MATIMYÁS MATEMATIKA
ISSN 0115-6926

Journal of the Mathematical Society of the Philippines
Vol. 30 No. 1 (2007) pp. 23-30

Heller-type Bounds for the Homogeneous Free Distance of Convolutional Codes over Finite Frobenius Rings

Virgilio P. Sison
Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines
email: vpsison@up.edu.ph

Abstract

Let R be a finite commutative Frobenius ring with identity, and $R[D]$ be the ring of polynomials in the delay operator D with coefficients from R. We consider a rate-k/n convolutional code $\mathcal{C}$ over R to be an $R[D]$-submodule of $R[D]^n$ which is obtained as the $R[D]$-rowspan of a $k \times n$ polynomial encoding matrix with linearly independent rows. A homogeneous weight with average value Γ is applied on R and extended naturally to $R[D]^n$. The homogeneous free distance $d_{free}^{\mathtt{hom}}$ of $\mathcal{C}$ is the minimum among the homogeneous weights of its nonzero codewords. We apply the generalized Plotkin bound to the truncations of $\mathcal{C}$ to derive upper bounds on $d_{free}^{\mathtt{hom}}$, both in systematic and non-systematic cases, in terms of the average value Γ, the encoder memory and the cardinality of R. These bounds generalize the well-known Heller bounds for the Hamming free distance of binary convolutional codes. We also show the particular case for convolutional codes over Galois rings.

Keywords: *Frobenius ring, Galois ring, convolutional code, free distance, Heller bound, Plotkin bound*

1 Introduction

Massey and Mittelholzer [17] introduced the theory of convolutional codes over rings when they showed that the most suitable codes for signalling in phase modulation are the linear codes over the residue class ring $\mathbb{Z}_M$ of integers modulo M. Codes over rings gained more attention when Hammons, Kumar, Calderbank, Sloane and Solé [8] discovered in 1994 that certain very good but peculiar non-linear codes over the binary field $\mathbb{F}_2$ can be viewed as images of linear codes over $\mathbb{Z}_4$ under the isometric mapping from $\mathbb{Z}_4$ onto $\mathbb{F}_2 \times \mathbb{F}_2$ defined by $0 \mapsto 00, 1 \mapsto 01, 2 \mapsto 11, 3 \mapsto 10$. Johannesson, Wan and Wittenmark [12] advanced the structural analysis of convolutional codes over rings which behave quite differently from codes over fields. Fagnani and Zampieri [4] extended the analysis further and presented quite a complete theory of convolutional codes over the ring $\mathbb{Z}_{p^r}$, where p is a prime and $r \geq 1$ is an integer, in the usual case where the input sequence space is a free module. Mahapakulchai and Van Dyck [16] employed non-catastrophic polynomial encoders over $\mathbb{Z}_4$ for the MAP decoding of MPEG-4 images. The search for and design of good convolutional codes over $\mathbb{Z}_4$ that give rise to binary trellis codes with high free distances were reported in several places in the literature, for instance in [1, 13, 14].

The distance of a code is the most important parameter that measures its ability to detect and correct transmission errors in noisy communication channels. In 1968, Heller [9] proved that the Hamming free distance of a binary convolutional code is bounded above in terms of the rate of the code and the encoder memory. In this present work, we generalize this well-known result to convolutional codes over finite commutative Frobenius rings with identity. These rings, which include the Galois rings $GR(p^r, m)$ and the integer rings $\mathbb{Z}_M$, constitute the most general class of rings that admit a homogeneous weight, a far reaching generalization of the Lee metric over $\mathbb{Z}_4$. Moreover, since two of the classical theorems in coding theory – namely the Extension Theorem and the MacWilliams identities – generalize to the case of finite Frobenious rings, these rings are viewed as being the most appropriate alphabet for coding theoretic purposes.

The material is organized as follows. Section 2 introduces the basic definitions and the relevant concepts needed in the next section. We refer the reader to [10] and [20] for a characterization of Frobenius rings and to [15] and [18] for a comprehensive treatment of Galois rings. We cite Constantinescu, Heise and Honold [2, 3] who introduced the notion of homogeneous weight on $\mathbb{Z}_M$, which was then extended by [11] to finite modules over arbitrary finite rings. The finite modules which admit a homogeneous weight are characterized in terms of the composition factors of their socle. Greferath and Schmidt [6] obtained an existence and characterization theorem for (left) homogeneous weights on arbitrary finite rings, and Honold [10] showed that a homogeneous weight on a finite Frobenius ring can be expressed in terms of its generating character [please see (3)]. The structural properties of ring convolutional encoders are given in [19], [12] and [4]. Section 3 derives upper bounds on the homogeneous free distance in both systematic and non-systematic cases.

2 Preliminaries and definitions

2.1 Frobenius rings and homogeneous weight

Let R be a finite ring with identity $1 \neq 0$, and $\mathbb{T}$ be the multiplicative group of unit complex numbers. The group $\mathbb{T}$ is a one-dimensional torus. A *character* of R (considered as an additive abelian group) is a group homomorphism $\chi : R \to \mathbb{T}$. The set of all characters $\widehat{R}$ (called the *character module of* R) is a right (resp. left) R-module whose group operation is pointwise multiplication of characters and scalar multiplication is given by $\chi^r(x) = \chi(rx)$ (resp. ${}^r\chi(x) = \chi(xr)$). A character χ of R is called a *right (resp. left) generating character* if the mapping $\phi : R \to \widehat{R}$ given by $\phi(r) = \chi^r$ (resp. $\phi(r) = {}^r\chi$) is an isomorphism of right (resp. left) R-modules. The ring R is called *Frobenius* if and only if R admits a right or a left generating character, or alternatively, if and only if $\widehat{R} \cong R$ as right or left R-modules. It is known that for finite rings, a character χ on R is a right generating character if and only if it is a left generating character.

Let $\mathbb{R}$ be the set of real numbers. We define a homogeneous weight on an arbitrary finite ring with identity in the sense of [6]. Let Rx denote the principal (left) ideal generated by $x \in R$.

Definition 1. *A weight function $w : R \to \mathbb{R}$ on a finite ring R is called (left) homogeneous if $w(0) = 0$ and the following is true.*

(i) If $Rx = Ry$, then $w(x) = w(y)$ for all $x, y \in R$.

(ii) There exists a real number $\Gamma \geq 0$ such that

$$\sum_{y \in Rx} w(y) = \Gamma \cdot |Rx|, \quad \textit{for all}\, x \in R \setminus \{0\}\,. \tag{1}$$

Right homogeneous weights are defined accordingly. If a weight is both left homogeneous and right homogeneous, we call it simply as a homogeneous weight. The constant Γ in (1) is called the *average value* of w. A homogeneous weight on a finite ring is said to be *normalized* if its average value is 1. We can normalize the weight w in Definition 1 by replacing it with $\widetilde{w} = \Gamma^{-1}w$ [11]. The weight w is extended naturally to R^n, the free module of rank n consisting of all the n-tuples of elements from R, via

$$w(z) = \sum_{i=0}^{n-1} w(z_i) \tag{2}$$

for $z = (z_0, z_1, \ldots, z_{n-1}) \in R^n$. The homogeneous distance metric $\delta : R^n \times R^n \longrightarrow \mathbb{R}$ is defined by $\delta(x, y) = w(x - y)$, for $x, y \in R^n$.

It was proved in [10] that, if R is Frobenius with generating character χ, then every homogeneous weight w on R can be expressed in terms of χ as follows.

$$w(x) = \Gamma \left[1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(xu) \right] \tag{3}$$

where $R^\times$ is the group of units of R.

A block code B of length n over an arbitrary finite ring R is a non-empty subset of R^n. The code B is called *right (resp. left) R-linear* if B is a right (resp. left) R-submodule of R^n. If B is both left R-linear and right R-linear, we simply call B a linear block code over R. If B is a free module, then B is said to be a *free code*. The minimum homogeneous distance $\delta_{\mathtt{min}}$ of B is defined to be $\delta_{\mathtt{min}} = \min\{\delta(x, y) \mid x, y \in B, x \neq y\}$.

The following proposition from [7] gives the Plotkin bound for block codes over a finite Frobenius ring that is equipped with a homogeneous weight.

Proposition 1 (Greferath and O'Sullivan, 2004)**.** *Let R be a finite Frobenius ring that is equipped with a homogeneous weight w of average value Γ. Let B be a (not necessarily linear) block code of length n over R with minimum homogenous distance $\delta_{\mathtt{min}}$. Then*

$$\delta_{\mathtt{min}} \leq \frac{|B|}{|B| - 1} \Gamma n \,. \tag{4}$$

2.2 Galois rings

Let p be a prime number and $r \geq 1$ an integer. Consider the finite commutative ring $\mathbb{Z}_{p^r}$ of integers modulo p^r. When $r = 1$ then the ring $\mathbb{Z}_p$ is a field and is usually denoted by $\mathbb{F}_p$. Let $\mathbb{Z}_{p^r}[x]$ be the ring of polynomials in the indeterminate x with coefficients in $\mathbb{Z}_{p^r}$. We denote by $\mathbb{F}_{p^m}$ the Galois field (unique up to isomorphism) with p^m elements, which is a field extension $\mathbb{F}_p[\alpha]$ of $\mathbb{F}_p$ by a root α of an irreducible polynomial of degree m in $\mathbb{F}_p[x]$.

The *Galois ring* $\mathcal{R}$ with characteristic p^r and cardinality p^{rm} is the residue class ring $\mathbb{Z}_{p^r}[x]/(h(x))$, where $h(x)$ is a monic polynomial of degree m in $\mathbb{Z}_{p^r}[x]$ whose image under the mod p reduction map is an irreducible polynomial in $\mathbb{F}_p[x]$. We can think of $\mathcal{R}$ as a Galois extension $\mathbb{Z}_{p^r}[\omega]$ of $\mathbb{Z}_{p^r}$ by a root ω of $h(x)$. Thus every element $z \in \mathcal{R}$ has a unique additive representation

$$z = \sum_{i=0}^{m-1} b_i \omega^i \tag{5}$$

where $b_i \in \mathbb{Z}_{p^r}$. The Galois ring $\mathcal{R}$ is a finite chain ring of length r, that is, $\mathcal{R}$ is a local principal ideal ring whose ideals $p^i\mathcal{R}$, with cardinality $p^{(r-i)m}$, $i = 0, 1, \ldots, r$, are linearly ordered by inclusion,

$$\{0\} = p^r\mathcal{R} \subset p^{r-1}\mathcal{R} \subset \ldots \subset p\mathcal{R} \subset \mathcal{R} \tag{6}$$

with its unique maximal ideal $p\mathcal{R}$ containing the nilpotent elements. The residue field $\mathcal{R}/p\mathcal{R}$ of $\mathcal{R}$ is the Galois field $\mathbb{F}_{p^m}$ and the elements of $\mathcal{R} \setminus p\mathcal{R}$ are units.

Since any two Galois rings of the same characteristic and the same cardinality are isomorphic, we shall often use the notation $GR(p^r, m)$ for any Galois ring with p^{rm} elements and characteristic p^r. When $m = 1$, the Galois ring $GR(p^r, m)$ becomes the integer ring $\mathbb{Z}_{p^r}$, and when $r = 1$, we obtain the Galois field $\mathbb{F}_{p^m}$. The Galois ring $GR(p^r, m)$ is a commutative Frobenius ring with identity whose generating character is $\chi(z) = \xi^{b_{m-1}}$, where $\xi = \exp(2\pi i/p^r)$ for $z = \sum_{i=0}^{m-1} b_i\omega^i$.

For the Galois ring $GR(p^r, m)$ we fix the following homogeneous weight as given in [5] for finite chain rings.

$$w_{\mathtt{hom}}(x) = \begin{cases} 0 & \text{if } x = 0 \\ p^{m(r-1)} & \text{if } x \in \left(p^{r-1}\right) \setminus \{0\} \\ (p^m - 1)p^{m(r-2)} & \text{otherwise} \end{cases} \tag{7}$$

where $\left(p^{r-1}\right)$ is the principal ideal generated by the element p^{r-1} of $GR(p^r, m)$. The weight (7) can actually be derived from (3), the group of units of $GR(p^r, m)$ has cardinality $p^{m(r-1)}(p^m - 1)$ and it easy to compute from (1) that its average value is equal to

$$\Gamma = (p^m - 1)p^{m(r-2)} \tag{8}$$

which is its minimum non-zero value. When $r = 1$, we have $\Gamma = (p^m - 1)/p^m$ and $w_{\mathtt{hom}}$ is just the usual Hamming weight $w_{\mathtt{Ham}}$ on $\mathbb{F}_{p^m}$. When $m = 1$, the average value is $\Gamma = (p-1)p^{r-2}$ for the integer ring $\mathbb{Z}_{p^r}$.

2.3 Convolutional codes over finite Frobenius rings

Let $R[D]$ be the ring of polynomials in the delay operator D with coefficients from a finite Frobenius ring R with identity $1 \neq 0$. In this section, we further assume that R is commutative. We shall consider a *rate-k/n convolutional code $\mathcal{C}$ over R* to be an $R[D]$-submodule of $R[D]^n$ obtained as the $R[D]$-rowspan of a matrix $G(D) \in R[D]^{k\times n}$. The rows of $G(D)$ are assumed to be linearly independent. The polynomial matrix $G(D)$ is called a *generator matrix* or a *convolutional encoder* of $\mathcal{C}$. Polynomial encoders are feedback-free (or non-recursive), they do not re-enter part of the output into the encoder as part of the next input. If we denote an information sequence by the k-vector

$$u(D) = [u_1(D), u_2(D), \ldots, u_k(D)], \tag{9}$$

the corresponding code sequence (or codeword) is the n-vector

$$v(D) = [v_1(D), v_2(D), \ldots, v_n(D)] \tag{10}$$

which results from the product $v(D) = u(D)G(D)$.

The encoder $G(D)$ for $\mathcal{C}$ is said to be *systematic* if it causes the information symbols to appear unchanged among the code symbols, or equivalently, if some k of its columns form the $k \times k$ identity matrix. The ith *constraint length*, denoted by ν_i, is defined to be the maximum among the degrees of the component polynomials of the ith row of $G(D)$. The *overall constraint length* of $G(D)$ is given by $\nu = \sum_{i=1}^{k} \nu_i$. The *memory* μ of $G(D)$ is the maximum among the constraint lengths of $G(D)$.

We apply a homogeneous weight w to the coefficients of a polynomial $f = \sum f_i D^i \in R[D]$, and define the *homogeneous weight* of f, denoted by $w(f)$, to be the sum of the homogeneous weights of the coefficients $f_i \in R$. If $z(D) = [z_1(D), z_2(D), \ldots, z_n(D)]$ is a vector in $R[D]^n$, the *homogeneous weight* of $z(D)$, denoted $w(z(D))$, is the sum of the homogeneous weights of the n component polynomials $z_i(D)$. The *homogeneous free distance* $d_{free}^{\mathtt{hom}}$ of $\mathcal{C}$ is the minimum $w(v(D))$ over all nonzero codewords $v(D)$ of $\mathcal{C}$.

3 Heller-type Bounds

The Heller upper bound on the free distance d_{free} of a binary, rate-b/c convolutional code is given by

$$d_{free} \leq \min_{L \geq 1} \left\{ \left\lfloor \frac{(\mu + L)c}{2(1 - 2^{-bL})} \right\rfloor \right\} \tag{11}$$

where the free distance d_{free} is with respect to the Hamming metric. This bound is also valid for any non-linear, time-invariant, binary, rate-b/c trellis code.

If $\mathcal{C}$ is a rate-k/n convolutional code over $\mathbb{Z}_4$ with memory μ and d_{free}^{L} is its free distance with respect to the Lee metric, then the image $\phi(\mathcal{C})$ of $\mathcal{C}$ under the Gray map ϕ is a binary (possibly non-linear) trellis code of rate $2k/2n$ and same memory μ with the property that $d_{free}^{L}(\mathcal{C}) = d_{free}(\phi(\mathcal{C}))$. Therefore,

$$d_{free}^{L} \leq \min_{L \geq 1} \left\{ \left\lfloor \frac{(\mu + L)n}{(1 - 4^{-kL})} \right\rfloor \right\}. \tag{12}$$

The Plotkin-type bound of Proposition 1 allows for a quick extension of (11) to a convolutional code over a finite Frobenius ring R in terms of the truncations of the code.

Theorem 1. *Let R be a finite Frobenius ring equipped with a homogeneous weight with average value Γ. The homogeneous free distance $d_{free}^{\mathtt{hom}}$ of a rate-k/n convolutional code over R encoded by a polynomial matrix of memory μ satisfies*

$$d_{free}^{\mathtt{hom}} \leq \min_{L \geq 1} \left\{ \left\lfloor \frac{(\mu + L)\,\Gamma n}{(1 - |R|^{-kL})} \right\rfloor \right\}. \tag{13}$$

Proof: Define the *degree* of a vector $x(D)$ of polynomials over R, denoted $\deg x(D)$, to be the maximum degree of any component polynomial in $x(D)$. Let $u(D)$ be an information word of $\mathcal{C}$ as in (9). We truncate $\mathcal{C}$ by making the restriction that $\deg u_i(D) \leq L - 1$. The corresponding codeword $v(D)$ therefore satisfies $\deg v(D) \leq \mu + L - 1$ since $\nu_i \leq \mu$. The truncated code becomes a block code of length $n(\mu + L)$ with $|R|^{kL}$ codewords. From Proposition 1, the minimum homogeneous distance $\delta_{\mathtt{min}}$ of this block code is bounded above by

$$\delta_{\mathtt{min}} \leq \frac{|R|^{kL}(\mu + L)\Gamma n}{|R|^{kL} - 1}. \tag{14}$$

Apply Proposition 1 for $L = 1, 2, \ldots$ and the proof is complete. □

We give the asymptotic version of the bound given above.

Corollary 1. *The homogeneous free distance of any rate-k/n convolutional code over R with encoder memory μ satisfies*

$$\lim_{\mu\to\infty} \frac{d_{free}^{\mathtt{hom}}}{\mu n} \leq \Gamma \,. \tag{15}$$

Proof: By straightforward manipulation, we get

$$\frac{d_{free}^{\mathtt{hom}}}{\mu n} \leq \min_{L\geq 1}\left\{\theta\cdot\Gamma + \theta\frac{L\cdot\Gamma}{\mu}\right\} \tag{16}$$

where $\theta = |R|^{kL}/(|R|^{kL}-1)$. By taking the limit, we get the result. □

We have a sharper bound if the generator matrix of $\mathcal{C}$ is systematic, as the next theorem shows.

Theorem 2. *The homogeneous free distance $d_{free}^{\mathtt{hom}}$ of a rate $\rho = k/n$ convolutional code with a systematic generator matrix $G(D)$ of memory μ satisfies*

$$d_{free}^{\mathtt{hom}} \leq \min_{L\geq 1}\left\{\left\lfloor \frac{(\mu(1-\rho)+L)\,\Gamma n}{1-|R|^{-kL}}\right\rfloor\right\} . \tag{17}$$

Proof: Let $u(D) = [u_1(D), u_2(D), \ldots, v_k(D)]$ be an input vector. Again we require that $\deg(u_i(D)) \leq L-1,\ i = 1,2,\ldots,k$. Let $v(D) = [v_1(D), v_2(D), \ldots, v_n(D)]$ be the resulting code vector via the encoding rule $v(D) = u(D)G(D)$. Since $G(D)$ is systematic, exactly k components of $v(D)$ are the $u_i(D)$'s. Hence k components of $v(D)$ will have degree $\leq L-1$, while the remaining $n-k$ components will have degree $\leq \mu+L-1$. The effective block length of the truncated code with $|R|^{kL}$ codewords is $kL+(n-k)(\mu+L) = (\mu(1-\rho)+L)n$. We get the result by applying Proposition 1 to the truncated code for $L = 1,2,\ldots$ □

The asymptotic version of the bound above is given in the following corollary.

Corollary 2. *The homogeneous free distance $d_{free}^{\mathtt{hom}}$ of a rate $\rho = k/n$ convolutional code with a systematic generator matrix of memory μ satisfies*

$$\lim_{\mu\to\infty} \frac{d_{free}^{\mathtt{hom}}}{\mu n} \leq (1-\rho)\cdot\Gamma \,. \tag{18}$$

Proof: We use the following equality

$$\frac{1}{\mu n}\left[\frac{(\mu(1-\rho)+L)\,\Gamma n}{1-|R|^{-kL}}\right] = \frac{(1-\rho)\Gamma}{1-|R|^{-kL}} + \frac{L\cdot\Gamma}{\mu(1-|R|^{-kL})} \,. \tag{19}$$

and then take the limit. □

In particular, for the Galois ring $\mathcal{R} = GR(p^r, m)$ equipped with the weight $w_{\mathtt{hom}}$ in (7), the homogeneous free distance of a rate-k/n convolutional code over $\mathcal{R}$ with encoder memory μ satisfies

$$d_{free}^{\mathtt{hom}} \leq \min_{L\geq 1}\left\{\left\lfloor \frac{(\mu+L)\ (p^m-1)p^{m(r-2)}n}{(1-p^{-rmkL})}\right\rfloor\right\} . \tag{20}$$

For the quaternary case $p=r=2$ and $m=1$, we get exactly (12). For the binary case $p=2$ and $r=m=1$, we get (11). Moreover, if $G(D)$ is systematic, we have

$$d_{free}^{\mathtt{hom}} \leq \min_{L\geq 1}\left\{\left\lfloor \frac{(\mu(1-\rho)+L)\ (p^m-1)p^{m(r-2)}n}{1-p^{-rmkL}}\right\rfloor\right\} . \tag{21}$$

Acknowledgement. The author thanks Patrick Solé of CNRS France for helpful comments, and gratefully acknowledges financial support from the UPLB Basic Research Grant.

References

[1] A. Ashikhmin and V. Zyablov, Samples of Unit-Memory Codes over $\mathbb{Z}_4$, *Proc. 1994 IEEE International Workshop on Information Theory*, Moscow, Russia (1994) pp. 119–121.

[2] I. Constantinescu and W. Heise, A metric for codes over residue class rings, *Problems Inform. Transmission*, vol. 33 no.3 (1997) pp. 208–213.

[3] I. Constantinescu, W. Heise and T. Honold Monomial extensions of isometries between codes over $\mathbb{Z}_M$, *Proc. of the 5th International Workshop on Algebraic and Combinatorial Coding Theory*, Unicorn Shumen, (1996) pp. 98–104.

[4] F. Fagnani and S. Zampieri, System-theoretic properties of convolutional codes over rings, *IEEE Trans. Inform. Theory*, vol. 47 no.6 (2001) pp. 2256–2274.

[5] M. Greferath and S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, *IEEE Trans. Inform. Theory*, vol. 45 no. 7 (2001) pp. 2522–2524.

[6] M. Greferath and S.E. Schmidt, Finite-ring combinatorics and MacWilliams Equivalence Theorem, *J. Combin Theory, Series A*, vol. 92 (2000) pp. 17–28.

[7] M. Greferath and M. E. O'Sullivan, On bounds for codes over Frobenius rings under homogeneous weights," *Discrete Math.*, vol. 289 (2004) pp. 11–24.

[8] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, vol. 40 no. 2 (1994) pp. 301–319.

[9] J. Heller, "Short constraint length convolutional codes," Jet Propulsion Lab., California Inst. Technol., Pasadena, Space Programs Summary 37-54, 3 : 171–177, 1968.

[10] T. Honold, A characterization of finite Frobenius rings, *Arch. Math. (Basel)*, vol. 76 (2001) pp. 406–415.

[11] Th. Honold and A. Nechaev, Weighted modules and representations of codes, *Probl. Inform. Transm.*, vol. 35 no. 3 (1999) pp. 205–222.

[12] R. Johannesson, Z. Wan and E. Wittenmark, Some structural properties of convolutional codes over rings, *IEEE Trans. Inform. Theory*, vol. 44 (1998) pp. 839–845.

[13] R. Johannesson and E. Wittenmark, Two 16-state, rate $R = 2/4$ trellis codes whose free distances meet the Heller bound, *IEEE Trans. Inform. Theory*, vol. 44 no. 4 (1998) pp. 1602–1604.

[14] R. Kötter, U. Dettmar and U.K. Sorger, On the construction of trellis codes based on (P)UM codes over $\mathbb{Z}_4$, *Probl. Inf. Trans.*, vol. 31 no.2 (1995) pp. 154–161.

[15] B.R. MacDonald, *Finite Rings with Identity*, Marcel Dekker, 1974.

[16] S. Mahapakulchai and R. Van Dyck, Design of ring convolutional trellis codes for MAP decoding of MPEG-4 images *IEEE Trans. Commun.*, vol. 52 no. 7 (2004) pp. 1033–1037.

[17] J.L. Massey and T. Mittelholzer, Convolutional codes over rings, *Proc. 4th Joint Swedish-Soviet Int. Workshop on Inform. Th.*, Gotland, Sweden, pp. 14–18, Aug. 27 - Sept. 1, 1989.

[18] Z.X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific, 2003.

[19] E. Wittenmark, "An encounter with convolutional codes over rings," *Ph.D. Dissertation*, Lund University, Sweden, 1998.

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