Generalized Hamming weights for almost affine codes

Trygve Johnsen* Hugues Verdure†

January 8, 2016

Abstract

We define generalized Hamming weights for almost affine codes. We show how various aspects and applications of generalized Hamming weights for linear codes, such as Wei duality, generalized Kung's bound, profiles, connection to wire-tap channels of type II, apply to the larger class of almost affine codes in general. In addition we discuss duality of almost affine codes,and of the smaller class of multilinear codes. We also give results about weight distributions of infinite series of almost affine codes, each series obtained from a fixed code by extending the code alphabet. 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 [22], 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 ([22]) 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. [22], [7], [1], [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 bigger than that of linear codes, and strictly smaller than that of all almost affine codes, consists of multilinear codes. These are usual linear codes over a finite field $\mathbb{F}_q$, with an additional structure as (almost affine) codes over a finite dimensional vector space F over $\mathbb{F}_q$. An natural case is to consider $F = \mathbb{F}_q^m$ for some integer $m \geq 2$.

In this paper we will study some well-known properties of linear codes over finite fields, and investigate to what extent they carry over to this bigger class of almost affine codes C. In some cases we will limit ourselves to results about the intermediate class of multilinear codes.

The properties we will study are Hamming weights, (virtual) Wei duality, and the interplay with properties of the associated matroids M_C and its dual. Furthermore we will study series of extension codes over a given almost affine code, and how to count code words of specified weights.

We will also investigate 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.

*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

We proceed to prove a version of Kung's theorem for almost affine codes, that is a formula for how many code words 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 the result, by using the associated matroid of the code. We also extend a recent generalization of Kung's theorem, given in [11], from linear codes to almost affine codes. Here we give formulas for how many code words 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 paper we will discuss some concepts intimately connected to linear codes. These are dimension/length and length/dimension profiles, and the wire-tap channel of Type II. We show how all these concepts give meaning for almost affine codes in general, and a lot of results can easily be generalized to this larger class of codes.

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 [19] for a complete overview of the theory of matroids, and we use its notation.

Definition 1 *A matroid M on the finite ground set E is a collection $\mathcal{B}$ of subsets of E satisfying*

(B1) $\mathcal{B} \neq \emptyset$,

(B2) *For every distinct $B_1, B_2 \in \mathcal{B}$, for every $x \in B_1 - B_2$, there exists $y \in B_2 - B_1$ such that $B_1 - \{x\} \cup \{y\} \in \mathcal{B}$.*

The set $\mathcal{B}$ is known as the set of bases of the matroid M. All the bases of a matroid have the same cardinality.

We can associate a matroid to any linear code in the following way. Let H be a parity check matrix of the code. Let H_i, $1 \leqslant i \leqslant n$ be the columns of this matrix. Then

$$\mathcal{B} = \{X \subset E,\ (H_i)_{i \in X} \text{ is a maximal independent set}\}$$

is the set of bases of a matroid. It can be proved that this matroid doesn't depend on the parity check matrix of the code. We denote this matroid by $M(C)$.

Every matroid M admits a dual matroid M^* on the same ground set defined as follows: the set of bases of M^* is

$$\mathcal{B}^* = \{E - B,\ B \in \mathcal{B}\}.$$

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

The set $\mathcal{I}$ of subsets of bases is known as the set of independent sets of M, and then $\mathcal{B}$ is the set of maximal independent sets. The set $\mathcal{C}$ of minimal dependent sets (that is, not independent sets), is known as the set of circuits of M. Finally, there are two important functions on the power set of E, namely the rank and nullity functions : for $X \subset E$,

$$r(X) = Max\{|X \cap B|,\ B \in \mathcal{B}\}$$

and

$$n(X) = |X| - r(X).$$

The rank functions of the matroid M and its dual M^* are related by the equation

$$r^*(X) = |X| + r(E - X) - r(E).$$

The rank of a matroid is equal to the cardinality of any basis, or equivalently is $r(E)$.

A notion that will be used later is the fundamental circuit of an element with respect to a basis [19, Corollary 1.2.6]:

Definition 2 *If B is a basis and $e \in E - B$, 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 [23, Theorem 2], the author generalizes the notion of minimum distance of codes (the generalized Hamming weights), and this can be further extended to matroids in general ([12]):

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 [23, Theorem 3] for linear codes, and then generalized in [15] (in Norwegian, unpublished) 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 [22] 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.

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

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

To any almost affine code C of length n and dimension k on the alphabet F, we can associate a matroid M_C defined by its rank function, namely, for every $X \subset \{1, \cdots, n\}$,

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

Remark 1 *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.

Remark 2 *The class of almost affine codes is strictly bigger than the class of linear codes. It can namely be shown that the non-Pappus matroid is the matroid associated to an almost affine code ([22, Example 2]), but is not the matroid associated to any linear code ([19, Proposition 6.1.10]).*

Example 1 *We will use a running example throughout this paper. It is the almost affine code C' in [22, Example 5]. It is a code of length 3 and dimension 2 on the alphabet $\{0,1,2,3\}$. 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. This is an example of an almost affine code which is not equivalent to a linear code, and not even to a multilinear code (see Section 3.2 for the definition of multilinear codes)

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

Definition 4 *Let C be an almost affine 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 [22], that many quantities don't 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 [22]:

Definition 5 *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.

In the sequel, some proofs can be made clearer if one uses a equivalent code instead. An equivalent code is a code obtained from the original one by a succession of the three following operations:

- replace the alphabet F by an alphabet F' of same cardinality,
- permute the positions of the code,
- permute the symbols appearing at a fixed position.

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 $F = \{0, \cdots, q-1\}$ (change of alphabet), that $\{1, \cdots, k\}$ is a basis of the matroid associated to the code (permutation of the positions of the code), and that the word $(0, \cdots, 0) \in C$ (multiple permutations of the symbols appearing at a fixed position).

2 Generalized Hamming weights

2.1 Definition via the associated matroid

For a block code C, the minimal distance d is defined as

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

where $d(\boldsymbol{x}, \boldsymbol{y})$ is the Hamming distance between the codewords $\boldsymbol{x}$ and $\boldsymbol{y}$, that is, the number of indices where the two codewords differ. Then we have that

$$d(\boldsymbol{x}, \boldsymbol{y}) = |Supp(\boldsymbol{x}, \boldsymbol{y})|.$$

Then from [22, Prop. 5], the minimal distance of 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 6 *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. Its generalized Hamming weights are*

$$d_1(C') = 2$$
$$d_2(C') = 3.$$

Remark 3 For a linear code C, the generalized Hamming weights correspond to the generalized Hamming weights for the matroid associated to (any) parity check matrix of the code ([23, Theorem 2]). In [12], the matroid associated to parity check matrices is called the matroid associated to the code itself. All linear codes are of course almost affine too. In [22], the associated matroid M_C would correspond to the matroid associated to generator matrices of the linear code, that is the dual of the matroid associated to the linear code. While this can be confusing, by Wei duality for generalized Hamming weights for linear codes and for matroids, this is unproblematic, we just have to be cautious. We can of course use the matroid M_C instead of its dual in the definition.

Proposition 3 *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 $1 \leqslant i \leqslant k$,*

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

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

Proof The first two equality follows simply from the fact that

$$r^*(X) = |X| + r(E - X) + k$$

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 subcodes of a given dimension. While for linear codes of dimension k over the finite field $\mathbb{F}_q$, the number of 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 affine codes having the same associated matroid don't 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.

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

$$\bigcup_{\boldsymbol{w} \in D} Supp(\boldsymbol{w}, \boldsymbol{c}) = \bigcup_{\boldsymbol{w} \in D} Supp(\boldsymbol{w}, \boldsymbol{d}).$$

Proof Namely, let $i \in \bigcup_{\boldsymbol{w} \in D} Supp(\boldsymbol{w}, \boldsymbol{c})$. Then there exists $\boldsymbol{w} \in D$ such that $\boldsymbol{w}_i \neq \boldsymbol{c}_i$. If $\boldsymbol{w}_i \neq \boldsymbol{d}_i$, then of course $i \in \bigcup_{\boldsymbol{w} \in D} Supp(\boldsymbol{w}, \boldsymbol{d})$. Otherwise $\boldsymbol{c}_i \neq \boldsymbol{w}_i = \boldsymbol{d}_i$ and again, $i \in \bigcup_{\boldsymbol{w} \in D} Supp(\boldsymbol{w}, \boldsymbol{d})$. 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 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*

$$d_i(C) = Min\{|Supp(D)|,\ D \text{ is a subcode of dim. } i \text{ of } C\}$$

for $1 \leqslant i \leqslant k$.

Remark 4 *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 For $1 \leqslant i \leqslant k$, let

$$d_i = d_i(C)$$

and

$$e_i = Min\{|Supp(D)|,\ D \text{ is a subcode of dim. } i \text{ of C}\}.$$

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 $\boldsymbol{d} \in D \subset C$, and let $X = Supp(D, \boldsymbol{d})$. We look at $D' = C(E - X, \boldsymbol{d})$. By Proposition 2, we know that this is a subcode of dimension $l = k - r(E - X)$. It is obvious that $D \subset D'$, and in particular

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

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

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

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

$$d_i = |X| \geqslant |Supp(D'', \boldsymbol{c})| \geqslant Min\{|Supp(D), dim\ D = i\} = e_i.$$

Example 3 *Let C' be the code of Example 1. This code has 12 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 [12], 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 7 *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 [12] we have:

Proposition 4 *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 [22, 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 8 *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 4 gives rise to the following characterization of the generalized Hamming weights for a matroid.

Proposition 5 *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*

$$d_i(M) = Min\{|\bigcup_{j=1}^{i} X_j|,\ X_1, \cdots, X_i \text{ are non-redundant circuits}\}.$$

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 4, $j = n(Y) \geqslant i$. 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 4 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 6 *Let C be an almost affine code of dimension k. Then the generalized Hamming weights for C are given by*

$$d_i(C) = Min\{|\bigcup_{j=1}^{i} Supp(\boldsymbol{c_j}, \tilde{\boldsymbol{c}})|,\ (\boldsymbol{c_1}, \cdots, \boldsymbol{c_i}) \text{ are } \tilde{\boldsymbol{c}} - \text{minimal non-redundant codewords}\}$$

For a linear code, we have that a 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 subcode of dimension i. This is not the case for almost affine codes. There is for example no 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 a subcode of dimension i and such that $|Supp(D)| = d_i$. 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*

$$|\bigcup Supp(\boldsymbol{c_i}, \tilde{\boldsymbol{c}})| = |Supp(D)| = d_i.$$

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. Then $D \approx D_X = F^X$. In particular 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 $\boldsymbol{d_x}$ 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 the word $\boldsymbol{d_x}$ would be such that $(\boldsymbol{d_x})_X = (0, \cdots, 0)$, that is, $\boldsymbol{d_x} = \tilde{\boldsymbol{c}}$, which is absurd. Thus, these codewords $\boldsymbol{d_x}$ are $\tilde{\boldsymbol{c}}$-minimal non-redundant. Then by the word description of d_i, we have that

$$|\bigcup Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}})| \geqslant |\bigcup Supp(\boldsymbol{d_x}, \tilde{\boldsymbol{c}})| \geqslant d_i.$$

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

$$\bigcup Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}}) \subset Supp(D)$$

so that

$$d_i \leqslant |\bigcup Supp(\boldsymbol{c_x}, \tilde{\boldsymbol{c}})| \leqslant |Supp(D)| = d_i$$

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 $\tilde{\boldsymbol{c}}$ non-redundant and such that $|\bigcup Supp(\boldsymbol{c_j}, \tilde{\boldsymbol{c}})| = d_i$. Then there exists a subcode D of C containing $\tilde{\boldsymbol{c}}, \boldsymbol{c_1}, \cdots, \boldsymbol{c_i}$, of dimension i, and $|Supp(D)| = d_i$.*

Proof Let $X = \bigcup Supp(\boldsymbol{c_i}, \tilde{\boldsymbol{c}})$. From matroid theory, we know that $n^*(X) = i$, i.e $i = k - r(E - X)$. This also means that the subcode $D = C(E - X, \tilde{\boldsymbol{c}})$ is a 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, $Supp(C(E - X, \tilde{\boldsymbol{c}})) \subset X$, so that $|Supp(D)| \leqslant |X| = d_i$. By the subcode characterization of d_i, 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 ([23, 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 don't 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 doesn't exist in general

It is natural to ask the following about dual 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

Remark 5 *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 subcodes of C_1 and C_2 are the same.*

Proof This is obvious since two codes are equivalent if they can be obtained from one another by a series of operations of the following type:

- permutation of the positions of the code
- permutation of the symbols of the alphabet appearing at a fixed position.

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 $x \in E - B$. We have two possibilities:

- $b \notin \sigma(B,x)$, i.e. x is a loop. Let $\boldsymbol{w_i} \in C_i$ for $i \in \{1,2\}$. By Proposition 2,

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

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 $(\boldsymbol{w_2})_x$.

- $b \in \sigma(B,x)$. In that case, $\sigma(B,x) = \{b,x\}$. We then have, for $i \in \{1,2\}$,

$$|C_i| = |F| = |(C_i)_B|\,,$$

then for every $f \in F$, there exists a unique word $\boldsymbol{w_{i,f}} \in C_i$ such that

$$(\boldsymbol{w_{i,f}})_b = f.$$

Note that by cardinality

$$C_i = \{\boldsymbol{w_{i,f}},\ f \in F\}\,.$$

Since $\{b,x\}$ is a circuit, $\{x\}$ is independent, and therefore

$$\left|(C_i)_{\{x\}}\right| = |F|,$$

and there exists for every $g \in F$, a word $\boldsymbol{v_i} \in C_i$ such that $(\boldsymbol{v_i})_x = g$. This has to be one of the $\boldsymbol{w_{i,f}}$. Thus,

$$\forall i \in \{1,2\},\ \forall g \in F,\ \exists f \in F,\ (\boldsymbol{w_{i,f}})_x = g.$$

By a cardinality argument, we also have that

$$\forall i \in \{1,2\},\ \forall f, f' \in F,\ f \neq f',\ (\boldsymbol{w_{i,f}})_x \neq \left(\boldsymbol{w_{i,f'}}\right)_x.$$

This shows that

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

is well defined and 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 doesn't exist. Namely, the codes $\mathcal{C}$ and $\mathcal{C}'$ from [22, 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 isn't possible by Lemma 4 since it is known that $\mathcal{C}$ has 20 1-dimensional subcodes, while $\mathcal{C}'$ has just 12 of them.

Remark 6 Summing up: For $\mathbb{F}_q$-linear codes we then have that the d_i of a code are equal to the d_i of the matroid M_C^*, and that the d_j of the dual (orthogonal complement) code C^* are equal to the d_j of M_C. But for almost affine code we don't always have a dual almost affine code in the the (strong) sense above.

On the other hand an almost affine code C can be associated to some socalled (connected) access structure, say $\mathcal{A}_\mathcal{C}$. See e.g. [22], or [7]. To each such access structure $\mathcal{A}$ there is an associated matroid $M_\mathcal{A}$. Moreover $M_{\mathcal{A}_C} = M_C$. See [22, Remark 1], where one cites [23, Theorem 5.4.1]. Furthermore such access structures have dual access structures $\mathcal{A}^*$, described in [7, p. 84]. Moreover $M_{\mathcal{A}^*} = M_\mathcal{A}^*$ by [7, Theorem 10]. Hence the d_i of C are directly related to this object $\mathcal{A}^*$, and the d_i of M_C,

which are not in general equal to the d_i of any code in a natural way associated with M_C, at least are related to $\mathcal{A}$ in the same way as the d_i of C are related to $\mathcal{A}^*$.

Even if the access structure as such has a dual, it does not automatically tell us that another object, the associated ideal secret sharing scheme, has a dual such scheme, and it is this secret sharing scheme that corresponds directly to the almost affine code associated to the access structure. In the next subsection we will study almost affine codes C, which are not necessarily linear over the (main) alphabet we are considering, but where one nevertheless can define dual codes C^* because of an extra structure over another alphabet.

3.2 Duality of multilinear codes

An important case of almost affine codes are multilinear codes. For simplicity we will here use the following:

Definition 9 *A multilinear code is a $\mathbb{F}_q$-linear subspace of F^n, where $F = {\mathbb{F}_q}^m$, for some natural number m, such that $rk_{\mathbb{F}_q}(C_X)$ is divisible by m, for each $X \subset E = \{1, 2, \cdots, n\}$.*

Remark 7 Such a code is an almost affine code over the alphabet F. We will call it a multilinear code over F, which implicitly implies that it is also a usual linear code over the alphabet $\mathbb{F}_q$.

There are several definitions of multilinear codes, this one is essentially taken from [22, Example 2] (where one is not so concrete that one says $F = {\mathbb{F}_q}^m$, instead one says that F is a vector space over $\mathbb{F}_q$ of dimension m, but we claim that there is no loss in generality by setting $F = {\mathbb{F}_q}^m$).

The goal with this section is to show that a multilinear code C in a natural way has a dual multilinear code $C^\perp$ over F. Interpreted over the alphabet $\mathbb{F}_q$ this code $C^\perp$ is just the usual orthogonal complement of C in $\mathbb{F}_q^{mn}$.

Let C be such a multilinear code for a given m and n, and let G be a generator matrix for C over $\mathbb{F}_q$, like in [22, Example 2]. Hence C is the row space of G over $\mathbb{F}_q$, which makes C an $\mathbb{F}_q$-linear subspace of ${\mathbb{F}_q}^{mn}$, and a subset of F^n.

We assume that the rows of G are independent over $\mathbb{F}_q$ and the number of such rows is therefore $dim_{\mathbb{F}_q} C = dim_{\mathbb{F}_q} C_E$, which is divisible by m, by assumption, we call this number of rows $k_1 = mk$. Hence G is a $[mk \times mn]$-matrix over $\mathbb{F}_q$.

The set of column positions of G are $1_m \cup 2_m \cdots n_m$, where

$$a_m = \{(a-1)m + 1, (a-1)m + 2, \cdots, (a-1)m + m\},$$

for any natural number a. For any $X \subset E$, let X_m be the union of the x_m, for the $x \in X$. For comparison, see [21, proof of Theorem 4.3]. Let r_1 be the rank function associated to the (matroid $M|_G$ of the) generator matrix G, interpreted over $\mathbb{F}_q$. Let r_2 be the rank function associated to the almost affine code C over F.

By the assumptions above we have $r_1(X_m) = dim_{\mathbb{F}_q} C_X = m dim_F C_X = m r_2(X)$, for any $X \in E$.

Now let H be a parity check matrix of C over $\mathbb{F}_q$. The column rank function of H is r_1^*, which is the rank of the matroid dual of $M|_G$. For any $X \in E$ we have:

$$\begin{aligned} r_1^*(X_m) &= |X_m| + r_1(E_m) - r_1(E_m - X_m) \\ &= |X_m| + r_1(E_m) - r_1((E - X)_m) \\ &= m|X| + m r_2(E) - m r_2(E - X) \\ &= m r_2^*(X). \end{aligned} \tag{1}$$

We then the make three observations:

- We may interpret H as a generator matrix of a dual code over $\mathbb{F}_q$, which is also a subcode over F^n, by interpreting each group of succesive symbols in each row of H as an element of $F = \mathbb{F}_q^m$.
- $dim_{\mathbb{F}_q}(C^\perp)_X = r_1^*(X_m)$ is divisible by m for any $X \subset E$, by Equation (1). Hence $C^\perp$ is an almost affine code.
- $dim_F(C^\perp)_X = \frac{1}{m} dim_{\mathbb{F}_q}(C^\perp)_X = r_2^*(X)$, so also as an almost affine code over F, the rank function of the dual code $C^\perp$ of C is the dual matroid rank function of that of C.

Theorem 2 *Wei duality holds for the codes C and $C^\perp$, viewed as almost affine codes over F.*

Proof We know that Wei duality holds between the matroid, say N, associated to the rank function r_2 on $\mathcal{P}(E)$, and its dual matroid M, by general facts about Wei duality for matroids. Moreover the Hamming weights for $C^\perp$, are those of the matroid dual to its rank function r_2^*, that is: the matroid with rank function r_2, that is : N. Since Wei-duality holds between M and N, it holds between C and $C^\perp$ also.

We started this subsection by hinting at two different definitions of (a matroid being representable over) a multilinear code:

(a) A matroid M is derived from an $\mathbb{F}_q$-linear subspace of F^n, where $F = {\mathbb{F}_q}^m$. We also assume that C is an almost affine code over F, that is $rk_{\mathbb{F}_q}(C_X)$ is divisible by m for each $X \subset E = \{1, 2, \cdots, n\}$ (our working definition so far, and also the definition given in the paper that was the starting point of this investigation, [24, p. 10]).

(b) As (a), but we allow for an $\mathbb{F}_q$-linear subspace of F^n, where F could be any $m-$dimensional vector space over $\mathbb{F}_q$ (not necessarily $F = {\mathbb{F}_q}^m$). This is the the definition in [22].

Although (a) seems to be a special case of (b), these definitions are equivalent for all practical purposes.

Let us also introduce two other definitions, taken from [21].

(c) Let $M = (E, \rho)$ be a rank r matroid, m a positive integer, and $\mathbb{F}$ a skew field (i.e. $\mathbb{F}_q$ if finite, by Wedderburn). An m-multilinear representation of M (for this $\mathbb{F}$) is a function $V : E \to Gr(m, \mathbb{F}^{mr})$ that assigns to each element $e \in E$, an m-dimensional subspace $V(e)$ of the right vector space $\mathbb{F}^{mr}$, such that for all $X \subset E$ we have:

$$\dim(\Sigma_{e \in X} V(e)) = m.rk_M(X).$$

(d) The matroid M is representable over the skew partial field (for definitions of skew partial fields, and what it means to be representable over them, see [21, Definition 3.1] and [21, Definition 3.8], respectively):

$$\mathbb{P}(m\mathbb{F}) = (M(m, \mathbb{F}), GL(m, \mathbb{F}^m).$$

Here $M(m, \mathbb{F})$ is the ring of all $(m \times m)$-matrices over $\mathbb{F}$, while $GL(m, \mathbb{F}^m)$ as usual is the multiplicative subgroup of invertible matrices.

In the proof of [21, Theorem 4.3], one shows (c) and (d) to be equivalent.

Remark 8 *Hence (c) and (d) are equivalent, and so are (a) and (b), interpreted in a reasonable way. There remains a challenge, with us, in revealing the relationship between (a) and (b) on one hand, and (c) and (d) on the other. The definitions (c) and (d) seem to allow for a non-commutative setting, since e.g. the matrices in (d) do not commute. In (c), however, there is no non-commutativity unless $\mathbb{F}$ itself is not a usual field, but a non-commutative division ring. By Wedderburn again, this leads to a situation where $\mathbb{F}$ is infinite, which is probably outside the scope of this article.*

4 Extended weight polynomials of almost affine codes

In [9], and in [8, p. 323], one points out that for linear block codes of length n over a finite field $\mathbb{F}_q$, one can produce an infinite series of codes by extending the alphabet to $\mathbb{F}_{q^s}$, for $s = 1, 2, \cdots$, and nevertheless find polynomials $A_0, \cdots, A_n$, such that $A_j(q^s)$ computes the number of codewords of weight j, for all s simultaneously, for each of $j = 0, \cdots, n$. Hence knowledge of a finite number of coefficients of the A_j compute an infinite number of weights. (A crude upper bound for this finite number is $(k+1)(n+1)$, for the length n and the dimension k of the code. Set $d_0 = 0$. A better bound for the finite number of coefficients of all the A_j taken together is $1+\Sigma_{j=1}^{k}(j+1)(d_j - d_{j-1})$.) In this subsection we will show that a corresponding result holds for almost affine codes, and we will mimick the arguments in [10, Section 3] to find weight polynomials for an infinite series of almost affine codes C_Q, which we will now define.

Let $q = |F|$, where F is the alphabet over which an almost affine code C of block length n is defined. Let $Q = q^s$, and $F_Q = F^s$ and $C_Q = C^s$. Then C_Q is a code of block length n over the alphabet F_Q, if an element $((c_{1,1}, \cdots, c_{1,n}), \cdots, (c_{s,1}, \cdots, c_{s,n}))$ instead is interpreted as:

$$((c_{1,1}, \cdots, c_{s,1}), \cdots, (c_{1,n}, \cdots, c_{s,n})). \tag{2}$$

It is then automatic that $|(C_Q)_X| = Q^r$ if $|C_X| = q^r$, for some $X \subset E = \{1, 2, \cdots, n\}$, and natural number r. Hence C_Q is an almost affine code over F_Q, since C is an almost affine code over F. Moreover the matroid $M_{C_Q} = M_C$ since the rank functions are the same. Call the rank function r. Put $k = r(E)$.

Let $U \subset E$, and let $\boldsymbol{c_Q}$ be a fixed codeword in C_Q. Similarly as in [10] we define: $S_U(Q)$ is the subset of C_Q, viewed over F_Q, with the same coordinates as $\boldsymbol{c_Q}$ in the positions corresponding to U, in other words $S_U(Q) = C_Q(U, \boldsymbol{c_Q})$. But, since C_Q is an almost affine code we see that $|S_U(Q)| = Q^{k-r(U)}$. In the next definition, there is no explicit reference to the codeword $\boldsymbol{c_Q}$, since this is independent of the word chosen.

Definition 10 *For each $j = 1, \cdots, n$ let $A_{C,j}(Q)$ be the set of codewords of weight j in C_Q.*

Example 4 *Let C' be the code of Example 1. Then we have*

$$A_{C',3}(Q) = Q^2 - 3Q + 2$$

$$A_{C',2}(Q) = 3Q - 3$$

$$A_{C',1}(Q) = 0$$

and

$$A_{C',0}(Q) = 1.$$

Using the exclusion/inclusion principle and same formulas as in [10, Formula (9) p. 638], we obtain :

$$A_{C,n}(Q) = (-1)^n \sum_{X \subset E} (-1)^{|X|} Q^{n^*(X)}.$$

To obtain a similar formula for any $j \in \{1, 2, \cdots, n\}$, we proceed exactly as in [10, p. 638], and obtain:

Proposition 7 *For each $j = 0, 1, \cdots, n$ there are polynomials*

$$A_{C,j}(Q) = (-1)^j \sum_{|X|=j} \sum_{Y \subset X} (-1)^{|Y|} Q^{n^*(Y)}.$$

counting the number over codewords of weight j in C_Q.

In [10, Sections 4 and 5], one shows how this matroid expression can be expressed by $\mathbb{N}_0$-graded Betti numbers of the Stanley-Reisner rings of the matroid M_C^* and its elongations, viewed as simplicial complexes via their independence sets ([10, Theorem 5.1]). From the arguments above we now see that its concequence, [10, Corollary 5.1], formulated for linear codes in that corollary, carries over to almost affine codes, except that the matroid $M(H)$ appearing in [10, Corollary 5.1], must be replaced by the matroid dual M_C^*. See also [10, Proposition 4.1], which can be applied to determine the generalized Hamming weights for almost affine codes from the degrees of the polynomials $A_j(Q)$.

Example 5 *Let C be a multilinear code, like above, in particular a linear code over $\mathbb{F}_q$, and an almost affine code over $F = \mathbb{F}_q^m$. Let $Q = q^s$, for a natural number s.*

Let $C_Q = C \otimes_{\mathbb{F}_q} \mathbb{F}_Q$. By this we mean the row space over $\mathbb{F}_Q$ of G for any generator matrix G of C over $\mathbb{F}_q$.

For a moment, let us forget that C is multilinear, and remember only its linear structure over $A = \mathbb{F}_q$. We see that the alphabet $A_Q = \mathbb{F}_Q$ is an $A = \mathbb{F}_q$-vector space of dimension s, and can be identified with A^s, via a fixed basis. Furthermore C_Q can be identified with C^s and indeed is a code over the alphabet $A_Q = \mathbb{F}_Q$ as in formulated in (2). Let us now combine the fixed m with a varying s. For any s the code C_Q can also be viewed as a code over $\mathbb{F}_Q^m$, by "merging" groups of m successive symbols in each word, just as one did in the case $s = 1$. One might choose to look at this alphabet as

$$((\mathbb{F}_q)^s)^m = (\mathbb{F}_q)^{ms} = ((\mathbb{F}_q)^m)^s = F^s.$$

if one prefers. This can again be achieved by choosing a fixed base of the Galois field extension from $\mathbb{F}_q$, to $\mathbb{F}_Q$.

Since C is a linear code it has a dual code $C^\perp$, and two matroidal structures, r_1 acorresponding to the linear structure, and r_2, when remembering m, each with a dual matroidal structure. The important thing to note here is all these 4 matroid structures survive when s varies, and are simultanous for each s. The basic point is that a generator matrix for C is a generator matrix for all C_Q, and a parity check matrix for C is a parity check matrix for each C_Q. In particular we observe that the dimension of any projection $(C_Q)_X$, over $\mathbb{F}_Q$, for any $X \subset E$, is the same as the dimension of the projection $(C)_X$, over $\mathbb{F}_q$. Hence it is a multiple of m, and its cardinality a power of Q^m with integral exponent. Hence it is an almost affine code over $\mathbb{F}_Q^m$.

We also obtain:

Example 6 *The weight distributions of all the codes in the hierarchy over the one given in [22, Example 2], viewed over the alphabet $\mathbb{F}_q^2$, are given by the polynomials, appearing as coefficients of $X^t Y^{9-t}$ in the polynomial $W_{\mathcal{M}^*}(X, Y, T)$ in [6, p. 102].*

Let C be a multilinear code, and let B_j^r be the number of $r-$dimensional (over $\mathbb{F}_q$) subspaces of C, with support weight j interpreted as subsets of F^n, where $F = \mathbb{F}_q^m$, for some natural number $m \geq 2$.

We then have:

Proposition 8 $A_{C,j}(q^s) = \sum_{r=0}^{s} B_j^r \prod_{i=0}^{r-1}(q^s - q^i)$.

Proof The support, now in $\{1, \cdots, n\}$ of a word in C_Q, corresponding to s words in $C \subset F^n$, is the same as the support of the $\mathbb{F}_q$-subspace of C generated by these s words. Using this observation, the logic is the same as in the proof of [8, Proposition 6] (which is the case $m = 1$).

5 Generalized Kung's bound

In [13, Lemma 4.24], the author 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 bound of the dual linear code. In [11], 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 11 *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*

$$\gamma_i(\tilde{\boldsymbol{c}}) = Min\{j,\ \exists \boldsymbol{c_1}, \cdots, \boldsymbol{c_j} \in C,\ |\bigcup Supp(\boldsymbol{c_k}, \tilde{\boldsymbol{c}})| \geqslant i\}.$$

Remark 9 *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.

We can express these generalized critical exponents using the extended weight polynomials of the previous section.

Proposition 9 *Let C be an almost affine code of length n on the alphabet F. Let $\tilde{\boldsymbol{c}} \in C$. Let $q = |F|$. Then, for $1 \leqslant i \leqslant n$,*

$$\gamma_i(\tilde{\boldsymbol{c}}) = Min\{j,\ \sum_{l=i}^{n} A_{C,l}(q^j) \neq 0\}.$$

Proof This is obvious from Definitions 11 and 10.

Corollary 1 *The generalized critical exponents are independent of the chosen word $\tilde{\boldsymbol{c}}$.*

Proof It follows from the fact that the extended weight polynomials are independent of this word. They just depend on the underlying matroid.

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. Recall Definition 2.

Lemma 6 *Let M be a matroid on the ground set E. Let B a basis and $x \in E - B$. 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 Remember that $\sigma(B, x)$ is the only circuit of M included in $B \cup \{x\}$. Of course it contains x.
Assume that B' is not a basis. Then by cardinality, it is dependent, and contains therefore a circuit X. Obviously, $X \subset B' \subset B \cup \{x\}$ and thus $X = \sigma(B, x)$. Since $y \notin X$, one way is shown.
Assume now that $y \notin \sigma(B, x)$. Then $\sigma(B, x) \subset B' = B - \{y\} \cup \{x\}$ and B' is dependent, and a fortiori not a basis.

Theorem 3 *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 bound of M_C,

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

Remark 10 *We recall that the generalized Hamming weights d_i of the 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) [11, Theorem 9].

Proof 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. Since $C \approx C_B = F^k$, 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 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 4, 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

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

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 11 *These bounds are the best that can be found. Linear codes are namely almost affine codes, and in [11], it is mentioned that for simplex codes, the bounds are reached.*

Example 7 *Let C' be the code of Example 1. Let $\tilde{\boldsymbol{c}} = 321$. Then $\gamma_3(\tilde{\boldsymbol{c}}) = 1$ since $Supp(213, \tilde{\boldsymbol{c}}) = \{1,2,3\}$ (or we see from Example 4 that $A_{C',3}(4^1) = 6 \neq 0$). 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 3 says that*

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

6 Profiles of almost affine codes

In [4] one defines various distance/length and length/distance profiles for linear codes. Everything that does not involve dual codes, can be done also for almost affine codes. In [4] one defines

$$m_j(C) = \min\{|X|,\ dim C_X = j\},$$

where C_X, in contrast to how we defined it in at the start of our introduction, is defined as the set of code words with support on X (In the present paper we have chosen to use the notation from [22] at this point). By looking at $E-X$ in place of X we get, using our own notation from Definition 5:

$$m_j(C) = n - \max\{|X|,\ |C(X, \tilde{\boldsymbol{c}})| = q^j\}.$$

We see that this is in perfect harmony with our Proposition 3, valid for almost affine codes in general, saying:

$$d_j(C) = n - \max\{|X|,\ |C(X, \tilde{\boldsymbol{c}})| = q^j\},$$

so we can conclude $m_j(C) = d_j(C)$ for almost affine codes in general. Forney also defines:

$$k_j(C) = \max\{dim C_X,\ |X| = i\}$$

for linear codes, again using his definition of C_X. For almost affine codes the obvious generalization is:

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

using the notation from Definition 5. So, this will be our definition. In [4] one comments that for linear codes:

$$m_j(C)(= d_j(C)) = \min\{i,\ k_i(C) \geq j\}.$$

It is clear, by essentially the same argument as for linear codes, that this is true also for almost affine codes

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

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 one comments in [4] that for linear codes

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

But this latter statement also follows as naturally for almost affine codes, as for linear codes, since the last expression is equal to:

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

But this is $k_i(C)$.

Moreover, in [4], one defines

$$\tilde{k}_i(C) = \min\{dim P_X(C)||X| = i\}.$$

By $P_X(C)$, Forney here means the same object as we denote by C_X, the set of projections down on X, of all the code words in C. From Proposition 2 which is the almost affine version of the "linear" [4, Lemma 1] (first duality lemma), it is clear that this means:

$$\tilde{k}_i(C) = \min\{k - log_q|C(X, \tilde{\boldsymbol{c}})|,\ |X| = i\},$$

where $k = log_q|C|$ is the rank of the associated matroid. From this way of defining the $\tilde{k}_i(C)$ the almost affine version of [4, Theorem 2] comes out automatically:

$$k_i(C) + \tilde{k}_{n-i}(C) = k.$$

In [4] one also defines corresponding invariants for the dual code of a linear code C. For almost affine codes we do not have any dual almost affine code available in general, but we do have the dual matroid M_C^* of the matroid M_C, with rank function of M_C equal to $r(X) = k - log_q(C(X, c))$. Hence it is possible to use the formalism in e.g. [3] to define profiles $d_j, k_i, \tilde{k}_j \cdots$ also for the dual matroid M_C^* (the profiles for the matroid M_C will be the same as for the almost affine code C. And the formulas for the interactions between the profiles for C and the dual matroid M_C^* will be the same as the ones for the interaction between the profiles for C and its dual code, when C is linear over a field $\mathbb{F}_q$. This matroid formalism gives alternative proofs of (the admittedly very simple observations)

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

and

$$k_i(C) = \max\{j | m_j(C)(= d_j(C)) \geqslant i\}$$

above.

Remark 12 *In e.g. [14] (in Norwegian), and [18] more classically and authoritatively, one describes trellis decoding. It is clear that the way this is described, it goes just as well for almost affine codes (in general) as for linear codes (in particular). Knowledge of the profiles gives lower bounds for the complexity of the socalled state diagrams involved. Everything on [14, p. 46–59] seems to go through just as well for almost affine codes as for linear codes.*

7 Wire-tap channel of type II

In [20], the authors 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 [23], the author relates the equivocation (that is, a measure on the maximum of information an intruder might get access to) 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 $\{1, \cdots, k\}$ is a basis of the associated matroid M_C. Let $\varphi : F \times F \to F$ be a mapping such that for all $f \in F$, $\varphi(., f)$ and $\varphi(f, .)$ are bijections. For every $m = (m_{k+1}, \cdots, m_n) \in F^{n-k}$, define

$$C_m = \{(w_1, \cdots, w_k, \varphi(w_{k+1}, m_{k+1}), \cdots, \varphi(w_n, m_n)), \text{for } (w_1, \cdots, w_n) \in C\}.$$

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

Proof It is obvious that there is a bijection between C_m and C, since $\varphi(., m_t)$ is a bijection for every $k + 1 \leqslant t \leqslant n$. Now, suppose that $c = (c_1, \cdots, c_n) \in C_m \cap C_{m'}$. In particular, we have that

$$(c_1, \cdots, c_k, c_{k+1}, \cdots, c_n) = (w_1, \cdots, w_k, \varphi(w_{k+1}, m_{k+1}) \cdots, \varphi(w_n, m_n))$$

and

$$(c_1, \cdots, c_k, c_{k+1}, \cdots, c_n) = (w'_1, \cdots, w'_k, \varphi(w'_{k+1}, m'_{k+1}) \cdots, \varphi(w'_n, m'_n))$$

for some words $w, w' \in C$. Then $w_i = w'_i$ for all $1 \leqslant i \leqslant k$, and by Proposition 2 applied to $X = \{1 \cdots, k\}$ and $x = w$, $w_i = w'_i$ for every $k+1 \leqslant i \leqslant n$ also. Then $\varphi(w_i, m_i) = \varphi(w_i, m'_i)$, and thus $m_i = m'_i$ for all $k+1 \leqslant i \leqslant n$, that is $m = m'$. We conclude by a cardinality argument.

Corollary 2 *The sets $C_m \subset F^n$ are almost affine codes with associated matroid M_C.*

Proof We have namely, for $X \subset \{1, \cdots, n\}$,

$$(C_m)_X = (C_X)_{\overline{m}}$$

where $\overline{m}$ is the restriction of m to $X \cap \{n-k, \cdots, n\}$. Then

$$|(C_m)_X| = |(C_X)_{\overline{m}}| = |C_X|\,.$$

Our scheme is then the following: the encoder wants to send the message $m \in F^{n-k}$, and chooses randomly and uniformly any element $\boldsymbol{c} \in C_m$, and sends it. The decoder gets $\boldsymbol{c} = (c_1, \cdots, c_n)$, finds the unique codeword $\boldsymbol{w} = (w_1, \cdots, w_n) \in C$ such that $w_i = c_i$ for all $1 \leqslant i \leqslant k$. Then $m = (m_{k+1}, \cdots, m_n)$ is the unique element of F^{n-k} such that $\varphi(w_i, m_i) = c_i$ for all $k+1 \leqslant i \leqslant n$.

If the message $t \in F^n$ is sent over the channel, and an intruder is able to listen to a subset $X \subset \{1, \cdots, n\}$ of the digits of t, we will now see how much the intruder knows about m, namely which 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 $m = 2$. We construct therefore C'_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 m such that $m + 3 = 1$, that is $m = 2$.
An intruder able to listen to 1 digit, say the second, knows nothing about m. Namely, there are exactly 4 elements in C'_2 such that the second digit is 2, but the same is true also for $C' = C'_0$, C'_1 and C'_3. The same is true if the intruder is able to listen to 2 digits, say the first and second. There is exactly 1 word in C'_0, C'_1, C'_2 and C'_3 looking like $(1 \cdot 1)$, namely 101, 131, 121 and 111 respectively.

Lemma 8 *Let $\boldsymbol{t} \in F^n$ be any word, and $X \subset \{1, \cdots, n\}$. Then we have the following*

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

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

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

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

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

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

For the second point of the proof, we have

$$\begin{aligned} |\{\boldsymbol{w} \in F^n,\ \boldsymbol{w}_X = \boldsymbol{t}_X\}| &= \sum_{m \in F^{n-k}} |\{\boldsymbol{w} \in C_m,\ \boldsymbol{w}_X = \boldsymbol{t}_X\}| \\ &= \sum_{m \in F^{n-k}} |\Lambda_{\boldsymbol{t},X}(m)| \\ &= \sum_{m \in F^{n-k},\ \Lambda_{\boldsymbol{t},X}(m) \neq \emptyset} |\Lambda_{\boldsymbol{t},X}(m)| \\ &= \sum_{m \in F^{n-k},\ \Lambda_{\boldsymbol{t},X}(m) \neq \emptyset} |F|^{k - r(X)} \\ &= \big|\{m \in F^{n-k},\ \Lambda_{\boldsymbol{t},X}(m) \neq \emptyset\}\big|\, |F|^{k - r(X)} \end{aligned}$$

On the other hand, it is obvious that

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

and the result follows easily since $n(X) = |X| - r(X)$.

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 m. Namely, for every $m' \in F^{n-k}$, there are exactly $|F|^{k - |X|}$ words in $C_{m'}$ 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

$$H(F^{n-k}|T_X) = -\sum_{\boldsymbol{t}_X \in T_X} p(\boldsymbol{t}_X) \sum_{m \in F^{n-k}} p(m|\boldsymbol{t}_X) log_{|F|} p(m|\boldsymbol{t}_X).$$

Now, we assume that all messages 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

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

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 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 equirevocation of the system:

Theorem 4 *The equivocation Δ_μ of the system described above is entirely determined by the dual generalized Hamming weights for the 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

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

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

Remark 13 *In [16, Corollary 1], the equivocation of the two-party wiretap channel of type II is related to a profile of the pair of codes. If the second code is the 0 code, then this is the dual case of the scheme presented in [20] (namely, while they use a parity check matrix in [20], they use a generator matrix in [16]). In our case, we don't have a dual code, but we can use [4, Theorem 3] to define some dual DLP, namely*

$$\tilde{l}_\mu(C) = \mu - k_\mu(C).$$

Then it is easy to see that

$$E_\mu = \tilde{l}_{n-\mu}(C),$$

or written in other ways

$$E_\mu = n - \mu - \tilde{k}_{n-\mu}(C)$$

or again

$$\Delta_\mu = \mu - \tilde{k}_\mu(C)$$

Acknowledgements

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

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, pp. 331–341, 2012.

[3] T. Britz, T. Johnsen and J. Martin, *Chains, demi-matroids and profiles*, IEEE Transactions on Information Theory, vol. 60, No. 1 pp. 986–991, 2014.

[4] 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.

[5] G. Gordon, *On Brylaswski's Generalized Duality*, Mathematics in Computer Science vol. 6, no. 2, pp. 135–146, 2012.

[6] V. Huerga Represa, *Towers of Betti Numbers of Matroids and Weight Distribution of Linear Codes and their Duals*, Master's thesis in Pure Mathematics, University of Tromsø - The Arctic University of Norway, 2015. Available at http://hdl.handle.net/10037/7736.

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

[8] R.P.M.J. Jurrius, *Weight enumeration of codes from finite spaces* Des. Codes Cryptogr., vol. 63, pp. 321–330, 2012.

[9] R.P.M.J. Jurrius and G.R. Pellikaan, *Algebraic geometric modeling in information theory*, In: Codes, arrangements and matroids. Seroes on Coding Theory and Cryptology. World Scientific Publishing, Hackensack, NJ, 2001

[10] T. Johnsen, J. Roksvold and H. Verdure, *Generalized weight polynomials of matroids*, Discrete Mathematics, vol. 339, No, 2, pp. 632–645, 2016.

[11] T. Johnsen, K. Shiromoto and H. Verdure, *A generalization of Kung's bound*, Designs, Codes and Cryptography, to appear.

[12] 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.

[13] 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).

[14] E. Kvale, *Noen sammenhenger mellom grafer, matroider, lineære koder og trelliser*, Masters thesis, University of Bergen, 2008. Available at http://hdl.handle.net/1956/3365.

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

[16] Y. Luo, C. Mitrpant, A.J. van Vinck, and K. Chen, *Some New Characters on the Wire-Tap Channel of Type II*, IEEE Transactions on Information Theory, vol. 51, No. 3, pp. 1222–1229, 2005.

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

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

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

[20] L.H. Ozarow and A.D. Wyner, *Wire-tap-channel II*, AT&T Bell Labs Tech J., vol. 63, pp. 2135–2157, 1984.

[21] R.A. Pendavingh, and S.H.M. van Zvam, *Skew partial fields, multilinear representations of matroids, and a matrix tree theorem*, Advances in Applied Mathematics, vol. 50, pp. 201–227, 2013.

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

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

[24] T. Westerbäck, R. Freij, T. Ernvall and C. Hollanti, *On the Combinatorics of Locally Repairable Codes via Matroid Theory,* arXiv:1501.00153, 2015.

[25] Z. Zhuang, B. Dai, Y. Luo, A.J. van Vinck and K. Chen, *On the relative profiles of a linear code and a subcode*, Des. Codes Cryptogr., vol. 72, No. 2, pp. 219–247, 2014.