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

M. Greferath
Shannon Labs, AT&T
Florham Park
NJ 07632, USA
greferath@research.att.com

E. Viterbo[1]
Politecnico di Torino
C. Duca degli Abruzzi 24
Torino, Italy
viterbo@polito.it

In this paper we investigate $\mathbb{Z}_4$-linear and $\mathbb{Z}_9$-linear lifts[2] of the extended binary and ternary Golay codes. Following the line of a recent work [4] 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 [5]) and give algebraic decoding schemes using the general decoder presented in [3] and the algebraic decoder in [1]. In the following we will illustrate the 9-ary case. Similar results were obtained for the quaternary case.

In our discussion of different weight functions on the alphabet $\mathbb{Z}_9$ we will compute the volumes of the balls of radius $d_{\min}/2 - 1$ where $d_{\min}$ is the minimum distance, in order to obtain a measure for the quality of the induced packing.

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.

Using a computer program we compute the symmetrized enumerator $\mathrm{SE}_{E_9}(x, y, z)$ where 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 by the substitution $z \mapsto 1$ and $x, y \mapsto t$. 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 [5] on $\mathbb{Z}_9$, which assigns the units the weight 2 and the nonzero non-units the weight 3, we compute the weight enumerator of E_9 by substituting $x \mapsto t^2, y \mapsto t^3$, and $z \mapsto 1$. Like in the case of the Hamming weight it turns out that E_9 possesses only 8 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 before. 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.

We found 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. Let us consider the weight function $w_9 : \mathbb{Z}_9 \longrightarrow \mathbb{N}$ such that $w_9(0) = 0$, $w_9(u) = 5$ if $u \in \mathbb{Z}_9^*$ and $w_9(x) = 6$ otherwise.

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

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

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 errors of type $\pm 3^3$.

A complete algebraic decoder for the cyclic Golay codes has been developed in [1]. This algorithm can be upgraded to decode the extended ternary code E_3 by simply appending the parity check symbol to the codeword decoded by the decoding algorithm for C_3. The resulting decoder $\mathbb{D}_3$ then reliably corrects all errors of Hamming weight 2. Furthermore all 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_3, provides a set $\mathcal{P}_3$ of permutations such that for every error e of Hamming weight at most 3 there exists $\pi \in \mathcal{P}_3$ such that $\pi(e)$ can reliably be corrected by $\mathbb{D}_3$. This is due to the fact that π moves one of the nonzero positions of e into the extension position of E_3.

We first obtain the permutation $(5, 7)(6, 11)(8, 9)(10, 12)$ of E_3 using `Magma V2.3-1`. Multiplying these permutations with the cyclic shifts (in the respective cyclic component) we obtain the necessary permutations.

In order to implement the full error-correcting capabilities of E_9 we combine the general decoding technique given in [3] with an application of the above permutations to the 3-adic components of the received word. This is possible because the codes in question are free, and hence splitting in the sense of [2]. This yields a set of $|\mathcal{P}_3|$ 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_9) to the received word.

[1] This work was performed during his visit at Shannon Labs.

[2] 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.

References

[1] M. Elia, E. Viterbo: "Algebraic Decoding of the Ternary (11,6,5) Golay Code", *Electronics Letters*, Vol. 28, No. 21, pp. 2021–2022, Oct. 1992.

[2] M. Greferath: "Cyclic Codes over Finite Rings", *Disc. Math*, 177, pp. 273–277, 1997.

[3] M. Greferath, U. Vellbinger: "Efficient Decoding of $\mathbb{Z}_{p^k}$-linear Codes", *IEEE Trans. Inf. Th.*, Vol. 44, pp. 1288–1291, 1998.

[4] M. Greferath, U. Vellbinger: "On the Extended Error Correcting Capabilities of the Quaternary Preparata Codes", *IEEE Trans. Inf. Th.*, Vol. 44, pp. 2018–2019, 1998.

[5] I. Constantinescu, W. Heise: "A metric for codes over residue class rings of integers", *Problemy Peredachi Informatsii*, Vol. 33, no. 3, pp. 22–28, 1997.

0-7803-5268-8/99/$10.00 ©1999 IEEE