Quantum Cyclic Code of length dividing $p^t + 1$

Sagarmoy Dutta*
Dept of Computer Science and Engineering
Indian Institute of Technology Kanpur
Kanpur, UP, India, 208016
sagarmoy@cse.iitk.ac.in

Piyush P Kurur
Dept of Computer Science and Engineering
Indian Institute of Technology Kanpur
Kanpur, UP, India, 208016
ppk@cse.iitk.ac.in
and
Max-Planck Institut für Informatik
Campus E1 4, 66123, Saarbrücken, Germany

***Abstract*—In this paper, we study cyclic stabiliser codes over $\mathbb{F}_p$ of length dividing $p^t + 1$ for some positive integer t. We call these t-Frobenius codes or just Frobenius codes for short. We give methods to construct them and show that they have efficient decoding algorithms.**

An important subclass of stabiliser codes are the linear stabiliser codes. For linear Frobenius codes we have stronger results: We completely characterise all linear Frobenius codes. As a consequence, we show that for every integer n that divides $p^t + 1$ for an odd t, there are no linear cyclic codes of length n. On the other hand for even t, we give an explicit method to construct all of them. This gives us many explicit examples of Frobenius code which include the well studied Laflamme code.

We show that the classical notion of BCH distance can be generalised to all the Frobenius codes that we construct, including the non-linear ones, and show that the algorithm of Berlekamp can be generalised to correct quantum errors within the BCH limit. This gives, for the first time, a family of codes that are neither CSS nor linear for which efficient decoding algorithm exits.

I. Introduction

Successful implementation of quantum computing requires handling errors that occur while processing, storing and communicating quantum information. Good quantum error correcting codes are therefore a key technology in the eventual building of quantum computing devices, besides, perhaps more importantly, their theory provides some elegant mathematics. An important class of codes are the stabiliser codes [1], which not only captured the isolated examples constructed earlier [2]–[5], but built a solid foundation for subsequent works [6]–[8].

Constructing stabiliser codes require handling the slightly non-standard symplectic inner product. The CSS construction [9], [10] gives one elegant and natural way, albeit with some loss of generality, to handle this difficulty. For this, one needs a self-dual classical code, or more generally two classical codes one contained in the dual of the other, thereby reusing the intuition built for classical codes. Another approach to the problem, again with some loss of generality, is to look at linear stabiliser codes [6]. Linear stabiliser codes can also be characterised as linear classical codes over a quadratic extension of the base field [6, Theorem 3] [11, Lemma 18] which are Hermitian self-dual.

In this article, we study mainly cyclic stabiliser codes. Cyclic codes, being well studied classically, have recently been studied in detail [6], [11]–[13], mostly from the perspective of either self dual codes or Hermitian self dual codes. We explore another approach to simplify the symplectic condition, namely, we restrict our attention to cyclic codes of length dividing $p^t + 1$ over $\mathbb{F}_p$.

Our contribution: In this article, we focus on cyclic stabiliser codes over the field $\mathbb{F}_p$ whose lengths divide $p^t + 1$, for some positive integer t. We call such codes *t-Frobenius codes*, or just *Frobenius codes*, because of the key role played by the Frobenius automorphism. Restricting to such lengths, while constraining, is not that bad, as there is a healthy, i.e. almost linear, density of such lengths (see [14]). In bargain, we get a simpler formulation of the isotropy condition, which helps in the analysis of these codes considerably. Furthermore, this simplicity of the isotropic condition allows us to extend the notion of BCH distance for these codes and give efficient decoding algorithms. Since none of the codes that we construct are CSS — all our codes are uniquely cyclic (See Section III for a definition) and by Proposition III.5 are not CSS — and some of them are non-linear, this gives a family of codes for which efficient decoding algorithms were not known before.

We study the subfamily of *linear* Frobenius codes in detail and completely characterise them (Theorems IV.4 and IV.6). This has two consequences, one negative and another positive. Firstly, over $\mathbb{F}_p$, we show that there are no t-Frobenius linear codes when t is odd (Corollary IV.5). This is a somewhat serious limitation of linear cyclic codes as the density of such lengths n seems to be almost linear (see [14] for details). Moreover, this impossibility is purely Galois theoretic unlike other known restriction that arise from sphere packing bounds or linear programming bounds.

On the positive side, the characterisation of linear Frobenius codes gives us ways to explicitly construct examples of linear Frobenius codes of lengths $p^{2t} + 1$. Again, since the density of such lengths are also healthy, this technique give sizable number of explicit examples including the well studied Laflamme code. Table I give such examples for $p = 2$ and lengths less than 100.

*Part of this work was done while the author was visiting Max Planck Institut für Informatik funded by Research I foundation and MPI

II. Preliminaries

We give a brief overview of the notation used in this paper. For a prime power $q = p^k$, $\mathbb{F}_q$ denotes the unique finite field of cardinality q. The product $\mathbb{F}_p^n$ is a vector space over the finite field $\mathbb{F}_p$ and an element $\mathbf{a} = (a_1, \ldots, a_n)^{\mathrm{T}}$ in it is thought of as a column vectors. Fix a p-dimensional Hilbert space $\mathcal{H}$. An orthonormal basis for $\mathcal{H}$ is of cardinality p. Fix one such basis and denote it by $\{|a\rangle | a \in \mathbb{F}_p\}$. As is standard in quantum computing, for an element $\mathbf{a} = (a_1, \ldots, a_n)^{\mathrm{T}}$ in $\mathbb{F}_p^n$, $|\mathbf{a}\rangle$ denotes the tensor product $|a_1\rangle \otimes \ldots \otimes |a_n\rangle$. The set $\{|\mathbf{a}\rangle | \mathbf{a} \in \mathbb{F}_p^n\}$ forms a basis for the n-fold tensor product $\mathcal{H}^{\otimes^n}$. A *quantum code* over $\mathbb{F}_p$ of *length* n is a subspace of the tensor product $\mathcal{H}^{\otimes^n}$. There is by now a significant literature on quantum codes [1], [6], [15].

Let ζ denote the primitive p-th root of unity $\exp \frac{2\pi\iota}{p}$. For $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_p^n$, define the operators $U_{\mathbf{a}}$ and $V_{\mathbf{b}}$ on $\mathcal{H}^{\otimes^n}$ as $U_{\mathbf{a}}|\mathbf{x}\rangle = |\mathbf{x} + \mathbf{a}\rangle$ and $V_{\mathbf{b}}|\mathbf{x}\rangle = \zeta^{\mathbf{b}^{\mathrm{T}}\mathbf{x}}|\mathbf{x}\rangle$ respectively. The operator $U_{\mathbf{a}}$ can be thought of as a *position error* and $V_{\mathbf{b}}$ as a *phase error*. In a quantum channel, both position errors and phase errors can occur simultaneously. These are captured by the *Weyl* operators $U_{\mathbf{a}}V_{\mathbf{b}}$.

For elements $\mathbf{a}$ and $\mathbf{b}$ of the vector space $\mathbb{F}_p^n$ the *joint weight* $\mathrm{w}(\mathbf{a}, \mathbf{b})$ is the number of positions i such that at least one of a_i or b_i is not zero. The *weight* of the Weyl operator $U_{\mathbf{a}}V_{\mathbf{b}}$ is the joint weight $\mathrm{w}(\mathbf{a}, \mathbf{b})$. Occurrence of a quantum error at t positions is modelled as the channel applying an unknown Weyl operator $U_{\mathbf{a}}V_{\mathbf{b}}$ of weight t on the transmitted message.

An important subclass of quantum codes are stabiliser codes [1]. These are closely connected to isotropic subsets. For any two vectors $\mathbf{u} = (\mathbf{a}, \mathbf{b})$ and $\mathbf{v} = (\mathbf{c}, \mathbf{d})$ of $\mathbb{F}_p^n \times \mathbb{F}_p^n$, define the *symplectic inner product* $\langle \mathbf{u}, \mathbf{v} \rangle$ as the scalar $\mathbf{a}^{\mathrm{T}}\mathbf{d} - \mathbf{b}^{\mathrm{T}}\mathbf{c}$ of $\mathbb{F}_p$. A subset S of $\mathbb{F}_p^{2n}$ is called *totally isotropic* [6], or just *isotropic*, if for any two elements $\mathbf{u}$ and $\mathbf{v}$ of S, $\langle \mathbf{u}, \mathbf{v} \rangle = 0$.

Isotropic subspaces of $\mathbb{F}_p^{2n}$ are closely related to stabiliser codes. Calderbank *et al* [6], [16] were the first to study this relation when the underlying field is $\mathbb{F}_2$. Later, this was generalised to arbitrary fields [7], [8]. We summaries these results in a form convenient for our purposes.

Theorem II.1 ([7], [8], [16])**.** *Let S be a isotropic subspace of $\mathbb{F}_p^{2n}$ for some positive integer n. Let ω be either the primitive p-th root of unity $\exp \frac{2\pi\iota}{p}$ or $\sqrt{-1}$, depending on whether p is odd or even respectively. Then, the subset $\mathcal{S} = \{\omega^{\mathbf{a}^{\mathrm{T}}\mathbf{b}} U_{\mathbf{a}}V_{\mathbf{b}} | (\mathbf{a}, \mathbf{b}) \in S\}$ of unitary operators forms an Abelian group. Furthermore, the set of vectors invariant under the operators in $\mathcal{S}$ forms a quantum stabiliser code and the operator $P = \frac{1}{\#\mathcal{S}} \sum_{U \in \mathcal{S}} U$ is the projection to it.*

Let S be a subspace of $\mathbb{F}_p^{2n}$. By the *centraliser* of S, denoted by $\overline{S}$, we mean the subspace of all $\mathbf{u}$ in $\mathbb{F}_p^{2n}$, such that $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, for all $\mathbf{v}$ in S. We have the following theorem on the error correcting properties of the stabiliser codes.

Theorem II.2 ([7], [8], [16])**.** *Let S be a isotropic subspace of $\mathbb{F}_p^{2n}$ and let $\mathcal{C}$ be the associated stabiliser code. Then the dimension of the subspace S is at most n. If S has dimension $n-k$ for some $k > 0$ then the centraliser $\overline{S}$, as a vector space over $\mathbb{F}_p$, is of dimension $n + k$ and the code $\mathcal{C}$, as a Hilbert space, is of dimension p^k. Furthermore, if the minimum weight $min\{\mathrm{w}(\mathbf{u}) | \mathbf{u} \in \overline{S} \setminus S\}$ is d then $\mathcal{C}$ can detect up to $d-1$ errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.*

Let $\mathcal{C}$ be a stabiliser code associated with an $n - k$ dimensional totally isotropic subspace S of $\mathbb{F}_p^{2n}$. By the *stabiliser dimension* of $\mathcal{C}$ we mean the integer k. Similarly, we call the weight $\min\{\mathrm{w}(\mathbf{u}) | \mathbf{u} \in \overline{S} \setminus S\}$ the *distance* of $\mathcal{C}$. In this context, recall that the stabiliser code associated to the isotropic set S is called δ-*pure*, if the minimum of the joint weights of non-zero elements of the centraliser $\overline{S}$ is δ. It follows from Theorem II.2 that a δ-pure code is of distance at least δ. A stabiliser code over $\mathbb{F}_p$ of length n, stabiliser dimension k and distance δ is called an $[[n, k, \delta]]_p$ code.

III. Quantum Cyclic codes

In this section we define quantum cyclic codes and study some of its properties. Fix a prime p and a positive integer n coprime to p for the rest of the section. Let N denote the right shift operator over $\mathbb{F}_p^n$, i.e. the operator that maps $\mathbf{u} = (u_1, \ldots, u_n)$ to $(u_n, u_1, \ldots, u_{n-1})$. Consider the unitary operator $\mathcal{N}$ defined as $\mathcal{N}|\mathbf{u}\rangle = |N\mathbf{u}\rangle$. Recall that a classical code over $\mathbb{F}_p$ is cyclic if for all code words $\mathbf{u}$, its right shift $N\mathbf{u}$ is also a code word. Motivated by this definition, we have the following definition for quantum cyclic codes.

Definition III.1. *A quantum code $\mathcal{C}$ is* cyclic *if for any vector $|\psi\rangle$ in $\mathcal{C}$, the vector $\mathcal{N}|\psi\rangle$ is in $\mathcal{C}$.*

Let S be a subspace of $\mathbb{F}_p^n \times \mathbb{F}_p^n$. We say that S is *simultaneously cyclic* if for all $(\mathbf{a}, \mathbf{b})$ in S, $(N\mathbf{a}, N\mathbf{b})$ is also in S. Stabiliser codes with simultaneously cyclic isotropic sets were first studied by Calderbank *et al* [6, Section 5] and was taken as the definition of cyclic codes in subsequent works [11]–[13]. In this context, we show that for stabiliser codes, simultaneous cyclicity and our definition of cyclicity coincide.

Proposition III.2. *An isotropic subset of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ is simultaneously cyclic if and only if the associated stabiliser code is cyclic.*

Let $\mathcal{R}$ denote the cyclotomic ring $\mathbb{F}_p[X]/X^n - 1$ of polynomials modulo $X^n - 1$. When dealing with cyclic codes, it is often convenient to think of vectors of $\mathbb{F}_p^n$ as polynomials in $\mathcal{R}$ by identifying the vector $\mathbf{a} = (a_0, \ldots, a_{n-1})$ with the polynomials $a(X) = a_0 + \ldots + a_{n-1}X^{n-1}$. We use the bold face Latin letter, for example $\mathbf{a}$, $\mathbf{b}$ etc, to denote vectors and the corresponding plain face letter, $a(X)$, $b(X)$ respectively, for the associated polynomial. Recall that, classical cyclic codes are ideals of this ring $\mathcal{R}$. In the ring $\mathcal{R}$, the polynomial X has a multiplicative inverse namely X^{n-1}. Often, we write X^{-1} to denote this inverse. Notice that for any two vectors $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_p^n$, if $a(X)$ and $b(X)$ denote the corresponding polynomials in $\mathcal{R}$, then the coefficient of X^k in the product $a(X)b(X^{-1}) \mod X^n - 1$ is the inner product $\mathbf{a}^{\mathrm{T}}N^k\mathbf{b}$, where N is the right shift operator. An immediate consequence is the following.

Proposition III.3. *Let S be a simultaneously cyclic subset of $\mathbb{F}_p^n \times \mathbb{F}_p^n$. Then S is isotropic if and only if for any two elements $\mathbf{u} = (\mathbf{a}, \mathbf{b})$ and $\mathbf{v} = (\mathbf{c}, \mathbf{d})$, the corresponding polynomials satisfy the condition*

$$b(X)c(X^{-1}) - a(X)d(X^{-1}) = 0 \mod X^n - 1.$$

Let S be a simultaneously cyclic subspace of $\mathbb{F}_p^n \times \mathbb{F}_p^n$. Define A and B to be the projections of S onto the first and last n coordinates respectively, i.e. $A = \{\mathbf{a} | (\mathbf{a}, \mathbf{b}) \in S\}$ and $B = \{\mathbf{b} | (\mathbf{a}, \mathbf{b}) \in S\}$. Since S is simultaneously cyclic, A and B are cyclic subspaces of $\mathbb{F}_p^n$ and hence are ideals of the ring $\mathcal{R}$. Let $g(X)$ be the factor of $X^n - 1$ that generates A. Since $g(X)$ is an element of A, there exists a polynomial $f(X)$ in $\mathcal{R}$ such that $(\mathbf{g}, \mathbf{f}) \in S$. If this $\mathbf{f}$ is unique then we say that S is *uniquely cyclic* and call the pair $(g(X), f(X))$ of polynomials, a *generating pair* for S. We have the following proposition.

Proposition III.4. *A simultaneously cyclic subspace S of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ is uniquely cyclic if and only if for every element $(0, \mathbf{a})$ in S, $\mathbf{a} = 0$. If S is uniquely cyclic generated by the pair (g, f), then every element of S is of the form (ag, af) for some $a(X)$ in $\mathbb{F}_p[X]/X^n - 1$.*

For a CSS code, the underlying isotropic set S is a product $C_1 \times C_2$ of two n-length classical codes over $\mathbb{F}_p$ In particular, elements $(\mathbf{a}, 0)$ and $(0, \mathbf{b})$ for $\mathbf{a}$ and $\mathbf{b}$ in C_1 and C_2 respectively belong to S. Therefore, we have the following proposition as a consequences of Proposition III.4.

Proposition III.5. *Any uniquely cyclic stabiliser code is not CSS unless it is of distance* 1.

For uniquely cyclic codes the isotropy condition in Proposition III.3 can be simplified as follows.

Proposition III.6. *Let S be a simultaneously cyclic subspace of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ with generating pair (g, f). Then S is isotropic if and only if $g(X)f(X^{-1}) = g(X^{-1})f(X)$ modulo $X^n - 1$. Moreover, any pair (a, b) belongs to $\overline{S}$ if and only if $g(X)b(X^{-1}) = a(X^{-1})f(X)$ modulo $X^n - 1$.*

Consider a quadratic extension $\mathbb{F}_{p^2} = \mathbb{F}_p(\eta)$ of $\mathbb{F}_p$ obtained by adjoining a root η of some quadratic irreducible polynomial over $\mathbb{F}_p$. Identify the product $\mathbb{F}_p^n \times \mathbb{F}_p^n$ with the the vector space $\mathbb{F}_{p^2}^n$ by mapping a pair of vectors $(\mathbf{a}, \mathbf{b})$ to the vector $\mathbf{a} + \eta\mathbf{b}$. Similarly for the cyclotomic ring $\mathcal{R}$, identify the product ring $\mathcal{R} \times \mathcal{R}$ with the cyclotomic ring $\mathcal{R}(\eta) = \mathbb{F}_{p^2}[X]/X^n - 1$. Let S be any isotropic subspace of $\mathbb{F}_p^n \times \mathbb{F}_p^n$. The associated stabiliser code $\mathcal{C}_S$ is said to be *linear* [6] if S under the above identification is a subspace of $\mathbb{F}_{p^2}^n$. Isotropic subspaces of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ associated to linear stabiliser codes are classical cyclic codes of length n over $\mathbb{F}_p(\eta)$. Thus the following proposition follows.

Proposition III.7. *Let S be an isotropic simultaneously cyclic subspace of the product $\mathbb{F}_p^n \times \mathbb{F}_p^n$. The associated stabiliser code $\mathcal{C}_S$ is linear if and only if S is an ideal of the cyclotomic ring $\mathbb{F}_{p^2}[X]/X^n - 1$. Furthermore, if $\mathcal{C}_S$ is linear then the centraliser $\overline{S}$ is also an ideal of $\mathbb{F}_{p^2}[X]/X^n - 1$.*

It follows from the theory of classical codes that both S and $\overline{S}$ are ideals generated by factors of $X^n - 1$ over $\mathbb{F}_{p^2}$. In this context, we make the following definition.

Definition III.8 (BCH distance)**.** *Let $g(X)$ be a factor of the polynomial $X^n - 1$ over the field $\mathbb{F}_q$, n coprime to q. The* BCH distance *of the polynomial $g(X)$ is the largest integer d such that the consecutive distinct powers $\beta^\ell, \beta^{\ell+1}, \ldots, \beta^{\ell+d-2}$ are roots of g, for some primitive n-th root β.*

Recall that, the distance of a classical cyclic code is at least the BCH distance of its generating polynomial. In the setting of stabiliser codes, the distance is related to the minimum joint weight of elements of $\overline{S}$ (Theorem II.2). Motivated by this analogy, we define the BCH distance of linear stabiliser codes as follows.

Definition III.9. *Let S be a isotropic subset of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ associated to a linear cyclic stabiliser code $\mathcal{C}$. The* BCH distance of $\mathcal{C}$ *is the BCH distance of the generator polynomial of the centraliser $\overline{S}$.*

We have the following theorem which follows from Theorem II.2.

Theorem III.10. *Let $\mathcal{C}$ is be any linear cyclic stabiliser code of BCH distance d. Then it is d-pure and hence has distance at least d.*

IV. Linear cyclic codes of length dividing $p^t + 1$

In this section, we study linear cyclic stabiliser codes over $\mathbb{F}_p$ whose length divides $p^t + 1$. The main motivation to restrict our attention to lengths of this form is captured in the following proposition.

Proposition IV.1. *If the integer n divides $p^t + 1$, for some positive integer t then X^{-1} in the cyclotomic ring $\mathbb{F}_p[X]/X^{p^t+1} - 1$ is X^{p^t}. Therefore, for every polynomial $g(X)$ over any extension of $\mathbb{F}_p$ we have $g(X^{-1})$ is $g(X)^{p^t}$.*

The above-mentioned property simplifies the isotropy condition for polynomials considerably and allows us to completely characterise all linear cyclic codes of such lengths.

Let $\mathbb{F}_p(\eta)/\mathbb{F}_p$ be an extension of degree d. When dealing with cyclic quantum codes of length n, we use $\mathcal{R}$ to denote the cyclotomic ring $\mathbb{F}_p[X]/X^n - 1$. The extension ring $\mathcal{R}(\eta)$ is then the cyclotomic ring $\mathbb{F}_p(\eta)[X]/X^n - 1$. Linear codes are associated with quadratic extension and identification of the pair of vectors $(\mathbf{a}, \mathbf{b})$ with $\mathbf{a} + \eta\mathbf{b}$ maps its isotropic set to an ideal of $\mathcal{R}(\eta)$.

Lemma IV.2. *Let S be the isotropic ideal associated to a linear cyclic stabiliser code over $\mathbb{F}_p$ of length dividing $p^t + 1$. Then S is uniquely cyclic.*

Consider the Frobenius automorphism σ on a degree d extension $\mathbb{F}_p(\eta)/\mathbb{F}_p$ which maps any element α in $\mathbb{F}_p(\eta)$ to α^p. This can be naturally extended to polynomials over $\mathbb{F}_p(\eta)$ and therefore on $\mathcal{R}(\eta)$ as follows: For a polynomial $a(X) = a_0 + \ldots + a_n X^n$ where a_i are in $\mathbb{F}_p(\eta)$, $\sigma(a)$ is

defined as $\sigma(a_0)+\ldots+\sigma(a_n)X^n$. We call this the *Frobenius involution*.

Constructing linear cyclic codes correspond to constructing generators for the associated isotropic ideal. We make use of the following Galois theoretic lemma to characterise such generators.

Lemma IV.3. *Let the integer n divide p^t+1 for some positive integer t.*

1) *Any irreducible factor of X^n-1 over $\mathbb{F}_p$ other than the factors $X-1$ or $X+1$ has even degree.*
2) *Let $f(X)$ be any irreducible factor of X^n-1 over $\mathbb{F}_p$ whose degree is divisible by d for some positive integer d. Over the extension field $\mathbb{F}_{p^d}=\mathbb{F}_p(\eta)$, $f(X)$ splits into d irreducible factors $f_0(X,\eta),\ldots,f_{d-1}(X,\eta)$ such that $f_i=\sigma^i(f_0)$.*

Consider the extension field $\mathbb{F}(\eta)=\mathbb{F}_{p^2}$ and let S be any ideal of $\mathcal{R}(\eta)$. The following theorem gives a necessary condition for it to be isotropic and hence give a linear cyclic code.

Theorem IV.4. *Let $\mathbb{F}_p(\eta)$ be a quadratic extension of $\mathbb{F}_p$. Let n divide p^t+1 and S be an isotropic ideal of $\mathbb{F}_p(\eta)[X]/X^n-1$. Then t is even and the ideal S is generated by the product polynomial $g(X)\cdot h(X,\eta)$ where $g(X)$ and $h(X,\eta)$ are two coprime factors of X^n-1 satisfying the following condition.*

1) *$g(X)$ is any factor of X^n-1 over $\mathbb{F}_p$ which contains both $X-1$ and $X+1$ as factors.*
2) *$h(X,\eta)$ is any factor of $\frac{X^n-1}{g}$ over $\mathbb{F}_{p^2}$, such that for any irreducible factor $r(X,\eta)$ of $\frac{X^n-1}{g}$ over $\mathbb{F}_{p^2}$, $r(X,\eta)$ divides $h(X,\eta)$ if and only if $\sigma(r)=r(X,\eta')$* does not.

A corollary of the above theorem is the following impossibility result.

Corollary IV.5. *Let n be any integer that divides p^t+1, where t is odd. Then there does not exist any linear cyclic stabiliser codes of length n over $\mathbb{F}_p$.*

For example, $9, 11, 19, 27, 33, 43, 57, 59, 67, 81, 83, 99$ are the numbers less then hundred that divide 2^t+1 for some odd t. Hence there is no binary linear cyclic code of such lengths.

The next theorem shows that the conditions in Theorem IV.4 are also sufficient to construct isotropic ideals of $\mathcal{R}(\eta)$. This gives us a way of constructing linear cyclic stabiliser of length dividing $p^{2m}+1$. This theorem directly follows from a more generalised construction given in Theorem V.1 and Theorem V.2.

Theorem IV.6. *Let n divide $p^{2m}+1$ and $\mathbb{F}_p(\eta)$ be a quadratic extension of $\mathbb{F}_p$. Let $g(X)$ and $h(X,\eta)$ be factors of X^n-1 satisfying the properties 1 and 2 of Theorem IV.4. Then the ideal S of $\mathbb{F}_p(\eta)[X]/X^n-1$ generated by the product $g\cdot h$ is isotropic as a subset of $\mathbb{F}_p^n\times\mathbb{F}_p^n$ and the associated stabiliser code is linear and cyclic.*

In the rest of the article, we refer to cyclic stabiliser codes whose length divide p^t+1 as t-Frobenius codes. For linear $2m$-Frobenius codes, we call the factorisation $g(X)\cdot h(X,\eta)$ characterised above as the *canonical factorisation* associated to the code.

Theorem IV.7. *Let $\mathcal{C}$ be a linear $2m$-Frobenius code over $\mathbb{F}_p$ with canonical factorisation $g\cdot h$. The stabiliser dimension of the code $\mathcal{C}$ is $\deg(g)$. The centraliser $\overline{S}$ of S is the ideal generated by $h(X,\eta)$ and hence the BCH distance of $\mathcal{C}$ is BCH distance of h.*

Again the proof follows from the more general theorem V.3 and V.2.

V. Generalisation to nonlinear codes

We have already shown that if n divides p^t+1 for some odd integer t then no linear code of length n exists. In this section we show how to construct nonlinear codes of such length. The construction is a generalisation of Theorem IV.6. The major difference is that the extension of $\mathbb{F}_p$ is no longer restricted to be quadratic.

Theorem V.1. *Let n divide $p^{dm}+1$ and $\mathbb{F}_p(\eta)$ be a degree d extension of $\mathbb{F}_p$. Let $g(X)$ and $h(X,\eta)$ be co-prime factors of X^n-1 satisfying the following properties.*

1) *$g(X)$ is any factor of X^n-1 over $\mathbb{F}_p$ which contains all the the irreducible factor of X^n-1 over $\mathbb{F}_p$ whose degree is not divisible by d.*
2) *$h(X,\eta)$ is any factor of $\frac{X^n-1}{g}$ over $\mathbb{F}_p(\eta)$ such that for any irreducible factor $r(X,\eta)$ of $\frac{X^n-1}{g}$ over $\mathbb{F}_p(\eta)$, $r(X,\eta)$ divides $h(X,\eta)$ if and only if none of the factors $\sigma(r),\ldots,\sigma^{d-1}(r)$ divide h i.e. $\frac{X^n-1}{g(X)}=\prod_{i=0}^{d-1}\sigma^i(h)$.*

Fix any nonzero α in $\mathbb{F}_p$ and let $a(X,\eta)$ be the polynomial, uniquely defined by Chinese remaindering, as follows.

$$a=\begin{cases}1 & \mod g\\ \sigma^i(\alpha\eta) & \mod \sigma^i(h) \text{ for all } 0\le i<d\end{cases}$$

Then $a(X,\eta)$ is a polynomial in $\mathbb{F}_p[X]$ and the uniquely cyclic subspace generated by (g,ag) is isotropic.

The following theorem shows that the linear codes obtained from Theorem IV.6 are indeed a subclass of the codes generated from Theorem V.1

Theorem V.2. *Let $c(X)=X^2+c_1X+c_0$ be an irreducible polynomial over $\mathbb{F}_p$ and η,η' be roots of $c(X)$. Fix $d=2$, $\mathbb{F}_p(\eta')/\mathbb{F}_p$ to be the extension and $\alpha=-c_0^{-1}$ in Theorem V.1 and let S be the corresponding isotropic subspace. Then the image of S under the map $(u,v)\mapsto u+\eta v$ is an ideal of the cyclotomic ring $\mathbb{F}_p(\eta)[X]/(X^n-1)$ and its generator is given by the polynomial $g(X)h(X,\eta)$ where g,h satisfies the properties in Theorem IV.4. Moreover the centraliser $\overline{S}$ also maps to an the ideal generated by h.*

As before, we call $g\cdot h$ as the canonical factorisation associated with the above mentioned t-Frobenius codes. We also call the BCH distance of h to be the BCH distance of $\mathcal{C}$.

Theorem V.3. *Let $g(X) \cdot h(X, \eta)$ be the canonical factorisation associated with a t-Frobenius code $\mathcal{C}$ as in Theorem V.1. The stabiliser dimension of $\mathcal{C}$ is $\deg(g)$. If the BCH distance of h is δ then $\mathcal{C}$ is δ-pure and hence has distance at least δ.*

As a demonstration of our construction we list (Table I) some explicit examples of codes where the characteristic p of the underlying finite field is 2. The distance given in this table is the BCH distance. The actual distance can be larger. Canonical factors and their roots are given in [14]. We have both linear and non-linear codes for parameters with dagger whereas star denotes only nonlinear codes.

Length	Parameters
5	[[5,1,3]]
9	[[9,3,3]]*
13	[[13,1,5]]
17	[[17,1,7]] , [[17,9,3]]
19	[[19,1,3]]*
25	[[25,1,4]] , [[25,5,3]]
27	[[27,21,2]]*, [[27,9,3]]*
29	[[29,1,5]]
37	[[37,1,5]]
41	[[41,1,7]] , [[41,21,4]]
53	[[53,1,7]]
57	[[57,21,5]]*, [[57,39,3]]*
61	[[61,1,7]]
65	[[65,5,13]]*, [[65,13,8]] , [[65,17,9]], [[65,17,11]]* , [[65,29,7]]† , [[65,41,5]]† , [[65,53,3]]†
67	[[67,1,7]]*
81	[[81,21,4]]*, [[81,75,2]]*
97	[[97,1,9]] , [[97,49,5]]
99	[[99,69,3]]*

TABLE I
EXPLICIT EXAMPLES OF FROBENIUS CODES OVER $\mathbb{F}_2$

VI. DECODING

Let $\mathcal{C}$ be a t-Frobenius code based on a degree d extension $\mathbb{F}_p(\eta)$ as in Theorem V.1. Let the code $\mathcal{C}$ have length n and BCH distance $\delta = 2\tau + 1$. Much like in the classical case, we show that there is an poly(n) time quantum algorithm to correct any quantum error of weight at most τ. We use two key algorithms: (1) Kitaev's phase estimation [17, 5.2] algorithm and (2) The Berlekamp decoding algorithm [18, p-98,6.7] for classical BCH codes.

Theorem VI.1 (Berlekamp)**.** *Let $h(X)$ be a factor of $X^n - 1$ of BCH distance $\delta = 2\tau + 1$ over a finite field $\mathbb{F}_q$, q and n coprime. Let $e(X)$ be any polynomial of weight at most τ over $\mathbb{F}_q$. Given a polynomial $r(X) = e(X) \mod h(X)$, there is a polynomial time algorithm to find $e(X)$.*

Let the canonical factorisation of the $\mathcal{C}$ be $g \cdot h$ so that its isotropic subspace is generated by the pair (g, ag) where $a = \sigma^i(\alpha\eta) \mod \sigma^i(h)$. Assume that we transmitted a quantum message $|\varphi\rangle \in \mathcal{C}$ over the quantum channel and received the corrupted state $|\psi\rangle = U_{\mathbf{u}} V_{\mathbf{v}} |\varphi\rangle$, where the vectors $\mathbf{u}$ and $\mathbf{v}$ are unknown but fixed for the rest of the section. We show that using quantum phase finding we can recover the polynomial $\alpha\eta u(X^{-1}) - v(X^{-1}) \mod h$ without disturbing $|\psi\rangle$. Provided the joint weight $\mathrm{w}(\mathbf{u}, \mathbf{v}) \leq \tau$ we can now find $\mathbf{u}$ and $\mathbf{v}$ using Berlekamp algorithm. The sent message is recovered by applying the inverse map $V_{\mathbf{v}}^\dagger U_{\mathbf{u}}^\dagger$ on $|\psi\rangle$. Hence we have the following theorem about decoding.

Theorem VI.2. *Let $\mathcal{C}$ be a t-Frobenius code, as in Theorem V.1, of length n and BCH distance $\delta = 2\tau + 1$. There is quantum algorithm that takes time polynomial in n to correct errors of weight at most τ.*

VII. CONCLUSION

In this paper, we studied cyclic stabiliser codes of length dividing $p^t + 1$ over $\mathbb{F}_p$. It is natural to ask whether the construction can be generalised for arbitrary code length. For higher degree extensions the gap between actual and BCH distance could be significant. Therefore, it would be interesting to find a better lower bound and in particular to know whether Berlekamp like algorithms can be used to decode up to that bound. Unlike previous definition of cyclicity, our definition is applicable to non-stabiliser codes as well. An open problem is to construct cyclic non-stabiliser codes.

REFERENCES

[1] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862–1868, 1996.

[2] P. W. Shor, "Scheme for reducing decoherence in quantum computing memory," *Phys. Rev. A*, vol. 52, pp. 2493–2496, 1995.

[3] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, p. 793, 1996.

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, pp. 3824–3851, 1996.

[5] R. Laflamme, C. Miquel, J. P. Paz, , and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, p. 198, 1996.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum Error Correction Via Codes Over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, 1998.

[7] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *Information Theory, IEEE Transactions on*, vol. 47, no. 7, pp. 3065 –3072, nov 2001.

[8] V. Arvind and K. R. Parthasarathy, "A family of stabilizer codes based on Weyl commutation relation over a finite field," *Volume in honor of C.S. Seshadri's 70th birthday*, pp. 133–153, 2003.

[9] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review Letters A*, vol. 54, pp. 1098–1105, 1996.

[10] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Royal Soc. A*, vol. 452, pp. 2551–77, 1996.

[11] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *Information Theory, IEEE Transactions on*, vol. 52, no. 11, pp. 4892 –4914, nov. 2006.

[12] A. Thangaraj and S. W. McLaughlin, "Quantum codes from cyclic codes over GF(4^m)," *IEEE Transactions on Information Theory*, vol. 47, no. 1, pp. 1176–1178, 2001.

[13] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical bch codes," *Information Theory, IEEE Transactions on*, vol. 53, no. 3, pp. 1183 –1188, march 2007.

[14] S. Dutta and P. P. Kurur, arXiv:1011.5814v2 [cs.IT].

[15] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Physical Review letters*, vol. 84, pp. 2525–2528, 2000.

[16] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Physical Review Letters*, vol. 78, no. 3, pp. 405–408, January 1997.

[17] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 2000.

[18] J. H. van Lint, *Introduction to Coding Theory*, 3^{rd} ed., ser. Graduate Texts in Mathematics. New York Inc: Springer-Verlag, 1998, vol. 86.