Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

Codes over finite rings

Marcus Greferath

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

May 2023

Equivalence of linear codes

Two definitions

Definition 1: Two codes $C, D \leq {}_R R^n$ are called equivalent, if there is a monomial transformation $\varphi : {}_R R^n \longrightarrow {}_R R^n$ such that $\varphi(C) = D$.

Recall: A monomial transformation φ on ${}_R R^n$ can be written as $\varphi = PD$ where $P \in M_n(R)$ is a permutation matrix, and $D \in M_n(R)$ is an invertible diagonal matrix.

Definition 2: Call two R-linear codes C and D isometric, if there is an isomorphism $\varphi : C \longrightarrow D$ that preserves the distance of codewords.

Equivalence of linear codes

A general justification

MacWilliams' 1962: Every isometry between two linear codes over $\mathbb{F}_q$ can be extended to a monomial transformation of the ambient space.

Honold et al 1995: If $R = \mathbb{Z}_m$ then every homogeneous isometry (and every Hamming isometry) between R-linear codes can be monomially extended.

Wood 1997: If R is a finite Frobenius ring then every Hamming isometry between two R-linear codes can be monomially extended.

Further Results and Projects

G. and Schmidt 2000: Honold et al's results are true for all finite Frobenius rings. Moreover, a linear mapping between two R-linear codes is a homogeneous isometry if and only if it is a Hamming isometry.

Wood 2000: Characterisation of weight functions on a commutative chain ring that allow for MacWilliams' extension theorem.

G., Honold, Wood, and Zumbrägel 2015: Characterisation of all weight functions on a finite Frobenius ring that allow for MacWilliams' equivalence theorem.

Code duality

Basic definitions

Definition: Let R be a finite Frobenius ring, and let $C \leq {}_R R^n$ be a linear code.

- The dual of C is defined as

$$C^{\perp} := \left\{ x \in R^n \mid \sum_{i=1}^{n} c_i x_i = 0 \ \text{ for all } \ c \in C \right\}.$$

- The (Hamming) weight enumerator of C is the polynomial

$$W_C(x, y) = \sum_{c \in C} x^{w_H(c)} y^{n - w_H(c)}.$$

Code duality

A classical result

Question: Relation between weight enumerators of mutually dual codes?

Theorem: (MacWilliams' 1962) If $C \leq \mathbb{F}_q^n$ is a linear code then

$$W_{C^\perp}(x, y) \;=\; \frac{1}{|C|} W_C\Big(x + (q-1)y, x - y\Big).$$

Question: What can be said about this theorem in the framework of ring-linear coding?

Code duality

Generalisations

Wood 1997: If R is a finite Frobenius ring and C an R-linear code of length n, then

$$W_{C^\perp}(x,y) \; = \; \frac{1}{|C|} W_C\Big(x + (|R|-1)y, x - y\Big).$$

Wood 1997: An according result holds for the complete weight enumerators, and certain symmetrised weight enumerators.

Byrne, G., and O'Sullivan 2007: A general MacWilliams relation for compatible pairs of partitions on the base ring R.

Existence bounds

A Plotkin bound

Premises:

- Let R be a finite Frobenius ring, and let w be the homogeneous weight of average value γ on R.
- Agree on $A_w(n,d)$ denoting the maximal possible code cardinality under length n and distance d.

G. and O'Sullivan 2004: For every n, d with $\gamma\, n < d$ there holds

$$A_w(n,d) \;\leq\; \frac{d}{d-\gamma\, n}.$$

Existence bounds

An Elias bound

Premise: Additionally, denote by $V_w(n,t)$ the volume of the homogeneous disk of radius t in n-space.

G. and O'Sullivan 2004: For every n, d, t with $t \leq \gamma\, n$ and $t^2 - 2\, t\gamma\, n + d\gamma\, n > 0$ there holds

$$A_w(n,d) \;\leq\; \frac{\gamma\, n\, d}{t^2 - 2\, t\gamma\, n + d\gamma\, n} \cdot \frac{|R|^n}{V_w(n,t)}.$$

Remark: The first result is the Plotkin bound, the second is the Elias bound. Both results can also be combined to derive an asymptotic version of the Elias bound.

Existence bounds

Further bounds

Byrne, G., and O'Sullivan: Several versions of the LP-bound allowing for symmetrisation with respect to

- homogeneous weights,
- subgroups of the group $R^\times$ of invertible elements,
- further important weights, like the Lee-weight.

Remark:

- It is comparably trivial to formulate a sphere-packing and a Gilbert-Varshamov bound (regardless of the underlying weight).
- For a Singleton bound and further refinements see **Byrne, G., Kohnert, and Skachek 2010**.

A final remark

Is the Frobenius property necessary?

Question: The Frobenius property is sufficient. Is it necessary?

Results:

- Wood 1997: For commutative rings this can be shown easily.
- Wood 2008: This also holds in the non-commutative case.
- G., Nechaev, and Wisbauer 2004: Exchanging the alphabet R by the R-module $\hat{R}$ all foundational statements hold for **any** finite ring R.