On asymmetric quantum error-correcting codes

Martianus Frederic Ezerman

2011

Martianus, F. E. (2011). On asymmetric quantum error-correcting codes. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/46253>

<https://doi.org/10.32657/10356/46253>

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

**ON ASYMMETRIC QUANTUM
ERROR-CORRECTING CODES**

MARTIANUS FREDERIC EZERMAN

**DIVISION OF MATHEMATICAL SCIENCES
SCHOOL OF PHYSICAL AND MATHEMATICAL
SCIENCES**

2011

ON ASYMMETRIC QUANTUM ERROR-CORRECTING CODES

MARTIANUS FREDERIC EZERMAN

DIVISION OF MATHEMATICAL SCIENCES
SCHOOL OF PHYSICAL AND MATHEMATICAL
SCIENCES

MARTIANUS FREDERIC EZERMAN

A thesis submitted to Nanyang Technological University
in partial fulfillment of the requirement for the degree of
Doctor of Philosophy in Mathematical Sciences

2011

Acknowledgements

My debt of gratitude goes to Prof. Ling San for teaching me how to do research, for giving me the freedom to pursue my interests, for being patient and, above all, for believing in me.

I thank my collaborators and mentors Patrick Solé and Markus Grassl for numerous discussions online and in person and for easing my way into the wider community of researchers. Somphong Jitman has become not just a close collaborator but also a dear friend who shares with me the joy of food and of traveling. To my collaborators Rado Kirov, Dima Pasechnik, and Olfa Yemen, thank you for the chance to learn and work together. Looking forward to collaborating again in future projects.

I am grateful for Mike Samson's friendship. Thanks for our semi-regular afternoon break sessions and weekend outings. It is always fun to have you around, Mike. The paper is a nice bonus. Birk Eisermann introduced me to the joy of German beers, sausages, and cookies. Thank you for your calming presence and for being my lifeline when it comes to Linux trouble shootings. Of those sharing Lab SPMS-MAS-04-21 with me, I would like to single out two friends: Romar de la Cruz for his deep faith and generosity and Lin Fuchun, whom I will never be able to beat at dining table.

The Cryptology and Coding Theory Research Group (CCRG) has been providing me with good research environment. I recall fondly various discussions during reading group and seminars.

Special thanks to Melvin Soh for his enthusiastic helps with matters related to computing resources.

I remember with deep gratitude some special teachers. The shorter list includes

Mr. Moedjiono and Ms. Lies Ernawati who taught me mathematics and science in elementary school back home in Madiun, East Java, Indonesia; Profs. Mari-Jo Ruiz, Evangeline Bautista, and Jose Marasigan of the Mathematics Department at the Ateneo de Manila Univeristy; Prof. Fidel Nemenzo of the University of the Philippines' Mathematics Department; Profs. Manny Dy, Ramon Reyes, and Fr. Luis David, SJ, of the Philosophy Department at the Ateneo de Manila Univeristy; Profs. Frédérique Oggier, Alfred Bruckstein, and Chaoping Xing at Nanyang Technological University.

A lot of personal support comes from two disjoint sets of beloved friends: the Manresa98 community, now scattered throughout the globe, and the XJ community here in Singapore. Indeed, our bonds extend far beyond the vows.

My parents and families from both sides have been most supportive. They welcome me home when I am weary and need to recharge. They encourage me to push forward despite knowing almost nothing of my work and allow me to share the joys and pains of research and life with them. My two brothers, both named Edward, know me more than anyone else but one. Thank you for the privilege.

To my best friend and partner Madeline Pe, thank you so much for sharing your life with me these past seven years. Would not be able to complete this without you, Love.

This work is specially dedicated to my sister Rina, whose courage and kindness throughout a prolonged period of personal struggle have taught me the meaning of perseverance.

Martianus Frederic EZERMAN

June 2011

List of Works

Below is the list of work done, in chronological order of completion, during my PhD studies in NTU.

1. M. F. Ezerman, M. Grassl, and P. Solé, *The Weights in MDS Codes*, IEEE Transactions on Information Theory, Vol. 57, No. 1, pp. 392–396, January 2011. Preprint at <http://arxiv.org/pdf/0908.1669v2>.
2. M. F. Ezerman, S. Ling, and P. Solé, *Additive Asymmetric Quantum Codes*, IEEE Transactions on Information Theory, to appear. Accepted for publication on March 2, 2011. Preprint at <http://arxiv.org/pdf/1002.4088>.
3. M. F. Ezerman, S. Ling, P. Solé, and O. Yemen, *From Skew-Cyclic Codes to Asymmetric Quantum Codes*, Advances in Mathematics of Communications, Vol. 5, No. 1, pp. 41–57, February 2011. Preprint at <http://arxiv.org/pdf/1005.0879>.
4. M. D. V. Samson and M. F. Ezerman, *Factoring Permutation Matrices Into a Product of Tridiagonal Matrices*. Preprint at <http://arxiv.org/pdf/1007.3467>.
5. M. F. Ezerman and R. Kirov, *Nonbinary Quantum Codes from Two-Point Divisors on Hermitian Curves*, Accepted and nominated for best student paper

award at International Symposium on Information Theory (ISIT) 2011, St. Petersburg, July 31 to August 5, 2011. Preprint at <http://arxiv.org/pdf/1102.3605>.

6. M. F. Ezerman, S. Jitman, and S. Ling, *Pure Asymmetric Quantum MDS Codes from CSS Construction*, Accepted for Third International Castle Meeting on Coding Theory and Applications (3ICMCTA) 2011, Castell de Cardona, September 11 to 15, 2011.
7. M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik, *CSS-like Constructions of Asymmetric Quantum Codes*. Work in progress, in final stage of preparation.

Contents

Acknowledgements	iii
List of Works	v
Abstract	xiv
1 Introduction	1
2 Preliminaries	9
2.1 Classical Coding Theory	10
2.2 Asymmetric Stabilizer Quantum Codes	14
3 The Functional Approach	22
3.1 The Closure Property	23
3.2 CSS-like Constructions	26
3.3 CSS-like is a Subset of Stabilizer	38
4 The Weights in Classical MDS Codes	42
4.1 Motivations to Study the Weights	43
4.2 Trivial MDS Codes	44

4.3	MDS Codes of Length $n \leq q$	45
4.4	MDS Codes of Length $q + 1$	47
4.5	MDS Codes of Length $q + 2$	50
4.6	An Alternative Approach	51
4.7	Summary on the Weights	53
5	Pure Asymmetric Quantum MDS Codes from CSS Construction	55
5.1	Quantum MDS Codes with $d_z \geq d_x = 2$	57
5.2	Quantum MDS Codes of Length $n \leq q$ with $d_z \geq d_x \geq 3$	60
5.3	Quantum MDS Codes of Length $n = q + 1$ with $d_z \geq d_x \geq 3$	64
5.4	Quantum MDS Codes of Length $n = 2^m + 2 \geq 6$ with $d_z = d_x = 4$	67
5.5	Explicit List for $\mathbb{F}_7$ and $\mathbb{F}_8$	67
5.6	Conclusions and Open Problems	68
6	Three Constructions of Nested Pairs of Classical Codes	71
6.1	Cyclic Construction	72
6.2	Construction from Group Character Codes	78
6.3	BKLC Construction	81
7	Additional Constructions for 4-ary Asymmetric Quantum Codes	82
7.1	Additive Codes over $\mathbb{F}_4$	83
7.2	From Extremal or Optimal Additive Self-Dual Codes over $\mathbb{F}_4$	84
7.3	From Self-Orthogonal Linear Codes	87
7.4	From Nested Additive Codes over $\mathbb{F}_4$	93
7.4.1	From Circulant Codes	93

7.4.2	From 4-Circulant and Bordered 4-Circulant Codes	95
7.4.3	From Two Proper Subcodes	96
7.5	Conclusions and Open Problems	97
8	From Skew-Cyclic Codes to 4-ary Asymmetric Quantum Codes	98
8.1	Preliminaries	99
8.2	The Mapping S on Codes over $\mathbb{F}_4$	100
8.3	Module θ -Cyclic Codes over $\mathbb{F}_4$	102
8.4	Analysis on the Weight Enumerators	111
8.5	Two Constructions	114
8.5.1	From Best-Known Linear Codes	114
8.5.2	From Concatenated Reed-Solomon Codes	117
8.6	Conclusions and Open Problems	120
9	Linear Programming and Optimal Pure CSS-like Codes	121
9.1	Linear Programming Bound	122
9.2	Tables of Optimal Pure Asymmetric CSS-like Codes and their Explicit Constructions	125
9.2.1	Optimal Pure Binary AQECCs	126
9.2.2	Optimal Pure Ternary AQECCs	130
9.2.3	Optimal and Good Pure 4-ary AQECCs	137
9.2.4	Optimal Pure 5-ary AQECCs	143
9.2.5	Optimal Pure 7-ary AQECCs	149
9.2.6	Optimal and Good Pure 8-ary AQECCs	153
9.2.7	Optimal and Good Pure 9-ary AQECCs	157

9.3	Scattered Notes and Ad Hoc Constructions	162
9.3.1	A Non Existence Result	162
9.3.2	Some BKLC' Construction	163
9.3.3	Ad Hoc Constructions	163
9.4	Conclusion and Open Problems	166

List of Tables

1.1	Some Examples Comparing Symmetric and Asymmetric QECCs for $q = 2$	4
5.1	Nontrivial AQMDS Codes for $\mathbb{F}_7$ and $\mathbb{F}_8$	70
7.1	Best-Known Additive Self-Dual Codes over $\mathbb{F}_4$ for even $n \leq 30$ and the Resulting AQECCs	86
7.2	Best-Known Additive Self-Dual Codes over $\mathbb{F}_4$ for odd $n \leq 30$ and the Resulting AQECCs	86
7.3	Good AQECCs from Classified Hermitian Self-Orthogonal $\mathbb{F}_4$ -Linear Codes in [14]	89
7.4	Good AQECCs from Hermitian Self-Dual $\mathbb{F}_4$ -Linear Codes based on [38, Table 7] for $32 \leq n \leq 80$	90
7.5	More AQECCs from Hermitian Self-orthogonal $\mathbb{F}_4$ -Linear Codes for $n \leq 40$	91
7.6	AQECCs from Hermitian Self-orthogonal Quasi-Twisted Codes Found in [42]	92
7.7	AQECCs from MacDonald codes	93

7.8	Best-Known AQECCs from Additive Circulant Codes for $n \leq 30$	94
7.9	Good AQECCs from Additive Bordered 4-Circulant Codes for $n \leq 30$	96
8.1	Asymmetric QECC from BKLC	116
8.2	$[[64, k', d_z/2]]_4$ -code Q from $[16, k, 16 - k + 1]_{16}$ -extended RS codes . .	119
8.3	$[[384, k', d_z/2]]_4$ -code Q from $[64, k, 64 - k + 1]_{64}$ -extended RS codes .	119
9.1	Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_2$	127
9.2	Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_2$ and the Resulting CSS Codes	130
9.3	Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_3$	133
9.4	Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_3$ and the Resulting CSS Codes	136
9.5	Optimal and Good Pure Asymmetric CSS-like Codes over $\mathbb{F}_4$	141
9.6	Explicit Lists of Nested $\mathbb{F}_2$ -linear Cyclic Codes over $\mathbb{F}_4$ and the Result- ing CSS-like Codes	142
9.7	Explicit Lists of Nested Linear Cyclic Codes over $\mathbb{F}_4$ and the Resulting CSS-like Codes	143
9.8	Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_5$	146
9.9	Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_5$ and the Resulting CSS Codes	148
9.10	Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_7$	151
9.11	Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_7$ and the Resulting CSS Codes	152
9.12	Optimal and Good Pure Asymmetric CSS-like Codes over $\mathbb{F}_8$	155

9.13 Explicit Lists of Nested $\mathbb{F}_2$ -Linear Cyclic Codes over $\mathbb{F}_8 = \mathbb{F}_2(w)$ and the Resulting CSS-like Codes	156
9.14 Explicit Lists of Nested Linear Cyclic Codes over $\mathbb{F}_8$ and the Resulting CSS-like Codes	157
9.15 Optimal and Good Pure Asymmetric CSS-like Codes over $\mathbb{F}_9$	160
9.16 Explicit Lists of Nested $\mathbb{F}_3$ -Linear Cyclic Codes over $\mathbb{F}_9 = \mathbb{F}_3(w)$ and the Resulting CSS-like Codes	161
9.17 Explicit Lists of Nested Linear Cyclic Codes over $\mathbb{F}_8$ and the Resulting CSS-like Codes	162

Abstract

This thesis focuses on the construction and analysis of the parameters of asymmetric quantum error-correcting codes (AQECCs). We use the so-called functional approach to connect AQECCs to classical codes via orthogonal arrays.

Based on the functional approach, we derive pure AQECCs from CSS-like constructions that include the standard CSS construction known prior to this work. The CSS-like constructions remove both the specific choice of Euclidean inner product and the $\mathbb{F}_q$ -linearity condition imposed by the standard variant. Hence, pure AQECCs can now be constructed by using pairs of nested $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ where $\mathbb{F}_r$ is any subfield of $\mathbb{F}_q$ under the Euclidean, trace Euclidean, Hermitian, and trace Hermitian inner products. Relationships between the various CSS-like constructions are also exhibited.

A formal definition of asymmetric stabilizer codes is given and a connection between pure asymmetric stabilizer codes and AQECCs derived from the CSS-like constructions is established. It is shown that the class of pure CSS-like AQECCs forms a subset of asymmetric stabilizer codes.

We show how classical linear MDS codes can be used to construct AQECCs that satisfy the quantum Singleton bound with $d_z \geq d_x \geq 2$ for all possible values of length n for which linear MDS codes over $\mathbb{F}_q$ are known to exist.

Beyond the lengths specified by the classical MDS conjecture, various explicit constructions of nested pairs of classical codes can be combined with linear programming to establish the optimality of pure CSS-like codes with parameters $[[n, k, d_z/d_x]]_q$. For $q = \{2, 3, 4, 5, 7, 8, 9\}$, lists of optimal asymmetric CSS-like codes for reasonable

lengths are presented. The explicit choices for the nested pairs of classical codes are given as well.

With explicit examples, it is shown that by using nested pairs of $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ with fixed n, d_z and d_x , we can get AQECCs with larger dimensions than relying solely on the best ones obtainable from nested $\mathbb{F}_q$ -linear codes. This justifies our effort of extending the standard CSS construction.

Chapter 1

Introduction

Throughout this thesis, the term *quantum code* is used as a shorthand for quantum error-correcting code. Hence, the abbreviation AQECCs stands for asymmetric quantum error-correcting codes.

Quantum codes have been garnering a lot of interest due to their salient roles in quantum information processing. They protect information-carrying quantum states against decoherence and play an important part in making fault-tolerant quantum computation possible.

There will never exist a quantum computer without efficient quantum error correction.

Quantum codes can also be distinguished into *pure* and *degenerate*. The pure ones are usually easier to implement due to their simpler decoding process.

A firm connection between classical error-correcting codes and quantum codes has been well-established in [16] for the binary case, and in [3] and [51] for the q -ary cases. Pioneering works on this so-called *stabilizer formalism* can also be found in Daniel

Gottesman's PhD dissertation [34]. The formalism allows us to construct quantum codes from classical codes under some conditions. Such quantum codes are known as *stabilizer codes*.

One way to construct stabilizer codes based on classical codes is by using the so-called CSS method, due to Calderbank, Shor, and Steane. A pair of nested classical linear codes is the main ingredient of this construction.

In terms of the implementation of quantum error-correction, the state-of-the-art is still binary. There is, however, some theoretical interest in exploring whether nonbinary quantum codes can be useful in fault-tolerant quantum computation. As noted in [62], there is a possible implementation of such codes in certain ion trap models. Over $q = 2^l$, they are useful for constructing easily decodable binary codes via concatenation.

There have been several attempts at generalizing the stabilizer approach. Using any valid basis for the abstract quantum error group, one can define *Clifford codes* [54]. It remained unclear whether or not these codes can be superior to stabilizer codes in terms of parameters. It is known that Clifford codes are stabilizer codes whenever the abstract error group is given by an extraspecial p -group.

The union stabilizer approach explained, for instance, in [39] provides another extension of the stabilizer formalism. This approach has been further extended to *codeword stabilized codes* [20].

In constructing quantum codes, it is of course important to aim for the codes with the best possible parameters. To know the limit of what set of parameters can be theoretically achieved, we need to establish bounds on them as a measure of how good the constructed codes are.

There are known bounds on the parameters of quantum codes. The quantum analogue of the Gilbert-Varshamov (GV) bound was first established in [3]. The quantum analogues of the Singleton and Hamming bounds are also well-known.

Another exciting recent development comes from the realization that, in many quantum mechanical systems, different types of error are not equiprobable. The phase-flip or X -errors, for instance, may happen less frequently than the bit-flip or Z -errors as well as the combined bit-phase flip or Y -errors. In the words of Ioffe and Mézard [49],

The noise in physical qubits is fundamentally asymmetric: in most devices, phase errors are much more probable than bit flips.

Further details from physics, both theoretical and experimental, can be found in [24] and [49] as well as the references therein.

These recent realizations motivate the task of designing good quantum codes, *i.e.* codes that detect and, hence, correct as many errors as possible, given the ratio of asymmetry in a particular quantum channel.

Table 1.1 lists down some comparison between best performing asymmetric and symmetric qubit codes. Notice that, given more information on the asymmetry present in a particular channel, we can better tailor our codes to get better error-correcting performance. The parameters will be explained in details in the sequels.

The standard CSS construction immediately extends to the asymmetric case. Early work on mostly binary AQECCs can be found in [1] and in [65]. It is noted in the latter reference that, in general, any class of nested classical $\mathbb{F}_q$ -linear codes can be used to construct AQECCs, provided that one can compute or approximate

Table 1.1: Some Examples Comparing Symmetric and Asymmetric QECCs for $q = 2$

n	k	Symmetric d	Asymmetric (d_z, d_x)
7	3	2	(3, 2)
8	3	3	(4, 2)
15	1	5	(7, 3)

the dual distance of the inner code. Obvious candidates that have been investigated before are binary AQECCs derived from nested pair of Reed-Muller codes and from nested cyclic, especially BCH, codes as well as from the pairing of LDPC codes and BCH codes.

Using a different approach, which we call the *functional approach*, to quantum codes, necessary and sufficient conditions for the existence of general quantum codes are given in [30]. This approach leads to the improvement of the asymptotic quantum GV bound and opens up new directions to pursue.

Following the method suggested in [30], a general mathematical characterization using the functional approach and some constructions of AQECCs are given in [69]. In the said reference, some asymptotic facts regarding the parameters of AQECCs have been established.

While we know quite a lot regarding AQECCs, much remains to be investigated. In this thesis, we investigate the constructions and parameters of optimal or good codes, under the functional approach, in the context of channel asymmetry and establish their connection to nested pairs of classical codes under various inner products, not limited to the usual Euclidean inner product employed in the standard CSS construction.

Problem 1: A major advantage of the functional approach to quantum codes in

both the symmetric and asymmetric cases is the combinatorial nature of the characterization. In the construction of q -ary AQECCs from a pair of nested classical codes, can the particular choice of an inner product be shown to be non critical?

More specifically, can the CSS construction be extended by relaxing the condition that the inner product used must be Euclidean and that the classical codes in the nested pair must be $\mathbb{F}_q$ -linear? What gain do we get from the extension?

Problem 2: Is it possible to formally establish an analogue of the stabilizer formalism for the asymmetric case?

Problem 3: In the symmetric case, it is well-known that the class of CSS codes is strictly a subset of the stabilizer codes. The $[[5, 1, 3]]_2$ -stabilizer code, for instance, can not be derived from the CSS construction. Assuming that the answer to Problem 1 above is positive, what can we say about the parameters of pure asymmetric stabilizer codes as compared to those derived from CSS-like constructions?

Problem 4: Construct AQECCs that achieve the equality of the quantum Singleton bound.

Problem 5: Compute the linear programming bound for pure AQECCs to decide on the optimality of q -ary AQECCs of reasonable lengths for small $q \in \{2, 3, 4, 5, 7, 8, 9\}$.

The followings are the contributions of this thesis:

Contribution 1: We extend the functional approach to include the so-called CSS-like constructions based on pairs of nested $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ where $\mathbb{F}_r$ is any subfield of $\mathbb{F}_q$. We call such codes *subfield linear codes*.

Contribution 2: It is shown that the stabilizer formalism extends naturally to the asymmetric case. Further, the fact that CSS-like AQECCs constitute a subclass

of asymmetric stabilizer codes is established. It remains an open question whether CSS-like AQECCs are as good as pure asymmetric stabilizer codes in the sense that they have equal parameters.

Contribution 3: Assuming the validity of the classical MDS Conjecture, we show how linear MDS codes can be used to construct asymmetric quantum MDS codes with $d_z \geq d_x \geq 2$ for all possible values of length n for which linear MDS codes over $\mathbb{F}_q$ are known to exist.

Contribution 4: By explicit examples, we show that by using nested pairs of $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ with fixed n, d_z and d_x , we can get AQECCs with larger dimensions than relying solely on the best ones obtainable from nested $\mathbb{F}_q$ -linear codes. This justifies our effort of extending the standard CSS construction. The tools used are specific constructions of nested $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ to establish existence and linear programming to derive a theoretical upper bound on the dimension of the possible AQECCs, given each set of parameters (n, q, d_z, d_x) under consideration. Some of the constructed quantum codes are then shown to be optimal.

Contribution 5: Lists of optimal or best known pure CSS-like codes for reasonable lengths for $q \in \{2, 3, 4, 5, 7, 8, 9\}$ are presented.

The thesis is organized into nine chapters. This Chapter 1 presents a brief history and the motivation behind the studies of quantum codes in general and of asymmetric quantum codes in particular. Also provided are the list of problems being considered and this thesis' contributions in solving the problems.

Chapter 2 provides necessary definitions and results needed in the sequels. It collects relevant background materials from classical coding theory and formally defines asymmetric stabilizer quantum codes. The highlight of the chapter is Theorem 2.2.8

which establishes their link to classical codes.

The most theoretical part of the thesis can be found in Chapter 3. We begin by deriving the closure property of an $\mathbb{F}_r$ -linear code C over $\mathbb{F}_q$ under the trace Euclidean inner product and establish the MacWilliams equation for this family of codes. Three important tasks are accomplished in this chapter. First, a proof using the functional approach on how to derive pure AQECCs based on nested pairs of $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ under the trace Euclidean inner product is given. Second, we show how this construction is related to other previously known CSS-like constructions. Finally, the fact that CSS-like AQECCs constitute a subclass of asymmetric stabilizer codes is shown.

When constructing AQECCs, it is important to know what we are aiming at, in terms of parameters. In Chapter 5 we discuss the class of asymmetric quantum MDS codes based on CSS construction. This class consists of AQECCs that achieve the equality of the quantum Singleton bound. The discussion makes use of important facts regarding the weights of classical MDS codes provided in Chapter 4.

If we assume the classical MDS conjecture, CSS asymmetric quantum MDS codes are limited in length. For q -ary quantum codes, the largest length possible is bounded by $q + 1$ for odd q and by $q + 2$ for even q . In Chapter 6 we are interested in the best-possible parameters that a q -ary AQECC can achieve for lengths above the largest MDS length. We call such a code *optimal*.

To get AQECCs with relatively good parameters, we directly construct nested pairs of classical codes and derive the parameters of the resulting codes. Three constructions are considered, namely a construction based on nested cyclic $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$, a construction from nested group character codes, and a construction

based on best-known linear codes (BKLC) of length n having a codeword $\mathbf{v}$ such that $\text{wt}_H(\mathbf{v}) = n$. This last construction yields AQECCs with $d_x = 2$.

In Chapter 7 we discuss some additional constructions of nested pairs of codes over $\mathbb{F}_4$.

In the scenario where we need to detect a lot of Z -errors while the detection for X -errors is not critical, say when $d_x = 2$ can be safely assumed, the construction discussed in Chapter 8 is of great use.

In Chapter 9 we compare the parameters of the AQECCs derived from the nested pairs of classical codes constructed by the methods outlined in Chapters 6, 7, and 8 against the parameters derived from linear programming.

When optimality can be inferred, the explicit constructions of the corresponding nested classical codes are listed down. The last section prior to the summary contains some instructive ad-hoc constructions which give us some optimal AQECCs or rule out the possibility of certain AQECCs.

Chapters 5, 7, 8, and 9 end with a summary and some open problems for future investigations.

Chapter 2

Preliminaries

This chapter provides necessary definitions and results needed in the sequels. Section 2.1 collects relevant background materials from classical coding theory. We treat asymmetric stabilizer quantum codes in Section 2.2 and contribute Theorem 2.2.8 which establishes their link to classical codes.

Throughout this thesis, let $\mathbb{F}_p \subseteq \mathbb{F}_r \subseteq \mathbb{F}_q$ with $r = p^l$ and $q = r^m$ be finite fields. The trace mapping $\text{Tr}_{q/r} : \mathbb{F}_q \rightarrow \mathbb{F}_r$ is given by $\text{Tr}_{q/r}(\beta) = \beta + \beta^r + \beta^{r^2} + \dots + \beta^{r^{m-1}}$. The subscript q/r is omitted whenever $r = p$ and q is clear from the context. Important properties of the trace mapping can be found in [56, Th. 2.23].

If $q = r^2$, let $\bar{a}$ denote a^r for all $a \in \mathbb{F}_q$. For $\mathbf{u} = (u_1, u_2, \dots, u_n) \in \mathbb{F}_q^n$, $\bar{\mathbf{u}}$ stands for $(\bar{u}_1, \bar{u}_2, \dots, \bar{u}_n)$. Hence, for any set $C \subseteq \mathbb{F}_q^n$, $\bar{C} := \{\bar{\mathbf{c}} : \mathbf{c} \in C\}$.

If G is a group, then the *center* of G is $Z(G) := \{g \in G : gx = xg \text{ for all } x \in G\}$. If $S \subseteq G$, then the *centralizer* of S in G , written as $C_G(S)$, is $\{g \in G : gxg^{-1} = x \text{ for all } x \in S\}$. We denote by $SZ(G)$ the group generated by S and $Z(G)$. The notation $H \leq G$ signifies that H is a subgroup of G .

If M is a square matrix, then $\text{Trace}(M)$ is the sum of its diagonal elements.

2.1 Classical Coding Theory

The *Hamming weight* of a vector $\mathbf{v} \in \mathbb{F}_q^n$, denoted by $\text{wt}_H(\mathbf{v})$, is the number of its nonzero entries. Given two elements $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, the number of positions where their respective entries disagree, written as $\text{dist}(\mathbf{u}, \mathbf{v})$, is called the *Hamming distance* of $\mathbf{u}$ and $\mathbf{v}$. Let $C \subseteq \mathbb{F}_q^n$ be nonempty. The *minimum distance* $d = d(C)$ is given by

$$d = \min\{\text{dist}(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}.$$

Given any two distinct codes C and D , let the notation $\text{wt}_H(C \setminus D)$ denote $\min\{\text{wt}_H(\mathbf{u}) : \mathbf{u} \in C \setminus D, \mathbf{u} \neq \mathbf{0}\}$.

An $[n, k, d]_q$ -linear code C of length n , dimension k , and minimum distance d is a subspace of dimension k of the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. For a general, not necessarily $\mathbb{F}_q$ -linear, code $C \subseteq \mathbb{F}_q^n$, the notation $(n, M = |C|, d)_q$ is commonly used. A code C is said to be an $\mathbb{F}_r$ -linear code over $\mathbb{F}_q$ if C is a subspace of the $\mathbb{F}_r$ -vector space $\mathbb{F}_q^n$.

It is often useful to determine when two codes are essentially the same in terms of their properties. The concept of *equivalence* of codes is introduced to serve such a purpose. A more detailed discussion on equivalence can be found in [48, Sects. 1.6 and 1.7].

A *monomial matrix* L is a square matrix over $\mathbb{F}_q$ with exactly one nonzero entry in each row and each column. Such a matrix can be written either as DP or PD' where D and D' are diagonal matrices and P is a permutation matrix.

Definition 2.1.1. Two $\mathbb{F}_q$ -linear codes C_1 and C_2 of the same length n are said to

be equivalent if there exist a monomial matrix L and an automorphism γ of $\mathbb{F}_q$ such that

$$C_2 = \{\gamma(v_1), \gamma(v_2), \dots, \gamma(v_n)\}$$

where $\{\mathbf{v} = \mathbf{c}L : \mathbf{c} \in C_1\}$. If γ is the identity automorphism, then we say that C_1 and C_2 are monomially equivalent.

Note that equivalent codes have the same parameters.

For $\mathbf{u} = (u_1, u_2, \dots, u_n)$ and $\mathbf{v} = (v_1, v_2, \dots, v_n)$ in $\mathbb{F}_q^n$, we define the following inner products:

1. $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{E}} := \sum_{i=1}^n u_i v_i$ is the *Euclidean inner product* of $\mathbf{u}$ and $\mathbf{v}$.
2. $\langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr}_{q/r} \mathbb{E}} := \text{Tr}_{q/r}(\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{E}})$ is the *trace Euclidean inner product* of $\mathbf{u}$ and $\mathbf{v}$ valued in $\mathbb{F}_r$.
3. When $\mathbb{F}_q$ is a quadratic extension of $\mathbb{F}_r$, $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{H}} := \sum_{i=1}^n u_i \bar{v}_i = \langle \mathbf{u}, \bar{\mathbf{v}} \rangle_{\mathbb{E}}$ is the *Hermitian inner product* of $\mathbf{u}$ and $\mathbf{v}$.
4. Let $q = r^2$. Then there are two cases of *trace Hermitian inner product* depending on the field characteristic:
 - (a) For even q , $\langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr} \mathbb{H}} := \text{Tr}_{q/r}(\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{H}})$.
 - (b) For odd q , $\langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr} \mathbb{H}} := \text{Tr}_{q/r}(\alpha \langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{H}})$ where $\alpha \in \mathbb{F}_q \setminus \{0\}$ is such that $\bar{\alpha} = -\alpha$.

To define asymmetric stabilizer codes, we need yet another inner product. Given $(\mathbf{a}|\mathbf{b}), (\mathbf{c}|\mathbf{d}) \in \mathbb{F}_q^{2n}$,

$$\langle (\mathbf{a}|\mathbf{b}), (\mathbf{c}|\mathbf{d}) \rangle_{\text{s}} := \text{Tr}(\langle \mathbf{a}, \mathbf{d} \rangle_{\mathbb{E}} - \langle \mathbf{b}, \mathbf{c} \rangle_{\mathbb{E}})$$

is the *trace-symplectic inner product* of $(\mathbf{a}|\mathbf{b})$ and $(\mathbf{c}|\mathbf{d})$. The *symplectic weight* $\text{wt}_s(\mathbf{a}|\mathbf{b})$ of $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$ is given by

$$\text{wt}_s(\mathbf{a}|\mathbf{b}) := |\{1 \leq i \leq n : (a_i, b_i) \neq (0, 0)\}|.$$

Let $\mathcal{C} \subseteq \mathbb{F}_q^{2n}$. The trace-symplectic dual $\mathcal{C}^{\perp_s}$ of $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_s} := \{(\mathbf{c}|\mathbf{d}) \in \mathbb{F}_q^{2n} : \langle (\mathbf{a}|\mathbf{b}), (\mathbf{c}|\mathbf{d}) \rangle_s = 0 \ \forall (\mathbf{a}|\mathbf{b}) \in \mathcal{C}\}.$$

Let C be a code. Let $*$ represent one of the Euclidean, trace Euclidean, Hermitian and trace Hermitian inner products, the *dual code* $C^{\perp*}$ of C is given by

$$C^{\perp*} := \{\mathbf{u} \in \mathbb{F}_q^n : \langle \mathbf{u}, \mathbf{v} \rangle_* = 0 \text{ for all } \mathbf{v} \in C\}$$

while the dual distance $d^{\perp*}$ is defined to be $d(C^{\perp*})$.

If $C \subseteq C^{\perp*}$, then C is said to be *self-orthogonal*. C is *self-dual* when equality holds.

A family of codes is *closed* under a particular inner product $*$ if $(C^{\perp*})^{\perp*} = C$ for each C in the family. The closure property under the Euclidean, Hermitian and trace Hermitian inner products is well-known from [61, Ch. 3]. The said property under the trace Euclidean inner product will be established in Theorem 3.1.2.

Definition 2.1.2. *The weight enumerator $W_C(X, Y)$ of an $(n, M = |C|, d)_q$ -code C is the polynomial*

$$W_C(X, Y) = \sum_{i=0}^n A_i X^{n-i} Y^i, \quad (2.1.1)$$

where A_i is the number of codewords of Hamming weight i in the code C .

Under the Euclidean, Hermitian, and trace Hermitian inner products, the weight enumerator of the dual code of an $(n, M = |C|, d)_q$ -code C is connected to the weight

enumerator of the code C via the MacWilliams Equation

$$W_{C^{\perp*}}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y). \quad (2.1.2)$$

For computational purposes, it is often more convenient to set the variable $X = 1$. A useful equivalent statement to Equation (2.1.2) requires the use of the *Krawtchouk polynomials*.

Definition 2.1.3. A *Krawtchouk polynomial of degree j in variable i* is given by

$$K_j^{n,q}(i) := \sum_{l=0}^j (-1)^l (q-1)^{j-l} \binom{i}{l} \binom{n-i}{j-l}. \quad (2.1.3)$$

For $0 \leq j \leq n$, let $A_j^{\perp*}$ denote the number of codewords of weight j in $C^{\perp*}$. Then

$$A_j^{\perp*} = \frac{1}{|C|} \sum_{i=0}^n A_i K_j^{n,q}(i). \quad (2.1.4)$$

Equation (2.1.4) will feature prominently in the linear programming set-up detailed in Chapter 9.

An important tool that will be used in the proof of Theorem 3.2.3 is a natural correspondence between classical codes and orthogonal arrays. We start with the definition of orthogonal arrays before providing more details on the said correspondence.

Definition 2.1.4. Let F be a set of q symbols or levels. An orthogonal array A with M runs, n factors, q levels and strength t with index λ , denoted by $OA(M, n, q, t)$, is an $M \times n$ array A with entries from F such that every $M \times t$ subarray of A contains each t -tuple of F^t exactly $\lambda = \frac{M}{q^t}$ times as a row.

The codewords in a code C can be seen as the rows of an orthogonal array A and vice versa. The following proposition is due to Delsarte (see [22, Th. 4.5]). Note that the code C in the proposition is a general code, not requiring $\mathbb{F}_q$ -linearity. The duality here is defined over any valid inner product.

Proposition 2.1.5. [44, Th. 4.9] *If C is an $(n, M = |C|, d)_q$ code with dual distance $d^\perp$, then the corresponding orthogonal array is an $OA(M, n, q, d^\perp - 1)$. Conversely, the code corresponding to an $OA(M, n, q, t)$ is an $(n, M, d)_q$ code with dual distance $d^\perp \geq t + 1$. If the orthogonal array has strength t but not $t + 1$, then $d^\perp$ is precisely $t + 1$.*

2.2 Asymmetric Stabilizer Quantum Codes

Let $\mathbb{C}$ be the field of complex numbers and $\eta = e^{\frac{2\pi\sqrt{-1}}{p}} \in \mathbb{C}$. We fix an orthonormal basis of $\mathbb{C}^q$

$$\{|\varphi\rangle : \varphi \in \mathbb{F}_q\}$$

with respect to the Hermitian inner product on $\mathbb{C}^q$. For a positive integer n , let $V_n = (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$ be the n th tensor product of $\mathbb{C}^q$. Then V_n has the following orthonormal basis

$$\{|\mathbf{c}\rangle = |c_1 c_2 \dots c_n\rangle : \mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n\}, \quad (2.2.1)$$

where $|c_1 c_2 \dots c_n\rangle$ abbreviates $|c_1\rangle \otimes |c_2\rangle \otimes \dots \otimes |c_n\rangle$.

For two quantum states $|\varphi\rangle$ and $|\psi\rangle$ in V_n with

$$|\varphi\rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \alpha(\mathbf{c}) |\mathbf{c}\rangle \text{ and } |\psi\rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \beta(\mathbf{c}) |\mathbf{c}\rangle,$$

where $\alpha(\mathbf{c}), \beta(\mathbf{c}) \in \mathbb{C}$, the Hermitian inner product of $|\varphi\rangle$ and $|\psi\rangle$ is given by

$$\langle \varphi | \psi \rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \widetilde{\alpha(\mathbf{c})} \beta(\mathbf{c}) \in \mathbb{C},$$

where $\widetilde{\alpha(\mathbf{c})}$ is the complex conjugate of $\alpha(\mathbf{c})$. We say $|\varphi\rangle$ and $|\psi\rangle$ are *orthogonal* if $\langle \varphi | \psi \rangle = 0$.

To measure the performance of a quantum code, an appropriate error model must be chosen. Essentials on the standard mathematical error model of quantum error-correction can be found, for instance, in [30] and in [51] for the symmetric case and in [69] for the asymmetric case. For brevity, necessary definitions and known results are listed without elaboration or proof.

To define a quantum code Q , we need to consider the set of error operators that Q can handle. First, a nice basis $\mathcal{E}_n$ of the vector space of complex $q^n \times q^n$ matrices $\mathcal{M}_{q^n}(\mathbb{C})$ needs to be chosen. Let $a, b \in \mathbb{F}_q$. The unitary operators $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ are defined by

$$X(a)|\varphi\rangle = |\varphi + a\rangle \text{ and } Z(b)|\varphi\rangle = \eta^{\langle b, \varphi \rangle_{\text{Tr E}}} |\varphi\rangle. \quad (2.2.2)$$

Based on Equation (2.2.2), for $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$, we can write $X(\mathbf{a}) = X(a_1) \otimes \dots \otimes X(a_n)$ and $Z(\mathbf{a}) = Z(a_1) \otimes \dots \otimes Z(a_n)$ for the tensor product of n error operators. The set $\mathcal{E}_n := \{X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ is a nice error basis on V_n .

The error group G_n is generated by the matrices in $\mathcal{E}_n$. Here we need to make a distinction according to the characteristic of $\mathbb{F}_q$. When $\mathbb{F}_q$ is of characteristic odd prime p , G_n is a group of exponent p and of order pq^{2n} .

$$G_n := \{\eta^c X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}.$$

When $\mathbb{F}_q$ is of characteristic 2, the error group G_n is of exponent 4 and is given by

$$G_n := \{\pm X(\mathbf{a})Z(\mathbf{b}), \pm iX(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}.$$

In this case, $Z(G_n) = \{\pm I, \pm iI\}$.

Let $E = \eta^c X(\mathbf{a})Z(\mathbf{b}) \in G_n$. Then the *quantum weight* $\text{wt}_Q(E)$ of E is $\text{wt}_s(\mathbf{a}|\mathbf{b})$. The number of X -errors $\text{wt}_X(E)$ and the number of Z -errors $\text{wt}_Z(E)$ in the error

operator E are given, respectively, by $\text{wt}_H(\mathbf{a})$ and $\text{wt}_H(\mathbf{b})$. For a nonempty subset $\mathcal{S}$ of G_n , $\text{wt}_X(\mathcal{S}) = \min\{\text{wt}_X(E) : E \in \mathcal{S} \setminus \{I_n\}\}$. Similarly for $\text{wt}_Z(\mathcal{S})$.

Definition 2.2.1. A q -ary quantum code of length n is a subspace Q of V_n with dimension $K \geq 1$. A quantum code Q of dimension $K \geq 2$ is said to detect $d - 1$ qudits of errors for $d \geq 1$ if, for every orthogonal pair $|\varphi\rangle$ and $|\psi\rangle$ in Q and every $E \in G_n$ with $\text{wt}_Q(E) \leq d - 1$, $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal. In this case, we call Q a symmetric quantum code with parameters $((n, K, d))_q$ or $[[n, k, d]]_q$, where $k = \log_q K$. Such a quantum code is called pure if $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal for any (not necessarily orthogonal) $|\varphi\rangle$ and $|\psi\rangle$ in Q and any $E \in G_n$ with $1 \leq \text{wt}_Q(E) \leq d - 1$. A quantum code Q with $K = 1$ is assumed to be pure.

Let d_x and d_z be positive integers. A quantum code Q in V_n with dimension $K \geq 2$ is called an asymmetric quantum code with parameters $((n, K, d_z/d_x))_q$ or $[[n, k, d_z/d_x]]_q$, where $k = \log_q K$, if Q detects $d_x - 1$ qudits of X -errors and, at the same time, $d_z - 1$ qudits of Z -errors. That is, if $\langle \varphi | \psi \rangle = 0$ for $|\varphi\rangle, |\psi\rangle \in Q$, then $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal for any $E \in G_n$ such that $\text{wt}_X(E) \leq d_x - 1$ and $\text{wt}_Z(E) \leq d_z - 1$. Such an asymmetric quantum code Q is called pure if $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal for any $|\varphi\rangle, |\psi\rangle \in Q$ and any $E \in G_n$ such that $\text{wt}_Q(E) \geq 1$ and E satisfies

$$\begin{cases} \text{wt}_X(E) \leq d_x - 1 \\ \text{wt}_Z(E) \leq d_z - 1 \end{cases}.$$

An asymmetric quantum code Q with $K = 1$ is assumed to be pure.

Remark 2.2.2. An asymmetric quantum code with parameters $((n, K, d/d))_q$ is a symmetric quantum code with parameters $((n, K, d))_q$, but the converse is not true

since, for $E \in G_n$ with $\text{wt}_X(E) \leq d - 1$ and $\text{wt}_Z(E) \leq d - 1$, $\text{wt}_Q(E)$ may be bigger than $d - 1$. Whenever appropriate, our results regarding asymmetric quantum codes apply to the symmetric cases as well.

The set of stabilizer codes constitutes a specific type of quantum codes. For both symmetric and asymmetric cases, the usual definition of stabilizer codes applies.

Definition 2.2.3. A stabilizer code Q is a nonzero subspace of V_n that satisfies

$$Q = \bigcap_{E \in S} \{|\varphi\rangle \in V_n : E|\varphi\rangle = |\varphi\rangle\} \quad (2.2.3)$$

for some subgroup S of G_n . That is Q is the joint eigenspace of eigenvalue 1 of a subgroup S of the error group G_n .

The term *asymmetric stabilizer codes* refer to stabilizer codes which are robust under the effect of operators $E \in G_n$ with $\text{wt}_X(E) \leq d_x - 1$ and $\text{wt}_Z(E) \leq d_z - 1$.

We start by recalling two important aspects of quantum error-correction established previously, namely:

1. The Galois connection between the lattice $\mathcal{G}$ of subgroups of G_n and the set $\mathcal{Q}$ of all subspaces of V_n . This connection highlights the importance of the class of stabilizer codes.
2. How to use classical codes to characterize the errors in G_n that a stabilizer code can handle accurately.

For brevity, only pertinent and relevant definitions and results are listed down. We refer readers interested in further details to Sections III and IV of [51].

The set $\mathcal{Q}$ is a poset under the inclusion relation. In fact, $\mathcal{Q}$ is a complete order lattice whose elements are quantum codes or the zero trivial vector space. Two order-reversing maps between $\mathcal{G}$ and $\mathcal{Q}$ can be defined as follows

$$\text{Fix} : \mathcal{G} \rightarrow \mathcal{Q}$$

$$S \mapsto \bigcap_{E \in S} \{|\varphi\rangle \in V_n : E|\varphi\rangle = |\varphi\rangle\} \text{ and}$$

$$\text{Stab} : \mathcal{Q} \rightarrow \mathcal{G}$$

$$Q \mapsto \{E \in G_n : E|\varphi\rangle = |\varphi\rangle \text{ for all } |\varphi\rangle \in Q\}.$$

The two maps form a Galois correspondence. A subspace Q of the vector space V_n satisfying $Q = \text{Fix}(\text{Stab}(Q))$ is called a *closed subspace*, and a subgroup $S \leq G_n$ satisfying $S = \text{Stab}(\text{Fix}(S))$ is called a *closed subgroup*. A closed subspace is a stabilizer code or is 0-dimensional.

Proposition 2.2.4. [51, Prop. 6] *The closed subspaces of V_n form a complete sublattice $\mathcal{Q}_c$ of the lattice $\mathcal{Q}$. The closed subgroups of G_n form a complete sublattice $\mathcal{G}_c$ of the lattice $\mathcal{G}$ that is dual isomorphic to the lattice $\mathcal{Q}_c$.*

The usefulness of the Galois correspondence becomes apparent if we consider the fact that an arbitrary quantum code Q' is contained in the larger stabilizer code $Q = \text{Fix}(\text{Stab}(Q'))$. If an error operator E can be detected by Q , then it can be detected by Q' as well. Therefore, if the stabilizer code Q has distances d_x and d_z , then the code Q' has distances at least d_x and d_z .

Given a stabilizer group $S \leq G_n$ and its corresponding stabilizer code Q , we recall some facts about the error operators involved.

Lemma 2.2.5. [51, Lem. 5] Let $E := \eta^c X(\mathbf{a})Z(\mathbf{b})$ and $E' := \eta^{c'} X(\mathbf{a}')Z(\mathbf{b}')$ be elements of G_n . Then

$$EE' = \eta^{\text{Tr}(\langle \mathbf{b}, \mathbf{a}' \rangle_{\mathbb{E}} - \langle \mathbf{b}', \mathbf{a} \rangle_{\mathbb{E}})} E' E.$$

Lemma 2.2.6. [51, Lem. 10] $S \leq G_n$ is closed if and only if S is an abelian subgroup satisfying $S \cap Z(G_n) = \{I\}$ or $S = G_n$.

The characterization of detectable error operator is given in the following theorem. This allows us to use classical codes in the construction of AQECCs.

Lemma 2.2.7. [51, Lem. 11] Suppose that $S \leq G_n$ is the stabilizer group of a stabilizer code Q of dimension $\dim Q > 1$. An error E in G_n is detectable by the quantum code Q if and only if E is an element of $SZ(G_n)$ or E does not belong to the centralizer $C_{G_n}(S)$.

Theorem 2.2.8. An $((n, K, d_z/d_x))_q$ -stabilizer code Q exists if and only if there exists an $\mathbb{F}_p$ -linear code $\mathcal{C} \subseteq \mathbb{F}_q^{2n}$ of size $|\mathcal{C}| = \frac{q^n}{K}$ such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$ and for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ such that $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s} \setminus \mathcal{C}$, $\text{wt}_H(\mathbf{a}) \geq d_x$ or $\text{wt}_H(\mathbf{b}) \geq d_z$ if $K > 1$ (for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ such that $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s}$, $\text{wt}_H(\mathbf{a}) \geq d_x$ or $\text{wt}_H(\mathbf{b}) \geq d_z$ if $K = 1$).

Proof. The proof is patterned after the proof of [51, Th. 13]. Suppose that an $((n, K, d_z/d_x))_q$ -stabilizer code Q exists. Then there exists a closed subgroup S of G_n of order $\frac{q^n}{K}$ such that $Q = \text{Fix}(S)$. The group S is abelian and satisfies $S \cap Z(G_n) = \{1\}$, by Lemma 2.2.6. The quotient $\mathcal{C} \cong SZ(G_n)/Z(G_n)$ is an $\mathbb{F}_p$ -linear subset of $\mathbb{F}_q^{2n}$ such that $|\mathcal{C}| = |S| = \frac{q^n}{K}$. We have $\mathcal{C}^{\perp_s} = C_{G_n}(S)/Z(G_n)$ by Lemma 2.2.5. Since S is an abelian group, $SZ(G_n) \leq C_{G_n}(S)$, making $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$.

Recall that for $E = \eta^c X(\mathbf{a})Z(\mathbf{b})$ in G_n , the X -weight $w_X(E) := \text{wt}_H(\mathbf{a})$ and the Z -weight $w_Z(E) := \text{wt}_H(\mathbf{b})$. If $K = 1$, then $\mathcal{Q}$ is a pure quantum code by consensus. Thus, for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ such that $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s}$, $\text{wt}_H(\mathbf{a}) \geq d_x$ or $\text{wt}_H(\mathbf{b}) \geq d_z$.

If $K > 1$, then the elements of $C_{G_n}(S) \setminus SZ(G_n)$ have at least X -weight d_x or Z -weight d_z by Lemma 2.2.7. Hence, for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ such that $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s} \setminus \mathcal{C}$, $\text{wt}_H(\mathbf{a}) \geq d_x$ or $\text{wt}_H(\mathbf{b}) \geq d_z$.

Conversely, suppose that $\mathcal{C}$ is an $\mathbb{F}_p$ -linear subset of $\mathbb{F}_q^{2n}$ such that $|\mathcal{C}| = \frac{q^n}{K}$, $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$ and for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ such that $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s} \setminus \mathcal{C}$, $\text{wt}_H(\mathbf{a}) \geq d_x$ or $\text{wt}_H(\mathbf{b}) \geq d_z$ if $K > 1$ (for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ such that $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s}$, $\text{wt}_H(\mathbf{a}) \geq d_x$ or $\text{wt}_H(\mathbf{b}) \geq d_z$ if $K = 1$). Let

$$N = \{\eta^c X(\mathbf{a})Z(\mathbf{b}) : c \in \mathbb{F}_p \text{ and } (\mathbf{a}|\mathbf{b}) \in \mathcal{C}\}.$$

Note that N is an abelian normal subgroup of G_n , because it is the pre-image of $\mathcal{C} = N/Z(G_n)$. Choose an additive character χ of N such that $\chi(\eta^c \mathbf{1}) = \eta^c$. Then

$$P_N = \frac{1}{|N|} \sum_{E \in N} \chi(E^{-1})E$$

defines an orthogonal projection onto a vector space Q , because P_N is an idempotent in the group ring $\mathbb{C}[G_n]$ (See [54, Th. 1] for further details). We have

$$\dim Q = \text{Trace}(P_N) = |Z(G_n)| \frac{q^n}{|N|} = \frac{q^n}{|\mathcal{C}|} = K.$$

Each coset of N modulo $Z(G_n)$ contains exactly one operator E such that $E|\varphi\rangle = |\varphi\rangle$ for all $|\varphi\rangle$ in Q . Define $S := \{E \in N : E|\varphi\rangle = |\varphi\rangle \text{ for all } |\varphi\rangle \in Q\}$. Then S is an abelian subgroup of G_n of order $|S| = |\mathcal{C}| = \frac{q^n}{K}$. We have $Q = \text{Fix}(S)$, because Q is clearly a subspace of $\text{Fix}(S)$, and $\dim Q = \frac{q^n}{|S|} = K$.

An element $\eta^c X(\mathbf{a})Z(\mathbf{b})$ in $C_{G_n}(S) \setminus SZ(G_n)$ cannot have X -weight less than d_x

and Z -weight less than d_z , because this would imply that there are $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ such that $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s} \setminus \mathcal{C}$ and $\text{wt}_H(\mathbf{a}) < d_x$ and $\text{wt}_H(\mathbf{b}) < d_z$, which is absurd.

Similarly, if $K = 1$, then all nonidentity elements in the centralizer $C_{G_n}(S)$ must have X -weight $\geq d_x$ or Z -weight $\geq d_z$. Hence, Q is an $((n, K, d_z/d_x))_q$ -stabilizer code. $\square$

The code Q is pure if and only if $\text{wt}_X(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = \text{wt}_X(\mathcal{C}^{\perp_s})$ and $\text{wt}_Z(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = \text{wt}_Z(\mathcal{C}^{\perp_s})$.

As a final note, we thank one of the examiners for pointing out the need to define the error group G_n according to the characteristic of $\mathbb{F}_q$.

Chapter 3

The Functional Approach

This chapter forms the most theoretical part of the thesis. The main source is [27, Sect. III] with some additional material taken from [28, Sect. IV].

In this chapter we derive the closure property of an $\mathbb{F}_r$ -linear code C over $\mathbb{F}_q$ under the trace Euclidean inner product and establish the MacWilliams equation for this family of codes. This constitutes Section 3.1.

Section 3.2 accomplishes two important tasks. First, a proof using the functional approach on how to derive pure AQECCs based on nested pairs of $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ under the trace Euclidean inner product is given. Second, we show how this construction is related to other previously known CSS-like constructions.

In Section 3.3, the fact that CSS-like AQECCs constitute a subclass of asymmetric stabilizer codes is shown.

3.1 The Closure Property

Given that $\mathbb{F}_p \subseteq \mathbb{F}_r \subseteq \mathbb{F}_q$, we equip the space $\mathbb{F}_q^n$ with the trace Euclidean inner product.

Lemma 3.1.1. $\langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr}_{q/r} \mathbb{E}}$ is a valid inner product on $\mathbb{F}_q^n$.

Proof. The only property to check is non-degeneracy since everything else follows immediately from $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{E}}$. We show that if $\langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr}_{q/r} \mathbb{E}} = 0$ for all $\mathbf{u} \in \mathbb{F}_q^n$, then $\mathbf{v} = \mathbf{0}$, the converse being trivial.

We prove the contrapositive. That is, if $\mathbf{v} \neq \mathbf{0}$, then there exists a vector $\mathbf{u} \in \mathbb{F}_q^n$ such that $\langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr}_{q/r} \mathbb{E}} \neq 0$. Since the trace mapping is onto, there exists $0 \neq a \in \mathbb{F}_q$ such that $\text{Tr}_{q/r}(a) \neq 0$. Let j be the first index for which $v_j \neq 0$. Define $\mathbf{u} \in \mathbb{F}_q^n$ as follows: $u_j = v_j^{-1}a$ and $u_i = 0$ for all $i \neq j$. This completes the proof. $\square$

With this lemma at hand, the following important result can be established.

Theorem 3.1.2. Let C be an $\mathbb{F}_r$ -linear code over $\mathbb{F}_q$. Then C has the same MacWilliams equation as the one stated in Equation (2.1.2). Explicitly,

$$W_{C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y). \quad (3.1.1)$$

Moreover, C is closed under the trace Euclidean inner product. That is,

$$(C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}})^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} = C.$$

Proof. Let $A(Y) := \sum_0^n A_j Y^j$ and $B(Y) := \sum_0^n B_j Y^j$ be, respectively, the weight enumerators of C and of $C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}$. We first prove the following identity

$$B(Y) = \frac{(1 + (q-1)Y)^n}{|C|} \cdot A\left(\frac{1-Y}{1+(q-1)Y}\right). \quad (3.1.2)$$

Let χ be a nontrivial additive character of $\mathbb{F}_r$. Since C is $\mathbb{F}_r$ -linear, we can define for every $\mathbf{b} \in \mathbb{F}_q^n$ a character $\chi_{\mathbf{b}}$ of the additive group C by substituting the trace Euclidean form for the argument of the character χ , such that

$$\chi_{\mathbf{b}}(\mathbf{c}) = \chi\left(\langle \mathbf{b}, \mathbf{c} \rangle_{\text{Tr}_{q/r} \mathbb{E}}\right) = \chi\left(\sum_{i=1}^n \text{Tr}_{q/r}(b_i c_i)\right) \in \mathbb{C}$$

for all $\mathbf{c} \in C$. Hence, $\chi_{\mathbf{b}}(\mathbf{c} + \mathbf{d}) = \chi\left(\langle \mathbf{b}, \mathbf{c} + \mathbf{d} \rangle_{\text{Tr}_{q/r} \mathbb{E}}\right)$. The character $\chi_{\mathbf{b}}$ is trivial if and only if $\mathbf{b} \in C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}$. Thus, we have the orthogonality relation of characters

$$\sum_{\mathbf{c} \in C} \chi_{\mathbf{b}}(\mathbf{c}) = \begin{cases} |C| & \text{if } \mathbf{b} \in C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} \\ 0 & \text{otherwise} \end{cases}. \quad (3.1.3)$$

By Equation (3.1.3),

$$\begin{aligned} \sum_{\mathbf{c} \in C} \sum_{\mathbf{b} \in \mathbb{F}_q^n} \chi_{\mathbf{b}}(\mathbf{c}) Y^{\text{wt}_{\mathbf{H}}(\mathbf{b})} &= \sum_{\mathbf{b} \in \mathbb{F}_q^n} Y^{\text{wt}_{\mathbf{H}}(\mathbf{b})} \sum_{\mathbf{c} \in C} \chi_{\mathbf{b}}(\mathbf{c}) \\ &= |C| \sum_{i=0}^n B_i Y^i = |C| \cdot B(Y). \end{aligned} \quad (3.1.4)$$

Let us take a closer look at the inner sum on the left hand side of Equation (3.1.4). By the property of the trace mapping, we can distribute the trace mapping over each element.

$$\begin{aligned} \sum_{\mathbf{b} \in \mathbb{F}_q^n} \chi_{\mathbf{b}}(\mathbf{c}) Y^{\text{wt}_{\mathbf{H}}(\mathbf{b})} &= \sum_{(b_1, b_2, \dots, b_n) \in \mathbb{F}_q^n} \left(Y^{\left(\sum_{i=1}^n \text{wt}_{\mathbf{H}}(b_i)\right)} \right) \chi\left(\sum_{i=1}^n \text{Tr}_{q/r}(b_i c_i)\right) \\ &= \sum_{(b_1, b_2, \dots, b_n) \in \mathbb{F}_q^n} \left(\prod_{i=1}^n Y^{\text{wt}_{\mathbf{H}}(b_i)} \cdot \chi\left(\text{Tr}_{q/r}(b_i c_i)\right) \right) \\ &= \prod_{i=1}^n \sum_{b_i \in \mathbb{F}_q} Y^{\text{wt}_{\mathbf{H}}(b_i)} \chi\left(\text{Tr}_{q/r}(b_i c_i)\right). \end{aligned} \quad (3.1.5)$$

Note that if $(c_i, b_i) = (0, 0)$, the contribution to the sum is 1. If $c_i = 0$ but $b_i \neq 0$, the contribution to the sum is $(q-1)Y$. Similarly, for $c_i \neq 0$, if $b_i = 0$, we get 1, while if

$b_i \neq 0$, we get $-Y$. Therefore, the sum in Equation (3.1.5) can be simplified to

$$\sum_{b_i \in \mathbb{F}_q} Y^{\text{wt}_H(b_i)} \chi(\text{Tr}_{q/r}(b_i c_i)) = \begin{cases} 1 + (q-1)Y & \text{if } c_i = 0 \\ 1 - Y & \text{if } c_i \neq 0 \end{cases}, \quad (3.1.6)$$

yielding, after plugging this result back to Equation (3.1.4),

$$\begin{aligned} B(Y) &= \frac{1}{|C|} \sum_{\mathbf{c} \in C} \sum_{\mathbf{b} \in \mathbb{F}_q^n} \chi_{\mathbf{b}}(\mathbf{c}) Y^{\text{wt}_H(\mathbf{b})} \\ &= \frac{1}{|C|} \sum_{\mathbf{c} \in C} (1 + (q-1)Y)^{n - \text{wt}_H(\mathbf{c})} (1 - Y)^{\text{wt}_H(\mathbf{c})} \\ &= \frac{1}{|C|} (1 + (q-1)Y)^n \sum_{\mathbf{c} \in C} \left(\frac{(1-Y)}{1 + (q-1)Y} \right)^{\text{wt}_H(\mathbf{c})} \\ &= \frac{(1 + (q-1)Y)^n}{|C|} \cdot A \left(\frac{(1-Y)}{1 + (q-1)Y} \right). \end{aligned}$$

This establishes Equation (3.1.1).

Observe that the Krawtchouk polynomial of degree j in variable i in Equation (2.1.3) is the coefficient of Y^j in $(1 + (q-1)Y)^{n-i}(1-Y)^i$.

Hence, $B(Y)$ can be expressed as

$$B(Y) = \frac{1}{|C|} \sum_{i=0}^n A_i (1 + (q-1)Y)^{n-i} (1-Y)^i.$$

Comparing the coefficients of Y^j on both sides gives us the claimed MacWilliams equation.

Note that the size of $C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}$ is given by substituting $Y = 1$ in Equation (3.1.2) from whence we have $|C| |C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}| = q^n$. This is sufficient to establish the closure property of C under the trace Euclidean inner product. This brings the proof to conclusion. $\square$

Remark 3.1.3. *The closure property and the MacWilliams equation for an $\mathbb{F}_r$ -linear code C over $\mathbb{F}_q$ under the trace Euclidean inner product can also be deduced from [61, Cor. 3.2.3 on p. 88]. The explicit approach above is preferred so as to eliminate the need for a more sophisticated algebraic build-up in the exposition.*

With the preparatory results in place, we can now proceed to proving the main theorem of this chapter connecting AQECCs and nested pairs of $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$.

3.2 CSS-like Constructions

Recall the following characterization of AQECCs presented in [69].

Theorem 3.2.1. *[69, Th. 3.1]*

1. *There exists an asymmetric quantum code with parameters $((n, K, d_z/d_x))_q$ with $K \geq 2$ if and only if there exist K nonzero mappings*

$$\varphi_i : \mathbb{F}_q^n \rightarrow \mathbb{C} \text{ for } 1 \leq i \leq K \quad (3.2.1)$$

satisfying the following conditions: for each d such that $1 \leq d \leq \min\{d_x, d_z\}$ and partition of $\{1, 2, \dots, n\}$,

$$\left\{ \begin{array}{l} \{1, 2, \dots, n\} = A \cup X \cup Z \cup B \\ |A| = d - 1, \quad |B| = n + d - d_x - d_z + 1 \\ |X| = d_x - d, \quad |Z| = d_z - d \end{array} \right. , \quad (3.2.2)$$

and each $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_q^{|A|}$, $\mathbf{c}_Z \in \mathbb{F}_q^{|Z|}$ and $\mathbf{a}_X \in \mathbb{F}_q^{|X|}$, we have the equality

$$\sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|}, \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_X - \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B) = \begin{cases} 0 & \text{for } i \neq j \\ I(\mathbf{c}_A, \mathbf{c}'_A, \mathbf{c}_Z, \mathbf{a}_X) & \text{for } i = j \end{cases}, \quad (3.2.3)$$

where $I(\mathbf{c}_A, \mathbf{c}'_A, \mathbf{c}_Z, \mathbf{a}_X)$ is an element of $\mathbb{C}$ which is independent of i . The notation $(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)$ represents the rearrangement of the entries of the vector $\mathbf{c} \in \mathbb{F}_q^n$ according to the partition of $\{1, 2, \dots, n\}$ given in Equation (3.2.2).

2. Let (φ_i, φ_j) stand for $\sum_{\mathbf{c} \in \mathbb{F}_q^n} \overline{\varphi_i(\mathbf{c})} \varphi_j(\mathbf{c})$. There exists a pure asymmetric quantum code with parameters $((n, K \geq 1, d_z/d_x))_q$ if and only if there exist K nonzero mappings φ_i as shown in Equation (3.2.1) such that

- φ_i are linearly independent for $1 \leq i \leq K$, i.e., the rank of the $K \times q^n$ matrix $(\varphi_i(\mathbf{c}))_{1 \leq i \leq K, \mathbf{c} \in \mathbb{F}_q^n}$ is K ; and
- for each d with $1 \leq d \leq \min\{d_x, d_z\}$, a partition in Equation (3.2.2) and $\mathbf{c}_A, \mathbf{a}_A \in \mathbb{F}_q^{|A|}$, $\mathbf{c}_Z \in \mathbb{F}_q^{|Z|}$ and $\mathbf{a}_X \in \mathbb{F}_q^{|X|}$, we have the equality

$$\sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|}, \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B) = \begin{cases} 0 & \text{for } (\mathbf{a}_A, \mathbf{a}_X) \neq (\mathbf{0}, \mathbf{0}) \\ \frac{(\varphi_i, \varphi_j)}{q^{d_z-1}} & \text{for } (\mathbf{a}_A, \mathbf{a}_X) = (\mathbf{0}, \mathbf{0}) \end{cases}. \quad (3.2.4)$$

It is important to note that the values d_x and d_z are in fact interchangeable. Physically, such an interchange can be effected by applying the Hadamard transform. One can then always assume $d_z \geq d_x$. This will have a bearing when we perform linear programming to derive upper bounds to evaluate the goodness of an AQECC. The following result is due to Keqin Feng and Long Wang but has never been published formally. We present it here with a proof.

Proposition 3.2.2. (*K. Feng and L. Wang*) *Let a, b be positive integers. There exists an asymmetric quantum code Q with parameters $((n, K, a/b))_q$ if and only if there exists an asymmetric quantum code Q' with parameters $((n, K, b/a))_q$. Q' is pure if and only if Q is pure.*

Proof. We begin by assuming the existence of an $((n, K, a/b))_q$ asymmetric quantum code Q . Let φ_i with $1 \leq i \leq K$ be the K mappings given in Theorem 3.2.1. Define the following K mappings

$$\begin{aligned} \Phi_i : \mathbb{F}_q^n &\rightarrow \mathbb{C} \text{ for } 1 \leq i \leq K \\ \mathbf{v} &\mapsto \sum_{\mathbf{c} \in \mathbb{F}_q^n} \varphi_i(\mathbf{c}) \eta^{T(\mathbf{c} \cdot \mathbf{v})}. \end{aligned} \tag{3.2.5}$$

Let $\mathbf{v}_A, \mathbf{b}_A \in \mathbb{F}_q^{|A|}$, $\mathbf{v}_X \in \mathbb{F}_q^{|X|}$, and $\mathbf{b}_Z \in \mathbb{F}_q^{|Z|}$. For each d such that $1 \leq d \leq \min\{d_x, d_z\}$ and a partition of $\{1, 2, \dots, n\}$ given in Equation (3.2.2), we show that

$$\begin{aligned} S &= \sum_{\substack{\mathbf{v}_Z \in \mathbb{F}_q^{|Z|}, \\ \mathbf{v}_B \in \mathbb{F}_q^{|B|}}} \overline{\Phi_i(\mathbf{v})} \Phi_j(\mathbf{v}_A + \mathbf{b}_A, \mathbf{v}_X, \mathbf{v}_Z + \mathbf{b}_Z, \mathbf{v}_B) \\ &= \begin{cases} 0 & \text{for } i \neq j, \\ I'(\mathbf{v}_A, \mathbf{b}_A, \mathbf{b}_Z, \mathbf{v}_X) & \text{for } i = j, \end{cases} \end{aligned} \tag{3.2.6}$$

where $I'(\mathbf{v}_A, \mathbf{b}_A, \mathbf{b}_Z, \mathbf{v}_X)$ is an element of $\mathbb{C}$ which is independent of i .

Let $\mathbf{t} = (\mathbf{v}_A + \mathbf{b}_A, \mathbf{v}_X, \mathbf{v}_Z + \mathbf{b}_Z, \mathbf{v}_B)$. Applying Equation (3.2.5) yields

$$S = \sum_{\substack{\mathbf{v}_Z \in \mathbb{F}_q^{|Z|} \\ \mathbf{v}_B \in \mathbb{F}_q^{|B|}}} \sum_{\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n} \overline{\varphi_i(\mathbf{c})} \varphi_j(\mathbf{d}) \eta^{T((- \mathbf{c} \cdot \mathbf{v}) + (\mathbf{d} \cdot \mathbf{t}))}. \quad (3.2.7)$$

By carefully rearranging the summations and grouping the terms, we get

$$S = \sum_{\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n} \overline{\varphi_i(\mathbf{c})} \varphi_j(\mathbf{d}) \cdot \kappa \cdot \lambda, \quad (3.2.8)$$

where

$$\begin{aligned} \kappa &= \eta^{T(\mathbf{v}_A \cdot (\mathbf{d}_A - \mathbf{c}_A) + \mathbf{v}_X \cdot (\mathbf{d}_X - \mathbf{c}_X) + \mathbf{d}_A \cdot \mathbf{b}_A + \mathbf{d}_Z \cdot \mathbf{b}_Z)}, \\ \lambda &= \sum_{\substack{\mathbf{v}_Z \in \mathbb{F}_q^{|Z|} \\ \mathbf{v}_B \in \mathbb{F}_q^{|B|}}} \eta^{T(\mathbf{v}_B \cdot (\mathbf{d}_B - \mathbf{c}_B) + \mathbf{v}_Z \cdot (\mathbf{d}_Z - \mathbf{c}_Z))}. \end{aligned}$$

By orthogonality of characters,

$$\lambda = \begin{cases} q^{|Z|+|B|} & \text{if } \mathbf{d}_B = \mathbf{c}_B \text{ and } \mathbf{d}_Z = \mathbf{c}_Z, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$S = \sum_{\substack{\mathbf{c} \in \mathbb{F}_q^n \\ \mathbf{d}_A \in \mathbb{F}_q^{|A|}, \mathbf{d}_X \in \mathbb{F}_q^{|X|}}} q^{|Z|+|B|} \cdot \overline{\varphi_i(\mathbf{c})} \varphi_j(\mathbf{d}_A, \mathbf{d}_X, \mathbf{c}_Z, \mathbf{c}_B) \cdot \pi, \quad (3.2.9)$$

where

$$\pi = \eta^{T(\mathbf{v}_A \cdot (\mathbf{d}_A - \mathbf{c}_A) + \mathbf{v}_X \cdot (\mathbf{d}_X - \mathbf{c}_X) + \mathbf{d}_A \cdot \mathbf{b}_A + \mathbf{c}_Z \cdot \mathbf{b}_Z)}.$$

Now, we let $k = n - d_x + 1$, $\mathbf{a}_A = \mathbf{d}_A - \mathbf{c}_A$, and $\mathbf{a}_X = \mathbf{d}_X - \mathbf{c}_X$. Splitting up the

summation once again yields

$$\begin{aligned}
S = q^k \sum_{\substack{\mathbf{c}_A, \mathbf{a}_A \in \mathbb{F}_q^{|A|} \\ \mathbf{c}_Z \in \mathbb{F}_q^{|Z|}, \mathbf{a}_X \in \mathbb{F}_q^{|X|}}} \eta^{T(\mathbf{v}_A \cdot \mathbf{a}_A + \mathbf{v}_X \cdot \mathbf{a}_X + \mathbf{b}_A \cdot (\mathbf{c}_A + \mathbf{a}_A) + \mathbf{c}_Z \cdot \mathbf{b}_Z)} \\
\cdot \sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|}, \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B). \quad (3.2.10)
\end{aligned}$$

Invoking Equation (3.2.3) concludes the proof for the first part with I' given by

$$I' = q^k I \sum_{\substack{\mathbf{c}_A, \mathbf{a}_A \in \mathbb{F}_q^{|A|} \\ \mathbf{c}_Z \in \mathbb{F}_q^{|Z|}, \mathbf{a}_X \in \mathbb{F}_q^{|X|}}} \eta^{T(\mathbf{v}_A \cdot \mathbf{a}_A + \mathbf{v}_X \cdot \mathbf{a}_X + \mathbf{b}_A \cdot (\mathbf{c}_A + \mathbf{a}_A) + \mathbf{c}_Z \cdot \mathbf{b}_Z)}. \quad (3.2.11)$$

For the second part, let us assume the existence of a pure $((n, K, a/b))_q$ asymmetric quantum code Q . Note that the Fourier transformations Φ_i for $1 \leq i \leq K$ are linearly independent. We use Equations (3.2.10) and (3.2.4) to establish the equality

$$\begin{aligned}
S = \sum_{\substack{\mathbf{v}_Z \in \mathbb{F}_q^{|Z|}, \\ \mathbf{v}_B \in \mathbb{F}_q^{|B|}}} \overline{\Phi_i(\mathbf{v})} \Phi_j(\mathbf{v}_A + \mathbf{b}_A, \mathbf{v}_X, \mathbf{v}_Z + \mathbf{b}_Z, \mathbf{v}_B) \\
= \begin{cases} 0 & \text{for } (\mathbf{b}_A, \mathbf{b}_Z) \neq (\mathbf{0}, \mathbf{0}), \\ q^n \frac{(\varphi_i, \varphi_j)}{q^{d_x-1}} & \text{for } (\mathbf{b}_A, \mathbf{b}_Z) = (\mathbf{0}, \mathbf{0}). \end{cases} \quad (3.2.12)
\end{aligned}$$

Consider the term

$$M := \sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|}, \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i(\mathbf{c})} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B)$$

in Equation (3.2.10). By the purity assumption, for $(\mathbf{a}_A, \mathbf{a}_X) \neq (\mathbf{0}, \mathbf{0})$, $M = 0$. For $(\mathbf{a}_A, \mathbf{a}_X) = (\mathbf{0}, \mathbf{0})$, $M = \frac{(\varphi_i, \varphi_j)}{q^{d_z-1}}$. Hence,

$$S = q^k \sum_{\substack{\mathbf{c}_A \in \mathbb{F}_q^{|A|}, \\ \mathbf{c}_Z \in \mathbb{F}_q^{|Z|}}} \eta^{T(\mathbf{b}_A \cdot \mathbf{c}_A + \mathbf{b}_Z \cdot \mathbf{c}_Z)} \cdot \frac{(\varphi_i, \varphi_j)}{q^{d_z-1}}. \quad (3.2.13)$$

By orthogonality of characters, if $(\mathbf{b}_A, \mathbf{b}_Z) \neq (\mathbf{0}, \mathbf{0})$, then

$$\sum_{\substack{\mathbf{c}_A \in \mathbb{F}_q^{|A|}, \\ \mathbf{c}_Z \in \mathbb{F}_q^{|Z|}}} \eta^{T(\mathbf{b}_A \cdot \mathbf{c}_A + \mathbf{b}_Z \cdot \mathbf{c}_Z)} = 0,$$

making $S = 0$. If $(\mathbf{b}_A, \mathbf{b}_Z) = (\mathbf{0}, \mathbf{0})$, then

$$S = q^k \cdot q^{|A|+|Z|} \cdot \frac{(\varphi_i, \varphi_j)}{q^{d_z-1}}.$$

This completes the proof of the second part. $\square$

The next result is a generalization of a result in [69] as well as in [28].

Theorem 3.2.3. *Let d_x and d_z be positive integers. Let C be an $\mathbb{F}_r$ -linear code over $\mathbb{F}_q$ of length n . Assume that $d^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} = d(C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}})$ is the minimum distance of the dual code $C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}$ of C under the trace Euclidean inner product. For a set $V := \{\mathbf{v}_i : 1 \leq i \leq K\}$ of K distinct vectors in $\mathbb{F}_q^n$, let*

$$d_v := \min \{ \text{wt}_H(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) : 1 \leq i \neq j \leq K, \mathbf{c} \in C \}.$$

If $d^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} \geq d_z$ and $d_v \geq d_x$, then there exists a pure asymmetric quantum code Q with parameters $((n, K, d_z/d_x))_q$.

Proof. The proof is modeled after the proof of [28, Th. 4.4]. Define the following functions

$$\begin{aligned} \varphi_i : \mathbb{F}_q^n &\rightarrow \mathbb{C} \text{ for } 1 \leq i \leq K \\ \mathbf{u} &\mapsto \begin{cases} 1 & \text{if } \mathbf{u} \in \mathbf{v}_i + C \\ 0 & \text{if } \mathbf{u} \notin \mathbf{v}_i + C \end{cases}. \end{aligned} \tag{3.2.14}$$

For each d such that $1 \leq d \leq \min \{d_x, d_z\}$ and a partition of $\{1, 2, \dots, n\}$ given in Equation (3.2.2),

$$\overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B) \neq 0$$

if and only if

$$\begin{cases} (\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B) & \in \mathbf{v}_i + C \\ (\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B) & \in \mathbf{v}_j + C \end{cases},$$

which, in turn, is equivalent to

$$\begin{cases} (\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B) & \in \mathbf{v}_i + C \\ (\mathbf{a}_A, \mathbf{a}_X, \mathbf{0}_Z, \mathbf{0}_B) & \in \mathbf{v}_j - \mathbf{v}_i + C \end{cases}. \quad (3.2.15)$$

Note that since $\text{wt}_H(\mathbf{a}_A, \mathbf{a}_X, \mathbf{0}_Z, \mathbf{0}_B) \leq |A| + |X| = d_x - 1$, we know that $(\mathbf{a}_A, \mathbf{a}_X, \mathbf{0}_Z, \mathbf{0}_B) \in \mathbf{v}_j - \mathbf{v}_i + C$ means $i = j$ by the definition of d_v above. Thus, if $i \neq j$,

$$\sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|} \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)} \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B) = 0. \quad (3.2.16)$$

Now, consider the case of $i = j$. By Equation (3.2.15), if $(\mathbf{a}_A, \mathbf{a}_X, \mathbf{0}_Z, \mathbf{0}_B) \notin C$, then it has no contribution to the sum we are interested in.

If $(\mathbf{a}_A, \mathbf{a}_X, \mathbf{0}_Z, \mathbf{0}_B) \in C$, then

$$\sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|} \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)} \varphi_i(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B) = \sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|}, \mathbf{c}_B \in \mathbb{F}_q^{|B|} \\ (\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B) \in \mathbf{v}_i + C}} 1. \quad (3.2.17)$$

Proposition 2.1.5 tells us that, if C is any $\mathbb{F}_r$ -linear classical q -ary code of length n and size M such that the minimum distance of its dual is greater than or equal to d_z , then any coset of C is an orthogonal array of level q and of strength exactly $d_z - 1$.

In other words, there are exactly $\frac{|C|}{q^{d_z-1}}$ vectors $(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B) \in \mathbf{v}_i + C$ for any fixed $(\mathbf{c}_A, \mathbf{c}_Z) \in \mathbb{F}_q^{d_z-1}$. Thus, for $i = j$, the sum on the right hand side of Equation (3.2.17) is $\frac{|C|}{q^{d_z-1}}$, which is independent of i . By Part 1 of Theorem 3.2.1 we have an asymmetric quantum code Q with parameters $((n, K, d_z/d_x))_q$. Part 2 of Theorem 3.2.1 ascertains the purity of the resulting code. $\square$

Theorem 3.2.4. *For $i = 1, 2$, let C_i be an $\mathbb{F}_r$ -linear code with parameters $(n, K_i, d_i)_q$. If $C_1^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} \subseteq C_2$, then there exists an asymmetric quantum code Q with parameters $\left(\left(n, \frac{K_1 \cdot K_2}{q^n}, d_z/d_x\right)\right)_q = [[n, \log_q K_1 + \log_q K_2 - n, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{d_1, d_2\}$.*

Proof. We take $C = C_1^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}$ in Theorem 3.2.3 above. Since $C_1^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} \subseteq C_2$, we have $C_2 = C_1^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} \oplus C'$, where C' is an $\mathbb{F}_r$ -submodule of C_2 and $\oplus$ is the direct sum so that $|C'| = \frac{|C_2|}{|C_1^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}|}$. Let $C' = \{\mathbf{v}_1, \dots, \mathbf{v}_K\}$, where $K = \frac{|C_2|}{|C_1^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}|} = \frac{K_1 \cdot K_2}{q^n}$ by Theorem 3.1.2. Then

$$d^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} = d(C^{\perp_{\text{Tr}_{q/r} \mathbb{E}}}) = d(C_1) = d_1 \text{ and}$$

$$\begin{aligned} d_v &= \min \{ \text{wt}_H(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) : 1 \leq i \neq j \leq K, \mathbf{c} \in C \} \\ &= \min \left\{ \text{wt}_H(\mathbf{v} + \mathbf{c}) : \mathbf{0} \neq \mathbf{v} \in C', \mathbf{c} \in C_1^{\perp_{\text{Tr}_{q/r} \mathbb{E}}} \right\} \geq d_2. \end{aligned}$$

$\square$

The usage of orthogonal arrays in the proof of Theorem 3.2.3 above allows us to construct AQECCs by applying the CSS method on a pair of nested codes while widening the choice of inner products that we can utilise and removing the requirement of $\mathbb{F}_q$ -linearity. In fact, any valid bilinear form can be used to set up the inner product.

The standard CSS construction for pure asymmetric q -ary quantum codes employs the pair $C_1^{\perp_E} \subseteq C_2$ with both C_1 and C_2 being $\mathbb{F}_q$ -linear codes of length n . Another proof for this construction using the functional approach is given in [69, Th. 3.3]. In the case of $q = r^2$, we can interchange the Euclidean and Hermitian inner products in the statement of the theorem.

In fact, the standard CSS construction also follows immediately from Theorem 3.2.4 and the fact that the trace Euclidean inner product is just the Euclidean inner product when the codes involved are $\mathbb{F}_q$ -linear.

Let $\mathbb{F}_q$ be a quadratic extension of $\mathbb{F}_r$. Let the codes in the nested pair be $\mathbb{F}_r$ -linear codes in $\mathbb{F}_q^n$. Under the trace Hermitian inner product, we can derive AQECCs according to [28, Th. 4.5].

In summary, the standard CSS construction for pure AQECCs can be extended to include the constructions of pure AQECCs from nested pairs of classical codes under the Hermitian, trace Hermitian, and trace Euclidean inner products. We call all of the above constructions *CSS-like*. More formally, we have the following definition.

Definition 3.2.5. (*CSS-like Constructions of Pure AQECCs based on the Functional Approach*). Let $*$ be any one of the Euclidean, trace Euclidean, Hermitian, and trace Hermitian inner products. We call a pure AQECC Q of parameters $((n, K, d_z/d_x))$ a *CSS-like code* if Q is constructed from a nested pair of subfield linear codes $C_1^{\perp_*} \subset C_2$ of equal length n such that $K = \frac{|C_2|}{|C_1^{\perp_*}|}$ and $\{d_z, d_x\} = \{d(C_1), d(C_2)\}$.

To show the generality of Theorem 3.2.4, we show how to derive [28, Th. 4.5] when $q = r^2$ from it. That is, given a nested pair $C_1^{\perp_{\text{Tr}_{q/r^E}}} \subseteq C_2$ of codes yielding a quantum code of parameters $((n, K, d_z/d_x))_q$ we construct a nested pair $D_1^{\perp_{\text{Tr}_H}} \subseteq D_2$

of codes yielding a quantum code of equal parameters and vice versa. To do so, some preparatory lemmas are needed.

Lemma 3.2.6. [26, Lem. 2.5] *Let $q = r^2$. If a code C is $\mathbb{F}_q$ -linear of length n over $\mathbb{F}_q$, then $C^{\perp_H} = C^{\perp_{\text{Tr } H}}$.*

Recall that $\text{Tr } E$ stands for $\text{Tr}_{q/p} E$.

Lemma 3.2.7. *If C is an $\mathbb{F}_r$ -linear code of length n over $\mathbb{F}_q$, then $C^{\perp_{\text{Tr } E}} = C^{\perp_{\text{Tr}_{q/r} E}}$.*

Proof. Clearly, $C^{\perp_{\text{Tr}_{q/r} E}} \subseteq C^{\perp_{\text{Tr } E}}$ by transitivity of the trace mapping. Since, by Theorem 3.1.2, $|C^{\perp_{\text{Tr}_{q/r} E}}| = \frac{q^n}{|C|} = |C^{\perp_{\text{Tr } E}}|$, the result follows. $\square$

Lemma 3.2.8. *Suppose that $q = r^2$ is odd. Let C_1 and C_2 be $\mathbb{F}_r$ -linear codes of length n over $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_q \setminus \{0\}$ such that $\bar{\alpha} = -\alpha$, the following statements hold:*

- i) *If $C_1^{\perp_{\text{Tr } E}} \subseteq C_2$, then $\alpha^{-1} \overline{C_1^{\perp_{\text{Tr } E}}} \subseteq \left(C_2^{\perp_{\text{Tr } E}}\right)^{\perp_{\text{Tr } H}}$.*
- ii) *If $C_1^{\perp_{\text{Tr } H}} \subseteq C_2$, then $\alpha \overline{C_1^{\perp_{\text{Tr } H}}} \subseteq \left(C_2^{\perp_{\text{Tr } H}}\right)^{\perp_{\text{Tr } E}}$.*

Proof. Let $\mathbf{u} \in C_1^{\perp_{\text{Tr } E}}$ and $\mathbf{v} \in C_2^{\perp_{\text{Tr } E}}$. By Lemma 3.2.7,

$$0 = \langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr}_{q/r} E} = \langle \mathbf{u}, \mathbf{v} \rangle_E + \overline{\langle \mathbf{u}, \mathbf{v} \rangle_E}.$$

Therefore,

$$\langle \alpha^{-1} \bar{\mathbf{u}}, \mathbf{v} \rangle_{\text{Tr } H} = \alpha \langle \alpha^{-1} \bar{\mathbf{u}}, \mathbf{v} \rangle_H + \overline{\alpha \langle \alpha^{-1} \bar{\mathbf{u}}, \mathbf{v} \rangle_H} = \overline{\langle \mathbf{u}, \mathbf{v} \rangle_E} + \langle \mathbf{u}, \mathbf{v} \rangle_E = 0.$$

Hence, $\alpha^{-1} \overline{C_1^{\perp_{\text{Tr } E}}} \subseteq \left(C_2^{\perp_{\text{Tr } E}}\right)^{\perp_{\text{Tr } H}}$. This proves i).

To prove ii), let $\mathbf{u} \in C_1^{\perp_{\text{Tr } H}}$ and $\mathbf{v} \in C_2^{\perp_{\text{Tr } H}}$. Then

$$0 = \langle \mathbf{u}, \mathbf{v} \rangle_{\text{Tr } H} = \alpha \langle \mathbf{u}, \bar{\mathbf{v}} \rangle_E + \bar{\alpha} \langle \bar{\mathbf{u}}, \mathbf{v} \rangle_E.$$

By Lemma 3.2.7, it suffices to show that $\alpha \overline{C_1^{\perp_{\text{Tr H}}}} \subseteq \left(C_2^{\perp_{\text{Tr H}}}\right)^{\perp_{\text{Tr}_{q/r} \text{ E}}}$. Note that

$$\begin{aligned} \langle \alpha \bar{\mathbf{u}}, \mathbf{v} \rangle_{\text{Tr}_{q/r} \text{ E}} &= \langle \alpha \bar{\mathbf{u}}, \mathbf{v} \rangle_{\text{E}} + \langle \bar{\alpha} \mathbf{u}, \bar{\mathbf{v}} \rangle_{\text{E}} = \alpha \langle \bar{\mathbf{u}}, \mathbf{v} \rangle_{\text{E}} + \bar{\alpha} \langle \mathbf{u}, \bar{\mathbf{v}} \rangle_{\text{E}} \\ &= -(\bar{\alpha} \langle \bar{\mathbf{u}}, \mathbf{v} \rangle_{\text{E}} + \alpha \langle \mathbf{u}, \bar{\mathbf{v}} \rangle_{\text{E}}) = 0, \end{aligned}$$

since $\bar{\alpha} = -\alpha$. Therefore, $\alpha \overline{C_1^{\perp_{\text{Tr H}}}} \subseteq \left(C_2^{\perp_{\text{Tr H}}}\right)^{\perp_{\text{Tr E}}}$. $\square$

Lemma 3.2.9. *Suppose that $q = r^2$ is even. Let C_1 and C_2 be $\mathbb{F}_r$ -linear codes of length n over $\mathbb{F}_q$. Then the following statements hold:*

- i) *If $C_1^{\perp_{\text{Tr E}}} \subseteq C_2$, then $\overline{C_1^{\perp_{\text{Tr E}}}} \subseteq \left(C_2^{\perp_{\text{Tr E}}}\right)^{\perp_{\text{Tr H}}}$.*
- ii) *If $C_1^{\perp_{\text{Tr H}}} \subseteq C_2$, then $\overline{C_1^{\perp_{\text{Tr H}}}} \subseteq \left(C_2^{\perp_{\text{Tr H}}}\right)^{\perp_{\text{Tr E}}}$.*

Proof. The proof follows from the proof of Lemma 3.2.8 by setting $\alpha = 1$. $\square$

Theorem 3.2.10. *Let $q = r^2$. Then an $((n, K, d_z/d_x))_q$ -CSS-like quantum code with respect to the trace Euclidean inner product exists if and only if there exists an $((n, K, d_z/d_x))_q$ -CSS-like quantum code with respect to the trace Hermitian inner product.*

Proof. Assume there exists a pair of $\mathbb{F}_r$ -linear codes C_1 and C_2 of length n over $\mathbb{F}_q$ such that $C_1^{\perp_{\text{Tr}_{q/r} \text{ E}}} \subseteq C_2$ with $\frac{|C_2|}{|C_1^{\perp_{\text{Tr}_{q/r} \text{ E}}}|} = K$ and $\{d_z, d_x\} = \{d_1, d_2\}$.

Case 1. If q is odd, then by Lemmas 3.2.7 and 3.2.8 i), we have

$$\alpha^{-1} \overline{C_1^{\perp_{\text{Tr E}}}} \subseteq \left(C_2^{\perp_{\text{Tr E}}}\right)^{\perp_{\text{Tr H}}}$$

with

$$K = \frac{|C_2|}{|C_1^{\perp_{\text{Tr}_{q/r} \text{ E}}}|} = \frac{\left|\left(C_2^{\perp_{\text{Tr E}}}\right)^{\perp_{\text{Tr H}}}\right|}{\left|\alpha^{-1} \overline{C_1^{\perp_{\text{Tr E}}}}\right|},$$

$d\left(\left(C_2^{\perp_{\text{Tr E}}}\right)^{\perp_{\text{Tr H}}}\right) = d_2$ and $d\left(\alpha^{-1}\overline{C_1^{\perp_{\text{Tr E}}}}\right) = d_1$. The conclusion follows from [28, Th. 4.5].

Case 2. If q is even, then the proof is similar to that of Case 1 with $\alpha = 1$ and using Lemma 3.2.9 i) instead of Lemma 3.2.8 i).

Conversely, assume that there exists a pair of $\mathbb{F}_r$ -linear codes C_1 and C_2 of length n over $\mathbb{F}_q$ such that $C_1^{\perp_{\text{Tr H}}} \subseteq C_2$ with $\frac{|C_2|}{|C_1^{\perp_{\text{Tr H}}}|} = K$ and $\{d_z, d_x\} = \{d_1, d_2\}$.

Case 1. If q is odd, then by Lemmas 3.2.7 and 3.2.8 ii), we have

$$\overline{\alpha C_1^{\perp_{\text{Tr H}}}} \subseteq \left(C_2^{\perp_{\text{Tr H}}}\right)^{\perp_{\text{Tr}_{q/r} \text{ E}}}$$

with

$$K = \frac{|C_2|}{|C_1^{\perp_{\text{Tr H}}}|} = \frac{\left|\left(C_2^{\perp_{\text{Tr H}}}\right)^{\perp_{\text{Tr}_{q/r} \text{ E}}}\right|}{\left|\overline{\alpha C_1^{\perp_{\text{Tr H}}}}\right|},$$

$d\left(\left(C_2^{\perp_{\text{Tr H}}}\right)^{\perp_{\text{Tr}_{q/r} \text{ E}}}\right) = d_2$ and $d\left(\overline{\alpha C_1^{\perp_{\text{Tr H}}}}\right) = d_1$. The conclusion follows from Theorem 3.2.4.

Case 2. If q is even, then the proof is similar to that of Case 1 with $\alpha = 1$ and using Lemma 3.2.9 ii) instead of Lemma 3.2.8 ii).

□

If, in Theorem 3.2.10, the codes in the nested pairs are $\mathbb{F}_q$ -linear, then we get the derivation of asymmetric quantum codes based on the CSS-like construction under the Hermitian inner product.

Applying a suitable CSS-like construction to the pair $C \subseteq C^{\perp*}$ gives us the following proposition.

Proposition 3.2.11. *Let C be a self-orthogonal $(n, |C|, d)_q$ -code. Then there exists an AQECC Q with parameters $[[n, n - 2 \log_q(|C|), d^{\perp*}/d^{\perp*}]]_q$.*

The relationships among different CSS-like constructions can be seen in the following diagram

3.3 CSS-like is a Subset of Stabilizer

In this section, we prove Theorem 3.3.1 which states that the existence of a CSS-like code implies the existence of a pure stabilizer code.

Theorem 3.3.1. *A pure $((n, K, d_z/d_x))_q$ -stabilizer code exists if there exists an $((n, K, d_z/d_x))_q$ -CSS-like code.*

Proof. Assume that there is an $((n, K, d_z/d_x))_q$ -quantum code Q derived from a CSS-like construction with $C_1^{\perp*} \subseteq C_2$ and $*$ a suitable inner product. We consider the following cases according to the types of the nested pair of codes and the inner products concerned.

Case 1. Let $C_1^{\perp_E} \subseteq C_2$ with C_i an $\mathbb{F}_q$ -linear code of parameters $[n, k_i, d_i]_q$ for $i = 1, 2$.

Define

$$\mathcal{C} := \{(\mathbf{u}|\mathbf{v}) : \mathbf{u} \in C_1^{\perp_E}, \mathbf{v} \in C_2^{\perp_E}\}.$$

It is easy to see that $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$.

Case 2. Let $q = r^2$, $C_1^{\perp_H} \subseteq C_2$ with C_i an $\mathbb{F}_q$ -linear code of parameters $[n, k_i, d_i]_q$ for $i = 1, 2$. Define

$$\mathcal{C} := \{(\mathbf{u}|\overline{\mathbf{v}}) : \mathbf{u} \in C_1^{\perp_H}, \mathbf{v} \in C_2^{\perp_H}\}.$$

Note that $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$ since, for $\mathbf{u}, \mathbf{u}' \in C_1^{\perp_H}$ and $\mathbf{v}, \mathbf{v}' \in C_2^{\perp_H}$,

$$\langle \mathbf{u}, \overline{\mathbf{v}'} \rangle_E - \langle \mathbf{u}', \overline{\mathbf{v}} \rangle_E = \langle \mathbf{u}, \mathbf{v}' \rangle_H - \langle \mathbf{u}', \mathbf{v} \rangle_H = 0.$$

Case 3. Let $q = r^2$ be even, $C_1^{\perp_{\text{Tr } H}} \subseteq C_2$ with C_i an $\mathbb{F}_r$ -linear code of parameters $(n, r^{k_i}, d_i)_q$ for $i = 1, 2$. Define

$$\mathcal{C} := \{(\mathbf{u}|\overline{\mathbf{v}}) : \mathbf{u} \in C_1^{\perp_{\text{Tr } H}}, \mathbf{v} \in C_2^{\perp_{\text{Tr } H}}\}.$$

To show $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$, it suffices to verify that, for $\mathbf{u}, \mathbf{u}' \in C_1^{\perp_{\text{Tr } H}}$ and $\mathbf{v}, \mathbf{v}' \in C_2^{\perp_{\text{Tr } H}}$,

$$\langle \mathbf{u}, \overline{\mathbf{v}'} \rangle_{\text{Tr}_{q/r} E} - \langle \mathbf{u}', \overline{\mathbf{v}} \rangle_{\text{Tr}_{q/r} E} = \langle \mathbf{u}, \mathbf{v}' \rangle_{\text{Tr } H} - \langle \mathbf{u}', \mathbf{v} \rangle_{\text{Tr } H} = 0.$$

Case 4. Let $q = r^2$ be odd, $\alpha \in \mathbb{F}_q \setminus \{0\}$ such that $\overline{\alpha} = -\alpha$. Let $C_1^{\perp_{\text{Tr } H}} \subseteq C_2$ with C_i an $\mathbb{F}_r$ -linear code of parameters $(n, r^{k_i}, d_i)_q$ for $i = 1, 2$. Define

$$\mathcal{C} := \{(\alpha^{-1}\mathbf{u}|\overline{\mathbf{v}}) : \mathbf{u} \in C_1^{\perp_{\text{Tr } H}}, \mathbf{v} \in C_2^{\perp_{\text{Tr } H}}\}.$$

To show $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$, we compute, for $\mathbf{u}, \mathbf{u}' \in C_1^{\perp_{\text{Tr } H}}$ and $\mathbf{v}, \mathbf{v}' \in C_2^{\perp_{\text{Tr } H}}$,

$$\langle \alpha^{-1}\mathbf{u}, \overline{\mathbf{v}'} \rangle_{\text{Tr}_{q/r} E} - \langle \alpha^{-1}\mathbf{u}', \overline{\mathbf{v}} \rangle_{\text{Tr}_{q/r} E} = \langle \mathbf{u}, \mathbf{v}' \rangle_{\text{Tr } H} - \langle \mathbf{u}', \mathbf{v} \rangle_{\text{Tr } H} = 0.$$

Case 5. Let $C_1^{\perp_{\text{Tr } E}} \subseteq C_2$ with C_i an $\mathbb{F}_p$ -linear code of parameters $(n, p^{k_i}, d_i)_q$ for $i = 1, 2$. Define

$$\mathcal{C} := \{\mathbf{u}|\mathbf{v} : \mathbf{u} \in C_1^{\perp_{\text{Tr } E}}, \mathbf{v} \in C_2^{\perp_{\text{Tr } E}}\}.$$

It follows immediately that $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$.

In all of the above cases, $K = \frac{|C_2|}{|C_1^{\perp*}|}$. Moreover, since our CSS-like code is pure,

$$\text{wt}_H(C_1 \setminus C_2^{\perp*}) = d(C_1) \geq d_z \text{ and } \text{wt}_H(C_2 \setminus C_1^{\perp*}) = d(C_2) \geq d_x.$$

Since $\text{wt}_X(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = \text{wt}_X(\mathcal{C}^{\perp_s})$ and $\text{wt}_Z(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = \text{wt}_Z(\mathcal{C}^{\perp_s})$, the purity condition holds. Thus, all the conditions stipulated in Theorem 2.2.8 are satisfied. The proof is complete. $\square$

For classical codes of parameters $(n, M, d)_q$, the Singleton bound states that $M \leq q^{n-d+1}$, and a code achieving equality is called a *maximum distance separable* (MDS) code.

In [65], the quantum version of the Singleton bound for an $((n, K, d_z/d_x))_q$ -code is given by

$$K \leq q^{n-d_x-d_z+2}. \quad (3.3.1)$$

An asymmetric quantum code Q is said to be MDS if it attains the equality of the bound. This bound is believed to hold for all asymmetric quantum codes.

For CSS-like AQECCs, we can derive the following result.

Proposition 3.3.2. *Any CSS-like asymmetric code satisfies the quantum Singleton bound. Moreover, assuming the validity of the MDS Conjecture, every non-trivial q -ary pure asymmetric quantum MDS code has length $\leq q+1$ if q is odd and $\leq q+2$ if q is even.*

Proof. To show the first assertion, suppose that Q is constructed from the nested pair $C_1^{\perp*} \subseteq C_2$ where C_i is of parameters $(n, M_i, d_i)_q$ for $i = 1, 2$.

By the classical Singleton bound, we have $M_i \leq q^{n-d_i+1}$. Hence,

$$K = \frac{M_2 M_1}{q^n} \leq \frac{q^{(n-d_2+1)+(n-d_1+1)}}{q^n} = q^{n-d_x-d_z+2}.$$

It is known from [69, Cor. 2.5] that Q is MDS if and only if both C_1 and C_2 are (classical) MDS codes. The second assertion then follows from the assumption of the validity of the MDS conjecture on C_i . When $q = p$, this assumption is no longer needed [5]. $\square$

Based on the established results in this chapter, we can rule out the existence of some CSS-like codes with specified parameters. The following example provides a partial answer to a question raised in [65, p. 1652].

Example 3.3.3. *A pure $[[12, 1, 5/3]]_2$ -CSS code does not exist.*

Proof. For a contradiction, assume that such a code exists. Then we have a pair of binary classical codes C_1 with parameters $[12, k_1, d_1]_2$ and C_2 with parameters $[12, k_2, d_2]_2$, such that $C_1^{\perp_E} \subset C_2$ with $k_1 + k_2 - 12 = 1$ and $\{d_1, d_2\} = \{3, 5\}$.

Case 1: $d_1 = 3$ and $d_2 = 5$: From [35], $2 \leq k_2 \leq 4$. This forces $9 \leq k_1 \leq 11$. However, for $[12, k_1]_2$ with $9 \leq k_1 \leq 11$, $d_1 \leq 2 < 3$.

Case 2: $d_1 = 5$ and $d_2 = 3$: From [35], $2 \leq k_2 \leq 8$. This forces $5 \leq k_1 \leq 11$. However, for $[12, k_1]_2$ with $5 \leq k_1 \leq 11$, $d_1 \leq 4 < 5$. $\square$

Chapter 4

The Weights in Classical MDS Codes

When constructing AQECCs, it is important to know what we are aiming at in terms of parameters. In this chapter and the next one we discuss the class of asymmetric quantum MDS (AQMDS) codes, which are among the best possible quantum codes.

Before proceeding to the construction of AQMDS codes using the standard CSS method, we discuss the weights in classical MDS codes in details in this chapter. In the next chapter we use what we learn here to explicitly construct AQMDS codes. The content of this chapter is taken from [25].

As we know, for classical MDS codes we can restrict our attention to the $\mathbb{F}_q$ -linear case only since there is no apparent gain from considering non $\mathbb{F}_q$ -linear classical MDS codes. Up to some explicit exceptional cases, the MDS codes with parameters given by the MDS conjecture are shown to contain all k weights in the range $n - k + 1$ to n . The proof uses the covering radius of the dual code.

This chapter is organized as follows. After some necessary definitions and notation, we dispose of the trivial codes. Section 4.3 studies codes with $n \leq q$. Section 4.4 and Section 4.5 study codes of lengths $q + 1$ and $q + 2$, respectively. At the end, conclusions and an alternative approach to proving some of the results are presented.

4.1 Motivations to Study the Weights

One of the main properties of a linear error-correcting code is its minimum distance since this determines the maximal number of errors that can be corrected independently of the position of the errors. More information about the error-correcting properties of a code can be derived from its weight distribution.

In some cases, one does not need to know the number of codewords of a given weight, but only the set of weights of the codewords. Assmus and Mattson [4] established a connection between codes and designs based on the non-zero weights in the codes. Hill and Lizak [45, 46] derived conditions on the non-zero weights that imply that a code can be extended. Rains [62] showed that a (symmetric) quantum code of length $n' < n$ can be derived from a quantum code of length n if an auxiliary code contains a word of weight n' . Using this result, Rötteler *et al.* [36, 63] constructed quantum MDS codes for all lengths $n \leq q + 1$. The construction relies on the following statement which can be found in [60, p. 320] without an explicit proof:

$$\begin{aligned} &\text{An MDS code with parameters } [n, k, d]_q \text{ has} \\ &k \text{ distinct nonzero weights, } n - k + 1, \dots, n. \end{aligned} \tag{4.1.1}$$

We first show that this statement is not true in general and investigate for which parameters of MDS codes it holds.

Recall that, given an $[n, k, d]_q$ -code, the Singleton bound states that $d \leq n - k + 1$, and C is MDS if it satisfies the equality in this bound. Trivial families of linear MDS codes are the full vector space $[n, n, 1]_q$, codes equivalent to the repetition codes $[n, 1, n]_q$ of any length, and their duals $[n, n - 1, 2]_q$. MDS codes other than these are said to be *nontrivial MDS codes*.

Conjecture 4.1.1. (*MDS Conjecture*) [48, Chapter 7.4, p. 265] *If there is a nontrivial $[n, k, d]_q$ MDS code, then $n \leq q + 1$, except when q is even and $k = 3$ or $k = q - 1$ in which case $n \leq q + 2$.*

Recently, in [5] Simeon Ball shows the validity of the MDS conjecture for $q = p$.

The weight enumerator of an MDS code is unique. It is given by $A_0 = 1$, $A_w = 0$ for $0 < w < d$, and

$$\begin{aligned} A_w &= \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} (q^{w-d+1-j} - 1) \\ &= \binom{n}{w} (q-1) \sum_{j=0}^{w-d} (-1)^j \binom{w-1}{j} q^{w-d-j}, \end{aligned} \quad (4.1.2)$$

for $d \leq w \leq n$ (see [60, Ch. 11, §3, Theorem 6]).

While this formula allows us to compute the weight enumerator of any MDS code, it is not obvious for which weights w there is a codeword of weight w in the code C , that is, $A_w > 0$.

4.2 Trivial MDS Codes

Statement (4.1.1) is clearly true for the trivial MDS codes with parameters $[n, 1, n]_q$ and $[n, n, 1]_q$ over any field $\mathbb{F}_q$. For the dual of the repetition code, we have the first counterexample.

Theorem 4.2.1. *The code with parameters $[n, n-1, 2]_q$ contains words of all weights $2, \dots, n$ if and only if $q > 2$ or $n = 2$.*

Proof. The dual of the binary repetition code of length n is an even weight code with parameters $[n, n-1, 2]_2$. It contains only words of even weight, so statement (4.1.1) is false for $q = 2$ and $n > 2$.

Now let $q > 2$. The codewords of the code C with parameters $[n, n-1, 2]_q$ are exactly those vectors for which the sum of the coefficients is zero. We prove by induction that C contains vectors of all weights $w = 2, \dots, n$. For $w = 2$, the code contains the vector $\mathbf{v}^{(2)} = (1, -1, 0, 0, \dots, 0)$. Now assume that there exists a vector $\mathbf{v}^{(w)} \in C$ with $\text{wt}_H(\mathbf{v}^{(w)}) = w < n$. Without loss of generality, let the first w coordinates of $\mathbf{v}^{(w)}$ be non-zero. We construct a vector $\mathbf{v}^{(w+1)} \in C$ with $\text{wt}_H(\mathbf{v}^{(w+1)}) = w+1$ as follows. Replace the non-zero element $v_w^{(w)}$ by a different non-zero element of $\mathbb{F}_q$ to obtain a vector $\mathbf{x}$ with $\sum_i x_i = s \neq 0$. Next, replace $\mathbf{x}_{w+1} = 0$ by $-s$. The resulting vector is the desired new codeword $\mathbf{v}^{(w+1)}$. $\square$

4.3 MDS Codes of Length $n \leq q$

In this section we show that statement (4.1.1) is true for all MDS codes of length $n \leq q$. The main tool is a relation, due to Delsarte [22], between the external distance s' of a code and the covering radius which we define first.

Definition 4.3.1 (Covering radius). *The covering radius $\rho(C)$ of a linear code with parameters $[n, k, d]_q$ is the maximal distance of any vector in $\mathbb{F}_q^n$ to the code C , i. e.*

$$\rho(C) = \max_{\mathbf{v} \in \mathbb{F}_q^n} \min_{\mathbf{c} \in C} d(\mathbf{v}, \mathbf{c}).$$

Definition 4.3.2 (External distance). *The external distance s' of a linear code with parameters $[n, k, d]_q$ is the number of non-zero weights in the dual code $C' = C^\perp$, i. e.*

$$s' = |\{i: i = 1, \dots, n | B_i \neq 0\}|,$$

where B_i denotes the number of codewords of weight i in the dual code $C^\perp$. The dual code $C^\perp$ is given by

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n: \mathbf{v} \cdot \mathbf{c} = \sum_{i=1}^n v_i c_i = 0 \ \forall \mathbf{c} \in C\}.$$

Theorem 4.3.3 (External distance bound [22, Theorem 3.3]).

For a code with parameters $[n, k, d]_q$ with external distance s' , every vector in $\mathbb{F}_q^n$ is at distance less than or equal to s' from at least one codeword. Hence, for the covering radius $\rho(C)$, we have $\rho(C) \leq s'$.

This implies that statement (4.1.1) holds for codes C for which the covering radius $\rho(C^\perp)$ of the dual code $C^\perp$ is at least k . Then by Theorem 4.3.3, the number s of nonzero weights in C is at least $s \geq k$. Trivially, we have $s \leq n - d + 1$ and therefore $s \leq k$ for MDS codes.

Furthermore, we use the following “supercode lemma” which can, *e. g.*, be found in [18, Lemma 8.2.1].

Lemma 4.3.4. *Let $C_0 \subset C$ and $D(C_0, C)$ be the maximum distance of a vector in C to C_0 . Then $\rho(C_0) \geq D(C_0, C)$. In particular, $\rho(C_0) \geq d(C)$.*

With this preparation, we are ready to prove the following.

Theorem 4.3.5. *Any MDS code with parameters $[n, k, d]_q$ of length $n \leq q$ has k nonzero weights.*

Proof. Trivially, a code with minimum distance $n - k + 1$ can have at most k non-zero weights. The extended narrow-sense Reed-Solomon (RS) codes with parameters $[q, k, q - k + 1]_q$ form a sequence of nested MDS codes [48, Theorem 5.3.2]. Shortening these codes, we obtain sequences of nested MDS codes $C_{n,k} = [n, k, n - k + 1]_q$ with $C_{n,k} \subset C_{n,k+1}$ for any length $n \leq q$. For the dual codes we have $C_{n,k}^\perp = [n, n - k, k + 1]_q \subset C_{n,k-1}^\perp = [n, n - k + 1, k]_q$. By Lemma 4.3.4 the code $C_{n,k}^\perp$ has covering radius $\rho(C_{n,k}^\perp) \geq k$. Using Theorem 4.3.3, it follows that $s \geq k$, i. e., the code C has at least k non-zero weights. Recall that the weight distribution of an MDS code with parameters $[n, k, d]_q$ is uniquely determined by its parameters. Hence the result does not only hold for the MDS codes derived from extended RS codes, but for all MDS codes. $\square$

Remark 4.3.6. *The covering radius of extended RS codes is also given in [18, Theorem 10.5.7]. The lower bound on the covering radius of MDS codes of length $n \leq q$ can also be found in [32].*

4.4 MDS Codes of Length $q + 1$

In [32, Theorem 2] it has been shown that the covering radius of some MDS codes with parameters $[q + 1, k, d]_q$ is $\rho(C) = d - 2$. In this case, Theorem 4.3.3 only implies that there are at least $k - 1$ non-zero weights, and there is indeed a family of MDS codes of length $q + 1$ for which statement (4.1.1) is false, namely the simplex codes with parameters $[q + 1, 2, q]_q$ over $\mathbb{F}_q$ which contain only words of weight zero or q (see, e. g., [48, Theorem 2.7.5]).

Furthermore, if $\rho(C) = d - 2$, we can not have a sequence of nested MDS codes

of length $q + 1$ with co-dimension one. However, there are sequences of nested MDS codes with co-dimension two. For this, we recall the explicit construction of MDS codes of length $q + 1$ as cyclic or consta-cyclic codes (see also [37, 63]).

Theorem 4.4.1. *For any k , $1 \leq k \leq q + 1$, there exists an MDS code $C_{q+1,k}$ over $\mathbb{F}_q$ with parameters $[q + 1, k, q - k + 2]_q$ that is either cyclic or consta-cyclic. The codes of even dimension and the codes of odd dimension form two sequences of nested codes, i. e., $C_{q+1,k} \subset C_{q+1,k+2}$.*

Proof. Let ω denote a primitive element of $\mathbb{F}_{q^2}$. Hence $\alpha := \omega^{q-1}$ is a primitive $(q + 1)$ -th root of unity.

First we consider the case when $q + 1 - k$ is odd. We define the following polynomial of degree $2\mu + 1$:

$$g_1(z) := \prod_{i=-\mu}^{\mu} (z - \alpha^i).$$

Its zeros α^i and α^{-i} are conjugates of each other since $\alpha^q = \alpha^{-1}$. Hence, $g_1(z)$ is a polynomial over $\mathbb{F}_q$. The resulting cyclic code C over $\mathbb{F}_q$ has length $q + 1$ and dimension $q - 2\mu$. The generator polynomial $g_1(z)$ has $2\mu + 1$ consecutive zeros, so the BCH bound yields $d \geq 2\mu + 2$. Therefore C is an MDS code $[q + 1, q - 2\mu, 2\mu + 2]_q$.

If $q + 1 - k$ is even and q is even too, the polynomial

$$g_2(z) := \prod_{i=q/2-\mu}^{q/2+1+\mu} (z - \alpha^i) = \prod_{i=q/2-\mu}^{q/2} (z - \alpha^i)(z - \alpha^{-i})$$

has degree $2\mu + 2$. It is a polynomial over $\mathbb{F}_q$ with $2\mu + 2$ consecutive zeros, so the resulting code is an MDS code with parameters $[q + 1, q - 1 - 2\mu, 2\mu + 3]_q$.

Finally, if $q + 1 - k$ is even and q is odd, consider the polynomial

$$g_3(z) := \prod_{i=1}^{\mu} (z - \omega\alpha^i)(z - \omega\alpha^{1-i})$$

of degree 2μ . The roots $\omega\alpha^i$ and $\omega\alpha^{1-i}$ are conjugates of each other as $(\omega\alpha^i)^q = \omega^{1+(q-1)i} = \omega^{q+(1-q)i} = \omega^{1+(q-1)(1-i)} = \omega\alpha^{1-i}$, so $g_3(z)$ is a polynomial over $\mathbb{F}_q$. Furthermore, $g_3(z)$ divides $z^{q+1} - \omega^{q+1} \in \mathbb{F}_{q^2}[z]$ as $(\omega\alpha^i)^{q+1} = \omega^{q+1}$. Therefore $g_3(z)$ defines a constacyclic code C of length $q+1$ and dimension $q+1-2\mu$ over $\mathbb{F}_q$. Note that C can be considered as a shortened subcode of the cyclic code of length q^2-1 over $\mathbb{F}_{q^2}$ generated by $g_3(z)$. For the latter, the BCH bound yields $d \geq 2\mu+1$, hence C is an MDS code with parameters $[q+1, q+1-2\mu, 2\mu+1]_q$.

The statement $C_{q+1,k} \subset C_{q+1,k+2}$ follows from the particular form of the polynomials $g_i(z)$. $\square$

Remark 4.4.2. *Theorem 4.4.1 is a slightly modified version of Theorem 9 in [60, Ch. 11, §5]. There only cyclic codes are considered; the construction fails when both q and k are odd (see also the preface to the third printing of [60]).*

Theorem 4.4.3. *An MDS code with parameters $[q+1, k, d]_q$ has k nonzero weights, except when $k=2$.*

Proof. The statement is clearly true for $k=1$, and it does not hold for $k=2$ since the code with parameters $[q+1, 2, q]_q$ is a simplex code. For $k>2$, let $C^{(p)} = [q, k, d-1]_q$ and $C^{(s)} = [q, k-1, d]_q$ be the MDS codes obtained by puncturing and shortening of C , respectively. Without loss of generality, we may assume that we have deleted the last position. By Theorem 4.3.5, $C^{(s)}$ contains codewords of all $k-1$ weights $q-k+2, \dots, q$. Appending zero to the codewords in $C^{(s)}$, we obtain a subcode of C with the same weight distribution as that of $C^{(s)}$. Thus it remains to show that C contains a word of weight $q+1$. If the dimension of C is odd, by Theorem 4.4.1 the code C contains a subcode $[q+1, 1, q+1]_q$ and hence a word of weight $q+1$. If the

dimension of C is even, we know that statement (4.1.1) is false for dimension $k = 2$. If the dimension is at least four, the code C contains a subcode $[q + 1, 4, q - 2]_q$. For this code of dimension four, using (4.1.2) we compute

$$A_{q+1} = (q - 1) \sum_{j=0}^3 (-1)^j \binom{q}{j} q^{3-j} = \frac{1}{3} q (q - 1) (q^2 - 1).$$

This shows that the code with parameters $[q + 1, 4, q - 3]_q$ contains words of weight $q + 1$. $\square$

4.5 MDS Codes of Length $q + 2$

MDS codes of length $q + 2$ are known for $q = 2^m$, and $k = 3$ or $k = 2^m - 1$ (see, *e. g.*, [60, Theorem 10, Ch. 11, §5]). For $m > 1$, a generator matrix or parity check matrix is given by

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^4 & \dots & \alpha^{q-2} & 0 & 1 & 0 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(q-2)} & 0 & 0 & 1 \end{pmatrix}, \quad (4.5.1)$$

where α is a primitive element of the field $GF(2^m)$.

First consider the code with parameters $[2^m + 2, 3, 2^m]_{2^m}$. Assume that there is a codeword $\mathbf{v} \in C$ of weight $n - 1 = 2^m + 1$. Shortening C at the position where $\mathbf{v}$ is zero, we get a code $C^{(s)} = [2^m + 1, 2, 2^m]_{2^m}$ which contains a codeword v' of weight $2^m + 1$. But we already know that the code $C^{(s)}$ is a q -ary simplex code which does not contain a codeword of weight $2^m + 1$. Hence the code with parameters $[2^m + 2, 3, 2^m]_{2^m}$ does not contain a word of weight $2^m + 1$. Using (4.1.2), the non-zero coefficients of the weight enumerator are computed as $A_{2^m} = (2^{2^m} - 1)(2^{m-1} + 1)$, $A_{2^m+2} = 2^{m-1}(2^m - 1)^2$, and $A_0 = 1$.

Next, consider the dual code with parameters $[2^m + 2, 2^m - 1, 4]_{2^m}$ with the parity check matrix H given in (4.5.1).

Theorem 4.5.1. *The MDS code with parameters $[2^m + 2, 2^m - 1, 4]_{2^m}$ contains words of all weights $w = 4, \dots, 2^m + 2$ if and only if $m \neq 2$.*

Proof. For $m = 1$, the code is the binary repetition code $[4, 1, 4]_2$ for which the statement holds. For $m = 2$, we obtain the hexacode, a famous two-weight code (see [19, Chapter 3, (2.5.2)]). So let $m > 2$. Similar to the proof of Theorem 4.4.3, considering the shortened code $C^{(s)} = [2^m + 1, 2^m - 2, 4]_{2^m}$ we find that the code C contains words of all weights $w = 4, \dots, 2^m + 1$. It remains to show that C contains a word $\mathbf{v}$ of weight $2^m + 2$. Consider the following vector

$$\mathbf{v} = (\alpha, \underbrace{1, \dots, 1}_{q-2}, \alpha, \alpha + 1, \alpha + 1),$$

where $q = 2^m$. In order to show that $\mathbf{v}$ is in the kernel of H and hence $\mathbf{v} \in C$, we note that $\sum_{i=0}^{q-2} (\alpha^j)^i = 0$ for $0 < j < q - 1$. $\square$

4.6 An Alternative Approach

To prove the results concerning the weights of MDS codes above we have used a purely coding-theoretic approach. There is an instructive alternative approach which we can use to better understand the weights.

Ludo Tolhuizen showed in 1988 in an unpublished research report that $A_w \geq f(q, n, d, w)$ where

$$f(q, n, d, w) = \binom{n}{w} (q - d)(q - 1)^{w-d} > 0$$

for $d < q$.

Most results can also be derived through a careful analysis of Equation (4.1.2).

Let us rewrite the said equation as

$$A_w = \binom{n}{w} (q-1) \sum_{j=0}^{w-d} (-1)^j a_j, \text{ with } a_j = \binom{w-1}{j} q^{w-d-j} \quad (4.6.1)$$

for $d \leq w \leq n$ and investigate the cases for which $A_w = 0$.

First we show that for the $[n, n-1, 2]_2$ -code C with $n > 2$, $A_w = 0$ if and only if w is odd. Note that if l is an odd positive integer and

$$S := \sum_{j=0}^l (-1)^j \binom{l+1}{j} 2^{l-j},$$

we have

$$2S + 1 = \sum_{j=0}^{l+1} (-1)^j \binom{l+1}{j} 2^{l+1-j} = (2-1)^{l+1} = 1,$$

which implies that $S = 0$. If l is an even positive integer, it follows that

$$S := \sum_{j=0}^l (-1)^j \binom{l+1}{j} 2^{l-j} = l + 1.$$

Thus, we have an alternative proof for the assertion regarding the dual of the binary repetition code in Theorem 4.2.1.

For the nontrivial cases, observe that

$$R_j := \frac{a_j}{a_{j+1}} = q \frac{j+1}{w-1-j}.$$

Clearly, for $w \leq q$ we have $R_j > 1$, which implies that $A_w > 0$ for $n \leq q$.

For $n = q+1$, $R_j = 1$ if and only if $j = 0$ and $w = q+1$ since $q(j+1) > w-1-j$ for $j \geq 1$. Hence, $d = q$ and $k = 2$. Therefore, an MDS code with parameters $[q+1, 2, q]_q$ has $A_{q+1} = 0$.

Similarly for $n = q + 2$ with $q = 2^m$. $R_j = 1$ if and only if $j = 0$ and $w = q + 1$, forcing $d = q$ and $k = 3$. There are no codewords of weight $2^m + 1$ in any MDS code with parameters $[2^m + 2, 3, 2^m]_{2^m}$.

4.7 Summary on the Weights

In summary, we have the following:

Fact 1 The trivial MDS codes with parameters $[n, n, 1]_q$, $[n, 1, n]_q$, and $[n, n - 1, 2]_q$ have k non-zero weights with the exception of the dual of the binary repetition code of length $n > 2$ which contains only words of even weights.

Fact 2 The MDS codes with parameters $[n, k, d]_q$ of length $n \leq q + 1$ have k non-zero weights, with the exception of the q -ary simplex code with parameters $[q + 1, 2, q]_q$ which contains only words of weight zero or q .

Fact 3 For $m \neq 2$, the codes with parameters $[2^m + 2, 2^m - 1, 4]_{2^m}$ have $k = 2^m - 1$ non-zero weights. These codes are quasi perfect with covering radius 2.

Fact 4 The code with parameters $[2^m + 2, 3, 2^m]_{2^m}$ has only non-zero codewords of weight 2^m and $2^m + 2$, with $A_{2^m} = (2^{2^m} - 1)(2^{m-1} + 1)$ and $A_{2^m+2} = 2^{m-1}(2^m - 1)^2$. These two-weight codes are known as family TF1 in [15].

Our result covers the parameters of all non-trivial MDS codes given by the MDS conjecture. In general, if a non-trivial MDS code with parameters $[n, k, d]_q$ exists, then $2 \leq k \leq \min\{n - 2, q - 1\}$ and $n \leq q + k - 1 \leq 2q - 2$ (see [48, Corollary 7.4.4]).

Finally, note that the result confirms the construction of quantum MDS codes given in [36, 63] as statement (4.1.1) holds for all MDS codes used therein to derive shortened quantum codes.

Chapter 5

Pure Asymmetric Quantum MDS Codes from CSS Construction

In this chapter, the standard CSS construction is deployed to explicitly construct pure q -ary asymmetric quantum error-correcting codes reaching the quantum Singleton bound. Such codes are called asymmetric quantum maximum distance separable (AQMDS) codes. Appropriate pairs of nested classical MDS codes are used as the main ingredients. The parameters of AQMDS codes can be derived from the properties of the corresponding pairs of the nested MDS codes.

After disposing the trivial cases, we begin with the treatment for the case $d_x = 2$ in Section 5.1. For $d_x \geq 3$ and $n \leq q$ with $q \geq 5$, a construction based on Generalized Reed-Solomon Codes is detailed in Section 5.2. The case of length $n = q + 1$ is discussed in details in Section 5.3. If $q = 2^m \geq 4$, it is possible to construct AQMDS codes with $d_z = d_x = 4$. A construction is given in Section 5.4.

An explicit list of codes Q over $\mathbb{F}_7$ and $\mathbb{F}_8$ is given in Table 5.1 in Section 5.5

to illustrate the results. Except for some open cases for $n = q + 1$, we exhibit how to obtain q -ary AQMDS codes with all theoretically obtainable parameters for all lengths for which linear MDS codes over $\mathbb{F}_q$ are known to exist. We provide a detailed summary of results and open problems in Section 5.6.

It has been previously noted that any $[[n, k, d_z/d_x]]_q$ -CSS code satisfies the quantum version of the Singleton bound

$$k \leq n - d_x - d_z + 2.$$

This bound is conjectured to hold for all asymmetric quantum codes. An asymmetric quantum code Q is said to be MDS if it attains the equality of the bound.

We know that, for convenience, $d_z \geq d_x$ can be safely assumed. For error-detecting reason, it is usually required that $d_x \geq 2$, which we will follow.

Here we say something about the case of $d_x = 1$ for completeness. Let C be a linear MDS code with parameters $[n, k, d]_q$ for all possible values of k for which linear MDS codes are known to exist, given q and n . We can always use the usual CSS construction with $C_2 := \mathbb{F}_q^n$ and $C_1 := C^{\perp_E}$ to derive an $[[n, n - k, (k + 1)/1]]_q$ -asymmetric quantum MDS code Q .

Let Q be a pure asymmetric quantum codes constructed by using the usual CSS construction. Then we know from [69, Cor. 2.5] that Q is MDS if and only if both C_1 and C_2 are (classical) MDS codes. Hence, we can immediately derive the following result treating the asymmetric quantum codes with $K = 1$.

Proposition 5.0.1. *Let C be any $[n, k, n - k + 1]_q$ -MDS code with $1 \leq k < n$. Then there exists an asymmetric quantum code Q with parameters $[[n, 0, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{n - k + 1, k + 1\}$.*

Proof. Use $C_1^{\perp_E} = C_2 = C$. □

5.1 Quantum MDS Codes with $d_z \geq d_x = 2$

Let us begin with a more general result.

Theorem 5.1.1. *Let C be a linear $[n, k, d]_q$ -code. If C has a codeword $\mathbf{u}$ such that $\text{wt}_H(\mathbf{u}) = n$, then there exists an asymmetric quantum $[[n, k - 1, d/2]]_q$ -code Q .*

Proof. Construct a subcode $D := \{\lambda \mathbf{u} : \lambda \in \mathbb{F}_q\} \subset C$. Since D is MDS, $D^{\perp_E}$ is also MDS with parameters $[n, n - 1, 2]_q$. Applying the usual CSS construction with $C_1 = D^{\perp_E}$ and $C_2 = C$ completes the proof. □

Remark 5.1.2. *In proving Theorem 5.1.1, $C_1 = D^{\perp_H}$ can be chosen if so desired provided that $q = r^2$. In this case, we use the CSS-like construction under the Hermitian inner product instead of the usual CSS construction.*

We can now use Theorem 5.1.1 and our knowledge of the weights of linear MDS codes to derive AQMDS codes with $d_x = 2$. First, we dispose of the trivial cases.

Corollary 5.1.3. *For even $n \in \mathbb{N}$, there exists an $[[n, n - 2, 2/2]]_2$ -AQMDS code. For positive integers $n, q \geq 3$, there exists an $[[n, n - 2, 2/2]]_q$ -AQMDS code Q .*

Proof. This follows directly from Theorem 5.1.1 and Fact 1 in Section 4.7. □

Remark 5.1.4. *The existence of $[[n, n - 2, 2/2]]_q$ -asymmetric quantum MDS codes Q for $n, q \geq 3$ is proved differently (without using the linear MDS codes C and D) in [69, Cor. 3.4]. Our proof here is simpler.*

Corollary 5.1.5. *Given positive integers $q \geq n > 3$, there exists an AQMDS code for $1 < k \leq n - 2$ with parameters*

$$[[n, k - 1, (n - k + 1)/2]]_q.$$

Proof. This follows directly from Theorem 5.1.1 and Fact 2 in Section 4.7. $\square$

Fact 2 in Section 4.7 also says that, excluding the case $k = 2$, a $[q + 1, 1, q + 1]_q$ -code $D \subset C$ can be constructed by using any codeword $\mathbf{u} \in C$ of weight $q + 1$. Thus, the following corollary to Theorem 5.1.1 can be derived.

Corollary 5.1.6. *Given $q \geq 4$, there exists an AQMDS code for $3 \leq k \leq q - 1$ with parameters*

$$[[q + 1, k - 1, (q - k + 2)/2]]_q.$$

We note here that it is not possible to derive a pure $[[q + 1, 1, q/2]]_q$ -AQMDS code Q based on nested linear MDS codes following the usual CSS construction. By Fact 2 in Section 4.7, it is not possible to construct Q based on the $[q + 1, 2, q]_q$ -simplex code $\mathcal{H}_{q,2}^{\perp_E}$ since there is no codeword of weight $q + 1$ in $\mathcal{H}_{q,2}^{\perp_E}$. An alternative is to construct Q based on nested codes $C \subset D$ with parameters $[q + 1, q - 1, 3]_q$ and $[q + 1, q, 2]_q$, respectively. Assume that this is possible. We have $D^{\perp_E} \subset C^{\perp_E}$ with $C^{\perp_E}$ equivalent to the simplex code $\mathcal{H}_{q,2}^{\perp_E}$ and $D^{\perp_E}$ a code with parameters $[q + 1, 1, q + 1]_q$, a contradiction.

MDS codes of length $q + 2$ are known to exist for $q = 2^m$, and $k = 3$ or $k = 2^m - 1$ (see, for example, [60, Theorem 10, Ch. 11, §5]). For $m > 1$, a generator matrix for

$k = 3$ or a parity check matrix for $k = 2^m - 1$ is given by

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{q-2} & 0 & 1 & 0 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(q-2)} & 0 & 0 & 1 \end{pmatrix}, \quad (5.1.1)$$

where α is a primitive element of the field $\mathbb{F}_{2^m}$.

Corollary 5.1.7. *Given a positive integer m and $q = 2^m$, there exists an AQMDS code with parameters*

$$[[2^m + 2, 2, 2^m/2]]_{2^m}.$$

If, moreover, $m \neq 2$, then there exists an AQMDS code with parameters

$$[[2^m + 2, 2^m - 2, 4/2]]_{2^m}.$$

Proof. The first assertion follows from combining Theorem 5.1.1 and Fact 4 in Section 4.7. For the second assertion, use Fact 3 instead of Fact 4. $\square$

In the case of AQMDS codes with $d_z \geq d_x = 2$, there is no gain from using strictly $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$ for $q = r^2$.

Proposition 5.1.8. *Let $q = r^2$. There does not exist an $\mathbb{F}_r$ -linear code C with parameters $(n, r = \sqrt{q}, d)_q$ with $d(C^{\perp_{\text{TrH}}}) \geq 2$.*

Proof. Let $\mathbf{c} := (c_1, c_2, \dots, c_n) \in \mathbb{F}_q^n$ be a nonzero vector and $C := \{\lambda \mathbf{c} : \lambda \in \mathbb{F}_r\}$. Then there exists s with $1 \leq s \leq n$ where $c_s \neq 0$. Since $\lambda \in \mathbb{F}_r$, $\lambda^r = \lambda$. Let $\mathbf{d} := (0, \dots, 0, c_s, 0, \dots, 0)$. If q is even,

$$\langle \lambda \mathbf{c}, \mathbf{d} \rangle_{\text{TrH}} = \lambda c_s \cdot c_s^r + (\lambda c_s)^r \cdot c_s = 0.$$

Similarly, if q is odd, letting $\alpha \in \mathbb{F}_q \setminus \{0\}$ with $\alpha^r = -\alpha$,

$$\langle \lambda \mathbf{c}, \mathbf{d} \rangle_{\text{Tr}_H} = \alpha \cdot (\lambda c_s \cdot c_s^r - (\lambda c_s)^r \cdot c_s) = 0.$$

Thus, $\mathbf{d} \in C^{\perp_{\text{Tr}_H}}$. □

An alternative proof can be supplied as well by considering the weight distribution of the code and applying the MacWilliams transform to find the weight distribution of its dual.

The results derived in this Section 5.1 do not depend on the specific construction of the chosen linear MDS codes, only on whether or not they contain a codeword of weight equal to the length n .

5.2 Quantum MDS Codes of Length $n \leq q$ with

$$d_z \geq d_x \geq 3$$

Shifting our attention to AQMDs codes with $d_x \geq 3$, let us recall some basic results on Generalized Reed-Solomon (GRS) codes. To construct a GRS code, one begins by choosing n distinct elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ and define $\boldsymbol{\alpha} := (\alpha_1, \dots, \alpha_n)$. Let $\mathbf{v} := (v_1, \dots, v_n)$ with $v_i \in \mathbb{F}_q \setminus \{0\}$. Let $\mathbb{F}_q[X]_k$ denote the set of all polynomials of degree less than k in $\mathbb{F}_q[X]$. Then, given $\boldsymbol{\alpha}$ and $\mathbf{v}$, a GRS code of length $n \leq |\mathbb{F}_q|$ and dimension $k \leq n$ can be defined as

$$\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) := \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) : f(X) \in \mathbb{F}_q[X]_k\}. \quad (5.2.1)$$

Since $\mathbb{F}_q[X]_k \subset \mathbb{F}_q[X]_{k+1}$ by embedding, for fixed $n, \mathbf{v}$, and $\boldsymbol{\alpha}$, it follows immedi-

ately that

$$\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) \subset \mathcal{GRS}_{n,k+1}(\boldsymbol{\alpha}, \mathbf{v}). \quad (5.2.2)$$

By a slight abuse of notation, we can associate a polynomial $f(X) \in \mathbb{F}_q[X]_k$ with a codeword $\mathbf{f}$, depending on $\boldsymbol{\alpha}$ and $\mathbf{v}$ by employing the following bijective evaluation map

$$\begin{aligned} \mathbf{ev} : \mathbb{F}_q[X]_k &\rightarrow \mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) \\ f(X) &\mapsto \mathbf{f} = (v_1 f(\alpha_1), \dots, v_n f(\alpha_n)). \end{aligned}$$

Let C be $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$. If we choose the standard basis $\{1, x, \dots, x^{k-1}\}$ for $\mathbb{F}_q[X]_k$, then a generator matrix G for C is given by

$$G = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1 \alpha_1 & v_2 \alpha_2 & \dots & v_n \alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \dots & v_n \alpha_n^{k-1} \end{pmatrix}. \quad (5.2.3)$$

Since any nonzero polynomial $h(X) \in \mathbb{F}_q[X]_k$ has at most $k - 1$ zeros, $\text{wt}_H(\mathbf{h}) \geq n - (k - 1)$. By the Singleton bound, we conclude that $\text{wt}_H(\mathbf{h}) = n - k + 1$. Thus $C = \mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ is an MDS code with parameters $[n, k, n - k + 1]_q$.

Let $\mathbf{u} := (u_1, \dots, u_n)$ with

$$u_i^{-1} = v_i \prod_{j \neq i} (\alpha_i - \alpha_j).$$

It is known (see, for instance, [48, Th. 5.3.3]) that the Euclidean dual $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})^{\perp_E}$

of C is the code $C^{\perp_E} = \mathcal{GRS}_{n,n-k}(\boldsymbol{\alpha}, \mathbf{u})$ with generator matrix

$$H = \begin{pmatrix} u_1 & u_2 & \dots & u_n \\ u_1\alpha_1 & u_2\alpha_2 & \dots & u_n\alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ u_1\alpha_1^{n-k-1} & u_2\alpha_2^{n-k-1} & \dots & u_n\alpha_n^{n-k-1} \end{pmatrix}. \quad (5.2.4)$$

The code $C^{\perp_E} = \mathcal{GRS}_{n,n-k}(\boldsymbol{\alpha}, \mathbf{u})$ is MDS of parameters $[n, n-k, k+1]_q$.

In the case of $q = r^2$, let $\mathbf{v}^r := (v_1^r, v_2^r, \dots, v_n^r)$ and $\boldsymbol{\alpha}^r := (\alpha_1^r, \alpha_2^r, \dots, \alpha_n^r)$. Define $C^r := \{\mathbf{c}^r : \mathbf{c} \in C\}$ for $C = \mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$. It can be verified directly that the Hermitian dual $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})^{\perp_H}$ is the MDS code $\mathcal{GRS}_{n,n-k}(\boldsymbol{\alpha}^r, \mathbf{u}^r)$. That is, $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})^{\perp_H} = ((\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v}))^r)^{\perp_E}$. If $\mathbf{b}$ is another n -tuple of nonzero elements of $\mathbb{F}_q$, then $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ and $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{b})$ are monomially equivalent.

Let α be a primitive element of $\mathbb{F}_q$ and let k be an integer with $0 \leq k \leq n = q-1$. Define $\boldsymbol{\alpha} := (1, \alpha, \alpha^2, \dots, \alpha^{q-2})$ and $\mathbf{v} = (1, \dots, 1)$. Then $C := \mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ is the $[q-1, k, q-k]_q$ -(narrow-sense) Reed-Solomon (RS) code. This code C can be extended by adding an extra coordinate entry $c_q = -\sum_{i=1}^{q-1} c_i$ for every codeword $\mathbf{c} = (c_1, c_2, \dots, c_{q-1}) \in C$, yielding a $[q, k, q-k+1]_q$ -extended RS code $\widehat{C}$.

Seen as a q -ary BCH code with designed distance δ , an RS code C has a generator polynomial

$$g(X) = (X - \alpha^{a+1})(X - \alpha^{a+2}) \dots (X - \alpha^{a+\delta-1})$$

with $a \geq 0$ and $2 \leq \delta (= q-k) \leq q-1$.

To prove the following general result, nested GRS codes will be used, while for the example illustrating the result for $n = q-1$ and $n = q$ we will explicitly construct asymmetric quantum codes from nested RS and nested extended RS codes.

Theorem 5.2.1. *Let $q \geq 5$. Let n, k and j be positive integers with $n \leq q$, $2 \leq k \leq n-3$ and $j \leq n-k-2$. Then there exists an asymmetric quantum MDS code Q with parameters $[[n, j, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{n-k-j+1, k+1\}$.*

Proof. One can choose $C_1 = \mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})^{\perp_E}$ (or $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})^{\perp_H}$ if $q = r^2$) and $C_2 = \mathcal{GRS}_{n,k+j}(\boldsymbol{\alpha}, \mathbf{v})$. Hence, $\{d_z, d_x\} = \{d(C_1) = k+1, d(C_2) = n-(k+j)+1\}$ and $\frac{|C_2|}{|C_1^{\perp_E}|} = q^j$ as required. $\square$

Example 5.2.2. *For $q \geq 7$, we have the following chain of nested RS codes*

$$\left\langle \prod_{i=1}^{q-3} (X - \alpha^i) \right\rangle \subset \left\langle \prod_{i=1}^{q-4} (X - \alpha^i) \right\rangle \subset \cdots \subset \left\langle \prod_{i=1}^2 (X - \alpha^i) \right\rangle \quad (5.2.5)$$

with parameters $[q-1, 2, q-2]_q, [q-1, 3, q-3]_q, \dots, [q-1, q-3, 3]_q$, respectively. Let l and j be positive integers with $l \leq q-5$ and $j \leq q-4-l$. Choosing

$$D := \left\langle \prod_{i=1}^{q-2-l} (X - \alpha^i) \right\rangle \subset C := \left\langle \prod_{i=1}^{q-2-l-j} (X - \alpha^i) \right\rangle$$

from Equation (5.2.5), we know that $\log_q \frac{|C|}{|D|} = j$, C is a $[q-1, l+j+1, q-l-j-1]_q$ -code and D is a $[q-1, l+1, q-l-1]_q$ -code. Hence, $d(D^{\perp_E}) = l+2$ and an AQMDS code Q with parameters $[[q-1, j, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{(q-l-j-1), (l+2)\}$ is derived.

For $q \geq 5$, we have the following chain of nested extended RS codes

$$\left\langle \widehat{\prod_{i=1}^{q-3} (X - \alpha^i)} \right\rangle \subset \left\langle \widehat{\prod_{i=1}^{q-4} (X - \alpha^i)} \right\rangle \subset \cdots \subset \langle \widehat{(X - \alpha)} \rangle \quad (5.2.6)$$

with parameters $[q, 2, q-1]_q, [q, 3, q-2]_q, \dots, [q, q-2, 3]_q$, respectively. Let l and j be positive integers with $l \leq q-4$ and $j \leq q-3-l$. Choosing

$$D := \left\langle \widehat{\prod_{i=1}^{q-2-l} (X - \alpha^i)} \right\rangle \subset C := \left\langle \widehat{\prod_{i=1}^{q-2-l-j} (X - \alpha^i)} \right\rangle$$

from Equation (5.2.6), it is easy to compute that $\log_q \frac{|C|}{|D|} = j$, C is a $[q, l + j + 1, q - l - j]_q$ -code and D is a $[q, l + 1, q - l]_q$ -code with $d(D^{\perp_E}) = l + 2$. Hence, an AQMDS code Q with parameters $[[q, j, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{(q - l - j), (l + 2)\}$ is derived.

Remark 5.2.3. By puncturing nested RS codes $D \subset C$ with parameters $[n, k_1, n - k_1 + 1]_q$ and $[n, k_2, n - k_2 + 1]_q$, respectively, we can derive nested MDS codes $D' \subset C'$ with parameters $[n - t, k_1, n - k_1 + 1 - t]_q$ and $[n - t, k_2, n - k_2 + 1 - t]_q$, respectively, with $1 \leq t \leq n - k_2$. This allows us to construct AQMDS codes of lower lengths. The more general approach of using GRS codes is preferred since it eliminates the need to puncture the codes.

5.3 Quantum MDS Codes of Length $n = q + 1$ with

$$d_z \geq d_x \geq 3$$

The construction is based on the following result.

Theorem 5.3.1. [25, Th. 8] For any k , $1 \leq k \leq q + 1$, there exists an MDS code $C_{q+1,k}$ over $\mathbb{F}_q$ with parameters $[q+1, k, q-k+2]_q$ that is either cyclic or consta-cyclic. The codes of even dimension and the codes of odd dimension form two sequences of nested codes, i. e., $C_{q+1,k} \subset C_{q+1,k+2}$.

Based on this theorem, for $q = 5$ we have the following nested codes

$$C := [6, 2, 5]_5 \subset D := [6, 4, 3]_5,$$

which yield an asymmetric MDS code Q with parameters $[[6, 2, 3/3]]_5$. Generalizing this observation, we have

Theorem 5.3.2. *Let j be a positive integer. For $q \geq 5, k \geq 2$ and $k + 2j \leq q - 1$, there exists an asymmetric quantum code Q with parameters $[[q + 1, 2j, d_z/d_x]]_q$ where*

$$\{d_z, d_x\} = \{q - k - 2j + 2, k + 1\}.$$

Proof. Let $C_1 := C_{q+1,k}^\perp$ and $C_2 := C_{q+1,k+2j}$. Then by the usual CSS construction there exists an asymmetric quantum code Q with parameters $[[q + 1, 2j, d_z/d_x]]_q$ with $\{d_z, d_x\} = \{d(C_1), d(C_2)\}$. Since both C_1 and C_2 are MDS, we know that $d(C_1) = (q + 1) - (q + 1 - k) + 1 = k + 1$ and $d(C_2) = (q + 1) - (k + 2j) + 1 = q - k - 2j + 2$. $\square$

The asymmetric quantum code Q given in Theorem 5.3.2 above has $K = q^{2j}$, making $\log_q(K)$ always even. In the case $q = 2^m \geq 4$, we can do better.

Lemma 5.3.3. *Let $q = 2^m \geq 4$ and let s be a positive integer $< q/2$. Then there exist nested MDS codes $C_{q+1,2s} \subset D$ with parameters $[q + 1, 2s, q - 2s + 2]_q$ and $[q + 1, q - 1, 3]_q$, respectively.*

Proof. Let ω be a primitive element in $\mathbb{F}_{q^2}$. Then $\alpha := \omega^{q-1}$ is a primitive $(q + 1)$ -th root of unity in $\mathbb{F}_{q^2}$. Following [25, Th. 8], the code $C_{q+1,2s}$ generated by

$$g_1(X) := \prod_{i=-(q/2-s)}^{(q/2-s)} (X - \alpha^i)$$

is a $[q + 1, 2s, q - 2s + 2]_q$ -code. The code D generated by $g(X) := (X - \alpha)(X - \alpha^{-1})$ is a $[q + 1, q - 1]_q$ -code containing $C_{q+1,2s}$ since $g(X)$ divides $g_1(X)$ and both polynomials are in $\mathbb{F}_q[X]$.

Now, consider the polynomial

$$g'(X) := (X - \alpha^{q/2})(X - \alpha^{q/2+1}),$$

having two consecutive zeros. Combining the BCH and Singleton bounds, the code D' generated by $g'(X)$ is a $[q+1, q-1, 3]_q$ -code.

Let θ be an automorphism on $\mathbb{F}_q$ defined by $\theta(a) = a^{q/2}$ for all $a \in \mathbb{F}_q$. Given their respective generator polynomials, to show that D and D' are equivalent, it suffices to prove that $\theta(\alpha + \alpha^{-1}) = \alpha^{q/2} + \alpha^{(q/2)+1}$. Note that

$$\theta(\alpha^{-1}) = \alpha^{-q/2} = \alpha^{q+1-(q/2)} = \alpha^{(q/2)+1}.$$

Therefore, $d(D) = 3$. □

Using Lemma 5.3.3 and applying the usual CSS construction with $C_1 = C_{q+1, 2s}^{\perp_E}$ and $C_2 = D$, the following result can then be derived.

Theorem 5.3.4. *Let $q = 2^m \geq 4$. For positive integer $s \leq q/2 - 1$, there exists a $[[q+1, q-1-2s, (2s+1)/3]]_q$ -asymmetric quantum MDS code Q .*

Remark 5.3.5. *Let q be odd and let α and ω be as given in the proof of Lemma 5.3.3. Consider the polynomial*

$$g_3(X) := \prod_{i=1}^{\mu} (X - \omega\alpha^i)(X - \omega\alpha^{1-i})$$

that generates a $[q+1, q+1-2\mu, 2\mu+1]_q$ -consta-cyclic code C as shown in the proof of [25, Th. 8]. It is not possible to construct a code D generated by any degree-one polynomial $f(X) \in \mathbb{F}_q[X]$ such that D contains C . Any divisor $f(X)$ of $g_3(X)$ in $\mathbb{F}_q[X]$ must be of even degree since $f(X)$ can only be constructed by removing the linear factors of $g_3(X)$ pair by pair. Removing only one linear factor of $(X - \omega\alpha^i)(X - \omega\alpha^{1-i})$ will put $f(X)$ in $\mathbb{F}_{q^2}[X] \setminus \mathbb{F}_q[X]$, a contradiction.

5.4 Quantum MDS Codes of Length $n = 2^m + 2 \geq 6$

with $d_z = d_x = 4$

As mentioned earlier, MDS codes of length $q + 2$ are known to exist for $q = 2^m$, and $k = 3$ or $k = 2^m - 1$. Let α be a primitive element of $\mathbb{F}_{2^m}$. Let C be a $[2^m + 2, 2^m - 1, 4]_{2^m}$ -code with parity check matrix H given in Equation (5.1.1). Let D be the $[2^m + 2, 3, 2^m]_{2^m}$ -code whose generator matrix G is given by

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 & 0 & 0 \\ 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \dots & \alpha^{-(q-2)} & 0 & 1 & 0 \\ 1 & \alpha^{-2} & \alpha^{-4} & \alpha^{-6} & \dots & \alpha^{-2(q-2)} & 0 & 0 & 1 \end{pmatrix}. \quad (5.4.1)$$

Theorem 5.4.1. *Let $q = 2^m \geq 4$. Then there exists an asymmetric quantum MDS code Q with parameters $[[2^m + 2, 2^m - 4, 4/4]]_{2^m}$.*

Proof. First we prove the claim that $D \subset C$ by showing that $M = (m_{i,j}) := GH^T = \mathbf{0}$.

Note that

$$m_{i,j} = \sum_{r=1}^{2^m+2} g_{i,r} \cdot h_{j,r}$$

for $1 \leq i, j \leq 3$. If $i = j$, then $m_{i,j} = 2^m = 0$. If $i \neq j$, the desired conclusion follows from the fact that $\sum_{l=0}^{2^m-2} \alpha^l = \sum_{l=0}^{2^m-2} \alpha^{-l} = 0$. Applying the usual CSS construction with $C_1 = D^{\perp_E}$ and $C_2 = C$ completes the proof. $\square$

5.5 Explicit List for $\mathbb{F}_7$ and $\mathbb{F}_8$

To illustrate the various constructions discussed above, an explicit list of asymmetric quantum codes for $\mathbb{F}_7$ and $\mathbb{F}_8$ is provided in Table 5.1. We exclude the case $d_z = d_x = 2$

from Corollary 5.1.3 and the case $K = 1$ from Proposition 5.0.1 for brevity. $\mathbb{F}_7$ is chosen since $\mathbb{F}_5$ does not give us many AQMDS codes and $\mathbb{F}_8$ is selected since it is the smallest interesting power of 2 for our purpose. Explicit lists for other finite fields can be easily generated if so desired.

5.6 Conclusions and Open Problems

Based on known facts about linear MDS codes and their nestedness, we have constructed q -ary AQMDS codes for all possible lengths for which linear MDS codes over $\mathbb{F}_q$ are known to exist.

If we consider the parameters of all theoretically obtainable nontrivial pure quantum MDS codes from our CSS-like constructions, we have the following summary and open problems:

1. For $n \leq q$ all possible cases are taken care of. The nontrivial possibilities are covered by Corollary 5.1.5 for $d_x = 2$ and by Theorem 5.2.1 for $d_z \geq d_x \geq 3$.
2. Corollary 5.1.7 and Theorem 5.4.1 show that we have covered all nontrivial possibilities in the case of $n = q + 2$ with $q = 2^m$.
3. Consider q odd and $n = q + 1$.
 - (a) Corollary 5.1.6 and Theorem 5.3.2 take care of the cases where $K = q^{2j}$ with $1 \leq j \leq \frac{q-1}{2}$.
 - (b) The cases where $K = q^{2j+1}$ are still open for $1 \leq j \leq \frac{q-5}{2}$. The upper bound for j is $\frac{q-5}{2}$ since Corollary 5.1.6 allows us to construct a $[[q+1, q-2, 3/2]]_q$ -quantum code.

- (c) For $K = q$ with $d_z \geq d_x \geq 3$, all possibilities are still open.
4. Consider $q = 2^m$ with $m \geq 2$ and $n = q + 1$.
- (a) For $K = q$ with $d_z \geq d_x \geq 3$, the only case done is the construction of a $[[q + 1, 1, (q - 1)/3]]_q$ -quantum code Q based on Theorem 5.3.4 with $s = \frac{q}{2} - 1$. All other possibilities remain open.
- (b) Corollary 5.1.6 and Theorem 5.3.2 take care of the cases where $K = q^{2j}$ with $1 \leq j \leq \frac{q-2}{2}$.
- (c) For $K = q^{2j+1}$, Corollary 5.1.6 and Theorem 5.3.4 settle the cases of $d_x = 2$ and $d_x = 3$, respectively. Hence, the only open cases are those with $1 \leq j \leq \frac{q-6}{2}$.

Table 5.1: Nontrivial AQMDS Codes for $\mathbb{F}_7$ and $\mathbb{F}_8$.

q	n	Code Q	Construction	q	n	Code Q	Construction	q	n	Code Q	Construction
7	4	$[[4, 1, 3/2]]_7$	Cor. 5.1.5, $k = 2$	7	7	$[[7, 3, 4/2]]_7$	Cor. 5.1.5, $k = 4$	7	6	$[[6, 2, 3/3]]_7$	Th. 5.2.1, $k = 2, j = 2$
	5	$[[5, 1, 4/2]]_7$	Cor. 5.1.5, $k = 2$			$[[7, 4, 3/2]]_7$	Cor. 5.1.5, $k = 5$		7	$[[7, 1, 5/3]]_7$	Th. 5.2.1, $k = 2, j = 1$
		$[[5, 2, 3/2]]_7$	Cor. 5.1.5, $k = 3$			$[[8, 2, 6/2]]_7$	Cor. 5.1.6, $k = 3$			$[[7, 2, 4/3]]_7$	Th. 5.2.1, $k = 2, j = 2$
	6	$[[6, 1, 5/2]]_7$	Cor. 5.1.5, $k = 2$			$[[8, 3, 5/2]]_7$	Cor. 5.1.6, $k = 4$			$[[7, 3, 3/3]]_7$	Th. 5.2.1, $k = 2, j = 3$
		$[[6, 2, 4/2]]_7$	Cor. 5.1.5, $k = 3$			$[[8, 4, 4/2]]_7$	Cor. 5.1.6, $k = 5$			$[[7, 1, 4/4]]_7$	Th. 5.2.1, $k = 3, j = 1$
		$[[6, 3, 3/2]]_7$	Cor. 5.1.5, $k = 4$			$[[8, 5, 3/2]]_7$	Cor. 5.1.6, $k = 6$		8	$[[8, 2, 5/3]]_7$	Th. 5.3.2, $k = 2, j = 1$
	7	$[[7, 1, 6/2]]_7$	Cor. 5.1.5, $k = 2$		5	$[[5, 1, 3/3]]_7$	Th. 5.2.1, $k = 2, j = 1$			$[[8, 2, 4/4]]_7$	Th. 5.3.2, $k = 3, j = 1$
		$[[7, 2, 5/2]]_7$	Cor. 5.1.5, $k = 3$		6	$[[6, 1, 4/3]]_7$	Th. 5.2.1, $k = 2, j = 1$			$[[8, 4, 3/3]]_7$	Th. 5.3.2, $k = 2, j = 2$
8	4	$[[4, 1, 3/2]]_8$	Cor. 5.1.5, $k = 2$	8	8	$[[8, 5, 3/2]]_8$	Cor. 5.1.5, $k = 6$	8	8	$[[8, 1, 6/3]]_8$	Th. 5.2.1, $k = 2, j = 1$
	5	$[[5, 1, 4/2]]_8$	Cor. 5.1.5, $k = 2$		9	$[[9, 2, 7/2]]_8$	Cor. 5.1.6, $k = 3$			$[[8, 2, 5/3]]_8$	Th. 5.2.1, $k = 2, j = 2$
		$[[5, 2, 3/2]]_8$	Cor. 5.1.5, $k = 3$			$[[9, 3, 6/2]]_8$	Cor. 5.1.6, $k = 4$			$[[8, 3, 4/3]]_8$	Th. 5.2.1, $k = 2, j = 3$
	6	$[[6, 1, 5/2]]_8$	Cor. 5.1.5, $k = 2$			$[[9, 4, 5/2]]_8$	Cor. 5.1.6, $k = 5$			$[[8, 4, 3/3]]_8$	Th. 5.2.1, $k = 2, j = 4$
		$[[6, 2, 4/2]]_8$	Cor. 5.1.5, $k = 3$			$[[9, 5, 4/2]]_8$	Cor. 5.1.6, $k = 6$			$[[8, 1, 5/4]]_8$	Th. 5.2.1, $k = 3, j = 1$
		$[[6, 3, 3/2]]_8$	Cor. 5.1.5, $k = 4$			$[[9, 6, 3/2]]_8$	Cor. 5.1.6, $k = 7$			$[[8, 2, 4/4]]_8$	Th. 5.2.1, $k = 3, j = 2$
	7	$[[7, 1, 6/2]]_8$	Cor. 5.1.5, $k = 2$		10	$[[10, 2, 8/2]]_8$	Cor. 5.1.7		9	$[[9, 2, 6/3]]_8$	Th. 5.3.2, $k = 2, j = 1$
		$[[7, 2, 5/2]]_8$	Cor. 5.1.5, $k = 3$			$[[10, 6, 4/2]]_8$	Cor. 5.1.7			$[[9, 2, 5/4]]_8$	Th. 5.3.2, $k = 3, j = 1$
		$[[7, 3, 4/2]]_8$	Cor. 5.1.5, $k = 4$		5	$[[5, 1, 3/3]]_8$	Th. 5.2.1, $k = 2, j = 1$			$[[9, 4, 4/3]]_8$	Th. 5.3.2, $k = 2, j = 2$
		$[[7, 4, 3/2]]_8$	Cor. 5.1.5, $k = 5$		6	$[[6, 1, 4/3]]_8$	Th. 5.2.1, $k = 2, j = 1$			$[[9, 1, 7/3]]_8$	Th. 5.3.4, $s = 3$
	8	$[[8, 1, 7/2]]_8$	Cor. 5.1.5, $k = 2$			$[[6, 2, 3/3]]_8$	Th. 5.2.1, $k = 2, j = 2$			$[[9, 3, 5/3]]_8$	Th. 5.3.4, $s = 2$
		$[[8, 2, 6/2]]_8$	Cor. 5.1.5, $k = 3$		7	$[[7, 1, 5/3]]_8$	Th. 5.2.1, $k = 2, j = 1$			$[[9, 5, 3/3]]_8$	Th. 5.3.4, $s = 1$
		$[[8, 3, 5/2]]_8$	Cor. 5.1.5, $k = 4$			$[[7, 2, 4/3]]_8$	Th. 5.2.1, $k = 2, j = 2$		10	$[[10, 4, 4/4]]_8$	Th. 5.4.1
		$[[8, 4, 4/2]]_8$	Cor. 5.1.5, $k = 5$			$[[7, 3, 3/3]]_8$	Th. 5.2.1, $k = 2, j = 3$				

Chapter 6

Three Constructions of Nested Pairs of Classical Codes

In the preceding chapter, we have discussed the construction of asymmetric quantum codes that reach the equality of the quantum Singleton bound. Such quantum MDS codes, however, are limited in length. For q -ary quantum codes, the largest length possible is bounded by $q + 1$ for odd q and by $q + 2$ for even q .

In this chapter we are interested in the best-possible parameters that a q -ary AQECC can achieve for lengths above the largest MDS length. We call such a code *optimal*.

To get AQECCs with relatively good parameters, we directly construct nested pairs of classical codes and derive the parameters of the resulting CSS-like codes.

Three constructions are considered, namely a construction based on nested cyclic $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$, a construction from nested group character codes, and a construction based on best-known linear codes (BKLC) of length n having a code-

word $\mathbf{v}$ such that $\text{wt}_H(\mathbf{v}) = n$. This last construction yields AQECCs with $d_x = 2$. All computations concerning constructions and parameters of the codes are done in MAGMA [6] version V2.16-5.

6.1 Cyclic Construction

An obvious choice for the construction of nested pair of $\mathbb{F}_q$ -linear codes is the well-known cyclic construction. Under the natural correspondence of vectors and polynomials, the study of $\mathbb{F}_q$ -linear cyclic codes in $\mathbb{F}_q^n$ is equivalent to the study of ideals in the residue class ring

$$\mathcal{R}_n = \mathbb{F}_q[x]/\langle x^n - 1 \rangle.$$

The study of ideals in $\mathcal{R}_n$ depends on factoring $x^n - 1$. Basic results concerning and the properties of cyclic codes can be found in [48, Ch. 4] or [60, Ch. 7]. A cyclic code D is a subset of a cyclic code C of equal length over $\mathbb{F}_q$ if and only if the generator polynomial of C divides the generator polynomial of D . Both polynomials divide $x^n - 1$. Once the factorization of $x^n - 1$ into irreducible polynomials is known, the nestedness property becomes obvious.

Since we are also interested in nested pairs of $\mathbb{F}_r$ -linear codes over $\mathbb{F}_q$, a generalization to the construction of $\mathbb{F}_r$ -linear nested cyclic codes over $\mathbb{F}_q$ is provided here. Our construction is a further generalization of [16, Th. 14].

Definition 6.1.1. *An $(n, r^l)_q$ -code C is said to be cyclic $\mathbb{F}_r$ -linear over $\mathbb{F}_q$ if C is a subspace of the $\mathbb{F}_r$ -vector space $\mathbb{F}_q^n$ which is closed under one cyclic shift. That is, if $\mathbf{c} := (c_0, c_1, \dots, c_{n-1}) \in C$, then so is $\mathbf{c}' := (c_{n-1}, c_0, \dots, c_{n-2})$.*

Let $\mathbb{F}_q$ be the field extension of $\mathbb{F}_r$ of degree m such that $\mathbb{F}_q = \mathbb{F}_r(\omega)$. Every polynomial in $\mathbb{F}_q[x]$ can be uniquely written as

$$f_0(x) + \omega f_1(x) + \cdots + \omega^{m-1} f_{m-1}(x),$$

where $f_i(x) \in \mathbb{F}_r[x]$ for all i .

Given a cyclic $\mathbb{F}_r$ -linear code C of length n over $\mathbb{F}_q$, we can view the codewords of C as polynomials in $\mathbb{F}_q[x]$. It is often convenient to refer to C as the set

$$\{v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}\}$$

where

$$\mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in C.$$

Note that both C and $\mathbb{F}_s[x]/\langle x^n - 1 \rangle$ are $\mathbb{F}_r[x]$ -modules for all $\mathbb{F}_r \subseteq \mathbb{F}_s$ under the usual polynomial multiplication together with the rule $x^n = 1$.

Lemma 6.1.2. *Let $\mathbb{F}_q = \mathbb{F}_r(\omega)$ be a quadratic extension of $\mathbb{F}_r$. Then the following statements hold:*

- i) Any $(n, r^l)_q$ -cyclic $\mathbb{F}_r$ -linear code C over $\mathbb{F}_q$ has two generators and can be written as $C := \langle a(x) + \omega b(x), c(x) \rangle$, where $a(x)$, $b(x)$, and $c(x)$ are polynomials in $\mathbb{F}_r[x]$, $b(x)$ and $c(x)$ are monic divisors of $x^n - 1$ in $\mathbb{F}_r[x]$, $c(x)$ divides $a(x)(x^n - 1)/b(x)$ in $\mathbb{F}_r[x]$, and $l = 2n - \deg(b(x)) - \deg(c(x))$.*
- ii) If $\langle a'(x) + \omega b'(x), c'(x) \rangle$ is another representation of C then $b'(x) = b(x)$, $c'(x) = c(x)$ and $a'(x) \equiv a(x) \pmod{c(x)}$.*

Proof. To prove *i*), let C be an $(n, r^l)_q$ -cyclic $\mathbb{F}_r$ -linear code over $\mathbb{F}_q$. Define an $\mathbb{F}_r[x]$ -module homomorphism

$$\begin{aligned}\varphi : C &\rightarrow \mathbb{F}_r[x]/\langle x^n - 1 \rangle \text{ sending} \\ v(x) := f_0(x) + \omega f_1(x) &\mapsto f_1(x),\end{aligned}$$

where $f_0(x)$ and $f_1(x)$ are polynomials in $\mathbb{F}_r[x]$.

The zero code is viewed as the one generated by $x^n - 1$. The kernel $\ker(\varphi) := \{v(x) \in C : f_1(x) \equiv 0\} = \{f_0(x) \in C\}$ and the image $\varphi(C) = \{f_1(x) : v(x) \in C\}$ are linear cyclic codes over $\mathbb{F}_r$. Hence, there exist unique, monic generators $c(x)$ and $b(x)$ of minimal degree, respectively, such that $\ker(\varphi) = \langle c(x) \rangle$ and $\varphi(C) = \langle b(x) \rangle$.

Seen as $\mathbb{F}_r[x]$ -modules, for all $a(x) \in \mathbb{F}_r[x]$,

$$\begin{aligned}\text{rank}(C) &= \text{rank}(\langle c(x) \rangle) + \text{rank}(\langle b(x) \rangle) \\ &\leq \text{rank}(\langle c(x) \rangle) + \text{rank}(\langle a(x) + \omega b(x) \rangle).\end{aligned}$$

Thus, C is an $\mathbb{F}_r[x]$ -module generated by $a(x) + \omega b(x)$ and $c(x)$ where $a(x) + \omega b(x)$ is an inverse image of $b(x)$.

Clearly, $c(x)$ and $b(x)$ divide $x^n - 1$ in $\mathbb{F}_r[x]$. Let $g(x) := (x^n - 1)/b(x)$. Since

$$a(x)g(x) \equiv (a(x) + \omega b(x))g(x) \in \ker(\varphi),$$

$c(x)$ divides $a(x)g(x)$ in $\mathbb{F}_r[x]$.

Now, since the set

$$\{x^i(a(x) + \omega b(x)), x^j c(x)\}$$

such that $0 \leq i \leq n - \deg(b(x)) - 1$ and $0 \leq j \leq n - \deg(c(x)) - 1$ is $\mathbb{F}_r$ -linearly independent, we derive $l = 2n - \deg(b(x)) - \deg(c(x))$.

To prove *ii*), assume $C := \langle a'(x) + \omega b'(x), c'(x) \rangle$. Then $b(x)|b'(x)$, $c(x)|c'(x)$ and

$$\begin{aligned} \deg(b'(x)c'(x)) &= \deg(b'(x)) + \deg(c'(x)) \\ &= 2n - l = \deg(b(x)) + \deg(c(x)) = \deg(b(x)c(x)). \end{aligned}$$

Hence, we have $b(x) = b'(x)$ and $c(x) = c'(x)$.

Since $a'(x) + \omega b(x) \in \langle a(x) + \omega b(x), c(x) \rangle$, there exist polynomials $s(x), t(x) \in \mathbb{F}_r[x]$ such that

$$a'(x) + \omega b(x) = s(x)(a(x) + \omega b(x)) + t(x)c(x).$$

By comparing the coefficients on both sides of the equation, $s(x) = 1$. Therefore, $a'(x) = a(x) + t(x)c(x)$, making $a'(x) \equiv a(x) \pmod{c(x)}$. $\square$

Theorem 6.1.3. *Let $\mathbb{F}_q = \mathbb{F}_r(\omega)$ be an extension of degree m over $\mathbb{F}_r$. Any $(n, r^l)_q$ -cyclic $\mathbb{F}_r$ -linear code C over $\mathbb{F}_q$ has m generators, and can be represented as*

$$\begin{aligned} C = & \langle a_{0,0}(x) + \omega a_{0,1}(x) + \dots + \omega^{m-1} a_{0,m-1}(x), \\ & a_{1,0}(x) + \omega a_{1,1}(x) + \dots + \omega^{m-2} a_{1,m-2}(x), \\ & \vdots \quad \quad \quad \vdots \quad \quad \quad \ddots \\ & a_{m-2,0}(x) + \omega a_{m-2,1}(x), \\ & a_{m-1,0}(x) \rangle, \end{aligned}$$

where $a_{i,j}(x) \in \mathbb{F}_r[x]$ for all $0 \leq i \leq m-1$ and $0 \leq j \leq i-1$. Moreover, these polynomials can be chosen such that the following properties hold:

- i)* $a_{i,m-1-i}(x)|(x^n - 1)$ in $\mathbb{F}_r[x]$ for all $0 \leq i \leq m-1$.
- ii)* $a_{i,m-1-i}(x)|(a_{i-1,m-1-i}(x)(x^n - 1)/a_{i-1,m-i}(x))$ in $\mathbb{F}_r[x]$ for all $1 \leq i \leq m-1$.

$$iii) \quad l = mn - \sum_{i=0}^{m-1} \deg(a_{i,m-1-i}(x)).$$

iv) The sets

$$\{a_{i,m-1-i}(x) : 0 \leq i \leq m-1\} \text{ and } \{a_{i,j}(x) \bmod (a_{m-j,j}(x)) : 0 \leq i \leq m-1-j\}$$

are unique for all $1 \leq j \leq m-1$.

Proof. We prove by induction on m . If $m = 2$, the statement follows from Lemma 6.1.2.

Assume that the theorem holds for $m-1$. Let C be an $(n, r^l)_q$ -cyclic $\mathbb{F}_r$ -linear code over $\mathbb{F}_q$ and let $\mathbb{F}_s$ be the field extension of $\mathbb{F}_r$ of degree $m-1$ such that $\mathbb{F}_s = \mathbb{F}_r(\alpha)$.

Let $\phi : C \rightarrow \mathbb{F}_s[x]/\langle x^n - 1 \rangle$ be an $\mathbb{F}_r[x]$ -module homomorphism defined by

$$\begin{aligned} & f_0(x) + \omega f_1(x) + \omega^2 f_2(x) + \cdots + \omega^{m-1} f_{m-1}(x) \\ & \mapsto f_1(x) + \alpha f_2(x) + \cdots + \alpha^{m-2} f_{m-1}(x). \end{aligned}$$

The kernel $\ker(\phi)$ and the image $\phi(C)$ are a linear cyclic code over $\mathbb{F}_r$ and a cyclic $\mathbb{F}_r$ -linear code over $\mathbb{F}_s$, respectively.

Let $a_{m-1,0}(x)$ be the unique monic generator of $\ker(\phi)$ of minimal degree. By the induction hypothesis, $\phi(C)$ has $m-1$ generators, say

$$\begin{aligned} \phi(C) = \langle & a_{0,1}(x) + \alpha a_{0,2}(x) + \cdots + \alpha^{m-2} a_{0,m-1}(x), \\ & a_{1,1}(x) + \alpha a_{1,2}(x) + \cdots + \alpha^{m-3} a_{1,m-2}(x), \\ & \vdots \quad \quad \quad \vdots \quad \quad \quad \ddots \\ & a_{m-3,1}(x) + \alpha a_{m-3,2}(x), \\ & a_{m-2,1}(x) \rangle, \end{aligned}$$

satisfying properties *i*) to *iv*). Therefore, C is an $\mathbb{F}_r[x]$ -module generated by

$$\begin{aligned} & \langle a_{0,0}(x) + \omega a_{0,1}(x) + \dots + \omega^{m-1} a_{0,m-1}(x), \\ & a_{1,0}(x) + \omega a_{1,1}(x) + \dots + \omega^{m-2} a_{1,m-2}(x), \\ & \vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \ddots \\ & a_{m-2,0}(x) + \omega a_{m-2,1}(x), \\ & a_{m-1,0}(x) \rangle, \end{aligned}$$

where $a_{i,0}(x) + \omega a_{i,1}(x) + \dots + \omega^{m-1-i} a_{i,m-1-i}(x)$ is an inverse image of $a_{i,1}(x) + \alpha a_{i,2}(x) + \dots + \alpha^{m-2-i} a_{i,m-1-i}(x)$ for all $0 \leq i \leq m-2$. Clearly, property *i*) holds.

Using a similar reasoning to the proof of Lemma 6.1.2, we obtain the fact that $a_{m-2,0}(x)(x^n - 1)/a_{m-2,1}(x)$ is divisible by $a_{m-1,0}(x)$. Hence, property *ii*) follows.

Since

$$\text{rank}(\ker(\phi)) = n - \deg(a_{m-1,0}(x))$$

and

$$\text{rank}(\phi(C)) = (m-1)n - \sum_{i=0}^{m-2} \deg(a_{i,m-1-i}(x)),$$

we have

$$\begin{aligned} l &= \text{rank}(\ker(\phi)) + \text{rank}(\phi(C)) \\ &= mn - \sum_{i=0}^{m-1} \deg(a_{i,m-1-i}(x)). \end{aligned}$$

This proves property *iii*).

The uniqueness stated in property *iv)* can be obtained from an argument similar to the one used in the proof of *b)* in Lemma 6.1.2. $\square$

To construct an asymmetric quantum code, from a given cyclic $\mathbb{F}_r$ -linear code C over $\mathbb{F}_q$ with representation

$$\begin{aligned} C = \langle & g_0(x) = a_{0,0}(x) + \omega a_{0,1}(x) + \dots + \omega^{m-1} a_{0,m-1}(x), \\ & g_1(x) = a_{1,0}(x) + \omega a_{1,1}(x) + \dots + \omega^{m-2} a_{1,m-2}(x), \\ & \vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \ddots \\ & g_{m-2}(x) = a_{m-2,0}(x) + \omega a_{m-2,1}(x), \\ & g_{m-1}(x) = a_{m-1,0}(x) \rangle, \end{aligned}$$

define D to be the code generated by

$$\{g_0(x)b_0(x), g_1(x)b_1(x), \dots, g_{m-1}(x)b_{m-1}(x)\},$$

where $b_i(x)$ is a divisor of $(x^n - 1)/a_{i,m-1-i}(x)$ for all $0 \leq i \leq m-1$. D is a cyclic $\mathbb{F}_r$ -linear subcode of C .

6.2 Construction from Group Character Codes

Group character codes are introduced in [23] based on elementary abelian 2-groups and are further generalized in [57] to include the case where the group is $(\mathbb{Z}/t\mathbb{Z})^l$ for any positive integer t .

The requirement for nestedness and relevant properties of the dual codes in this class of $\mathbb{F}_q$ -linear codes are well-established. Based on the properties, we can immediately derive pure CSS-like codes, some of which are optimal. For odd q , the symmetric quantum codes derivation based on the results established in [23] can be found in [51, Sect. XIV].

We use the definitions and results in [57] for generality.

For any positive integer t , the elements of $(\mathbb{Z}/t\mathbb{Z})^l$ can be written as $(a_1, \dots, a_l)$ where $0 \leq a_i \leq t-1$ for $1 \leq i \leq l$. Let $\|a\| = \sum_{i=1}^l a_i \in \mathbb{Z}$. Note that $0 \leq \|a\| \leq (t-1)l$ for all $a \in (\mathbb{Z}/t\mathbb{Z})^l$.

Let r be any integer and the set $\mathcal{X}$ be given by

$$\mathcal{X}(r, l; t) = \{a \in (\mathbb{Z}/t\mathbb{Z})^l : \|a\| > r\}. \quad (6.2.1)$$

Observe that $\mathcal{X}(r, l; t) = (\mathbb{Z}/t\mathbb{Z})^l$ for all $r < 0$, and $\mathcal{X}(r, l; t)$ is the null set for all $r \geq l(t-1)$. Hence, we consider only $0 \leq r < l(t-1)$.

To ensure that $\mathbb{F}_q$ contains a t -th root of unity, we require $t|q-1$. Every j satisfying $0 \leq j \leq t^l - 1$ has a unique t -adic expansion of the form

$$j = \sum_{i=1}^l j_i t^{i-1} \text{ where } 0 \leq j_i \leq t-1.$$

Let ζ be a fixed t -th root of unity in $\mathbb{F}_q$. Then the group characters from $(\mathbb{Z}/t\mathbb{Z})^l$ to $\mathbb{F}_q \setminus \{0\}$ are precisely $f_0, f_1, \dots, f_{t^l-1}$, where

$$f_j((a_1, \dots, a_l)) = \zeta^{a_1 j_1 + \dots + a_l j_l}.$$

Definition 6.2.1. Let $\mathbb{F}_q$ be a finite field with $t|q-1$ having a fixed t -th root of unity ζ . Let $\mathbf{c} = (c_0, c_1, \dots, c_{t^l-1}) \in \mathbb{F}_q^{t^l}$. For a given integer r such that $0 \leq r < l(t-1)$, let $C_q(r, l; t)$ denote the q -ary code

$$C_q(r, l; t) = \left\{ \mathbf{c} : \sum_{j=0}^{t^l-1} c_j f_j(x) = 0 \text{ for all } x \in \mathcal{X}(r, l; t) \right\}. \quad (6.2.2)$$

The code $C_q(r, l; 2)$ is exactly the code $C_q(r, l)$ of [23].

The properties of $C_q(r, l; t)$ are known.

Theorem 6.2.2. [57, Th. 8] Writing $r = a(t-1) + b$, where $0 \leq b \leq t-2$, the code $C_q(r, l; t)$ has parameters

$$[t^l, k_l(r), (t-b)t^{l-1-a}]_q, \quad (6.2.3)$$

where

$$k_l(r) = \sum_{i=0}^r \sum_{j=0}^l (-1)^j \binom{l}{j} \binom{l-1+i-jt}{t-1}.$$

The nestedness condition can be deduced directly from Equations (6.2.1) and (6.2.2).

Lemma 6.2.3. If $0 \leq r_1 \leq r_2 < l(t-1)$, then $C_q(r_1, l; t) \subseteq C_q(r_2, l; t)$.

Theorem 6.2.4. [57, Th. 10] The Euclidean dual $(C_q(r, l; t))^{\perp_E}$ of $C_q(r, l; t)$ is monomially equivalent to $C_q(l(t-1) - 1 - r, l; t)$

Hence, $d((C_q(r, l; t))^{\perp_E})$ can be computed explicitly.

Theorem 6.2.5. Let $0 \leq r_1 \leq r_2 < l(t-1)$. Let $a, b, \gamma, \delta, k, d_1$ and d_2 be nonnegative integers satisfying

$$r_2 = a(t-1) + b \text{ where } 0 \leq b < t-1,$$

$$l(t-1) - 1 - r_1 = \gamma(t-1) + \delta \text{ with } 0 \leq \delta < t-1,$$

$$k = k_l r_2 - k_l r_1,$$

$$d_1 = (t-\delta)t^{l-1-\gamma}, \text{ and}$$

$$d_2 = (t-b)t^{l-1-a}.$$

Then there exists an asymmetric CSS code Q with parameters

$$[[t^l, k, \max\{d_1, d_2\} / \min\{d_1, d_2\}]]_q.$$

Proof. We use the standard CSS construction on the nested pair $C_q(r_1, l; t) \subseteq C_q(r_2, l; t)$.

By combining Theorem 6.2.4 and Equation (6.2.3), we get

$$d((C_q(r, l; t))^{\perp_E}) = (t - \delta)t^{l-1-\gamma} = d_1,$$

if we write $l(t - 1) - 1 - r_1 = \gamma(t - 1) + \delta$ with $0 \leq \delta < t - 1$. The other values are clear. $\square$

6.3 BKLC Construction

This construction makes use of Theorem 5.1.1. The strategy is to identify the best-known linear codes stored in the database of MAGMA that contain a codeword of weight equal to the length n for small fields of cardinality q such that $2 \leq q \leq 9$. We call this construction the *BKLC construction*.

Note that sometimes the database does not contain a linear code of specified length n and dimension k satisfying the required condition since this specific requirement has not been recognized as important before. This in no way excludes the possibility of the existence of a linear code that has a codeword of weight n .

The above three constructions and some additional constructions more specific to nested codes over $\mathbb{F}_4$ in the next two chapters provide lower bounds to the best possible pure asymmetric CSS-like codes in terms of parameters. To establish optimality, we use linear programming to derive theoretical upper bounds for some specified parameters (n, q, d_x, d_z) . This will be the main topic of Chapter 9.

Chapter 7

Additional Constructions for 4-ary Asymmetric Quantum Codes

There have been many specific constructions of nested classical codes discussed in previous chapters. In this chapter we discuss some additional constructions of nested pairs of codes over $\mathbb{F}_4$. For brevity, we use the terms *additive codes over $\mathbb{F}_4$* to denote $\mathbb{F}_2$ -linear codes over $\mathbb{F}_4$.

Various families of additive codes over $\mathbb{F}_4$ are used in the construction of many asymmetric quantum codes over $\mathbb{F}_4$. In general, in light of prior chapters on quantum asymmetric MDS codes and on optimal asymmetric CSS-like codes, this chapter presents only codes which have not been previously covered. Exemptions will be given to optimal and good AQECCs derived from self-orthogonal codes since in the case of $\mathbb{F}_4$ -linear codes checking self-orthogonality is equivalent to verifying a simple condition on the weights of the codes.

Section [7.1](#) recalls briefly important known facts regarding additive codes over $\mathbb{F}_4$.

A construction of AQECCs from extremal or optimal self-dual additive codes is given in Section 7.2. A construction from Hermitian self-orthogonal $\mathbb{F}_4$ -linear codes is the topic of Section 7.3. Some previously unknown AQECCs constructed from nested strictly additive codes over $\mathbb{F}_4$ are presented in Section 7.4, exhibiting again the gain of extending the CSS construction to include additive codes. Section 7.5 provides a brief summary and an acknowledgement note.

7.1 Additive Codes over $\mathbb{F}_4$

Let $\mathbb{F}_4 := \{0, 1, \omega, \omega^2 = \bar{\omega}\}$. For $x \in \mathbb{F}_4$, $\bar{x} = x^2$, the conjugate of x . An $\mathbb{F}_2$ -linear code C of length n over $\mathbb{F}_4$ is said to be an additive code over $\mathbb{F}_4$. It has size 2^l for some $0 \leq l \leq 2n$. As a free $\mathbb{F}_2$ -module, C has a basis consisting of l basis vectors. A *generator matrix* of C is an $l \times n$ matrix with entries elements of $\mathbb{F}_4$ whose rows form a basis of C .

Additive codes over $\mathbb{F}_4$ equipped with the trace Hermitian inner product have been studied primarily in connection to designs (e.g. [53]) and to stabilizer quantum codes (e.g. [33] and [48, Sec. 9.10]). It is well known that if C is an additive $(n, 2^l)_4$ -code, then $C^{\perp_{\text{Tr H}}}$ is an additive $(n, 2^{2n-l})_4$ -code.

Remark 7.1.1. *If the code C is $\mathbb{F}_4$ -linear with parameters $[n, k, d]_4$, then $C^{\perp_{\text{H}}} = C^{\perp_{\text{Tr H}}}$. This is because $C^{\perp_{\text{H}}}$ is of size $4^{n-k} = 2^{2n-2k}$ which is also the size of $C^{\perp_{\text{Tr H}}}$. Alternatively, one can invoke [16, Th. 3].*

From here on, we assume the trace Hermitian inner product whenever additive codes over $\mathbb{F}_4$ are discussed and the Hermitian inner product whenever $\mathbb{F}_4$ -linear codes are used.

Two additive codes C_1 and C_2 over $\mathbb{F}_4$ are said to be *equivalent* if there is a map sending the codewords of one code onto the codewords of the other where the map consists of a permutation of coordinates, followed by a scaling of coordinates by elements of $\mathbb{F}_4$, followed by a conjugation of the entries of some of the coordinates.

7.2 From Extremal or Optimal Additive Self-Dual Codes over $\mathbb{F}_4$

As a direct consequence of the CSS-like constructions, we have the following result.

Theorem 7.2.1. *If C is an additive self-dual code of parameters $(n, 2^n, d)_4$, then there exists an $[[n, 0, d_z/d_x]]_4$ asymmetric quantum code Q with $d_z = d_x = d(C^{\perp_{\text{Tr H}}})$.*

Additive self-dual codes over $\mathbb{F}_4$ exist for any length n since the identity matrix I_n clearly generates a self-dual $(n, 2^n, 1)_4$ -code. Any linear self-dual $[n, n/2, d]_4$ -code is also an additive self-dual $(n, 2^n, d)_4$ -code.

Definition 7.2.2. *A self-dual $(n, 2^n, d)_4$ -code C is Type II if all of its codewords have even weight. If C has a codeword of odd weight, then C is Type I.*

It is known (see [64, Sec. 4.2]) that Type II codes of length n exist only if n is even and that a Type I code is not $\mathbb{F}_4$ -linear. There is a bound in [64, Th. 33] on the minimum weight of an additive self-dual code. If d_I and d_{II} are the minimum

weights of Type I and Type II codes of length n , respectively, then

$$d_I \leq \begin{cases} 2\lfloor \frac{n}{6} \rfloor + 1, & \text{if } n \equiv 0 \pmod{6} \\ 2\lfloor \frac{n}{6} \rfloor + 3, & \text{if } n \equiv 0 \pmod{6} \\ 2\lfloor \frac{n}{6} \rfloor + 2, & \text{otherwise} \end{cases}, \quad (7.2.1)$$

$$d_{II} \leq 2\lfloor \frac{n}{6} \rfloor + 2.$$

A code that meets the appropriate bound is called *extremal*. If a code is not extremal yet no code of the given type can exist with a larger minimum weight, then we call the code *optimal*.

The complete classification, up to equivalence, of additive self-dual codes over $\mathbb{F}_4$ up to $n = 12$ can be found in [21]. Classification for $n = 13$ and $n = 14$ is presented in [67]. Many examples of good additive codes for larger values of n are presented in [40], [67], and [68].

Tables 7.1 and 7.2 summarize the results thus far and lists down the resulting asymmetric quantum codes for lengths up to $n = 30$. The subscripts I and II indicates the types of the codes. The superscripts e, o, b indicate the fact that the minimum distance d is extremal, optimal, and best-known (not necessarily extremal or optimal), respectively. The number of codes for each set of given parameters is listed in the column under the heading **num**.

Remark 7.2.3. 1. The unique additive $(12, 2^{12}, 6)_4$ -code is also known as dodecacode. It is well known that the best Hermitian self-dual linear code is of parameters $[12, 6, 4]_4$.

2. In [68], four so-called additive circulant graph codes of parameters $(30, 2^{30}, 12)_4$

Table 7.1: Best-Known Additive Self-Dual Codes over $\mathbb{F}_4$ for even $n \leq 30$ and the Resulting AQECCs

n	d_I	num_I	Ref.	Code Q	d_{II}	num_{II}	Ref.	Code Q
2	1^o	1	[21]	$[[2, 0, 1/1]]_4$	2^e	1	[21]	$[[2, 0, 2/2]]_4$
4	2^e	1	[21]	$[[4, 0, 2/2]]_4$	2^e	2	[21]	$[[4, 0, 2/2]]_4$
6	3^e	1	[21]	$[[6, 0, 3/3]]_4$	4^e	1	[21]	$[[6, 0, 4/4]]_4$
8	4^e	2	[21]	$[[8, 0, 4/4]]_4$	4^e	3	[21]	$[[8, 0, 4/4]]_4$
10	4^e	101	[21]	$[[10, 0, 4/4]]_4$	4^e	19	[21]	$[[10, 0, 4/4]]_4$
12	5^e	63	[21]	$[[12, 0, 5/5]]_4$	6^e	1	[21]	$[[12, 0, 6/6]]_4$
14	6^e	2	[67]	$[[14, 0, 6/6]]_4$	6^e	1020	[67]	$[[14, 0, 6/6]]_4$
16	6^e	≥ 8369	[67]	$[[16, 0, 6/6]]_4$	6^e	≥ 112	[67]	$[[16, 0, 6/6]]_4$
18	7^e	≥ 2	[67]	$[[18, 0, 7/7]]_4$	8^e	≥ 1	[67]	$[[18, 0, 8/8]]_4$
20	8^e	≥ 3	[40]	$[[20, 0, 8/8]]_4$	8^e	≥ 5	[40]	$[[20, 0, 8/8]]_4$
22	8^e	≥ 1	[40]	$[[22, 0, 8/8]]_4$	8^e	≥ 67	[40]	$[[22, 0, 8/8]]_4$
24	8^b	≥ 5	[68]	$[[24, 0, 8/8]]_4$	8^b	≥ 51	[40]	$[[24, 0, 8/8]]_4$
26	8^b	≥ 49	[68]	$[[26, 0, 8/8]]_4$	8^b	≥ 161	[68]	$[[26, 0, 8/8]]_4$
28	10	?	[40]		10^e	≥ 1	[40]	$[[28, 0, 10/10]]_4$
30	11	?	[40]		12^e	≥ 1	[40]	$[[30, 0, 12/12]]_4$

Table 7.2: Best-Known Additive Self-Dual Codes over $\mathbb{F}_4$ for odd $n \leq 30$ and the Resulting AQECCs

n	d_I	num_I	Ref.	Code Q
3	2^e	1	[21]	$[[3, 0, 2/2]]_4$
5	3^e	1	[21]	$[[5, 0, 3/3]]_4$
7	3^o	4	[21]	$[[7, 0, 3/3]]_4$
9	4^e	8	[21]	$[[9, 0, 4/4]]_4$
11	5^e	1	[21]	$[[11, 0, 5/5]]_4$
13	5^o	85845	[67]	$[[13, 0, 5/5]]_4$
15	6^e	≥ 2118	[67]	$[[15, 0, 6/6]]_4$
17	7^e	≥ 2	[67]	$[[17, 0, 7/7]]_4$
19	7^b	≥ 17	[67]	$[[19, 0, 7/7]]_4$
21	8^e	≥ 2	[67]	$[[21, 0, 8/8]]_4$
23	8^b	≥ 2	[40]	$[[23, 0, 8/8]]_4$
25	8^b	≥ 30	[40]	$[[25, 0, 8/8]]_4$
27	8^b	≥ 15	[40]	$[[27, 0, 9/9]]_4$
29	11^e	≥ 1	[40]	$[[29, 0, 11/11]]_4$

are constructed without classification. It is yet unknown if any of these four codes is inequivalent to the one listed in [40].

7.3 From Self-Orthogonal Linear Codes

It is well known (see [48, Th. 1.4.10]) that a linear code C over $\mathbb{F}_4$ is Hermitian self-orthogonal if and only if the weights of its codewords are all even.

Theorem 7.3.1. *If C is a Hermitian self-orthogonal code of parameters $[n, k, d]_4$, then there exists an asymmetric quantum code Q with parameters $[[n, n - 2k, d_z/d_x]]_4$, where*

$$d_x = d_z = d(C^{\perp_H}). \quad (7.3.1)$$

Proof. Seen as an additive code, C is of parameters $(n, 2^{2k}, d)_4$ with $C^{\perp_{\text{Tr H}}}$ being the code $C^{\perp_H}$ seen as an $(n, 2^{2n-2k}, d^{\perp_{\text{Tr H}}})$ additive code (see Remark 7.1.1). Taking $C_1 = C^{\perp_{\text{Tr H}}} = C_2$ to satisfy $C_1^{\perp_{\text{Tr H}}} \subseteq C_2$ completes the proof. $\square$

Example 7.3.2. *Let n be an even positive integer. Consider the repetition code $[n, 1, n]_4$ with weight enumerator $1 + 3Y^n$. Since the weights are all even, this $\mathbb{F}_4$ -linear code is Hermitian self-orthogonal. We then have a quantum MDS code Q with parameters $[[n, n - 2, 2/2]]_4$.*

Table 7.3 below presents the resulting asymmetric quantum codes based on the classification of self-orthogonal $\mathbb{F}_4$ -linear codes of length up to 29 and of dimensions 3 up to 6 as presented in [14]. I. Bouyukliev [11] shared with us the original data used in the said classification plus some additional results for lengths 30 and 31.

Given fixed length n and dimension k , we only consider $[n, k, d]_4$ -codes C with maximal possible value for the minimum distances of their duals. For example, among 12 self-orthogonal $[10, 4, 4]_4$ -codes, there are 4 distinct codes with $d^{\perp_H} = 3$ while the remaining 8 codes have $d^{\perp_H} = 2$. We take only the first 4 codes.

The number of distinct codes that can be used for the construction of the asymmetric quantum codes for each set of given parameters is listed in the fourth column of the table.

In [38, Table 7], examples of $\mathbb{F}_4$ -linear self-dual codes for even lengths $2 \leq n \leq 80$ are presented. Table 7.4 lists down the resulting asymmetric quantum codes for $32 \leq n \leq 80$.

For parameters other than those listed in Table 7.3, we do not have complete classification just yet. The Q-extension program described in [12] can be used to extend the classification effort given sufficient resources. Some classifications based on the optimality of the minimum distances of the codes can be found in [13] and in [70], although when used in the construction of asymmetric quantum codes using our framework, they do not yield good $d_z = d_x$ relative to the length n .

Many other $\mathbb{F}_4$ -linear self-orthogonal codes are known. Examples can be found in [16, Table II], [59], as well as from the list of best known linear codes (BKLC) over $\mathbb{F}_4$ as explained in [35].

Table 7.5 presents more examples of asymmetric quantum codes constructed based on known self-orthogonal linear codes up to length $n = 40$. The list of codes in Table 7.5 is by no means exhaustive. It may be possible to find asymmetric codes with better parameters.

Table 7.3: Good AQECCs from Classified Hermitian Self-Orthogonal $\mathbb{F}_4$ -Linear Codes in [14]

No.	Code C	Code Q	num	Remarks
1	$[10, 3, 6]_4$	$[[10, 4, 3/3]]_4$	1	Optimal
2	$[11, 3, 6]_4$	$[[11, 5, 3/3]]_4$	1	Optimal
3	$[12, 3, 8]_4$	$[[12, 6, 3/3]]_4$	1	Optimal
4	$[12, 4, 6]_4$	$[[12, 4, 4/4]]_4$	1	Optimal
5	$[13, 3, 8]_4$	$[[13, 7, 3/3]]_4$	1	Optimal
6	$[13, 5, 6]_4$	$[[13, 3, 4/4]]_4$	1	Best-Known
7	$[13, 6, 6]_4$	$[[13, 1, 5/5]]_4$	1	Best-Known
8	$[14, 3, 10]_4$	$[[14, 8, 3/3]]_4$	1	Optimal
9	$[14, 4, 8]_4$	$[[14, 6, 4/4]]_4$	1	Optimal
10	$[14, 6, 6]_4$	$[[14, 2, 5/5]]_4$	1	Best-Known
11	$[15, 3, 10]_4$	$[[15, 9, 3/3]]_4$	1	Optimal
12	$[15, 6, 8]_4$	$[[15, 3, 5/5]]_4$	3	Best-Known
13	$[16, 3, 12]_4$	$[[16, 10, 3/3]]_4$	1	Optimal
14	$[16, 5, 8]_4$	$[[16, 6, 4/4]]_4$	519	Best-Known
15	$[17, 4, 12]_4$	$[[17, 9, 4/4]]_4$	1	Optimal
16	$[18, 4, 12]_4$	$[[18, 10, 3/3]]_4$	11	Best-Known
17	$[18, 6, 10]_4$	$[[18, 6, 5/5]]_4$	2	Best-Known
18	$[19, 4, 12]_4$	$[[19, 11, 3/3]]_4$	2570	Best-Known
19	$[21, 3, 16]_4$	$[[21, 15, 3/3]]_4$	1	Optimal
20	$[22, 3, 16]_4$	$[[22, 16, 3/3]]_4$	4	Best-Known
21	$[22, 5, 14]_4$	$[[22, 12, 4/4]]_4$	67	Best-Known
22	$[23, 4, 16]_4$	$[[23, 15, 3/3]]_4$	1	Best-Known
23	$[24, 4, 16]_4$	$[[24, 16, 3/3]]_4$	20456	Best-Known
24	$[25, 4, 16]_4$	$[[25, 17, 3/3]]_4$	19	Best-Known
25	$[26, 4, 18]_4$	$[[26, 18, 3/3]]_4$	14	Best-Known
26	$[28, 4, 20]_4$	$[[28, 20, 3/3]]_4$	1	Best-Known
27	$[29, 4, 20]_4$	$[[29, 21, 3/3]]_4$	11365	Best-Known
28	$[31, 4, 22]_4$	$[[31, 23, 3/3]]_4$	1	Best-Known

Table 7.4: Good AQECCs from Hermitian Self-Dual $\mathbb{F}_4$ -Linear Codes based on [38, Table 7] for $32 \leq n \leq 80$

Code C	Code Q	Code C	Code Q
$[32, 16, 10]_4$	$[[32, 0, 10/10]]_4$	$[58, 29, 14]_4$	$[[58, 0, 14/14]]_4$
$[34, 17, 10]_4$	$[[34, 0, 10/10]]_4$	$[60, 30, 16]_4$	$[[60, 0, 16/16]]_4$
$[36, 18, 12]_4$	$[[36, 0, 12/12]]_4$	$[62, 31, 18]_4$	$[[62, 0, 18/18]]_4$
$[38, 19, 12]_4$	$[[38, 0, 12/12]]_4$	$[64, 32, 16]_4$	$[[64, 0, 16/16]]_4$
$[40, 20, 12]_4$	$[[40, 0, 12/12]]_4$	$[66, 33, 16]_4$	$[[66, 0, 16/16]]_4$
$[42, 21, 12]_4$	$[[42, 0, 12/12]]_4$	$[68, 34, 18]_4$	$[[68, 0, 18/18]]_4$
$[44, 22, 12]_4$	$[[44, 0, 12/12]]_4$	$[70, 35, 18]_4$	$[[70, 0, 18/18]]_4$
$[46, 23, 14]_4$	$[[46, 0, 14/14]]_4$	$[72, 36, 18]_4$	$[[72, 0, 18/18]]_4$
$[48, 24, 14]_4$	$[[48, 0, 14/14]]_4$	$[74, 37, 18]_4$	$[[74, 0, 18/18]]_4$
$[50, 25, 14]_4$	$[[50, 0, 14/14]]_4$	$[76, 38, 18]_4$	$[[76, 0, 18/18]]_4$
$[52, 26, 14]_4$	$[[52, 0, 14/14]]_4$	$[78, 39, 18]_4$	$[[78, 0, 18/18]]_4$
$[54, 27, 16]_4$	$[[54, 0, 16/16]]_4$	$[80, 40, 20]_4$	$[[80, 0, 20/20]]_4$
$[56, 28, 14]_4$	$[[56, 0, 14/14]]_4$		

No.	Code C	Code Q	Ref.
1	$[20, 10, 8]_4$	$[[20, 0, 8/8]]_4$	[38, Table 7]
2	$[22, 11, 8]_4$	$[[22, 0, 8/8]]_4$	[38, Table 7]
3	$[23, 8, 10]_4$	$[[23, 7, 5/5]]_4$	[55]
4	$[23, 10, 8]_4$	$[[23, 3, 6/6]]_4$	[55]
5	$[24, 5, 16]_4$	$[[24, 14, 3/3]]_4$	[35, BKLC]
6	$[24, 8, 10]_4$	$[[24, 8, 5/5]]_4$	[55]
7	$[24, 9, 12]_4$	$[[24, 6, 6/6]]_4$	[35, BKLC]
8	$[24, 12, 8]_4$	$[[24, 0, 8/8]]_4$	[38, Table 7]
9	$[25, 2, 20]_4$	$[[25, 21, 2/2]]_4$	[35, BKLC]
10	$[25, 10, 12]_4$	$[[25, 5, 7/7]]_4$	[55]
11	$[26, 2, 20]_4$	$[[26, 22, 2/2]]_4$	[35, BKLC]
12	$[26, 6, 16]_4$	$[[26, 14, 4/4]]_4$	[35, BKLC]
13	$[26, 10, 10]_4$	$[[26, 6, 6/6]]_4$	[55]
14	$[26, 11, 12]_4$	$[[26, 4, 8/8]]_4$	[35, BKLC]
15	$[27, 6, 16]_4$	$[[27, 15, 3/3]]_4$	[35, BKLC]
16	$[27, 10, 10]_4$	$[[27, 7, 6/6]]_4$	[55]
17	$[27, 12, 12]_4$	$[[27, 3, 9/9]]_4$	[35, BKLC]
18	$[28, 7, 16]_4$	$[[28, 14, 5/5]]_4$	[16, Table II]
19	$[28, 8, 12]_4$	$[[28, 12, 5/5]]_4$	[55]

continued on next page

<i>continued from previous page</i>			
No.	Code C	Code Q	Ref.
20	$[28, 10, 10]_4$	$[[28, 8, 6/6]]_4$	[55]
21	$[29, 8, 16]_4$	$[[29, 13, 5/5]]_4$	[35, BKLC]
22	$[29, 11, 10]_4$	$[[29, 7, 6/6]]_4$	[55]
23	$[29, 14, 12]_4$	$[[29, 1, 11/11]]_4$	[35, BKLC]
24	$[30, 2, 24]_4$	$[[30, 26, 2/2]]_4$	[35, BKLC]
25	$[30, 5, 20]_4$	$[[30, 20, 4/4]]_4$	[61, Table 13.2]
26	$[30, 11, 10]_4$	$[[30, 8, 6/6]]_4$	[55]
27	$[30, 15, 12]_4$	$[[30, 0, 12/12]]_4$	[38, Table 7]
28	$[32, 9, 14]_4$	$[[32, 14, 5/5]]_4$	[55]
29	$[32, 11, 12]_4$	$[[32, 10, 6/6]]_4$	[55]
30	$[33, 7, 20]_4$	$[[33, 19, 4/4]]_4$	[35, BKLC]
31	$[33, 9, 14]_4$	$[[33, 15, 5/5]]_4$	[55]
32	$[33, 10, 16]_4$	$[[33, 13, 6/6]]_4$	[35, BKLC]
33	$[33, 12, 14]_4$	$[[33, 9, 7/7]]_4$	[35, BKLC]
34	$[33, 15, 12]_4$	$[[33, 3, 9/9]]_4$	[35, BKLC]
35	$[34, 9, 18]_4$	$[[34, 16, 6/6]]_4$	[55]
36	$[34, 13, 14]_4$	$[[34, 8, 8/8]]_4$	[35, BKLC]
37	$[34, 16, 12]_4$	$[[34, 2, 10/10]]_4$	[35, BKLC]
38	$[35, 5, 24]_4$	$[[35, 25, 3/3]]_4$	[35, BKLC]
39	$[35, 8, 20]_4$	$[[35, 19, 5/5]]_4$	[35, BKLC]
40	$[35, 11, 14]_4$	$[[35, 13, 6/6]]_4$	[55]
41	$[35, 17, 12]_4$	$[[35, 1, 11/11]]_4$	[35, BKLC]
42	$[36, 9, 16]_4$	$[[36, 18, 4/4]]_4$	[55]
43	$[36, 11, 14]_4$	$[[36, 14, 6/6]]_4$	[55]
44	$[37, 9, 20]_4$	$[[37, 19, 5/5]]_4$	[35, BKLC]
45	$[37, 18, 12]_4$	$[[37, 1, 11/11]]_4$	[35, BKLC]
46	$[38, 6, 24]_4$	$[[38, 26, 3/3]]_4$	[35, BKLC]
47	$[38, 11, 18]_4$	$[[38, 16, 6/6]]_4$	[35, BKLC]
48	$[39, 12, 18]_4$	$[[39, 15, 7/7]]_4$	[35, BKLC]
49	$[39, 4, 28]_4$	$[[39, 31, 3/3]]_4$	[35, BKLC]
50	$[39, 7, 24]_4$	$[[39, 25, 4/4]]_4$	[35, BKLC]
51	$[40, 5, 28]_4$	$[[40, 30, 4/4]]_4$	[16, Table II]
52	$[40, 15, 16]_4$	$[[40, 10, 7/7]]_4$	[35, BKLC]

Table 7.5: More AQECCs from Hermitian Self-orthogonal $\mathbb{F}_4$ -Linear Codes for $n \leq 40$.

For lengths larger than $n = 40$, [42] provides some known $\mathbb{F}_4$ -linear codes of dimension 6 that belong to the class of *quasi-twisted codes*. Based on the weight distribution of these codes [42, Table 3], we know which ones of them are self-orthogonal. They

Table 7.6: AQECCs from Hermitian Self-orthogonal Quasi-Twisted Codes Found in [42]

Code C	Code Q	Code C	Code Q
$[48, 6, 32]_4$	$[[48, 36, 3/3]]_4$	$[144, 6, 104]_4$	$[[144, 132, 3/3]]_4$
$[78, 6, 56]_4$	$[[78, 66, 4/4]]_4$	$[150, 6, 108]_4$	$[[150, 138, 3/3]]_4$
$[102, 6, 72]_4$	$[[102, 90, 3/3]]_4$	$[160, 6, 116]_4$	$[[160, 148, 3/3]]_4$
$[112, 6, 80]_4$	$[[112, 100, 3/3]]_4$	$[182, 6, 132]_4$	$[[182, 170, 3/3]]_4$
$[120, 6, 86]_4$	$[[120, 108, 4/4]]_4$	$[192, 6, 138]_4$	$[[192, 180, 3/3]]_4$
$[132, 6, 94]_4$	$[[132, 120, 3/3]]_4$	$[200, 6, 144]_4$	$[[200, 188, 3/3]]_4$

yield the 12 quantum codes listed in Table 7.6.

Another family of codes that we can use is the *MacDonald codes*, commonly denoted by $C_{k,u}$ with $k > u > 0$. The MacDonald codes are linear codes with parameters $[(q^k - q^u)/(q - 1), k, q^{k-1} - q^{u-1}]_q$. Some historical background and a construction of their generator matrices can be found in [7]. It is known that these codes are *two-weight codes*. That is, they have nonzero codewords of only two possible weights. In [15, Figures 1a and 2a], the MacDonald codes are labeled SU1. There are $q^k - q^{k-u}$ codewords of weight $q^{k-1} - q^{u-1}$ and $q^{k-u} - 1$ codewords of weight q^{k-1} .

The MacDonald codes satisfy the equality of the *Griesmer bound* which says that, for any $[n, k \geq 1, d]_q$ -code,

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil. \quad (7.3.2)$$

Example 7.3.3. For $q = 4, k > u > 1$, the MacDonald codes are self-orthogonal since both $4^{k-1} - 4^{u-1}$ and 4^{k-1} are even. For a $[(4^k - 4^u)/3, k, 4^{k-1} - 4^{u-1}]_4$ -code $C_{k,u}$, we know (see [7, Lemma 4]) that $d(C_{k,u}^{\perp_H}) \geq 3$. Using $C_{k,u}$ and applying Theorem 7.3.1, we get an AQECC Q with parameters

$$[[(4^k - 4^u)/3, ((4^k - 4^u)/3) - 2k, (\geq 3)/(\geq 3)]_4.$$

For $k \leq 5$, Table 7.7 present explicit parameters.

Table 7.7: AQECCs from MacDonald codes

k	u	Code C	Code Q	Remark
3	2	$[16, 3, 12]_4$	$[[16, 10, 3/3]]_4$	See Table 7.3
4	3	$[64, 4, 48]_4$	$[[64, 56, 3/3]]_4$	
4	2	$[80, 4, 60]_4$	$[[80, 72, 3/3]]_4$	
5	4	$[256, 5, 192]_4$	$[[256, 246, 3/3]]_4$	
5	3	$[320, 5, 240]_4$	$[[320, 310, 3/3]]_4$	
5	2	$[336, 5, 252]_4$	$[[336, 326, 3/3]]_4$	

7.4 From Nested Additive Codes over $\mathbb{F}_4$

To show the gain that we can get over the construction which is based solely on $\mathbb{F}_4$ -linear codes, we exhibit asymmetric quantum codes which are derived from nested additive codes. Here we exclude the additive cyclic construction discussed in a prior chapter.

An example of asymmetric quantum code with $k > 0$ can be derived from a self-orthogonal additive cyclic code listed as Entry 3 in [16, Table I]. The code is of parameters $(21, 2^{16}, 9)_4$ yielding a $[[21, 5, 6/6]]_4$ quantum code Q . In a similar manner, a $[[23, 12, 4/4]]_4$ quantum code can be derived from Entry 5 of the same table.

The next three subsections present more systematic approaches to finding good asymmetric quantum codes based on nested additive codes.

7.4.1 From Circulant Codes

Instead of using additive cyclic codes, a subfamily which is called *additive circulant* $(n, 2^n)_4$ -code in [40] can be used for ease of computation. An additive circulant code C has as a generator matrix G the complete cyclic shifts of just one codeword $\mathbf{v} = (v_1, v_2, \dots, v_n)$. We call G the *cyclic development of $\mathbf{v}$* . More explicitly, G is

Table 7.8: Best-Known AQECCs from Additive Circulant Codes for $n \leq 30$

No.	n	Generator $\mathbf{v}$	del	Code Q
1	19	$(1, 0, \omega, \bar{\omega}, 1, \bar{\omega}, \omega, 0, 1)$	4	$[[19, 2, 7/4]]_4$
2	22	$(\omega, \omega, \omega, \omega, 1, 1, \bar{\omega}, \omega, 0, \omega, \omega, 0, \omega, \omega, 1, 1)$	4	$[[22, 2, 8/5]]_4$
3			10	$[[22, 5, 8/3]]_4$
4	23	$(1, \omega, \omega, 1, \bar{\omega}, 1, \omega, \omega, 1)$	2	$[[23, 1, 8/4]]_4$
5			6	$[[23, 3, 8/3]]_4$
6			6	$[[25, 3, 8/4]]_4$
7	27	$(1, 0, \omega, 1, \omega, \bar{\omega}, \omega, 1, \omega, 0, 1)$	1	$[[27, 0.5, 8/5]]_4$
8	27	$(1, 0, \omega, \omega, 1, \bar{\omega}, 1, \omega, \omega, 0, 1)$	5	$[[27, 2.5, 8/4]]_4$
9			6	$[[27, 3, 8/3]]_4$
10	28	$(\bar{\omega}, \omega, \bar{\omega}, 1, \bar{\omega}, 1, \omega, \omega, \bar{\omega}, \bar{\omega}, \omega, \omega, 0, 1, 1)$	1	$[[28, 0.5, 10/7]]_4$
11			2	$[[28, 1, 10/5]]_4$
12			11	$[[28, 5.5, 10/3]]_4$
13			3	$[[29, 1.5, 11/6]]_4$
14			8	$[[29, 4, 11/4]]_4$
15			12	$[[29, 6, 11/3]]_4$
16	30	$(\bar{\omega}, 0, \bar{\omega}, \omega, 1, \omega, 0, \bar{\omega}, \omega, 0, 1, \omega, 1, 1, 0, 1)$	5	$[[30, 2.5, 12/6]]_4$
17			6	$[[30, 3, 12/5]]_4$

given by

$$G = \begin{pmatrix} v_1 & v_2 & v_3 & \dots & v_{n-1} & v_n \\ v_n & v_1 & v_2 & \dots & v_{n-2} & v_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ v_2 & v_3 & v_4 & \dots & v_n & v_1 \end{pmatrix}. \quad (7.4.1)$$

To generate a subcode of a circulant extremal self-dual code C we delete the rows of its generator matrix G starting from the last row, the first row being the generating codeword $\mathbf{v}$. We record the best possible combinations of the size of the resulting code Q and $\{d_z, d_x\}$.

Table 7.8 summarizes the finding for $n \leq 30$. Zeros on the right of each generating codeword are omitted. The number of last rows to be deleted to obtain the desired subcode is given in the column denoted by **del**.

7.4.2 From 4-Circulant and Bordered 4-Circulant Codes

Following [40], a 4-circulant additive $(n, 2^n)_4$ -code of even length n has the following generator matrix:

$$G = \begin{pmatrix} I_{\frac{n}{2}} & A_{\frac{n}{2}} \\ B_{\frac{n}{2}} & I_{\frac{n}{2}} \end{pmatrix} \quad (7.4.2)$$

where $I_{\frac{n}{2}}$ is an identity matrix of size $n/2$ and $A_{\frac{n}{2}}, B_{\frac{n}{2}}$ are circulant matrices of the form given in Equation (7.4.1).

Starting from a generator matrix G_C of an additive 4-circulant code C , a matrix G_D is constructed by deleting the last r rows of G_C to derive an additive subcode D of C .

Let $\mathbf{d} = (\omega, \dots, \omega)$ and $\mathbf{c}$ be the transpose of $\mathbf{d}$. A bordered 4-circulant additive $(n, 2^n)_4$ -code of odd length n has the following generator matrix:

$$G = \begin{pmatrix} e & \mathbf{1} & \mathbf{d} \\ \mathbf{1} & I_{\frac{n-1}{2}} & A_{\frac{n-1}{2}} \\ \mathbf{c} & B_{\frac{n-1}{2}} & I_{\frac{n-1}{2}} \end{pmatrix} \quad (7.4.3)$$

where e is one of $0, 1, \omega$, or $\overline{\omega}$, and $A_{\frac{n-1}{2}}, B_{\frac{n-1}{2}}$ are circulant matrices.

We perform the procedure of constructing a subcode D of C by deleting the rows of G_C , starting from the last row. For $n \leq 30$, the three relatively good AQECCs found can be seen in Table 7.9. As before, under the column denoted by A, B we list down the generating codewords for the matrices A and B , in that order.

Remark 7.4.1. A similar procedure has been done to the generator matrices of s -extremal additive codes found in [8] and [68] as well as to the formally self-dual additive codes of [43]. So far we have found no new or better asymmetric codes from these sources.

Table 7.9: Good AQECCs from Additive Bordered 4-Circulant Codes for $n \leq 30$

n	e	A, B	del	Code Q
23	ω	$(\overline{\omega}, 1, \overline{\omega}, \omega, \omega, 1, 1, 0, 0, 0, 0),$ $(0, \overline{\omega}, \omega, \omega, \omega, \omega, \overline{\omega}, 1, 0, 1, \omega)$	1	$[[23, 0.5, 8/5]]_4$
23	ω	$(\overline{\omega}, 1, \overline{\omega}, \omega, \omega, 1, 1, 0, 0, 0, 0),$ $(0, \overline{\omega}, \omega, \omega, \omega, \omega, \overline{\omega}, 1, 0, 1, \omega)$	4	$[[23, 2, 8/4]]_4$
25	ω	$(\omega, 1, 1, \omega, \overline{\omega}, 1, 0, 1, 0, 0, 0, 0),$ $(1, \overline{\omega}, \overline{\omega}, \omega, \omega, \overline{\omega}, \omega, \overline{\omega}, 1, 0, \overline{\omega}, \omega)$	4	$[[25, 2, 8/5]]_4$

Deleting the rows of G_C in a more careful way than just doing so consecutively starting from the last row may yield new or better asymmetric quantum codes. The process, however, is more time consuming.

Let C be a bordered 4-circulant code of length $n = 23$ with generator matrix G_C in the form given in Equation (7.4.3) with $e = \omega$ and with the circulant matrices A, B generated by, respectively,

$$(\overline{\omega}, 1, \overline{\omega}, \omega, \omega, 1, 1, 0, 0, 0, 0), \text{ and}$$

$$(0, \overline{\omega}, \omega, \omega, \omega, \omega, \overline{\omega}, 1, 0, 1, \omega).$$

Let G_D be G_C with rows 3,6,7,9, and 11 deleted. Then, we get a $[[23, 2.5, 8/4]]_4$ -code Q .

7.4.3 From Two Proper Subcodes

In the previous two subsections, the larger code C is an additive self-dual code while the subcode D of C is constructed by deleting rows of G_C . New AQECCs can be constructed from two nested proper subcodes of an additive self-dual code. The following example illustrate this fact.

Example 7.4.2. Let C be a self-dual Type I additive code of length 25 labeled $C_{25,4}$

in $[40]$ with generating vector

$$\mathbf{v} = (1, 1, \omega, 0, 1, \overline{\omega}, 1, 0, \omega, 1, 1, 0, 0, \dots, 0).$$

Let G_C be the generator matrix of C from the cyclic development of $\mathbf{v}$. Derive the generator matrices G_D of D and G_E of E by deleting, respectively, the last 5 and 6 rows of G_C . An asymmetric $[[25, 0.5, 9/4]]_4$ -code Q is hence constructed.

7.5 Conclusions and Open Problems

In this chapter we have discussed additional constructions of nested pairs of additive codes over $\mathbb{F}_4$. Many 4-ary AQECCs are constructed. These codes either have the same parameters as the optimal pure asymmetric CSS-like codes or are, thus far, the best-known.

Extension to codes over $\mathbb{F}_9$ or $\mathbb{F}_{16}$ is worth considering. More generally, establishing propagation rules may help us find better bounds on the parameters.

As a final note, we thank Iliya Bouyukliev, Yuena Ma, and Ruihu Li for sharing their data on known Hermitian self-orthogonal $\mathbb{F}_4$ -codes.

Chapter 8

From Skew-Cyclic Codes to 4-ary Asymmetric Quantum Codes

This chapter is based on [29], which is a joint work with San Ling, Patrick Solé and Olfa Yemen. In the scenario where we need to detect a lot of Z -errors while the detection for X -errors is not critical, say when $d_x = 2$ can be safely assumed, the construction discussed below can be of considerable value.

The class of *skew-cyclic codes* was introduced in [9]. These linear codes have the property of being invariant under the operation of cyclic shift composed with overall conjugation. Demanding an ideal structure on the codes forces us, over $\mathbb{F}_4$, to work in even lengths only. By relaxing this structure to that of a module [10], it is now possible to deal with skew-cyclic codes of any lengths.

A mapping S is introduced to map any skew-cyclic codes of length n over $\mathbb{F}_4$ into codes of length $2n$ which are invariant under a coordinate permutation denoted by σ . The permutation σ is a cyclic permutation for n odd and a product of two cycles of

equal length for n even.

Besides these structural properties, the mapping S has interesting duality properties and preserves nestedness. These allow us to construct AQECCs following the CSS-like method under the trace Hermitian inner product given in [28] or, more generally, in [27].

The material is organized as follows. In Section 8.1, we state some basic definitions and properties of the classical codes under consideration. Section 8.2 introduces the mapping S and its basic properties. The definition of and some algebraic background on module θ -cyclic codes are discussed in Section 8.3. The study of the images of these codes under the mapping S is also given.

In Section 8.4, an analysis of the weight enumerators is performed. This is important in understanding the parameters of the asymmetric quantum codes that can be obtained under the mapping S . Two systematic constructions of asymmetric quantum codes are given in Section 8.5. The one based on best-known linear codes is presented in Subsection 8.5.1 while the other one, based on concatenated Reed-Solomon codes, is given in Subsection 8.5.2. The last section contains conclusions and open problems.

8.1 Preliminaries

Recall that an $(n, M, d)_q$ -code C is said to be *cyclic* if C is invariant under the cyclic shift. That is, whenever $\mathbf{v} = (v_0, v_1, \dots, v_{n-2}, v_{n-1}) \in C$, we have

$$\mathbf{v}' = (v_{n-1}, v_0, v_1, \dots, v_{n-2}) \in C.$$

Let n be a positive integer and let $1 \leq l < n$ be a divisor of n . An $(n, M, d)_q$ -code

C is *quasi-cyclic of index l* or *l -quasi-cyclic* if

$$\mathbf{v}'' = (v_{n-l}, v_{n-l+1}, \dots, v_{n-1}, v_0, v_1, \dots, v_{n-l-1}) \in C$$

whenever $\mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in C$. In particular, a 1-quasi-cyclic code is a cyclic code.

To be more specific, let $\mathbb{F}_4 := \{0, 1, \omega, \omega^2 = \bar{\omega}\}$. For $x \in \mathbb{F}_4$, set $\bar{x} = x^2$, the conjugate of x . Let n be a positive integer and $\mathbf{u} = (u_0, u_1, \dots, u_{n-1}), \mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_4^n$. We consider the space $\mathbb{F}_4^n$ under the Hermitian and the trace Hermitian inner products.

Definition 8.1.1. *A code C of length n over $\mathbb{F}_4$ is said to be an additive code if C is $\mathbb{F}_2$ -linear. Hence, in constructing AQECCs, we use the trace Hermitian inner product.*

If C is an additive $(n, 2^k, d)_4$ -code, then $C^{\perp_{\text{Tr H}}}$ is an additive code with parameters $(n, 2^{2n-k}, d^{\perp_{\text{Tr H}}})_4$ satisfying

$$W_{C^{\perp_{\text{Tr H}}}}(X, Y) = \frac{1}{|C|} W_C(X + 3Y, X - Y). \quad (8.1.1)$$

8.2 The Mapping S on Codes over $\mathbb{F}_4$

Additive codes over $\mathbb{F}_4$ have been studied primarily in connection to designs (e.g. [53]) and to stabilizer quantum codes (e.g. [48, Sec. 9.10]).

Note that if the code C is $\mathbb{F}_4$ -linear with parameters $[n, k, d]_4$, then $C^{\perp_{\text{H}}} = C^{\perp_{\text{Tr H}}}$. This is because $C^{\perp_{\text{H}}} \subseteq C^{\perp_{\text{Tr H}}}$ and $C^{\perp_{\text{H}}}$ is of size $4^{n-k} = 2^{2n-2k}$ which is also the size of $C^{\perp_{\text{Tr H}}}$.

We are now ready to introduce the mapping S in aid of later constructions.

Definition 8.2.1. In $\mathbb{F}_4^n$, define the mapping

$$\begin{aligned} S : \mathbb{F}_4^n &\rightarrow \mathbb{F}_4^{2n} \\ (v_0, v_1, \dots, v_{n-1}) &\mapsto (v_0, \overline{v_0}, v_1, \overline{v_1}, \dots, v_{n-1}, \overline{v_{n-1}}). \end{aligned} \tag{8.2.1}$$

It is immediately clear from the definition that S is an $\mathbb{F}_2$ -linear map, injective but not surjective.

Example 8.2.2. The mapping S is not $\mathbb{F}_4$ -linear. Consider $n = 2$ and $\mathbf{u} = (\omega, \overline{\omega})$.

We have

$$\begin{aligned} S(\mathbf{u}) &= (\omega, \overline{\omega}, \overline{\omega}, \omega), \\ S(\omega \cdot \mathbf{u}) &= S((\overline{\omega}, 1)) = (\overline{\omega}, \omega, 1, 1) \\ &\neq \omega \cdot S(\mathbf{u}) = (\overline{\omega}, 1, 1, \overline{\omega}). \end{aligned}$$

Lemma 8.2.3. Let C be an $(n, M, d)_4$ -code. For all $\mathbf{u} \in C$ we have

$$\text{wt}_H(S(\mathbf{u})) = 2 \text{wt}_H(\mathbf{u}) \text{ and } d(S(C)) = 2d(C).$$

Proof. For all $u \in \mathbb{F}_4$, $S(u) = (u, \overline{u})$. Now, $\overline{u} = 0$ if and only if $u = 0$. □

The mapping S is therefore a scaled isometry for the Hamming metric that preserves the code size. It sends an additive $(n, M, d)_4$ -code C to an additive code $S(C)$ with parameters $(2n, M, 2d)_4$.

Lemma 8.2.4. If C is an additive $(n, M, d)_4$ -cyclic code then $S(C)$ is an additive $(2n, M, 2d)_4$ -2-quasi-cyclic code.

Proof. Since C is cyclic,

$$\mathbf{v} = (v_0, \dots, v_{n-2}, v_{n-1}) \in C \text{ if and only if } \mathbf{v}' = (v_{n-1}, v_0, \dots, v_{n-2}) \in C.$$

Applying S yields

$$S(\mathbf{v}) = (v_0, \overline{v_0}, \dots, v_{n-2}, \overline{v_{n-2}}, v_{n-1}, \overline{v_{n-1}}) \in S(C),$$

$$S(\mathbf{v}') = (v_{n-1}, \overline{v_{n-1}}, v_0, \overline{v_0}, \dots, v_{n-2}, \overline{v_{n-2}}) \in S(C).$$

By definition, $S(C)$ is an additive 2-quasi-cyclic code. □

Proposition 8.2.5. *Given an additive $(n, M, d)_4$ -code C , $S(C) \subseteq S(C)^{\perp_{\text{TrH}}}$.*

Proof. Let $\mathbf{v} = (v_0, v_1, \dots, v_{n-1}), \mathbf{u} = (u_0, u_1, \dots, u_{n-1}) \in C$. Then

$$\langle S(\mathbf{v}), S(\mathbf{u}) \rangle_{\text{TrH}} = \sum_{i=0}^{n-1} (v_i \overline{u_i} + \overline{v_i} u_i) + \sum_{i=0}^{n-1} (\overline{v_i} u_i + v_i \overline{u_i}) = 2 \sum_{i=0}^{n-1} (v_i \overline{u_i} + \overline{v_i} u_i) = 0.$$

□

8.3 Module θ -Cyclic Codes over $\mathbb{F}_4$

The motivation for our definition of *module θ -cyclic codes* comes from [9] and [10].

Given $\mathbb{F}_q$ and an automorphism θ of $\mathbb{F}_q$, we can define a ring structure on the set

$$\mathcal{R} = \mathbb{F}_q[X, \theta] = \{a_n X^n + \dots + a_1 X + a_0 : a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}.$$

In $\mathcal{R}$, the addition operation is the usual polynomial addition and the multiplication is defined by the extension to all elements of $\mathcal{R}$, by associativity and distributivity, the basic rule $Xa = \theta(a)X$ for all $a \in \mathbb{F}_q$.

The ring $\mathcal{R}$ is a left and right Euclidean ring whose left and right ideals are principal. Right division means that for nonzero $f(X), g(X) \in \mathcal{R}$, there exist unique polynomials $Q_r(X), R_r(X) \in \mathcal{R}$ such that

$$f(X) = Q_r(X) \cdot g(X) + R_r(X)$$

with $\deg(R_r(X)) < \deg(g(X))$ or $R_r(X) = 0$. If $R_r(X) = 0$, then $g(X)$ is a *right divisor* of $f(X)$ in $\mathcal{R}$.

Definition 8.3.1. [10, cf. Defs. 1 and 3] Let θ be an automorphism of $\mathbb{F}_q$. Let $f(X) \in \mathcal{R}$ be of degree n . If $I = (f(X))$ is a two-sided ideal of $\mathcal{R}$, then an ideal θ -code C is a left ideal $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ where $g(X)$ is a right divisor of $f(X)$ in $\mathcal{R}$. If $f(X) = X^n - 1$, we call the ideal θ -code corresponding to the left ideal $\mathcal{R}g(X)/\mathcal{R}(X^n - 1) \subset \mathcal{R}/\mathcal{R}(X^n - 1)$ an ideal θ -cyclic code.

A module θ -code C is a left $\mathcal{R}$ -submodule $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ where $g(X)$ is a right divisor of $f(X)$ in $\mathcal{R}$. Furthermore,

1. if $f(X) = X^n - c$, with $c \in \mathbb{F}_q$, we call the module θ -code corresponding to the left $\mathcal{R}$ -module $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ a module θ -constacyclic code;
2. if $f(X) = X^n - 1$, we call the module θ -code corresponding to the left $\mathcal{R}$ -module $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ a module θ -cyclic code.

The length of the module θ -code C is $n = \deg(f(X))$ and its dimension is $k = \deg(f(X)) - \deg(g(X))$. If the minimum distance of C is d , the code C is said to be of type $[n, k, d]_q$.

If the codewords of C are identified with the list of the coefficients of the remainder of a right division by $f(X)$ in $\mathcal{R}$, the elements of $\mathcal{R}g(X)/\mathcal{R}f(X)$ are all of the left multiples of $g(X) = g_r X^r + \dots + g_1 X + g_0$.

Thus, a generator matrix G of the corresponding module θ -code of length $n =$

$\deg(f(X))$ is given by

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_{r-1}) & \theta(g_r) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \theta^{n-r-1}(g_0) & \cdots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix} \quad (8.3.1)$$

depending only on $g(X)$ and n .

Theorem 8.3.2. *A module θ -cyclic code C_θ has the following property*

$$(v_0, v_1, \dots, v_{n-2}, v_{n-1}) \in C_\theta \Rightarrow (\theta(v_{n-1}), \theta(v_0), \theta(v_1), \dots, \theta(v_{n-2})) \in C_\theta. \quad (8.3.2)$$

Proof. The proof of this property for an ideal θ -cyclic code C is established in [9, Theorem 1]. The same proof works when we replace ideal by module. $\square$

Since a module θ -cyclic code C_θ has a representation in the skew polynomial ring $\mathcal{R} = \mathbb{F}_q[X, \theta]$ (see [10]), when θ is fixed, we call C_θ a *skew-cyclic code*.

We consider, for the rest of the paper, the Frobenius automorphism defined in $\mathbb{F}_4$ by $\theta(x) = x^2 = \bar{x}$ for $x \in \mathbb{F}_4$. Let $[2n]$ denote the set $\{1, 2, \dots, 2n\}$. Let $\sigma = \tau \circ T^2$ be a permutation on $[2n]$ where T is the cyclic shift module $2n$ and $\tau = (12)(34) \dots (2n-1, 2n)$. Since T^2 and τ commute, σ can be written as $T^2 \circ \tau$ as well. We denote the identity permutation by (1).

Let Σ be the permutation on elements of $\mathbb{F}_4^{2n}$ induced by σ . That is, for $\mathbf{v} = (v_1, v_2, \dots, v_{2n}) \in \mathbb{F}_4^{2n}$,

$$\Sigma(\mathbf{v}) = (v_{\sigma(1)}, v_{\sigma(2)}, \dots, v_{\sigma(2n)}). \quad (8.3.3)$$

Lemma 8.3.3. *Given an $(n, M, d)_4$ -skew-cyclic code C_θ , the code $S(C_\theta)$ is invariant under Σ .*

Proof. Let $\mathbf{v} = (v_1, v_2, \dots, v_{2n}) \in S(C_\theta)$. Let $\mathbf{u} = (u_1, u_2, \dots, u_n) \in C_\theta$ such that

$$\mathbf{v} = (u_1, \overline{u_1}, u_2, \overline{u_2}, \dots, u_n, \overline{u_n}) = S(\mathbf{u}).$$

Since C_θ is a skew-cyclic code, we have

$$\overline{\mathbf{u}} := (\overline{u_n}, \overline{u_1}, \dots, \overline{u_{n-1}}) \in C_\theta.$$

Hence,

$$\begin{aligned} \Sigma(\mathbf{v}) &= (\overline{u_n}, u_n, \overline{u_1}, u_1, \dots, \overline{u_{n-1}}, u_{n-1}) \\ &= S((\overline{u_n}, \overline{u_1}, \dots, \overline{u_{n-1}})), \end{aligned}$$

implying $\Sigma(S(C_\theta)) \subset S(C_\theta)$. □

Lemma 8.3.4. *The order of σ is $2n$ if n is odd and n if n is even.*

Proof. For $1 \leq i \leq 2n$, σ follows the following rule

$$\sigma : i \mapsto \begin{cases} i + 3 & (\text{mod } 2n) \text{ if } i \text{ is odd} \\ i + 1 & (\text{mod } 2n) \text{ if } i \text{ is even} \end{cases}. \quad (8.3.4)$$

With computation done modulo $2n$, observe that if i is odd, then $\sigma(i) = i + 3$ and $\sigma^2(i) = \sigma(i + 3) = i + 4$. If i is even, then $\sigma(i) = i + 1$ and $\sigma^2(i) = \sigma(i + 1) = i + 4$. Hence, $\sigma^2 = T^4$.

Now, let $n = 2l$ for some positive integer l . We have

$$\sigma^n = \sigma^{2l} = T^{4l} = T^{2n} = (1),$$

the identity permutation. For $1 \leq k < n$, if $k = 2i$, then

$$\sigma^k = \sigma^{2i} = T^{4i} \neq (1)$$

since $4i = 2k < 2n$. If $k = 2i + 1$,

$$\sigma^k = \sigma^{2i+1} = T^{4i} \circ \tau \neq (1)$$

since σ^k sends 1 to $4i + 1 \neq 1$. Consequently, the order of σ is n .

In the case where $n = 2l + 1$, we have

$$\sigma^{2n} = (T^{2n})^2 = (1).$$

To show minimality, we first note that $\sigma^n = \tau$ since

$$\sigma^n = \sigma^{2l+1} = T^{4l} \circ \sigma = T^{2n-2} \circ (\tau \circ T^2) = T^{2n-2} \circ (T^2 \circ \tau) = \tau.$$

Consider the following two subcases. For $1 \leq k < n$, the same argument as in the even case above shows that $\sigma^k \neq (1)$. For $n + 1 \leq k < 2n$,

$$\sigma^k = \sigma^n \circ \sigma^{k-n} = \tau \circ \sigma^{k-n} \neq (1).$$

We conclude that the order of σ is $2n$. □

For conciseness, we adopt the following expressions following Lemma 8.3.4.

1. For n odd, σ is the following cycle of length $2n$

$$\sigma = (1, \sigma(1), \sigma^2(1), \dots, \sigma^{2n-2}(1), \sigma^{2n-1}(1)). \quad (8.3.5)$$

2. Since $\sigma^k(1) \neq 2$ for all $0 \leq k \leq n - 1$, for n even, σ can be written as the following product of two cycles, each of length n

$$\sigma = (1, \sigma(1), \sigma^2(1), \dots, \sigma^{n-1}(1))(2, \sigma(2), \sigma^2(2), \dots, \sigma^{n-1}(2)). \quad (8.3.6)$$

When it is clear from the context, we write C instead of C_θ .

Theorem 8.3.5. *Let C be an $[n, k, d]_4$ -skew-cyclic code. If n is odd then $S(C)$ is equivalent to an additive $(2n, 2^{2k}, 2d)_4$ -cyclic code C' . If n is even then $S(C)$ is equivalent to an additive $(2n, 2^{2k}, 2d)_4$ -2-quasi-cyclic code C' .*

Proof. Recall that the permutation σ on $[2n]$ induces a permutation Σ on the vectors of $\mathbb{F}_4^{2n}$. Consider first the case n odd where Equation (8.3.5) holds. Define the permutation σ' by

$$\sigma' = \begin{pmatrix} 1 & 2 & \dots & 2n-1 & 2n \\ \sigma^{2n-1}(1) & \sigma^{2n-2}(1) & \dots & \sigma(1) & 1 \end{pmatrix}. \quad (8.3.7)$$

It is clear that for all $1 \leq j \leq 2n$,

$$\sigma'(j) = \sigma^{2n-j}(1). \quad (8.3.8)$$

The permutation σ' induces a permutation Σ' acting on the elements of $\mathbb{F}_4^{2n}$. For $\mathbf{v} = (v_1, v_2, \dots, v_{2n}) \in \mathbb{F}_4^{2n}$,

$$\Sigma'(\mathbf{v}) = (v_{\sigma'(1)}, v_{\sigma'(2)}, \dots, v_{\sigma'(2n)}). \quad (8.3.9)$$

To show that $\Sigma'(S(C))$ is cyclic we must prove that for all codewords $\mathbf{v} \in S(C)$, $T(\Sigma'(\mathbf{v})) \in \Sigma'(S(C))$ where T is the vector cyclic shift. We only need to show that

$$T(\Sigma'(\mathbf{v})) = \Sigma'(\Sigma(\mathbf{v})). \quad (8.3.10)$$

since $\Sigma(S(C)) = S(C)$ by Lemma 8.3.3. Let us start from the right hand side. By definition,

$$\Sigma(\mathbf{v}) = (v_{\sigma(1)}, v_{\sigma(2)}, \dots, v_{\sigma(2n)}) := (v'_1, v'_2, \dots, v'_{2n}) = \mathbf{v}'. \quad (8.3.11)$$

From Equation (8.3.8), we know that

$$\Sigma'(\Sigma(\mathbf{v})) = (v'_{\sigma'(1)}, v'_{\sigma'(2)}, \dots, v'_{\sigma'(2n)}) = (v'_{\sigma^{2n-1}(1)}, v'_{\sigma^{2n-2}(1)}, \dots, v'_{\sigma^1(1)}, v'_{\sigma^0(1)}).$$

By Equation (8.3.11),

$$\Sigma'(\Sigma(\mathbf{v})) = (v_1, v_{\sigma^{2n-1}(1)}, \dots, v_{\sigma^2(1)}, v_{\sigma(1)}). \quad (8.3.12)$$

Moving on to the left hand side. Equation (8.3.8) implies

$$\Sigma'(\mathbf{v}) = (v_{\sigma'(1)}, v_{\sigma'(2)}, \dots, v_{\sigma'(2n)}) = (v_{\sigma^{2n-1}(1)}, v_{\sigma^{2n-2}(1)}, \dots, v_{\sigma(1)}, v_1).$$

Applying the vector cyclic shift T on $\Sigma'(\mathbf{v})$ completes the proof of this case.

For n even, Equation (8.3.6) holds. Let the permutation σ'' be given by

$$\sigma'' = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 2n-1 & 2n \\ \sigma^{n-1}(1) & \sigma^{n-1}(2) & \sigma^{n-2}(1) & \sigma^{n-2}(2) & \dots & \sigma^0(1) & \sigma^0(2) \end{pmatrix}. \quad (8.3.13)$$

Let b be an integer such that $1 \leq b \leq n$. For all $1 \leq j \leq 2n$,

$$\sigma''(j) = \begin{cases} \sigma^{n-b}(1) & \text{if } j = 2b-1 \\ \sigma^{n-b}(2) & \text{if } j = 2b \end{cases}. \quad (8.3.14)$$

Let Σ'' be the permutation on vectors in $\mathbb{F}_4^{2n}$ induced by σ'' . Applying Σ'' and by Equation (8.3.11), we have

$$\begin{aligned} \Sigma''(\Sigma(\mathbf{v})) &= (v'_{\sigma''(1)}, v'_{\sigma''(2)}, v'_{\sigma''(3)}, v'_{\sigma''(4)}, \dots, v'_{\sigma''(2n-1)}, v'_{\sigma''(2n)}) \\ &= (v'_{\sigma^{n-1}(1)}, v'_{\sigma^{n-1}(2)}, v'_{\sigma^{n-2}(1)}, v'_{\sigma^{n-2}(2)}, \dots, v'_{\sigma(1)}, v'_{\sigma(2)}, v'_1, v'_2) \end{aligned}$$

by Equation (8.3.14). Now, Equation(8.3.11) allows us to write

$$\Sigma''(\Sigma(\mathbf{v})) = (v_1, v_2, v_{\sigma^{n-1}(1)}, v_{\sigma^{n-1}(2)}, \dots, v_{\sigma^2(1)}, v_{\sigma^2(2)}, v_{\sigma(1)}, v_{\sigma(2)}).$$

Since

$$\begin{aligned} \Sigma''(\mathbf{v}) &= (v_{\sigma''(1)}, v_{\sigma''(2)}, v_{\sigma''(3)}, v_{\sigma''(4)}, \dots, v_{\sigma''(2n-3)}, v_{\sigma''(2n-2)}, v_{\sigma''(2n-1)}, v_{\sigma''(2n)}) \\ &= (v_{\sigma^{n-1}(1)}, v_{\sigma^{n-1}(2)}, v_{\sigma^{n-2}(1)}, v_{\sigma^{n-2}(2)}, \dots, v_{\sigma(1)}, v_{\sigma(2)}, v_1, v_2) \end{aligned}$$

and $\Sigma(S(C)) = S(C)$, we get

$$T^2(\Sigma''(\mathbf{v})) = \Sigma''(\Sigma(\mathbf{v})) \in \Sigma''(S(C)).$$

Thus, $\Sigma''(S(C))$ is a 2-quasi-cyclic code. This completes the entire proof. $\square$

Example 8.3.6. For $n = 4$, we have

$$\sigma = (1, 4, 5, 8)(2, 3, 6, 7) \text{ and}$$

$$\sigma'' = (1, 8, 2, 7)(3, 5, 4, 6).$$

Following [9, Example 2], let C be a $[4, 2, 3]_4$ -skew-cyclic code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & \bar{\omega} & \omega \\ 0 & 1 & \omega & \bar{\omega} \end{pmatrix}. \quad (8.3.15)$$

Verifying that $S(C)$ is invariant under Σ is immediate.

Choose $\mathbf{u} = (1, 0, \bar{\omega}, \omega) \in C$. Let $\mathbf{v} = S(\mathbf{u}) = (1, 1, 0, 0, \bar{\omega}, \omega, \omega, \bar{\omega})$. Then

$$\begin{aligned} \Sigma''(\Sigma(\mathbf{v})) &= (v_{\sigma^4(1)}, v_{\sigma^4(2)}, v_{\sigma^3(1)}, v_{\sigma^3(2)}, v_{\sigma^2(1)}, v_{\sigma^2(2)}, v_{\sigma(1)}, v_{\sigma(2)}) \\ &= (v_1, v_2, v_8, v_7, v_5, v_6, v_4, v_3) = (1, 1, \bar{\omega}, \omega, \bar{\omega}, \omega, 0, 0), \text{ while} \\ \Sigma''(\mathbf{v}) &= (v_{\sigma^3(1)}, v_{\sigma^3(2)}, v_{\sigma^2(1)}, v_{\sigma^2(2)}, v_{\sigma(1)}, v_{\sigma(2)}, v_1, v_2) \\ &= (v_8, v_7, v_5, v_6, v_4, v_3, v_1, v_2) = (\bar{\omega}, \omega, \bar{\omega}, \omega, 0, 0, 1, 1). \end{aligned}$$

Explicit computation up to length $n = 21$ shows that the only examples of module θ -cyclic codes of odd lengths are the usual cyclic codes.

Example 8.3.7. For $n = 7$, we have

$$\sigma = (1, 4, 5, 8, 9, 12, 13, 2, 3, 6, 7, 10, 11, 14) \text{ and}$$

$$\sigma' = (1, 14)(2, 11, 8, 13, 4, 7)(3, 10, 9, 12, 5, 6).$$

Let C be a $[7, 4, 3]_4$ -skew-cyclic code with generator matrix

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \quad (8.3.16)$$

Let $\mathbf{v} = (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$. Then

$$\begin{aligned}
\Sigma'(\Sigma(\mathbf{v})) &= (v_1, v_{14}, v_{11}, v_{10}, v_7, v_6, v_3, v_2, v_{13}, v_{12}, v_9, v_8, v_5, v_4) \\
&= (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1), \text{ while} \\
\Sigma'(\mathbf{v}) &= (v_{\sigma^{13}(1)}, v_{\sigma^{12}(1)}, v_{\sigma^{11}(1)}, v_{\sigma^{10}(1)}, \dots, v_{\sigma(1)}, v_1) \\
&= (v_{14}, v_{11}, v_{10}, v_7, v_6, v_3, v_2, v_{13}, v_{12}, v_9, v_8, v_5, v_4, v_1) \\
&= (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1).
\end{aligned}$$

Theorem 8.3.5, our main result in this section, reveals the structural connection between skew-cyclic codes under the mapping S and additive cyclic or additive 2-quasi-cyclic codes, depending on the parity of the length. Combined with the orthogonality property that the mapping S induces, we can further make a connection to asymmetric quantum codes via the CSS-like construction under the trace Hermitian inner product.

As explained in [9] and in [10], there are two major gains of using module θ -codes. First, there is more flexibility and generality in constructing (linear) codes without increasing the complexity of the encoding and decoding process. The notion of q -cyclic codes, introduced in [31], for instance, covers ideal θ -cyclic codes with θ limited to the Frobenius automorphism only.

More important to the agenda of constructing asymmetric quantum codes is the second gain, which is the minimum distance improvement. Exhaustive search on module θ -codes up to certain length has yielded linear codes with better parameters. More systematically, the BCH approach of constructing codes with a prescribed lower bound on the minimum distance can be extended to module θ -codes as well. Section 3 of [10] contains the construction details. The resulting improvements have been added to the database of *best-known linear codes* (BKLC) of MAGMA [6].

For the remaining of this chapter, we will concentrate on constructing asymmetric quan-

tum codes with $d_z \geq d_x = 2$ and see how the mapping S can be used as an aid in the construction process.

8.4 Analysis on the Weight Enumerators

In this section, the weight enumerators of $S(C)$ and of $S(C)^{\perp_{\text{Tr H}}}$ are analyzed. This analysis will be useful in determining d_x .

Let A_i be the number of codewords of weight i in an additive $(n, M, d)_4$ -code C . Then the weight enumerators of $S(C)$ and $S(C)^{\perp_{\text{Tr H}}}$ can be written in terms of the weight enumerator of C with the help of Equation (8.1.1)

$$W_{S(C)}(X, Y) = \sum_{i=0}^n A_i X^{2(n-i)} Y^{2i}, \quad (8.4.1)$$

$$W_{S(C)^{\perp_{\text{Tr H}}}}(X, Y) = \frac{1}{|S(C)|} W_{S(C)}(X + 3Y, X - Y). \quad (8.4.2)$$

More explicitly,

$$W_{S(C)^{\perp_{\text{Tr H}}}}(X, Y) = \frac{1}{M} \sum_{i=0}^n A_i L_i, \quad (8.4.3)$$

where L_i is given by

$$\left(\sum_{j=0}^{n-i} \binom{n-i}{j} X^{n-i-j} (3Y)^j \right)^2 \left(\sum_{l=0}^i \binom{i}{l} X^{i-l} (-Y)^l \right)^2. \quad (8.4.4)$$

Denote the number of codewords of weight i in the code $C^{\perp_{\text{Tr H}}}$ by $A_i^{\perp_{\text{Tr H}}}$. By using the *Pless power moments* with $q = 4$ (see [48, p. 259] for the linear version), we have

$$\sum_{i=0}^n A_i = |C| = M, \quad (8.4.5)$$

$$\sum_{i=0}^n i A_i = \frac{M}{4} (3n - A_1^{\perp_{\text{Tr H}}}), \quad (8.4.6)$$

$$\sum_{i=0}^n i^2 A_i = \frac{M}{4^2} \left\{ (9n^2 + 3n) - (6n - 2)A_1^{\perp_{\text{Tr H}}} + 2A_2^{\perp_{\text{Tr H}}} \right\}. \quad (8.4.7)$$

If we further assume that $A_1^{\perp_{\text{Tr H}}} = A_2^{\perp_{\text{Tr H}}} = 0$, then the following statements hold for Equation (8.4.2).

1. The coefficient of $Y^0 X^{2n}$ is $\frac{1}{M} \sum_{i=0}^n A_i = 1$.

2. The coefficient of $Y X^{2n-1}$ is

$$\frac{1}{M} \sum_{i=0}^n A_i (2 \cdot (n - i) \cdot 3 - 2i) = \frac{1}{M} \sum_{i=0}^n A_i (6n - 8i) = 6n - 4^{-1} \cdot 8(3n) = 0$$

by Equation (8.4.6).

3. The coefficient of $Y^2 X^{2n-2}$ is

$$\begin{aligned} & \frac{1}{M} \sum_{i=0}^n A_i (18n^2 - 48ni + 32i^2 - 9n + 8i) \\ &= \frac{18n^2 - 9n}{M} \sum_{i=0}^n A_i + \frac{8 - 48n}{M} \sum_{i=0}^n i A_i + \frac{32}{M} \sum_{i=0}^n i^2 A_i = 3n \end{aligned}$$

by Equations (8.4.6) and (8.4.7).

If we rewrite

$$W_{S(C)^{\perp_{\text{Tr H}}}}(X, Y) = \sum_{i=0}^{2n} B_i X^{2n-i} Y^i, \quad (8.4.8)$$

then $B_0 = 1$, $B_1 = 0$, and $B_2 = 3n$. This is true for any additive $(n, M, d)_4$ -code C with $d(C^{\perp_{\text{Tr H}}}) \geq 3$. If $d(C^{\perp_{\text{Tr H}}}) = 1$, then $B_1 = 2A_1^{\perp_{\text{Tr H}}} > 0$. If $d(C^{\perp_{\text{Tr H}}}) = 2$, then $B_1 = 0$ and $B_2 = 3n + 4A_2^{\perp_{\text{Tr H}}} > 0$.

As a direct consequence of Proposition 8.2.5 and the above analysis on the weight enumerators, we derive the following result.

Proposition 8.4.1. *Given any additive $(n, M, d)_4$ -code C with $d(C^{\perp_{\text{Tr H}}}) \geq 2$, there exists an asymmetric quantum code Q with parameters $[[2n, k, 2/2]]_4$ where $k = \log_4 \left(\frac{|S(C)^{\perp_{\text{Tr H}}}|}{|S(C)|} \right)$.*

Proof. By Proposition 8.2.5, $S(C) \subseteq S(C)^{\perp_{\text{Tr H}}}$. Hence, we can take $C_1 = C_2 = S(C)^{\perp_{\text{Tr H}}}$. The values $d_z = d_x = 2$ follow from the analysis on the weight enumerators. $\square$

The parameters of the resulting code Q based on the construction in Proposition 8.4.1 are not so good. Fortunately, the mapping S preserves nestedness. This fact can be used to derive asymmetric quantum codes with better parameters.

Theorem 8.4.2. *Let C be an additive $(n, M_1, d_1)_4$ -code such that $d(C^{\perp_{\text{Tr H}}}) \geq 2$. Let D be an additive $(n, M_2, d_2)_4$ -code satisfying $C \subseteq D$. Then there exists an asymmetric quantum code Q with parameters $[[2n, \log_4 \left(\frac{M_2}{M_1} \right), 2d_2/2]]_4$.*

Proof. Take $C_1 = S(C)^{\perp_{\text{Tr H}}}$ and $C_2 = S(D)$. The code $S(C)$ is an additive $(2n, M_1, 2d_1)_4$ -code. Similarly, $S(D)$ is an additive code of parameters $(2n, M_2, 2d_2)_4$. The values for d_z and d_x follow from the discussion on the weight enumerators above. $\square$

Example 8.4.3. *Let $C = D$ be the $[n, 1, n]_4$ -repetition code generated by the all one vector $\mathbf{1} = (1, \dots, 1)$. It can be directly verified that $d(C^{\perp_{\text{Tr H}}}) = 2$. Hence, we get an asymmetric quantum MDS code Q with parameters $[[2n, 0, 2n/2]]_4$ by Theorem 8.4.2.*

Example 8.4.4. *Consider the $[4, 2, 3]_4$ -module θ -cyclic code D with generator matrix G in Equation (8.3.15) above. The code D contains the $[4, 1, 4]_4$ -repetition code C generated by $\mathbf{1}$. Letting $C = C_1^{\perp_{\text{Tr H}}}$ and $D = C_2$ results in a $[[4, 1, 3/2]]_4$ -asymmetric quantum MDS code. Under the mapping S , by Theorem 8.4.2, we arrive at an $[[8, 1, 6/2]]_4$ -asymmetric quantum code.*

The investigation on self-dual module θ -code yields new Hermitian self-dual linear $\mathbb{F}_4$ -codes with parameters $[50, 25, 14]_4$ and $[58, 29, 16]_4$. These codes are listed down in [10, Table 3]. They can be used to derive asymmetric quantum codes Q with parameters $[[50, 0, 14/14]]_4$ and $[[58, 0, 16/16]]_4$ following [28, Th. 7.1]. The latter code improves on the $[[58, 0, 14/14]]_4$ -code in Table 7.4.

The next section presents two systematic constructions of asymmetric quantum codes with $d_z \geq d_x = 2$ by using the database of BKLC and by applying the mapping S on concatenated Reed-Solomon codes, respectively.

8.5 Two Constructions

Under the mapping S , Theorem 8.4.2 says that while we cannot improve on $d_x = 2$, we can relax the condition on the inner code C to possibly improve on the size of Q as well as on d_z . Our aim, then, is to choose the smallest possible subcode C of D such that $d(C^{\perp_{\text{TrH}}}) \geq 2$ while keeping the size and the minimum distance of D relatively large.

Note that there is no additive $(n, 2, d)_4$ -code with $d(C^{\perp_{\text{TrH}}}) \geq 2$. The smallest additive code with $d(C^{\perp_{\text{TrH}}}) = 2$ is an $(n, 4, n)_4 = [n, 1, n]_4$ -code C consisting of the scalar multiples of a codeword $\mathbf{v}$ of weight n . Since this code C is MDS, its dual $C^{\perp_{\text{TrH}}} = C^{\perp_{\text{H}}}$ is of parameters $[n, n-1, 2]_4$.

8.5.1 From Best-Known Linear Codes

Let n, k be fixed with $2 \leq k \leq n-1$. The strategy here is to consider the best-known linear code D of length n and dimension k stored in the MAGMA database and check if the code contains codewords of weight n and put them in a set R . If R is non-empty, we choose an arbitrary codeword $\mathbf{v} \in R$ and construct a subcode $C \subset D$ of parameters $[n, 1, n]_4$ whose elements are the four scalar multiples of $\mathbf{v}$.

Based on the codes C and D , two asymmetric quantum codes can be derived, one directly without the mapping S by letting $C_1^{\perp_{\text{TrH}}} = C$ and $C_2 = D$ and another from Theorem 8.4.2 under the mapping S . We label the first quantum code Q while the second one Q_S .

Theorem 8.5.1. *For $n \geq 3, n \in \mathbb{N}$, we have an $[[n, n-2, 2/2]]_4$ -asymmetric quantum MDS code.*

Proof. A general proof for the existence of an $[[n, n-2, 2/2]]_q$ -asymmetric quantum MDS code is already given in [69, Cor. 3.4]. Here we present a simple constructive proof for $q = 4$. A cyclic code D with parameters $[n, n-1, 2]_4$ can be constructed by using $X + 1$ as its generator polynomial. Its minimum distance is two since the check polynomial is $1 + X + \dots + X^{n-1}$. Moreover, we know that D has codewords of length n . One such codeword can be chosen to form an $[n, 1, n]_4$ -code C . Choosing $C_1^{\perp_{\text{TrH}}} = C$ and $C_2 = D$ brings us to the conclusion. $\square$

For a fixed n , it is not guaranteed that for all $k \in \{2, \dots, n-2\}$, the best-known linear code with parameters $[n, k, d]_4$ has codewords of weight n . For example, there is no codeword of weight 6 in the best-known $[6, 4, 2]_4$ -code stored in the database of MAGMA that we use here.

Table 8.1 lists down the resulting quantum codes for $n = 4$ to $n = 20$ based on the list of best-known linear codes with parameters $[n, k]_4$ invoked under the command BKLC in MAGMA. We exclude the case of $k = n-1$ in light of Theorem 8.5.1 and the case of $k = 1$ due to [28, Ex. 8.2]. The process can of course be done for larger values of n if so desired.

Remark 8.5.2. *Aside from its nice structural property, the advantage of using the mapping S can be seen, for instance, from the fact that we have the $[[18, 2, 12/2]]_4$ -code Q_S which cannot be derived directly from MAGMA's list of best-known linear codes for $n = 18$. Similarly for the following Q_S codes:*

$$\begin{aligned} & [[30, 2, 22/2]]_4, \quad [[30, 3, 20/2]]_4, \quad [[32, 3, 22/2]]_4, \quad [[38, 4, 22/2]]_4, \\ & [[40, 4, 24/2]]_4, \quad [[42, 4, 26/2]]_4, \quad [[44, 4, 28/2]]_4, \quad [[46, 4, 28/2]]_4. \end{aligned}$$

Table 8.1: Asymmetric QECC from BKLC

n	Code Q	Code Q_S	n	Code Q	Code Q_S
4	$[[4, 1, 3/2]]_4$	$[[8, 1, 6/2]]_4$	15	$[[15, 7, 6/2]]_4$	$[[30, 7, 12/2]]_4$
5	$[[5, 2, 3/2]]_4$	$[[10, 2, 6/2]]_4$		$[[15, 8, 5/2]]_4$	$[[30, 8, 10/2]]_4$
6	$[[6, 2, 4/2]]_4$	$[[12, 2, 8/2]]_4$		$[[15, 10, 4/2]]_4$	$[[30, 10, 8/2]]_4$
7	$[[7, 2, 4/2]]_4$	$[[14, 2, 8/2]]_4$		$[[15, 11, 3/2]]_4$	$[[30, 11, 6/2]]_4$
	$[[7, 3, 3/2]]_4$	$[[14, 3, 6/2]]_4$	16	$[[16, 2, 12/2]]_4$	$[[32, 2, 24/2]]_4$
8	$[[8, 1, 6/2]]_4$	$[[16, 1, 12/2]]_4$		$[[16, 3, 11/2]]_4$	$[[32, 3, 22/2]]_4$
	$[[8, 2, 5/2]]_4$	$[[16, 2, 10/2]]_4$		$[[16, 6, 8/2]]_4$	$[[32, 6, 16/2]]_4$
	$[[8, 3, 4/2]]_4$	$[[16, 3, 8/2]]_4$		$[[16, 7, 7/2]]_4$	$[[32, 7, 14/2]]_4$
	$[[8, 4, 3/2]]_4$	$[[16, 4, 6/2]]_4$		$[[16, 8, 6/2]]_4$	$[[32, 8, 12/2]]_4$
9	$[[9, 2, 6/2]]_4$	$[[18, 2, 12/2]]_4$		$[[16, 9, 5/2]]_4$	$[[32, 9, 10/2]]_4$
	$[[9, 3, 5/2]]_4$	$[[18, 3, 10/2]]_4$		$[[16, 11, 4/2]]_4$	$[[32, 11, 8/2]]_4$
	$[[9, 4, 4/2]]_4$	$[[18, 4, 8/2]]_4$		$[[16, 12, 3/2]]_4$	$[[32, 12, 6/2]]_4$
	$[[9, 5, 3/2]]_4$	$[[18, 5, 6/2]]_4$	17	$[[17, 5, 9/2]]_4$	$[[34, 5, 18/2]]_4$
10	$[[10, 3, 6/2]]_4$	$[[20, 3, 12/2]]_4$		$[[17, 8, 7/2]]_4$	$[[34, 8, 14/2]]_4$
	$[[10, 4, 5/2]]_4$	$[[20, 4, 10/2]]_4$		$[[17, 9, 6/2]]_4$	$[[34, 9, 12/2]]_4$
	$[[10, 5, 4/2]]_4$	$[[20, 5, 8/2]]_4$		$[[17, 10, 5/2]]_4$	$[[34, 10, 10/2]]_4$
	$[[10, 6, 3/2]]_4$	$[[20, 6, 6/2]]_4$		$[[17, 12, 4/2]]_4$	$[[34, 12, 8/2]]_4$
11	$[[11, 2, 7/2]]_4$	$[[22, 2, 14/2]]_4$		$[[17, 13, 3/2]]_4$	$[[34, 13, 6/2]]_4$
	$[[11, 4, 6/2]]_4$	$[[22, 4, 12/2]]_4$	18	$[[18, 5, 10/2]]_4$	$[[36, 5, 20/2]]_4$
	$[[11, 5, 5/2]]_4$	$[[22, 5, 10/2]]_4$		$[[18, 6, 9/2]]_4$	$[[36, 6, 18/2]]_4$
	$[[11, 6, 4/2]]_4$	$[[22, 6, 8/2]]_4$		$[[18, 8, 8/2]]_4$	$[[36, 8, 16/2]]_4$
	$[[11, 7, 3/2]]_4$	$[[22, 7, 6/2]]_4$		$[[18, 10, 6/2]]_4$	$[[36, 10, 12/2]]_4$
12	$[[12, 2, 8/2]]_4$	$[[24, 2, 16/2]]_4$		$[[18, 11, 5/2]]_4$	$[[36, 11, 10/2]]_4$
	$[[12, 3, 7/2]]_4$	$[[24, 3, 14/2]]_4$		$[[18, 12, 4/2]]_4$	$[[36, 12, 8/2]]_4$
	$[[12, 5, 6/2]]_4$	$[[24, 5, 12/2]]_4$		$[[18, 14, 3/2]]_4$	$[[36, 14, 6/2]]_4$
	$[[12, 7, 4/2]]_4$	$[[24, 7, 8/2]]_4$	19	$[[19, 4, 11/2]]_4$	$[[38, 4, 22/2]]_4$
	$[[12, 8, 3/2]]_4$	$[[24, 8, 6/2]]_4$		$[[19, 5, 10/2]]_4$	$[[38, 5, 20/2]]_4$
13	$[[13, 2, 9/2]]_4$	$[[26, 2, 18/2]]_4$		$[[19, 6, 9/2]]_4$	$[[38, 6, 18/2]]_4$
	$[[13, 4, 7/2]]_4$	$[[26, 4, 14/2]]_4$		$[[19, 8, 8/2]]_4$	$[[38, 8, 16/2]]_4$
	$[[13, 5, 6/2]]_4$	$[[26, 5, 12/2]]_4$		$[[19, 9, 7/2]]_4$	$[[38, 9, 14/2]]_4$
	$[[13, 6, 5/2]]_4$	$[[26, 6, 10/2]]_4$		$[[19, 11, 6/2]]_4$	$[[38, 11, 12/2]]_4$
	$[[13, 8, 4/2]]_4$	$[[26, 8, 8/2]]_4$		$[[19, 12, 5/2]]_4$	$[[38, 12, 10/2]]_4$
	$[[13, 9, 3/2]]_4$	$[[26, 9, 6/2]]_4$		$[[19, 13, 4/2]]_4$	$[[38, 13, 8/2]]_4$
14	$[[14, 2, 10/2]]_4$	$[[28, 2, 20/2]]_4$		$[[19, 15, 3/2]]_4$	$[[38, 15, 6/2]]_4$
	$[[14, 3, 9/2]]_4$	$[[28, 3, 18/2]]_4$	20	$[[20, 4, 12/2]]_4$	$[[40, 4, 24/2]]_4$
	$[[14, 4, 8/2]]_4$	$[[28, 4, 16/2]]_4$		$[[20, 5, 11/2]]_4$	$[[40, 5, 22/2]]_4$
	$[[14, 5, 7/2]]_4$	$[[28, 5, 14/2]]_4$		$[[20, 6, 10/2]]_4$	$[[40, 6, 20/2]]_4$
	$[[14, 6, 6/2]]_4$	$[[28, 6, 12/2]]_4$		$[[20, 7, 9/2]]_4$	$[[40, 7, 18/2]]_4$
	$[[14, 7, 5/2]]_4$	$[[28, 7, 10/2]]_4$		$[[20, 9, 8/2]]_4$	$[[40, 9, 16/2]]_4$
	$[[14, 9, 4/2]]_4$	$[[28, 9, 8/2]]_4$		$[[20, 10, 7/2]]_4$	$[[40, 10, 14/2]]_4$
	$[[14, 10, 3/2]]_4$	$[[28, 10, 6/2]]_4$		$[[20, 12, 6/2]]_4$	$[[40, 12, 12/2]]_4$
15	$[[15, 2, 11/2]]_4$	$[[30, 2, 22/2]]_4$		$[[20, 13, 5/2]]_4$	$[[40, 13, 10/2]]_4$
	$[[15, 3, 10/2]]_4$	$[[30, 3, 20/2]]_4$		$[[20, 14, 4/2]]_4$	$[[40, 14, 8/2]]_4$
	$[[15, 6, 7/2]]_4$	$[[30, 6, 14/2]]_4$		$[[20, 16, 3/2]]_4$	$[[40, 16, 6/2]]_4$

8.5.2 From Concatenated Reed-Solomon Codes

Let m be a positive integer. Concatenation is used to obtain codes over $\mathbb{F}_q$ from codes over an extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. A general method of performing concatenation is presented in [58, Sec. 6.3] and in [60, Ch. 10].

Our strategy here is to construct nested codes $C \subset D$ over $\mathbb{F}_4$ from nested codes $A \subset B$ over $\mathbb{F}_{4^m}$. We then use the codes C and D and the mapping S to get a quantum code Q .

The field $\mathbb{F}_{4^m}$ can be viewed as an $\mathbb{F}_4$ -vector space with basis $\{\beta_1, \dots, \beta_m\}$. Then, an element $x \in \mathbb{F}_{4^m}$ can be written uniquely as

$$x = \sum_{j=1}^m a_j \beta_j \text{ with } a_j \in \mathbb{F}_4.$$

We define a mapping $\phi : \mathbb{F}_{4^m} \rightarrow \mathbb{F}_4^m$ given by $x \mapsto (a_1, \dots, a_m)$. This mapping is a bijective $\mathbb{F}_4$ -linear transformation and extends naturally to the mapping ϕ^*

$$\begin{aligned} \phi^* : \mathbb{F}_{4^m}^N &\rightarrow \mathbb{F}_4^{mN} \\ (x_1, \dots, x_n) &\mapsto (\phi(x_1), \dots, \phi(x_n)). \end{aligned} \tag{8.5.1}$$

If A is an $[N, K, D]_{4^m}$ -code and letting $C = \phi^*(A)$, then it is easy to verify that C is an $[mN, mK, \geq D]_4$ -code. Moreover, the mapping ϕ^* preserves nestedness by its $\mathbb{F}_4$ -linearity. That is, if an $[N, K_1, D_1]_{4^m}$ -code A is a subcode of an $[N, K_2, D_2]_{4^m}$ -code B , then $C = \phi^*(A)$ is a subcode of $D = \phi^*(B)$ as codes over $\mathbb{F}_4$.

Let $q = 4^m$ and $\alpha_1, \dots, \alpha_{q-1}$ be the nonzero elements of $\mathbb{F}_q$. It is well-known (see, e.g., [60, Ch. 10 and Ch.11]) that the $[q, k, q - k + 1]_q$ -extended Reed-Solomon

(henceforth, RS) code B has a parity check matrix

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{q-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{q-1}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{q-k-1} & \alpha_2^{q-k-1} & \dots & \alpha_{q-1}^{q-k-1} & 0 \end{pmatrix}. \quad (8.5.2)$$

Let A be the $[q, 1, q]_q$ -repetition code generated by $\mathbf{1} = (1, \dots, 1)$. For $1 \leq j \leq q-2$, the sum $s = \sum_{l=1}^{q-1} \alpha_l^j = 0$. To see this, we choose α a primitive element of $\mathbb{F}_q$. Then $\alpha^j s = \sum_{l=1}^{q-1} (\alpha \cdot \alpha_l)^j = s$. Since $\alpha^j \neq 1$, we conclude that $s = 0$. This implies that $A \subset B$.

Note that we can choose an $\mathbb{F}_4$ -basis $\{\beta_1, \dots, \beta_m\}$ of $\mathbb{F}_q$ such that a generator matrix of $C' = \phi^*(A)$ is given by the $m \times mq$ matrix $G = (I_m | I_m | \dots | I_m)$ where I_m is the $m \times m$ identity matrix. Hence, C' is of parameters $[mq, m, q]_4$. Define C to be the $[mq, 1, mq]_4$ -repetition code subset of C' . This is valid since we know that $\mathbf{1} = (1, \dots, 1) \in C'$. The code $D = \phi^*(B)$ is an $[mq, mk, d' \geq (q - k + 1)]_4$ -code that contains C . Repeating the proof of Theorem 8.4.2 yields the following result.

Theorem 8.5.3. *Let m be a positive integer, $q = 4^m$, and $1 \leq k \leq q$. Then there exists a $[[2mq, mk - 1, (\geq 2(q - k + 1))/2]]_4$ -asymmetric quantum code Q .*

Remark 8.5.4. *For a specific value of m and a given basis $\{\beta_1, \dots, \beta_m\}$, $d' = d(D)$ can be explicitly computed. As noted in [60, Ch. 10], a change of basis may change the weight distribution and even the minimum weight of the code D .*

Example 8.5.5. *For $m = 2$ and $1 \leq k \leq 16$ we get the $[[64, k', d_z/2]]_4$ -quantum codes listed in Table 8.2.*

Table 8.2: $[[64, k', d_z/2]]_4$ -code Q from $[16, k, 16 - k + 1]_{16}$ -extended RS codes

k	1	2	3	4	5	6	7	8
k'	1	3	5	7	9	11	13	15
$d_z \geq$	32	30	28	26	24	22	20	18
k	9	10	11	12	13	14	15	16
k'	17	19	21	23	25	27	29	31
$d_z \geq$	16	14	12	10	8	6	4	2

Example 8.5.6. For $m = 3$ and $1 \leq k \leq 64$ the $[[384, k', d_z/2]]_4$ -quantum codes listed in Table 8.3 are derived.

Table 8.3: $[[384, k', d_z/2]]_4$ -code Q from $[64, k, 64 - k + 1]_{64}$ -extended RS codes

k	1	2	3	4	5	6	7	8
k'	2	5	8	11	14	17	20	23
$d_z \geq$	128	126	124	122	120	118	116	114
k	9	10	11	12	13	14	15	16
k'	26	29	32	35	38	41	44	47
$d_z \geq$	112	110	108	106	104	102	100	98
k	17	18	19	20	21	22	23	24
k'	50	53	56	59	62	65	68	71
$d_z \geq$	96	94	92	90	88	86	84	82
k	25	26	27	28	29	30	31	32
k'	74	77	80	83	86	89	92	95
$d_z \geq$	80	78	76	74	72	70	68	66
k	33	34	35	36	37	38	39	40
k'	98	101	104	107	110	113	116	119
$d_z \geq$	64	62	60	58	56	54	52	50
k	41	42	43	44	45	46	47	48
k'	122	125	128	131	134	137	140	143
$d_z \geq$	48	46	44	42	40	38	36	34
k	49	50	51	52	53	54	55	56
k'	146	149	152	155	158	161	164	167
$d_z \geq$	32	30	28	26	24	22	20	18
k	57	58	59	60	61	62	63	64
k'	170	173	176	179	182	185	188	191
$d_z \geq$	16	14	12	10	8	6	4	2

8.6 Conclusions and Open Problems

In this chapter we have given a special construction of AQECCs. An analysis on the weight enumerators of the resulting quantum codes is also presented. The construction is especially useful when the constraint on d_x is minimal and the demand on d_z is critical.

This allows us to give a more general criterion to use in choosing a pair of $\mathbb{F}_4$ -linear codes $C \subset D$ that, in some cases, yields asymmetric quantum codes with improved parameters compared to those previously known. Many new asymmetric quantum codes are also found.

There are direct generalizations of the mapping S . One direction might be to use non-quadratic extensions. Another one is to generalize it to fields of odd characteristics. The latter might be more promising than the former.

Chapter 9

Linear Programming and Optimal Pure CSS-like Codes

In this chapter, we compare the parameters of the quantum codes derived from the nested pairs of classical codes constructed by the methods outlined in Chapters 6, 7 and 8 against the parameters derived from linear programming. For linear programming, the software CPLEX is used. We gratefully acknowledge IBM for CPLEX, which is the LP/ILP solver in IBM ILOG CPLEX Optimization Studio 12.2 that IBM provides free of charge via the IBM Academic Initiative.

When optimality can be inferred, the explicit constructions of the corresponding nested classical codes are listed down. In the case where optimality can not be established with certainty, we sometimes present the linear programming upper bounds and the nearest AQECCs with known explicit constructions.

The last section of this chapter contains some instructive ad-hoc constructions which give us optimal CSS-like AQECCs or rule out the possibility of certain AQECCs.

By Proposition 3.2.11, good AQECCs with $K = 1$ and $d_z = d_x$ can be derived from self-dual codes having the largest possible minimal distance. Self-dual codes have been extensively studied, mostly due to their many connections to lattices and invariant theories. Reference [61] provides the most comprehensive treatment on this fascinating topic to date.

Lists of extremal and optimal self-dual codes over various finite fields can be found in [61, Ch. 11]. New extremal or optimal self-dual codes continue to be discovered. See, for instance, [38] and [41] as well as prominent references therein for more recent results. The parameters of the AQECCs that can be derived from these extremal or optimal self-dual codes via CSS-like constructions can be computed easily. In the case of $q = 4$, for example, Tables 7.1 and 7.2 provide the most updated list. Henceforth in this chapter, we do not consider AQECCs with $K = 1$.

9.1 Linear Programming Bound

Let $*$ stand for any one of the Euclidean, trace Euclidean, Hermitian, and trace Hermitian inner products. Since d_z and d_x can be interchanged, our notations need to be adjusted slightly. Let C_x and C_z be, respectively, an $(n, M_x, d_x)_q$ -code and an $(n, M_z, d_z)_q$ -code such that $C_x^{\perp*} \subset C_z$. For $0 \leq j \leq n$, let A_j and B_j be, respectively, the number of codewords of weight j in $C_z^{\perp*}$ and in $C_x^{\perp*}$. Let $k_x := \log_q M_x$ and $k_z := \log_q M_z$.

Given a specific pure CSS-like code Q of parameters $[[n, k_Q = \log_q K, d_z = a/d_x = b]]_q$ derived from a concrete pair $C_x^{\perp*} \subset C_z$, we check if it is possible to derive feasible higher value(s) of k from linear programming. As input, $(n, q, k, k', d_x = b, d_z = a)$

and $(n, q, k, k', d_x = a, d_z = b)$, where k and k' are to be defined below, are provided.

The LP process outputs the values of k which are not ruled out. If k_Q reaches the highest possible value of k indicated in the output, then Q is said to be *optimal*.

Formally, we define our linear programming as follows.

The objective function is to maximize

$$\sum_{j=1}^{d_z-1} A_j, \quad (9.1.1)$$

subject to the following constraints:

1. $A_0 = B_0 = A_0^\perp = B_0^\perp = 1$.
2. $A_j = 0$ for $1 \leq j < d(C_z^{\perp*})$ and $A_j \geq 0$ for $j \geq d(C_z^{\perp*})$.
3. $B_j = 0$ for $1 \leq j < d(C_x^{\perp*})$ and $B_j \geq 0$ for $j \geq d(C_x^{\perp*})$.
4. $A_j^\perp = 0$ for $1 \leq j < d_z$ and $A_j^\perp \geq 0$ for $j \geq d_z$.
5. $B_j^\perp = 0$ for $1 \leq j < d_x$ and $B_j^\perp \geq 0$ for $j \geq d_x$.
6. To ensure that $d_x, d_z > 1$, set $0 < k' < n - k$.
7. $\sum_{j=0}^n A_j = q^{k'}$.
8. $\sum_{j=0}^n B_j = q^{n-k-k'}$.
9. $A_j^\perp = \frac{1}{q^{k'}} \sum_{r=0}^n K_j^{n,q}(r) A_r$ for $0 \leq j \leq n$.
10. $B_j^\perp = \frac{1}{q^{n-k-k'}} \sum_{r=0}^n K_j^{n,q}(r) B_r$ for $0 \leq j \leq n$.
11. $A_j = B_j^\perp$ for $0 \leq j \leq d_x - 1$, $A_j < B_j^\perp$ for $j = d_x$, and $A_j \leq B_j^\perp$ for all $d_x < j \leq n$.

12. $B_j = A_j^\perp$ for $0 \leq j \leq d_z - 1$, $B_j < A_j^\perp$ for $j = d_z$, and $B_j \leq A_j^\perp$ for all $d_z < j \leq n$.

Constraint 6 is included to ensure that we have both X -error and Z -error detection capability. Constraints 9 and 10 are derived from Equation (2.1.4). The assumption of purity gives us the last two constraints.

To implement, we must fix the value of k' . Let $\mathbb{F}_q = \mathbb{F}_{r^m}$. Given a known $[[n, k_Q, d_z = a/d_x = b]]_q$ -code Q , Algorithm 1 gives the outline of the implementation process.

Algorithm 1 LP Upper Bound for k :

```

for  $k := k_Q$  to  $n - d_x - d_z + 2$  step  $\frac{1}{m}$  do
  for  $k' := \frac{1}{m}$  to  $n - k$  step  $\frac{1}{m}$  do
    if  $k, k' \in \mathbb{N}$  then
      if  $\text{BKLCUpperBound}(\mathbb{F}_q, n, n - k') \geq a$ 
        and  $\text{BKLCUpperBound}(\mathbb{F}_q, n, k + k') \geq b$  then
          Compute  $\text{LP}(n, q, k, k', d_x = b, d_z = a)$ 
        else
          if  $\text{BKLCUpperBound}(\mathbb{F}_q, n, n - k') \geq b$ 
            and  $\text{BKLCUpperBound}(\mathbb{F}_q, n, k + k') \geq a$  then
              Compute  $\text{LP}(n, q, k, k', d_x = a, d_z = b)$ 
            end if
          end if
        end if
      else
        Compute  $\text{LP}(n, q, k, k', d_x = b, d_z = a)$ 
        Compute  $\text{LP}(n, q, k, k', d_x = a, d_z = b)$ 
      end if
    end for
  end for

```

9.2 Tables of Optimal Pure Asymmetric CSS-like Codes and their Explicit Constructions

The lists of optimal pure asymmetric CSS-like codes for $q \in \{2, 3, 4, 5, 7, 8, 9\}$ are given in a series of tables below. For $q \in \{4, 8, 9\}$, we differentiate between the strictly $\mathbb{F}_q$ -linear cases and the $\mathbb{F}_r$ -linear cases. AQECCs from $\mathbb{F}_r$ -linear construction beating the best that the strictly $\mathbb{F}_q$ -linear construction can achieve are highlighted to show the gain that we get from going non $\mathbb{F}_q$ -linear.

We use the following nomenclatures to indicate the type of nested pair of codes used to derive the indicated quantum codes:

1. AddCyclic stands for $\mathbb{F}_r$ -linear but not $\mathbb{F}_q$ -linear nested cyclic codes pair. That is, at least one of the codes in the pair is not $\mathbb{F}_q$ -linear.
2. Cyclic stands for $\mathbb{F}_q$ -linear nested cyclic codes pair.
3. GroupChar stands for $\mathbb{F}_q$ -linear nested group character codes pair.
4. BKLC stands for a nested pair where the supercode can be found in the current database of MAGMA.
5. BKLC' stands for a nested pair where the code containing codeword $\mathbf{v}$ with $\text{wt}_H(\mathbf{v}) = n$ satisfies the parameters of the best-known linear codes but the code itself is not yet included in the database of MAGMA.
6. S-Ort stands for the construction where the classical code is a self-orthogonal $\mathbb{F}_4$ -linear code discussed in Chapter 7.

7. Ad Hoc means that the construction of the nested pair does not fall into any of the above types. We supply the explicit construction in Section 9.3.3.

9.2.1 Optimal Pure Binary AQECCs

Let us begin with 2-ary quantum codes. Table 9.1 presents optimal pure CSS codes of lengths up to 40.

No.	AQECC Q	Type	No.	AQECC Q	Type
1	$[[6, 1, 3/2]]_2$	Cyclic	42	$[[24, 17, 4/2]]_2$	BKLC
2	$[[7, 3, 3/2]]_2$	Cyclic	43	$[[24, 13, 6/2]]_2$	BKLC
3	$[[7, 1, 3/3]]_2$	Cyclic	44	$[[24, 11, 8/2]]_2$	BKLC
4	$[[8, 3, 4/2]]_2$	BKLC	45	$[[26, 1, 13/2]]_2$	Cyclic
5	$[[10, 1, 5/2]]_2$	Cyclic	46	$[[27, 13, 7/2]]_2$	BKLC
6	$[[11, 6, 3/2]]_2$	BKLC	47	$[[28, 22, 3/2]]_2$	BKLC
7	$[[12, 6, 4/2]]_2$	Cyclic	48	$[[28, 21, 4/2]]_2$	Cyclic
8	$[[13, 1, 5/3]]_2$	Ad Hoc	49	$[[28, 13, 8/2]]_2$	BKLC
9	$[[14, 4, 6/2]]_2$	Cyclic	50	$[[29, 5, 13/2]]_2$	BKLC
10	$[[14, 1, 7/2]]_2$	Cyclic	51	$[[30, 22, 4/2]]_2$	Cyclic
11	$[[15, 10, 3/2]]_2$	Cyclic	52	$[[30, 5, 14/2]]_2$	BKLC
12	$[[15, 8, 4/2]]_2$	Cyclic	53	$[[30, 1, 15/2]]_2$	Cyclic
13	$[[15, 6, 5/2]]_2$	Cyclic	54	$[[31, 25, 3/2]]_2$	Cyclic
14	$[[15, 4, 7/2]]_2$	Cyclic	55	$[[31, 20, 5/2]]_2$	Cyclic
15	$[[15, 6, 4/3]]_2$	Cyclic	56	$[[31, 16, 7/2]]_2$	BKLC
16	$[[15, 2, 6/3]]_2$	Cyclic	57	$[[31, 10, 11/2]]_2$	Cyclic
17	$[[15, 4, 4/4]]_2$	Cyclic	58	$[[31, 5, 15/2]]_2$	Cyclic
18	$[[15, 2, 5/4]]_2$	Cyclic	59	$[[31, 21, 3/3]]_2$	Cyclic
19	$[[15, 7, 3/3]]_2$	Cyclic	60	$[[31, 20, 4/3]]_2$	Cyclic
20	$[[15, 3, 5/3]]_2$	Cyclic	61	$[[31, 16, 5/3]]_2$	Cyclic
21	$[[15, 1, 7/3]]_2$	Cyclic, Ad Hoc	62	$[[31, 15, 6/3]]_2$	Cyclic
22	$[[16, 10, 4/2]]_2$	BKLC	63	$[[31, 6, 11/3]]_2$	Cyclic
23	$[[16, 4, 8/2]]_2$	BKLC	64	$[[31, 5, 12/3]]_2$	Cyclic
24	$[[17, 1, 5/5]]_2$	Cyclic	65	$[[31, 1, 15/3]]_2$	Cyclic
25	$[[17, 8, 5/2]]_2$	Cyclic	66	$[[31, 15, 5/4]]_2$	Cyclic
26	$[[18, 8, 6/2]]_2$	BKLC	67	$[[31, 5, 11/4]]_2$	Cyclic
27	$[[18, 1, 9/2]]_2$	Cyclic	68	$[[31, 11, 5/5]]_2$	Cyclic

continued on next page

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
28	$[[20, 14, 3/2]]_2$	BKLC	69	$[[31, 10, 6/5]]_2$	Cyclic
29	$[[20, 13, 4/2]]_2$	BKLC	70	$[[31, 1, 11/5]]_2$	Cyclic
30	$[[21, 15, 3/2]]_2$	Cyclic	71	$[[32, 25, 4/2]]_2$	BKLC
31	$[[21, 11, 5/2]]_2$	Cyclic	72	$[[32, 16, 8/2]]_2$	BKLC
32	$[[21, 7, 5/3]]_2$	Cyclic	73	$[[32, 10, 12/2]]_2$	BKLC
33	$[[21, 6, 6/3]]_2$	Cyclic	74	$[[32, 5, 16/2]]_2$	BKLC
34	$[[21, 6, 5/4]]_2$	Cyclic	75	$[[33, 22, 5/2]]_2$	BKLC
35	$[[21, 3, 5/5]]_2$	Cyclic	76	$[[34, 22, 6/2]]_2$	BKLC
36	$[[21, 2, 6/5]]_2$	Cyclic	77	$[[35, 27, 4/2]]_2$	Cyclic
37	$[[22, 1, 11/2]]_2$	Cyclic	78	$[[36, 29, 3/2]]_2$	BKLC
38	$[[23, 13, 5/2]]_2$	BKLC	79	$[[36, 28, 4/2]]_2$	BKLC
39	$[[23, 11, 7/2]]_2$	Cyclic	80	$[[40, 33, 3/2]]_2$	BKLC
40	$[[23, 1, 7/7]]_2$	Cyclic	81	$[[40, 32, 4/2]]_2$	BKLC
41	$[[24, 18, 3/2]]_2$	BKLC			

Table 9.1: Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_2$

In Table 9.2 explicit cyclic codes pairs $D \subset C$ are listed. To save space, we present the generator polynomials of the codes C and D in abbreviated forms. The generator polynomial $g_C(x)$ of the $[n, k_C]_2$ -code C is written as $(c_0, c_1, \dots, c_{n-k_C})$ instead of as the polynomial $c_0 + c_1x + \dots + c_{n-k_C}x^{n-k_C}$. Since $g_C(x)$ divides the generator polynomial of D , we write the latter as $(d_0, d_1, \dots, d_{k_C-k_D})$ where k_D is the dimension of D .

C and D	Generator Polynomials	Code Q
$[6, 5, 2]_2$	$g_C(x) = (11)$	$[[6, 1, 3/2]]_2$
$[6, 4, 2]_2$	$(11)g_C(x)$	
$[7, 4, 3]_2$	$g_C(x) = (1011)$	$[[7, 3, 3/2]]_2$
$[7, 1, 7]_2$	$(1101)g_C(x)$	
$[7, 4, 3]_2$	$g_C(x) = (1011)$	$[[7, 1, 3/3]]_2$
$[7, 3, 4]_2$	$(11)g_C(x)$	
$[10, 9, 2]_2$	$g_C(x) = (11)$	$[[10, 1, 5/2]]_2$
$[10, 8, 2]_2$	$(11)g_C(x)$	
<i>continued on next page</i>		

<i>continued from previous page</i>		
C and D	Generator Polynomials	Code Q
$[12, 11, 2]_2$	$g_C(x) = (11)$	$[[12, 6, 4/2]]_2$
$[12, 5, 4]_2$	$(1101011)g_C(x)$	
$[14, 13, 2]_2$	$g_C(x) = (11)$	$[[14, 4, 6/2]]_2$
$[14, 9, 4]_2$	$(11101)g_C(x)$	
$[14, 2, 7]_2$	$g_C(x) = (1010101010101)$	$[[14, 1, 7/2]]_2$
$[14, 1, 14]_2$	$(11)g_C(x)$	
$[15, 11, 3]_2$	$g_C(x) = (10011)$	$[[15, 10, 3/2]]_2$
$[15, 1, 15]_2$	$(11101100101)g_C(x)$	
$[15, 13, 2]_2$	$g_C(x) = (111)$	$[[15, 8, 4/2]]_2$
$[15, 5, 7]_2$	$(111010001)g_C(x)$	
$[15, 7, 5]_2$	$g_C(x) = (100010111)$	$[[15, 6, 5/2]]_2$
$[15, 1, 15]_2$	$(1111001)g_C(x)$	
$[15, 14, 2]_2$	$g_C(x) = (11)$	$[[15, 4, 7/2]]_2$
$[15, 10, 4]_2$	$(10011)g_C(x)$	
$[15, 10, 4]_2$	$g_C(x) = (101011)$	$[[15, 6, 4/3]]_2$
$[15, 4, 8]_2$	$(1011101)g_C(x)$	
$[15, 6, 6]_2$	$g_C(x) = (1100111001)$	$[[15, 2, 6/3]]_2$
$[15, 4, 8]_2$	$(111)g_C(x)$	
$[15, 10, 4]_2$	$g_C(x) = (101011)$	$[[15, 4, 4/4]]_2$
$[15, 6, 6]_2$	$(10011)g_C(x)$	
$[15, 10, 4]_2$	$g_C(x) = (101011)$	$[[15, 2, 5/4]]_2$
$[15, 8, 4]_2$	$(111)g_C(x)$	
$[15, 11, 3]_2$	$g_C(x) = (10011)$	$[[15, 7, 3/3]]_2$
$[15, 4, 8]_2$	$(11100111)g_C(x)$	
$[15, 11, 3]_2$	$g_C(x) = (10011)$	$[[15, 3, 5/3]]_2$
$[15, 8, 4]_2$	$(1001)g_C(x)$	
$[15, 11, 3]_2$	$g_C(x) = (10011)$	$[[15, 1, 7/3]]_2$
$[15, 10, 4]_2$	$(11)g_C(x)$	
$[17, 9, 5]_2$	$g_C(x) = (111010111)$	$[[17, 1, 5/5]]_2$
$[17, 8, 6]_2$	$(11)g_C(x)$	
$[17, 9, 5]_2$	$g_C(x) = (111010111)$	$[[17, 8, 5/2]]_2$
$[17, 1, 17]_2$	$(100111001)g_C(x)$	
$[18, 2, 9]_2$	$g_C(x) = (10101010101010101)$	$[[18, 1, 9/2]]_2$
$[18, 1, 18]_2$	$(11)g_C(x)$	
$[21, 20, 2]_2$	$g_C(x) = (11)$	$[[21, 15, 3/2]]_2$
$[21, 5, 10]_2$	$(1111011100110101)g_C(x)$	
$[21, 20, 2]_2$	$g_C(x) = (11)$	$[[21, 11, 5/2]]_2$
<i>continued on next page</i>		

<i>continued from previous page</i>		
<i>C and D</i>	Generator Polynomials	Code Q
$[21, 9, 8]_2$	$(100110000101)g_C(x)$	
$[21, 12, 5]_2$	$g_C(x) = (1110110011)$	$[[21, 7, 5/3]]_2$
$[21, 5, 10]_2$	$(10011111)g_C(x)$	
$[21, 11, 6]_2$	$g_C(x) = (10101011001)$	$[[21, 6, 6/3]]_2$
$[21, 5, 10]_2$	$(1010111)g_C(x)$	
$[21, 12, 5]_2$	$g_C(x) = (1110110011)$	$[[21, 6, 5/4]]_2$
$[21, 6, 7]_2$	$(1110101)g_C(x)$	
$[21, 12, 5]_2$	$g_C(x) = (1110110011)$	$[[21, 3, 5/5]]_2$
$[21, 9, 8]_2$	$(1001)g_C(x)$	
$[21, 12, 5]_2$	$g_C(x) = (1110110011)$	$[[21, 2, 6/5]]_2$
$[21, 10, 5]_2$	$(111)g_C(x)$	
$[22, 21, 2]_2$	$g_C(x) = (11)$	$[[22, 1, 11/2]]_2$
$[22, 20, 2]_2$	$(11)g_C(x)$	
$[23, 12, 7]_2$	$g_C(x) = (110001110101)$	$[[23, 11, 7/2]]_2$
$[23, 1, 23]_2$	$(101011100011)g_C(x)$	
$[23, 12, 7]_2$	$g_C(x) = (110001110101)$	$[[23, 1, 7/7]]_2$
$[23, 11, 8]_2$	$(11)g_C(x)$	
$[26, 25, 2]_2$	$g_C(x) = (11)$	$[[26, 1, 13/2]]_2$
$[26, 24, 2]_2$	$(11)g_C(x)$	
$[28, 22, 4]_2$	$g_C(x) = (1001011)$	$[[28, 21, 4/2]]_2$
$[28, 1, 28]_2$	$(1110011110101001001101)g_C(x)$	
$[30, 28, 2]_2$	$g_C(x) = (111)$	$[[30, 22, 4/2]]_2$
$[30, 6, 14]_2$	$(11110010111111100001101)g_C(x)$	
$[30, 29, 2]_2$	$g_C(x) = (11)$	$[[30, 1, 15/2]]_2$
$[30, 28, 2]_2$	$(11)g_C(x)$	
$[31, 26, 3]_2$	$g_C(x) = (111101)$	$[[31, 25, 3/2]]_2$
$[31, 1, 31]_2$	$(10001110101001011110011011)g_C(x)$	
$[31, 21, 5]_2$	$g_C(x) = (10001110001)$	$[[31, 20, 5/2]]_2$
$[31, 1, 31]_2$	$(111101001111100101111)g_C(x)$	
$[31, 11, 11]_2$	$g_C(x) = (111001110001010011001)$	$[[31, 10, 11/2]]_2$
$[31, 1, 31]_2$	$(10010110111)g_C(x)$	
$[31, 6, 15]_2$	$g_C(x) = (11001011011110101000100111)$	$[[31, 5, 15/2]]_2$
$[31, 1, 31]_2$	$(101001)g_C(x)$	
$[31, 26, 3]_2$	$g_C(x) = (111101)$	$[[31, 21, 3/3]]_2$
$[31, 5, 16]_2$	$(1011001010111010100011)g_C(x)$	
$[31, 25, 4]_2$	$g_C(x) = (1000111)$	$[[31, 20, 4/3]]_2$
$[31, 5, 16]_2$	$(110111001101001100001)g_C(x)$	
<i>continued on next page</i>		

<i>continued from previous page</i>		
C and D	Generator Polynomials	Code Q
$[31, 21, 5]_2$	$g_C(x) = (10001110001)$	$[[31, 16, 5/3]]_2$
$[31, 5, 16]_2$	$(10111001100000011)g_C(x)$	
$[31, 20, 6]_2$	$g_C(x) = (100110110001)$	$[[31, 15, 6/3]]_2$
$[31, 5, 16]_2$	$(1101110101011101)g_C(x)$	
$[31, 11, 11]_2$	$g_C(x) = (111001110001010011001)$	$[[31, 6, 11/3]]_2$
$[31, 5, 16]_2$	$(1110001)g_C(x)$	
$[31, 10, 12]_2$	$g_C(x) = (1010010010101101001111)$	$[[31, 5, 12/3]]_2$
$[31, 5, 16]_2$	$(100101)g_C(x)$	
$[31, 26, 3]_2$	$g_C(x) = (111101)$	$[[31, 1, 15/3]]_2$
$[31, 25, 4]_2$	$(11)g_C(x)$	
$[31, 21, 5]_2$	$g_C(x) = (10001110001)$	$[[31, 15, 5/4]]_2$
$[31, 6, 15]_2$	$(1101000100000001)g_C(x)$	
$[31, 11, 11]_2$	$g_C(x) = (111001110001010011001)$	$[[31, 5, 11/4]]_2$
$[31, 6, 15]_2$	$(101001)g_C(x)$	
$[31, 21, 5]_2$	$g_C(x) = (10001110001)$	$[[31, 11, 5/5]]_2$
$[31, 10, 12]_2$	$(100110111011)g_C(x)$	
$[31, 20, 6]_2$	$g_C(x) = (100110110001)$	$[[31, 10, 6/5]]_2$
$[31, 10, 12]_2$	$(10111011111)g_C(x)$	
$[31, 11, 11]_2$	$g_C(x) = (111001110001010011001)$	$[[31, 1, 11/5]]_2$
$[31, 10, 12]_2$	$(11)g_C(x)$	
$[35, 34, 2]_2$	$g_C(x) = (11)$	$[[35, 27, 4/2]]_2$
$[35, 7, 14]_2$	$(1110111010100110100100111101)g_C(x)$	

Table 9.2: Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_2$ and the Resulting CSS Codes

9.2.2 Optimal Pure Ternary AQECCs

Table 9.3 presents the list of optimal pure 3-ary CSS codes. Most of the codes come from BKLC construction. Those coming from the cyclic construction are listed in Table 9.4 where we use the same abbreviated forms for the generator polynomials as in Subsection 9.2.1 above.

No.	AQECC Q	Type	No.	AQECC Q	Type
1	$[[6, 2, 3/2]]_3$	Cyclic	97	$[[24, 16, 5/2]]_3$	BKLC
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
2	$[[6, 1, 4/2]]_3$	Cyclic	98	$[[24, 15, 6/2]]_3$	BKLC
3	$[[7, 3, 3/2]]_3$	BKLC	99	$[[24, 11, 9/2]]_3$	BKLC
4	$[[7, 2, 4/2]]_3$	BKLC	100	$[[24, 6, 12/2]]_3$	BKLC
5	$[[8, 4, 3/2]]_3$	Cyclic	101	$[[24, 3, 15/2]]_3$	Cyclic
6	$[[8, 3, 4/2]]_3$	Cyclic, GroupChar	102	$[[24, 16, 3/3]]_3$	Cyclic
7	$[[8, 2, 5/2]]_3$	Cyclic	103	$[[24, 14, 4/3]]_3$	Cyclic
8	$[[8, 2, 3/3]]_3$	Cyclic	104	$[[25, 20, 3/2]]_3$	BKLC
9	$[[8, 1, 4/3]]_3$	Cyclic	105	$[[25, 18, 4/2]]_3$	BKLC
10	$[[9, 5, 3/2]]_3$	BKLC	106	$[[25, 17, 5/2]]_3$	BKLC
11	$[[9, 4, 4/2]]_3$	BKLC	107	$[[25, 16, 6/2]]_3$	BKLC
12	$[[9, 3, 5/2]]_3$	BKLC	108	$[[25, 7, 12/2]]_3$	BKLC
13	$[[9, 2, 6/2]]_3$	BKLC	109	$[[25, 6, 13/2]]_3$	BKLC
14	$[[10, 6, 3/2]]_3$	BKLC	110	$[[25, 3, 16/2]]_3$	BKLC
15	$[[10, 5, 4/2]]_3$	BKLC	111	$[[26, 21, 3/2]]_3$	Cyclic
16	$[[11, 7, 3/2]]_3$	BKLC	112	$[[26, 19, 4/2]]_3$	Cyclic
17	$[[11, 5, 5/2]]_3$	Cyclic	113	$[[26, 18, 5/2]]_3$	Cyclic
18	$[[11, 1, 5/5]]_3$	Cyclic	114	$[[26, 17, 6/2]]_3$	BKLC
19	$[[12, 8, 3/2]]_3$	BKLC	115	$[[26, 7, 13/2]]_3$	Cyclic
20	$[[12, 6, 4/2]]_3$	Cyclic	116	$[[26, 6, 14/2]]_3$	Cyclic
21	$[[12, 5, 6/2]]_3$	BKLC	117	$[[26, 3, 17/2]]_3$	Cyclic
22	$[[12, 2, 4/4]]_3$	Cyclic	118	$[[26, 18, 3/3]]_3$	Cyclic
23	$[[13, 9, 3/2]]_3$	Cyclic	119	$[[26, 16, 4/3]]_3$	Cyclic
24	$[[13, 7, 4/2]]_3$	BKLC	120	$[[26, 15, 5/3]]_3$	Cyclic
25	$[[13, 6, 5/2]]_3$	Cyclic	121	$[[26, 4, 13/3]]_3$	Cyclic
26	$[[13, 3, 7/2]]_3$	Cyclic	122	$[[26, 3, 14/3]]_3$	Cyclic
27	$[[13, 7, 3/3]]_3$	Cyclic	123	$[[26, 14, 4/4]]_3$	Cyclic
28	$[[13, 4, 5/3]]_3$	Cyclic	124	$[[26, 13, 5/4]]_3$	Cyclic
29	$[[13, 3, 6/3]]_3$	Cyclic	125	$[[26, 12, 6/4]]_3$	Cyclic
30	$[[13, 1, 7/3]]_3$	Cyclic	126	$[[26, 2, 13/4]]_3$	Cyclic
31	$[[13, 1, 5/5]]_3$	Cyclic	127	$[[26, 1, 14/4]]_3$	Cyclic
32	$[[14, 9, 3/2]]_3$	BKLC	128	$[[26, 12, 5/5]]_3$	Cyclic
33	$[[14, 8, 4/2]]_3$	BKLC	129	$[[26, 1, 13/5]]_3$	Cyclic
34	$[[14, 7, 5/2]]_3$	BKLC	130	$[[27, 22, 3/2]]_3$	BKLC
35	$[[14, 6, 6/2]]_3$	BKLC	131	$[[27, 20, 4/2]]_3$	BKLC
36	$[[14, 4, 7/2]]_3$	BKLC	132	$[[27, 19, 5/2]]_3$	BKLC
37	$[[15, 10, 3/2]]_3$	BKLC	133	$[[27, 18, 6/2]]_3$	BKLC
38	$[[15, 9, 4/2]]_3$	BKLC	134	$[[27, 7, 14/2]]_3$	BKLC
39	$[[15, 7, 5/2]]_3$	BKLC	135	$[[27, 6, 15/2]]_3$	BKLC
40	$[[15, 6, 6/2]]_3$	BKLC	136	$[[27, 3, 18/2]]_3$	BKLC
41	$[[16, 11, 3/2]]_3$	BKLC	137	$[[27, 1, 20/2]]_3$	BKLC
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
42	$[[16, 10, 4/2]]_3$	BKLC, GroupChar	138	$[[28, 23, 3/2]]_3$	BKLC
43	$[[16, 8, 5/2]]_3$	BKLC	139	$[[28, 21, 4/2]]_3$	BKLC
44	$[[16, 7, 6/2]]_3$	BKLC	140	$[[28, 19, 6/2]]_3$	BKLC
45	$[[16, 5, 7/2]]_3$	BKLC	141	$[[28, 1, 21/2]]_3$	BKLC
46	$[[16, 2, 10/2]]_3$	Cyclic	142	$[[29, 24, 3/2]]_3$	BKLC
47	$[[16, 2, 5/5]]_3$	Cyclic	143	$[[29, 22, 4/2]]_3$	BKLC
48	$[[17, 12, 3/2]]_3$	BKLC	144	$[[29, 1, 21/2]]_3$	BKLC
49	$[[17, 11, 4/2]]_3$	BKLC	145	$[[30, 25, 3/2]]_3$	BKLC
50	$[[17, 9, 5/2]]_3$	BKLC	146	$[[30, 23, 4/2]]_3$	BKLC
51	$[[17, 8, 6/2]]_3$	BKLC	147	$[[30, 4, 18/2]]_3$	BKLC
52	$[[17, 6, 7/2]]_3$	BKLC	148	$[[30, 1, 22/2]]_3$	BKLC
53	$[[17, 5, 8/2]]_3$	BKLC	149	$[[31, 26, 3/2]]_3$	BKLC
54	$[[18, 13, 3/2]]_3$	BKLC	150	$[[31, 24, 4/2]]_3$	BKLC
55	$[[18, 12, 4/2]]_3$	BKLC	151	$[[31, 1, 23/2]]_3$	BKLC
56	$[[18, 10, 5/2]]_3$	BKLC	152	$[[32, 27, 3/2]]_3$	BKLC
57	$[[18, 9, 6/2]]_3$	BKLC	153	$[[32, 25, 4/2]]_3$	BKLC, GroupChar
58	$[[19, 14, 3/2]]_3$	BKLC	154	$[[32, 1, 24/2]]_3$	BKLC
59	$[[19, 13, 4/2]]_3$	BKLC	155	$[[33, 28, 3/2]]_3$	BKLC
60	$[[19, 11, 5/2]]_3$	BKLC	156	$[[33, 26, 4/2]]_3$	BKLC
61	$[[19, 10, 6/2]]_3$	BKLC	157	$[[33, 24, 5/2]]_3$	BKLC
62	$[[19, 8, 7/2]]_3$	BKLC	158	$[[33, 16, 10/2]]_3$	BKLC
63	$[[20, 15, 3/2]]_3$	BKLC	159	$[[33, 1, 24/2]]_3$	BKLC
64	$[[20, 14, 4/2]]_3$	Cyclic	160	$[[34, 29, 3/2]]_3$	BKLC
65	$[[20, 12, 5/2]]_3$	BKLC	161	$[[34, 27, 4/2]]_3$	BKLC
66	$[[20, 11, 6/2]]_3$	BKLC	162	$[[34, 25, 5/2]]_3$	BKLC
67	$[[20, 9, 7/2]]_3$	BKLC	163	$[[34, 17, 10/2]]_3$	BKLC
68	$[[20, 8, 8/2]]_3$	BKLC	164	$[[34, 1, 25/2]]_3$	BKLC
69	$[[20, 5, 10/2]]_3$	Cyclic	165	$[[35, 30, 3/2]]_3$	BKLC
70	$[[20, 4, 11/2]]_3$	Cyclic	166	$[[35, 28, 4/2]]_3$	BKLC
71	$[[20, 10, 4/4]]_3$	Cyclic	167	$[[35, 26, 5/2]]_3$	BKLC
72	$[[20, 1, 10/4]]_3$	Cyclic	168	$[[35, 17, 11/2]]_3$	BKLC
73	$[[21, 16, 3/2]]_3$	BKLC	169	$[[35, 1, 26/2]]_3$	BKLC
74	$[[21, 14, 4/2]]_3$	BKLC	170	$[[36, 31, 3/2]]_3$	BKLC
75	$[[21, 13, 5/2]]_3$	BKLC	171	$[[36, 29, 4/2]]_3$	BKLC
76	$[[21, 12, 6/2]]_3$	BKLC	172	$[[36, 27, 5/2]]_3$	BKLC
77	$[[21, 10, 7/2]]_3$	BKLC	173	$[[36, 17, 12/2]]_3$	BKLC
78	$[[21, 9, 8/2]]_3$	BKLC	174	$[[36, 1, 27/2]]_3$	BKLC
79	$[[21, 8, 9/2]]_3$	BKLC	175	$[[37, 32, 3/2]]_3$	BKLC
80	$[[22, 17, 3/2]]_3$	BKLC	176	$[[37, 30, 4/2]]_3$	BKLC
81	$[[22, 15, 4/2]]_3$	Cyclic	177	$[[37, 28, 5/2]]_3$	BKLC
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
82	$[[22, 14, 5/2]]_3$	BKLC	178	$[[37, 1, 27/2]]_3$	BKLC
83	$[[22, 13, 6/2]]_3$	BKLC	179	$[[38, 33, 3/2]]_3$	BKLC
84	$[[22, 11, 7/2]]_3$	Cyclic	180	$[[38, 31, 4/2]]_3$	BKLC
85	$[[22, 5, 12/2]]_3$	Cyclic	181	$[[38, 29, 5/2]]_3$	BKLC
86	$[[22, 10, 4/4]]_3$	Cyclic	182	$[[38, 1, 28/2]]_3$	BKLC
87	$[[22, 6, 7/4]]_3$	Cyclic	183	$[[39, 34, 3/2]]_3$	BKLC
88	$[[22, 2, 7/7]]_3$	Cyclic	184	$[[39, 32, 4/2]]_3$	BKLC
89	$[[23, 18, 3/2]]_3$	BKLC	185	$[[39, 30, 5/2]]_3$	BKLC
90	$[[23, 16, 4/2]]_3$	BKLC	186	$[[39, 1, 29/2]]_3$	BKLC
91	$[[23, 15, 5/2]]_3$	BKLC	187	$[[40, 35, 3/2]]_3$	BKLC
92	$[[23, 14, 6/2]]_3$	BKLC	188	$[[40, 33, 4/2]]_3$	BKLC
93	$[[23, 11, 8/2]]_3$	BKLC	189	$[[40, 31, 5/2]]_3$	BKLC
94	$[[23, 1, 8/8]]_3$	Cyclic	190	$[[40, 1, 30/2]]_3$	BKLC
95	$[[24, 19, 3/2]]_3$	Cyclic	191	$[[40, 28, 4/4]]_3$	Cyclic
96	$[[24, 17, 4/2]]_3$	Cyclic			

Table 9.3: Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_3$

C and D	Generator Polynomials	Code Q
$[6, 5, 2]_3$	$g_C(x) = (21)$	$[[6, 2, 3/2]]_3$
$[6, 3, 3]_3$	$(121)g_C(x)$	
$[6, 5, 2]_3$	$g_C(x) = (21)$	$[[6, 1, 4/2]]_3$
$[6, 4, 2]_3$	$(21)g_C(x)$	
$[8, 7, 2]_3$	$g_C(x) = (11)$	$[[8, 4, 3/2]]_3$
$[8, 3, 5]_3$	$(22021)g_C(x)$	
$[8, 7, 2]_3$	$g_C(x) = (11)$	$[[8, 3, 4/2]]_3$
$[8, 4, 4]_3$	$(1101)g_C(x)$	
$[8, 7, 2]_3$	$g_C(x) = (11)$	$[[8, 2, 5/2]]_3$
$[8, 5, 3]_3$	$(211)g_C(x)$	
$[8, 5, 3]_3$	$g_C(x) = (1011)$	$[[8, 2, 3/3]]_3$
$[8, 3, 5]_3$	$(101)g_C(x)$	
$[8, 4, 4]_3$	$g_C(x) = (21011)$	$[[8, 1, 4/3]]_3$
$[8, 3, 5]_3$	$(21)g_C(x)$	
$[11, 10, 2]_3$	$g_C(x) = (21)$	$[[11, 5, 5/2]]_3$
$[11, 5, 6]_3$	$(201211)g_C(x)$	
$[11, 6, 5]_3$	$g_C(x) = (201211)$	$[[11, 1, 5/5]]_3$
$[11, 5, 6]_3$	$(21)g_C(x)$	
$[12, 7, 4]_3$	$g_C(x) = (101101)$	$[[12, 6, 4/2]]_3$
<i>continued on next page</i>		

<i>continued from previous page</i>		
C and D	Generator Polynomials	Code Q
$[12, 1, 12]_3$	$(1102011)g_C(x)$	
$[12, 7, 4]_3$	$g_C(x) = (101101)$	$[[12, 2, 4/4]]_3$
$[12, 5, 4]_3$	$(101)g_C(x)$	
$[13, 10, 3]_3$	$g_C(x) = (2201)$	$[[13, 9, 3/2]]_3$
$[13, 1, 13]_3$	$(2022010211)g_C(x)$	
$[13, 7, 5]_3$	$g_C(x) = (1120211)$	$[[13, 6, 5/2]]_3$
$[13, 1, 13]_3$	$(1022201)g_C(x)$	
$[13, 4, 7]_3$	$g_C(x) = (2001102121)$	$[[13, 3, 7/2]]_3$
$[13, 1, 13]_3$	$(2221)g_C(x)$	
$[13, 10, 3]_3$	$g_C(x) = (2201)$	$[[13, 7, 3/3]]_3$
$[13, 3, 9]_3$	$(20102121)g_C(x)$	
$[13, 7, 5]_3$	$g_C(x) = (1120211)$	$[[13, 4, 5/3]]_3$
$[13, 3, 9]_3$	$(10011)g_C(x)$	
$[13, 6, 6]_3$	$g_C(x) = (21210201)$	$[[13, 3, 6/3]]_3$
$[13, 3, 9]_3$	$(2221)g_C(x)$	
$[13, 4, 7]_3$	$g_C(x) = (2001102121)$	$[[13, 1, 7/3]]_3$
$[13, 3, 9]_3$	$(21)g_C(x)$	
$[13, 7, 5]_3$	$g_C(x) = (1120211)$	$[[13, 1, 5/5]]_3$
$[13, 6, 6]_3$	$(21)g_C(x)$	
$[16, 3, 10]_3$	$g_C(x) = (20112100201121)$	$[[16, 2, 10/2]]_3$
$[16, 1, 16]_3$	$(221)g_C(x)$	
$[16, 9, 5]_3$	$g_C(x) = (10021121)$	$[[16, 2, 5/5]]_3$
$[16, 7, 6]_3$	$(101)g_C(x)$	
$[20, 15, 4]_3$	$g_C(x) = (201111)$	$[[20, 14, 4/2]]_3$
$[20, 1, 20]_3$	$(122200101001211)g_C(x)$	
$[20, 6, 10]_3$	$g_C(x) = (112100101002221)$	$[[20, 5, 10/2]]_3$
$[20, 1, 20]_3$	$(102121)g_C(x)$	
$[20, 5, 11]_3$	$g_C(x) = (1200101111021101)$	$[[20, 4, 11/2]]_3$
$[20, 1, 20]_3$	$(12011)g_C(x)$	
$[20, 15, 4]_3$	$g_C(x) = (201111)$	$[[20, 10, 4/4]]_3$
$[20, 5, 11]_3$	$(10202020201)g_C(x)$	
$[20, 6, 10]_3$	$g_C(x) = (112100101002221)$	$[[20, 1, 10/4]]_3$
$[20, 5, 11]_3$	$(21)g_C(x)$	
$[22, 21, 2]_3$	$g_C(x) = (11)$	$[[22, 15, 4/2]]_3$
$[22, 6, 12]_3$	$(110212222211201)g_C(x)$	
$[22, 21, 2]_3$	$g_C(x) = (11)$	$[[22, 11, 7/2]]_3$
$[22, 10, 9]_3$	$(100100210211)g_C(x)$	
<i>continued on next page</i>		

<i>continued from previous page</i>		
<i>C</i> and <i>D</i>	Generator Polynomials	Code <i>Q</i>
$[22, 21, 2]_3$	$g_C(x) = (11)$	$[[22, 5, 12/2]]_3$
$[22, 16, 4]_3$	$(201211)g_C(x)$	
$[22, 16, 4]_3$	$g_C(x) = (2100211)$	$[[22, 10, 4/4]]_3$
$[22, 6, 12]_3$	$(21221222111)g_C(x)$	
$[22, 12, 7]_3$	$g_C(x) = (22211121121)$	$[[22, 6, 7/4]]_3$
$[22, 6, 12]_3$	$(2210021)g_C(x)$	
$[22, 12, 7]_3$	$g_C(x) = (22211121121)$	$[[22, 2, 7/7]]_3$
$[22, 10, 9]_3$	$(201)g_C(x)$	
$[23, 12, 8]_3$	$g_C(x) = (222110202001)$	$[[23, 1, 8/8]]_3$
$[23, 11, 9]_3$	$(21)g_C(x)$	
$[24, 20, 3]_3$	$g_C(x) = (21201)$	$[[24, 19, 3/2]]_3$
$[24, 1, 24]_3$	$(21122012220202101211)g_C(x)$	
$[24, 18, 4]_3$	$g_C(x) = (1012011)$	$[[24, 17, 4/2]]_3$
$[24, 1, 24]_3$	$(110122101220021101)g_C(x)$	
$[24, 4, 15]_3$	$g_C(x) = (120101210022221221101)$	$[[24, 3, 15/2]]_3$
$[24, 1, 24]_3$	$(2021)g_C(x)$	
$[24, 20, 3]_3$	$g_C(x) = (21201)$	$[[24, 16, 3/3]]_3$
$[24, 4, 15]_3$	$(20101010002020201)g_C(x)$	
$[24, 20, 3]_3$	$g_C(x) = (21201)$	$[[24, 14, 4/3]]_3$
$[24, 6, 8]_3$	$(112221000221221)g_C(x)$	
$[26, 22, 3]_3$	$g_C(x) = (21211)$	$[[26, 21, 3/2]]_3$
$[26, 1, 26]_3$	$(2111221101212002001201)g_C(x)$	
$[26, 20, 4]_3$	$g_C(x) = (2120111)$	$[[26, 19, 4/2]]_3$
$[26, 1, 26]_3$	$(21122201201010111001)g_C(x)$	
$[26, 19, 5]_3$	$g_C(x) = (20012011)$	$[[26, 18, 5/2]]_3$
$[26, 1, 26]_3$	$(2221220100021021101)g_C(x)$	
$[26, 8, 13]_3$	$g_C(x) = (2220200112210010121)$	$[[26, 7, 13/2]]_3$
$[26, 1, 26]_3$	$(20021221)g_C(x)$	
$[26, 7, 14]_3$	$g_C(x) = (11102200221112020201)$	$[[26, 6, 14/2]]_3$
$[26, 1, 26]_3$	$(2211221)g_C(x)$	
$[26, 4, 17]_3$	$g_C(x) = (10212112201110120200221)$	$[[26, 3, 17/2]]_3$
$[26, 1, 26]_3$	$(1121)g_C(x)$	
$[26, 22, 3]_3$	$g_C(x) = (21211)$	$[[26, 18, 3/3]]_3$
$[26, 4, 17]_3$	$(2210102112021111211)g_C(x)$	
$[26, 22, 3]_3$	$g_C(x) = (21211)$	$[[26, 16, 4/3]]_3$
$[26, 6, 15]_3$	$(21212100100021011)g_C(x)$	
$[26, 22, 3]_3$	$g_C(x) = (21211)$	$[[26, 15, 5/3]]_3$
<i>continued on next page</i>		

<i>continued from previous page</i>		
C and D	Generator Polynomials	Code Q
$[26, 7, 14]_3$	$(1110010120102021)g_C(x)$	
$[26, 22, 3]_3$	$g_C(x) = (21211)$	$[[26, 4, 13/3]]_3$
$[26, 18, 6]_3$	$(21111)g_C(x)$	
$[26, 22, 3]_3$	$g_C(x) = (21211)$	$[[26, 3, 14/3]]_3$
$[26, 19, 5]_3$	$(1021)g_C(x)$	
$[26, 20, 4]_3$	$g_C(x) = (2120111)$	$[[26, 14, 4/4]]_3$
$[26, 6, 15]_3$	$(202122201211101)g_C(x)$	
$[26, 19, 5]_3$	$g_C(x) = (20012011)$	$[[26, 13, 5/4]]_3$
$[26, 6, 15]_3$	$(22221022102101)g_C(x)$	
$[26, 18, 6]_3$	$g_C(x) = (120112011)$	$[[26, 12, 6/4]]_3$
$[26, 6, 15]_3$	$(1022001001201)g_C(x)$	
$[26, 20, 4]_3$	$g_C(x) = (2120111)$	$[[26, 2, 13/4]]_3$
$[26, 18, 6]_3$	$(201)g_C(x)$	
$[26, 7, 14]_3$	$g_C(x) = (11102200221112020201)$	$[[26, 1, 14/4]]_3$
$[26, 6, 15]_3$	$(11)g_C(x)$	
$[26, 19, 5]_3$	$g_C(x) = (20012011)$	$[[26, 12, 5/5]]_3$
$[26, 7, 14]_3$	$(1211001221021)g_C(x)$	
$[26, 19, 5]_3$	$g_C(x) = (21020101)$	$[[26, 1, 13/5]]_3$
$[26, 18, 6]_3$	$(21)g_C(x)$	
$[40, 34, 4]_3$	$g_C(x) = (1021211)$	$[[40, 28, 4/4]]_3$
$[40, 6, 24]_3$	$(12210120100111122010200120201)g_C(x)$	

Table 9.4: Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_3$ and the Resulting CSS Codes

Based on Theorem 6.2.5, the following choices give us the requisite quantum codes from nested pairs of group character codes:

1. For an $[[8, 3, 4/2]]_3$ -code, set $r_1 = 1$, $r_2 = 2$, $l = 3$, and $t = 2$.
2. For a $[[16, 10, 4/2]]_3$ -code, set $r_1 = 1$, $r_2 = 3$, $l = 4$, and $t = 2$.
3. For a $[[32, 25, 4/2]]_3$ -code, set $r_1 = 1$, $r_2 = 4$, $l = 5$, and $t = 2$.

9.2.3 Optimal and Good Pure 4-ary AQECCs

Table 9.5 contains optimal and good pure 4-ary CSS-like codes. To measure the goodness of a specific code under consideration, the theoretical LP bound for $k = \log_q K$ is explicitly provided. The defect is measured by subtracting the actual value of k from the theoretical value derived from linear programming.

If the code is the best possible, given that we require the nested classical codes to be both $\mathbb{F}_4$ -linear, we write *OptLin* in the column titled Remarks. We write *reach bound OptLin* for a quantum code which is derived from a nested classical pair of codes with at least one member strictly $\mathbb{F}_2$ -linear whenever the quantum code reaches the best theoretical bound obtainable from any $\mathbb{F}_4$ -linear pair.

It is interesting to note that in some cases, it is possible to derive an optimal pure CSS-like code of a specified parameters from both an $\mathbb{F}_2$ -linear pair and an $\mathbb{F}_4$ -linear pair of classical codes.

No.	AQECC Q	Type	LP	Defect	Remarks
1.	$[[6, 2, 4/2]]_4$	AddCyclic	2	0	Optimal
2.	$[[6, 1, 3/3]]_4$	AddCyclic	1	0	Optimal
3.	$[[7, 3, 3/2]]_4$	BKLC	$7/2$	$1/2$	OptLin
4.	$[[7, 2, 4/2]]_4$	BKLC	$5/2$	$1/2$	OptLin
5.	$[[7, 3/2, 5/2]]_4$	AddCyclic	$3/2$	0	Optimal
6.	$[[8, 4, 3/2]]_4$	BKLC	$9/2$	$1/2$	OptLin
7.	$[[8, 3, 4/2]]_4$	BKLC	$7/2$	$1/2$	OptLin
8.	$[[8, 2, 5/2]]_4$	BKLC	$5/2$	$1/2$	OptLin
9.	$[[8, 1, 6/2]]_4$	BKLC	$3/2$	$1/2$	OptLin
10.	$[[9, 5, 3/2]]_4$	BKLC	$11/2$	$1/2$	OptLin
11.	$[[9, 4, 4/2]]_4$	BKLC	$9/2$	$1/2$	OptLin
12.	$[[9, 3, 5/2]]_4$	BKLC	$7/2$	$1/2$	OptLin
13.	$[[9, 2, 6/2]]_4$	BKLC	$5/2$	$1/2$	OptLin
14.	$[[10, 6, 3/2]]_4$	BKLC	6	0	Optimal
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
15.	$[[10, 5, 4/2]]_4$	BKLC	11/2	1/2	OptLin
16.	$[[10, 4, 5/2]]_4$	BKLC	9/2	1/2	OptLin
17.	$[[10, 3, 6/2]]_4$	BKLC	7/2	1/2	OptLin
18.	$[[10, 4, 3/3]]_4$	S-Ort	4	0	Optimal Cf. Table 7.3
19.	$[[11, 7, 3/2]]_4$	BKLC	7	0	Optimal
20.	$[[11, 6, 4/2]]_4$	BKLC	6	0	Optimal
21.	$[[11, 5, 5/2]]_4$	BKLC	5	0	Optimal
22.	$[[11, 5, 3/3]]_4$	S-Ort	5	0	Optimal Cf. Table 7.3
23.	$[[11, 1, 5/5]]_4$	Cyclic	1	0	Optimal
24.	$[[12, 8, 3/2]]_4$	BKLC	8	0	Optimal
25.	$[[12, 7, 4/2]]_4$	BKLC	7	0	Optimal
26.	$[[12, 11/2, 5/2]]_4$	AddCyclic	11/2	0	Optimal
27.	$[[12, 5, 6/2]]_4$	BKLC	5	0	Optimal
28.	$[[12, 3, 7/2]]_4$	BKLC	7/2	1/2	OptLin
29.	$[[12, 2, 8/2]]_4$	BKLC	5/2	1/2	OptLin
30.	$[[12, 1, 9/2]]_4$	AddCyclic	3/2	1/2	reach bound OptLin
31.	$[[12, 6, 3/3]]_4$	AddCyclic	6	0	Optimal
		S-Ort			Optimal Cf. Table 7.3
32.	$[[12, 7/2, 5/3]]_4$	AddCyclic	7/2	0	Optimal
33.	$[[12, 3, 6/3]]_4$	AddCyclic	3	0	Optimal
34.	$[[12, 4, 4/4]]_4$	AddCyclic	4	0	Optimal
		S-Ort			Optimal Cf. Table 7.3
35.	$[[12, 2, 5/4]]_4$	AddCyclic	5/2	1/2	reach bound OptLin
36.	$[[12, 1, 5/5]]_4$	AddCyclic	3/2	1/2	reach bound OptLin
37.	$[[13, 9, 3/2]]_4$	BKLC	9	0	Optimal
38.	$[[13, 8, 4/2]]_4$	BKLC	8	0	Optimal
39.	$[[13, 6, 5/2]]_4$	BKLC	13/2	1/2	OptLin
40.	$[[13, 5, 6/2]]_4$	BKLC	11/2	1/2	OptLin
41.	$[[13, 4, 7/2]]_4$	BKLC	9/2	1/2	OptLin
42.	$[[13, 2, 9/2]]_4$	BKLC	5/2	1/2	OptLin
43.	$[[13, 7, 3/3]]_4$	S-Ort	7	0	Optimal Cf. Table 7.3
44.	$[[14, 10, 3/2]]_4$	BKLC	10	0	Optimal
45.	$[[14, 9, 4/2]]_4$	BKLC	9	0	Optimal
46.	$[[14, 7, 5/2]]_4$	BKLC	15/2	1/2	OptLin
47.	$[[14, 6, 6/2]]_4$	BKLC	13/2	1/2	OptLin
48.	$[[14, 5, 7/2]]_4$	BKLC	11/2	1/2	OptLin
49.	$[[14, 4, 8/2]]_4$	BKLC	9/2	1/2	OptLin
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
50.	$[[14, 3, 9/2]]_4$	BKLC	7/2	1/2	OptLin
51.	$[[14, 2, 10/2]]_4$	BKLC	5/2	1/2	OptLin
52.	$[[14, 8, 3/3]]_4$	AddCyclic S-Ort	8	0	Optimal Optimal Cf. Table 7.3
53.	$[[14, 7, 4/3]]_4$	AddCyclic	7	0	Optimal
54.	$[[14, 5, 5/3]]_4$	AddCyclic	11/2	1/2	reach bound OptLin
55.	$[[14, 4, 6/3]]_4$	AddCyclic	9/2	1/2	reach bound OptLin
56.	$[[14, 3, 7/3]]_4$	AddCyclic	7/2	1/2	reach bound OptLin
57.	$[[14, 3/2, 8/3]]_4$	AddCyclic	5/2	1	may be Optimal
58.	$[[14, 6, 4/4]]_4$	AddCyclic S-Ort	6	0	Optimal Optimal Cf. Table 7.3
59.	$[[14, 4, 5/4]]_4$	AddCyclic	9/2	1/2	reach bound OptLin
60.	$[[14, 3, 6/4]]_4$	AddCyclic	7/2	1/2	reach bound OptLin
61.	$[[15, 11, 3/2]]_4$	BKLC	11	0	Optimal
62.	$[[15, 10, 4/2]]_4$	BKLC	10	0	Optimal
63.	$[[15, 8, 5/2]]_4$	BKLC	17/2	0	Optimal
64.	$[[15, 7, 6/2]]_4$	BKLC	15/2	1/2	OptLin
65.	$[[15, 6, 7/2]]_4$	BKLC	13/2	1/2	OptLin
66.	$[[15, 3, 10/2]]_4$	BKLC	3	0	Optimal
67.	$[[15, 2, 11/2]]_4$	BKLC	2	0	Optimal
68.	$[[15, 9, 3/3]]_4$	Cyclic S-Ort	9	0	Optimal Optimal Cf. Table 7.3
69.	$[[15, 8, 4/3]]_4$	Cyclic	8	0	Optimal
70.	$[[15, 6, 5/3]]_4$	Cyclic	13/2	1/2	OptLin
71.	$[[15, 5, 6/3]]_4$	Cyclic	11/2	1/2	OptLin
72.	$[[15, 4, 7/3]]_4$	Cyclic	9/2	1/2	OptLin
73.	$[[15, 1, 10/3]]_4$	Cyclic	1	0	Optimal
74.	$[[15, 5, 5/4]]_4$	Cyclic	11/2	1/2	OptLin
75.	$[[15, 4, 6/4]]_4$	Cyclic	9/2	1/2	OptLin
76.	$[[16, 12, 3/2]]_4$	BKLC	12	0	Optimal
77.	$[[16, 11, 4/2]]_4$	BKLC	11	0	Optimal
78.	$[[16, 9, 5/2]]_4$	BKLC	19/2	1/2	OptLin
79.	$[[16, 8, 6/2]]_4$	BKLC	17/2	1/2	OptLin
80.	$[[16, 7, 7/2]]_4$	BKLC	15/2	1/2	OptLin
81.	$[[16, 6, 8/2]]_4$	BKLC	13/2	1/2	OptLin
82.	$[[16, 3, 11/2]]_4$	BKLC	3	0	Optimal
83.	$[[16, 2, 12/2]]_4$	BKLC	2	0	Optimal
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
84.	$[[16, 10, 3/3]]_4$	BKLC	10	0	Optimal Cf. Table 7.3
85.	$[[17, 13, 3/2]]_4$	BKLC	13	0	Optimal
86.	$[[17, 12, 4/2]]_4$	BKLC	12	0	Optimal
87.	$[[17, 10, 5/2]]_4$	BKLC	21/2	1/2	OptLin
88.	$[[17, 9, 6/2]]_4$	BKLC	19/2	1/2	OptLin
89.	$[[17, 8, 7/2]]_4$	BKLC	17/2	1/2	OptLin
90.	$[[17, 9, 4/4]]_4$	Cyclic S-Ort	9	0	Optimal Optimal Cf. Table 7.3
91.	$[[17, 5, 7/4]]_4$	Cyclic	11/2	1/2	OptLin
92.	$[[17, 4, 8/4]]_4$	Cyclic	9/2	1/2	OptLin
93.	$[[18, 14, 3/2]]_4$	BKLC	14	0	Optimal
94.	$[[18, 12, 4/2]]_4$	BKLC	25/2	1/2	OptLin
95.	$[[18, 11, 5/2]]_4$	BKLC	23/2	1/2	OptLin
96.	$[[18, 10, 6/2]]_4$	BKLC	21/2	1/2	OptLin
97.	$[[18, 8, 8/2]]_4$	BKLC	17/2	1/2	OptLin
98.	$[[18, 5, 10/2]]_4$	BKLC	11/2	1/2	OptLin
99.	$[[19, 15, 3/2]]_4$	BKLC	15	0	OptLin
100.	$[[19, 13, 4/2]]_4$	BKLC	27/2	1/2	OptLin
101.	$[[19, 12, 5/2]]_4$	BKLC	25/2	1/2	OptLin
102.	$[[19, 11, 6/2]]_4$	BKLC	23/2	1/2	OptLin
103.	$[[20, 16, 3/2]]_4$	BKLC	16	0	OptLin
104.	$[[20, 14, 4/2]]_4$	BKLC	29/2	1/2	OptLin
105.	$[[20, 13, 5/2]]_4$	BKLC	27/2	1/2	OptLin
106.	$[[20, 12, 6/2]]_4$	BKLC	25/2	1/2	OptLin
107.	$[[20, 10, 7/2]]_4$	BKLC	21/2	1/2	OptLin
108.	$[[21, 17, 3/2]]_4$	BKLC	17	0	Optimal
109.	$[[21, 15, 4/2]]_4$	BKLC	31/2	1/2	OptLin
110.	$[[21, 14, 5/2]]_4$	BKLC	14	0	Optimal
111.	$[[21, 11, 7/2]]_4$	BKLC	23/2	1/2	OptLin
112.	$[[21, 15, 3/3]]_4$	S-Ort	15	0	Optimal Cf. Table 7.3
113.	$[[22, 17, 3/2]]_4$	BKLC	35/2	1/2	OptLin
114.	$[[22, 16, 4/2]]_4$	BKLC	33/2	1/2	OptLin
115.	$[[22, 4, 14/2]]_4$	BKLC	9/2	1/2	OptLin
116.	$[[23, 18, 3/2]]_4$	BKLC	37/2	1/2	OptLin
117.	$[[23, 17, 4/2]]_4$	BKLC	35/2	1/2	OptLin
118.	$[[23, 4, 15/2]]_4$	BKLC	9/2	1/2	OptLin
119.	$[[24, 19, 3/2]]_4$	BKLC	39/2	1/2	OptLin
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
120.	$[[24, 18, 4/2]]_4$	BKLC	37/2	1/2	OptLin
121.	$[[24, 8, 12/2]]_4$	BKLC	17/2	1/2	OptLin
122.	$[[25, 20, 3/2]]_4$	BKLC	41/2	1/2	OptLin
123.	$[[25, 19, 4/2]]_4$	BKLC	39/2	1/2	OptLin
124.	$[[26, 21, 3/2]]_4$	BKLC	43/2	1/2	OptLin
125.	$[[26, 20, 4/2]]_4$	BKLC	41/2	1/2	OptLin
126.	$[[26, 10, 12/2]]_4$	BKLC	21/2	1/2	OptLin
127.	$[[27, 22, 3/2]]_4$	BKLC	45/2	1/2	OptLin
128.	$[[27, 21, 4/2]]_4$	BKLC	43/2	1/2	OptLin
129.	$[[28, 23, 3/2]]_4$	BKLC	47/2	1/2	OptLin
130.	$[[28, 22, 4/2]]_4$	BKLC	45/2	1/2	OptLin
131.	$[[28, 13, 11/2]]_4$	BKLC	27/2	1/2	OptLin
132.	$[[28, 12, 12/2]]_4$	BKLC	25/2	1/2	OptLin
133.	$[[29, 24, 3/2]]_4$	BKLC	49/2	1/2	OptLin
134.	$[[29, 23, 4/2]]_4$	BKLC	47/2	1/2	OptLin
135.	$[[30, 22, 5/2]]_4$	BKLC	45/2	1/2	OptLin
136.	$[[30, 14, 12/2]]_4$	BKLC	29/2	1/2	OptLin

Table 9.5: Optimal and Good Pure Asymmetric CSS-like Codes over $\mathbb{F}_4$

In Tables 9.6 and 9.7, explicit choices for nested additive cyclic and cyclic codes, respectively, yielding optimal or good AQECCs are listed down. We use the notations indicated in Theorem 6.1.3 and the abbreviation already detailed above.

C and D	Generator Polynomials	Code Q
$(6, 2^6, 4)_4$	$g_4(x) = (1011) + w(11), g_2(x) = (111111)$	$[[6, 2, 4/2]]_4$
$(6, 2^2, 6)_4$	$(10101)g_4(x), (1)g_2(x)$	
$(6, 2^7, 3)_4$	$g_4(x) = (101) + w(11), g_2(x) = (10101)$	$[[6, 1, 3/3]]_4$
$(6, 2^5, 4)_4$	$(11)g_4(x), (11)g_2(x)$	
$(12, 2^4, 9)_4$	$g_4(x) = (00100010001) + w(1100110011),$ $g_2(x) = (111111111111)$	$[[12, 1, 9/2]]_4$
$(12, 2^2, 12)_4$	$(101)g_4(x), (1)g_2(x)$	
$(12, 2^{18}, 3)_4$	$g_4(x) = (0001) + w(11), g_2(x) = (101101)$	$[[12, 6, 3/3]]_4$
$(12, 2^6, 8)_4$	$(1101011)g_4(x), (1101011)g_2(x)$	
$(12, 2^{12}, 6)_4$	$g_4(x) = (001110101) + w(11), g_2(x) = (111111111111)$	$[[12, 3, 6/3]]_4$
$(12, 2^6, 8)_4$	$(1101011)g_4(x), (1)g_2(x)$	
$(12, 2^7, 7)_4$	$g_4(x) = (1000010011) + w(1110111), g_2(x) = (111111111111)$	$[[12, 1/2, 7/3]]_4$
$(12, 2^6, 8)_4$	$(1)g_4(x), (11)g_2(x)$	
<i>continued on next page</i>		

<i>continued from previous page</i>		
<i>C and D</i>	Generator Polynomials	Code <i>Q</i>
$(12, 2^{16}, 4)_4$	$g_4(x) = (1101) + w(111), g_2(x) = (1110111)$	$[[12, 4, 4/4]]_4$
$(12, 2^8, 6)_4$	$(10101)g_4(x), (10101)g_2(x)$	
$(12, 2^{12}, 5)_4$	$g_4(x) = (1000101) + w(111), g_2(x) = (11011011011)$	$[[12, 2, 5/4]]_4$
$(12, 2^8, 7)_4$	$(10101)g_4(x), (1)g_2(x)$	
$(12, 2^{10}, 6)_4$	$g_4(x) = (01100101) + w(10101), g_2(x) = (11011011011)$	$[[12, 1, 6/4]]_4$
$(12, 2^8, 6)_4$	$(111)g_4(x), (1)g_2(x)$	
$(12, 2^{13}, 5)_4$	$g_4(x) = (001101) + w(11), g_2(x) = (10101010101)$	$[[12, 1, 5/5]]_4$
$(12, 2^{11}, 5)_4$	$(11)g_4(x), (11)g_2(x)$	
$(14, 2^{22}, 3)_4$	$g_4(x) = (011) + w(1), g_2(x) = (1000101)$	$[[14, 8, 3/3]]_4$
$(14, 2^6, 10)_4$	$(101010001)g_4(x), (100010101)g_2(x)$	
$(14, 2^{20}, 4)_4$	$g_4(x) = (00001011) + w(1), g_2(x) = (101010001)$	$[[14, 7, 4/3]]_4$
$(14, 2^6, 10)_4$	$(101010001)g_4(x), (1010001)g_2(x)$	
$(14, 2^{22}, 3)_4$	$g_4(x) = (010111) + w(1), g_2(x) = (1000101)$	$[[14, 5, 5/3]]_4$
$(14, 2^{12}, 6)_4$	$(101)g_4(x), (100010101)g_2(x)$	
$(14, 2^{14}, 6)_4$	$g_4(x) = (110011101) + w(101), g_2(x) = (1010101010101)$	$[[14, 4, 6/3]]_4$
$(14, 2^6, 10)_4$	$(1010001)g_4(x), (101)g_2(x)$	
$(14, 2^{12}, 7)_4$	$g_4(x) = (010111011) + w(101), g_2(x) = (100000000000001)$	$[[14, 3, 7/3]]_4$
$(14, 2^6, 10)_4$	$(1000101)g_4(x), (1)g_2(x)$	
$(14, 2^9, 8)_4$	$g_4(x) = (0001001011) + w(111001), g_2(x) = (100000000000001)$	$[[14, 3/2, 8/3]]_4$
$(14, 2^6, 10)_4$	$(1101)g_4(x), (1)g_2(x)$	
$(14, 2^{20}, 4)_4$	$g_4(x) = (001011) + w(11), g_2(x) = (11001111)$	$[[14, 6, 4/4]]_4$
$(14, 2^8, 8)_4$	$(1010001)g_4(x), (1010001)g_2(x)$	
$(14, 2^{20}, 4)_4$	$g_4(x) = (01001) + w(1011), g_2(x) = (100111)$	$[[14, 4, 5/4]]_4$
$(14, 2^{12}, 6)_4$	$(101)g_4(x), (1010001)g_2(x)$	
$(14, 2^{14}, 6)_4$	$g_4(x) = (0001010111) + w(11), g_2(x) = (11111111111111)$	$[[14, 3, 6/4]]_4$
$(14, 2^8, 8)_4$	$(1000101)g_4(x), (1)g_2(x)$	

Table 9.6: Explicit Lists of Nested $\mathbb{F}_2$ -linear Cyclic Codes over $\mathbb{F}_4$ and the Resulting CSS-like Codes

<i>C and D</i>	Generator Polynomials	Code <i>Q</i>
$[11, 6, 5]_4$	$g_C(x) = (1w^211w1)$	$[[11, 1, 5/5]]_4$
$[11, 5, 6]_4$	$(11)g_C(x)$	
$[15, 12, 3]_4$	$g_C(x) = (w^2011)$	$[[15, 9, 3/3]]_4$
$[15, 3, 11]_4$	$(w^20w00w^210w1)g_C(x)$	
$[15, 12, 3]_4$	$g_C(x) = (w^2011)$	$[[15, 8, 4/3]]_4$
$[15, 4, 10]_4$	$(w^2w^2111ww^2w^21)g_C(x)$	
$[15, 12, 3]_4$	$g_C(x) = (w^2011)$	$[[15, 6, 5/3]]_4$
$[15, 6, 8]_4$	$(www0w^201)g_C(x)$	
$[15, 8, 6]_4$	$g_C(x) = (ww^2w0w0w^21)$	$[[15, 5, 6/3]]_4$
$[15, 3, 11]_4$	$(ww^20w01)g_C(x)$	
$[15, 12, 3]_4$	$g_C(x) = (w^2011)$	$[[15, 4, 7/3]]_4$
<i>continued on next page</i>		

<i>continued from previous page</i>		
C and D	Generator Polynomials	Code Q
$[15, 8, 6]_4$	$(1w^2w^2w^21)g_C(x)$	
$[15, 12, 3]_4$	$g_C(x) = (w^2011)$	$[[15, 1, 10/3]]_4$
$[15, 11, 4]_4$	$(w1)g_C(x)$	
$[15, 9, 5]_4$	$g_C(x) = (1w11w^2w^21)$	$[[15, 5, 5/4]]_4$
$[15, 4, 10]_4$	$(w^2w0w^201)g_C(x)$	
$[15, 8, 6]_4$	$g_C(x) = (ww^2w0w0w^21)$	$[[15, 4, 6/4]]_4$
$[15, 4, 10]_4$	$(w1001)g_C(x)$	
$[17, 13, 4]_4$	$g_C(x) = (11w11)$	$[[17, 9, 4/4]]_4$
$[17, 4, 12]_4$	$(1001111001)g_C(x)$	
$[17, 9, 7]_4$	$g_C(x) = (1w^20w^2w^2w^20w^21)$	$[[17, 5, 7/4]]_4$
$[17, 4, 12]_4$	$(1wwww1)g_C(x)$	
$[17, 8, 8]_4$	$g_C(x) = (1ww^2w^200w^2w^2w1)$	$[[17, 4, 8/4]]_4$
$[17, 4, 12]_4$	$(1w^21w^21)g_C(x)$	

Table 9.7: Explicit Lists of Nested Linear Cyclic Codes over $\mathbb{F}_4$ and the Resulting CSS-like Codes

9.2.4 Optimal Pure 5-ary AQECCs

Here we present the table for optimal 5-ary pure asymmetric CSS codes.

No.	AQECC Q	Type	No.	AQECC Q	Type
1	$[[6, 2, 4/2]]_5$	Cyclic	93	$[[19, 3, 13/2]]_5$	BKLC
2	$[[7, 2, 4/2]]_5$	BKLC	94	$[[19, 2, 14/2]]_5$	BKLC
3	$[[7, 3, 3/2]]_5$	BKLC	95	$[[20, 16, 3/2]]_5$	Cyclic, BKLC
4	$[[8, 4, 3/2]]_5$	Cyclic	96	$[[20, 15, 4/2]]_5$	BKLC
5	$[[8, 3, 4/2]]_5$	BKLC, GroupChar	97	$[[20, 13, 5/2]]_5$	BKLC
6	$[[8, 2, 5/2]]_5$	BKLC	98	$[[20, 12, 6/2]]_5$	BKLC
7	$[[8, 1, 6/2]]_5$	Cyclic, BKLC	99	$[[20, 5, 12/2]]_5$	BKLC
8	$[[8, 2, 3/3]]_5$	Cyclic	100	$[[20, 4, 13/2]]_5$	BKLC
9	$[[8, 1, 4/3]]_5$	Cyclic,	101	$[[20, 3, 14/2]]_5$	BKLC
10	$[[9, 4, 4/2]]_5$	BKLC	102	$[[20, 2, 15/2]]_5$	Cyclic, BKLC
11	$[[9, 3, 5/2]]_5$	BKLC	103	$[[20, 1, 16/2]]_5$	Cyclic
12	$[[9, 2, 6/2]]_5$	BKLC	104	$[[20, 14, 3/3]]_5$	Cyclic
13	$[[9, 1, 7/2]]_5$	BKLC	105	$[[21, 17, 3/2]]_5$	BKLC
14	$[[10, 6, 3/2]]_5$	Cyclic, BKLC	106	$[[21, 16, 4/2]]_5$	BKLC
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
15	$[[10, 5, 4/2]]_5$	Cyclic, BKLC	107	$[[21, 14, 5/2]]_5$	BKLC
16	$[[10, 4, 5/2]]_5$	BKLC	108	$[[21, 13, 6/2]]_5$	BKLC
17	$[[10, 3, 6/2]]_5$	BKLC	109	$[[21, 3, 15/2]]_5$	BKLC
18	$[[10, 2, 7/2]]_5$	BKLC	110	$[[21, 2, 16/2]]_5$	BKLC
19	$[[10, 1, 8/2]]_5$	Cyclic	111	$[[22, 18, 3/2]]_5$	BKLC
20	$[[10, 4, 3/3]]_5$	Cyclic	112	$[[22, 17, 4/2]]_5$	BKLC
21	$[[10, 3, 4/3]]_5$	Cyclic	113	$[[22, 15, 5/2]]_5$	BKLC
22	$[[10, 2, 4/4]]_5$	Cyclic	114	$[[22, 14, 6/2]]_5$	BKLC
23	$[[11, 7, 3/2]]_5$	BKLC	115	$[[22, 3, 16/2]]_5$	BKLC
24	$[[11, 6, 4/2]]_5$	BKLC	116	$[[22, 2, 17/2]]_5$	BKLC
25	$[[11, 5, 5/2]]_5$	Cyclic, BKLC	117	$[[23, 19, 3/2]]_5$	BKLC
26	$[[11, 4, 6/2]]_5$	BKLC	118	$[[23, 18, 4/2]]_5$	BKLC
27	$[[11, 3, 7/2]]_5$	BKLC	119	$[[23, 16, 5/2]]_5$	BKLC
28	$[[11, 2, 8/2]]_5$	BKLC	120	$[[23, 15, 6/2]]_5$	BKLC
29	$[[11, 1, 5/5]]_5$	Cyclic	121	$[[23, 3, 17/2]]_5$	BKLC
30	$[[12, 8, 3/2]]_5$	Cyclic, BKLC	122	$[[23, 2, 18/2]]_5$	BKLC
31	$[[12, 7, 4/2]]_5$	Cyclic, BKLC	123	$[[24, 20, 3/2]]_5$	Cyclic, BKLC
32	$[[12, 6, 5/2]]_5$	BKLC	124	$[[24, 19, 4/2]]_5$	Cyclic, BKLC
33	$[[12, 5, 6/2]]_5$	BKLC	125	$[[24, 4, 16/2]]_5$	BKLC
34	$[[12, 3, 7/2]]_5$	Cyclic	126	$[[24, 3, 18/2]]_5$	Cyclic, BKLC
35	$[[12, 3, 8/2]]_5$	BKLC	127	$[[24, 2, 19/2]]_5$	Cyclic, BKLC
36	$[[12, 1, 9/2]]_5$	Cyclic	128	$[[24, 18, 3/3]]_5$	Cyclic
37	$[[12, 6, 3/3]]_5$	Cyclic	129	$[[24, 17, 4/3]]_5$	Cyclic
38	$[[12, 5, 4/3]]_5$	Cyclic	130	$[[24, 1, 18/3]]_5$	Cyclic
39	$[[12, 1, 7/3]]_5$	Cyclic	131	$[[24, 16, 4/4]]_5$	Cyclic
40	$[[12, 4, 4/4]]_5$	Cyclic	132	$[[25, 21, 3/2]]_5$	BKLC
41	$[[13, 9, 3/2]]_5$	BKLC	133	$[[25, 20, 4/2]]_5$	BKLC
42	$[[13, 8, 4/2]]_5$	Cyclic, BKLC	134	$[[25, 18, 5/2]]_5$	BKLC
43	$[[13, 6, 5/2]]_5$	BKLC	135	$[[25, 17, 6/2]]_5$	BKLC
44	$[[13, 4, 7/2]]_5$	Cyclic, BKLC	136	$[[25, 8, 13/2]]_5$	BKLC
45	$[[13, 3, 8/2]]_5$	BKLC	137	$[[25, 5, 16/2]]_5$	BKLC
46	$[[13, 2, 9/2]]_5$	BKLC	138	$[[25, 3, 19/2]]_5$	BKLC
47	$[[13, 5, 4/4]]_5$	Cyclic	139	$[[25, 2, 20/2]]_5$	BKLC
48	$[[13, 1, 7/4]]_5$	Cyclic	140	$[[26, 22, 3/2]]_5$	BKLC
49	$[[14, 10, 3/2]]_5$	BKLC	141	$[[26, 21, 4/2]]_5$	BKLC
50	$[[14, 9, 4/2]]_5$	BKLC	142	$[[26, 19, 5/2]]_5$	BKLC
51	$[[14, 7, 5/2]]_5$	BKLC	143	$[[26, 18, 6/2]]_5$	BKLC
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
52	$[[14, 6, 6/2]]_5$	BKLC	144	$[[26, 6, 16/2]]_5$	BKLC
53	$[[14, 5, 7/2]]_5$	BKLC	145	$[[27, 23, 3/2]]_5$	BKLC
54	$[[14, 4, 8/2]]_5$	BKLC	146	$[[27, 21, 4/2]]_5$	BKLC
55	$[[14, 3, 9/2]]_5$	BKLC	147	$[[27, 20, 5/2]]_5$	BKLC
56	$[[14, 2, 10/2]]_5$	BKLC	148	$[[27, 19, 6/2]]_5$	BKLC
57	$[[14, 1, 11/2]]_5$	BKLC	149	$[[28, 24, 3/2]]_5$	BKLC
58	$[[15, 11, 3/2]]_5$	BKLC	150	$[[28, 22, 4/2]]_5$	BKLC
59	$[[15, 10, 4/2]]_5$	BKLC	151	$[[28, 21, 5/2]]_5$	BKLC
60	$[[15, 8, 5/2]]_5$	BKLC	152	$[[28, 20, 6/2]]_5$	BKLC
61	$[[15, 7, 6/2]]_5$	BKLC	153	$[[29, 25, 3/2]]_5$	BKLC
62	$[[15, 6, 7/2]]_5$	BKLC	154	$[[29, 23, 4/2]]_5$	BKLC
63	$[[15, 5, 8/2]]_5$	BKLC	155	$[[29, 22, 5/2]]_5$	BKLC
64	$[[15, 4, 9/2]]_5$	BKLC	156	$[[29, 13, 12/2]]_5$	BKLC
65	$[[15, 3, 10/2]]_5$	BKLC	157	$[[30, 26, 3/2]]_5$	BKLC
66	$[[15, 2, 11/2]]_5$	BKLC	158	$[[30, 24, 4/2]]_5$	Cyclic, BKLC
67	$[[15, 1, 12/2]]_5$	Cyclic	159	$[[30, 23, 5/2]]_5$	BKLC
68	$[[16, 12, 3/2]]_5$	BKLC	160	$[[30, 14, 12/2]]_5$	BKLC
69	$[[16, 11, 4/2]]_5$	BKLC	161	$[[30, 20, 4/4]]_5$	Cyclic
70	$[[16, 9, 5/2]]_5$	BKLC	162	$[[31, 27, 3/2]]_5$	Cyclic, BKLC
71	$[[16, 8, 6/2]]_5$	BKLC	163	$[[31, 25, 4/2]]_5$	BKLC
72	$[[16, 7, 7/2]]_5$	BKLC	164	$[[31, 25, 3/3]]_5$	Cyclic
73	$[[16, 3, 11/2]]_5$	BKLC	165	$[[32, 26, 4/2]]_5$	BKLC
74	$[[16, 2, 12/2]]_5$	BKLC	166	$[[33, 28, 3/2]]_5$	BKLC
75	$[[17, 13, 3/2]]_5$	BKLC	167	$[[33, 27, 4/2]]_5$	BKLC
76	$[[17, 12, 4/2]]_5$	BKLC	168	$[[34, 29, 3/2]]_5$	BKLC
77	$[[17, 10, 5/2]]_5$	BKLC	169	$[[34, 28, 4/2]]_5$	BKLC
78	$[[17, 9, 6/2]]_5$	BKLC	170	$[[35, 30, 3/2]]_5$	BKLC
79	$[[17, 8, 7/2]]_5$	BKLC	171	$[[35, 29, 4/2]]_5$	BKLC
80	$[[17, 3, 11/2]]_5$	BKLC	172	$[[35, 1, 28/2]]_5$	Cyclic
81	$[[18, 14, 3/2]]_5$	BKLC	173	$[[36, 31, 3/2]]_5$	BKLC
82	$[[18, 13, 4/2]]_5$	BKLC	174	$[[36, 30, 4/2]]_5$	BKLC
83	$[[18, 11, 5/2]]_5$	BKLC	175	$[[37, 32, 3/2]]_5$	BKLC
84	$[[18, 10, 6/2]]_5$	BKLC	176	$[[37, 31, 4/2]]_5$	BKLC
85	$[[18, 4, 11/2]]_5$	BKLC	177	$[[38, 33, 3/2]]_5$	BKLC
86	$[[18, 3, 12/2]]_5$	BKLC	178	$[[38, 32, 4/2]]_5$	BKLC
87	$[[19, 15, 3/2]]_5$	BKLC	179	$[[39, 34, 3/2]]_5$	Cyclic, BKLC
88	$[[19, 14, 4/2]]_5$	BKLC	180	$[[39, 33, 4/2]]_5$	BKLC
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
89	$[[19, 12, 5/2]]_5$	BKLC	181	$[[39, 31, 3/3]]_5$	Cyclic
90	$[[19, 11, 6/2]]_5$	BKLC	182	$[[40, 35, 3/2]]_5$	Cyclic, BKLC
91	$[[19, 5, 11/2]]_5$	BKLC	183	$[[40, 34, 4/2]]_5$	BKLC
92	$[[19, 4, 12/2]]_5$	BKLC	184	$[[40, 1, 32/2]]_5$	Cyclic

Table 9.8: Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_5$

Table 9.9 contains the pairs of cyclic codes yielding optimal pure asymmetric 5-ary quantum codes.

C and D	Generator Polynomials	Code Q
$[6, 3, 4]_5$	$g_C(x) = (1221)$	$[[6, 2, 4/2]]_5$
$[6, 1, 6]_5$	$(141)g_C(x)$	
$[8, 7, 2]_5$	$g_C(x) = (11)$	$[[8, 4, 3/2]]_5$
$[8, 3, 4]_5$	$(11021)g_C(x)$	
$[8, 7, 2]_5$	$g_C(x) = (11)$	$[[8, 3, 4/2]]_5$
$[8, 4, 4]_5$	$(4221)g_C(x)$	
$[8, 7, 2]_5$	$g_C(x) = (11)$	$[[8, 1, 6/2]]_5$
$[8, 6, 2]_5$	$(21)g_C(x)$	
$[8, 5, 3]_5$	$g_C(x) = (2211)$	$[[8, 2, 3/3]]_5$
$[8, 3, 4]_5$	$(311)g_C(x)$	
$[8, 5, 3]_5$	$g_C(x) = (2211)$	$[[8, 1, 4/3]]_5$
$[8, 4, 4]_5$	$(21)g_C(x)$	
$[10, 7, 3]_5$	$g_C(x) = (4411)$	$[[10, 6, 3/2]]_5$
$[10, 1, 10]_5$	$(4030201)g_C(x)$	
$[10, 6, 4]_5$	$g_C(x) = (42031)$	$[[10, 5, 4/2]]_5$
$[10, 1, 10]_5$	$(113311)g_C(x)$	
$[10, 2, 8]_5$	$g_C(x) = (432104321)$	$[[10, 1, 8/2]]_5$
$[10, 1, 10]_5$	$(41)g_C(x)$	
$[10, 7, 3]_5$	$g_C(x) = (4411)$	$[[10, 4, 3/3]]_5$
$[10, 3, 5]_5$	$(10301)g_C(x)$	
$[10, 7, 3]_5$	$g_C(x) = (4411)$	$[[10, 3, 4/3]]_5$
$[10, 4, 5]_5$	$(4411)g_C(x)$	
$[10, 6, 4]_5$	$g_C(x) = (42031)$	$[[10, 2, 4/4]]_5$
$[10, 4, 5]_5$	$(401)g_C(x)$	
$[11, 6, 5]_5$	$g_C(x) = (431441)$	$[[11, 5, 5/2]]_5$
$[11, 1, 11]_5$	$(411421)g_C(x)$	
<i>continued on next page</i>		

<i>continued from previous page</i>		
<i>C and D</i>	Generator Polynomials	Code Q
$[11, 6, 5]_5$	$g_C(x) = (431441)$	$[[11, 1, 5/5]]_5$
$[11, 5, 6]_5$	$(41)g_C(x)$	
$[12, 9, 3]_5$	$g_C(x) = (2331)$	$[[12, 8, 3/2]]_5$
$[12, 1, 12]_5$	$(411302441)g_C(x)$	
$[12, 8, 4]_5$	$g_C(x) = (33301)$	$[[12, 7, 4/2]]_5$
$[12, 1, 12]_5$	$(12144121)g_C(x)$	
$[12, 4, 7]_5$	$g_C(x) = (330213201)$	$[[12, 3, 7/2]]_5$
$[12, 1, 12]_5$	$(3441)g_C(x)$	
$[12, 11, 2]_5$	$g_C(x) = (11)$	$[[12, 1, 9/2]]_5$
$[12, 10, 2]_5$	$(21)g_C(x)$	
$[12, 9, 3]_5$	$g_C(x) = (2331)$	$[[12, 6, 3/3]]_5$
$[12, 3, 8]_5$	$(2313311)g_C(x)$	
$[12, 9, 3]_5$	$g_C(x) = (2331)$	$[[12, 5, 4/3]]_5$
$[12, 4, 6]_5$	$(232141)g_C(x)$	
$[12, 9, 3]_5$	$g_C(x) = (2331)$	$[[12, 1, 7/3]]_5$
$[12, 8, 4]_5$	$(11)g_C(x)$	
$[12, 8, 4]_5$	$g_C(x) = (33301)$	$[[12, 4, 4/4]]_5$
$[12, 4, 7]_5$	$(10401)g_C(x)$	
$[13, 9, 4]_5$	$g_C(x) = (11411)$	$[[13, 8, 4/2]]_5$
$[13, 1, 13]_5$	$(102343201)g_C(x)$	
$[13, 12, 2]_5$	$g_C(x) = (41)$	$[[13, 4, 7/2]]_5$
$[13, 8, 4]_5$	$(13031)g_C(x)$	
$[13, 9, 4]_5$	$g_C(x) = (11411)$	$[[13, 5, 4/4]]_5$
$[13, 4, 8]_5$	$(441411)g_C(x)$	
$[13, 9, 4]_5$	$g_C(x) = (11411)$	$[[13, 1, 7/4]]_5$
$[13, 8, 4]_5$	$(41)g_C(x)$	
$[15, 2, 12]_5$	$g_C(x) = (43210432104321)$	$[[15, 1, 12/2]]_5$
$[15, 1, 15]_5$	$(41)g_C(x)$	
$[20, 17, 3]_5$	$g_C(x) = (4021)$	$[[20, 16, 3/2]]_5$
$[20, 1, 20]_5$	$(14331311124411221)g_C(x)$	
$[20, 3, 15]_5$	$g_C(x) = (333210144241242301)$	$[[20, 2, 15/2]]_5$
$[20, 1, 20]_5$	$(121)g_C(x)$	
$[20, 2, 16]_5$	$g_C(x) = (4321043210432104321)$	$[[20, 1, 16/2]]_5$
$[20, 1, 20]_5$	$(41)g_C(x)$	
$[20, 17, 3]_5$	$g_C(x) = (4021)$	$[[20, 14, 3/3]]_5$
$[20, 3, 15]_5$	$(104020303020401)g_C(x)$	
$[24, 23, 2]_5$	$g_C(x) = (11)$	$[[24, 20, 3/2]]_5$
$[24, 3, 19]_5$	$(311434221121401242041)g_C(x)$	
$[24, 23, 2]_5$	$g_C(x) = (11)$	$[[24, 19, 4/2]]_5$
$[24, 4, 18]_5$	$(11022330241113140131)g_C(x)$	
<i>continued on next page</i>		

<i>continued from previous page</i>		
<i>C and D</i>	Generator Polynomials	Code Q
$[24, 4, 18]_5$	$g_C(x) = (142420213204333022331)$	$[[24, 3, 18/2]]_5$
$[24, 1, 24]_5$	$(2101)g_C(x)$	
$[24, 3, 19]_5$	$g_C(x) = (2034221230114132440431)$	$[[24, 2, 19/2]]_5$
$[24, 1, 24]_5$	$(331)g_C(x)$	
$[24, 21, 3]_5$	$g_C(x) = (1041)$	$[[24, 18, 3/3]]_5$
$[24, 3, 19]_5$	$(4241414203021111121)g_C(x)$	
$[24, 21, 3]_5$	$g_C(x) = (1041)$	$[[24, 17, 4/3]]_5$
$[24, 4, 18]_5$	$(124440331133044421)g_C(x)$	
$[24, 4, 18]_5$	$g_C(x) = (142420213204333022331)$	$[[24, 1, 18/3]]_5$
$[24, 3, 19]_5$	$(21)g_C(x)$	
$[24, 20, 4]_5$	$g_C(x) = (41131)$	$[[24, 16, 4/4]]_5$
$[24, 4, 18]_5$	$(40204040004010201)g_C(x)$	
$[30, 25, 4]_5$	$g_C(x) = (142241)$	$[[30, 24, 4/2]]_5$
$[30, 1, 30]_5$	$(4014024424320321311301401)g_C(x)$	
$[30, 25, 4]_5$	$g_C(x) = (142241)$	$[[30, 20, 4/4]]_5$
$[30, 5, 18]_5$	$(102030002040200030201)g_C(x)$	
$[31, 30, 2]_5$	$g_C(x) = (41)$	$[[31, 27, 3/2]]_5$
$[31, 3, 25]_5$	$(4131013234032212113312241021)g_C(x)$	
$[31, 28, 3]_5$	$g_C(x) = (4031)$	$[[31, 25, 3/3]]_5$
$[31, 3, 25]_5$	$(41200111423221200310021331)g_C(x)$	
$[35, 2, 28]_5$	$g_C(x) = (43210432104321043210432104321)$	$[[35, 1, 28/2]]_5$
$[35, 1, 35]_5$	$(41)g_C(x)$	
$[39, 35, 3]_5$	$g_C(x) = (14101)$	$[[39, 34, 3/2]]_5$
$[39, 1, 39]_5$	$(12214220043030014412330141321411011)g_C(x)$	
$[39, 35, 3]_5$	$g_C(x) = (14101)$	$[[39, 31, 3/3]]_5$
$[39, 4, 28]_5$	$(44111344333444200311122211244411)g_C(x)$	
$[40, 39, 2]_5$	$g_C(x) = (11)$	$[[40, 35, 3/2]]_5$
$[40, 4, 20]_5$	$(343224310313431222441243412031241001)g_C(x)$	
$[40, 2, 32]_5$	$g_C(x) = (142202344041330321101422023440413303211)$	$[[40, 1, 32/2]]_5$
$[40, 1, 40]_5$	$(21)g_C(x)$	

Table 9.9: Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_5$ and the Resulting CSS Codes

An $[[8, 3, 4/2]]_5$ -code can be derived via the character codes pair with $r_1 = 1$, $r_2 = 2$, $l = 3$, and $t = 2$.

9.2.5 Optimal Pure 7-ary AQECCs

Next, we provide the list of optimal 7-ary pure asymmetric CSS codes that we have been established so far in Table 9.10.

No.	AQECC Q	Type	No.	AQECC Q	Type
1.	$[[9, 5, 3/2]]_7$	GroupChar	77.	$[[17, 5, 10/2]]_7$	BKLC
2.	$[[9, 4, 4/2]]_7$	BKLC	78.	$[[17, 4, 11/2]]_7$	BKLC
3.	$[[9, 3, 5/2]]_7$	BKLC	79.	$[[17, 3, 12/2]]_7$	BKLC
4.	$[[9, 2, 6/2]]_7$	BKLC, GroupChar	80.	$[[17, 2, 13/2]]_7$	BKLC
5.	$[[9, 1, 7/2]]_7$	BKLC	81.	$[[17, 1, 14/2]]_7$	BKLC
6.	$[[10, 6, 3/2]]_7$	BKLC	82.	$[[18, 14, 3/2]]_7$	BKLC
7.	$[[10, 5, 4/2]]_7$	BKLC	83.	$[[18, 13, 4/2]]_7$	BKLC
8.	$[[10, 4, 5/2]]_7$	BKLC	84.	$[[18, 12, 5/2]]_7$	BKLC
9.	$[[10, 3, 6/2]]_7$	BKLC	85.	$[[18, 8, 8/2]]_7$	BKLC
10.	$[[10, 2, 7/2]]_7$	BKLC	86.	$[[18, 7, 9/2]]_7$	BKLC
11.	$[[10, 1, 8/2]]_7$	BKLC	87.	$[[18, 5, 11/2]]_7$	BKLC
12.	$[[11, 7, 3/2]]_7$	BKLC	88.	$[[18, 4, 12/2]]_7$	BKLC
13.	$[[11, 6, 4/2]]_7$	BKLC	89.	$[[18, 3, 13/2]]_7$	BKLC
14.	$[[11, 5, 5/2]]_7$	BKLC	90.	$[[18, 2, 14/2]]_7$	BKLC
15.	$[[11, 4, 6/2]]_7$	BKLC	91.	$[[18, 1, 15/2]]_7$	BKLC, Cyclic
16.	$[[11, 3, 7/2]]_7$	BKLC	92.	$[[19, 15, 3/2]]_7$	BKLC, Cyclic
17.	$[[11, 2, 8/2]]_7$	BKLC	93.	$[[19, 14, 4/2]]_7$	BKLC
18.	$[[11, 1, 9/2]]_7$	BKLC	94.	$[[19, 9, 8/2]]_7$	BKLC, Cyclic
19.	$[[12, 8, 3/2]]_7$	BKLC, Cyclic	95.	$[[19, 8, 9/2]]_7$	BKLC
20.	$[[12, 7, 4/2]]_7$	BKLC, Cyclic	96.	$[[19, 5, 12/2]]_7$	BKLC
21.	$[[12, 6, 5/2]]_7$	BKLC	97.	$[[19, 4, 13/2]]_7$	BKLC
22.	$[[12, 5, 6/2]]_7$	BKLC	98.	$[[19, 3, 14/2]]_7$	BKLC
23.	$[[12, 4, 7/2]]_7$	BKLC	99.	$[[19, 2, 15/2]]_7$	BKLC
24.	$[[12, 3, 8/2]]_7$	BKLC	100.	$[[19, 13, 3/3]]_7$	Cyclic
25.	$[[12, 2, 9/2]]_7$	BKLC	101.	$[[19, 7, 8/3]]_7$	Cyclic
26.	$[[12, 1, 10/2]]_7$	BKLC, Cyclic	102.	$[[19, 6, 9/3]]_7$	Cyclic
27.	$[[12, 6, 3/3]]_7$	Cyclic	103.	$[[19, 3, 12/3]]_7$	Cyclic
28.	$[[12, 5, 4/3]]_7$	Cyclic	104.	$[[19, 1, 8/8]]_7$	Cyclic
29.	$[[12, 4, 4/4]]_7$	Cyclic	105.	$[[20, 16, 3/2]]_7$	BKLC
30.	$[[13, 9, 3/2]]_7$	BKLC	106.	$[[20, 15, 4/2]]_7$	BKLC
31.	$[[13, 8, 4/2]]_7$	BKLC	107.	$[[20, 9, 9/2]]_7$	BKLC

continued on next page

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
32.	$[[13, 7, 5/2]]_7$	BKLC	108.	$[[20, 4, 14/2]]_7$	BKLC
33.	$[[13, 6, 6/2]]_7$	BKLC	109.	$[[20, 3, 15/2]]_7$	BKLC
34.	$[[13, 5, 7/2]]_7$	BKLC	110.	$[[20, 2, 16/2]]_7$	BKLC
35.	$[[13, 4, 8/2]]_7$	BKLC	111.	$[[21, 17, 3/2]]_7$	BKLC, Cyclic
36.	$[[13, 3, 9/2]]_7$	BKLC	112.	$[[21, 16, 4/2]]_7$	BKLC
37.	$[[13, 2, 10/2]]_7$	BKLC	113.	$[[21, 2, 17/2]]_7$	BKLC
38.	$[[14, 10, 3/2]]_7$	BKLC, Cyclic	114.	$[[21, 1, 18/2]]_7$	Cyclic
39.	$[[14, 9, 4/2]]_7$	BKLC, Cyclic	115.	$[[21, 15, 3/3]]_7$	Cyclic
40.	$[[14, 8, 5/2]]_7$	BKLC	116.	$[[22, 18, 3/2]]_7$	BKLC
41.	$[[14, 7, 6/2]]_7$	BKLC	117.	$[[22, 17, 4/2]]_7$	BKLC
42.	$[[14, 6, 7/2]]_7$	BKLC	118.	$[[22, 2, 18/2]]_7$	BKLC
43.	$[[14, 4, 8/2]]_7$	BKLC	119.	$[[23, 19, 3/2]]_7$	BKLC
44.	$[[14, 3, 10/2]]_7$	BKLC	120.	$[[23, 18, 4/2]]_7$	BKLC
45.	$[[14, 2, 11/2]]_7$	BKLC	121.	$[[24, 20, 3/2]]_7$	BKLC, Cyclic
46.	$[[14, 1, 12/2]]_7$	Cyclic	122.	$[[24, 19, 4/2]]_7$	BKLC
47.	$[[14, 8, 3/3]]_7$	Cyclic	123.	$[[24, 2, 19/2]]_7$	BKLC
48.	$[[14, 7, 4/3]]_7$	Cyclic	124.	$[[24, 1, 20/2]]_7$	Cyclic
49.	$[[14, 6, 4/4]]_7$	Cyclic	125.	$[[24, 18, 3/3]]_7$	Cyclic
50.	$[[15, 11, 3/2]]_7$	BKLC	126.	$[[24, 17, 4/3]]_7$	Cyclic
51.	$[[15, 10, 4/2]]_7$	BKLC	127.	$[[24, 16, 4/4]]_7$	Cyclic
52.	$[[15, 9, 5/2]]_7$	BKLC	128.	$[[25, 21, 3/2]]_7$	BKLC
53.	$[[15, 8, 6/2]]_7$	BKLC	129.	$[[25, 20, 4/2]]_7$	BKLC, Cyclic
54.	$[[15, 5, 8/2]]_7$	BKLC	130.	$[[25, 3, 19/2]]_7$	BKLC
55.	$[[15, 4, 9/2]]_7$	BKLC	131.	$[[25, 2, 20/2]]_7$	BKLC
56.	$[[15, 3, 10/2]]_7$	BKLC	132.	$[[25, 17, 4/4]]_7$	Cyclic
57.	$[[15, 2, 12/2]]_7$	BKLC	133.	$[[26, 22, 3/2]]_7$	BKLC
58.	$[[16, 12, 3/2]]_7$	BKLC, Cyclic	134.	$[[26, 21, 4/2]]_7$	BKLC
59.	$[[16, 11, 4/2]]_7$	BKLC, Cyclic	135.	$[[26, 3, 20/2]]_7$	BKLC
60.	$[[16, 10, 5/2]]_7$	BKLC	136.	$[[26, 2, 21/2]]_7$	BKLC
61.	$[[16, 6, 8/2]]_7$	BKLC, Cyclic	137.	$[[27, 23, 3/2]]_7$	BKLC
62.	$[[16, 5, 9/2]]_7$	BKLC	138.	$[[27, 22, 4/2]]_7$	BKLC
63.	$[[16, 4, 10/2]]_7$	BKLC, Cyclic	139.	$[[27, 2, 22/2]]_7$	BKLC
64.	$[[16, 3, 11/2]]_7$	BKLC	140.	$[[28, 24, 3/2]]_7$	BKLC
65.	$[[16, 2, 12/2]]_7$	BKLC, Cyclic	141.	$[[28, 23, 4/2]]_7$	BKLC
66.	$[[16, 10, 3/3]]_7$	Cyclic	142.	$[[28, 2, 23/2]]_7$	BKLC
67.	$[[16, 9, 4/3]]_7$	Cyclic	143.	$[[28, 1, 24/2]]_7$	Cyclic
68.	$[[16, 4, 8/3]]_7$	Cyclic	144.	$[[29, 25, 3/2]]_7$	BKLC
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	No.	AQECC Q	Type
69.	$[[16, 2, 10/3]]_7$	Cyclic	145.	$[[29, 24, 4/2]]_7$	BKLC
70.	$[[16, 8, 4/4]]_7$	Cyclic	146.	$[[29, 22, 5/2]]_7$	BKLC
71.	$[[16, 3, 8/4]]_7$	Cyclic	147.	$[[29, 2, 24/2]]_7$	BKLC
72.	$[[17, 13, 3/2]]_7$	BKLC	148.	$[[30, 26, 3/2]]_7$	BKLC
73.	$[[17, 12, 4/2]]_7$	BKLC	149.	$[[30, 25, 4/2]]_7$	BKLC
74.	$[[17, 11, 5/2]]_7$	BKLC	150.	$[[30, 23, 5/2]]_7$	BKLC
75.	$[[17, 7, 8/2]]_7$	BKLC	151.	$[[30, 22, 6/2]]_7$	BKLC
76.	$[[17, 6, 9/2]]_7$	BKLC	152.	$[[30, 1, 25/2]]_7$	Cyclic

Table 9.10: Optimal Pure Asymmetric CSS Codes over $\mathbb{F}_7$

Table 9.11 contains the pairs of cyclic codes yielding optimal pure asymmetric 7-ary quantum codes. In the case where we have both the BKLC and the cyclic constructions for a particular set of parameters, we do not include the cyclic pair.

C and D	Generator Polynomials	Code Q
$[12, 9, 3]_7$	$g_C(x) = (2441)$	$[[12, 6, 3/3]]_7$
$[12, 3, 6]_7$	$(5651121)g_C(x)$	
$[12, 8, 4]_7$	$g_C(x) = (16261)$	$[[12, 5, 4/3]]_7$
$[12, 3, 6]_7$	$(412621)g_C(x)$	
$[12, 8, 4]_7$	$g_C(x) = (16261)$	$[[12, 4, 4/4]]_7$
$[12, 4, 6]_7$	$(21121)g_C(x)$	
$[14, 13, 2]_7$	$g_C(x) = (11)$	$[[14, 1, 12/2]]_7$
$[14, 12, 2]_7$	$(11)g_C(x)$	
$[14, 11, 3]_7$	$g_C(x) = (6611)$	$[[14, 8, 3/3]]_7$
$[14, 3, 7]_7$	$(622106551)g_C(x)$	
$[14, 11, 3]_7$	$g_C(x) = (6611)$	$[[14, 7, 4/3]]_7$
$[14, 4, 7]_7$	$(66334411)g_C(x)$	
$[14, 10, 4]_7$	$g_C(x) = (65021)$	$[[14, 6, 4/4]]_7$
$[14, 4, 7]_7$	$(6030401)g_C(x)$	
$[16, 13, 3]_7$	$g_C(x) = (1051)$	$[[16, 10, 3/3]]_7$
$[16, 3, 12]_7$	$(13203030241)g_C(x)$	
$[16, 12, 4]_7$	$g_C(x) = (63031)$	$[[16, 9, 4/3]]_7$
$[16, 3, 12]_7$	$(1340044061)g_C(x)$	
$[16, 7, 8]_7$	$g_C(x) = (1265630161)$	$[[16, 4, 8/3]]_7$
<i>continued on next page</i>		

<i>continued from previous page</i>		
<i>C</i> and <i>D</i>	Generator Polynomials	Code <i>Q</i>
$[16, 3, 12]_7$	$(60211)g_C(x)$	
$[16, 5, 10]_7$	$g_C(x) = (611361010341)$	$[[16, 2, 10/3]]_7$
$[16, 3, 12]_7$	$(131)g_C(x)$	
$[16, 12, 4]_7$	$g_C(x) = (16511)$	$[[16, 8, 4/4]]_7$
$[16, 4, 8]_7$	$(103020301)g_C(x)$	
$[16, 7, 8]_7$	$g_C(x) = (1626554051)$	$[[16, 3, 8/4]]_7$
$[16, 4, 8]_7$	$(1551)g_C(x)$	
$[19, 16, 3]_7$	$g_C(x) = (6331)$	$[[19, 13, 3/3]]_7$
$[19, 3, 15]_7$	$(62600465666441)g_C(x)$	
$[19, 10, 8]_7$	$g_C(x) = (6520313561)$	$[[19, 7, 8/3]]_7$
$[19, 3, 15]_7$	$(66666221)g_C(x)$	
$[19, 16, 3]_7$	$g_C(x) = (6331)$	$[[19, 6, 9/3]]_7$
$[19, 10, 8]_7$	$(1203561)g_C(x)$	
$[19, 6, 12]_7$	$g_C(x) = (63116244011501)$	$[[19, 3, 12/3]]_7$
$[19, 3, 15]_7$	$(6331)g_C(x)$	
$[19, 10, 8]_7$	$g_C(x) = (6520313561)$	$[[19, 1, 8/8]]_7$
$[19, 9, 9]_7$	$(61)g_C(x)$	
$[21, 2, 18]_7$	$g_C(x) = (35152206323440564611)$	$[[21, 1, 18/2]]_7$
$[21, 1, 21]_7$	$(31)g_C(x)$	
$[21, 18, 3]_7$	$g_C(x) = (3121)$	$[[21, 15, 3/3]]_7$
$[21, 3, 14]_7$	$(3443550331556441)g_C(x)$	
$[24, 2, 20]_7$	$g_C(x) = (25641025641025641025641)$	$[[24, 1, 20/2]]_7$
$[24, 1, 24]_7$	$(61)g_C(x)$	
$[24, 21, 3]_7$	$g_C(x) = (2031)$	$[[24, 18, 3/3]]_7$
$[24, 3, 18]_7$	$(5203204022050526551)g_C(x)$	
$[24, 20, 4]_7$	$g_C(x) = (65161)$	$[[24, 17, 4/3]]_7$
$[24, 3, 18]_7$	$(300162464233164141)g_C(x)$	
$[24, 20, 4]_7$	$g_C(x) = (65161)$	$[[24, 16, 4/4]]_7$
$[24, 4, 16]_7$	$(25340520601502331)g_C(x)$	
$[25, 21, 4]_7$	$g_C(x) = (14041)$	$[[25, 17, 4/4]]_7$
$[25, 4, 19]_7$	$(636241612561635141)g_C(x)$	
$[28, 27, 2]_7$	$g_C(x) = (11)$	$[[28, 1, 24/2]]_7$
$[28, 26, 2]_7$	$(11)g_C(x)$	
$[30, 29, 2]_7$	$g_C(x) = (11)$	$[[30, 1, 25/2]]_7$
$[30, 28, 2]_7$	$(31)g_C(x)$	

Table 9.11: Explicit Lists of Nested Cyclic Codes over $\mathbb{F}_7$ and the Resulting CSS Codes

There are two specific codes derived from nested group character codes. Using the notation of Theorem 6.2.5, we can explicitly state that we get a $[[9, 5, 3/2]]_7$ -code by setting $r_1 = 1$, $r_2 = 3$, $l = 2$, and $t = 3$. A $[[9, 2, 6/2]]_7$ -code can be derived from $r_1 = 2$, $r_2 = 3$, $l = 2$, and $t = 3$.

9.2.6 Optimal and Good Pure 8-ary AQECCs

For brevity, let us use the convention that $\mathbb{F}_8 = \mathbb{F}_2(w)$ where w is a primitive root of an irreducible polynomial of degree 3 in $\mathbb{F}_2[X]$. When optimality can not be immediately established but it is known that the best possible value from a pair of nested $\mathbb{F}_8$ -linear codes is inferior, we write *better than OptLin*.

The list of optimal and good 8-ary pure asymmetric CSS-like codes that we have managed, at the moment, to ascertain is given in Table 9.12.

No.	AQECC Q	Type	LP	Defect	Remarks
1.	$[[10, 19/3, 3/2]]_8$	AddCyclic	20/3	1/3	better than OptLin
2.	$[[10, 6, 4/2]]_8$	BKLC	6	0	OptLin
3.	$[[10, 4, 5/2]]_8$	BKLC	14/3	2/3	OptLin
4.	$[[10, 3, 6/2]]_8$	BKLC	11/3	2/3	OptLin
5.	$[[10, 2, 8/2]]_8$	BKLC	2	0	OptLin
6.	$[[11, 7, 3/2]]_8$	BKLC	23/3	2/3	OptLin
7.	$[[11, 6, 4/2]]_8$	BKLC	20/3	2/3	OptLin
8.	$[[11, 5, 5/2]]_8$	BKLC	17/3	2/3	OptLin
9.	$[[11, 4, 6/2]]_8$	BKLC	14/3	2/3	OptLin
10.	$[[11, 3, 7/2]]_8$	BKLC	11/3	2/3	OptLin
11.	$[[11, 2, 8/2]]_8$	BKLC	8/3	2/3	OptLin
12.	$[[11, 1, 9/2]]_8$	BKLC	5/3	2/3	OptLin
13.	$[[12, 8, 3/2]]_8$	BKLC	26/3	2/3	OptLin
14.	$[[12, 7, 4/2]]_8$	BKLC	23/3	2/3	OptLin
15.	$[[12, 6, 5/2]]_8$	BKLC	20/3	2/3	OptLin
16.	$[[12, 5, 6/2]]_8$	BKLC	17/3	2/3	OptLin
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
17.	$[[12, 4, 7/2]]_8$	BKLC	14/3	2/3	OptLin
18.	$[[12, 3, 8/2]]_8$	BKLC	11/3	2/3	OptLin
19.	$[[12, 2, 9/2]]_8$	BKLC	8/3	2/3	OptLin
20.	$[[12, 1, 10/2]]_8$	BKLC	4/3	1/3	OptLin
21.	$[[13, 9, 3/2]]_8$	BKLC	29/3	2/3	OptLin
22.	$[[13, 8, 4/2]]_8$	Cyclic	26/3	2/3	OptLin
23.	$[[13, 7, 5/2]]_8$	BKLC	23/3	2/3	OptLin
24.	$[[13, 6, 6/2]]_8$	BKLC	20/3	2/3	OptLin
25.	$[[13, 5, 7/2]]_8$	BKLC	17/3	2/3	OptLin
26.	$[[13, 4, 8/2]]_8$	BKLC	14/3	2/3	OptLin
27.	$[[13, 3, 9/2]]_8$	BKLC	11/3	2/3	OptLin
28.	$[[13, 2, 10/2]]_8$	BKLC	7/3	1/3	OptLin
29.	$[[13, 1, 11/2]]_8$	BKLC	4/3	1/3	OptLin
30.	$[[14, 10, 3/2]]_8$	Cyclic	32/3	2/3	OptLin
31.	$[[14, 9, 4/2]]_8$	Cyclic	29/3	2/3	OptLin
32.	$[[14, 8, 5/2]]_8$	BKLC	26/3	2/3	OptLin
33.	$[[14, 7, 6/2]]_8$	BKLC	23/3	2/3	OptLin
34.	$[[14, 6, 7/2]]_8$	BKLC	20/3	2/3	OptLin
35.	$[[14, 5, 8/2]]_8$	BKLC	17/3	2/3	OptLin
36.	$[[14, 4, 9/2]]_8$	BKLC	14/3	2/3	OptLin
37.	$[[14, 3, 10/2]]_8$	BKLC	10/3	1/3	OptLin
38.	$[[14, 2, 11/2]]_8$	BKLC	7/3	1/3	OptLin
39.	$[[14, 1, 12/2]]_8$	Cyclic	4/3	1/3	OptLin
40.	$[[15, 34/3, 3/2]]_8$	AddCyclic	35/3	1/3	better than OptLin
41.	$[[15, 31/3, 4/2]]_8$	AddCyclic	32/3	1/3	better than OptLin
42.	$[[15, 9, 5/2]]_8$	BKLC	29/3	2/3	OptLin
43.	$[[15, 8, 6/2]]_8$	BKLC	26/3	2/3	OptLin
44.	$[[15, 7, 7/2]]_8$	BKLC	23/3	2/3	OptLin
45.	$[[15, 6, 8/2]]_8$	BKLC	20/3	2/3	OptLin
46.	$[[15, 4, 10/2]]_8$	BKLC	13/3	1/3	OptLin
47.	$[[15, 3, 11/2]]_8$	BKLC	10/3	1/3	OptLin
48.	$[[15, 2, 12/2]]_8$	BKLC	7/3	1/3	OptLin
49.	$[[15, 29/3, 3/3]]_8$	AddCyclic	31/3	2/3	small defect
50.	$[[15, 26/3, 4/3]]_8$	AddCyclic	28/3	2/3	small defect
51.	$[[16, 12, 3/2]]_8$	BKLC	38/3	2/3	OptLin
52.	$[[16, 11, 4/2]]_8$	BKLC	35/3	2/3	OptLin
53.	$[[16, 10, 5/2]]_8$	BKLC	32/3	2/3	OptLin
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
54.	$[[16, 9, 6/2]]_8$	BKLC	29/3	2/3	OptLin
55.	$[[16, 7, 8/2]]_8$	BKLC	23/3	2/3	OptLin
56.	$[[16, 3, 12/2]]_8$	BKLC	10/3	1/3	OptLin
57.	$[[17, 40/3, 3/2]]_8$	AddCyclic	41/3	1/3	better than OptLin
58.	$[[17, 12, 4/2]]_8$	BKLC	38/3	2/3	OptLin
59.	$[[17, 11, 5/2]]_8$	BKLC	35/3	2/3	OptLin
60.	$[[17, 10, 6/2]]_8$	BKLC	32/3	2/3	OptLin
61.	$[[18, 14, 3/2]]_8$	BKLC	43/3	1/3	OptLin
62.	$[[18, 13, 4/2]]_8$	BKLC	41/3	2/3	OptLin
63.	$[[18, 12, 5/2]]_8$	BKLC	38/3	2/3	OptLin
64.	$[[18, 11, 6/2]]_8$	BKLC	35/3	2/3	OptLin
65.	$[[19, 15, 3/2]]_8$	BKLC	46/3	1/3	OptLin
66.	$[[19, 14, 4/2]]_8$	BKLC	43/3	1/3	OptLin
67.	$[[19, 13, 5/2]]_8$	BKLC	40/3	1/3	OptLin
68.	$[[19, 12, 6/2]]_8$	Cyclic	38/3	2/3	OptLin
69.	$[[20, 16, 3/2]]_8$	BKLC	49/3	1/3	OptLin
70.	$[[20, 15, 4/2]]_8$	BKLC	46/3	1/3	OptLin
71.	$[[20, 14, 5/2]]_8$	BKLC	43/3	1/3	OptLin
72.	$[[21, 17, 3/2]]_8$	Cyclic	52/3	1/3	OptLin
73.	$[[21, 16, 4/2]]_8$	Cyclic	49/3	1/3	OptLin
74.	$[[21, 15, 3/3]]_8$	Cyclic	47/3	2/3	OptLin
75.	$[[21, 14, 4/3]]_8$	Cyclic	44/3	2/3	OptLin
76.	$[[21, 13, 4/4]]_8$	Cyclic	41/3	2/3	OptLin
77.	$[[22, 18, 3/2]]_8$	BKLC	55/3	1/3	OptLin
78.	$[[22, 17, 4/2]]_8$	BKLC	52/3	1/3	OptLin
79.	$[[23, 19, 3/2]]_8$	BKLC	58/3	1/3	OptLin
80.	$[[23, 18, 4/2]]_8$	BKLC	55/3	1/3	OptLin
81.	$[[24, 20, 3/2]]_8$	BKLC	61/3	1/3	OptLin
82.	$[[24, 19, 4/2]]_8$	BKLC	58/3	1/3	OptLin
83.	$[[25, 21, 3/2]]_8$	BKLC	64/3	1/3	OptLin
84.	$[[25, 20, 4/2]]_8$	BKLC	61/3	1/3	OptLin
85.	$[[26, 22, 3/2]]_8$	BKLC	67/3	1/3	OptLin
86.	$[[26, 21, 4/2]]_8$	BKLC	64/3	1/3	OptLin
87.	$[[27, 23, 3/2]]_8$	BKLC	70/3	1/3	OptLin
88.	$[[27, 22, 4/2]]_8$	BKLC	67/3	1/3	OptLin

Table 9.12: Optimal and Good Pure Asymmetric CSS-like Codes over $\mathbb{F}_8$

Table 9.13 contains the pairs of $\mathbb{F}_2$ -linear cyclic codes yielding optimal or good

pure asymmetric 8-ary quantum codes.

C and D	Generator Polynomials	Code Q
$(10, 2^{22}, 3)_8$	$g_1(x) = (000011) + w(0) + w^2(1),$	$[[10, 19/3, 3/2]]_8$
$(10, 2^3, 10)_8$	$g_2(x) = (1101001) + w(1), g_3(x) = (101010101)$ $(1111111111)g_1(x),$ $(1111111111)g_2(x), (11)g_3(x)$	
$(15, 2^{37}, 3)_8$	$g_1(x) = (1001) + w(0) + w^2(111),$	$[[15, 34/3, 3/2]]_8$
$(15, 2^3, 15)_8$	$g_2(x) = (010011) + w(1), g_3(x) = (1001111)$ $(1001001001001)g_1(x),$ $(11011011011011)g_2(x), (1001110011)g_3(x)$	
$(15, 2^{34}, 4)_8$	$g_1(x) = (111011111) + w(0) + w^2(111),$	$[[15, 31/3, 4/2]]_8$
$(15, 2^3, 15)_8$	$g_2(x) = (0000111) + w(1), g_3(x) = (1001110011)$ $(1001001001001)(111)g_1(x),$ $(11011011011011)g_2(x) + (1001001001001)(011)g_1(x),$ $(1001111)g_3(x)$	
$(15, 2^{37}, 3)_8$	$g_1(x) = (1001) + w(0) + w^2(111),$	$[[15, 29/3, 3/3]]_8$
$(15, 2^8, 11)_8$	$g_2(x) = (010011) + w(1), g_3(x) = (1001111)$ $(1100111001)g_1(x),$ $(111101011001)g_2(x), (1001110011)g_3(x)$	
$(15, 2^{34}, 4)_8$	$g_1(x) = (110010011) + w(0) + w^2(111),$	$[[15, 26/3, 4/3]]_8$
$(15, 2^8, 12)_8$	$g_2(x) = (001101) + w(1), g_3(x) = (1001110011)$ $(1100111001)g_1(x), (100110101111)g_2(x),$ $(1001111)g_3(x)$	
$(17, 2^{43}, 3)_8$	$g_1(x) = (00100101) + w(0) + w^2(1),$	$[[17, 40/3, 3/2]]_8$
$(17, 2^3, 17)_8$	$g_2(x) = (01000101) + w(1), g_3(x) = (111010111)$ $(1111111111111111)g_1(x), (1111111111111111)g_2(x),$ $(100111001)g_3(x)$	

Table 9.13: Explicit Lists of Nested $\mathbb{F}_2$ -Linear Cyclic Codes over $\mathbb{F}_8 = \mathbb{F}_2(w)$ and the Resulting CSS-like Codes

Table 9.14 contains the pairs of $\mathbb{F}_8$ -linear cyclic codes yielding optimal or good pure asymmetric 8-ary quantum codes.

C and D	Generator Polynomials	Code Q
$[13, 9, 4]_8$	$g_C(x) = (1w^3w^5w^31)$	$[[13, 8, 4/2]]_8$
$[13, 1, 13]_8$	$(1w0w^5w^2w^50w1)g_C(x)$	
$[14, 11, 3]_8$	$g_C(x) = (w^2w^3w^61)$	$[[14, 10, 3/2]]_8$
$[14, 1, 14]_8$	$(w^5ww^5w^41w^2w^4w0w^21)g_C(x)$	
<i>continued on next page</i>		

<i>continued from previous page</i>		
C and D	Generator Polynomials	Code Q
$[14, 10, 4]_8$	$g_C(x) = (ww^41w^21)$	$[[14, 9, 4/2]]_8$
$[14, 1, 14]_8$	$(ww^6ww^2w1w^6w^6w^31)g_C(x)$	
$[14, 2, 12]_8$	$g_C(x) = (w^6w^51w^3110w^6w^51w^311)$	$[[14, 1, 12/2]]_8$
$[14, 1, 14]_8$	$(w^61)g_C(x)$	
$[19, 13, 6]_8$	$g_C(x) = (1w^3w^6w^6w^6w^31)$	$[[19, 12, 6/2]]_8$
$[19, 1, 19]_8$	$(1www^31w^6ww^61w^3ww1)g_C(x)$	
$[21, 20, 2]_8$	$g_C(x) = (11)$	$[[21, 17, 3/2]]_8$
$[21, 3, 14]_8$	$(w^5w^6w^4w^21w^31w^6w^3w^20w^4w^5w00w1)g_C(x)$	
$[21, 20, 2]_8$	$g_C(x) = (11)$	$[[21, 16, 4/2]]_8$
$[21, 4, 14]_8$	$(w^50w^3ww^5w^3w^3w^4w^5w^2w^4w^4ww^6ww^31)g_C(x)$	
$[21, 18, 3]_8$	$g_C(x) = (110w^31)$	$[[21, 15, 3/3]]_8$
$[21, 3, 14]_8$	$(w^5w^6w^2w^6w01w^5ww^4w^3w^4w^2w^301)g_C(x)$	
$[21, 17, 4]_8$	$g_C(x) = (1ww^3w1)$	$[[21, 14, 4/3]]_8$
$[21, 3, 14]_8$	$(11w^6w^6w^61w^3w^61ww^4ww^5w^31)g_C(x)$	
$[21, 17, 4]_8$	$g_C(x) = (1ww^3w1)$	$[[21, 13, 4/4]]_8$
$[21, 4, 14]_8$	$(w^6w^4ww^6w^3w^2w^6w^5w^6w^5w^6w^611)g_C(x)$	

Table 9.14: Explicit Lists of Nested Linear Cyclic Codes over $\mathbb{F}_8$ and the Resulting CSS-like Codes

9.2.7 Optimal and Good Pure 9-ary AQECCs

Here we use the convention that $\mathbb{F}_9 = \mathbb{F}_3(w)$ where w is a primitive root of a monic irreducible polynomial of degree 2 in $\mathbb{F}_3[X]$.

Table 9.15 provides the list of optimal and good 9-ary pure asymmetric CSS-like code.

No.	AQECC Q	Type	LP	Defect	Remarks
1.	$[[10, 7, 3/2]]_9$	BKLC	7	0	OptLin
2.	$[[10, 6, 4/2]]_9$	Cyclic	6	0	OptLin
3.	$[[10, 5, 5/2]]_9$	BKLC	5	0	OptLin
4.	$[[10, 4, 6/2]]_9$	Cyclic	4	0	OptLin
5.	$[[10, 3, 7/2]]_9$	BKLC	3	0	OptLin
6.	$[[10, 2, 8/2]]_9$	Cyclic	2	0	OptLin
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
7.	$[[10, 5/2, 5/4]]_9$	AddCyclic	3	1/2	$[[10, 3, 5/4]]_9$ is open
8.	$[[10, 2, 6/4]]_9$	Cyclic	2	0	OptLin
9.	$[[11, 15/2, 3/2]]_9$	AddCyclic	15/2	0	better than OptLin
10.	$[[11, 6, 4/2]]_9$	BKLC	13/2	1/2	OptLin
11.	$[[11, 5, 5/2]]_9$	Cyclic	11/2	1/2	OptLin
12.	$[[11, 4, 6/2]]_9$	BKLC	9/2	1/2	OptLin
13.	$[[11, 3, 7/2]]_9$	BKLC	7/2	1/2	OptLin
14.	$[[11, 2, 8/2]]_9$	BKLC	5/2	1/2	OptLin
15.	$[[11, 1, 9/2]]_9$	BKLC	3/2	1/2	OptLin
16.	$[[11, 6, 3/3]]_9$	AddCyclic	6	0	reach bound OptLin
17.	$[[11, 3, 6/3]]_9$	AddCyclic	7/2	1/2	reach bound OptLin
18.	$[[12, 17/2, 3/2]]_9$	AddCyclic	17/2	0	better than OptLin
19.	$[[12, 7, 4/2]]_9$	AddCyclic	15/2	1/2	reach bound OptLin
20.	$[[12, 6, 5/2]]_9$	AddCyclic	13/2	1/2	reach bound OptLin
21.	$[[12, 5, 6/2]]_9$	AddCyclic	11/2	1/2	reach bound OptLin
22.	$[[12, 4, 7/2]]_9$	AddCyclic	9/2	1/2	reach bound OptLin
23.	$[[12, 2, 9/2]]_9$	BKLC	5/2	1/2	OptLin
24.	$[[12, 1, 10/2]]_9$	BKLC	3/2	1/2	OptLin
25.	$[[12, 7, 3/3]]_9$	AddCyclic	7	0	reach bound OptLin
26.	$[[13, 9, 3/2]]_9$	Cyclic	19/2	1/2	OptLin
27.	$[[13, 8, 4/2]]_9$	AddCyclic	17/2	1/2	reach bound OptLin
28.	$[[13, 15/2, 5/2]]_9$	AddCyclic	15/2	0	better than OptLin
29.	$[[13, 6, 6/2]]_9$	AddCyclic	13/2	1/2	reach bound OptLin
30.	$[[13, 5, 7/2]]_9$	BKLC	11/2	1/2	OptLin
31.	$[[13, 4, 8/2]]_9$	BKLC	9/2	1/2	OptLin
32.	$[[13, 3, 9/2]]_9$	BKLC	7/2	1/2	OptLin
33.	$[[13, 2, 10/2]]_9$	BKLC	5/2	1/2	OptLin
34.	$[[13, 1, 11/2]]_9$	BKLC	3/2	1/2	OptLin
35.	$[[13, 6, 5/3]]_9$	AddCyclic	6	0	reach bound OptLin
36.	$[[13, 6, 4/4]]_9$	AddCyclic	6	0	reach bound OptLin
37.	$[[13, 5, 5/4]]_9$	AddCyclic	5	0	reach bound OptLin
38.	$[[13, 4, 5/5]]_9$	AddCyclic	4	0	reach bound OptLin
39.	$[[14, 10, 3/2]]_9$	BKLC	21/2	1/2	OptLin
40.	$[[14, 9, 4/2]]_9$	Cyclic	19/2	1/2	OptLin
41.	$[[14, 8, 5/2]]_9$	BKLC	17/2	1/2	OptLin
42.	$[[14, 7, 6/2]]_9$	AddCyclic	15/2	1/2	reach bound OptLin
43.	$[[14, 6, 7/2]]_9$	AddCyclic	13/2	1/2	reach bound OptLin
					<i>continued on next page</i>

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
44.	$[[14, 5, 8/2]]_9$	BKLC	11/2	1/2	OptLin
45.	$[[14, 4, 9/2]]_9$	BKLC	9/2	1/2	OptLin
46.	$[[14, 3, 10/2]]_9$	BKLC	7/2	1/2	OptLin
47.	$[[14, 2, 11/2]]_9$	BKLC	5/2	1/2	OptLin
48.	$[[14, 1, 12/2]]_9$	BKLC	3/2	1/2	OptLin
49.	$[[15, 11, 3/2]]_9$	BKLC	23/2	1/2	OptLin
50.	$[[15, 10, 4/2]]_9$	BKLC	21/2	1/2	OptLin
51.	$[[15, 9, 5/2]]_9$	BKLC	19/2	1/2	OptLin
52.	$[[15, 8, 6/2]]_9$	BKLC	17/2	1/2	OptLin
53.	$[[15, 7, 7/2]]_9$	BKLC	15/2	1/2	OptLin
54.	$[[15, 6, 8/2]]_9$	BKLC	13/2	1/2	OptLin
55.	$[[15, 5, 9/2]]_9$	BKLC	11/2	1/2	OptLin
56.	$[[15, 4, 10/2]]_9$	BKLC	9/2	1/2	OptLin
57.	$[[15, 3, 11/2]]_9$	BKLC	7/2	1/2	OptLin
58.	$[[15, 2, 12/2]]_9$	BKLC	5/2	1/2	OptLin
59.	$[[15, 1, 13/2]]_9$	BKLC	3/2	1/2	OptLin
60.	$[[16, 12, 3/2]]_9$	Cyclic	25/2	1/2	OptLin
61.	$[[16, 11, 4/2]]_9$	Cyclic	23/2	1/2	OptLin
62.	$[[16, 10, 5/2]]_9$	AddCyclic	21/2	1/2	reach bound OptLin
63.	$[[16, 9, 6/2]]_9$	BKLC	19/2	1/2	OptLin
64.	$[[16, 8, 7/2]]_9$	BKLC	17/2	1/2	OptLin
65.	$[[16, 7, 8/2]]_9$	BKLC	15/2	1/2	OptLin
66.	$[[16, 6, 9/2]]_9$	BKLC	13/2	1/2	OptLin
67.	$[[16, 5, 10/2]]_9$	BKLC	11/2	1/2	OptLin
68.	$[[16, 4, 11/2]]_9$	BKLC	9/2	1/2	OptLin
69.	$[[16, 3, 12/2]]_9$	BKLC	7/2	1/2	OptLin
70.	$[[16, 1, 14/2]]_9$	Cyclic	3/2	1/2	OptLin
71.	$[[17, 13, 3/2]]_9$	BKLC	27/2	1/2	OptLin
72.	$[[17, 12, 4/2]]_9$	BKLC	25/2	1/2	OptLin
73.	$[[17, 11, 5/2]]_9$	BKLC	23/2	1/2	OptLin
74.	$[[17, 9, 7/2]]_9$	BKLC	19/2	1/2	OptLin
75.	$[[17, 8, 8/2]]_9$	BKLC	17/2	1/2	OptLin
76.	$[[17, 7, 9/2]]_9$	BKLC	15/2	1/2	OptLin
77.	$[[17, 6, 10/2]]_9$	BKLC	13/2	1/2	OptLin
78.	$[[17, 2, 14/2]]_9$	BKLC	5/2	1/2	OptLin
79.	$[[18, 14, 3/2]]_9$	BKLC	29/2	1/2	OptLin
80.	$[[18, 13, 4/2]]_9$	BKLC	27/2	1/2	OptLin
<i>continued on next page</i>					

<i>continued from previous page</i>					
No.	AQECC Q	Type	LP	Defect	Remarks
81.	$[[18, 12, 5/2]]_9$	BKLC	25/2	1/2	OptLin
82.	$[[18, 9, 8/2]]_9$	BKLC	19/2	1/2	OptLin
83.	$[[18, 8, 9/2]]_9$	BKLC	17/2	1/2	OptLin
84.	$[[18, 7, 10/2]]_9$	BKLC	15/2	1/2	OptLin
85.	$[[18, 2, 14/2]]_9$	BKLC	5/2	1/2	OptLin
86.	$[[19, 15, 3/2]]_9$	BKLC	31/2	1/2	OptLin
87.	$[[19, 14, 4/2]]_9$	BKLC	29/2	1/2	OptLin
88.	$[[19, 13, 5/2]]_9$	BKLC	27/2	1/2	OptLin
89.	$[[19, 9, 9/2]]_9$	BKLC	19/2	1/2	OptLin
90.	$[[19, 8, 10/2]]_9$	BKLC	17/2	1/2	OptLin
91.	$[[20, 16, 3/2]]_9$	Cyclic	33/2	1/2	OptLin
92.	$[[20, 15, 4/2]]_9$	Cyclic	31/2	1/2	OptLin
93.	$[[20, 14, 5/2]]_9$	BKLC	29/2	1/2	OptLin
94.	$[[20, 9, 10/2]]_9$	BKLC	19/2	1/2	OptLin
95.	$[[21, 17, 3/2]]_9$	BKLC	35/2	1/2	OptLin
96.	$[[21, 16, 4/2]]_9$	BKLC	33/2	1/2	OptLin
97.	$[[22, 18, 3/2]]_9$	BKLC	37/2	1/2	OptLin
98.	$[[22, 17, 4/2]]_9$	BKLC	35/2	1/2	OptLin

Table 9.15: Optimal and Good Pure Asymmetric CSS-like Codes over $\mathbb{F}_9$

Table 9.16 contains the pairs of $\mathbb{F}_3$ -linear cyclic codes yielding optimal or good pure asymmetric 9-ary quantum codes.

C and D	Generator Polynomials	Code Q
$(10, 3^{11}, 5)_9$ $(10, 3^6, 8)_9$	$g_9(x) = (10002111) + w(21), g_3(x) = (101010101)$ $(12121)g_9(x), (21)g_3(x)$	$[[10, 5/2, 5/4]]_9$
$(11, 3^{17}, 3)_9$ $(11, 3^2, 11)_9$	$g_9(x) = (011) + w(1), g_3(x) = (201211)$ $(11111111111)g_9(x), (221201)g_3(x)$	$[[11, 15/2, 3/2]]_9$
$(11, 3^{17}, 3)_9$ $(11, 3^5, 8)_9$	$g_9(x) = (011) + w(1), g_3(x) = (201211)$ $(1012221)g_9(x), (1012221)g_3(x)$	$[[11, 6, 3/3]]_9$
$(11, 3^{11}, 6)_9$ $(11, 3^5, 8)_9$	$g_9(x) = (1010211) + w(21), g_3(x) = (1111111111)$ $(201211)g_9(x), (21)g_3(x)$	$[[11, 3, 6/3]]_9$
$(12, 3^{19}, 3)_9$ $(12, 3^2, 12)_9$	$g_9(x) = (001) + w(11), g_3(x) = (12221)$ $(10101010101)g_9(x), (20112201)g_3(x)$	$[[12, 17/2, 3/2]]_9$
$(12, 3^{16}, 4)_9$ $(12, 3^2, 12)_9$	$g_9(x) = (1112121) + w(11), g_3(x) = (21000021)$ $(10101010101)g_9(x), (10101)g_3(x)$	$[[12, 7, 4/2]]_9$
$(12, 3^{14}, 5)_9$ $(12, 3^2, 12)_9$	$g_9(x) = (02021012) + w(11), g_3(x) = (1221001221)$ $(10101010101)g_9(x), (201)g_3(x)$	$[[12, 6, 5/2]]_9$
<i>continued on next page</i>		

<i>continued from previous page</i>		
<i>C and D</i>	Generator Polynomials	Code Q
$(12, 3^{12}, 6)_9$ $(12, 3^2, 12)_9$	$g_9(x) = (2021201) + w(2211), g_3(x) = (1221001221)$ $(111000111)g_9(x), (121)g_3(x)$	$[[12, 5, 6/2]]_9$
$(12, 3^{10}, 7)_9$ $(12, 3^2, 12)_9$	$g_9(x) = (0110212102) + w(2211), g_3(x) = (111111111111)$ $(111000111)g_9(x), (1)g_3(x)$	$[[12, 4, 7/2]]_9$
$(12, 3^8, 8)_9$ $(12, 3^2, 12)_9$	$g_9(x) = (01212222102) + w(120021), g_3(x) = (111111111111)$ $(1201021)g_9(x), (1)g_3(x)$	$[[12, 3, 8/2]]_9$
$(12, 3^{19}, 3)_9$ $(12, 3^5, 8)_9$	$g_9(x) = (001) + w(11), g_3(x) = (12221)$ $(20112201)g_9(x), (20112201)g_3(x)$	$[[12, 7, 3/3]]_9$
$(13, 3^{19}, 4)_9$ $(13, 3^3, 12)_9$	$g_9(x) = (2221011) + w(1), g_3(x) = (21210201)$ $(12020111211)g_9(x), (1100101)g_3(x)$	$[[13, 8, 4/2]]_9$
$(13, 3^{17}, 5)_9$ $(13, 3^2, 13)_9$	$g_9(x) = (122001222) + w(1), g_3(x) = (2001102121)$ $(111111111111)g_9(x), (2221)g_3(x)$	$[[13, 15/2, 5/2]]_9$
$(13, 3^{14}, 6)_9$ $(13, 3^2, 13)_9$	$g_9(x) = (110200000122) + w(1), g_3(x) = (111111111111)$ $(111111111111)g_9(x), (1)g_3(x)$	$[[13, 6, 6/2]]_9$
$(13, 3^{17}, 5)_9$ $(13, 3^5, 10)_9$	$g_9(x) = (122001222) + w(1), g_3(x) = (2001102121)$ $(2001102121)g_9(x), (2221)g_3(x)$	$[[13, 6, 5/3]]_9$
$(13, 3^{19}, 4)_9$ $(13, 3^7, 9)_9$	$g_9(x) = (2221011) + w(1), g_3(x) = (21210201)$ $(1100101)g_9(x), (1100101)g_3(x)$	$[[13, 6, 4/4]]_9$
$(13, 3^{17}, 5)_9$ $(13, 3^7, 9)_9$	$g_9(x) = (011100002) + w(1), g_3(x) = (2022010211)$ $(22001211)g_9(x), (2201)g_3(x)$	$[[13, 5, 5/4]]_9$
$(13, 3^{17}, 5)_9$ $(13, 3^9, 8)_9$	$g_9(x) = (122001222) + w(1), g_3(x) = (2001102121)$ $(10011)g_9(x), (10011)g_3(x)$	$[[13, 4, 5/5]]_9$
$(14, 3^{16}, 6)_9$ $(14, 3^2, 14)_9$	$g_9(x) = (1121101101) + w(1), g_3(x) = (1010101010101)$ $(1010101010101)g_9(x), (201)g_3(x)$	$[[14, 7, 6/2]]_9$
$(14, 3^{14}, 7)_9$ $(14, 3^2, 14)_9$	$g_9(x) = (122202010101) + w(21), g_3(x) = (111111111111111)$ $(1010101010101)g_9(x), (1)g_3(x)$	$[[14, 6, 7/2]]_9$
$(16, 3^{22}, 5)_9$ $(16, 3^2, 16)_9$	$g_9(x) = (02102001) + w(201), g_3(x) = (220210221)$ $(1000100010001)g_9(x), (121110211)g_3(x)$	$[[16, 10, 5/2]]_9$

Table 9.16: Explicit Lists of Nested $\mathbb{F}_3$ -Linear Cyclic Codes over $\mathbb{F}_9 = \mathbb{F}_3(w)$ and the Resulting CSS-like Codes

Table 9.17 contains the pairs of $\mathbb{F}_9$ -linear cyclic codes yielding optimal or good pure asymmetric 9-ary quantum codes.

<i>C and D</i>	Generator Polynomials	Code Q
$[10, 7, 4]_9$ $[10, 1, 10]_9$	$g_C(x) = (1w^2w^21)$ $(1w^5w^2w^6w^2w^51)g_C(x)$	$[[10, 6, 4/2]]_9$
$[10, 9, 2]_9$ $[10, 5, 6]_9$	$g_C(x) = (21)$ $(1w^20w^21)g_C(x)$	$[[10, 4, 6/2]]_9$
$[10, 9, 2]_9$	$g_C(x) = (21)$	$[[10, 2, 8/2]]_9$
<i>continued on next page</i>		

<i>continued from previous page</i>		
C and D	Generator Polynomials	Code Q
$[10, 7, 4]_9$	$(1w^51)g_C(x)$	
$[10, 7, 4]_9$	$g_C(x) = (1w^2w^21)$	$[[10, 2, 6/4]]_9$
$[10, 5, 6]_9$	$(1w^71)g_C(x)$	
$[11, 6, 5]_9$	$g_C(x) = (201211)$	$[[11, 5, 5/2]]_9$
$[11, 1, 11]_9$	$(221201)g_C(x)$	
$[13, 10, 3]_9$	$g_C(x) = (2111)$	$[[13, 9, 3/2]]_9$
$[13, 1, 13]_9$	$(2121022001)g_C(x)$	
$[14, 10, 4]_9$	$g_C(x) = (2w^2w^2w^21)$	$[[14, 9, 4/2]]_9$
$[14, 1, 14]_9$	$(1w011110w^31)g_C(x)$	
$[16, 13, 3]_9$	$g_C(x) = (1w^3w^51)$	$[[16, 12, 3/2]]_9$
$[16, 1, 16]_9$	$(1ww^70w^6w^721w^3w^51w^21)g_C(x)$	
$[16, 12, 4]_9$	$g_C(x) = (w^6w^5021)$	$[[16, 11, 4/2]]_9$
$[16, 1, 16]_9$	$(w0w^7w^3w^31w^6w^3w^5w^6w^21)g_C(x)$	
$[16, 2, 14]_9$	$g_C(x) = (w^3w^3w21w10w^3w^3w21w1)$	$[[16, 1, 14/2]]_9$
$[16, 1, 16]_9$	$(w^21)g_C(x)$	
$[20, 17, 3]_9$	$g_C(x) = (1w^2w^51)$	$[[20, 16, 3/2]]_9$
$[20, 1, 20]_9$	$(w^20w20w^7ww^2w^20w^21w^7w^221)g_C(x)$	
$[20, 16, 4]_9$	$g_C(x) = (w^62w^701)$	$[[20, 15, 4/2]]_9$
$[20, 1, 20]_9$	$(2w^2ww^21ww^3w^3w^7w^7w^52w^6w^5w^61)g_C(x)$	

Table 9.17: Explicit Lists of Nested Linear Cyclic Codes over $\mathbb{F}_8$ and the Resulting CSS-like Codes

9.3 Scattered Notes and Ad Hoc Constructions

9.3.1 A Non Existence Result

There does not exist a pure $[[5, 1, 3/2]]_2$ -CSS code since the followings do not exist.

1. A $[5, 2, 3]_2$ -code that contains a codeword $\mathbf{v}$ of weight 5. Let $\mathbf{c} \in C$ such that $\text{wt}_H(\mathbf{c}) = 3$. If such a codeword $\mathbf{v}$ exists, then $\mathbf{c} + \mathbf{v}$ is a codeword of weight 2 in C , a contradiction.
2. A nested pair $[5, 1, d]_2 \subset [5, 2, 3]_2$ with $d^{\perp_E} = 2$.

3. A nested pair $[5, 1, d]_2 \subset [5, 2, 2]_2$ with $d^{\perp_E} = 3$.
4. A nested pair $[5, 2, d]_2 \subset [5, 3, 2]_2$ with $d^{\perp_E} = 3$.
5. A nested pair $[5, 3, d]_2 \subset [5, 4, 2]_2$ with $d^{\perp_E} = 3$.

For small lengths and a small q , the same approach can be used to rule out the existence of some pure asymmetric CSS-like codes. Care must be exercised to ensure that all possible nested pairs have been considered and properly ruled out.

9.3.2 Some BKLC' Construction

Recently, some new optimal codes over $\mathbb{F}_5$ are presented in [50, Sec. 5]. The first one is of parameters $[36, 28, 6]_5$ and is labeled $\mathcal{C}_{36}$ in said reference. By shortening this code at the first position an optimal $[35, 27, 6]_5$ is derived. If we shorten $\mathcal{C}_{36}$ at the first two positions, we get an optimal $[34, 26, 6]_5$ -code.

It can be easily checked, starting with the generator matrix of $\mathcal{C}_{36}$, that each of these three codes contains a codeword $\mathbf{v}$ of weight equals its length. By BKLC construction, we get optimal AQECCs with parameters $[[36, 27, 6/2]]_5$, $[[35, 26, 6/2]]_5$, and $[[34, 25, 6/2]]_5$.

9.3.3 Ad Hoc Constructions

We show an explicit construction for pure CSS code Q with parameters $[[4, 1, 2/2]]_2$ and $[[5, 2, 2/2]]_2$ by exhibiting a generator matrix for each of $[4, 2, 2]_2$ and $[5, 3, 2]_2$ -

codes containing a codeword of weight 4 and 5, respectively. The matrices are

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A $[[13, 1, 5/3]]_2$ -CSS code alluded to by a referee of [65] can also be constructed. The trick is to consider best-known $[13, 9, 3]_2$ linear code (BKLC), say C , from the MAGMA database. Its dual is a $[13, 4, 6]_2$ -code D . Next, we add the row vector $\mathbf{1} := (1, 1, \dots, 1)$ to the generator matrix of D to get a $[13, 5, 5]_2$ -code E . The dual of E is a $[13, 8, 4]_2$ -code F which is a subcode of C . Hence, to get a $[[13, 1, 5/3]]_2$ -quantum code Q , we use a code F with parameters $[13, 8, 4]_2 \subset C$ with parameters $[13, 9, 3]_2$.

At the moment we know of two different ways of constructing a $[[15, 1, 7/3]]_2$ quantum code. One construction is suggested in [65] with $C_z := \text{BCHCode}(\mathbb{F}_2, 15, 7)$ and $C_x := \text{BCHCode}(\mathbb{F}_2, 15, 3)$. Simple calculations yield C_z , C_x , and $C_x^{\perp_E}$ are codes with parameters $[15, 5, 7]_2$, $[15, 11, 3]_2$, and $[15, 4, 8]_2$, respectively, satisfying $C_x^{\perp_E} \subset C_z$.

An alternative is to let $C := \text{BKLC}(\mathbb{F}_2, 15, 4)$ be a $[15, 4, 8]_2$ -code with generator matrix

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

and $D := \text{BKLC}(\mathbb{F}_2, 15, 5)$ be a $[15, 5, 7]_2$ -code with generator matrix

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

It is easy to check that $C \subset D$ and that $C^{\perp_E}$ is a $[15, 11, 3]_2$ -code with generator matrix

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Thus, we arrive at a $[[15, 1, 7/3]]_2$ -code Q .

9.4 Conclusion and Open Problems

In this chapter, many optimal and good pure asymmetric CSS-like codes have been derived from comparing the parameters of the AQECCs that we can construct explicitly with the corresponding parameters that we derive from linear programming.

While this approach is sufficiently effective for small values of q and n , better approaches need to be develop if we are to handle larger values of q and n .

Bibliography

- [1] S. A. Aly, “On quantum and classical error control codes: constructions and applications,” preprint, 2008. Available at <http://arxiv.org/pdf/0812.5104>.
- [2] S. A. Aly and A. Ashikhmin, “Nonbinary quantum cyclic and subsystem codes over asymmetrically-decohered quantum channels,” preprint, 2010. Available at <http://arxiv.org/pdf/1002.2966>.
- [3] A. Ashikhmin and E. Knill, “Nonbinary quantum stabilizer codes,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.
- [4] E. F. Assmus, Jr. and H. F. Mattson, Jr., “New 5-Designs,” *J. Combinatorial Theory*, vol. 6, no. 2, pp. 122–151, Mar. 1969.
- [5] S. Ball, “On large subsets of a finite vector space in which every subset of basis size is a basis,” *J. of the European Math. Soc.*, to appear.
- [6] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system. I. The user language,” *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997.

- [7] M. C. Bhandari and C. Durairajan, “A note on covering radius of MacDonald codes,” in *Proc. the International Conference on Information Technology : Computers and Communications (ITCC 03)*, 2003.
- [8] E. P. Bautista, P. Gaborit, J. L. Kim, and J. L. Walker, “s-Extremal additive $\mathbb{F}_4$ codes,” *Adv. in Math. of Communications*, vol. 1, pp. 111–130, 2007.
- [9] D. Boucher, W. Geiselmann, and F. Ulmer, “Skew-cyclic codes,” *Applied Algebra Engin. Commun. Comput.*, vol. 18, pp. 379–389, 2007.
- [10] D. Boucher and F. Ulmer, “Codes as modules over skew polynomial rings,” *Proc. the 12th IMA Conference on Cryptography and Coding*, pp. 38–55, Cirencester, 2009.
- [11] I. Bouyukliev, private email communication, October 12, 2009.
- [12] I. Bouyukliev, “What is Q-extension?,” *Serdica J. Computing*, vol. 1, pp. 115–130, 2007.
- [13] I. Bouyukliev, M. Grassl, and Z. Varbanov, “New bounds for $n_4(k, d)$ and classification of some optimal codes over $GF(4)$,” *Disc. Math.*, vol. 281, pp. 43–66, 2004.
- [14] I. Bouyukliev and P. Östergård, “Classification of self-orthogonal codes over $\mathbb{F}_3$ and $\mathbb{F}_4$,” *SIAM J. Disc. Math.*, vol. 19, no. 2, pp. 363–370, 2005.
- [15] R. Calderbank and W. Kantor, “The geometry of two-weight codes,” *Bulletin of the London Mathematical Society*, vol. 18, no. 2, pp. 97–122, 1986.

- [16] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over $GF(4)$,” *IEEE Trans. Inf. Theory*, vol. 44, pp. 1369–1387, 1998.
- [17] P. Charpin, “Open problems on cyclic codes,” in *Handbook of Coding Theory I*, eds. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, pp. 963–1063.
- [18] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam: Elsevier, 1997.
- [19] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York: Springer, 1998.
- [20] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, “Codeword stabilized quantum codes,” *Proceeding ISIT 2008, Toronto*.
- [21] L. E. Danielsen and M. G. Parker, “On the classification of all self-dual additive codes over $GF(4)$ of length up to 12,” *J. Combinatorial Theory, Series A*, vol. 113, pp. 1351–1367, 2006.
- [22] P. Delsarte, “Four fundamental parameters of a code and their combinatorial significance,” *Information and Control*, vol. 23, pp. 407–438, 1973.
- [23] C. Ding, D. R. Kohel, and S. Ling, “Elementary 2-group character codes,” *IEEE Trans. Inf. Theory*, vol. 46, pp. 280–284, 2000.
- [24] Z. W. E. Evans, A. M. Stephens, J. H. Cole, and L. C. L. Hollenberg, “Error correction optimisation in the presence of x/z asymmetry,” preprint, 2007. Available at <http://arXiv:quant-ph/0709.3875>.

- [25] M. F. Ezerman, M. Grassl, and P. Solé, “The weights in MDS codes,” *IEEE Trans. Inf. Theory*, vol. 57, pp. 392–396, 2011.
- [26] M. F. Ezerman, S. Jitman, and S. Ling, “On Asymmetric Quantum MDS Codes,” preprint, 2010. Available at <http://arxiv.org/pdf/1006.1694>.
- [27] M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik, “CSS-like constructions of asymmetric quantum codes,” preprint, 2011.
- [28] M. F. Ezerman, S. Ling, and P. Solé, “Additive asymmetric quantum codes,” *IEEE Trans. Inf. Theory*, to appear.
Available at <http://arxiv.org/pdf/1002.4088>.
- [29] M. F. Ezerman, S. Ling, P. Solé, and O. Yemen, “From skew-cyclic codes to asymmetric quantum codes,” *Advances in Mathematics of Communication*, vol. 5, no. 1, pp. 41–57, 2011.
- [30] K. Feng, S. Ling, and C. Xing, “Asymptotic bounds on quantum codes from algebraic geometry codes,” *IEEE Trans. Inf. Theory*, vol. 52, pp. 986–991, 2006.
- [31] E. M. Gabidulin, “Theory of codes with maximum rank distance,” *Probl. Peredach. Inform. (in Russian)*, vol. 21, pp. 3–16, 1985; English translation, pp. 1–12.
- [32] E. M. Gabidulin and T. Kløve, “The Newton Radius of MDS Codes,” in *Proceedings IEEE Information Theory Workshop (ITW 1998)*, Killarney, Ireland, 1998, pp. 50–51.

- [33] P. Gaborit, W. C. Huffman, J. L. Kim, and V. Pless, “On additive $GF(4)$ -codes,” in *DIMACS Workshop on Codes and Association Schemes, DIMACS Ser. in Disc. Math. and Theor. Computer Science*, vol. 56, pp.135-149, American Mathematical Society, 2001.
- [34] D. Gottesman, “Stabilizer Codes and Quantum Error Correction,” Ph.D. dissertation, California Inst. of Technology., Pasadena, CA, 1997.
- [35] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. Online available at <http://www.codetables.de>, accessed on March 7, 2011.
- [36] M. Grassl, T. Beth, and M. Rötteler, “On Optimal Quantum Codes,” *International J. Quantum Information*, vol. 2, no. 1, pp. 55–64, 2004.
- [37] M. Grassl and T. A. Gulliver, “On Self-Dual MDS Codes,” in *Proceedings 2008 IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, Canada, 2008, pp. 1954–1957.
- [38] M. Grassl and T. A. Gulliver, “On circulant self-dual codes over small fields,” *Designs, Codes and Cryptography*, vol. 52, pp. 57–81, 2009.
- [39] M. Grassl and M. Rötteler, “Non-additive quantum codes from Goethals and Preparata codes,” *Proc. IEEE Information Theory Workshop (ITW 2008)*, Porto.
- [40] T. A. Gulliver and J. L. Kim, “Circulant based extremal additive self-dual codes over $GF(4)$,” *IEEE Trans. Inf. Theory*, vol. 50, pp. 359–366, 2004.

- [41] T. A. Gulliver, J-L. Kim, and Y. Lee, “New MDS or Near-MDS self-dual codes,” *IEEE Trans. Inf. Theory*, vol. 54, pp. 4354–4360, 2008.
- [42] T. A. Gulliver and P. Östergård, “Improved bounds for quaternary linear codes of dimension 6,” *Applicable Algebra in Engineering, Communication and Computing*, vol. 9, pp. 153–159, 1998.
- [43] S. Han and J. L. Kim, “Formally self-dual additive codes over $\mathbb{F}_4$,” to appear in the special issue of *J. Symbolic Computation on Algebraic Coding Theory and Applications*.
- [44] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays, Theory and Applications*. New York: Springer-Verlag, 1999.
- [45] R. Hill and P. Lizak, “Extensions of Linear Codes,” in *Proceedings 1995 International Symposium on Information Theory*, Whistler, BC, Canada, 1995, p. 345.
- [46] R. Hill, “An Extension Theorem for Linear Codes,” *Designs, Codes and Cryptography*, vol. 17, no. 1–3, pp. 151–157, Sep. 1999.
- [47] W. C. Huffman, “Additive cyclic codes over $\mathbb{F}_4$,” *Adv. in Math. of Communications*, vol. 1, pp. 427–459, 2007.
- [48] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press, 2003.
- [49] L. Ioffe and M. M. Mézard, “Asymmetric quantum error-correcting codes,” *Phys. Rev. A*, 75(032345), 2007.

- [50] S. Jitman, S. Ling, H. Liu, and X. Xie, “Checkable codes from group rings,” preprint, 2010. Available at <http://arxiv.org/pdf/1012.5498>.
- [51] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, “Nonbinary stabilizer codes over finite fields,” *IEEE Trans. Inf. Theory*, vol. 52, pp. 4892–4914, 2006.
- [52] J. L. Kim, “New quantum error-correcting codes from Hermitian self-orthogonal codes over $GF(4)$,” in *Proc. the Sixth International Conference on Finite Fields and Applications*, Oaxaca, Mexico, May 21–25, 2001, pp. 209–213, Springer Verlag, 2002.
- [53] J. L. Kim and V. Pless, “Designs in additive codes over $GF(4)$,” *Designs, Codes and Cryptography*, vol. 30, pp. 187–199, 2003.
- [54] A. Klappenecker and M. Rötteler, “Beyond stabilizer codes II: Clifford codes,” *IEEE Trans. Inf. Theory*, vol. 48, pp. 2396–2399, 2002.
- [55] R. Li and Y. Ma, private email communication, September 27, 2009.
- [56] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications vol. 20. Cambridge: Cambridge University Press, 1997.
- [57] S. Ling, “A family of group character codes,” *European J. Combinatorics*, vol. 25, pp. 579–590, 2004.
- [58] S. Ling and C. P. Xing, *Coding Theory. A First Course*, Cambridge: Cambridge University Press, 2004.

- [59] Y. Ma, R. Li, X. Zhao, and Y. Feng, “Three quantum error-correcting codes constructed from self-orthogonal codes over $GF(4)$,” in *Proc. 2007 Int. Symp. on Intelligent Signal Processing and Communication System*, Xiamen, China, Nov.28-Dec.1, 2007.
- [60] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
- [61] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics vol. 17. Berlin Heidelberg: Springer-Verlag, 2006.
- [62] E. M. Rains, “Nonbinary quantum codes,” *IEEE Trans. Inf. Theory*, vol. 45, pp. 1827–1832, 1999.
- [63] M. Rötteler, M. Grassl, and T. Beth, “On Quantum MDS Codes,” in *Proc. IEEE International Symposium on Information Theory (ISIT 2004)*, Chicago, USA, 2004, p. 355.
- [64] E. M. Rains and N. J. A. Sloane, “Self-dual codes,” in *Handbook of Coding Theory I*, eds. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, pp. 177–294.
- [65] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, “Asymmetric quantum codes: constructions, bounds and performance,” *Proc. of the Royal Soc. A (2009)*, vol. 465, pp. 1645–1672, 4 March 2009.

- [66] A. M. Steane, “Multiple particle interference and quantum error correction,” *Proc. of the Royal Soc. A*, vol. 452, pp. 2551-2577, 1996.
- [67] Z. Varbanov, “Some new results for additive self-dual codes over $GF(4)$,” *Serdica J. Computing*, vol. 1, pp. 213–227, 2007.
- [68] Z. Varbanov, “Additive circulant graph codes over $GF(4)$,” in *Proc. Sixth International Workshop on Optimal Codes and Related Topics*, Varna, Bulgaria, June 16-22, 2009.
- [69] L. Wang, K. Feng, S. Ling, and C. Xing, “Asymmetric quantum codes: characterization and constructions,” *IEEE Trans. Inf. Theory*, vol. 56, pp. 2938–2945, 2010.
- [70] X. Zhao, Y. Lei, and R. Li, “On the classification of some three dimensional quaternary optimal self-orthogonal codes,” in *Second International Workshop on Knowledge Discovery and Data Mining*, 2009.