Generalized Hamming weights for almost affine codes*

Trygve Johnsen† Hugues Verdure‡

January 30, 2018

Abstract

We define generalized Hamming weights for almost affine codes. We show that this definition is natural since we can extend some well known properties of the generalized Hamming weights for linear codes, to almost affine codes. In addition we discuss duality of almost affine codes, and of the smaller class of multilinear codes. Keywords: Block codes, Hamming weight, Kung's bound, profiles, wire-tap channel of type II.

1 Introduction

Let C be an almost affine code as defined in [14], that is: $C \subset F^n$ for some finite alphabet F, and the projection C_X has cardinality $|F|^s$ for a non-negative integer s for each $X \subset \{1, \cdots, n\}$.

It is well known ([14]) that C defines a matroid M_C through the rank function

$$r(X) = \log_{|F|} |C_X|.$$

Such codes were studied in connection with access structures over $E = \{1, 2, \cdots, n\}$ and are strongly related to ideal perfect secret sharing schemes for such access structures. See e.g. [14], [5], [1], [10]. Recently, almost affine codes have been used in network coding. See e.g. [17]

An important subclass of almost affine codes are linear codes over finite fields $\mathbb{F}_q$. A bigger class consists of affine codes, which are translates of linear codes within their ambient space. Another class of codes strictly contained in the class of all almost affine codes, consists of multilinear codes (see Section 3.2 for the definition of multilinear codes).

In this paper we will study some well-known properties of linear codes over finite fields, and investigate to what extend they carry over to this bigger class of almost affine codes C.

We start by defining the Hamming weights of almost affine codes and show that the different characterizations of Hamming weights for linear codes apply to almost affine codes.

We carry on by investigating the possibility of defining in a natural way a dual code $C^\perp$ of an almost affine code C. This turns out to be problematic in general, although the dual matroid of M_C exists, so that we know what matroid structure $C^\perp$ should have induced, if it had existed. For multilinear codes, however, there is a nice duality of codes, which matches that of the dual matroids.

We proceed to prove a version of Kung's theorem for almost affine codes, that is a formula for how many codewords it takes for their unions of supports to cover all of $E = \{1, 2, \cdots, n\}$. For linear codes this formula in formulated in terms of the minimum distance of the dual code. In our case there is not necessarily a dual code, but we succeed in formulating a similar result, by using the associated matroid of the code. We also extend a recent generalization of Kung's theorem, given

*The original publication is available at http://ieeexplore.ieee.org/document/7820189/

†Dept. of Mathematics, UiT The Arctic University of Norway, N-9037 Tromsø, Norway, Trygve.Johnsen@uit.no

‡Dept. of Mathematics, UiT The Arctic University of Norway, N-9037 Tromsø, Norway, Hugues.Verdure@uit.no

in [6], from linear codes to almost affine codes. Here we give formulas for how many codewords it takes for their unions of supports to cover subsets of $E = \{1, 2, \cdots, n\}$ of specified cardinalities. To formulate this result we use the full set of Hamming weights for the matroid M_C.

At the end of the the paper, we look at two notions from linear codes that transpose nicely to almost affine codes, and that emphasize that our definition of Hamming weights is the right one. Namely, we look at dimension/length profiles of an almost affine code and its application to trellis decoding, and at the wire-tap channel of type II. In both cases, the Hamming weights of the code give an indication on how complex decoding will be, and how much information an intruder can get.

Our exposition contains several examples of almost affine codes that are not necessarily linear. Apart from a simple running example introduced in Example 1 below, we look at codes arising from a simple interleaving scheme (Section 3.2) and folded Reed-Solomon codes (Section 6). The way almost affine codes arise in a natural way from ideal perfect secret sharing schemes is also explained, in Section 1.1.2

1.1 Notation and known results

1.1.1 Matroids

A matroid is a combinatorial structure that extend the notion of dependency. There are many equivalent definitions for matroids, but we give just one here. We refer to [12] for a complete overview of the theory of matroids, and we use the notation from [12].

Definition 1 *A matroid M is a pair (E, ρ) where E is a finite set and $\rho : 2^E \to \mathbb{N}$ is a function satisfying*

(R1) $\rho(\emptyset) = 0$,

(R2) *If $X \subset E$ and $x \in E$, then*

$$\rho(X) \leqslant \rho(X \cup \{x\}) \leqslant \rho(X) + 1.$$

(R3) *If $X \subset E$, $x, y \in E$ and*

$$\rho(X) = \rho(X \cup \{x\}) = \rho(X \cup \{y\})$$

then

$$\rho(X \cup \{x, y\}) = \rho(X).$$

A basis of the matroid is a subset $X \subset E$ such that $|X| = \rho(X) = \rho(E)$, while a circuit is a minimum subset of $X \subset E$ (for inclusion) satisfying $\rho(X) = |X| - 1$. The nullity function is the function

$$n(X) = |X| - \rho(X).$$

The rank of the matroid is $\rho(E)$.

Remark 1 *If C is a $[n, k]$ linear code over a finite field $\mathbb{F}_q$, we can associate to it a matroid $M(C)$ in the following way: let H be a parity check matrix of the code. Then $E = \{1, \cdots, n\}$ and the rank function is given by*

$$\rho(X) = rk_{\mathbb{F}_q} H_X$$

for $X \subset E$, where H_X is the submatrix of H obtained by keeping the columns indexed by X. It can be proved that this matroid does not depend on the parity check matrix.

Every matroid M admits a dual matroid M^* on the same ground set and with rank function

$$\rho^*(X) = |X| + \rho(EX) - \rho(E).$$

Of course, $(M^*)^* = M$.

A notion that will be used later is the fundamental circuit of an element with respect to a basis [12, Corollary 1.2.6]:

Definition 2 *If B is a basis and $e \in EB$, then there exists a unique circuit X such that $X \subset B \cup \{e\}$. This circuit will be denoted $\sigma(B, e)$ in the sequel.*

In [16, Theorem 2], Wei generalizes the notion of minimum distance of linear codes (the generalized Hamming weights), and this can be further extended to matroids in general ([7]):

Definition 3 *Let M be a matroid of rank k on the ground set E, and let n be its nullity function. Then the generalized Hamming weights are*

$$d_i(M) = \min\{|X|, n(X) = i\} \text{ for } 1 \leqslant i \leqslant |E| - k.$$

Notice that the generalized Hamming weights for a matroid are a strictly increasing function of i.

In the same way, we can define the generalized Hamming weights for the dual matroid M^*. These are related by Wei duality, first proved in [16, Theorem 3] for linear codes, and then generalized in [9] (in Norwegian) and also in [2, Theorem 5], where one may disregard the partial ordering P appearing in that theorem since we now are considering the case where P is trivial (antichain):

Proposition 1 *The $d_i(M)$ and the $d_i(M^*)$ satisfy Wei duality:*

$$\{d_1(M), \cdots, d_{n-k}(M)\} \cup$$

$$\{n + 1 - d_k(M^*), \cdots, n + 1 - d_1(M^*)\} = \{1, 2, \cdots, n\}$$

where $n = |E|$.

1.1.2 Almost affine codes

We refer to [14] for an introduction to almost affine codes, and will mainly use their notation. We give here the main definitions, and the result that will be used in the sequel.

Definition 4 *An almost affine code on a finite alphabet F, of length n and dimension k is a subset $C \subset F^n$ such that $|C| = |F|^k$ and such that for every subset $X \subset \{1, \cdots, n\}$,*

$$\log_{|F|} |C_X| \in \mathbb{N},$$

where C_X is the puncturing of C with respect to $\{1, \cdots, n\}X$.

The code C is non-degenerate when it is of effective length n, that is, when $\forall x \in \{1, \cdots, n\}$, $\log_{|F|} |C_{\{x\}}| > 0$.

An almost affine subcode of C is a subset $D \subset C$ which is itself an almost affine code on the same alphabet.

To any almost affine code C of length n and dimension k on the alphabet F, we can associate a matroid M_C on the ground set $E = \{1, \cdots, n\}$ and with rank function

$$r(X) = \log_{|F|} |C_X|,$$

for $X \subset E$.

It is easily checked that this is the rank function of a matroid. The first axiom is trivial. The second axiom comes from the fact that a new coordinate position either leaves the number of codewords unchanged, or increases it by a factor $|F|$. The third axiom comes from the fact that if the number of codewords do not increase when we add new coordinate positions x or y, then it does not increase when we add both.

Remark 2 *Obviously, any linear code C over the field $\mathbb{F}_q$ is an almost affine code on the alphabet $\mathbb{F}_q$. We have two matroids associated to this code, namely $M(C)$ and M_C. Unfortunately, they are different, but they remain related, since they are dual of each other. We have namely*

$$M_C = M(C)^* = M(C^\perp)$$

where $C^\perp$ is the dual linear code of C, that is the orthogonal complement of C.

Example 1 *We will use a running example throughout this paper. It is the almost affine code C' in [14, Example 5]. It is a code of length 3 and dimension 2 on the alphabet $F = \{0, 1, 2, 3\}$. Its set of codewords is*

000	011	022	033
101	112	123	130
202	213	220	231
303	310	321	332

Its matroid is the uniform matroid $U_{2,3}$ of rank 2 on 3 elements. Namely, $r(\{1, 2, 3\}) = \log_4 16 = 2$ while for any $X \subsetneq \{1, 2, 3\}$, it is is easy to see that $C'_X = F^{|X|}$ so that $r(X) = |X|$. This is an example of an almost affine code which is not equivalent to a linear code, and not even to a multilinear code.

When talking about the support of a codeword in a linear code, one implicitly makes reference to the zero-codeword. Such a "canonical" codeword does not generally exist in almost affine codes, so we are bound to specify the codeword we compare to in almost all our definitions.

Definition 5 *Let C be a block code of length n, and let $\tilde{\boldsymbol{c}} \in C$ be fixed. The $\tilde{\boldsymbol{c}}$-support of any codeword $\boldsymbol{c}$ is*

$$Supp(\boldsymbol{c}, \tilde{\boldsymbol{c}}) = \{i, \boldsymbol{c}_i \neq \tilde{\boldsymbol{c}}_i\}.$$

Even if this is defined using a fixed codeword $\tilde{\boldsymbol{c}}$, it is shown in [14], that many quantities defined for almost affine codes do not depend on the codeword $\tilde{\boldsymbol{c}}$ used, but just on the matroid associated to the code. We mention, among other definitions and results taken from [14]:

Definition 6 *Let C be an almost affine code of length n, and let $\tilde{\boldsymbol{c}} \in F^n$ be fixed. Then*

$$C(X, \tilde{\boldsymbol{c}}) = \{\boldsymbol{c} \in C,\ \boldsymbol{c}_X = \tilde{\boldsymbol{c}}_X\},$$

where $\boldsymbol{c}_X$ is the projection of $\boldsymbol{c}$ to X.

Proposition 2 *Let C be an almost affine code of length n and dimension k on the alphabet F. Let $\tilde{\boldsymbol{c}} \in C$. Let $X \subset \{1, \cdots, n\}$. Then $C(X, \tilde{\boldsymbol{c}})$ is an almost affine subcode of C, and moreover,*

$$|C(X, \tilde{\boldsymbol{c}})| = |F|^{k - r(X)}$$

where r is the rank function of the matroid M_C.

Corollary 1 *If B is a basis of M_C, then given any tuple $\boldsymbol{w} \in F^B$, there exists a unique word $\boldsymbol{w}' \in C$ such that $\boldsymbol{w}'|_B = \boldsymbol{w}$.*

Proof Such a word exists since by definition of a basis, $C_B = F^B$, and it is unique by the previous proposition, since $r(B) = k$.

In the sequel, some proofs can be made clearer if one uses a equivalent code instead. Two block codes C and C' of length n on alphabets F and F' respectively are equivalent if there exists a permutation $\sigma \in S_n$ and bijections $\tau_i : F \to F'$ for $1 \leqslant i \leqslant n$ such that C' is the result of applying τ_i to the symbols in position i for all words in C, for $1 \leqslant i \leqslant n$, followed by permuting the n digits of each word according to σ.

It is obvious that a code equivalent to an almost affine code is almost affine too. It will be obvious in the sequel that it will be enough to prove the properties we want to prove for an equivalent almost affine code. Then we can assume that the alphabet is $F = \{0, \cdots, q-1\}$, that $\{1, \cdots, k\}$ is a basis of the matroid associated to the code, and that the word $(0, \cdots, 0) \in C$.

1.2 The relation with access structures and ideal perfect sharing schemes

The interest in almost affine codes has arisen in a natural way in connection with secret sharing schemes and their associated access structures. The connection with these structures is thoroughly explained for example in [14], and we briefly recollect some central elements, to motivate our study of almost affine codes. We essentially follow the exposition in [14].

Let $E_1 = \{2, 3, \cdots, n\}$ be a set of $n-1$ participants, for an integer $n \geq 2$.

Definition 7

- *An access structure over E_1 is a set Γ of subsets of E_1, such that $A \in \Gamma$ and $A \subset B$ implies $B \in \Gamma$.*
- *For an access structure Γ we let Γ_0 denote the set of minimal elements of Γ.*
- *The access structure Γ is said to be connected if the union of the sets in Γ_0 is all of E_1.*

Let F be a finite set of secrets, and denote by q its cardinality. A perfect secret sharing scheme for the access structure Γ is a method of distributing shares to the participants in such a way that all groups of participants in Γ can retrieve the secret, but no other group has any a posteriori information about the secret. A perfect secret sharing scheme is said to be ideal if the share set for each participant is equal to the set of secrets F. In mathematical terms:

Definition 8 *Set $E = \{1, 2, \cdots, n\}$, and denote by $\overline{A}$ the set $A \cup \{1\}$, for any $A \subset E_1$. An ideal perfect secret sharing scheme for the access structure Γ is a subset $\mathcal{C} \subset F^E (= F^n))$ such that:*

- *$C_{\{i\}} = F$, for $i = 1, \cdots, n$.*
- *$|\mathcal{C}_{\overline{A}}| = |\mathcal{C}_A|$, for all $A \in \Gamma$.*
- *$|\mathcal{C}_{\overline{A}}| = q|\mathcal{C}_A|$, for all A not contained in Γ.*

It is then clear that if you start with a non-degenerate almost affine code $\mathcal{C} \subset F^n$, then $\mathcal{C}$ is a ideal secret sharing scheme for the access structure $\Gamma_{\mathcal{C}}$ defined by

$(\Gamma_{\mathcal{C}})_0 = \{A \subset E_1 | \overline{A}$ is a circuit in $M_{\mathcal{C}}\}$

Definition 9 *A matroid with ground set E is connected if every subset of E of cardinality 2 is contained in a circuit.*

It is then clear that the access structure $\Gamma_{\mathcal{C}}$ is connected if and only if the matroid $M_{\mathcal{C}}$ is connected.

We also have ([1]):

Proposition 3 *An ideal perfect secret sharing scheme for a connected access structure is an almost affine code.*

For more on this subject we refer to [14], [5], [1], [10].

2 Generalized Hamming weights

2.1 Definition via the associated matroid

For a block code C, let $d(\boldsymbol{x}, \boldsymbol{y})$ be the Hamming distance between the codewords $\boldsymbol{x}$ and $\boldsymbol{y}$, that is $d(\boldsymbol{x}, \boldsymbol{y}) = |Supp(\boldsymbol{x}, \boldsymbol{y})|$. The minimal distance d is defined as

$$d = \min\{d(\boldsymbol{x}, \boldsymbol{y}),\ \boldsymbol{x}, \boldsymbol{y} \in C,\ \boldsymbol{x} \neq \boldsymbol{y}\}.$$

Then from [14, Prop. 5], the minimal distance of an almost affine code C is equal to the minimum cardinality of the circuits of the dual of the matroid associated to C, in other words,

$$d = d_1(M_C^*).$$

This suggests the following definition of generalized Hamming weights for an almost affine code:

Definition 10 *The generalized Hamming weights for an almost affine code C of dimension k are*

$$d_i(C) = d_i(M_C^*) = \min\{|X|,\ |X| - r^*(X) = i\}$$

for $1 \leqslant i \leqslant k$, where r^* is the rank function of M_C^*.

Example 2 *Let C' be the almost affine code of Example 1. The dual of $M_{C'} = U_{2,3}$ is $M_{C'}^* = U_{1,3}$, the uniform matroid of rank 1 on 3 elements. Its generalized Hamming weights are*

$$\begin{aligned} d_1(C') &= d_1(M_{C'}^*) = 2 \\ d_2(C') &= d_2(M_{C'}^*) = 3. \end{aligned}$$

Proposition 4 *Let C be an almost affine code of length n and dimension k on the alphabet F. Let $\tilde{\boldsymbol{c}} \in C$ be any codeword. Then for every $1 \leqslant i \leqslant k$,*

$$\begin{aligned} d_i(C) &= \min\{|X|,\ r(EX) = k - i\} \\ &= n - \max\{|X|,\ r(X) = k - i\} \\ &= n - \max\{|X|,\ |C(X, \tilde{\boldsymbol{c}})| = |F|^i\}. \end{aligned}$$

The third equality is independent of the choice of $\tilde{\boldsymbol{c}}$.

Proof The first equality follows simply from the fact that

$$r^*(X) = |X| + r(EX) + k$$

while the third equality is derived from Proposition 2.

2.2 Generalized Hamming weights and subcodes

For linear codes, the generalized Hamming weights are originally defined as minimal supports of linear subcodes of a given dimension ([16]). While for linear codes of dimension k over the finite field $\mathbb{F}_q$, the number of linear subcodes of dimension $1 \leqslant i \leqslant k$ is known, namely $\begin{bmatrix} k \\ i \end{bmatrix}_q$, this is not the case for almost affine codes. Even two almost affine codes having the same associated matroid do not necessarily have the same number of almost affine subcodes. Nevertheless, we can express the generalized Hamming weights for an almost affine code in terms of supports of almost affine subcodes.

Definition 11 *Let C be an almost affine code, and let $\tilde{\boldsymbol{c}} \in C$. The $\tilde{\boldsymbol{c}}$-support of C is*

$$Supp(C, \tilde{\boldsymbol{c}}) = \bigcup_{\boldsymbol{w} \in C} Supp(\boldsymbol{w}, \tilde{\boldsymbol{c}}).$$

Lemma 1 *Let C be an almost affine code, and $\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{d}} \in C$. Then we have*

$$Supp(C, \tilde{\boldsymbol{c}}) = Supp(C, \tilde{\boldsymbol{d}}).$$

Proof Namely, let $i \in \bigcup_{\boldsymbol{w} \in C} Supp(\boldsymbol{w}, \tilde{\boldsymbol{c}})$. Then there exists $\boldsymbol{w} \in C$ such that $\boldsymbol{w}_i \neq \tilde{\boldsymbol{c}}_i$. If $\boldsymbol{w}_i \neq \tilde{\boldsymbol{d}}_i$, then of course $i \in \bigcup_{\boldsymbol{w} \in C} Supp(\boldsymbol{w}, \tilde{\boldsymbol{d}})$. Otherwise $\tilde{\boldsymbol{c}}_i \neq \boldsymbol{w}_i = \tilde{\boldsymbol{d}}_i$ and again, $i \in \bigcup_{\boldsymbol{w} \in C} Supp(\boldsymbol{w}, \tilde{\boldsymbol{d}})$. By symmetry, we get equality.

The support of any almost affine subcode is thus well defined, as long as we take the $\tilde{\boldsymbol{c}}$-support of any codeword $\tilde{\boldsymbol{c}}$ in the subcode, and we may omit the reference to this codeword. For linear codes, we have an obvious candidate that is in any subcode, namely the $\mathbf{0}$-codeword. For almost affine codes, we may have to use different codewords for different subcodes. Indeed, in the almost affine code C' of Example 1, the following almost affine subcodes of dimension 1 are disjoint:

$$\{0,0,0\}, \{1,0,1\}, \{2,0,2\}, \{3,0,3\}$$

and

$$\{1,1,2\}, \{2,1,3\}, \{0,1,1\}, \{3,1,0\}.$$

In that case, their supports are $(1,3)$ for both.

Theorem 1 *Let C be an almost affine code of length n and dimension k on an alphabet F of cardinality q. Then the generalized Hamming weights for C are*

$$d_i(C) = \min \left\{ \begin{array}{c} |Supp(D)|,\ D \text{ is an almost affine} \\ \text{subcode of dimension } i \text{ of } C \end{array} \right\}$$

for $1 \leqslant i \leqslant k$.

Remark 3 *Almost affine subcodes of dimension i always exist by Proposition 2, since we can always find in the matroid M_C a set X with $r(X) = k - i$.*

Proof of Theorem 1 For $1 \leqslant i \leqslant k$, let

$$d_i = d_i(C)$$

and

$$e_i = \min \left\{ \begin{array}{c} |Supp(D)|,\ D \text{ is an almost affine subcode} \\ \text{of dimension } i \text{ of } C \end{array} \right\}.$$

We show first that $d_i \leqslant e_i$. Let D be an almost affine subcode of C of dimension i such that $|Supp(D)| = e_i$. By definition of the dimension, $|D| = q^i$. Let $\tilde{\boldsymbol{d}} \in D \subset C$, and let $X = Supp(D, \tilde{\boldsymbol{d}})$. We look at $D' = C(EX, \tilde{\boldsymbol{d}})$. By Proposition 2, we know that this is an almost affine subcode of dimension $l = k - r(EX)$. It is obvious that $D \subset D'$, and in particular

$$i \leqslant l = k - r(EX).$$

By the monotone property of generalized Hamming weights for matroids, we have that

$$d_i \leqslant d_l = \min\{|Y|, k - r(EY) = l\} \leqslant |X| = e_i.$$

We show now that $e_i \leqslant d_i$. Let $X \subset E$ be such that $|X| = d_i$ and $r(EX) = k - i$. Consider $D'' = C(EX, \tilde{\boldsymbol{c}})$ where $\tilde{\boldsymbol{c}}$ is any codeword of C. By Proposition 2, the dimension of D'' is i. Of course $\tilde{\boldsymbol{c}} \in D''$, and by construction $Supp(D'', \tilde{\boldsymbol{c}}) \subset X$. Then

$$\begin{aligned} d_i = |X| &\geqslant |Supp(D'', \tilde{\boldsymbol{c}})| \\ &\geqslant \min\{|Supp(D), \dim\ D = i\} = e_i. \end{aligned}$$

Example 3 *Let C' be the almost affine code of Example 1. This code has* 12 *almost affine subcodes of dimension* 1*, and it can be shown that all of them have support of cardinality* 2*. One of these subcodes is* $\{022, 332, 202, 112\}$ *which has support* $\{1, 2\}$*.*

2.3 Generalized Hamming weights and codewords

In [7], it is shown that the nullity function (and a posteriori the generalized Hamming weights) can be expressed as the support of non-redundant circuits.

Definition 12 *Let $\{X_1, \cdots, X_s\}$ be a set of distinct subsets of a given set. We say that this is a non-redundant set of subsets if the union of the s subsets is not equal to any union of $s-1$ of the subsets.*

By abuse of notation we then also just say that $X_1, \cdots, X_s$ are non-redundant subsets.
From [7] we have:

Proposition 5 *Let M be a matroid and X a subset of the ground set. Then the nullity of X is equal to the number of elements in a maximal non-redundant subset of circuits included in X.*

For linear codes, circuits of the matroid associated to (any) parity check matrix are in one to one correspondence with supports of minimal codewords. In [14, Proposition 5], it is proved that an analogous result holds for almost affine codes, namely that if C is an almost affine code and $\tilde{\boldsymbol{c}} \in C$, then the $\tilde{\boldsymbol{c}}$-supports of the $\tilde{\boldsymbol{c}}$-minimal codewords are the circuits of the dual matroid associated to the code. They are of course independent of the codeword $\tilde{\boldsymbol{c}}$. This gives rise to the following:

Definition 13 *Let $\tilde{\boldsymbol{c}}$ be a codeword in an almost affine code C. A set $\{\boldsymbol{c_1}, \cdots, \boldsymbol{c_i}\} \subset C$ is called a $\tilde{\boldsymbol{c}}$-non-redundant set of codewords if $\{Supp(\boldsymbol{c_1}, \tilde{\boldsymbol{c}}), \cdots, Supp(\boldsymbol{c_i}, \tilde{\boldsymbol{c}})\}$ is a non-redundant set of subsets. It is called a $\tilde{\boldsymbol{c}}$-minimal non-redundant set of codewords if in addition the $\boldsymbol{c_j}$ are $\tilde{\boldsymbol{c}}$-minimal for all j.*

By abuse of notation we also just say that $\boldsymbol{c_1}, \cdots, \boldsymbol{c_i}$ are $\tilde{\boldsymbol{c}}$-non-redundant codewords (respectively $\tilde{\boldsymbol{c}}$-minimal non-redundant codewords), and we may omit the reference to $\tilde{\boldsymbol{c}}$ when there is no risk of confusion.

Proposition 5 gives rise to the following characterization of the generalized Hamming weights for a matroid.

Proposition 6 *Let M be a matroid of rank k on the ground set E. Then the i-th generalized Hamming weight, for $1 \leqslant i \leqslant |E| - k$ is given by*

$$d_i(M) = \min \left\{ |\bigcup_{j=1}^{i} X_j|, \quad \begin{array}{c} X_1, \cdots, X_i \\ \textit{are non-redundant circuits} \end{array} \right\}.$$

Proof Let

$$d_i = \min\{|X|,\ n(X) = i\}$$

and

$$e_i = \min\{|\bigcup_{j=1}^{i} X_j|,\ X_1, \cdots, X_i \text{ are non-redundant circuits}\}$$

Let $X_1 \cdots, X_i$ non-redundant circuits such that $|\bigcup X_j| = e_i$, and let $Y = \bigcup X_j$. Then by Proposition 5, $j = n(Y) \geqslant i$. By the monotony of the generalized Hamming weights for a matroid,

$$d_i \leqslant d_j \leqslant |Y| = e_i$$

and one inequality is proved. For the second inequality, let $Y \subset E$ such that $|Y| = d_i$ and $n(Y) = i$. Then by Proposition 5 again, there exists i non-redundant circuits $Y_1, \cdots, Y_i$ such that $\bigcup Y_j \subset Y$. Then

$$e_i \leqslant |\bigcup Y_j| \leqslant |Y| = d_i$$

and this proves the proposition.

Then we have the following characterization of the generalized Hamming weights for an almost affine code (and thus linear code):

Proposition 7 *Let C be an almost affine code of dimension k. Then the generalized Hamming weights for C are given by*

$$d_i(C) = \min \left\{ \begin{array}{c} |\bigcup_{j=1}^{i} Supp(\boldsymbol{c_j}, \tilde{\boldsymbol{c}})|,\ (\boldsymbol{c_1}, \cdots, \boldsymbol{c_i}) \textit{ are} \\ \tilde{\boldsymbol{c}} - \textit{minimal non-redundant codewords} \end{array} \right\}$$

For a linear code, we have that a linear subcode of dimension i and minimal support gives i codewords with non-redundant supports that define d_i, and the converse. And actually, that any i non-redundant codewords defines a linear subcode of dimension i. This is not the case for almost affine codes. There is for example no almost affine subcodes of dimension 1 in the code C' of Example 1 containing the origin (in this case 000) and the word 112.

Lemma 2 *Let $D \subset C$ be an almost affine subcode of dimension i and such that $|Supp(D)| = d_i(C)$. Let $\tilde{\boldsymbol{c}} \in D$. Then we can find $\boldsymbol{c_1}, \cdots, \boldsymbol{c_i} \in D$, $\tilde{\boldsymbol{c}}$ non-redundant and such that*

$$|\bigcup_{j=1}^{i} Supp(\boldsymbol{c_j}, \tilde{\boldsymbol{c}})| = |Supp(D)| = d_i(C).$$

Proof Without loss of generality, we may assume that $F = \{0, \cdots, |F| - 1\}$ and that $\tilde{\boldsymbol{c}}$ is the 0 word. Let X be a basis of M_D. In particular, by Corollary 1, there exists for each $x \in X$ a (unique) word $\boldsymbol{c_x} \in D$ such that $(\boldsymbol{c_x})_{X\{x\}} = (0, \cdots, 0)$ and $(\boldsymbol{c_x})_x = 1$. Let $\boldsymbol{d_x} \in D$ be a word such that $Supp(\boldsymbol{d_x}, \tilde{\boldsymbol{c}})$ is minimal and contained in $Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}})$. We claim that $x \in Supp(\boldsymbol{d_x}, \tilde{\boldsymbol{c}})$. Namely, if not, then

$$Supp(\boldsymbol{d}_x, \tilde{\boldsymbol{c}}) \subset Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}}) \subset E(X\{x\})$$

together with $x \notin Supp(\boldsymbol{d_x}, \tilde{\boldsymbol{c}})$ would imply that $(\boldsymbol{d_x})_X = (0, \cdots, 0)$, that is, $\boldsymbol{d_x} = \tilde{\boldsymbol{c}}$ by Corollary 1 again, which is absurd. Thus, these codewords $\boldsymbol{d_x}$ are $\tilde{\boldsymbol{c}}$-minimal non-redundant. Then by Proposition 7, we have that

$$|\bigcup_{x\in X} Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}})| \geqslant |\bigcup_{x\in X} Supp(\boldsymbol{d_x}, \tilde{\boldsymbol{c}})| \geqslant d_i(C).$$

By construction, since all the $\boldsymbol{c_x} \in D$,

$$\bigcup_{x\in X} Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}}) \subset Supp(D)$$

so that

$$d_i(C) \leqslant |\bigcup_{x\in X} Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}})| \leqslant |Supp(D)| = d_i(C)$$

and there must be equality everywhere.

And the converse:

Lemma 3 *Let C be an almost affine code and $\tilde{\boldsymbol{c}} \in C$. Assume that $\boldsymbol{c_1}, \cdots, \boldsymbol{c_i}$ are $\tilde{\boldsymbol{c}}$-minimal non-redundant and such that $|\bigcup Supp(\boldsymbol{c_j}, \tilde{\boldsymbol{c}})| = d_i(C)$. Then there exists an almost affine subcode D of C containing $\tilde{\boldsymbol{c}}, \boldsymbol{c_1}, \cdots, \boldsymbol{c_i}$, of dimension i, and $|Supp(D)| = d_i(C)$.*

Proof Let $X = \bigcup_{j=1}^{i} Supp(\boldsymbol{c_j}, \tilde{\boldsymbol{c}})$. We have that

$$|X| = d_i(C) < d_l(C) = \min\{|Y|,\ n^*(Y) = l\}$$

for every $i < l$, so that $n^*(X) \leqslant i$. The inequality $n^*(X) \geqslant i$ is a direct consequence of [14, Proposition 5] and Proposition 5. This shows that $n^*(X) = i$, i.e $i = k - r(EX)$. This also means that the subcode $D = C(EX, \tilde{\boldsymbol{c}})$ is an almost affine subcode of dimension i by Proposition 2. By construction, $\boldsymbol{c_i} \in D$ for all i, and of course $\tilde{\boldsymbol{c}} \in D$. Moreover, generally, $Supp(C(EX, \tilde{\boldsymbol{c}})) \subset X$, so that $|Supp(D)| \leqslant |X| = d_i(C)$. By Theorem 1, there has to be equality.

3 Duality and Wei duality

For linear codes, we can easily define a dual code, namely the orthogonal complement of the code. The generalized Hamming weights for the code and its dual are related by Wei duality ([16, Theorem 3]). This was generalized to matroids (coming from linear codes or not), as presented in Proposition 1. So, if C is an almost affine code, we could define the dual generalized Hamming weights as the generalized Hamming weights for the dual of the associated matroid, and we would get a Wei duality by Proposition 1, coming essentially from matroid theory. It would be nice if these weights would come from a dual almost affine code. Unfortunately, we will see that such duals do not exist in general. But for a large class of almost affine codes, we can nevertheless define a dual code.

3.1 The dual of an almost affine code does not exist in general

It is natural to ask the following about dual almost affine codes:

- The matroid associated to the dual code should be the dual of the matroid associated to the code.

- Two equivalent codes should have equivalent duals.
- The dual of the dual should be the code we started with.

In addition, the dual of a linear code and of a linear code seen as an almost affine code should coincide.

Remark 4 *In the case of linear codes, we replace the condition on equivalent codes by a stronger condition, namely linear equivalence. It is unknown to the authors if two linear codes can be equivalent in the wider sense without being linearly equivalent.*

Lemma 4 *Let C_1, C_2 be two equivalent almost affine codes on the alphabet F. Then for every $1 \leqslant r \leqslant \dim(C_1) = \dim(C_2)$, the number of r-dimensional almost affine subcodes of C_1 and C_2 are the same.*

Proof This is obvious by the definition of equivalency.

Lemma 5 *Let C_1, C_2 be two almost affine codes of dimension 1 on the alphabet F with the same matroid. Then they are equivalent.*

Proof Let $B = \{b\}$ be a basis of the matroid. Let $x \in EB$. We have two possibilities:

- $\sigma(B, x) = \{x\}$. Let $\boldsymbol{w_i} \in C_i$ for $i \in \{1, 2\}$. By Proposition 2,

  $$|C_i(\{x\}, \boldsymbol{w_i})| = |F|^{1-r(\{x\})} = |F| = |C_i|$$

  so that all words of C_i have the same digit, namely $(\boldsymbol{w_i})_x$ at position x. Let τ_x be any permutation of F that sends $(\boldsymbol{w_1})_x$ to $(\boldsymbol{w_2})_x$.
- $\sigma(B, x) = \{b, x\}$. For every $i \in \{1, 2\}$ and $f \in F$, let $\boldsymbol{w_{i,f}} \in C_i$ be the unique word such that $(\boldsymbol{w_{i,f}})_{\{b\}} = f$. Since $\{x\}$ is a basis of $M_{C_1} = M_{C_2}$, by Corollary 1,

  $$\begin{array}{rccc} \tau_x : & F & \longrightarrow & F \\ & (\boldsymbol{w_{1,f}})_x & \longmapsto & (\boldsymbol{w_{2,f}})_x \end{array}$$

  is a permutation.

The series of permutations τ_x of the symbols of the alphabet at position x makes C_1 equivalent to C_2.

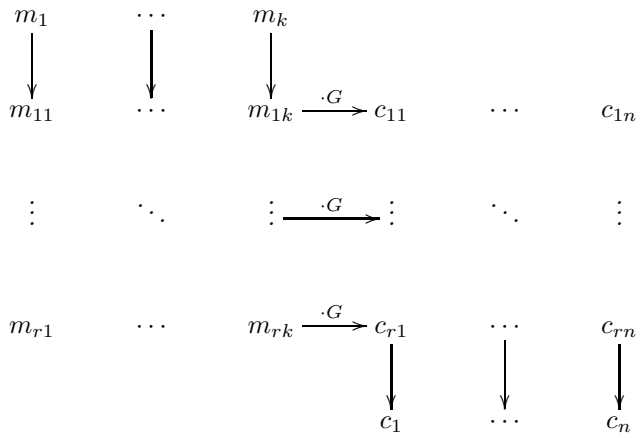
We can now show that the concept of dual of an almost affine code does not exist. Namely, the codes $\mathcal{C}$ and $\mathcal{C}'$ from [14, Example 5], have the same associated matroid. The dual matroid is the uniform matroid $U_{1,3}$. Therefore, the possible duals $\mathcal{C}^\perp$ and $\mathcal{C}'^\perp$ would be equivalent by Lemma 5. Thus $\mathcal{C} = \mathcal{C}^{\perp\perp}$ and $\mathcal{C}' = \mathcal{C}'^{\perp\perp}$ would also be equivalent. But this is not possible by Lemma 4 since it is known that $\mathcal{C}$ has 20 1-dimensional almost affine subcodes, while $\mathcal{C}'$ has just 12 of them.

3.2 Duality of multilinear codes

In this subsection, we will study an important class of almost affine codes, namely multilinear codes.

Definition 14 *Let q be a prime power and $r, n \geqslant 1$. Let F be the $\mathbb{F}_q$-vector space $\mathbb{F}_q^r$. A multilinear code C is a $\mathbb{F}_q$-linear subspace of F^n such that $\forall X \subset \{1, \cdots, n\}$, $\dim_{\mathbb{F}_q} C_X$ is divisible by r.*

Example 4 *Let C be a $[n,k]$ linear code on the field $\mathbb{F}_q$ with generator matrix $G = \left[g_{i,j}\right]$. Let F be the $\mathbb{F}_q$-vector space $\mathbb{F}_q^r$ for some r. Consider the following interleaving encoding scheme:*



where $m_i \in F$ is decomposed into $m_{1,i}, \cdots, m_{r,i} \in \mathbb{F}_q$. Then every row $[m_{j,1}, \cdots, m_{j,k}]$ is encoded via G to a row $[c_{j,1}, \cdots, c_{j,n}]$. Now all the columns $c_{l,1} \cdots, c_{l,r}$ forms an element of F. This code C' is the row space of the $kr \times rn$ block matrix

$$G' = \left[D_{g_{ij}}^{(r)}\right]$$

on $\mathbb{F}_q$, where $D_l^{(r)}$ is the $r \times r$ diagonal matrix with l on the diagonal. This is therefore a multilinear code.

It is shown in [14] that a multilinear code C is an almost affine code on the alphabet $F = \mathbb{F}_q^m$. The rank function of the associated matroid is given by

$$\rho(X) = \frac{1}{r} \dim_{\mathbb{F}_q} C_X, \ X \subset \{1, \cdots, n\}.$$

By the canonical isomorphism $F^n \approx \mathbb{F}_q^{nr}$, we may think of C as the row space of a $kr \times rn$ matrix G over $\mathbb{F}_q$. The code C can also be seen as a linear code of length rn and rank kr over $\mathbb{F}_q$, and thus as an almost affine code over the alphabet $\mathbb{F}_q$. We denote by ρ_1 and ρ_r the rank functions of the almost affine codes C over F and $\mathbb{F}_q$ respectively. For $1 \leqslant x \leqslant n$, we also denote by x_r the set

$$x_r = \{(x-1)r + 1, \cdots, (x-1)r + r\}$$

and if $X \subset \{1, \cdots, n\}$,

$$X_r = \bigcup_{x \in X} x_r.$$

The rank functions ρ_1 and ρ_r are given by

$$\rho_1(Y) = \mathrm{rk}_{\mathbb{F}_q} G_Y$$

for $Y \subset \{1, \cdots, rn\}$. Also, for $X \subset \{1, \cdots, n\}$,

$$\rho_r(X) = \frac{1}{r} \mathrm{rk}_{\mathbb{F}_q} G_{X_r} = \frac{1}{r} \rho_1(X_r).$$

The goal of this section is to show that a multilinear code C in a natural way has a dual multilinear code. Interpreted as a linear code over $\mathbb{F}_q$, C has a dual linear code $C^\perp$, namely the

orthogonal complement of C in $\mathbb{F}_q^{nr}$. Let H be a generator matrix of $C^\perp$. This is a $(rn-kr)\times rn$ matrix over $\mathbb{F}_q$. Then, for $Y\subset\{1,\cdots,rn\}$,

$$\mathrm{rk}_{\mathbb{F}_q} H_Y = |Y| + \mathrm{rk}_{\mathbb{F}_q} G_{\{1,\cdots,rn\}Y} - kr.$$

In particular, for every $X\subset\{1,\cdots,n\}$,

$$\begin{aligned}\mathrm{rk}_{\mathbb{F}_q} H_{X_r} &= |X_r| + \mathrm{rk}_{\mathbb{F}_q} G_{\{1,\cdots,rn\}X_r} - kr\\ &= r|X| + \mathrm{rk}_{\mathbb{F}_q} G_{(\{1,\cdots,n\}X)_r} - kr\\ &= r|X| + r\rho_m(C_{\{1,\cdots,n\}X}) - kr\end{aligned}$$

is divisible by r, and makes therefore $C^\perp$ a multilinear code.

Remark 5 *As almost affine codes over the alphabet $\mathbb{F}_q^r$, the codes C and $C^\perp$ have dual matroids. As a consequence, Wei duality holds for C and $C^\perp$*

4 Generalized Kung's bound

In [8, Lemma 4.24], Kung gives a bound for the minimum number of codewords of a linear code that are sufficient to cover the whole space. This bound is related to the Singleton defect of the dual linear code. In [6], this was generalized to find a bound for the number of codewords that are necessary to cover a subspace of the whole space. Both results rely heavily on linear algebra. In this section, we prove a similar result for almost affine codes.

We begin by defining the generalized critical exponents.

Definition 15 *Let C be a non-degenerate almost affine code of length n. Let $\tilde{\boldsymbol{c}}\in C$ and $1\leqslant i\leqslant n$. Then the i-th critical exponent with respect to $\tilde{\boldsymbol{c}}$ is*

$$\gamma_i(\tilde{\boldsymbol{c}}) = \min\{j,\ \exists \boldsymbol{c_1},\cdots,\boldsymbol{c_j}\in C,\ |\bigcup_{l=1}^{j} Supp(\boldsymbol{c_l},\tilde{\boldsymbol{c}})|\geqslant i\}.$$

Remark 6 *If the dimension of C is k, then it is obvious that*

$$\gamma_i(\tilde{\boldsymbol{c}}) = 1\ \forall 1\leqslant i\leqslant k$$

since there exists at least a word of support k. Take namely a basis B of M_C, then $C_B = F^{|B|}$ and we can find a word whose $\tilde{\boldsymbol{c}}$-support contains B.

In [14], one can find the following result:

Proposition 8 *The number of codewords in C with given $\tilde{\boldsymbol{c}}$-support X is equal to*

$$\sum_{Y\subseteq X}(-1)^{|XY|}q^{k-r(EY)}$$

Proof This is [14, Proposition 6].

Corollary 2 *The generalized critical exponents are independent of the chosen word $\tilde{\boldsymbol{c}}$.*

Proof Let $\tilde{\boldsymbol{d}} \in C$ be another word. Let $j = \gamma_i(\tilde{\boldsymbol{c}})$ and $\boldsymbol{c_1}, \cdots \boldsymbol{c_j}$ be such that

$$\left| \bigcup_{1 \leqslant l \leqslant j} Supp(\boldsymbol{c_l}, \tilde{\boldsymbol{c}}) \right| \geqslant i.$$

Let $X_i = Supp(\boldsymbol{c_i}, \tilde{\boldsymbol{c}})$. By definition, there exists at least one word, namely $\boldsymbol{c_i}$ whose $\tilde{\boldsymbol{c}}$-support is X_i. So, by the previous proposition,

$$\begin{aligned} &\left| \{ \boldsymbol{w} \in C,\ Supp(\boldsymbol{w}, \tilde{\boldsymbol{d}}) = X_i \} \right| \\ &= \sum_{Y \subseteq X_i} (-1)^{|X_i Y|} q^{k - r(EY)} \\ &= |\{ \boldsymbol{w} \in C,\ Supp(\boldsymbol{w}, \tilde{\boldsymbol{c}}) = X_i \}| \\ &\geqslant 1 \end{aligned}$$

Thus there exists a word $\boldsymbol{d_i} \in C$ such that $Supp(\boldsymbol{d_i}, \tilde{\boldsymbol{d}}) = X_i$. Then

$$\left| \bigcup_{1 \leqslant l \leqslant j} Supp(\boldsymbol{d_l}, \tilde{\boldsymbol{d}}) \right| = \left| \bigcup_{1 \leqslant l \leqslant j} Supp(\boldsymbol{c_l}, \tilde{\boldsymbol{c}}) \right| \geqslant i,$$

and this shows that

$$\gamma_i(\tilde{\boldsymbol{d}}) \leqslant \gamma_i(\tilde{\boldsymbol{c}})$$

and equality comes by symmetry.

In the sequel, we will therefore omit the reference to a particular word in the critical exponents. Before stating and proving the main result of this section, we need a lemma on matroid theory.

Lemma 6 *Let M be a matroid on the ground set E. Let B a basis and $x \in EB$. Then for every $y \in B$, we have: $B' = B\{y\} \cup \{x\}$ is a basis of M if and only if $y \in \sigma(B, x)\{x\}$*

Proof Assume that B' is not a basis. Then $\rho(B') \neq |B'|$, and by a repeated use of axiom $(R2)$, $\rho(B') < |B'|$. By the same axiom again, since $\rho(B) = |B|$, we get successively $\rho(B\{y\}) = |B| - 1$ and $\rho(B') = \rho(B\{y\}) = |B| - 1 = |B'| - 1$. This shows that B' contains a circuit, say τ. Of course, this circuit contains x, otherwise it is contained in B, and a repeated use of axiom $(R2)$ again would show that any subset of B has rank equal to its cardinality. Thus, τ is a circuit contained in $B \cup \{x\}$, and by Lemma 2, $\tau = \sigma(B, x)$. Since $y \notin \tau$, one way is shown.
Assume now that $y \notin \sigma(B, x)$. Then

$$\sigma(B, x) \subset B' = B\{y\} \cup \{x\}.$$

Since $\rho(\sigma(B, x)) = |\sigma(B, x)| - 1$, by a repeated use of axiom $(R2)$ again,

$$\begin{aligned} \rho(B') &= \rho(\sigma(B, x) \cup (B'\sigma(B, x)) \\ &\leqslant \rho(\sigma(B, x)) + |B'\sigma(B, x)| \\ &\leqslant |\sigma(B, x)| - 1 + |B'\sigma(B, x)| \\ &\leqslant |B'| - 1 \end{aligned}$$

and B' is not a basis.

Theorem 2 *Let C be a non-degenerate almost affine code of dimension k and length n on the alphabet F. Let $k+1 \leqslant i \leqslant n$. Then we have*

$$\gamma_i \leqslant s^*_{n+1-i} + 2$$

where s^*_j denotes the j-th generalized Singleton defect of M_C,

$$s^*_j = k + j - d^*_j.$$

Remark 7 *We recall that the generalized Hamming weights d_i of the almost affine code C are defined as the generalized Hamming weights for the dual M^*_C of M_C. From Wei duality, we get the dual generalized Hamming weights d^*_i of the code C - and these do not in general correspond to the Hamming weights for an almost affine code, since we have not been able to define dual codes of almost affine codes in general. If we think of matroids, these latter weights correspond to generalized Hamming weights for the matroid M_C, that is*

$$d^*_j = \min\{|X|,\ n(X) = j\}.$$

In the special case that C is a linear code over $\mathbb{F}_q$, then these d^*_i are the usual Hamming weights for the orthogonal complement $C^\perp$, and we obtain (a new proof of) [6, Theorem 9].

Proof of Theorem 2 Let $q = |F|$. Without loss of generality, we may assume that the alphabet is $F = \{0, \cdots, q-1\}$, that $\tilde{\boldsymbol{c}} = (0, \cdots, 0)$, and that $B = \{1, \cdots, k\}$ is a basis of M_C. By Corollary 1, there exists for each $1 \leqslant j \leqslant k$ a unique word $\boldsymbol{w^{(j)}} \in C$ such that $\boldsymbol{w}^{(\boldsymbol{j})}_l = 0$ for $l \in \{1, \cdots, k\}\{j\}$ and $\boldsymbol{w}^{(\boldsymbol{j})}_j = 1$. Now, let $S \subset \{k+1, \cdots, n\}$ be of cardinality $n+1-i$, and set

$$T_S = \{l \in \{1, \cdots, k\},\ \exists j \in S,\ \boldsymbol{w}^{(\boldsymbol{l})}_j \neq 0\}.$$

We claim that

$$|T_S| \geqslant d_{n+1-i} - (n+1-i).$$

Indeed, let $j \in S$ and $l \in \sigma(B, y)\{y\}$. This latter is non-empty since the code is non-degenerate and thus the matroid M_C has no loops. By Lemma 6, $B_l = B\{j\} \cup \{l\}$ is still a basis of M_C. By Proposition 2, the almost affine subcode $C(B_l, \tilde{\boldsymbol{c}})$ is such that

$$|C(B_l, \tilde{\boldsymbol{c}})| = q^{k - r(B_l)} = 1$$

Since $\tilde{\boldsymbol{c}} \in C(B_l, \tilde{\boldsymbol{c}})$, this means that $\boldsymbol{w^{(l)}} \notin C(B_l, \tilde{\boldsymbol{c}})$, and in particular $\boldsymbol{w}^{(\boldsymbol{l})}_j \neq 0$. This shows that

$$\bigcup_{j \in S} (\sigma(B, j)\{j\}) \subset T_S$$

and therefore

$$|T_S| \geqslant \left| \bigcup_{j \in S} (C(B, j)\{j\}) \right| = \left| \bigcup_{j \in S} \sigma(B, j) \right| - |S|.$$

Now, the circuits $\sigma(B, j)$ are non-redundant, so from Proposition 5, we know that

$$n \left(\bigcup_{j \in S} \sigma(B, j) \right) \geqslant |S| = n + 1 - i.$$

This in turn implies that

$$\left|\bigcup_{j\in S}\sigma(B,j)\right| \geqslant d^*_{n(\bigcup_{j\in S}\sigma(B,j))} \geqslant d^*_{n+1-i},$$

the first inequality coming from the definition

$$d^*_l = \min\{|X|,\ n^*(X) = l\}$$

and the second inequality from the monotony property of generalized Hamming weights.
Now, if we take $t = k+n+2-i-d^*_{n+1-i}$ distinct words among $(\boldsymbol{w^{(1)}}, \cdots, \boldsymbol{w^{(k)}})$, say $\boldsymbol{w^{(l_1)}}, \cdots, \boldsymbol{w^{(l_t)}}$, then we claim that

$$\left|\bigcup_{1\leqslant s\leqslant t} Supp(\boldsymbol{w^{(l_s)}}, \tilde{\boldsymbol{c}}) \cap \{k+1, \cdots, n\}\right| \geqslant i-k.$$

If not, then there would exist at least $n+1-i$ distinct indices j in $\{k+1, \cdots, n\}$ such that

$$\forall 1 \leqslant s \leqslant t,\ \boldsymbol{w}_j^{(\boldsymbol{l_s})} = 0.$$

Take S to be $n+1-i$ such indices. Then for this particular S, we would have

$$|T_S| \leqslant k - t < d^*_{n+1-i} - (n+1-i)$$

which is absurd.
These t words, together with the word $\boldsymbol{w_0} \in C$ such that $(\boldsymbol{w_0})_B = (1, \cdots, 1)$ gives a $t+1$-tuple whose support has cardinality at least i, and this concludes the proof.

Remark 8 *These bounds are the best that can be found. Linear codes are namely almost affine codes, and in [6], it is mentioned that for simplex codes, the bounds are reached.*

Example 5 *Let C' be the code of Example 1. Let $\tilde{\boldsymbol{c}} = 321$. Then $\gamma_3(\tilde{\boldsymbol{c}}) = 1$ since $Supp(213, \tilde{\boldsymbol{c}}) = \{1,2,3\}$. We have seen that $d_1(C') = 2$ and $d_3(C') = 3$, so that by Wei duality, $d^*_1(C') = 3$. The bound of theorem 2 says that*

$$1 = \gamma_3(\tilde{\boldsymbol{c}}) \leqslant s^*_1(C') + 2 = 2.$$

5 Profiles of almost affine codes and trellis decoding

In [11], Muder describes trellis decoding for block codes. In [3], Forney defines various dimension/length profiles for linear codes. These profiles give a lower bound for the complexity of the minimal trellis associated to the code, and thus an indication on how well decoding using the Viterbi algorithm will work.

In this section, we observe how the Viterbi algorithm immediately works for almost affine codes, and we show how the dimension/length profile concept can be generalized to these codes as well and how they are related to the generalized Hamming weights. For self-containment and clarity, we include the trellis decoding algorithm.

5.1 Dimension/length profiles and generalized Hamming weights

Definition 16 *The dimension/length profile of an almost affine code C of dimension k and length n is the sequence $k_i(C)$ for $1 \leqslant i \leqslant n$ where*

$$k_i(C) = \max \left\{ \begin{array}{c} \dim D,\ D \subset C \text{ is an almost affine} \\ \text{code with } |Supp(D)| \leqslant i \end{array} \right\}.$$

In the definition above, we can actually restrict to subcodes of the type $C(X, \tilde{\boldsymbol{c}})$:

Proposition 9 *Let $\tilde{\boldsymbol{c}} \in C$. We have*

$$k_i(C) = \max \left\{ \log_q |C(X, \tilde{\boldsymbol{c}})|, |X| = n - i \right\}.$$

Proof It is clear that $Supp(C(X, \tilde{\boldsymbol{c}})) \subset EX$, so that $|Supp(C(X, \tilde{\boldsymbol{c}}))| \leqslant i$. This proves that

$$k_i(C) \geqslant \max \left\{ \log_q |C(X, \tilde{\boldsymbol{c}})|, |X| = n - i \right\}.$$

On the other hand, let $D \subset C$ be an almost affine subcode such that $|Supp(D)| \leqslant i$ and $\dim D = k_i(C)$. Let $X = Supp(D)$ and $X \subset Y \subset E$ be such that $|Y| = i$. Consider $D' = C(EY, \tilde{\boldsymbol{c}})$ for any $\tilde{\boldsymbol{c}} \in D$. Obviously $|Supp(D')| \leqslant i$ and $\dim D' \geqslant \dim D = k_i(C)$ proving the proposition.

Corollary 3 *We have*

$$\begin{aligned} k_i(C) &= \max \{k - r(X), |X| = n - i\} \\ &= k - \min \{r(X), |X| = n - i\}. \end{aligned}$$

The dimension/length profile is related to the generalized Hamming weights of the code in the following way:

Proposition 10 *We have*

$$d_j(C) = \min\{i,\ k_i(C) \geqslant j\}$$

and

$$k_i(C) = \max\{j,\ d_j(C) \leqslant i\}.$$

Proof We have

$$\begin{aligned} &\min\{i,\ k_i(C) \geqslant j\} \\ &= \min\{i,\ \max\{\log_q |C(X, \tilde{\boldsymbol{c}})|,\ |X| = n - i\} \geqslant j\} \\ &= n - \max\{i,\ \max\{\log_q |C(X, \tilde{\boldsymbol{c}})|,\ |X| = i\} \geqslant j\} \\ &= n - \max\{|X|,\ \log_q |C(X, \tilde{\boldsymbol{c}})| \geqslant i\} \\ &= n - \max\{|X|,\ \log_q |C(X, \tilde{\boldsymbol{c}})| = i\} \\ &= d_j(C), \end{aligned}$$

the penultimate equality coming from the fact that $\log_q |C(X, \tilde{\boldsymbol{c}})|$ decreases by at most 1 if X is augmented with 1 element.

Moreover we have:

$$\begin{aligned} &\max\{j,\ d_j(C) \leqslant i\} \\ &= \max\{j,\ (n - \max\{|X|,\ \log_q |C(X, \tilde{\boldsymbol{c}})| = j\}) \leqslant i\} \\ &= \max\{j,\ (\max\{|X|,\ \log_q |C(X, \tilde{\boldsymbol{c}})| = j\}) \geqslant n - i\} \\ &= \max\{\log_q |C(X, \tilde{\boldsymbol{c}})|,\ |X| \geqslant n - i\} \\ &= \max\{\log_q |C(X, \tilde{\boldsymbol{c}})|,\ |X| = n - i\} \\ &= k_i(C). \end{aligned}$$

5.2 Trellis decoding for almost affine codes

Definition 17 *A proper trellis is a labelled directed graph such that the vertices can be partitioned into subsets $V_0, \cdots, V_n$ such that the only possible directed edges are between an element in V_i and an element in V_{i+1}. Moreover, $|V_0| = |V_n| = 1$, and every vertex in V_i for $1 \leqslant i \leqslant n-1$ is connected to at least one vertex in V_{i-1} and one vertex in V_{i+1}. It is proper when no two edges from the same vertex have the same label. We say that it represents C if C is equal to the set of concatenations of the labels of the edges of paths from V_0 to V_n. It is minimal if it has fewer vertices at every stage than any other proper trellis representing C.*

Let C be an almost affine code of dimension k and length n on an alphabet of F cardinality q. We define a labelled directed graph $G = (V, T)$ in the following way. For $0 \leqslant i \leqslant n$, let $C_i = C_{\{1,\cdots,i\}}$. In particular, $C_0 = \{\emptyset\}$ and $C_n = C$. We define an equivalence relation $\sim$ on C_i by: for $\boldsymbol{v}, \boldsymbol{w} \in C_i$, let $\boldsymbol{v'}, \boldsymbol{w'} \in C$ be such that $\boldsymbol{v'}_{\{1,\cdots,i\}} = \boldsymbol{v}$ and $\boldsymbol{w'}_{\{1,\cdots,i\}} = \boldsymbol{w}$,

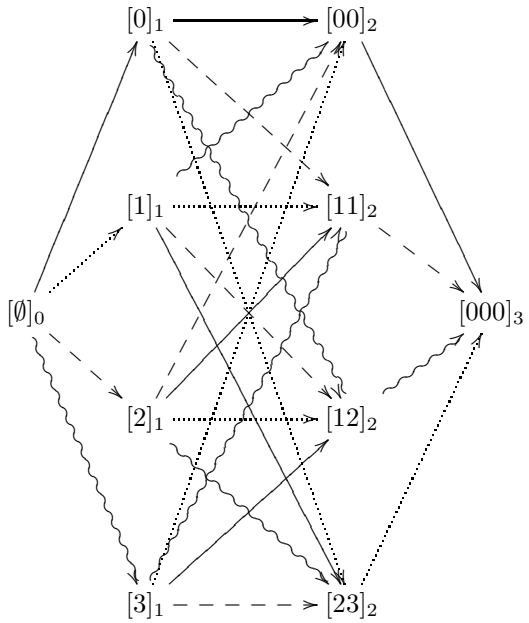
$$\boldsymbol{w} \sim \boldsymbol{v} \Leftrightarrow \begin{array}{c} C(\{1,\cdots,i\}, \boldsymbol{v'})_{\{i+1,\cdots,n\}} \\ || \\ C(\{1,\cdots,i\}, \boldsymbol{w'})_{\{i+1,\cdots,n\}} \end{array}.$$

It is independent of the choice of $\boldsymbol{v'}$ and $\boldsymbol{w'}$. In other words, $\boldsymbol{v}$ and $\boldsymbol{w}$ are equivalent if and only if every ending of a word in C starting with $\boldsymbol{v}$ is an ending of a word in C starting with $\boldsymbol{w}$, and conversely. We denote by $[\boldsymbol{v}]_i$ the equivalence class of $\boldsymbol{v}$. Let $V_i = C_i/\sim$, for $0 \leqslant i \leqslant n$. In particular, $V_0 = \{[\emptyset]_0\}$ and $V_n = \{[\boldsymbol{w}]_n\}$ for any $\boldsymbol{w} \in C$. The set of vertices of G is then defined by $V = \bigcup_{i=0}^{n} V_i$. The set of labelled edges is

$$T = \left\{ ([\boldsymbol{v}]_i, [\boldsymbol{w}]_{i+1}, \alpha), \begin{array}{c} \exists \boldsymbol{v'} \in [\boldsymbol{v}]_i,\ \exists \boldsymbol{w'} \in [\boldsymbol{w}]_{i+1}, \\ \boldsymbol{w'} = \boldsymbol{v'}|\alpha \end{array} \right\},$$

where $\boldsymbol{v'}|\alpha$ is the concatenation of $\boldsymbol{v'}$ and α, and α is the label on the edge. One can show that this graph is a minimal proper trellis representing C.

Example 6 *Let C be the code from Example 1. Then $V_0 = \{[\emptyset]_0\}$. $V_1 = C_1 = \{[0]_1, [1]_1, [2]_1, [3]_1\}$. Namely, the ending of the words beginning with 0 ($00, 11, 22, 33$) are different than the endings of the word starting with 1 ($01, 12, 23, 30$) and so on. It is different for V_2. Namely, all the words beginning with $00, 31, 22, 13$ have the same ending, namely 0, so they are in the same equivalence class. We get that $V_2 = \{[00]_2, [11]_2, [12]_2, [23]_2\}$. Finally, $V_3 = \{[000]_3\}$. For the edges, there is for example one edge going from $[\emptyset]_0$ to $[1]_1$, with label 1. There is also one edge going from $[1]_1$ to $[00]_2$ with label 3. Namely, $1 \in [1]_1$, $13 \in [00]_2$ and $13 = 1|3$. The minimum trellis representing C is the following, where the plain, dotted, dashed and wave arrows are labelled with 0, 1, 2 and 3 respectively:*



Any trellis representing C, and thus this minimal trellis, can be used for decoding, using the Viterbi algorithm ([15]). Given a word $\boldsymbol{c} \in F^n$, the algorithm finds the words in C such that their Hamming distance to $\boldsymbol{c}$ is minimal. The algorithm runs as follows:

$W \leftarrow \{\boldsymbol{\emptyset}\}$
for $1 \leqslant i \leqslant n$ **do**
  $W' \leftarrow \emptyset$
  for all $[\boldsymbol{v}]_i \in V_i$ **do**
    $H \leftarrow \{\boldsymbol{w}|\alpha, \boldsymbol{w} \in W, (End(\boldsymbol{w}), [\boldsymbol{v}]_i, \alpha) \in T\}$
    $H \leftarrow \{\boldsymbol{w} \in H,\ d(\boldsymbol{w}, \boldsymbol{c}_{\{1,\cdots,i\}})\ minimal\}$
    $W' \leftarrow W' \cup H$
  end for
  $W \leftarrow W'$
end for
return W

Here, if $\boldsymbol{w} \in C_i$, $End(\boldsymbol{w})$ is the unique edge corresponding to the path from $[\boldsymbol{\emptyset}]_0$ and label $\boldsymbol{w}$. In the previous example, $End(20) = [11]_2$.

We will not do an analysis of the Viterbi algorithm. The idea of why it works is that whenever one comes to a node $[\boldsymbol{v}]_i \in V_i$, one can keep the words ending there that have minimal Hamming distance with $\boldsymbol{c}_{\{1,\cdots,i\}}$. Namely, all the other words ending there will have a strictly larger Hamming distance in further stages, since the possible endings of all these words are all the same (by definition of the equivalence relation).

Example 7 *We continue with Example 6. Suppose that we receive the word* 320*. In the first loop, we keep all the words of length* 1 *(each vertex has just one incoming edge, and it must be kept). In the second loop, we look first at the vertex* $[00]_2$*. It has* 4 *incoming edges, that give the following words:* $00, 13, 22, 31$*, with Hamming distance* $2, 2, 1, 1$ *to* 32 *respectively. So we just keep the two last ones, namely* 22 *and* 31*. For the vertex* $[11]_2$ *we keep the words* $02, 33$*, for the vertex* $[12]_2$ *we keep the words* $12, 30$*, all of them having Hamming distance* 1 *to* 32*. For the vertex* $[23]_2$*, we keep*

only 32*, with Hamming distance* 0 *to* 32*. For the third loop, there are* 4 *incoming edges to* $[000]_3$*, and this leads to the following words to look at:* $220, 310, 022, 332, 123, 303, 321$*. We keep those with minimal Hamming distance to* 322*, namely:* $022, 332, 321$*.*

The complexity of the algorithm is related to the number of vertices at each stage, that is $|V_i|$. Here, we give a minimal bound for this number.

Proposition 11 *For every* $1 \leqslant i \leqslant n$*,*

$$\log_q |V_i| \geqslant k - k_i(C) - k_{n-i}(C).$$

Proof Let $\boldsymbol{v} \in C_i$ and $\boldsymbol{w} \in C$ such that $\boldsymbol{v} = \boldsymbol{w}_{\{1,\cdots,i\}}$. Let $\boldsymbol{t} = \boldsymbol{w}_{\{i+1\cdots,n\}}$. Let $\boldsymbol{c} \in C_i$. Then if $\boldsymbol{c} \in [\boldsymbol{v}]_i$, it implies that $\boldsymbol{c}|\boldsymbol{t} \in C$. In particular,

$$\boldsymbol{c}|\boldsymbol{t} \in C(\{i+1, \cdots, n\}, \boldsymbol{w})$$

In turn, this implies that

$$|[\boldsymbol{v}]_i| \leqslant |C(\{i+1, \cdots, n\}, \boldsymbol{w})| = q^{k-r(\{i+1,\cdots,n\})}.$$

Now, C_i is a disjoint union of these equivalence classes, and has cardinality $q^{r(\{1,\cdots,i\})}$ so that we get that

$$|V_i| \geqslant \frac{q^{r(\{1,\cdots,i\})}}{q^{k-r(\{i+1,\cdots,n\})}}.$$

Thus, by Corollary 3

$$\begin{aligned}
\log_q |V_i| &\geqslant r(\{1, \cdots, i\}) + r(\{i+1, \cdots, n\}) - k \\
&\geqslant \min\{r(X),\ |X| = i\} \\
&\quad + \min\{r(X),\ |X| = n - i\} - k \\
&\geqslant k - k_i(C) - k_{n-i}(C).
\end{aligned}$$

Remark 9 *It would have been beneficial to have upper bounds, and not only lower bounds, for the complexity of the trellis decoding algorithm. But as far as we know, no such non-trivial bounds are known, even for linear codes.*

6 Wire-tap channel of type II

In [13], Ozarow and Wyner introduce the wire-tap channel of type II. A sender wants to send k elements of information. In order to do so, the information is encoded into n elements, and sent to the receiver. An intruder is allowed to listen to any s elements of the sent message. The channel is noiseless, so the receiver can decode the message correctly. The authors look at how much information the intruder is able to get. In their paper, they present an encoder/decoder system using linear codes. In [16], Wei relates the equivocation (that is, a measure on the minimum of uncertainty for an intruder about the source) of the system to the generalized Hamming weights for the code (and its dual code).

In this section, we extend their results to almost affine codes. We show that we can use almost affine codes to design an encoder/decoder system, and we relate the equivocation of the system to the generalized Hamming weights for the dual of the matroid associated to the almost affine code.

So let C be an almost affine code on the alphabet F with $|F| = q$, of dimension k and length n. Without loss of generality, we may assume that the set $B = \{1, \cdots, k\}$ is a basis of the associated

matroid M_C. Let $\varphi : F^{n-k} \times F^{n-k} \to F^{n-k}$ be a mapping such that for all $\boldsymbol{f} \in F^{n-k}$, $\varphi(\boldsymbol{f}, .)$ is a bijection and such that

$$\forall X \subset \{1, \cdots, n-k\}, \forall \boldsymbol{m}, \boldsymbol{f}, \boldsymbol{g} \in F^{n-k},$$
$$\boldsymbol{g}|_X = \boldsymbol{h}|_X \Leftrightarrow \varphi(\boldsymbol{g}, \boldsymbol{m})|_X = \varphi(\boldsymbol{h}, \boldsymbol{m})|_X.$$

Remark 10 *All these conditions are true if $\varphi_0 : F \times F \longrightarrow F$ is a mapping such that $\varphi_0(x, .) : F \longrightarrow F$ is a bijection for every $x \in F$, and $\varphi : F^{n-k} \times F^{n-k} \longrightarrow F^{n-k}$ is defined by*

$$\varphi((a_1, \cdots, a_{n-k}), (b_1, \cdots, b_{n-k}))$$
$$= (\varphi_0(a_1, b_1), \cdots, \varphi_0(a_{n-k}, b_{n-k})).$$

Extend φ to $\tilde{\varphi} : F^n \times F^{n-k} \to F^n$ in the following way: for every $\boldsymbol{f} \in F^n$ and $\boldsymbol{g} \in F^{n-k}$,

$$\tilde{\varphi}(\boldsymbol{f}, \boldsymbol{g})_i = \begin{cases} \boldsymbol{f}_i & \text{if } 1 \leqslant i \leqslant k, \\ \varphi(\boldsymbol{f}|_{EB}, \boldsymbol{g})_{i-k} & \text{otherwise} \end{cases}$$

For every $\boldsymbol{m} \in F^{n-k}$, define

$$C_{\varphi, \boldsymbol{m}} = \{\tilde{\varphi}(\boldsymbol{w}, \boldsymbol{m}),\ \boldsymbol{w} \in C\}.$$

When φ is obvious from the context, we will omit it and write $C_{\boldsymbol{m}}$ for $C_{\varphi, \boldsymbol{m}}$.

Lemma 7 *The sets $\{C_{\boldsymbol{m}},\ \boldsymbol{m} \in F^{n-k}\}$ form a partition of F^n.*

Proof It is obvious that there is a bijection between $C_{\boldsymbol{m}}$ and C, since $\tilde{\varphi}(., \boldsymbol{m})$ is a bijection when restricted to C, since it leaves the coordinates on a basis unchanged. Now, suppose that $\boldsymbol{c} = (c_1, \cdots, c_n) \in C_{\boldsymbol{m}} \cap C_{\boldsymbol{m'}}$. In particular, we have that

$$(c_1, \cdots, c_k, c_{k+1}, \cdots, c_n) = \tilde{\varphi}(\boldsymbol{w}, \boldsymbol{m}) = \tilde{\varphi}(\boldsymbol{w'}, \boldsymbol{m'})$$

for some words $\boldsymbol{w}, \boldsymbol{w'} \in C$. Then $\boldsymbol{w}|B = \boldsymbol{w'}|B$, and by Proposition 2, $\boldsymbol{w} = \boldsymbol{w'}$. On the other hand, we have

$$\varphi(\boldsymbol{w}, \boldsymbol{m}) = \tilde{\varphi}(\boldsymbol{w}, \boldsymbol{m})|_{EB}$$
$$= \tilde{\varphi}(\boldsymbol{w'}, \boldsymbol{m'})|_{EB} = \tilde{\varphi}(\boldsymbol{w}, \boldsymbol{m'})|_{EB} = \varphi(\boldsymbol{w}, \boldsymbol{m'})$$

which implies that $\boldsymbol{m} = \boldsymbol{m'}$ since $\varphi(\boldsymbol{w}, .)$ is a bijection. We conclude by a cardinality argument.

Lemma 8 *The sets $C_{\boldsymbol{m}} \subset F^n$ are almost affine codes with associated matroid M_C.*

Proof Let $X \subset \{1, \cdots, n\}$ and $Y = X \cap B$, $Z = XY$. We will construct a bijection

$$\theta : C_X \longrightarrow (C_{\boldsymbol{m}})_X$$

in the following way: let $\boldsymbol{v} \in C_X$ and $\boldsymbol{w} \in C$ such that $\boldsymbol{w}|_X = \boldsymbol{v}$. Then let $\theta(\boldsymbol{v}) = \tilde{\varphi}(\boldsymbol{w}, \boldsymbol{m})|_X$. This is well defined since if $\boldsymbol{w}, \boldsymbol{w'} \in C$ are such that $\boldsymbol{w}|_X = \boldsymbol{w'}|_X$, then $\boldsymbol{w}|_Z = \boldsymbol{w'}|_Z$. This in turn implies that $\varphi(\boldsymbol{w}|_{EB}, \boldsymbol{m})|_Z = \varphi(\boldsymbol{w'}|_{EB}, \boldsymbol{m})|_Z$, and thus, combined with the fact that $\boldsymbol{w}|_Y = \boldsymbol{w'}|_Y$, $\tilde{\varphi}(\boldsymbol{w}, \boldsymbol{m})|_X = \tilde{\varphi}(\boldsymbol{w'}, \boldsymbol{m})|_X$.

This is injective because if $\boldsymbol{v_1}, \boldsymbol{v_2} \in C_X$ are such that $\boldsymbol{v_1} \neq \boldsymbol{v_2}$, let $\boldsymbol{w_1}, \boldsymbol{w_2} \in C$ be such that $\boldsymbol{w_1}|_X = \boldsymbol{v_1}$ and $\boldsymbol{w_2}|_X = \boldsymbol{v_2}$. Then at least one of the two cases is true:

- $\boldsymbol{w_1}|_Y \neq \boldsymbol{w_2}|_Y$ and then trivially $\tilde{\varphi}(\boldsymbol{w_1}, \boldsymbol{m})|_X \neq \tilde{\varphi}(\boldsymbol{w_2}, \boldsymbol{m})|_X$

- $\boldsymbol{w_1}|_Z \neq \boldsymbol{w_2}|_Z$. Then $\varphi(\boldsymbol{w_1}|_{EB}, \boldsymbol{m})|_Z \neq \varphi(\boldsymbol{w_2}|_{EB}, \boldsymbol{m})|_Z$, and in turn $\tilde{\varphi}(\boldsymbol{w_1}, \boldsymbol{m})|_X \neq \tilde{\varphi}(\boldsymbol{w_2}, \boldsymbol{m})|_X$.

Surjectivity is obvious by construction.

Then,

$$|(C_{\boldsymbol{m}})_X| = |C_X|$$

which proves the lemma.

Our scheme is then the following: the encoder wants to send the message $\boldsymbol{m} \in F^{n-k}$, and chooses randomly and uniformly any element $\boldsymbol{c} \in C_{\boldsymbol{m}}$, and sends it. The decoder gets $\boldsymbol{c} \in F^n$, finds the unique codeword $\boldsymbol{w} \in C$ such that $\boldsymbol{w}|_B = \boldsymbol{c}|_B$. Then $\boldsymbol{m} \in F^{n-k}$ is the unique element such that $\varphi(\boldsymbol{w}|_{EB}, \boldsymbol{m}) = \boldsymbol{c}|_{EB}$.

If the message $\boldsymbol{t} \in F^n$ is sent over the channel, and an intruder is able to listen to a subset $X \subset \{1, \cdots, n\}$ of the digits of $\boldsymbol{t}$, we will now see how much the intruder knows about $\boldsymbol{m}$, namely which $\boldsymbol{m}$ the sender could possibly have tried to send, and with which probability.

Example 8 *Let C' be the code of Example 1. Here the alphabet is $\{0, 1, 2, 3\}$, and we take $\varphi(a, b) = a + b \ (mod\ 4)$. We want to send the message $\boldsymbol{m} = 2$. We therefore construct $C'_{\boldsymbol{2}}$:*

002	013	020	031
103	110	121	132
200	211	222	233
301	312	323	330

We choose at random any element there, say 121 and send it to the receiver. The receiver sees that the only word in C' starting with 12 is 123, so that the message that was sent is $\boldsymbol{m}$ such that $\boldsymbol{m} + 3 = 1$, that is $\boldsymbol{m} = 2$.
An intruder able to listen to 1 digit, say the second, knows nothing about $\boldsymbol{m}$. Namely, there are exactly 4 elements in $C'_{\boldsymbol{2}}$ such that the second digit is 2, but the same is true also for $C' = C'_{\boldsymbol{0}}$, $C'_{\boldsymbol{1}}$ and $C'_{\boldsymbol{3}}$. The same is true if the intruder is able to listen to 2 digits, say the first and third. There is exactly 1 word in each of $C'_{\boldsymbol{0}}$, $C'_{\boldsymbol{1}}$, $C'_{\boldsymbol{2}}$ and $C'_{\boldsymbol{3}}$ looking like $(1 \cdot 1)$, namely 101, 131, 121 and 111 respectively.

Lemma 9 *Let $\boldsymbol{t} \in F^n$ be any word, and $X \subset \{1, \cdots, n\}$. Then we have the following*

- *Let $\boldsymbol{m} \in F^{n-k}$. Then the set*

$$\Lambda_{\boldsymbol{t},X}(\boldsymbol{m}) = \{\boldsymbol{w} \in C_{\boldsymbol{m}},\ \boldsymbol{w}_X = \boldsymbol{t}_X\}$$

  is either empty, or has cardinality $|F|^{k-r(X)}$.

- $$\left|\{\boldsymbol{m} \in F^{n-k},\ \Lambda_{\boldsymbol{t},X}(\boldsymbol{m}) \neq \emptyset\}\right| = |F|^{n-k-n(X)}.$$

Proof Let's assume that $\Lambda_{\boldsymbol{t},X}(\boldsymbol{m}) \neq \emptyset$, and let $\boldsymbol{s} \in \Lambda_{\boldsymbol{t},X}(\boldsymbol{m})$. In particular, $\boldsymbol{s} \in C_{\boldsymbol{m}}$, and we have

$$\begin{aligned}
|\Lambda_{\boldsymbol{t},X}(\boldsymbol{m})| &= |\{\boldsymbol{w} \in C_{\boldsymbol{m}},\ \boldsymbol{w}_X = \boldsymbol{t}_X\}| \\
&= |\{\boldsymbol{w} \in C_{\boldsymbol{m}},\ \boldsymbol{w}_X = \boldsymbol{s}_X\}| \\
&= |C_{\boldsymbol{m}}(X, \boldsymbol{s})| \\
&= |F|^{\mathrm{rk}(C_{\boldsymbol{m}}) - r_{C_{\boldsymbol{m}}}(X)} \\
&= |F|^{k-r(X)}.
\end{aligned}$$

For the second point of the proof, since

$$|\{\boldsymbol{w} \in F^n,\ \boldsymbol{w}|_X = \boldsymbol{t}|_X\}| = |F|^{n-|X|},$$

and all $C_{\boldsymbol{m}}$ are disjoint, each such $\boldsymbol{w}$ must be in a different set $\Lambda_{\boldsymbol{t},X}(\boldsymbol{m})$. We conclude using the first point.

In particular, if $|X| < d_1^* = \min\{|X|,\ n(X) = 1\}$, then an intruder that is able to listen to the subset X of digits of $\boldsymbol{t}$ gets no information whatsoever on the message $\boldsymbol{m}$. Namely, for every $\boldsymbol{m'} \in F^{n-k}$, there are exactly $|F|^{k-|X|}$ words in $C_{\boldsymbol{m'}}$ whose restriction to X is $\boldsymbol{t}_X$.

A way of measuring how much an intruder gains information is the conditional entropy of the system, namely

$$\begin{aligned} &H(F^{n-k}|T_X) \\ &= -\sum_{\boldsymbol{t}_X \in T_X} p(\boldsymbol{t}_X) \sum_{\boldsymbol{m} \in F^{n-k}} p(\boldsymbol{m}|\boldsymbol{t}_X) \log_{|F|} p(\boldsymbol{m}|\boldsymbol{t}_X), \end{aligned}$$

where T_X is the set of possible observations made by the eavesdropper at places $X \subset \{1, \cdots, n\}$. Now, we assume that all messages $\boldsymbol{m}$ have the same probability to be chosen, and then that the sent message $\boldsymbol{w} \in C_m$ the same probability to be chosen, so that $p(\boldsymbol{t}_X) = \frac{1}{|F|^X}$. From the previous lemma, we have that

$$p(\boldsymbol{m}|\boldsymbol{t}_X) = \begin{cases} 0 & \text{if } \Lambda_{\boldsymbol{t},X}(\boldsymbol{m}) = \emptyset \\ \frac{1}{|F|^{n-k-n(X)}} & \text{otherwise} \end{cases}.$$

This gives that

$$H(F^{n-k}|T_X) = n - k - n(X).$$

The system designer is interested in maximizing the equivocation

$$E_\mu = \min_{|X|=\mu} H(F^{n-k}|T_X)$$

for all possible $\mu \in \{0, \cdots, n\}$. This way, the designer is assured that no matter which μ digits an intruder is able to listen to, the uncertainty about the message $\boldsymbol{m}$ is at least E_μ. The maximum of information gained by an intruder with μ taps is therefore

$$\Delta_\mu = n - k - E_\mu = \max_{|X|=\mu} \{n(X)\}.$$

By the definition of the generalized Hamming weights for the dual of the matroid M_C associated to the code C,

$$d_i^* = \min\{|X|, n(X) = i\},$$

we get that

$$\max_{|X|=\mu} \{n(X)\} = j \Leftrightarrow d_j^* \leqslant \mu < d_{j+1}^*,$$

with the convention that $d_0^* = 0$ and $d_{n-k+1}^* = n + 1$. We get then the following characterization of the equivocation of the system:

Theorem 3 *The quantity Δ_μ of the system described above is entirely determined by the dual generalized Hamming weights for the almost affine code C, namely*

$$d_{\Delta_\mu}^* \leqslant \mu < d_{\Delta_\mu+1}^*$$

with the same convention as above.

Example 9 *We continue with Example 8. Since the matroid associated to C' is $U_{3,2}$, the nullity function is 0 everywhere, except that it is 1 at $\{1,2,3\}$. We therefore find that*

$$E_0 = E_1 = E_2 = 1 \Leftrightarrow \Delta_0 = \Delta_1 = \Delta_2 = 0$$

and

$$E_3 = 0 \Leftrightarrow \Delta_3 = 1.$$

We have seen that $d_1^*(C') = 3$, so that for $\mu < 3$, the Theorem gives $\Delta_\mu = 0$, while it gives $\Delta_3 = 1$.

Example 10 *Let q be a prime power, $k \leqslant q-1$ and let $r \geqslant 2$ be such that $r \mid q-1$ and $r \mid k$. Let $\gamma \in \mathbb{F}_q^*$ be a generator of $\mathbb{F}_q^*$. A generator matrix of the Reed-Solomon code $RS_{q,\gamma,k} \subset \mathbb{F}_q^{q-1}$ is given by*

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \gamma & \gamma^2 & \cdots & \gamma^{q-1} \\ \gamma^2 & \gamma^4 & \cdots & \gamma^{2(q-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{k-1} & \gamma^{2(k-1)} & \cdots & \gamma^{(k-1)(q-1)} \end{bmatrix}.$$

We consider the r-folded Reed-Solomon code $FRS_{q,\gamma,r,k}$ defined in the following way (see [4]): let ϕ be

$$\begin{array}{ccc} \mathbb{F}_q^{q-1} & \longrightarrow & \left(\mathbb{F}_q^r\right)^{\frac{q-1}{r}} \\ (x_1 \cdots, x_{q-1}) & \longmapsto & ((x_1, \cdots, x_r), (x_{r+1}, \cdots, x_{2r}), \cdots) \end{array}.$$

Then

$$FRS_{q,\gamma,r,k} = \phi(RS_{q,\gamma,k}).$$

This is a block code of length $\frac{q-1}{r}$ on the alphabet $\mathbb{F}_q^r$.

We use the notation of section 3.2. If $X \subset \{1, \cdots, \frac{q-1}{r}\}$, then the submatrix G_{X_r} is a Vandermonde matrix, and as such, we have

$$rk_{\mathbb{F}_q} G_{X_r} = \min\{|X_r|, k\},$$

which is obviously divisible by r. This shows that the r-folded Reed-Solomon code is a multilinear code over $\mathbb{F}_q^r$. Now,

$$rk_{\mathbb{F}_q} G_{X_r} = \min\{|X_r|, k\}$$

which implies

$$\left|FRS_{q,\gamma,r,k_X}\right| = q^{rk_{\mathbb{F}_q} G_{X_r}} = \begin{cases} (q^r)^{|X|} & \text{if } |X| \leqslant \frac{k}{r} \\ (q^r)^{\frac{k}{r}} & \text{if } |X| > k \end{cases}$$

This shows that the matroid associated to the r-folded Reed-Solomon code is the uniform matroid $U_{\frac{k}{r},\frac{q-1}{r}}$ on $\frac{q-1}{r}$ elements and rank $\frac{k}{r}$, and its generalized Hamming weights are

$$d_i(FRS_{q,\gamma,r,k}) = \frac{q-1-k}{r} + i$$

for $1 \leqslant i \leqslant \frac{k}{r}$ and

$$d_i(FRS_{q,\gamma,r,k})^* = \frac{k}{r} + i$$

for $1 \leqslant i \leqslant \frac{q-1-k}{r}$. It is therefore an MDS-code.

Let $\varphi : \left(\mathbb{F}_q^r\right)^{\frac{q-1-k}{r}} \times \left(\mathbb{F}_q^r\right)^{\frac{q-1-k}{r}} \to \left(\mathbb{F}_q^r\right)^{\frac{q-1-k}{r}}$ is an application as described above, for example componentwise addition. By the above description of the generalized Hamming weights, an intruder

does not get any digit of information if he is able to listen up to $\frac{k}{r} - 1$ *digits of the sent message, he gets* i *digits of information if he is able to listen to* $\frac{k}{r} + i - 1$ *digits of the sent message.*

If we want to keep the same robustness again intruders with a linear code on a field with the same alphabet size, we have to use an MDS-code over $\mathbb{F}_{q^r}$ *(for example a punctured Reed-Solomon code of dimension* $\frac{k}{r}$ *where we only keep* $\frac{q-1}{r}$ *columns of a generator matrix). It is easy to see that it gives the same robustness than the scheme presented above, since both are MDS. The benefit of using a folded Reed-Solomon code is that the computations are done over the smaller field* $\mathbb{F}_q$ *instead of* $\mathbb{F}_{q^r}$*.*

Acknowledgements

The authors would like to thank IMPA, Rio de Janeiro, where a part of the first named author's work with this article was done, during the special trimester April-June 2015.

The authors would also like to thank the anonymous referee for a series of comments that led to a significant improvement of the article.

References

[1] E.F. Brickell and D.M. Davenport, *On the classification of ideal secret sharing schemes*, Journal of Cryptology, vol. 4, pp. 123–134, 1991.

[2] T. Britz, T. Johnsen, D. Mayhew, and K. Shiromoto, *Wei-type duality theorems for matroids*, Designs, Codes and Crypography, vol. 62, No. 3, pp. 331–341, 2012.

[3] G.F. Forney, *Dimension/Length Profiles and Trellis Complexity of Linear Block Codes*, IEEE Transactions on Information Theory, vol. 40, No. 6, pp. 1741–1751, 1994.

[4] V. Guruswami and A. Rudra, *Explicit capacity-achieving list-decodable codes.* In STOC '06 Proceedings of the thirty-eighth annual ACM symposium on Theory of computing, pp. 1–10, 2006.

[5] W-A. Jackson, K.M. Martin, *Geometric Secret Sharing Schemes and their Duals*, Des. Codes Cryptogr., vol. 4, pp. 83–95, 1994.

[6] T. Johnsen, K. Shiromoto and H. Verdure, *A generalization of Kung's bound*, Designs, Codes Cryptogr., vol. 81, No. 1, pp. 169–178, 2016.

[7] T. Johnsen, H. Verdure, *Hamming weights of linear codes and Betti numbers of Stanley-Reisner rings associated to matroids*, AAECC, vol. 24, pp. 73–93, 2013.

[8] J.P.S. Kung, *Critical problems*, in: Matroid Theory, Seattle, WA, 1995, Contemporary Mathematics, vol. 197, American Mathematical Society, Providence, RI, pp. 1–127 (1996).

[9] A.H. Larsen, *Matroider og lineære koder*, Masters thesis, University of Bergen, 2005. Available at http://bora.uib.no/handle/1956/10780.

[10] F. Matus, *Matroid representations by partitions*, Discrete Mathematics, vol. 203, pp. 69–194, 1999.

[11] D.J. Muder, *Minimal trellises for block codes*, IEEE Transactions on Information Theory, vol. 34, No. 5, pp. 1049–1053, 1988.

[12] J.G. Oxley, *Matroid theory*, Oxford university press, 1992.

[13] L.H. Ozarow and A.D. Wyner, *Wire-tap-channel II*, Advances in Cryptology (Paris, 1984), pp. 33–50, Lecture Notes in Compu. Sci., 209, Springer, Berlin, 1985.

[14] J. Simonis and A. Ashikhmin, *Almost Affine Codes*, Des. Codes Crypogr., vol. 14, pp. 179–197, 1998.

[15] A.J. Viterbi, *Error bounds for convolutional codes and an asymptotically optimum decoding algorithm*, IEEE Trans. Inf. Th., vol.13, No. 2, pp. 260–269, 1967

[16] V.K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inf. Th., vol. 37, No. 5, pp. 1412–1418, 1991.

[17] T. Westerbäck, T. Ernvall and C. Hollanti, *Almost affine locally repairable codes and matroid theory*, in Proc. IEEE Inf. Theory Workshop (ITW), Nov. 2014, pp. 621–625.