Linear codes over finite rings are trace codes

Yaqi Lu, Minjia Shi, Marcus Greferath, Patrick Solé

Linear Codes over Finite Rings are Trace Codes

Yaqi Lu*, Minjia Shi†, Marcus Greferath‡, Patrick Solé§

April 16, 2020

Abstract: Linear codes over finite rings are described here as trace codes for a suitable generalization of the trace called a GF-trace. Cyclic codes over Galois rings are given a trace description as well. The main tools are the notion of trace dual bases, in the case of linear codes, and of normal bases of an extension ring over a ring, in the case of cyclic codes.

Keywords: Finite ring · GF-trace · basis · linear codes · cyclic codes · trace representation

MSC (2010): Primary 68P30, Secondary 11T71.

1 Introduction

In recent years, trace codes over finite rings have been very successful in producing new classes of few weight codes [4, 5, 6, 7, 8] (see section 4 below for a technical definition of trace codes and defining sequences). This prompts the question of the genericity of the construction: can all linear codes over a large class of finite rings be described as trace codes, for a suitable definition of the trace and suitable defining sequences? For the class of finite fields this question was answered to the affirmative in [11].

In the present paper, we solve this problem for the class of all finite rings. The trace we employ here is the Generalized Frobenius trace (hereby called GF-trace)

*This research is supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20).

†School of Mathematical Sciences of Anhui University, Anhui, 230601, P. R. China.

‡School of Mathematics and Statistics, University College Dublin, Ireland

§CNRS/I2M, University of Aix-Marseille Centrale Marseille, Marseille, France.

introduced in [2]. It coincides with the trace defined in an ad hoc manner for the special ring alphabets of [4, 5, 6, 7, 8].

In the special case of cyclic codes over Galois rings, we give a similar description. Important technical tools are the notions of trace dual basis, in the case of linear codes, and of normal basis in the case of cyclic codes. Note that normal bases over Galois rings are defined in [12], and, in a more algorithmic way in [3]. There is no generalization of that concept at the level of general finite rings.

The material is organized as follows. In the following section, we will collect a few basic facts regarding Linear Algebra on a finite ring. Section 3 develops the theory of the GF-trace as far as needed. Section 4 covers linear codes over finite rings, and Section 5 considers cyclic codes in particular. Section 6 concludes the article, and mentions some challenging open problems.

2 Preliminaries

All rings that we are dealing with in this article are associative rings with identity, usually denoted by 1. A ring S is called a *unital extension* of the ring R, if R is a unital subring of S, which means that R and S share the identity.

Unless specified otherwise, we assume that all rings are finite. Linear Algebra on finite rings allows for stronger statements than possible for the class of rings in general. This is based on purely combinatorial arguments.

Remark 1. Let R be a finite ring and let n be a positive integer. For an n-element subset B of R^n the following are equivalent:

(a) B is a basis of ${}_RR^n$.

(b) B is linearly independent in ${}_RR^n$.

(c) B is a generating set of ${}_RR^n$.

For the proof the reader is referred to any standard text on finite rings and modules.

In a similar spirit, we have the following statement on $n \times n$-matrices over the finite ring R.

Remark 2. Let R be a finite ring and let n be a positive integer. For an $n \times n$-matrix A over R the following are equivalent:

(a) A is invertible.

(b) A represents an injective linear mapping of ${}_R R^n$.

(c) A represents a surjective linear mapping of ${}_R R^n$.

(b') A represents an injective linear mapping of R_R^n.

(c') A represents a surjective linear mapping of R_R^n.

In terms of systems of linear equations, the previous statements take the following form.

Remark 3. Let R be a finite ring. The system of linear equations

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = & 0 \\ \vdots \qquad\qquad\quad \vdots & \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = & 0 \end{cases}$$

with coefficients $a_{ij} \in R$ for $i, j \leq n$, has a nontrivial solution if and only if the columns of the matrix $(a_{ij})_{i,j \leq n}$ are right linearly dependent elements of R_R^n.

3 Trace functions on finite rings

Definition 4 (see [2, Def. 10])**.** Let S be a finite ring that is a unital extension of the ring R. A homomorphism of left and right R-modules $\mathrm{Tr} : S \longrightarrow R$ is called a *generalized Frobenius trace* (GF-trace) from S to R if

(i) Tr is surjective, which means $\mathrm{Im}(\mathrm{Tr}) = R$, and

(ii) $\mathrm{Ker}(\mathrm{Tr})$ does not contain any nonzero left or right ideal of S.

To avoid misunderstandings, we denote such a trace also by the symbol Tr_R^S, whereas we omit this addition, whenever such a misunderstanding is excluded. A careful treatment of ring extensions and according trace functions can be found in the recent paper [9] by J. G.-Torrecillas et al.

The notion of generalized Frobenius trace in closely related to the concept of *Frobenius Functional* in the paper [10] by Nakayama and Tsuzuku. In that paper, they are introduced as an extension of the former notion of Frobenius functional over a field.

In fact, a Frobenius functional is a GF-trace Tr, such that the right S-module $\mathrm{Hom}(S_R, R_R)$ is generated by Tr. Using the dual bases that we introduce in section 4, it can be proved that GF-traces are indeed Frobenius functionals if S is free over R. For details, see the mentioned paper [10, p. 12].

Regarding the existence of extensions that allow for a GF-trace, a few things can be stated in slight generalization of ideas presented in J. Wood [13].

To start with, a finite ring R is called a *Frobenius ring* if its character bi-module $\widehat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$ is a free left R-module [1, 2, 14]. Equivalently it can be defined as a unital ring extension of its characteristic subring $\mathbb{Z}_k$ (where k is the additive order of the identity of R), such that a GF-trace onto this subring exists. This and the following remark was the deeper reason for this paper to investigate into ring extensions that allow for a GF-trace.

Remark 5. If the (finite) unital extension S of the finite Frobenius ring R allows for a GF-trace from S onto R, then S will be a Frobenius ring as well.

Proof. For a proof assume $\mathrm{Tr} : S \longrightarrow R$ is an R-linear GF-trace from S onto R, and $\mathrm{tr} : R \longrightarrow \mathbb{Z}_m$ is a $\mathbb{Z}_m$-linear trace of R onto its characteristic subring $\mathbb{Z}_m$. It is then clear that $T := \mathrm{tr} \circ \mathrm{Tr}$ is surjective onto $\mathbb{Z}_m$ and clearly $\mathbb{Z}_m$-linear. To show that $\ker(T)$ does not contain any proper left (or right) ideal of S, let $I \subseteq \ker(T)$ be a left (or right) ideal. This means, I is a left S-submodule of S contained in $\ker(T)$, and we need to show that $I = 0$. First, we observe that $\mathrm{Tr}(I)$ is a left R-submodule of R, because Tr is R-linear, and I is certainly a left R-submodule of S. In particular, $\mathrm{Tr}(I)$ is a left $\mathbb{Z}_m$-submodule of R. Now note that $I \subseteq \ker(T)$ implies that $\mathrm{Tr}(I) \subseteq \ker(\mathrm{tr})$. As tr is a $\mathbb{Z}_m$-linear trace, we conclude that $\mathrm{Tr}(I) = 0$, which means $I \subseteq \ker(\mathrm{Tr})$. Finally, as Tr is an R-linear GF-trace, we conclude that $I = 0$, as desired. □

The following examples contain claims that are easily verified. We leave the short proofs to the interested reader.

Example 6. Let R be a finite ring.

(i) For every positive integer n, the full matrix ring $M_n(R)$ allows for a GF-trace, namely the usual matrix trace on $M_n(R)$ given by

$$\mathrm{Tr} : M_n(R) \longrightarrow R, \quad (a_{ij})_{i,j \leq n} \mapsto \sum_{i \leq n} a_{ii}.$$

(ii) If G is a finite group, then the group ring $R[G]$ allows for a GF-trace. For $f : G \longrightarrow R$ in this group ring, the trace is given by

$$\mathrm{Tr} : R[G] \longrightarrow R, \quad f \mapsto f(e),$$

where e is the identity of the group.

Both of these examples have the property, that the extension S of R is free as a left and right R-module. This will become important later, when we need the existence of such extensions for any prescribed rank.

Example 7. Let p be a prime number, and let m and d be positive integers. For $R = \mathbb{Z}_{p^m}$ and $S = \mathrm{GR}(p^m, d)$, consider the function from $\mathrm{Tr} : S \longrightarrow R$, with

$$\mathrm{Tr}(x) \;:=\; \sum_{\sigma \in \mathrm{Aut}(S:R)} \sigma(x), \quad \text{for all } x \in S.$$

This function is in fact a GF-trace.

Example 8. Let q be a prime power and d a positive integer, and assume $\mathrm{tr} : \mathbb{F}_{q^d} \longrightarrow \mathbb{F}_q$ to be the known trace function between finite fields and their subfields. For a positive integer a, consider the finite chain rings

$$R \;:=\; \frac{\mathbb{F}_q[u]}{(u^a)} \quad \text{and} \quad S \;:=\; \frac{\mathbb{F}_{q^d}[u]}{(u^a)},$$

together with the function $\mathrm{Tr}_R^S : S \longrightarrow R$, with

$$\mathrm{Tr}_R^S\big(\sum_{i=0}^{a-1} u^i\, \gamma_i\big) \;:=\; \sum_{i=0}^{a-1} u^i\, \mathrm{tr}(\gamma_i),$$

for all $\gamma_i \in \mathbb{F}_{q^d}$. This function is in fact a GF-trace.

Example 9. Let q, d, and tr be as in the preceding example. For the two rings

$$R \;:=\; \frac{\mathbb{F}_q[u,v]}{(u^2, v^2)} \quad \text{and } S \;:=\; \frac{\mathbb{F}_{q^d}[u,v]}{(u^2, v^2)},$$

where we assume that u and v commute, consider the function $\mathrm{Tr}_R^S : S \longrightarrow R$, with

$$\mathrm{Tr}_R^S(\xi_0 + u\,\xi_1 + v\,\xi_2 + uv\,\xi_3) \;:=\; \mathrm{tr}(\xi_0) + u\,\mathrm{tr}(\xi_1) + v\,\mathrm{tr}(\xi_2) + uv\,\mathrm{tr}(\xi_3),$$

where $\xi_0, \xi_1, \xi_2, \xi_3 \in \mathbb{F}_{q^d}$. This function is a GF-trace.

Example 10. Let q be a prime power, let d be a positive integer, and assume $\mathrm{tr} : \mathbb{F}_{q^d} \longrightarrow \mathbb{F}_q$ to be the traditional finite field trace. Consider the rings

$$R \;:=\; \frac{\mathbb{F}_q[v]}{(v^4 - v)} \quad \text{and} \quad S \;:=\; \frac{\mathbb{F}_{q^d}[v]}{(v^4 - v)}$$

with the function $\mathrm{Tr}_R^S : S \longrightarrow R$, such that

$$\mathrm{Tr}_R^S\,(\eta_0 + v\,\eta_1 + v^2\eta_2 + v^3\eta_3) \;:=\; \mathrm{tr}(\eta_0) + v\,\mathrm{tr}(\eta_1) + v^2\mathrm{tr}(\eta_2) + v^3\mathrm{tr}(\eta_3),$$

for $\eta_0, \eta_1, \eta_2, \eta_3 \in \mathbb{F}_{q^d}$. This function is indeed a GF-trace.

4 Trace Codes and Dual Bases

For the rest of this paper, let R be a finite ring, and let S be a free unital extension of rank m of R that allows for a GF-trace from S onto R.

Let $D = [d_1, d_2, \ldots, d_n]$ be a sequence of elements of S. We define a code of length n over R by

$$C_D \;:=\; \{[\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)] \mid x \in S\},$$

and we call D the *defining sequence* of the code C_D. Since the trace function from S to R is (particularly) left R-linear, the code C_D is left R-linear.

Our goal is to study generator matrices for trace codes C_D with defining sequence $D = [d_1, d_2, \ldots, d_n]$. We will get into this in subsection 4.2. As a preparation, we will need to discuss the important concept of dual bases.

4.1 Bases and dual bases

Theorem 11. *Let S be a free unital extension of rank m over R allowing for the GF-trace* Tr*, and let $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_m$ be elements of S. The following statements are equivalent:*

- **(i)** *$\{\alpha_1, \ldots, \alpha_m\}$ forms a basis of ${}_RS$ and $\{\beta_1, \ldots, \beta_m\}$ forms a basis of S_R.*
- **(ii)** *The matrix $(\mathrm{Tr}(\alpha_i\beta_j))_{i,j\le m}$ is invertible.*

Proof. Assume **(i)**, and suppose the matrix $A := (\mathrm{Tr}(\alpha_i\beta_j))_{i,j\le m}$ is not invertible. Then its columns are linearly dependent in R_R^m, and hence, by Remark 3, the system of linear equations

$$\begin{cases} \mathrm{Tr}(\alpha_1\beta_1)\, x_1 + \cdots + \mathrm{Tr}(\alpha_1\beta_m)\, x_m = \;\; 0 \\ \qquad\vdots \qquad\qquad\qquad\qquad\quad \vdots \quad\; \vdots \\ \mathrm{Tr}(\alpha_m\beta_1)\, x_1 + \cdots + \mathrm{Tr}(\alpha_m\beta_m)\, x_m = \;\; 0 \end{cases}$$

has a nontrivial solution, meaning a non-zero $(x_1, x_2, \ldots, x_m) \in R_R^m$ satisfies the system. The element $\gamma := \sum_{j=1}^{m} \beta_j\, x_j$ is nonzero (by our above basis assumption for S_R), and

$$\mathrm{Tr}(\alpha_i\gamma) \;=\; \sum_{j=1}^{m} \mathrm{Tr}(\alpha_i\beta_j)x_j \;=\; 0,$$

for all $i = 1, \ldots, m$. By the basis assumption on ${}_RS$, any $\delta \in S$ is of the form $\delta = \sum_{i=1}^{m} c_i \alpha_i$, where $c_i \in R$. This yields $\mathrm{Tr}(\delta\gamma) = 0$, and it means that $\ker(\mathrm{Tr})$ contains the nonzero ideal $S\gamma$ of S, which contradicts the definition of the trace function and therefore proves that A must be invertible.

Conversely, let the matrix A be invertible, and assume that

$$\sum_{j=1}^{m} \beta_j \, x_j \;=\; 0, \quad \text{where } x_1, \ldots, x_m \in R.$$

Then, for all $i = 1, \ldots, m$, we have

$$0 \;= \mathrm{Tr}(0) \;=\; \mathrm{Tr}(\alpha_i \sum_{j=1}^{m} \beta_j \, x_j) \;=\; \sum_{j=1}^{m} \mathrm{Tr}(\alpha_i \beta_j) x_j,$$

because of the R-linearity of Tr. Consequently, $x = (x_1, \ldots, x_m)^T$ is a solution of the equation $Ax = 0$, which forces $x = 0$. Hence, $\beta_1, \ldots, \beta_m$ are linearly independent and thus a basis of S_R. The respective basis property for $\alpha_1, \ldots, \alpha_m$ in ${}_RS$ follows by symmetry. □

Corollary 12. *The elements $\alpha_1, \ldots, \alpha_m \in S$ form an basis of ${}_RS$ and of S_R, if and only if the matrix $(\mathrm{Tr}(\alpha_i \alpha_j))_{i,j \le m}$ is invertible.*

The following statement will be used for our further considerations.

Theorem 13. *Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis of ${}_RS$, and let $A := (a_{ij})_{i,j \le m}$ be an invertible $m \times m$-matrix over R. For $j = 1, \ldots, m$ define $\beta_j := \sum_{i=1}^{m} a_{ji} \alpha_i$. Then $\{\beta_1, \ldots, \beta_m\}$ is a basis of ${}_RS$ as well.*

Proof. Let $\sum_{j=1}^{m} x_j \beta_j = 0$ for some $x_i \in R$. We compute

$$0 \;=\; \sum_{j=1}^{m} x_j \sum_{i=1}^{m} a_{ji} \alpha_i \;=\; \sum_{i=1}^{m} (\sum_{j=1}^{m} x_j \, a_{ji}) \alpha_i$$

and hence $\sum_{j=1}^{m} x_j a_{ji} = 0$ for all $i = 1, \ldots, m$, as the α_i form a basis of ${}_RS$. This forces $x_j = 0$ for all $j = 1, \ldots, m$, because A is invertible. □

It is needless to emphasize that the left-right symmetric version of the previous statement is true as well. We will need this in a proof further below.

The case, where the matrix $(\mathrm{Tr}(\alpha_i \beta_j))_{i,j \le m}$ is not only invertible, but coincides with the identity matrix, deserves particular attention.

Definition 14. A basis $\{\beta_1, \ldots, \beta_m\}$ of S_R is said to be *dual* to the basis $\{\alpha_1, \ldots, \alpha_m\}$ of ${}_RS$, if $\mathrm{Tr}(\alpha_i\beta_j) = \delta_{ij}$ for all $1 \leq i, j \leq m$, where δ_{ij} denotes the Kronecker symbol.

Theorem 15. *Every basis of ${}_RS$ allows for a dual basis (of S_R) and vice versa.*

Proof. Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis of ${}_RS$ and let $\{\beta_1, \ldots, \beta_m\}$ be a basis of S_R. By Theorem 11, we obtain that the matrix $A = (\mathrm{Tr}(\alpha_i\beta_j))_{i,j\leq m}$ is an invertible matrix. For $A^{-1} =: B = (b_{ij})_{i,j\leq m}$, define $\gamma_j = \sum_{k=1}^{m} \beta_k b_{kj}$ for $j = 1, \ldots, m$. Then, by Theorem 13, the set $\{\gamma_1, \ldots, \gamma_m\}$ forms a basis of S_R, and we obtain

$$\mathrm{Tr}(\alpha_i\gamma_j) \;=\; \sum_{k=1}^{n} \mathrm{Tr}(\alpha_i\beta_k)b_{kj} \;=\; \sum_{k=1}^{m} a_{ik}b_{kj} = \delta_{ij},$$

which shows the claim. The converse direction (vice versa) follows by logical symmetry. □

4.2 Generator matrices for trace codes

Assume we consider the left R-linear code C_D with defining sequence $[d_1, \ldots, d_n]$. For some positive integer m, let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis of ${}_RS$, and let $\{\beta_1, \ldots, \beta_m\}$ be a basis for S_R that is dual to that one. By definition, we have

$$\mathrm{Tr}(\alpha_i\beta_j) = \begin{cases} 0 & \text{for } i \neq j, \\ 1 & \text{for } i = j. \end{cases} \tag{1}$$

For the defining sequence $[d_1, \ldots, d_n] \in S^n$, and $x \in S$, define coefficients d_{ij} and $x_h \in R$ by

$$d_j \;=:\; \sum_{i=1}^{m} \beta_i d_{ij}, \quad \text{and} \quad x \;=:\; \sum_{h=1}^{m} x_h\alpha_h.$$

For these, we compute

$$\mathrm{Tr}(xd_j) \;=\; \sum_{h=1}^{m}\sum_{i=1}^{m} x_h\mathrm{Tr}(\alpha_h\beta_i)d_{ij} \;=\; \sum_{h=1}^{m} x_h d_{hj}.$$

Consequently, the codeword

$$[\mathrm{Tr}(x\,d_1), \ldots, \mathrm{Tr}(x\,d_n)] = [x_1, \ldots, x_m]\,G,$$

where

$$G = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2n} \\ \vdots & \vdots & & \vdots \\ d_{m1} & d_{m2} & \cdots & d_{mn} \end{bmatrix},$$

and where $[x_1, \ldots, x_m] \in R^m$.

Hence, G is a generator matrix of the code C_D. This matrix clearly depends on the choice of the bases $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_m\}$.

4.3 A trace representation of linear codes over a finite ring

In the section at hand, we will investigate into the converse direction, and give any linear code over a finite ring a trace description. This description will depend on the chosen generator matrix for the code in question.

Theorem 16. *Let C be a left-linear code of length n over R. Then there is a free extension S of R that allows for a GF-trace, say* Tr*, along with a defining sequence D of elements in S, such that $C = C_D$.*

Proof. Let

$$G = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2n} \\ \vdots & \vdots & & \vdots \\ d_{k1} & d_{k2} & \cdots & d_{kn} \end{bmatrix}$$

be a generator matrix for C, meaning a matrix whose row vectors span C in ${}_RR^n$. Note, that we do not assume C to be a free code. Our earlier example 6 provides a free unital extension S of rank k, that allow for a GF-trace, say Tr.

If $\{\alpha_1, \ldots, \alpha_k\}$ is a basis of ${}_RS$ with a dual basis $\{\beta_1, \ldots, \beta_k\}$ of S_R, then setting $d_i = \sum_{j=1}^{k} \beta_j d_{ji}$ for all $1 \leq i \leq n$ yields the sequence $D = [d_1, \ldots, d_n]$ of elements in S.

For arbitrary $x \in S$, we have a look at the word $[\mathrm{Tr}(xd_1), \ldots, \mathrm{Tr}(xd_n)] \in C_D$ and need to show that it is a codeword of C. We may assume that x is of the form $x = \sum_{h=1}^{k} x_h \alpha_h$ for suitable $x_h \in R$. Then we obtain

$$\mathrm{Tr}(xd_i) = \mathrm{Tr}(x \sum_{j=1}^{k} \beta_j d_{ji}) = \sum_{h=1}^{k} \sum_{j=1}^{k} x_h \mathrm{Tr}(\alpha_h \beta_j) d_{ji} = \sum_{h=1}^{k} x_h d_{hi},$$

which shows that $C_D \subseteq C$. The reverse containment $C \subseteq C_D$ follows accordingly, and hence $C = C_D$. □

5 Representation of cyclic codes over Galois rings and the chain ring $\frac{\mathbb{F}_2[u]}{(u^2)}$

In this section, we study a trace representation of a particular class, namely that of all cyclic codes over Galois rings and the chain ring $\frac{\mathbb{F}_2[u]}{(u^2)}$. Let p be a prime power and s, r, m be some positive integers. Consider a Galois ring $R := \mathrm{GR}(p^s, r)$, and let $g(x) \in R[x]$ be a basic primitive irreducible polynomial of degree m. Then the ring $S := R[x]/(g(x))$ is a Galois ring, and moreover a degree m Galois extension of R allowing for the following GF-trace.

Assume θ is a root of $g(x)$ of order $p^{rm} - 1$, then $S = R[\theta]$. Define the mapping

$$\phi : S \longrightarrow S, \;\; a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1} \;\mapsto\; a_0 + a_1\theta^{p^r} + \cdots + a_{m-1}\theta^{(m-1)p^r}.$$

As all the a_i are elements of R, the mapping ϕ is an automorphism of S that leaves R pointwise fixed. In fact, it is an analogue of the *Frobenius automorphism* in the theory of finite fields, and it is of order m, which means $\phi^m = \mathrm{id}$.

Very much like in the case of (finite) field extensions, this Frobenius type automorphism gives rise to a trace function, namely:

$$\mathrm{Tr}_R^S : S \longrightarrow R, \quad a \mapsto \sum_{i=0}^{m-1} \phi^i(a).$$

We leave the easy steps to validate the trace properties to the interested reader.

Definition 17 (see [3], Definition 1)**.** Let S be a degree m Galois extension of the Galois ring R, and let ϕ be a generator of the Galois group $\mathrm{Gal}(S, R)$. A normal basis of S over R is a basis of the form $\{\phi^i(\alpha) \mid i = 1, \ldots, m\}$, for suitable $\alpha \in S$.

We would like to emphasize (cf. [12, Lemma 2]) that there always exists a normal basis for S over R.

Theorem 18. *Let S be a degree m Galois extensions of the Galois ring R, and let $\{\phi^i(\alpha) \mid i = 0, \ldots, m-1\}$ be a normal basis for S over R in the sense of the above. Let $f(x) = \sum_{i=0}^{m-1} f_i x^i \in R[x]$ be a polynomial that generates a cyclic code C of length m over R. Define*

$$d \;:=\; \sum_{j=0}^{m-1} f_{m-1-j}\, \phi^j(\alpha) \;\; \textit{and} \;\; D := [\phi(d), \ldots, \phi^{m-1}(d), d].$$

Then $C = C_D$ in the sense of Thm 16, which is the trace code with defining sequence D, where the basis $\{\beta_0, \ldots, \beta_{m-1}\}$ is given as $\beta_i := \phi^i(\alpha)$, for all $i = 0, \ldots, m-1$.

Proof. Since f generates the cyclic code C, the rows of the circulant matrix F span the code C, where F is given as:

$$F \;=\; \begin{bmatrix} f_0 & f_1 & f_2 & f_3 & \cdots & f_{m-3} & f_{m-2} & f_{m-1} \\ f_{m-1} & f_0 & f_1 & f_2 & \cdots & f_{m-4} & f_{m-3} & f_{m-2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ f_2 & f_3 & f_4 & f_5 & \cdots & f_{m-1} & f_0 & f_1 \\ f_1 & f_2 & f_3 & f_4 & \cdots & f_{m-2} & f_{m-1} & f_0 \end{bmatrix}.$$

By the above definition of d, we find

$$\phi^i(d) \;=\; \sum_{j=0}^{m-1} f_{m-1-j}\, \phi^{i+j}(\alpha).$$

With $\beta_i = \phi^i(\alpha)$, for all $i = 0, \ldots, m-1$, we obtain

$$\begin{aligned} \sum_{j=0}^{m-1} \beta_j F_{ji} \;&=\; \sum_{j=0}^{m-1} \phi^j(\alpha) f_{i-j} \\ &=\; \sum_{j=0}^{m-1} \phi^{i+j}(\alpha) f_{m-j} \;=\; \sum_{j=0}^{m-1} \phi^{i+j+1}(\alpha) f_{m-1-j} \;=\; \phi^{i+1}(d). \end{aligned}$$

Here, all subscripts are meant to be taken modulo m. Now, this implies $C = C_D$: in fact, using $D = [d_1, \ldots, d_m] = [\phi(d), \ldots, \phi^m(d), d]$, we find that for $x \in S$ and $i = 0, \ldots, m-1$ the above equation implies that

$$\mathrm{Tr}(x d_{i+1}) \;=\; \mathrm{Tr}(x\phi^{i+1}(d)) \;=\; \mathrm{Tr}(x \sum_{j=0}^{m-1} \beta_j F_{ji}) \;=\; \sum_{j=0}^{m-1} \mathrm{Tr}(x\beta_j) F_{ji},$$

and this immediately yields $C_D \subseteq C$.

For the reverse containment, suppose that $\alpha_0, \ldots, \alpha_{m-1}$ is a basis of S dual to the normal basis $\beta_0, \ldots, \beta_{m-1}$. Then $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{ij}$, and, by taking $x = \alpha_k$ in the above equation, we obtain

$$\mathrm{Tr}(\alpha_k d_{i+1}) \;=\; \sum_{j=0}^{m-1} \mathrm{Tr}(\alpha_k \beta_j) F_{ji} \;=\; \sum_{j=0}^{m-1} \delta_{kj} F_{ji} \;=\; F_{ki}.$$

This shows that the rows of F belong to C_D, so that $C \subseteq C_D$. □

The following result and its proof are very much in the same spirit as Thm. 18, thus we omit the proof here and leave it to the interested reader.

To get prepared, let m be a positive integer, and let

$$R := \frac{\mathbb{F}_2[u]}{(u^2)} \quad \text{and} \quad S := \frac{\mathbb{F}_{2^m}[u]}{(u^2)}.$$

We define

$$\phi : S \longrightarrow S,\ x + uy = x^2 + uy^2,$$

where $x, y, x^2, y^2 \in \mathbb{F}_{2^m}$. This mapping is an automorphism of S that fixes R elementwise and has order m. Again, we use the according trace function

$$\mathrm{Tr}_R^S : S \longrightarrow R, \quad a \mapsto \sum_{i=0}^{m-1} \phi^i(a).$$

Theorem 19. *Let $\{\phi^i(\alpha) \mid i = 0, \ldots, m-1\}$ be a normal basis for S over R. Let $f(x) = \sum_{i=0}^{m-1} f_i x^i \in R[x]$ be a polynomial that generates a cyclic code C of length m over R. Define*

$$d := \sum_{j=0}^{m-1} f_{m-1-j}\, \phi^j(\alpha) \quad \textit{and} \quad D := [\phi(d), \ldots, \phi^{m-1}(d), d].$$

Then, using the basis $\{\beta_0, \ldots, \beta_{m-1}\}$, where $\beta_i = \phi^i(\alpha)$, we find $C = C_D$, which is the trace code with defining sequence D as described in Thm. 16.

What we have just seen should be easy to generalize to $R = \mathbb{F}_q[u]/(u^k)$ and $S = \mathbb{F}_{q^m}[u]/(u^k)$. We leave this as a simple exercise to the interested reader.

6 Conclusion and open problems

In this note we have introduced a notion of trace codes over rings that encompasses all previous such notions defined for rings that have been treated in [5, 6, 7, 8]. This notion is generic, in the sense that every linear code over a finite ring can be represented in that way by introducing a suitable unital extension, that allows for a GF-trace.

A more traditionally oriented trace description in terms of Frobenius automorphisms is presented for cyclic codes over Galois rings and falls under the umbrella described in the earlier sections.

The proof being based on the existence of a normal basis, it would be nice to find the largest class of finite ring extensions that admit such a basis. This is the main open problem of this work, and it appears to be non-trivial, as it will require the concept of Galois theory for a large class of finite rings.

References

[1] M. Shi, A. Alahmadi, and P. Solé, *Codes and Rings: Theory and Practice*, Academic Press (2017).

[2] M. Greferath and A. Nechaev, Generalized Frobenius extensions of finite rings and trace functions, IEEE Information Theory Workshop, 2010, 23(3), 1–5.

[3] Irwansyah, I. Muchtadi-Alamsyah, A. Barra, and A. Muchlis, Self-dual normal basis of a Galois Ring, Journal of Mathematics, 2014, Article ID 258187, 7 pages.

[4] Yan Liu, Minjia Shi, and Patrick Solé, Two-weight and three-weight codes from trace codes. Discrete Mathematics **341** (2018), 350–357.

[5] Minjia Shi, Yue Guan, and Patrick Solé, Two New Families of Two-Weight Codes. IEEE Trans. on Inform. Theory **63** (2017), 6240–6246.

[6] Minjia Shi, Yan Liu, and Patrick Solé, Optimal binary codes from trace codes over a non-chain ring. Discrete Applied Mathematics **219** (2017), 176–181.

[7] Minjia Shi, Rongsheng Wu, Yan Liu, and Patrick Solé, Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$. Cryptography and Communications **9** (2017), 637–646.

[8] Minjia Shi, Liqin Qian, and Patrick Solé, Few-weight codes from trace codes over a local ring. Appl. Algebra Eng. Commun. Comput. **29** (2018), 335–350.

[9] J. Gomez-Torrecillas, E. Hieta-Aho, F. J. Lobillo, S. Lopez-Permouth, and G. Navarro, Some Remarks on Non Projective Frobenius Algebras and Linear Codes. Designs, Codes, and Cryptography. **88** (2020), 1–15.

[10] T. Nakayama and T. Tsuzuku, A remark on Frobenius extensions and endomorphism rings. Nagoya Math. J. **15** (1959), 9–16.

[11] C. Xiang, It is indeed a fundamental construction of all linear codes, `arXiv:1610.06355v1 [cs.IT] 20 Oct 2016`.

[12] Z. X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing, Singapore, 2012.

[13] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. **121** (1999), 555–575.

[14] J. Wood, Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities, in P. Solé, *Codes over rings*, World Scientific, (2008), Singapore.