Math. J. Okayama Univ. **58** (2016), 133–140

ON FINITE RINGS OVER WHICH ALL FREE CODES ARE SPLITTING

Yasuyuki Hirano

Abstract. In this paper, we study the structure of finite rings over which all free codes are splitting. In particular, we show that over the matrix rings over finite local rings all free codes are splitting.

1. Introduction

Recently linear codes over finite rings have raised a great interest for their role in algebraic coding theory. Firstly classical algebraic coding theory over finite fields has been extended to algebraic coding theory over Galois rings and finite commutative rings (see [3]). Next, algebraic coding theory over finite noncommutative rings is studied by many authors (see the references in [6]). In particular, Wood [8] showed that linear coding theory is particularly well-behaved over finite Frobenius rings (see also [9]). Finite Frobenius rings have many good properties. Over a finite Frobenius ring, every projective module is injective, and hence all free codes are splitting. In this paper, we assign light to only this property and we study the structure of finite rings with this property: (†) All free codes are splitting. First we show that finite rings which are Morita equivalent to finite commutative rings have property (†). Next we give a necessary and sufficient condition for a free code C over any finite ring to be splitting. Then we give a sufficient condition for a finite ring to have property (†). Using this result, we show that matrix rings over finite local rings have property (†). Finally we give an example of a finite indecomposable ring with property (†), but it is not quasi-Frobenius and also is not Morita equivalent to any finite local ring.

2. Preliminary results

First we give some definitions. Let n be a positive number. Following Greferath [5], a *linear (left) code* C of length n over a finite ring R is a submodule of ${}_RR^n$. We call C *splitting* if it is a direct summand of ${}_RR^n$. If C has a basis, then C is said to be *free*. If $C \cong {}_RR^m$ for some $m(\leqq n)$, then C is called a *free code of rank* m.

For some notations and fundamental results on finite rings, we refer the reader to McDonald [7].

Mathematics Subject Classification. Primary 16P10; Secondary 94B05.
Key words and phrases. finite rings, ring-linear codes, free codes.

In this paper, we consider the structure of finite rings R over which every free codes of length n over R is splitting for every natural number n. In this section, we state some general results on rings over which every finitely generated free submodule N of any finitely generated free module M is a direct summand of M.

Proposition 2.1. *The following conditions are equivalent for a ring R:*

(1) *Every finitely generated free submodule N of any finitely generated free module M is a direct summand of M.*

(2) *Every finitely generated projective submodule P of any finitely generated projective module Q is a direct summand of Q.*

Proof. (1) $\Rightarrow$ (2). Let P be a finitely generated projective submodule of a finitely generated projective module Q. Then we find some projective modules P' and Q' such that $P \oplus P'$ and $Q \oplus P' \oplus Q'$ are free modules. Since we assume that (1) holds, $P \oplus P'$ is a direct summand of $Q \oplus P' \oplus Q'$, that is $Q \oplus P' \oplus Q' = P \oplus P' \oplus X$ for some submodule X of $Q \oplus P' \oplus Q'$. Then, using modular law, we have $Q = Q \cap (Q \oplus P' \oplus Q') = Q \cap (P \oplus P' \oplus X) = P \oplus (Q \cap P' \oplus Q')$.

(2) $\Rightarrow$ (1). This is trivial. □

Proposition 2.2. *Let R be a ring and consider the property:*

(‡) *Every finitely generated free submodule N of any finitely generated free module M is a direct summand of M.*

Then there holds the following:

(1) *The property (‡) is Morita invariant.*

(2) *Let $e_1, \cdots, e_n$ are central and orthogonal idempotents of a ring R such that $e_1 + \cdots + e_n = 1$. Then R has property (‡) if and only if all rings $Re_1, \cdots, Re_n$ have property (‡).*

Proof. (1) Assume that two rings R and S are Morita equivalent via a category equivalence $F : R\text{-}Mod \to S\text{-}Mod$ and its inverse $G : S\text{-}Mod \to R\text{-}Mod$. Assume that R has property (‡). Let $0 \to N \to M \to M/N \to 0$ be an exact sequence with projective modules N and M. Then, by [1, Propositions 21.4 and 21.6], $0 \to \mathrm{G}(N) \to \mathrm{G}(M) \to \mathrm{G}(M/N) \to 0$ be an exact sequence with projective modules $\mathrm{G}(N)$ and $\mathrm{G}(M)$. By hypothesis, the exact sequence $0 \to \mathrm{G}(N) \to \mathrm{G}(M) \to \mathrm{G}(M/N) \to 0$ splits. Then $0 \to \mathrm{FG}(N) \to \mathrm{FG}(M) \to \mathrm{FG}(M/N) \to 0$ splits by [1, Propositions 21.4], This implies that $0 \to N \to M \to M/N \to 0$ splits. By Proposition 2.1, S has property (‡).

(2) This follows from Proposition 2.1. □

3. Finite commutative rings

A ring R with Jacobson radical J is called a local ring if R/J is a division ring. Since a finite division ring is a field by Wedderburn's theorem, a finite ring R is *local* if R/J is a finite field.

Lemma 3.1. *Let R be a finite commutative local ring with Jacobson radical J. Let C be a free code of rank m of ${}_RR^n$. Then the code $\bar{C} = (C + JR^n)/JR^n$ of ${}_{R/J}(R/J)^n$ is a free code of rank m.*

Proof. We may assume that $J \neq 0$. We identify R^n/JR^n with $(R/J)^n$ in a natural way. Then there is a positive integer k such that $J^k \neq 0$ and $J^{k+1} = 0$. Let $C = Rx_1 \oplus \cdots \oplus Rx_m$ be a free code of rank m with free basis $\{x_1, \cdots, x_m\}$ and let $\bar{x}_i = x_i + JR^n \in (R/J)^n$ for each $i = 1, \cdots, m$. Suppose $\bar{a}_1\bar{x}_1 + \cdots + \bar{a}_m\bar{x}_m = 0$ for some $\bar{a}_i = a_i + J \in R/J$. Then $a_1x_1 + \cdots + a_nx_n \in JR^n$. Since $J^k \neq 0$, we can take $b_1, \cdots, b_k \in J$ such that $b_1 \cdots b_k \neq 0$. Since $J^{k+1} = 0$, $b_1 \cdots b_k a_1 x_1 + \cdots + b_1 \cdots b_k a_m x_m = 0$. However $x_1, \cdots, x_m$ are linearly independent over R, we obtain $b_1 \cdots b_k a_1 = \cdots = b_1 \cdots b_k a_m = 0$. Since R is a local ring, these mean $a_1, \cdots, a_m \in J$, that is $\bar{a}_i = a_i + J = 0$ for all $i \in \{1, \cdots, m\}$. □

Theorem 3.2. *Let R be a finite commutative ring. Then every free code C of ${}_RR^n$ is splitting for any positive integer n.*

Proof. First consider the case when R is a local ring. Let $C = Rx_1 \oplus \cdots \oplus Rx_m$ $(m < n)$ with free basis $\{x_1, \cdots, x_m\}$ and let $\{y_1, \cdots, y_n\}$ be the standard basis of ${}_RR^n$. By Lemma 3.1, $\bar{C} = \bar{R}\bar{x}_1 \oplus \cdots \oplus \bar{R}\bar{x}_m$ is a free code of rank m of $\bar{R}\bar{y}_1 \oplus \cdots \oplus \bar{R}\bar{y}_n = (R/J)^n$. Then we can select $\bar{y}_{i_1}, \cdots, \bar{y}_{i_{n-m}}$ from $\{\bar{y}_1, \cdots, \bar{y}_n\}$ such that $\{\bar{x}_1, \cdots, \bar{x}_m, \bar{y}_{i_1}, \cdots, \bar{y}_{i_{n-m}}\}$ is a basis of $(R/J)^n$. Then $R^n = (Rx_1 + \cdots + Rx_n) + (Ry_{i_1} + \cdots + Ry_{i_{n-m}}) + JR^n = R^n$. Since JR^n is small in R^n, we obtain $R^n = (Rx_1 + \cdots + Rx_n) + (Ry_{i_1} + \cdots + Ry_{i_{n-m}}) = R^n$. This means that R^n is a homomorphic image of $(Rx_1 \oplus \cdots \oplus Rx_n) \oplus (Ry_{i_1} \oplus \cdots \oplus Ry_{i_{n-m}})$. Since R^n is a free module of rank n over a finite commutative local ring R, by Theorem of Jordan-Hölder ([2, Theorerm 2.5.2]), the composition length of R^n is equal to that of $(Rx_1 \oplus \cdots \oplus Rx_n) \oplus (Ry_{i_1} \oplus \cdots \oplus Ry_{i_{n-m}})$. Therefore we conclude that $R^n = (Rx_1 \oplus \cdots \oplus Rx_n) \oplus (Ry_{i_1} \oplus \cdots \oplus Ry_{i_{n-m}}) = C \oplus (Ry_{i_1} \oplus \cdots \oplus Ry_{i_{n-m}})$.

Next consider the case when R is a finite commutative ring. We can easily see that R is a direct sum of finite commutative local rings. So let $R = Re_1 \oplus \cdots \oplus Re_k$, where each Re_i is a local ring. Now let C be a free code of ${}_RR^n$. Then, for each i, e_iC be a free Re_i-submodule of rank m of a free Re_i-module e_iR^n. Then $e_iR^n = e_iC \oplus C_i'$ for some Re_i-submodule C_i' of e_iR^n. Then $R^n = (e_1C \oplus \cdots \oplus e_kC) \oplus (C_1' \oplus \cdots \oplus C_k') = C \oplus (C_1' \oplus \cdots \oplus C_k')$. □

4. Non-commutative artinian rings

We denote the ring of $n \times n$-matrices over a ring R by $\mathrm{M}_n(R)$. By Theorem 3.2 and Proposition 2.2 we have the following proposition.

Proposition 4.1. *Let $R_1, \cdots, R_k$ be finite commutative rings. Then, for any positive integers $n_1, \cdots, n_k$, the ring $R = \mathrm{M}_{n_1}(R_1) \oplus \cdots \oplus \mathrm{M}_{n_k}(R_k)$ has the following property:*

(†) *Every free code C of ${}_RR^n$ is splitting for every positive integer n.*

However the following example shows that a non-commutative finite ring need not have property (†).

Example 1. Let K be a finite field and consider the subring $R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$ of the ring $\begin{pmatrix} K & K \\ K & K \end{pmatrix}$ of 2×2 matrices over K. Since the left ideal $\begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix}$ of R is isomorphic to the left ideal $\begin{pmatrix} K & 0 \\ 0 & 0 \end{pmatrix}$, the code $C = \begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & K \\ 0 & K \end{pmatrix}$ of $R \oplus R = R^2$ is isomorphic to ${}_RR$, and hence C is a free code. However C is not a direct summand of R^2, because $\begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix}$ is small in ${}_RR$.

Next we give a necessary and sufficient condition for a free code C over a finite ring to be splitting.

Theorem 4.2. *Let R be a finite ring and let C be a free code of ${}_RR^n$. Then the following are equivalent:*

(1) *C is splitting.*

(2) *$\bar{C} = (C + JR^n)/JR^n$ is a free code of ${}_{R/J}(R/J)^n$ and the rank of $\bar{C}$ equals the rank of C.*

Proof. (1) $\Rightarrow$ (2). This is clear.

(2) $\Rightarrow$ (1). Assume the rank of C is m. Since R/J is a finite semisimple ring, $(R/J)^n = (C + JR^n)/JR^n \oplus L$ for some code L of $(R/J)^n$. Clearly L is a free code of rank $n - m$. Hence there exist $x_1, \cdots, x_{n-m} \in {}_RR^n$ such that $\{\bar{x}_1, \cdots, \bar{x}_{n-m}\}$ is a free basis of L over R/J. Then $R^n = C + (Rx_1 + \cdots + Rx_{n-m}) + JR^n$. By Nakayama's lemma, we obtain $R^n = C + (Rx_1 + \cdots + Rx_{n-m})$. Since C is of rank m over R, there is an isomorphism $f : {}_RR^m \to C$. Also there is an epimorphism $g : {}_RR^{n-m} \to Rx_1 + \cdots + Rx_{n-m}$. Since ${}_RR^n = {}_RR^m \oplus {}_RR^{n-m}$, we can define an epimorphism $\phi : {}_RR^n \to C + (Rx_1 + \cdots + Rx_{n-m}) = {}_RR^n$ by $\phi = f$ on ${}_RR^m$ and $\phi = g$ on ${}_RR^{n-m}$. Since ${}_RR^n$ is a finite set, the epimorphism ϕ is an isomorphism. Therefore $Rx_1 + \cdots + Rx_{n-m}$ is a free R-module of rank $n - m$ and $R^n = C \oplus (Rx_1 + \cdots + Rx_{n-m})$. □

In the proof of Theorem 4.2, we used that fact that ${}_RR^n$ is a finite set. But we can also use the following easy lemma.

Lemma 4.3. *Let R be a ring and let M be a left R-module of finite composition length. Consider an R-endomorphism f of M. Then the following are equivalent:*

(1) *f is an epimorphism.*
(2) *f is a monomorphism.*
(3) *f is an isomorphism.*

Using the lemma above, we can generalize Theorem 4.2 to left artinian rings.

Theorem 4.4. *Let R be a left artinian ring and let N be a finitely generated free submodule of a finitely generated free module M. Then the following are equivalent:*

(1) *N is a direct summand of M.*
(2) *$\bar{N} = (N + JM)/JM$ is a free R/J-module and the rank of $\bar{N}$ over R/J equals the rank of N over R.*

A left principal indecomposable module of a ring R is a left submodule of ${}_RR$ that is a direct summand of R and is an indecomposable module. Now we state a sufficient condition for a left artinian ring to have the property that every finitely generated free submodule N of any finitely generated free module M is a direct summand of M.

Theorem 4.5. *Let R be a left artinian ring with non-zero Jacobson radical J of nilpotency index $k+1$. Assume that for every left principal indecomposable module L, $J^kL \neq 0$. Then every finitely generated free submodule N of any finitely generated free module M is a direct summand of M.*

Proof. Since R is a left artinian ring, by [2, Proposition 2.5.6] N is a direct sum of indecomposable modules, say $N = L_1 \oplus \cdots \oplus L_n$. Since $N \cong R^m$ for some positive integer m, by Theorem of Krull-Schmidt ([2, Theorem 2.5.11]) each L_i is isomorphic some indecomposable direct summand of ${}_RR$.

Let us set $\bar{L}_i = (L_i+JM)/JM \subset M/JM$. We claim that $\bar{L}_i$ is a simple R-module for all $i \in \{1, \cdots, n\}$. If $\bar{L}_i = 0$ for some i, then $L_i \subset JM$, and hence $J^kL_i \subset J^{k+1}M = 0$. This contradicts our assumption. Therefore $\bar{L}_i \neq 0$ for all $i \in \{1, \cdots, n\}$. There is an isomorphism $\bar{L}_i = (L_i + JM)/JM \cong L_i/(L_i \cap JM)$. Since $JL_i \subset L_i \cap JM$ and since L_i/JL_i is a simple R-module by [1, Proposition 27.10], we conclude that $\bar{L}_i$ is a simple R-module for all $i \in \{1, \cdots, n\}$.

Next we claim that $\bar{L}_1 + \cdots + \bar{L}_n$ is a direct sum. Assume $\bar{a}_1 + \cdots + \bar{a}_n = 0 \in M/JM$, where $a_i \in L_i$ and $\bar{a}_i = a_i + JM$ for each $i = 1, \cdots, n$. Then $a_1 + \cdots + a_n \in JM$ and so $J^k(a_1 + \cdots + a_n) = 0$. Since $L_1 + \cdots + L_n$ is a

direct sum, we obtain $J^k a_i = 0$ for each $i = 1, \cdots, n$. By our assumption, $J^k L_i \neq 0$ and L_i/JL_i is simple, we conclude that $a_i \in JL_i \subset JM$ for each $i = 1, \cdots, n$. Hence $\bar{a}_1 = \cdots = \bar{a}_n = 0$. This proves our claim.

Hence $\bar{N} = \bar{L}_1 \oplus \cdots \oplus \bar{L}_n$ is isomorphic to ${}_{R/J}(R/J)^m$. Thus the rank of $\bar{N}$ over R/J and the rank of N over R are same m. Therefore by Theorem 4.4 N is a direct summand of M. □

Remark. If R be a left artinian ring (or more generally, if R is a semiperfect ring), then there are finitely many left principal indecomposable modules $L_1, \cdots, L_m$ such that every finitely generated indecomposable projective left R-module is isomorphic to one and only one of $L_1, \cdots, L_m$ (see [1, Proposition 27.10]). Hence we need only check the condition of Theorem 4.5 holds for $L_1, \cdots, L_m$.

We can easily see that local rings satisfy the condition in Theorem 4.5. Hence we have the following corollary.

Corollary 4.6. *Let R be a finite local ring. Every free code C of ${}_R R^n$ is splitting for any positive integer n.*

By Corollry 4.6 and Proposition 2.2 we obtain the following theorem.

Theorem 4.7. *Let $R_1, \cdots, R_k$ be finite local rings. Then, for any positive integers $n_1, \cdots, n_k$, the ring $R = \mathrm{M}_{n_1}(R_1) \oplus \cdots \oplus \mathrm{M}_{n_k}(R_k)$ has the following property:*

(†) *Every free code C of ${}_R R^n$ is splitting for any positive integer n.*

Finally we give an example of a finite indecomposable ring with property (†), but it is not quasi-Frobenius and also is not Morita equivalent to any finite local ring.

Example 2. Let K be a finite field and let $A = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in K,\ b \in K \oplus K\}$.

Consider the following subring of $\mathrm{M}_2(A)$:

$R = \left\{ \left(\begin{array}{cc|cc} a & 0 & 0 & b \\ 0 & a & 0 & 0 \\ \hline 0 & c & d & 0 \\ 0 & 0 & 0 & d \end{array}\right) \mid a, d \in K,\ b, c \in K \oplus K \right\}$. Then we see $J(R) = \left\{ \left(\begin{array}{cc|cc} 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ \hline 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \mid b, c \in K \oplus K \right\}$ and $R/J(R) \cong K \oplus K$. We can also see $J(R)^2 = 0$, and hence $J(R)$ is nilpotent of index 2. Consider the idempotent

$e = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$. Then $L_1 = Re$ is an indecomposable left ideal of R and the socle of L_1 is $S_1 = \left\{ \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \mid c \in K \oplus K \right\}$. We can easily see that $JL_1 = S_1 \neq 0$. If we set $L_2 = R(1-e)$, then L_2 is also an indecomposable left ideal of R. The socle of L_2 is $S_2 = \left\{ \left(\begin{array}{cc|cc} 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \mid b \in K \oplus K \right\}$ and we can see that $JL_2 = S_2 \neq 0$. By Theorem 4.5, every free code C of ${}_RR^n$ is splitting for every positive integer n. Clearly S_1 and S_2 are not simple. Hence R is not quasi-Frobenius (cf. [4, Theorem 9.3.7]). Also R is not Morita equivalent to any finite local ring.

References

[1] F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*, Second Edition, Springer-Verlag, New York-Heidelberg-Berlin, 1992.

[2] J. Beachy, *Introductory Lectures on Rings and Modules*, London Mathematical Society Student Texts, **47**, Cambridge University Press, Cambridge, 1999.

[3] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications*, Kluwer Academic Press Publishers, 2002.

[4] Y. A. Drozd and V. V. Kirichenko, *Finite Dimensional Algebras*, Springer-Verlag, Berlin, 1994.

[5] M. Greferath, *Cyclic codes over finite rings*, Discrete Math., **177**, no. 1 (1997), 273–277.

[6] M. Greferath, *An Introduction to Ring-Linear Coding Theory*, Gröbner Bases, Coding, and Cryptography, Edited by M. Sala, T. M. L. Perret, S. Sakata and C.Traverso, Springer-Verlag, Berlin, 2009, 219–238.

[7] B. R. McDonald, *Finite Rings With Identity*, (Pure and Applied Mathematics, Vol. 28), Marcel Dekker, Inc., New York, 1974.

[8] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math., **121**, no. 3 (1999), 555-575.

[9] J. A. Wood, *Applications of finite Frobenius rings to the foundations of algebraic coding theory*, Proceedings of the 44th Symposium on Ring Theory and Representation Theory, Nagoya, 2012, 223–245.

Yasuyuki Hirano
Department of Mathematics
Naruto university of Education
Naruto, 772-8502 Japan
e-mail address: yahirano@naruto-u.ac.jp

(*Received September 11, 2013*)
(*Accepted October 8, 2013*)