Irish Math. Soc. Bulletin
Number 72, Winter 2013, 35–36
ISSN 0791-5578

CONTRIBUTIONS TO ALGEBRAIC CODING THEORY OVER RINGS: FROM CODE EQUIVALENCE TO EFFICIENT DECODING

CATHY A. MC FADDEN

This is an abstract of the PhD thesis *Contributions to Algebraic Coding Theory over Rings: From Code Equivalence to Efficient Decoding* written by C. Mc Fadden under the supervision of Dr. Hab. M. Greferath at the Claude Shannon Institute and the School of Mathematical Sciences, University College Dublin, and submitted in May 2013.

The ceaseless drive to devise superior codes for a given application is competitive and utilises extensive resources. Determining whether a newly developed code differs significantly from its predecessors may be arduous. Mac Williams' Equivalence Theorem [2] simplifies this comparison for codes over finite fields. The theorem states that two codes are monomially equivalent if and only if there is an isometry between the codes that preserves Hamming weight.

As newer technologies continue to fuel the development of codes with more diverse alphabets and different weights, broader variants of the Equivalence Theorem have become necessary. It has been proved that the Equivalence Theorem holds for isometries preserving Hamming or homogeneous weights precisely when the alphabet is a finite Frobenius module. It remains to determine for which weights on a given alphabet an analogous theorem will hold for isometries preserving that weight. Greferath, Honold and Wood established the requirements for chain rings, integer residue rings [1] and matrix rings over finite fields [4].

We develop an algebraic framework to classify functions on modules for which the Equivalence Theorem holds, called extending weight functions. For ring alphabets this structure allows for a

2010 *Mathematics Subject Classification.* 94B05, 94B35, 16S36, 06C05.
Key words and phrases. Codes over rings, code equivalence, LDPC codes.
Received on 15-12-2013.
Support from Science Foundation Ireland through the Claude Shannon Institute is gratefully acknowledged.

character theoretic description in terms of the Fourier transform. We consider the case of functions which are invariant under multiplication by units of the ring. Applying the framework to finite direct products of finite chain rings specifies the invariant extending weight functions in terms of the Möbius function on the ideal lattice. Further generalisation of this result to principal ideal rings produces necessary and sufficient conditions for rational-valued invariant extending weight functions on that alphabet.

Taking a similar approach to iterative decoding algorithms as for the Equivalence Theorem delivers an algebraic aspect of the theory. Defining appropriate operations for distributions on rings yields a structural view of probabilistic message passing algorithms. Specifically a description of a ring-theoretic variant of the Sum-Product algorithm is supplied. We present decoding performance of the algorithm on $\mathbb{Z}_4$-linear codes, constructed from the binary LDPC codes of Rößing [3].

References

[1] M. Greferath, T. Honold: *Monomial extensions of isometries of linear codes II: Invariant weight functions on Z_m.* Proc. ACCT-10, 106–111. Russia, 2006.

[2] J. MacWilliams: *A theorem on the distribution of weights in a systematic code.* Bell System Tech. J. 42 (1963) 79–94.

[3] C. Rößing: *Contributions to Pure and Applicable Galois Geometry.* Ph.D. Thesis, Universiteit Gent, Belgium, 2012.

[4] J. A. Wood: *Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities.* In Codes over rings, Ser. Coding Theory Cryptol. 6 (2009) 124–190. World Sci. Publ., NJ, 2009.

School of Mathematical Sciences, University College Dublin
E-mail address, C. Mc Fadden: `cathy.mcfadden@ucd.ie`