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

by:

Marcus Greferath and Emanuele Viterbo

AT&T Shannon Labs, Florham Park, NJ

Politecnico di Torino, Italy

Information Theory Workshop 1999

Structure of the Talk

- Motivation
- The $\mathbb{Z}_9$-linear Hensel lifted ternary Golay Code
- Weight Functions on $\mathbb{Z}_9$ and symmetrized Weight Distributions
- A Bounded Distance Decoder

The $\mathbb{Z}_9$-linear Hensel lifted ternary Golay Code

- The Ternary Golay code is a cyclic $[11,6,5]$-code. Hensel-lifting its generator polynomial to $\mathbb{Z}_9[x]$ results in polynomial
$$x^5 - 2\,x^4 - x^3 + x^2 - 3\,x - 1,$$
which generates (free) $[11,6]$ code over $\mathbb{Z}_9$.
- Extension of this code by parity check produces a (free) $\mathbb{Z}_9$-linear self-dual $[12,6]$-code C with (unit) symmetrized enumerator:
$$\begin{aligned}\mathrm{SE}_C(x,y,z) \;=\; & 17496\,x^{12} + 95040\,x^9y^3 + 142560\,x^9y^2z \\ & + 71280\,x^9yz^2 + 11880\,x^9z^3 + 16632\,x^6y^6 \\ & + 52272\,x^6y^5z + 59400\,x^6y^4z^2 + 47520\,x^6y^3z^3 \\ & + 11880\,x^6y^2z^4 + \boxed{4752\,x^6yz^5} + 24\,y^{12} \\ & + 440\,y^9z^3 + \boxed{264\,y^6z^6} + z^{12}.\end{aligned}$$

Weight Functions on $\mathbb{Z}_9$ and symmetrized Weight Distributions

- We obtain Hamming weight enumerator
$$\begin{aligned}W_H(t) \;=\; & 129192\,t^{12} + 194832\,t^{11} + 130680\,t^{10} + 59840\,t^9 \\ & + 11880\,t^8 + 4752\,t^7 + \boxed{264\,t^6} + 1,\end{aligned}$$
having only 8 different terms.
- Minimum Hamming weight 6 induces sphere packing with Hamming balls of volume 4321.
- It can be shown, that minimum Lee weight of C is given by 9 producing packing with Lee balls of volume 16641.

- Constantinescu and Heise introduce the *homogeneous weight* on integer residue class rings. On $\mathbb{Z}_9$ it takes the form:

$$w_{\text{hom}} : \mathbb{Z}_9 \longrightarrow \mathbb{N}, \quad r \mapsto \begin{cases} 0 & \text{if } r = 0 \\ 2 & \text{if } r \in \mathbb{Z}_9^* \\ 3 & \text{else} \end{cases}$$

- The weight enumerator belonging to the homogeneous weight consists of only 8 terms, too, and is given by:

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

- Due to a minimum homogeneous weight of 15 this yields a packing with balls of volume 99361.

- We introduce an alternative weight function on $\mathbb{Z}_9$:

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

- The weight enumerator belonging to the homogeneous weight consists of only 12 terms, and is given by:

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

- Due to a minimum homogeneous weight of 36 this yields a packing with balls of volume 115201. The set of all correctable errors by C coincides with the set of all errors up to Hamming-weight 3 except the $\binom{12}{3} \cdot 8$ errors of type $\pm 3^3$.

A Bounded Distance Decoder

- Elia and Viterbo (1992) give an algebraic decoder for the $[11, 6, 5]$ ternary Golay Code.
- We extend this to a decoder $\mathbb{D}_3$ for the extended $[12, 6, 6]$ code as follows:

  If $(r_1, \ldots, r_{12})$ is received, then decode cyclic part $(r_1, \ldots, r_{11})$ using E&V-scheme and modify the check position r_{12} as necessary:

$$(\underbrace{r_1, \ldots, r_{11}}_{\text{E\&V}}, \underbrace{r_{12}}_{\text{Check}})$$

- This decoding scheme reliably corrects all single and double Hamming errors and all triple errors affecting the check position. Triple errors in the cyclic part cause a decoding error.

- Using `Magma V2.3-1` we determine the Permutation Group of the Extended Golay Code as a 7920-element group generated by:

$$\begin{array}{ll} (1,2)(5,10)(7,12)(8,9) & (2,3)(6,11)(8,12)(9,10) \\ (3,4)(6,8)(9,11)(10,12) & (4,6)(5,10)(7,8)(9,12) \\ (5,7)(6,11)(8,9)(10,12) & \end{array}$$

- We construct a set $\mathcal{P}$ of 10 permutations using the identity, the permutation $(5,7)(6,11)(8,9)(10,12)$ and powers of $(1,2,3,4,5,6,7,8,9,10,11)$ that satisfies:

> If e is an error vector of Hamming weight (at most) 3, then there exists $\pi \in \mathcal{P}$, such that $\pi(e)$ is correctable by $\mathbb{D}_3$.

- This yields the following permutation table:

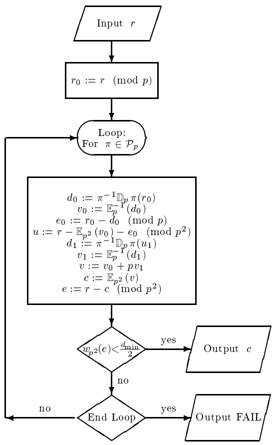
$\mathcal{P}$	1	2	3	4	5	6	7	8	9	10	11	12
π_1	1	2	3	4	5	6	7	8	9	10	11	12
π_2	2	3	4	7	11	5	9	8	12	6	1	10
π_3	3	4	7	11	5	9	8	12	6	1	2	10
π_4	4	7	11	5	9	8	12	6	1	2	3	10
π_5	7	11	5	9	8	12	6	1	2	3	4	10
π_6	11	5	9	8	12	6	1	2	3	4	7	10
π_7	5	9	8	12	6	1	2	3	4	7	11	10
π_8	9	8	12	6	1	2	3	4	7	11	5	10
π_9	8	12	6	1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

The lifted decoder

- In order to implement the full error-correcting capabilities of the lifted code we combine the general decoding technique proposed by Greferath and Vellbinger (1998) with an application of the above permutations to the 3-adic components of the received word ($r = r_0 + r_1 p$).

- All the above discussion was also applied to the extended $\mathbb{Z}_4$-lifted binary Golay code $[24, 12]$ over $\mathbb{Z}_4$.

The lifted decoder



Lifted codes decoder by a simple example

- Decoding of $\mathrm{RM}(1,3)$ can be done efficiently by Majority Logic.
- Generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

- Equation $(a_0, a_1, a_2, a_3)G = (x_0, x_1, \ldots, x_7)$ leads to majoriy vote:

$$\begin{aligned} a_3 &= x_1 + x_0 \\ &= x_3 + x_2 \\ &= x_5 + x_4 \\ &= x_7 + x_6 \end{aligned}$$

- After determination of a_3 subtract $(0,0,0,a_3)G$ from received word and determine a_2, a_1 und a_0 using similar equations.

- Consider $\mathbb{Z}_4$-linear Octacode generated by the matrix

$$G' := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 0 & 1 & 3 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 & 0 & 1 \end{pmatrix}$$

- Relation $(a_0, a_1, a_2, a_3)G' = (x_0, x_1, \ldots, x_7)$ leads to a System of Equations:

$$\begin{aligned} a_3 &= x_1 - x_0 + 2a_1 + 2a_2 \\ &= x_3 - x_2 \\ &= x_5 - x_4 + 2a_1 \\ &= x_7 - x_6 + 2a_2 \end{aligned}$$

Dipartimento di Elettronica
Politecnico di Torino

- **Idea:** First determine $2a_3, 2a_2, 2a_1$ and $2a_0$ using Majority Logic Decoding for RM$(1,3)$; then exploit knowledge of these values in a second Majority logic application.

- **Question:** Can this be generalized?

- **Answer:** Yes, to very large class of rings and large class of codes.
  - Demonstration for $\mathbb{Z}_{p^k}$ – valid for any (Artinian) commutative chain ring.
  - Code class given by *splitting* Codes defined as having a complement in the ambient module.

Dipartimento di Elettronica
Politecnico di Torino