Aalto University
School of Science
and Technology

On Rings, Weights, Codes, and Isometries

Marcus Greferath

Department of Mathematics and Systems Analysis
Aalto University School of Science
marcus.greferath@aalto.fi

March 10, 2015

What are rings and modules?

- Rings are like fields, however: no general division.
- Every field is a ring, but (of course) not vice versa!
- Proper examples are $\mathbb{Z}$, together with what we call the integer residue rings $\mathbb{Z}/n\mathbb{Z}$.
- Given rings R and S, the direct product $R \times S$ with componentwise operations is again a ring.
- For a given ring R, we can form the polynomial ring $R[x]$ and the matrix ring $M_n(R)$.
- Another prominent structure coming from a ring R and a semigroup G is the semigroup ring $R[G]$.

What are rings and modules?

- A favourable way of representing the elements in $R[G]$ is by R-valued mappings on G.
- Then the multiplication in $R[G]$ takes the particularly welcome form of a convolution:

$$f \star g\,(x) \;:=\; \sum_{\substack{a,b \in G \\ ab = x}} f(a)\,g(b)$$

- Modules generalise the idea of a vector space; a module over a ring is exactly what a vector space is over a field.
- We denote a (right) module by M_R, which indicates that the ring R is operating from the *right* on the abelian group M.

What are rings and modules?

- If R is a finite ring, then an (additive) character on R is a mapping $\chi : R \longrightarrow \mathbb{C}^{\times}$, and we emphasize the relation

$$\chi(a+b) \;=\; \chi(a)\cdot\chi(b).$$

- For this reason, we may consider the character as a kind of exponential function on the given ring.
- The set $\widehat{R} := \mathrm{Hom}(R, \mathbb{C}^{\times})$ of all characters on R is called the character module of R.
- It is indeed a right module by the definition:

$$\chi^{r}(x) \;:=\; \chi(rx), \quad \text{for all } r, x \in R \text{ and } \chi \in \widehat{R}$$

And what are Frobenius rings?

- In general the modules $\widehat{R}_R$ and R_R are non-isomorphic.
- If they are, however, we call the ring R a Frobenius ring.
- Frobenius rings are abundant, although not omnipresent.
- Examples start at finite fields and integer residue rings...
- ...and survive the ring-direct product, matrix and group ring constructions discussed earlier.
- The smallest non-Frobenius ring to be aware of is the 8-element ring
$$\mathbb{F}_2[x, y]/(x^2, y^2, xy).$$

What do I need to memorize from this section?

1. Modules over rings are a generalisation of vector spaces over fields.
2. Characters are exponential functions on a ring R.
3. A Frobenius ring R possesses a character χ such that all other characters have the form ${}^r\chi$ for suitable $r \in R$.
4. Many, although not all finite rings are actually Frobenius.
5. Until further notice, all finite rings considered in this talk will be Frobenius rings.

Weight functions and ring-linear codes

- Given a (finite Frobenius) ring R, coding theory first needs a distance function $\delta : R \times R \longrightarrow \mathbb{R}_+$.
- To keep things simple, one usually starts with a weight function $w : R \longrightarrow \mathbb{R}_+$ in order to define

$$\delta(r,s) \;:=\; w(r-s) \quad \text{for all } r,s \in R.$$

- On top of this, we identify this weight with its natural additive extension to R^n, writing

$$w(x) \;:=\; \sum_{i=1}^{n} w(x_i) \quad \text{for all } x \in R^n.$$

Weight functions and ring-linear codes

- **Example 1:** R is the finite field $\mathbb{F}_q$, and $w := w_H$, the Hamming weight, defined as

$$w_H(r) := \begin{cases} 0 & : \quad r = 0, \\ 1 & : \quad \text{otherwise.} \end{cases}$$

- In this case the resulting distance is the Hamming distance, which means for $x, y \in \mathbb{F}_q^n$, we have

$$\delta_H(x, y) = \#\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}.$$

- This is the metric basis for coding theory on finite fields!

Weight functions and ring-linear codes

- **Example 2:** R is $\mathbb{Z}/4\,\mathbb{Z}$, and $w := w_{\text{Lee}}$, the Lee weight, defined as

$$w_{\text{Lee}}(r) \;:=\; \begin{cases} 0 & : \quad r = 0, \\ 2 & : \quad r = 2, \\ 1 & : \quad \text{otherwise.} \end{cases}$$

- In this case the resulting distance is the Lee distance δ_{Lee}.
- This is the metric basis for coding theory on $\mathbb{Z}/4\,\mathbb{Z}$ that became important by a prize-winning paper in 1994.

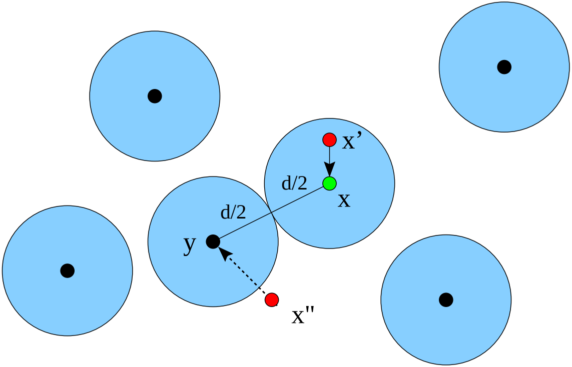
Weight functions and ring-linear codes

- Whatever is assumed on R and w, a (left) R-linear code will be a submodule $C \leq {}_R R^n$.
- Its minimum weight will be

$$w_{\min}(C) \ := \ \min\{w(c) \mid c \in C,\ c \neq 0\}.$$

- If $|C| = M$ and $d = w_{\min}(C)$ then we will refer to C as an (n, M, d)-code.
- The significance of the minimum weight results from the error-correcting capabilities illustrated on the next transparency.

Error correction in terms of minimum distance



- From the above it becomes evident, that maximising both $M = |C|$ and $d = w_{\min}(C)$ are conflicting goals.

What is equivalence of codes?

- **Definition:** Two codes $C, D \leq {}_R R^n$ are equivalent if they are isometric, i.e. there exists an R-linear bijection $\varphi : C \longrightarrow D$ such that

$$w(\varphi(c)) = w(c) \quad \text{for all } c \in C.$$

- **Textbook:** C and D in $\mathbb{F}_q^n$ are equivalent, if there is a monomial transformation Φ on $\mathbb{F}_q^n$ that takes C to D.

- **Reminder:** A monomial transformation Φ is a product of a permutation matrix Π and an invertible diagonal matrix D.

$$\Phi = \Pi \cdot D$$

What is equivalence of codes?

- **Question:** Why two different definitions?
- **Answer:** Because they might be the same!
- **Theorem:** (MacWilliams' 1962) Every Hamming isometry between two codes over a finite field is the restriction of a monomial theorem of the ambient space.
- **Question:** Is this only true for finite-field coding theory, and for the Hamming distance?
- **Answer:** Well, this is what we are talking about today!

What do I need to memorize from this section?

1. Coding theory requires a weight function on the alphabet. Very common is the Hamming weight.

2. A linear code is a submodule C of ${}_R R^n$. Optimal codes maximise both
   - the minimum distance $w_{\min}(C)$ between words in C (for good error correction capabilities), and
   - the number of words $|C|$ (for good transmission rates).

3. Morphisms in coding theory are code isometries.

4. MacWilliams' proved that these are restrictions of monomial transformations in traditional finite-field coding theory.

Hamming isometries and their extension

- **Theorem 1:** (Wood 1999) Hamming isometries between linear codes over finite Frobenius rings allow for monomial extension.
- **Theorem 2:** (Wood 2008) If the finite ring R is such that all Hamming isometries between linear codes allow for monomial extension, then R is a Frobenius ring.
- **Conclusion:** Regarding the Hamming distance, finite Frobenius rings are the appropriate class in ring-linear coding theory, since the extension theorem holds.
- **However:** Is the Hamming weight as important for ring-linear coding as it is for finite-field linear coding?

Which weights are good for ring-linear coding?

- **Theorem 3:** (Nechaev 20??) It is impossible to outperform finite-field linear codes by codes over rings while relying on the Hamming distance.
- **Conclusion:** Ring-linear coding must consider metrics different from the Hamming distance, otherwise pointless!
- **Question:** Is there a weight function on a finite ring that is as tailored for codes over rings as the Hamming weight for codes over fields?
- **Answer:** Yes, and this comes next...

Which weights are good for ring-linear coding?

- **Definition:** (Heise 1995) A weight $w : R \longrightarrow \mathbb{R}$ is called homogeneous, if $w(0) = 0$ and there exists nonzero $\gamma \in \mathbb{R}$ such that for all $x, y \in R$ the following holds:
  - $w(x) = w(y)$ provided $Rx = Ry$.
  - $\frac{1}{|Rx|} \sum_{y \in Rx} w(y) \; = \; \gamma$ for all $x \neq 0$.
- **Examples:**
  - The Hamming weight on $\mathbb{F}_q$ is homogeneous with $\gamma = \frac{q-1}{q}$.
  - The Lee weight on $\mathbb{Z}/4\,\mathbb{Z}$ is homogeneous with $\gamma = 1$.

Which weights are good for ring-linear coding?

- **Theorem 4:** (G. and Schmidt 2000)
  - Homogeneous weights exist on any ring.
  - Homogeneous isometries between codes over finite Frobenius rings allow for monomial extension.
  - Homogeneous and Hamming isometries are the same.
- A number of codes over finite Frobenius rings have been discovered outperforming finite-field codes.
- In each of these cases, the homogeneous weight provided the underlying distance.

What do I need to memorize from this section?

1. A very useful weight for ring-linear coding theory is the homogeneous weight.
2. Other weights may also be useful, if not for engineering then at least for scholarly purposes.
3. Hamming and homogeneous isometries allow for the extension theorem.
4. The Hamming and homogenoeus weight are therefore two weights satisfying foundational results in the theory.
5. A natural question is then, if we can characterise **all** weights on a Frobenius ring that behave in this way.

General assumptions

- From now on R will always be a finite Frobenius ring.
- A weight will be any complex valued function on R regardless of metric properties.
- We will assume one fundamental relationship that underlies all results of this talk and paper:

  BI: For all $x \in R$ and $u \in R^{\times}$ (the group of invertible elements of R), there holds $w(ux) = w(x) = w(xu)$.

- Weights satisfying this condition are referred to as bi-invariant weights.
- Of course, the Hamming weight and the homogeneous weight are bi-invariant weights on any ring.

Goal and first preparations

- **Goal:** provide a characterisation of all bi-invariant weights on R that allow for the extension theorem.
- The space $\mathbb{W} := \mathbb{W}(R)$ of all bi-invariant weight functions that map 0_R to $0_{\mathbb{C}}$ forms a complex vector space.
- We will make $\mathbb{W}$ a module over a subalgebra $\mathbb{S}$ of the multiplicative semigroup algebra $\mathbb{C}[R]$ by defining

$$\mathbb{S} \;:=\; \{f : R \longrightarrow \mathbb{C} \mid f \text{ bi-invariant and } \sum_{r \in R} f(r) = 0\}.$$

- **Remark:** $\mathbb{S}$ has an identity different from that of $\mathbb{C}[R]$.

Preparations

- The identity of $\mathbb{S}$ is given by

$$e_{\mathbb{S}} := \frac{1}{|R^{\times}|}\delta_{R^{\times}} - \delta_0.$$

- Here, we adopt the notation

$$\delta_X(t) := \begin{cases} 1 & : \quad t \in X, \\ 0 & : \quad \text{otherwise}, \end{cases}$$

for the indicator function of a set or element.

- As module scalar multiplication we then use

$$f * w\,(x) := \sum_{r \in R} f(r)\, w(xr), \text{ for all } x \in R.$$

Results

- **Nota Bene:** '$*$' is not the same as '$\star$' that denotes multiplication in $\mathbb{S}$.
- To be precise, for all $f, g \in \mathbb{S}$ and $w \in \mathbb{W}$, we have the following:

$$(f \star g) * w \;=\; f * (g * w).$$

- This latter equality secures the action of $\mathbb{S}$ on $\mathbb{W}$ in the desired way!
- **Main Theorem I:** The rational weight $w \in \mathbb{W}$ allows for the extension theorem if and only if w is a free element of ${}_{\mathbb{S}}\mathbb{W}$, meaning that $f * w = 0$ implies $f = 0$ for all $f \in \mathbb{S}$.

Results

- **Examples:** Both the Hamming and the homogenous weight are examples for this result.
- **Main Theorem II:** A weight $w \in \mathbb{W}$ is free if and only if there holds
$$\sum_{Rt \leq Rx} \mu(0, Rt)\, w(t) \neq 0,$$
for all $Rx \leq R$.
- Here μ denotes the Möbius function on the partially ordered set of left principal ideals of the ring R.

Examples

(a) Every rational weight w on $\mathbb{Z}/4\,\mathbb{Z}$ allows for isometry extension if and only if $w(2) \neq 0$.

(b) Every rational weight w on $\mathbb{Z}/6\,\mathbb{Z}$ admits the extension theorem if and only if

$$w(2) \neq 0 \neq w(3) \text{ and } w(1) \neq w(2) + w(3).$$

(c) Let R be the ring of all 2×2-matrices over $\mathbb{F}_2$. Assume w is a rational weight on R with

$$w(X) = \begin{cases} a & : \quad \mathrm{rk}(X) = 1, \\ b & : \quad \mathrm{rk}(X) = 2, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

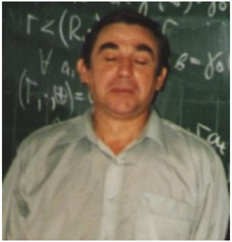
Then the extension theorem holds iff $a \neq 0$ and $b \neq \frac{3}{2}\,a$.

Conclusions: what to take home?

1. In pursuing ring-linear coding theory, variations on the distance measures must be considered.
2. A chosen distance is more useful if it allows for foundational theorems of the theory to hold.
3. This talk has characterized all such distances in terms of a set of simple inequalities to be satisfied.
4. Its methods are largely linear-algebraic and require a firm knowledge of the combinatorics of partially ordered sets.
5. Of course, a sound preparation in (non-commutative) ring and module theory will help understanding more details.

Acknowledgement

- This result would not have been achieved without the co-authors O. Gnilke, Th. Honold, J. Wood, and J. Zumbrägel.



Alexandr Nechaev died in November 2014 after a series of strokes. His constant encouragement and belief in the topic of this work was a highly motivating factor when deriving these results.

Talk and paper will be dedicated to his memory.