Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$

Rama Krishna Bandi

Indian Institute of Technology Roorkee, India
Joint work with Maheshanand Bhaintwal

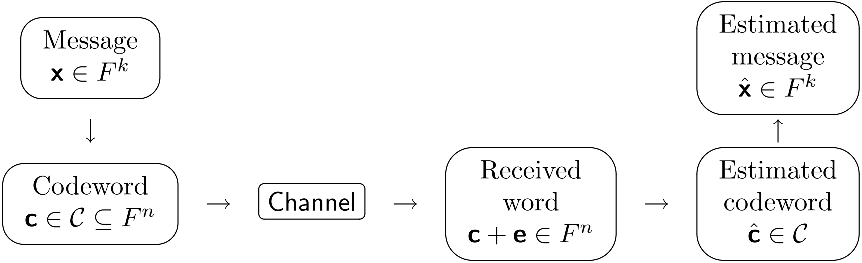
September 24, 2014
International Conference on Advances in Computing, Communications and Informatics (ICACCI 2014)

Outline

Introduction

- Coding theory addresses the problem of controlling errors on noisy communication channels.

Schematic representation of coding:



- Classically codes have been studied over finite fields. (A linear code is a subspace of $\mathbb{F}_q^n$, $\mathbb{F}_q$ a finite field.)

Algebraic Codes

- Algebraic codes: Mostly studied over finite fields.
- Recently, finite rings have got the attention of many researchers especially after (Hammons *et al.*, 1994).
- These codes have been mostly generalized to codes over:
  - Finite chain rings
  - Galois rings ($\mathbb{Z}_4$ and its generalization)
  - Rings of the form:
    - $\mathbb{F}_2 + u\mathbb{F}_2$ (Bonnecaze and Udaya, 1999)
    - $\mathbb{F}_2 + v\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ (Zhu *et al.*, 2010 and Yildiz and Karandiz, 2010)
    - $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p + \ldots + u^{m-1}\mathbb{F}_p$, etc.
  - Recently a new ring structure $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$ has been introduced in (Yildiz and Karandiz, 2014).
  - We have studied the codes with respect to Rosenbloom-Tsfasman metric over a similar ring structure $\mathbb{Z}_4 + v\mathbb{Z}_4$, where $v^2 = v$ in (R. K. Bandi and Bhaintwal, 2013).

Why codes over Rings ?

- Many well known non-linear binary codes are images of linear codes over $\mathbb{Z}_4$.
- Several good codes have been obtained over different finite rings.
- Many structural properties of codes over rings are still not well understood.
- The families of codes studied here are among the most popular families of codes studied over finite fields. They have rich algebraic structures. They have provided several good codes (over finite fields and over some finite rings).

The ring $R = \mathbb{Z}_4 + v\mathbb{Z}_4$ and its properties

Let $R = \mathbb{Z}_4 + v\mathbb{Z}_4 = \{a + ub \mid a, b \in \mathbb{Z}_4, v^2 = v\}$.

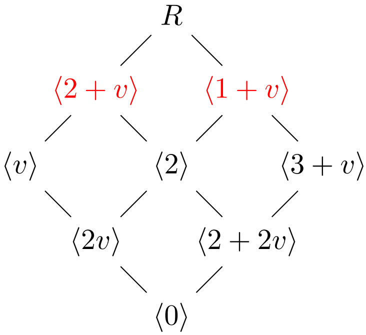
$R \cong \mathbb{Z}_4[u]/\langle u^2 \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_4$.

Units: $1, 3, 1 + 2v, 3 + 2v$.

R is a principal ideal ring with 7 non-trivial principal ideals:

$$
\begin{aligned}
\langle 2v \rangle &= \{0, 2v\} \\
\langle 2 + 2v \rangle &= \{0, 2 + 2v\} \\
\langle v \rangle &= \{0, v, 2v, 3v\} = \langle 3v \rangle \\
\langle 2 \rangle &= \{0, 2, 2v, 2 + 2v\} \\
\langle 3 + v \rangle &= \{0, 1 + 3v, 2 + 2v, 3 + v\} = \langle 1 + 3v \rangle \\
\langle 1 + v \rangle &= \{0, 2, 2v, 1 + v, 1 + 3v, 2 + 2v, 3 + v, 3 + 3v\} = \langle 3 + 3v \rangle \\
\langle 2 + v \rangle &= \{0, 2, v, 2v, 3v, 2 + v, 2 + 2v, 2 + 3v\} = \langle 2 + 3v \rangle
\end{aligned}
$$

Lattice diagram of ideals of R



- R is semi-local ring with two maximal ideals $\langle 2+v \rangle$ and $\langle 1+v \rangle$.
- R can be expressed as: $R = \langle 1+3v \rangle \oplus \langle v \rangle$.

Gray map on R

Gray map

For any $x = a(1+3v) + (a+b)v \in R$ the Gray map $\psi : R \to \mathbb{Z}_4^2$ is defined by $\psi(x) = (a,\ a+b)$.

- This map can be extended componentwise to R^n.
- ϕ is a Z_4-module isomorphism.

Weights on R

$$\begin{aligned} \text{Lee weight} &: \quad w_L(a+ub) = w_L(a, a+b) \\ \text{Gray weight} &: \quad w_G(a+ub) = w_H(a, a+b) \\ \text{Euclidean weight} &: \quad w_E(a+vb) = w_E(a, a+b). \end{aligned}$$

These weight are then extended componentwise to R^n.

Theorem

The Gray map $\phi : R^n \to \mathbb{Z}_4^{2n}$ is a distance preserving linear isometry.

A linear code C of length n over R is an R-submodule of R^n.

Define $C_1 = \{a \in \mathbb{Z}_4^n : \ a + bv \in C \ \text{ for some } \ b \in \mathbb{Z}_4^n\}$ and $C_2 = \{a + b \in \mathbb{Z}_4^n : \ a + bv \in C \ \text{ for some } \ a \in \mathbb{Z}_4^n\}$, where C_1, C_2 are linear codes of length n over $\mathbb{Z}_4$.

The dual of C is $C^{\perp} = \{x \in R_i^n \mid x \cdot c = 0, \ \forall \ c \in C\}$, where $x \cdot y$ denotes the usual inner product of x and y over R_i.

The ring R is a Frobenius ring, and then $|C||C^{\perp}| = 16^n$ (Wood, 1999).

Theorem

Let C be a linear code of length n over R. Then $\phi(C) = C_1 \otimes C_2$ and $|C| = |C_1||C_2|$.

Corollary

A linear code C over R can be expressed as $C = (1+3v)C_1 \oplus vC_2$.

Theorem

Let C be a linear code of length n over R. Then $\phi(C^{\perp}) = \phi(C)^{\perp}$.

Lee weight distribution on R

Elements (X) of R	Representative of X	Gray image of X	Lee weight of X	Weight representative
0	a_1	$(0,0)$	0	x
1	a_2	$(1,1)$	2	z
2	a_3	$(2,2)$	4	s
3	a_4	$(3,3)$	2	z
v	a_5	$(0,1)$	1	y
2v	a_6	$(0,2)$	2	z
3v	a_7	$(0,3)$	1	y
1+v	a_8	$(1,2)$	3	w
1+2v	a_9	$(1,3)$	2	z
1+3v	a_{10}	$(1,0)$	1	y
2+v	a_{11}	$(2,3)$	3	w
2+2v	a_{12}	$(2,0)$	2	z
2+3v	a_{13}	$(2,1)$	3	w
3+v	a_{14}	$(3,0)$	1	y
3+2v	a_{15}	$(3,1)$	2	z
3+3v	a_{16}	$(3,2)$	3	w

Let I be a non-zero ideal of R. Define the Character

$$\chi : I \longrightarrow \mathbb{C}^* \text{ by } \chi(a + bv) = i^b,$$

where $\mathbb{C}^*$ is the multiplicative group of unit complex numbers.

- χ is a non-trivial character of I, and hence $\sum_{a \in I} \chi(a) = 0$.

Let I be a non-zero ideal of R. Define the Character

$$\chi : I \longrightarrow \mathbb{C}^* \quad \text{by} \quad \chi(a+bv) = i^b,$$

where $\mathbb{C}^*$ is the multiplicative group of unit complex numbers.

- χ is a non-trivial character of I, and hence $\sum_{a \in I} \chi(a) = 0$.

Complete Lee Weight Enumerator :

$clwe_C(x_1, x_2, \ldots, x_{16}) = \sum_{c \in C} x_1^{wt_{a_1}(c)} x_2^{wt_{a_2}(c)} \cdots \; x_{16}^{wt_{a_{16}}(c)}$, where $wt_{a_i}(c)$ is the number of a_i's in c.

Let I be a non-zero ideal of R. Define the Character

$$\chi : I \longrightarrow \mathbb{C}^* \text{ by } \chi(a+bv) = i^b,$$

where $\mathbb{C}^*$ is the multiplicative group of unit complex numbers.

- χ is a non-trivial character of I, and hence $\sum_{a \in I} \chi(a) = 0$.

Complete Lee Weight Enumerator :

$clwe_C(x_1, x_2, \ldots, x_{16}) = \sum_{c \in C} x_1^{wt_{a_1}(c)} x_2^{wt_{a_2}(c)} \cdots x_{16}^{wt_{a_{16}}(c)}$, where $wt_{a_i}(c)$ is the number of a_i's in c.

Theorem (MacWilliams, 1977)

Let C be a linear code of length n over R. Then

$$clwe_{C^\perp}(x_1, x_2, \ldots, x_{16}) = \frac{1}{|C|} clwe_C(M \cdot (x_1, x_2, \ldots, x_{16})^T),$$

where M is an $|R| \times |R|$ matrix defined by $M(i,j) = \chi(a_i a_j)$.

Symmetrized Lee weight enumerator (slwe) :

$$slwe_C(x,y,z,w,s) = clwe_C(x,z,s,z,y,z,y,w,z,y,w,z,w,y,z,w),$$

$$slwe_C(x,y,z,w,s) = \sum_{c\in C} x^{wt_0} y^{wt_1} z^{wt_2} w^{wt_3} s^{wt_4},$$

where

$$\begin{aligned} wt_0 &= wt_{a_1}(c); \\ wt_1 &= wt_{a_5}(c) + wt_{a_7}(c) + wt_{a_{10}}(c) + wt_{a_{14}}(c); \\ wt_2 &= wt_{a_2}(c) + wt_{a_4}(c) + wt_{a_6}(c) + wt_{a_9}(c) + wt_{a_{12}}(c) + wt_{a_{15}}(c); \\ wt_3 &= wt_{a_8}(c) + wt_{a_{11}}(c) + wt_{a_{13}}(c) + wt_{a_{16}}(c); \qquad (1) \\ wt_4 &= wt_{a_3}(c). \end{aligned}$$

Theorem

Let C be a linear code of length n over R. Then
$slwe_{C^\perp}(x, y, z, w, s) = \frac{1}{|C|} slwe_C(x + 4y + 6z + 4w + s, x - 2y + 2w - s, x - 2z + s, x + 2y - 2w - s, x - 4y + 6z - 4w + s)$.

Theorem

Let C be a linear code of length n over R. Then $slwe_{C^{\perp}}(x,y,z,w,s) = \frac{1}{|C|} slwe_C(x+4y+6z+4w+s, x-2y+2w-s, x-2z+s, x+2y-2w-s, x-4y+6z-4w+s)$.

The Lee weight enumerator (Lee) of the linear code C over R is defined as

$$Lee_C(x,y) = \sum_{c \in C} x^{4n-wt_L(c)} y^{wt_L(c)}.$$

Theorem

Let C be a linear code of length n over R. Then

$$Lee_C(x,y) = slwe_C(x^4, x^3y, x^2y^2, xy^3, y^4).$$

MacWillimas identities

Theorem (MacWillimas identity 1)

Let C be a linear code of length n over R. Then

$$Lee_{C^{\perp}}(x,y) = \frac{1}{|C|} Lee_C(x+y, x-y).$$

Theorem (MacWillimas identity 2)

Let C be a linear code of length n over R. Then

$$G_{C^{\perp}}(x,y) = \frac{1}{|C|} G_C(x+3y, x-y).$$

Example

Let C be a linear code of length 2 over R generated by $\{(1, 3 + 2v), (0, 2)\}$. The Gray map image of this code is a code of length 4 over $\mathbb{Z}_4$ and it is of type $4^2 2^2$. The Lee and Gray weight enumerators of C are $1 + 12z^2 + 39z^4 + 11z^6 + z^8$ and $1 + 4z + 12z^2 + 24z^3 + 23z^4$, respectively.

Example

The linear code C of length 4 over R generated by $\{(1 + 3v, 1 + v, 3 + 3v, 3 + v), (2 + 2v, 2v, 0, 2)\}$ is a self-orthogonal code of 32 codewords and its Gray image is also a self-orthogonal code of length 8 over $\mathbb{Z}_4$. The code C has all even Lee weight codewords and the minimum Lee weight of C is 4. The Lee and Gray weight enumerators of C are $1 + 3z^4 + 19z^8 + 9z^{12}$ and $1 + 5z^2 + 12z^4 + 14z^6$, respectively.

Self-dual codes over R

A code C is said to be *self-orthogonal* if $C \subseteq C^{\perp}$

and *self-dual* if $C = C^{\perp}$.

Theorem

If C is a self-dual code over R then so are $\phi(C)$, C_1 and C_2 over $\mathbb{Z}_4$.

Proof.

This follows from the fact that $\phi(C^{\perp}) = \phi(C)^{\perp}$. □

Theorem

A self-dual code of any length over R exists.

Proof.

We know that $|C||C^{\perp}| = 16^n$ for any linear code C of length n over R.

Since C is a self-dual code over R, $|C| = 16^{\frac{n}{2}} = 4^n$.

The code of length 1 generated by $\langle 2 \rangle$ is a self-dual code.

Therefore, by taking direct sums of self-dual codes of length 1 we can obtain a self-dual code of any length over R. □

Lemma

There is no free self-dual code of odd length over R.

Proof.

Let C be a free self-dual code over R of length n with basis A.

Then $|C| = 16^{k_0}$, where $|A| = k_0$.

Since C is self-dual, $|C| = 16^{\frac{n}{2}}$.

So, $k_0 = \frac{n}{2}$. Therefore n must be even. □

Theorem

The length of any free self-dual code over R is at least 6.

Proof.

No free self-dual code of odd length over R.

A free self-dual code of length 2 over R must contain a codeword $(1, x)$, where $x \in R$. So $1 + x^2 = 0 \pmod 4$, impossible in R.

Let C be a free self-dual code of length 4 generated by $G = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & c_1 & d_1 \\ 0 & 1 & c_2 & d_2 \end{pmatrix}$. Since C is self-dual, $1 + c_1^2 + d_1^2 = 0$, impossible in R.

Consider $G = (g_1, g_2, g_3)^T = \begin{pmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 \\ 0 & 1 & 0 & a_3 & a_1 & a_2 \\ 0 & 0 & 1 & a_2 & a_3 & a_1 \end{pmatrix}$, where each a_i, $i = 1, 2, 3$ is a self inverse element of R such that $a_1a_2 + a_1a_3 + a_2a_3 = 0$. This generates a free self-dual code of length 6 over R. □

Theorem

A self-dual code C of length n over R contains $\overline{2} = (2, 2, \ldots, 2)$.

Proof.

The ring R can be partitioned into 4 sets as
$A_0 = \{0, 2, 2v, 2 + 2v\}$, $A_1 = \{1, 3, 1 + 2v, 3 + 2v\}$,
$A_v = \{v, 3v, 2 + v, 2 + 3v\}$, $A_{1+3v} = \{1 + v, 1 + 3v, 3 + v, 3 + 3v\}$,
where A_i, contains $a \in R$ such that $a^2 = i$.
Let n_i denote the number of components of
$c = (c_1, c_2, \ldots, c_n) \in C$ which are from A_i.
Since C is a self-dual code, so

$$\langle c, c\rangle = n_1 + v\ n_v + (1 + 3v)\ n_{1+3v} = 0.$$

$$\text{Now, } c \cdot \overline{2} = 2n_1 + (2v)n_v + (2 + 2v)n_{1+3v} = 0.$$

Therefore, $(2, 2, \ldots, 2) \in C^{\perp} = C$. □

Construction of Self-dual codes

Theorem (Construction 1)

Let $G = [I_n \mid A_n]$, where $A_n = (a_{ij})$, is a square matrix of order n such that $\sum_{j=1}^{n} a_{ij} = 1$ or 3, for $i = 1, 2, \ldots, n$. If G is a generator matrix of a free self-dual code C of length $2n$ (n is an even integer) over R, then

$$G' = \begin{pmatrix} I_n & B_n & \cdots & B_n & A_n & B_n & \cdots & B_n \\ B_n & I_n & \cdots & B_n & B_n & A_n & \cdots & B_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ B_n & B_n & \cdots & I_n & B_n & B_n & \cdots & A_n \end{pmatrix}$$

generates a free self-dual code C' of length $2kn$ over R, where B_n is an all α matrix of order n, α a unit in R, and B_n is being repeated $2(k-1)$ times in each row of G'.

Example

Let C be a self-dual code of length 8 over R generated by

$$G = \begin{pmatrix} 1000 & 0 & 1+2v & 3+2v & 3 \\ 0100 & 1 & 1 & 1 & 0 \\ 0010 & 3+2v & 0 & 1+2v & 3 \\ 0001 & 1+2v & 3+2v & 0 & 3 \end{pmatrix}.$$

Then the matrix $G' = \begin{pmatrix} I_4 & B_4 & A_4 & B_4 \\ B_4 & I_4 & B_4 & A_4 \end{pmatrix}$

$$= \begin{pmatrix} 1\,0\,0\,0 & \alpha\alpha\alpha\alpha & 0\;a\;b\;3 & \alpha\alpha\alpha\alpha \\ 0\,1\,0\,0 & \alpha\alpha\alpha\alpha & 1\,1\,1\,0 & \alpha\alpha\alpha\alpha \\ 0\,0\,1\,0 & \alpha\alpha\alpha\alpha & b\;0\;a\;3 & \alpha\alpha\alpha\alpha \\ 0\,0\,0\,1 & \alpha\alpha\alpha\alpha & a\;b\;0\;3 & \alpha\alpha\alpha\alpha \\ \alpha\alpha\alpha\alpha & 1\,0\,0\,0 & \alpha\alpha\alpha\alpha & 0\;a\;b\;3 \\ \alpha\alpha\alpha\alpha & 0\,1\,0\,0 & \alpha\alpha\alpha\alpha & 1\,1\,1\,0 \\ \alpha\alpha\alpha\alpha & 0\,0\,1\,0 & \alpha\alpha\alpha\alpha & b\;0\;a\;3 \\ & 0\,0\,0\,1 & & b\;0\;3 \end{pmatrix},$$

Construction of Self-dual codes

Theorem (Construction 2)

Let $G = (g_1, g_2, \ldots, g_n)^T$*, where* $g_i = (g_{i1}, g_{i2}, \ldots, g_{in})$*, be a generator matrix of a free self-dual code* C *of length* n *over* R*. Let* $x \in R^n$ *such that* $1 + x^2 = 0$*, and* $y_i := x \cdot g_i$*. Then* $G' = \begin{pmatrix} 1 & 0 & 0 & 0 & x \\ 3y & y & y & y & G \end{pmatrix}$*, generates a free self-orthogonal code* C' *of length* $(2n+4)$ *over* R*, where* $y = (y_1, y_2, \ldots, y_n)^T$*.*

Example

The matrix $G = \begin{pmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 \\ 0 & 1 & 0 & a_3 & a_1 & a_2 \\ 0 & 0 & 1 & a_2 & a_3 & a_1 \end{pmatrix}$, where $a_1 = 1 + 2v$, $a_2 = 3$ and $a_3 = 3 + 2v$, generates a free self-dual code of length 4 over R. From the above code we can construct a self-orthogonal code over R, as follows:

We have $A_3 = \begin{pmatrix} 1+2v & 3 & 3+2v \\ 3+2v & 1+2v & 3 \\ 3 & 3+2v & 1+2v \end{pmatrix}$ then

$X = (vI_3 + A_3)(1,1,1)^T = (3+v, 3+v, 3+v)^T$. Then $G' =$

$$\begin{pmatrix} 1 & v & 0 & 0 & 0 & v & v & v & 1 & 1 & 1 \\ 0 & 1+3v & 3+v & 3+v & 3+v & v & 0 & 0 & 3v & 3v & v \\ 0 & 1+3v & 3+v & 3+v & 3+v & 0 & v & 0 & v & 3v & 3v \\ 0 & 1+3v & 3+v & 3+v & 3+v & 0 & 0 & v & 3v & v & 3v \end{pmatrix}$$

generates a self-orthogonal code of length 11.

Type II codes

A self-dual code C over R is said to be Type II code if the Euclidean weight of every code word is divisible by 8, otherwise C is said to be Type I code.

Theorem

A Type II code of length n over R exists if and only if n is a multiple of 4.

The following Theorem is analogous to ([Theorem 2.13] Yildiz and Karandiz, 2010).

Theorem

Let $d_E(II)$ and $d_E(I)$ be the minimum Euclidean weights of a Type II code and a Type I code of length n, respectively, over R. Then $d_E(II)$, $d_E(I) \leq 8\lfloor \frac{n}{12} \rfloor + 8$.

Conclusion

- We have studied linear codes over R.
- We have derived MacWilliams identities.
- We have discussed the properties of self-dual codes over R.
- Some constructions of self-dual codes have also been seen.
- Type II codes over R are also considered.

- [R. K. Bandi and M. Bhaintwal, 2013] R. K. Bandi and M. Bhaintwal, *On codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with respect to Rosenbloom-Tsfasman metric*, Proceedings of ICACCI 2013 (IEEE Explore 2013).
- [Bonnecaze and Udaya, 1999] A. Bonnecaze and P. Udaya, *Cyclic and self-dual Codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Transactions on Information Theory, 45, pp. 1250-1255, 1999.
- [Hammons et. al., 1994] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Slone and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Transactions on Information Theory, 44, pp. 301–319, 1994.
- [MacWilliams and Sloane, 1977] F. J. MacWilliams and N. J. A. Sloane *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.

- [Yildiz and Karandiz, 2010] B. Yildiz and S. Karadeniz, *Self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst., 347, 1888–1894, 2010.
- [Yildiz and Karandiz, 2014] B. Yildiz and S. Karadeniz, *Linear codes over* $\mathbb{Z}_4 + u\mathbb{Z}_4$*, MacWilliams identities, projections, and formally self-dual codes*, Finite Fields Appl., 27, pp. 24–40, 2014.
- [Wood, 1999] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, American Journal of Mathematics, 121 (3), pp. 555-575, 1999.
- [Zhu et. al., 2010] S. Zhu, Y. Wang and M. Shi, *Some Results on Cyclic Codes Over* $\mathbb{F}_2 + v\mathbb{F}_2$, IEEE Transactions on Information Theory, 56, pp. 1680–1684, 2010.


Thank You


Queries please...