

Aalborg Universitet



AALBORG UNIVERSITY
DENMARK

Quantum Codes and Multiparty Computation

A Coding Theoretic Approach

Christensen, René Bødker

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

[Link to publication from Aalborg University](#)

Citation for published version (APA):
Christensen, R. B. (2020). *Quantum Codes and Multiparty Computation: A Coding Theoretic Approach*. Aalborg Universitetsforlag.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

QUANTUM CODES AND MULTIPARTY COMPUTATION

A CODING THEORETIC APPROACH

BY
RENÉ BØDKER CHRISTENSEN

DISSERTATION SUBMITTED 2020



AALBORG UNIVERSITY
DENMARK

Quantum Codes and Multiparty Computation

A Coding Theoretic Approach

PhD Thesis of
René Bødker Christensen

July 2020

Dissertation submitted: 6th July, 2020

PhD supervisor: Professor WSR. Olav Geil
Aalborg University

PhD committee: Professor Morten Nielsen (chairman)
Aalborg University
Professor Serge Fehr
Leiden University
Cem Güneri, PhD
Vice President at Sabanci University

PhD Series: Faculty of Engineering and Science, Aalborg University

Department: Department of Mathematical Sciences

ISSN (online): 2446-1636
ISBN (online): 978-87-7210-674-8

Published by:
Aalborg University Press
Kroghstræde 3
DK – 9220 Aalborg Ø
Phone: +45 99407140
aauf@forlag.aau.dk
forlag.aau.dk

© Copyright: René Bødker Christensen

Printed in Denmark by Rosendahls, 2020

Abstracts

Dansk

I denne afhandling anvendes resultater og teknikker fra klassisk kodningsteori som grundlag for kryptografiske protokoller samt til konstruktion af fejlkorrigerende kvantekoder. De grundlæggende definitioner og resultater indenfor disse emner præsenteres i første del af afhandlingen, som også giver et overblik over den anden del. Denne anden del, som udgør størstedelen af afhandlingen indeholder fem videnskabelige artikler.

Artiklerne A og B har fokus på kryptografiske anvendelser. I Artikel A forbedres to eksisterende protokoller til pålidelig beskedoverførsel, så der enten kan sendes flere informationssymboler per overførsel eller så protokollen fungerer over et mindre legeme. Artikel B omhandler OT-udvidelse, som kan bruges til at opbygge større kryptografiske protokoller. Det vises her, hvordan brugen af ikke-binære koder leder til et kompromis mellem antallet af grund-OT's og antallet af bits, der skal sendes, sammenlignet med binære koder.

Artikel C berører både anvendelser indenfor kryptografi og kvantekoder. Mere specifikt gives to nye konstruktioner af indlejrede, forbedrede Hermite-koder. Disse indlejrede koder anvendes så til konstruktion af såvel *secret sharing schemes* som asymmetriske kvantekoder via CSS-konstruktionen.

Artiklerne D og E tager afsæt i Artikel C og omhandler kvantekoder fra Steane-udvidelse. Denne udvidelse gør det i nogle tilfælde muligt at hæve dimensionen af en kvantekode uden at sænke mindsteafstanden. De resulterende kvantekoder er symmetriske. I Artikel D benyttes teknikken på forbedrede Hermite-koder, mens den i Artikel E benyttes på kode defineret fra kartesiske produkter af punktmængder.

English

This thesis treats the application of results and techniques from classical coding theory to protocols in cryptography and construction of quantum error-correcting codes. The basic definitions and results from these topics are presented in the first part of the thesis, which also gives an overview on the second part. This second part, in which the majority of the thesis is found, contains five scientific papers.

Papers A and B both focus on cryptographic applications. In Paper A, two existing protocols for reliable message transmission are improved in such a

way that it is either possible to increase the number of information symbols per transmission, or decrease the required field size for the protocol to work. Paper B treats OT-extension, which can be used to build larger cryptographic protocols. Here, it is shown how the use of non-binary codes leads to a trade-off between the number of base-OT's and the number of transmitted bits when compared to binary codes.

Paper C contains applications to both cryptography and quantum codes. More specifically, two new constructions of nested, improved Hermitian codes are given. These nested codes are then used to construct secret sharing schemes as well as asymmetric quantum codes from the CSS-construction.

Papers D and E take Paper C as their starting point and treat quantum codes from Steane-enlargement. In some cases, this enlargement makes it possible to increase the dimension of a quantum code without decreasing the minimal distance. The resulting quantum codes are symmetric. In Paper D, the technique is applied to improved Hermitian codes, while it is applied to codes from Cartesian product point sets in Paper E.

Preface

This thesis is the culmination of my PhD studies at the Department of Mathematical Sciences at Aalborg University in the period from August 2016 to June 2020. During this time, I have had the pleasure of being supervised by Diego Ruano (currently Ramón-y-Cajal fellow at the University of Valladolid), Ignacio Cascudo (currently assistant research professor at IMDEA Software Institute), and Professor WSR. Olav Geil.

The focus of my work has been classical coding theory with applications to the areas of cryptography – in particular to multiparty computation – and to quantum error-correcting codes. As expected, this focus permeates the thesis, which comprises two parts. The first contains preliminary material and an introduction to the treated topics. This leads to the second part, which makes up the majority of the thesis. This latter part comprises five scientific papers, four of which have been published in peer-reviewed journals or proceedings. At the time of submission, the remaining paper is undergoing peer-review.

I thank each of my three supervisors for their collaboration on research projects, patience with my – at times stupid – questions, and guidance in general. All three have brought their individual influences to my research profile. I also extend my gratitude to Professor Gretchen L. Matthews who hosted my research stay at Virginia Tech in the Spring of 2019. I really appreciate her taking time out of her calendar to supervise me during the months I spent in Blacksburg.

Finally, I thank my colleagues at the Department of Mathematical Sciences for a variety of reasons too numerous to list. Special thanks, however, goes to Jaron S. Gundersen, who has been my fellow guinea pig in the 4+4-PhD programme. Over the years, we have had many delightful conversations related to our field and our studies in general.

René Bødker Christensen
23rd June 2020

Contents

I	Background	1
	Introduction	3
	Preliminaries	5
1	Error-correcting codes	5
2	Multiparty computation	6
3	From classical to quantum computers	10
A	Additional results	20
	Overview of Part II	21
	References	23
II	Papers	27
	Paper A: On one-round reliable message transmission	29
1	Introduction	31
2	Preliminaries	32
3	Constant-size messages	33
4	A method based on list-decoding	34
5	A method based on erasure decoding	35
6	Comparison with existing protocols	38
7	Acknowledgements	39
8	References	39
	Paper B: Actively Secure OT-Extension from q -ary Linear Codes	41
1	Introduction	43
2	Preliminaries	46
3	Actively Secure OT-Extension	48
4	Consistency check in a subfield	55
5	Comparison	56
6	Acknowledgements	59
7	References	59

Contents

Paper C: On nested code pairs from the Hermitian curve	61
1 Introduction	63
2 Hermitian codes and their parameters	65
3 The dimension of improved codes	69
4 Inclusion of improved codes	71
5 Improved nested codes of not too small codimension	75
6 Improved information on nested codes of small codimension	78
7 Comparison with bounds and existing constructions	79
8 Concluding remarks	85
9 Acknowledgements	85
10 References	85
A Additional results on σ and μ	87
 Paper D: Steane-enlargement of quantum codes from the Hermitian function field	 93
1 Introduction	95
2 Preliminaries	96
3 Steane-enlargement of Hermitian codes	100
4 Comparison with existing constructions	104
5 Concluding remarks	109
6 Acknowledgements	109
7 References	109
 Paper E: On Steane-enlargement of quantum codes from Cartesian product point sets	 113
1 Introduction	115
2 Preliminaries	116
3 Steane-enlargement of improved codes	120
4 Conclusion	129
5 Acknowledgements	129
6 References	129

Part I

Background

Introduction

An ever-increasing part of modern life is digital. Paying for goods or services often happen without exchanging physical currency, but instead via a credit card or a payment app, causing a change in those bytes on the bank's server that represent our balance. Or the payment may even be made with one of the many purely digital cryptocurrencies, whose value is not backed by a government. In Denmark, medical records are stored in digital form and can – at least partially – be accessed online. In some countries, casting a vote in an election is handled electronically.

With such sensitive information being handled by computers and sent across networks, we must use cryptographic techniques to ensure that our data is secured against the prying eyes of anyone but the intended recipient. Additionally, we should be able to trust the data we receive even if errors happen during transmission, be it caused by bad luck or by the deliberate tampering of an adversary. The techniques that we use to enable such security generally rely on the assumption that some problems are computationally intractable. For instance, the security of the widely used RSA cryptosystem relies on the assumption that no classical computer can feasibly factor a sufficiently large integer [RSA78]. Similarly, some versions of the Diffie-Hellman key exchange rely on the assumption that computing the so-called discrete log in a group is infeasible [DH76].

Using such security assumptions, we can build cryptographic protocols to solve a number of different problems. In this thesis, one of the topics of interest are protocols that enable what is known as secure multiparty computation. Here, a number of participants each have an input to a publicly known function, and they wish to compute the function value with the given inputs. They wish to do this, however, without revealing their individual inputs to the other participants. As an example, a user of a messaging app will find it convenient to know which of his friends, colleagues, and acquaintances use the same app. Of course, he could simply reveal all of his contacts to the app provider, but this leaks more information than necessary. Using multiparty computation, it is possible for the user and the app provider to learn only the intersection between the user's contact list and the app provider's user database. This example is what is known as *private set intersection*. The protocols considered in thesis are not aimed at such specific problems. Instead, they serve as subprotocols that can be used to build larger protocols for solving those problems.

Introduction

In recent years, there has been an increasing interest in quantum computation, and the computational power provided by such systems. For instance the factoring and discrete log problems mentioned above are considered intractable by a classical computer, but a quantum computers will – at least in theory – be able to solve them in polynomial time [Sho94; Sim94]. One major obstacle to the development of large-scale quantum computers is that the quantum bits that make up such a system are highly susceptible to errors. Thus, the output of a quantum computation can only be useful if we have some form of error-correction on the quantum bits themselves. Such error-correction can be provided by quantum error-correcting codes. While these codes are different from those studied in classical coding theory, there are a number of results – such as the CSS-construction – which allow the construction of quantum codes given classical linear codes with specific properties. This gives coding theorists an opportunity to exploit knowledge of good classical codes to construct quantum error correcting codes.

This thesis takes its starting point in classical coding theory and then applies this in to the two problems mentioned above: multiparty computation and quantum error-correcting codes. More concretely, the thesis contains a paper where decoding of linear codes is used to provide reliable communication between two parties, even in the presence of an adversary. In a separate paper, linear codes are used for so-called extension of oblivious transfer. Both of these are related to multiparty computation. For instance, the latter can be used to solve the private set intersection problem mentioned earlier, see e.g. [OOS17]. The final three papers in the thesis describe various constructions of quantum codes. Hermitian codes are a well-known class of algebraic geometric codes that are generally agreed to have relatively good parameters. Two papers use these to construct quantum error-correcting codes via the CSS-construction and Steane-enlargement, respectively. The third paper applies the Steane-enlargement technique to a different family of codes, namely the codes from Cartesian product point sets.

Preliminaries

This chapter reiterates the mathematical framework that will be used prominently in Part II of the thesis. Concretely, the treated subjects are (a) classical error-correcting codes, (b) proving the security of a protocol in multiparty computation, and (c) the fundamentals of quantum error-correcting codes. A reader familiar with these topics may want to read the chapter cursorily.

1 Error-correcting codes

In this section, the basic coding theoretic notation used in this work is introduced. Some of these definitions will reappear in the papers included in Part II. In particular, the exposition below bears resemblance to the introduction of Paper B since that paper was written for cryptographers rather than coding theorists. A more detailed treatment of coding theory can be found in one of the many textbooks on the subject, e.g., [HP03; JH04].

A linear code \mathcal{C} is a linear subspace of \mathbb{F}_q^n . The vectors in \mathbb{F}_q^n are traditionally called *words*, and those that are also in \mathcal{C} are called *codewords*. When working with error-correction, we typically assume that the codewords are subjected to a type of error where some symbol in the codeword is altered to a different symbol. We refer to such an error as a *bit flip* since it corresponds exactly to flipping a bit in the binary case. Crucially, when receiving a word with one or more bit-flip errors, we do not know the positions where they happened. Depending on the concrete problem, we may sometimes consider *erasures*, which are errors where the error positions are known, but the error values themselves are not. For instance, such errors are considered in Papers A and B.

For each word $\mathbf{x} \in \mathbb{F}_q^n$, we use the Hamming weight $w_H(\mathbf{x}) = |\text{supp } \mathbf{x}|$ to denote the number of non-zero entries in \mathbf{x} . This weight induces the Hamming distance $d_H(\mathbf{x}, \mathbf{y}) = w_H(\mathbf{x} - \mathbf{y})$, which turns \mathbb{F}_q^n into a metric space. In the context of error-correction, an especially important property of the code \mathcal{C} is its minimal distance

$$d(\mathcal{C}) = \min_{\substack{\mathbf{x}, \mathbf{y} \in \mathcal{C} \\ \mathbf{x} \neq \mathbf{y}}} d_H(\mathbf{x}, \mathbf{y})$$

since this represents the minimal number of errors that can take one codeword to another. Rather than considering the distance between each pair of codewords, the linearity of \mathcal{C} implies that $d(\mathcal{C}) = \min_{\mathbf{c} \in \mathcal{C} \setminus \{0\}} w_H(\mathbf{c})$.

2. Multiparty computation

If the linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ has dimension k as an \mathbb{F}_q -vector space and minimal distance $d(\mathcal{C}) = d$, we commonly refer to \mathcal{C} as an $[n, k, d]_q$ -code, or alternatively an $[n, k]_q$ -code if the minimal distance is unknown.

In Papers C, D and E, the concepts of nested codes and their relative distance are essential. Two codes $\mathcal{C}_1, \mathcal{C}_2$ are called a nested pair of codes if $\mathcal{C}_2 \subsetneq \mathcal{C}_1$. Their relative distance is then defined as

$$d(\mathcal{C}_1, \mathcal{C}_2) = \min\{w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2\}.$$

For arbitrary codes, it is generally difficult to determine the relative distance, and resorting to the bound $d(\mathcal{C}_1, \mathcal{C}_2) \geq d(\mathcal{C}_1)$ is commonplace. For some codes – such as those codes considered in Papers C, D, and E – it is, however, possible to determine the relative distances exactly.

2 Multiparty computation

In Paper B, we use a simulation strategy to prove that a cryptographic protocol is secure. For readers who are not familiar with this kind of proof, the current section gives a brief introduction to the fundamental idea. A more in-depth exposition can for instance be found in [CDN15] or [CF01], on both of which the following is based.

Model assumptions

A multiparty computation protocol consists of a number of participants interacting with each other by following a set of predefined instructions. Each participant has a secret input, and the purpose of the protocol is to compute the output of a function when using the given inputs, but doing so without revealing the individual inputs. Some participants may, however, attempt to gain information about the input of another participant. We model this behaviour by introducing an *adversary* which controls a number of participants in the protocol. The participants under adversarial control are called *corrupt*, and the remaining participants are called *honest*.

The adversary may be either *passive* or *active*. The former means that the corrupt participants follow the protocol, but collude and pool their knowledge to gain as much information as possible about the inputs of the honest participants. The latter means that in addition to the pooling of information, the corrupt participants may also deviate from the protocol in an attempt to extract more information. Thus, an active adversary is more powerful than a passive, and protocols designed to protect against active adversaries are typically more complex.

Defining security

In order to prove that a cryptographic protocol is secure, we commonly consider a ‘game’ where an entity called *the environment* provides the

I. Background

inputs of the participants and receives their final outputs. In addition, the environment will interact with the adversary, which is able to corrupt participants. In this game, the environment must try to distinguish between the execution of the protocol in question and an execution in the ideal world. Here, ideal world refers to a setting where a magical black box provides the exact functionality that we are looking for. This black box is commonly called the *ideal functionality*. But since the protocol has several additional steps compared to the ideal functionality, we allow ourselves to introduce a *simulator* in the ideal world. This simulator acts as an intermediate link between the environment and the ideal functionality, and its purpose is to emulate the steps and messages that would be found in the real-world execution of the protocol.

In essence, the environment is placed in one of two different scenarios with equal probability: either (a) the environment is interacting directly with the adversary, and the honest participants act as specified by the protocol, or (b) the environment is interacting with the simulator, which in turn interacts with the ideal functionality via the corrupted participants. For an illustration, see Figure 1. If the environment can successfully distinguish these two scenarios, it wins the game. The protocol is considered secure if the probability that the environment wins is sufficiently small.

Initially, it might not be clear why this should provide evidence that the protocol is in fact secure. Scenario (a) above is the protocol execution as it would be if we rolled it out in the real world. In scenario (b), however, we consider a theoretical execution where the desired operation is performed by the ideal functionality – which is secure by definition – and the simulator merely emulates the steps of the protocol. If the environment cannot

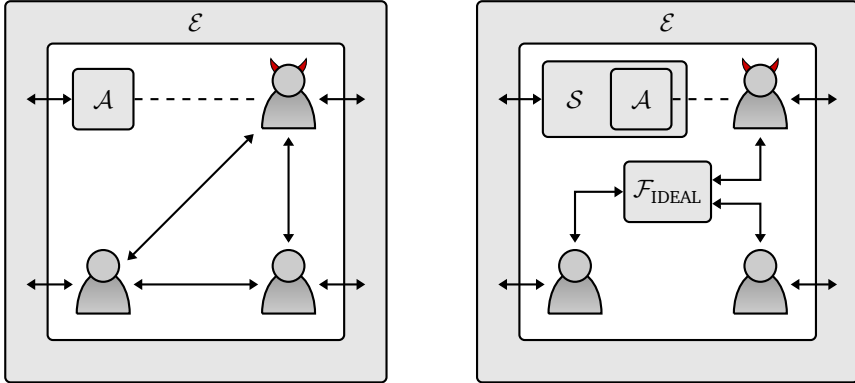


Figure 1. A simple illustration of the two scenarios of the game in the case where the adversary \mathcal{A} controls a single participant as indicated by the dashed line. On the left, the environment \mathcal{E} interacts with the adversary as in scenario (a). On the right, the environment interacts with the ideal functionality $\mathcal{F}_{\text{IDEAL}}$ via a simulator S that emulates \mathcal{A} . This is scenario (b).

2. Multiparty computation

distinguish these two scenarios, the information obtained during protocol execution might as well have been the random information produced by the simulator. For a precise treatment, see [CF01] or [CDN15; Ch. 4].

As mentioned previously, we call the protocol secure if the environment wins the game with ‘sufficiently small’ probability, but as of yet it is unclear exactly what ‘sufficiently small’ means. In order to quantify this, we will use the concept of distinguishing *advantage*. That is, we measure how much better the environment can distinguish the two scenarios compared to guessing uniformly at random. More precisely, let $b \in \{0, 1\}$ be a bit denoting which of the scenarios (a) and (b) the environment is placed in, and let X_0 and X_1 be random variables describing the information the environment sees during the game in each of the two scenarios. Further, assume that the environment uses some (possibly probabilistic) distinguishing algorithm \mathcal{D} . With these notations in place and following [CDN15; pp. 18–19], the probability that the environment wins is given by

$$\begin{aligned} \Pr[\mathcal{D}(X_b) = b] &= \frac{1}{2} \Pr[\mathcal{D}(X_b) = b \mid b = 0] + \frac{1}{2} \Pr[\mathcal{D}(X_b) = b \mid b = 1] \\ &= \frac{1}{2} (\Pr[\mathcal{D}(X_0) = 0] + \Pr[\mathcal{D}(X_1) = 1]) \end{aligned} \quad (2.1)$$

by the law of total probability. Since the distinguisher \mathcal{D} will always return either 0 or 1, we must have $\Pr[\mathcal{D}(X_1) = 1] = 1 - \Pr[\mathcal{D}(X_1) = 0]$, and therefore (2.1) can be rewritten as

$$\Pr[\mathcal{D}(X_b) = b] = \frac{1}{2} + \frac{1}{2} (\Pr[\mathcal{D}(X_0) = 0] - \Pr[\mathcal{D}(X_1) = 0]). \quad (2.2)$$

To go from the probability in (2.2) to the advantage, let $\mathcal{D}_{\text{unif}}$ return 0 or 1 uniformly at random. The probability that this simple distinguisher produces the right guess is $\Pr[\mathcal{D}_{\text{unif}}(X_b) = b] = \frac{1}{2}$, meaning that the increased probability of using \mathcal{D} compared to $\mathcal{D}_{\text{unif}}$ is the second term in (2.2). This leads to the formal definition of advantage as given in [CDN15; Def. 2.3], where we consider the absolute value¹ and scale it to be a value in $[0, 1]$.

Definition 2.1:

Let X_0 and X_1 be random variables, and let \mathcal{D} be a distinguisher. The advantage of \mathcal{D} distinguishing X_0 and X_1 is defined as

$$\text{Adv}(\mathcal{D}) = |\Pr[\mathcal{D}(X_0) = 0] - \Pr[\mathcal{D}(X_1) = 0]|.$$

Since we now have a way to measure how well the environment can distinguish the two scenarios of the cryptographic game, we can also give a precise definition of a probability being ‘sufficiently small’, or rather it being

¹If $\Pr[\mathcal{D}(X_0) = 0] - \Pr[\mathcal{D}(X_1) = 0] < 0$, the distinguisher \mathcal{D} is worse than random guessing, i.e. $\mathcal{D}_{\text{unif}}$. But the distinguisher $\mathcal{D}'(X_b) = 1 - \mathcal{D}(X_b)$, which flips the output of \mathcal{D} , outperforms $\mathcal{D}_{\text{unif}}$ by the same amount.

I. Background

negligible in some security parameter. We use the same definition as [CDN15; Def. 2.6].

Definition 2.2:

Consider a map $f : \mathbb{N} \rightarrow \mathbb{R}$. If for any $c \in \mathbb{N}$ there exists $n_c \in \mathbb{N}$ such that $f(n) \leq n^{-c}$ whenever $n \geq n_c$, then f is called *negligible* in n .

In practice, we rarely use this definition directly. Instead, it is commonly shown that $f(n) \leq k^{-n}$ for some $k > 1$. This implies negligibility in n as $\lim_{n \rightarrow \infty} n^c / k^n = 0$ for any $c \in \mathbb{N}$.

Definition 2.3 (Statistical indistinguishability):

Let X_0 and X_1 be random variables whose distributions depend on a parameter $\kappa \in \mathbb{N}$, and let \mathcal{D} be a distinguisher. If $\text{Adv}(\mathcal{D})$ is negligible in κ , then X_0 and X_1 are said to be *statistically indistinguishable* by \mathcal{D} .

In the definition, we think of κ as a security parameter that we can use to adjust the security level of a cryptographic protocol.

Definition 2.3 only considers a single distinguisher, but it can easily be extended to a set of distinguishers. In particular, we often look at the set of distinguishers running in polynomial time since it is in many cases reasonable to assume that the environment is computationally bounded.

Definition 2.4 (Computational indistinguishability):

Let X_0 and X_1 be random variables whose distributions depend on a parameter $\kappa \in \mathbb{N}$. If X_0 and X_1 are statistically indistinguishable by every distinguisher running in polynomial time, then X_0 and X_1 are said to be *computationally indistinguishable*.

Remark:

It is possible to present Definitions 2.3 and 2.4 in a more general way by using the concept of *statistical distance*. This generalization is not necessary to understand Paper B, so it is omitted here. Further details may be found in [CDN15; Ch. 2].

Recall that in the cryptographic game, the two variables X_0 and X_1 represent the information seen by the environment in each of the scenarios (a) and (b). Having established Definitions 2.3 and 2.4, we say that the protocol is *statistically secure* if X_0 and X_1 are statistically indistinguishable by all distinguishers. Similarly, we say that the protocol is *computationally secure* if X_0 and X_1 are computationally indistinguishable.

3 From classical to quantum computers

This section covers the basics of quantum error correcting codes from a mathematical point of view. Therefore, it is not meant as a precise physical description of quantum mechanics and quantum systems. Instead it is meant as a concise description of the mathematical framework necessary to understand asymmetric, non-binary quantum codes. Such a description may be difficult to find elsewhere in the literature. The exposition is based on [AK01; Aly08; Got97; KKKS06; NC10]. Parts of the introduction below bear a similarity to the introductions of Papers D and E, where symmetric and asymmetric quantum codes are also defined.

As described in Section 1, codewords of classical information are subject to a single type of error – namely the bit flip. When moving to quantum information, we still need to correct for bit flips as before, but a new type of error emerges as well. This new type of error is the so-called *phase shift*, where the relative phase between the quantum bits is changed.

Because of this, there are two types of minimal distance for a quantum code: one for bit flips and one for phase shifts. For reasons that will become apparent later, these distances are denoted d_x and d_z , respectively. These two distances has led to two different approaches when describing quantum codes. One approach is not to differentiate between the two types of errors and simply associate the quantum code with a single minimal distance $d = \min\{d_x, d_z\}$, ignoring the higher of the two distances. Alternatively, if the two error types are assumed to happen with different probabilities as suggested in [AKS06], both distances are seen as part of the code parameters. Quantum codes of the latter type are called *asymmetric*, and codes of the former *symmetric*. Inspired by the $[[n, k, d]]_q$ notation for classical codes, the parameters of an asymmetric quantum code are presented as $[[[n, k, d_z/d_x]]_q]$, and those of a symmetric code as $[[n, k, d]]_q$. As in the classical case, n and k are called the length and dimension, respectively. However, when we say that a quantum code has length n and dimension k , this actually means that it is a q^k -dimensional subspace of \mathbb{C}^{q^n} .

One very common way to construct quantum error-correcting codes is by using the so-called CSS-construction named after Calderbank, Shor, and Steane [CS96; Ste96]. The original construction uses only binary, dual-containing codes, but it has later been generalized to arbitrary finite fields and to nested codes. The theorem below echoes the version found in [SKR09].

Theorem 3.1 (CSS-construction):

Given \mathbb{F}_q -linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ of length n and codimension ℓ , the CSS-construction ensures the existence of an asymmetric quantum code with parameters

$$[[[n, \ell, d_z/d_x]]_q]$$

where $d_z = d(\mathcal{C}_1, \mathcal{C}_2)$ and $d_x = d(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$.

I. Background

This is, in principle, all that is needed to start searching for parameters of asymmetric quantum codes over arbitrary finite fields. Theorem 3.1 does not, however, give any insight into the underlying construction. The following sections aim to give at least some intuition about the quantum codes produced by the CSS-construction.

Notation

In quantum mechanics, vectors are usually represented in *ket*-notation, meaning that a vector \mathbf{v} in matrix notation is instead denoted $|\mathbf{v}\rangle$. This is paired with the *bra*-notation $\langle \mathbf{v}|$ which denotes the linear map in the dual space such that $\langle \mathbf{v}|\mathbf{u}\rangle$ gives the inner product between $|\mathbf{v}\rangle$ and $|\mathbf{u}\rangle$. In this thesis, the vectors $|\mathbf{v}\rangle$ will always be elements of \mathbb{C}^{q^n} , and in this case $\langle \mathbf{v}|$ has matrix representation $|\mathbf{v}\rangle^\dagger$, where \dagger denotes conjugate transposition. For more details, see [NC10; Ch. 2].

A single-qubit system

As a very simple example, we may consider a quantum system consisting of a single quantum bit or *qubit*. The physical implementation of such a qubit could for instance be the phase of a photon or an electron orbiting a single atom [NC10]. The state of a system like this can be represented by a vector in \mathbb{C}^2 . It is common practice to fix an orthonormal basis of \mathbb{C}^2 and label its two vectors as $|0\rangle$ and $|1\rangle$, which correspond, in a certain sense, to the bits 0 and 1 in the classical case. In contrast to the classical setting, however, the qubit is not restricted to be in either state $|0\rangle$ or $|1\rangle$. Instead, it can also be a linear combination $\alpha|0\rangle + \beta|1\rangle$ of the two, where $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta|^2 = 1$. This corresponds to the qubit being in a superposition between the two basis states, which can be interpreted in the following way: If measure this superposition in the computational basis $\{|0\rangle, |1\rangle\}$, it will collapse to one of the two basis states. The probability of it collapsing to $|0\rangle$ is $|\alpha|^2$, and the probability of it collapsing to $|1\rangle$ is $|\beta|^2$.

The bit flip and phase shift errors for the single-qubit system can be described as operators X and Z , respectively, defined by

$$X: \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{array} \quad \text{and} \quad Z: \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{array} .$$

That these operators are called X and Z is the reason why the two distances of a quantum code are denoted d_x and d_z .

The phase shift error Z changes the *relative phase* of the two basis states. It is also possible to change the *global phase* of a quantum state $|\varphi\rangle$ by taking it to $e^{i\theta}|\varphi\rangle$ for some $\theta \in \mathbb{R}$. The difference between these two types of phases is that a change in relative phase may alter the results of a measurement, whereas a change in global phase cannot; see for instance [NC10; p. 93].

3. From classical to quantum computers

Non-binary alphabets

In the theoretical framework, nothing prevents us from generalizing the quantum systems under consideration to q -ary alphabets. Instead of labelling the basis vectors as $|0\rangle$ and $|1\rangle$ as before, we consider an orthonormal basis $\{|u\rangle\}_{u \in \mathbb{F}_q} \subseteq \mathbb{C}^q$. Of course, the errors that we aim to correct must reflect the larger alphabet size. Following [KKKS06], for every $v \in \mathbb{F}_q$ the error operators are now

$$X(v): |u\rangle \mapsto |u + v\rangle \quad \text{and} \quad Z(v): |u\rangle \mapsto \omega^{\text{tr}(uv)}|u\rangle$$

where $\omega \in \mathbb{C}$ is a fixed p 'th root of unity, and $\text{tr}: \mathbb{F}_q \rightarrow \mathbb{F}_p$ is the field trace $\text{tr}(a) = \sum_{i=0}^{r-1} a^{q^i}$ with $q = p^r$. If $q = 2$, it may be noted that $X(1)$ and $Z(1)$ give the same operators as X and Z mentioned in the previous section. From the definitions, simple calculations lead to the following result.

Proposition 3.2:

For any $v, v' \in \mathbb{F}_q$, we have the following:

- (i) $X(0) = Z(0) = I$
- (ii) $X(v)X(v') = X(v + v')$ and $Z(v)Z(v') = Z(v + v')$
- (iii) $X(v)^{-1} = X(v)^{p-1}$ and $Z(v)^{-1} = Z(v)^{p-1}$
- (iv) $X(v)$ and $Z(v)$ are unitary²

Multiple-qubit systems

In order to take systems of single qubits and combine them into a single system of multiple qubits, the postulates of quantum mechanics specify that the state of the full system is described by the tensor product of the individual qubit states [NC10; p. 94]. That is, if a system has n qubits each in states $|\varphi_1\rangle$, $|\varphi_2\rangle$, and $|\varphi_n\rangle$, respectively, then the state of the combined system is $|\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_n\rangle$.

In terms of the errors operators, we use a similar approach and describe the errors that act on the full system by the tensor product of single-qubit errors [KKKS06]. Thus, for any $\mathbf{v} \in \mathbb{F}_q^n$ we let $X(\mathbf{v}) = X(v_1) \otimes X(v_2) \otimes \cdots \otimes X(v_n)$. This notation means that $X(\mathbf{v})$ applied to the state $|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_n\rangle$ results in the state

$$X(\mathbf{v})|\varphi\rangle = X(v_1)|\varphi_1\rangle \otimes X(v_2)|\varphi_2\rangle \otimes \cdots \otimes X(v_n)|\varphi_n\rangle. \quad (2.3)$$

That is, the operator $X(\mathbf{v})$ is acting in a component-wise fashion. The phase-shift error $Z(\mathbf{v})$ is defined analogously. Note that these operators have similar properties to the ones presented in Proposition 3.2, albeit in a componentwise fashion. For instance, we have $X(\mathbf{v})X(\mathbf{v}') = X(\mathbf{v} + \mathbf{v}')$ for any $\mathbf{v}, \mathbf{v}' \in \mathbb{F}_q^n$. Additionally, the properties of the tensor product imply that $X(\mathbf{v})$ and $Z(\mathbf{v})$ are also unitary.

²An operator U is called unitary if it satisfies $U^\dagger = U^{-1}$.

I. Background

Now, define the multiplicative group

$$\mathcal{G}_n = \{\omega^c X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}$$

as in [KKKS06]. Later, it shall be important to know whether two elements of this group commute or not. In order to determine a condition for this, note that

$$Z(\mathbf{b})X(\mathbf{a}) = \omega^{\text{tr}(\mathbf{b} \cdot \mathbf{a})} X(\mathbf{a})Z(\mathbf{b}),$$

and therefore

$$X(\mathbf{a})Z(\mathbf{b})X(\mathbf{a}')Z(\mathbf{b}') = \omega^{\text{tr}(\mathbf{b} \cdot \mathbf{a}')} X(\mathbf{a} + \mathbf{a}')Z(\mathbf{b} + \mathbf{b}'). \quad (2.4)$$

From this observation, we obtain the following result, which can also be found in [KKKS06; Lem. 5].

Proposition 3.3:

Let $E = \omega^c X(\mathbf{a})Z(\mathbf{b})$ and $E' = \omega^{c'} X(\mathbf{a}')Z(\mathbf{b}')$ be elements of \mathcal{G}_n . Then E and E' commute if and only if $\text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a}) = 0$.

Proof:

From (2.4), we have the two equalities

$$\begin{aligned} EE' &= \omega^{\text{tr}(\mathbf{b} \cdot \mathbf{a}')} X(\mathbf{a} + \mathbf{a}')Z(\mathbf{b} + \mathbf{b}') \\ E'E &= \omega^{\text{tr}(\mathbf{b}' \cdot \mathbf{a})} X(\mathbf{a} + \mathbf{a}')Z(\mathbf{b} + \mathbf{b}'), \end{aligned}$$

and from the linearity of tr we therefore have

$$EE' = \omega^{\text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a})} E'E. \quad (2.5)$$

Thus, $EE' = E'E$ if and only if $\omega^{\text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a})} = 1$. Since ω is a p 'th root of unity, this happens if and only if $\text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a}) \equiv 0 \pmod{p}$. Because tr maps to \mathbb{F}_p , this is equivalent to $\text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a}) = 0$. ■

Errors as an additive group

For an element $\omega^c X(\mathbf{a})Z(\mathbf{b})$ of \mathcal{G}_n , the overall factor ω^c corresponds to a global phase, which – as mentioned previously – does not change measurement results. Hence, we may ignore this factor, and as described in [KKKS06] each element $\omega^c X(\mathbf{a})Z(\mathbf{b})$ of \mathcal{G}_n can then be identified with a vector $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$. By Proposition 3.3, two elements $E, E' \in \mathcal{G}_n$ commute if and only if $\text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a}) = 0$. Because of this, we define the symplectic inner product $\langle (\mathbf{a}|\mathbf{b}), (\mathbf{a}'|\mathbf{b}') \rangle_s = \text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a})$. Two errors in \mathcal{G}_n then commute, if and only if the corresponding vectors in \mathbb{F}_q^{2n} are orthogonal with respect to the symplectic inner product.

In addition, the observation in (2.4) implies that apart from a factor of ω , a product of two operators in \mathcal{G}_n corresponds exactly to the sum of the associated elements in \mathbb{F}_q^{2n} . More precisely, we have the following result.

3. From classical to quantum computers

Proposition 3.4:

The quotient group $\mathcal{G}_n / \langle \omega I \rangle$ is isomorphic to the additive group \mathbb{F}_q^{2n} .

Proof:

The mapping $\psi: \mathcal{G}_n \rightarrow \mathbb{F}_q^{2n}$ given by $\psi(\omega^k X(\mathbf{a})Z(\mathbf{b})) = (\mathbf{a}|\mathbf{b})$ is a group homomorphism by (2.4). Moreover, it is surjective and $\ker \psi = \langle \omega I \rangle$. Thus, $\mathcal{G}_n / \langle \omega I \rangle \simeq \mathbb{F}_q^{2n}$ by the Isomorphism Theorem. ■

For an element $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$, we define x - and z -weights as $w_x(\mathbf{a}|\mathbf{b}) = w_H(\mathbf{a})$ and $w_z(\mathbf{a}|\mathbf{b}) = w_H(\mathbf{b})$, where w_H denotes the usual Hamming weight. Additionally, we denote by w_s the symplectic weight given by $w_s(\mathbf{a}|\mathbf{b}) = |\text{supp } \mathbf{a} \cup \text{supp } \mathbf{b}|$. Comparing this with (2.3), the x - and z -weights correspond exactly to the number of qubits affected by a bit-flip and a phase-flip, respectively, when a quantum state is subjected to the error $X(\mathbf{a})Z(\mathbf{b})$. Similarly, the symplectic weight is the number of qubits affected by some error regardless of error type.

Stabilizer codes

Let S be an abelian subgroup of \mathcal{G}_n , and further assume that $\omega^k I \notin S$ for every $k \in \mathbb{Z}_p^*$. Since the operators in S are unitary, the Spectral Theorem implies that they are diagonalizable, see e.g. [Lan02; p. 583]. Because they all commute, they are also simultaneously diagonalizable [HJ13; Thm. 1.3.21]. As done in [AK01; KKKS06], we therefore define the vector space

$$Q = \bigcap_{E \in S} \{ \mathbf{v} \in \mathbb{C}^{q^n} \mid E\mathbf{v} = \mathbf{v} \}.$$

In other words, Q is the joint 1-eigenspaces of the operators in S . We call Q the quantum code stabilized by S , and we call S a stabilizer. The following proposition, whose binary equivalent can be found in [NC10; p. 455], explains why we require S to be abelian and $\omega^k I \notin S$.

Proposition 3.5:

Let S be a subgroup of \mathcal{G}_n , and assume that S is non-abelian or $\omega^k I \in S$ for some $k \in \mathbb{Z}_p^$. Then the quantum code Q stabilized by S contains only the zero vector.*

Proof:

Assume first that S is non-abelian. This means that there exist $E, E' \in S$ such that $EE' = \omega^c E'E$ for some non-zero c by (2.5). Thus, for any $|\varphi\rangle \in Q$ we have

$$\langle \varphi | \varphi \rangle = \langle \varphi | EE' | \varphi \rangle = \omega^c \langle \varphi | E'E | \varphi \rangle = \omega^c \langle \varphi | \varphi \rangle,$$

implying that $|\varphi\rangle$ is the zero vector. Similarly, $\omega^k I \in S$ leads to $\omega^k |\varphi\rangle = |\varphi\rangle$ for all $|\varphi\rangle \in Q$, giving the same conclusion. ■

I. Background

Consider a stabilizer S , and let $S = \langle E_1, E_2, \dots, E_\ell \rangle$ be a minimal generating set. It may be shown that any such set has the same number of generators; see, for instance, [DF04; Sec. 6.1 Ex. 26(c)]. By using the structure from Proposition 3.4, we obtain the following characterization of the minimal generating sets, which is similar to the one found in [NC10; Prop. 10.3].

Lemma 3.6:

Let $S \subseteq \mathcal{G}_n$ be an abelian subgroup satisfying $\omega^k I \notin S$ for every $k \in \mathbb{Z}_p^$, and let $\mathcal{E} = \{E_1, E_2, \dots, E_\ell\}$ be a generating set for S . Additionally, let ψ be the isomorphism from the proof of Proposition 3.4. Then \mathcal{E} is a minimal generating set for S if and only if $\{\psi(E) \mid E \in \mathcal{E}\}$ is linearly independent in \mathbb{F}_q^{2n} as an \mathbb{F}_p -vector space.*

Proof:

Denote by $\mathbf{v}_i = \psi(E_i)$ the images of the generators. Aiming to show the contrapositive, assume that there exist coefficients $c_i \in \mathbb{F}_p$, not all zero, such that $\sum_{i=1}^\ell c_i \mathbf{v}_i = \mathbf{0}$. By Proposition 3.4, this happens if and only if

$$\prod_{i=1}^\ell E_i^{c_i} = \omega^k I \quad (2.6)$$

for some $k \in \mathbb{Z}_p$. By the assumptions on S , however, we must have $k = 0$. Thus, Proposition 3.2 implies that (2.6) is equivalent to

$$E_j = \prod_{i \neq j} E_i^{-c_i c_j^{-1} \bmod p}$$

for some index j with $c_j \neq 0$, meaning that \mathcal{E} is not minimal. ■

To determine the dimension of a stabilizer code, we will rely on the following lemmata from [NC10; Prop. 10.4] and [Pre99; p. 36], respectively. The proofs can be found in Appendix A on page 20.

Lemma 3.7:

Let S be a stabilizer, and let $\{E_1, E_2, \dots, E_\ell\}$ be a minimal generating set for S . Further, assume that $\omega^k I \notin S$ for every $k \in \mathbb{Z}_p^$. For any $i \in \{1, 2, \dots, \ell\}$ and any $c \in \mathbb{Z}_p$, there exists an $F \in \mathcal{G}_n$, such that $E_i F = \omega^c F E_i$, and $E_j F = F E_j$ for all $j \neq i$.*

Lemma 3.8:

Let F be a unitary operator such that $EF = \omega FE$. Then for any $k \in \mathbb{Z}_p$, we have $E|\varphi\rangle = \omega^k |\varphi\rangle$ if and only if $E(F|\varphi\rangle) = \omega^{k+1} F|\varphi\rangle$.

Having stated these lemmata, we can determine the dimensions of stabilizer codes. The proof below follows the strategy from [Pre99].

3. From classical to quantum computers

Proposition 3.9:

Let Q be a quantum stabilizer code of length n . If its stabilizer S is generated by ℓ generators, then Q has dimension q^n/p^ℓ .

Proof:

Let S be a stabilizer, and let $\{E_1, E_2, \dots, E_\ell\}$ be a minimal generating set for S . Considering the first generator E_1 , Lemma 3.7 implies the existence of a unitary operator $F \in \mathcal{G}_n$ satisfying $E_1 F = \omega F E_1$. Lemma 3.8 then shows that F sends each 1-eigenstate of E_1 to a distinct ω -eigenstate, each ω -eigenstate to a distinct ω^2 -eigenstate, and so forth. From this it follows that each eigenspace has the same dimension, namely one p 'th of the dimension of the full space. In particular, the 1-eigenspace of E_1 has dimension q^n/p .

Consider now the operator E_2 . Again, Lemma 3.7 implies the existence of an operator F , such that $E_1 F = F E_1$, but $E_2 F = \omega F E_2$. Then for any 1-eigenstate $|\varphi\rangle$ of E_1 , it follows that $F|\varphi\rangle$ is also a 1-eigenstate of E_1 . Simultaneously, Lemma 3.8 implies that within the 1-eigenspace of E_1 , the operator F permutes the eigenspaces of E_2 . This leads us to the conclusion that the p different eigenspaces of E_2 have the same dimension when intersected with the 1-eigenspace of E_1 . Thus, the joint 1-eigenspace of E_1 and E_2 has dimension q^n/p^2 . Continuing in this fashion, we see that the quantum code Q stabilized by S has dimension q^n/p^ℓ . ■

Detectable and correctable errors

When analysing a quantum stabilizer code and the errors it offers protection against, it turns out that those operators that commute with all elements of the stabilizer S play a vital role [AK01; Got97; KKS06]. That is, we need to consider the centralizer

$$Z(S) = \{F \in \mathcal{G}_n \mid \forall E \in S: FE = EF\}$$

of S . But in the literature, the normalizer

$$N(S) = \{F \in \mathcal{G}_n \mid \forall E \in S: FEF^\dagger \in S\}$$

is more commonly used since $N(S) = Z(S)$ in the case of a stabilizer group [Got97; p. 19]. For a proof of this, see Proposition A.1 on page 20. Additionally, we note that $S \subseteq N(S)$.

If a quantum state $|\varphi\rangle$ is subjected to an error F , we will attempt to recover it by performing a set of measurements dictated by the stabilizer. More precisely, we will measure the eigenvalues of $F|\varphi\rangle$ for each generator E_1, E_2, \dots, E_ℓ of the stabilizer, which yields an error syndrome $s_1 s_2 \dots s_\ell$, where each $s_i \in \{1, \omega, \dots, \omega^{p-1}\}$. This leads to a strategy similar to the one used in classical coding theory, where we choose our correction depending on the resulting syndrome [Got97; Sec. 3.2][NC10; p. 466].

Let us now consider a situation where two errors $F_1, F_2 \in \mathcal{G}_n$ have the same syndrome for any word. That is, for each i , we have both $E_i F_1 = \omega^{k_i} F_1 E_i$ and

I. Background

$E_i F_2 = \omega^{k_i} F_2 E_i$, meaning in particular that $F_1^\dagger = \omega^{-k_i} E_i^\dagger F_1^\dagger E_i$. Therefore, the operator $F_1^\dagger F_2$ satisfies $E_i(F_1^\dagger F_2) = (F_1^\dagger F_2)E_i$ for every i . Thus, F_1 and F_2 have the same syndrome, if and only if $F_1^\dagger F_2 \in N(S)$.

All is not lost, however, if F_1 and F_2 have the same syndrome. In the case where $F_1^\dagger F_2$ is not only in $N(S)$, but also in S , we have that $F_1^\dagger F_2|\varphi\rangle = |\varphi\rangle$, leading to $F_2|\varphi\rangle = F_1|\varphi\rangle$ for every $|\varphi\rangle \in Q$. Thus, F_1 and F_2 affect the coded states in the same way in this case, meaning that it not even necessary to distinguish between them – correcting either of the two errors will recover the original quantum state $|\varphi\rangle$. These observations lead to the following theorem [Got97; NC10].³

Theorem 3.10:

Let Q be a quantum code stabilized by S . A set of errors $\mathcal{E} \subseteq \mathcal{G}_n$ is correctable by Q if $F_1^\dagger F_2 \notin N(S) \setminus S$ for all $F_1, F_2 \in \mathcal{E}$.

If we merely want to determine if an error $F \in \mathcal{G}_n \setminus S$ has happened, it is enough to ensure that F does not have a zero syndrome – which is the syndrome of any operator in S . In particular, we can use the same arguments as above, letting $F_1 = I$ and $F_2 = F$, to conclude that the quantum code Q can detect any error $F \notin N(S) \setminus S$. Thus, the minimal distances d_x and d_z of the code can be determined by finding the operators in $N(S) \setminus S$ that have the lowest x - and z -weights, respectively.

The CSS-construction

We can now tie all of this together to describe the underlying construction in Theorem 3.1. Consider two linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^n$ with dimensions k_2 and k_1 , respectively. Further, let $\ell = k_1 - k_2$ denote their codimension. We will use these codes to construct an \mathbb{F}_p -subspace of \mathbb{F}_q^{2n} , and then exploit the connection between \mathcal{G}_n and \mathbb{F}_q^{2n} to construct quantum error correcting codes.

Define the \mathbb{F}_q -vector space

$$\Gamma = \{(\mathbf{a}|\mathbf{b}) \mid \mathbf{a} \in \mathcal{C}_1^\perp, \mathbf{b} \in \mathcal{C}_2\} \subseteq \mathbb{F}_q^{2n}.$$

If we let \mathcal{B}_1^\perp and \mathcal{B}_2 denote bases for \mathcal{C}_1^\perp and \mathcal{C}_2 , respectively, then it is clear that

$$\mathcal{B}_\Gamma = \{(\mathbf{a}|\mathbf{0}) \mid \mathbf{a} \in \mathcal{B}_1^\perp\} \cup \{(\mathbf{0}|\mathbf{b}) \mid \mathbf{b} \in \mathcal{B}_2\},$$

is a basis for Γ . Subsequently, Γ has dimension $n - k_1 + k_2 = n - \ell$. We will construct a stabilizer based on \mathcal{B}_Γ , but whereas Γ is an \mathbb{F}_q -vector space, the stabilizer S can only be given the structure of an \mathbb{F}_p -vector space. Therefore, we first expand the elements of \mathcal{B}_Γ in a basis of \mathbb{F}_q over \mathbb{F}_p . Thus, let $q = p^r$, and fix an $\alpha \in \mathbb{F}_q$ such that $\mathbb{F}_q = \text{span}_{\mathbb{F}_p}\{1, \alpha, \dots, \alpha^{r-1}\}$. Define the map

³A general condition for quantum errors to be correctable is given in [KL97].

3. From classical to quantum computers

$\gamma: \mathbb{F}_q^{2n} \rightarrow \mathcal{P}(\mathbb{F}_q^{2n})$ given by $\mathbf{v} \mapsto \{\mathbf{v}, \alpha\mathbf{v}, \dots, \alpha^{p-1}\mathbf{v}\}$. The following lemma lists two properties of γ .

Lemma 3.11:

The map $\gamma: \mathbb{F}_q^{2n} \rightarrow \mathcal{P}(\mathbb{F}_q^{2n})$ has the following properties.

- (i) *A set $V \subseteq \mathbb{F}_q^{2n}$ is linearly independent over \mathbb{F}_q if and only if $\bigcup_{\mathbf{v} \in V} \gamma(\mathbf{v})$ is linearly independent over \mathbb{F}_p*
- (ii) *Any vector $\mathbf{v}' \in \gamma(\mathbf{v})$ satisfies $w_H(\mathbf{v}') = w_H(\mathbf{v})$*

We will use the image of \mathcal{B}_Γ under γ to form the generators for a stabilizer code. Abusing notation, let

$$\gamma(\mathcal{B}_\Gamma) = \bigcup_{\mathbf{v} \in \mathcal{B}_\Gamma} \gamma(\mathbf{v}),$$

and let S be the subgroup of \mathcal{G}_n generated by $\mathcal{E} = \{X(\mathbf{a})Z(\mathbf{b}) \mid (\mathbf{a}|\mathbf{b}) \in \gamma(\mathcal{B}_\Gamma)\}$. Of course, we must check that S does in fact possess the properties required for a stabilizer. The following proposition guarantees that this is indeed the case.

Proposition 3.12:

The subgroup $S \subseteq \mathcal{G}_n$ generated by the operators $\mathcal{E} = \{X(\mathbf{a})Z(\mathbf{b}) \mid (\mathbf{a}|\mathbf{b}) \in \gamma(\mathcal{B}_\Gamma)\}$ is abelian, and $\omega^k I \notin S$ for every $k \in \mathbb{Z}_p^$. Furthermore, \mathcal{E} is a minimal generating set.*

Proof:

Observe first that for any two vectors $(\mathbf{a}|\mathbf{b}), (\mathbf{a}'|\mathbf{b}') \in \Gamma$, we have

$$\langle (\mathbf{a}|\mathbf{b}), (\mathbf{a}'|\mathbf{b}') \rangle_s = \text{tr}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a}) = \text{tr}(0 - 0) = 0 \quad (2.7)$$

since $\mathbf{b}, \mathbf{b}' \in \mathcal{C}_2$ and $\mathbf{a}, \mathbf{a}' \in \mathcal{C}_1^\perp \subsetneq \mathcal{C}_2^\perp$. In particular, this also holds true for $(\mathbf{0}|\mathbf{b}), (\mathbf{a}'|\mathbf{0}) \in \Gamma$, and combining this with (2.4), we see that S can in fact be described as

$$S = \{X(\mathbf{a})Z(\mathbf{b}) \mid (\mathbf{a}|\mathbf{b}) \in \Gamma\}.$$

Thus, $\omega^k I \notin S$ for any $k \in \mathbb{Z}_p^*$, and (2.7) combined with Proposition 3.3 imply that S is abelian.

That \mathcal{E} is a minimal generating set, follows from the fact that \mathcal{B}_Γ is a basis combined with Lemmata 3.6 and 3.11. ■

We can now restate Theorem 3.1 in the language of quantum stabilizer codes.

Proposition 3.13:

Let $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^n$ be nested codes of codimension ℓ , and let S be defined as in Proposition 3.12. Then the corresponding stabilizer quantum code Q has

I. Background

parameters

$$[[n, \ell, d_z/d_x]]_q$$

where $d_z = d(\mathcal{C}_1, \mathcal{C}_2)$ and $d_x = d(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$.

Before giving the proof, recall that the notation $[[n, \ell]]_q$ means that the quantum code Q is a q^ℓ -dimensional subspace of \mathbb{C}^{q^n} .

Proof:

From Proposition 3.12 it is already known, that S is a valid stabilizer, so Q is indeed defined. To find its dimension, we only need to determine the number of elements in \mathcal{E} by Propositions 3.9 and 3.12. Each of the $n - \ell$ vectors in \mathcal{B}_Γ gives rise to a set of r vectors when applying γ . These vectors are all distinct, so Proposition 3.9 gives

$$\dim Q = \frac{q^n}{p^{r(n-\ell)}} = \frac{q^n}{q^{n-\ell}} = q^\ell$$

as claimed.

To determine the minimal distance, we must consider the elements in $N(S)$. In order for an error E to commute with all elements of S , it must be the case that the corresponding vector $(\mathbf{a}|\mathbf{b})$ is symplectically orthogonal to all vectors in Γ . Thus, $E \in N(S)$ if and only if $\mathbf{a} \in \mathcal{C}_2^\perp$ and $\mathbf{b} \in \mathcal{C}_1$. We now use that it is possible to correct bit-flips and phase-shifts independently when working with CSS-codes, see e.g. [CS96] or [NC10]. For the x -weight, we thus consider some $E \in N(S)$ corresponding to $(\mathbf{a}|\mathbf{0})$ with $\mathbf{a} \in \mathcal{C}_2^\perp$. But as described in Theorem 3.10, we need not correct errors in S ; i.e. we can disregard the vectors with $\mathbf{a} \in \mathcal{C}_1^\perp$. Thus, we conclude that $w_x(E) \geq d(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$. The z -weight is analogous. ■

Steane-enlargement

In Papers D and E, we use a different technique based on the CSS-construction. This other construction – called Steane-enlargement – stems from [Ste99], and the central idea is to add additional generators to the stabilizer from the CSS-construction. These additional generators are chosen in such a way that we can still bound the minimal distance. In this way, the dimension of the quantum code is increased – justifying why the technique is called *enlargement* – while the decrease in minimal distance can be controlled. In certain cases, it is even possible to increase the dimension without sacrificing minimal distance.

One requirement of this technique, however, is that the nested codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_q^n$ used must satisfy $\mathcal{C}_2 = \mathcal{C}_1^\perp$. In other words, the technique relies on dual-containing codes. Like the CSS-construction, Steane's original paper considered only binary codes, but the technique has later been generalized to finite fields of any size [Ham08; LLX10].

Appendix A Additional results

This appendix contains a selection of additional results and proofs that were omitted in the previous sections.

We first show that the centralizer and normalizer coincide for stabilizers. The binary case is, for instance, described in [Got97; p. 19].

Proposition A.1:

Let S be a subgroup of \mathcal{G}_n . If $\omega^k I \notin S$ for every $k \in \mathbb{Z}_p^$, then $N(S) = Z(S)$.*

Proof:

From the definitions of the centralizer and normalizer, it follows immediately that $Z(S) \subseteq N(S)$. Thus, let $F \in N(S)$, meaning that for every $E \in S$ we have $FEF^\dagger = E'$ for some $E' \in S$. Equation (2.5) then ensures the existence of some $c \in \mathbb{Z}_p$ such that $FE = E'F = \omega^c FE'$. Since F is invertible, this implies $\omega^c I = E(E')^\dagger \in S$. By assumption, this can only happen if $c = 0$, meaning $E = E'$ and $F \in Z(S)$. ■

Proof (Lemma 3.7):

The proof is essentially the same as the binary case given in [NC10; p. 458]. Consider the matrix G whose rows are given by the vectors in \mathbb{F}_q^{2n} corresponding to E_1, E_2, \dots, E_ℓ . By Lemma 3.6, these rows are linearly independent, so G has full rank. Thus, some $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$ provides a solution to the matrix system

$$G \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} \mathbf{a}^T \\ \mathbf{b}^T \end{bmatrix} = \omega^c \mathbf{e}_i,$$

where \mathbf{e}_i denotes the i 'th canonical basis (column) vector. The operator $X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{G}_n$ has the desired properties. ■

Proof (Lemma 3.8):

We adapt the arguments from [Pre99; p. 36] to the non-binary case. If $E|\varphi\rangle = \omega^k|\varphi\rangle$, it follows easily that $E(F|\varphi\rangle) = \omega F(E|\varphi\rangle) = \omega^{k+1}F|\varphi\rangle$. On the other hand, if $E(F|\varphi\rangle) = \omega^{k+1}F|\varphi\rangle$, then $\omega F(E|\varphi\rangle) = \omega F(\omega^k|\varphi\rangle)$. The results now follows from F being unitary and therefore invertible. ■

Overview of Part II

Part II of this thesis comprises five scientific papers. Papers A and B treat problems related to multiparty computation, Paper C applies to both secret sharing and quantum error-correcting codes, and Papers D and E treat the construction of quantum error-correcting codes. The papers are kept as close to the published versions as possible, but in some cases, the layout and notation has been adjusted for consistency.

- **Paper A [Chr19]:** This work treats the relatively unknown problem of reliable message transmission (RMT), whose solution can be used as a subprotocol in a larger multiparty computation protocol. The literature already contained RMT-protocols that were asymptotically optimal, but since the focus was proving the existence of such protocols, they were relatively unoptimized. Thus, the aim of Paper A was to utilize more of the error-correcting capabilities of the underlying codes in order to provide more efficient protocols. Specifically, the improved protocols allow more information symbols per transmission or smaller field sizes.
- **Paper B [CCG18]:** The origin of this work is the observation that many protocols for extension of oblivious transfer (OT) are based on linear codes in some way, and that better code parameters lead to more efficient OT-extension. The papers describing these protocols restricted themselves to binary codes, but it is generally easier to construct good codes over larger fields. This led us to show that the same OT-extension techniques generalize to the q -ary case, and it turns out that using larger field sizes leads to a trade-off between the number of base OT's and the communication complexity.
- **Paper C [CG18]:** Having seen that the construction of secret sharing schemes from [Che+07; KUM12] and the CSS-construction of quantum codes both rely on nested codes and knowledge of their codimension and relative distances, this paper set out to explore these applications in the case of the Hermitian function field. By using a Feng-Rao type construction [FR95], where the relative distances are known, we gave a number of quantum codes whose parameters were better than other known constructions.

In addition, this paper served as a starting point for Paper D.

Overview of Part II

- **Paper D [CG20a]:** With the Hermitian function field giving rise to good quantum codes via the CSS construction in Paper C, it is natural to ask if the same is true when applying Steane-enlargement. This paper answers that question in the affirmative if symmetric quantum codes with a relatively small minimal distance are desired.
- **Paper E [CG20b]:** After working on Steane-enlargement of Hermitian codes in Paper D, Olav Geil and I realized that certain codes from Cartesian product point sets are particularly easy to apply Steane-enlargement to. More precisely, for sufficiently small distances we can often guarantee that the dimension can be increased without sacrificing minimal distance merely by knowing the sizes of the sets in the Cartesian products.

References

- [AK01] **A.E. Ashikhmin and E. Knill.** 'Nonbinary quantum stabilizer codes'. In: *IEEE Trans. Inf. Theory* 47(7) (2001), pp. 3065–3072. DOI: 10.1109/18.959288.
- [AKS06] **S.A. Aly, A. Klappenecker and P.K. Sarvepalli.** 'Remarkable Degenerate Quantum Stabilizer Codes Derived from Duadic Codes'. In: *2006 IEEE International Symposium on Information Theory*. July 2006, pp. 1105–1108. DOI: 10.1109/ISIT.2006.261955.
- [Aly08] **S.A. Aly.** 'Quantum Error Control Codes'. PhD thesis. Texas A&M University, May 2008. URL: <http://hdl.handle.net/1969.1/85910>.
- [CCG18] **I. Cascudo, R.B. Christensen and J.S. Gundersen.** 'Actively Secure OT-Extension from q -ary Linear Codes'. In: *Security and Cryptography for Networks*. Springer International Publishing, 2018, pp. 333–348. ISBN: 978-3-319-98113-0. DOI: 10.1007/978-3-319-98113-0_18.
- [CDN15] **R. Cramer, I.B. Damgård and J.B. Nielsen.** *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015. ISBN: 978-1-107-04305-3.
- [CF01] **R. Canetti and M. Fischlin.** 'Universally Composable Commitments'. In: *Advances in Cryptology – CRYPTO 2001*. Springer Berlin Heidelberg, 2001, pp. 19–40. ISBN: 978-3-540-44647-7. DOI: 10.1007/3-540-44647-8_2.
- [CG18] **R.B. Christensen and O. Geil.** 'On nested code pairs from the Hermitian curve'. In: *CoRR* abs/1807.04042 (2018). arXiv: 1807.04042. URL: <http://arxiv.org/abs/1807.04042>.
- [CG20a] **R.B. Christensen and O. Geil.** 'Steane-enlargement of quantum codes from the Hermitian function field'. In: *Des. Codes Cryptogr.* (2020). To appear. DOI: 10.1007/s10623-019-00709-7.
- [CG20b] **R.B. Christensen and O. Geil.** 'On Steane-Enlargement of Quantum Codes from Cartesian Product Point Sets'. In: *Quantum Inf. Process.* 19(7) (2020). DOI: 10.1007/s11128-020-02691-9.
- [Che+07] **H. Chen, R. Cramer, S. Goldwasser, R. de Haan and V. Vaikuntanathan.** 'Secure Computation from Random Error Correcting Codes'. In: *Advances in Cryptology – EUROCRYPT 2007*. Springer Berlin Heidelberg,

References

- 2007, pp. 291–310. ISBN: 978-3-540-72540-4. DOI: 10.1007/978-3-540-72540-4_17.
- [Chr19] **R.B. Christensen**. ‘On one-round reliable message transmission’. In: *Inf. Process. Lett.* 147 (2019), pp. 22–26. ISSN: 0020-0190. DOI: 10.1016/j.ipl.2019.02.011.
- [CS96] **A.R. Calderbank and P.W. Shor**. ‘Good quantum error-correcting codes exist’. In: *Phys. Rev. A* 54(2) (Aug. 1996), pp. 1098–1105. DOI: 10.1103/PhysRevA.54.1098.
- [DF04] **D.S. Dummit and R.M. Foote**. *Abstract Algebra*. 3rd ed. John Wiley & Sons, 2004. ISBN: 978-0-471-43334-7.
- [DH76] **W. Diffie and M. Hellman**. ‘New directions in cryptography’. In: *IEEE Trans. Inf. Theory* 22(6) (Nov. 1976), pp. 644–654. ISSN: 1557-9654. DOI: 10.1109/TIT.1976.1055638.
- [FR95] **G.-L. Feng and T.R.N. Rao**. ‘Improved geometric Goppa codes. Part I: Basic Theory’. In: *IEEE Trans. Inf. Theory* 41(6) (1995), pp. 1678–1693. DOI: 10.1109/18.476241.
- [Got97] **D.E. Gottesman**. ‘Stabilizer Codes and Quantum Error Correction’. PhD thesis. California Institute of Technology, May 1997. DOI: 10.7907/rzr7-dt72.
- [Ham08] **M. Hamada**. ‘Concatenated Quantum Codes Constructible in Polynomial Time: Efficient Decoding and Error Correction’. In: *IEEE Trans. Inf. Theory* 54(12) (Dec. 2008), pp. 5689–5704. ISSN: 0018-9448. DOI: 10.1109/TIT.2008.2006416.
- [HJ13] **R.A. Horn and C.R. Johnson**. *Matrix Analysis*. 2nd ed. Cambridge University Press, 2013. ISBN: 978-0-521-83940-2.
- [HP03] **W.C. Huffman and V. Pless**. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003. ISBN: 978-0-521-78280-7.
- [JH04] **J. Justesen and T. Høholdt**. *A Course in Error-Correcting Codes*. 1st ed. European Mathematical Society, 2004. ISBN: 978-3-03719-001-2.
- [KKKS06] **A. Ketkar, A. Klappenecker, S. Kumar and P.K. Sarvepalli**. ‘Nonbinary Stabilizer Codes Over Finite Fields’. In: *IEEE Trans. Inf. Theory* 52(11) (2006), pp. 4892–4914. DOI: 10.1109/TIT.2006.883612.
- [KL97] **E. Knill and R. Laflamme**. ‘Theory of quantum error-correcting codes’. In: *Phys. Rev. A* 55(2) (Feb. 1997), pp. 900–911. DOI: 10.1103/PhysRevA.55.900.
- [KUM12] **J. Kurihara, T. Uyematsu and R. Matsumoto**. ‘Secret Sharing Schemes Based on Linear Codes Can Be Precisely Characterized by the Relative Generalized Hamming Weight’. In: *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E95.A(11) (2012), pp. 2067–2075. DOI: 10.1587/transfun.E95.A.2067.

I. Background

- [Lan02] **S. Lang.** *Algebra*. 3rd ed. Graduate Texts in Mathematics 211. Springer, 2002. ISBN: 978-0-387-95385-4.
- [LLX10] **S. Ling, J. Luo and C. Xing.** ‘Generalization of Steane’s enlargement construction of quantum codes and applications’. In: *IEEE Trans. Inf. Theory* 56(8) (2010), pp. 4080–4084. DOI: 10.1109/TIT.2010.2050828.
- [NC10] **M.A. Nielsen and I.L. Chuang.** *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge University Press, 2010. ISBN: 978-1-107-00217-3.
- [OOS17] **M. Orrù, E. Orsini and P. Scholl.** ‘Actively Secure 1-out-of-N OT Extension with Application to Private Set Intersection’. In: *Topics in Cryptology – CT-RSA 2017*. Springer International Publishing, 2017, pp. 381–396. ISBN: 978-3-319-52153-4. DOI: 10.1007/978-3-319-52153-4_22.
- [Pre99] **J. Preskill.** *Chapter 7. Quantum Error Correction*. Lecture notes. California Institute of Technology, 1999. URL: <http://www.theory.caltech.edu/people/preskill/ph229/notes/chap7.pdf> (visited on 12/02/2020).
- [RSA78] **R.L. Rivest, A. Shamir and L. Adleman.** ‘A Method for Obtaining Digital Signatures and Public-Key Cryptosystems’. In: *Commun. ACM* 21(2) (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342.
- [Sho94] **P. Shor.** ‘Algorithms for quantum computation: discrete logarithms and factoring’. In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society, Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.
- [Sim94] **D. Simon.** ‘On the power of quantum computation’. In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society, Nov. 1994, pp. 116–123. DOI: 10.1109/SFCS.1994.365701.
- [SKR09] **P.K. Sarvepalli, A. Klappenecker and M. Rötteler.** ‘Asymmetric quantum codes: constructions, bounds and performance’. In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 465(2105) (2009), pp. 1645–1672. DOI: 10.1098/rspa.2008.0439.
- [Ste96] **A. Steane.** ‘Multiple-Particle Interference and Quantum Error Correction’. In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 452(1954) (1996), pp. 2551–2577. ISSN: 13645021. DOI: 10.1098/rspa.1996.0136.
- [Ste99] **A.M. Steane.** ‘Enlargement of Calderbank-Shor-Steane quantum codes’. In: *IEEE Trans. Inf. Theory* 45(7) (1999), pp. 2492–2495. DOI: 10.1109/18.796388.


Part II

Papers

Paper A

On one-round reliable message transmission

René Bødker Christensen

 0000-0002-9209-3739

Published in:

Information Processing Letters, vol. 147, pp. 22–26.

DOI: 10.1016/j.ipl.2019.02.011

© 2019 Elsevier B.V.

Abstract

In this paper, we consider one-round protocols for reliable message transmission (RMT) when t out of $n = 2t + 1$ available channels are controlled by an adversary. We show impossibility of constructing such a protocol that achieves a transmission rate of less than $\Theta(n)$ for constant-size messages and arbitrary reliability parameter. In addition, we show how to improve two existing protocols for RMT to allow for either larger messages or reduced field sizes.

1 Introduction

The concept of secure message transmission was first introduced in [DDWY93], and the term comprises a model where a sender and a receiver are connected via n channels. Up to t of these channels are controlled by a computationally unbounded active adversary who can read and alter the symbols sent across these t channels. More specifically, we consider the setting where $n = 2t + 1$. In keeping with cryptographic tradition, we will call the sender ‘Alice’, the receiver ‘Bob’, and the adversary ‘Eve’. The challenge is to devise a strategy that allows Alice and Bob to communicate securely and reliably in a limited number of transmission rounds. We focus on one-round protocols.

In the original setting of [DDWY93], the protocols are required to be perfectly secure, meaning that no matter what Eve might attempt, she will gain no information about the message. They are also required to be perfectly reliable such that Bob will always recover the correct message. Later, [FW00] relaxed these conditions to allow some small failure probabilities for both security and reliability. Taking this idea even further, [PCRS10] considers protocols where the security of the message delivery is *not* required, but only reliable transmission is of interest. They call this *unconditionally reliable message transmission*, but we will omit ‘unconditionally’ and write RMT instead.

To assess the efficiency of a message transmission-protocol, it is common to use the *transmission rate* defined as the total number of transmitted bits divided by the bit-length of the message. Hence, a low transmission rate is preferable. As shown in [PCRS10; Theorem 3], we cannot do better than $\Omega(1)$ for RMT, and this bound is tight. In Section 3, however, we show that this transmission rate is not achievable for messages of a constant size.

Related work

RMT has also been studied in [PCRS10; STW12]. The protocol in [STW12] is based on list-decoding of folded Reed-Solomon codes, but although it attains the optimal transmission rate, the computational cost for the receiver to recover the message is exponential in the number of channels. The work [PCRS10] contains bounds and constructions for both the secure and the

reliable-only settings. In addition, they achieve this while tolerating a mixed adversary, giving more fine-grained control of the adversarial assumptions.

Although this paper is only concerned with RMT, we also direct the reader to related works on secure message transmission; that is, protocols that also offer privacy. This additional guarantee comes at a cost. As shown by [DDWY93], perfect security for $n = 2t + 1$ requires at least two rounds, and a single-round protocol can only offer security in the case $n \geq 3t + 1$. In the former setting, Agarwal et al. [ACH06] gave a perfectly secure two-round protocol that achieves optimal performance asymptotically, albeit at a high computational cost. A computationally efficient protocol was subsequently achieved by Kurosawa and Suzuki [KS09] using the concept of pseudobases. This idea was also taken up by [SZ16], who obtained further improvements, reducing the minimally required message size from $\mathcal{O}(n^2 \log n)$ to $\mathcal{O}(n \log n)$.

The setting where privacy is perfect, but reliability is not, was initially handled by [FW00] under the assumption that channels support multicast. The proposed solution, however, was inefficient for certain values of t and n . This was rectified in [WD01], where an efficient protocol for these values was given.

2 Preliminaries

Model assumptions

We assume that Alice and Bob are connected via $n = 2t + 1$ *simple* channels, meaning that the channels allow both Alice and Bob to transmit data, but no additional functionality is assumed. Before the protocol begins, Eve chooses t of these to be under her control. In other words, the adversary in our model is *static* and *active*.

For simple channels, [FW00] showed that $2t \geq n$ leads to a probability of failure of at least $1/4$. Hence, the setting where $n = 2t + 1$ has the maximal number of corruptions that we can hope to overcome. Since a majority of the channels are honest – i.e. not controlled by the adversary – a naive solution to the RMT-problem is to broadcast the message across all n channels. This leads to a transmission rate of n , but gives perfect reliability. Thus, this is the benchmark performance.

Universal hash families

The methods we present rely on the concept of ε -almost universal hash families as introduced by [Sti94].

Definition 2.1:

Let \mathcal{H} be a family of hash functions from \mathcal{M} to A , and let $\varepsilon \in \mathbb{R}_+$. Then \mathcal{H} is called ε -almost universal if for any $m \neq m' \in \mathcal{M}$,

$$\Pr_{h \leftarrow \mathcal{H}} [h(m) = h(m')] \leq \varepsilon.$$

II. Papers

In particular, we use a hash family based on polynomial evaluation similar to the one used in [BPRW16], but generalized to evaluate in several points.

Definition 2.2:

Let \mathbb{F} be a finite field, and $\mathcal{K} \subseteq \mathbb{F}$. For every pair of positive integers $\eta \leq a$, define the map $\text{PEval}^\eta: \mathbb{F}^a \times \mathcal{K}^\eta \rightarrow \mathbb{F}^\eta$ by

$$\text{PEval}^\eta(\mathbf{m}, \mathbf{k}) = (f_{\mathbf{m}}(k_1), f_{\mathbf{m}}(k_2), \dots, f_{\mathbf{m}}(k_\eta)),$$

where $f_{\mathbf{m}}(x) = \sum_{i=1}^a m_i x^i$. We use the notation $\text{PEval}_{\mathbf{k}}^\eta(\mathbf{m}) = \text{PEval}^\eta(\mathbf{m}, \mathbf{k})$.

It may be shown that the family $\mathcal{H}_{\text{PEval}}^\eta = \{\text{PEval}_{\mathbf{k}}^\eta: \mathbb{F}^a \rightarrow \mathbb{F}^\eta\}_{\mathbf{k} \in \mathcal{K}^\eta}$ of hashes is $(a/|\mathcal{K}|)^\eta$ -almost universal.

3 Constant-size messages

One could hope that the overall optimal transmission rate $\Theta(1)$ is achievable for constant-size messages. As we show in Proposition 3.2, however, this is not possible for arbitrary reliability parameters. The proof of the proposition relies on the following result from [FW00; Theorem 5.1].

Theorem 3.1:

Assume that $n \leq 2t$, and denote by \mathcal{M} the message space. Then any reliable message transmission protocol fails with probability at least $\frac{1}{2}(1 - 1/|\mathcal{M}|)$.

Proposition 3.2:

Let $n = 2t + 1$, and consider the RMT-problem for a message of size $\Theta(1)$ bits. Then it is impossible to construct a protocol attaining a transmission rate lower than $\Theta(n)$ for arbitrary reliability parameters.

Proof:

Assume for contradiction that \mathcal{P} is such a protocol. We show the existence of an adversarial strategy such that \mathcal{P} will fail with a probability greater than a constant.

Note that if all n available channels are used, at least n bits will be transmitted during the protocol. Hence, \mathcal{P} can use at most $n - 1$ channels. Let $X \in \{1, 2, \dots, n\}$ be a random variable describing the unused channel. No assumptions are made about the probability distribution of X ; it simply depends on \mathcal{P} . Consider an adversarial strategy where the corrupt channels are chosen uniformly at random. Equivalently, we can assume that the honest channels are given by the set $\{I_1, I_2, \dots, I_{t+1}\}$, where each I_j is chosen uniformly at random in $\{1, 2, \dots, n\}$ under the condition that $I_j \neq I_{j'}$ for $j \neq j'$. It may be shown that in fact $\Pr[I_j = a] = 1/(2t + 1)$ for any $j \in \{1, 2, \dots, t + 1\}$ and $a \in \{1, 2, \dots, n\}$.

Denote by E the event that Alice leaves out one of the honest channels when following \mathcal{P} ; that is, $X = I_j$ for some $j \in \{1, 2, \dots, t+1\}$. Since Alice does not know the outcomes of I_1, I_2, \dots, I_{t+1} , it follows that X is independent from these variables. Using this fact and the fact that the events $X = I_1, X = I_2, \dots, X = I_{t+1}$ are disjoint, we obtain that

$$\begin{aligned} \Pr[E] &= \Pr[X = I_1 \vee \dots \vee X = I_{t+1}] = \sum_{j=1}^{t+1} \Pr[X = I_j] \\ &= \sum_{j=1}^{t+1} \sum_{k=1}^n \Pr[X = k] \Pr[I_j = k] = \sum_{j=1}^{t+1} \frac{1}{2t+1} \sum_{k=1}^n \Pr[X = k] = \frac{t+1}{2t+1}. \end{aligned}$$

If E occurs, it follows from Theorem 3.1 that the probability of protocol failure is at least $\frac{1}{2}(1 - 1/|\mathcal{M}|)$, where \mathcal{M} is the message space. Otherwise, the protocol \mathcal{P} gives a contradiction to Theorem 3.1 since for $n = 2t$, we could introduce a ‘dummy channel’, discard it, and then mimic protocol \mathcal{P} to obtain a lower probability of failure.

By applying the law of total probability, we obtain

$$\begin{aligned} \Pr[\mathcal{P} \text{ fails}] &= \Pr[\mathcal{P} \text{ fails} \mid E] \Pr[E] + \Pr[\mathcal{P} \text{ fails} \mid \bar{E}] \Pr[\bar{E}] \\ &\geq \Pr[\mathcal{P} \text{ fails} \mid E] \Pr[E] \\ &\geq \frac{1}{2} \left(1 - \frac{1}{|\mathcal{M}|}\right) \frac{t+1}{2t+1} > \frac{1}{4} \left(1 - \frac{1}{|\mathcal{M}|}\right). \end{aligned}$$

In conclusion, it is not possible to obtain arbitrarily levels of reliability with a transmission rate of less than $\Theta(n)$ for constant size messages. ■

It is worth pointing out that this result is true for any RMT-protocol; not only one-round ones.

4 A method based on list-decoding

As part of a protocol for robust secret sharing, [BPRW16] introduced the notion of a ‘robust distributed storage’. Their method for achieving this can easily be converted to a one-round protocol for RMT. In brief, the idea is to encode the message using a list-decodable code – e.g. a Reed-Solomon code – and transmit each position of the resulting codeword across the corresponding channel. In addition, each channel will deliver a key/tag-pair from an ε -almost universal hash family. The receiver can then use these tags to recover the intended message from the list of potential messages returned by the list-decoding algorithm.

However, since the original authors only need the asymptotical performance, they base their method on the list-decoding algorithm of Sudan [Sud97], and use messages of size at most $\lfloor n/8 \rfloor + 1$. This may be increased to $\lfloor n/5 \rfloor + 1$ with no penalty in reliability by applying the Guruswami-Sudan algorithm

[GS98] instead. This protocol has optimal transmission rate when the message has size $\Theta(n)$.

5 A method based on erasure decoding

In the following, we will describe the one-round RMT-protocol given in [PCRS10] in the language of Reed-Solomon codes and hash families. In this representation, the original authors are essentially relying only on the erasure correcting capabilities of the codes. We show that a careful choice of parameters allows correction of errors as well, causing the required field size to be quadratic rather than cubic in n .

The message we consider is an $a \times b$ -matrix M over a finite field \mathbb{F} . Each row of this message is encoded by means of an $[n, b]$ Reed-Solomon code, yielding an $a \times n$ -matrix S where each row is a codeword. Across the i 'th channel, Alice sends the i 'th column s_i of S . Since Bob needs to determine if Eve modified some of these columns during transmission, Alice also computes n verification tags $\{v_{i1}, v_{i2}, \dots, v_{in}\}$ for each s_i by applying uniformly sampled hash functions from some family \mathcal{H} . Denote the keys of these functions by $\{k_{i1}, k_{i2}, \dots, k_{in}\}$. Across the i 'th channel, Alice then sends $\{s_i\} \cup \{k_{ji}, v_{ji}\}_{j=1}^n$. That is, each channel will transmit the codeword entries s_i , and a key/tag-pair (k_{ji}, v_{ji}) for every channel j .

When Bob receives the possibly modified values $\{s'_i\} \cup \{k'_{ji}, v'_{ji}\}_{j=1}^n$, he will check the integrity of s'_i by computing the hash value $h_{k'_{ji}}(s'_i)$ and comparing the result with the received tag v'_{ji} . He will do so for each received key/tag-pair, and if more than t tags disagree with the computed values, Bob will mark s'_i as modified and treat it as an erasure when recovering the message.

With large probability, these checks performed by Bob reveal a considerable part of the corrupt channels delivering erroneous information. This causes a number of columns in S' to be marked as erasures. However, some small number e of corrupted channels may have passed the checks, meaning that the remaining entries in S' may still contain errors. In fact, each row of S' may contain up to $t - e$ erasures and e errors. If the parameter b agreed upon by Alice and Bob is sufficiently small, Bob may nevertheless correct these erasures and errors in S' . Since the rows of S' are codewords of an $[n, b]$ Reed-Solomon code which has minimal distance $n - b + 1$, Bob can recover the correct message if

$$2e + t - e < n - b + 1 \implies b \leq n - (t + e) = t + 1 - e.$$

Thus, after verifying the received values, Bob can determine if the message can be recovered by simply counting the number of non-erased columns and computing syndromes. The complete description of our protocol is given in Protocol 1 on page 37. The correctness of the protocol follows from essentially the same arguments as used by [PCRS10], albeit with the following modification.

Lemma 5.1:

If at least $t - e$ columns of S' are marked as erasures in step 4. of the protocol, Bob will recover the correct message.

Proof:

Let $u \geq t - e$ be the number of erased columns, meaning that each row of S' contains at most $t - u$ errors. The minimal distance of the code is $d = n - b + 1$, which means that u erasures and $t - u$ errors can be corrected if $2(t - u) + u < d$. This is true because

$$2(t - u) + u = 2t - u \leq t + e \leq n - b,$$

where the last inequality follows from the requirement $e \leq t + 1 - b$ given in the protocol specification. ■

Protocol reliability

Under the assumption that the hash family \mathcal{H} applied in the protocol is ε -almost universal, we can bound the probability that Bob cannot recover the correct message.

Proposition 5.2:

If \mathcal{H} is an ε -almost universal family of hash functions, then

$$\Pr[\text{The protocol fails}] \leq \frac{t(t + 1)\varepsilon}{e + 1}.$$

Proof:

By Lemma 5.1, at least $e + 1$ of the channels modified by Eve must pass the integrity check performed by Bob. To achieve this, it is necessary that the hash value of the modified s'_i matches at least one verification tag v_{ij} sent across an honest channel.

The ε -almost universality of \mathcal{H} implies that $\Pr_{h \leftarrow \mathcal{H}}[h(s_i) = h(s'_i)] \leq \varepsilon$ whenever $s_i \neq s'_i$. Hence, ε is an upper bound on the probability that a single corrupt channel agrees with a single honest channel. Since there are $t + 1$ honest channels, the probability for a modified channel to be consistent with at least one honest can be bounded above by $(t + 1)\varepsilon$.

Let X be the random variable counting the number of modified but uncaught channels. Since the hash keys $k_{ij}, k_{i'j'}$ are independent whenever $(i, j) \neq (i', j')$, the integrity checks of the modified channels can be considered as t independent Bernoulli trials, each with a success probability of at most $(t + 1)\varepsilon$. Thus, X follows a binomial distribution, and has expected value $\mathbb{E}[X] \leq t(t + 1)\varepsilon$. The Markov inequality now gives

$$\Pr[X \geq e + 1] \leq \frac{\mathbb{E}[X]}{e + 1} \leq \frac{t(t + 1)\varepsilon}{e + 1},$$

and the result follows. ■

II. Papers

Protocol 1: One-round RMT

This protocol allows Alice to reliably send ab symbols of a finite field \mathbb{F} to Bob in one round by using $n = 2t + 1$ channels, t of which may be controlled by an adversary. Beforehand, Alice and Bob have agreed upon a parameter $e \in \mathbb{N}$, which satisfies $e \leq t + 1 - b$. Additionally, they agree on an ε -almost universal hash family $\mathcal{H} = \{h_k: \mathbb{F}^a \rightarrow \mathbb{F}^\eta \mid \mathbb{F}^\eta\}$.

1. The message is represented as a matrix $M \in \mathbb{F}^{a \times b}$ and each row is encoded using an $[n, b]$ Reed-Solomon code over \mathbb{F} .
 2. For each column s_i of the resulting codewords, Alice samples uniformly and independently n keys $\{k_{i1}, k_{i2}, \dots, k_{in}\}$ and computes $v_{ij} = h_{k_{ij}}(s_i)$ for each $j \in \{1, 2, \dots, n\}$.
 3. Across the i 'th channel, Alice transmits $\{s_i\} \cup \{k_{ji}, v_{ji}\}_{j=1,2,\dots,n}$.
 4. Bob receives the possibly modified values $\{s'_i\} \cup \{k'_{ji}, v'_{ji}\}_{j=1,2,\dots,n}$ for $i = 1, 2, \dots, n$. For each i , he compares the tag v'_{ij} received from the j 'th channel to the hash value $h_{k'_{ij}}(s'_i)$. If these disagree for more than t channels, he will mark s_i as modified.
 5. For each row in S' , Bob computes the syndrome to check if it contains errors. Depending on the result, he proceeds with one of the three following steps.
 - (a) **The syndrome is zero:** S' contains no errors, meaning that Bob can simply use polynomial interpolation to recover the message.
 - (b) **The syndrome is nonzero, and S' contains at least $t - e$ erased columns:** Bob uses a decoding algorithm for Reed-Solomon codes to correct the erasures and errors, hereby recovering the message.
 - (c) **The syndrome is nonzero, and S' contains less than $t - e$ erased columns:** Too many modified channels have passed the integrity checks. The protocol has failed.
-

Number of bits transmitted

When the proposed protocol is used to transmit a message, the total number of \mathbb{F} -symbols transmitted is $n(a + n|\mathcal{V}| + n|\mathcal{K}|)$, where $|\mathcal{V}|$ and $|\mathcal{K}|$ denote the number of field symbols necessary to represent v_{ij} and k_{ij} , respectively.

Using polynomial evaluation

For concreteness, we analyse the reliability when $\mathcal{H}_{\text{PEval}}^\eta$ is applied with $\mathcal{K} = \mathbb{F}$. Here, both the keys and the verification tags consist of η field elements. Hence, the total number of transmitted bits is $2\eta n^2 + an$. Depending on the message size, this can give various transmission rates, but under the assumption that η is some constant value, the optimal transmission rate of $\Theta(1)$ is obtained when both a and b are $\Theta(n)$. That is, when the message is of size $\Theta(n^2)$.

Since the hash family is $\frac{a^\eta}{|\mathbb{F}|^\eta}$ -almost universal, it follows from Proposition

5.2 that we must require

$$\frac{t(t+1)a^\eta}{(e+1)|\mathbb{F}|^\eta} \leq \delta \implies |\mathbb{F}| \geq a \left(\frac{t(t+1)}{(e+1)\delta} \right)^{\frac{1}{\eta}}.$$

in order to obtain reliability δ . In particular, we note that for $\eta = 1$, the original protocol by [PCRS10] requires $|\mathbb{F}| \geq n^3/\delta$. In the proposed protocol, we can set both b and e to be $\Theta(n)$ and obtain the requirement $|\mathbb{F}| \geq \Theta(n^2/\delta)$. In other words, by reducing the second dimension of the message, the required field size is reduced by a factor of n asymptotically. Furthermore, introducing the parameter η highlights the trade-off between the number of \mathbb{F} -symbols transmitted and the required field size.

6 Comparison with existing protocols

In order to compare the RMT-protocols proposed in Sections 4 and 5 to those already in the literature, we will restrict ourselves to the hash family $\mathcal{H}_{\text{PEval}}^\eta$ from Definition 2.2 with $\mathcal{K} = \mathbb{F}$ and $\eta = 1$.

For five protocols, Table 1 gives an overview of the required field size given δ ; the message size in \mathbb{F} -symbols; whether the protocol attains the optimal transmission rate; and whether it is computationally efficient. Here, *efficient* means polynomial in the number of available channels. We use the Θ -notation to keep the presentation as clear and self-contained as possible.

For the protocol of Section 5, we remark that $a = \Theta(n)$ was chosen even though it is in principle possible to use any value smaller than $|\mathbb{F}|$. Choosing greater values, however, also increases the required field size. We shall refrain from doing such analysis here since Table 1 already shows the desired improvement.

As the table indicates, the first two protocols are better suited for small message sizes. Although both have the same asymptotic performance,

Protocol	Field size	Message size	Optimal	Computational efficiency
[BPRW16; Sec. 4.1]	$\Theta(n^2/\delta)$	$\lfloor n/8 \rfloor + 1$	✓	✓
This work, Sec. 4	$\Theta(n^2/\delta)$	$\lfloor n/5 \rfloor + 1$	✓	✓
[PCRS10; Sec. 4]	n^3/δ	$\Theta(n^2)$	✓	✓
[STW12; Sec. 3.1]	$\Theta(n^4)$	$\Theta(n^2)$	✓	✗
This work, Sec. 5	$\Theta(n^2/\delta)$	$\Theta(n^2)$	✓	✓

Table 1. Comparison of one-round RMT-protocols. The second column shows the minimal field size given a desired reliability parameter δ . The third column gives the message size (in terms of \mathbb{F} -elements) that leads to an optimal transmission rate, and the fourth indicates whether such an optimal transmission rate is achievable. The final column states whether the computational cost is at most polynomial in the number of channels.

II. Papers

the modification suggested in Section 4 allows a larger message size. The remaining three protocols all have $\Theta(n^2)$ as the optimal message size, which suggests that they should fare better when transmitting larger messages. It may be noted that the protocol proposed in Section 5 achieves this while reducing the required field size by a factor of n asymptotically.

Even though Table 1 gives an overview of the general properties of each protocol, it does not reveal how they will perform in concrete problem instances. If the message size and the number of channels have already been fixed, a separate analysis is needed to determine the protocol that will perform the best.

7 Acknowledgements

The author extends his gratitude towards Ignacio Cascudo and Diego Ruano for helpful guidance and fruitful discussions.

8 References


- [ACH06] **S. Agarwal, R. Cramer and R. de Haan.** ‘Asymptotically Optimal Two-Round Perfectly Secure Message Transmission’. In: *CRYPTO 2006*. Springer, Heidelberg, 2006, pp. 394–408. ISBN: 978-3-540-37433-6. DOI: 10.1007/11818175_24.
- [BPRW16] **A. Bishop, V. Pastro, R. Rajaraman and D. Wichs.** ‘Essentially Optimal Robust Secret Sharing with Maximal Corruptions’. In: *EUROCRYPT 2016*. 2016, pp. 58–86. DOI: 10.1007/978-3-662-49890-3_3.
- [DDWY93] **D. Dolev, C. Dwork, O. Waarts and M. Yung.** ‘Perfectly Secure Message Transmission’. In: *J. ACM* 40(1) (Jan. 1993), pp. 17–47. ISSN: 0004-5411. DOI: 10.1145/138027.138036.
- [FW00] **M. Franklin and R.N. Wright.** ‘Secure Communication in Minimal Connectivity Models’. In: *J. Cryptol.* 13(1) (Jan. 2000), pp. 9–30. ISSN: 1432-1378. DOI: 10.1007/s001459910002.
- [GS98] **V. Guruswami and M. Sudan.** ‘Improved decoding of Reed-Solomon and algebraic-geometric codes’. In: *FOCS 1998*. Nov. 1998, pp. 28–37. DOI: 10.1109/SFCS.1998.743426.
- [KS09] **K. Kurosawa and K. Suzuki.** ‘Truly efficient 2-round perfectly secure message transmission scheme’. In: *IEEE Trans. Inf. Theory* 55(11) (2009), pp. 5223–5232. DOI: 10.1109/TIT.2009.2030434.
- [PCRS10] **A. Patra, A. Choudhury, C.P. Rangan and K. Srinathan.** ‘Unconditionally reliable and secure message transmission in undirected synchronous networks: Possibility, feasibility and optimality’. In: *Int. J. Appl. Cryptogr.* 2(2) (2010), pp. 159–197. DOI: 10.1504/IJACT.2010.038309.

- [Sti94] **D. Stinson.** 'Universal hashing and authentication codes'. In: *Des. Codes Cryptogr.* 4(3) (1994), pp. 369–380. ISSN: 1573-7586. DOI: 10.1007/BF01388651.
- [STW12] **R. Safavi-Naini, M. A. A. Tuhin and P. Wang.** 'A General Construction for 1-Round δ -RMT and $(0, \delta)$ -SMT'. In: *ACNS 2012*. Springer, Heidelberg, 2012, pp. 344–362. ISBN: 978-3-642-31284-7. DOI: 10.1007/978-3-642-31284-7_21.
- [Sud97] **M. Sudan.** 'Decoding of Reed Solomon Codes beyond the Error-Correction Bound'. In: *J. Complexity* 13(1) (1997), pp. 180–193. ISSN: 0885-064X. DOI: 10.1006/jcom.1997.0439.
- [SZ16] **G. Spini and G. Zémor.** 'Perfectly Secure Message Transmission in Two Rounds'. In: *TCC 2016-B*. 2016, pp. 286–304. DOI: 10.1007/978-3-662-53641-4_12.
- [WD01] **Y. Wang and Y. Desmedt.** 'Secure Communication in Multicast Channels: The Answer to Franklin and Wright's Question'. In: *J. Cryptol.* 14(2) (Mar. 2001), pp. 121–135. ISSN: 1432-1378. DOI: 10.1007/s00145-001-0002-y.


Paper B

Actively Secure OT-Extension from q -ary Linear Codes


Ignacio Cascudo

 0000-0001-5520-5386

René Bødker Christensen

 0000-0002-9209-3739

Jaron Skovsted Gundersen

 0000-0003-0882-4621

Published in:

International Conference on Security and Cryptography for Networks;

Lecture Notes in Computer Science, vol. 11035, pp. 333–348.

DOI: 10.1007/978-3-319-98113-0_18

© 2018 Springer Nature Switzerland AG

Abstract

We consider recent constructions of 1-out-of- N OT-extension from Kolesnikov and Kumaresan (CRYPTO 2013) and from Orrù et al. (CT-RSA 2017), based on binary error-correcting codes. We generalize their constructions such that q -ary codes can be used for any prime power q . This allows to reduce the number of base 1-out-of-2 OT's that are needed to instantiate the construction for any value of N , at the cost of increasing the complexity of the remaining part of the protocol. We analyze these trade-offs in some concrete cases.

1 Introduction

A K -out-of- N oblivious transfer, or $\binom{N}{K}$ -OT, is a cryptographic primitive that allows a sender to input N messages and a receiver to learn exactly K of these with neither the receiver revealing which messages he has chosen to learn nor the sender revealing the other $N - K$ input messages. This is a fundamental cryptographic primitive in the area of secure multiparty computation, and in fact [Kil88] showed that any protocol for secure multiparty computation can be implemented if the OT functionality is available. However, the results in [IR89] indicate that OT is very likely to require a public key cryptosystem, and therefore implementing OT is relatively expensive. Unfortunately, well-known protocols such as Yao's garbled circuits [Yao82] and the GMW-compiler [GMW87] rely on using a large number of independent instances of OT. It is therefore of interest to reduce the number of OT's used in a protocol in an attempt to reduce the overall cost. This can be done using what is called OT-extensions, where a large number of OT's are simulated by a much smaller number of base OT's together with the use of cheaper symmetric crypto primitives, such as pseudorandom generators.

Beaver showed in [Bea96] that OT-extension is indeed possible, but it was not before 2003 that an efficient $\binom{2}{1}$ -OT-extension protocol was presented by Ishai et al. in [IKNP03]. In addition, while this protocol had security against passive adversaries, subsequent work showed that active security can be achieved at a small additional cost [KOS15].

In [KK13], Kolesnikov and Kumaresan noticed that Ishai et al. were in essence relying on the fact that the receiver encodes its input as a codeword in a repetition code, and therefore one can generalize their idea by using other codes, such as the Walsh-Hadamard code, which not only obtains efficiency improvements for $\binom{2}{1}$ -OT-extension, but also allows to generalize the protocol into passively secure $\binom{N}{1}$ -OT-extension. In such an extension protocol the base OT's are $\binom{2}{1}$ -OT's, but the output consist of a number of $\binom{N}{1}$ -OT's. In more recent work, Orrù et al. [OOS17] transformed the protocol by [KK13] into an actively secure $\binom{N}{1}$ -OT-extension protocol by adding a "consistency check" which is basically a zero-knowledge proof that the receiver is indeed using codewords of the designated code to encode his selections. As shown in [OOS17], 1-out-of- N oblivious transfer has a direct

application to the problem of private set inclusion and, via this connection, to the problem of private set intersection. In fact this application requires only a randomized version of $\binom{N}{1}$ -OT, where the sender does not have input messages, but these are generated by the functionality and can be accessed on demand by the sender. The structure of the aforementioned OT extension protocols is especially well suited for this application, since such a randomized functionality is essentially implemented by the same protocol without the last step, where the sender would send its masked inputs to the receiver.

The aforementioned papers on $\binom{N}{1}$ -OT-extension relied on the use of binary linear codes, and the concrete parameters of the resulting construction, the number of OT's and the value of N , are given respectively by the length and size of the binary linear code being used. Furthermore, the construction requires that the minimum distance of the code is at least the desired security parameter. Well-known bounds on linear codes, such as the Plotkin, Griesmer or Hamming bounds [MS83], provide lower bounds for the length of a code with certain size and minimum distance, and therefore these imply lower bounds on the number of base OT's for the OT-extension protocol. In fact, even if we omit the requirement on the minimum distance, we can see that at least $\log_2 N$ base OT's are needed for those extension protocols.

In this paper, we discuss the use of q -ary linear codes, where q can be any power of a prime, as a way of reducing the number of required base OT's in the 1-out-of- N OT-extension constructions mentioned above. We show that one can easily modify the protocol in [OOS17] to work with q -ary codes, rather than just binary. Given that all parameters of the code still have the same significance for the construction and, in particular, N is still the size (the number of codewords) of the code, we obtain a reduction in the number of base OT's required: indeed, for given fixed values N and d , the minimal length among all q -ary linear codes of size N and minimum distance d becomes smaller as q increases. In particular one can show cases where the lower bound of $\log_2 N$ base OT's can be improved even if we have relatively large minimum distance.

This improvement, however, comes at a cost: since we need to communicate elements of a larger field, the communication complexity of the OT-extension protocol (not counting the complexity of the base OT's) increases. This increase is compensated to some extent by the fact that this communication complexity also depends on the number of base OT's.

The concrete tradeoffs obtained by the use of q -ary codes depend of course on N and the security level. We show several examples comparing explicit results listed in [OOS17] and the q -ary alternative achieving the same (or similar) N and security level. For example, for the largest value of N considered in [OOS17] we show that by using a linear code over the finite field of 8 elements, we need less than half of the base OT's, while the communication complexity increases only by 33%.

When q is a power of two, we can show an improvement on the complexity

II. Papers

of the consistency check that we use in the case of a general q . Namely, the consistency check in [OOS17] works by asking the receiver, who has previously used the base OT's to commit to both the codewords encoding his selections and some additional random codewords, to open sums of random subsets of these codewords. The natural way of generalizing this to a general prime power q is to ask the receiver to open random linear combinations over \mathbb{F}_q of the codewords. However, in case q is a power of two, we show that it is enough to open random linear combinations over \mathbb{F}_2 , i.e., sums, just as in [OOS17] (naturally, this extends to the case where q is a power of p , where it would be enough to open combinations over \mathbb{F}_p). The advantage of this generalization is of course that the verifier needs to send less information to describe the linear combinations that it requests to open, and in addition less computation is required from the committer to open these combinations.

We give a presentation of the protocol and its security proof that is inspired by a recent work on homomorphic universally composable secure commitments [Cas+16]. As noted in [OOS17], there is a strong similarity between the OT-extension protocol constructions in the aforementioned works and several protocol constructions in a line of work on homomorphic UC commitments [Cas+15; Cas+16; FJNT16]. In the first part of the OT-extension protocol in [KK13], the base OT's are used for the receiver to eventually create an additive 1-out-of-2 sharing of each coordinate in the codewords encoding his selection, so that the sender learns exactly one share of each. This is essentially the same as the committing phase of the passively secure homomorphic UC commitment proposed in [Cas+15] (one can say that the receiver from the OT-extension protocol has actually committed to his inputs at that point). In order to achieve active security, a consistency check was added in [FJNT16], which is basically the same as the one introduced in [OOS17] in the context of OT-extension. Finally, [Cas+16] generalized this consistency check by proving that rather than requesting the opening of uniformly random linear combinations of codewords, these combinations can be determined by a hash function randomly selected from an almost universal family of hash functions. This leads to asymptotical complexity gains, both in terms of communication and computation (since one can use linear time encodable almost universal hash functions which can in addition be described by short seeds), but in our case it also allows us to give a unified proof of security in both the case where the linear combinations for the consistency check are taken over \mathbb{F}_q and when they are taken over the subfield.

The work is structured as follows. After the preliminaries in Section 2, we present our OT-extension protocol and prove its security in Section 3. In Section 4, we show that the communication cost can be reduced by performing the consistency checks over a subfield, and finally Section 5 contains a comparison with previous protocols.

2 Preliminaries

This section contains the basic definitions needed to present and analyse the protocol for OT-extension.

Notation

Throughout this paper, q will denote a prime power and \mathbb{F}_q a finite field of q elements. Every finite field has elements 0 and 1, and hence it will be natural to embed the set $\{0, 1\}$ in \mathbb{F}_q .¹ Bitstrings in $\{0, 1\}^n$ and vectors from \mathbb{F}_q^n are denoted in boldface. The i -th coordinate of a vector or bitstring \mathbf{b} is denoted b_i .

For a bitstring $\mathbf{b} \in \{0, 1\}^n$, we will use the notation $\Delta_{\mathbf{b}}$ to denote the diagonal matrix in $\mathbb{F}_q^{n \times n}$ with entries from the vector \mathbf{b} , i.e. the (i, i) -entry of $\Delta_{\mathbf{b}}$ is b_i . Note that for vectors $\mathbf{b}, \mathbf{c} \in \mathbb{F}_q^n$, the product $\mathbf{c}\Delta_{\mathbf{b}}$ equals the componentwise product of \mathbf{b} and \mathbf{c} .

Linear Codes

Since our protocol depends heavily on linear codes, we recall here the basics of this concept. First, a (not necessarily linear) code of length n over an alphabet Q is a subset $\mathcal{C} \subseteq Q^n$. An \mathbb{F}_q -linear code \mathcal{C} is an \mathbb{F}_q -linear subspace of \mathbb{F}_q^n . The dimension k of this subspace is called the dimension of the code, and therefore \mathcal{C} is isomorphic to \mathbb{F}_q^k . A linear map $\mathbb{F}_q^k \rightarrow \mathcal{C}$ can be described by a matrix $G \in \mathbb{F}_q^{k \times n}$, which is called a generator matrix for \mathcal{C} . Note that G acts on the right, so $\mathbf{w} \in \mathbb{F}_q^k$ is mapped to $\mathbf{w}G \in \mathcal{C}$ by the aforementioned linear map.

For $\mathbf{x} \in \mathbb{F}_q^n$ we define the support of \mathbf{x} to be the set indices where \mathbf{x} is nonzero, and we denote this set by $\text{supp}(\mathbf{x})$. Using this definition we can turn \mathbb{F}_q^n into a metric space. This is done by introducing the Hamming weight and distance. The Hamming weight of \mathbf{x} is defined as $w_H(\mathbf{x}) = |\text{supp}(\mathbf{x})|$, and this induces the Hamming distance $d_H(\mathbf{x}, \mathbf{y}) = w_H(\mathbf{x} - \mathbf{y})$, where $\mathbf{y} \in \mathbb{F}_q^n$ as well. The minimum distance d of a linear code \mathcal{C} is defined to be

$$d = \min\{d_H(\mathbf{c}, \mathbf{c}') \mid \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\},$$

and by the linearity of the code it can be shown that in fact

$$d = \min\{w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}\}.$$

Since n , k , and d are fixed for a given linear code \mathcal{C} over \mathbb{F}_q , we often refer to it as an $[n, k, d]_q$ -code.

¹Of course, the elements of $\{0, 1\}$ could be identified with the elements of the field of two elements, \mathbb{F}_2 . But for the sake of clarity, we will prefer to use $\{0, 1\}$ where we refer to bits and bitstrings and no algebraic properties are needed.

II. Papers

It may be shown that if $\mathbf{x} \in \mathbb{F}_q^n$ is given by $\mathbf{c} + \mathbf{e}$ for some codeword $\mathbf{c} \in \mathcal{C}$ and an error vector \mathbf{e} with $w_H(\mathbf{e}) < d$, it is possible to recover \mathbf{c} from \mathbf{x} and $\text{supp}(\mathbf{e})$. This process is called erasure decoding.

Another way to see erasure decoding is by considering punctured codes. For a set of indices $E \subseteq \{1, 2, \dots, n\}$ we denote the projection of $\mathbf{x} \in \mathbb{F}_q^n$ onto the indices not in E by $\pi_E(\mathbf{x})$. For a code \mathcal{C} and a set of indices E , we call $\pi_E(\mathcal{C})$ a punctured code. Now consider the case where $|E| < d$, which implies the existence of a bijection between \mathcal{C} and $\pi_E(\mathcal{C})$. This is the fact exploited in erasure decoding, where E is the set of indices where the errors occur.

As in [Cas+16], we will use interleaved codes. If $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a linear code, \mathcal{C}^{os} denotes the set of $s \times n$ -matrices with entries in \mathbb{F}_q whose rows are codewords of \mathcal{C} . We can also see such an $s \times n$ -matrix as a vector of length n with entries in the alphabet \mathbb{F}_q^s . Then we can see \mathcal{C}^{os} as a non-linear² code of length n over the alphabet \mathbb{F}_q^s .

Since the alphabet \mathbb{F}_q^s contains a zero element (the all zero vector), we can define the notions of Hamming weight and Hamming distance in the space $(\mathbb{F}_q^s)^n$. We can then speak about the minimum distance of \mathcal{C}^{os} and even though \mathcal{C}^{os} is not a linear code, it is easy to see that the minimum distance of \mathcal{C}^{os} coincides with its minimum nonzero weight, and also with the minimum distance of \mathcal{C} .

Cryptographic Definitions

Consider a sender S and a receiver R participating in a cryptographic protocol. The sender holds $\mathbf{v}_{j,i} \in \{0, 1\}^\kappa$ for $j = 1, 2, \dots, N$ and $i = 1, 2, \dots, m$. For each i the receiver holds a choice integer $w_i \in [1, N]$. We let $\mathcal{F}_{N\text{-OT}}^{\kappa,m}$ denote the ideal functionality that, on inputs $\mathbf{v}_{j,i}$ from S and w_i from R , outputs $\mathbf{v}_{w_i,i}$ for $i = 1, 2, \dots, m$ to the receiver R . For ease of notation, we will let the sender input N matrices of size $\kappa \times m$ with entries in $\{0, 1\}$, and the receiver a vector of length m , with entries in $[1, N]$. Hence, for the i 'th OT the sender's inputs are the i 'th column of each matrix, and the receiver's input is the i 'th entry of the vector.

The protocol presented in Section 3 relies on two functions with certain security assumptions, the foundations of which we define in the following. For the first function let \mathcal{X} be a probability distribution. The min-entropy of \mathcal{X} is given by

$$H_\infty(\mathcal{X}) = -\log(\max_x \Pr[X = x]),$$

where X is any random variable following the distribution \mathcal{X} . If $H_\infty(\mathcal{X}) = t$ we say that \mathcal{X} is t -min-entropy. This is used in the following definition.

²The code is linear over \mathbb{F}_q , but not the alphabet \mathbb{F}_q^s .

Definition 2.1 (t -min-entropy strongly \mathcal{C} -correlation robustness):

Consider a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$, and let \mathcal{X} be a distribution on $\{0, 1\}^n$ with min-entropy t . Fix $\{\mathbf{t}_i \in \mathbb{F}_q^n \mid i = 1, 2, \dots, m\}$ from some probability distribution and let κ be a positive integer. An efficiently computable function $H: \mathbb{F}_q^n \rightarrow \{0, 1\}^\kappa$ is said to be t -min-entropy strongly \mathcal{C} -correlation robust if

$$\{H(\mathbf{t}_i + \mathbf{c}\Delta_{\mathbf{b}}) \mid i = 1, 2, \dots, m, \mathbf{c} \in \mathcal{C}\}$$

is computationally indistinguishable from the uniform distribution on $\{0, 1\}^{\kappa m |\mathcal{C}|}$ when \mathbf{b} is sampled according to the distribution \mathcal{X} .

The second type of function we need is a pseudorandom generator.

Definition 2.2:

A pseudorandom generator is a function $\text{PRG}: \{0, 1\}^\kappa \rightarrow \mathbb{F}_q^m$ such that the output of PRG is computationally indistinguishable from the uniform distribution on \mathbb{F}_q^m .

If $A = [\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n]$ is a $\kappa \times n$ -matrix with entries in $\{0, 1\}$ for some integer n , we use the notation $\text{PRG}(A) = [\text{PRG}(\mathbf{a}_1), \text{PRG}(\mathbf{a}_2), \dots, \text{PRG}(\mathbf{a}_n)]$ where we see $\text{PRG}(\mathbf{a}_i)$ as columns of an $m \times n$ matrix.

In addition to the usual concept of advantage, one can also consider the conditional advantage as it is done in [OOS17]. Let A be an event such that there exist x_0 and x_1 in the sample space of the two random variables X_0 and X_1 , respectively, where $\Pr[X_i = x_i \mid A] > 0$ for $i = 0, 1$. Then we define the conditional advantage of a distinguisher \mathcal{D} given A as

$$\text{Adv}(\mathcal{D} \mid A) = \left| \Pr[\mathcal{D}(X_0) = 0 \mid A] - \Pr[\mathcal{D}(X_1) = 0 \mid A] \right|.$$

We end this section by presenting the following lemma, which allows us to bound the advantage by considering disjoint cases. The proof follows by the law of total probability and the triangle inequality.

Lemma 2.3:

Let A_1, A_2, \dots, A_n be events as above. Additionally, assume that the events are disjoint. If $\sum_{i=1}^n \Pr[A_i] = 1$, then

$$\text{Adv}(\mathcal{D}) \leq \sum_{i=1}^n \text{Adv}(\mathcal{D} \mid A_i) \Pr[A_i]$$

for any distinguisher \mathcal{D} .

3 Actively Secure OT-Extension

In this section we describe and analyse a generalization of the protocol described in [OOS17] which uses OT-extensions to implement the functionality

II. Papers

$\mathcal{F}_{N\text{-OT}}^{\kappa,m}$ by using only $n \leq m$ base OT's, which are 1-out-of-2. Our OT-extension protocol is also using 1-out-of-2 base OT's, but works with q -ary linear codes instead of binary. Our main result is summarized in the following theorem.

Theorem 3.1:

Given security parameters κ and s , let \mathcal{C} be an $[n, k, d]_q$ linear code with $k = \log_q(N)$ and $d \geq \max\{\kappa, s\}$. Additionally, let $\text{PRG}: \{0, 1\}^\kappa \rightarrow \mathbb{F}_q^{m+2s}$ be a pseudorandom generator and let $\text{H}: \mathbb{F}_q^n \rightarrow \{0, 1\}^\kappa$ be a t -min-entropy strongly \mathcal{C} -correlation robust function for all $t \in \{n-d+1, n-d+2, \dots, n\}$. If we have access to \mathcal{C} , the functions PRG and H , and the functionality $\mathcal{F}_{2\text{-OT}}^{\kappa,n}$, then the protocol in Protocol 1 on page 50 implements the functionality $\mathcal{F}_{N\text{-OT}}^{\kappa,m}$.

The protocol is computationally secure against an actively corrupt adversary.

The Protocol

We start by noticing that in our protocol R has inputs $\mathbf{w}_i \in \mathbb{F}_q^k$ rather than choice integers $w_i \in [1, N]$. However, the number of elements in \mathbb{F}_q^k is $q^k = N$, and hence \mathbf{w}_i can for instance be the q -ary representation of w_i . In this way we have a bijection between selection integers and input vectors.

Our protocol is, like the protocol in [OOS17], very similar to the original protocol in [IKNP03]. The idea in this protocol is that we first do OT's with the roles of the participants interchanged such that the sender learns some randomness chosen by the receiver. Afterwards, R encodes his choice vectors using the linear code \mathcal{C} and hides the value with a one-time pad. He sends these to S , who will combine this information with the outputs of the OT functionality to obtain a set of vectors, only m of which R can compute; namely the ones corresponding to his input vectors. When S applies a t -min-entropy strongly \mathcal{C} -correlation robust function H to the set of vectors, he can use the outputs as one-time pads of his input strings. Like in [OOS17] the protocol contains a consistency check to ensure that R acts honestly, or otherwise he will get caught with overwhelming probability. The full protocol is presented in Protocol 1 on page 50.

In order to argue that the protocol is correct, we see that for each i , the sender S computes and sends the values $\mathbf{y}_{\mathbf{w},i}$ for all $\mathbf{w} \in \mathbb{F}_q^k$. Since $k = \log_q(N)$, this yields N strings for each $i \in \{1, 2, \dots, m\}$. The receiver R obtains one of these because

$$\text{H}(\mathbf{q}_i - \mathbf{w}_i G \Delta_{\mathbf{b}}) = \text{H}(\mathbf{q}_i - \mathbf{c}_i \Delta_{\mathbf{b}}) = \text{H}(\mathbf{t}_i).$$

Furthermore, if both S and R act honestly, the consistency checks in phase III will always pass. This follows from the observation that

$$\tilde{T} + \tilde{W} G \Delta_{\mathbf{b}} = M(T_0 + C \Delta_{\mathbf{b}}) = MQ.$$

Hence, we note that if only passive security is needed in Protocol 1, we can omit phase III and set $s = 0$. The aforementioned steps are included to

Protocol 1: OT-Extension

This protocol implements the functionality $\mathcal{F}_{N\text{-OT}}^{k,m}$ having access to $\mathcal{F}_{2\text{-OT}}^{k,n}$. The security of the protocol is controlled by the security parameters κ and s . The sender S and the receiver R have agreed on a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with generator matrix G of dimension $k = \log_q(N)$ and minimum distance $d \geq \max\{\kappa, s\}$. The protocol uses a pseudorandom generator $\text{PRG}: \{0, 1\}^\kappa \rightarrow \mathbb{F}_q^{m+2s}$ and a function $H: \mathbb{F}_q^n \rightarrow \{0, 1\}^\kappa$, which is t -min-entropy strongly \mathcal{C} -correlation robust for all $t \in \{n - d + 1, n - d + 2, \dots, n\}$. R has m inputs $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_m \in \mathbb{F}_q^k$, which act as selection integers. S has inputs $\mathbf{v}_{w,i} \in \{0, 1\}^\kappa$, indexed by $i \in \{1, 2, \dots, m\}$ and $\mathbf{w} \in \mathbb{F}_q^k$.

I. Initialization phase

- (a) S chooses uniformly at random $\mathbf{b} \in \{0, 1\}^n$.
- (b) R generates uniformly at random two seed matrices $N_0, N_1 \in \{0, 1\}^{\kappa \times n}$ and defines the matrices $T_i = \text{PRG}(N_i) \in \mathbb{F}_q^{(m+2s) \times n}$ for $i = 0, 1$.
- (c) The participants call the functionality $\mathcal{F}_{2\text{-OT}}^{k,n}$, where S acts as the receiver with input \mathbf{b} , and R acts as the sender with inputs (N_0, N_1) . S receives $N = N_0 + (N_1 - N_0)\Delta_{\mathbf{b}}$, and by using PRG, he can compute $T = T_0 + (T_1 - T_0)\Delta_{\mathbf{b}}$.

II. Encoding phase

- (a) Let $W' \in \mathbb{F}_q^{k \times m}$ be the matrix which has \mathbf{w}_i as its columns. R generates a uniformly random matrix $W'' \in \mathbb{F}_q^{k \times 2s}$, and defines the $(m + 2s) \times k$ -matrix $W = [W' \mid W'']^T$.
- (b) R sets $C = WG$, and sends $U = C + T_0 - T_1$.
- (c) S computes $Q = T + U\Delta_{\mathbf{b}}$. This implies that $Q = T_0 + C\Delta_{\mathbf{b}}$.

III. Consistency check

- (a) S samples a uniformly random matrix $M' \in \mathbb{F}_q^{2s \times m}$ and sends this to R .³ They both define $M = [M' \mid I_{2s}]$.
- (b) R computes the $2s \times n$ -matrix $\tilde{T} = MT_0$ and the $2s \times k$ -matrix $\tilde{W} = MW$ and sends these matrices to S .
- (c) S verifies that $MQ = \tilde{T} + \tilde{W}G\Delta_{\mathbf{b}}$. If this fails, S aborts the protocol.

IV. Output phase

- (a) Denote by \mathbf{q}_i and \mathbf{t}_i , the i 'th rows of Q and T_0 , respectively. For $i = 1, 2, \dots, m$ and for all $\mathbf{w} \in \mathbb{F}_q^k$, S computes $\mathbf{y}_{w,i} = \mathbf{v}_{w,i} \oplus H(\mathbf{q}_i - \mathbf{w}G\Delta_{\mathbf{b}})$ and sends these to R . For $i = 1, 2, \dots, m$, R can recover $\mathbf{v}_{w,i} = \mathbf{y}_{w,i} \oplus H(\mathbf{t}_i)$.

³In Section 4, we show if the protocol relies on a code over \mathbb{F}_{p^r} , it is enough to choose $M' \in \mathbb{F}_p^{2s \times m}$

ensure that the receiver uses codewords in the matrix C . What a malicious receiver might gain by choosing rows which are not codewords is explained in [IKNP03; Sec. 4].

Proofs of Security

In this section we give formal proofs for security. The proof of security against a malicious sender works more or less the same as the proof in [OOS17] but in

II. Papers

a different notation. For completeness, we have included this proof. However, we present the proof against a malicious receiver in another way, where the structure, some strategies, and some arguments differ from the original proof.

Theorem 3.2:

Protocol 1 is computationally secure against an actively corrupt sender.

Proof:

To show this theorem we give a simulator, which simulates the view of the sender during the protocol. The view of S is $\text{View}_S = \{N, U, \tilde{T}, \tilde{W}\}$. The simulator Sim_S works as follows.

- (i) Sim_S receives \mathbf{b} from S and defines a uniformly random matrix N , sets $T = \text{PRG}(N)$, and passes N back to S .
- (ii) Then Sim_S samples U uniformly at random and sends this to S . Additionally, it computes Q as S should.
- (iii) In phase III the simulator receives M' from S , and constructs M . The matrix \tilde{W} is sampled uniformly at random in $\mathbb{F}_q^{2s \times k}$, and using this, Sim_S sets $\tilde{T} = MQ - \tilde{W}G\Delta_{\mathbf{b}}$. It sends \tilde{T} and \tilde{W} to S .
- (iv) Sim_S receives $\mathbf{y}_{w,i}$ from S and since Sim_S already knows Q and \mathbf{b} , it can recover $\mathbf{v}_{w,i} = \mathbf{y}_{w,i} \oplus H(\mathbf{q}_i - \mathbf{w}G\Delta_{\mathbf{b}})$ and pass these to the ideal functionality $\mathcal{F}_{N\text{-OT}}^{\kappa,m}$.

We now argue that the simulator produces values indistinguishable from View_S . The matrix N is distributed identically in the real and ideal world. Since both T_0 and T_1 are outputs of a pseudorandom generator, the matrix $T_0 - T_1$, and therefore also U , is computationally indistinguishable from a uniformly random matrix. In the real world, $\tilde{W} = M'(W')^T + (W'')^T$ is uniform since W'' is chosen uniformly. The simulator Sim_S constructs \tilde{T} such that the consistency check will pass. This will always be the case in the real world, and hence S cannot distinguish between the real and ideal world. Additionally, we note that step (iv) ensures that the receiver obtains the same output in both worlds. This shows security against an actively corrupt sender. ■

We now shift our attention to an actively corrupt receiver. This proof is not as straight forward as for the sender. The idea is to reduce the problem of breaking the security of the protocol to the problem of breaking the assumptions on H . Before delving into the proof itself, we will introduce some lemmata and notations that will aid in the proof. The focus of these will be the probability that certain events happen during the protocol. These events are based on situations that determine the simulator's ability or inability to simulate the real world. Essentially, they are the event that R passes the consistency check, which we denote by PC; the event that R has introduced errors in too many positions, denoted by LS; and the event that the error

positions from the consistency check line up with the errors in C , which we call ES. These will be defined more precisely below.

Inspired by the notation in the protocol, we define

$$\tilde{C} = MC. \quad (4.1)$$

A corrupt receiver may deviate from the protocol and may send an erroneous \tilde{W} , which we denote by \tilde{W}_* . Let

$$\bar{C} = \tilde{C} - \tilde{W}_* G$$

and let $E = \text{supp}(\bar{C})$, where \bar{C} is interpreted in $\mathcal{C}^{\odot 2s}$. When writing \tilde{C} , \bar{C} , and E later in this section these are the definitions we are implicitly referring to.

Lemma 3.3:

Let C , C , and M be as in Protocol 1. Further, let LS be the event that $|E| \geq s$, and let ES be the event that for every $C' \in \mathcal{C}^{\odot 2s}$ there exists a $\hat{C} \in \mathcal{C}^{\odot m+2s}$ such that $\text{supp}(\tilde{C} - C') = \text{supp}(C - \hat{C})$. Then the probability that neither ES nor LS happen is at most q^{-s} .

Proof:

The matrix M' in Protocol 1 is chosen uniformly at random, and hence M can be interpreted as a member of a universal family of linear hashes. Thus, this lemma is a special case of [Cas+16; Theorem 1] when letting $m' = m + 2s$, $s' = s$, and $t' = 0$ where the primes denote the parameters in [Cas+16]. Additionally, note that our event LS happens if MC has distance at least s from $\mathcal{C}^{\odot 2s}$. ■

We will now bound the probability that an adversary is able to pass the consistency check, even if C contains errors.

Lemma 3.4:

Let PC denote the event that the consistency check passes. Then

$$\Pr[\text{PC}] \leq 2^{-|E|}.$$

Proof:

In order to compute $\Pr[\text{PC}]$, we consider \bar{C} and $\bar{T} = \tilde{T} - \tilde{T}_*$, where the $*$ indicates that the matrix may not be constructed as described in the protocol. The event PC happens if $MQ = \tilde{T}_* + \tilde{W}_* G \Delta_b$. However, from the definition of Q , $MQ = \tilde{T} + \tilde{C} \Delta_b$, implying that PC happens if and only if

$$\tilde{T} + \tilde{C} \Delta_b = \tilde{T}_* + \tilde{W}_* G \Delta_b \iff \bar{T} = -\bar{C} \Delta_b.$$

Now consider \bar{T} and \bar{C} in $(\mathbb{F}_q^n)^{\odot 2s}$, meaning that the entries \bar{C}_j and \bar{T}_j are elements in \mathbb{F}_q^{2s} . If the adversary chooses $\bar{C}_j = 0$ for some $j \in \{1, 2, \dots, n\}$, it

II. Papers

must choose $\tilde{T}_j = 0$ as well since the check would fail otherwise. If it chooses $\tilde{C}_j \neq 0$, it has two options. Either bet that $b_j = 0$ and set $\tilde{T}_j = 0$ or bet that $b_j = 1$ and set $\tilde{T}_j = -\tilde{C}_j$. This means that for each entry $j \in E$ the adversary has probability $\frac{1}{2}$ of guessing the correct value of b_j . For every entry $j \notin E$, each possible b_j gives a consistent value since $\tilde{C}_j = \tilde{T}_j = 0$. By this and the independence of the entries in \mathbf{b} , it follows that the probability of the check passing is bounded by $\Pr[\text{PC}] \leq 2^{-|E|}$. ■

This immediately gives the following corollary.

Corollary 3.5:

If LS denotes the same event as in Lemma 3.3, then

$$\Pr[\text{PC} \mid \text{LS}] \leq 2^{-s}.$$

We now have the required results to prove the security of Protocol 1 against an actively corrupt receiver. The events PC, LS, and ES from the previous lemmata and corollaries will also be used in the proof of the following theorem.

Theorem 3.6:

Protocol 1 is computationally secure against an actively corrupt receiver.

Proof:

As in the proof of Theorem 3.2, we construct a simulator Sim_R simulating the view of the receiver, which is $\text{View}_R = \{M', \mathbf{y}_{\mathbf{w},i}\}$. The simulator works as follows.

- (i) Sim_R receives N_0 and N_1 from R .
- (ii) The simulator receives U from R and combines these with $T_0 = \text{PRG}(N_0)$ and $T_1 = \text{PRG}(N_1)$ to reconstruct the matrix C . Additionally, it samples uniformly at random an internal value \mathbf{b} . Using this \mathbf{b} , the simulator Sim_R computes $Q = T_0 + C\Delta_{\mathbf{b}}$.
- (iii) Sim_R samples a random M' like the sender would have done in the protocol and sends this to R . In return, it receives \tilde{T}_* and \tilde{W}_* , where the $*$ indicates that the vectors may not be computed according to the protocol. The simulator runs the consistency check and aborts if it fails.
- (iv) Otherwise, it erasure decodes each row of C by letting E be the erasures to obtain W' . If the decoding fails, it aborts. If the decoding succeeds, the simulator gives W' as inputs to the ideal functionality $\mathcal{F}_{N-\text{OT}}^{k,m}$, which returns the values $\mathbf{v}_{\mathbf{w}_i,i}$ to Sim_R . It can now compute $\mathbf{y}_{\mathbf{w}_i,i} = \mathbf{v}_{\mathbf{w}_i,i} \oplus H(\mathbf{q}_i - \mathbf{w}_i G \Delta_{\mathbf{b}})$, and chooses $\mathbf{y}_{\mathbf{w},i}$ uniformly at random in \mathbb{F}_q^k for all $\mathbf{w} \neq \mathbf{w}_i$.

The matrix M' is uniformly distributed both in the real and ideal world. Hence, we only need to show that the output $\mathbf{y}_{w,i}$ produced by the simulator is indistinguishable from the output of the protocol.

Let \mathcal{Z} be a distinguisher for distinguishing between a real world execution of the protocol and an ideal execution using the simulator. By Lemma 2.3 its advantage is bounded by

$$\begin{aligned} \text{Adv}(\mathcal{Z}) \leq & \text{Adv}(\mathcal{Z} \mid \overline{\text{PC}}) + \text{Adv}(\mathcal{Z} \mid \text{PC}, \text{LS}) \Pr[\text{PC} \mid \text{LS}] \\ & + \text{Adv}(\mathcal{Z} \mid \text{PC}, \overline{\text{LS}}, \overline{\text{ES}}) \Pr[\overline{\text{LS}}, \overline{\text{ES}}] + \text{Adv}(\mathcal{Z} \mid \text{PC}, \overline{\text{LS}}, \text{ES}) \Pr[\text{PC}], \end{aligned} \quad (4.2)$$

where we have omitted some probability factors since they are all at most 1. Notice that $\mathbf{y}_{w,i}$ is constructed identically in both worlds. The remaining $\mathbf{y}_{w,i}$ are uniformly distributed in the ideal world, but constructed as

$$\mathbf{y}_{w,i} = \mathbf{v}_{w,i} \oplus H(\mathbf{q}_i - \mathbf{w}G\Delta_{\mathbf{b}}) \quad (4.3)$$

in the real world. Also notice that, if the consistency check fails, the simulator aborts before constructing the $\mathbf{y}_{w,i}$. This is the same as in the real world, and the only information R has received before this is M' , which is identically distributed in both worlds. Hence, the simulator is perfect in this case. This implies that the first term on the right-hand side in (4.2) is zero.

Since the consistency check by the simulator is identical to the consistency check done by S , it follows that the probability for the consistency check to pass even if R might have sent inconsistent values is the same in both worlds. This means that $\Pr[\text{PC} \mid \text{LS}] \leq 2^{-s}$ by Corollary 3.5. In a similar fashion, Lemma 3.3 implies that the penultimate term in (4.2) can be bounded above by q^{-s} . In summary, (4.2) can be rewritten as

$$\text{Adv}(\mathcal{Z}) \leq 2^{-s} + q^{-s} + \text{Adv}(\mathcal{Z} \mid \text{PC}, \overline{\text{LS}}, \text{ES}) 2^{-|E|}. \quad (4.4)$$

To show that this is negligible in κ and s , assume the opposite; that is, \mathcal{Z} has non-negligible advantage. We then construct a distinguisher \mathcal{D} breaking the security assumptions on H .

The distinguisher \mathcal{D} simulates the protocol with minor changes in order to produce its input to the challenger. After receiving the challenge it uses the output of \mathcal{Z} to respond. There exist inputs and random choices for R and S , which maximize the advantage of \mathcal{Z} , and we can assume that \mathcal{D} has fixed these in its simulation. This also means that PC , $\overline{\text{LS}}$ and ES happen in the simulation since otherwise, $\text{Adv}(\mathcal{Z})$ is negligible.

Because ES happens, puncturing C in the positions in E gives a codeword in $\pi_E(\mathcal{C}^{\otimes m+2s})$. Further, the event $\overline{\text{LS}}$ ensures that this corresponds to a unique codeword in $\mathcal{C}^{\otimes m+2s}$. Hence, \mathcal{D} is able to erasure decode and for $i = 1, 2, \dots, m+2s$ obtain $\mathbf{c}_i = \mathbf{w}_i G + \mathbf{e}_i$, where \mathbf{c}_i is the i 'th row of C , $w_H(\mathbf{e}_i) < d$, and $\text{supp}(\mathbf{e}_i) \subseteq E$.

The following arguments use that no matter which \mathbf{b} the challenger chooses, the distinguisher \mathcal{D} knows $\mathbf{e}_i \Delta_{\mathbf{b}}$. This follows from the fact that PC

II. Papers

has happened and therefore b_j for $j \in E$ is known to the adversary, which is simulated by \mathcal{D} . Hence, the distinguisher is able to construct $\mathbf{t}'_i = \mathbf{t}_i + \mathbf{e}_i \Delta_{\mathbf{b}}$, where the \mathbf{b} is the vector eventually chosen by the challenger, and \mathbf{t}_i the i 'th row of T_0 . Letting $t = n - |E|$, define the probability distribution \mathcal{X} to be the uniform distribution on \mathbb{F}_2^n under the condition that the indices in E are fixed to the corresponding entry of \mathbf{b} . By uniformity this distribution has min-entropy t . The distinguisher passes \mathcal{X} and the \mathbf{t}'_i to the challenger. It receives back $\mathbf{x}_{\mathbf{w},i}$ for all $i = 1, 2, \dots, n$ and $\mathbf{w} \in \mathbb{F}_q^k$ and needs to distinguish them between being uniformly random and being constructed as

$$\mathbf{x}_{\mathbf{w},i} = H(\mathbf{t}'_i + \mathbf{w}G\Delta_{\mathbf{b}}), \quad (4.5)$$

As in the protocol, let $Q = T_0 + C\Delta_{\mathbf{b}}$, where \mathbf{b} is again the vector chosen by the challenger. Therefore, if $\mathbf{x}_{\mathbf{w},i}$ is constructed as in (4.5), we have that

$$\begin{aligned} \mathbf{x}_{\mathbf{w},i} &= H(\mathbf{t}_i + \mathbf{e}_i \Delta_{\mathbf{b}} + \mathbf{w}G\Delta_{\mathbf{b}}) \\ &= H(\mathbf{q}_i - \mathbf{c}_i \Delta_{\mathbf{b}} + \mathbf{e}_i \Delta_{\mathbf{b}} + \mathbf{w}G\Delta_{\mathbf{b}}) \\ &= H(\mathbf{q}_i - (\mathbf{w}_i - \mathbf{w})G\Delta_{\mathbf{b}}). \end{aligned}$$

The distinguisher will now construct and input to \mathcal{Z} the following

$$\begin{aligned} \mathbf{y}_{\mathbf{w}_i,i} &= \mathbf{v}_{\mathbf{w}_i,i} \oplus H(\mathbf{t}'_i), \\ \mathbf{y}_{\mathbf{w},i} &= \mathbf{v}_{\mathbf{w},i} \oplus \mathbf{x}_{\mathbf{w}_i - \mathbf{w},i}, \quad \text{for } \mathbf{w} \neq \mathbf{w}_i. \end{aligned}$$

Since $\mathbf{t}'_i = \mathbf{t}_i + \mathbf{e}_i \Delta_{\mathbf{b}} = \mathbf{q}_i - \mathbf{w}_i G\Delta_{\mathbf{b}}$, we have that $\mathbf{y}_{\mathbf{w}_i,i}$ is identical to the value computed in both the real and ideal worlds.

For the remaining \mathbf{w} we notice that if the challenger has chosen $\mathbf{x}_{\mathbf{w},i}$ uniformly at random, then the values $\mathbf{y}_{\mathbf{w},i}$ are uniformly distributed as well. This is the same as the simulator will produce in the ideal world. On the other hand, if $\mathbf{x}_{\mathbf{w},i} = H(\mathbf{t}'_i + \mathbf{w}G\Delta_{\mathbf{b}})$, then we have $\mathbf{y}_{\mathbf{w},i} = \mathbf{v}_{\mathbf{w},i} \oplus H(\mathbf{q}_i - \mathbf{w}\Delta_{\mathbf{b}})$. This is exactly the same as produced during the protocol in the real world. Hence, \mathcal{D} can feed the values $\mathbf{y}_{\mathbf{w},i}$ to \mathcal{Z} , which can distinguish between the real and ideal world, and depending on the answer from \mathcal{Z} , \mathcal{D} can distinguish whether the $\mathbf{x}_{\mathbf{w},i}$ are uniformly distributed or are constructed as $H(\mathbf{t}'_i + \mathbf{w}G\Delta_{\mathbf{b}})$. Hence, the advantage of \mathcal{D} is the same as that of \mathcal{Z} under the restriction that PC, $\overline{\text{LS}}$, and ES happen. This means that

$$\text{Adv}(\mathcal{D}) = \text{Adv}(\mathcal{Z}|\text{PC}, \overline{\text{LS}}, \text{ES}) \geq 2^{|E|} (\text{Adv}(\mathcal{Z}) - 2^{-s} - q^{-s}), \quad (4.6)$$

where the inequality comes from (4.4). This contradicts that H is t -min-entropy strongly \mathcal{C} -correlation robust, and therefore \mathcal{Z} must have negligible advantage in the security parameters κ and s . \blacksquare

4 Consistency check in a subfield

Assume that $q = 2^r$ and that $r \mid s$. By restricting the matrix M' in Protocol 1 to have entries in \mathbb{F}_2 , the set of possible matrices M form a 2^{-2s} -almost universal

family of hashes. The probability in Lemma 3.3 can then be replaced by 2^{-s} by setting $m' = m + 2s$, $s' = \frac{s}{r}$, and $t' = 2s(1 - 1/r)$. This modification will show itself in (4.4), but here only the term q^{-s} is replaced by 2^{-s} , and hence the advantage will still be negligible in κ and s . However, choosing M' in a subfield reduces the communication complexity, since the number of bits needed to transmit M' is lowered by a factor of r . Furthermore, the computation of \tilde{T} and \tilde{W} can be done using only sums in \mathbb{F}_q , instead of multiplication and sums.

This method of reducing the communication complexity can be done to an intermediate subfield, which will give a probability bound between q^{-s} and 2^{-s} . In a similar way, this procedure could also be applied to fields of other characteristics.

5 Comparison

We compare the parameters of our modified construction with those that can be achieved by the actively secure OT-extension construction from [OOS17]. We will show that the ability to use larger finite fields in our modified construction induces a tradeoff between the number of base OT's that are needed for a given N and given security parameters (and hence also the complexity of the set-up phase), and the complexity of the encoding and consistency check phases of the extension protocol.

We have shown that given an $[n, k, d]_q$ -code, with $d \geq \max\{\kappa, s\}$, one can build an OT-extension protocol that implements the functionality $\mathcal{F}_{N\text{-OT}}^{k,m}$ using the functionality $\mathcal{F}_{2\text{-OT}}^{\kappa,n}$, where $N = q^k$. The parameters achieved in [OOS17] are the same as we obtain in the case $q = 2$.

We will limit our analysis to the case where $q = 2^r$, and $r \mid s$. We fix the security parameters s and κ , and fix N to be a power of q , $N = q^k$. Note then that $N = 2^{k \cdot \log_2 q}$. Let n' and n be the smallest integers for which there exist an $[n', k \log_2 q, \geq d]_2$ -linear code and an $[n, k, \geq d]_q$ -linear code, respectively. As we discuss later, we can always assume that $n \leq n'$, and in most cases it is in fact strictly smaller. Therefore, by using q -ary codes one obtains a reduction on the number of base OT's from n' to n , and therefore a more efficient initialization phase. Note for example that the binary construction always requires at least a minimum of $\log_2 N$ base OT's, while using q -ary codes allows to weaken this lower bound to $n \geq \log_q N$.

On the other hand, however, this comes at the cost of an increase in the communication complexity of what we have called the encoding and consistency check phases of the protocol since we need to send a masking of codewords over a larger field. We compare these two phases separately since the consistency check is only needed for an actively secure version of the protocol and it has a smaller cost than the encoding phase anyway. In the encoding phase, [OOS17] communicates a total of $(m + s)n'$ bits, while our construction communicates $(m + 2s)n \log_2 q$ bits. However, typically $m \gg s$, and therefore we only compare the terms mn' and $mn \log_2 q$. Hence, the communication complexity of this phase gets multiplied by a factor $\log_2 q \cdot n/n'$.

II. Papers

During the consistency check phase, which is less communication intensive, [OOS17] communicates a total of $sm + sn' + sk \log_2 q$ bits while our construction communicates $2sm + 2sn \log_2 q + 2sk \log_2 q$ bits when using the method from Section 4.

We now discuss in more detail the rates between n and n' that we can obtain for different values of q . In order to do that, having fixed d and k , let n' and n denote the minimum values for which $[n', k \log_2 q, \geq d]_2$ -linear codes and $[n, k, \geq d]_q$ -linear codes exist. Let k' denote $k \log_2 q$. It is easy to see that $n \leq n'$ by considering a generator matrix for the binary code of length n' and considering the code spanned over \mathbb{F}_q by that same matrix. In many situations, however, n is in fact considerably smaller than n' . The extreme case is when $q = N$, and therefore $k = 1$, in which case one can take the repetition code over \mathbb{F}_q and set $n = d$. It is difficult to give a general tight bound on the relation between n and n' , although at least we can argue that $n \leq n' - k' + k$: indeed, given an $[n', k', \geq d]_2$ -code \mathcal{C}_2 then one can obtain an $[n', k', \geq d]_q$ -code \mathcal{C}_q by simply considering the linear code spanned over the field \mathbb{F}_q by the generator matrix of \mathcal{C}_2 and then shorten⁴ \mathcal{C}_q at $k' - k$ positions, after which we obtain an $[n, \geq k, \geq d]_q$ -code \mathcal{C} , with $n = n' - k' + k$. This bound is however by no means tight in general. We now consider concrete examples of codes, that will be summarized in Table 1.

Code	N	n (Base OT's)	d	Comparison	
				n	CC
Walsh-Had. [KK13]	256	256	128		
Juxt. simplex code over \mathbb{F}_4	256	170	128	$\div 1.51$	$\times 1.33$
Punct. Walsh-Had. [OOS17]	512	256	128		
Juxt. simplex code over \mathbb{F}_8	512	146	128	$\div 1.75$	$\times 1.71$
$[511, 76, \geq 171]_2$ -BCH [OOS17]	2^{76}	511	≥ 171		
$[455, 48, \geq 174]_4$ -BCH over \mathbb{F}_4	2^{96}	455	≥ 174	$\div 1.12$	$\times 1.78$
$[1023, 443, \geq 128]_2$ -BCH [OOS17]	2^{443}	1023	≥ 128		
$[455, 154, \geq 128]_8$ -BCH over \mathbb{F}_8	2^{462}	455	≥ 128	$\div 2.25$	$\times 1.33$

Table 1. Comparison of using binary and q -ary codes for OT-extension. In the last two columns we consider the decrease in the number of base OT's and increase in the dominant term of the communication complexity in the encoding phase when we consider a q -ary construction.

Small values of N

For relatively small values of N ($N < 1000$), [KK13] suggests the use of Walsh-Hadamard codes, with parameters $[2^{k'}, k', 2^{k'-1}]_2$, while [OOS17] improves

⁴Shortening a code at positions i_1, \dots, i_t means first taking the subcode consisting of all codewords with 0's at all those positions and then erasing those coordinates.

on this by using punctured Walsh-Hadamard codes instead. Punctured Walsh-Hadamard codes (also known as first order Reed-Muller codes) are $[2^{k'-1}, k', 2^{k'-2}]_2$ -linear codes. These are the shortest possible binary linear codes for those values of N and d , as they attain the Griesmer bound. In terms of N , the parameters can be written as $[N/2, \log_2 N, N/4]_2$.

The natural generalization of these codes to \mathbb{F}_q are first order q -ary Reed Muller codes, which have parameters $[q^{k-1}, k, q^{k-1} - q^{k-2}]_q$. Moreover, there is a q -ary generalization of Walsh-Hadamard codes, known as simplex codes, which have parameters $[\frac{q^k-1}{q-1}, k, q^{k-1}]_q$.

For example for $q = 4$, the parameters of the simplex code can be written in terms of N as $[(N-1)/3, \log_4 N, N/4]_4$, and hence, for the same values of d and N , the number of base OT's is reduced by a factor $3/2$ since $n/n' < 2/3$. On the other hand, the communication complexity of the encoding phase increases by a factor $2n/n' < 4/3$ compared to using binary punctured Walsh-Hadamard codes. We note, however, that this comparison is only valid if N is a power of 4.

Because of the fact that N needs to be a power of q , in the comparison table below it will be convenient to use the juxtaposition of two copies of the same code. This means that given an $[n, k, d]_q$ code C' , we can obtain a $[2n, k, 2d]_q$ code by sending each symbol in a codeword twice. With respect to the examples listed in [OOS17], we see that by choosing an adequate finite field and using juxtapositions of simplex codes, the number of OT's gets divided by a factor slightly over 1.5, while the communication complexity increases by a somewhat smaller factor.

Larger values of N

For larger values of N , [OOS17] suggests using binary BCH codes. We use q -ary BCH codes instead. It is difficult to find BCH codes that match exactly the parameters (N, d) from [OOS17] so in our comparison we have always used larger values of both N and d . This is actually not too advantageous for our construction since the codes in [OOS17] were selected so that their length is of the form $2^m - 1$ (what is called primitive binary BCH codes, which usually yields the constructions with best parameters) and that results in a range of parameters where it is not adequate to choose primitive q -ary BCH codes. Nevertheless, in the case where the large value $N' = 2^{443}$ is considered in [OOS17], we can reduce the number of base OT's needed to less than half, while the communication complexity only increases by $4/3$, and in addition to that we achieve a larger value $N = 2^{462}$. Observe that, for this value of N , with a binary code the number of base OT's would be restricted by the naïve bound $n' \geq \log_2 N = 462$ in any case (i.e. even if $d = 1$), while using a code over \mathbb{F}_8 we only need to use 455.

6 Acknowledgements

The authors wish to thank Claudio Orlandi for providing helpful suggestions during the early stages of this work, and Peter Scholl for his valuable comments.

7 References


- [Bea96] **D. Beaver**. ‘Correlated Pseudorandomness and the Complexity of Private Computations’. In: *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*. STOC ’96. ACM, 1996, pp. 479–488. ISBN: 0-89791-785-5. DOI: 10.1145/237814.237996.
- [Cas+15] **I. Cascudo, I. Damgård, B. David, I. Giacomelli, J.B. Nielsen and R. Trifiletti**. ‘Additively Homomorphic UC Commitments with Optimal Amortized Overhead’. In: *Public-Key Cryptography – PKC 2015*. Springer Berlin Heidelberg, 2015, pp. 495–515. ISBN: 978-3-662-46447-2. DOI: 10.1007/978-3-662-46447-2_22.
- [Cas+16] **I. Cascudo, I. Damgård, B. David, N. Döttling and J.B. Nielsen**. ‘Rate-1, Linear Time and Additively Homomorphic UC Commitments’. In: *Advances in Cryptology – CRYPTO 2016*. Springer Berlin Heidelberg, 2016, pp. 179–207. ISBN: 978-3-662-53015-3. DOI: 10.1007/978-3-662-53015-3_7.
- [FJNT16] **T.K. Frederiksen, T.P. Jakobsen, J.B. Nielsen and R. Trifiletti**. ‘On the Complexity of Additively Homomorphic UC Commitments’. In: *Theory of Cryptography*. Springer Berlin Heidelberg, 2016, pp. 542–565. ISBN: 978-3-662-49096-9. DOI: 10.1007/978-3-662-49096-9_23.
- [GMW87] **O. Goldreich, S. Micali and A. Wigderson**. ‘How to Play ANY Mental Game’. In: *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*. STOC ’87. ACM, 1987, pp. 218–229. ISBN: 0-89791-221-7. DOI: 10.1145/28395.28420.
- [IKNP03] **Y. Ishai, J. Kilian, K. Nissim and E. Petrank**. ‘Extending Oblivious Transfers Efficiently’. In: *Advances in Cryptology – CRYPTO 2003*. Springer Berlin Heidelberg, 2003, pp. 145–161. ISBN: 978-3-540-45146-4. DOI: 10.1007/978-3-540-45146-4_9.
- [IR89] **R. Impagliazzo and S. Rudich**. ‘Limits on the Provable Consequences of One-way Permutations’. In: *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*. STOC ’89. ACM, 1989, pp. 44–61. ISBN: 0-89791-307-8. DOI: 10.1145/73007.73012.
- [Kil88] **J. Kilian**. ‘Founding Cryptography on Oblivious Transfer’. In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC ’88. ACM, 1988, pp. 20–31. ISBN: 0-89791-264-0. DOI: 10.1145/62212.62215.
- [KK13] **V. Kolesnikov and R. Kumaresan**. ‘Improved OT Extension for Transferring Short Secrets’. In: *Advances in Cryptology – CRYPTO 2013*. Springer

- Berlin Heidelberg, 2013, pp. 54–70. ISBN: 978-3-642-40084-1. DOI: 10 . 1007/978-3-642-40084-1_4.
- [KOS15] **M. Keller, E. Orsini and P. Scholl.** 'Actively Secure OT Extension with Optimal Overhead'. In: *Advances in Cryptology – CRYPTO 2015*. Springer Berlin Heidelberg, 2015, pp. 724–741. ISBN: 978-3-662-47989-6. DOI: 10 . 1007/978-3-662-47989-6_35.
- [MS83] **F. MacWilliams and N. Sloane.** *The Theory of Error-Correcting Codes*. 1st ed. North Holland, 1983. ISBN: 978-0-444-85193-2.
- [OOS17] **M. Orrù, E. Orsini and P. Scholl.** 'Actively Secure 1-out-of-N OT Extension with Application to Private Set Intersection'. In: *Topics in Cryptology – CT-RSA 2017*. Springer International Publishing, 2017, pp. 381–396. ISBN: 978-3-319-52153-4. DOI: 10 . 1007/978-3-319-52153-4_22.
- [Yao82] **A.C. Yao.** 'Protocols for Secure Computations'. In: *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*. SFCS '82. IEEE Computer Society, 1982, pp. 160–164. DOI: 10 . 1109 / SFCS . 1982 . 88.


Paper C

On nested code pairs from the Hermitian curve

René Bødker Christensen

 0000-0002-9209-3739

Olav Geil

 0000-0002-9666-3399

Submitted to:

Finite Fields and Their Applications.

Preprint available at [arXiv:1807.04042](https://arxiv.org/abs/1807.04042) [cs.IT]

© 2018 The authors

Abstract

Nested code pairs play a crucial role in the construction of ramp secret sharing schemes [KUM12] and in the CSS construction of quantum codes [KKKS06]. The important parameters are (1) the codimension, (2) the relative minimum distance of the codes, and (3) the relative minimum distance of the dual set of codes. Given values for two of them, one aims at finding a set of nested codes having parameters with these values and with the remaining parameter being as large as possible. In this work we study nested codes from the Hermitian curve. For not too small codimension, we present improved constructions and provide closed formula estimates on their performance. For small codimension we show how to choose pairs of one-point algebraic geometric codes in such a way that one of the relative minimum distances is larger than the corresponding non-relative minimum distance.

1 Introduction

In this paper we study improved constructions of nested code pairs from the Hermitian curve. Here the phrase ‘improved construction’ refers to optimizing those parameters important for the corresponding linear ramp secret sharing schemes as well as stabilizer asymmetric quantum codes. Our work is a natural continuation of [GGHR18], where improved constructions of nested code pairs were defined from Cartesian product point sets. The analysis in the present paper includes a closed formula estimate on the dimension of order bound improved Hermitian codes, which is of interest in its own right, i.e. also without the above mentioned applications.

A linear ramp secret sharing scheme is a cryptographic method to encode a secret message in \mathbb{F}_q^ℓ into n shares from \mathbb{F}_q . These shares are then distributed among a group of n parties and only specified subgroups are able to reconstruct the secret. A secret sharing scheme is characterized by its privacy number t and its reconstruction number r . The first is defined as the largest number such that no subgroup of this size can obtain any information on the secret. The second is defined to be the smallest number such that any subgroup of this size can reconstruct the entire secret. A linear ramp secret sharing scheme can be understood as the following coset construction. Consider linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$. Let $\{\mathbf{b}_1, \dots, \mathbf{b}_{k_2}\}$ be a basis for C_2 and extend it to a basis $\{\mathbf{b}_1, \dots, \mathbf{b}_{k_2}, \mathbf{b}_{k_2+1}, \dots, \mathbf{b}_{k_2+\ell}\}$ for C_1 . Here, of course, ℓ is the codimension of C_1 and C_2 . Choose elements a_1, \dots, a_{k_2} uniformly and independent at random and encode the secret $\mathbf{s} = (s_1, \dots, s_\ell)$ as the codeword $\mathbf{c} = (c_1, \dots, c_n) = a_1 \mathbf{b}_1 + \dots + a_{k_2} \mathbf{b}_{k_2} + s_1 \mathbf{b}_{k_2+1} + \dots + s_\ell \mathbf{b}_{k_2+\ell}$. Then use c_1, \dots, c_n as the shares. The crucial parameters for the construction are the codimension of the pair of nested codes and their relative minimum distances $d(C_1, C_2)$ and $d(C_2^\perp, C_1^\perp)$. Recall that these are defined as

$$d(C_1, C_2) = \min\{w_H(\mathbf{c}) \mid \mathbf{c} \in C_1 \setminus C_2\}$$

and similar for the dual codes. The following well-known theorem (see for instance [KUM12]) shows how to determine the privacy number and the reconstruction number.

Theorem 1.1:

Given \mathbb{F}_q -linear codes $C_2 \subset C_1$ of length n and codimension ℓ , the corresponding ramp secret sharing scheme encodes secrets $\mathbf{s} \in \mathbb{F}_q^\ell$ into a set of n shares from \mathbb{F}_q . The privacy number equals $t = d(C_2^\perp, C_1^\perp) - 1$, and the reconstruction number is $r = n - d(C_1, C_2) + 1$.

A linear q -ary asymmetric quantum error-correcting code is a q^k dimensional subspace of the Hilbert space \mathbb{C}^{q^n} where error bases are defined by unitary operators Z and X , the first representing phase-shift errors, and the second representing bit-flip errors [CRSS98; KKKS06; Ste96]. In [IM07] it was identified that in some realistic models phase-shift errors occur more frequently than bit-flip errors, and the asymmetric codes were therefore introduced [EJLP13; IM07; LaG12a; SKR09; WFLX10] to balance the error correcting ability accordingly. For such codes we write the set of parameters as $[[n, k, d_z/d_x]]_q$ where d_z is the minimum distance related to phase-shift errors and d_x is the minimum distance related to bit-flip errors. The CSS construction transforms a pair of nested classical linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ into an asymmetric quantum code. From [SKR09] we have

Theorem 1.2:

Consider linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$. Then the corresponding asymmetric quantum code defined using the CSS construction has parameters

$$[[n, \ell = \dim C_1 - \dim C_2, d_z/d_x]]_q$$

where $d_z = d(C_1, C_2)$ and $d_x = d(C_2^\perp, C_1^\perp)$.

Quantum codes with $d(C_1, C_2) > d(C_1)$ or $d(C_2^\perp, C_1^\perp) > d(C_2^\perp)$ are called impure, and they are desirable due to the fact that one can take advantage of this property in connection with the error-correction. More precisely, one can tolerate $\lfloor (d(C_1, C_2) - 1)/2 \rfloor$ phase-shift errors and $\lfloor (d(C_2^\perp, C_1^\perp) - 1)/2 \rfloor$ bit-flip errors, respectively, but in the decoding algorithms it is only necessary to correct up to $\lfloor (d(C_1) - 1)/2 \rfloor$ and $\lfloor (d(C_2^\perp) - 1)/2 \rfloor$ errors, respectively. Despite this observation, only few impure codes have been presented in the literature.

With the above two applications in mind, the challenge is to find nested codes $C_2 \subset C_1$ such that two of the parameters ℓ , $d(C_1, C_2)$, $d(C_2^\perp, C_1^\perp)$ attain given prescribed values, and the remaining parameter is as large as possible. In this paper we analyse two good constructions from the Hermitian function field. In the first we consider code pairs such that C_1 is an order bound improved primary code [AG08; GMRT11] and such that C_2 is the dual of an order bound improved dual code [HLP98]. Considering in this case the

II. Papers

minimum distances rather than the relative distances is no restriction due to the optimized choice of codes – the minimum distances $d(C_1)$ and $d(C_2^\perp)$ being so good that there is essentially no room for $d(C_1, C_2) > d(C_1)$ or $d(C_2^\perp, C_1^\perp) > d(C_2^\perp)$ to hold. For this construction to work, the codimension cannot be very small. For small codimension when $d(C_1)$ and $d(C_2^\perp)$ are far from each other we then show how to choose ordinary one-point algebraic geometric codes such that one of the relative distances becomes larger than the corresponding ordinary minimum distance. In particular, this construction leads to impure asymmetric quantum codes.

The paper is organized as follows. In Section 2 we collect material from the literature on how to determine parameters of primary and dual codes coming from the Hermitian curve, and we introduce the order bound improved codes¹. In Section 3 we establish closed formula lower bounds on the dimension of order bound improved Hermitian codes of any designed minimum distance. We then continue in Section 4 by determining the pairs $(\delta_1, \delta_2) \in \{1, \dots, n\} \times \{1, \dots, n\}$ for which the order bound improved primary code C_1 of designed distance δ_1 contains C_2 , the dual of an order bound improved dual code of designed distance δ_2 . This and the information from Section 3 is then translated into information on improved nested code pairs of not too small codimension in Section 5. Next, in Section 6 we determine parameters of nested one-point algebraic geometric code pairs of small codimension for which one of the relative distances is larger than the non-relative. Finally, in Section 7 samples of the given constructions are compared with known asymmetric quantum codes, with existence bounds on asymmetric quantum codes, and with non-existence bounds on linear ramp secret sharing schemes. Section 8 is the conclusion.

2 Hermitian codes and their parameters

Given an algebraic function field over a finite field, let P_1, \dots, P_n, Q be rational places. By $H(Q)$ we denote the Weierstrass semigroup of Q , and we write

$$H^*(Q) = \{\lambda \in H(Q) \mid C_\mathcal{L}(D, \lambda Q) \neq C_\mathcal{L}(D, (\lambda - 1)Q)\}$$

where $D = P_1 + \dots + P_n$. Recall that the dual code of $C_\mathcal{L}(D, \lambda Q)$ is written $C_\Omega(D, \lambda Q)$. The order bound [DP10; HLP98] then tells us that if

$$\mathbf{c} \in C_\Omega(D, (\lambda - 1)Q) \setminus C_\Omega(D, \lambda Q)$$

(which can only happen if $\lambda \in H^*(Q)$), then the Hamming weight of \mathbf{c} satisfies

$$w_H(\mathbf{c}) \geq \mu(\lambda) \tag{4.1}$$

¹This section also contains a collective treatment of the order bounds for general primary as well as dual (improved) one-point algebraic geometric codes which may not be easy to find in the literature.

where

$$\mu(\lambda) = \#\{\eta \in H(Q) \mid \lambda - \eta \in H(Q)\}.$$

The similar bound for the primary case [AG08; Gei03; GMRT11] tells us that if

$$\mathbf{c} \in C_{\mathcal{L}}(D, \lambda Q) \setminus C_{\mathcal{L}}(D, (\lambda - 1)Q),$$

then

$$w_H(\mathbf{c}) \geq \sigma(\lambda) \quad (4.2)$$

where

$$\sigma(\lambda) = \#\{\eta \in H^*(Q) \mid \eta - \lambda \in H(Q)\}.$$

Besides implying that

$$\begin{aligned} d(C_{\mathcal{L}}(D, \lambda Q)) &\geq \min\{\sigma(\gamma) \mid 0 \leq \gamma \leq \lambda, \gamma \in H^*(Q)\} \\ d(C_{\Omega}(D, \lambda Q)) &\geq \min\{\mu(\gamma) \mid \lambda < \gamma, \gamma \in H^*(Q)\}, \end{aligned} \quad (4.3)$$

which are both as strong as the Goppa bound, it tells us that for $\epsilon, \lambda \in H^*(Q)$ with $\epsilon < \lambda$ it holds that

$$d(C_{\mathcal{L}}(D, \lambda Q), C_{\mathcal{L}}(D, \epsilon Q)) \geq \min\{\sigma(\gamma) \mid \epsilon < \gamma \leq \lambda, \gamma \in H^*(Q)\}, \quad (4.4)$$

and similarly

$$d(C_{\Omega}(D, \epsilon Q), C_{\Omega}(D, \lambda Q)) \geq \min\{\mu(\gamma) \mid \epsilon < \gamma \leq \lambda, \gamma \in H^*(Q)\}. \quad (4.5)$$

Furthermore, for $i \in H^*(Q)$ let $f_i \in \mathcal{L}(iQ) \setminus \mathcal{L}((i-1)Q)$. Then we obtain the improved primary code

$$\tilde{E}(\delta) = \text{Span}\{(f_i(P_1), \dots, f_i(P_n)) \mid \sigma(i) \geq \delta\},$$

which clearly has minimum distance at least δ and highest possible dimension for a primary code with that designed distance. Similarly, the improved dual code

$$\tilde{C}(\delta) = (\text{Span}\{(f_i(P_1), \dots, f_i(P_n)) \mid \mu(i) < \delta\})^{\perp}$$

has minimum distance at least δ and again the highest possible dimension for a dual code with that designed distance.

Turning to the Hermitian curve $x^{q+1} - y^q - y$ over \mathbb{F}_{q^2} where q is a prime power, it is well-known that the corresponding function field has exactly $q^3 + 1$ rational places P_1, \dots, P_{q^3}, Q . Choosing $n = q^3$ one obtains $H(Q) = \langle q, q+1 \rangle$ and

$$H^*(Q) = \{iq + j(q+1) \mid 0 \leq i \leq q^2 - 1, 0 \leq j \leq q - 1\}. \quad (4.6)$$

In [Sti88] it was shown that

$$C_{\mathcal{L}}(D, \lambda Q) = C_{\Omega}(D, (q^3 + q^2 - q - 2 - \lambda)Q) \quad (4.7)$$

for any $\lambda \in H^*(Q)$, and the minimum distance was established for dimensions up to a certain value. The minimum distance for the remaining dimensions

II. Papers

was then settled in [YK92]. In the present paper we shall need improved code constructions, and we will in some cases also be occupied with the relative distances rather than minimum distances. To this end we recall material from [Gei03] on the functions μ and σ – stated there in the more general case of norm-trace curves, but adapted here to the Hermitian case.

Proposition 2.1:

Consider the Hermitian curve. For $iq + j(q + 1) \in H^(Q)$ we have*

$$\sigma(iq + j(q + 1)) = \begin{cases} q^3 - iq - j(q + 1) & \text{if } 0 \leq i < q^2 - q \\ (q^2 - i)(q - j) & \text{if } q^2 - q \leq i \leq q^2 - 1, \end{cases} \quad (4.8)$$

and $\mu((q^2 - 1 - i)q + (q - 1 - j)(q + 1)) = \sigma(iq + j(q + 1))$. For each $\lambda \in H^(Q)$ there exists a word $\mathbf{c} \in (C_{\mathcal{L}}(D, \lambda Q) \setminus C_{\mathcal{L}}(D, (\lambda - 1)Q)) \cap \tilde{E}(\sigma(\lambda))$ having Hamming weight equal to $\sigma(\lambda)$.*

Proof:

Given a numerical semigroup Λ with finitely many gaps and an element $\lambda \in \Lambda$, we know from [HLP98; Lem. 5.15] that $\#(\Lambda \setminus (\lambda + \Lambda)) = \lambda$. As $\#H^*(Q) = q^3$ we therefore obtain $\sigma(iq + j(q + 1)) \geq q^3 - (iq + j(q + 1))$. On the other hand, it is clear that $\sigma(iq + j(q + 1)) \geq (q^2 - i)(q - j)$ by the definition of σ . Taking the maximum between these two expressions, we obtain the right hand side of (4.8). That these estimates on σ are the true values and that the last part of the proposition holds true both follow as a consequence of [Gei03; Lem. 4]. The details of applying [Gei03; Lem. 4] are left for the reader. Finally, the relation between μ and σ is a consequence of $H^*(Q)$ being a box in the parameters i and j , see (4.6). ■

In Appendix A we list a series of lemmas which all follow as corollaries to Proposition 2.1 and which will be needed in Sections 3 and 4.

Throughout the rest of the paper we restrict to considering codes derived from the Hermitian curve, and we always assume the length to be $n = q^3$. From Proposition 2.1 we see that the bound (4.4) on the relative distance of $C_{\mathcal{L}}(D, \epsilon Q) \subset C_{\mathcal{L}}(D, \lambda Q)$ is sharp. A similar remark then holds for the bound (4.5) on the dual codes due to (4.7). Finally, we observe from [Gei03; Sec. 4] that

$$\tilde{E}(\delta) = \tilde{C}(\delta) \quad (4.9)$$

holds. Proposition 2.1 therefore not only gives us the true value of the minimum distance of the improved primary codes (without loss of generality we may assume $\delta = \sigma(\lambda)$ for some $\lambda \in H^*(Q)$), but also does it for the improved dual codes.

We conclude the section with some information on the cases where the improved primary codes coincide with one-point algebraic geometric codes.

Corollary 2.2:

For $\delta > q^2 - q$ we have $\tilde{E}(\delta) = C_{\mathcal{L}}(D, (q^3 - \delta)Q)$, but $C_{\mathcal{L}}(D, (q^3 - (q^2 - q))Q)$ is strictly contained in $\tilde{E}(q^2 - q)$.

This corollary implies that the dimension of $\tilde{E}(\delta)$ can be determined from the usual one-point Hermitian codes whenever $\delta > q^2 - q$. For later reference we state these dimensions in terms of δ .

Proposition 2.3:

Denote by $g = q(q-1)/2$ the genus of Hermitian function field. If $q^2 - q < \delta < q^3 - 2g + 2$, then the dimension of $\tilde{E}(\delta)$ is given by $q^3 - g + 1 - \delta$. If $q^3 - 2g + 2 \leq \delta \leq q^3$, we have

$$\dim \tilde{E}(\delta) = \sum_{s=0}^{a+b} (s+1) - \max\{a, 0\}$$

where $q^3 - \delta = aq + b(q+1)$ for $-q < a < q$ and $0 \leq b < q$.

Proof:

First, note that in both cases Corollary 2.2 implies the equality $\tilde{E}(\delta) = C_{\mathcal{L}}(D, (q^3 - \delta)Q)$. For the first case recall from [Sti93; Cor. II.2.3] that the code $C_{\mathcal{L}}(D, \lambda G)$ has dimension $\lambda + 1 - g$ whenever $2g - 2 < \lambda < n$. By the assumptions on δ , we have $q^3 - \delta > q^3 - (q^3 - 2g + 2) = 2g - 2$, meaning that $C_{\mathcal{L}}(D, (q^3 - \delta)Q)$ has dimension $q^3 - \delta + 1 - g$. By the observation in the beginning of the proof, the same holds true for $\tilde{E}(\delta)$.

To prove the second case, observe that the dimension of $C_{\mathcal{L}}(d, (q^3 - \delta)Q)$ is exactly the number of elements λ in $H^*(Q)$ with $\lambda \leq q^3 - \delta$. By (4.6) such elements have the form $\lambda = iq + j(q+1)$, but equivalently we can write $\lambda = i'q + j$ where $i' = i + j$. By the division algorithm this representation is unique for $0 \leq j < q$. For $i'q + j$ to satisfy the requirements of (4.6), we also require $i' - j = i \geq 0$. That is, $H^*(Q)$ contains the integers whose quotients modulo q are at least their remainders modulo q .

Writing $q^3 - \delta = (a+b)q + b$ with $0 \leq b < q$ using the division algorithm, the number of elements in $H^*(Q)$ less than $(a+b+1)q$ is given by $\sum_{s=0}^{a+b} (s+1)$. If $b \geq a+b$, which happens only if $a \leq 0$, this number is also the number of elements with value at most $q^3 - \delta$. Otherwise, the count includes $b - (a+b) = a$ elements of $H^*(Q)$ that are greater than $q^3 - \delta$. Hence, subtracting $\max\{a, 0\}$ gives the desired count in both cases. ■

It remains to establish information on the dimension of $\tilde{E}(\delta)$ for $\delta \leq q^2 - q$ since the improved codes differ from the usual Hermitian codes in this case. This subject is treated in the next section.

3 The dimension of improved codes

As explained in the previous section, the dimension of $\tilde{E}(\delta)$ can be determined from well-known methods as long as $\delta > q^2 - q$. In this section we present closed formula lower bounds on the dimension in the remaining cases. We start with an important lemma.

Lemma 3.1:

Let $\delta \leq q^2$. The number of integer points

$$(x, y) \in \{q^2 - q, \dots, q^2 - 1\} \times \{0, \dots, q - 1\}$$

with $(q^2 - x)(q - y) \geq \delta$ is at least

$$q^2 - \lfloor \delta + \delta \ln(q^2/\delta) \rfloor. \quad (4.10)$$

If $\delta < q$, then the number of integer points is at least

$$q^2 - \lfloor \delta + \delta \ln(\delta) \rfloor, \quad (4.11)$$

which is stronger than (4.10).

Proof:

The number of integer points in the given Cartesian product is at least that of the volume of

$$\{(x, y) \in [q^2 - q, q^2] \times [0, q] \mid (q^2 - x)(q - y) \geq \delta\},$$

which equals

$$\begin{aligned} & \int_{q^2 - q}^{q^2 - \frac{\delta}{q}} \int_0^{q - \frac{\delta}{q^2 - x}} dy \, dx \\ &= q(q^2 - \frac{\delta}{q} - q^2 + q) + \int_{q^2 - \frac{\delta}{q}}^{q^2 - q} \frac{\delta}{q^2 - x} \, dx \\ &= q^2 - \delta - \delta [\ln(z)]_{\frac{\delta}{q}}^q = q^2 - \delta - \delta \ln(q^2/\delta), \end{aligned}$$

where we used the substitution $z = q^2 - x$. Since the number of integer points is integral, we obtain the bound $\lfloor q^2 - \delta - \delta \ln(q^2/\delta) \rfloor$, which is the same as (4.10).

If $\delta < q$, then the number of integer points is at least the combined volumes of

$$\{(x, y) \in [q^2 - q, q^2] \times [0, q] \mid x \leq q^2 - \delta \text{ or } y \leq q - \delta\}$$

and

$$\{(x, y) \in [q^2 - \delta, q^2] \times [q - \delta, q] \mid (q^2 - x)(q - y) \geq \delta\}.$$

The first mentioned volume equals $q^2 - \delta^2$. The latter volume is

$$\begin{aligned} & \int_{q^2-\delta}^{q^2-1} \int_{q-\delta}^{q-\frac{\delta}{q^2-x}} dy \, dx \\ &= \int_{q^2-\delta}^{q^2-1} \left(\delta - \frac{\delta}{q^2-x} \right) dx \\ &= \delta(\delta-1) - \delta[\ln(z)]_1^\delta = \delta(\delta-1) - \delta \ln(\delta). \end{aligned}$$

Adding up the two volumes, we obtain (4.11) by applying the ceiling function as above. ■

The dimension of the improved codes of designed distance at most $q^2 - q$ is covered by the following two propositions. Recall from (4.9) that the equality $\tilde{C}(\delta) = \tilde{E}(\delta)$ holds for codes defined from the Hermitian function field. Hence, the stated formulas for primary codes also hold for the dual codes.

Proposition 3.2:

Given $q < \delta \leq q^2 - q$ write

$$q^3 - \delta = q^3 - q^2 + aq + b(q+1)$$

where $-q < a < q$ and $0 \leq b < q$.

If $0 < a$, then

$$\dim(\tilde{E}(\delta)) \geq q^3 - \delta - g + 1 - \sum_{s=0}^{a+b} (s+1) + a + q^2 - \lfloor \delta + \delta \ln(q^2/\delta) \rfloor.$$

If $a \leq 0$, then

$$\dim(\tilde{E}(\delta)) \geq q^3 - \delta - g + 1 - \sum_{s=0}^{a+b} (s+1) + q^2 - \lfloor \delta + \delta \ln(q^2/\delta) \rfloor.$$

Proof:

Let $g = q(q-1)/2$ be the number of gaps in $H(Q)$, i.e. the genus of the function field. As is well-known, for $2g \leq \lambda < q^3 - 1$ the number of $\epsilon \in H^*(Q)$ with $\epsilon \leq \lambda$ equals $\lambda - g + 1$. Therefore, by choosing $\lambda = q^3 - \delta$ the restriction on δ as given in the proposition implies that there are exactly $q^3 - \delta - g + 1$ elements $\epsilon \in H^*(Q)$ with $\epsilon \leq q^3 - \delta$. These elements then satisfy $\sigma(\epsilon) \geq \delta$ by Lemma A.2. From (4.8) we see that the additional elements in $H^*(Q)$ with $\sigma(\epsilon) \geq \delta$ must belong to

$$\{iq + j(q+1) \mid q^2 - q \leq i \leq q^2 - 1, 0 \leq j \leq q-1\}. \quad (4.12)$$

Lemma 3.1 gives an estimate on the total number of elements ϵ in (4.12) with $\sigma(\epsilon) \geq \delta$. Adding this number to $q^3 - \delta - g + 1$, we have counted the elements

II. Papers

ϵ in (4.12) with $\epsilon \leq q^3 - \delta$ twice. By using similar arguments as in the proof of Proposition 2.3, the number of such elements equals $\sum_{s=0}^{a+b} (s+1) - a$ when $0 \leq a < q$, and it equals $\sum_{s=0}^{a+b} (s+1)$ when $-q < a < 0$. This proves the proposition. ■

Proposition 3.3:

Given $1 \leq \delta \leq q$ the dimension of the code $\tilde{E}(\delta)$ satisfies

$$\dim(\tilde{E}(\delta)) \geq q^3 - \lfloor \delta + \delta \ln(\delta) \rfloor.$$

Proof:

By Lemma A.7 the elements $\lambda \in H^*(Q)$ which do not satisfy $\sigma(\lambda) \geq \delta$ must belong to $\{iq + j(q+1) \mid q^2 - \delta \leq i \leq q^2, q - \delta \leq j < q\}$. The number of elements in this set having $\sigma(\lambda) < \delta$ is bounded above by $\lfloor \delta + \delta \ln(\delta) \rfloor$ by Lemma 3.1. Since the total number of monomials in $H^*(Q)$ is q^3 , the result follows. ■

4 Inclusion of improved codes

As already mentioned our first construction of improved nested code pairs consists of choosing $\tilde{C}(\delta_2)$ and $\tilde{E}(\delta_1)$ such that $\tilde{C}(\delta_2)^\perp \subset \tilde{E}(\delta_1)$. To treat this construction we therefore need a clear picture of the pairs (δ_1, δ_2) of minimum distances that imply this inclusion. We establish this in the present section. As it turns out, the formulas for σ and μ given in Proposition 2.1 mean that several cases must be considered, and each case is presented as a separate proposition.

In the following, quantifiers on λ, ϵ are considered on the domain $H^*(Q)$. Given $\delta_1 \in \sigma(H^*(Q))$, define δ_2^{\max} to be the maximal value of δ_2 such that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ holds. This inclusion is equivalent to

$$\forall \lambda: [(\sigma(\lambda) < \delta_1) \rightarrow (\mu(\lambda) \geq \delta_2)]. \quad (4.13)$$

We first observe that if we can find a $\lambda_1 \in H^*(Q)$ such that

$$[\forall \epsilon > \lambda_1: \mu(\epsilon) \geq \mu(\lambda_1)] \wedge [\forall \epsilon < \lambda_1: \sigma(\epsilon) \geq \delta_1] \quad (4.14)$$

is true, then (4.13) is also true whenever $\delta_2 \leq \mu(\lambda_1)$. In particular, we therefore have

$$\delta_2^{\max} \geq \mu(\lambda_1). \quad (4.15)$$

On the other hand, we immediately see from (4.13) that a $\lambda_2 \in H^*(Q)$ with

$$\sigma(\lambda_2) < \delta_1 \quad (4.16)$$

implies the bound

$$\delta_2^{\max} \leq \mu(\lambda_2). \quad (4.17)$$

In the proofs of each of the following propositions, our strategy therefore is to determine λ_1 and λ_2 satisfying (4.14) and (4.16), respectively, while also satisfying $\mu(\lambda_1) = \mu(\lambda_2)$. From (4.15) and (4.17) it then follows that $\delta_2^{\max} = \mu(\lambda_1)$. Note, however, that λ_1 and λ_2 need not be distinct. If $\lambda_1 = \lambda_2$, we shall simply use λ .

With this strategy in mind, the following lemmas will prove very useful.

Lemma 4.1:

Let $\lambda = iq + j(q+1) \in H^(Q)$, meaning that $0 \leq i < q^2$ and $0 \leq j < q$. In addition, assume that $i \leq q^2 - q$, $i = q^2 - 1$, or $j = 0$. If $\varepsilon \in H^*(Q)$ satisfies $\varepsilon < \lambda$, then $\sigma(\varepsilon) \geq \sigma(\lambda)$.*

Proof:

For both the cases $i < q^2 - q$ and $j = 0$, the claim follows by Lemma A.3. If $i = q^2 - q$, Lemma A.5 implies that $\sigma(\lambda) = \sigma((i+j)q)$, and any $\varepsilon \in H^*(Q)$ satisfying $\lambda > \varepsilon > (i+j)q$ has $\sigma(\varepsilon) \geq \sigma((i+j)q)$ by Lemma A.6. This also holds true for $\varepsilon < (i+j)q$ by the first part of the proof.

Finally, for $i = q^2 - 1$ consider $\varepsilon = i'q + j'(q+1) \in H^*(Q)$ with $\varepsilon < \lambda$. If $q^2 - q \leq i' \leq q^2 - 1$, the claim follows by Lemmas A.4 and A.6. Otherwise, ε is at most $(q^2 - q - 1)q + (q-1)(q+1) = q^3 - q - 1$, meaning that $\sigma(\varepsilon) \geq q+1$ by Lemma A.3. The proof follows by noting that $\sigma(\lambda) \leq q$. ■

Lemma 4.2:

Let $\lambda = iq + j(q+1) \in H^(Q)$, meaning that $0 \leq i < q^2$ and $0 \leq j < q$. In addition, assume that $i \geq q-1$ or $j = 0$. If $\varepsilon \in H^*(Q)$ satisfies $\varepsilon > \lambda$, then $\mu(\varepsilon) \geq \mu(\lambda)$.*

Proof:

This proof is similar to the one of Lemma 4.1. Defining the notation $\lambda' = (q^2 - 1 - i)q + (q-1-j)(q+1)$, the translation of Lemma A.2 into information on μ gives $\mu(\lambda) = n - \lambda'$ whenever

$$i > q-1 \text{ or } j = q-1. \quad (4.18)$$

Additionally, if $\varepsilon \in H^*(Q)$ with $\varepsilon > \lambda$, then $\varepsilon' < \lambda'$ where the ε' is defined in the same way as λ' . This implies that $\mu(\lambda) < \mu(\varepsilon)$ when $\lambda = iq + j(q+1)$ satisfies (4.18). This immediately proves the claim for $i > q-1$.

For $i = q-1$ the μ -equivalent of Lemma A.5 gives $\mu(\lambda) = \mu((i - (q-1-j)) + (q-1)(q+1))$, and any elements between have greater μ -value by the translation of Lemma A.6. The remaining elements greater than λ are covered by the first part of the proof.

The last part of the proof is $j = 0$ and $i < q-1$, which follows the same procedure as the last part of the proof of Lemma 4.1. ■

Proposition 4.3:

Let $2 \leq \delta_1 \leq q$. Then $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ if and only if $\delta_2 \leq q^3 - (\delta_1 - 2)(q+1)$.

Proof:

Let $\lambda' = (q^2 - 1)q + (q - \delta_1)(q + 1)$. We have $\sigma(\lambda') = \delta_1$ by (4.8), and Lemma 4.1 implies that $\sigma(\varepsilon) \geq \delta_1$ for all $\varepsilon < \lambda'$. Additionally, Lemmas A.4 and A.6 yield that $\lambda = \lambda' + q + 1$ is the smallest element in $H^*(Q)$ with a strictly smaller σ -value. Combining this with Lemma 4.2 applied to λ reveals that λ satisfies (4.14). However, (4.16) is satisfied as well since $\sigma(\lambda) < \delta_1$. Thus, $\delta_2^{\max} = \mu(\lambda) = q^3 - (\delta_1 - 2)(q + 1)$. ■

Proposition 4.4:

Let $q < \delta_1 \leq q^2 - q$. Then $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ if and only if

$$\delta_2 \leq \begin{cases} q^3 - q^2 + q - \delta_1 + 2 & \text{if } 0 \leq b \leq a \\ q^3 - q^2 - a(q + 1) & \text{if } b > a \end{cases}$$

where $\delta_1 - (q + 1) = aq + b$ for $a \geq 0$ and $0 \leq b < q$.

Proof:

First, observe that $aq + b \leq (q - 3)q + (q - 1)$, meaning that a is at most $q - 3$.

Assume that $b = 0$. Then $\lambda = (q^2 - 1 - a)q$ has $\sigma(\lambda) = \delta_1 - 1$, meaning that it satisfies (4.16). Note that $\mu(\lambda) = q^3 - q^2 - aq + 1$, which can be rewritten to obtain the claimed expression.

If $0 < b \leq a$, we can use $\lambda = (q^2 - q - 1 - a + (b - 1))q + (q - 1 - (b - 1))(q + 1)$, which satisfies (4.16) since $\sigma(\lambda) = \delta_1 - 1$. Here, we see that

$$\mu(\lambda) = q^3 - q^2 - aq - b + 1 = q^3 - q^2 + q - \delta_1 + 2.$$

Finally, for $b > a$ we can let $\lambda = (q^2 - q - 1)q + (q - 1 - a)(q + 1)$ with $\sigma(\lambda) = (a + 1)q + a + 1 < \delta_1$. Again, λ satisfies (4.16). Calculating the value of μ gives $\mu(\lambda) = q^3 - q^2 - a(q + 1)$.

In all three of the above situations, the element immediately preceding λ in $H^*(Q)$ is given by $\lambda' = \lambda - 1$, and the reader may verify that $\sigma(\lambda') \geq \delta_1$. In each case applying Lemma 4.1 to λ' implies that $\sigma(\varepsilon) \geq \delta_1$ for all $\varepsilon < \lambda$. Lemma 4.2 applied to λ then shows that λ satisfies (4.14) as well. In conclusion, the specified values of λ satisfy both (4.14) and (4.16), and computing each value of $\mu(\lambda)$ gives the expression in the proposition. ■

Proposition 4.5:

Let $q^2 - q < \delta_1 \leq q^3 - 2q^2 + 2q$. Then $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ if and only if $\delta_2 \leq q^3 - q^2 + q + 2 - \delta_1$.

Proof:

Set $\lambda' = n - \delta_1$ and observe that $\lambda' \geq 2q^2 - 2q = 4g$ where g is the genus of the Hermitian function field. Thus, λ' is a non-gap in $H^*(Q)$, and $\sigma(\lambda') = \delta_1$ by (4.8). Lemma 4.1 implies that any smaller element of $H^*(Q)$ has σ -value at least δ_1 . We see, however, that $\lambda = \lambda' + 1$ has $\sigma(\lambda) = \delta_1 - 1$, and it must be the

smallest such value. At the same time it meets the requirements of Lemma 4.2, implying that (4.14) is fulfilled. As already noted λ satisfies (4.16) as well, meaning that $\delta_2^{\max} = \mu(\lambda) = q^3 - q^2 + q + 2 - \delta_1$. ■

Proposition 4.6:

Let $q^3 - 2q^2 + 2q < \delta_1 \leq q^3 - q^2$. Then $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ if and only if

$$\delta_2 \leq \begin{cases} (a+1)q + b + 2 & \text{if } b < a \\ (a+2)q & \text{if } a \leq b < q-1 \\ (a+2)q + 1 & \text{if } b = q-1 \end{cases}$$

where $q^3 - q^2 - \delta_1 = aq + b$ for $a \geq 0$ and $0 \leq b < q$.

Proof:

First note that $aq + b \leq (q-2)q$, implying that a is at most $q-2$. Assume that $b < a$ and let $\lambda = (q+a-(b+1))q + (b+1)(q+1)$. This element satisfies the requirements of Lemma 4.2, and $\lambda-1$ satisfies the requirements of Lemma 4.1. This means that λ fulfils (4.14). Simultaneously, (4.16) is met since $\sigma(\lambda) = \delta_1 - 1$. Thus, $\delta_2^{\max} = \mu(\lambda) = (a+1)q + b + 2$.

Let $a = b$ and $\lambda = (q-1)q + (a+1)(q+1)$. Applying Lemmas 4.1 and 4.2 to $\lambda-1$ and λ as above, we see that λ satisfies (4.14). It also meets (4.16) since $\sigma(\lambda) = \delta_1 - 1$. Subsequently, $\delta_2^{\max} = \mu(\lambda) = (a+2)q$.

Now, consider $a < b < q-1$ and let $\lambda_1 = (q-1)q + (a+1)(q+1)$ and $\lambda_2 = (a+1)q + (q-1)(q+1)$. We can apply both Lemmas 4.1 and 4.2 to λ_1 to obtain that it satisfies (4.14). On the other hand, $\sigma(\lambda_2) < \delta_1$ implies that (4.16) is fulfilled. In addition, $\mu(\lambda_1) = \mu(\lambda_2)$, which gives $\delta_2^{\max} = \mu(\lambda_1) = (a+2)q$.

The remaining part is $b = q-1$. If this happens, note that $\lambda = (q+a+1)q$ has $\sigma(\lambda) = \delta_1 - 1$, whereas $\lambda-1 = (a+1)q + (q-1)(q+1)$ has $\sigma(\lambda-1) = \delta_1$. By the same arguments as in the first part of the proof, we obtain that $\delta_2^{\max} = \mu(\lambda) = (a+2)q + 1$. ■

Proposition 4.7:

Let $q^3 - q^2 \leq \delta_1 \leq q^3$. Then $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ if and only if

$$\delta_2 \leq \begin{cases} a+1 & \text{if } b < a \\ a+2 & \text{if } b \geq a \end{cases}$$

where $q^3 - \delta_1 = aq + b$ for $a \geq 0$ and $0 \leq b < q$.

Proof:

Assume first that $b < a$, and set $\lambda_1 = aq$ and $\lambda_2 = a(q+1)$. The latter meets the assumptions of Lemmas 4.1 and 4.2, meaning that λ_2 satisfies (4.14). Observe that $\sigma(\lambda_1) < \delta_1$ and $\mu(\lambda_1) = \mu(\lambda_2)$. From this we see that $\delta_2^{\max} = \mu(\lambda_1) = a+1$.

II. Papers

Otherwise, if $b \geq a$, let $\lambda = (a+1)q$, which satisfies (4.16) by the observation that $\sigma(\lambda) < \delta_1$. The element of $H^*(Q)$ immediately preceding λ is $\lambda' = a(q+1)$, which has $\sigma(\lambda') \geq \delta_1$. As in the previous proofs, applying Lemmas 4.1 and 4.2 to λ' and λ , respectively, shows that λ fulfils (4.14). Hence, $\delta_2^{\max} = \mu(\lambda) = a + 2$. ■

It is worth noting that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ if and only if every $\lambda \in H^*(Q)$ with $\sigma(\lambda) < \delta_1$ also satisfies $\mu(\lambda) \geq \delta_2$. By Proposition 2.1 this may be rewritten as $\mu(\lambda) < \delta_1$ implying $\sigma(\lambda) \geq \delta_2$. Hence, the inclusion of codes is symmetric in the sense that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ if and only if $\tilde{C}(\delta_1)^\perp \subseteq \tilde{E}(\delta_2)$.

One could expect that this symmetry would show up in Propositions 4.3–4.7 as well. However, this is not the case since the propositions describe the *maximal* value of δ_2 such that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ for a given value of δ_1 . Although this implies that $\tilde{C}(\delta_1)^\perp \subseteq \tilde{E}(\delta_2)$, there may be a $\delta' > \delta_1$ such that $\tilde{C}(\delta')^\perp \subseteq \tilde{E}(\delta_2)$ as shown in Example 4.8 below.

Example 4.8:

Let $q = 4$ and set $\delta_1 = 6$. Then considering the values of σ and μ as given in Table 4 of the Appendix reveals that the greatest possible value of δ_2 such that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$ is given by $\delta_2 = 48$. By the observations above we know that this implies $\tilde{C}(6)^\perp \subseteq \tilde{E}(48)$ as well. However, inspecting the tables again will reveal that the $\tilde{C}(8)^\perp$ is also a subset of $\tilde{E}(48)$. Notice that both of these observations agree with the formulas in Propositions 4.4 and 4.6. ◀

5 Improved nested codes of not too small codimension

Based on our findings in Sections 3 and 4, we are now able to describe the parameters of our first construction of nested code pairs, namely the one where the codimension is not too small. If $\delta_1, \delta_2 \in H^*(Q)$ satisfy the conditions in one of the Propositions 4.3–4.7, it follows that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$. By the bounds (4.4) and (4.5) and the observation following Proposition 2.1, the relative distance of this code pair is exactly $d(\tilde{E}(\delta_1)) = \delta_1$, and the relative distance of its dual is $d(\tilde{C}(\delta_2)^\perp) = \delta_2$.

For each possible pair of designed distances described in Propositions 4.3–4.7, we can combine the dimensions of the usual Hermitian codes with the dimension bounds of Propositions 3.2 and 3.3. This gives bounds on the codimension, ℓ , of $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$.

Proposition 5.1:

Let $\delta_1, \delta_2 \in H^*(Q)$, and $\delta_1 \leq q$. Further, let δ_2 satisfy the conditions of Proposition 4.3, meaning that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$. Denote their codimension by ℓ .

If $\delta_2 \leq q$, then

$$\ell \geq q^3 - \lfloor \delta_1 + \delta_1 \ln(\delta_1) \rfloor - \lfloor \delta_2 + \delta_2 \ln(\delta_2) \rfloor.$$

If $q < \delta_2 \leq q^2 - q$, then

$$\begin{aligned} \ell \geq q^3 + q^2 - g + 1 - \lfloor \delta_1 + \delta_1 \ln(\delta_1) \rfloor - \delta_2 - \sum_{s=0}^{a+b} (s+1) \\ - \lfloor \delta_2 + \delta_2 \ln(q^2/\delta_2) \rfloor + \max\{a, 0\} \end{aligned}$$

where a and b are as in Proposition 3.2 applied to δ_2 .

If $q^2 - q < \delta_2 < q^3 - 2g + 2$, then

$$\ell \geq q^3 - g + 1 - \lfloor \delta_1 + \delta_1 \ln(\delta_1) \rfloor - \delta_2.$$

Finally, if $q^3 - 2g + 2 \leq \delta_2$, we have

$$\ell \geq \sum_{s=0}^{a+b} (s+1) - \lfloor \delta_1 + \delta_1 \ln(\delta_1) \rfloor - \max\{a, 0\}$$

where $q^3 - \delta_2 = aq + b(q+1)$ for $-q < a < q$ and $0 \leq b < q$.

Proof:

By Proposition 3.3 we have $\dim \tilde{E}(\delta_1) \geq q^3 - \lfloor \delta_1 + \delta_1 \ln(\delta_1) \rfloor$. In each case, we can obtain a bound on the codimension ℓ by subtracting an upper bound on $\tilde{C}(\delta_2)^\perp = q^3 - \dim \tilde{E}(\delta_2)$. In turn, such a bound can be obtained via a lower bound on $\dim \tilde{E}(\delta_2)$.

In the case $\delta_2 \leq q$ the dimension of $\tilde{E}(\delta_2)$ can again be bounded by Proposition 3.3. In the second case the bound on $\dim \tilde{E}(\delta_2)$ follows by Proposition 3.2. Proposition 2.3 delivers the bounds in the two final cases. ■

Proposition 5.2:

Let $\delta_1, \delta_2 \in H^*(Q)$ and $q < \delta_1 \leq q^2 - q$. Further, let δ_2 satisfy the conditions of Proposition 4.3, meaning that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$. Denote their codimension by ℓ and let a_1, b_1 be as in Proposition 3.2 applied to δ_1 .

If $\delta_2 \leq q$, then

$$\begin{aligned} \ell \geq q^3 + q^2 - g + 1 - \delta_1 - \sum_{s=0}^{a_1+b_1} (s+1) + \max\{a_1, 0\} \\ - \lfloor \delta_1 + \delta_1 \ln(q^2/\delta_1) \rfloor - \lfloor \delta_2 + \delta_2 \ln(\delta_2) \rfloor. \end{aligned}$$

If $q < \delta_2 \leq q^2 - q$, then

$$\begin{aligned} \ell \geq q^3 + 2q^2 - 2g + 2 - (\delta_1 + \delta_2) - \sum_{s=0}^{a_1+b_1} (s+1) + \max\{a_1, 0\} \\ - \sum_{s=0}^{a_2+b_2} (s+1) + \max\{a_2, 0\} - \lfloor \delta_1 + \delta_1 \ln(q^2/\delta_1) \rfloor - \lfloor \delta_2 + \delta_2 \ln(q^2/\delta_2) \rfloor \end{aligned}$$

II. Papers

where a_2 and b_2 are as in Proposition 3.2 applied to δ_2 .

Finally, if $q^2 - q < \delta_2$, then

$$\ell \geq q^3 + q^2 - 2g + 2 - (\delta_1 + \delta_2) - \sum_{s=0}^{a_1+b_1} (s+1) - \lfloor \delta_1 + \delta_1 \ln(q^2/\delta_1) \rfloor + \max\{a_1, 0\}.$$

Proof:

We use the same strategy as in the proof of Proposition 5.1. A bound for the dimension of $\tilde{E}(\delta_1)$ can be found in Proposition 3.2. For $\delta_2 \leq q$ the bound on $\dim \tilde{E}(\delta_2)$ comes from Proposition 3.3, and in the case $q < \delta_2 \leq q^2 - q$ it comes from Proposition 3.2. In the final case the bound follows from Proposition 2.3, where we note that $\delta_2 \leq q^3 - 2g + 2$ by Proposition 4.4 and the assumption on δ_1 . ■

Proposition 5.3:

Let $\delta_1, \delta_2 \in H^*(Q)$ and $q^2 - q < \delta_1 < q^3 - 2g + 2$. Further, let δ_2 satisfy the conditions of Proposition 4.3, meaning that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$. Denote their codimension by ℓ .

If $\delta_2 \leq q$, we have

$$\ell \geq q^3 - g + 1 - \delta_1 - \lfloor \delta_2 + \delta_2 \ln(\delta_2) \rfloor.$$

If $q < \delta_2 \leq q^2 - q$, then

$$\ell \geq q^3 + q^2 - 2g + 2 - (\delta_1 + \delta_2) - \sum_{s=0}^{a+b} (s+1) - \lfloor \delta_2 + \delta_2 \ln(q^2/\delta_2) \rfloor + \max\{a, 0\}$$

where a and b are as in Proposition 3.2 applied to δ_2 .

Finally, for $q^2 - q < \delta_2$ we have

$$\ell = q^3 - \delta_1 - \delta_2 - 2g + 2.$$

Proof:

Again, the the strategy is the same as in the proof of Proposition 5.1. The exact dimension of $\tilde{E}(\delta_1)$ is given by Proposition 2.3. For $\delta_2 \leq q$ the dimension of $\tilde{E}(\delta_2)$ can be bounded by applying Proposition 3.3, and in the case $q < \delta_2 \leq q^2 - q$ the bound follows by Proposition 3.2. For the final case we note by Proposition 4.5 that $\delta_2 < q^3 - q^2 + q + 2 - (q^2 - q) = q^3 - 4g + 2$. Hence, the exact dimension of $\tilde{E}(\delta_2)$ is given by the first part of Proposition 2.3 in this case. ■

Proposition 5.4:

Let $\delta_1, \delta_2 \in H^*(Q)$ and $q^3 - 2g + 2 \leq \delta_1$. Further, let δ_2 satisfy the conditions of Proposition 4.3, meaning that $\tilde{C}(\delta_2)^\perp \subseteq \tilde{E}(\delta_1)$. Denote their codimension by ℓ . Then

$$\ell \geq \sum_{s=0}^{a+b} (s+1) - \max\{a, 0\} - \lfloor \delta_2 + \delta_2 \ln(\delta_2) \rfloor$$

where $q^3 - \delta_1 = aq + b(q+1)$ for $-q < a < q$ and $0 \leq b < q$.

Proof:

The dimension of $\tilde{E}(\delta_1)$ is given by the last part of Proposition 2.3. To obtain a bound on the maximal value of δ_2 , note that the minimal value of $q^3 - \delta_1$ can be written as $q^2 - q - 2 = q(q-2) + (q-2)$. Proposition 4.7 now implies $\delta_2 \leq q$. Hence, $\dim \tilde{E}(\delta_2) \geq q^3 - \lfloor \delta_2 + \delta_2 \ln(\delta_2) \rfloor$ by Proposition 3.3. ■

The application of Theorem 1.1 or 1.2 translates Propositions 5.1–5.4 into information on improved linear ramp secret sharing schemes and improved asymmetric quantum codes, respectively. The details are left for the reader.

6 Improved information on nested codes of small codimension

We will now consider a second construction which in general gives nested code pairs of smaller codimension than the construction in Section 5. This construction bears some resemblance to the one given in [GGHR18; Sec. IV], but in the setting of Hermitian codes.

From the definition of the codes, $C_{\mathcal{L}}(D, \lambda_2 Q) \subsetneq C_{\mathcal{L}}(D, \lambda_1 Q)$ whenever $\lambda_2 < \lambda_1$ and both λ_1 and λ_2 belongs to $H^*(Q)$. Our second construction is captured by the following two propositions.

Proposition 6.1:

Let $\lambda_1 = iq + j(q+1) \in H^*(Q)$ where $i \leq j < q$, and define $\lambda_2 = jq + i(q+1) - 1$. Then $C_{\mathcal{L}}(D, \lambda_2 Q) \subsetneq C_{\mathcal{L}}(D, \lambda_1 Q)$ have codimension $\ell = j - i + 1$, and their relative distances satisfy

$$d(C_{\mathcal{L}}(D, \lambda_1 Q), C_{\mathcal{L}}(D, \lambda_2 Q)) = q^3 - \lambda_1 = d(C_{\mathcal{L}}(D, \lambda_1 Q)), \quad (4.19)$$

and

$$d(C_{\mathcal{L}}(D, \lambda_2 Q)^\perp, C_{\mathcal{L}}(D, \lambda_1 Q)^\perp) = (i+1)(j+1) \geq d(C_{\mathcal{L}}(D, \lambda_2 Q)^\perp). \quad (4.20)$$

The inequality in (4.20) is strict if and only if $i \neq 0$ and $j \neq q-1$.

Proof:

The codimension of $C_{\mathcal{L}}(D, \lambda_1 Q)$ and $C_{\mathcal{L}}(D, \lambda_2 Q)$ is given by the number of elements ε in $H^*(Q)$ with $\lambda_2 < \varepsilon \leq \lambda_1$. By (4.6) $H^*(Q)$ contains every integer between λ_2 and λ_1 , meaning that the codimension is exactly $\lambda_1 - \lambda_2 = j - i + 1$.

To prove the first equalities in (4.19) and (4.20), we use Proposition 2.1 to obtain $\sigma(\lambda_1) = q^3 - \lambda_1$ and $\mu(\lambda_2) = (i+1)(j+1)$. Applying (4.4) and (4.5) then implies that the relative distances are at least $q^3 - \lambda_1$ and $(i+1)(j+1)$, respectively. That these are indeed equalities follows from the observations following Proposition 2.1.

In (4.19) the last equality follows from the last part of Proposition 2.1. For (4.20) the observations in [Gei03; Rem. 4] imply that (4.3) is in fact an equality.

II. Papers

Thus, the minimal distance of $d(C_{\mathcal{L}}(D, \lambda_2 Q)^\perp)$ is given by $\mu((i+j)(q+1)) = i+j+1$ if $i+j < q$ and

$$\mu((i - (q-1-j))q + (q-1)(q+1)) = q(i+j-q+2)$$

otherwise. In the first case equality with $(i+1)(j+1)$ occurs if and only if $i = 0$, and in the second if and only if $j = q-1$. ■

In the above construction we only consider values of i less than q . A similar technique can be used for $q^2 - q \leq i < q^2$. We state the proposition, but omit the proof since it follows by similar arguments as above.

Proposition 6.2:

Let $\lambda_1 = (q^2 - 1 - i)q + (q - 1 - j)(q + 1) \in H^*(Q)$ where $i \leq j < q$, and define $\lambda_2 = (q^2 - 1 - j)q + (q - 1 - i)(q + 1) - 1$. Then $C_{\mathcal{L}}(D, \lambda_2 Q) \subsetneq C_{\mathcal{L}}(D, \lambda_1 Q)$ have codimension $\ell = j - i + 1$, and their relative distances satisfy

$$d(C_{\mathcal{L}}(D, \lambda_1 Q), C_{\mathcal{L}}(D, \lambda_2 Q)) = (i+1)(j+1) \geq d(C_{\mathcal{L}}(D, \lambda_1 Q)), \quad (4.21)$$

and

$$d(C_{\mathcal{L}}(D, \lambda_2 Q)^\perp, C_{\mathcal{L}}(D, \lambda_1 Q)^\perp) = q^3 - iq - j(q+1) = d(C_{\mathcal{L}}(D, \lambda_2 Q)^\perp).$$

The inequality in (4.21) is strict if $i \neq 0$ and $j \neq q-1$.

By applying one of Theorems 1.1 and 1.2, we can transform Propositions 6.1 and 6.2 into information on improved linear ramp secret sharing schemes and improved asymmetric quantum codes, respectively. The details of this translation are left for the reader.

7 Comparison with bounds and existing constructions

Having presented two improved constructions of nested code pairs in Sections 5 and 6, this section is devoted to the comparison between the corresponding asymmetric quantum codes and codes that already exist in the literature. The codes are also compared with the Gilbert-Varshamov bound for asymmetric quantum codes. Moreover, we compare the corresponding secret sharing schemes with a recent lower bound on the threshold gap [CSR19]. When presenting code parameters we give the actual codimension rather than using the estimates in Section 5 which rely on the bounds in Propositions 3.2 and 3.3.

Since the codes obtained in Sections 5 and 6 are relatively long compared to the field size, the literature does not contain many immediately comparable codes. Yet, one way to obtain such codes is by using Construction II of La Guardia [LaG12b; Thm. 7.1], which gives asymmetric quantum generalized Reed-Solomon codes. Adjusting the theorem to codes over \mathbb{F}_{q^2} gives the following result.

Theorem 7.1:

Let q be a prime power. There exist asymmetric quantum generalized Reed-Solomon codes with parameters

$$[[m_1 m_2, m_1(2k - m_2 + c), \geq d / \geq d - c]]_{q^2}$$

where $1 < k < m_2 < 2k + c \leq q^{2m_1}$ and $k = m_2 - d + 1$, and where $m_2, d > c + 1$, $c \geq 1$, and $m_1 \geq 1$ are integers.

Example 7.2:

By using different values for the parameters in Theorem 7.1, we obtain asymmetric quantum codes of varying lengths. If the chosen parameters give a code of length less than q^3 , we can pad each codeword with zeroes in order to obtain the correct length. Note that this does not change the relative distance of the nested codes nor of their duals.

For $q = 3$ Table 1 lists the best code parameters that can be obtained in this way together with the comparable codes from the constructions in Sections 5 and 6. In the third column, the parameter d_z is maximized under the condition that the dimension and the distance d_x are at least as high as in [LaG12b]. In the fourth, the dimension is maximized, keeping at least the same minimal distances. As is evident, the codes of the present paper perform very favourably.

We further note that all presented new codes exceed the Gilbert-Varshamov bound for asymmetric quantum codes [Mat17; Thm. 4]. Additionally, we remark that nesting usual one-point Hermitian codes and using the Goppa bound does not provide asymmetric quantum codes as good as the ones in columns three and four. ◀

The two constructions in Theorem 24 and Corollary 29 of [GGHR18] based on codes defined from Cartesian product point sets provide another way to obtain asymmetric quantum codes that can be compared to the ones in this paper. We summarize these constructions in the following two theorems.

Theorem 7.3:

Consider integers $m \geq 2$ and $s \leq q$ where q is a prime power. Given $\delta_1 \in \{1, 2, \dots, s^m\}$ define $v \in \{0, 1, \dots, m-1\}$ such that $s^v \leq \delta \leq s^{v+1}$, and choose an integer $\delta_2 \leq \lfloor (s - \delta_1/s^v + 1)s^{m-v+1} \rfloor$. Then there exists an asymmetric quantum code with parameters

$$[[s^m, \ell, \delta_1/\delta_2]]_q$$

where

$$\ell \geq s^m - \sum_{t=1}^m \frac{1}{(t-1)!} \left(\delta_1 \left(\ln \left(\frac{s^m}{\delta_1} \right) \right)^{t-1} + \delta_2 \left(\ln \left(\frac{s^m}{\delta_2} \right) \right)^{t-1} \right).$$

II. Papers

Theorem 7.4:

Consider integers $1 < s \leq q$ where q is a prime power, and let $m \in \{0, 1, \dots, s-1\}$. Then for any $\ell \leq m+1$ such that ℓ is even if and only if m is odd, there exists an asymmetric quantum code with parameters

$$[[s^2, \ell, d_z/d_x]]_q$$

where the distances are $d_z = \frac{1}{4}(2s - (m - \ell + 1))(2s - (m + \ell - 1))$ and $d_x = \frac{1}{4}(m - \ell + 3)(m + \ell + 1)$. The two distances may also be interchanged.

Construction of [LaG12b; Thm. 7.1]		This paper	
(m_1, m_2, k, c)	Code	d_z maximized	ℓ maximized
(2, 13, 2, 10)	[[27, 2, 12/2]] ₉	[[27, 2, 23/2]] ₉	[[27, 12, 12/2]] ₉
(2, 13, 3, 8)	[[27, 2, 11/3]] ₉	[[27, 2, 18/4]] ₉	[[27, 11, 11/3]] ₉
(2, 13, 4, 6)	[[27, 2, 10/4]] ₉	[[27, 2, 18/4]] ₉	[[27, 10, 10/4]] ₉
(2, 13, 5, 4)	[[27, 2, 9/5]] ₉	[[27, 2, 16/6]] ₉	[[27, 9, 9/6]] ₉
(2, 13, 6, 2)	[[27, 2, 8/6]] ₉	[[27, 2, 16/6]] ₉	[[27, 10, 8/6]] ₉
(3, 9, 3, 4)	[[27, 3, 7/3]] ₉	[[27, 3, 19/3]] ₉	[[27, 15, 7/3]] ₉
(3, 9, 4, 2)	[[27, 3, 6/4]] ₉	[[27, 3, 17/4]] ₉	[[27, 15, 6/4]] ₉
(2, 13, 3, 9)	[[27, 4, 11/2]] ₉	[[27, 4, 20/2]] ₉	[[27, 13, 11/2]] ₉
(2, 13, 4, 7)	[[27, 4, 10/3]] ₉	[[27, 4, 18/3]] ₉	[[27, 12, 10/3]] ₉
(2, 13, 5, 5)	[[27, 4, 9/4]] ₉	[[27, 4, 16/4]] ₉	[[27, 11, 9/4]] ₉
(2, 13, 6, 3)	[[27, 4, 8/5]] ₉	[[27, 4, 14/6]] ₉	[[27, 10, 8/6]] ₉
(2, 13, 7, 1)	[[27, 4, 7/6]] ₉	[[27, 4, 14/6]] ₉	[[27, 11, 7/6]] ₉
(2, 13, 4, 8)	[[27, 6, 10/2]] ₉	[[27, 6, 18/2]] ₉	[[27, 14, 10/2]] ₉
(2, 13, 5, 6)	[[27, 6, 9/3]] ₉	[[27, 6, 16/3]] ₉	[[27, 13, 9/3]] ₉
(2, 13, 6, 4)	[[27, 6, 8/4]] ₉	[[27, 6, 14/4]] ₉	[[27, 12, 8/4]] ₉
(2, 13, 7, 2)	[[27, 6, 7/5]] ₉	[[27, 6, 12/6]] ₉	[[27, 11, 7/6]] ₉
(2, 13, 5, 7)	[[27, 8, 9/2]] ₉	[[27, 8, 16/2]] ₉	[[27, 15, 9/2]] ₉
(2, 13, 6, 5)	[[27, 8, 8/3]] ₉	[[27, 8, 14/3]] ₉	[[27, 14, 8/3]] ₉
(2, 13, 7, 3)	[[27, 8, 7/4]] ₉	[[27, 8, 12/4]] ₉	[[27, 13, 7/4]] ₉
(2, 13, 8, 1)	[[27, 8, 6/5]] ₉	[[27, 8, 10/6]] ₉	[[27, 13, 6/6]] ₉
(2, 13, 6, 6)	[[27, 10, 8/2]] ₉	[[27, 10, 14/2]] ₉	[[27, 16, 8/2]] ₉
(2, 13, 7, 4)	[[27, 10, 7/3]] ₉	[[27, 10, 12/3]] ₉	[[27, 15, 7/3]] ₉
(2, 13, 8, 2)	[[27, 10, 6/4]] ₉	[[27, 10, 10/4]] ₉	[[27, 15, 6/4]] ₉
(2, 13, 7, 5)	[[27, 12, 7/2]] ₉	[[27, 12, 12/2]] ₉	[[27, 17, 7/2]] ₉
(2, 13, 8, 3)	[[27, 12, 6/3]] ₉	[[27, 12, 10/3]] ₉	[[27, 17, 6/3]] ₉
(2, 13, 9, 1)	[[27, 12, 5/4]] ₉	[[27, 12, 8/4]] ₉	[[27, 15, 6/4]] ₉
(2, 13, 8, 4)	[[27, 14, 6/2]] ₉	[[27, 14, 10/2]] ₉	[[27, 19, 6/2]] ₉
(2, 13, 9, 2)	[[27, 14, 5/3]] ₉	[[27, 14, 8/3]] ₉	[[27, 14, 8/3]] ₉
(2, 13, 9, 3)	[[27, 16, 5/2]] ₉	[[27, 16, 8/2]] ₉	[[27, 19, 6/2]] ₉
(2, 13, 10, 1)	[[27, 16, 4/3]] ₉	[[27, 17, 6/3]] ₉	[[27, 19, 4/3]] ₉
(2, 13, 10, 2)	[[27, 18, 4/2]] ₉	[[27, 19, 6/2]] ₉	[[27, 21, 4/2]] ₉
(2, 13, 11, 1)	[[27, 20, 3/2]] ₉	[[27, 21, 4/2]] ₉	[[27, 23, 3/2]] ₉

Table 1. Asymmetric quantum codes of length 27 over \mathbb{F}_9 . The first column states the parameters used in Theorem 7.1 to obtain the codes in the second. If necessary, these have been padded with zeroes to obtain length 27. The codes in the third and fourth columns are based on the construction in Sections 5 and 6.

Example 7.5:

By using different parameters in Theorems 7.3 and 7.4 and padding with zeroes if necessary, we obtain the asymmetric quantum codes presented in Table 2. This table also shows comparable codes from the constructions in Sections 5 and 6 which have either d_z or ℓ maximized as in Example 7.2. From the table it is evident that the codes of the present paper perform very favourably.

Again, we further note that all presented new codes exceed the Gilbert-Varshamov bound [Mat17; Thm. 4], and that these codes cannot be constructed using information from the Goppa bound applied to nested one-point Hermitian codes. ◀

Example 7.6:

A few codes of length 8 over \mathbb{F}_4 are given in [EJS15]. The construction in Section 5 can match – but not improve on – the codes $[[8, 1, 4/3]]_4$, $[[8, 2, 5/2]]_4$, $[[8, 2, 3/3]]_4$, $[[8, 3, 4/2]]_4$, and $[[8, 4, 3/2]]_4$. Additionally, [EJS15] presents a code with parameters $[[8, 1, 6/2]]_4$, where we can construct an $[[8, 1, 4/3]]_4$ -code instead. All of these codes exceed the quantum Gilbert-Varshamov bound [Mat17; Thm. 4], and the Goppa bound applied to nested one-point Hermitian codes cannot provide such parameters.

Some codes over \mathbb{F}_9 are presented as well. These codes do, however, have a length that is at least 36. ◀

When presenting constructions of codes, it is customary to compare it to tables of ‘best known’ linear codes such as [Gra18; SS18]. Unfortunately, similar tables do not exist for asymmetric quantum codes. As we shall recall in a moment, however, one can still measure asymmetric quantum codes against the usual bounds on linear codes.

Before doing so, we observe that the tables in [Gra18] only contains alphabets up to \mathbb{F}_9 , whereas [SS18] has \mathbb{F}_{256} as its largest alphabet. As indicated by the following example, however, the latter tables are generally not as optimized as the ones by [Gra18].

Example 7.7:

In some cases the improved codes $\tilde{E}(\delta)$ exceed the codes given by [SS18]. For instance, when considering codes over \mathbb{F}_{16} , the codes $\tilde{E}(12)$, $\tilde{E}(9)$, and $\tilde{E}(8)$ with parameters $[64, 48, 12]_{16}$, $[64, 51, 9]_{16}$, and $[64, 53, 8]_{16}$, respectively, all provide a minimal distance that is one higher than the corresponding code in the table.

Over \mathbb{F}_{25} the same is true for the codes $\tilde{E}(20)$, $\tilde{E}(16)$, and $\tilde{E}(12)$, which have parameters $[125, 97, 20]_{25}$, $[125, 101, 16]_{25}$, and $[125, 106, 12]_{25}$. Additionally, $\tilde{E}(15)$ has parameters $[125, 103, 15]_{25}$, exceeding the table distance by 2. ◀

Recall from Section 6 that our second construction of nested code pairs

II. Papers

(which are code pairs of small codimension) gives impure asymmetric quantum codes. This is already an advantage as the error-correcting algorithms can take advantage of the impurity. Another advantage of considering relative distances rather than only minimal distances emerges when analysing the error-correcting ability of asymmetric quantum codes. In order to illustrate this advantage, we can compare nested codes from the construction in Section 6 with pairs of best known linear codes from the tables in [Gra18; SS18]. Note that the pairs of best known linear codes from such tables generally do not result in nested code pairs; that is, they are not guaranteed to satisfy the requirement that the dual of one code is contained in the other. The comparison with tables of best known linear codes is done in the following example. Whenever the tables of [SS18] are considered, we will use the minimum distance of an improved algebraic geometric Goppa code from the Hermitian curve if this exceeds the table value as in Example 7.7.

Example 7.8:

Having fixed a code pair $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ of codimension ℓ and $d(C_1) = \delta_1$, we consider the greatest value $g(\ell, \delta)$ such that the tables of best known linear codes ensure the existence of $C, C' \subseteq \mathbb{F}_q^n$ with $\dim C - \dim C' = \ell$, $d(C) = \delta_1$, and $d(C'^\perp) \geq g(\ell, \delta_1)$. This is the same method as used in [GGHR18], and bears resemblance to the idea in [EJS15; Thm. 2]. Using this procedure it is in no way guaranteed that $C' \subset C$. However, as shown in Table 3 the construction in Section 6 is in many cases on par with the best known codes, while simultaneously guaranteeing the inclusion $C_2 \subset C_1$. In some cases the use of relative distances will even exceed the values obtained from the best known codes. As in the previous examples, the codes in Table 3 all exceed the Gilbert-Varshamov bound for asymmetric quantum codes [Mat17; Thm. 4]. ◀

Turning to secret sharing schemes, [CSR19] presents a lower bound on the threshold gap $r - t$. That is, the authors bound the smallest possible difference between the reconstruction number r and the privacy number t for q -ary linear ramp secret sharing schemes with n shares and secrets from \mathbb{F}_q^ℓ . For linear ramp secret sharing schemes over \mathbb{F}_{q^2} , they show that

$$r \geq t + \frac{(q^{2m} - 1)(n + 2) + (q^{2m+2} - q^{2m})(\ell - 2m)}{q^{2m+2} - 1} \quad (4.22)$$

for every $m \in \{0, 1, \dots, \ell - 1\}$. Of course, one should choose the m that gives the best bound. Comparing the secret sharing schemes obtained in this paper with the bound (4.22) helps to quantify how optimal the construction is. This is done in the following example, which also illustrates the advantage of using the improved codes from Section 5 and the improved information from Section 6 rather than relying solely on the Goppa bound applied to nested one-point Hermitian codes.

Constructions of [GGHR18]			This paper	
Type	(s, m)	Code	d_z maximized	ℓ maximized
Thm. 7.4	(5, 2)	$[[27, 1, 16/4]]_9$	$[[27, 1, 20/4]]_9$	$[[27, 4, 16/4]]_9$
Thm. 7.4	(5, 4)	$[[27, 1, 9/9]]_9$	$[[27, 1, 13/9]]_9$	$[[27, 5, 9/9]]_9$
Thm. 7.4	(5, 1)	$[[27, 2, 20/2]]_9$	$[[27, 2, 23/2]]_9$	$[[27, 4, 20/2]]_9$
Thm. 7.4	(5, 3)	$[[27, 2, 12/6]]_9$	$[[27, 2, 16/6]]_9$	$[[27, 6, 12/6]]_9$
Thm. 7.4	(5, 2)	$[[27, 3, 15/3]]_9$	$[[27, 3, 19/3]]_9$	$[[27, 7, 15/3]]_9$
Thm. 7.4	(5, 4)	$[[27, 3, 8/8]]_9$	$[[27, 3, 12/8]]_9$	$[[27, 7, 8/8]]_9$
Thm. 7.4	(5, 3)	$[[27, 4, 10/4]]_9$	$[[27, 4, 16/4]]_9$	$[[27, 10, 10/4]]_9$
Thm. 7.3	(5, 2)	$[[27, 5, 7/1]]_9$	$[[27, 5, 19/2]]_9$	$[[27, 17, 7/2]]_9$
Thm. 7.4	(5, 4)	$[[27, 5, 5/5]]_9$	$[[27, 5, 13/6]]_9$	$[[27, 13, 6/6]]_9$
Thm. 7.3	(5, 2)	$[[27, 7, 6/1]]_9$	$[[27, 7, 17/2]]_9$	$[[27, 19, 6/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 7, 4/2]]_9$	$[[27, 7, 17/2]]_9$	$[[27, 21, 4/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 7, 3/3]]_9$	$[[27, 7, 15/3]]_9$	$[[27, 21, 3/3]]_9$
Thm. 7.3	(5, 2)	$[[27, 8, 5/1]]_9$	$[[27, 8, 16/2]]_9$	$[[27, 19, 6/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 9, 3/2]]_9$	$[[27, 9, 15/2]]_9$	$[[27, 23, 3/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 10, 4/1]]_9$	$[[27, 10, 14/2]]_9$	$[[27, 21, 4/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 11, 2/2]]_9$	$[[27, 11, 13/2]]_9$	$[[27, 25, 2/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 12, 3/1]]_9$	$[[27, 12, 12/2]]_9$	$[[27, 23, 3/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 14, 2/1]]_9$	$[[27, 14, 10/2]]_9$	$[[27, 25, 2/2]]_9$
Thm. 7.3	(5, 2)	$[[27, 17, 1/1]]_9$	$[[27, 17, 7/2]]_9$	$[[27, 25, 2/2]]_9$

Table 2. Asymmetric quantum codes of length 27 over \mathbb{F}_9 . The first column indicates whether Theorem 7.3 or 7.4 was used in the codes given in the third column. The second states the parameters used, except for those that can be read off directly from the code. The codes in the fourth and fifth columns are based on the construction in Sections 5 and 6.

(i, j)	Parameters	$g(\ell, \delta_1)$	(i, j)	Parameters	$g(\ell, \delta_1)$
(2, 2)	$[[27, 1, 13/9]]_9$	9	(4, 4)	$[[125, 1, 81/25]]_{25}$	25
(1, 1)	$[[27, 1, 20/4]]_9$	4	(3, 3)	$[[125, 1, 92/16]]_{25}$	14
(1, 2)	$[[27, 2, 16/6]]_9$	6	(2, 2)	$[[125, 1, 103/9]]_{25}$	–
(0, 1)	$[[27, 2, 23/2]]_9$	2	(1, 1)	$[[125, 1, 114/4]]_{25}$	–
(0, 2)	$[[27, 3, 19/3]]_9$	3	(3, 4)	$[[125, 2, 86/20]]_{25}$	19
(3, 3)	$[[64, 1, 37/16]]_{16}$	16	(2, 3)	$[[125, 2, 97/12]]_{25}$	10
(2, 2)	$[[64, 1, 46/9]]_{16}$	8	(1, 2)	$[[125, 2, 108/6]]_{25}$	–
(1, 1)	$[[64, 1, 55/4]]_{16}$	4	(0, 1)	$[[125, 2, 119/2]]_{25}$	–
(2, 3)	$[[64, 2, 41/12]]_{16}$	12*	(2, 4)	$[[125, 3, 91/15]]_{25}$	13
(1, 2)	$[[64, 2, 50/6]]_{16}$	6	(1, 3)	$[[125, 3, 102/8]]_{25}$	–
(0, 1)	$[[64, 2, 59/2]]_{16}$	2	(0, 2)	$[[125, 3, 113/3]]_{25}$	–
(1, 3)	$[[64, 3, 45/8]]_{16}$	8*	(1, 4)	$[[125, 4, 96/10]]_{25}$	10
(0, 2)	$[[64, 3, 54/3]]_{16}$	3	(0, 3)	$[[125, 4, 107/4]]_{25}$	–
(0, 3)	$[[64, 4, 49/4]]_{16}$	5	(0, 4)	$[[125, 5, 101/5]]_{25}$	6

Table 3. Comparing the asymmetric quantum codes from Section 6 with the best known codes. For $q = 3$ [Gra18] is used, and for the remaining values of q , [SS18] is used. The codes marked in bold exceed $g(\ell, \delta_1)$, and the values of $g(\ell, \delta_1)$ marked with an asterisk stem from the improvements in Example 7.7. A dash indicates that the tables do not contain enough information to determine $g(\ell, \delta_1)$.

Example 7.9:

In each of the plots in Figures 1 and 2 on pages 90 and 91, respectively, a desired privacy number t has been fixed. For each codimension the plots then show the minimal reconstruction number r achievable with the constructions from Sections 5 and 6 when privacy number at least t is required. The plots also show the lower bound in (4.22).

Recall that the codes under consideration have length q^3 , meaning that the four corresponding secret sharing schemes support 27, 64, 125, and 343 participants, respectively. As the plots demonstrate, the constructions of this paper provide secret sharing schemes with parameters that could not be obtained by using nested Hermitian one-point codes and the Goppa bound alone.

We remark that the four given examples use a relatively large privacy parameter t . Yet, it is also possible to obtain improved reconstruction numbers for small values of t . ◀

8 Concluding remarks

In this paper we presented two improved constructions of nested code pairs from the Hermitian curve, and gave a detailed analysis of their performance when applied to the concepts of secret sharing and asymmetric quantum codes. Regarding information leakage in secret sharing we studied the reconstruction number r and the privacy number t , which give information on full recovery and full privacy, respectively. We note that it is possible to obtain information about partial information leakage by studying relative generalized Hamming weights rather than just relative minimum distances [Gei+14; KUM12]. For asymmetric quantum codes we applied the CSS construction. Applying the method of Steane's enlargements [Ste99] is a future research agenda.

9 Acknowledgements

The authors would like to thank Ignacio Cascudo for helpful discussions.

10 References

- [AG08] **H.E. Andersen and O. Geil.** 'Evaluation codes from order domain theory'. In: *Finite Fields Appl.* 14(1) (2008), pp. 92–123. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2006.12.004.
- [CRSS98] **A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane.** 'Quantum error correction via codes over $GF(4)$ '. In: *IEEE Trans. Inf. Theory* 44(4) (1998), pp. 1369–1387. DOI: 10.1109/18.681315.

- [CSR19] **I. Cascudo, J. Skovsted Gundersen and D. Ruano.** ‘Improved Bounds on the Threshold Gap in Ramp Secret Sharing’. In: *IEEE Trans. Inf. Theory* 65(7) (2019), pp. 4620–4633. DOI: 10.1109/TIT.2019.2902151.
- [DP10] **I.M. Duursma and S. Park.** ‘Coset bounds for algebraic geometric codes’. In: *Finite Fields Appl.* 16(1) (2010), pp. 36–55. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2009.11.006.
- [EJLP13] **M.F. Ezerman, S. Jitman, S. Ling and D.V. Pasechnik.** ‘CSS-like constructions of asymmetric quantum codes’. In: *IEEE Trans. Inf. Theory* 59(10) (2013), pp. 6732–6754. DOI: 10.1109/TIT.2013.2272575.
- [EJS15] **M.F. Ezerman, S. Jitman and P. Solé.** ‘Xing–Ling codes, duals of their subcodes, and good asymmetric quantum codes’. In: *Des. Codes Cryptogr.* 75(1) (2015), pp. 21–42. ISSN: 1573-7586. DOI: 10.1007/s10623-013-9885-5.
- [Gei+14] **O. Geil, S. Martin, R. Matsumoto, D. Ruano and Y. Luo.** ‘Relative generalized Hamming weights of one-point algebraic geometric codes’. In: *IEEE Trans. Inf. Theory* 60(10) (2014), pp. 5938–5949. DOI: 10.1109/TIT.2014.2345375.
- [Gei03] **O. Geil.** ‘On codes from norm–trace curves’. In: *Finite Fields Appl.* 9(3) (2003), pp. 351–371. DOI: 10.1016/S1071-5797(03)00010-8.
- [GGHR18] **C. Galindo, O. Geil, F. Hernando and D. Ruano.** ‘Improved Constructions of Nested Code Pairs’. In: *IEEE Trans. Inf. Theory* 64(4) (2018), pp. 2444–2459. DOI: 10.1109/TIT.2017.2755682.
- [GMRT11] **O. Geil, C. Munuera, D. Ruano and F. Torres.** ‘On the order bounds for one-point AG codes’. In: *Adv. Math. Commun.* 5(3) (2011), pp. 489–504. ISSN: 1930-5346. DOI: 10.3934/amc.2011.5.489.
- [Gra18] **M. Grassl.** *Code Tables: Bounds on the parameters of various types of codes.* <http://www.codetables.de>. June 2018.
- [HLP98] **T. Høholdt, J.H. van Lint and R. Pellikaan.** ‘Algebraic Geometry Codes’. In: *Handbook of Coding Theory*. Vol. 1. Elsevier, 1998, pp. 871–961.
- [IM07] **L. Ioffe and M. Mézard.** ‘Asymmetric quantum error-correcting codes’. In: *Phys. Rev. A* 75(3) (2007), p. 032345. DOI: 10.1103/PhysRevA.75.032345.
- [KKKS06] **A. Ketkar, A. Klappenecker, S. Kumar and P.K. Sarvepalli.** ‘Nonbinary stabilizer codes over finite fields’. In: *IEEE Trans. Inf. Theory* 52(11) (2006), pp. 4892–4914. DOI: 10.1109/TIT.2006.883612.
- [KUM12] **J. Kurihara, T. Uyematsu and R. Matsumoto.** ‘Secret Sharing Schemes Based on Linear Codes Can Be Precisely Characterized by the Relative Generalized Hamming Weight’. In: *IEICE Trans. Fundam. Electron. Comput. Sci.* E95.A(11) (2012), pp. 2067–2075. DOI: 10.1587/transfun.E95.A.2067.

II. Papers

- [LaG12a] **G.G. La Guardia.** 'Asymmetric quantum product codes'. In: *Int. J. Quantum Inf.* 10(01) (2012), p. 1250005. ISSN: 0219-7499. DOI: 10.1142/S0219749912500050.
- [LaG12b] **G.G. La Guardia.** 'Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes'. In: *Quantum Inf. Process.* 11(2) (2012), pp. 591-604. DOI: 10.1007/s11128-011-0269-3.
- [Mat17] **R. Matsumoto.** 'Two Gilbert-Varshamov-type existential bounds for asymmetric quantum error-correcting codes'. In: *Quantum Inf. Process.* 16(12) (2017), p. 285. ISSN: 1573-1332. DOI: 10.1007/s11128-017-1748-y.
- [SKR09] **P.K. Sarvepalli, A. Klappenecker and M. Rötteler.** 'Asymmetric quantum codes: constructions, bounds and performance'. In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* Vol. 465. The Royal Society, 2009, pp. 1645-1672. DOI: 10.1098/rspa.2008.0439.
- [SS18] **W.C. Schmid and R. Schürer.** *MinT*. <http://mint.sbg.ac.at/>. June 2018.
- [Ste96] **A.M. Steane.** 'Simple quantum error-correcting codes'. In: *Phys. Rev. A* 54(6) (1996), p. 4741. DOI: 10.1103/PhysRevA.54.4741.
- [Ste99] **A.M. Steane.** 'Enlargement of Calderbank-Shor-Steane quantum codes'. In: *IEEE Trans. Inf. Theory* 45(7) (1999), pp. 2492-2495. ISSN: 0018-9448. DOI: 10.1109/18.796388.
- [Sti88] **H. Stichtenoth.** 'A note on Hermitian codes over $\text{GF}(q^2)$ '. In: *IEEE Trans. Inf. Theory* 34(5) (1988), pp. 1345-1348. DOI: 10.1109/18.21267.
- [Sti93] **H. Stichtenoth.** *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993, pp. x+260. ISBN: 3-540-56489-6.
- [WFLX10] **L. Wang, K. Feng, S. Ling and C. Xing.** 'Asymmetric quantum codes: characterization and constructions'. In: *IEEE Trans. Inf. Theory* 56(6) (2010), pp. 2938-2945. ISSN: 0018-9448. DOI: 10.1109/TIT.2010.2046221.
- [YK92] **K. Yang and P.V. Kumar.** 'On the true minimum distance of Hermitian codes'. In: *Coding theory and algebraic geometry*. Springer, 1992, pp. 99-107. DOI: 10.1007/BFb0087995.

Appendix A Additional results on σ and μ

In this section we state a number of lemmas that are needed in Sections 3 and 4. The lemmas all follow as corollaries to Proposition 2.1. To aid the reader in understanding them more easily, we first give an example for reference.

Example A.1:

In Table 4 we list $H^*(Q)$, $\sigma(H^*(Q))$, and $\mu(H^*(Q))$ for the Hermitian function field over \mathbb{F}_{16} , i.e. for $q = 4$. Entries are ordered according to (i, j) where $\lambda = iq + j(q + 1)$.

15	19	23	27	31	35	39	43	47	51	55	59	63	67	71	75
10	14	18	22	26	30	34	38	42	46	50	54	58	62	66	70
5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65
0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
49	45	41	37	33	29	25	21	17	13	9	5	4	3	2	1
54	50	46	42	38	34	30	26	22	18	14	10	8	6	4	2
59	55	51	47	43	39	35	31	27	23	19	15	12	9	6	3
64	60	56	52	48	44	40	36	32	28	24	20	16	12	8	4
4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64
3	6	9	12	15	19	23	27	31	35	39	43	47	51	55	59
2	4	6	8	10	14	18	22	26	30	34	38	42	46	50	54
1	2	3	4	5	9	13	17	21	25	29	33	37	41	45	49

Table 4. Upper table: $H^*(Q)$. Middle table: $\sigma(H^*(Q))$. Lower table: $\mu(H^*(Q))$

The first lemma explains when (4.2) equals the Goppa bound and when it is sharper.

Lemma A.2:

For all $\lambda = iq + j(q+1) \in H^(Q)$ it holds that $\sigma(\lambda) \geq n - \lambda$ where $n = q^3$. The inequality is strict if and only if $q^2 - q \leq i < q^2$ and $1 \leq j < q\}$.*

The next five lemmas give information on the relation between the values $\sigma(iq + j(q+1))$ and $\sigma(i'q + j'(q+1))$ for different constellations of i, j, i', j' . Using the translation from σ to μ as given in Proposition 2.1, this simultaneously implies relations on μ .

Lemma A.3:

For $0 < i \leq q^2 - q - 1$ and $0 \leq j < q - 1$ it holds that $\sigma(iq + j(q+1)) = \sigma((i-1)q + (j+1)(q+1)) + 1$. Furthermore, for $0 \leq i \leq q^2 - q - 1$ it holds that $\sigma(iq + (q-1)(q+1)) = \sigma((i+q)q) + 1$.

Lemma A.4:

The sequence

$$\begin{aligned} &(\sigma(0 \cdot q), \sigma(q), \dots, \sigma((q^2-1)q), \sigma((q^2-1)q + (q+1)), \\ &\sigma((q^2-1)q + 2(q+1)), \dots, \sigma((q^2-1)q + (q-1)(q+1))) \end{aligned}$$

is strictly decreasing.

Lemma A.5:

We have $\sigma((q^2-q+s)q + t(q+1)) = \sigma((q^2-q+t)q + s(q+1))$ for $0 \leq s, t < q-1$.

II. Papers

Lemma A.6:

Given $q^2 - q \leq i \leq q^2 - 1$ then for non-negative s such that $q^2 - q \leq i - s$ we have $\sigma((i - s)q + s(q + 1)) \geq \sigma(iq)$. Similarly, given $0 \leq j \leq q^2 - 1$ then for non-negative s such that $j + s \leq q - 1$ we have $\sigma((q^2 - 1 - s)q + (j + s)(q + 1)) \geq \sigma((q^2 - 1)q + j(q + 1))$.

Lemma A.7:

If $\sigma(iq + j(q + 1)) \leq q$ then $q^2 - q \leq i < q^2$.

Finally, we present a lemma on the relation between $\sigma(\lambda)$ and $\mu(\lambda)$ for λ belonging to a certain window.

Lemma A.8:

For $\lambda = iq + j(q + 1) \in H^*(Q)$ with $q \leq i < q^2 - q$ and j arbitrary; or $q^2 - q < i \leq q^2 - 1$ and $j = 0$; or $0 \leq i < q$ and $j = q - 1$, we have $\mu(\lambda) + \sigma(\lambda) = q^3 - (q^2 - q - 1)$.

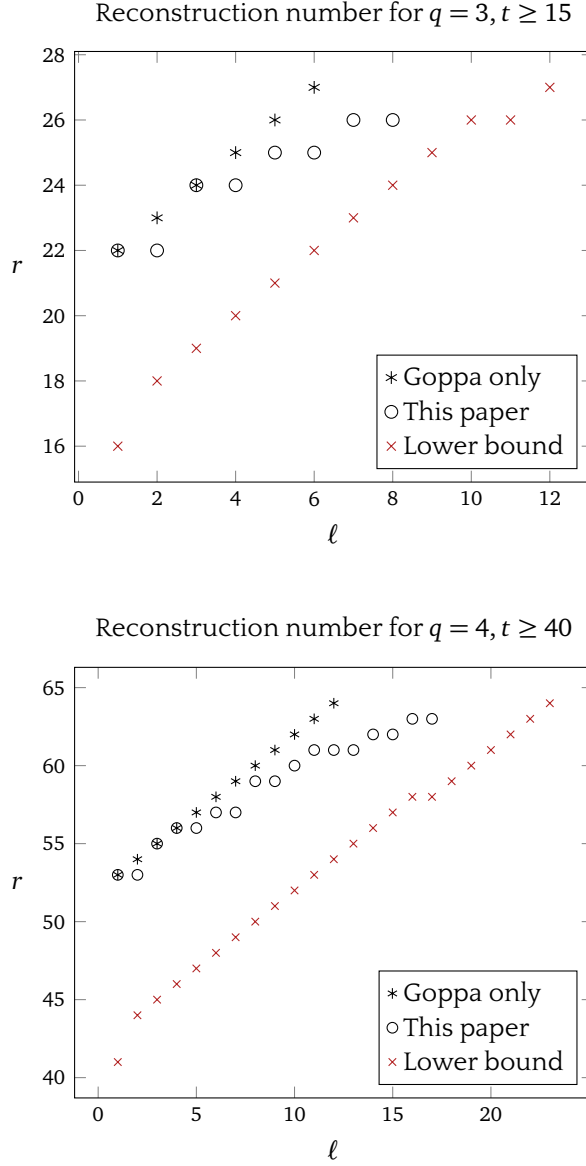


Figure 1. The minimal achievable reconstruction number r given a desired privacy number t . The plots show the constructions from Sections 5 and 6, a construction using the Goppa bound only, and the lower bound from (4.22).

II. Papers

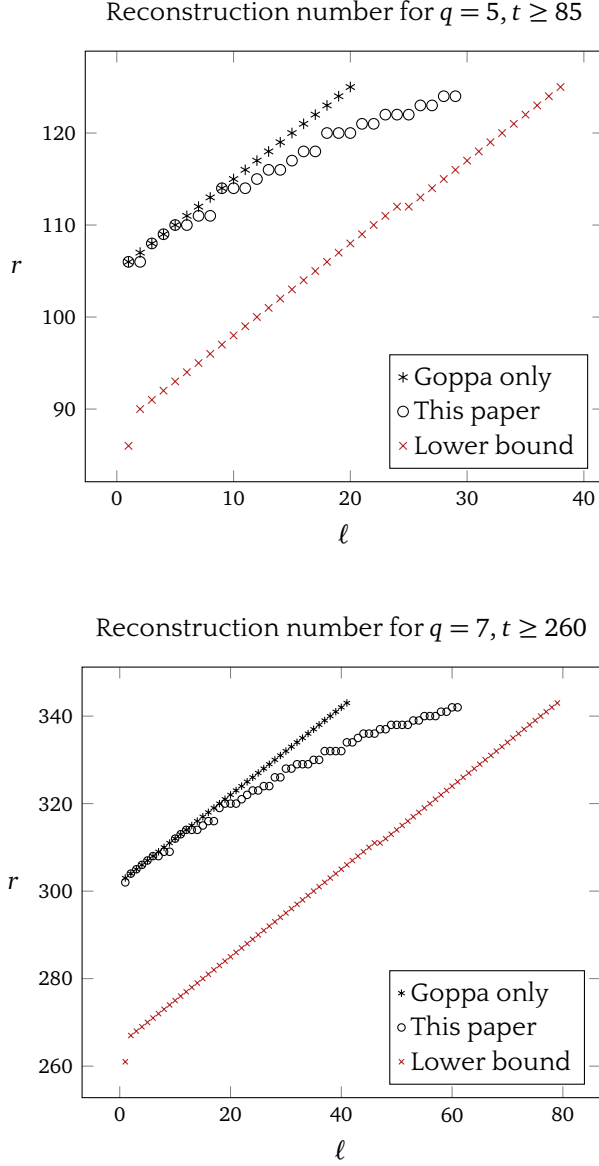



Figure 2. The minimal achievable reconstruction number r given a desired privacy number t . The plots show the constructions from Sections 5 and 6, a construction using the Goppa bound only, and the lower bound from (4.22).


Paper D

Steane-enlargement of quantum codes from the Hermitian function field

René Bødker Christensen

 0000-0002-9209-3739

Olav Geil

 0000-0002-9666-3399

Published in:

Codes, Cryptology and Curves (in honour of Ruud Pellikaan);

Special issue of *Designs, Codes and Cryptography*.

DOI: 10.1007/s10623-019-00709-7

© 2020 Springer Science+Business Media, LLC

Abstract

In this paper, we study the construction of quantum codes by applying Steane-enlargement to codes from the Hermitian function field. We cover Steane-enlargement of both usual one-point Hermitian codes and of order bound improved Hermitian codes. In particular, the paper contains two constructions of quantum codes whose parameters are described by explicit formulae, and we show that these codes compare favourably to existing, comparable constructions in the literature. Furthermore, a number of the new codes meet or even exceed the quantum Gilbert-Varshamov bound.

1 Introduction

The prospect of quantum computers potentially surpassing the computational abilities of classical computers has spawned much interest in studying and building large-scale quantum computers. Since such quantum systems would be very susceptible to disturbances from the environment and to imperfections in the quantum gates acting on the system, the implementation of a working quantum computer requires some form of error-correction. This has led to the study of quantum error-correcting codes, and although such codes are conceptually similar to their classical brethren, their construction calls for different techniques. Nevertheless, results have been found that link classical codes to quantum ones, suggesting that good quantum codes may be found by considering good classical codes.

A well-known class of algebraic geometric codes is the one-point codes from the Hermitian function field. For these one-point Hermitian codes, one of the simplest bounds on the minimal distance is the Goppa bound. For codes of sufficiently large dimension, however, the Goppa bound does not give the true minimal distance, and the order bound for dual codes [DP10; HLP98] and for primary codes [AG08; Gei03; GMRT11] give more information on the minimal distance of the codes. These improved bounds also give rise to a family of improved codes with designed minimal distances, and we shall refer to such codes as *order bound improved codes*.

The construction of quantum codes from one-point Hermitian codes has already been considered in [SK06], and from order bound improved Hermitian codes in [CG18]. Neither of these works, however, explore the potential benefit from applying Steane-enlargement to the codes under consideration. Thus, this paper will address this question, and describe the quantum codes that can be obtained in this manner.

The work is structured as follows. Section 2 contains the preliminary theory on quantum codes and order bound improved Hermitian codes that will be necessary in the subsequent sections. Afterwards, Section 3 covers the results of applying Steane-enlargement to one-point Hermitian codes and order bound improved Hermitian codes. The parameters of the resulting codes are then compared to codes already in the literature and to the quantum

Gilbert-Varshamov bound in Section 4. Section 5 contains the concluding remarks.

2 Preliminaries

In this section, we shall reiterate the necessary definitions and results regarding both quantum error-correcting codes and order bound improved Hermitian codes. For both of these, we will be relying on nested pairs of classical codes, and on the relative distance of such pairs. Thus, recall that for classical, linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1$, we define the relative distance of the pair as

$$d(\mathcal{C}_1, \mathcal{C}_2) = \min\{w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2\},$$

where w_H denotes the Hamming weight.

Quantum codes

A k -dimensional quantum code of length n over \mathbb{F}_q is a q^k -dimensional subspace of the Hilbert space \mathbb{C}^{q^n} . This space is subject to phase-shift errors, bit-flip errors, and combinations thereof. For a quantum code, we define its two minimal distances d_z and d_x as the maximal integers such that the code allows simultaneous detection of any $d_z - 1$ phase-shift errors and any $d_x - 1$ bit-flip errors. When such a code has length n and dimension k , we refer to it as an $[[n, k, d_z/d_x]]_q$ -quantum code.

The literature contains many works based on the assumption that it is not necessary to distinguish between the two types of errors. Thus, the quantum code is only associated with a single minimal distance. That is, we say that its minimal distance is $d = \min\{d_z, d_x\}$, and the notation for the parameters is presented slightly more compactly as $[[n, k, d]]_q$. In this case, we refer to the quantum code as being *symmetric*, and in the previous case we refer to it as being *asymmetric*.

One of the commonly used constructions of quantum codes was provided by Calderbank, Shor, and Steane [CS96; Ste96] and relies on a dual-containing, classical error-correcting code in order to obtain a quantum stabilizer code. That is, it relies on a classical code \mathcal{C} which contains its Euclidean dual \mathcal{C}^\perp . It was later shown that the dual-containing code can be replaced by a pair of nested codes, giving asymmetric quantum codes. This generalized CSS-construction is captured in the following theorem found in [SKR09].

Theorem 2.1:

Given \mathbb{F}_q -linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ of length n and codimension ℓ , the CSS-construction ensures the existence of an asymmetric quantum code with parameters

$$[[n, \ell, d_z/d_x]]_q$$

where $d_z = d(\mathcal{C}_1, \mathcal{C}_2)$ and $d_x = d(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$.

II. Papers

Corollary 2.2:

If the $[n, k, d]$ linear code $C \subseteq \mathbb{F}_q^n$ is dual-containing, then a

$$[[n, 2k - n, d]]_q$$

symmetric quantum code exists.

When the CSS-construction is applied to a dual-containing binary linear code as in Corollary 2.2, Steane [Ste99] proposed a procedure whereby the dimension of the resulting quantum code may be increased. In the best case, this can be done with little or no decrease in the minimal distance of the quantum code. This procedure – eponymously named Steane-enlargement in the literature – has later been generalized to q -ary codes as well [Ham08; LLX10].

Theorem 2.3:

Consider a linear $[n, k]$ code $C \subseteq \mathbb{F}_q^n$ that contains its Euclidean dual C^\perp . If C' is an $[n, k']$ code such that $C \subsetneq C'$ and $k' \geq k + 2$, then an

$$[[[n, k + k' - n, \geq \min\{d, \lceil (1 + \frac{1}{q})d' \rceil\}]]_q$$

quantum code exists with $d = d(C, C'^\perp)$ and $d' = d(C', C'^\perp)$.

When presenting the parameters of a Steane-enlarged code in propositions of this paper, we will often state the dimension in the form $2k - n + (k' - k)$. In this way, we highlight the dimension increase since $2k - n$ is the dimension of the non-enlarged quantum code.

Order bound improved Hermitian codes

We first recall a number of definitions regarding the Hermitian function field. For more details, the reader is referred to [Sti09]. The Hermitian function field \mathbb{H} over \mathbb{F}_{q^2} is the function field $\mathbb{F}_{q^2}(X, Y)$ defined by the equation $X^{q+1} = Y^q + Y$. It is well-known that \mathbb{H} has $q^3 + 1$ rational places, which we will denote by $P_1, P_2, \dots, P_{q^3}, Q$ where Q is the unique common pole of X and Y . A divisor of a function field is a formal sum of places, and for the purpose of coding theory the divisor $D = P_1 + P_2 + \dots + P_n$ where $n = q^3$ is commonly used.

For any integer λ , the Riemann-Roch space $\mathcal{L}(\lambda Q) = \{f \in \mathbb{H} \mid (f) \geq -\lambda Q\} \cup \{0\}$ contains – in addition to zero – all the elements of \mathbb{H} that have pole order at most λ in Q and no other poles. Here, (f) is the principal divisor of f . The one-point algebraic geometric code associated with the divisors D and λQ is then

$$C_{\mathcal{L}}(D, \lambda Q) = \{(f(P_1), f(P_2), \dots, f(P_n)) \mid f \in \mathcal{L}(\lambda Q)\},$$

where $f(P_i)$ denotes the residue class map. Since the support of D contains only rational places and none of these are Q , it may be shown that $C_{\mathcal{L}}(D, \lambda Q) \subseteq \mathbb{F}_{q^2}^n$ and that it is indeed a linear code.

The codes defined below rely heavily on the Weierstraß semigroup of Q . We denote this by $H(Q)$, and it contains the non-negative integers λ such that $-\nu_Q(f) = \lambda$ for some $f \in \bigcup_{i=0}^{\infty} \mathcal{L}(iQ)$. As in [CG18; GMRT11], we consider a special subset of $H(Q)$, namely

$$H^*(Q) = \{\lambda \in H(Q) \mid C_{\mathcal{L}}(D, \lambda Q) \neq C_{\mathcal{L}}(D, (\lambda - 1)Q)\}.$$

It may be shown that in fact

$$H^*(Q) = \{iq + j(q + 1) \mid 0 \leq i < q^2, 0 \leq j < q\}. \quad (4.1)$$

Now, fix an element $f_{\lambda} \in \mathcal{L}(\lambda Q) \setminus \mathcal{L}((\lambda - 1)Q)$ for each $\lambda \in H^*(Q)$, and define the map $\sigma : H^*(Q) \rightarrow \mathbb{N}$ given by

$$\sigma(iq + j(q + 1)) = \begin{cases} q^3 - iq - j(q + 1) & \text{if } 0 \leq i < q^2 - q \\ (q^2 - i)(q - j) & \text{if } q^2 - q \leq i < q^2 \end{cases}. \quad (4.2)$$

This map is the order bound for primary Hermitian codes, and it provides a lower bound on the weight of codewords. In particular, any codeword in $C_{\mathcal{L}}(D, \lambda Q) \setminus C_{\mathcal{L}}(D, (\lambda - 1)Q)$ has weight at least $\sigma(\lambda)$. Thus, by strategically picking out only those codewords that are guaranteed to have a certain designed distance, it is possible to construct an improved primary code

$$\tilde{E}(\delta) = \text{Span}_{\mathbb{F}_{q^2}} \{(f_{\lambda}(P_1), f_{\lambda}(P_2), \dots, f_{\lambda}(P_n)) \mid \sigma(\lambda) \geq \delta\}.$$

Furthermore, it was shown in [CG18] as a special case of [Gei03] that $\tilde{E}(\delta)$ has minimal distance exactly δ whenever $\delta \in \sigma(H^*(Q))$.

For the order bound to produce an improved code, the designed distance must be sufficiently small. Otherwise, the code $\tilde{E}(\delta)$ simply corresponds to one of the usual one-point Hermitian codes. This correspondence is given in the following result from [CG18; Cor. 4].

Lemma 2.4:

For $\delta > q^2 - q$ we have $\tilde{E}(\delta) = C_{\mathcal{L}}(D, (q^3 - \delta)Q)$, but $C_{\mathcal{L}}(D, (q^3 - (q^2 - q))Q)$ is strictly contained in $\tilde{E}(q^2 - q)$.

For $\delta \leq q^2 - q$, the work [CG18] contains a lower bound on the dimension of $\tilde{E}(\delta)$. In Proposition 2.6 below, we give an explicit formula describing the dimension in this case. This formula relies on the number of (number theoretic) divisors of a certain type, as specified in the following definition.

Definition 2.5:

For $n \in \mathbb{Z}_+$, we let $\tau^{(q)}(n)$ denote the number of divisors d of n such that $0 \leq d \leq q$ and $n/d \leq q$.

II. Papers

From the definition it should be clear that $\tau^{(q)}(n)$ can be computed in $\mathcal{O}(q)$ operations.

Proposition 2.6:

Let $1 \leq \delta \leq q^2$, and write $\delta - 1 = aq + b$ for $0 \leq b < q$. Then

$$\dim(\tilde{E}(\delta)) = q^3 - q^2 - \frac{a(a-1)}{2} - \min\{a, b\} + \sum_{i=\delta}^{q^2} \tau^{(q)}(i).$$

Proof:

We give the proof by partitioning $H^*(Q)$ in three disjoint sets:

$$\Lambda_1 = \{iq + j(q+1) \in H^*(Q) \mid i+j < q^2 - q, 0 \leq i < q^2 - q, 0 \leq j < q\}$$

$$\Lambda_2 = \{iq + j(q+1) \in H^*(Q) \mid i+j \geq q^2 - q, 0 \leq i < q^2 - q, 0 \leq j < q\}$$

$$\Lambda_3 = \{iq + j(q+1) \in H^*(Q) \mid q^2 - q \leq i < q^2, 0 \leq j < q\}.$$

We first determine the cardinality of Λ_2 . Considering some $iq + j(q+1) \in \Lambda_2$, and writing $i = q^2 - q - k$, there are $q - k$ possible values of j . There are $q - 1$ such integers k since $q^2 - 2q + 1 \leq i < q^2 - q$ within the set Λ_2 . This implies that

$$|\Lambda_2| = \sum_{k=1}^{q-1} (q-k) = \frac{q(q-1)}{2} = g,$$

where g is the genus of the Hermitian function field. From this, it is also seen that $|\Lambda_1| = q^3 - q^2 - |\Lambda_2| = q^3 - q^2 - g$.

All elements λ of Λ_1 satisfy $\sigma(\lambda) = q^3 - \lambda$. The largest element λ' in Λ_1 is given by $\lambda' = (q^2 - 2q)q + (q-1)(q+1)$, which has $\sigma(\lambda') = q^2 + 1$. Thus, all elements of Λ_1 have $\sigma(\lambda) \geq \delta$, meaning that Λ_1 contributes $|\Lambda_1| = q^3 - q^2 - g$ to the dimension of $\tilde{E}(\delta)$.

In order to determine the number of elements in Λ_2 that satisfy $\sigma(\lambda) \geq \delta$, we compute $|\Lambda_2| - |\{\lambda \in \Lambda_2 \mid \sigma(\lambda) < \delta\}|$. As was the case for Λ_1 , all elements of Λ_2 have $\sigma(\lambda) = q^3 - \lambda$. From this it follows that

$$\sigma(\Lambda_2) = \{q+1, 2q+1, 2q+2, 3q+1, 3q+2, 3q+3, 4q+1, \dots, (q-1)q + (q-1)\}.$$

Combining this with the assumption that $\delta - 1 = aq + b$, where both a and b are non-negative, the number of elements in $\sigma(\Lambda_2)$ smaller than δ is exactly

$$\sum_{i=1}^{a-1} i + \min\{a, b\} = \frac{a(a-1)}{2} + \min\{a, b\}.$$

Because the total number of elements is $|\Lambda_2| = g$, the set Λ_2 contributes $g - a(a-1)/2 - \min\{a, b\}$ to the dimension.

Finally, consider $\sigma(\Lambda_3) = \{\sigma(\lambda) \mid \lambda \in \Lambda_3\}$ as a multiset. We will count (with multiplicity) the number of elements $s \in \sigma(\Lambda_3)$ with $s \geq \delta$. Observe

that $\sigma(\lambda) = (q^2 - i)(q - j)$ for all the elements $\lambda = iq + j(q + 1) \in \Lambda_3$. Hence, $s \in \sigma(\Lambda_3)$, if and only if $s = d \cdot \frac{s}{d}$ where $d \leq q$ and $\frac{s}{d} \leq q$. Since there are $\tau^{(q)}(s)$ such divisors d , it follows that the multiplicity of s in $\sigma(\Lambda_3)$ is given by $\tau^{(q)}(s)$. Subsequently, the number of elements satisfying $s \geq \delta$ is

$$\sum_{s=\delta}^{q^2} \tau^{(q)}(s).$$

By summing the contribution from each of the sets Λ_1 , Λ_2 , and Λ_3 , we obtain the dimension as claimed. \blacksquare

We note that the dimension formula in Proposition 2.6 does not provide an efficient method for computing the dimension of the code $\tilde{E}(\delta)$. Since the set Λ_3 defined in the proof has q^2 elements, we can loop over all of these and compute the σ -value of each in $\Theta(q^2)$ operations, thus determining the dimension of $\tilde{E}(\delta)$. Using the formula in Proposition 2.6, however, requires the computation of $\tau^{(q)}(s)$ for up to q^2 values of s . This gives a total complexity of $\mathcal{O}(q^3)$ operations. The formula in Proposition 2.6 does, however, provide an advantage when we are not interested in a dimension, but rather certain codimensions as will be the case in Section 3. Here, we will only need to compute $\tau^{(q)}$ for m values, where m is a small integer; typically $m = 1$ or $m = 2$.

If only a lower bound for the dimension is needed, Lemma 6 of [CG18] implies that the sum in Proposition 2.6 can be bounded below by $q^2 - \lfloor \delta + \delta \ln(q^2/\delta) \rfloor$ for $q \leq \delta < q^2$ and by $q^2 - \lfloor \delta + \delta \ln(\delta) \rfloor$ for $\delta < q$.

3 Steane-enlargement of Hermitian codes

In order to apply Steane-enlargement to the codes defined in Section 2, we now determine a necessary and sufficient condition for $\tilde{E}(\delta)$ to be dual-containing. While this is possible to do by considering the improved codes directly, it is easier to prove via a condition for the usual one-point Hermitian codes to be dual-containing. The latter is well-known, and the following result was given in [Tie87], and can also be found in [Sti09; Prop. 8.3.2].

Proposition 3.1:

The code $C_{\mathcal{L}}(D, (q^3 - \delta)Q)$ is dual-containing, if and only if

$$\delta \leq \left\lfloor \frac{1}{2}(q^3 - q^2 + q) \right\rfloor + 1. \quad (4.3)$$

Corollary 3.2:

The code $\tilde{E}(\delta)$ is dual-containing, if and only if δ satisfies (4.3).

II. Papers

Proof:

For $\delta > q^2 - q$, Lemma 2.4 ensures that $\tilde{E}(\delta) = C_{\mathcal{L}}(D, (q^3 - \delta)Q)$, and the result follows from Proposition 3.1. For smaller values of δ , the result follows from the observation that $\tilde{E}(q^2 - q + 1) \subsetneq \tilde{E}(\delta)$. ■

In Theorem 2.3, the relative distances $d(\mathcal{C}, \mathcal{C}'^\perp)$ and $d(\mathcal{C}', \mathcal{C}'^\perp)$ of the code pairs are used to determine the distance of the resulting quantum code. In the case of one-point Hermitian codes and order bound improved Hermitian codes, however, these specific relative distances coincide with the corresponding non-relative distances. To see this, consider two codes \mathcal{C} and \mathcal{C}' that are either of the form $C_{\mathcal{L}}(D, \lambda Q)$ or $\tilde{E}(\delta)$. In order to apply Theorem 2.3, we must require $\mathcal{C}^\perp \subsetneq \mathcal{C} \subsetneq \mathcal{C}'$, and we claim that this implies $d(\mathcal{C}, \mathcal{C}'^\perp) = d(\mathcal{C})$ and $d(\mathcal{C}', \mathcal{C}'^\perp) = d(\mathcal{C}')$. Indeed, since \mathcal{C} is dual-containing, Proposition 3.1 and Corollary 3.2 ensure that it contains the smallest dual-containing Hermitian code. That is, $C_{\mathcal{L}}(D, (q^3 - \delta_{\max})Q) \subseteq \mathcal{C}$ where $\delta_{\max} = \lfloor \frac{1}{2}(q^3 - q^2 + q) \rfloor + 1$ as in (4.3). This observation combined with $\mathcal{C} \subsetneq \mathcal{C}'$ implies the inclusion $\mathcal{C}'^\perp \subsetneq C_{\mathcal{L}}(D, (q^3 - \delta_{\max})Q)$, which in turn gives $\mathcal{C}'^\perp \subseteq C_{\mathcal{L}}(D, (q^3 - \delta_{\max} - 1)Q)$. Thus, every codeword of \mathcal{C}'^\perp has Hamming weight at least $d(C_{\mathcal{L}}(D, (q^3 - \delta_{\max} - 1)Q)) = \delta_{\max} + 1$. This exceeds both $d(\mathcal{C})$ and $d(\mathcal{C}')$, and our claim on the relative distances follows. For this reason, we only need to consider the non-relative distances in the proofs below.

In the following proposition, we explore the Steane-enlargement from Theorem 2.3 applied to the usual one-point Hermitian codes. That is, we show by how much the dimension of the symmetric quantum error correcting code can be increased without decreasing its minimal distance. Before giving the result itself, we state the following lemma, which follows from [YK92].

Lemma 3.3:

Let $g = q(q - 1)/2$ be the genus of the Hermitian function field. If $\lambda \in \mathbb{N}$ satisfies $2g \leq \lambda < q^3$, then $\lambda \in H^*(Q)$.

Proposition 3.4:

Assume that δ satisfies (4.3), and additionally that $\delta \geq q^2 + 3$. If k denotes the dimension of $C_{\mathcal{L}}(D, (q^3 - \delta)Q)$, then there exists a quantum code with parameters

$$\left[\left[q^3, 2k - q^3 + \left\lceil \frac{\delta - 1}{q^2 + 1} \right\rceil, \geq \delta \right] \right]_{q^2}. \quad (4.4)$$

Proof:

According to Proposition 3.1, the code $C_{\mathcal{L}}(D, (q^3 - \delta)Q)$ is dual-containing. Letting $\delta' = \delta - \lceil (\delta - 1)/(q^2 + 1) \rceil$, it is also seen that $C_{\mathcal{L}}(D, (q^3 - \delta)Q) \subseteq C_{\mathcal{L}}(D, (q^3 - \delta')Q)$. Lemma 3.3 ensures that the $\lceil (\delta - 1)/(q^2 + 1) \rceil$ integers $\delta - 1, \delta - 2, \dots, \delta'$ are all included in $H^*(Q)$, meaning that the dimension of $C_{\mathcal{L}}(D, (q^3 - \delta')Q)$ is $k + \lceil (\delta - 1)/(q^2 + 1) \rceil \geq k + 2$. Thus, we can apply Theorem 2.3 to obtain a quantum code over \mathbb{F}_{q^2} of length and dimension as in (4.4). This

code has minimal distance at least δ since

$$\left(1 + \frac{1}{q^2}\right)\delta' > \left(1 + \frac{1}{q^2}\right)\left(\delta - \frac{\delta-1}{q^2+1} - 1\right) = \delta - 1,$$

and since Lemma 2.4 ensures that $d(C_{\mathcal{L}}(D, (q^3 - \delta)Q)) = d(\tilde{E}(\delta)) = \delta$. ■

We now turn our attention to the order bound improved codes, and begin by considering the case where both codes can be described as improved codes.

Proposition 3.5:

Assume that $\delta \in \sigma(H^*(Q))$, and that $2 \leq \delta \leq q^2$. Let k denote the dimension of $\tilde{E}(\delta)$, and choose an $m \in \{1, 2, \dots, \delta - 1\}$. Write $\delta - 1 = aq + b$ and $\delta - m - 1 = a'q + b'$ such that $0 \leq b, b' < q$, and define

$$K = \min\{a, b\} - \min\{a', b'\} + \frac{a(a-1) - a'(a'-1)}{2} + \sum_{i=1}^m \tau^{(q)}(\delta - i). \quad (4.5)$$

If $K \geq 2$, then there exists a $[[q^3, 2k - q^3 + K, \geq \delta - m + 1]]_{q^2}$ quantum code.

Proof:

Consider any m such that $1 \leq m < \delta$, and define $\delta' = \delta - m$. By Corollary 3.2, the code $\tilde{E}(\delta)$ is dual-containing. Furthermore, $\tilde{E}(\delta) \subseteq \tilde{E}(\delta')$, and Proposition 2.6 implies that the dimension difference is $\dim(\tilde{E}(\delta')) - \dim(\tilde{E}(\delta)) = K$. Thus, if $K \geq 2$, we can apply Theorem 2.3 to obtain a quantum code, whose dimension is $2k - q^3 + K$. To determine its minimal distance, we see that

$$\left\lceil \left(1 + \frac{1}{q^2}\right)\delta' \right\rceil = \left\lceil (\delta - m) + \frac{\delta - m}{q^2} \right\rceil = \delta - m + 1.$$

The result follows from the fact that $\min\{\delta, \delta - m + 1\} = \delta - m + 1$. ■

To fully describe the quantum codes that can be constructed using the order bound improved codes, it is also necessary to consider the case where an ordinary one-point Hermitian code is enlarged to an improved code. Otherwise, we would neglect certain cases where the order bound improved codes are in some sense ‘too good’ to be used for enlargement as shown in the following example.

Example 3.6:

Consider the code pair $C_{\mathcal{L}}(D, 52Q) \subsetneq C_{\mathcal{L}}(D, 54Q)$ over \mathbb{F}_{16} . These codes have codimension 2, and $C_{\mathcal{L}}(D, 52Q)$ is dual-containing, meaning that we can apply Theorem 2.3 to obtain a quantum code of dimension $2 \cdot 47 - 64 + 2 = 32$ and minimal distance $d = \min\{12, (1 + 1/16) \cdot 10\} = 11$. Using improved codes only, it is not possible to obtain as good parameters. The reason for this is

II. Papers

that the codimension between $\tilde{E}(12)$ and $\tilde{E}(10)$ is only 1. In fact, we have the inclusions

$$C_{\mathcal{L}}(D, 52Q) \subsetneq \tilde{E}(12) \subsetneq \tilde{E}(10) = C_{\mathcal{L}}(D, 54Q).$$

Thus, if we restrict ourselves to improved codes only, we need to either start from a code smaller than $\tilde{E}(12)$ or enlarge to a code larger than $\tilde{E}(10)$. But neither option gives as good parameters as applying Steane-enlargement to $C_{\mathcal{L}}(D, 52Q) \subsetneq \tilde{E}(10)$. ◀

Despite the above observations, we shall refrain from stating the resulting parameters in a separate proposition since it would essentially say no more than Theorem 2.3. That is, such enlargements are generally not well-behaved enough to give meaningful formulae for their codimensions and minimal distances apart from the obvious ones, which already appear in Theorem 2.3.

To conclude this section, we give a few examples over \mathbb{F}_{16} to illustrate the constructions presented in this section.

Example 3.7:

Let $q = 4$, $\delta = 20$, and consider the code $C_{\mathcal{L}}(D, (q^3 - \delta)Q) = C_{\mathcal{L}}(D, 44Q)$. As in Proposition 3.4 we set $\delta' = 20 - \lceil 19/17 \rceil = 18$, and apply Theorem 2.3 to the pair $C_{\mathcal{L}}(D, 44Q) \subsetneq C_{\mathcal{L}}(D, 46Q)$. This yields a quantum code with parameters $[[64, 16, 20]]_{16}$. Had we instead applied Corollary 2.2 directly to $C_{\mathcal{L}}(D, 44Q)$, the resulting parameters would be $[[64, 14, 20]]_{16}$. ◀

Example 3.8:

The order bound improved code $\tilde{E}(5)$ is dual-containing by Corollary 3.2, and has parameters $[64, 56, 5]_{16}$. This code is contained in $\tilde{E}(4)$, which is a $[64, 59, 4]_{16}$ -code. By applying the Steane-enlargement-technique, Theorem 2.3, we obtain a quantum code of length 64, dimension $2 \cdot 56 - 64 + 3$,

15	19	23	27	31	35	39	43	47	51	55	59	63	67	71	75
10	14	18	22	26	30	34	38	42	46	50	54	58	62	66	70
5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65
0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
49	45	41	37	33	29	25	21	17	13	9	5	4	3	2	1
54	50	46	42	38	34	30	26	22	18	14	10	8	6	4	2
59	55	51	47	43	39	35	31	27	23	19	15	12	9	6	3
64	60	56	52	48	44	40	36	32	28	24	20	16	12	8	4

Figure 1. Graphical representation of the inclusions $\tilde{E}(5) \subsetneq \tilde{E}(4)$ over \mathbb{F}_{16} from Example 3.8. Additional explanation may be found within the example.

and a minimal distance of at least

$$\min \left\{ 5, \left\lceil \left(1 + \frac{1}{16} \right) 4 \right\rceil \right\} = 5.$$

That is, we can construct a $[[64, 51, 5]]_{16}$ -quantum code. If only one-point Hermitian codes are used, the best quantum code of dimension 51 has parameters $[[64, 51, 4]]_{16}$ stemming from $C_{\mathcal{L}}(D, 60Q) \subsetneq C_{\mathcal{L}}(D, 66Q)$.

A graphical representation of the code inclusions can be found in Figure 1. Here, the top grid shows $H^*(Q)$ arranged according to indices i and j as in (4.1). The bottom grid shows the same arrangement, but with the map σ from (4.2) applied to each element.

The different shaded regions indicate the basis vectors of the codes $\tilde{E}(5)$, and $\tilde{E}(4)$ used above. The code $\tilde{E}(5)$ is spanned by the codewords $(f_{\lambda}(P_1), f_{\lambda}(P_2), \dots, f_{\lambda}(P_n))$ with $\sigma(\lambda) \geq 5$. The elements $\lambda \in H(Q)^*$ satisfying this are exactly those in the lightly shaded regions. The elements in the darkly shaded region contains those $\lambda \in H^*(Q)$ for which $\sigma(\lambda) = 4$, meaning that the corresponding codewords $(f_{\lambda}(P_1), f_{\lambda}(P_2), \dots, f_{\lambda}(P_n))$ are in $\tilde{E}(4)$, but not in $\tilde{E}(5)$. ◀

4 Comparison with existing constructions

We will now compare the Steane-enlarged quantum codes from Section 3 to some of those already in the literature. In order to conserve space, the examples presented in this section will primarily be those where the constructions of the present paper improve upon existing constructions. This is not meant to imply that such improvements can always be expected – the cited works also contain specific examples of quantum codes whose parameters exceed what can be obtained using the results in Section 3.

For each code presented here, its parameters will also be compared to the Gilbert-Varshamov bound from [FM04].

Theorem 4.1:

Let $n > k \geq 2$ with $n \equiv k \pmod{2}$, and let $d \geq 2$. Then there exists a pure stabilizer quantum code $[[n, k, d]]_q$ if the inequality

$$\sum_{i=1}^{d-1} (q^2 - 1)^i \binom{n}{i} < q^{n-k+2} - 1 \quad (4.6)$$

is satisfied.

We will follow the same convention as [MTT16] and write $[[n, k, d]]_q^{\ddagger}$ if the parameters (n, k, d) do not satisfy (4.6). That is, the \ddagger indicates that the code parameters exceed those that are guaranteed by the Gilbert-Varshamov bound. If (4.6) instead holds for (n, k, d) , but not for $(n, k, d + 1)$, we will

II. Papers

denote the parameters of the code by $[[n, k, d]]_q^\dagger$. As stated in Theorem 4.1, these comparisons are only possible for $n \equiv k \pmod{2}$. For code parameters (n, k, d) with $n \not\equiv k \pmod{2}$ we shall use the same notation, but applied to $(n, k - 1, d)$. We note that [JX11; Cor. 4.3] is another Gilbert-Varshamov-type bound that allows $n \not\equiv k \pmod{2}$, but for the codes presented in the following, Theorem 4.1 is stronger than [JX11; Cor. 4.3]. Therefore, only Theorem 4.1 will be used.

Example 4.2:

Comparing the codes found in Example 3.7 to Theorem 4.1, we obtain $[[64, 16, 20]]_{16}^\dagger$ and $[[64, 14, 20]]_{16}^\dagger$. Thus, the Steane-enlarged code exceeds the Gilbert-Varshamov bound, whereas the CSS-code only meets the bound.

Neither of the two codes presented in Example 3.8 meet or exceed the bound of Theorem 4.1. ◀

In the two following examples, we will focus on comparison of quantum codes derived from the Hermitian function field. Specifically, we will compare the Steane-enlarged codes from Section 3 with the CSS-codes considered in [CG18].

Example 4.3:

For the order bound improved Hermitian codes from Section 3, we give in Table 1 a number of examples where the Steane-enlargement in Proposition 2.6 yields better parameters than those achievable in [CG18]. In all of these examples, the construction of [CG18] gives an asymmetric quantum code where $d_z - d_x = 1$. By using the Steane-enlargement technique, the minimal distance d_x can be increased by one, yielding a symmetric quantum code of the same dimension. That is, Steane-enlargement yields a code of parameters $[[n, k, d]]_{q^2}$, where the construction of [CG18] yields $[[n, k, d/(d-1)]]_{q^2}$. Had we not applied Steane-enlargement in these cases, we would have to resort to the lower of the minimal distances when considering symmetric codes.

All the codes given in Table 1 retain their original minimal distance during enlargement, and the columns marked *Dim. increase* indicate the increase in dimension when applying Theorem 2.3 rather than Corollary 2.2. ◀

Example 4.4:

To exemplify the advantage of using the order bound improved codes and the Steane-enlargement technique, Table 2 shows a number of possible quantum code parameters over \mathbb{F}_{16} when using different constructions based on the Hermitian function field. The codes in the first two columns stem from the CSS-construction applied to the usual one-point Hermitian codes, when bounding the distance by either the Goppa bound or the order bound.

Code	Dim. increase	Code	Dim. increase
$[[8, 4, 3]]_4^*$	2	$[[125, 67, 21]]_{25}$	2
$[[27, 23, 3]]_9^*$	2	$[[343, 339, 3]]_{49}^*$	2
$[[27, 19, 4]]_9^\dagger$	2	$[[343, 335, 4]]_{49}^*$	2
$[[27, 11, 7]]_9^\dagger$	2	$[[343, 330, 5]]_{49}^\dagger$	3
$[[64, 60, 3]]_{16}^*$	2	$[[343, 325, 6]]_{49}$	2
$[[64, 56, 4]]_{16}^\dagger$	2	$[[343, 319, 7]]_{49}$	4
$[[64, 51, 5]]_{16}$	3	$[[343, 313, 8]]_{49}$	2
$[[64, 40, 9]]_{16}^\dagger$	2	$[[343, 308, 9]]_{49}$	3
$[[64, 36, 10]]_{16}$	2	$[[343, 289, 15]]_{49}$	2
$[[64, 30, 13]]_{16}^\dagger$	2	$[[343, 284, 16]]_{49}$	3
$[[125, 121, 3]]_{25}^*$	2	$[[343, 271, 21]]_{49}$	2
$[[125, 117, 4]]_{25}^\dagger$	2	$[[343, 267, 22]]_{49}$	2
$[[125, 112, 5]]_{25}$	3	$[[343, 258, 25]]_{49}$	3
$[[125, 107, 6]]_{25}$	2	$[[343, 251, 29]]_{49}$	2
$[[125, 97, 9]]_{25}$	2	$[[343, 244, 31]]_{49}$	3
$[[125, 91, 11]]_{25}$	2	$[[343, 235, 36]]_{49}$	2
$[[125, 79, 16]]_{25}$	2	$[[343, 231, 37]]_{49}$	2
$[[125, 75, 17]]_{25}$	2	$[[343, 219, 43]]_{49}$	2

Table 1. Comparison between nearly symmetric codes obtained via the procedure in Section 5 of [CG18] and the Steane enlarged codes from this paper. Further details are given in Example 4.3.

The third and fourth columns show the possible quantum code parameters when using order bound improved codes. In the third column, only the CSS-construction is used, and in the fourth Steane-enlargement is applied. Codes marked with * have better parameters than all preceding codes in the same row.

As is evident from the table, the use of the order bound gives more knowledge on the minimal distance in column two, but also provides even better parameters when applying Steane-enlargement to the order bound improved codes. ◀

A different way to produce codes over \mathbb{F}_9 of length 27 is to consider codes from a Cartesian product of size $3 \cdot 9 = 27$, e.g. $\mathbb{F}_3 \times \mathbb{F}_9$, as described in [GGHR18]. In the next example, we consider two such Cartesian products and show how the resulting quantum code parameters compare against those of the Steane-enlarged codes from Section 3.

Example 4.5:

If we apply Theorem 2.3 to $\tilde{E}(7) \subsetneq \tilde{E}(6)$, we obtain a quantum code with parameters $[[27, 11, 7]]_9^\dagger$. Had we instead used the CSS-construction, Theorem 2.1, the best parameters would be $[[27, 9, 7]]_9^\dagger$ obtained from the code $\tilde{E}(7) = C_{\mathcal{L}}(D, 20Q)$. If we apply the CSS-construction to codes defined from the Cartesian product $\mathbb{F}_3 \times \mathbb{F}_9$, the best parameters with minimal

II. Papers

distance 7 are $[[27, 5, 7]]_9$. By considering Steane-enlargement of codes from such Cartesian products as done in [CG19], the best parameters are instead $[[27, 8, 7]]_9$. Hence, the quantum code derived from Steane-enlargement of Hermitian codes improves the dimension significantly compared to the other three methods.

Similar examples can be found over other fields. For instance, over \mathbb{F}_{16} the Steane-enlargement of $\tilde{E}(9) \subsetneq \tilde{E}(8)$ produces parameters $[[64, 40, 9]]_{16}^\dagger$, whereas the CSS-construction applied to Hermitian codes yields $[[64, 38, 9]]_{16}$. The two Cartesian constructions give $[[64, 32, 9]]_{16}$ and $[[64, 35, 9]]_{16}$. ◀

Instead of considering one-point algebraic geometric codes, it is also possible to consider the more general t -point codes in the hope of finding better parameters. The next example considers quantum codes from two- and three-point codes.

Example 4.6:

In [LP17], the authors give a general description of quantum codes that can be obtained by applying Theorem 2.1 to nested t -point algebraic geometric codes. They also give a number of corollaries [LP17; Cors. 3.3, 3.5, 3.6] that can readily be applied to the Hermitian function field to give specific parameters. For instance, [LP17; Table 2] contains the two-point Hermitian codes listed in the first column of Table 3. Turning to the three-point codes produced by [LP17; Cor. 3.6], the quantum codes with the same distances as the aforementioned two-point codes are given in the second column of Table 3. Finally, the third column shows the parameters produced by applying Theorem 2.3 to improved codes. The lengths of these are all one or two higher than the corresponding quantum code from the two-point and three-point Hermitian codes, respectively, but as evident from Table 3 the dimensions are significantly higher for small distances. ◀

The last construction we will consider is La Guardia's construction of quantum generalized Reed-Solomon codes defined in [La 12]. These codes are asymmetric, but as mentioned in Section 2 they can be considered as symmetric by disregarding the highest of the two minimal distances.

Example 4.7:

Figure 2 on page 110 shows the best possible dimension that can be obtained from three different methods given a desired minimal distance. The first method is the Steane-enlargement described in Section 3, and the second is the CSS-construction applied to Hermitian codes as in [CG18]. The final method comes from [La 12; Thm. 7.1] which yields quantum generalized Reed-Solomon codes. In this latter construction, codes of length q^3 over \mathbb{F}_{q^2} are produced by choosing the defining parameters appropriately. But as noted in [GGHR18], better parameters can commonly be found by searching for

One-point codes		Order bound improved	
Goppa bound	Order bound	CSS	Steane-enlargement
$[[64, 30, 12]]_{16}$	$[[64, 30, 12]]_{16}$	$[[64, 30, 12]]_{16}$	$[[64, 30, 13]]_{16}^{\dagger*}$
$[[64, 32, 11]]_{16}$	$[[64, 32, 11]]_{16}$	$[[64, 32, 12]]_{16}^{\dagger*}$	$[[64, 32, 11]]_{16}$
$[[64, 34, 10]]_{16}$	$[[64, 34, 10]]_{16}$	$[[64, 34, 10]]_{16}$	$[[64, 34, 10]]_{16}$
$[[64, 36, 9]]_{16}$	$[[64, 36, 9]]_{16}$	$[[64, 36, 9]]_{16}$	$[[64, 36, 10]]_{16}^{\dagger*}$
$[[64, 38, 8]]_{16}$	$[[64, 38, 9]]_{16}^{\dagger*}$	$[[64, 38, 9]]_{16}$	$[[64, 38, 9]]_{16}$
$[[64, 39, 7]]_{16}$	$[[64, 39, 9]]_{16}^{\dagger*}$	$[[64, 39, 6]]_{16}$	$[[64, 39, 9]]_{16}$
$[[64, 40, 7]]_{16}$	$[[64, 40, 8]]_{16}^{\dagger*}$	$[[64, 40, 8]]_{16}$	$[[64, 40, 9]]_{16}^{\dagger*}$
$[[64, 42, 6]]_{16}$	$[[64, 42, 6]]_{16}$	$[[64, 42, 8]]_{16}^{\dagger*}$	$[[64, 42, 7]]_{16}$
$[[64, 44, 5]]_{16}$	$[[64, 44, 5]]_{16}$	$[[64, 44, 6]]_{16}^{\dagger*}$	$[[64, 44, 7]]_{16}^{\dagger*}$
$[[64, 45, 4]]_{16}$	$[[64, 45, 5]]_{16}^{\dagger*}$	$[[64, 45, 5]]_{16}$	$[[64, 45, 6]]_{16}^{\dagger*}$
$[[64, 46, 4]]_{16}$	$[[64, 46, 5]]_{16}^{\dagger*}$	$[[64, 46, 6]]_{16}^{\dagger*}$	$[[64, 46, 5]]_{16}$
$[[64, 48, 3]]_{16}$	$[[64, 48, 5]]_{16}^{\dagger*}$	$[[64, 48, 5]]_{16}$	$[[64, 48, 5]]_{16}$
$[[64, 50, 2]]_{16}$	$[[64, 50, 4]]_{16}^{\dagger*}$	$[[64, 50, 4]]_{16}$	$[[64, 50, 5]]_{16}^{\dagger*}$
$[[64, 51, 0]]_{16}$	$[[64, 51, 4]]_{16}^{\dagger*}$	$[[64, 51, 4]]_{16}$	$[[64, 51, 5]]_{16}^{\dagger*}$
$[[64, 54, 0]]_{16}$	$[[64, 54, 4]]_{16}^{\dagger*}$	$[[64, 54, 4]]_{16}$	$[[64, 54, 3]]_{16}$
$[[64, 56, 0]]_{16}$	$[[64, 56, 3]]_{16}^{\dagger*}$	$[[64, 56, 3]]_{16}$	$[[64, 56, 4]]_{16}^{\dagger*}$
$[[64, 58, 3]]_{16}^{\dagger}$	$[[64, 58, 3]]_{16}^{\dagger*}$	$[[64, 58, 3]]_{16}^{\dagger}$	$[[64, 58, 3]]_{16}^{\dagger}$
$[[64, 60, 0]]_{16}$	$[[64, 60, 2]]_{16}^{\dagger*}$	$[[64, 60, 2]]_{16}^{\dagger}$	$[[64, 60, 3]]_{16}^{\dagger*}$
$[[64, 62, 0]]_{16}$	$[[64, 62, 2]]_{16}^{\dagger*}$	$[[64, 62, 2]]_{16}^{\dagger}$	$[[64, 62, 2]]_{16}^{\dagger}$

Table 2. Comparison between different methods for constructing quantum codes from the Hermitian function field over \mathbb{F}_{16} . Further details are given in Example 4.9.

Two-Point Code	Three-Point Code	Section 3
$[[26, 16, 3]]_9$	$[[25, 15, 3]]_9$	$[[27, 23, 3]]_9^{\dagger}$
$[[26, 14, 4]]_9$	$[[25, 13, 4]]_9$	$[[27, 19, 4]]_9^{\dagger}$
$[[26, 12, 5]]_9$	$[[25, 11, 5]]_9$	$[[27, 15, 5]]_9^{\dagger}$
$[[26, 4, 9]]_9^{\dagger}$	$[[25, 3, 9]]_9^{\dagger}$	$[[27, 5, 9]]_9^{\dagger}$
$[[26, 2, 10]]_9^{\dagger}$	$[[25, 1, 10]]_9^{\dagger}$	$[[27, 3, 10]]_9^{\dagger}$

Table 3. Examples of quantum codes from two- and three-point Hermitian codes over \mathbb{F}_9 from [LP17; Cor. 3.5] and [LP17; Cor. 3.6], respectively, along with the comparable codes from Section 3.

II. Papers

codes of shorter length and then padding with zeros to obtain codes of length q^3 . Thus, Figure 2 shows the best parameters when using this trick. ◀

As a final example, we will compare the codes from the current section to the quantum Singleton bound [KL97; Rai99].

Theorem 4.8:

Let \mathcal{C} be a quantum code with parameters $[[n, k, d]]_q$, where $k > 0$. Then

$$2d \leq n - k + 2.$$

Example 4.9:

A number of the codes presented in the preceding examples meet the quantum Singleton bound, Theorem 4.8. More precisely, this holds true for the code $[[27, 23, 3]]_9^\dagger$ from Tables 1 and 3; the codes $[[64, 60, 3]]_{16}^\dagger$, $[[125, 121, 3]]_{25}^\dagger$, and $[[343, 339, 3]]_{49}^\dagger$ from Table 1; and the codes $[[64, 62, 2]]_{16}^\dagger$ and $[[64, 60, 3]]_{16}^\dagger$ from Table 2. ◀

5 Concluding remarks

The results obtained in this work demonstrate that Steane-enlargement of improved Hermitian codes can produce quantum codes with significantly better parameters than other known constructions, especially for small designed distances. It is interesting whether similar, or better, parameters can be produced by the Steane-like technique from [GHR15] when applied to such codes, but we leave this question open.

6 Acknowledgements

The authors wish to thank the anonymous reviewers for their thorough reading of the manuscript and their valuable suggestions.

7 References

- [AG08] **H.E. Andersen and O. Geil.** ‘Evaluation codes from order domain theory’. In: *Finite Fields Appl.* 14(1) (2008), pp. 92–123. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2006.12.004.
- [CG18] **R.B. Christensen and O. Geil.** ‘On nested code pairs from the Hermitian curve’. In: *CoRR* abs/1807.04042 (2018). arXiv: 1807.04042. URL: <http://arxiv.org/abs/1807.04042>.
- [CG19] **R.B. Christensen and O. Geil.** ‘On Steane-Enlargement of Quantum Codes from Cartesian Product Point Sets’. In: *CoRR* abs/1908.04560 (2019). arXiv: 1908.04560. URL: <http://arxiv.org/abs/1908.04560>.

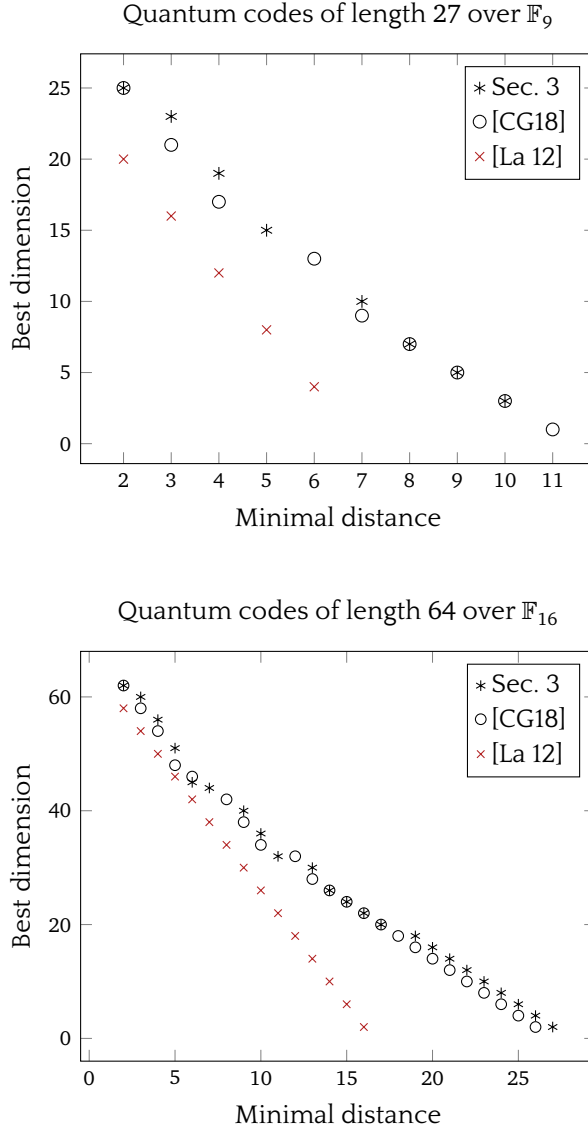


Figure 2. Plots showing the highest achievable dimension for a given minimal distance using the methods from Section 3, [CG18], and [La 12; Thm. 7.1].

II. Papers

- [CS96] **A.R. Calderbank and P.W. Shor.** ‘Good quantum error-correcting codes exist’. In: *Phys. Rev. A* 54(2) (Aug. 1996), pp. 1098–1105. DOI: 10.1103/PhysRevA.54.1098.
- [DP10] **I.M. Duursma and S. Park.** ‘Coset bounds for algebraic geometric codes’. In: *Finite Fields Appl.* 16(1) (2010), pp. 36–55. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2009.11.006.
- [FM04] **K. Feng and Z. Ma.** ‘A finite Gilbert-Varshamov bound for pure stabilizer quantum codes’. In: *IEEE Trans. Information Theory* 50(12) (Dec. 2004), pp. 3323–3325. ISSN: 0018-9448. DOI: 10.1109/TIT.2004.838088.
- [Gei03] **O. Geil.** ‘On codes from norm-trace curves’. In: *Finite Fields Appl.* 9(3) (2003), pp. 351–371. DOI: 10.1016/S1071-5797(03)00010-8.
- [GGHR18] **C. Galindo, O. Geil, F. Hernando and D. Ruano.** ‘Improved Constructions of Nested Code Pairs’. In: *IEEE Trans. Information Theory* 64(4) (2018), pp. 2444–2459. DOI: 10.1109/TIT.2017.2755682.
- [GHR15] **C. Galindo, F. Hernando and D. Ruano.** ‘Stabilizer quantum codes from J -affine variety codes and a new Steane-like enlargement’. In: *Quantum Inf. Process.* 14(9) (2015), pp. 3211–3231. DOI: 10.1007/s11128-015-1057-2.
- [GMRT11] **O. Geil, C. Munuera, D. Ruano and F. Torres.** ‘On the order bounds for one-point AG codes’. In: *Adv. Math. Commun.* 5(3) (2011), pp. 489–504. ISSN: 1930-5346. DOI: 10.3934/amc.2011.5.489.
- [Ham08] **M. Hamada.** ‘Concatenated Quantum Codes Constructible in Polynomial Time: Efficient Decoding and Error Correction’. In: *IEEE Trans. Information Theory* 54(12) (Dec. 2008), pp. 5689–5704. ISSN: 0018-9448. DOI: 10.1109/TIT.2008.2006416.
- [HLP98] **T. Høholdt, J.H. van Lint and R. Pellikaan.** ‘Algebraic Geometry Codes’. In: *Handbook of Coding Theory*. Vol. 1. Elsevier, 1998, pp. 871–961.
- [JX11] **L. Jin and C. Xing.** ‘Quantum Gilbert-Varshamov bound through symplectic self-orthogonal codes’. In: *2011 IEEE International Symposium on Information Theory Proceedings*. July 2011, pp. 455–458. DOI: 10.1109/ISIT.2011.6034167.
- [KL97] **E. Knill and R. Laflamme.** ‘Theory of quantum error-correcting codes’. In: *Phys. Rev. A* 55(2) (Feb. 1997), pp. 900–911. DOI: 10.1103/PhysRevA.55.900.
- [La 12] **G.G. La Guardia.** ‘Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes’. In: *Quantum Inf. Process.* 11(2) (Apr. 2012), pp. 591–604. ISSN: 1573-1332. DOI: 10.1007/s11128-011-0269-3.
- [LLX10] **S. Ling, J. Luo and C. Xing.** ‘Generalization of Steane’s enlargement construction of quantum codes and applications’. In: *IEEE Trans. Information Theory* 56(8) (2010), pp. 4080–4084. DOI: 10.1109/TIT.2010.2050828.

- [LP17] **G.G. La Guardia and F.R.F. Pereira.** ‘Good and asymptotically good quantum codes derived from algebraic geometry’. In: *Quantum Inf. Process.* 16(6) (May 2017), p. 165. ISSN: 1573-1332. DOI: 10.1007/s11128-017-1618-7.
- [MTT16] **C. Munuera, W. Tenório and F. Torres.** ‘Quantum error-correcting codes from algebraic geometry codes of Castle type’. In: *Quantum Inf. Process.* 15(10) (Oct. 2016), pp. 4071–4088. ISSN: 1573-1332. DOI: 10.1007/s11128-016-1378-9.
- [Rai99] **E.M. Rains.** ‘Nonbinary quantum codes’. In: *IEEE Trans. Information Theory* 45(6) (Sept. 1999), pp. 1827–1832. ISSN: 0018-9448. DOI: 10.1109/18.782103.
- [SK06] **P.K. Sarvepalli and A. Klappenecker.** ‘Nonbinary Quantum Codes from Hermitian Curves’. In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Springer Berlin Heidelberg, 2006, pp. 136–143. ISBN: 978-3-540-31424-0. DOI: 10.1007/11617983_13.
- [SKR09] **P.K. Sarvepalli, A. Klappenecker and M. Rötteler.** ‘Asymmetric quantum codes: constructions, bounds and performance’. In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 465 (2009), pp. 1645–1672. DOI: 10.1098/rspa.2008.0439.
- [Ste96] **A. Steane.** ‘Multiple-Particle Interference and Quantum Error Correction’. In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 452(1954) (1996), pp. 2551–2577. ISSN: 13645021.
- [Ste99] **A.M. Steane.** ‘Enlargement of Calderbank-Shor-Steane quantum codes’. In: *IEEE Trans. Information Theory* 45(7) (1999), pp. 2492–2495. DOI: 10.1109/18.796388.
- [Sti09] **H. Stichtenoth.** *Algebraic Function Fields and Codes*. 2nd ed. Graduate Texts in Mathematics. Springer, 2009. ISBN: 978-3-540-76877-7.
- [Tie87] **H. Tiersma.** ‘Remarks on codes from Hermitian curves’. In: *IEEE Trans. Information Theory* 33(4) (July 1987), pp. 605–609. ISSN: 0018-9448. DOI: 10.1109/TIT.1987.1057327.
- [YK92] **K. Yang and P.V. Kumar.** ‘On the true minimum distance of Hermitian codes’. In: *Coding theory and algebraic geometry*. Springer, 1992, pp. 99–107.


Paper E

On Steane-enlargement of quantum codes from Cartesian product point sets

René Bødker Christensen

 0000-0002-9209-3739

Olav Geil

 0000-0002-9666-3399

Published in:

Quantum Information Processing, vol. 19(7)

DOI: 10.1007/s11128-020-02691-9

© 2020 Springer Science+Business Media, LLC

Abstract

In this work, we study quantum error-correcting codes obtained by using Steane-enlargement. We apply this technique to certain codes defined from Cartesian products previously considered by Galindo et al. in [GGHR18]. We give bounds on the dimension increase obtained via enlargement, and additionally give an algorithm to compute the true increase. A number of examples of codes are provided, and their parameters are compared to relevant codes in the literature, which shows that the parameters of the enlarged codes are advantageous. Furthermore, comparison with the Gilbert-Varshamov bound for stabilizer quantum codes shows that several of the enlarged codes match or exceed the parameters promised by the bound.

1 Introduction

Quantum computers promise to deliver computational power far exceeding what can be achieved by classical computers, see for instance [Sho94; Sim94]. Naturally, this has led to much interest in the construction of large scale quantum computers. The quantum bits used in such a system would, however, be prone to errors caused by interaction with the environment. Therefore, methods for correcting such errors are essential, and quantum error correcting codes provide a possible solution.

As in classical coding theory, the performance of a quantum code is assessed based on parameters such as the size of the underlying field, the length of the code and its dimension, and the number of errors that the code can correct. Some of the earliest quantum codes such as [CRSS98; CS96; Sho95] were binary, but just as in classical coding theory it is also possible to study codes over arbitrary finite fields [KKKS06; Rai99]. When working over \mathbb{F}_q – i.e. the finite field of q elements – a quantum code of length n and dimension k is a q^k -dimensional subspace of \mathbb{C}^{q^n} .

One important difference between classical and quantum error correction lies in the types of errors that can happen. Whereas classical bits are susceptible only to *bit flip* errors, quantum bits are also affected by *phase shift* errors. Thus, we can consider two measures of minimal distance for quantum codes: d_x for bit flips, and d_z for phase shifts. Some authors treat the two types of errors equally, and in this case only a single minimal distance $d = \min\{d_x, d_z\}$ is associated to the quantum code. The code is then called *symmetric*. Alternatively, the two types of errors can be treated separately – e.g. to account for the two types of errors happening with different probabilities [IM07]. In this case both of the distances are of interest, and the codes are called *asymmetric*. Clearly, the parameters in the asymmetric setting can be translated into the symmetric setting by ignoring the highest distance.

Traditionally, quantum codes were only studied in the symmetric case, but by now the literature contains a great number of works studying either

of the two types of codes. In this work, we only consider symmetric codes, and some recent developments in this field are [GHR19; LLW19; LMS20; LP17; LWLG19; SYW19; TZ19]. In this setting, the code parameters are commonly written in the form $[[n, k, d]]_q$, and we will follow this convention.

In [GGHR18], Galindo et al. gave two constructions of asymmetric quantum error-correcting codes constructed by applying the CSS-construction to nested classical codes based on Cartesian product point sets. The resulting codes have good parameters compared to existing constructions when investigating which combinations of n , k , d_x , and d_z are possible for various values of q . In addition, these codes compare favourably to the Gilbert-Varshamov bound for asymmetric quantum codes. As mentioned above, someone interested in symmetric codes could use the results from [GGHR18] by discarding the highest distance, but this essentially wastes coding space which could instead be used to increase the dimensions of the codes. In this work, we take an alternative approach and apply Steane-enlargement to that family of codes in order to produce symmetric codes directly. We thereby produce quantum error-correcting codes with good – sometimes even optimal – parameters.

The classical codes considered in this work are special cases of what is called *monomial Cartesian codes* in a recent work [LMS20]. In that paper, the authors derived a way to determine if a monomial Cartesian code is dual-containing, and used this to construct quantum codes via the CSS-construction. The classical codes used in their construction are, however, different from the ones used in the current paper. In particular, the improved codes considered in this work have the best possible dimension given any designed distance.

This work is structured as follows: Section 2 recalls the definitions and results needed in subsequent sections. This includes the CSS-construction and Steane-enlargement as well as results from the theory of classical algebraic geometry codes. Afterwards, Section 3 describes a new construction of quantum codes, including bounds on and exact values of the dimension increase. The section ends by comparing the resulting parameters to other known constructions. Finally, Section 4 contains the conclusion and outlines open problems for future work.

2 Preliminaries

In this section, we recall two results on the CSS-construction and Steane-enlargement that allow construction of quantum codes from classical codes. Then we give a description of a family of codes and the corresponding improved codes, both of which were previously considered in [GGHR18]. In our analysis, we will rely on the notion of relative distances of nested pairs of classical linear codes. Thus, recall that for codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ their relative distance is defined as

$$d(\mathcal{C}_1, \mathcal{C}_2) = \min\{w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2\},$$

II. Papers

where w_H denotes the usual Hamming weight. In general, however, the relative distance is difficult to determine, and the bound $d(\mathcal{C}_1, \mathcal{C}_2) \geq d(\mathcal{C}_1)$ is commonly used instead.

The CSS-construction and Steane-enlargement

One way to construct quantum error-correcting codes is by using the so-called CSS-construction [CS96; Ste96] named after Calderbank, Shor, and Steane. The original construction uses a dual-containing classical linear code to construct a symmetric quantum error-correcting code.

Theorem 2.1:

If the $[n, k, d]$ linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ contains its Euclidean dual, then an

$$[[n, 2k - n, d]]_q$$

symmetric quantum code exists.

Steane [Ste99] proposed a variation on this procedure, which in some cases allows an increase in dimension compared to the corresponding CSS-code but without reducing the minimal distance. Below, we state the q -ary generalization of this procedure, which may be found in [Ham08; LLX10].

Theorem 2.2:

Consider a linear $[n, k]$ code $\mathcal{C} \subseteq \mathbb{F}_q^n$ that contains its Euclidean dual \mathcal{C}^\perp . If \mathcal{C}' is an $[n, k']$ code such that $\mathcal{C} \subsetneq \mathcal{C}'$ and $k' \geq k + 2$, then an

$$[[n, k + k' - n, \geq \min\{d, \lceil (1 + \frac{1}{q})d' \rceil\}]]_q$$

quantum code exists with $d = d(\mathcal{C}, \mathcal{C}'^\perp)$ and $d' = d(\mathcal{C}', \mathcal{C}'^\perp)$.

Remark:

Here we note that if \mathcal{C} and \mathcal{C}' are codes that satisfy the conditions of Theorem 2.2, then the inclusions $\mathcal{C}'^\perp \subsetneq \mathcal{C}^\perp \subseteq \mathcal{C} \subsetneq \mathcal{C}'$ hold, which implies $d(\mathcal{C}'^\perp) \geq d(\mathcal{C})$. In particular, this means that whenever $d(\mathcal{C}') < d(\mathcal{C})$, it must be the case that $d' = d(\mathcal{C}', \mathcal{C}'^\perp) = d(\mathcal{C}')$. For the specific enlargements considered in Section 3, it turns out that this observation allows us to use the usual minimal distances rather than the relative distances while still obtaining the same parameters of the quantum codes.

Codes from Cartesian product point sets

Let $q = p^r$ where p is a prime number, and let r_1, r_2, \dots, r_m be positive integers such that $r_i \mid r$. Then we have the inclusions $\mathbb{F}_{p^{r_i}} \subseteq \mathbb{F}_q$, and it is possible to

consider the Cartesian product $S = \mathbb{F}_{p^{r_1}} \times \mathbb{F}_{p^{r_2}} \times \cdots \times \mathbb{F}_{p^{r_m}} \subseteq \mathbb{F}_q^m$. Now, define the polynomials

$$F_i(X_i) = \prod_{\alpha \in \mathbb{F}_{p^{r_i}}} (X_i - \alpha) = X_i^{p^{r_i}} - X_i,$$

and consider the ring $R = \mathbb{F}_q[X_1, X_2, \dots, X_m]/I$ where

$$I = \langle F_1(X_1), F_2(X_2), \dots, F_m(X_m) \rangle$$

is the vanishing ideal of the F_i 's. Letting $n = |S| = \prod_{i=1}^m p^{r_i}$ and $S = \{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n\}$, we obtain a vector space homomorphism $\text{ev}: R \rightarrow \mathbb{F}_q^n$ given by

$$\text{ev}(F + I) = (F(\mathbf{a}_1), F(\mathbf{a}_2), \dots, F(\mathbf{a}_n))$$

as described in [GGHR18]. Adopting a vectorized version of their notation, we define for $\mathbf{r} = (r_1, r_2, \dots, r_m)$ the set

$$\Delta(\mathbf{r}) = \{X^{\mathbf{a}} \mid \mathbf{a} \in \mathbb{N}^m, 0 \leq a_j < p^{r_j}, j = 1, 2, \dots, m\},$$

where we use the multi-index notation $X^{\mathbf{a}} = X_1^{a_1} X_2^{a_2} \cdots X_m^{a_m}$. For a subset $L \subseteq \Delta(\mathbf{r})$, define the code

$$C(L) = \text{Span}_{\mathbb{F}_q} \{\text{ev}(X^{\mathbf{a}} + I) \mid X^{\mathbf{a}} \in L\}, \quad (4.1)$$

which clearly has length n . To describe the distance of $C(L)$, we use the map $\sigma: \Delta(\mathbf{r}) \rightarrow \mathbb{N}$ given by

$$\sigma(X^{\mathbf{a}}) = \prod_{j=1}^m (p^{r_j} - a_j).$$

Proposition 2.4:

Let $C(L)$ be defined as in (4.1). Then $\dim C(L) = |L|$, and

$$d(C(L)) \geq \min\{\sigma(X^{\mathbf{a}}) \mid X^{\mathbf{a}} \in L\} \quad (4.2)$$

with equality if $X^{\mathbf{a}} \in L$ implies $X^{\mathbf{b}} \in L$ for all choices of $b_1 \leq a_1, b_2 \leq a_2, \dots, b_m \leq a_m$.

Proof:

The claim about the dimension is for instance shown in the proof of [GGHR18; Thm. 16]. The inequality (4.2) can be proved by using the footprint bound as done in [GH01; Prop. 1].

To see the equality, write $\mathbb{F}_{p^{r_i}} = \{v_1^{(i)}, v_2^{(i)}, \dots, v_{p^{r_i}}^{(i)}\}$, let $X^{\mathbf{a}} \in L$, and observe that the expansion of the polynomial

$$f = \prod_{j=1}^m \prod_{i=1}^{a_j} (X_j - v_i^{(j)})$$

II. Papers

contains only monomials $X^{\mathbf{b}}$ with \mathbf{b} as described in the proposition. This means that $\text{ev}(f + I) \in C(L)$. Moreover, f possesses exactly $\prod_{j=1}^m (p^{r_i} - a_j) = \sigma(X^{\mathbf{a}})$ non-zeros. ■

This proposition not only allows us to determine the exact minimal distance of the codes considered in the following section, but more importantly it also enables us to determine certain relative distances when combined with the observations in Remark 2.3.

Improved codes

The information on the minimal distance provided by σ leads to improved code constructions in a straightforward manner. By defining

$$L(\delta) = \{X^{\mathbf{a}} \in \Delta(\mathbf{r}) \mid \sigma(X^{\mathbf{a}}) \geq \delta\}, \quad (4.3)$$

the code $C(L(\delta))$ has designed distance δ by Proposition 2.4. In addition, this is the true minimal distance since $\sigma(X^{\mathbf{b}}) \geq \sigma(X^{\mathbf{a}})$ if $b_1 \leq a_1, b_2 \leq a_2, \dots, b_m \leq a_m$. The dual of $C(L(\delta))$ can be described by studying the map $\mu: \Delta(\mathbf{r}) \rightarrow \mathbb{N}$ defined as

$$\mu(X^{\mathbf{a}}) = \prod_{j=1}^m (a_j + 1).$$

In particular, by letting $L^\perp(\delta) = \{X^{\mathbf{a}} \in \Delta(\mathbf{r}) \mid \mu(X^{\mathbf{a}}) < \delta\}$ we obtain the following result.

Proposition 2.5:

Let $L(\delta)$ be defined as in (4.3). Then $C(L(\delta))^\perp = C(L^\perp(\delta))$.

Proof:

First, note that $\sigma(X^{\mathbf{a}}) = \mu(X^{\mathbf{b}})$ for $b_i = p^{r_i} - a_i - 1$. This implies that the number of monomials with a given σ -value δ is exactly the number of monomials with μ -value δ . As a consequence,

$$\dim C(L^\perp(\delta)) = |\{X^{\mathbf{a}} \in \Delta(\mathbf{r}) \mid \sigma(X^{\mathbf{a}}) < \delta\}| = n - \dim C(L(\delta)) = \dim C(L(\delta))^\perp.$$

Hence, it suffices to show that $C(L^\perp(\delta)) \subseteq C(L(\delta))^\perp$, and we do so by proving that the evaluation of any $X^{\mathbf{b}}$ with $\mu(X^{\mathbf{b}}) < \delta$ must be in $C(L(\delta))^\perp$.

Using contraposition, assume that $X^{\mathbf{b}} \notin C(L(\delta))^\perp$. Then some $\text{ev}(X^{\mathbf{a}}) \in C(L(\delta))$ satisfies $\text{ev}(X^{\mathbf{a}}) \cdot \text{ev}(X^{\mathbf{b}}) \neq 0$. As shown in [GHR15; Prop. 1], this happens if and only if¹ $a_i + b_i > 0$ and $a_i + b_i \equiv 0 \pmod{p^{r_i} - 1}$ holds true for each index $i \in \{1, 2, \dots, m\}$. In other words, we have $a_i + b_i = p^{r_i} - 1$ or $a_i + b_i = 2(p^{r_i} - 1)$.

¹In their notation, the situation in consideration has $J = \emptyset$ and $p \mid N_j$ for each j

In each case, this implies $p^{r_i} - a_i \leq b_i + 1$. In combination with the fact that $\sigma(X^a) \geq \delta$ since $\text{ev}(X^a) \in C(L(\delta))$, we obtain the inequalities

$$\delta \leq \sigma(X^a) = \prod_{i=1}^m (p^{r_i} - a_i) \leq \prod_{i=1}^m (b_i + 1) = \mu(X^b).$$

In conclusion, if $\mu(X^b) < \delta$, we have $\text{ev}(X^b) \in C(L(\delta))^\perp$, which proves the proposition by the observations in the beginning of the proof. ■

3 Steane-enlargement of improved codes

We are now ready to apply Steane-enlargement to the codes defined in Section 2. Our results rely on a simple, but crucial, observation: for each index $i = 1, 2, \dots, m$, $\sigma(\Delta(\mathbf{r}))$ contains an ‘edge’ with values $1, 2, \dots, p^{r_i}$. This is illustrated in Figures 1 and 2. This means that we can easily give a lower bound on the dimension increase when enlarging the code $C(L(\delta))$. To ease the notation in the following, we will order the exponents r_i such that $r_1 \geq r_2 \geq \dots \geq r_m$.

Proposition 3.1:

Let $q = p^r$, and let $\mathbf{r} \in \mathbb{Z}_+^m$ be a vector such that $r_i \mid r$ for each i and $r_1 \geq r_2 \geq \dots \geq r_m$. Additionally, let $2 < \delta \leq p^{r_2} + 1$, and let K be the largest index such that $\delta - 1 \leq p^{r_K}$. Then if $C(L(\delta))$ is a dual-containing $[n, k]$ code, there exists a quantum error-correcting code with parameters

$$[[n, \geq 2k - n + K, \geq \delta]]_q. \quad (4.4)$$

Proof:

Write $\mathcal{C} = C(L(\delta))$, and let $\mathcal{C}' = C(L(\delta - 1))$. Since $1 < \delta - 1 \leq p^{r_K}$, the observation at the start of this section implies that there are at least $K \geq 2$ monomials $X^a \in \Delta(\mathbf{r})$ such that $\sigma(X^a) = \delta - 1$. Thus, \mathcal{C}' has dimension $k' \geq k + K$. As described in Section 2, \mathcal{C} and \mathcal{C}' have minimal distances δ and $\delta - 1$, respectively. Thus the observation in Remark 2.3 ensures that $d(\mathcal{C}', \mathcal{C}'^\perp) = d(\mathcal{C}') = \delta - 1$, and we obtain

$$\lceil (1 + \frac{1}{q})d(\mathcal{C}') \rceil = \lceil (1 + \frac{1}{q})(\delta - 1) \rceil = \delta,$$

where the last equality stems from the assumption that $\delta - 1 \leq p^{r_2} \leq q$. The claim now follows by applying Theorem 2.2 to \mathcal{C} and \mathcal{C}' , and by using the bound $d(\mathcal{C}, \mathcal{C}'^\perp) \geq d(\mathcal{C}) = \delta$. ■

A few additional remarks can be made about the Steane-enlargement described in Proposition 2.4.

II. Papers

9	8	7	6	5	4	3	2	1
18	16	14	12	10	8	6	4	2
27	24	21	18	15	12	9	6	3

Figure 1. The values of $\sigma(\Delta(\mathbf{r}))$ for $p = 3$ and $\mathbf{r} = (2, 1)$. The shaded region shows the edges with values $1, 2, \dots, 9 = p^{r_1}$ and $1, 2, 3 = p^{r_2}$, respectively.

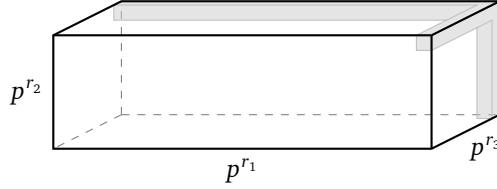


Figure 2. A sketch of $\Delta(\mathbf{r})$ in the case $m = 3$. As in the 2-dimensional case in Figure 1, the shaded region shows the edges where the σ -values are $1, 2, \dots, p^{r_i}$ for each i .

Remark:

The observation that leads to Proposition 2.4 does not help in the case $\delta > q + 1$ since we require $\delta \leq p^{r_2} + 1 \leq q + 1$. This does not mean that Steane-enlargement is impossible for $\delta > q + 1$, but merely that we cannot *guarantee* that it is possible.

Remark:

The increase in dimension when applying Steane-enlargement to the code $C(L(\delta))$ may be greater than the K specified in Proposition 3.1 since this K is determined by considering monomials along the ‘edges’ as in Figure 2. There may be several other monomials that have σ -value $\delta - 1$, yielding a quantum error-correcting code with even better parameters. In Section 3, we characterize the situations where this may happen, and give an improved bound in such cases.

Before studying the dimension increase more thoroughly, we illustrate Proposition 3.1 through an example.

Example 3.4:

Let $q = 3^2 = 9$ and $\mathbf{r} = (2, 2, 1)$. The classical code $C(L(4))$ has parameters $[243, 236, 4]_9$, whence the CSS-construction, Theorem 2.1, gives a $[[243, 229, 4]]_9$ quantum code. Since $\delta - 1 = 3 = p^{r_3}$, Proposition 3.1 ensures that Steane-enlargement will instead provide a code with parameters $[[243, \geq 232, \geq 4]]_9$. In this case, the true dimension is in fact 232.

Using the same q and \mathbf{r} , the code $C(L(7))$ is a $[243, 221, 7]_9$ classical code, yielding a $[[243, 199, 7]]_9$ quantum code via the CSS-construction. This time,

Proposition 3.1 only guarantees a dimension increase of 2 when applying Steane-enlargement, but the actual parameters of the enlarged code are $[[243, 207, \geq 7]]_9$, meaning that the dimension has been increased by 8. ◀

Determining the exact dimension increase

As mentioned in Remark 3.3, the dimension of an enlarged code may be greater than predicted in (4.4). In this section, we will generalize the map $\tau^{(q)}$ from [CG20] to provide an algorithm for computing the exact dimension increase when applying Steane-enlargement to the code $C(L(\delta))$. This generalization will also aid in characterizing those values of δ where Proposition 3.1 underestimates the dimension.

Definition 3.5:

For $s \in \mathbb{Z}_+$ and $\mathbf{r} \in \mathbb{Z}_+^m$, we let $\tau^{(\mathbf{r})}(s)$ denote the number of tuples (d_1, d_2, \dots, d_m) such that $1 \leq d_i \leq p^{r_i}$ for every i , and such that $s = \prod_{i=1}^m d_i$.

Proposition 3.6:

Let s and \mathbf{r} be as in Definition 3.5, and assume that $r_1 \geq r_2 \geq \dots \geq r_m$. Let K be the largest index such that $s \leq p^{r_K}$. Then if s is...

- ...prime, we have $\tau^{(\mathbf{r})}(s) = K$.
- ...square, we have $\tau^{(\mathbf{r})}(s) \geq K + \binom{K}{2}$.
- ...non-prime and non-square, we have $\tau^{(\mathbf{r})}(s) \geq K^2$.

Proof:

Assume first that s is prime. Then any tuple $(d_1, d_2, \dots, d_m) \in \mathbb{Z}_+^m$ with $s = \prod_{i=1}^m d_i$ must have $d_i = s$ for some i and $d_j = 1$ for $j \neq i$. Hence, in this case $\tau^{(\mathbf{r})}(s)$ is the number of indices i such that $d_i \leq p^{r_i}$, which is exactly K .

If s is non-prime, there are still K tuples with a single entry greater than 1 as in the prime case. But we may also split s in two factors $s = f_1 f_2$ such that $f_1, f_2 < s \leq p^{r_K}$. Now, for any distinct indices $i_1, i_2 \in \{1, 2, \dots, K\}$, the tuple (d_1, d_2, \dots, d_m) with $d_{i_1} = f_1$, $d_{i_2} = f_2$, and $d_i = 1$ for $i \notin \{i_1, i_2\}$ is one of the tuples counted by $\tau^{(\mathbf{r})}(s)$. The number of ways to choose the indices i_1, i_2 is $K(K-1)$. If s is not a square number, f_1 and f_2 are distinct, and each of the $K(K-1)$ choices of i_1, i_2 leads to a distinct tuple. If s is a square, we may have $f_1 = f_2$, and the number of distinct tuples is instead $K(K-1)/2 = \binom{K}{2}$. In both cases, we obtain the claimed inequality by adding K . ■

Proposition 3.7:

Let $s \in \mathbb{Z}_+$. Then the number of monomials $X^{\mathbf{a}} \in \Delta(\mathbf{r})$ that have $\sigma(X^{\mathbf{a}}) = s$ is $\tau^{(\mathbf{r})}(s)$.

II. Papers

Proof:

We have $\sigma(X^a) = s$ if and only if $\prod_{i=1}^m (p^{r_i} - a_i) = s$. Since $0 \leq a_i < p^{r_i}$, this is equivalent to $\prod_{i=1}^m d_i = s$ for $1 \leq d_i \leq p^{r_i}$, proving the proposition. ■

Combining Propositions 3.6 and 3.7, we obtain the following immediate corollary.

Corollary 3.8:

Let q , \mathbf{r} , and δ be as in Proposition 3.1. Then (4.4) gives the true dimension if and only if $\delta - 1$ is a prime number. If $\delta - 1$ is not a prime, the bound on the dimension may be increased by $\binom{K}{2}$ if $\delta - 1$ is a square number and by $K(K-1)$ otherwise.

Example 3.9:

We now return to the codes in Example 3.4. In the case of $C(L(4))$, we saw that Proposition 3.1 gave the true minimal distance. Having established Corollary 3.8, we now know that this is no coincidence since $\delta - 1 = 3$ is a prime number.

For the code $C(L(7))$, $\delta - 1 = 6$ is neither prime nor square. Consequently, Corollary 3.8 tells us that the dimension must increase by at least $K^2 = 2^2 = 4$, which is 2 more than the bound from Proposition 3.1. Both bounds are, however, still smaller than the true value of 8. ◀

Since it may not be obvious how to compute $\tau^{(\mathbf{r})}$, we give the following recursive algorithm. Its correctness can be shown by a simple inductive argument.

Algorithm 1: Recursive computation of $\tau^{(\mathbf{r})}(s)$

On input $\mathbf{r} = (r_1, r_2, \dots, r_m)$ and $s \in \mathbb{Z}_+$, this algorithm computes $\tau^{(\mathbf{r})}(s)$

1. Check if \mathbf{r} is a single value r_1 . If this is the case, return 1 if $s \leq r_1$, and 0 otherwise.
 2. Initialize a counter variable $c := 0$.
 3. For each integer $d \in \{1, 2, \dots, p^{r_1}\}$ with $d \mid s$, do the following:
 - Let $\mathbf{r}' = (r_2, r_3, \dots, r_m)$, and compute $\tau^{(\mathbf{r}')} (s/d)$.
 - Update c to be $c := c + \tau^{(\mathbf{r}')} (s/d)$.
 4. Return c .
-

Since the number of d 's considered in Algorithm 1 is at most $\prod_{i=1}^{m-1} p^{r_i} = n/p^{r_m}$, the total number of operations is $\mathcal{O}(n/p^{r_m})$. This is a factor p^{r_m} better than considering all $X^a \in \Delta(\mathbf{r})$ and counting the ones with $\sigma(X^a) = s$. We collect these observations on Algorithm 1 and its relation to Proposition 3.1 in the following proposition.

Proposition 3.10:

Let q , r , and δ be as in Proposition 3.1. Then the true dimension of the quantum code in (4.4) is $2k - n + \tau^{(r)}(\delta)$. Furthermore, Algorithm 1 correctly computes $\tau^{(r)}(\delta)$ in $\mathcal{O}(n/p^{r_m})$ operations, where $n = \prod_{i=1}^m p^{r_i}$.

Examples of parameters

To conclude our exposition, we give concrete parameters of Steane-enlarged codes in several examples. We then compare the parameters of these codes to those of other known constructions and bounds. For each code presented here, we will compare it to the Gilbert-Varshamov bound from [FM04].

Theorem 3.11:

Let $n > k \geq 2$ with $n \equiv k \pmod{2}$, and let $d \geq 2$. Then there exists a pure stabilizer quantum code $[[n, k, d]]_q$ if the inequality

$$\sum_{i=1}^{d-1} (q^2 - 1)^i \binom{n}{i} < q^{n-k+2} - 1 \quad (4.5)$$

is satisfied.

In the same way as [MTT16], we will use the notation $[[n, k, d]]_q^\ddagger$ in the following to indicate that the parameters (n, k, d) exceed the Gilbert-Varshamov bound – i.e. that (4.5) is not satisfied – and we will write $[[n, k, d]]_q^\dagger$ if (n, k, d) satisfies (4.5), but $(n, k, d + 1)$ does not. This is only possible for $n \equiv k \pmod{2}$, which is always the case for CSS-codes from dual-containing codes, but not necessarily for Steane-enlarged codes. Thus, for code parameters (n, k, d) with $n \not\equiv k \pmod{2}$, we will use the same notation, albeit with the bound applied to the parameters $(n, k - 1, d)$.

Remark:

There is another bound, [JX11; Cor. 4.3], which covers all values of n and k . For the parameters presented in the current work, however, that bound is weaker than (4.5), and several of the codes in the examples below exceed [JX11; Cor. 4.3] but not Theorem 3.11. For this reason, we shall use Theorem 3.11 throughout.

In addition to the Gilbert-Varshamov bound, we will refer to the quantum Singleton bound in some cases. This bound is

$$2d \leq n - k + 2, \quad (4.6)$$

and its proof can be found in [KL97; Rai99].

II. Papers

Example 3.13:

This is a continuation of Examples 3.4 and 3.9. When compared with the Gilbert-Varshamov bound, Theorem 3.11, the CSS-code with parameters $[[243, 229, 4]]_9^\dagger$ and the Steane-enlarged code with parameters $[[243, 232, 4]]_9^\dagger$ meet the bound, whereas the two codes of minimal distance 7 neither meet nor exceed the bound. ◀

Example 3.14:

Consider $q = 3^2 = 9$ and $\mathbf{r} = (2, 1)$ as in Figure 1. Here, Proposition 3.1 guarantees that we can enlarge the CSS-codes $[[27, 21, 3]]_9^\dagger$ and $[[27, 17, 4]]_9^\dagger$ to codes of parameters $[[27, 23, \geq 3]]_9^\dagger$ and $[[27, 19, \geq 4]]_9^\dagger$, respectively. Furthermore, Corollary 3.8 ensures that these are the true dimensions. In fact, the code $[[27, 23, 3]]_9^\dagger$ is optimal since it meets the Singleton-bound (4.6).

There are two additional Steane-enlarged codes that are not captured by Proposition 3.1. These are $[[27, 13, 5]]_9$ enlarged to $[[27, 15, \geq 5]]_9^\dagger$, and $[[27, 5, 7]]_9$ enlarged to $[[27, 8, \geq 7]]_9$, where the increases in dimension have been computed using Algorithm 1. In both cases, the technique in Proposition 3.1 fails because $\delta > 4 = p'^2 + 1$. ◀

Initially, we compare the parameters that can be achieved by using the CSS-construction, Theorem 2.1, and those from Steane-enlargement, Theorem 2.2. At the same time, the difference in dimension between these two constructions is compared with the bounds that were given in Propositions 3.1 and Corollary 3.8.

Example 3.15:

In Tables 1–4, we list parameters of quantum codes in various cases where Proposition 3.1 guarantees that enlargement is possible. The tables contain both the original CSS-code and its Steane-enlarged code along with the predicted dimension increases from Proposition 3.1 and Corollary 3.8.

In these tables, the first column shows the parameters of quantum codes obtained by applying Theorem 2.1 to dual-containing codes of the form $C = C(L(\delta))$. The second column shows the results of enlarging the codes in the first column using $C' = C(L(\delta - 1))$ in Theorem 2.2. Both of these columns contain the true dimensions of the codes, and the three final columns highlight the bounds on the dimension increase provided in Proposition 3.1, Corollary 3.8, and Proposition 3.10. More precisely, the third column gives the dimension increase guaranteed by Proposition 3.1, and the fourth shows the bound provided by Corollary 3.8. Any number marked with an asterisk is *known* to be the true value since $\delta - 1$ is a prime. The final column shows the actual increase as computed by Algorithm 1.

Studying the tables, it is evident that Corollary 3.8 provides a better bound for the dimension than Proposition 3.1, but that the actual increase in dimension may be significantly higher. In any case, however, Proposition 3.10 ensures that the true increase can be computed using Algorithm 1. ◀

Construction		Dimension increase		
Thm. 2.1	Thm. 2.2	Prop. 3.1	Cor. 3.8	Prop. 3.10
$[[729, 721, 3]]_9^\dagger$	$[[729, 724, 3]]_9^\ddagger$	3	3^*	3
$[[729, 715, 4]]_9^\dagger$	$[[729, 718, 4]]_9^\ddagger$	3	3^*	3
$[[729, 703, 5]]_9^\dagger$	$[[729, 709, 5]]_9^\dagger$	3	6	6
$[[729, 697, 6]]_9^\dagger$	$[[729, 700, 6]]_9^\dagger$	3	3^*	3
$[[729, 679, 7]]_9^\dagger$	$[[729, 688, 7]]_9^\dagger$	3	9	9
$[[729, 673, 8]]_9^\dagger$	$[[729, 676, 8]]_9^\dagger$	3	3^*	3
$[[729, 653, 9]]_9^\dagger$	$[[729, 663, 9]]_9^\dagger$	3	9	10
$[[729, 641, 10]]_9^\dagger$	$[[729, 647, 10]]_9^\dagger$	3	6	6

Table 1. Code parameters from the Cartesian product with $q = 3^2 = 9$ and $\mathbf{r} = (2, 2, 2)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with $*$ denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 3.10.

Construction		Dimension increase		
Thm. 2.1	Thm. 2.2	Prop. 3.1	Cor. 3.8	Prop. 3.10
$[[64, 58, 3]]_8^\dagger$	$[[64, 60, 3]]_8^\ddagger$	2	2^*	2
$[[64, 54, 4]]_8^\dagger$	$[[64, 56, 4]]_8^\ddagger$	2	2^*	2
$[[64, 48, 5]]_8^\dagger$	$[[64, 51, 5]]_8^\dagger$	2	3	3
$[[64, 44, 6]]_8^\dagger$	$[[64, 46, 6]]_8^\dagger$	2	2^*	2
$[[64, 36, 7]]_8^\dagger$	$[[64, 40, 7]]_8^\dagger$	2	4	4
$[[64, 32, 8]]_8^\dagger$	$[[64, 34, 8]]_8^\dagger$	2	2^*	2

Table 2. Code parameters from the Cartesian product with $q = 2^3 = 8$ and $\mathbf{r} = (3, 3)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with $*$ denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 3.10.

Having compared the two methods considered in this work, we now turn our attention to other constructions of quantum codes. Thus, Examples 3.16–3.19 illustrate how the parameters given in Tables 1–4 compare against existing parameters in the literature. First, we consider the codes obtained from cyclic codes in [LA16; LP10].

Example 3.16:

For $\delta < 8$ the parameters of the codes in Table 1 surpass those presented in [LP10; Tables 1 and 3]. There, codes with parameters $[[728, 714, \geq 3]]_9$, $[[728, 704, \geq 4]]_9$, $[[728, 690, \geq 6]]_9$, $[[728, 679, \geq 7]]_9$, and $[[728, 678, \geq 8]]_9$ are given. Apart from the one with $\delta = 8$, the Steane-enlarged codes in Table 1 are one symbol longer, but have a dimension that is at least 9 higher than the corresponding code in [LP10]. Likewise, the codes in Table 2

II. Papers

have better parameters than those in [LA16; Tables 1 and 2] whenever $\delta \leq 6$. More concretely, [LA16] lists quantum codes with parameters $[[63, 57, \geq 3]]_8^\dagger$, $[[63, 53, \geq 4]]_8^\dagger$, $[[63, 49, \geq 5]]_8^\dagger$, and $[[63, 45, \geq 6]]_8^\dagger$. For larger values of δ , however, [LA16] outperforms the codes in Table 2.

All the codes in Tables 1 and 2 have $q = p^r$ and $r_i = r$, which are in fact hyperbolic codes. It seems to be a general pattern for such codes, that the Steane-enlargements with small distances outperform the codes in [LA16; LP10], but that this relation is reversed for larger distances.

The codes in Tables 3 and 4 have parameters that cannot be achieved using the method from [LA16; LP10] since those codes all have lengths $q^m - 1$ for some $m \geq 2$, where q is the field size. \blacktriangleleft

As a second comparison, we consider the parameters of quantum twisted codes that have been compiled in [Ede].

Example 3.17:

Based on [BE00], the webpage [Ede] contains lists of quantum code parameters derived from twisted codes. For instance, the list for $q = 9$ contains the codes $[[730, 718, 3]]_9^\dagger$, $[[730, 712, 4]]_9$, $[[730, 706, 5]]_9$, and $[[730, 700, 6]]_9$. The comparable codes in Table 1 are both one symbol shorter and have higher dimension. It may also be noted that two of the codes in Table 1 exceed the Gilbert-Varshamov bound, while this is not the case for any of the codes listed in this example.

The codes $[[730, 694, 7]]_9$, $[[730, 688, 8]]_9$, and $[[730, 682, 9]]_9$ from [Ede] have better parameters than those in Table 1, but they are included in the table for completeness.

A previous version of this paper contained an example of quantum codes over \mathbb{F}_5 of length 625. As pointed out by a reviewer, however, the parameters of those codes did not exceed the parameters of the codes listed in [Ede]. \blacktriangleleft

Next, we compare the quantum codes derived from the Suzuki curve in [MTT16] to the Steane-enlarged codes presented in Table 2.

Example 3.18:

The codes in Table 2 have favourable parameters compared to those given in [MTT16; Ex. 5], which are defined from the Suzuki curve. Specifically, the codes in [MTT16] have parameters $[[64, 54, 3]]_8$, $[[64, 52, 4]]_8^\dagger$, $[[64, 42, 5]]_8$, $[[64, 40, 6]]_8$, $[[64, 38, 7]]_8$, and $[[64, 36, 8]]_8$, which are all worse than those in Table 2 except the one with distance 8. As a final remark, the code with parameters $[[64, 60, 3]]_8^\dagger$ meets the quantum Singleton bound (4.6). \blacktriangleleft

As a final example, we consider the monomial Cartesian codes from [LMS20] that are guaranteed to be MDS.

Construction		Dimension increase		
Thm. 2.1	Thm. 2.2	Prop. 3.1	Cor. 3.8	Prop. 3.10
$[[1024, 1016, 3]]_{16}^{\dagger}$	$[[1024, 1019, 3]]_{16}^{\ddagger}$	3	3*	3
$[[1024, 1010, 4]]_{16}^{\dagger}$	$[[1024, 1013, 4]]_{16}^{\ddagger}$	3	3*	3
$[[1024, 998, 5]]_{16}^{\dagger}$	$[[1024, 1004, 5]]_{16}^{\ddagger}$	3	6	6
$[[1024, 994, 6]]_{16}^{\dagger}$	$[[1024, 996, 6]]_{16}^{\ddagger}$	2	2*	2
$[[1024, 978, 7]]_{16}^{\dagger}$	$[[1024, 986, 7]]_{16}^{\ddagger}$	2	4	8
$[[1024, 974, 8]]_{16}^{\dagger}$	$[[1024, 976, 8]]_{16}^{\ddagger}$	2	2*	2
$[[1024, 956, 9]]_{16}^{\dagger}$	$[[1024, 965, 9]]_{16}^{\ddagger}$	2	4	9
$[[1024, 946, 10]]_{16}^{\dagger}$	$[[1024, 951, 10]]_{16}^{\ddagger}$	2	3	5
$[[1024, 934, 11]]_{16}^{\dagger}$	$[[1024, 940, 11]]_{16}^{\ddagger}$	2	4	6
$[[1024, 930, 12]]_{16}^{\dagger}$	$[[1024, 932, 12]]_{16}^{\ddagger}$	2	2*	2
$[[1024, 900, 13]]_{16}^{\dagger}$	$[[1024, 915, 13]]_{16}^{\ddagger}$	2	4	15
$[[1024, 896, 14]]_{16}^{\dagger}$	$[[1024, 898, 14]]_{16}^{\ddagger}$	2	2*	2
$[[1024, 884, 15]]_{16}^{\dagger}$	$[[1024, 890, 15]]_{16}^{\ddagger}$	2	4	6
$[[1024, 872, 16]]_{16}^{\dagger}$	$[[1024, 878, 16]]_{16}^{\ddagger}$	2	4	6
$[[1024, 848, 17]]_{16}^{\dagger}$	$[[1024, 860, 17]]_{16}^{\ddagger}$	2	3	12

Table 3. Code parameters from the Cartesian product with $q = 2^4 = 16$ and $\mathbf{r} = (4, 4, 2)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with * denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 3.10.

Construction		Dimension increase		
Thm. 2.1	Thm. 2.2	Prop. 3.1	Cor. 3.8	Prop. 3.10
$[[1024, 1014, 3]]_8^{\ddagger}$	$[[1024, 1018, 3]]_8^{\ddagger}$	4	4*	4
$[[1024, 1008, 4]]_8^{\ddagger}$	$[[1024, 1011, 4]]_8^{\ddagger}$	3	3*	3
$[[1024, 990, 5]]_8^{\ddagger}$	$[[1024, 999, 5]]_8^{\ddagger}$	3	6	9
$[[1024, 984, 6]]_8^{\ddagger}$	$[[1024, 987, 6]]_8^{\ddagger}$	3	3*	3
$[[1024, 960, 7]]_8^{\ddagger}$	$[[1024, 972, 7]]_8^{\ddagger}$	3	9	12
$[[1024, 954, 8]]_8^{\ddagger}$	$[[1024, 957, 8]]_8^{\ddagger}$	3	3*	3
$[[1024, 922, 9]]_8^{\ddagger}$	$[[1024, 938, 9]]_8^{\ddagger}$	3	9	16

Table 4. Code parameters from the Cartesian product with $q = 2^3 = 8$ and $\mathbf{r} = (3, 3, 1)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with * denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 3.10.

Example 3.19:

Among the codes presented in this Tables 1–4, two were MDS-codes: $[[27, 23, 3]]_9^*$ and $[[64, 60, 3]]_8^*$. From recent work [LMS20; Cor. 3.10] the same lengths, dimensions, and minimal distances can be achieved, but the field size is much larger. In particular, they require $q > n$ so the corresponding field sizes are at least 29 and 67, respectively. ◀

4 Conclusion

In this work, we showed how Steane-enlargement can be applied to codes defined from Cartesian product point sets. Concretely, Proposition 3.1 contains a simple condition that, when satisfied, guarantees that Steane-enlargement produces a higher dimension when compared to the CSS-construction without reducing the distance. Furthermore, we gave an improved, but still easily computable, bound on the dimension increase during this enlargement, and provided an algorithm to compute the true value.

Comparing the resulting quantum code parameters to existing constructions revealed several cases where the Steane-enlarged codes from Cartesian product point sets provide better parameters than comparable constructions. Such improvements were especially common for small designed distances, where the Steane-enlarged codes also exceed the Gilbert-Varshamov bound in many cases.

This work and the work [CG20] shows that Steane-enlargement can provide quantum codes with good parameters when the underlying classical codes are defined from relatively simple point sets. Thus, it is natural to ask whether other, more complicated point sets lead to good parameters in the same way. We leave this question for future research.

5 Acknowledgements

The authors express their gratitude to Diego Ruano for delightful discussions in relation to this work. In addition, the authors thank the anonymous reviewers for their comments, which led to a better manuscript.

6 References

- [BE00] **J. Bierbrauer and Y. Edel.** ‘Quantum twisted codes’. In: *J. Comb. Des.* 8(3) (2000), pp. 174–188. DOI: 10.1002/(SICI)1520-6610(2000)8:3<174::AID-JCD3>3.0.CO;2-T.
- [CG20] **R.B. Christensen and O. Geil.** ‘Steane-enlargement of quantum codes from the Hermitian function field’. In: *Des. Codes Cryptogr.* (2020). To appear. DOI: 10.1007/s10623-019-00709-7.

- [CRSS98] **A.R. Calderbank, E.M. Rains, P.M. Shor and N.J.A. Sloane.** 'Quantum error correction via codes over $GF(4)$ '. In: *IEEE Trans. Inf. Theory* 44(4) (July 1998), pp. 1369–1387. DOI: 10.1109/18.681315.
- [CS96] **A.R. Calderbank and P.W. Shor.** 'Good quantum error-correcting codes exist'. In: *Phys. Rev. A* 54(2) (Aug. 1996), pp. 1098–1105. DOI: 10.1103/PhysRevA.54.1098.
- [Ede] **Y. Edel.** *Some good quantum twisted codes*. Accessed on 13th November 2019. URL: <https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QT BCH/QT BCHIndex.html>.
- [FM04] **K. Feng and Z. Ma.** 'A finite Gilbert-Varshamov bound for pure stabilizer quantum codes'. In: *IEEE Trans. Inf. Theory* 50(12) (Dec. 2004), pp. 3323–3325. ISSN: 0018-9448. DOI: 10.1109/TIT.2004.838088.
- [GGHR18] **C. Galindo, O. Geil, F. Hernando and D. Ruano.** 'Improved Constructions of Nested Code Pairs'. In: *IEEE Trans. Inf. Theory* 64(4) (2018), pp. 2444–2459. DOI: 10.1109/TIT.2017.2755682.
- [GH01] **O. Geil and T. Høholdt.** 'On Hyperbolic Codes'. In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 14th International Symposium, AAECC-14, Melbourne, Australia November 26-30, 2001, Proceedings*. 2001, pp. 159–171. DOI: 10.1007/3-540-45624-4_17.
- [GHR15] **C. Galindo, F. Hernando and D. Ruano.** 'Stabilizer quantum codes from J -affine variety codes and a new Steane-like enlargement'. In: *Quantum Inf. Process.* 14(9) (Sept. 2015), pp. 3211–3231. ISSN: 1573-1332. DOI: 10.1007/s11128-015-1057-2.
- [GHR19] **C. Galindo, F. Hernando and D. Ruano.** 'Classical and Quantum Evaluation Codes at the Trace Roots'. In: *IEEE Trans. Inf. Theory* 65(4) (2019), pp. 2593–2602. DOI: 10.1109/TIT.2018.2868442.
- [Ham08] **M. Hamada.** 'Concatenated Quantum Codes Constructible in Polynomial Time: Efficient Decoding and Error Correction'. In: *IEEE Trans. Inf. Theory* 54(12) (Dec. 2008), pp. 5689–5704. ISSN: 0018-9448. DOI: 10.1109/TIT.2008.2006416.
- [IM07] **L. Ioffe and M. Mézard.** 'Asymmetric quantum error-correcting codes'. In: *Phys. Rev. A* 75(3) (Mar. 2007), p. 032345. DOI: 10.1103/PhysRevA.75.032345.
- [JX11] **L. Jin and C. Xing.** 'Quantum Gilbert-Varshamov bound through symplectic self-orthogonal codes'. In: *2011 IEEE International Symposium on Information Theory Proceedings*. July 2011, pp. 455–458. DOI: 10.1109/ISIT.2011.6034167.
- [KKKS06] **A. Ketkar, A. Klappenecker, S. Kumar and P.K. Sarvepalli.** 'Nonbinary Stabilizer Codes Over Finite Fields'. In: *IEEE Trans. Inf. Theory* 52(11) (Nov. 2006), pp. 4892–4914. DOI: 10.1109/TIT.2006.883612.

II. Papers

- [KL97] **E. Knill and R. Laflamme.** ‘Theory of quantum error-correcting codes’. In: *Phys. Rev. A* 55(2) (Feb. 1997), pp. 900–911. DOI: 10.1103/PhysRevA.55.900.
- [LA16] **G.G. La Guardia and M.M.S. Alves.** ‘On cyclotomic cosets and code constructions’. In: *Linear Algebra Appl.* 488 (2016), pp. 302–319. ISSN: 0024-3795. DOI: 10.1016/j.laa.2015.09.034.
- [LLW19] **J. Lv, R. Li and J. Wang.** ‘New Binary Quantum Codes Derived From One-Generator Quasi-Cyclic Codes’. In: *IEEE Access* 7 (2019), pp. 85782–85785. DOI: 10.1109/ACCESS.2019.2923800.
- [LLX10] **S. Ling, J. Luo and C. Xing.** ‘Generalization of Steane’s enlargement construction of quantum codes and applications’. In: *IEEE Trans. Inf. Theory* 56(8) (2010), pp. 4080–4084. DOI: 10.1109/TIT.2010.2050828.
- [LMS20] **H.H. López, G.L. Matthews and I. Soprunov.** ‘Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes’. In: *Des. Codes Cryptogr.* (2020). To appear. DOI: 10.1007/s10623-020-00726-x.
- [LP10] **G.G. La Guardia and R. Palazzo.** ‘Constructions of new families of nonbinary CSS codes’. In: *Discrete Math.* 310(21) (2010), pp. 2935–2945. ISSN: 0012-365X. DOI: 10.1016/j.disc.2010.06.043.
- [LP17] **G.G. La Guardia and F.R.F. Pereira.** ‘Good and asymptotically good quantum codes derived from algebraic geometry’. In: *Quantum Inf. Process.* 16(6) (May 2017), p. 165. ISSN: 1573-1332. DOI: 10.1007/s11128-017-1618-7.
- [LWLG19] **R. Li, J. Wang, Y. Liu and G. Guo.** ‘New quantum constacyclic codes’. In: *Quantum Inf. Process.* 18(5) (Mar. 2019), p. 127. ISSN: 1573-1332. DOI: 10.1007/s11128-019-2242-5.
- [MTT16] **C. Munuera, W. Tenório and F. Torres.** ‘Quantum error-correcting codes from algebraic geometry codes of Castle type’. In: *Quantum Inf. Process.* 15(10) (Oct. 2016), pp. 4071–4088. ISSN: 1573-1332. DOI: 10.1007/s11128-016-1378-9.
- [Rai99] **E.M. Rains.** ‘Nonbinary quantum codes’. In: *IEEE Trans. Inf. Theory* 45(6) (Sept. 1999), pp. 1827–1832. ISSN: 0018-9448. DOI: 10.1109/18.782103.
- [Sho94] **P. Shor.** ‘Algorithms for quantum computation: discrete logarithms and factoring’. In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science.* IEEE Computer Society, Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.
- [Sho95] **P.W. Shor.** ‘Scheme for reducing decoherence in quantum computer memory’. In: *Phys. Rev. A* 52(4) (Oct. 1995), R2493–R2496. DOI: 10.1103/PhysRevA.52.R2493.
- [Sim94] **D. Simon.** ‘On the power of quantum computation’. In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science.* IEEE

- Computer Society, Nov. 1994, pp. 116–123. DOI: 10.1109/SFCS.1994.365701.
- [Ste96] **A. Steane**. 'Multiple-Particle Interference and Quantum Error Correction'. In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 452(1954) (1996), pp. 2551–2577. ISSN: 13645021.
- [Ste99] **A.M. Steane**. 'Enlargement of Calderbank-Shor-Steane quantum codes'. In: *IEEE Trans. Inf. Theory* 45(7) (1999), pp. 2492–2495. DOI: 10.1109/18.796388.
- [SYW19] **X. Shi, Q. Yue and Y. Wu**. 'New quantum MDS codes with large minimum distance and short length from generalized Reed–Solomon codes'. In: *Discrete Math.* 342(7) (2019), pp. 1989–2001. ISSN: 0012-365X. DOI: <https://doi.org/10.1016/j.disc.2019.03.019>.
- [TZ19] **F. Tian and S. Zhu**. 'Some new quantum MDS codes from generalized Reed–Solomon codes'. In: *Discrete Math.* 342(12) (2019), p. 111593. ISSN: 0012-365X. DOI: <https://doi.org/10.1016/j.disc.2019.07.009>.

About the type

This thesis was typeset using \LaTeX

Text is set in Quattrocento and Cabin

Mathematics is set in Math Design

URL's are set in Source Code Pro

ISSN (online): 2446-1636
ISBN (online): 978-87-7210-674-8

AALBORG UNIVERSITY PRESS