HAL
open science

On the decoding of quasi-BCH codes

Morgan Barbier, Clément Pernet, Guillaume Quintin

To cite this version:

Morgan Barbier, Clément Pernet, Guillaume Quintin. On the decoding of quasi-BCH codes. WCC - International Workshop on Coding and Cryptography, Apr 2013, Bergen, Norway. hal-00768566

HAL Id: hal-00768566

https://inria.hal.science/hal-00768566v1

Submitted on 21 Dec 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On the decoding of quasi-BCH codes

Morgan Barbier*
morgan.barbier@unicaen.fr

Clément Pernet†
clement.pernet@imag.fr

Guillaume Quintin‡
quintin@lix.polytechnique.fr

2012/12/21

Abstract

In this paper we investigate the structure of quasi-BCH codes. In the first part of this paper we show that quasi-BCH codes can be derived from Reed-Solomon codes over square matrices extending the known relation about classical BCH and Reed-Solomon codes. This allows us to adapt the Welch-Berlekamp algorithm to quasi-BCH codes. In the second part of this paper we show that quasi-BCH codes can be seen as subcodes of interleaved Reed-Solomon codes over finite fields. This provides another approach for decoding quasi-BCH codes.

keywords: Quasi-cyclic code, quasi-BCH code, BCH code, Reed-Solomon, interleaved code

1 Introduction

Many codes with best known minimum distances are quasi-cyclic codes or derived from them [LS03, Gra07]. This family of codes is therefore very interesting. Quasi-cyclic codes were studied and applied in the context of McEliece's cryptosystem [McE78, BCGO09] and Niederreiter's [Nie86, LDW94]. They permit to reduce the size of keys in opposition to Goppa codes. However, since the decoding of random quasi-cyclic codes is difficult, only quasi-cyclic alternant codes were proposed for the latter cryptosystem. The high structure of alternant codes is actually a weakness and two cryptanalysis were proposed in [FOPT10, UL10]

*Université de Caen - GREYC, Boulevard Maréchal Juin, BP 5186, 14032 Caen

†Univ. Joseph Fourier INRIA/LIG-MOAIS, 51 avenue Jean Kuntzmann, 38330 Montbonnot

‡École polytechnique - LIX, 91128 Palaiseau Cedex

1.1 Our contributions

In this paper we investigate the structure of quasi-BCH codes. In the first part of this paper we show that quasi-BCH codes can be derived from Reed-Solomon codes over square matrices. It is well known that BCH codes can be obtained from Reed-Solomon codes [MS86, Theorem 2, page 300]. We extend this property to quasi-BCH codes which allows us to adapt the Welch-Berlekamp algorithm to quasi-BCH codes.

Theorem 1. *Let $\Gamma \in M_{\ell\times\ell}(\mathbb{F}_{q^s})$ be a primitive m-th root of unity and $\mathcal{C} = \text{Q-BCH}_q(m,\ell,\delta,\Gamma)$. Then there exists a RRS code $\mathcal{R}$ over the ring $M_{\ell\times\ell}(\mathbb{F}_{q^s})$ with parameters $[n, n-\delta+1]_{M_{\ell\times\ell}(\mathbb{F}_{q^s})}$ and a $\mathbb{F}_q$-linear, F_q-isometric embedding $\psi : \mathcal{C} \to \mathcal{R}$.*

In the second part we show that quasi-BCH codes can be seen as subcodes of interleaved Reed-Solomon codes.

Theorem 2. *The quasi-BCH code $\mathcal{C}$ over $\mathbb{F}_q$ is an interleaved code of ℓ subcodes of Reed-Solomon codes over $\mathbb{F}_{q^{s'}}$ in the following sense: there exists ℓ Reed-Solomon codes $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ over $\mathbb{F}_q$ and an isometric isomorphism from $\mathcal{C}$, equipped with the ℓ-block distance, to a subcode of the interleaved code with respect to $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$.*

1.2 Related work

In [LF01, LS01], ℓ-quasi-cyclic codes of length $m\ell$ are seen as R-submodules of R^ℓ for a certain ring R. However, in [LF01], Gröbner bases are used in order to describe polynomial generators of quasi-cyclic codes whereas in [LS01], the authors decompose quasi-cyclic codes as direct sums of shorter linear codes over various extensions of $\mathbb{F}_q$ (when $\gcd(m,q) = 1$). This last work leads to an interesting trace representation of quasi-cyclic codes. In [CCN10], the approach is more analogous to the cyclic case. The authors consider the factorization of $X^m - 1 \in M_\ell(F_q)[X]$ with reversible polynomials in order to construct ℓ-quasi-cyclic codes canceled by those polynomials and called $\Omega(P)$-codes. This leads to the construction of self-dual codes and codes beating known bounds. But the factorization of univariate polynomials over a matrix ring remains difficult. In [Cha11] the author gives an improved method for particular cases of the latter factorization problem.

2 Prerequisites

2.1 Reed-Solomon codes over rings

We recall some basic definitions of Reed-Solomon codes over rings in this section. We let A be a ring with identity, we denote by $A^\times$ the *group of units* of A and by $Z(A)$ the *center* of A, the commutative subring of A consisting of all the elements of A which commutes with all the other elements of A. We denote by

$A[X]$ the ring of polynomials over A and by $A[X]_{<k}$ the polynomials over A of degree at most $k-1$.

Definition 1. *Let*

$$f = \sum_{i=0}^{d} f_i X^i \in A[X]$$

be a polynomial with coefficients in A and $a \in A$. We call left evaluation of f at a *the quantity*

$$f(a) := \sum_{i=0}^{d} f_i a^i \in A$$

and right evaluation of f at a *the quantity*

$$(a)f := \sum_{i=0}^{d} a^i f_i \in A.$$

Remark 1. *For $f, g \in A[X]$ and $a \in A$, we obviously have $f(a) = (a)f$ whenever $a \in Z(A)$, $(f+g)(a) = f(a) + g(a)$, $(a)(f+g) = (a)f + (a)g$. If a commutes with all the coefficients of g we also have $(fg)(a) = f(a)g(a)$ and $(a)(gf) = (a)g(a)f$.*

Definition 2. *Let $0 < k \leq n$ be two integers. Let $(x_1, \ldots, x_n)$ and $v = (v_1, \ldots, v_n)$ be two vectors of A^n be such that $x_i - x_j \in A^\times$ and $x_i x_j = x_j x_i$ for all $i \neq j$ and $v_i \in A^\times$ for all i.*

The left *submodule of A^n generated by the vectors*

$$(f(x_1) \cdot v_1, \ldots, f(x_n) \cdot v_n) \in A^n \text{ with } f \in A[X]_{<k}$$

is called a left generalized Reed-Solomon code (LGRS) over A with parameters $[v, x, k]_A$ *or* $[n, k]$ *if there is no confusion on x and v.*

The right *submodule of A^n generated by the vectors*

$$(v_1 \cdot (x_1)f, \ldots, v_n \cdot (x_n)f) \in A^n \text{ with } f \in A[X]_{<k}$$

is called a right generalized Reed-Solomon code (RGRS) over A with parameters $[v, x, k]_A$ *or* $[n, k]$ *if there is no confusion on x and v. The vector x is called the* support *of the code. If $v = (1, \ldots, 1)$, the codes constructed above are called left Reed-Solomon (LRS) and right Reed-Solomon (RRS) codes.*

Definition 3. *Let $x = (x_1, \ldots, x_n) \in A^n$. We call the* Hamming weight of x *the number of nonzero coordinates.*

$$w(x) := w(x_1, \ldots, x_n) = |\{i : x_i \neq 0\}|.$$

Let $y = (y_1, \ldots, y_n) \in A^n$. The Hamming distance between x and y *is*

$$d(x, y) = w(x - y) = |\{i : x_i \neq x_j\}|.$$

The minimum distance *of any subset $S \subseteq A^n$ is defined as*

$$\min\{d(x, y) : x, y \in S \text{ and } x \neq y\}.$$

Proposition 1. *A LGRS (resp. RGRS) code is a free left (resp. right) submodule of A^n. A LGRS (resp. RGRS) code with parameters $[n, k]$ has minimum distance $n - k + 1$.*

Proof. It suffices to see that the maps

$$\begin{array}{rcl} A^n & \longrightarrow & A^n \\ (a_1, \ldots, a_n) & \longmapsto & (a_1 v_1, \ldots, a_n v_n) \\ (a_1, \ldots, a_n) & \longmapsto & (v_1 a_1, \ldots, v_n a_n) \end{array}$$

are respectively left and right isometric automorphisms of A^n. □

2.2 Quasi cyclic and quasi BCH codes

Quasi cyclic codes form an important family of codes defined as follow.

Definition 4. *Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ to be the left cyclic shift defined by*

$$T(c_1, c_2, \ldots, c_n) = (c_2, c_3, \ldots, c_1).$$

We call ℓ-quasi-cyclic code over $\mathbb{F}_q$ of length n *any code of length n over $\mathbb{F}_q$ stable by T^ℓ. If the context is clear we will simply say* ℓ-quasi-cyclic code.

We will focus in this paper on quasi-BCH codes which form a subfamily of quasi-cyclic codes. They can be seen as a generalization of BCH codes in the context of quasi-cyclic codes. For we need primitive roots of unity defined in a extension of $\mathbb{F}_q$, say $\mathbb{F}_{q^s}$ to construct BCH codes over $\mathbb{F}_q$.

Proposition 2. *Then there exists a primitive $q^{s\ell}-1$-th root of unity in $M_\ell(\mathbb{F}_{q^s})$.*

Proof. The proof can be found in [BCQ12b, Proposition 16, page 911]. □

Definition 5. *Let Γ be a primitive m-th root of unity in $M_\ell(\mathbb{F}_{q^s})$ and $\delta \leq m$. We define the ℓ-quasi-BCH code of length $m\ell$, with respect to Γ, with designed minimum distance δ, over $\mathbb{F}_q$ by*

$$\text{Q-BCH}_q(m, \ell, \delta, \Gamma) := \left\{ (c_1, \ldots, c_m) \in (\mathbb{F}_q^\ell)^m : \sum_{j=0}^{m-1} (\Gamma^i)^j (c_{j+1})^T = 0 \text{ for } i = 1, \ldots, \delta - 1 \right\}.$$

Note that $\text{Q-BCH}_q(m, \ell, \delta, \Gamma)$ *is a quasi-cyclic code.*

Definition 6. *The* ℓ-block weight *of $(x_{11}, \ldots, x_{1\ell}, \ldots, x_{m1}, \ldots, x_{m\ell}) \in \mathbb{F}_q^{m\ell}$ is defined to be*

$$\text{Block-w}_\ell(x) := |\{i : (x_{i1}, \ldots, x_{i\ell}) \neq 0\}|.$$

The ℓ-block distance *between $x, y \in \mathbb{F}_q^{m\ell}$ is defined to be* $\text{Block-w}_\ell(x - y)$.

3 Reed-Solomon codes and quasi-BCH codes

3.1 The relation between quasi-BCH and Reed-Solomon codes

We show in this section that under certain assumptions on the support of Reed-Solomon codes, the dual of a LRS code is a RRS code. From this fact we show that quasi-BCH can be constructed from Reed-Solomon codes over square matrices rings. In this Subsection we let A designate a finite ring with identity.

Definition 7. *Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two vectors of A^n. The* inner product *is defined as*

$$\langle x, y \rangle := \sum_{i=0}^{n} x_i y_i.$$

Remark 2. *Let S be a subset of A^n. Then the set $\{x \in A^n : \forall s \in S, \langle s, x \rangle = 0\}$ denoted by $S^{\perp}$ is called the* right dual of S *and is a right submodule of A^n. Similarly, Let S be a subset of A^n. Then the set $\{x \in A^n : \forall s \in S, \langle x, s \rangle = 0\}$ denoted by ${}^{\perp}S$ is called the* left dual of S *and is a left submodule of A^n. Note that for all $x, y \in A^n$ and $\mu \in A$ we have $\mu \langle x, y \rangle = \langle \mu x, y \rangle$ and $\langle x, y \rangle \mu = \langle x, y\mu \rangle$.*

Definition 8. *We say that $a \in A$ is a* primitive m-th root of unity *if $a^m = 1$ and $\forall 0 \leq i < m, (a^i - 1) \in A^{\times}$.*

Remark 3. *Let $x = (1, \gamma, \gamma^2, \ldots, \gamma^{m-1}) \in A^m$ where γ is a primitive m-th root of unity. Then a RRS or LRS code whose support is x is cyclic.*

Proposition 3. *Let $\gamma \in A$ be a primitive m-th root of unity. Let $x = (1, \gamma, \gamma^2, \ldots, \gamma^{m-1}) \in A^n$. Then the right (resp. left) dual of the LGRS (resp. RGRS) code with parameters $[x, x, k]_A$ is the RRS (resp. LRS) code with parameters $[x, n-k]_A$.*

Proof. We denote respectively by $\mathcal{L}$ and $\mathcal{R}$ the left generalized Reed-Solomon code with parameters $[x, x, k]_A$ and the right Reed-Solomon code with parameters $[x, n-k]_A$.

First note that $\mathcal{L}$ is generated by the vectors

$$(1, \gamma^i, \gamma^{2i}, \ldots, \gamma^{(m-1)i}) \text{ for } i = 1, \ldots, k$$

and that $\mathcal{R}$ is generated by the vectors

$$(1, \gamma^i, \gamma^{2i}, \ldots, \gamma^{(m-1)i}) \text{ for } i = 0, \ldots, n-k-1.$$

And we have for $0 \leq i + j < n - 1$ in the commutative ring $Z(A)[\gamma]$

$$\sum_{i=0}^{m-1} \gamma^{(i+1)\ell} \cdot \gamma^{j\ell} = \sum_{i=0}^{m-1} \left(\gamma^{i+j+1}\right)^{\ell} = \frac{1 - \left(\gamma^{i+j+1}\right)^m}{1 - \gamma^{i+j+1}} = 0.$$

Therefore, by Proposition 1 and Remark 2, $\mathcal{L}^\perp \subseteq \mathcal{R}$ and ${}^\perp\mathcal{R} \subseteq \mathcal{L}$.

Again by Proposition 1 and Remark 2 an element $x \in A^n$ lies in $\mathcal{L}^\perp$ if and only if

$$\left[\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \gamma & \gamma^2 & \dots & \gamma^{m-1} \\ 1 & \vdots & \vdots & & \vdots \\ 1 & \gamma^{k-1} & \gamma^{2(k-1)} & \dots & \gamma^{(k-1)(m-1)} \end{pmatrix} \begin{pmatrix} 1 & & & \\ & \gamma & & \\ & & \ddots & \\ & & & \gamma^{m-1} \end{pmatrix}\right] \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0. \tag{1}$$

But in the commutative ring $Z(A)[\gamma]$ the matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \gamma & \gamma^2 & \dots & \gamma^{2(k-1)} \\ 1 & \vdots & \vdots & & \vdots \\ 1 & \gamma^{k-1} & \gamma^{2(k-1)} & \dots & \gamma^{(k-1)(k-1)} \end{pmatrix} \in M_{k\times k}\left(Z(A)[\gamma]\right)$$

is invertible. Therefore H is also invertible in $M_{k\times k}(A)$ and thus induces a group automorphism of A^k. If we let $x_H = (x_1, \dots, x_k)$, $x_U = (x_{k+1}, \dots, x_n)$, we can rewrite equation (1) as

$$\left(\begin{array}{c|c} H & U \end{array}\right)\left(\frac{x_H}{x_U}\right) = 0 \text{ and } \left(\begin{array}{c|c} H & 0 \end{array}\right)\left(\frac{x_H}{0}\right) = -\left(\begin{array}{c|c} 0 & U \end{array}\right)\left(\frac{0}{x_U}\right).$$

For each choice of x_U we have only one possible value for x_H. Thus $|\mathcal{L}^\perp| = |A|^{n-k} = |\mathcal{R}|$ by Proposition 1 and therefore $\mathcal{L}^\perp = \mathcal{R}$. Similarly, we have ${}^\perp\mathcal{R} = \mathcal{L}$. □

Theorem 3. *Let $\Gamma \in M_{\ell\times\ell}(\mathbb{F}_{q^s})$ be a primitive m-th root of unity and $\mathcal{C} =$ Q-BCH$_q(m, \ell, \delta, \Gamma)$. Then there exists a RRS code $\mathcal{R}$ over the ring $M_{\ell\times\ell}(\mathbb{F}_{q^s})$ with parameters $[n, n-\delta+1]_{M_{\ell\times\ell}(\mathbb{F}_{q^s})}$ and a $\mathbb{F}_q$-linear, F_q-isometric embedding $\psi : \mathcal{C} \to \mathcal{R}$.*

Proof. A parity-check matrix of $\mathcal{C}$ is

$$H = \begin{pmatrix} I_\ell & \Gamma & \dots & \Gamma^{m-1} \\ I_\ell & \Gamma^2 & \dots & \Gamma^{2(m-1)} \\ \vdots & \vdots & & \vdots \\ I_\ell & \Gamma^{\delta-1} & \dots & \Gamma^{(\delta-1)(m-1)} \end{pmatrix} \in M_{(\delta-1)\ell, m\ell}(\mathbb{F}_{q^s}).$$

Remark that H is a generator matrix of the LGRS code with parameters $[x, x, \delta-1]_{M_{\ell\times\ell}(\mathbb{F}_{q^s})}$ over the ring $M_{\ell\times\ell}(\mathbb{F}_{q^s})$ and by Proposition 3 its dual is the RRS with parameters $[x, \delta-1]_{M_{\ell\times\ell}(\mathbb{F}_{q^s})}$.

Now let

$$\begin{array}{rcl} \psi : \mathcal{C} & \longrightarrow & (M_{\ell\times\ell}(\mathbb{F}_{q^s}))^m \\ (c_{11}, \dots, c_{1\ell}, \dots, c_{m1}, \dots, c_{m\ell}) & \longmapsto & \left[\begin{pmatrix} c_{11} & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ c_{1\ell} & 0 & \dots & 0 \end{pmatrix}, \dots, \begin{pmatrix} c_{m1} & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ c_{m\ell} & 0 & \dots & 0 \end{pmatrix}\right]. \end{array}$$

Obviously, ψ is $\mathbb{F}_q$-linear, injective and isometric and by the above remark we have $\psi(\mathcal{C}) \subseteq \mathcal{R}$. $\square$

Theorem 3 generalizes the well-known [MS86, Theorem 2, page 300] relation between BCH codes and Reed-Solomon codes. The above relation will allow us to adapt the unique decoding algorithm from [BCQ12a] to quasi-BCH codes.

3.2 The Welch-Berlekamp algorithm for quasi-BCH codes

In this Subsection we let A designate a finite ring with identity. Before giving the Welch-Berlekamp decoding algorithm, we need to define what the *evaluation* of a bivariate polynomial over A is. Let $Q = \sum Q_{i,j} X^i Y^j \in A[X,Y]$ be such a polynomial. We define the *evaluation of Q at $(a,b) \in A^2$* to be

$$(a,b)Q = \sum a^i b^j Q_{i,j} \in A.$$

Be careful of the order of a, b and $Q_{i,j}$. This choice will be explained in the proof of Lemma 1. Let $f \in A[X]$, we define *the evaluation of Q at f* to be

$$(X, f(X))Q = \sum X^j (f(X))^j Q_{i,j} \in A[X].$$

As in the univariate case, the evaluation maps defined above are not ring homomorphisms in general.

Lemma 1. *Let $g \in A[X]$, $Q \in A[X,Y]$ of degree at most 1 in Y and $a \in A$. Then*

$$(a)((X, g(X))Q) = (a, (a)g)Q.$$

Proof. We write

$$\begin{aligned} Q(X,Y) &= Q_0(X) + Q_1(X)Y \\ &= Q_0(X) + \left(\sum_i Q_{1i} X^i \right) Y. \end{aligned}$$

The proof is an easy calculation:

$$\begin{aligned} (a)((X, g(X))Q) &= (a) \left(Q_0(X) + \sum_i X^i g(X) Q_{1i} \right) \\ &= (a)Q_0 + \sum_i a^i (a) g Q_{1i} \\ &= (a, (a)g)Q \text{ by definition.} \end{aligned}$$

$\square$

We let $\mathcal{C} = \text{Q-BCH}_q(m, \ell, \delta, \Gamma)$, $\tau = \left\lfloor \frac{\delta-1}{2} \right\rfloor$, $n = m$, $k = n - \delta + 1$ and

$$\begin{array}{rcl} \text{pr} : (M_{\ell\times\ell}(\mathbb{F}_{q^s}))^m & \longrightarrow & \mathbb{F}_q^{m\ell} \\ \left[\begin{pmatrix} a_{11}^1 & \dots & a_{1\ell}^1 \\ \vdots & & \vdots \\ a_{\ell 1}^1 & \dots & a_{\ell\ell}^1 \end{pmatrix}, \dots, \begin{pmatrix} a_{11}^m & \dots & a_{1\ell}^m \\ \vdots & & \vdots \\ a_{\ell 1}^m & \dots & a_{\ell\ell}^m \end{pmatrix} \right] & \longmapsto & (a_{11}^1, \dots, a_{\ell 1}^1, \dots, a_{11}^m, \dots, a_{\ell 1}^m). \end{array}$$

Algorithm 1 Welch-Berlekamp for quasi-BCH codes

Input: a received vector $y \in \mathbb{F}_q^{m\ell}$ with at most τ errors.
Output: the unique codeword within distance τ of y.

1: $(Z_1, \dots, Z_m) \leftarrow \psi(y)$ where ψ is the map from Theorem 3.
2: Find $Q = Q_0(X) + Q_1(X)Y \in (M_{\ell\times\ell}(\mathbb{F}_{q^s})[X])[Y]$ of degree 1 such that

1. $(\Gamma^{i-1}, Z_i)Q = 0$ for all $i = 1, \dots, m-1$,
2. $\deg Q_0 \leq n - \tau - 1$,
3. $\deg Q_1 \leq n - \tau - 1 - (k-1)$.

3: $f \leftarrow$ the unique root of Q in $(M_{\ell\times\ell}(\mathbb{F}_{q^s}))[X]_{<k}$ such that $d\left((Z_1, \dots, Z_m), ((I_\ell)f, \dots, (\Gamma^{m-1})f)\right) \leq \tau$.
4: **return** $\text{pr}\left((I_\ell)f, (\Gamma)f, \dots, (\Gamma^{m-1})f\right)$.

Lemma 2. *Let $y \in \mathbb{F}_q^{m\ell}$ be a received word containing at most τ errors. Then there exists a nonzero bivariate polynomial $Q = Q_0 + Q_1 Y \in (M_{\ell\times\ell}(\mathbb{F}_{q^s}))[X, Y]$ satisfying*

1. $(\Gamma^{i-1}, Z_i)Q = 0$ *for* $i = 1, \dots, n$.
2. $\deg Q_0 \leq n - \tau - 1$.
3. $\deg Q_1 \leq n - \tau - 1 - (k-1)$.

Proof. We solve the problem with linear algebra over $\mathbb{F}_{q^s}$. We have, for each column of the solution, $n\ell$ equations and $\ell\left[(n-\tau) + (n-\tau-(k-1))\right] = \ell(n+1)$ unknowns by Proposition 1. □

Lemma 3. *Let $Q \in (M_{\ell\times\ell}(\mathbb{F}_{q^s}))[X, Y]$ satisfying the three conditions of Lemma 2 and $f \in (M_{\ell\times\ell}(\mathbb{F}_{q^s}))[X]_{<k}$ be such that $d((Z_1, \dots, Z_m), ((I_\ell)f, \dots, (\Gamma^{m-1})f)) \leq \tau$. Then $(X, f(X))Q = 0$.*

Proof. The polynomial $(X, f(X))Q$ has degree at most $n - \tau - 1$. By Lemma 1 we have $(\Gamma^{i-1})((X, f(X))Q) = (\Gamma^{i-1}, (\Gamma^{i-1})f)Q = (\Gamma^{i-1}, Z_i)Q = 0$ for at least $n - \tau$ values of $i \in \{1, \dots, n\}$. And therefore we must have $(X, f(X))Q = 0$. □

Proposition 4. *Algorithm 1 works correctly as expected and can correct up to $\left\lfloor \frac{\delta-1}{2} \right\rfloor$ errors.*

Proof. This is a direct consequence of Lemmas 2 and 3. □

4 Quasi-BCH codes as interleaved codes

In this Section we prove that quasi BCH codes can be viewed as an interleaving of classical BCH codes. We fix for this Section $\Gamma \in M_{\ell\times\ell}(\mathbb{F}_{q^s})$ a primitive m-th root of unity and $\mathcal{C} = \text{Q-BCH}_q(m, \ell, \delta, \Gamma)$. We first recall the definition of interleaved codes.

Definition 9. *Let $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ be error correcting codes over $\mathbb{F}_q$. The* interleaved code $\mathcal{C}$ with respect to $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ *is a subset of $M_{\ell\times m}(\mathbb{F}_q)$, equipped with the ℓ-bloc distance with respect to the columns, such that $c \in \mathcal{C}$ if and only if the i-th row of c is a codeword of $\mathcal{C}_i$ for $i = 1, \ldots, \ell$.*

Lemma 4. *The matrix Γ diagonalizes over an extension of $\mathbb{F}_{q^s}$ and its eigenvalues are all primitive m-th roots of unity.*

Proof. Let $\mathbb{F}_{q^{s'}} \supseteq \mathbb{F}_{q^s}$ be the splitting field of $X^m - 1$. The polynomial $X^m - 1$ is a multiple of the minimal polynomial $\mu(X)$ of Γ. Hence the egeinvalues of Γ are m-roots of unity. Let $P \in \text{GL}_\ell(\mathbb{F}_{q^{s'}})$ be such that $P^{-1}\Gamma P$ is diagonal. Now if an eigenvalue λ_i of Γ has order $d < m$, then

$$P^{-1}(\Gamma^d - I_\ell)P = \begin{pmatrix} \lambda_1^d & & & & \\ & \ddots & & & \\ & & \lambda_i^d & & \\ & & & \ddots & \\ & & & & \lambda_\ell^d \end{pmatrix} - I_\ell$$

is singular as its i-th diagonal element would be zero. Consequently $\Gamma^d - I_\ell \notin \text{GL}_\ell(\mathbb{F}_{q^{s'}})$ which is absurd. □

Theorem 4. *The quasi-BCH code $\mathcal{C}$ over $\mathbb{F}_q$ is an interleaved code of ℓ subcodes of Reed-Solomon codes over $\mathbb{F}_{q^{s'}}$ in the following sense: there exists ℓ Reed-Solomon codes $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ over $\mathbb{F}_q$ and an isometric isomorphism from $\mathcal{C}$, equipped with the ℓ-block distance, to a subcode of the interleaved code with respect to $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$.*

Proof. We take the notation of the proof of Lemma 4. Recall that

$$H = \begin{pmatrix} I_\ell & \Gamma & \cdots & \Gamma^{m-1} \\ I_\ell & \Gamma^2 & \cdots & \Gamma^{2(m-1)} \\ \vdots & \vdots & & \vdots \\ I_\ell & \Gamma^{\delta-1} & \cdots & \Gamma^{(\delta-1)(m-1)} \end{pmatrix} \in M_{(\delta-1)\ell, m\ell}(\mathbb{F}_{q^s})$$

is a parity check matrix for $\mathcal{C}$ (proof of Theorem 3). By Lemma 4 we have that

$$(c_{11},\dots,c_{1\ell},\dots,c_{m1},\dots,c_{m\ell})\in\mathcal{C}\iff$$
$$\begin{pmatrix} P^{-1} & & \\ & \ddots & \\ & & P^{-1}\end{pmatrix}\begin{pmatrix} I_\ell & \Gamma & \cdots & \Gamma^{m-1}\\ I_\ell & \Gamma^2 & \cdots & \Gamma^{2(m-1)}\\ \vdots & \vdots & & \vdots\\ I_\ell & \Gamma^{\delta-1} & \cdots & \Gamma^{(\delta-1)(m-1)}\end{pmatrix}\begin{pmatrix} P & & \\ & \ddots & \\ & & P\end{pmatrix}\times$$
$$\left[\begin{pmatrix} P^{-1} & & \\ & \ddots & \\ & & P^{-1}\end{pmatrix}\begin{pmatrix} c_{11}\\ \vdots\\ c_{1\ell}\\ \vdots\\ c_{m1}\\ \vdots\\ c_{m\ell}\end{pmatrix}\right]=0$$
$$\text{and } (c_{11},\dots,c_{1\ell},\dots,c_{m1},\dots,c_{m\ell})\in\mathbb{F}_q^{m\ell}$$

Let

$$\begin{pmatrix} v_{11}\\ \vdots\\ v_{1\ell}\\ \vdots\\ v_{m1}\\ \vdots\\ v_{m\ell}\end{pmatrix}=\begin{pmatrix} P^{-1} & & \\ & \ddots & \\ & & P^{-1}\end{pmatrix}\begin{pmatrix} c_{11}\\ \vdots\\ c_{1\ell}\\ \vdots\\ c_{m1}\\ \vdots\\ c_{m\ell}\end{pmatrix}\tag{2}$$

Denote by σ the application defined by equation (2). Then

$$(c_{11},\dots,c_{1\ell},\dots,c_{m1},\dots,c_{m\ell})\in\mathcal{C}\iff$$
$$\sigma^{-1}(v_{11},\dots,v_{1\ell},\dots,v_{m1},\dots,v_{m\ell})\in\mathbb{F}_q^{m\ell}\text{ and for } i=1,\dots,\ell$$
$$\begin{pmatrix} 1 & \lambda_i & \dots & \lambda_i^{m-1}\\ 1 & \lambda_i^2 & \dots & \lambda_i^{2(m-1)}\\ \dots & \dots & \dots & \dots\\ 1 & \lambda_i^{\delta-1} & \dots & \lambda_i^{(\delta-1)(m-1)}\end{pmatrix}\begin{pmatrix} v_{1i}\\ \vdots\\ v_{mi}\end{pmatrix}=0.\tag{3}$$

Then it is straightforward that σ is an isometric isomorphism from $\mathcal{C}$ equipped with the ℓ-block distance and $\sigma(\mathcal{C})$, which is by equation (3) a subcode of the interleaved code with respect to ℓ subcodes of Reed-Solomon codes over $\mathbb{F}_q$. For $i=1,\dots,\ell$ take $\mathcal{C}_i$ to be the Reed-Solomon code defined by the parity check matrix of equation (3). □

Note that if the minimal polynomial of Γ has degree one: $\Gamma = X-\lambda$, then $s'=s$ and Γ diagonalizes as λI_ℓ. Consequently the Reed-Solomon codes

$\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ are isomorphic, as they are defined by the same control equations in equation (3). In such a case, we can apply the result on the correction capacity for interleaved Reed-Solomon codes [SSB06, BKY07].

Corollary 1. *There exists a decoding algorithm that is guaranteed to correct up to* $\frac{\delta-1}{2}$ *errors. In particular, if the minimal polynomial of* Γ *has degree* 1 *over* $\mathbb{F}_{q^s}$ *then it can correct up to* $\frac{\ell}{\ell+1}(\delta-1)$ *errors with high probability.*

Proof. Taking the notation of Theorem 4 and if $y = c+e$ is a received word, one can decode $\sigma(y)$ with the decoding algorithms of $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ obtaining $c' \in \mathbb{F}_{q^{s'}}^{m\ell}$. Then $c = \sigma^{-1}(c')$.

If the minimal polynomial of Γ has degree 1, then $\mathcal{C}_1 = \mathcal{C}_2 = \cdots = \mathcal{C}_\ell$ and one can apply the algorithm of [BKY07] or [SSB06]. □

References

[BCGO09] T. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing Key Length of the McEliece Cryptosystem. In *Proceedings of the 2nd International Conference on Cryptology in Africa: Progress in Cryptology*, AFRICACRYPT '09, pages 77–97, Berlin, Heidelberg, 2009. Springer-Verlag.

[BCQ12a] M. Barbier, C. Chabot, and G. Quintin. On Generalized Reed-Solomon Codes Over Commutative and Noncommutative Rings, 2012.

[BCQ12b] M. Barbier, C. Chabot, and G. Quintin. On quasi-cyclic codes as a generalization of cyclic codes. *Finite Fields and Their Applications*, 18(5):904–919, 2012.

[BKY07] D. Bleichenbacher, A Kiayias, and M. Yung. Decoding interleaved Reed-Solomon codes over noisy channels. *Theoretical Computer Science*, 379(3):348–360, 2007. Automata, Languages and Programming.

[CCN10] P.-L. Cayrel, C. Chabot, and A. Necer. Quasi-cyclic codes as codes over rings of matrices. *Finite Fields and Their Applications*, 16(2):100–115, 2010.

[Cha11] C. Chabot. Factorisation in $M_\ell(\mathbb{F}_q)[X]$. Construction of quasi-cyclic codes. In *WCC 2011 - Workshop on coding and cryptography*, pages 209–218, Paris, France, apr 2011.

[FOPT10] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece Variants with Compact Keys. In Henri Gilbert, editor, *Advances in Cryptology EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 279–298. Springer Berlin / Heidelberg, 2010.

[Gra07] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, 2007. Accessed on 2011-04-19.

[LDW94] Y. X. Li, R. H. Deng, and X. M. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Trans. Inform. Theory*, 40(1):271–273, January 1994.

[LF01] K. Lally and P. Fitzpatrick. Algebraic structure of quasicyclic codes. *Discrete Applied Mathematics*, 111(1–2):157–175, 2001.

[LS01] S. Ling and P. Solé. On the algebraic structure of quasi-cyclic codes .I. Finite fields. *IEEE Trans. Inform. Theory*, 47(7):2751–2760, nov 2001.

[LS03] S. Ling and P. Solé. Good self-dual quasi-cyclic codes exist. *IEEE Trans. Inform. Theory*, 49(4):1052–1053, april 2003.

[McE78] R. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114–116, 1978.

[MS86] F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland mathematical library. North-Holland, 1986.

[Nie86] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[SSB06] G. Schmidt, V. Sidorenko, and M. Bossert. Error and Erasure Correction of Interleaved ReedSolomon Codes. In Øyvind Ytrehus, editor, *Coding and Cryptography*, volume 3969 of *Lecture Notes in Computer Science*, pages 22–35. Springer Berlin / Heidelberg, 2006.

[UL10] V. G. Umaña and G. Leander. Practical Key Recovery Attacks On Two McEliece Variants. In Carlos Cid and Jean-Charles Faugére, editors, *Proceedings of the Second International Conference on Symbolic Computation and Cryptography*, pages 27–44, June 2010.