[10] A. A. Nechaev and A. S. Kuzmin, “Kerdock codes in a cyclic form,” *Discr. Math. Appl.*, vol. 1, pp. 365–384, 1991.

[11] ——, “Linearly presentable codes,” in *Proc. IEEE Int. Symp. Information Theory and Its Applications*, 1996, pp. 31–34.

[12] P. Solé, “A quaternary cyclic code and a family of quadriphase sequences with low correlation properties,” *Lecture Notes in Computer Science*, vol. 388. Berlin, Germany: Springer-Verlag, 1989, pp. 193–201.

[13] J. V. Uspensky, *Theory of Equations.* New York: McGraw-Hill, 1948.

On $\mathbb{Z}_4$- and $\mathbb{Z}_9$-Linear Lifts of the Golay Codes

Marcus Greferath and Emanuele Viterbo, *Member, IEEE*

***Abstract*—We analyze $\mathbb{Z}_4$- and $\mathbb{Z}_9$-linear lifts of the binary $[24, 12]$ and ternary $[12, 6]$-Golay code under different weight functions on the underlying ring, and present algebraic decoding schemes for these codes.**

***Index Terms*—Codes over rings, decoding, Golay codes, weight functions on rings.**

I. Introduction

At the begining of the 1990’s, A. A. Nechaev [12] and later R. Hammons *et al.* [10] hinted at the significance of rings in Coding Theory. Since then many papers dealing with codes over $\mathbb{Z}_4$ (equipped with the Lee metric) and also other integer residue rings have been published. Foundational aspects involving more general rings and more general weight functions on these rings can be found in [15], [16], [11], [13], [8], and [9].

In this correspondence we investigate $\mathbb{Z}_4$-linear and $\mathbb{Z}_9$-linear lifts[1] of the extended binary and ternary Golay codes which have also been considered in [2], [14], and [4]. The paper [14] completely classifies the set of isomorphy classes of self-dual $\mathbb{Z}_4$-preimages of the binary code, and we mention that these can be used to construct the Leech lattice.

Following the line of a recent work [9] we introduce weight functions on $\mathbb{Z}_4$ and $\mathbb{Z}_9$ which reflect previously unknown error-correcting and packing capabilities of these codes. We compare their properties with those of the Hamming, Lee, and homogeneous weight (as presented in [11]) and give algebraic decoding schemes using the general decoder presented in [8]. The decoding method presented works for all free preimages of the Golay codes under the natural binary (ternary) reduction.

In our discussion of different weight functions on the alphabet $\mathbb{Z}_4$ or $\mathbb{Z}_9$ we will compute the volumes of the (open) balls of radius $d_{\min}/2$ where $d_{\min}$ is the minimum distance, in order to obtain a measure for the quality of the induced packing. This is done by an application of the generating function technique in [1, p. 298]. For the characterization of the errors being corrected we adopt the notation of [10] defining the *type* of a word e as its (complete) enumerator. For instance, 2^4 denotes the type of a word the nonzero components of which equal two in four positions, and by abuse of notation $(\pm 3)^3$ is the type of a word with exactly three nonzero components each of which is chosen from $\{3, -3\}$.

II. The Quaternary $[24, 12]$-Golay Code

The binary Golay code is a cyclic $[23, 12, 7]$-code generated by the polynomial $x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 \in \mathbb{Z}_2[x]$. Hensel-lifting this polynomial to $\mathbb{Z}_4[x]$ results in the polynomial $x^{11} - 2x^{10} - x^9 - x^7 - x^6 - x^5 - 2x^4 + x - 1$, which generates a free $[23, 12]$-code over $\mathbb{Z}_4$. Extending the latter code by a parity check produces a $\mathbb{Z}_4$-linear self-dual free $[24, 12]$-code E_4 which will be the subject of the following considerations.

In [3], the complete enumerator of E_4 has been computed. Using this, we determine the symmetrized enumerator as

$$\begin{aligned}\mathrm{SE}_{E_4}(x, y, z) = {} & 4096x^{24} + 24288x^{16}y^8 + 680064x^{16}y^6z^2 \\ & + 1700160x^{16}y^4z^4 + 680064x^{16}y^2z^6 \\ & + 24288x^{16}z^8 + 61824x^{12}y^{11}z \\ & + 1133440x^{12}y^9z^3 + 4080384x^{12}y^7z^5 \\ & + 4080384x^{12}y^5z^7 + 1133440x^{12}y^3z^9 \\ & + 61824x^{12}yz^{11} + 12144x^8y^{14}z^2 \\ & + 170016x^8y^{12}z^4 + 765072x^8y^{10}z^6 \\ & + 1214400x^8y^8z^8 + 765072x^8y^6z^{10} \\ & + 170016x^8y^4z^{12} + 12144x^8y^2z^{14} + y^{24} \\ & + 759y^{16}z^8 + 2576y^{12}z^{12} + 759y^8z^{16} + z^{24}.\end{aligned}$$

Here the variable x corresponds to the units, y to the element 2, and z to the zero element of $\mathbb{Z}_4$.Substituting $z \mapsto 1$ and $x, y \mapsto t$ we produce the 16-term Hamming weight enumerator.

$$\begin{aligned}W_H(t) = {} & 28385t^{24} + 61824t^{23} + 692208t^{22} \\ & + 1133440t^{21} + 1870176t^{20} + 4080384t^{19} \\ & + 1445136t^{18} + 4080384t^{17} + 1239447t^{16} \\ & + 1133440t^{15} + 765072t^{14} + 61824t^{13} \\ & + 172592t^{12} + 12144t^{10} + 759t^8 + 1.\end{aligned}$$

By the substitution $z \mapsto 1, x \mapsto t$ and $y \mapsto t^2$, we obtain the 15-term Lee weight enumerator

$$\begin{aligned}W_L(t) = {} & t^{48} + 12144t^{36} + 61824t^{34} \\ & + 195063t^{32} + 1133440t^{30} + 1445136t^{28} \\ & + 4080384t^{26} + 2921232t^{24} + 4080384t^{22} \\ & + 1445136t^{20} + 1133440t^{18} + 195063t^{16} \\ & + 61824t^{14} + 12144t^{12} + 1.\end{aligned}$$

Note that the Lee weight on $\mathbb{Z}_4$ coincides with the homogeneous weight introduced in [11].

Let us introduce the weight function

$$w_4 \colon \mathbb{Z}_4 \longrightarrow \mathbb{N}, \qquad r \mapsto \begin{cases} 0, & \text{if } r = 0 \\ 4, & \text{if } r \in \mathbb{Z}_4^* \\ 5, & \text{else.} \end{cases}$$

Manuscript received October 21, 1998; revised April 21, 1999.

M. Greferath is with AT&T Labs–Research, Florham Park, NJ 08732 USA, on leave from the Department of Mathematics, University of Duisburg, Duisburg, Germany.

E. Viterbo is with Dipartimento di Elettronica, Politecnico di Torino, I-10129 Torino, Italy.

Communicated by I. F. Blake, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(99)07005-4.

[1] By lifting an extended cyclic code we mean, by abuse of notation, the canonical way of Hensel-lifting its generator polynomial to the ring in question and then introducing the standard extension of the resulting cyclic code by a check position.

TABLE I
PERMUTATIONS USED FOR DECODING OF E_4

$\mathcal{P}_2$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
π_1	1	2	3	4	11	9	7	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	18
π_2	2	3	4	11	9	7	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	18
π_3	3	4	11	9	7	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	18
π_4	4	11	9	7	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	18
π_5	11	9	7	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	18
π_6	9	7	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	18
π_7	7	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	18
π_8	22	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	18
π_9	14	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	18
π_{10}	16	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	18
π_{11}	13	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	18
π_{12}	24	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	18
π_{13}	5	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	18
π_{14}	6	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	18
π_{15}	20	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	6	18
π_{16}	19	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	6	20	18
π_{17}	17	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	6	20	19	18
π_{18}	12	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	6	20	19	17	18
π_{19}	10	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	6	20	19	17	12	18
π_{20}	23	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	6	20	19	17	12	10	18
π_{21}	8	21	15	1	2	3	4	11	9	7	22	14	16	13	24	5	6	20	19	17	12	10	23	18

For this weight the substitution $z \mapsto 1$, $x \mapsto t^4$, and $y \mapsto t^5$ yields the weight enumerator

$$\begin{aligned} W_{w_4} = {} & t^{120} + 24288t^{104} + 61824t^{103} \\ & + 12144t^{102} + 4096t^{96} + 680064t^{94} \\ & + 1133440t^{93} + 170016t^{92} + 1700160t^{84} \\ & + 4080384t^{83} + 765072t^{82} + 759t^{80} \\ & + 680064t^{74} + 4080384t^{73} + 1214400t^{72} \\ & + 24288t^{64} + 1133440t^{63} + 765072t^{62} \\ & + 2576t^{60} + 61824t^{53} + 170016t^{52} \\ & + 12144t^{42} + 759t^{40} + 1. \end{aligned}$$

The respective sphere packings, and accordingly, the error-correcting capabilities reflected by the different weights, are quite different: the Hamming ball of radius 3 contains exacly 57 205 words. In contrast, the Lee ball of radius 5 contains 1 925 357 words, wheras the w_4-ball of radius 19 covers 907 285 words. In Section IV, we develop a bounded distance decoder for E_4, which implements the error-correcting capabilities reflected by the latter weight. Note that the set of correctable errors is given by the set of all words of Hamming weight up to 4 except the word of type 2^4.

Remark 2.1: For the weight function

$$w: \mathbb{Z}_4 \longrightarrow \mathbb{N}, \quad r \mapsto \begin{cases} 0, & \text{if } r = 0 \\ 3, & \text{if } r \in \mathbb{Z}_4^* \\ 4, & \text{else} \end{cases}$$

which, up to a normalization, was first introduced in [9], we obtain the nine-term weight enumerator

$$\begin{aligned} W_w(t) = {} & t^{96} + 98256t^{80} + 1987616t^{72} \\ & + 6546375t^{64} + 5974848t^{56} + 1925376t^{48} \\ & + 231840t^{40} + 12903t^{32} + 1. \end{aligned}$$

The w-ball of radius 15 covers 2 267 413 words; it consists of the w_4-ball of radius 19 together with the $\binom{24}{5} \cdot 2^5$ words of type $(\pm 1)^5$ and it is an open problem to find a decoding algorithm that implements the corresponding error correction.

III. THE $\mathbb{Z}_9$-LINEAR [12, 6]-GOLAY CODE

The ternary Golay code is a cyclic [11, 6, 5]-code generated by the polynomial $x^5 + x^4 - x^3 + x^2 - 1 \in \mathbb{Z}_3[x]$. Hensel-lifting this polynomial to $\mathbb{Z}_9[x]$ results in the polynomial $x^5 - 2x^4 - x^3 + x^2 - 3x - 1$, which generates a free [11, 6] code over $\mathbb{Z}_9$. Extending the latter code by a parity check produces a $\mathbb{Z}_9$-linear free [12, 6]-code E_9 which is the subject of this section.

Using a computer program we compute the symmetrized enumerator as

$$\begin{aligned} \mathrm{SE}_{E_9}(x, y, z) = {} & 17496x^{12} + 95040x^9y^3 + 142560x^9y^2z \\ & + 71280x^9yz^2 + 11880x^9z^3 + 16632x^6y^6 \\ & + 52272x^6y^5z + 59400x^6y^4z^2 + 47520x^6y^3z^3 \\ & + 11880x^6y^2z^4 + 4752x^6yz^5 + 24y^{12} \\ & + 440y^9z^3 + 264y^6z^6 + z^{12}. \end{aligned}$$

Here the x, y, and z denote the variables for the unital multiples of 1, 3, and 0, respectively. From this we obtain the Hamming weight enumerator

$$\begin{aligned} W_H(t) = {} & 129192t^{12} + 194832t^{11} + 130680t^{10} + 59840t^9 \\ & + 11880t^8 + 4752t^7 + 264t^6 + 1 \end{aligned}$$

by the substitution $z \mapsto 1$ and $x, y \mapsto t$, which shows that E_9 possesses only eight different Hamming weights. Since its minimum weight is given by 6 this code corrects all Hamming errors of weight ≤ 2 which yields a sphere packing with Hamming balls of volume 4321. It can furthermore be seen, that the minimum Lee weight of E_9 equals 9 producing a packing with Lee balls of volume 16641.

For the homogeneous weight w_{hom} on $\mathbb{Z}_9$, which assigns the units the weight 2 and the nonzero nonunits the weight 3, we compute the weight enumerator of E_9 by substituting $x \mapsto t^2, y \mapsto t^3$, and $z \mapsto 1$ and get

$$\begin{aligned} W_{w_{\mathrm{hom}}}(t) = {} & 24t^{36} + 16632t^{30} + 147752t^{27} + 219456t^{24} \\ & + 118800t^{21} + 24024t^{18} + 4752t^{15} + 1. \end{aligned}$$

As in the case of the Hamming weight it turns out that E_9 possesses only eight different homogeneous weights and it can be seen that this is not true in general for other choices of the weight function. The homogeneous weight produces a packing which is denser than the Hamming or Lee packings discussed earlier. Since E_9 has a minimum homogeneous weight of 15 we easily see that the volume of the balls in this packing is given by 99361.

Like in the preceding section, there exists a weight function on $\mathbb{Z}_9$, which produces an even denser packing and hence reflects additional error-correcting capabilities of the code at hand. To see this we establish the weight function

$$w_9: \mathbb{Z}_9 \longrightarrow \mathbb{N}, \quad r \mapsto \begin{cases} 0, & \text{if } r = 0 \\ 5, & \text{if } r \in \mathbb{Z}_9^* \\ 6, & \text{else.} \end{cases}$$

TABLE II
PERMUTATIONS USED FOR DECODING OF E_9

$\mathcal{P}_3$	1	2	3	4	5	6	7	8	9	10	11	12
π_1	1	2	3	4	7	11	5	9	8	12	6	10
π_2	2	3	4	7	11	5	9	8	12	6	1	10
π_3	3	4	7	11	5	9	8	12	6	1	2	10
π_4	4	7	11	5	9	8	12	6	1	2	3	10
π_5	7	11	5	9	8	12	6	1	2	3	4	10
π_6	11	5	9	8	12	6	1	2	3	4	7	10
π_7	5	9	8	12	6	1	2	3	4	7	11	10
π_8	9	8	12	6	1	2	3	4	7	11	5	10
π_9	8	12	6	1	2	3	4	7	11	5	9	10
π_{10}	12	6	1	2	3	4	7	11	5	9	8	10

The weight enumerator of E_9 with respect to this function is computed by substituting $x \mapsto t^5, y \mapsto t^6$, and $z \mapsto 1$, which yields the 12-term enumerator

$$\begin{aligned} W_{w_9}(t) = {} & 24t^{72} + 16632t^{66} + 95040t^{63} \\ & + 69768t^{60} + 142560t^{57} + 59840t^{54} \\ & + 71280t^{51} + 47520t^{48} + 11880t^{45} \\ & + 11880t^{42} + 5016t^{36} + 1. \end{aligned}$$

Due to the minimum weight of 36 we find that E_9 is able to correct all error patterns of weight up to 17, which yields a packing by balls of volume 115201. The set of all errors correctable by E_9 is simply described by the set of all errors up to Hamming-weight 3 except the $8 \cdot \binom{12}{3}$ errors of type $(\pm 3)^3$.

IV. A BOUNDED DISTANCE DECODER

In all what follows let C_p, $p \in \{2, 3\}$, denote the respective cyclic Golay code, and let E_p denote its extension by a parity check. We now develop decoding schemes for E_{p^2} as defined in the foregoing sections correcting all error patterns of weight less than half of the respective w_{p^2}-minimum distances.

A Decoder for E_p and a Set of Permutations

Complete algebraic decoders for the cyclic Golay codes have been developed in [5] and [6]. These algorithms can be upgraded to decode E_p by simply appending the parity-check symbol to the codeword decoded by the decoding algorithm for C_p. The resulting decoder $\mathbb{D}_p$ then reliably corrects all errors of Hamming weight ≤ 3 in case of $p = 2$, and of Hamming weight ≤ 2 in case $p = 3$. Furthermore, all quadruple (triple) errors affecting the check position are reliably corrected, whereas if such errors occur in the cyclic part then they will cause a decoding error.

The permutation group of E_p, provides a set $\mathcal{P}_p$ of permutations such that for every error e of Hamming weight at most 4 (3) there exists $\pi \in \mathcal{P}_p$ such that $\pi(e)$ can reliably be corrected by $\mathbb{D}_p$. This is due to the fact that π moves one of the nonzero positions of e into the extension position of E_p.

We first obtain the permutation $(5, 11, 13)$ $(6, 9, 14)$ $(8, 22, 21)$ $(10, 16, 19)$ $(12, 24, 18)$ $(15, 20, 23)$ of E_2 and $(5, 7)$ $(6, 11)$ $(8, 9)$ $(10, 12)$ of E_3 by consulting `Magma V2.3-1`. Multiplying these permutations with the cyclic shifts (in the respective cyclic component) we obtain the permutation Tables I and II.

In order to implement the full error-correcting capabilities of E_{p^2} we combine the general decoding technique presented in [8] with an application of the above permutations to the p-adic components of the received word. This is possible because the codes in question are free, and hence splitting in the sense of [7].

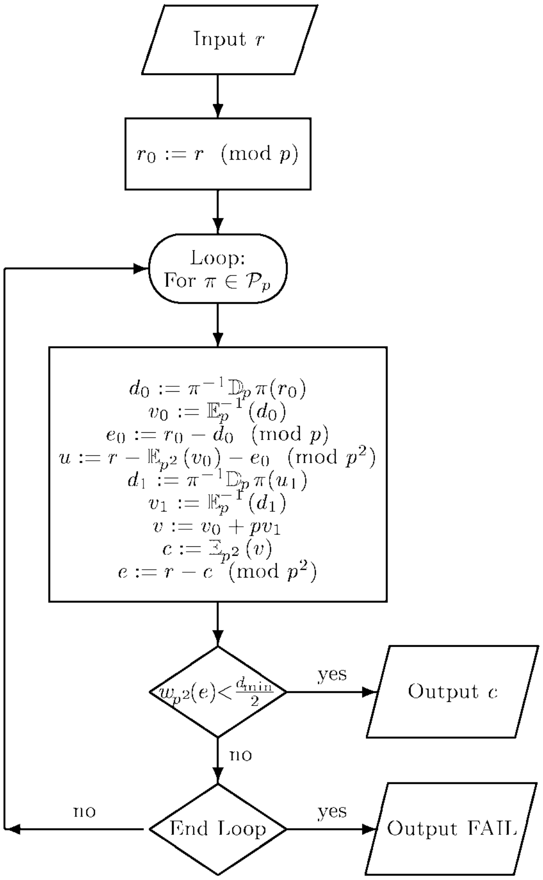
Input r
$r_0 := r \pmod{p}$
Loop:
For $\pi \in \mathcal{P}_p$
$d_0 := \pi^{-1}\mathbb{D}_p\pi(r_0)$
$v_0 := \mathbb{E}_p^{-1}(d_0)$
$e_0 := r_0 - d_0 \pmod{p}$
$u := r - \mathbb{E}_{p^2}(v_0) - e_0 \pmod{p^2}$
$d_1 := \pi^{-1}\mathbb{D}_p\pi(u_1)$
$v_1 := \mathbb{E}_p^{-1}(d_1)$
$v := v_0 + pv_1$
$c := \mathbb{E}_{p^2}(v)$
$e := r - c \pmod{p^2}$
$w_{p^2}(e) < \frac{d_{\min}}{2}$
yes
Output c
no
End Loop
yes
Output FAIL
no

Fig. 1. Flowchart of the decoder.

This yields a set of $|\mathcal{P}_p|$ votes for the transmitted word which contains the word actually sent. This word can easily be identified as the unique one closest (with respect to w_{p^2}) to the received word.

We illustrate the bounded distance decoder $\mathbb{D}_{p^2}$ in Fig. 1, where we denote the encoder and decoder of E_p with $\mathbb{E}_p$ and $\mathbb{D}_p$, respectively. We denote by $\mathbb{E}_p^{-1}$ the reverse encoding operation which extracts the information symbols from a codeword of E_p. Finally $\mathbb{E}_{p^2}$ denotes the encoder for the code E_{p^2}.

REFERENCES

[1] E. R. Berlekamp, *Algebraic Coding Theory*, rev. ed. Laguna Hills, CA: Aegean Park, 1984.

[2] A. Bonnecaze, A. R. Calderbank, and P. Solé, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory*, vol. 41, pp. 366–377, 1995.

[3] A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain, "Type II codes over Z_4," *IEEE Trans. Inform. Theory*, vol. 43, pp. 969–976, 1997.

[4] A. R. Calderbank and N. J. A. Sloane, "The ternary Golay code, the integers $\bmod 9$, and the Coxeter–Todd lattice," *IEEE Trans. Inform. Theory*, vol. 42 pp. 636–637, Mar. 1996.

[5] M. Elia, "Algebraic decoding of the binary $(23, 12, 7)$ Golay code," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 150–151, Oct. 1987.

[6] M. Elia and E. Viterbo, "Algebraic decoding of the Ternary $(11, 6, 5)$ Golay code," *Electron. Lett.*, vol. 28, no. 21, pp. 2021–2022, Oct. 1992.

[7] M. Greferath, "Cyclic codes over finite rings," *Discr. Math*, vol. 177, pp. 273–277, 1997.

[8] M. Greferath and U. Vellbinger, "Efficient decoding of $\mathbb{Z}_{p^k}$-linear codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1288–1291, 1998.

[9] ——, "On the extended error-correcting capabilities of the quaternary Preparata codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2018–2019, 1998.

[10] A. R. Hammons, 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, pp. 301–319, 1994.

[11] I. Constantinescu and W. Heise, “A metric for codes over residue class rings of integers,” *Probl. Pered. Inform.*, vol. 33, no. 3, pp. 22–28, 1997.
[12] A. A. Nechaev, “Kerdock code in a cyclic form,” *Discr. Math. Appl.*, vol. 1, pp. 365–384, 1991.
[13] A. A. Nechaev and A. S. Kuzmin, “Linearly presentable codes,” *Proc. IEEE Int. Symp. Information Theory and Its Applications*, 1996, pp. 31–34.
[14] E. Rains, “Optimal self-dual codes over $\mathbb{Z}_4$,” preprint, 1996.
[15] J. A. Wood, “Extension theorems for linear codes over finite rings,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, T. Mora and H. Mattson, Eds. Berlin, Germany: Springer-Verlag, 1997, pp. 329–340.
[16] ——, “Weight functions and the extension theorem for linear codes over finite rings,” *Contemp. Math.*, vol. 225, pp. 231–243, 1999.

Negacyclic and Cyclic Codes Over $\mathbb{Z}_4$

Jacques Wolfmann, *Member, IEEE*

***Abstract*—The negashift ν of $\mathbb{Z}_4^n$ is defined as the permutation of $\mathbb{Z}_4^n$ such that**

$$\nu(a_0, a_1, \cdots, a_i, \cdots, a_{n-1}) = (-a_{n-1}, a_0, \cdots, a_i, \cdots, a_{n-2})$$

and a negacyclic code of length n over $\mathbb{Z}_4$ is defined as a subset C of $\mathbb{Z}_4^n$ such that $\nu(C) = C$. We prove that the Gray image of a linear negacyclic code over $\mathbb{Z}_4$ of length n is a binary distance invariant (not necessary linear) cyclic code. We also prove that, if n is odd, then every binary code which is the Gray image of a linear cyclic code over $\mathbb{Z}_4$ of length n is equivalent to a (not necessary linear) cyclic code and this equivalence is explicitely described. This last result explains and generalizes the existence, already known, of versions of Kerdock, Preparata, and others codes as doubly extended cyclic codes. Furthermore, we introduce a family of binary linear cyclic codes which are Gray images of $\mathbb{Z}_4$-linear negacyclic codes.

***Index Terms*—Gray map, negacyclic and cyclic codes over $\mathbb{Z}_4$.**

I. Introduction

As usual, $\mathbb{Z}_4$ is the ring of integers modulo 4 and $\mathbb{F}_2$ is the finite field of order 2.

The negashift ν of $\mathbb{Z}_4^n$ is defined as the permutation of $\mathbb{Z}_4^n$ such that

$$\nu(a_0, a_1, \cdots, a_i, \cdots, a_{n-1}) = (-a_{n-1}, a_0, \cdots, a_i, \cdots, a_{n-2})$$

and a negacyclic code of length n over $\mathbb{Z}_4$ is defined as a subset C of $\mathbb{Z}_4^n$ such that $\nu(C) = C$.

Recently, the Gray map of $\mathbb{Z}_4^n$ into $\mathbb{F}_2^{2n}$ was used to solve an important old problem in Coding Theory about Kerdock and Preparata codes and this gives a new point of view on some binary codes (see [6] for a survey).

We prove that the Gray image of a linear negacyclic code over $\mathbb{Z}_4$ of length n is a binary distance-invariant (not necessary linear) cyclic code. We also prove that, if n is odd, then the Gray image of a linear cyclic code over $\mathbb{Z}_4$ of length n is equivalent to a (not necessary linear) cyclic code and this equivalence is explicitly described. This last result explains and generalizes the existence, already known, of versions of Kerdock, Preparata, and others codes as doubly extended cyclic codes.

In general, the Gray image of a $\mathbb{Z}_4$-linear code is not a binary linear code. In Section IV we introduce a family of binary linear cyclic codes which are Gray images of $\mathbb{Z}_4$ linear negacyclic codes.

The reader can find more information on Coding Theory in [10] and on codes over $\mathbb{Z}_4$ in [19].

Warning:

1) Classicaly, “cyclic code” means linear and shift-invariant code. In this correspondence we consider shift-invariant codes which are not necessary linear.Consequently, we use “cyclic code” for every shift-invariant code, linear or not.
2) If A is any commutative ring, and $f(x)$ is a polynomial of degree d in $A[x]$, we represent the factor ring $A[x]/(f(x))$ as the set of polynomials of $A[x]$ which are zero or of degree at most $d-1$, endowed with modulo $f(x)$ addition and multiplication. In other words, every nonzero class modulo $f(x)$ is represented by its member of smallest degree. In this way, a member of this factor ring can be viewed as a member of $A[x]$ as well. If necessary, we specify if calculations are made in $A[x]$ or in the factor ring.

II. Negacyclic Codes

A. Definitions

First recall that a linear code of length n over $\mathbb{Z}_4$ is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$ and that the polynomial representation of $\mathbb{Z}_4^n$ is the map $\mathcal{P}$ of $\mathbb{Z}_4^n$ into $\mathbb{Z}_4[x]$ such that

$$\mathcal{P}(a_0, a_1, \cdots, a_i, \cdots, a_{n-1}) = \sum_{i=0}^{n-1} a_i x^i.$$

If C is a subset of $\mathbb{Z}_4^n$, its polynomial representation is $\mathcal{P}(C)$.

We now introduce less familiar definitions about codes over $\mathbb{Z}_4$.

Definitions 2.1:

1) The negashift ν of $\mathbb{Z}_4^n$ is the permutation of $\mathbb{Z}_4^n$ defined by

$$\nu(a_0, a_1, \cdots, a_i, \cdots, a_{n-1}) = (-a_{n-1}, a_0, \cdots, a_i, \cdots, a_{n-2}).$$

2) Let ν be the negashift of $\mathbb{Z}_4^n$.

A negacyclic code of length n over $\mathbb{Z}_4$ is a subset C of $\mathbb{Z}_4^n$ such that $\nu(C) = C$.

Proposition 2.2: A subset C of $\mathbb{Z}_4^n$ is a linear negacyclic code of length n over $\mathbb{Z}_4$ if and only if its polynomial representation is an ideal of the factor ring $\mathbb{Z}_4[x]/(x^n+1)$.

Proof: The proof is quite similar to the proof about polynomial representations of linear cyclic codes over a finite field $\mathbb{F}_q$ as ideals of $\mathbb{F}_q[x]/(x^n-1)$ and is left to the reader (see [10]). □

B. Negacyclic Codes of Odd Length

Proposition 2.3: Let μ be the map of $\mathbb{Z}_4[x]/(x^n-1)$ into $\mathbb{Z}_4[x]/(x^n+1)$ defined by

$$\mu(a(x)) = a(-x).$$

If n is odd then μ is a ring isomorphism.

Manuscript received June 7, 1998; revised May 28, 1999. The material in this correspondence was presented in part at the Workshop on Coding and Cryptography, Paris, France, January 1999.

The author is with GECT, Université Toulon-Var, 83957 La Garde Cedex, France.

Communicated by A. M. Barg, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(99)07448-9.