BUTSON-HADAMARD CODES AND RELATED QUANTUM CODES

BUTSON-HADAMARD KODLAR VE İLGİLİ KUANTUM KODLAR

DAMLA ACAR

PROF. DR. BÜLENT SARAÇ

Supervisor

ASSOC. PROF. DR. OĞUZ YAYLA

Co-supervisor

Submitted to

Graduate School of Science and Engineering of Hacettepe University

as a Partial Fulfillment to the Requirements

for the Award of the Degree of Doctor of Philosophy

in Mathematics

July 2024

ABSTRACT

BUTSON-HADAMARD CODES AND RELATED QUANTUM CODES

Damla Acar

Doctor of Philosophy, Mathematics

Supervisor: Prof. Dr. Bülent SARAÇ

Co-supervisor: Assoc. Prof. Dr. OĞUZ YAYLA

July 2024, 117 pages

A Butson-Hadamard (BH) matrix H is a square matrix of dimension n whose entries are complex roots of unity such that $HH^* = nI$. In the first part of this thesis, we deal with codes obtained from BH matrices, called BH codes, focusing on their minimum distances. We first consider the usual Hamming distance and find lower bounds for distances of BH codes. Then we turn our attention to homogeneous weights, and search for distances of BH code families under these weights. Next, we introduce the notion of quasi-homogeneous weights as a generalization of homogeneous weights and show that certain BH codes equipped with quasi-homogeneous weights are Plotkin optimal. In addition, we obtain distances of BH codes under certain quasi-homogeneous weights. Our results are applied to determine parameters of p-ary codes projected under Gray isometries from BH codes over $\mathbb{Z}_{p^e}$, where p is a prime number and $e \geq 2$ is an integer. In the second part of this thesis, we study quantum stabilizer codes and give two constructions. In particular, we give a constructive proof to show that if there exist a classical linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ of dimension k and a classical linear code $\mathscr{D} \subseteq \mathbb{F}_{q^k}^m$ of dimension s, where q is a power of a prime number p, then there exists an $[\![nm, ks, \delta]\!]_q$ quantum stabilizer code with δ determined by $\mathscr{C}$ and $\mathscr{D}$ by identifying the stabilizer group of the code. In the construction, we use a particular type of Butson

Hadamard matrices equivalent to multiple Kronecker products of the Fourier matrix of order p. We also consider the same construction of a quantum code for a general normalized Butson Hadamard matrix and search for a condition for the quantum code to be a stabilizer code.

Keywords: Butson-Hadamard matrices; BH-codes; generalized Gray map; Plotkin bound; quantum stabilizer codes.

ÖZET

BUTSON-HADAMARD KODLAR VE İLGİLİ KUANTUM KODLAR

Damla Acar

Doktora, Matematik

Danışman: Prof. Dr. Bülent SARAÇ

Eş Danışman: Doç. Dr. OĞUZ YAYLA

Ocak 2024, 117 sayfa

n boyutlu bir Butson-Hadamard matrisi, H, girişleri birimin karmaşık kökleri olan ve $HH^* = nI$ koşulunu sağlayan bir kare matristir.

Bu tez çalışmasının birinci kısmında Butson-Hadamard matrislerinden elde edilen kodlar ve bu kodların minimum uzaklığı üzerine bazı sınırlar kanıtlanmıştır. Ayrıca yarı-homojen ağırlık kavramı tanımlanıp bu ağırlık altında BH-matrislerden elde dilen kod ailelerinin minimum uzaklıkları incelenmiştir. Modifiye Butson-Hadamard matrislerinden elde edilen kodların parametreleri homojen olmayan Gray dönüşüm altında verilmiş ve bu kodların Plotkin optimal olduğu sonucuna ulaşılmıştır. Tezin ilk kısmında, BH matrislerinden elde edilen, BH kodları olarak adlandırılan kodlar ele alınarak bu kodların minimum uzaklıkları ile ilgili sonuçlar elde edilmiştir. İlk olarak, bilinen Hamming uzaklığı ele alınarak BH kodlarının uzaklıkları için alt sınırlar verilmiştir. Ardından homojen ağırlıklar göz önüne alınıp bu ağırlıklar altında BH kod ailelerinin uzaklıkları incelenmiştir. Daha sonra, homojen ağırlıkların genelleştirmesi olarak kabul edilen yarı-homojen ağırlık kavramı tanıtılmıştır. Ayrıca bu ağırlıklar altında belirli BH kodlarının Plotkin-optimal olduğu gösterilmiştir. Daha sonra belirli yarı-homojen ağırlıklar altında BH kodlarının mimimum uzaklıkları elde

edilmiştir. Elde edilen sonuçlar p asal sayısı $e \geq 2$ için $\mathbb{Z}_{p^e}$ üzerindeki BH kodlarından Gray dönüşümü altında p-ary kodların parametrelerini belirlemek için uygulanmıştır. İkinci kısımda ise BH matrisler ile kuantum kodları arasındaki bağlantıyı belirlemek adına kuantum sabitleyen kodları çalışılarak iki kuantum kod yapısı verilmiştir. p bir asal sayı ve q, p'nin bir kuvveti olsun. Sırasıyla $\mathscr{C} \subset \mathbb{F}_q^n$ ve $\mathscr{D} \subset \mathbb{F}_{q^k}^m$ k ve s boyutlu iki lineer kod ise o zaman sabitleyen grubu ile tanımlanan ve $\mathscr{C}, \mathscr{D}$ ile belirli δ ile bir $[\![nm, ks, \delta]\!]_q$ kuantum sabitleyen kodunun varlığı kanıtlanmıştır. Bu kodu oluşturuken p boyutlu Fourier matrislerin Kronecker çarpımlarına denk olan Butson-Hadamard matrisler kullanılmıştır. Aynı zamanda genel bir normalleştirilmiş Butson-Hadamard matrisi için bir kuantum kodu yapısı ele alınarak kuantum kodunun sabitleyen bir kod olması için gerekli olan koşullar araştırılmıştır.

Keywords: Butson-Hadamard matrisler; kodlar; genelleştirilmiş Gray dönüşümü; Plotkin sınır; kuantum sabitleyen kodları.

ACKNOWLEDGEMENTS

First and foremost, I would like to sincerely thank my valuable advisors Prof. Dr. Bülent SARAÇ and Assoc. Prof. Dr. Oğuz YAYLA for patiently sharing their knowledge and experinces with me, for always encouraging and guiding me throughout my doctoral education, and for their invaluable advice.

I also extend my heartfelt thanks to the jury members Prof. Dr. Mesut ŞAHİN, Prof. Dr. Zülfükar SAYGI, Prof. Dr. Burcu GÜLMEZ TEMUR, Prof. Dr. Pınar AYDOĞDU, and Asst. Prof. Dr. Emrah Sercan YILMAZ for their valuable time and insights.

I would like to thank my dear colleagues Yağmur ÇAKIROĞLU and Sibel KURT, who have always supported me and never withheld their help during my thesis work.

To my dear father Yılmaz ACAR, who introduced a four year old girl to mathematics and has been one of my greatest supporters at every stage of my life, my dear mother Nahide ACAR, who is a source of strength and patience for of all us and has always stood behind my decisions with her unconditional love, and my dear brother Kemal Burak ACAR, who always made me feel his love and support and has been a light in my darkest times, I express my deepest gratitude.

I would like yo sincerely thank The Scientific and Technological Research Council of Turkey(TÜBİTAK) for the scholarship provided under the 2211-National PhD Scholarship Programs.

Finally, I wish to express my deepest gratitude to Council of Higher Education(YÖK) for providing the scholarship under YOK $100/2000$ PhD Scholarship Program.

GENİŞLETİLMİŞ ÖZET

Giriş

Kodlama teorisi, Claude Shannon tarafından 1948 yılında temelleri "A Mathematical Theory of Communication" çalışması ile atılan ve kriptografi, verilerin depolanması ve iletilmesi, hata düzeltme, uydu ve uzay iletişimi, DNA dizilimi gibi pek çok farklı alanda uygulaması olan bir disiplindir. Veri iletiminin gerçekleştiği fiziksel ortama kanal adı verilir. Kanal olarak telefon hatları, kompakt disk yüzeyleri kullanılabileceği gibi atmosfer ve uzay da kullanılabilir. Shannon çalışmasında kanal kapasitesi olarak adlandırılan bir sayı belirlemiş ve bu sayının altındaki oranda güvenilir bir iletişimin mümkün olduğunu kanıtlamıştır.

Kanal boyunca bilginin iletilmesi esnasında çeşitli nedenlerden dolayı bozulmalar meydana gelebilir. Eğer herhangi bir bozulma olmazsa bilgiler aynı şekilde iletilir ancak pratikte bu durum mümkün değildir. Bu nedenle kodlama teorisi kanaldaki gürültüden kaynaklı iletim hatalarının belirlenmesi ve mümkünse düzeltilmesi problemi ile ilgilenir.

Bilgilerin hızlı bir şekilde kodlanması ya da başka bir deyişle kanala uygun hale getirilmesi, kodlanmış bilgilerin kolayca iletilmesi, alınan mesajların hızlı bir şekilde dekodlanması, kanalda meydana gelen hataların düzeltilmesi ve birim zamanda maksimum bilginin iletilmesi kodlama teorisinin temel amaçlarıdır.

Kodlama işlemi için bilginin kanala uygun olacak şekilde sembollerle ifade edilmesi gerekir. Bu amaçla kullanılan sembollerin sonlu bir $\mathcal{A}$ kümesine alfabe ve $\mathcal{A}$ nın elemanlarına kod sembolü denir. Alfabe olarak genelde p bir asal olmak üzere $\mathbb{F}_p$ sonlu cismi kullanılmasına rağmen Z_k sonlu halkaları üzerindeki kodlar da literatürde oldukça fazla çalışılmıştır. Tez çalışmamızda Z_k üzerindeki kodları ele alacağız. n bir pozitif tamsayı olmak üzere, girişleri $\mathcal{A}$ kümesinin elemanları olan n-uzunluklu bir vektöre n-uzunluklu bir sözcük denir. n-uzunluklu bir C kodu, $\mathcal{A}^n$ in boştan farklı bir alt kümesidir ve C nin elemanları da n-uzunluklu kod sözcükleri olarak adlandırılır.

C, n-uzunluklu bir kod olmak üzere, herhangi bir $c = c_1c_2 \dots c_n \in C$ kod sözcüğünün Hamming ağırlığı sıfırdan faklı koordinatlarının sayısıdır ve $\mathrm{wt}(c)$ ile göstetilir. C kodundaki herhangi iki farklı $c = c_1c_2 \dots c_n,\ b = b_1b_2 \dots b_n$ kod sözcüğünün $d(b, c)$ şeklinde gösterilen Hamming uzaklığı ise b ve c nin farklı koordinatlarının sayısıdır. C kodunun farklı kod sözcüklerinin uzaklıklarının mimimum değerine kodun minimum uzaklığı denir ve $d(C)$ ile gösterilir.

Shannon ın çalışması güvenilir bir iletişimin mümkün olduğunu söylemesine rağmen bunun nasıl yapılacağı ilk kez Richard W. Hamming tarafından [1] çalışmasında gösterilmiştir. Eğer alınan mesaj kod sözcüğü değilse o zaman iletim esnasında bir hataya maruz kaldığı açıktır. Dolayısıyla hata belirlenebilir. Fakat alınan mesaj kod sözcüklerinden biri ise o zaman hata belirlenemeyebilir. Örneğin; C kodu olarak $\mathbb{F}_2^4$ uzayını alalım ve 0100 mesajını alıcıya gönderelim. İletim sonunda alıcının 1100 mesajını aldığını varsayalım. O halde $1100 \in C$ olduğundan alıcı herhangi bir hata meydana gelmediğini ve gönderilen mesajın 1100 olduğunu düşünebilir. Dolayısıyla bu durumda hata belirlenemez.

$C = \{00000, 01011, 10101, 11110\}$ kodu için alınan mesajın $r = 10000$ olduğunu varsayalım. O halde 10000, C nin bir elemenı olmadığı için hatalı iletildiği açıktır. Dolayısıyla r mesajı kendine en yakın olan kod sözcüğü olarak düzeltilir. Dolayısıyla

$$d(10000, 00000) = 1, d(10000, 01011) = 4, d(10000, 10101) = 2, d(10000, 11110) = 3$$

olduğundan 10000 mesajı 00000 şeklinde düzeltilir. Eğer alınan mesaj $r = 00011$ ise o zaman

$$d(00111, 00000) = 3, d(00111, 01011) = 2, d(00111, 10101) = 2, d(00111, 11110) = 3$$

olacağından gönderilen mesaj için iki olasılık vardır. Bu nedenle mesaj üzerinde meydana gelen hata düzeltilemez.

t bir pozitif tamsayı olmak üzere, bir C kodu, kod sözcükleri üzerindeki t veya daha az sayıda hatayı düzeltebiliyorsa bu koda t-hata düzeltici kodu denir. Kodların belirleyebilecekleri

ve düzeltebilcekleri hata miktarları minimum uzaklıklarına bağlı olarak verilir. Minimum uzaklığı d olan bir kod $t \leq \lfloor (d-1)/2 \rfloor$ için t hata düzeltici ve $(d-1)$ hata belirleyici koddur.

M adet kod sözcüğü içeren n uzunluklu bir kodun minimum uzaklığı d ise o zaman bu kod (n, M, d) şeklinde gösterilir. Kodlama teorisinin temel amaçları göz önüne alındığında kodlama işleminin hızlı olması için kodun uzunluğu küçük ve birim zamanda fazla bilginin iletilmesi için M değeri büyük olmalıdır. Ayrıca fazla sayıda hatanın düzeltilebilmesi d sayısının büyük olması ile mümkün olur.

Kolay kodlama ve dekodlama işlemlerine sahip olduğu için lineer kodlar kodlama teorisinde önemli bir yere sahiptir. $\mathbb{Z}_k$ üzerindeki n-uzunluklu bir lineer kod $\mathbb{Z}_k^n$ uzayının bir altmodülüdür. Bu tez çalışmasında, $\mathbb{Z}_k$ sonlu halkası üzerinde genel olarak lineer olmayan kodlar ele alınmış ve bu kodların Hamming ağırlığı, homojen ağırlıklar ile onların bir genellemesi olarak tanımladığımız yarı-homojen ağırlık (quasi-homogeneous) gibi farklı ağırlıklara göre minimum uzaklıkları çalışılmıştır.

Homojen ağırlık kavramı I. Constantinescu ve W. Heise tarafından 1997 yılında ilk kez [2] çalışmasında tanıtılmıştır. Sonlu bir R halkası üzerinde tanımlı reel değerli bir w fonksiyonu $w(0) = 0$ olmak üzere aşağıdaki iki koşulu sağlasın,

(i) x ile y, R halkasının iki farklı elemeanı olsun. O halde $Rx = Ry$ ise o zaman $w(x) = w(y)$.

(ii) x, R halkasının sıfırdan farklı bir elemanı olmak üzere

$$\sum_{y \in Rx} w(y) = \gamma |Rx|$$

olacak şekilde bir γ reel sayısı vardır. O zaman w fonksiyonuna bir homojen ağırlık denir ve γ, w ağırlığının R üzerindeki ortalama değeri olarak adlandırılır.

$\mathbb{Z}_k$ üzerinde tanımlı ve parametreleri (n, M, d) olan bir C kodunu ortalama değeri γ olan Z_k^n üzerindeki bir homojen ağırlından elde edilen uzaklık fonksiyonu ile ele alalım. O halde eğer

$d > \gamma n$ ise o zaman $M \leq d/(d-\gamma n)$ genelleştirilmiş Plotkin sınırı sağlanır ve $M > d/(d-\gamma n) - 1$ ise o zaman C koduna Plotkin-optimaldir denir. Bu tezde $\mathcal{A}_k$ olarak tanımlanan kodun homojen ağırlık altında Plotkin-optimal olduğu M. Greferath, G.McGuire ve M. E. O'Sullivan tarafından kanıtlanmıştır (bknz. [3]).

Nordstrom-Robinson, Kerdock, Preparata ve Goethals gibi lineer olmayan kodlar $\mathbb{Z}_4$ üzerindeki lineer kodların Gray dönüşüm altında ikili (binary) görüntüleri olarak inşa edilebilir [4]. Daha sonra Gray dönüşümler Z_p^e halkasına genellenerek [5], sadece ikili kodlar ile sınırlı kalmamıştır. Böylece Z_{p^e} halkası üzerinde Gray dönüşümler ile ağırlık fonksiyonları üretilebilir. Gray dönüşümün M. Greferath ve S. E. Schmidt tarafından verilen $\mathbb{Z}_{p^e}$ üzerine genellemesi aşağıdaki gibidir, $u \in \mathbb{Z}_{p^e}$ elemanının p-ary gösterimi $u_i \in \mathbb{Z}_p$ olmak üzere $u = \sum_{i=0}^{e-1} u_i p^i$ şeklinde olsun. O halde $\mathbf{1}$ tüm girişleri 1 olan p^{e-1} uzunluklu vektör ve Y, sütunları $\mathbb{Z}_p^{e-1}$ uzayının farklı vektörleri olan $(e-1) \times p^{e-1}$ matris olmak üzere

$$G_1 : \mathbb{Z}_{p^e} \to \mathbb{Z}_p^{p^{e-1}}, G_1(u) = (u_0, \ldots, u_{e-2})Y + u_{e-1}\mathbf{1}_{e-1}. \tag{1}$$

Dahası $G_1 : \mathbb{Z}_{p^e}^n \to (\mathbb{Z}_p^{p^{e-1}})^n$ olacak şekilde bileşensel olarak genişletebiliriz ve bunu yine G_1 ile göstereceğiz.

w_h ve d_h sırasıyla Hamming ağırlık ve Hamming uzaklığı göstersin. G_1 Gray dönüşümü ve w_h ağırlığı kullanarak $\mathbb{Z}_{p^e}$ halkası üzerinde bir $w_1(u) = w_h(G_1(u))$ ağırlığı tanımlayalım. O halde G_1, $(\mathbb{Z}_{p^e}^n, d_1)$ üzerinde uzaklık koruyan bir dönüşüm olur öyle ki

$$d_1(x, y) = \sum_{i=1}^{n} w_1(y_i - x_i)$$

$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{Z}_{p^e}^n$ ve w_1 ağırlığından türetilen uzaklık fonksiyonudur. Ayrıca w_1, ortalama değeri $\gamma = (p-1)p^{e-2}$ olan bir homojen ağırlıktır.

Kuantum Kodlama Teorisi

Kuantum mekaniği yasalarına göre çalışan kuantum bilgisayarların klasik bilgisayarlara göre hesaplama gücünün daha iyi olup olmayacağı düşüncesi 1980 li yılların başından itibaren çalışılmıştır. Peter Shor, 1994 yılında [6] çalışmasında kuantum bilgisayarlar kullanılarak büyük tam sayıların asal çarpanlarına etkili bir şekilde ayrılabileceğini göstermiştir. Asal çarpanlara ayırma probleminin zorluğuna dayanan RSA gibi şifreleme algoritmaları internet işlemlerinin güvenliğini sağladığından, Shor tarafından elde edilen sonuç kuantum bilgisayarlara olan ilgiyi artırmıştır.

Klasik bilgi teorisinin temel birimi bitlerdir. Bilgi bitlerde depolanır ve işlenir. Kuantum bilgi teorisinde ise bilgi, bitler yerine kuantum bit ya da kısaca kübit adı verilen birimlerde saklanır. Bitler 0 ve 1 ile temsil edilirken kübitler iki boyutlu bir Hilbert uzayın ($\mathcal{H}_2$) vektörleri ile temsil edilir. Bu tezde Hilbert uzayı olarak kompleks vektör uzayı alınarak hem iki boyutlu hem de daha yüksek boyutlu kuantum sistemler (küditler) çalışılmıştır.

$\mathbb{F}_q$, q-elemanlı sonlu cismi ve standart iç çarpım ile q-boyutlu $\mathbb{C}^q$ vektör uzayını alalım. Vektör uzayın bir ortonormal tabanı $\{|0\rangle, |1\rangle, \ldots, |q-1\rangle\}$ olsun. O halde bir küditin durumu $\mathbb{C}^q$ uzayının bir vektörüdür ve dolayısıyla taban elemanlarının bir lineer kombinasyonu olarak yazılabilir. O halde bir $|\psi\rangle$ küditin durumu $|\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{q-1}|^2 = 1$ olmak üzere aşağıdaki gibidir,

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{q-1} |q-1\rangle .$$

Kuantum bilgi teorisinin klasik bilgi teorisinden ayrıldığı bir diğer nokta q-ary bir klasik sistemde bitler $0, 1, \ldots, q$ durumlarında sadece birinde iken küditler $|0\rangle, |1\rangle, \ldots, |q-1\rangle$ durumlarının yanında bunların bir lineer kombinasyonu olan süperpozisyonunda da olabilir.

Küditler, kübitlere göre daha büyük bir durum uzayına sahip oldukları için daha fazla bilgi temsil ederler dolayısıyla kuantum bilginin depolanması ve işlenmesi için kübitlere göre daha elverişlidirler. Dahası birden fazla küdit içeren bir kuantum sistem ile aynı anda birden fazla

durum temsil edileceği için kuantum hesaplama daha etkili bir şekilde gerçekleşir. n-küdit içeren bir kuantum sistem $\mathbb{C}^q$ uzayının n kez tensör çarpılmasıyla elde edilir. n-küditlerin bir kümesine kuantum register denir. Bir küditte olduğu bir n-küditin durumu $(\mathbb{C}^q)^{\otimes n}$ uzayının ortonormal taban elemanlarının lineer kombinasyonu şeklindedir. Kübitin hesaplamalı taban elemanlarının n-kez tensör çarpılmasıyla elde edilen

$$\mathcal{B} = \{|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle \,|x_i \in \mathbb{F}_q, 1 \leq i \leq n\}$$

kümesi $(\mathbb{C}^q)^{\otimes n}$ uzayı için bir ortonormal taban olur. Taban elemanlarını ise $|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle$ yerine $|x_1 x_2 \ldots x_n\rangle$ şeklinde göstereceğiz.

Küditler süperpozisyon halinde olabilir bu yüzden durumları hakkında bilgi edinmek için ölçmemiz gerekir. Ölçüm sonucunda küdit taban durumlarından birine çöker ve süperpozisyon durumu bozulur. Böylece ölçüm sonucunda klasik bilgi elde edilir. Hangi taban durumuna çökeceği süperpozisyon durumundaki katsayılara bağlı olarak değişir. Daha açık bir şekilde ifade edersek; $(\mathbb{C}^q)^n$ uzayının alt uzaylarının bir $\mathcal{O} := \{M_1, \ldots, M_s\}$ kümesi, $i \neq j$ için $M_i \perp M_j$ ve $(\mathbb{C}^q)^n = M_1 \oplus M_2 \oplus \ldots \oplus M_s$ sağlıyorsa o zaman $\mathcal{O}$ kümesine bir gözlenebilir (observable) denir. O halde bir n-küditin herhangi bir $|\psi\rangle$ durumu, $|\psi_i\rangle$, $|\psi\rangle$ durumunun M_i alt uzayı üzerine izdüşümü olacak şekilde tek türlü $|\psi\rangle = \sum_{i=1}^{s} \alpha_i |\psi_i\rangle$ yazılır. $P_i : (\mathbb{C}^q)^n \to M_i, |\psi\rangle \to |\psi_i\rangle$ olsun. O halde $|\psi\rangle$ durumu $p(i) = |P_i \,||\psi\rangle|^2$ olasılıkla M_i alt uzayındadır ve ölçüm sonucu ise i olur. Ölçümden sonra n-küdit

$$|\psi_i\rangle = \frac{P_i \,|\psi\rangle}{\sqrt{p(i)}}$$

durumuna çöker.

Bir n-küditin bir durumunun ölçümünü örnekle açıklayalım. $q = 3$ ve $n = 2$ olmak üzere $(\mathbb{C}^q)^n$ uzayının $\mathcal{B} = \{|0\rangle = |00\rangle, |1\rangle = |01\rangle, |2\rangle = |02\rangle, |3\rangle = |10\rangle, |4\rangle = |11\rangle, |5\rangle = |12\rangle, |6\rangle = |20\rangle, |7\rangle = |21\rangle, |8\rangle = |22\rangle\}$ hesaplamalı tabanı ele alalım. Burada, $|0\rangle = (100)^T, |1\rangle = (010)^T, |2\rangle = (001)^T$ olmak üzere $|0\rangle := |00\rangle = |0\rangle \otimes |0\rangle = (100000000)^T$ olur ve diğer taban elemanları da benzer şekilde hesaplanır. $\sum_{i=1}^{8} |\alpha_i|^2 = 1$ olacak şekilde

2-küditin bir $|\psi\rangle = \sum_{i=0}^{8} \alpha_i |i\rangle$ durumunu ele alalım. O halde birinci küditi ölçmek için

$$M_0 = \mathrm{Span}_{\mathbb{C}}\{|00\rangle, |01\rangle, |02\rangle\},$$
$$M_1 = \mathrm{Span}_{\mathbb{C}}\{|10\rangle, |11\rangle, |12\rangle\},$$
$$M_2 = \mathrm{Span}_{\mathbb{C}}\{|20\rangle, |21\rangle, |22\rangle\}.$$

olmak üzere $\mathcal{O}_1 = \{M_0, M_1, M_2\}$ gözlenebilirini ele alalım. Ölçümden sonra $p_0 = \sum_{i=0}^{2} |\alpha_i|^2$ olasılıkla 0 elde edilir ve 2-küdit

$$\frac{\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |02\rangle}{\sqrt{|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2}}$$

durumuna çöker. Benzer şekilde ölçüm sonucunda $p_1 = \sum_{i=3}^{5}$ olasılık ile 1 elde edilir ve 2-kübit

$$\frac{\alpha_3 |10\rangle + \alpha_4 |11\rangle + \alpha_5 |12\rangle}{\sqrt{|\alpha_3|^2 + |\alpha_4|^2 + |\alpha_5|^2}}$$

durumuna çöker. İkinci küditi ölçmek için ise

$$M_3 = \mathrm{Span}_{\mathbb{C}}\{|00\rangle, |10\rangle, |20\rangle\},$$
$$M_4 = \mathrm{Span}_{\mathbb{C}}\{|01\rangle, |11\rangle, |21\rangle\},$$
$$M_5 = \mathrm{Span}_{\mathbb{C}}\{|02\rangle, |12\rangle, |22\rangle\}.$$

olmak üzere $\mathcal{O}_2 = \{M_3, M_4, M_5\}$ gözlenebiliri kullanılır ve yukarıdakine benzer şekilde ölçüm çıktısı ile olasılığı ve ölçüm sonucunda 2-küditin çöktüğü durum bulunabilir.

Kuantum Hata Belirleme ve Düzeltme

Klasik bilgi teorisinde olduğu gibi kuantum bilgi teorisinde de gürültülü bir ortamda bilginin iletilmesi veya depolanması problemi üzerine çalışılır. Kuantum bilginin dekoherans adı verilen çevresel etkileşimler ve diğer nedenlerden dolayı oluşabilecek gürültüden korunması

gerekir. Klasik bilgide sadece bit hatalarını düzeltmek gerekirken burada bit hatalarının yanı sıra faz hatalarının da düzeltilmesi gerekir. Dolayısıyla klasik duruma göre düzeltilmesi gereken hata uzayı çok daha büyüktür. Diğer bir zorluk ise küditin durumu üzerinde meydana gelecek hataları düzeltmek için o durumu ölçmemiz gerekir. Fakat ölçümler yukarıda bahsettiğimiz gibi durumu çökertebilir bu da durumun değişmesine neden olur. Son olarak klasik kodlarda hata düzeltmek için en basit hata düzeltme kodlarından olan tekrarlı kodlar kullanılır. 0 mesajının 000 ve 1 mesajının 111 şeklinde kodlandığı 3-tekrarlı kodu göz önüne alırsak 000 kod sözcüğünün ikinci bitinde bir hata meydana gelirse elde edilecek 010 iletisini majority vote kod çözme yöntemini kullanılarak 000 şeklinde düzeltebiliriz. Fakat kuantum kodlar için bu durum no-cloning teorem ile geçerli değildir. Tüm bu sebeplerden dolayı kuantum hata düzeltmenin mümkün olmadığı düşünülüyordu. Fakat 1995 yılında Shor tarafından, 1 kübit bilgiyi 9 kübite kodlayan ve herhangi 1 kübit (kuantum bit) üzerindeki rastgele bir hatayı düzeltebilen kuantum kodun [7] tanıtılmasıyla kuantum hata düzletme kodlarına olan ilgi artmıştır. Aynı yıl içerisinde bağımsız olarak Andrew Steane tarafından herhangi 1-kübit hatayı düzeltebilen 7-kübit kod [8] tanıtılmıştır. Ayrıca Bennett ve diğerleri 1 kübit bilgiyi 5-kübite kodlayan ve 1 kübit üzerindeki hatayı düzeltebilen kod tasarladılar (bknz. [9]).

Bir kuantum kodu tasarlamadan önce hangi tür hatalar ile karşı karşıya olacağımızı belirlemek, o hatalara uygun hata düzeltme yöntemlerini geliştirmek adına önem teşkil eder. Bunun yanı sıra bazı kuantum kodlar belirleyebilecekleri ya da düzeltebilecekleri hatalara göre tasarlanır. Dolayısıyle öncelikle çalışacağımız kuantum kodlara uygun hata modelini tanıtacağız.

q bir p asalının bir kuvveti olmak üzere n-uzunluklu bir q-ary kuantum kod, $(\mathbb{C}^q)^{\otimes n}$ uzayının bir alt uzayıdır ve $[\![n, k, d]\!]_q$ şeklinde gösterilir. $a, b \in \mathbb{F}_q$ ve ω birimin p-inci dereceden bir ilkel kökü olmak üzere $X(a)$, $Z(b)$ hataları $\mathbb{C}^q$ uzayı üzerinde unitary operatörlerdir ve aşağıdaki gibi tanımlanır:

$$X(a)\,|x\rangle := |x + a\rangle\,, \quad Z(b)\,|x\rangle := \omega^{tr(bx)}\,|x\rangle\,.$$

burada tr fonksiyonu $\mathbb{F}_q$ uzayından $\mathbb{F}_p$ uzayına iz fonksiyonudur.

Hataların aşağıda verilen özelliklere sahip bir $\mathcal{E} = \{X(a)Z(b) \mid a, b \in \mathbb{F}_q\}$ kümesini ele alalım.

(i) I birim matrisini içerir,

(ii) İki farklı elemanının çarpımı başka bir elemanın skaler bir katıdır,

(iii) Herhangi iki farklı $A, B \in \mathcal{E}$ elemanı için $\mathrm{tr}(A^\dagger B) = 0$ sağlanır.

q^2 üniter matrisin yukarıdaki özelliklere sahip bir kümesine bir iyi hata tabanı (nice error basis) denir. Bir küdit üzerinde tanımlı bu hata operatörlerini n-küdit üzerine genişletmek için iki iyi hata tabanının tensör çarpımının da yine bir iyi hata tabanı olduğu gerçeğinden faydalanabiliriz (bknz. [10]). Dolayısıyla, $X(a) = X(a_1) \otimes \ldots \otimes X(a_n)$ ve $Z(b) = Z(b_1) \otimes \ldots \otimes Z(b_n)$ olacak şekilde

$$\mathcal{E}_n = \{X(a)Z(b) | a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n\}$$

kümesi bir n-küdit için bir iyi hata tabanıdır. Örneğin, i kompleks birim olmak üzere bir kübitin hesaplamalı taban durumları üzerindeki etkisi

$$\begin{aligned}
\sigma_x |0\rangle &= |1\rangle\,,\ \sigma_x |1\rangle = |0\rangle \\
\sigma_z |0\rangle &= |0\rangle\,,\ \sigma_z |1\rangle = -|1\rangle \\
\sigma_y |0\rangle &= -i|1\rangle\,,\ \sigma_y |1\rangle = i|0\rangle
\end{aligned}$$

şeklinde olan 2×2 Pauli matrislerinin $\mathcal{G}_1 = \{I_2, \sigma_x, \sigma_y, \sigma_z\}$ kümesi $\mathbb{C}^2$ uzayı üzerinde bir iyi hata tabanıdır. Burada σ_x bit-değiştirme hatası ve σ_z faz-değiştirme hatası olarak da adlandırılır. Ayrıca $\sigma_y = -i\sigma_x\sigma_z$ olduğunu kolayca söyleyebiliriz. Bu hata tabanını n-kübit üzerine $\mathcal{G}_n = \{E_1 \otimes \ldots \otimes E_n \mid E_i \in \mathcal{G}_1\}$ olacak şekilde genişletebiliriz.

İlk kuantum hata düzeltme kodu Shor tarasından 1995 yılında tanıtılan 9-kübit koddur. 1-kübit bilgi 9-kübite kodlanır. Ayrıca 3-kübit bit değiştirme kodu ile 3-kübit faz değiştirme

kodunun birleşiminden oluşur. Bu kod üzerinden kodlama ve kod çözme adımlarını ele alalım.

3-kübit bit değiştirme kodu hesaplamalı taban durumları olan $|0\rangle$ ve $|1\rangle$ durumlarını aşağıdaki gibi kodlar ve böylece no-cloning teorem ile çelişmez,

$$|0\rangle \to |000\rangle\,, \qquad |1\rangle \to |111\rangle\,.$$

Dolayısıyla herhangi bir $\alpha\,|0\rangle + \beta\,|1\rangle$ kübit durumu $\alpha\,|000\rangle + \beta\,|111\rangle$ şeklinde kodlar.

3-kübit faz değiştirme kodunu kullanarak taban durumlarını $|0\rangle \to |+++\rangle\,, |1\rangle \to |---\rangle$ olacak şekilde kodlarız.

Burada

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

O halde 9-kübit kodu oluştururken öncelikle 3-kübit faz-değiştime kodu kullanarak hesaplamalı taban durumlarını $|0\rangle \to |+++\rangle$ ve $|1\rangle \to |---\rangle$ olarak kodlarız ve daha sonra bu kübitleri 3-kübit bit-değiştirme kodu kullanarak $|+\rangle \to |000\rangle + |111\rangle$ ve $|-\rangle \to |000\rangle - |111\rangle$ şeklinde kodlarız.

O halde $|0\rangle_L$ ve $|1\rangle_L$ sırasıyla $|0\rangle$ ve $|1\rangle$ durumlarının mantıksal durumlarını göstermek üzere Shor kodunun kod sözcükleri aşağıdaki gibidir,

$$\begin{aligned} |0\rangle \to |0_L\rangle &= \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\ |1\rangle \to |1_L\rangle &= \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \end{aligned}$$

İletim sırasında meydana gelebilecek herhangi bir hata durumunda hata düzeltme adımlarını açıklayalım. Bunun için öncelikle bir-değiştirme hatası σ_x meydana gelirse nasıl düzeltileceğini ele alalım. 3-kübit bit-değiştirme kodunu göz önüne alırsak $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ durumunun $|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$ şeklinde kodlanacağını biliyoruz. Hatanın meydana gelip gelmediğini anlamak için durumu ölçmemiz gerekir. Bu nedenler

$$H_0 = \mathrm{Span}_{\mathbb{C}}\{|000\rangle, |111\rangle\}, \quad H_1 = \mathrm{Span}_{\mathbb{C}}\{|100\rangle, |011\rangle\},$$
$$H_2 = \mathrm{Span}_{\mathbb{C}}\{|010\rangle, |101\rangle\}, \quad H_3 = \mathrm{Span}_{\mathbb{C}}\{|001\rangle, |110\rangle\}.$$

olmak üzere $\mathcal{O} = \{H_0, H_1, H_2, H_3\}$ gözlenebilirini alalım. O halde ölçüm sonucunda durum 0 elde edersek ya da başka bir deyişle $|\psi'\rangle \in H_0$ ise herhangi bir hata meydana gelmemiştir. Fakat eğer ölçüm sonucu i ise o zaman i-inci bitte hata meydana gelmiştir sonucunu elde ederiz. Düzeltmek için ise i-inci bite tekrar σ_x uygularız. Faz hatalarını düzeltmek için 3-kübit faz-değiştirme kodu, $Q = \mathrm{Span}_{\mathbb{C}}\{|+++\rangle, |---\rangle\}$ ele alalım. Bit değişme hataları için ele aldığımız gözlenebilire benzer bir gözlenebilir alıp aynı işlemleri yaparak faz değişme hatalarını düzeltebiliriz.

Kuantum Sabitleyen Kodları

Kuantum hata düzeltme kodları arasında önemli bir yere sahip olan kuantum sabitleyen kodlar birbirlerinden bağımsız olarak Daniel Gottesman [11] ile Calderbank ve diğerleri [12] tarafından 1990 lı yılların başında tanıtılmıştır. Böylece kuantum hata düzeltme kodlarının tanımlanması ve analizi için sistematik bir yol belirlemişlerdir. Klasik lineer kodlarla yakından ilişkilidir ve bu sayede klasik yöntemler ile analiz edilebilirler. Bu sebeplerden dolayı toplamsal kodlar olarak da adlandırılırlar.

Calderbank ve diğerleri [13] kuantum sabitleyen kodun hata düzeltme performansının dual kodları tarafından kapsanan (self-orthoganal) klasik ikili (binary) kodun özelliklerine göre belirlendiğini göstermişlerdir. İlk kuantum hata düzeltme kodları arasında yer alan Shor kodu, Steane kodu, CSS kodlar birer ikili kuantum sabitleyen kodlardır (bknz. [7], [14],

[13]). Daha sonra Ashikhmin ve Knill [15] tarafından bu yapı ikili olmayan kuantum kodlara genellenmiştir. Ketkar ve diğerleri ise [10] kuantum Hamming kodları, kuantum kuadratik kalan kodları gibi kodları incelemişlerdir.

Kuantum sabitleyen kodlarda durumların kendileri yerine onları sabit bırakan operatörler ile çalışılır. Bu nedenle hata belirleme ve düzeltme işlemleri kuantum hata düzeltme kodlarına göre daha basittir.

Örneğin; kod sözcükleri

$$
\begin{aligned}
|0\rangle_L &= \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle) \\
|1\rangle_L &= \frac{1}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle) \\
|2\rangle_L &= \frac{1}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle)
\end{aligned}
$$

olan 3-küdit kodu göz önüne alalım. ω birimin üçüncü dereceden bir kökü olsun ve X ile Z aşağıdaki tanımlansın

$$
X = X(1) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, Z = Z(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}.
$$

O halde XXX ve ZZZ operatörleri $C = \{|0\rangle_L, |1\rangle_L, |2\rangle_L\}$ kümesini sabit bırakır başka bir deyişle $1 \leq i \leq 3$ için $XXX\,|i\rangle_L = |i\rangle_L, ZZZ\,|i\rangle_L = |i\rangle_L$. Dolayısıyla $\{XXX, ZZZ\}$ operatörler C kümesini sabitler deriz.

Benzer şekilde, kod sözcükleri (5) eşitlikleri ile verilen bir kuantum sabitleyen kod olan 9-kübit kodu için sabitleyen operatörler aşağıdaki gibidir:

$$ZZIIIIIII,\ IZZIIIIII,\ IIIZZIIII,$$
$$IIIIZZIII,\ IIIIIIZZI,\ IIIIIIIZZ,$$
$$XXXXXXIII,\ IIIXXXXXX.$$

Burada I birim operatör olmak üzere, yukarıda tanımlandığı şekliyle $X(1)$ ve $Z(1)$ operatörlerini kolaylık olması açısından X, Z ile gösterdik.

Sabitleyen kuantum kodunun tanımını vermeden önce kullanacağımız bazı kavramları ele alalım. $\mathcal{E} = \{X(a)Z(b) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ daha önce tanımladığımız n-küdit için bir iyi hata tabanı olsun. Bu kümeyi bir grup yapmak istiyoruz dolayısıyla kompleks fazları elemanlara katsayı olacak şekilde düzenlersek $\mathcal{P}_n = \{\omega^c X(a)Z(b) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}$, pq^{2n} elemanlı bir grup olur. Burada ω birimin $p > 2$ asalı için p-inci dereceden bir ilken köküdür. $p = 2$ durumunda $\mathcal{P}_n$ grubu $4q^{2n}$ elemanlı olur.

n-uzunluklu bir q-ary kuantum kodu için $\mathcal{P}_n$ grubunun bir

$$\mathrm{Stab}(Q) = \{E \in \mathcal{P}_n : E\,|\psi\rangle = |\psi\rangle \text{ her } |\psi\rangle \in Q\}$$

alt grubuna Q kodunun sabitleyen grubu denir. Aşikar olmayan bir kuantum kod için $\mathcal{P}_n$ grubunun her alt grubu sabitleyen grup olmaz. Dolayısıyla aşikar olmayan bir kuantum Q kodu için $\mathrm{Stab}(Q)$, $-I$ operatörünü içermez ve $\mathcal{P}_n$ grubunun bir abel alt grubudur. Tersine eğer S, $\mathcal{P}_n$ grubunun $-I$ operatörünü içermeyen bir abel alt grubu ise o zaman

$$\mathrm{Fix}(S) = \{|\psi\rangle \in (\mathbb{C}^q)^{\otimes n} : E\,|\psi\rangle = |\psi\rangle \text{ her } E \in S\} = \bigcap_{E \in S} eig(E, 1).$$

olacak şekilde tanımlı $\mathrm{Fix}(S)$ bir kuantum koddur. O halde eğer $Q = \mathrm{Fix}(\mathrm{Stab}(Q))$ ise o zaman Q koduna bir kuantum sabitleyen kodu denir.

Q, n-uzunluklu bir q-ary kuantum sabitleyen kod ve $\mathrm{Stab}(Q) = S$ olsun. Eğer S alt grubunun üreteç sayısı r ise o zaman Q kodu n-mantıksal küditi $m = n - r$ fiziksel küdite kodlayan bir $[\![n, n-r]\!]_q$ koddur. Ayrıca S grubunun üreteçleri hata olup olmadığını kontrol etmek için kullanılan kontrol operatörleridir. Eğer iletim esnasında herhangi bir hata meydana gelmediyse ölçüm sonucu $+1$ olur aksi halde ω birimin p-inci dereceden bir ilkel kökü olmak üzere ölçüm sonucu $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ elemanlarından biri olur ve dolayısıyla bir hata meydana gelmiştir.

S sabitleyen grubu ile bir Q kuantum kodu ya S grubunda yer alan elemanların bir skaler katı olan ya da S deki en az bir eleman ile değişmeli olmayan hataları belirleyebilir. Bu nedenle $\mathcal{P}_n$ grubundaki değişmeli elemanlar önemlidir. Bu elemanları belirlemek için öncelikle

$$\mathcal{P}_n \to \mathbb{F}_q^{2n}, \omega^c X(a)Z(b) \to (a \mid b)$$

dönüşümünü tanımlayalım. Buradan $E = \omega^c X(a)Z(b), E' = \omega^{c'} X(a')Z(b') \in \mathcal{P}_n$ ise $EE' = \omega^{\mathrm{tr}(ba'-b'a)E'E}$ olduğundan E ve E' değişmelidir ancak ve ancak $\mathrm{tr}(ba' - b'a) = 0$ elde ederiz. O halde

$$\langle (a,b), (a',b') \rangle_s := \mathrm{tr}(ba' - b'a)$$

şeklinde tanımlanan fonksiyona iz simplektik iç çarpım (trace symplectic inner product) denir. O halde $\mathcal{P}_n$ grubundaki iki $\omega^c X(a)Z(b), \omega^{c'} X(a')Z(b')$ hatası değişmelidir ancak ve ancak karşılık gelen $(a,b), (a',b') \in \mathbb{F}_q^{2n}$ vektörleri iz simplektik iç çarpıma göre diktir ve $(a,b) \perp_s (a',b')$ şeklinde gösterilir. Buna göre $\mathcal{S}$ kümesinin simplektik duali ise

$$\bar{\mathcal{S}}^{\perp_s} = \{(a \mid b) \in \mathbb{F}_q^{2n} : \langle (a \mid b), (s \mid t) \rangle_s = 0 \text{ for all } (s,t) \in \bar{\mathcal{S}}\}.$$

$\mathcal{P}_n$ grubunun $E = \omega^c E_1 \ldots E_n$ şeklindeki elemanının ağırlığı, birim olmayan E_i operatörlerinin sayısı olarak tanımlanır. S sabitleyen grubu ile bir Q kuantum kodu için S grubunun elemanları kod sözcüklerine etki etmez ayrıca $C_{\mathcal{P}_n}(\mathcal{S})$, $\mathcal{S}$ grubunun $\mathcal{P}_n$ grubundaki merkezleyeni olmak üzere $C_{\mathcal{P}_n}(\mathcal{S})$ de olmayan bir hata kod tarafından belirlenebilir. Buradan

$\mathcal{S}$ sabitleyeni ile bir Q kuantum kodunun minimum uzaklığı aşağıdaki gibidir:

$$d(Q) = \begin{cases} \min\{\mathrm{wt}(E) \mid E \in C_{\mathcal{P}_n}(\mathcal{S}) \setminus \mathcal{S}\}, & \text{if } \mathcal{S} \subsetneq C_{\mathcal{P}_n}(\mathcal{S}) \\ \min\{\mathrm{wt}(E) \mid E \in \mathcal{S} \setminus \{I\}\}, & \text{if } \mathcal{S} = C_{\mathcal{P}_n}(\mathcal{S}). \end{cases}$$

Minimum uzaklığı d olan bir kuantum kod ağırlığı en fazla $\lfloor (d-1)/2 \rfloor$ olan tüm hataları düzeltir (bknz. [16]). Son olarak daha sonraki bölümlerde kullancağım simplektik ağırlık kavramını verelim. $C_{\mathcal{P}_n}(\mathcal{S})$ kümeasinin ψ altındaki görüntüsü $\bar{\mathcal{S}}^{\perp_S}$ olur. O halde Then we $(\mathbf{a} \mid \mathbf{b})$ in $\mathbb{F}_q^{2n}$ vektörünün simplektik ağırlığını, $\mathcal{P}_n$ grubundaki $X(\mathbf{a})Z(\mathbf{b})$ operatörünün ağırlığı olarak tanımlarız. Daha açık bir şekilde ifade edersek,

$$\mathrm{swt}(\mathbf{a} \mid \mathbf{b}) = |\{i : (a_i, b_i) \neq (0,0)\},$$

ve burada $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$.

Butson-Hadamard Matrisler

Bir Butson-Hadamard matrisi H, girişleri birimin kompleks kökleri olmak üzere $HH^\dagger = nI_n$ koşulunu sağlayan $n \times n$ kare matristir. H matrisinin girişleri birimin k-ıncı dereceden kökleri ise o zaman $\mathrm{BH}(n,k)$ şeklinde gösterilir. İlk kez A.T. Butson tarafından 1962 yılında [17] çalışmasında yer verilen Butson-Hadamard matrislerin kriptografi, hata düzeltme, kuantum bilgi teknolojisi, telekomünikasyon gibi pek çok alanda uygulaması vardır daha fazla bilgi için [18–21] çalışmalarına bakılabilir.

Tezin ilerleyen kısımlarında $\mathbb{Z}_k$ sonlu halkası üzerinde tanımlayacağımız kodları tanıtırken kolaylık sağlaması açısından BH matrislerin logaritmik form adı verilen farklı bir gösterimini kullancağız. Bir $H = [\zeta^{a_{ij}}]$, $BH(n,k)$ matrisinin logaritmik formu $L_\zeta(H)[a_{ij}]$ matrisidir.

H_1 ve H_2 iki $\mathrm{BH}(n,k)$ matris olmak üzere eğer biri diğerinden satır veye sütun permütasyonları ile ya da bir satır veye sütunu birimin aynı k-ıncı dereceden kökü ile çarpılarak elde ediliyorsa o zaman bu iki matrise dentirler denir. Her BH matris ilk satır ve

sütunu 1 olan bir BH matrise denktir. Bu formdaki matrislere normalleştirilmiş BH matrisler denir.

BH matrisleri oluşturmak için fark matrisleri adı verilen başka matris aileleri de kullanılabilir. G eleman sayısı k olan bir sonlu grup olsun o halde $i = 1, \ldots, r; j = 1, \ldots, k\lambda$ için $D = [d_{ij}]$ matrisinin girişlerinin her $1 \leq i \neq j \leq r$ için $\{d_{it} - d_{jt}\}$ kümesi G grubunun elemanlarını λ kez içeriyors o zaman D matrisine bir $(k, k\lambda; \lambda, G)$-fark matrisi denir. Genel Hadamard matrisler fark matrislerinin bir özel halidir. Bir H genel Hadamard matrisi Drake tarafından verilen tanıma göre girişleri $|G| = k$ olan G grubunun elemanları olan bir $k\lambda \times k\lambda$ matristir öyle ki H ile H^T, $(k, k\lambda; \lambda, G)$-fark matrisleridir ve $\mathrm{GH}(k, G)$ ile gösterilir. BH matrisler ile GH matrisler, G grubunu bir p asalı için birimin p-inci dereceden köklerinin çarpımsal grubu C_p olarak alırsak çakışırlar. Ayrıca bu durumda $\mathrm{BH}(p\lambda, p)$ matrislerinin logaritmik formları $\mathbb{Z}_p$ üzerindeki $p\lambda \times p\lambda$ GH matrislerdir.

Sonuçlar

Bu kısımda tez çalışmamız boyunca elde ettiğimiz sonuçları sunacağız. İlk olarak Butson-Hadamard matrislerin denkliği ile ilgili olarak yaptığımız çalışmaları ele alalım.

Bu kısım boyunca R bir sonlu Frobenius halka, M bir sonlu R-bimodül ve M üzerindeki dejenere olmayan bilineer formların kümesi de $\mathrm{BLF}(M)$ ile gösterilsin.

$\mathrm{BLF}(M)$ kümesinin M üzerindeki herhangi bir dejenere olmayan bilineer formu B, M modülünün sol(sağ) R-modül otomorfizmalarının kümesi $\mathrm{Aut}({}_RM)(\mathrm{Aut}(M_R))$ üzerine aşağıdaki gibi etkisini alalım,

$$B' : M \times M \longrightarrow R$$

$$(x, y) \longmapsto B(\gamma(x), y)$$

$$B'' : M \times M \longrightarrow R$$

$$(x, y) \longmapsto B(x, \eta(y)).$$

O halde ilk olarak $\mathrm{BLF}(M)$ kümesinin, M üzerinde herhangi bir dejenere olmayan B bilineer form ve M modülünün sol (sağ) R modül otomorfizmaları ile karakterize edilebileceğini gösterdik. Daha açık olarak

$$\begin{aligned}\mathrm{BLF}(M) &= \{B \cdot \gamma : \gamma \in \mathrm{Aut}({}_RM)\} \\ &= \{B \cdot \eta : \eta \in \mathrm{Aut}(M_R)\}.\end{aligned}$$

Daha sonra χ , R halkasının bir üreteç karakteri ve B, B' ise $M = \{x_0 = 0, x_1, \ldots, x_n\}$ R-bimodülünün iki dejenere olmayan bilineer formu olmak üzere

$$H = [\chi(B(x_i, x_j))]_{0 \leq i,j \leq n}$$

ve

$$H' = [\chi(B'(x_i, x_j))]_{0 \leq i,j \leq n}$$

matrislerinin satır denk (satır permütasyonu ile denk) olduğu sonucunu elde ettik. Burada üreteç karakteri sabit tutup dejenere olmayan bilineer formları değiştirdik. Bir sonraki sonuçta ise dejenere olmayan bilineer formu sabit tutarak üreteç karakterleri değiştirdiğimizde elde edeceğimiz

$$H = [\chi(B(x_i, x_j))]_{0 \leq i,j \leq n}$$

ve

$$H' = [\chi'(B(x_i, x_j))]_{0 \leq i,j \leq n}$$

matrislerinin yine satır-denk olduğunu gösterdik.

Böylece R halkasının herhangi bir χ üreteç karakteri ve $M = \{0 = x_0, x_1, \ldots, x_n\}$ R-bimodülü ile M üzerinde tanımlı herhangi bir dejenere olmayan bilineer form B için

$$[\chi(B(x_i, x_j))]_{0 \leq i,j \leq n},$$

şeklinde tanımlanan tüm matrislerin denk olduğunu elde ettik. Bu sonuçtan yola çıkarak, $\omega = e^{2\pi i/p}$ birimin p-inci dereceden bir kökü ve $f_i : \mathscr{C} \to \mathbb{F}_p$, $1 \leq i \leq q^k$ için lineer dönüşümler olmak üzere $H = [\omega^{f_i(\mathbf{c}_j)}]_{1 \leq i,j \leq q^k}$ şeklinde tanımlanan tüm matrislerin Fourier matrislerin bir Kronecker çarpımına denk olduğunu söyleyerek Butson-Hadamard matrisler için bir denklik koşulu verdik.

Tez boyunca ele aldığımız konulardan biri de Butson-Hadamard kodlardır. BH kodlar sonlu halkalar üzerinde tanımlı kod ailelerinden biridir. Kodlama teorisinde lineer kodların çok fazla çalışılmasının sebebi oluşturulma ve hata düzeltme işlemlerinin kolay bir şekilde gerçekleştirilmesidir. 1970 li yıllardan itibaren çalışılmaya başlayan sonlu halkalar üzerindeki kodlarla ilgili birçok çalışma yayınlanmıştır (bknz. [22–24]). Sonlu halkalar üzerindeki cebirsel kodlama teorisi, bazı doğrusal olmayan ikili kodların aslında $\mathbb{Z}_4$ halkası üzerinde tanımlı lineer kodların görüntüleri olduğu gerçeği ile önem kazanmıştır. Ayrıca BH kodların bir özel hali olan GH kodlar da yakın dönemde çalışılmıştır. Sonlu halka ve cisimler üzerinde farklı yöntemler ile GH kodlar oluşturulmuş ve sınıflandırılmıştır, (bknz. [22, 23, 25]). BH kodların parametrelerini belirlemek ve böylece etkililiğini ortaya koymak çalışmalarımızdaki temel problemdir. Burada farklı ağırlık fonksiyonları ve onlardan türetilmiş uzaklık fonksiyonlarını kullanarak elde ettiğimiz kodların minimum uzaklıkları için bazı durumlarda alt sınır vermemize rağmen bazı durumlarda ise tam olarak elde ettik. Öncelikle homojen ağırlıklar ile ilgili elde ettiğimiz sonuçlara yer vereceğiz. Bunlardan ilki sonlu değişmeli halkalar üzerinde tanımladığımız ve homojen olmayan ağırlıklar kümesinde olmasına rağmen homojen ağırlıkların gibi önemli özelliklere sahip olan yarı-homojen ağırlık kavramıdır.

R sonlu ve değişmeli bir halka ve $\omega(0) = 0$ olacak şekilde bir ω ağırlık fonksiyonu, R halkasının sıfırdan farklı herbir I idealinin tüm $a + I$ kosetlerindeki elemanların ağırlıkları

toplamı bir γ reel sayısı için $\gamma|I|$ değerine eşit oluyorsa o zaman ω ağırlık fonksiyonuna yarı-homojen ağırlık denir.

Yarı-homojen ağırlığı tanımladıktan sonra e pozitif bir tamsayı ve γ pozitif bir reel sayı olmak üzere aşağıdaki gibi verilen ağırlık fonksiyonunun yarı-homojen olduğunu söyledik.

$w : \mathbb{Z}_{p^e} \to \mathbb{R}$ ve p-ary açılımı $u = u_0 + u_1 p + \cdots + u_{e-1}p^{e-1}$ ile her $u \in \mathbb{Z}_{p^e}$ için

$$w(u) = \begin{cases} \frac{\gamma}{p^{e-2}(p-1)}u, & \text{if } u_{e-1} = 0 \\ \frac{\gamma p}{p-1}, & \text{if } 0 < u_{e-1} \leq p-2 \\ \frac{\gamma p^2}{p-1} - \frac{\gamma}{p^{e-2}(p-1)}u, & \text{if } u_{e-1} = p-1. \end{cases}$$

w, $\mathbb{Z}_{p^e}$ üzerinde tanımlı ve ortalama değeri γ olan bir yarı-homojen ağırlıktır.

Ele alacağımız BH kodları tanımlayalım. $\mathbb{Z}_k^n$ uzayının boştan farklı ve M boyutlu herhangi bir alt kümesine bir k-ary (n, M) kod denir. H bir normalleştirilmiş $\mathrm{BH}(n, k)$ matris ve $L(H)$ ile de onun logaritmik formunu gösterelim. Ayrıca, N birimin tüm k-ıncı dereceden köklerinin çarpımsal grubu olsun. O halde dört farklı tipteki k-ary kodu aşağıdaki gibi tanımlayacağız:

$\mathcal{A}_k$: k-ary $(n-1, n, d_A)$ kodu, $L(H)$ matrisinin ilk sütunu silinerek elde edilen matrisin satırlarından oluşur,

$\mathcal{B}_k$: k-ary $(n-1, nk, d_B)$ kodu her $\alpha \in N$ için αH translate lerinin $L(\alpha H)$ logaritmik formunun ilk sütunu silinerek elde edilen matrisin satırlarından oluşur,

$\mathcal{C}_k$: k-ary (n, nk, d_C) kodu her $\alpha \in N$ için αH translate lerinin $L(\alpha H)$ logaritmik formunun satırlarından oluşur

$\mathcal{D}_k$: k-ary $(n+1, n^2, d_D)$ kodu, $k = n$ olmak üzere her $\alpha \in N$ için $[L(\alpha H) \mid \boldsymbol{c}]$ blok matrisinin satırlarından oluşur, burada $\boldsymbol{c}$, $L(H)$ matrisinin ilk sütunu dışındaki herhangi bir sütunudur.

Herhangi $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, ya da $\mathcal{D}_k$ şeklindeki kodlar genel olarak bir H normalleştirilmiş $\mathrm{BH}(n,k)$ matrisinden elde edilen bir BH kodu olarak adlandırılır. Kolaylık olması açısından sırasıyla $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, ya da $\mathcal{D}_k$ kodlarının minimum uzaklıklarını d_A, d_B, d_C ve d_D ile göstereceğiz.

İlk olarak yukarıda tanımladığımız kodların klasik Hamming ağırlığı altındaki minimum uzaklıkları için $l = \min\{i \geq 2 : i|k\}$ ile $d_A \geq n - \frac{n}{l}$, $d_B \geq n - \frac{n}{l} - 1$, $d_C \geq n - \frac{n}{l}$, ve $d_D \geq n - \frac{n}{l}$ olacak şekilde birer alt sınır verdik ve SageMath yardımıyla örnekler üzerinde gösterdik.

Ağırlık fonksiyonunu herhangi bir homojen ağırlık alarak kodların minimum uzaklıklarını tam olarak hesapladık ve sonucu olarak $e \geq 2$ için normalleştirilmiş $\mathrm{BH}(n,p^e)$ matrisler için ağırlık fonksiyonu olarak Hamming ağırlık ve G_1 Gray dönüşümünden elde ettiğimiz w_1 ağırlık fonksiyonu ile minimum uzaklıklarını verdik. Normalleştirilmiş bir $\mathrm{BH}(9,9)$ matrisinden elde edilen kodların minimum uzaklıklarını SageMath programı yardımıyla elde ederek önek olarak verdik.

p bir asal sayı $e \geq 2$ bir tamsayı ve ω, γ ortalama değeri ile bir yarı-homojen ağırlık olmak üzere normalleştirilmiş bir $\mathrm{BH}(n,p^e)$ matristen elde edilen $\mathcal{A}_{p^e}$ tipteki BH kodun kod sözcüklerinin eşuzaklıklı ve bu uzaklığın da γn olduğunu söyledik. Ayrıca bu kod ailesinin Plotkin optimal olduğunu da elde ettik. Daha sonra $\mathcal{B}_k$, $\mathcal{C}_k$, ve $\mathcal{D}_k$ kodlarının da minimum uzaklıklarını kanıtladık ve $p = 2$ durumunu ayrı inceleyerek normalleştirilmiş $\mathrm{BH}(n,p^e)$ matrislerden elde edilen kodların yarı-homojen ağırlık altında minimum uzaklıklarını

(i) Eğer $e = 2$ ise o zaman $d_A = n\gamma$, $d_B = (n-2)\gamma$, $d_C = d_D = n\gamma$.

(ii) Eğer $e > 2$ ve $n \geq 4$ ise o zaman $d_A = n\gamma$, $d_B = (n-1)\gamma/2^{e-2}$, $d_C = d_D = n\gamma/2^{e-2}$.

olacak şekilde elde ettik. Bunun bir sonucu olarak da özel bir yarı-homojen ağırlık olan G_2 Gray dönüşümü ile klasik Hamming ağırlığı kullnarak minimum uzaklıkları $\mathcal{A}_k, \mathcal{B}_k$, $\mathcal{C}_k$, ve $\mathcal{D}_k$ kodları için kanıtladık.

Tezin son kısmında Butson-Hadamard kodların uygulamalarından biri olan kuantum hata düzeltme kodlarını inceledik. Burada iki klasik lineer kod ve Fourier matrislerin bir Kronecker çarpımı olan bir BH matris kullanarak bir kuantum kod elde ettik. Daha açık olarak,

$\mathscr{C} \subseteq \mathbb{F}_q^n$, $1 \leq k < r$ olmak üzere bir q-ary $[n, k, d_1]$ klasik lineer kod olsun. $\mathscr{C}$ kodunun kod sözcüklerini $(\mathbb{C}^q)^{\otimes n}$ uzayında kuantum durumları oluşturmak için kullanacağız. Bunu da aşağıdaki gibi yapacağız: $\mathscr{C}$ kodundan $\mathbb{F}_p$ uzayına fonksiyonların bir kümesi $\{f_\lambda : \lambda \in \mathbb{F}_{q^k}\}$, $\omega = e^{2\pi i/p}$ ve her $\lambda \in \mathbb{F}_{q^k}$ için

$$\phi_\lambda := \frac{1}{\sqrt{q^k}} \sum_{\mathbf{c} \in \mathscr{C}} \omega^{f_\lambda(\mathbf{c})} |\mathbf{c}\rangle \tag{2}$$

olsun. O halde ϕ_λ durumları $(\mathbb{C}^q)^{\otimes n}$ uzayının bir alt uzayı için ortonormal bir taban oluşturuu ancaj-k ve ancak satırları $\mathbb{F}_q$ in elemanları ve sütunları da $\mathcal{C}$ kodunun elemanları ile indislenen $q^k \times q^k$

$$H = [\omega^{f_\lambda(\mathbf{c})}]_{\lambda \in \mathbb{F}_{q^k}, \mathbf{c} \in \mathscr{C}}, \tag{3}$$

matrisi bir $\mathrm{BH}(q^k, p)$ olur. $\mathscr{D} \subseteq \mathbb{F}_{q^k}^m$, s boyutlu bir klasik lineer kodolsun ve her $\Lambda = (\lambda_1, \ldots, \lambda_m) \in \mathscr{D}$ için

$$\Phi_\Lambda := \phi_{\lambda_1} \otimes \ldots \otimes \phi_{\lambda_m} \in (\mathbb{C}^q)^{\otimes nm} \tag{4}$$

tanımlayalım. O halde $Q_H(\mathscr{C}, \mathscr{D})$ ile gösterilen nm uzunluklu bir kuantum kodu $(\mathbb{C}^q)^{\otimes nm}$ uzayının her $\Lambda \in \mathscr{D}$ için Φ_Λ tarafından gerilen altuzayı olarak tanımlayacağız. Yani,

$$Q_H(\mathscr{C}, \mathscr{D}) := \mathrm{span}\{\Phi_\Lambda : \Lambda \in \mathscr{D}\}. \tag{5}$$

$Q_H(\mathscr{C}, \mathscr{D})$, $(\mathbb{C}^q)^{\otimes nm}$ uzayının q^{ks}-boyutlu alt uzaydır dolayısıyla δ, $Q_H(\mathscr{C}, \mathscr{D})$ bir $[\![nm, ks, \delta]\!]_q$ kuantum koddur. Burada δ, $Q_H(\mathscr{C}, \mathscr{D})$ kodunun minimum uzaklığıdır. Shor tarafından verilen 9-kübit kod ile [26] çalışmasında verilen 9-küdit kod yukarıdaki şekilde tanımlanan kodların bir özel halidir. Daha genel olarak $\mathcal{C}$ ile $\mathcal{D}$ klasik lineer kodları tekrarlı kod ve $\mathrm{BH}(q, p)$ matrisi alınırsa o zaman elde edilcek kuantum $Q_H(\mathcal{C}, \mathcal{D})$ kodu [27] çalışmasında yer alan kodlar ile çakışır.

Yukarıda nasıl oluşturulacağını gösterdiğimiz $Q_H(\mathcal{C},\mathcal{D})$ kuantum kodları eşit ise o zaman H ve H' BH matrislerinin satır denk olduğunu gösterdik. Tersinin ise $\mathcal{D}$ kodunun 1-boyutlu tekrarlı kod alındığında doğru olacağını elde ettik. Buradaki kuantum kodun sabitleyen kuantum kod olması için gerekli olan koşulları araştırdık ve aşağıdaki sonuca ulaştık: $\Theta : \mathbb{F}_{q^k} \to \mathbb{F}_q^n/\mathscr{C}^\perp$, $\Theta(\lambda) = \overline{\mathbf{x}}_\lambda$ ile tnaımlanan bir $\mathbb{F}_p$-uzay izomorfizması olsun.

$$\mathscr{D}^\Theta := \{(\mathbf{x}_{\lambda_1},\ldots,\mathbf{x}_{\lambda_m}) : (\lambda_1,\ldots,\lambda_m) \in \mathscr{D} \text{ and } \mathbf{x}_{\lambda_i} \in \Theta(\lambda_i) \text{ for all } 1 \le i \le m\}.$$

tanımlayalım. O halde kuantum kodu oluştururken kullandığımız $H = [\omega^{f_\lambda(\mathbf{c})}]_{\lambda\in\mathbb{F}_{q^k},\mathbf{c}\in\mathscr{C}}$ matrisi her $\lambda,\lambda_1,\lambda_2 \in \mathbb{F}_q$ ve $c \in \mathbb{F}_p$ olmak üzere $f_{\lambda_1} + f_{\lambda_2} = f_{\lambda_1+\lambda_2}$ ve $f_{c\lambda} = cf_\lambda$ sağlanıyorsa o zaman $Q_H(\mathcal{C},\mathcal{D})$ kodu bir $[\![nm, ks, \delta]\!]_q$ kuantum sabitleyen koddur ve burada $\delta = \min\{d(\mathcal{C},\ell\}$ öyle ki $\ell = \min\{\mathrm{wt}(\mathbf{X}) : \mathbf{X} \in \mathscr{D}^\Theta \setminus (\mathscr{C}^\perp)^{(m)}\}$. Dahası literatürde yer alan CSS kodlardan farklı olarak sabitleyen grubun elemanlarını da söylüyoruz. $Q_H(\mathscr{C},\mathscr{D})$ kodunun sabitleyen grubu $X(\mathbf{c}_1,\ldots,\mathbf{c}_m)Z(\mathbf{d}_1,\ldots,\mathbf{d}_m)$, hatalarından oluşur öyle ki $(\mathbf{c}_1,\ldots,\mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)$ and $\mathbf{d}_1,\ldots,\mathbf{d}_m \in \mathscr{C}^\perp$. Burada eğer $\mathcal{D} = \{(\lambda,\ldots,\lambda) : \lambda \in \mathbb{F}_q\} \subset \mathbb{F}_q^m$ lineer kodunu tekrarlı kod alırsak o zaman kodun minimum uzaklığı $\delta = \min\{d(\mathcal{C}), m\}$ olur ve sabitleyen grubu da $X(c_1,\ldots,c_m)Z(d_1,\ldots,d_m)$ hatalarından oluşur öyle ki $c_1,\ldots,c_m \in \mathcal{C}$ ve $\sum_{i=1}^m c_i = 0, d_1\ldots,d_m \in \mathcal{C}^\perp$.

Son olarak, yukarıda verdiğimiz şekilde oluşturulan kuantum kodun hangi koşullar altında bir kuantum sabitleyen kod verdiğini araştırdık. Böylece q,p asalının bir kuvveti olmak üzere H bir $\mathrm{BH}(q^k,p)$ ve $\mathcal{C} \subseteq \mathbb{F}_q^n$ boyutu k olan bir klasik lineer kod, $\mathcal{D} = \{(\lambda,\ldots,\lambda) : \lambda \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^m$ ise $\mathbb{F}_q$ üzerinde 1-boyutlu lineer kod olsun. Eğer $Q_H(\mathcal{C},\mathcal{D})$ bir sabitleyen kod ise o zaman H, p-boyutlu Fourier matrisin rk-kez Kronecker çapımıdır. Bu sonuç ile aradığımız koşulları elde ettik.

CONTENTS

Page

Chapter 1

INTRODUCTION

The foundations of coding theory were laid with the publication of Claude Shannon's paper [28]. This theory studies the ways to recover the original information when data transmitted over a channel is subjected to noise and gets corrupted. Shannon proved that if the data is encoded before transmission, it can be corrected with a certain degree of accuracy in case of used in this sense is the Hamming codes, introduced by Richard Hamming and used in digital communication systems. These codes, which detect and correct single errors, were widely used in early computer systems. Until the early 1970s, error-correcting codes defined over finite fields and vector spaces were studied. In 1972, Hamming codes were generalized to arbitrary integer residue rings by Blake in [29].

The codes constructed by Nordstorm-Robinson, Kerdock, Preparate, Goethals, and Delsarte-Goethals have better parameters than any known linear codes. Hammons et.al [4] have shown that the codes can be constructed as the images of linear codes over $\mathbb{Z}_4$ under Gray map. This encourages the study of nonlinear codes over rings. Butson-Hadamard codes that derived from Butson-Hadamard matrices [25, 30, 31] and are a special case of codes over finite rings. These codes are used in a wide range of applications such as communications, signal processing, and combinatorial designs. The orthogonality of Butson-Hadamard matrices enhances the error-correcting capabilities of these codes. Additionally, their definition over finite rings allows for the design codes that are suitable for

different channel conditions and hardware constraints. In [3], it is shown that certain types of Butson-Hadamard codes, which correspond to type $\mathcal{A}$ codes in this thesis, meet Plotkin bound under a homogeneous weight by determining their parameters. In other words, it is shown that they have the maximum number of codewords for a fixed minimum distance and length. Furthermore, the minimum distance of another certain type of Butson-Hadamard codes, referred to as $\mathcal{B}$ in this thesis, have been found under a specific homogeneous weight (ω_1).

Generalized Hadamard codes, which are a particular type of Butson-Hadamard codes, have been studied in [23–25], recently. Here, generalized Hadamard codes, or simply GH codes, were constructed using different methods on finite rings and finite fields. In [23], for a prime p and $e > 1$, additive GH codes, that is, subsets of the vector space $\mathbb{F}_{p^e}^n$ which are linear over the prime field $\mathbb{F}_p$, were constructed over $\mathbb{F}_{p^e}$. The recursive construction of a particular type of GH codes over $\mathbb{Z}_p\mathbb{Z}_{p^2}$ and the relations between these obtained codes and the linear GH codes over $\mathbb{Z}_{p^2}$ were given in [25]. Finally, Bhunia et al. provided a classification of the corresponding linear GH codes over $\mathbb{Z}_{p^s}$ using certain types of GH codes over $\mathbb{Z}_{p^s}$.

Another application of Butson-Hadamard codes is quantum information theory. The interest in quantum error-correcting codes increased, with the publication of the 9-qubit code [7] by Shor in 1995, which can correct any error on a single qubit. The 7-qubit code [8] introduced by Steane, and 5-qubit code [9] introduced by Bennett et al. are some of these contributions. Later, a condition for when errors in a given set could be corrected was provided by Knil and Laflamme [32]. However, providing the basis states in these examples is not easy because the dimension of the code space increases exponentially with the number of qubits. Moreover, it is also important to find error correction methods easily. Quantum stabilizer codes, first introduced by Daniel Gottesman [11], and Robert Calderbank [13] eliminate these issues by compactly defining encoding and decoding steps. They also play a role similar to linear codes in classical coding theory. The first examples of quantum error-correcting codes are CSS(Calderbank-Shor-Steane) codes introduced by Robert Calderbank, Peter Shor and Andrew Steane, constructed using two classical linear codes and under certain conditions (see, [13], [8]).

The aim of this thesis is to determine the minimum distance of codes obtained from a normalized BH matrix. In Chapter 3 we give a proof of the fact that the BH matrices considered in Chapter 6 and Theorem 6.10 are equivalent to a Knocker product of Fourier matrices. In Theorem 5.1, a lower bound for the minimum distance of such codes is given, where the distance function is chosen as the usual Hamming distance. Then we consider distance functions induced by homogeneous weights and give the minimum distance of BH codes in Theorem 5.3. In chapter 5 with Section 2, we turn our attention to non-homogeneous weights and show that there is a particular type of non-homogeneous weights, that we call *quasi-homogeneous* weights, for which certain BH codes are Plotkin optimal. We note that our introduction of quasi-homogeneous weights is based on the fact that the non-homogeneous weight introduced in [33] satisfies a property that is also shared by homogeneous weights (see Definition 4.1 and the paragraph preceding it). Then we think of BH codes equipped with a certain type of quasi-homogeneous weights and find their minimum distances in Theorem 5.6. We apply our results to determine parameters of p-ary codes (p prime) which are images of BH codes under some Gray isometries (see Corollaries 5.4 and 5.8).

In Chapter 6, we give our general method for constructing a quantum code using p-ary and q-ary classical codes and a BH(q^k, p) matrix, where p is a prime and q is a power of p. In Chapter 6 and Section 2, we look for a BH matrix for which our construction gives a stabilizer quantum code. In particular, we show that if the BH matrix used in the construction has a particular form such that it is equivalent to a Kronecker product of the Fourier matrix of order p, then the resulting quantum code is a stabilizer code. In the next section, we search for a converse; and consider a certain q-ary classical code in the construction. In particular, we prove that if the resulting quantum code is a stabilizer code, then the BH matrix used in the construction must be equivalent to a Kronecker product of the Fourier matrix of order p.

Chapter 2

BASIC NOTIONS IN QUANTUM CODING THEORY

1. Classical coding theory

Coding theory studies the methods necessary for the efficient and effective transmission of information from one place to another. It is developed to minimize the effects of noise that may occur during the transmission. For example, it is used in cases such as transmission from a whether or a distant satellite, reducing noise from compact disc recordings, and transmitting Saturn and Jupiter photographs taken by the Voyager spacecraft.

The physical medium used for transmitting information is referred to as a channel. Atmosphere and telephone lines are examples of channels. The information received may differ from the information sent because of the undesirable disturbances called noise. Lightning, poor spelling, poor hearing, sunspots, and competing phone messages can cause noise. Coding theory deals with detecting and correcting errors caused by noise on the channel. The fundamental problem here is determining which message was sent based on the received information. To transmit information through a channel, we must express the information in a way that is suitable for the channel. We refer to the structures we use for

this purpose as alphabets. More formally, an alphabet $\mathcal{A}$ is a finite set. The alphabet $\mathcal{A}$ is generally chosen as finite fields. In binary codes, the finite field of two elements $\mathbb{F}_2 = \{0, 1\}$ is considered, while more generally, for a prime p, the finite fields $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ are also used the alphabet in many codes. In this thesis, we consider codes over finite rings, which have been extensively studied recently (see, [34], [35]). The elements of $\mathcal{A}$ are called code symbols. A word of length n is a sequence $a_1 \ldots a_n$, where each a_i belongs to $\mathcal{A}$, which is also represented by the vector $(a_1, \ldots, a_n)$. A code of length n is a non-empty subset C of $\mathcal{A}^n$ and the elements of C are called codewords.

Certain parameters have been established to decide which codes are good. Three fundamental parameters are used when defining and evaluating codes. The first parameter is the number of bits contained in the codewords, which is referred to as the code length. The second parameter is the number of codewords in the code. The last parameter is about the distance of distinct pairs of codewords.

Definition 2.1. Let C be a code of length n and $c = c_1 \ldots c_n$ be a codeword of C. Then the Hamming weight of c is $\mathrm{wt}(c) = |\{i \mid c_i \neq 0\}|$. Also, let $b = b_1 \ldots b_n, c = c_1, \ldots c_n$ with $b \neq c$. Then the Hamming distance between b and c is defined by

$$d(b, c) = \mathrm{wt}(b - c) = |\{i \mid b_i \neq c_i\}|.$$

The minimum distance of a code C is defined as the smallest distance between two distinct codewords in C.

A code containing M codewords of length n and having minimum distance d is expressed as (n, M, d). In the trasmission of messages, the goals are to quickly encode the messages to be sent, to ensure the easy transmission of the encoded messages, to rapidly decode the recieved message, and to transmit a large amount of information during each transmission. As the length of the code n increases, the transmission of the codewords slows down. Therefore, to increase the transmission speed, the length of the code should be small. Additionally, for detecting more errors, d should be large. Lastly, for transmitting a wide variety of messages,

M should be large. These are all considerations observed when constructing a code and are fundamental objectives of coding theory.

1.1. Error Detection and Error Correction

In this section, we discuss the conditions regarding which errors that may occur during encoding can be detected and corrected.We explain decoding process with examples.

Assume that the transmitted message is not a codeword. Then it is clear that there is an error during the transmission. Thus, the error can be detected. However, if the transmitted message is one of the codewords, then it might be assumed that there is no error, and thus the error cannot be detected.

Let C be a code. Assume that c is sent as a codeword and w is received as the message. Then, the vector $e = w - c$ is called the error vector. C detects an error e if and only if for every codeword $c \in C, e + c$ is not a codeword in C.

Example 2.1. *Let* $C = \{000, 001, 010, 011, 100, 101, 110, 111\}$. *Since all recieved codewords are again elements of* C*, any error that occurs during transmission cannot be detected by* C*. Also, since there is no need to do anything to convert it to a codeword when an error occurs in a recieved message, it does not correct errors.*

Example 2.2. *Let us consider* 3*-repetition code* $C' = \{000, 111\}$*. So,* 0 *and* 1 *are encoded as* 000 *and* 111*, respectively. If no errors occur during transmission, the message* 0 *is recieved as* 000*. However, suppose that an error occurred and it was recieved as* 010*. Then, this message is corrected to either* 000 *or* 111*. It is decoded as the codeword closest to it. If we calculate the distance between codewords of the recieved message, we obtain* $d(000, 010) = 1$ *and* $d(111, 010) = 2$*. Therefore, the message* 010 *is corrected to* 000*.*

Now, assume that the received message is 011*. Similarly, the message* 011 *is corrected to* 111*, but this decoding process is incorrect. As a result, while the code* C *is able to correct a one-bit error, it cannot correct a two-bit error.*

Definition 2.2. Let $\mathcal{A}$ be an alphabet and $C \subseteq \mathcal{A}^n$ be a code of length n. Then C is called t-error correcting code if for all $x \in C$ there exists at most one $c \in C$ with $d(x, c) \leq t$. Also, the code C detects t errors when $d(x, c) \leq t$ and $c \in C$, in the case that x cannot be a codeword. It is also called t-error detecting code.

Theorem 2.3. *[36] Let C be a code with minimum distance d. Then it is a t-error correcting code for $t \leq \lfloor (d-1)/2) \rfloor$ and it is $(d-1)$-error detecting code.*

Next, the alphabet $\mathcal{A}$ will be considered as the ring $\mathbb{Z}_k$ over which we often think of non-linear codes. A linear code of length n over $R = \mathbb{Z}_k$ is an R submodule of $\mathbb{Z}_k^n$ and additionally, if the minimum distance is d, then it is denoted as $[n, k, d]$.

There are many ways to create new codes from linear codes. One of these is through dual codes.

Definition 2.4. Suppose that $\mathcal{C}$ is a code of length n. Then the dual code of $\mathcal{C}$ consists of the vectors y of length n such that

$$\sum_{i=1}^{n} x_i y_i = 0$$

for all $x_i \in \mathcal{C}$. The dual code of $\mathcal{C}$ is denoted by $\mathcal{C}^{\perp}$.

Because of linear codes algebraic structures, defining, encoding and decoding processes of linear codes are easier compared to non-linear codes. Therefore, they have been studied more than non-linear codes. However, non-linear codes have been discovered with better error-correcting capabilities than any known linear code. More explicitly, some non-linear codes have more codewords than any linear code with the same length and minimum distance. Kerdock [37] and Preparata [38] codes are some examples of these codes.

1.2. Homogeneous Weight Function

Homogeneous weights were introduced by I. Constantinescu and W. Heise, [2]. They can be viewed as a generalization of Hamming weight in some sense. Also, the results obtained

regarding the Hamming weight for codes over finite fields have corresponding homogeneous weight versions for codes over rings. Now, we introduce some definitions and theorems used in this thesis.

Definition 2.5. [3] A real-valued function w on the finite ring R is called a homogeneous weight if $w(0) = 0$ and the following hold:
(i) $Rx = Ry$ implies $w(x) = w(y)$ for all $x, y \in R$.
(ii) There exists a real number γ such that

$$\sum_{y \in Rx} w(y) = \gamma |Rx|,$$

for all non-zero $x \in R$. The number γ is called the average value of w on R.

For instance, the Lee weight w_L on $\mathbb{Z}_4$ defined by $w_L(0) = 0, w_L(1) = w_L(3) = 1$ and $w_L(2) = 2$ is a homogeneous weight with the average value $\gamma = 1$.

The following theorem shows the existence and uniqueness of homogeneous weights on a finite ring for any given non-negative average value γ.

Theorem 2.6. *[39] A weight w on a finite ring R with identity is homogeneous if and only if there exists a real number $\gamma \geq 0$ such that $w(x) = \gamma(1 - \mu(0, Rx)/|R^{\times}x|)$ for all $x \in R$, where $R^{\times}$ denotes the set of unit elements of R and μ is the Möbius function on the partially ordered set of principal left ideals of R with respect to inclusion.*

Let $\mathcal{C}$ be a k-ary (n, M, d) code equipped with the distance function induced by a specified homogeneous weight on $\mathbb{Z}_k^n$ with the average value γ. If $d > \gamma n$, then the *generalized Plotkin bound* $M \leq d/(d - \gamma n)$ holds (see [40, Theorem 2.2]), and when

$$M > d/(d - \gamma n) - 1, \tag{1}$$

we say that $\mathcal{C}$ is *Plotkin-optimal*.

Greferath et al. in [3] consider BH codes of type $\mathcal{A}_k$ (see Ch. 5 for definition) in connection with the generalized Plotkin bound, where they employ homogeneous weights, and prove that these codes meet the Plotkind bound.

Theorem 2.7. *[3, Theorem 5.4] Let H be a normalized $\mathrm{BH}(n,k)$ matrix. Then the BH code of type $\mathcal{A}_k$ obtained from H equipped with a homogeneous weight on $\mathbb{Z}_k$ with the average value γ has parameters $(n-1,n,\gamma n)$, and so it meets the Plotkin bound.*

In order to produce weight functions on the ring $\mathbb{Z}_{p^e}$, where p is a prime number and $e \geq 2$ is an integer, it is customary to use Gray maps. The first use of Gray map appears in [41], in which it is shown that some well-known good non-linear binary codes can be expressed as images of linear codes over $\mathbb{Z}_4$. Later, the Gray map given in [41] has been generalized to a Gray map from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ by Carlet in [42]. Carlet's Gray map has been generalized to a map from $\mathbb{Z}_{p^e}$ to $\mathbb{Z}_p^{p^{e-1}}$ in [43], for a prime p, defined by

$$G_1(u) = (u_0, \ldots, u_{e-2})Y + u_{e-1}\mathbf{1}_{e-1}, \tag{2}$$

for every $u \in \mathbb{Z}_{p^e}$, where $u = \sum_{i=0}^{e-1} u_i p^i$ with $u_i \in \mathbb{Z}_p$, the p-ary expansion of u, $\mathbf{1}_{e-1}$ denotes the all-one vector of length p^{e-1}, and Y is a matrix whose columns are all different vectors in $\mathbb{Z}_p^{e-1}$ (see also [44]). The extension of G_1 from $\mathbb{Z}_{p^e}^n$ into $\left(\mathbb{Z}_p^{p^{e-1}}\right)^n$, also denoted G_1, is defined componentwise.

There also exists Boolean function theory based definition of the map G_1. Let u be any element of $\mathbb{Z}_{p^e}$ and $u = \sum_{i=1}^{e} u_i p^{i-1}$ its p-ary expansion for some $u_i \in \{0, 1, \ldots, p-1\}$. The image of u by a *Gray map* G_1 is defined to be the Boolean function on $GF(p)^{e-1}$:

$$G_1(u) : (y_1, \ldots, y_{e-1}) \to u_e + \textstyle\sum_{i=1}^{e-1} u_i y_i.$$

We remark that for every $u \in \mathbb{Z}_{p^e}$ with the p-ary expansion $u = \sum_{i=1}^{e} u_i p^{i-1}$, $G_1(u)$ is the evaluation map of the first-degree polynomial $P_u(X_1, \ldots, X_{e-1}) = u_1 X_{e-1} + \cdots + u_{e-1}X_1 + u_e$. Suppose that we write the elements of $GF(p)^{e-1}$ in a fixed order, say, as

$\alpha_1, \ldots, \alpha_{p^{e-1}}$. Then one may associate to $G_1(u)$, for each $u \in \mathbb{Z}_{p^e}$, a unique p^{e-1}-tuple, namely $(P_u(\alpha_1), \ldots, P_u(\alpha_{p^{e-1}}))$. Hence, G_1 gives a bijection between $\mathbb{Z}_{p^e}$ and the first-order generalized p-ary Reed-Muller code $GRM(1, e-1)$. Note that we do not distinguish between the map $G_1(u)$ and its correspondence in $GRM(1, e-1)$, which we demonstrate in the following example.

Example 2.3. *Suppose that $e = 3$ and $p = 2$. Then the Gray map for u is defined as follows:*

$$G_1(u) : (y_1, y_2) \to u_3 + u_1 y_1 + u_2 y_2,$$

where $(y_2, y_1) \in \mathbb{Z}_2^2$, in lexicographical order, are taken as follows:

y_1	y_2
0	*0*
0	*1*
1	*0*
1	*1*

If $u = 6$, then its binary representation is equal to $(u_3u_2u_1) = (110)$. Therefore if $(y_1, y_2) = (0, 0)$ then we get $G_1(6)(0, 0) = 1$. If we continue like this we can get Boolean function $G_1(6) = (1010)$.

Let w_h (resp., d_h) be the usual Hamming weight (resp., Hamming distance). We define the weight w_1 on $\mathbb{Z}_{p^e}$ by $w_1(u) = w_h(G_1(u))$ so that the Gray map G_1 turns into an isometric embedding of $(\mathbb{Z}_{p^e}^n, d_1)$ into $\left(\left(\mathbb{Z}_p^{p^{e-1}}\right)^n, d_h\right)$, where d_1 is the distance function induced by w_1, that is

$$d_1(\mathrm{x}, \mathrm{y}) = \sum_{i=1}^{n} w_1(y_i - x_i)$$

for all $\mathrm{x} = (x_1, \ldots, x_n)$ and $\mathrm{y} = (y_1, \ldots, y_n)$ in $\mathbb{Z}_{p^e}^n$. We note that $w_1(0) = 0$ and for any $u \neq 0$

$$w_1(u) := \begin{cases} p^{e-1} - p^{e-2}, & \text{if } u \in \mathbb{Z}_{p^e} \backslash \{p^{e-1}, 2p^{e-1}, \ldots, (p-1)p^{e-1}\} \\ p^{e-1}, & \text{otherwise.} \end{cases} \tag{3}$$

Note that w_1 is a homogeneous weight with the average value $\gamma = (p-1)p^{e-2}$

If w is a homogeneous weight with the average value γ over a Frobenius ring R, then $\sum_{r \in y+I} w(r) = \gamma |I|$ for every non-zero right or left ideal I of R, see [3, Proposition 2.6], a property which plays a crucial role in proving that some linear codes produced from a bimodule over R by using a non-degenerate bilinear form meet the Plotkin bound [3, Theorem 4.3]. Note that this important property of a homogeneous weight is shared also by some non-homogeneous weights. Later, we formalize such a weight (see Ch. 4).

2. Basic Notions in Quantum Coding Theory

This chapter consists of essential definitions and theorems from quantum coding theory used in this thesis without proof.

In this thesis, both two and higher-dimensional quantum systems have been studied. Let $\mathbb{F}_q$ be a finite field of q elements. We consider the q-ary quantum digits, or simply *qudits*, over $\mathbb{F}_q$ as the fundamental unit of quantum information. Specifically, in the case of $q = 2$, it is called a *qubit*.

The state of a qudit over $\mathbb{F}_q$ can be defined as a vector in the space $\mathbb{C}^q$, where the inner product is the standard inner product. The space is spanned by a set of orthonormal basis vectors $\{|0\rangle, |1\rangle, \ldots, |q-1\rangle\}$. These basis elements are also referred to as computational basis states. Therefore a state of a qudit can be represented as a linear combination of its computational basis states. In other words, a qudit can be in a superposition of its computational basis states, that is a qudit can be indicated as follows:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{q-1} |q-1\rangle \in \mathbb{C}^q$$

where $|\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{q-1}|^2 = 1$, and α_i for $0 \leq i \leq q-1$ are complex probability amplitudes.

One of the main differences between classical and quantum information is that in classical information, bits can be in states $0, 1, ..., q-1$. However, in quantum information, qudits can be in states $|0\rangle, |1\rangle, \ldots, |q-1\rangle$ or in superposition of them.

The n-fold tensor product of $\mathbb{C}^q$ extends naturally to quantum systems involving multiple qudits. A set of n qudits is called an n-qudit quantum register. We use

$$\mathcal{B} = \{|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle \mid x_i \in \mathbb{F}_q, 1 \leq i \leq n\} \tag{4}$$

as an orthonormal basis for $(\mathbb{C}^q)^n$. The basis elements are called computational basis states. For simplicity, we write the basis elements as $|x_1 x_2 \ldots x_n\rangle$ instead of $x_1 \otimes x_2 \otimes \ldots \otimes x_n$. Therefore every vector in $(\mathbb{C}^q)^n$ can be written as a linear combination of the vectors $|\mathbf{x}\rangle \in \mathbb{F}_q^n$.

Example 2.4. *Let $\mathbb{C}^3$ be three-dimensional complex vector space and label $|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, and $|2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Then some of the basis elements of $(\mathbb{C}^3)^2$ are as follows*

$$|0\rangle := |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |1\rangle := |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |2\rangle := |02\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |3\rangle := |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Other basis elements, such as $|4\rangle := |11\rangle, |5\rangle := |12\rangle, |6\rangle := |20\rangle, |7\rangle := |21\rangle, |8\rangle := |22\rangle$ can be found, similarly.

A state of any two-qutrit (i.e., ternary quantum digit) is $|\psi\rangle = \alpha_{00}|0\rangle + \alpha_{01}|1\rangle + \alpha_{02}|2\rangle + \alpha_{10}|3\rangle + \alpha_{11}|4\rangle + \alpha_{12}|5\rangle + \alpha_{20}|6\rangle + \alpha_{21}|7\rangle + \alpha_{22}|8\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{02} \\ \alpha_{10} \\ \alpha_{11} \\ \alpha_{12} \\ \alpha_{21} \\ \alpha_{22} \end{pmatrix}$, with $\sum_{x \in \mathbb{Z}_3^2} |\alpha_x|^2 = 1$. The complex coefficients α_x, for $x \in \mathbb{Z}_3^2$ are probability amplitudes.

A state of a quantum register is not known unless the state of the register is measured. For a measurement of $(\mathbb{C}_q)^{\otimes n}$ there are n possible outcomes which are classical information. After

the measurement the state is collapsed into a basis state and the original state of the register is destroyed, and cannot be reconstructed. More formally, it is defined as follows.

Definition 2.8. Let $\mathcal{O} := \{M_1, \ldots, M_s\}$ be the set of subspaces of $(\mathbb{C}^q)^n$ such that $M_i \perp M_j$ with $i \neq j$ and $(\mathbb{C}^q)^n = M_1 \oplus \ldots \oplus M_s$. Then $\mathcal{O}$ is called an observable. A measurement of an n-qudit with respect to the observable $\mathcal{O}$ is as follows: Any state $|\psi\rangle \in (\mathbb{C}_q)^{\otimes n}$ can be written uniquely $|\psi\rangle = \sum_{i=1}^{s} \alpha_i |\psi_i\rangle$ where $|\psi_i\rangle$ is the projection of $|\psi\rangle$ onto M_i. Let $P_i : (\mathbb{C}^q)^n \to M_i, |\psi\rangle \to |\psi_i\rangle$. For this state take a subspace M_i with probability $p(i) = \|P_i |\psi\rangle\|^2$, and output is i. After the measurement, the n-qudit collapses to the state

$$|\psi_i\rangle = \frac{P_i |\psi\rangle}{\sqrt{p(i)}}.$$

The orthonormal basis (4) is a nice observable which is called the standard observable. If $|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}$ then we write

$$|\psi\rangle = \sum_{j=1}^{n} \langle j \mid \psi \mid j\rangle.$$

After the measurement $|\psi\rangle$ will collapse to the basis state $|j\rangle$ with the probability $|\langle j \mid \psi\rangle|^2$.

Example 2.5. *Let $q = 2, n = 1$, and $H = \{|+\rangle, |-\rangle\}$ be the Hadamard basis where*

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

If we take a state $|\psi\rangle = \gamma |0\rangle + \zeta |1\rangle$

$$|\psi\rangle = \frac{\gamma + \zeta}{\sqrt{2}} |+\rangle + \frac{\gamma - \zeta}{\sqrt{2}} |-\rangle$$

then the outcome of a measurement $|\psi\rangle$ with respect to H will be 0 (resp.,1) with probability $|\gamma + \zeta|^2/2$ (resp.,$|\gamma - \zeta|^2/2$).

Example 2.6. *Suppose that*

$$|\psi\rangle = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle$$

is a state of 3*-qubit. Then the measurement of the first qubit of* 3*-qubit* $|\psi\rangle$ *is as follows. Consider the observable* $\mathcal{O} = \{M_0, M_1\}$ *where*

$$M_0 = \mathrm{Span}_{\mathbb{C}}\{|000\rangle, |001\rangle, |010\rangle, |011\rangle\} \text{ and } M_1 = \mathrm{Span}_{\mathbb{C}}\{|100\rangle, |101\rangle, |110\rangle, |111\rangle\}.$$

Then after measurement, we get 0 *as the outcome with probability* $p_0 = \sum_{i=0}^{3} |\alpha_i|^2$ *and the state is*

$$\frac{\alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle}{\sqrt{|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2}}.$$

We get 1 *as the outcome with probability* $p_1 = \sum_{i=4}^{7} |\alpha_i|^2$ *and the post-measurement state is*

$$\frac{\alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle}{\sqrt{|\alpha_4|^2 + |\alpha_5|^2 + |\alpha_6|^2 + |\alpha_7|^2}}.$$

Accordingly, the second qubit of $|\psi\rangle$ *can be measured using the observable* $\mathcal{O}' = \{M_2, M_3\}$ *where*

$$M_2 = \mathrm{Span}_{\mathbb{C}}\{|000\rangle, |001\rangle, |100\rangle, |101\rangle\} \text{ and } M_3 = \mathrm{Span}_{\mathbb{C}}\{|010\rangle, |011\rangle, |110\rangle, |111\rangle\}$$

Classical information can be copied, but this is not generally valid for quantum information. This is another important difference between classical and quantum information theory. The no-cloning theorem states that only non-orthonormal quantum states cannot be cloned. It is ensured by L.Park in 1970 [45] and then reconsidered in 1982 by W.Wootters and W.Zurek [46] and separately by D.Dieks [47]. It is one of the earliest results of quantum computation and quantum information.

Theorem 2.9. *There is no unitary operator* U *such that* $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ *for all* $|\psi\rangle, |\phi\rangle \in (\mathbb{C}^q)^n$.

3. Quantum Error Detection and Correction

Classical error-correcting codes have a well-developed theory but it cannot be directly carried over to quantum computers for some reasons. One of the classical techniques pretend that all the bits can be measured in the computer but for a quantum computer, this would destroy any superposition. Moreover, while a classical computer only needs to preserve the values of 0 and 1, a quantum computer also needs to preserve the phase information in addition to that. Secondly, considering the classical repetition code where 0 is encoded as 000 and 1 is encoded as 111, we correct the state 011 to 111 based on the majority vote but due to the No-cloning theorem, there is no quantum counterpart of such a code. However, Shor and Steane show that these challenges can be overcome [7, 48].

Quantum systems are not completely isolated from the environment. This exposes them to bit errors, phase errors, and even decoherence situations. Hence, it is important to determine the error model to characterize potential errors. On the other hand, some error-correcting codes are specifically designed based on the types of errors they will detect and correct.

Let q be a power of a prime p. A quantum code of length n is a subspace of $(\mathbb{C}^q)^{\otimes n}$. We represent a q-ary quantum code that encodes k qudit into n qudits as $[\![n, k]\!]_q$. Now, let $X(a)$and $Z(b)$ be unitary operators on $\mathbb{C}^q$ as follows, where $a, b \in \mathbb{F}_q$ and ω is a primitive p-th root of unity and tr denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$,

$$X(a)\,|x\rangle := |x + a\rangle\,, \quad Z(b)\,|x\rangle := \omega^{tr(bx)}\,|x\rangle\,.$$

That the set of error operators, $\mathcal{E} = \{X(a)Z(b) \mid a, b \in \mathbb{F}_q\}$ has the following properties:

(i) $\mathcal{E}$ contains the identity matrix I.

(ii) The product of two elements of $\mathcal{E}$ is equal to a scalar multiple of another element of $\mathcal{E}$.

(iii) $\mathrm{tr}(A^\dagger B) = 0$ for all $A, B \in \mathcal{E}$ and $A \neq B$.

Indeed, for $a = 0, X(a) = Z(a) = I$ and $X(a)Z(b)X(a')Z(b') = \omega^{\mathrm{tr}(ba')}X(a+a')Z(b+b')$ for all $a, a', b, b' \in \mathbb{F}_q$. Therefore, we see that (i) and (ii) are satisfied. Additionally, given $A = X(a)Z(b)$ and $B = X(a')Z(b')$,

$$\begin{aligned}\mathrm{tr}(A^\dagger B) &= \mathrm{tr}(Z(-b)X(a'-a)Z(b')) \\ &= \mathrm{tr}(X(a'-a)Z(b')Z(-b)) \\ &= \mathrm{tr}(X(a'-a)Z(b'-b)) = 0.\end{aligned}$$

Here we consider the case $p = 2$ separately.If we take $\omega = -1$ then we ignore the complex phases. Therefore, we take ω as the 4-th root of unity for $p = 2$.

A nice error basis is a set of q^2 unitary matrices that satisfies the above properties. (see [49]). The set $\mathcal{E}$ is a basis for the set of $q \times q$ complex matrices with the Frobenius inner product, that is, for two complex matrices A and B, $\langle A, B\rangle_F = \mathrm{tr}(A^\dagger B)$.

Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be two nice error bases. Then, according to the definition of a nice error basis and the identity

$$(E_1 \otimes E_2)(E_3 \otimes E_4) = E_1E_3 \otimes E_2E_4,$$

we obtain that $\mathcal{E}_1 \otimes \mathcal{E}_2$ is also a nice error basis. In this way, $\mathcal{E}$ can be extended to a nice error basis for an n-qudit as follows

$$\mathcal{E}_n = \{X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a} = (a_1, a_2, \ldots, a_n), \mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n\}$$

with $X(\mathbf{a}) = X(a_1) \otimes X(a_2) \otimes \ldots \otimes X(a_n)$ and $Z(\mathbf{b}) = Z(b_1) \otimes Z(b_2) \ldots \otimes Z(b_n)$. In other words, $\mathcal{E}_n$ is a nice error basis on complex vector space $(\mathbb{C})^{q^n}$ (see [50]).

For instance, $\mathcal{G}_1 = \{I_2, \sigma_x, \sigma_y, \sigma_z\}$ is a nice error basis on $\mathbb{C}^2$ where, I_2 is the 2×2 identity matrix and

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

are the well-known Pauli matrices. Furthermore, $\mathcal{G}_n = \{E_1 \otimes \cdots \otimes E_n \mid E_i \in \mathcal{G}_1\}$ is a nice error basis on $(\mathbb{C}^2)^{\otimes n}$.

3.1. Shor's nine qubit code

The code discovered by Shor [7] in 1995 is a simple example of quantum error-correcting codes that provides protection against the effects of any error on a single qubit. Additionally, along with the example discovered by Steane [48] in 1996, it is the first quantum error correction code. It encodes a single qubit of information into nine qubits. The code is obtained by combining three-qubit bit-flip and phase-flip code. First, we encode the qubit using the three-qubit phase flip code:

$$|0\rangle \to |+++\rangle\,, \quad |1\rangle \to |---\rangle$$

and then encode each of these qubits using the three-qubit bit-flip code:

$$|+\rangle \to \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \quad |-\rangle \to \frac{1}{\sqrt{2}}\,|000\rangle - |111\rangle\,.$$

Therefore the codewords of the Shor code are given as follows:

$$|0\rangle \to |0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \tag{5}$$

$$|1\rangle \to |1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \tag{6}$$

where $|0_L\rangle$ and $|1_L\rangle$ indicates logical $|0\rangle$ and logical $|1\rangle$ states. Now, we give the error correction procedure for this code. First, we show how the bit-flip error σ_x is corrected. Thus let us consider three-qubit bit-flip code with the following encoding,

$$|0\rangle \to |0_L\rangle = |000\rangle$$
$$|1\rangle \to |1_L\rangle = |111\rangle\,.$$

Thus the single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is encoded as $|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$. Let us consider the observable $\mathcal{O} = \{H_0, H_1, H_2, H_3\}$ where

$$H_0 = \mathrm{Span}_{\mathbb{C}}\{|000\rangle, |111\rangle\}, \quad H_1 = \mathrm{Span}_{\mathbb{C}}\{|100\rangle, |011\rangle\},$$
$$H_2 = \mathrm{Span}_{\mathbb{C}}\{|010\rangle, |101\rangle\}, \quad H_3 = \mathrm{Span}_{\mathbb{C}}\{|001\rangle, |110\rangle\}.$$

If the measurement of the encoded state $|\psi'\rangle$ yields 0 then no bit-flip error has occurred. Otherwise, if the measurement yields i, then a bit-flip error has occurred in the i-th bit. In other words after the measurement if $|\psi'\rangle \in H_0$ then there is no bit-flip error occurred. But if $|\psi'\rangle \in H_i$ then i-th bit is flipped. So, to correct the error that occurred in the i-th bit, that bit is flipped again. Now, if we consider the 3-qubit phase-flip code $Q = \mathrm{Span}_{\mathbb{C}}\{|+++\rangle, |---\rangle\}$ and use an observable similar to $\mathcal{O}$, we similarly correct the phase-flip errors.

4. Quantum Stabilizer Codes

Quantum stabilizer codes, introduced independently by Daniel Gottesman [11] and by Calderbank et al. [12] in the early 1990s, are an important class of quantum error-correcting codes. These codes, also known as additive codes, play a role similar to linear codes in classical coding theory. Quantum stabilizer codes have been extensively studied. Many well-known quantum error correcting codes are stabilizer codes. The Shor [7], Steane [14] codes, and CSS code [13] which are among the first quantum error-correcting codes, are binary quantum stabilizer codes. Additionally, they have also been studied in [51–55]. Then, the extension of binary quantum codes to qudits was given by Ashikhmin and Knill [15]. On the other hand, quantum stabilizer codes over finite fields were provided by Ketkar et al. [10] by characterizing non-binary stabilizer codes over $\mathbb{F}_q$ in terms of q-ary classical codes.

In quantum stabilizer codes, operators that stabilize the state are used instead of the state itself. Therefore, a more compact and efficient representation of quantum states is obtained. Focusing on stabilizer operators also simplifies the process of error detection and error

correction. For instance, consider the following codewords of 3-qutrit code,

$$\begin{aligned}|0\rangle_L &= \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle)\\ |1\rangle_L &= \frac{1}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle)\\ |2\rangle_L &= \frac{1}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle)\end{aligned}$$

and two operators XXX and ZZZ where ω is a primitive 3-rd root of unity

$$X = X(1) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, Z = Z(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}.$$

Then, these two operators have no effect on the codewords, that is $XXX\,|i\rangle_L = |i\rangle_L, ZZZ\,|i\rangle_L = |i\rangle_L$ for all $1 \leq i \leq 3$. It is said that the codewords $|0\rangle_L, |1\rangle_L, |2\rangle_L$ are stabilized by $\{XXX, ZZZ\}$.

Group theory concepts are used in the construction of stabilizer codes. Recall that the nice error basis $\mathcal{E}_n = \{X(a)Z(b) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$. If we define $\mathcal{P}_n = \{w^c X(a)Z(b) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}$, where ω is a p-th root of unity, then $\mathcal{P}_n$ is a finite group and its order is pq^{2n} for $p > 2$. When $p = 2$, we take $\omega = i$, the complex unit, with $c = 0, 1, 2, 3$; therefore the order of $\mathcal{P}_n$ is $4q^{2n}$.

Definition 2.10. Let Q be a quantum q-ary code of length n. Then the subgroup

$$\mathrm{Stab}(Q) = \{E \in \mathcal{P}_n : E\,|\psi\rangle = |\psi\rangle \text{ for all } |\psi\rangle \in Q\}$$

of $\mathcal{P}_n$ is called the stabilizer group of Q.

In addition, for a non-trivial quantum code Q, not all subgroups of $\mathcal{P}_n$ may be stabilizer groups, observe that $\mathrm{Stab}(Q)$ satisfies the following two conditions for any non-trivial code Q.

(i) Let ω be a primitive p-th root of unity and $c \in \mathbb{F}_p$, then $\omega^c I \notin \mathrm{Stab}(Q)$, since for all $|\psi\rangle \in Q, \omega^c I |\psi\rangle = \omega^c |\psi\rangle = |\psi\rangle$ would give $|\psi\rangle = 0$ or $\omega^c = 1$. Therefore, we can also say $\mathrm{Stab}(Q) \cap Z(\mathcal{P}_n) = I$.

(ii) $\mathrm{Stab}(Q)$ is an abelian subgroup of $\mathcal{P}_n$. If $E, F \in \mathrm{Stab}\, Q$ and $EF = \omega^c FE$ then $|\psi\rangle = EF |\psi\rangle\, \omega^c FE |\psi\rangle = \omega^c |\psi\rangle$ for all $|\psi\rangle \in \mathcal{Q}$, which yields $|\psi\rangle = 0$ or $\omega^c = 1$. Since Q is not a trivial $\omega^c = 1$, and thus $\mathrm{Stab}(Q)$ must abelian.

Conversely, suppose that S is a subgroup of $\mathcal{P}_n$ that satisfies the above two conditions. Then we can define a quantum code as follows,

$$\mathrm{Fix}(S) = \{|\psi\rangle \in (\mathbb{C}^q)^{\otimes n} : E |\psi\rangle = |\psi\rangle \text{ for all } E \in S\} = \bigcap_{E \in S} eig(E, 1).$$

In other words, the quantum code defined above is the joint eigenspace of all the operators with eigenvalue1 in the stabilizer group S. From the definition, if Q is a quantum code then it can be seen that $Q \subseteq \mathrm{Fix}(\mathrm{Stab}(Q))$. If the equality holds then, Q is called a *quantum stabilizer code*. Equivalently, there exists a subgroup S of $\mathcal{P}_n$ that satisfies the conditions (i) and (ii), and $\mathrm{Fix}(S) = Q$ if and only if Q is a quantum stabilizer code.

Now, let Q be a q-ary quantum stabilizer code of length n and $\mathrm{Stab}(Q) = S$. Then the dimension of Q is $q^n/|S|$ (see [16]). If S is generated by $\{s_1, s_2, \ldots, s_r\}$, which are independent stabilizer generators, then $|S| = q^r$, which gives that $\dim(Q) = q^{n-r}$. Therefore Q encodes n logical qudits into $m = n - r$ physical qudits, that is Q is $[\![n, n-r]\!]_q$-code.

The r stabilizer generators can be considered as the check operators of the code since they are used to identify and detect errors in the code. If the state remains undamaged during the transmission, the measurement outcome is $+1$; otherwise, the measurement outcome is an element of $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$, where ω is a primitive p-th root of unity.

For quantum codes, an error E is detectable by a quantum code Q if and only if $\langle c_1, c_2\rangle = \lambda_E \langle c_1, c_2\rangle$ for all $c_1, c_2 \in Q$. Before providing the characterization of detectable errors in quantum stabilizer codes, we need some group theory concepts. Let $C_{\mathcal{P}_n}(S)$ denote the

centralizer of S in $\mathcal{P}_n$, where S is a subgroup of $\mathcal{P}_n$. Also $SZ(\mathcal{P}_n)$ is the group generated by the subgroups S and $Z(\mathcal{P}_n)$ where $Z(\mathcal{P}_n)$ is the center of $\mathcal{P}_n$.

Proposition 2.11. *[10] Suppose that $S \leq \mathcal{P}_n$ is the stabilizer group of a stabilizer code Q of dimension $\dim(Q) > 1$. An error $E \in \mathcal{P}_n$ is detectable by the quantum code Q if and only if either E is an element of $SZ(\mathcal{P}_n)$ or does not belong to the centralizer $C_{\mathcal{P}_n}(S)$.*

In other words, a quantum code Q with the stabilizer group S can determine errors that are either a scalar multiple of the elements in S or do not commute with at least one element in S. Therefore, the classification of the commuting elements in $\mathcal{P}_n$ is important. First, we identify the following group homomorphism from the multiplicative group $\mathcal{P}_n$ onto the additive group $\mathbb{F}_q^{2n}$,

$$\psi : \mathcal{P}_n \to \mathbb{F}_q^{2n},\ \omega^c X(a)Z(b) \to (a \mid b). \tag{7}$$

Let $E = \omega^c X(a)Z(b)$ and $E' = \omega^{c'} X(a')Z(b')$ be elements of $\mathcal{P}_n$. Then, since

$$EE' = \omega^{\mathrm{tr}(ba' - b'a)} E'E,$$

the errors E and E' commute if and only if $\mathrm{tr}(ba' - b'a) = 0$. This leads to the definition of a function from $\mathbb{F}_q^{2n} \times \mathbb{F}_q^{2n}$ to $\mathbb{F}_p$ by

$$\langle (a \mid b), (a' \mid b') \rangle_s := \mathrm{tr}(ba' - b'a)$$

called the *trace symplectic inner product*. Hence the errors $\omega^c X(a)Z(b)$ and $\omega^{c'} X(a')Z(b')$ in $\mathcal{P}_n$ commute if and only if the corresponding vectors (a, b) and (a', b') in $\mathbb{F}_q^{2n}$ are orthogonal with respect to the trace symplectic inner product, denoted by $(a, b) \perp_s (a', b')$. Suppose that $\bar{\mathcal{S}}$ is the image of $\mathcal{S}$ under ψ and $\mathcal{S}$ is a subgroup of $\mathcal{P}_n$. Then, the symplectic dual of $\mathcal{S}$ is defined as

$$\bar{\mathcal{S}}^{\perp_s} = \{(a \mid b) \in \mathbb{F}_q^{2n} : \langle (a \mid b), (s \mid t) \rangle_s = 0 \text{ for all } (s, t) \in \bar{\mathcal{S}}\}.$$

Note that, the weight of an error operator E in $\mathcal{P}_n$ of the form $\omega^c E_1 \otimes \ldots \otimes E_n$ is given by

$$\mathrm{wt}(E) =\mid \{i : E_i \neq I\} \mid,$$

that is, the number of non-identity tensor factors. The minimum distance of a quantum code Q is an essential factor since it is used to determine the maximum number of errors that code can reliably detect and correct. A quantum code with minimum distance d can detect errors in $\mathcal{P}_n$ with weight up to d, since a corrupted codeword with an error of weight d or more could be a valid codeword in the code,and therefore it is undetectable.

Considering a quantum code Q with the stabilizer group $\mathcal{S}$, we know that errors in $\mathcal{S}$ have no impact on the codewords. Additionally, we say from Proposition 2.11 that an error not in $C_{\mathcal{P}_n}(\mathcal{S})$ can be detected by the code. Therefore, the minimum distance of the quantum stabilizer code Q with stabilizer $\mathcal{S}$ is given as,

$$d(Q) = \begin{cases} \min\{\mathrm{wt}(E) \mid E \in C_{\mathcal{P}_n}(\mathcal{S}) \setminus \mathcal{S}\}, & \text{if } \mathcal{S} \subsetneq C_{\mathcal{P}_n}(\mathcal{S}) \\ \min\{\mathrm{wt}(E) \mid E \in \mathcal{S} \setminus \{I\}\}, & \text{if } \mathcal{S} = C_{\mathcal{P}_n}(\mathcal{S}). \end{cases}$$

Also a quantum code with minimum distance d can correct all errors with weight at most $\lfloor (d-1)/2 \rfloor$ (see, [16]). Note that, the image of $C_{\mathcal{P}_n}(\mathcal{S})$ under ψ is $\bar{\mathcal{S}}^{\perp_s}$. Then we define the symplectic weight of the vector $(\mathbf{a} \mid \mathbf{b})$ in $\mathbb{F}_q^{2n}$ as the weight of $X(\mathbf{a})Z(\mathbf{b})$ in $\mathcal{P}_n$. More specifically,

$$\mathrm{swt}(\mathbf{a} \mid \mathbf{b}) = |\{i : (a_i, b_i) \neq (0,0)\},$$

where $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$.

4.1. Stean code

The Steane code [8] was constructed in 1996 by Andrew Steane which is a quantum stabilizer code that encodes one logical qubit into seven physical qubits and it can correct all single-qubit error and detect up to two-qubits errors. It is constructed from $[7, 4, 3]$ classical

binary Hamming code and its dual. Also, this code corrects the bit-flip and phase-flip errors, separately which simplifies the error correction process.

The stabilizer generators of the Steane code are

$$\begin{array}{c|ccccccc} M_1 & X & X & X & X & I & I & I \\ M_2 & X & X & I & I & X & X & I \\ M_3 & X & I & X & I & X & I & X \\ M_4 & Z & Z & Z & Z & I & I & I \\ M_5 & Z & Z & I & I & Z & Z & I \\ M_6 & Z & I & Z & I & Z & I & Z \end{array}$$

and the logical operators $\bar{X} = XXXXXXX, \bar{Z} = ZZZZZZZ$. Then, with the stabilizer group of the code being $\mathcal{S}$, the basis codewords of the code are written as follows.

$$\begin{aligned} |0\rangle_L = \sum_{M \in \mathcal{S}} =& \frac{1}{2\sqrt{2}}(|0000000\rangle + |1111000\rangle + |1100110\rangle + |1010101\rangle \\ &+ |0011110\rangle + |0101101\rangle + |0110011\rangle + |1001011\rangle), \end{aligned}$$

$$\begin{aligned} |1\rangle_L = \bar{X}\,|0\rangle_L =& \frac{1}{2\sqrt{2}}(|0000111\rangle + |1111111\rangle + |1100001\rangle + |1010010\rangle \\ &+ |0011001\rangle + |0101010\rangle + |0110100\rangle + |1001100\rangle). \end{aligned}$$

One can see that the generator elements of $C_{\mathcal{P}_n}(\mathcal{S}) \setminus \mathcal{S}$ are $XXXIIII$ and $ZZZIIII$.

5. Butson-Hadamard Matrices

A Butson-Hadamard matrix of order n is an $n \times n$ square matrix whose entries are the complex root of unity such that $HH^\dagger = nI$, where I is the identity matrix of order n and $H^\dagger$ is the complex conjugate transpose of H. If all the entries are k-th roots of unity, then we write it as $\mathrm{BH}(n, k)$. Butson-Hadamard matrices were introduced by A.T. Butson in [17]. They generalize the Hadamard matrices, which have entries of ± 1 and satisfy the condition $HH^T = nI_n$. Butson-Hadamard matrices are used in constructing orthogonal arrays and difference sets, which are important in experimental designs, error correction and cryptography, for more information see [18], [19], [20], [21].

Let $H = [\zeta^{a_{ij}}]$ be a $\mathrm{BH}(n, k)$ matrix. Then we denote its logarithmic form as $L_\zeta(H) = [a_{ij}]$, where ζ is a k-th primitive root of unity. This representation provides convenience in the description of the codes we obtain over $\mathbb{Z}_k$.

Suppose that H_1 and H_2 are two $\mathrm{BH}(n, k)$ matrices. If one can be obtained from other by row or column permutations or by multiplying all entries in a row or a column by the same primitive root of unity, then these two matrices are said to be equivalent. Every BH matrix is equivalent to a BH matrix with its first row and first column consisting of 1's. Matrices of this form are called *normalized*.

Note that when ζ is a primitive n-th root of unity, then the $n \times n$ Fourier matrix $\mathcal{F}_n = [\zeta^{(i-1)(j-1)}]_{i,j=1}^n$ is a normalized $\mathrm{BH}(n, n)$ matrix.

Example 2.7. *Let ζ be a primitive 6-th root of unity then*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^4 & \zeta^5 & \zeta^3 & \zeta^3 & \zeta \\ 1 & \zeta^4 & \zeta & \zeta^3 & \zeta^5 & \zeta^3 & \zeta \\ 1 & \zeta^5 & \zeta^3 & \zeta & \zeta^4 & \zeta & \zeta^3 \\ 1 & \zeta^3 & \zeta^5 & \zeta^4 & \zeta & \zeta & \zeta^3 \\ 1 & \zeta^3 & \zeta^3 & \zeta & \zeta & \zeta^4 & \zeta^5 \\ 1 & \zeta & \zeta & \zeta^3 & \zeta^3 & \zeta^5 & \zeta^4 \end{pmatrix}, \quad L(H) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 4 & 5 & 3 & 3 & 1 \\ 0 & 4 & 1 & 3 & 5 & 3 & 1 \\ 0 & 5 & 3 & 1 & 4 & 1 & 3 \\ 0 & 3 & 5 & 4 & 1 & 1 & 3 \\ 0 & 3 & 3 & 1 & 1 & 4 & 5 \\ 0 & 1 & 1 & 3 & 3 & 5 & 4 \end{pmatrix}$$

H and $L(H)$ are respectively a normalized $\mathrm{BH}(7,6)$ matrix and its logaritmic form.

The difference matrices introduced by Drake [56] are used to construct Butson-Hadamard matrices. A matrix $D = [d_{ij}], i = 1, \ldots r, ; j = 1, \ldots k\lambda$ with entries from the group G of order k is called an $(k, k\lambda; \lambda, G)$-difference matrix if each element of G occurs λ times in the sequence $\{d_{it} - d_{jt}\}_{t=1}^{k\lambda}$ for all $1 \leq i \neq j \leq r$, see [57]. Generalized Hadamard matrices, which are a special case of difference matrices, coincide with the logarithmic forms of Butson-Hadamard matrices under certain conditions. A generalized Hadamard matrix H in the sense of Drake is a $k\lambda \times k\lambda$ square matrix whose entries are the elements of a group G of order k, such that H and H^T are $(k, k\lambda; \lambda, G)$-difference matrices and denoted by $\mathrm{GH}(k, G)$ (see also [18], Definition 4.9, where G is considered multiplicative). Note that, if the multiplicative group $\mathcal{C}_p$ of all p-th roots of unity is taken as the group G, where p is prime, then the BH matrices over G coincide with the GH matrices. Furthermore, in this case, the logarithmic forms of $\mathrm{BH}(p\lambda, p)$ matrices coincide with the $p\lambda \times p\lambda$ GH matrices over $\mathbb{Z}_p$. In addition, if $G = \mathbb{Z}_k$, then every $\Lambda = [\lambda_{ij}]$ matrix of dimension $k\lambda$ is the logarithmic form of the $\mathrm{BH}(k\lambda, k)$ matrix.

Example 2.8. *Suppose that $G = \mathcal{C}_5$ is the cyclic group of order 5 and ζ is a generator of G then the following matrix is a* $\mathrm{GH}(5, \mathcal{C}_5)$*,*

$$H = \begin{pmatrix} 1 & \zeta & \zeta^4 & \zeta^4 & \zeta \\ \zeta & 1 & \zeta & \zeta^4 & \zeta^4 \\ \zeta^4 & \zeta & 1 & \zeta & \zeta^4 \\ \zeta^4 & \zeta^4 & \zeta & 1 & \zeta \\ \zeta & \zeta^4 & \zeta^4 & \zeta & 1 \end{pmatrix}.$$

Indeed, for $H = [h_{ij}]$, the difference set of the first two rows $\{h_{1j}h_{2j}\}_{j=1}^{5} = \{\zeta^4, \zeta, \zeta^3, 1, \zeta^2\}$ contains all elements of the group exactly once. Similarly, the pairwise difference sets of all rows can be also obtained. Moreover, since H is symmetric, we say that H is $\mathrm{GH}(5, \mathcal{C}_5)$*.*

Chapter 3

Equivalence of Butson-Hadamard Matrices

In this section, it has been established that BH matrices, which satisfy a condition on the powers of the roots of unity at their entries, are equivalent. Moreover, it has been stated that these matrices are also equal to a Kronecker product of Fourier matrices.

The conditions under which BH matrices exist and the equivalence problem of these matrices have been studied by various researchers. Among them are Ferenc Szöllesi, who demonstrated the existence of the $\mathrm{BH}(19, 6)$ matrices [58], and Ronan Egan and Patraig O Cathain [59], and Patric R. G. Östergard [60] who provided results on the classification of BH matrices.

First, we introduce some concepts that we used to obtain the results. Let $J(R)$ denote the intersection of all maximal left ideals of a finite ring R, which is known as the Jacobson radical of R. This is also equal to the intersection of all maximal right ideals. Furthermore, let $soc({}_R R)$ denote the sum of all left ideals of the ring R. Similarly, let $soc(R_R)$ denote the sum of all right ideals of R. Finally, if we denote by $\widehat{R}$ the character group of the additive group of R, that is the set of all $\mathbb{Z}$-homomorphisms from R to $\mathbb{C} - \{0\}$, then $\widehat{R}$ has the

structure of an $R - R$ bimodule by defining $\chi^r(x) := \chi(rx)$ and ${}^r\chi(x) := \chi(xr)$ for all $r, x \in R$ and $\chi \in \widehat{R}$.

Definition 3.1. [3] A finite ring R that satisfies the following equivalent conditions is called a Frobenius ring.

i. $R\ J(R)$ and $soc({}_RR)$ are isomorphic left R-modules.

ii. $R\ J(R)$ and $soc(R_R)$ are isomorphic right R-modules

iii $soc({}_RR)$ is left principal.

iv. $soc(R_R)$ is right principal.

v. $\widehat{R}$ and R are isomorphic as left R modules.

vi. $\widehat{R}$ and R are isomorphic as right R modules.

Definition 3.2. Let B be a bilinear form on an M module. If $B(v, w) = 0 \Rightarrow w = 0$, then B is called a non-degenerate bilinear form.

Throughout this chapter, R will denote a finite Frobenius ring and M a finite R-bimodule. We also denote the set of all non-degenerate bilinear forms on M by $\mathrm{BLF}(M)$.

Let $B : M \times M \longrightarrow R$ be a non-degenerate bilinear form on M. Associated to B are there right R-module homomorphisms, for all $x \in M$, defined by

$$B(x): \qquad M \longrightarrow R$$

$$y \longmapsto B(x, y)$$

that is $B(x)(y) = B(x, y)$ for all $x, y \in M$. It follows that $B(x) \in M^* = \mathrm{Hom}(M_R, R_R)$ for every $x \in M$. Note the following properties:

- $B(x_1 + x_2) = B(x_1) + B(x_2)$ for all $x_1, x_2 \in M$.

- $B(rx) = rB(x)$ in the left R-module $M^*$for all $r \in R$ and $x \in M$.
- $B(x) = B(x')$ if and only if $x = x'$ for all $x, x' \in M$.
- $M^* = \{B(x) : x \in M\}$.

Let $\mathrm{Aut}({}_RM)$ (respectively, $\mathrm{Aut}(M_R)$) denote the group of left (respectively, right) R-module automorphisms of M, equipped with the usual composition of maps. Given $\gamma \in \mathrm{Aut}({}_RM)$ and $\eta \in \mathrm{Aut}(M_R)$, one can define two mappings assosiated with B as follows:

$$B' : M \times M \longrightarrow R$$

$$(x, y) \longmapsto B(\gamma(x), y)$$

$$B'' : M \times M \longrightarrow R$$

$$(x, y) \longmapsto B(x, \eta(y))$$

Observe that both B' and B'' are non-degenerate bilinear forms. Thus both groups $\mathrm{Aut}({}_RM)$ and $\mathrm{Aut}(M_R)$ act on $\mathrm{BLF}(M)$. We write $B' = B \cdot \gamma$ and $B'' = B \cdot \eta$.

Theorem 3.3. *Let B be any non-degenerate bilinear form on M. Then we have*

$$\begin{aligned}\mathrm{BLF}(M) &= \{B \cdot \gamma : \gamma \in \mathrm{Aut}({}_RM)\} \\ &= \{B \cdot \eta : \eta \in \mathrm{Aut}(M_R)\}.\end{aligned}$$

Proof. The arguments above the theorem show that $\{B \cdot \gamma : \gamma \in \mathrm{Aut}({}_RM)\}$ lies in $\mathrm{BLF}(M)$.

Conversely, let B' be any other non-degenerate bilinear form on M. We shall show that $B' = B \cdot \gamma$ for a suitable $\gamma \in \mathrm{Aut}({}_RM)$.

Let $M = \{0, x_1, \ldots, x_n\}$. Since $M^* = \{B(0), B(x_1), \ldots, B(x_n)\} = \{B'(0), B'(x_1), \ldots, B'(x_n)\}$, there exists $\sigma \in S_n$ such that $B'(x_i) = B(x_{\sigma(i)})$. Now define

$\gamma : M \to M$ by $\gamma(0) = 0$ and $\gamma(x_i) = x_{\sigma(i)}$ for each $i = 1, \ldots, n$. Notice that

$$B'(x, y) = B(\gamma(x), y)$$

for all $x, y \in M$. Thus we complete the proof by showing that $\gamma \in \mathrm{Aut}({}_R M)$.

Let $x_i + x_j = x_k$. Since

$$\begin{aligned} B(x_{\sigma(k)}) &= B'(x_k) \\ &= B'(x_i + x_j) \\ &= B'(x_i) + B'(x_j) \\ &= B(x_{\sigma(i)}) + B(x_{\sigma(j)}) \\ &= B(x_{\sigma(i)} + x_{\sigma(j)}) \end{aligned}$$

we have $x_{\sigma(i)} + x_{\sigma(j)} = x_{\sigma(k)}$. It follows that

$$\gamma(x_i + x_j) = \gamma(x_k) = x_{\sigma(k)} = x_{\sigma(i)} + x_{\sigma(j)} = \gamma(x_i) + \gamma(x_j),$$

i.e. γ is additive. On the other hand if $r \in R$ and $rx_i = x_j$, then

$$\begin{aligned} B(x_{\sigma(j)}) &= B'(x_j) \\ &= B'(rx_i) \\ &= rB'(x_i) \\ &= rB(x_{\sigma(i)}) \\ &= B(rx_{\sigma(i)}), \end{aligned}$$

hence $x_{\sigma(j)} = rx_{\sigma(i)}$, which yields

$$\gamma(rx_i) = \gamma(x_j) = x_{\sigma(j)} = rx_{\sigma(i)} = r\gamma(x_i),$$

as desired. This completes the proof of the first equality. By symmetric arguments, one easily prove the other equality. □

Proposition 3.4. *Let χ be a generating character of R and let B, B' be two non-degenerate bilinear forms of the R-bimodule $M = \{x_0 = 0, x_1, \ldots, x_n\}$. Then the matrices*

$$H = [\chi(B(x_i, x_j))]_{0 \leq i,j \leq n}$$

and

$$H' = [\chi(B'(x_i, x_j))]_{0 \leq i,j \leq n}$$

are equivalent (by row permutation).

Proof. There exists an $\sigma \in S_n$ such that $B'(x_i, x_j) = B(x_{\sigma(i),x_j})$ for all $0 \leq i, j \leq n$ by the proof of Theorem 3.3. Thus $H' = [\chi(B'(x_i, x_j))] = [B(x_{\sigma(i)}, x_j)]$ is H with rows permuted by σ. □

Lemma 3.5. *Let χ and χ' be two generating characters of the ring R. Then there exists a unit element $a \in R$ such that $\chi' = \chi^a$.*

Proof. Since χ is a generating character then there exists an element a of R such that $\chi' = \chi a$. Similarly, there exists an element a' of R such that $\chi = \chi' a'$. Therefore $\chi(1 - aa') = 0$ and $\chi \neq 0$. Then $\chi' = \chi a = \chi^a$ and a is a unit element of R.

□

Proposition 3.6. *Let χ and χ' be two generating characters of the ring R and let B be a non-degenerate bilinear form on the R-bimodule $M = \{x_0 = 0, x_1, \ldots, x_n\}$. Then the matrices*

$$H = [\chi(B(x_i, x_j))]_{0 \leq i,j \leq n}$$

and

$$H' = [\chi'(B(x_i, x_j))]_{0 \leq i,j \leq n}$$

are equivalent (by row permutation).

Proof. By above lemma, there exists a unit element $a \in R$ such that $\chi' = \chi^a$. Since a is unit, we have $aM = M$. It follows that there exists $\sigma \in S_n$ such that $ax_i = x_{\sigma(i)}$ for all $i = 1, \ldots, n$. Now

$$H' = [\chi'(B(x_i, x_j))] = [\chi^a(B(x_i, x_j))] = [\chi(aB(x_i, x_j))] = [\chi(B(ax_i, x_j))] = [\chi(B(x_{\sigma(i)}, x_j))]$$

is clearly the matrix $[\chi(B(x_i, x_j))]$ with rows permuted by σ. □

Proposition 3.7. *For the R-bimodule $M = \{x_0 = 0, x_1, \ldots, x_n\}$, the matrices of the form*

$$[\chi(B(x_i, x_j))]_{0 \le i,j \le n},$$

where χ is a generating character of R and $B : M \times M \to R$ is a non-degenerate bilinear form on M, are all equivalent.

Proof. For every non-degenerate bilinear form B' on M distinct from B according to Proposition 3.4, $H' = [\chi(B'(x_i, x_j))]_{0 \le i,j \le n}$ is equivalent to H. Similarly for every χ' distinct from χ according to Proposition 3.6, $H'' = [\chi'(B(x_i, x_j))]_{0 \le i,j \le n}$ is equivalent to H. This completes the proof. □

Corollary 3.8. *Let $H = [\omega^{f_i(\mathbf{c}_j)}]_{1 \le i,j \le q^k}$, where $\omega = e^{2\pi i/p}$ and $f_i : \mathscr{C} \to \mathbb{F}_p$ is a linear transformation for each $1 \le i \le q^k$. Then H is equivalent to a Kronecker product of Fourier matrices.*

Proof. Since $f_i \in \mathcal{L}(\mathscr{C}, \mathbb{F}_p)$ for $1 \le i, j \le q^k$ and $\mathscr{C}$ is isomorphic to $\mathbb{F}_{q^k}$ then we use the composition of $\mathbb{F}_p$-space isomorphisms $\kappa : \mathscr{C} \to \mathbb{F}_{q^k} \to \mathcal{L}(\mathscr{C}, \mathbb{F}_p)$. Let $B : \mathscr{C} \times \mathscr{C} \to \mathbb{F}_p$ be a transformation defined as $B(c, c') = f_i(c')$ such that $\kappa(c) = f_i$. Then B is a non-degenerate bilinear form. Also $\chi : \mathbb{F}_p \to \mathbb{C} - \{0\}, \chi(a) = \omega^a$ is a generating character for $\mathbb{F}_p$. If we combine these we say $H = [\omega^{f_i(\mathbf{c}_j)}]_{1 \le i,j \le q^k} = [\chi(B(c_i, c_j))]_{1 \le i,j \le q^k}$. On the other hand $B' : \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \to \mathbb{F}_{q^k}, B(i, j) = ij$ is a non-degenerate bilinear form and $\chi' : \mathbb{F}_{q^k} \to \mathbb{C} - \{0\}, \chi'(a) = \omega^a$ is a generating character. Then the Fourier matrix $F_{ij} = [\omega^{ij}] = [\chi'(B'(i, j))]_{1 \le i,j \le q^k}$. The desired result is obtained by Proposition 3.7. □

Chapter 4

New Results on Weight Functions

1. Quasi-homogeneous weight function

In this section, we begin with the definition of new weight function over finite commutative rings, which we call quasi-homogeneous weight. This weight belongs to the set of non-homogeneous weights, but it possesses crucial properties as homogeneous ones.

Definition 4.1. A weight w on the commutative finite ring R is called *quasi-homogeneous* if $w(0) = 0$ and there exists a real number γ such that

$$\sum_{r \in a+I} w(r) = \gamma |I|,$$

for each $a \in R$ and each non-zero ideal I of R. The number γ is called the *average value* of w.

Proposition 4.2. *Let e be a positive integer and γ be a positive real number. Define a mapping $w : \mathbb{Z}_{p^e} \to \mathbb{R}$ by*

$$w(u) = \begin{cases} \frac{\gamma}{p^{e-2}(p-1)}u, & \text{if } u_{e-1} = 0 \\ \frac{\gamma p}{p-1}, & \text{if } 0 < u_{e-1} \leq p-2 \\ \frac{\gamma p^2}{p-1} - \frac{\gamma}{p^{e-2}(p-1)}u, & \text{if } u_{e-1} = p-1 \end{cases}$$

for all $u \in \mathbb{Z}_{p^e}$ with the p-ary expansion $u = u_0 + u_1 p + \cdots + u_{e-1}p^{e-1}$. Then w is a quasi-homogeneous weight on $\mathbb{Z}_{p^e}$ with the average value γ.

Proof. Fix $0 \leq s \leq e-1$. We show that for any $a \in \mathbb{Z}_{p^e}$,

$$\sum_{u \in a + \langle p^s \rangle} w(u) = \gamma p^{e-s},$$

which completes the proof. Note that it is enough to assume $0 \leq a \leq p^s - 1$. Note also that for any $u \in a + \langle p^s \rangle$, there exists a unique $n \in \mathbb{Z}_{p^e}$ such that $0 \leq n \leq p^{e-s} - 1$ and $u = a + np^s$. Write $a = a_0 + a_1 p + \cdots + a_{s-1}p^{s-1}$ and $n = n_0 + n_1 p + \cdots + n_{e-s-1}p^{e-s-1}$, where $0 \leq a_i, n_j \leq p-1$ for each $i = 0, \ldots, s-1$ and $j = 0, \ldots, e-s-1$. Hence, a typical element u of $a + \langle p^s \rangle$ can be written uniquely as

$$u = a_0 + a_1 p + \cdots + a_{s-1}p^{s-1} + n_0 p^s + n_1 p^{s+1} + \cdots + n_{e-s-2}p^{e-2} + n_{e-s-1}p^{e-1},$$

where the a_i's and n_j's all lie in $\{0, \ldots p-1\}$. We separate the sum of $w(u)$'s, where u ranges over $a + \langle p^s \rangle$, into three sums as follows:

(I) The sum of the $w(u)$'s for $u \in a + \langle p^s \rangle$ with $n_{e-s-1} = 0$, i.e.,

$$\frac{\gamma}{p^{e-2}(p-1)} \left[p^{e-s-1}a + p^s \frac{p^{e-s-1}(p^{e-s-1}-1)}{2} \right];$$

(II) the sum of the $w(u)$'s for $u \in a + \langle p^s \rangle$ with $0 \le n_{e-s-1} \le p-2$, i.e.,

$$\frac{\gamma p(p-2)p^{e-s-1}}{p-1};$$

(III) the sum of the $w(u)$'s for $u \in a + \langle p^s \rangle$ with $n_{e-s-1} = p-1$, i.e.,

$$\frac{\gamma p^2 p^{e-s-1}}{p-1} - \frac{\gamma}{p^{e-2}(p-1)} \left[p^{e-s-1}a + \frac{p^s p^{e-s-1}(p^{e-s-1}-1)}{2} + p^{e-s-1}(p-1)p^{e-1} \right].$$

It is now easy to see that the numbers in (I)–(III) sum up to γp^{e-s}. □

In [33], a Gray map (denoted G_2 in this chapter) on $\mathbb{Z}_{p^e}$ (for a prime number p) has been introduced as a generalization of the Gray map on $\mathbb{Z}_4$ as follows: For $u \in \mathbb{Z}_{p^e}$,

(i) if $u \le p^{e-1}$, then $G_2(u) \in \mathbb{Z}_p^{p^{e-1}}$ has 1's in the first u locations and 0's elsewhere;

(ii) if $u > p^{e-1}$, then $G_2(u) = \bar{q} + G_2(r)$, where q and $r < p^{e-1}$ are positive integers such that $u = qp^{e-1} + r$ and $\bar{q} = (q, q, \ldots, q, q) \in \mathbb{Z}_p^{p^{e-1}}$.

Let w_2 be the weight on $\mathbb{Z}_{p^e}$ defined by $w_2(u) = w_h(G_2(u))$. Then we have

$$w_2(u) := \begin{cases} u, & \text{if} \quad u \le p^{e-1} \\ p^{e-1}, & \text{if} \quad p^{e-1} \le u \le p^e - p^{e-1} \\ p^e - u, & \text{if} \quad p^e - p^{e-1} < u \le p^e. \end{cases}$$

It is now easy to see, by Proposition 4.2, that w_2 is a quasi-homogeneous weight (that is not homogeneous) with the average value $\gamma = p^{e-2}(p-1)$.

Define the distance function d_2 on $\mathbb{Z}_{p^e}$ by

$$d_2(u, v) = w_2(u - v)$$

for $u, v \in \mathbb{Z}_{p^e}$. Then $G_2 : (\mathbb{Z}_{p^e}, d_2) \to (\mathbb{Z}_p^{p^{e-1}}, d_h)$ is a distance preserving map, where d_h denotes the Hamming distance (see [33, Theorem 2.1]).

Remark 4.3. We see that both weights w_1 and w_2 share the same average value $\gamma = (p-1)p^{e-2}$. In fact, w_1 is the only homogeneous weight on $\mathbb{Z}_{p^e}$ with the average value $\gamma = (p-1)p^{e-2}$, see Theorem 2.2 in [3]. It follows that our consideration of quasi-homogeneous weights enables us to work with some non-homogeneous weights with the same common average value and flourishes our repository of weights in this manner.

Chapter 5

Butson-Hadamard codes

In this section, we present the results we obtained regarding Butson-Hadamard codes defined over finite rings. Interest in codes over finite rings has increased with the discovery that nonlinear codes such as Kerdock and Preparata can be obtained as the images of codes over $\mathbb{Z}_4$ under the Gray map [4]. Here we will present the results we obtained regarding the parameters of BH codes with different weight functions.

The codes we consider in this chapter are defined over rings $\mathbb{Z}_k$. Any non-empty subset of $\mathbb{Z}_k^n$ of size M will be called a k-ary (n, M) code. We follow the definitions from [61] to obtain codes over $\mathbb{Z}_k$ from a normalized BH matrix. Let H be a normalized BH(n, k) matrix and $L(H)$ its logarithmic form. Also, let N denote the multiplicative group of all k-th roots of unity. We define four types of k-ary codes as follows:

$\mathcal{A}_k$**:** k-ary $(n-1, n, d_A)$ code consisting of the rows of $L(H)$ with the first column deleted,

$\mathcal{B}_k$**:** k-ary $(n-1, nk, d_B)$ code consisting of the rows of the logarithmic form $L(\alpha H)$ of the translate αH, for all $\alpha \in N$, with the first column deleted,

$\mathcal{C}_k$**:** k-ary (n, nk, d_C) code consisting of the rows of the logarithmic form $L(\alpha H)$ of the translate αH, for all $\alpha \in N$,

$\mathcal{D}_k$**:** k-ary $(n+1, n^2, d_D)$ code, with $k = n$, consisting of the rows of the block matrix $[L(\alpha H) \mid \boldsymbol{c}]$ for all $\alpha \in N$, where $\boldsymbol{c}$ is a fixed non-initial column of $L(H)$.

Note that the deletion of the first column of $L(H)$ in defining codes of type $\mathcal{A}_k$ has no impact on the distance since the first coordinates of the lines of $L(H)$ are all zero.

Any code of type $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, or $\mathcal{D}_k$ is generally referred to as a BH code obtained from the normalized BH(n, k) matrix H. For the sake of simplicity, we denote the minimum distance of a BH code (with respect to a specified distance or weight function) by d_A, d_B, d_C, or d_D according to its type, being $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, or $\mathcal{D}_k$, respectively, with no reference to k and the distance function when they are trivial from the context.

In the first section of this chapter, we study codes obtained from Butson-Hadamard (BH) matrices and their translates under an homogeneous weight. Then, in the second section, we define quasi-homogeneous weight and study the parameters of codes obtained from BH matrices under a certain quasi-homogeneous weight.

1. BH codes with homogeneous weights

In this section we study the minimum distance of BH codes with respect to homogeneous weights. The following arguments, based on facts from [62], are repeatedly used in the sequel.

Given a BH(n, k) matrix $H = [\zeta^{a_{ij}}]$, where ζ is a primitive k-th root of unity, we have $\zeta^{a_{i1}-a_{j1}} + \cdots + \zeta^{a_{in}-a_{jn}} = 0$ for each pair (i, j) with $1 \leq i \neq j \leq n$. It is proved in [62] that if k has prime factorization $p_1^{e_1} \dots p_s^{e_s}$, then the number of terms in such a vanishing sum of powers of ζ is of the form $m_1 p_1 + \cdots + m_s p_s$, where each m_i $(1 \leq i \leq s)$ is a non-negative integer. Suppose that p_1 is the smallest prime divisor of k. Then $1 + \zeta_{p_1} + (\zeta_{p_1})^2 + \ldots + (\zeta_{p_1})^{p_1-1} = 0$, where $\zeta_{p_1} = \zeta^{k/p_1}$, and there are at least p_1 terms in a vanishing sum of powers of ζ. This yields that in any vanishing sum of powers of ζ with n terms, the number of 1's (equivalently, the number of a certain power ζ^a of ζ) cannot exceed n/p_1. In particular, the

number of columns with the same entry in two rows is at least n/p_1. Moreover; if $r = 1$, that is, $k = p^e$ is a power of a prime p, then any vanishing sum of powers of ζ is obtained from the relation $1 + \zeta_p + \ldots + \zeta_p^{p-1} = 0$ by addition and rotation. In particular, the difference of the i-th and j-th rows of $L(H)$, i.e., $[a_{i1} - a_{j1} \ldots a_{in} - a_{in}]$, is a disjoint union of cosets of the ideal $p^{e-1}\mathbb{Z}_{p^e}$ in $\mathbb{Z}_{p^e}$. For a detailed explanation see Corollary 3.4 and the paragraph after Theorem 2.2 in [62].

Although this section is reserved for investigations of BH codes equipped with distance functions induced by homogeneous weights, we start with the usual Hamming distance and give lower bounds for the minimal distances of BH codes.

Theorem 5.1. *Let H be a normalized $\mathrm{BH}(n, k)$ matrix. Then for a BH code obtained from H we have $d_A \geq n - \frac{n}{l}$, $d_B \geq n - \frac{n}{l} - 1$, $d_C \geq n - \frac{n}{l}$, and $d_D \geq n - \frac{n}{l}$, where $l = \min\{i \geq 2 : i|k\}$.*

Proof. Let ζ be a k-th primitive root of unity and suppose that $H = [\zeta^{a_{ij}}]$. Then there are at least l terms in a vanishing sum of powers of ζ and the number of columns with the same entry in two rows of H cannot exceed $\frac{n}{l}$ by arguments given before the theorem. That is, $n - d_A \leq \frac{n}{l}$, and so $d_A \geq n - \frac{n}{l}$.

Let α and β be different powers of ζ. As in the preceding paragraph, one can obtain that the distance between two rows of αH (or βH) is at least $n - \frac{n}{l}$. Let R_i denote the i-th row of H, for $i = 1, 2, \ldots, n$, with the first column deleted. Clearly, $d_h(\alpha R_i, \beta R_i) = n-1$. (Recall that d_h denotes the Hamming distance.) On the other hand, the number of the coordinates with the same entry between αR_i and βR_j is the same as the number of the terms equal to $\alpha^{-1}\beta$ in the vanishing sum $\zeta^{a_{i1}-a_{j1}} + \cdots + \zeta^{a_{in}-a_{jn}} = 0$. So, by a similar argument as the one used above, one can see that $d_h(\alpha R_i, \beta R_j) \geq n - 1 - \frac{n}{l}$ for $i \neq j$. It follows that $d_B \geq n - 1 - \frac{n}{l}$. Similarly, one can obtain that $d_C \geq n - \frac{n}{l}$ since $\mathcal{C}_k$ has codewords of length n.

Finally, since the codewords in $\mathcal{D}_k$ are obtained by adding an extra coordinate to the codewords of $\mathcal{C}_k$ we have $d_D \geq d_C \geq n - \frac{n}{l}$. □

Example 5.1. *Let ζ be a primitive 10-th root of unity and*

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta^5 & \zeta^3 & \zeta^3 & \zeta^5 & \zeta^9 & \zeta^8 & \zeta^7 & \zeta \\ 1 & \zeta^4 & \zeta^5 & \zeta^7 & \zeta & \zeta^3 & \zeta^5 & \zeta^9 & \zeta^9 \\ 1 & \zeta^3 & \zeta^7 & \zeta^5 & \zeta & \zeta^8 & \zeta^9 & \zeta^3 & \zeta^5 \\ 1 & \zeta^9 & \zeta & \zeta^5 & \zeta^5 & \zeta^3 & \zeta^7 & \zeta^2 & \zeta^7 \\ 1 & \zeta^9 & \zeta^5 & \zeta & \zeta^3 & \zeta^5 & \zeta & \zeta^7 & \zeta^6 \\ 1 & \zeta & \zeta^7 & \zeta^9 & \zeta^6 & \zeta & \zeta^5 & \zeta^5 & \zeta^3 \\ 1 & \zeta^7 & \zeta^9 & \zeta^4 & \zeta^9 & \zeta^5 & \zeta^3 & \zeta^5 & \zeta \\ 1 & \zeta^5 & \zeta^2 & \zeta^9 & \zeta^7 & \zeta^7 & \zeta^3 & \zeta & \zeta^5 \end{pmatrix}, L(H_1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 3 & 3 & 5 & 9 & 8 & 7 & 1 \\ 0 & 4 & 5 & 7 & 1 & 3 & 5 & 9 & 9 \\ 0 & 3 & 7 & 5 & 1 & 8 & 9 & 3 & 5 \\ 0 & 9 & 1 & 5 & 5 & 3 & 7 & 2 & 7 \\ 0 & 9 & 5 & 1 & 3 & 5 & 1 & 7 & 6 \\ 0 & 1 & 7 & 9 & 6 & 1 & 5 & 5 & 3 \\ 0 & 7 & 9 & 4 & 9 & 5 & 3 & 5 & 1 \\ 0 & 5 & 2 & 9 & 7 & 7 & 3 & 1 & 5 \end{pmatrix}$$

be a $\mathrm{BH}(9, 10)$ *matrix, and* $L(H_1)$ *its logarithmic form. It can be verified that the minimum distance between the rows of* H_1 *is equal to* $d_A = 7$ *and satisfies* $d_A \geq n - \frac{n}{l}$*, where* $n = 9$ *and* $l = 2$*. Now consider* B_k*. In this case, we have* A_k *and its translates as codewords. If we calculate the minimum distance by SageMath, we get* $d_B = 5$ *and so* $d_B \geq n(1 - \frac{1}{l}) - 1$*. Again, by using SageMath, we can get that the minimum distance for* C_k *is* $d_C = 6$*, which satisfies* $d_C \geq n - \frac{n}{l}$*.*

Example 5.2. *Let* ζ *be a primitive* 6*-th root of unity. Then*

$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 \\ 1 & \zeta^2 & \zeta^4 & 1 & \zeta^2 & \zeta^4 \\ 1 & \zeta^3 & 1 & \zeta^3 & 1 & \zeta^3 \\ 1 & \zeta^4 & \zeta^2 & 1 & \zeta^4 & \zeta^2 \\ 1 & \zeta^5 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{pmatrix}, L(H_2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 4 & 0 & 2 & 4 \\ 0 & 3 & 0 & 3 & 0 & 3 \\ 0 & 4 & 2 & 0 & 4 & 2 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

is a $\mathrm{BH}(6, 6)$ *matrix. If we take the second column of* $L(H_2)$ *and calculate the minimum distance for* D_k *by SageMath, we get* $d_D = 4$*, so* $d_D \geq n(1 - \frac{1}{l})$ *holds.*

Remark 5.2. We note that it is possible to find a code with larger alphabet without decreasing the minimum distance by combining two BH matrices with the help of the Chinese Remainder Theorem. Let h, k be coprime positive integers, ζ, α and β be primitive h-th, k-th and hk-th roots of unity, respectively. Also let $H_1 = [\zeta^{a_{ij}}]$ and $H_2 = [\alpha^{b_{ij}}]$ be normalized $\mathrm{BH}(n, h)$ and $\mathrm{BH}(n, k)$ matrices, respectively. Let d_1 and d_2 be the minimum distance between the rows of $[a_{ij}]$ and between the rows of $[b_{ij}]$, respectively. Let $H = [\beta^{c_{ij}}]$ be the normalized matrix obtained from H_1 and H_2 such that $c_{ij} \equiv a_{ij} \mod h$ and $c_{ij} \equiv b_{ij} \mod k$. Then the minimum distance between the rows of $[c_{ij}]$ satisfies $d \geq \max\{d_1, d_2\}$.

In Theorem 5.1 above, we have given lower bounds for the minimum distance of BH codes with respect to the Hamming distance. In the following theorem, we obtain minimum distances of BH codes with respect to the distance induced by a homogeneous weight.

Theorem 5.3. *Let H be a normalized $\mathrm{BH}(n, k)$ matrix and let $k = p_1^{e_1} \dots p_s^{e_s}$ be the prime factorization of k, where $p_1 < \dots < p_s$. Then for the BH codes obtained from H equipped with a homogeneous weight w on $\mathbb{Z}_k$ with the average value γ, the following hold:*

(i) $d_A = n\gamma$

(ii) For $s > 1$,

(a) $d_B = n\gamma - \frac{p_1\gamma}{p_1-1}$ *if* $n \leq p_2$ *and* $d_B = (n-1)\gamma\left(1 - \frac{1}{(p_1-1)(p_2-1)}\right)$ *if* $n > p_2$;

(b) $d_C = d_D = n\gamma\left(1 - \frac{1}{(p_1-1)(p_2-1)}\right)$.

(iii) For $s = 1$,

(a) $d_B = n\gamma - \frac{p_1\gamma}{p_1-1}$,

(b) $d_C = d_D = n\gamma$.

Proof. (i) follows from Theorem 2.7.

For the proof of (ii) and (iii), set $\ell = \max\{w(a) : a \in \mathbb{Z}_k\backslash\{0\}\}$ and $\ell' = \min\{w(a) : a \in \mathbb{Z}_k\backslash\{0\}\}$. Let $H = [\zeta^{a_{ij}}]$, where ζ is a primitive k-th root of unity, and $R_i = [a_{i1} =$

$0, a_{i2}, \ldots, a_{in}]$ be the i-th row of $L(H)$. For $u \in \mathbb{Z}_k$, we denote the i-th row of $L(\zeta^u H)$ by $u + R_i$. That is, $u + R_i = [u + a_{i1} = u, u + a_{i2}, \ldots, u + a_{in}]$. Let d denote the distance function induced by w. The distance between the rows $u + R_i$ and $v + R_j$, for $u, v \in \mathbb{Z}_k$, is

$$d(u + R_i, v + R_j) = \sum_{t=1}^{n} w(u + a_{it} - v - a_{jt}) = \sum_{t=1}^{n} w(a_{it} - a_{jt} + (u - v)).$$

First, assume that $i \neq j$. We follow the same circle of ideas given in the proof of [3, Theorem 5.4]. For $r \in \mathbb{Z}_k$, let

$$f_r = \left|\{t \in \{1, \ldots, n\} : a_{it} - a_{jt} + (u - v) = r\}\right| / n.$$

Then f_r is a probability distribution on $\mathbb{Z}_k$, which is admissible since

$$\begin{aligned} \sum_{r \in \mathbb{Z}_k} f_r \zeta^r &= \frac{1}{n} \sum_{t=1}^{n} \zeta^{a_{it} - a_{jt} + (u-v)} \\ &= \frac{\zeta^{u-v}}{n} \sum_{t=1}^{n} \zeta^{a_{it} - a_{jt}} = 0, \end{aligned}$$

see [3, Lemma 5.3]. Now

$$d(u + R_i, v + R_j) = \sum_{t=1}^{n} w(a_{it} - a_{jt} + (u - v)) = n \sum_{r \in R} f_r w(r) = n\gamma,$$

by [3, Proposition 3.3], and hence

$$\sum_{t=2}^{n} w(a_{it} - a_{jt} + (u - v)) = n\gamma - w(u - v).$$

If we choose $u - v$ such that $w(u - v) = \ell$, we see that the minimum distance between the rows $u + R_i$ and $v + R_j$ with the first column deleted, where $i \neq j$, is equal to $n\gamma - \ell$. On the other hand, $d(u + R_i, v + R_i) = nw(u - v)$. Then the minimal distance between the rows $u + R_i$ and $v + R_i$, where $u \neq v$, with the first column deleted, is equal to $(n - 1)\ell'$. It follows that $d_B = \min\{n\gamma - \ell, (n - 1)\ell'\}$.

The BH code of type $\mathcal{C}_k$ differs from the one of type $\mathcal{B}_k$ only in the first coordinate. It, therefore, follows from the discussions above $d_C = \min\{n\gamma, n\ell'\}$.

Note that

$$\ell = \frac{\gamma p_1}{p_1 - 1} \qquad \text{and} \qquad \ell' = \begin{cases} \gamma \left[1 - \frac{1}{(p_1-1)(p_2-1)}\right], & \text{if } s > 1 \\ \gamma, & \text{if } s = 1 \end{cases}$$

by Corollary 2 and Remark 2 in [63]. If $s = 1$, clearly, $d_B = \min\{n\gamma - \ell, (n-1)\ell'\} = n\gamma - \frac{\gamma p_1}{p_1 - 1}$ and $d_C = \min\{n\gamma, n\ell'\} = n\gamma = n\ell'$. Now suppose $s > 1$. Then $n\gamma - \ell = \gamma\left[n - \left(1 + \frac{1}{p_1 - 1}\right)\right]$ and $(n-1)\ell' = \gamma\left[n - \left(1 + \frac{n-1}{(p_1-1)(p_2-1)}\right)\right]$. Since

$$\frac{1}{p_1 - 1} \Big/ \frac{n-1}{(p_1-1)(p_2-1)} = \frac{p_2 - 1}{n-1},$$

$n\gamma - \ell > (n-1)\ell'$ if and only if $p_2 < n$. Therefore,

$$d_B = \begin{cases} n\gamma - \frac{p_1\gamma}{p_1 - 1}, & \text{if } n \leq p_2 \\ (n-1)\gamma\left(1 - \frac{1}{(p_1-1)(p_2-1)}\right), & \text{if } n > p_2. \end{cases}$$

On the other hand, $d_C = \min\{n\gamma, n\ell'\} = n\ell' = n\gamma\left(1 - \frac{1}{(p_1-1)(p_2-1)}\right)$.

Now we consider a BH code of type $\mathcal{D}_k$ for arbitrary $s > 0$. By definition, it is clear that $d_C \leq d_D \leq d_C + \ell$. On the other hand, for any $u \in \mathbb{Z}_k$ such that $w(u) = \ell'$, $\mathrm{u} = (u.\mathbf{1}_n, 0) \in \mathbb{Z}_k^{n+1}$, where $\mathbf{1}_n$ denotes the all 1's vector of length n, lies in any BH code of type $\mathcal{D}_k$. Since $w(\mathrm{u}) = n\ell' = d_C$. It follows that $d_D = d_C$, completing the proof. □

Corollary 5.4. *Let p be a prime number, $e \geq 2$ an integer and H a normalized BH(n, p^e) matrix. Then for BH codes obtained from H equipped with the homogeneous weight w_1 (see (3)), we have $d_A = d_C = d_D = n(p-1)p^{e-2}$ and $d_B = n(p-1)p^{e-2} - p^{e-1}$.*

Proof. Apply Theorem 5.3 for $s = 1$ and $\gamma = (p-1)p^{e-2}$. □

Example 5.3. *Let $p = 3$, $e = 2$ and ζ be the primitive 9-th root of unity. Then for the $\mathrm{BH}(9,9)$ matrix*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 & \zeta^6 & \zeta^7 & \zeta^8 \\ 1 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^8 & \zeta & \zeta^3 & \zeta^5 & \zeta^7 \\ 1 & \zeta^3 & \zeta^6 & 1 & \zeta^3 & \zeta^6 & 1 & \zeta^3 & \zeta^6 \\ 1 & \zeta^4 & \zeta^8 & \zeta^3 & \zeta^7 & \zeta^2 & \zeta^6 & \zeta & \zeta^5 \\ 1 & \zeta^5 & \zeta & \zeta^6 & \zeta^2 & \zeta^7 & \zeta^3 & \zeta^8 & \zeta^4 \\ 1 & \zeta^6 & \zeta^3 & 1 & \zeta^6 & \zeta^3 & 1 & \zeta^6 & \zeta^3 \\ 1 & \zeta^7 & \zeta^5 & \zeta^3 & \zeta & \zeta^8 & \zeta^6 & \zeta^4 & \zeta^2 \\ 1 & \zeta^8 & \zeta^7 & \zeta^6 & \zeta^5 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{pmatrix},$$

we have

$$G_1(L(H)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 0 & 1 & 0 & 2 & 2 & 2 & 2 & 2 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 1 & 2 & 0 & 2 & 2 & 2 & 2 & 1 & 0 & 0 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 1 & 1 & 1 & 2 & 0 & 1 & 0 & 2 & 1 & 2 & 2 & 2 & 0 & 1 & 2 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 & 2 & 2 & 2 & 0 & 2 & 1 & 2 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 & 0 & 1 & 1 & 0 & 2 & 1 & 1 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 & 1 & 0 & 2 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 & 2 & 0 & 1 & 1 & 1 & 0 & 2 & 1 & 0 & 1 & 2 \end{pmatrix}.$$

Here, the average value of the weight w_1 is calculated as $\gamma = 2$. By using SageMath [64], we obtain that $d_A = 18 = n\gamma$, $d_B = 15 = n\gamma - \frac{p\gamma}{p-1}$, $d_C = 18 = n\gamma$. Moreover, concatenating any non-initial column of $L(H)$ to $\mathcal{C}_9$, we get $d_D = 18$.

2. BH Codes with Quasi-homogeneous Weights

In this section, we study codes obtained from normalized BH matrices under a quasi-homogeneous weight. We explicitly give the minimum distance of code families of type $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, or $\mathcal{D}_k$ for some prime power $k = p^e$ and $p > 2$. The case $p = 2$, is also

studied separately. In particular, we studied similar code families under a certain Gray map of a quasi-homogeneous map.

Proposition 5.5. *Let p be a prime number, $e \geq 2$ be an integer, and w be a quasi-homogeneous weight with the average value γ. If H is a normalized BH(n, p^e) matrix, then the distance between distinct codewords of the BH code (of type $\mathcal{A}_{p^e}$) obtained from H with respect to w is always γn.*

Proof. Let d denote the distance function on $\mathbb{Z}_{p^e}^n$ induced by w. Since H is a Butson-Hadamard matrix, $n = mp$ for some $m \in \mathbb{Z}^+$. Let R_i denote the i-th row of $L(H)$ for $1 \leq i \leq p$. Then the difference $R_i - R_j$ of i-th and j-th rows, with $i \neq j$, consists of the elements of the disjoint union of m cosets of $p^{e-1}\mathbb{Z}_{p^e}$, say $\mathcal{C}_1, \ldots, \mathcal{C}_m$. It follows that

$$d(R_i, R_j) = \sum_{t=1}^{m} \sum_{r \in \mathcal{C}_t} w(r) = m\gamma p = \gamma n,$$

which completes the proof. □

The above proposition shows that any BH code of type $\mathcal{A}_k$, where $k = p^e$ is a prime power, is transformed by G_2 into an equidistant code over $\mathbb{Z}_p$. It also follows from the above result that a BH code of type $\mathcal{A}_k$, where $k = p^e$ is a prime power, equipped with a quasi-homogeneous weight is necessarily Plotkin optimal. Now we are ready to prove an analogous result to Corollary 5.4 for BH codes equipped with certain quasi-homogeneous weights.

Theorem 5.6. *Let $p > 2$ be a prime number, $e \geq 2$ be an integer, and H be a normalized BH(n, p^e) matrix. Also let w be a quasi-homogeneous weight with the average value γ defined as in Proposition 4.2. Then, for a BH code obtained from H equipped with the weight w, we have $d_A = n\gamma$, $d_B = (n-1)\gamma/p^{e-2}(p-1)$, $d_C = d_D = n\gamma/p^{e-2}(p-1)$.*

Proof. By Proposition 5.5, we have $d_A = \gamma n$.

Let d denote the distance function induced by w. Let $n = pm$. We write R_i and $u + R_i$, for $u \in \mathbb{Z}_{p^e}$, to denote the i-th row of $L(H)$ and $L(\zeta^u H)$, respectively. Since the elements of

$R_i - R_j$, the difference of the i-th and j-th rows of $L(H)$, with $i \neq j$, forms a disjoint union of m cosets of the ideal $p^{e-1}\mathbb{Z}_{p^e}$ of $\mathbb{Z}_{p^e}$, the same is also true for the translate $(u-v)+R_i-R_j$, where $u, v \in \mathbb{Z}_{p^e}$. Therefore,

$$d(u + R_i, v + R_j) = w((u - v) + R_i - R_j) = n\gamma$$

as in the proof of Proposition 5.5. If R_i' denotes the row matrix R_i with the first column omitted, $d(u + R_i', v + R_j') = n\gamma - w(u - v)$ for distinct i and j. On the other hand, $d(u + R_i', v + R_i') = (n - 1)w(u - v)$. It follows that $d_B = \min\{n\gamma - \ell, (n - 1)\ell'\}$, where $\ell = \max\{w(a) : a \in \mathbb{Z}_{p^e}\}$ and $\ell' = \min\{w(a) : a \in \mathbb{Z}_{p^e} \text{ and } a \neq 0\}$. Moreover, $d_C = d_D = \min\{n\gamma, n\ell'\}$. Notice that $\ell = w(p^{e-1}) = \gamma p/(p - 1)$ and $\ell' = w(1) = w(p^e - 1) = \gamma/p^{e-2}(p - 1)$. Thus d_B is the minimum of

$$n\gamma - \ell = n\gamma - \frac{p\gamma}{p-1} = \gamma\frac{np^{e-2}(p-1) - p^{e-1}}{p^{e-2}(p-1)} = \gamma\frac{p^{e-1}(pm - m - 1)}{p^{e-2}(p-1)}$$

and

$$(n-1)\ell' = \gamma\frac{n-1}{p^{e-2}(p-1)} = \gamma\frac{pm-1}{p^{e-2}(p-1)}.$$

Thus, in order to compare $n\gamma - \ell$ and $(n - 1)\ell'$, it is enough to compare $p^{e-1}(pm - m - 1)$ and $pm - 1$.

Define the function $f(x) = p^{e-1}(px - x - 1) - px + 1 = (p^e - p^{e-1} - p)x - p^{e-1} + 1$ on $\mathbb{R}$. Since $p^e - p^{e-1} - p > 0$, for $p > 2$, $f(x)$ is increasing. On the other hand, since

$$f(1) = p^{e-1}(p - 2) - p + 1 = (p^{e-1} - 1)(p - 2) - 1 > 0,$$

$f(x) > 0$ for all $x \geq 1$. In particular, we have $p^{e-1}(pm - m - 1) \geq pm - 1 = n - 1$; hence $d_B = (n - 1)\gamma/p^{e-2}(p - 1)$. Finally, we get $d_C = d_D = \min\{n\gamma, n\ell'\} = \min\{n\gamma, n\gamma/p^{e-2}(p - 1)\} = n\gamma/p^{e-2}(p - 1)$. □

The case when $p = 2$ is handled in the following theorem.

Theorem 5.7. *Let H be a normalized BH$(n, 2^e)$ matrix and let w be a quasi-homogeneous weight with the average value γ defined as in Proposition 4.2. Then, for a BH code obtained from H equipped with the weight w, the following hold:*

(i) If $e = 2$, then $d_A = n\gamma$, $d_B = (n-2)\gamma$, $d_C = d_D = n\gamma$.

(ii) If $e > 2$ and $n \geq 4$, then $d_A = n\gamma$, $d_B = (n-1)\gamma/2^{e-2}$, $d_C = d_D = n\gamma/2^{e-2}$.

Proof. Similar to the proof of Theorem 5.6. □

Example 5.4. *Let $H = [\zeta^{a_{ij}}]$ be the* $\mathrm{BH}(9, 9)$ *matrix given in Example 5.3. Then*

$$H' = [G_2(L(H))] = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&1&0&1&1&1&2&1&1&2&2&1&2&2&2&0&2&2&0&0&2\\
0&0&0&1&1&0&2&1&1&2&2&2&0&0&2&1&0&0&1&1&1&2&2&1&0&2&2\\
0&0&0&1&1&1&2&2&2&0&0&0&1&1&1&2&2&2&0&0&0&1&1&1&2&2&2\\
0&0&0&2&1&1&0&0&2&1&1&1&0&2&2&1&1&0&2&2&2&1&0&0&2&2&1\\
0&0&0&2&2&1&1&0&0&2&2&2&1&1&0&0&2&2&1&1&1&0&0&2&2&1&1\\
0&0&0&2&2&2&1&1&1&0&0&0&2&2&2&1&1&1&0&0&0&2&2&2&1&1&1\\
0&0&0&0&2&2&2&2&1&1&1&1&1&0&0&0&0&2&2&2&2&2&1&1&1&1&0\\
0&0&0&0&0&2&0&2&2&2&2&2&2&2&1&2&1&1&1&1&1&1&1&0&1&0&0
\end{pmatrix}.$$

$G_2(\mathcal{A}_9)$ contains of the rows of H' as codewords with the first 3 columns deleted. By SageMath [64], we have $d_{G_2(\mathcal{A}_9} = 18$. Similarly, we get that $d_{G_2(\mathcal{B}_9)} = 8$, $d_{G_2(\mathcal{C}_9)} = 9$ and $d_{G_2(\mathcal{D}_9)} = 9$.

Corollary 5.8. *Let p be a prime number and $e \geq 2$ be an integer. If either $p > 2$ or $p = 2$, $e > 2$, and $n \geq 4$, then the image of a length-n BH code of type $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, and $\mathcal{D}_k$, where $k = p^e$, under the Gray map G_2 are p-ary codes whose distances are given by $d_{G_2(\mathcal{A}_k)} = np^{e-2}(p-1)$, $d_{G_2(\mathcal{B}_k)} = n-1$, and $d_{G_2(\mathcal{C}_k)} = d_{G_2(\mathcal{D}_k)} = n$. On the other hand, if $p^e = 4$, then $d_{G_2(\mathcal{A}_k)} = np^{e-2}(p-1)$, $d_{G_2(\mathcal{B}_k)} = n-2$, and $d_{G_2(\mathcal{C}_k)} = d_{G_2(\mathcal{D}_k)} = n$.*

Proof. Apply Theorem 5.6 and Theorem 5.7 for $\gamma = p^{e-1}(p-1)$. □

Chapter 6

Quantum Stabilizer Codes

In this chapter, we demonstrate the construction of an $[\![nm, ks, \delta]\!]_q$ quantum stabilizer code, given classical linear codes $\mathscr{C} \subseteq \mathbb{F}_q^n$ with dimension k and $\mathscr{D} \subseteq \mathbb{F}_{q^k}^m$ with dimension s. The parameter δ is determined by identifying the stabilizer group associated with codes $\mathscr{C}$ and $\mathscr{D}$. Our approach employs a specific class of Butson Hadamard matrices, equivalent to multiple Kronecker products of the Fourier matrix of order p. We also investigate the conditions for a quantum code, constructed using a normalized Butson Hadamard matrix, to qualify as a stabilizer code.

1. The General Construction

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a q-ary $[n, k, d_1]$ classical linear code, where $1 \leq k < r$. We shall use the codewords of $\mathscr{C}$ to create quantum states in $(\mathbb{C}^q)^{\otimes n}$, as follows: Let $\{f_\lambda : \lambda \in \mathbb{F}_{q^k}\}$ be a set of functions from $\mathscr{C}$ into $\mathbb{F}_p$ and let

$$\phi_\lambda := \frac{1}{\sqrt{q^k}} \sum_{\mathbf{c} \in \mathscr{C}} \omega^{f_\lambda(\mathbf{c})} |\mathbf{c}\rangle \tag{1}$$

for all $\lambda \in \mathbb{F}_{q^k}$, where $\omega = e^{2\pi i/p}$. Note that the ϕ_λ's form an orthonormal basis for a subspace of $(\mathbb{C}^q)^{\otimes n}$ if and only if the $q^k \times q^k$ matrix

$$H = [\omega^{f_\lambda(\mathbf{c})}]_{\lambda \in \mathbb{F}_{q^k}, \mathbf{c} \in \mathscr{C}}, \tag{2}$$

with rows indexed by the elements of $\mathbb{F}_{q^k}$ and columns indexed by the elements of $\mathscr{C}$, both written in a fixed order, forms a BH(q^k, p) matrix.

Let $\mathscr{D} \subseteq \mathbb{F}_{q^k}^m$ be a classical linear code of dimension s and define

$$\Phi_\Lambda := \phi_{\lambda_1} \otimes \ldots \otimes \phi_{\lambda_m} \in (\mathbb{C}^q)^{\otimes nm} \tag{3}$$

for all $\Lambda = (\lambda_1, \ldots, \lambda_m) \in \mathscr{D}$. We form a quantum code, denoted $Q_H(\mathscr{C}, \mathscr{D})$, of length nm to be the subspace of $(\mathbb{C}^q)^{\otimes nm}$ spanned by Φ_Λ for all $\Lambda \in \mathscr{D}$, i.e.,

$$Q_H(\mathscr{C}, \mathscr{D}) := \operatorname{span}\{\Phi_\Lambda : \Lambda \in \mathscr{D}\}. \tag{4}$$

Note that $Q_H(\mathscr{C}, \mathscr{D})$ is a q^{ks}-dimensional subspace of $(\mathbb{C}^q)^{\otimes nm}$, namely, $Q_H(\mathscr{C}, \mathscr{D})$ is an $[\![nm, ks, \delta]\!]_q$ quantum code where δ is the minimum distance of $Q_H(\mathscr{C}, \mathscr{D})$. On the other hand, there exists a one-to-one correspondance $\nu : \mathbb{F}_q^{ks} \to \mathscr{D}$, and so one can set the logical state $|\mathbf{a}\rangle_L$ as $\Phi_{\nu(\mathbf{a})}$ for each $\mathbf{a} \in \mathbb{F}_q^{ks}$. Then $Q_H(\mathscr{C}, \mathscr{D})$ is a quantum code of length nm that encodes ks logical q-states.

Example 6.1. *If* $p = q = 2$, $\mathscr{C} = \mathscr{D} = \{000, 111\} \subseteq \mathbb{F}_2^3$, *and*

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

in (2)*, then the construction of the quantum code* $Q_H(\mathscr{C}, \mathscr{D})$ *as in* (4) *coincides with the well-known Shor's* 9*-qubit code.*

Example 6.2. *Let $p = q = 3$, $\mathscr{C} = \mathscr{D} = \{000, 111, 222\}$, and*

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

in (2)*, where $w = e^{2\pi i/3}$. Then the quantum code obtained as in* (4) *is the same as the nine-qutrit error correcting code considered in Sect. V of [65].*

More generally, if $\mathscr{C} = \mathscr{D} = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^m$, the one-dimensional linear code over $\mathbb{F}_{q^k}$ spanned by $(1, 1, \ldots, 1) \in \mathbb{F}_q^m$, and H is any BH(q, p) matrix, then the quantum code $Q_H(\mathscr{C}, \mathscr{D})$ in (4) *is among the $[\![m^2, 1, m]\!]_q$ quantum error-correcting codes studied in [66]. In view of the next section, we see that if the matrix H is chosen to be a normalized Butson-Hadamard matrix of Fourier type, then $Q_H(\mathscr{C}, \mathscr{D})$ turns out to be a stabilizer code.*

Remark 6.1. Let $\mathscr{D}$ be a q^k-ary linear code of length m. If there exists a positive integer i with $1 \leq i \leq m$ such that for every codeword Λ in $\mathscr{D}$, the i-th coordinate of Λ is zero, then we can project $\mathscr{D}$ onto a q^k-ary linear code $\mathscr{D}'$ of length $m-1$ by deleting the i-th coordinate of each codeword of $\mathscr{D}$, where the minimum distance remains unaltered, and use $\mathscr{D}'$ instead of $\mathscr{D}$ in the construction of $Q_H(\mathscr{C}, \mathscr{D})$. Thus, throughout this note, we shall assume that the code $\mathscr{D}$ in the above construction, is non-trivial (i,e., neither 0 nor $\mathbb{F}_{q^k}^m$) and that for every integer $1 \leq i \leq m$, there exists a codeword in $\mathscr{D}$ whose i-th coordinate is equal to 1.

Proposition 6.2. *Let $\mathscr{C}$ be a q-ary linear code of dimension k and length n, and let $\mathscr{D}$ be a q^k-ary linear code of dimension s and length m (where $0 < s < m$). Let H and H' be BH(q^k, p) matrices. If $Q_H(\mathscr{C}, \mathscr{D}) = Q_{H'}(\mathscr{C}, \mathscr{D})$, then H and H' are row-equivalent BH matrices. The converse also holds when $\mathscr{D} = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_{q^k}\} \subseteq \mathbb{F}_{q^k}^m$ is the one-dimensional linear code over $\mathbb{F}_{q^k}$.*

Proof. Assume that $Q_H(\mathscr{C}, \mathscr{D}) = Q_{H'}(\mathscr{C}, \mathscr{D})$. Given $\lambda \in \mathbb{F}_{q^k}$, we use the notations ϕ_λ or ϕ'_λ accordingly the coefficients of the quantum states in (1) come from H or H'. Similarly, we write Φ'_Λ to mean the tensor products of states of the form ϕ'_λ in (3).

Since the sets $\{\phi_\lambda : \lambda \in \mathbb{F}_{q^k}\}$ and $\{\phi'_\lambda : \lambda \in \mathbb{F}_{q^k}\}$ are orthonormal, they are independent; hence we have

$$\mathrm{span}\{\phi_\lambda : \lambda \in \mathbb{F}_{q^k}\} = \mathrm{span}\{|\mathbf{c}\rangle : \mathbf{c} \in \mathscr{C}\} = \mathrm{span}\{\phi'_\lambda : \lambda \in \mathbb{F}_{q^k}\}.$$

It follows that there exist $b_{\lambda\mu} \in \mathbb{C}$ $(\lambda, \mu \in \mathbb{F}_{q^k})$ such that

$$\phi_\lambda = \sum_{\mu \in \mathbb{F}_{q^k}} b_{\lambda\mu} \phi'_\mu \tag{5}$$

for all $\lambda \in \mathbb{F}_{q^k}$. On the other hand, since $Q_H(\mathscr{C}, \mathscr{D}) = Q_{H'}(\mathscr{C}, \mathscr{D})$, there exist $a_{\Lambda M} \in \mathbb{C}$ $(\Lambda, M \in \mathscr{D})$ such that $\Phi_\Lambda = \sum_{M \in \mathscr{D}} a_{\Lambda M} \Phi'_M$ for all $\Lambda \in \mathscr{D}$. Rewriting Φ_Λ for $\Lambda = (\lambda_1, \ldots, \lambda_m) \in \mathscr{D}$ as

$$\begin{aligned}\Phi_\Lambda &= \left(\sum_{\mu \in \mathbb{F}_{q^k}} b_{\lambda_1\mu} \phi'_\mu\right) \otimes \cdots \otimes \left(\sum_{\mu \in \mathbb{F}_{q^k}} b_{\lambda_1\mu} \phi'_\mu\right) \\ &= \sum_{(\mu_1, \ldots, \mu_m) \in \mathbb{F}_{q^k}^m} \left(\prod_{i=1}^m b_{\lambda_i\mu_i}\right) (\phi'_{\mu_1} \otimes \cdots \otimes \phi'_{\mu_m}),\end{aligned}$$

we see that for all $\Lambda = (\lambda_1, \ldots, \lambda_m) \in \mathscr{D}$, $\prod_{i=1}^m b_{\lambda_i\mu_i} = a_{\Lambda M}$ if $M = (\mu_1, \ldots, \mu_m) \in \mathscr{D}$ and $\prod_{i=1}^m b_{\lambda_i\mu_i} = 0$ if $M = (\mu_1, \ldots, \mu_m) \notin \mathscr{D}$.

Considering the equation (5), we see that there exists a function $\sigma : \mathbb{F}_{q^k} \to \mathbb{F}_{q^k}$ such that $b_{\lambda\sigma(\lambda)} \neq 0$. Since we assume that $\mathscr{D}$ is non-trivial, at least one of the standard basis element of $\mathbb{F}_{q^k}^m$ does not belong to $\mathscr{D}$. Without loss of generality, we assume that $(1, 0, \ldots, 0) \notin \mathscr{D}$. Let $\lambda \in \mathbb{F}_{q^k}$. By our assumption on $\mathscr{D}$ (see Remark 6.1), there exists $(\lambda_1, \ldots, \lambda_m) \in \mathscr{D}$ with $\lambda_1 = \lambda$. Then we must have $(\sigma(\lambda_1), \ldots, \sigma(\lambda_m)) \in \mathscr{D}$. Let $\alpha \in \mathbb{F}_{q^k} \setminus \{0\}$. Then $(\alpha + \sigma(\lambda_1), \sigma(\lambda_2), \ldots, \sigma(\lambda_m)) \notin \mathscr{D}$. This gives that $b_{\lambda\nu}.b_{\lambda_2\sigma(\lambda_2)} \ldots b_{\lambda_m\sigma(\lambda_m)} = 0$, where $\nu = \alpha + \sigma(\lambda)$; hence $b_{\lambda\nu} = 0$. It follows that $b_{\lambda\mu} = 0$ for all $\mu \in \mathbb{F}_{q^k}$ with $\mu \neq \sigma(\lambda)$. Therefore, $\phi_\lambda = b_{\lambda\sigma(\lambda)}\phi'_{\sigma(\lambda)}$ for all $\lambda \in \mathbb{F}_{q^k}$, and so σ is a permutation on $\mathbb{F}_{q^k}$. It is now straightforward to check that $b_{\lambda\sigma(\lambda)}$ is a power of ω for all $\lambda \in \mathbb{F}_{q^k}$. This completes the proof of the first assertion since we also have $H = [b_{\lambda\mu}]H'$. Now the second assertion follows

since in case $\mathscr{D} = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^m$, the row-equivalence of H and H' implies that Φ_Λ is a constant multiple of Φ'_Λ for every $\Lambda \in \mathscr{D}$. □

2. A Quantum Stabilizer Code

In this section, we use our general construction of quantum codes described in the preceding section to produce quantum stabilizer codes by choosing a particular set $\{f_\lambda : \lambda \in \mathbb{F}_{q^k}\}$ of functions from $\mathscr{C}$ into $\mathbb{F}_p$ in the formation of the ϕ_λ's in (1). We start with two lemmas.

Lemma 6.3. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code over $\mathbb{F}_q$ and let $\mathbf{u} \in \mathbb{F}_q^n$. Then $\mathrm{tr}_{q/p}(\mathbf{u}.\mathbf{c}) = 0$ for all $\mathbf{c} \in \mathscr{C}$ if and only if $\mathbf{u} \in \mathscr{C}^\perp$.*

Proof. It is enough to prove the "only if" part of the statement. So, suppose that $\mathrm{tr}_{q/p}(\mathbf{u}.\mathbf{c}) = 0$ for all $\mathbf{c} \in \mathscr{C}$. Choose an arbitrary nonzero element $\lambda \in \mathbb{F}_q$. Then $\mathscr{C} = \{\lambda\mathbf{c} : \mathbf{c} \in \mathscr{C}\}$, and so $\mathrm{tr}_{q/p}(\lambda(\mathbf{u}.\mathbf{c})) = 0$ for all $\mathbf{c} \in \mathscr{C}$. Since $\lambda \in \mathbb{F}_q$ is arbitrary, this implies that $\mathbf{u}.\mathbf{c} = 0$ for all $\mathbf{c} \in \mathscr{C}$; hence $\mathbf{u} \in \mathscr{C}^\perp$. □

Lemma 6.4. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code over $\mathbb{F}_q$ and let $\phi = \sum_{\mathbf{c}\in\mathscr{C}} \omega^{f(\mathbf{c})} |\mathbf{c}\rangle \in (\mathbb{C}^q)^{\otimes n}$, where $f : \mathscr{C} \to \mathbb{F}_p$ is a function. Let $\mathbf{u} \in \mathbb{F}_q^n$. Then $Z(\mathbf{u})$ stabilizes ϕ if and only if $\mathbf{u} \in \mathscr{C}^\perp$.*

Proof. This is clear by Lemma 6.3 since $Z(\mathbf{u})\phi = \sum_{\mathbf{c}\in\mathscr{C}} \omega^{f(c)+\mathrm{tr}_{q/p}(\mathbf{u}.\mathbf{c})} |\mathbf{c}\rangle$. □

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a classical linear code over $\mathbb{F}_q$ of dimension k, where $q = p^r$ and $1 \leq k < n$, and $\mathscr{D} \subseteq \mathbb{F}_{q^k}^m$ be a classical linear code over $\mathbb{F}_{q^k}$ of dimension s with $1 \leq s < m$. Note that $\mathscr{C}$ is also a vector space over $\mathbb{F}_p$ by restriction of scalars. Let $\mathcal{L}(\mathscr{C}, \mathbb{F}_p)$ be the $\mathbb{F}_p$-dual of $\mathscr{C}$. That is, $\mathcal{L}(\mathscr{C}, \mathbb{F}_p)$ is the set of all $\mathbb{F}_p$-linear transformations from $\mathscr{C}$ to $\mathbb{F}_p$. Then $\mathcal{L}(\mathscr{C}, \mathbb{F}_p)$ is a vector space over $\mathbb{F}_p$ of dimension rk; in other words, $\mathcal{L}(\mathscr{C}, \mathbb{F}_p)$ contains q^k linear transformations of $\mathbb{F}_p$-spaces. Also, there exists an $\mathbb{F}_p$-space isomorphism $\kappa : \mathbb{F}_{q^k} \to \mathcal{L}(\mathscr{C}, \mathbb{F}_p)$. We set $f_\lambda = \kappa(\lambda)$ for each $\lambda \in \mathbb{F}_{q^k}$, form the matrix $H = [\omega^{f_\lambda(\mathbf{c})}]_{\lambda\in\mathbb{F}_{q^k},\mathbf{c}\in\mathscr{C}}$ which is necessarily a BH matrix, and define $Q_H(\mathscr{C}, \mathscr{D})$ as in (4).

Note that the above setting of f_λ's yields that $f_{\lambda_1} + f_{\lambda_2} = f_{\lambda_1+\lambda_2}$ and $f_{c\lambda} = cf_\lambda$ for all $\lambda, \lambda_1, \lambda_2 \in \mathbb{F}_{q^k}$ and $c \in \mathbb{F}_p$. Given any $\Lambda = (\lambda_1, \ldots, \lambda_m) \in \mathscr{D}$, define a mapping $F_\Lambda : \mathscr{C}^m \to \mathbb{F}_p$ by $F_\Lambda(\mathbf{c}_1, \ldots, \mathbf{c}_m) = f_{\lambda_1}(\mathbf{c}_1) + \cdots + f_{\lambda_m}(\mathbf{c}_m)$ for all $(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \mathscr{C}^m$. Then F_Λ is a linear transformation of $\mathbb{F}_p$-spaces. Moreover, by definition of f_λ's above, the set $\{F_\Lambda : \Lambda \in \mathscr{D}\}$ is a vector space over $\mathbb{F}_p$ in a natural way since $F_{\Lambda_1} + F_{\Lambda_2} = F_{\Lambda_1+\Lambda_2}$ and $h.F_\Lambda = F_{h\Lambda}$ for all $h \in \mathbb{F}_p$ and $\Lambda, \Lambda_1, \Lambda_2 \in \mathscr{D}$.

For $\mathbf{x} \in \mathbb{F}_q^n$, define the mapping $\rho_\mathbf{x} : \mathscr{C} \to \mathbb{F}_p$ by $\rho_\mathbf{x}(\mathbf{c}) = \mathrm{tr}_{q/p}(\mathbf{c}.\mathbf{x})$. Then $\rho_\mathbf{x}$ is a linear transformation of $\mathbb{F}_p$-spaces, and given $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, $\rho_\mathbf{x} = \rho_\mathbf{y}$ if and only if $\mathbf{x} - \mathbf{y} \in \mathscr{C}^\perp$ by Lemma 6.3. Thus we sometimes write $\rho_{\overline{\mathbf{x}}}$ for $\rho_\mathbf{x}$, where $\overline{\mathbf{x}}$ denotes the image of $\mathbf{x}$ under the canonical projection $\mathbb{F}_q^n \to \mathbb{F}_q^n/\mathscr{C}^\perp$. Note that for each $\lambda \in \mathbb{F}_q$, there corresponds $\mathbf{x}_\lambda$ such that $f_\lambda = \rho_{\overline{\mathbf{x}}_\lambda}$. This correspondence yields an $\mathbb{F}_p$-space isomorphism $\Theta : \mathbb{F}_{q^k} \to \mathbb{F}_q^n/\mathscr{C}^\perp$, where $\Theta(\lambda) = \overline{\mathbf{x}}_\lambda$ for which $f_\lambda = \rho_{\overline{\mathbf{x}}_\lambda}$. Define

$$\mathscr{D}^\Theta := \{(\mathbf{x}_{\lambda_1}, \ldots, \mathbf{x}_{\lambda_m}) : (\lambda_1, \ldots, \lambda_m) \in \mathscr{D} \text{ and } \mathbf{x}_{\lambda_i} \in \Theta(\lambda_i) \text{ for all } 1 \le i \le m\}.$$

That is,

$$\mathscr{D}^\Theta = \bigcup_{(\lambda_1,\ldots,\lambda_m)\in\mathscr{D}} \Theta(\lambda_1) \times \cdots \times \Theta(\lambda_m).$$

Then, clearly, $\mathscr{D}^\Theta$ is an additive code over $\mathbb{F}_q$. Note that all the vectors in $(\mathscr{C}^\perp)^{(m)}$ are elements of $\mathscr{D}^\Theta$ corresponding to the zero codeword in $\mathscr{D}$. Thus, $(\mathscr{C}^\perp)^{(m)} \subseteq \mathscr{D}^\Theta$.

Now we are ready to state and prove the main theorem of this section.

Theorem 6.5. *With the above notation, $Q_H(\mathscr{C}, \mathscr{D})$ is an $[\![nm, ks, \delta]\!]_q$ quantum stabilizer code and $\delta = \min\{d(\mathscr{C}), \ell\}$, where $\ell = \min\{\mathrm{wt}(\mathbf{X}) : \mathbf{X} \in \mathscr{D}^\Theta \setminus (\mathscr{C}^\perp)^{(m)}\}$. Moreover, the stabilizer group of $Q_H(\mathscr{C}, \mathscr{D})$ consists of the errors $X(\mathbf{c}_1, \ldots, \mathbf{c}_m)Z(\mathbf{d}_1, \ldots, \mathbf{d}_m)$, where $(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)$ and $\mathbf{d}_1, \ldots, \mathbf{d}_m \in \mathscr{C}^\perp$.*

Proof. Let $\mathcal{S}$ be the stabilizer group of $Q_H(\mathscr{C}, \mathscr{D})$ and let $\overline{\mathcal{S}}$ be its image in $\mathbb{F}_q^{2nm}$.

If $\mathbf{d}_1, \ldots, \mathbf{d}_m \in \mathscr{C}^\perp$, then $Z(\mathbf{d}_1, \ldots, \mathbf{d}_m) \in \mathscr{C}^\perp$ by Lemma 6.4. On the other hand, given $\mathbf{e} \in \mathscr{C}$ and $\lambda \in \mathbb{F}_{q^k}$, we have

$$X(\mathbf{e})\phi_\lambda = \sum_{\mathbf{c}\in\mathscr{C}} \omega^{f_\lambda(\mathbf{c})} |\mathbf{c}+\mathbf{e}\rangle = \sum_{\mathbf{c}\in\mathscr{C}} \omega^{f_\lambda(\mathbf{c}-\mathbf{e})} |\mathbf{c}\rangle = \omega^{-f_\lambda(e)}\phi_\lambda,$$

and so

$$X(\mathbf{c}_1, \ldots, \mathbf{c}_m)\Phi_\Lambda = \omega^{F_\Lambda(\mathbf{c}_1,\ldots,\mathbf{c}_m)}\Phi_\Lambda$$

for all $\mathbf{c}_1, \ldots, \mathbf{c}_m \in \mathscr{C}$ and $\Lambda \in \mathscr{D}$. Thus, given codewords $\mathbf{c}_1, \ldots, \mathbf{c}_m$ of $\mathscr{C}$, $X(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \mathcal{S}$ if and only if $(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)$. Therefore, $\mathcal{S}$ contains all the errors of the form $X(\mathbf{c}_1, \ldots, \mathbf{c}_m)Z(\mathbf{d}_1, \ldots, \mathbf{d}_m)$ for which $\mathbf{c}_1, \ldots, \mathbf{c}_m \in \mathscr{C}$ with $(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)$ and $\mathbf{d}_1, \ldots, \mathbf{d}_m \in \mathscr{C}^\perp$. Clearly, the number of the errors $Z(\mathbf{d}_1, \ldots, \mathbf{d}_m)$, where $\mathbf{d}_1, \ldots, \mathbf{d}_m \in \mathscr{C}^\perp$ is equal to $|\mathscr{C}^\perp| = q^{(n-k)m}$. We shall show that the number of errors $X(\mathbf{c}_1, \ldots, \mathbf{c}_m)$, where $(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)$ is equal to $q^{k(m-s)}$.

Let $\{F_{\Lambda_1}, \ldots, F_{\Lambda_{rks}}\}$ be an $\mathbb{F}_p$-basis for $\{F_\Lambda : \Lambda \in \mathscr{D}\}$. Each F_{Λ_i} can be represented by a $1 \times rkm$ matrix, say R_i with respect to a fixed ordered basis of $\mathscr{C}^m$. Then the $rks \times rks$ matrix

$$\mathcal{R} = \begin{pmatrix} R_1 \\ \vdots \\ R_{rks} \end{pmatrix}$$

represents the $\mathbb{F}_p$-linear transformation $F : \mathscr{C}^m \to \mathbb{F}_p^{rks}$ defined by $F(x) = (F_{\Lambda_1}(x), \ldots, F_{\Lambda_{rks}}(x))$ with respect to the same ordered basis of $\mathscr{C}^m$. Since

$$c_1R_1 + \cdots + c_{rks}R_{rks} = 0 \text{ if and only if } c_1F_{\Lambda_1} + \cdots + c_{rks}F_{\Lambda_{rks}} = 0$$

for any $c_1, \ldots, c_{rks} \in \mathbb{F}_p$, we see that the set $\{R_1, \ldots, R_{rks}\}$ is linearly independent over $\mathbb{F}_p$. Thus $\mathcal{R}$ has rank rks, or equivalently, has nullity $rk(m-s)$. Since $\ker(F) = \bigcap_{i=1}^{rks} \ker(F_{\Lambda_i})$, $\dim_{\mathbb{F}_p}\left(\bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)\right) = \dim_{\mathbb{F}_p}\left(\bigcap_{i=1}^{rks} \ker(F_{\Lambda_i})\right) = rk(m-s)$. Then the number of errors $X(\mathbf{c}_1, \ldots, \mathbf{c}_m)$, where $(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)$ is equal to $p^{rk(m-s)} = q^{k(m-s)}$.

It follows that $|\mathcal{S}| \geq q^{(n-k)m}q^{k(m-s)} = q^{nm-ks}$. On the other hand, since $Q_H(\mathscr{C},\mathscr{D}) \subseteq \mathrm{Fix}(\mathcal{S})$, we have

$$q^{ks} = \dim_{\mathbb{F}_q}(Q_H(\mathscr{C},\mathscr{D})) \leq \dim_{\mathbb{F}_q}(\mathrm{Fix}(\mathcal{S})) = \frac{q^{nm}}{|\mathcal{S}|},$$

and so $|\mathcal{S}| \leq q^{nm-ks}$. This gives that $|\mathcal{S}| = q^{nm-ks}$, and hence $\mathcal{S}$ consists of the errors of the form $X(\mathbf{c}_1,\ldots,\mathbf{c}_m)Z(\mathbf{d}_1,\ldots,\mathbf{d}_m)$ for which $\mathbf{c}_1,\ldots,\mathbf{c}_m \in \mathscr{C}$ with $(\mathbf{c}_1,\ldots,\mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}}\ker(F_\Lambda)$ and $\mathbf{d}_1,\ldots,\mathbf{d}_m \in \mathscr{C}^\perp$. This shows, in particular, that $Q_H(\mathscr{C},\mathscr{D})$ is a stabilizer code.

Finally, we shall show that $\delta = \min\{d(\mathscr{C}),\ell\}$. To see this, we first need to determine $\overline{\mathcal{S}}^{\perp_s}$. We claim that $\overline{\mathcal{S}}^{\perp_s}$ consists of $(\mathbf{u}_1,\ldots,\mathbf{u}_m \mid \mathbf{v}_1,\ldots,\mathbf{v}_m)$ for which $\mathbf{u}_1,\ldots,\mathbf{u}_m \in \mathscr{C}$ and $(\mathbf{v}_1,\ldots,\mathbf{v}_m) \in \mathscr{D}^\Theta$. By above, we see that $\overline{\mathcal{S}}$ consists of the sequences $(\mathbf{c}_1,\ldots,\mathbf{c}_m \mid \mathbf{d}_1,\ldots,\mathbf{d}_m)$ such that $(\mathbf{c}_1,\ldots,\mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}}\ker(F_\Lambda)$ and $\mathbf{d}_1,\ldots,\mathbf{d}_m \in \mathscr{C}^\perp$. Let $(\mathbf{U} \mid \mathbf{V}) = (\mathbf{u}_1,\ldots,\mathbf{u}_m \mid \mathbf{v}_1,\ldots,\mathbf{v}_m)$ be such that $\mathbf{u}_1,\ldots,\mathbf{u}_m \in \mathscr{C}$ and $(\mathbf{v}_1,\ldots,\mathbf{v}_m) \in \mathscr{D}^\Theta$. Let $(\mathbf{C} \mid \mathbf{D}) = (\mathbf{c}_1,\ldots,\mathbf{c}_m \mid \mathbf{d}_1,\ldots,\mathbf{d}_m) \in \overline{\mathcal{S}}$. By the choice of $\mathbf{v}_1,\ldots,\mathbf{v}_m$, there exists $\Lambda = (\lambda_1,\ldots,\lambda_m) \in \mathscr{D}$ such that $\mathbf{v}_i \in \Theta(\lambda_i)$ for each $1 \leq i \leq m$. In other words, $f_{\lambda_i} = \rho_{\mathbf{v}_i}$ for each $1 \leq i \leq m$. This gives that

$$\mathrm{tr}_{q/p}(\mathbf{C}.\mathbf{V}) = \sum_{i=1}^{m}\mathrm{tr}_{q/p}(\mathbf{c}_i.\mathbf{v}_i) = \sum_{i=1}^{m} f_{\lambda_i}(\mathbf{c}_i) = F_\Lambda(\mathbf{c}_1,\ldots,\mathbf{c}_m) = 0. \tag{6}$$

It follows that $\langle(\mathbf{C} \mid \mathbf{D}),(\mathbf{U} \mid \mathbf{V})\rangle_s = \mathrm{tr}_{q/p}(\mathbf{d}.\mathbf{u} - \mathbf{v}.\mathbf{c}) = 0$; hence $(\mathbf{U} \mid \mathbf{V}) \in \overline{\mathcal{S}}^{\perp_s}$. Now let $(\mathbf{U} \mid \mathbf{V}) = (\mathbf{u}_1,\ldots,\mathbf{u}_m \mid \mathbf{v}_1,\ldots,\mathbf{v}_m) \in \overline{\mathcal{S}}^{\perp}$. Note that given any $\mathbf{d} \in \mathscr{C}^\perp$, $(0,\ldots,0 \mid \mathbf{d},0,\ldots,0),(0,\ldots,0 \mid 0,\mathbf{d},0,\ldots,0),\ldots,(0,\ldots,0 \mid 0,\ldots,0,\mathbf{d})$ all lie in $\overline{\mathcal{S}}$. Thus we have $\mathrm{tr}_{q/p}(\mathbf{u}_i.\mathbf{d}) = 0$ for all $\mathbf{d} \in \mathscr{C}^\perp$ and $1 \leq i \leq m$. It follows, from Lemma 6.3, that $\mathbf{u}_i \in \mathscr{C}$ for all $1 \leq i \leq m$. Now we shall show that $\mathbf{v} \in \mathscr{D}^\Theta$. To see this, it is enough to show that $\mathscr{D}^\Theta$ is equal to the additive code

$$\mathcal{V} := \{(\mathbf{z}_1,\ldots,\mathbf{z}_m) : \sum_{i=1}^{m}\mathrm{tr}_{q/p}(\mathbf{z}_i.\mathbf{c}_i) = 0 \text{ for all } (\mathbf{c}_1,\ldots,\mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}}\ker(F_\Lambda)\} \tag{7}$$

over $\mathbb{F}_q$. By (6), we see that $\mathscr{D}^\Theta \subseteq \mathcal{V}$. To see the reverse inclusion, define $R_{\mathbf{y}_1,\ldots,\mathbf{y}_m} : \mathbb{F}_q^{nm} \to \mathbb{F}_p$ by $R_{\mathbf{y}_1,\ldots,\mathbf{y}_m}(\mathbf{z}_1,\ldots,\mathbf{z}_m) = \mathrm{tr}_{q/p}\left(\sum_{i=1}^m \mathbf{y}_i.\mathbf{z}_i\right)$ for all $\mathbf{y}_1,\ldots,\mathbf{y}_m,\mathbf{z}_1,\ldots,\mathbf{z}_m \in \mathbb{F}_q^n$. Note that $\mathcal{V} = \bigcap\{\ker(R_{\mathbf{c}_1,\ldots,\mathbf{c}_m}) : (\mathbf{c}_1,\ldots,\mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)\}$. Moreover, $\{R_{\mathbf{c}_1,\ldots,\mathbf{c}_m} : (\mathbf{c}_1,\ldots,\mathbf{c}_m) \in \bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)\}$ is an $\mathbb{F}_p$-space, in a natural way, and the correspondence $(\mathbf{c}_1,\ldots,\mathbf{c}_m) \mapsto R_{\mathbf{c}_1,\ldots,\mathbf{c}_m}$ is an $\mathbb{F}_p$-space isomorphism. Thus, by similar arguments as used above, one can see that the $\mathbb{F}_p$-dimension of $\mathcal{V}$ is equal to

$$\dim_{\mathbb{F}_p}(\mathbb{F}_q^{nm}) - \dim_{\mathbb{F}_p}\left(\bigcap_{\Lambda\in\mathscr{D}} \ker(F_\Lambda)\right) = rnm - rkm + rks,$$

and so $|\mathcal{V}| = q^{(n-k)m}q^{ks}$. One can also see that $|\mathscr{D}^\Theta| = q^{(n-k)m}.q^{ks}$. Since we already have $\mathscr{D}^\Theta \subseteq \mathcal{V}$, we must have the equality $\mathscr{D}^\Theta = \mathcal{V}$. Therefore, $\overline{\mathcal{S}}^{\perp_s}$ consists of $(\mathbf{u}_1,\ldots,\mathbf{u}_m \mid \mathbf{v}_1,\ldots,\mathbf{v}_m)$ for which $\mathbf{u}_1,\ldots,\mathbf{u}_m \in \mathscr{C}$ and $(\mathbf{v}_1,\ldots,\mathbf{v}_m) \in \mathscr{D}^\Theta$.

Let $\mathbf{c} \in \mathscr{C}$ and suppose that $(\mathbf{c},\mathbf{0},\ldots,\mathbf{0}) \in \ker(F_\Lambda)$ for all $\Lambda \in \mathscr{D}$. By our assumption on $\mathscr{D}$ (see Remark 6.1) the first coordinates of the elements of $\mathscr{D}$ form up $\mathbb{F}_{q^k}$. It follows that $c \in \bigcap_{\lambda\in\mathbb{F}_{q^k}} \ker(f_\lambda) = 0$. This gives that for every nonzero $\mathbf{c} \in \mathscr{C}$, the element $(\mathbf{c},\mathbf{0},\ldots,\mathbf{0} \mid \mathbf{0},\ldots,\mathbf{0})$ of $(\mathbb{F}_q^n)^{2m}$ lies in $\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}$. Therefore, $\mathrm{swt}(\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}) \leq d(\mathscr{C})$. On the other hand, for any nonzero $\Lambda = (\lambda_1,\ldots,\lambda_m) \in \mathscr{D}$, an element $\mathbf{D} = (\mathbf{x}_{\lambda_1},\ldots,\mathbf{x}_{\lambda_m}) \in \mathscr{D}^\Theta$ cannot belong to $(\mathscr{C}^\perp)^{(m)}$; hence the element $(\mathbf{0},\ldots,\mathbf{0} \mid \mathbf{D})$ of $(\mathbb{F}_q^n)^{2m}$ belongs to $\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}$. Therefore, we also have $\mathrm{swt}(\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}) \leq \ell$. Consequently, $\mathrm{swt}(\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}) \leq \min\{d(\mathscr{C}),\ell\}$.

Now suppose that $\mathrm{swt}(\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}) < \min\{d(\mathscr{C}),\ell\}$. Let $(\mathbf{C} \mid \mathbf{D}) \in \overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}$ such that $\mathrm{swt}(\mathbf{C} \mid \mathbf{D}) = \mathrm{swt}(\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}})$. Since $\mathrm{swt}(\mathbf{C} \mid \mathbf{D}) < d(\mathscr{C})$ and $\mathbf{C} \in \mathscr{C}^{(m)}$, we must have $\mathbf{C} = \mathbf{0}$. But since $\mathbf{D} \notin (\mathscr{C}^\perp)^{(m)}$, we get $\ell \leq \mathrm{swt}(\mathbf{C} \mid \mathbf{D}) < \ell$, a contradiction. Therefore, $\mathrm{swt}(\overline{\mathcal{S}}^{\perp_s} \setminus \overline{\mathcal{S}}) = \min\{d(\mathscr{C}),\ell\}$. □

Corollary 6.6. *Let the situation be as in Theorem 6.5. If $d(\mathscr{C}) \leq d(\mathscr{D})$, then $\delta = d(\mathscr{C})$.*

Proof. It is not difficult to see that the number ℓ in Theorem 6.5 is at least $d(\mathscr{D})$. Now the result follows since $\delta = \min\{d(\mathscr{D}),\ell\}$. □

Corollary 6.7. *Let the situation be as in Theorem 6.5. Suppose that* $\mathscr{D} = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_{q^k}\} \subset \mathbb{F}_{q^k}^m$. *Then* $\delta = \min\{d(\mathscr{C}), m\}$ *and the stabilizer group of* $Q_H(\mathscr{C}, \mathscr{D})$ *consists of the errors* $X(\mathbf{c}_1, \ldots \mathbf{c}_m)Z(\mathbf{d}_1 \ldots \mathbf{d}_m)$, *where* $\mathbf{c}_1, \ldots, \mathbf{c}_m \in \mathscr{C}$ *with* $\sum_{i=1}^m \mathbf{c}_i = 0$ *and* $\mathbf{d}_1, \ldots, \mathbf{d}_m \in \mathscr{C}^\perp$.

Proof. It is known from the proof of Theorem 6.5 that $\mathscr{D}^\Theta$ is equivalent to the code

$$\mathcal{V} := \{(\mathbf{z}_1, \ldots, \mathbf{z}_m) : \sum_{i=1}^m \mathrm{tr}_{q/p}(\mathbf{z}_i.\mathbf{c}_i) = 0 \text{ for all } (\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \bigcap_{\Lambda \in \mathscr{D}} \ker(F_\Lambda)\}$$

over $\mathbb{F}_q$. Since $\mathscr{D} = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_{q^k}\} \subset \mathbb{F}_{q^k}^m$, $\bigcap_{\Lambda \in \mathscr{D}} \ker(F_\Lambda) = \{(c_1, \ldots, c_m) \in \mathscr{C}^{(m)} : c_1 + \cdots + c_m \in \bigcap_{\lambda \in \mathbb{F}_{q^k}} f_\lambda = 0\}$ such that f_λ's are all linear transformations from $\mathscr{C}$ to $\mathbb{F}_p$. So $\mathscr{D}^\Theta = \{(c_1, \cdots, c_m) \in \mathscr{C}^{(m)} : c_1 + \cdots + c_m = 0\}$. Therefore the stabilizer group of $Q_H(\mathscr{C}, \mathscr{D})$ consists of the errors $X(\mathbf{c}_1, \ldots \mathbf{c}_m)Z(\mathbf{d}_1 \ldots \mathbf{d}_m)$, where $\mathbf{c}_1, \ldots, \mathbf{c}_m \in \mathscr{C}$ with $\sum_{i=1}^m \mathbf{c}_i = 0$ and $\mathbf{d}_1, \ldots, \mathbf{d}_m \in \mathscr{C}^\perp$. For a suitable λ, x_λ could be $(10 \ldots 0)$. Then $\mathrm{wt}(\mathbf{X}) = m$, where $\mathbf{X}$ is the m-fold tensor product of x_λ. The result follows since $\ell = m$. □

Proposition 6.8. *Let the situation be as in Theorem 6.5, where* $\mathscr{D} = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_{q^k}\} \subset \mathbb{F}_{q^k}^m$. *Then*

$$Q_H(\mathscr{C}, \mathscr{D}) = \mathit{span}\left\{ \sum_{\substack{(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \mathscr{C}^{(m)} \\ \mathbf{c}_1 + \cdots + \mathbf{c}_m = c}} |\mathbf{c}_1 \ldots \mathbf{c}_m\rangle : \mathbf{c} \in \mathscr{C} \right\}.$$

Proof. Let

$$\mathcal{A} = \left\{ \sum_{\substack{(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \mathscr{C}^{(m)} \\ \mathbf{c}_1 + \cdots + \mathbf{c}_m = c}} |\mathbf{c}_1 \ldots \mathbf{c}_m\rangle : \mathbf{c} \in \mathscr{C} \right\}.$$

Since for any $\Lambda = (\lambda, \ldots, \lambda) \in \mathscr{D}$,

$$\begin{aligned}\Phi_\Lambda = \phi_\lambda^{\otimes m} &= \frac{1}{\sqrt{q^{km}}} \sum_{(\mathbf{c}_1,\ldots,\mathbf{c}_m)\in\mathscr{C}^{(m)}} \omega^{f_\lambda(\sum_{i=1}^m \mathbf{c}_i)} \left|\mathbf{c}_1 \ldots \mathbf{c}_m\right\rangle \\ &= \frac{1}{\sqrt{q^{km}}} \sum_{(\mathbf{c}_1,\ldots,\mathbf{c}_m)\in\mathscr{C}^{(m)}} \omega^{f_\lambda(\mathbf{c})} \sum_{\mathbf{c}_1+\cdots+\mathbf{c}_m=\mathbf{c}} \left|\mathbf{c}_1 \ldots \mathbf{c}_m\right\rangle,\end{aligned}$$

we have $Q_H(\mathscr{C}, \mathscr{D}) \subseteq \operatorname{span} \mathcal{A}$. Since $\dim(Q_H(\mathscr{C}, \mathscr{D})) = q^k = \dim(\operatorname{span} \mathcal{A})$, we have the equality $Q_H(\mathscr{C}, \mathscr{D}) = \operatorname{span} \mathcal{A}$. □

3. In Search of a Converse

In the previous section, we observed that a quantum stabilizer code can be obtained using two linear codes and a BH matrix with a condition on its rows. Conversely, in this section we will provide the conditions that need to be satisfied for a quantum code constructed with the previously given structure to be a quantum stabilizer code.

Lemma 6.9. *Let $\mathscr{C}$ be a non-empty subset of $\mathbb{F}_q^n$ and let $\phi_i = \sum_{\mathbf{c}\in\mathscr{C}} \omega^{\alpha_i(\mathbf{c})} |\mathbf{c}\rangle$, $\psi_i = \sum_{\mathbf{c}\in\mathscr{C}} \omega^{\beta_i(\mathbf{c})} |\mathbf{c}\rangle$ be elements of $(\mathbb{C}^q)^{\otimes n}$ for every $1 \le i \le m$, where $\omega = e^{2\pi i/p}$ and the α_i and β_i are functions from $\mathscr{C}$ into $\mathbb{F}_p$. Suppose that*

$$\phi_1 \otimes \cdots \otimes \phi_m = \psi_1 \otimes \cdots \otimes \psi_m.$$

Then there exist $b_r \in \mathbb{F}_p$ ($1 \le r \le m$) such that $\psi_r = \omega^{b_r}\phi_r$ for all $1 \le r \le m$.

Proof. By assumption, we have the equality

$$\sum_{(\mathbf{c}_1,\ldots,\mathbf{c}_m)\in\mathscr{C}^m} \omega^{\sum_{i=1}^m \alpha_i(\mathbf{c}_i)} \left|\mathbf{c}_1 \ldots \mathbf{c}_m\right\rangle = \sum_{(\mathbf{c}_1,\ldots,\mathbf{c}_m)\in\mathscr{C}^m} \omega^{\sum_{i=1}^m \beta_i(\mathbf{c}_i)} \left|\mathbf{c}_1 \ldots \mathbf{c}_m\right\rangle,$$

where $\mathscr{C}^m$ denotes the m-fold Cartesian product of $\mathscr{C}$. Hence $\sum_{i=1}^m \alpha_i(\mathbf{c}_i) = \sum_{i=1}^m \beta_i(\mathbf{c}_i)$ for every $(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in \mathscr{C}^m$. Fix a $\mathbf{c}_0 \in \mathscr{C}$. Then

$$\alpha_r(\mathbf{c}) + \sum_{\substack{i=1 \\ i \neq r}}^{m} \alpha_i(\mathbf{c}_0) = \beta_r(\mathbf{c}) + \sum_{\substack{i=1 \\ i \neq r}}^{m} \beta_i(\mathbf{c}_0)$$

for all $\mathbf{c} \in \mathscr{C}$ and $1 \leq r \leq m$. Let

$$b_r = \sum_{\substack{i=1 \\ i \neq r}}^{m} \big(\alpha_i(\mathbf{c}_0) - \beta_i(\mathbf{c}_0)\big) .$$

Then $\alpha_r(\mathbf{c}) + b_r = \beta_r(\mathbf{c})$ for all $\mathbf{c} \in \mathscr{C}$ and $1 \leq r \leq m$. It, therefore, follows that $\psi_r = \omega^{b_r}\phi_r$ for all $1 \leq r \leq m$. □

Theorem 6.10. *Let H be a normalized BH(q^k, p) matrix, where p is a prime number and $q = p^r$ for some positive integer r. Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a classical linear code over $\mathbb{F}_q$ of dimension k, where $1 \leq k < n$, and $\mathscr{D} = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_{q^k}\} \subset \mathbb{F}_{q^k}^m$ be the one-dimensional linear code over $\mathbb{F}_{q^k}$. If the quantum code $Q_H(\mathscr{C}, \mathscr{D})$ is a stabilizer code, then H is equivalent to the rk-fold Kronecker product of the Fourier matrix of order p.*

Proof. Let $\mathscr{C} = \{\mathbf{c}_1 = 0, \mathbf{c}_2, \ldots, \mathbf{c}_{q^k}\}$. We can write $H = [\omega^{f_i(\mathbf{c}_j)}]_{1 \leq i,j \leq q^k}$, where $\omega = e^{2\pi i/p}$ and $f_i : \mathscr{C} \to \mathbb{F}_p$ is a function for each $1 \leq i \leq q^k$. Now, $Q_H(\mathscr{C}, \mathscr{D})$ is the linear span of $\{\phi_1^{\otimes m}, \ldots, \phi_{q^k}^{\otimes m}\}$ over $\mathbb{F}_q$, where

$$\phi_i = \frac{1}{\sqrt{q^k}} \sum_{j=1}^{q^k} \omega^{f_i(\mathbf{c}_j)} \left|\mathbf{c}_j\right\rangle \in (\mathbb{C}^q)^{\otimes n}.$$

Suppose that $Q = Q_H(\mathscr{C}, \mathscr{D})$ is a stabilizer code and let $\mathcal{S} = \mathrm{Stab}(Q)$. By Lemma 6.4, $(\mathbf{0}, \ldots, \mathbf{0} \mid \mathbf{d}_1, \ldots, \mathbf{d}_m) \in \overline{\mathcal{S}}$ for all $\mathbf{d}_1, \ldots, \mathbf{d}_m \in \mathscr{C}^\perp$. Let $\mathbf{s} = (\mathbf{u}_1, \ldots, \mathbf{u}_m \mid \mathbf{v}_1, \ldots, \mathbf{v}_m) \in \overline{\mathcal{S}}$. Then $\mathbf{s}$ is sympletically orthogoanl to the elements of $\overline{\mathcal{S}}$ of the forms $(\mathbf{0}, \ldots, \mathbf{0} \mid \mathbf{d}, \mathbf{0}, \ldots, \mathbf{0}), \ldots, (\mathbf{0}, \ldots, \mathbf{0} \mid \mathbf{0}, \ldots, \mathbf{0}, \mathbf{d})$ for all $\mathbf{d} \in \mathscr{C}^\perp$. Thus, $\mathrm{tr}_{q/p}(\mathbf{u}_i.d) = 0$ for all $1 \leq i \leq m$ and $\mathbf{d} \in \mathscr{C}^\perp$. Therefore, $\mathbf{u}_i \in \mathscr{C}$ for all $1 \leq i \leq m$ by Lemma 6.3. Note that there exists $h \in \mathbb{F}_p$ such that $\omega^h X(\mathbf{u}_1, \ldots, \mathbf{u}_m) Z(\mathbf{v}_1, \ldots, \mathbf{v}_m) \phi_j^{\otimes m} = \phi_j^{\otimes m}$ for all

$1 \leq i \leq m$ and $\mathbf{u} \in \mathscr{C}^{\perp}$. This gives that $\omega^h X(\mathbf{u}_1)Z(\mathbf{v}_1)\phi_j \otimes \cdots \otimes X(\mathbf{u}_m)Z(\mathbf{v}_m)\phi_j = \phi_j \otimes \cdots \otimes \phi_j$, and so there exists $h_{ij} \in \mathbb{F}_p$ ($1 \leq i \leq m$, $1 \leq j \leq q^k$) such that $X(\mathbf{u}_i)Z(\mathbf{v}_i)\phi_j = \omega^{h_{ij}}\phi_j$ for all $1 \leq i \leq m$ and $1 \leq j \leq q^k$ by Lemma 6.9. Since $X(\mathbf{u}_i)Z(\mathbf{v}_i)\phi_j = \sum_{\mathbf{c}\in\mathscr{C}} \omega^{f_j(\mathbf{c}-\mathbf{u}_i)}\omega^{\mathrm{tr}_{q/p}(\mathbf{v}_i.\mathbf{c})}\,|\mathbf{c}\rangle$, we have

$$f_j(\mathbf{c}-\mathbf{u}_i) + \mathrm{tr}_{q/p}(\mathbf{v}_i.\mathbf{c}) = f_j(\mathbf{c}) + h_{ij} \tag{8}$$

for all $\mathbf{c} \in \mathscr{C}$, $1 \leq i \leq m$, and $1 \leq j \leq q^k$. Since H is assumed to be normalized, $f_1(\mathbf{c}) = 0$ for all $\mathbf{c} \in \mathscr{C}$ and $f_i(0) = 0$ for all $1 \leq i \leq q^k$. In parrticular, (8) yields $\mathrm{tr}_{q/p}(\mathbf{v}_i.\mathbf{c}) = h_{i1}$ for all $\mathbf{c} \in \mathscr{C}$ and $1 \leq i \leq m$. Substituting $\mathbf{c} = 0$ and $j = 1$ in (8), we obtain $h_{i1} = 0$ for all $1 \leq i \leq m$. Hence $\mathbf{v}_i \in \mathscr{C}^{\perp}$ for all $1 \leq i \leq m$ by Lemma 6.3. Since $\sum_{i=1}^m h_{ij} = -h$, this also shows that $h = 0$. Note that (8) turns into $f_j(\mathbf{c}-\mathbf{u}_i) = f_j(\mathbf{c}) + h_{ij}$, where $h_{ij} = f_j(-\mathbf{u}_i) = -f_j(\mathbf{u}_i)$ for all $1 \leq i \leq m$ and $1 \leq j \leq q^k$, and $\sum_{i=1}^m f_j(\mathbf{u}_i) = 0$ for all $1 \leq j \leq q^k$. It follows that

$$f_j(\mathbf{c}-\mathbf{u}_i) = f_j(\mathbf{c}) - f_j(\mathbf{u}_i) \tag{9}$$

for all $\mathbf{c} \in \mathscr{C}$, $1 \leq i \leq m$, and $1 \leq j \leq q^k$. Replacing $\mathbf{c}$ by $\mathbf{c} + \mathbf{u}_i$ in (9), we obtain that $f_j(\mathbf{c}+\mathbf{u}_i) = f_j(\mathbf{c}) + f_j(\mathbf{u}_i)$ for all $\mathbf{c} \in \mathscr{C}$, $1 \leq i \leq m$, and $1 \leq j \leq q^k$. In particular, we have $f_j(\sum_{i=1}^m \mathbf{u}_i) = \sum_{i=1}^m f_j(\mathbf{v}_i) = 0$ for all $1 \leq j \leq q^k$. Since H, whose rank is q^k, has its first column consisting of 1's, this is possible only when $\sum_{i=1}^m \mathbf{u}_i = 0$. It follows that $\overline{\mathcal{S}}$ is contained in

$$\mathcal{A} := \{(\mathbf{u}_1, \ldots, \mathbf{u}_m \mid \mathbf{v}_1, \ldots, \mathbf{v}_m) : \mathbf{v}_i \in \mathscr{C}^{\perp},\ \mathbf{u}_i \in \mathscr{C},\ \forall 1 \leq i \leq m \text{ with } \sum_{i=1}^m \mathbf{u}_i = 0\}.$$

Rewriting $\mathcal{A}$ as

$$\{(\mathbf{u}_1, \ldots \mathbf{u}_{m-1}, -\sum_{i=1}^{m-1} \mathbf{u}_i \mid \mathbf{v}_1, \ldots, \mathbf{v}_m) : \mathbf{u}_1, \ldots \mathbf{u}_m \in \mathscr{C},\ \mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathscr{C}^{\perp}\},$$

we have $|\overline{\mathcal{S}}| = q^{nm-k} = (q^k)^{m-1}(q^{n-k})^m = |\mathcal{A}|$; hence $\overline{\mathcal{S}} = \mathcal{A}$. Now (9) gives that $f_j(\mathbf{c}-\mathbf{c}') = f_j(\mathbf{c}) - f_j(\mathbf{c}')$ for all $\mathbf{c}, \mathbf{c}' \in \mathscr{C}$ and $1 \leq j \leq q^k$, proving that $f_j : \mathscr{C} \to \mathbb{F}_p$ is a linear transformation of $\mathbb{F}_p$-spaces. $\square$

Chapter 7

Conclusion

In this thesis, we investigate the distance parameter of BH codes over the rings $\mathbb{Z}_k$, which are mostly non-linear. We consider BH codes endowed with homogeneous weights firstly because it is proved in [3] that some BH codes (more precisely, the BH codes referred to as of type $\mathcal{A}$ in this thesis) are Plotkin optimal. Our results in this direction help us determine parameters of p-ary codes that are images of BH codes obtained from BH(n, p^e) matrices under the generalized Gray map G_1. In [33], another generalized Gray map has been introduced, which is denoted in this chapter by G_2. Although the weight induced by G_2 is not homogeneous, we see that it satisfies a nice property which leads us to define quasi-homogeneous weights (see Definition 4.1). We also see that BH codes of type $\mathcal{A}$ from BH(n, p^e) matrices are Plotkin optimal under quasi-homogeneous weights. We then apply our results to determine the parameters of codes that are images of BH codes under the Gray map G_2.

As noted in the introductory part of this thesis, a $k\lambda \times k\lambda$ GH matrix $\Lambda = [\ell_{ij}]$ is the logarithmic form of a BH$(k\lambda, k)$ matrix since it has the property that for every pair of distinct i, j with $1 \leq i, j \leq k\lambda$, the sequence $\{\ell_{it} - \ell_{jt}\}_{t=1}^{k\lambda}$ of differences contains each element of $\mathbb{Z}_k$ exactly λ times. Thus the arguments in Proposition 5.5 and Theorem 5.6 are applicable for GH codes endowed with quasi-homogeneous weights. More generally, Proposition 5.5 is applicable for every code over a finite commutative ring R equipped with

a quasi-homogeneous weight whose codewords are precisely the rows of an $n \times n$ matrix $A = [a_{ij}]$ over R such that every sequence $\{a_{it} - a_{jt}\}_{t=1}^{n}$ for distinct i and j with $1 \leq i, j \leq n$ is a disjoint union of cosets of ideals of R. If, in addition, R is a Frobenius ring with a generating character χ, this formation of A yields a BH matrix. Indeed, the complex matrix $H = [\chi(a_{ij})]$ turns out to be a BH matrix. To see this, let $1 \leq i, j \leq n$ with $i \neq j$ and suppose that the sequence $\{a_{it} - a_{jt}\}_{t=1}^{n}$ is equal to the disjoint union of cosets $b_1 + I_1, \ldots, b_r + I_r$, where $b_1, \ldots, b_r \in R$ and $I_1, \ldots, I_r$ are ideals of R. Then the (i, j)-entry of the product $H(\overline{H})^T$ is

$$\sum_{t=1}^{n} \chi(a_{it} - a_{jt}) = \sum_{l=1}^{r} \sum_{c \in I_l} \chi(b_l + c) = \sum_{l=1}^{r} \chi(b_l) \sum_{c \in I_l} \chi(c) = 0$$

since the sums over the ideals $I_1, \ldots, I_r$ are all zero. On the other hand, the (i, i)-entry of $H(\overline{H})^T$ is clearly equal to n. Therefore, H is a BH matrix. Note that Butson–Hadamard matrices constructed in [27] from bilinear forms over finite Frobenius rings are of the form described above.

In the latter part of this thesis, our focus shifts to the exploration of quantum stabilizer codes, presenting two distinct constructions. Specifically, we provide a constructive demonstration to establish that a quantum stabilizer code is guaranteed to exist from given two classical linear codes with certain parameters. Furthermore we also state the stabilizer group of this quantum stabilizer code. In our construction, we employ a specialized type of Butson Hadamard matrices, which are equivalent to multiple Kronecker products of the Fourier matrix. Furthermore, we extend our exploration to consider the construction of a quantum code using a generalized normalized Butson Hadamard matrix, aiming to discern conditions under which the resulting quantum code qualifies as a stabilizer code.

Chapter 8

Impacts of Quantum Technologies on the Defence Technologies

The concept of fourth-generation warfare emerged in the 1990s. Given its occurrence in an environment heavily reliant on information systems and network technologies, the use of advanced technologies has become crucial. Intelligence gathering systems and remotely controlled weapons significantly influence the course of warfare. Therefore, possessing state-of-the-art military technologies is among the primary objectives of countries. This leads to the consideration of quantum technologies.

The concept of quantum technology is generally the name given to the developments referred to as the first and second quantum revolutions. The first quantum revolution encompassed nuclear energy, magnetic resonance imaging, and advanced communication and imaging devices, while the second quantum revolution involved understanding the applications of quantum entanglement. In other words, the second quantum revolution aims to manipulate and control quantum systems such as atoms, ions, photons, and electrons.

Throughout this section, we will refer to the second quantum revolution with quantum technology. The two significant advancements of the second quantum revolution are understanding the applications of quantum entanglement and achieving stable qubits.

Quantum computing steps are highly sensitive to ecological factors called decoherence. Stable qubits enable the reduction or control of these environmental interactions. Thus, extending the lifetime of qubit states ensures more reliable results during computations.

Quantum technologies have the potential to affect human life in very different ways. Among these areas of impact is the defense industry. Because it is believed that quantum technologies have the potential to change the way and outcomes of war. It will lead to changes in modern warfare techniques, focusing on improving existing weapons rather than creating new ones. Areas where quantum technologies may have an impact include military service, security, space, and intelligence. However, theoretical progress is more advanced than practical implementation, especially challenging on military platforms.

Quantum bits are defined by their states, unlike classical bits. Additionally, since qubits can be in superposition meaning they can be both 1 and 0 simultaneously, they contribute to an increase in computational power. With n qubits, 2^n states can be represented. When a measurement occurs at the end of a quantum algorithm, the superposition collapses into a single state, so multiple about the statistical distribution of the qubits' states. As a result, since the computational capacity will increase, only quantum computers can achieve this. Furthermore, due to the no-cloning theorem, information cannot be copied, necessitating more complex error correction. Since the quantum state will be disturbed after measurement, the measurement must occur indirectly. Despite all these conditions, it provides secure communication that cannot be eavesdropped on by unwanted parties. Since a quantum measurement is required for unwanted interventions, the state is disturbed and the system collapses. Therefore, by comparing measurements, it is possible to detect any unwanted interference. Quantum systems cannot be directly applied to weapons due to their sensitivity to the environment and their ability to be manipulated only at temperatures close to absolute zero. Therefore, let us look at the potential application scenarios.

Quantum Computation

Quantum computing refers to performing calculations using the laws of quantum mechanics. Unlike classical computers, quantum computers can process all possible superpositions of the $|0\rangle$ and $|1\rangle$ states simultaneously, making them more efficient in some cases. For certain problems, they are faster than classical computers, and therefore, they can perform calculations that are impossible for classical computers.

Quantum computing was proposed in the 1980s to model the behavior of very small physical structures. Later, in the 1990s, it gained importance with the introduction of Shor's algorithm. This algorithm, if used in quantum computers, would exponentially speed up some cryptanalysis methods, thereby reducing the reliability of certain cryptographic systems used in both civilian and military communications. However, in general, quantum computing will not directly replace classical computing; it will only be used for problems with high complexity.

Although the work in the 1990s remained theoretical, advancements in creating and controlling qubits today have enabled many research groups to develop quantum computers to solve real-world problems in programming, optimization, machine learning, and simulation. However, the fundamental obstacles that need to be overcome when building these computers are problems of noise and decoherence.

Quantum systems interact with the external environment through electromagnetic waves and vibrations. Therefore, the information on qubits can be distorted. Since it is impossible to completely isolate them from the external environment, these interactions can be minimized. This can be achieved through quantum error correction, which increases the accuracy rate of quantum computing.

Another limitation is that the qubits are entangled, meaning the state of any qubit is related to the states of other qubits. For these reasons, many qubits will be required to compensate for the lost qubits. According to the upper bound given by Alexander Holevo in 1973, the information obtained from n-qubits cannot be more than the information obtained from

n-bits. Therefore, most of the data in qubits cannot be retrieved. A quantum computer needs a physical system that forms and manipulates the qubits. Superconductors, which are materials capable of demonstrating very small quantum effects, are used for this purpose. Despite the obstacles previously mentioned, superconducting quantum computers have made significant progress, and research on them is still ongoing.

The first demonstration of a superconducting qubit was in 1999, but since superconductors require a temperature of -273 degrees, achieving this is physically challenging and expensive to set up. These issues have increased interest in developing room-temperature superconductors. China, Japan, and the USA are reported having research efforts on this topic.

To summarize America's efforts, in 2018, they established the National Quantum Initiative Act, playing significant role in researching and developing quantum technologies over a five-year period. In 2021, they developed a chip named Eagle with 127 qubits, followed by the introduction of another chip named Osprey with 443 qubits in 2022. Aiming to double the number of qubits each year, IBM introduced the first quantum computer with over 1000 qubits in 2023. This computer is based on the Condor chip, which has 1121 superconducting qubits. These advancements in the private sector have paved the way for the use of quantum computers, one of the branches of quantum technologies used in defense in the military field as well.

Like the United States, China developed a quantum computer in 2021. In 2023, it introduced Zuchangzhi, a quantum processor with 176-qubits, and later that same year, it developed Jiuzhang, the world's largest photonic qubit quantum computer with 25 photons. Thus, China is the only country to have made advancements in both photonic and superconducting quantum computing technologies.

Lastly, Canada introduced the first commercial quantum computer, the D-Wave One. Also, it has two universal quantum computers: IBM Quantum One and MonarQ, which have 24 superconducting qubits.

We can explain the effects of quantum computers in the military fields as follows. First, since quantum computers can store much more data compared to classical computers, countries possessing these computers can create a significant impact on military operations. In addition, quantum computers can be used to create simulations for training purposes. Thus, the way armies operate can be changed.

Quantum sensing is another quantum technology used in the military field. Quantum sensors can detect very small changes in electric and magnetic fields. Thus, they can be used to determine the locations of enemy submarines and mines. Additionally, since they can measure very weak signals, quantum sensors can also be used to monitor radio communications. Moreover, they can accurately detect the location of a missile launched by the enemy and identify a nuclear signature, which refers to certain specific physical, chemical, or radioactive markers used in the detection and analysis of a nuclear explosion.

Quantum Communication

Quantum communication is fundamentally based on the transmission of quantum states between two or more parties. In 2019, for the first time, information was transmitted between two computer chips via quantum entanglement without physical electronic connections. Additionally, laboratory experiments showed that a good entanglement connection between two chips occurs when the photons in both chips share a single quantum state. Currently, research is focused on how quantum entanglement should work and how it can simplify communication processes.

One of the application areas of quantum communication is to protect the privacy of communication channels through quantum cryptography. In quantum cryptography, quantum key distribution(QKD) holds a significant place. Quantum key distribution uses quantum mechanical principles to perform cryptographic tasks and break cryptographic systems. We can simply explain how the QKD system works as follows. In a cryptographic communication between two parties, Alice and Bob, random sequences of numbers are used

as keys, and single photons polarized randomly as 0s and 1s are used to transmit these keys. Both parties are connected via a quantum channel and a classical channel. Alice generates a random stream of qubits sent over the quantum channel. After Bob receives this stream, he performs classical operations with Alice over the classical channel to check if an eavesdropper, will be revealed through the correlation of two-bit lists obtained after the transmission of qubits between the sender and receiver.

Most applications and protocols are limited to two communicating parties. Therefore, this reduces the practical applicability of QKD because it is difficult to create and manipulate more than two entangled particles. Work is being done to solve this problem. A quantum network architecture has been developed that distributes the quantum states of a single entangled photon source to many users while minimizing the necessary resources without compromising functionality and security. In this architecture, there is no need to adapt the entanglement source to add a user. The network can easily scale to a large number of users. Long-distance entanglement distribution is another problem. Quantum repeaters are used to overcome this. Classical repeaters simply measure and copy the signal coming from one side and transmit it to the other side at a higher power, but this is not possible in quantum. In quantum, this process is carried out by entanglement swapping. That is, entangled photons coming from Alice and Bob are received by the repeater and transformed into an entanglement between Alice and Bob. In this case, the photons need to travel only half the distance, increasing the chance of reaching their destination. One method used to solve the problems arising from the range of quantum communication is satellite-based QKD. With this method, encrypted messages are sent to distant ground stations using low-orbit satellites. This could change the sharing of sensitive data by protecting people's information against increasing cybersecurity threats.

At the current stage, quantum communication has reached a level where quantum information is transmitted and exchanged between remote nodes of a network. With these developments in the field of quantum communication, it is expected that specialized quantum communication networks will be built for the military and some changes will be made to

existing military communication applications, rather than directly replacing current military communication methods with quantum communication.

Quantum Cryptography

Quantum computers tend to break classical cryptographic methods and also threaten the future of cyber security. Modern cryptography is vulnerable to advances in computational power, such as progress made in factoring large integers. Therefore, quantum cryptography is needed for these reasons. Quantum cryptography emerged in the early 1970s with Steven Wiesner's book Conjugate Coding, [67]. Like other quantum technologies, it relies on the laws of quantum mechanics. It is based on two principles of quantum mechanics: Heisenberg's uncertainty principle and the photon polarization principle. These principles state, respectively, that the position and velocity of an object cannot be known precisely at the same time, and that an eavesdropper cannot copy an unknown quantum state. If any characteristic is measured, other information will be disturbed. Based on these laws, it ensures secure communication between two parties.

Although modern cryptography relies on mathematical algorithms and IT applications, quantum cryptography provides security based on fundamental physical laws. The biggest advantage in this case is that the encoded information cannot be copied. Quantum cryptography transmits information using a series of photons through a fiber optic cable from one place to another. By measuring and comparing certain properties of these photons, the key on both sides can be estimated and checked for security. More specifically, the sender transmits photons to the receiver using a filter that randomly assigns one of four polarizations and bit assignments: vertical(1 bit), horizontal (0 bit), $45°$right(1 bit), and $45°$left(0 bit). The photons reach a receiver that will read the photon polarization using two beam splitters, horizontal/vertical, and diagonal. The receiver cannot know which beam splitter to use for each photon. The receiver sends the used beam splitters to the sender, who compares them and discards the incorrect ones, leaving the remaining bit sequence as the key. If any

eavesdropper reads or copies the photon, the state of the photon will change, making this detectable. Therefore, the possibility of these operations going undetected is not possible

Communication is an important part of daily life. Additionally, it holds a very vital importance in military operations because information superiority is achieved through this means. Therefore, the security of communication is crucial for military applications, and quantum communication offers improvements in these capabilities. Since quantum computers can break asymmetric cryptographic protocols using Shor's algorithm, quantum-safe methods must be developed. Similarly, symmetric cryptographic algorithms can also be broken using Grover's algorithm. In symmetric encryption, it is possible to make it quantum-safe by doubling the key length. Maintaining information dominance and secure communication in the military field is important for the successful execution of missions. In symmetric encryption, which is preferred for secure communication, keys must be distributed between parties before the mission starts, and it is not possible to frequently change the keys during the mission.

A secret key exchange is required for secure communication. Using QKD protocols, a shared key can be securely generated. In a military environment, key distribution is often conducted among ships, satellites, submarines, aircraft or unmanned aerial vehicles, and ground-based stations and vehicles. Transmission between two ground-based stations can be carried out through fiber optic communication. This communication allows for key distribution among locations such as headquarters, bases, and airports. However, each situation presents unique challenges. For example, free-space quantum distribution is only possible with a direct line of sight. Various experiments have been conducted for the military applications of quantum key distribution, but these experiments were carried out without considering a specific user. QKD is one of the methods that can be used for secure quantum communication. Alternatively, post-quantum cryptography and secure couriers can also be used.

Post-Quantum Cryptography

Quantum computers can break RSA, Diffie-Hellman, and elliptic curve cryptography. These algorithms, which have a wide range of applications, protect inter-institutional communications, important government data, individual privacy, and corporate ownership. The need to develop secure encryption against quantum computers is urgent. For this, the concept of post-quantum cryptography has been developed. This concept involves the use of traditional cryptographic tools in conjunction with quantum computers to overcome cryptographic attacks. It is also known as quantum-resistant or quantum-resistant cryptography.

New quantum-resistant algorithms are based on mathematical problems that are hard for quantum computers and provide a new model when working with encrypted data. For example, fully homomorphic encryption allows operations to be performed on encrypted data. This eliminates the need for trusted third parties. Data remains secure and private in distrusted environments. Since it remains always encrypted, the likelihood of sensitive information being compromised is low. All features can be used since no feature needs to be removed to ensure data privacy. Fully homomorphic encryption is secure against quantum attacks.

The first significant studies related to post-quantum cryptography began in the late 1990s. One of the first proposed algorithms was the McEliece cryptosystem introduced by Robert McEliece in 1978. This algorithm is resistant to quantum attacks but has not been widely adopted due to its large key size. It is based on error-correcting codes. There are cryptosystems that are divided into different families depending on the problem of which their security is based. These include isogeny-based cryptography, which is based on the problem of finding an isogeny between two supersingular curves E and E'. Lattice-based cryptography uses lattices either in the system itself or in the security proof, multivariate polynomial cryptography consists of asymmetric cryptographic structures based on multivariate polynomials over a finite field, and finally, hash-based digital signatures involving cryptographic hash functions.

In 2016, the National Standards and Technology Institute requested post-quantum algorithm proposals to find quantum-resistant algorithms. The first round of the standardization process, which has now been completed, took place in 2016. During this round, 82 submissions were received and evaluated based on security performance and application features. These submissions consist of algorithms in one of the five categories mentioned above.

In the first round, algorithms that did not meet the minimum security and functionality criteria were eliminated, while the remaining algorithms were assessed for security flexibility and applicability for both classical and quantum computers. As a result, 26 candidate algorithms were selected for the second round. Thus, the strengths and weaknesses of the algorithms were identified.

In the second round, which started in 2019 and was completed in 2020, the candidate algorithms were evaluated in terms of their purpose, security effectiveness, and suitability for different conditions. They were assessed for security against various types of attacks, speed, key size, and memory usage performance. Based on the results, 7 finalists and 8 alternative candidates were determined.

Candidates were asked to analyze the algorithms they proposed in the third round, which started in 2020 and was completed in 2021, to prove their theoretical and practical security. After making the necessary updates, 3 digital signature algorithms and 4 PKE(Public Key Encryption)/KEM(Key Encapsulation Mechanism) encryption algorithms were selected at the end of this round. The selected algorithms are lattice-based, hash-based, and code-based algorithms.

In 2022, during the fourth stage, the candidate algorithms were discussed, and updates were explained. Then in 2024, NIST standardized the lattice-based post-quantum algorithm CRYSTALS-KYBER for public key encryption.

Institutions and organizations need to develop their quantum readiness roadmaps and make early plans for the transition to post-quantum cryptographic standards to protect against

potential future hostile cryptographic attacks. This standardization effort by NIST enables institutions to have a roadmap and inventory, initiating the risk assessment process against quantum attacks. It provides the necessary guidance for these processes and is important in this regard.

From the perspective of defense technologies, it holds significant importance to ensure secure communication resistant to quantum decryption for military operations, intelligence, and control systems. Thanks to standardization, multiple defense systems can operate securely together. This is important because it ensures that multiple systems can communicate securely in situations where joint operations are necessary.

One of the post-quantum cryptographic algorithm classes is code-based algorithms. These consist of cryptosystems based on error-correcting codes. Without detecting and correcting bit changes occurring during communication, secure communication cannot be ensured, which would cause problems with significant impacts, especially in military fields. Error detection by adding control bits is one of the fundamental features of error-detecting codes. Naturally, the primary goal is to increase the probability of secure transmission while keeping the number of additional bits to a minimum.

In this sense, the first error-correcting code is the McEliece code introduced in 1978. It consists of a known error-correcting code, the Goppa code, and a reversible linear transformation used to obscure it. This cryptosystem differs from those commonly used and isdependent on the difficulty of factoring integers or finding discrete logarithms. In the McEliece cryptosystem, a secret error-correcting code, initially corrupted by randomly added errors by the sender, is used to attempt to obtain plaintexts from ciphertexts. Its security depends on these processes. Thus, while other cryptosystems are not quantum-resistant, McEliece is resistant to quantum attacks.

Due to the large key sizes, this situation has been optimized through many modifications. In 1986, Niederreiter proposed the use of binary general Reed-Solomon codes. This change reduced the key size and thus improved speed in software and hardware applications. Additionally, McEliece has become an important candidate for post-quantum cryptography

after these modifications. Indeed, it was proposed by Daniel J. Bernstein and others for the competition initiated by NIST in 2017.

Quantum Network

The aim of a quantum network, or in other words, quantum internet, is to transmit quantum information through certain channels. Since quantum information is generally carried by photons, it is very susceptible to distortions. Optical fiber infrastructures are commonly used as channels for transmitting quantum information. Although they are preferred to minimize losses during transmission, high losses can still occur.

As the distance between parties increases, the complexity of the network grows because more nodes are required. This necessitates the use of components such as quantum repeaters or quantum keys. Another channel is space. It is used for transmitting quantum information over long distances. However, it is more challenging compared to other channels because photons have limited use in space. For these reasons, quantum satellites are used in quantum networks.

In communication with satellites, the losses between the satellite and the ground are less than the losses between two distant nodes on the ground. Quantum repeaters are used in long-distance quantum communication due to photon loss and decoherence. Since arbitrary qubit states cannot be copied, quantum repeaters entangle qubits located at the end nodes.

Quantum repeaters require quantum memory. However, there is currently no reliable quantum memory available. A reliable repeater could be used in quantum key distribution rather than for entanglement at end nodes.

Another step is quantum key distribution independent of the measurement devices in experiments. This not only replaces unreliable repeaters with reliable ones but also serves as a key itself. Even if the central node is attacked, the key remains secure. After these

steps, central nodes will be replaced with quantum keys and repeaters, providing a quantum information network.

Quantum internet is used for quantum key distribution, transmission of quantum information between quantum computers over long distances, authentication, performing distributed quantum computing tasks as a single quantum computer, and instead of gathering information about a system that reduces sensor errors, it evaluates universal properties in an entangled sensor network.

A quantum network enables direct and reliable communication between quantum computers. By dividing a task into smaller sub-tasks and performing them across several quantum computers, higher performance can be achieved based on the performance of a single quantum computer.

Protecting sensitive information plays a crucial role in securely transmitting defense-related data during operations. By offering a more resilient network infrastructure, it reduces the likelihood of eavesdropping on critical communications. Enhanced sensors can provide more accurate data and early warning systems, which can accelerate the decision-making process in the face of any threat. Finally, it ensures secure communication between countries on the same side.

Conclusion

Recent technological developments have impacted every area of life. Among these, defense technologies, which are one of the most important areas for countries, are included. Advances in physics have led to theoretical developments, which have been followed by changes in applications. Quantum physics, or quantum mechanics, has introduced new concepts into our lives. These concepts have led to the reorganization of classical communication methods, classical coding theory, and classical encryption methods according to the principles of quantum mechanics.

In defense technologies, which are crucial for information security and secure communication, error-correcting codes play a significant role. Because quantum systems are inherently more sensitive and interact more with the environment compared to classical systems. This increases the potential error rate. Developments related to quantum computers have accelerated recently, with many countries establishing their own quantum research units or collaborating with other countries to avoid falling behind in these advancements. Because in the future, quantum attacks and threats may occur. They want to develop defense methods against such situations.

Results of studies conducted for this purpose include simulations performed by quantum computers. Additionally, the competition to develop encryption algorithms resistant to quantum computers has ended, and post-quantum cryptographic algorithms in areas such as encryption and digital signatures have been standardized.

In this thesis, results have been obtained on classical coding theory. Classical error-correcting codes have been acquired, their parameters determined, and their properties examined in this context.

Subsequently, due to the above mentioned reasons, quantum coding theory has been studied. In this section, a structural method has been provided to obtain quantum error-correcting codes. Similarly, their parameters have been determined to assess their effectiveness. These codes, obtained using linear code families and BH matrices, are generalizations of some code families in the literature. The necessary condition for the obtained codes to be a stabilizer code family, which is a special family of quantum codes, has been specified, and the types of elements in the stabilizer set that could provide an advantage for the decoding process have been indicated.

Bibliography

[1] Richard W Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, **1950**.

[2] Ioana Constantinescu and Werner Heise. A metric for codes over residue class rings. *Problemy Peredachi Informatsii*, 33(3):22–28, **1997**.

[3] Marcus Greferath, Gary McGuire, and MICHAEL E O'SULLIVAN. On plotkin-optimal codes over finite frobenius rings. *Journal of Algebra and its Applications*, 5(06):799–815, **2006**.

[4] A Roger Hammons, P Vijay Kumar, A Robert Calderbank, Neil JA Sloane, and Patrick Solé. The z/sub 4/-linearity of kerdock, preparata, goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, **1994**.

[5] M Greferath and SE Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Transactions on Information Theory*, 45(7):2522–2524, **1999**.

[6] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, **1994**.

[7] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, **1995**.

[8] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, **1996**.

[9] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824, **1996**.

[10] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE transactions on information theory*, 52(11):4892–4914, **2006**.

[11] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Physical Review A*, 54(3):1862, **1996**.

[12] A Robert Calderbank, Eric M Rains, Peter W Shor, and Neil JA Sloane. Quantum error correction and orthogonal geometry. *Physical Review Letters*, 78(3):405, **1997**.

[13] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, **1996**.

[14] Andrew M Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793, **1996**.

[15] Alexei Ashikhmin and Emanuel Knill. Nonbinary quantum stabilizer codes. *IEEE Transactions on Information Theory*, 47(7):3065–3072, **2001**.

[16] Tefjol Pllaha. Equivalence of classical and quantum codes. **2019**.

[17] AT Butson. Generalized Hadamard matrices. *Proceedings of the American Mathematical Society*, 13(6):894–898, **1962**.

[18] Kathy J Horadam. *Hadamard matrices and their applications*. Princeton university press, **2012**.

[19] N Pinnawala and A Rao. Cocyclic butson hadamard matrices and codes over zn via the trace map. *Contemporary Mathematics*, 461:213–228, **2008**.

[20] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, **2002**.

[21] Sibel Kurt and Oğuz Yayla. Near butson-hadamard matrices and nonlinear boolean functions. In *International Conference on Number-Theoretic Methods in Cryptology*, pages 254–266. Springer, **2017**.

[22] Dipak Kumar Bhunia, Cristina Fernández-Córdoba, and Mercè Villanueva. On the classification of p p 2-linear generalized hadamard codes. In *2022 IEEE Information Theory Workshop (ITW)*, pages 523–528. IEEE, **2022**.

[23] Steven T Dougherty, Josep Rifà, and Mercè Villanueva. Rank and kernel of additive generalized hadamard codes. *IEEE Transactions on Information Theory*, 67(11):7210–7220, **2021**.

[24] Dipak K Bhunia, Cristina Fernández-Córdoba, and Mercè Villanueva. On the linearity and classification of z ps-linear generalized hadamard codes. *Designs, Codes and Cryptography*, 90(4):1037–1058, **2022**.

[25] Dipak K. Bhunia, Cristina Fernández-Córdoba, and Mercè Villanueva. On the constructions of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear generalized Hadamard codes. *Finite Fields and Their Applications*, 83:102093, **2022**. ISSN 1071-5797.

[26] Ritajit Majumdar, Saikat Basu, Shibashis Ghosh, and Susmita Sur-Kolay. Quantum error-correcting code for ternary logic. *Physical Review A*, 97(5):052302, **2018**.

[27] Gary McGuire and Harold N Ward. Cocyclic hadamard matrices from forms over finite frobenius rings. *Linear algebra and its applications*, 430(7):1730–1738, **2009**.

[28] Claude Elwood Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, **1948**.

[29] Ian F Blake. Codes over certain rings. *Information and Control*, 20(4):396–404, **1972**.

[30] José Andrés Armario, Ivan Bailera, and Ronan Egan. Butson full propelinear codes. *Designs, Codes and Cryptography*, 91(2):333–351, **2023**.

[31] Cristina Fernández-Córdoba, Carlos Vela, and Mercè Villanueva. Equivalences among z2s-linear hadamard codes. *Discrete Mathematics*, 343(3):111721, **2020**.

[32] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55(2):900, **1997**.

[33] Bahattin Yildiz and Zeynep Odemis Ozger. Generalization of the Lee weight to $\mathbb{Z}_{p^k}$. *TWMS Journal of Applied and Engineering Mathematics*, 2(2):145, **2012**.

[34] Minjia Shi, Wang Xuan, and Patrick Solé. Two families of two-weight codes over z 4. *Designs, Codes and Cryptography*, 88(12):2493–2505, **2020**.

[35] Jian Gao and Xiaotong Hou. 4-double cyclic codes are asymptotically good. *IEEE Communications Letters*, 24(8):1593–1597, **2020**.

[36] W Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge university press, **2010**.

[37] Anthony M Kerdock. A class of low-rate nonlinear binary codes. *Information and control*, 20(2):182–187, **1972**.

[38] Franco P Preparata. A class of optimum nonlinear double-error-correcting codes. *Information and Control*, 13(4):378–400, **1968**.

[39] M Greferath and SE Schmidt. Finite-ring combinatorics and Macwilliams' equivalence theorem. *Journal of Combinatorial Theory Series A*, 92(1):17–28, **2000**.

[40] M Greferath and ME O'Sullivan. On bounds for codes over Frobenius rings under homogeneous weights. *Discrete Mathematics*, 289(1-3):11–24, **2004**.

[41] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, **1994**.

[42] C Carlet. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Transactions on Information Theory*, 44(4):1543–1547, **1998**. ISSN 0018-9448.

[43] M Greferath and SE Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Transactions on Information Theory*, 45(7):2522–2524, **1999**. ISSN 0018-9448.

[44] Dipak K. Bhunia, Cristina Fernández-Córdoba, and Mercè Villanueva. On the linearity and classification of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes. *Designs, Codes and Cryptography*, 90(4):1037–1058, **2022**.

[45] James L Park. The concept of transition in quantum mechanics. *Foundations of physics*, 1(1):23–33, **1970**.

[46] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, **1982**.

[47] DGBJ Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, **1982**.

[48] Andrew M Steane. Simple quantum error-correcting codes. *Physical Review A*, 54(6):4741, **1996**.

[49] Emanuel Knill. Non-binary unitary error bases and quantum codes. *arXiv preprint quant-ph/9608048*, **1996**.

[50] Pradeep Kiran Sarvepalli. Quantum stabilizer codes and beyond. *arXiv preprint arXiv:0810.2574*, **2008**.

[51] Richard Cleve and Daniel Gottesman. Efficient computations of encodings for quantum error correction. *Physical Review A*, 56(1):76, **1997**.

[52] Richard Cleve. Quantum stabilizer codes and classical linear codes. *Physical Review A*, 55(6):4054, **1997**.

[53] Alexei E Ashikhmin, Alexander M Barg, Emanuel Knill, and Simon N Litsyn. Quantum error detection. i. statement of the problem. *IEEE transactions on information theory*, 46(3):778–788, **2000**.

[54] Jon-Lark Kim. New quantum error-correcting codes from hermitian self-orthogonal codes over gf (4). In *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas: Proceedings of the Sixth International Conference on Finite Fields and Applications, held at Oaxaca, México, May 21–25, 2001*, pages 209–213. Springer, **2002**.

[55] Jon-Lark Kim and Vera Pless. Designs in additive codes over gf (4). *Designs, Codes and Cryptography*, 30:187–199, **2003**.

[56] David A Drake. Partial λ-geometries and generalized hadamard matrices over groups. *Canadian Journal of Mathematics*, 31(3):617–627, **1979**.

[57] Dieter Jungnickel. On difference matrices and regular latin squares. **1980**.

[58] Ferenc Szöllősi. A note on the existence of bh (19, 6) matrices. *arXiv preprint arXiv:1204.5166*, **2012**.

[59] Ronan Egan and Padraig O Catháin. Morphisms of butson classes. *Linear algebra and its applications*, 577:78–93, **2019**.

[60] Patric RJ Östergård. Equivalence of butson-type hadamard matrices. *Journal of Algebraic Combinatorics*, 56(2):271–277, **2022**.

[61] Kathy J Horadam. *Hadamard Matrices and Their Applications*. Princeton University Press, **2007**.

[62] Tsit Yuen Lam and Ka Hin Leung. On vanishing sums of roots of unity. *Journal of algebra*, 224(1):91–109, **2000**.

[63] Yun Fan and Hongwei Liu. Homogeneous weights and Möbius functions on finite rings. **2013**. doi:10.48550/ARXIV.1304.4927.

[64] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.2.0)*, **2020**. `https://www.sagemath.org`.

[65] R. Majumdar, S. Basu, S. Ghosh, and S. Sur-Kolay. Quantum error-correcting code for ternary logic. *Physical Review A*, 97(5), **2018**. ISSN 2469-9926. doi:10.1103/PhysRevA.97.052302.

[66] W. F. Ke, K. F. Lai, and R. B. Zhang. Quantum codes from hadamard matrices. *Linear & Multilinear Algebra*, 58(7):847–854, **2010**. ISSN 0308-1087. doi:10.1080/03081080903062121.

[67] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, **1983**.