang. A coding theory construction of new systematic authentication codes. *Theor. Comput. Sci.*, 330(1):81–99, 2005. 1.2.2

[35] C. Ding and J. Yin. Signal sets from functions with optimum nonlinearity. *IEEE Trans. Commun.*, 55(5):936–940, 2007. 1.2.1

[36] C. Ding and J. Yuan. Covering and secret sharing with linear codes. In Cristian Calude, Michael J. Dinneen, and Vincent Vajnovszki, editors, *Discrete Mathematics and Theoretical Computer Science, 4th International Conference, DMTCS 2003, Dijon, France, July 7-12, 2003. Proceedings*, volume 2731 of *Lecture Notes in Computer Science*, pages 11–25. Springer, 2003. 2, 2.2.8

[37] K. Ding and C. Ding. Binary linear codes with three weights. *IEEE Commun. Lett.*, 18(11):1879–1882, 2014. 1.2.2

[38] K. Ding and C. Ding. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Trans. Inf. Theory*, 61(11):5835–5842, 2015. 1.2.2, 1.2.2

[39] S. T. Dougherty, J. Kim, B. Özkaya, L. Sok, and P. Solé. The combinatorics of LCD codes: linear programming bound and orthogonal matrices. *Int. J. Inf. Coding Theory*, 4(2/3):116–128, 2017. 1.2.3

[40] M. Esmaeili and S. Yari. On complementary-dual quasi-cyclic codes. *Finite Fields Their Appl.*, 15(3):375–386, 2009. 1.2.3

[41] W. Fang, F. Fu, L. Li, and S. Zhu. Euclidean and hermitian hulls of MDS codes and their applications to eaqeccs. *IEEE Trans. Inf. Theory*, 66(6):3527–3537, 2020. 1.2.3

[42] L. Galvez, J. L. Kim, N. Lee, Y. G. Roe, and B. S. Won. Some bounds on binary lcd codes. *Cryptogr. Commun.*, 10(4):719–728, 2018. 1.2.3

[43] M. J. E. Golay. Complementary series. *IRE Trans. Inf. Theory*, 7(2):82–87, 1961. 1.2.1

[44] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. *http://www.codetables. de*, 2019. 5.2.8, 5.2.11, 5.2.14, 6.1.5, 6.1.6, 6.1.8, 6.2.3, 6.2.4, 6.2.6

[45] J. H. Griesmer. A bound for error-correcting codes. *IBM J. Res. Dev.*, 4(5):532–542, 1960. 4.2.3, 4.2.4

[46] C. Güneri, B. Özkaya, and P. Solé. Quasi-cyclic complementary dual codes. *Finite Fields Their Appl.*, 42:67–80, 2016. 1.2.3

[47] T. Helleseth and P. V. Kumar. *Sequences with low correlation*. In Handbook of Coding Theory. V. Pless and C. Huffman, Eds. New York. Elsevier, 1998. 1.2.1

[48] Z. Heng. Nearly optimal codebooks based on generalized jacobi sums. *Discret. Appl. Math.*, 250:227–240, 2018. 1.2.1, 2, 3

[49] Z. Heng, C. Ding, and Q. Yue. New constructions of asymptotically optimal codebooks with multiplicative characters. *IEEE Trans. Inf. Theory*, 63(10):6179–6187, 2017. 1.2.1, 3, 3.3.1

[50] Z. Heng, W. Wang, and Y. Wang. Projective binary linear codes from special boolean functions. *Appl. Algebra Eng. Commun. Comput.*, 32(4):521–552, 2021. 1.2.2

[51] Z. Heng and Q. Yue. Optimal codebooks achieving the levenshtein bound from generalized bent functions over $\mathbb{Z}_4$. *Cryptogr. Commun.*, 9(1):41–53, 2017. 1.2.1

[52] S. Hong, H. Park, J. No, T. Helleseth, and Y. Kim. Near-optimal partial hadamard codebook construction using binary sequences obtained from quadratic residue mapping. *IEEE Trans. Inf. Theory*, 60(6):3698–3705, 2014. 1.2.1, 3, 3.3.1

[53] H. Hu and J. Wu. New constructions of codebooks nearly meeting the welch bound with equality. *IEEE Trans. Inf. Theory*, 60(2):1348–1355, 2014. 1.2.1, 3, 3.3.1

[54] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003. (document), 1.2.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2, 2.2.5, 2.2.6, 2.2.7, 5.1

[55] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate texts in mathematics*. Springer, 1982. 2, 2.3, 2.3.1

[56] G. Jian, Z. Lin, and R. Feng. Two-weight and three-weight linear codes based on weil sums. *Finite Fields Their Appl.*, 57:92–107, 2019. 1.2.2

[57] L. Jin. Construction of MDS codes with complementary duals. *IEEE Trans. Inf. Theory*, 63(5):2843–2847, 2017. 1.2.3

[58] L. Jin and C. Xing. Algebraic geometry codes with complementary duals exceed the asymptotic gilbert-varshamov bound. *IEEE Trans. Inf. Theory*, 64(9):6277–6282, 2018. 1.2.3

[59] E. Assmus Jr. and J. Key. Affine and projective planes. *Discret. Math.*, 83(2-3):161–187, 1990. (document), 1.2.3, 2, 2.2.2

[60] G. A. Kabatyanskii and V. I. Levenshtein. On bounds for packing on a sphere and in space. *Probl. Inf. Transmission*, 14(1):1–17, 1979. 1.2.2

[61] J. Kovacevic and A. Chebira. An introduction to frames. *Found. Trends Signal Process.*, 2(1):1–94, 2008. 1.2.1

[62] A. Lempel, M. Cohn, and W. L. Eastman. A class of balanced binary sequences with optimal autocorrelation properties. *IEEE Trans. Inf. Theory*, 23(1):38–42, 1977. 1.2.1

[63] J. S. Leon. An algorithm for computing the automorphism group of a hadamard matrix. *J. Comb. Theory, Ser. A*, 27(3):289–306, 1979. (document), 1.2.3

[64] J. S. Leon. Permutation group algorithms based on partitions, I: theory and algorithms. *J. Symb. Comput.*, 12(4/5):533–583, 1991. 1.2.3

[65] V. I. Levenshtein. Bounds for packing of metric spaces and some of their applications. *Probl. Cybern.*, 40:43–110, 1983. 1.2.2

[66] C. Li, C. Ding, and S. Li. LCD cyclic codes over finite fields. *IEEE Trans. Inf. Theory*, 63(7):4344–4356, 2017. 1.2.3, 5.2.9

[67] C. Li, N. Li, T. Helleseth, and C. Ding. The weight distributions of several classes of cyclic codes from APN monomials. *IEEE Trans. Inf. Theory*, 60(8):4710–4721, 2014. 1.2.2

[68] C. Li, Q. Yue, and F. Fu. A construction of several classes of two-weight and three-weight linear codes. *Appl. Algebra Eng. Commun. Comput.*, 28(1):11–30, 2017. 1.2.2, 1.2.2

[69] C. Li, Q. Yue, and Y. Huang. Two families of nearly optimal codebooks. *Des. Codes Cryptogr.*, 75(1):43–57, 2015. 1.2.1, 3, 3.3.1

[70] C. Li and P. Zeng. Constructions of linear codes with one-dimensional hull. *IEEE Trans. Inf. Theory*, 65(3):1668–1676, 2019. (document), 1.2.4, 1.2.3, 1.3, 4, 4.2, 4.2.1, 4.2.7, 4.2.1, 4.2.8, 4.2.2, 4.2.14, 4.2.2, 4.2.15, 4.2.2, 4.2.17, 4.3.4, 4.4

[71] J. Li, S. Zhu, and K. Feng. The gauss sums and jacobi sums over galois ring $\mathrm{gr}(p^2, r)$. *Science China Mathematics*, 56(7):1457–1465, 2013. 3

[72] K. Li, C. Li, T. Helleseth, and L. Qu. Binary linear codes with few weights from two-to-one functions. *IEEE Trans. Inf. Theory*, 67(7):4263–4275, 2021. (document), 1.2.2, 1.2.2, 1.3, 2, 2.4, 2.4.2, 2.4, 2.4.12, 5, 5.1, 5.1, 5.1, 5.1.1, 5.2.2, 5.2.3, 5.2.2, 5.2.2, 5.2.15, 5.2.2, 5.2.3, 5.2.3, 5.2.3, 5.4, 5.4.3, 5.4.4, 5.4, 5.5, 7.1

[73] K. Li, S. Mesnager, and L. Qu. Further study of 2-to-1 mappings over $\mathbb{F}_{2^n}$. In *Ninth International Workshop on Signal Design and its Applications in Communications, IWSDA 2019, Dongguan, China, October 20-24, 2019*, pages 1–5. IEEE, 2019. 2, 2.4, 2.4.3

[74] K. Li, S. Mesnager, and L. Qu. Further study of 2-to-1 mappings over $\mathbb{F}_{2^n}$. *IEEE Trans. Inf. Theory*, 67(6):3486–3496, 2021. 2, 2.4, 2.4.9, 2.4.10, 2.4.11

[75] N. Li and S. Mesnager. Recent results and problems on constructions of linear codes from cryptographic functions. *Cryptogr. Commun.*, 12(5):965–986, 2020. 1.2.2

[76] S. Li, C. Li, C. Ding, and H. Liu. Two families of LCD BCH codes. *IEEE Trans. Inf. Theory*, 63(9):5699–5717, 2017. 1.2.3

[77] R. Lidl, H. Niederreiter, and P. M. Cohn. *Finite Fields*. Cambridge University Press, 1997. 2, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.1, 2.1.9, 3, 4.1, 4.1, 5.4.1

[78] Y. Liu, M. Shi, and P. Solé. Two-weight and three-weight codes from trace codes over. *Discret. Math.*, 341(2):350–357, 2018. 1.2.2

[79] W. Lu, X. Wu, X. Cao, and M. Chen. Six constructions of asymptotically optimal codebooks via the character sums. *Des. Codes Cryptogr.*, 88(6):1139–1158, 2020. 3, 3.1.20, 3.3.1

[80] G. Luo and X. Cao. New constructions of codebooks asymptotically achieving the welch bound. In *2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018*, pages 2346–2350. IEEE, 2018. 1.2.1, 3, 3.3.1

[81] G. Luo and X. Cao. Two constructions of asymptotically optimal codebooks via the hyper eisenstein sum. *IEEE Trans. Inf. Theory*, 64(10):6498–6505, 2018. 1.2.1, 2, 2.1.10, 2.1, 2.1.11, 2.1.12, 2.1.13, 3, 3.1.2, 3.3.1

[82] G. Luo, X. Cao, and X. Chen. MDS codes with hulls of arbitrary dimensions and their quantum error correction. *IEEE Trans. Inf. Theory*, 65(5):2944–2952, 2019. 1.2.3, 3, 3.3.1

[83] G. Luo, X. Cao, S. Xu, and J. Mi. Binary linear codes with two or three weights from niho exponents. *Cryptogr. Commun.*, 10(2):301–318, 2018. 1.2.2, 2.4

[84] J. L. Massey. Linear codes with complementary duals. *Discret. Math.*, 106-107:337–342, 1992. 1.2.3

[85] S. Mesnager. Linear codes with few weights from weakly regular bent functions based on a generic construction. *Cryptogr. Commun.*, 9(1):71–84, 2017. 1.2.2, 1.2.3, 1.2.3

[86] S. Mesnager. Linear codes from functions. In a Concise Encyclopedia of Coding Theory Press/Taylor and Francis Group (Publisher) London, New York (94 pages in Chapter 20), W. C. Huffman, J-L Kim and P. Solé (eds), 2021. 1.2.2

[87] S. Mesnager, F. Özbudak, and A. Sinak. Linear codes from weakly regular plateaued functions and their secret sharing schemes. *Des. Codes Cryptogr.*, 87(2-3):463–480, 2019. 1.2.2

[88] S. Mesnager, Y. Qi, H. Ru, and C. Tang. Minimal linear codes from characteristic functions. *IEEE Trans. Inf. Theory*, 66(9):5404–5413, 2020. 1.2.2

[89] S. Mesnager and A. Sinak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Trans. Inf. Theory*, 66(4):2296–2310, 2020. 1.2.2, 1.2.2

[90] S. Mesnager, C. Tang, and Y. Qi. Complementary dual algebraic geometry codes. *IEEE Trans. Inf. Theory*, 64(4):2390–2397, 2018. 1.2.3

[91] Y. Qi, C. Tang, and D. Huang. Binary linear codes with few weights. *IEEE Commun. Lett.*, 20(2):208–211, 2016. 1.2.2

[92] D. V. Sarwate. Meeting the welch bound with equality. In C. Ding, T. Helleseth, and H. Niederreiter, editors, *Sequences and their Applications - Proceedings of SETA 1998, Singapore, December 14-17, 1998*, Discrete Mathematics and Theoretical Computer Science, pages 79–102. Springer, 1998. 1.2.1

[93] N. Sendrier. Finding the permutation between equivalent linear codes: The support splitting algorithm. *IEEE Trans. Inf. Theory*, 46(4):1193–1203, 2000. 1.2.3

[94] N. Sendrier and G. Skersys. On the computation of the automorphism group of a linear code. In *Proceedings of the 2001 IEEE International Symposium on Information Theory, ISIT 2001, Washington, DC*, page 132001. IEEE, 2001. (document), 1.2.3

[95] M. Shi, Y. Guan, and P. Solé. Two new families of two-weight codes. *IEEE Trans. Inf. Theory*, 63(10):6240–6246, 2017. 1.2.2, 1.2.2

[96] M. Shi, D. Huang, and P. Solé. Optimal ternary cubic two-weight codes. *Chinese Journal of Electronic*, 27(4):734–738, 2018. 1.2.2

[97] M. Shi, Y. Liu, and P. Solé. Optimal two-weight codes from trace codes over $\mathcal{O}_2$+u$\mathcal{O}_2$. *IEEE Commun. Lett.*, 20(12):2346–2349, 2016. 1.2.2

[98] M. Shi, Y. Liu, and P. Solé. Optimal binary codes from trace codes over a non-chain ring. *Discret. Appl. Math.*, 219:176–181, 2017. 1.2.2

[99] M. Shi, L. Qian, and P. Solé. Few-weight codes from trace codes over a local ring. *Appl. Algebra Eng. Commun. Comput.*, 29(4):335–350, 2018. 1.2.2, 1.2.2

[100] M. Shi, L. Qian, and P. Solé. Few-weight codes from trace codes over a local ring. *Appl. Algebra Eng. Commun. Comput.*, 29(4):335–350, 2018. 1.2.2

[101] M. Shi, R. Wu, Y. Liu, and P. Solé. Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$. *Cryptogr. Commun.*, 9(5):637–646, 2017. 1.2.2, 1.2.2

[102] M. Shi, R. Wu, L. Qian, L. Sok, and P. Solé. New classes of p-ary few weight codes. *Bull. Malays. Math. Sci. Soc.*, 42:1393–1412, 2019. 1.2.2

[103] X. Shi, Q. Yue, and S. Yang. New lcd mds codes constructed from generalized reed-solomon codes. *J. Algebra Appl.*, 18:1950150, 2018. 1.2.3

[104] V. M. Sidelnikov. Some k-valued pseudo-random sequences and nearly equidistant codes. *Probl. Inf. Transm.*, 5:12–16. 1.2.1

[105] A. Sinak. Minimal linear codes from weakly regular plateaued balanced functions. *Discret. Math.*, 344(3):112215, 2021. 1.2.2

[106] H. Singh and K. C. Meena. Multi-twisted reed-solomon codes with small dimensional hull. *CoRR*, abs/2201.13108, 2022. 1.2.3

[107] N. J. A. Sloane and D. S. Whitehead. New family of single-error correcting codes. *IEEE Trans. Inf. Theory*, 16(6):717–719, 1970. 1.2.1

[108] L. Sok. MDS linear codes with one dimensional hull. *CoRR*, abs/2012.11247, 2020. 1.2.3

[109] L. Sok. On linear codes with one-dimensional euclidean hull and their applications to eaqeccs. *CoRR*, abs/2101.06461, 2021. 1.2.3

[110] L. Sok. A new construction of linear codes with one-dimensional hull. *Des. Codes Cryptogr.,https://doi.org/10.1007/s10623-021-00991-4*, 2022. 1.2.3

[111] T. Strohmer and R. W. Heath Jr. Grassmannian frames with applications to coding and communication. *Appl. Comput. Harmon. Anal.*, 14(3):257–275. 1.2.1

[112] P. Tan, Z. Zhou, and D. Zhang. A construction of codebooks nearly achieving the levenshtein bound. *IEEE Signal Process. Lett.*, 23:1306–1309, 2016. 1.2.1

[113] C. Tang, N. Li, Y. Qi, Z. Zhou, and T. Helleseth. Linear codes with two or three weights from weakly regular bent functions. *IEEE Trans. Inf. Theory*, 62(3):1166–1176, 2016. 1.2.2

[114] C. Tang, C. Xiang, and K. Feng. Linear codes with few weights from inhomogeneous quadratic functions. *Des. Codes Cryptogr.*, 83(3):691–714, 2017. 1.2.2

[115] D. Tang, C. Carlet, and Z. Zhou. Binary linear codes from vectorial boolean functions and their weight distribution. *Discret. Math.*, 340(12):3055–3072, 2017. 1.2.2, 6.1.4

[116] X. Wang, D. Zheng, and C. Ding. Some punctured codes of several families of binary linear codes. *IEEE Trans. Inf. Theory*, 67(8):5133–5148, 2021. 1.2.2, 1.2.2, 6.1.4, 6.1.11, 7.1

[117] X. Wang, D. Zheng, and Y. Zhang. Binary linear codes with few weights from boolean functions. *Des. Codes Cryptogr.*, 89(8):2009–2030, 2021. 1.2.2

[118] L. R. Welch. Lower bounds on the maximum cross correlation of signals (corresp.). *IEEE Trans. Inf. Theory*, 20(3):397–399, 1974. 1.2.1, 1.2.1

[119] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.*, 191(2):363–381, 1989. 1.2.1

[120] Y. Wu. Twisted reed-solomon codes with one-dimensional hull. *IEEE Commun. Lett.*, 25(2):383–386, 2021. 1.2.3

[121] Y. Wu, N. Li, and X. Zeng. Linear codes with few weights from cyclotomic classes and weakly regular bent functions. *Des. Codes Cryptogr.*, 88(6):1255–1272, 2020. 1.2.2

[122] P. Xia, S. Zhou, and G. B. Giannakis. Achieving the welch bound with difference sets. *IEEE Trans. Inf. Theory*, 51(5):1900–1907, 2005. 1.2.1

[123] C. Xiang, C. Ding, and S. Mesnager. Optimal codebooks from binary codes meeting the levenshtein bound. *IEEE Trans. Inf. Theory*, 61(12):6526–6535, 2015. 1.2.1

[124] C. Xiang, C. Tang, and C. Ding. Shortened linear codes from APN and PN functions. *IEEE Trans. Inf. Theory*, 68(6):3780–3795, 2022. 1.2.2

[125] M. Yamada. Difference sets over galois rings with odd extension degrees and characteristic an even power of 2. *Des. Codes Cryptogr.*, 67(1):37–57, 2013. 1.2.1, 3.3.1

[126] H. Yan, H. Liu, C. Li, and S. Yang. Parameters of LCD BCH codes with two lengths. *Adv. Math. Commun.*, 12(3):579–594, 2018. 1.2.3

[127] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Trans. Inf. Theory*, 52(1):206–212, 2006. 1.2.2

[128] M. Yuan, D. Zheng, and Y. Wang. Two-to-one mappings and involutions without fixed points over f2n. *Finite Fields Their Appl.*, 76:101913, 2021. 2, 2.4, 2.4.4, 2.4.5, 2.4.6, 2.4.7

[129] A. Zhang and K. Feng. Construction of cyclotomic codebooks nearly meeting the welch bound. *Des. Codes Cryptogr.*, 63(2):209–224, 2012. 1.2.1, 3

[130] A. Zhang and K. Feng. Two classes of codebooks nearly meeting the welch bound. *IEEE Trans. Inf. Theory*, 58(4):2507–2511, 2012. 1.2.1, 3, 3.1.12, 3.2.8, 3.3.1

[131] Z. Zhou, C. Ding, and N. Li. New families of codebooks achieving the levenstein bound. *IEEE Trans. Inf. Theory*, 60(11):7382–7387, 2014. 1.2.1

[132] Z. Zhou, N. Li, C. Fan, and T. Helleseth. Linear codes with two or three weights from quadratic bent functions. *Des. Codes Cryptogr.*, 81(2):283–295, 2016. 1.2.2

[133] Z. Zhou and X. Tang. New nearly optimal codebooks from relative difference sets. *Adv. Math. Commun.*, 5(3):521–527, 2011. 1.2.1, 3, 3.3.1

Research achievements

[1] **Liqin Qian** and Xiwang Cao. Bounds and optimal q-ary codes derived from the $\mathbb{Z}_q R$-cyclic codes. IEEE Transactions on Information Theory, 2019, 66(2): 923-935.

[2] **Liqin Qian**, Xiwang Cao, Wei Lu and Patrick Solé. A new method for constructing linear codes with small hulls. Designs, Codes and Cryptography, DOI: 10.1007/s10623-021-00940-1, 2021.

[3] **Liqin Qian**, Xiwang Cao and Sihem Mesnager. Linear codes with one-dimensional hull associated with Gaussian sums. Cryptography and Communications, 2021, 13: 225-243.

[4] **Liqin Qian** and Xiwang Cao. Gaussian sums, hyper Eisenstein sums and Jacobi sums over a local ring and their applications. Applicable Algebra in Engineering, Communication and Computing, https://doi.org/10.1007/s00200-021-00491-x, 2021.

[5] **Liqin Qian** and Xiwang Cao. Character sums over a non-chain ring and their applications. Advances in Mathematics of Communications, doi:10.3934/amc.2020134, 2021.

[6] Xiwang Cao and **Liqin Qian**. A recursive formula and an estimation for a specific exponential sum. Commun. Math. Res., 2021, 38(2): 184-205.

[7] Yingjie Cheng, Xiwang Cao, **Liqin Qian** and Jinlong Wan. Estimations on some hybrid exponential sums related to Kloosterman sums. Turk J Math., DOI: 10.3906/mat-2010-89, 2021.