UiT
THE ARCTIC
UNIVERSITY
OF NORWAY

Faculty of Science and Technology

Department of Mathematics and Statistics

Almost Affine Codes and Matroids

—

Konstantin Diachkov

MAT-3900 Master's thesis in mathematics May 2017

Abstract

In this thesis we study various types of block codes, like linear, mutlti-linear, almost affine codes. We also look at how these codes can be described by associated matroids. In addition we look at flags (chains) of codes and see how their behavior can be described using demi-matroids. We also introduce weight polynomials for almost affine codes.

Contents

Almost Affine Codes and Matroids

1 Introduction

As long as people need to transmit data through noisy channels, we have to deal with errors. Error-correcting codes were made to help us to correct, or at least or to detect, errors that occurred through transmission. Such codes are used everywhere, from in a phone chat between two friends, to in computers where data corruption cannot be tolerated, and for example when receiving pictures from spacecrafts which are discovering cold dark undiscovered space. A typical situation is when data are digitalized and represented as strings of signs, or digits, taken from a given alphabet.

Basically we add some digits to the message we want to transmit, such that it is easier to correct the received message in case of an error. We will talk about block codes when the transmitted messages have the same length. The perhaps most common class of block codes is called *linear codes*. In this case the alphabet is a finite field $\mathbb{F}_q$, and a code C is a k-dimentional vector subspace of $\mathbb{F}_q^n$, and the linear code C is called an $[n, k]$-code. But there are also many other classes of codes; examples are *multilinear codes*, *affine codes*, *almost affine codes* and *quasi-uniform codes.*

Hence error-correcting codes is one interesting topic, both from an applied, and a theoretical viewpoint. Another interesting topic is that of matroids, which is simply a set of subsets of a given finite set E, such that this set of subsets satisfy three given axioms. At first sight matroids is just an abstract piece of mathematics, and has nothing to do with codes. But it is not so. And in this thesis we reveal some fundamental connections between matroids and some important classes of error-correcting codes. For instance, we can build a matroid over a generator matrix given by a linear code, and for larger classes of codes we can build a matroid over its rank functions; the connections between them leads us to generalization results.

In the two following chapters we recollect basic facts that we find relevant in our thesis. These facts are taken from standard textbooks or the booklet [1].

In particular, in Chapter 2 we introduce linear codes C over a finite alphabet A. And the alphabet A is then a finite field $\mathbb{F}$. Also we give some basic and important definitions, like the minimum distance of a code, the generalized Hamming weights of linear codes, the support of codeword in a linear code. Also we talk about how the code C can be represented through a matrix, a parity check matrix and a generator matrix. Also we define the dual code of C, denoted $C^{\perp}$.

In Chapter 3 we introduce matroids and describe some of their basic properties. We give three definitions of a matroid: via independent sets, via sets of bases and via rank functions. And we prove that all these definitions are equivalent. And for the givem matroid M we define its dual matroid M^*. Also in this chapter we talk about representability of matroids and how we can obtain a matroid from a linear code, denoted M_C, and we will get familiar with the important result, which says that $M_C^* = M_{C^{\perp}}$. We also introduce generalized Hamming weights of matroids, and Wei duality of matroids as well as for linear codes.

Chapter 4 treat larger classes of codes, these are classes that contain the linear codes. We define affine codes, multilinear codes, almost affine codes and quasi- uniform codes. And we make a comparison between these classes of codes and rank them in terms of generalization (with respect to inclusion).

In Chapter 5 we define demi-matroids, which is a generalization of matroids and enables us to study a larger class of objects. We give two definitions and prove they are equal. Also we define flags of matroids and almost affine codes, and we say in Corollary 104 and Corollary 108 that demi-matroids can be used to describe a pair of almost affine codes or even bigger chains of almost affine codes. A main purpose of this chapter is to extend well known properties for linear codes to results for almost affine codes. We will prove some statements like Theorem 110 which treats chains (or flags) of almost affine codes. This chapter is inspired by the preprint [3], but we will give some proofs that are not necessarily the same as those in [3].

In Chapter 6 we treat multilinear codes, in particular how a multilinear code can be viewed as an almost affine code. We also define the support of a set of codewords in an almost affine code in general, and study generalized Hamming weights for almost affine codes, and in particular for multilinear codes, and we show Wei duality for multilinear codes. We also show a Kung's bound for multilinear codes

In Chapter 7 we present a formula for calculating the cardinalities of the sets of codewords of given weights in an of almost affine code. Also we use the fact that a code $C^s \subseteq (F^n)^s$ can be viewed as a subcode of $(F^s)^n$ to obtain a hierarchy of codes over F^s, for $s \in \mathbb{N}$. The formula we obtained can be viewed as a result for all of these codes simultaneously, since the formula is given in terms of $Q = q^s$(the cardinality of the alphabet). In fact we use the matroid M_C in the same way for almost affine codes in the main result - Theorem 135, as for linear codes in [4].

2 Basic definitions of linear codes

In this section, we will introduce basic definitions of linear codes, some examples and proofs will be given as well. We assume that the reader already knows some algebra and linear algebra.

Definition 1 *An alphabet A is a finite set of symbols.*

Example 2 $A = \mathbb{F}_q$*, the field with q elements and q is a prime power.*

Definition 3 *Let q be an integer. Then a q-ary code is a set of r-tuples $(a_1, \cdots, a_r)$ (r can vary) where $a_i \in A$ and A is an alphabet of cardinality q. An element in this set is called a codeword. In case $A = \mathbb{F}_2$ the code is called binary code.*

From now on and further we will treat codes whose codewords all have the same length (r from the definition above is fixed). These codes are called block codes.

Example 4 *The set of all Norwegian postal codes is a 10-ary block code, every postal code has 4 digits.*

Definition 5 *The length n of a block code is equal to the length of any codeword.*

Definition 6 *Consider the alphabet, A and let A^n be the set of all words of length n. Let $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ be two words. The Hamming distance between x and y is*

$$d(x, y) = \# \{i | x_i \neq y_i\}.$$

If the alphabet is a field $\mathbb{F}_q$, then the weight of the codeword x is

$$wt(x) = \# \{i, x_i \neq 0\}.$$

Example 7 *One of the Oslo's postal codes is 0029. The postal code the University of Tromsø belongs to is 9019. And the Hamming distance between them is*

$$d(0029, 9019) = 2$$

since just the first and the third digits are different.

Definition 8 *The minimum distance of a code C is*

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

Code C can be define well by three numbers (n, M, d). Where n is a code length, M is a quantity of codewords and d is a minimum distance.

Example 9 *Let C be* $\{(0000), (1100), (0011), (1010)\}$. *It is easy to see that the minimum distance is 2.*

Definition 10 *A linear code over the finite field $\mathbb{F}_q$ is a linear subspace of the vector space $\mathbb{F}_q^n$.*

A subset C of $\mathbb{F}_q^n$ is a linear code if and only if it is closed under addition and scalar multiplication. If C is a k-dimentional vector subspace of $\mathbb{F}_q^n$, then the linear code C is called an $[n, k]$-code or $[n, k, d]$ if we need to specify minimum distance d as well.

Lemma 11 *Let x, y be two codewords of a linear code. Then*

$$d(x, y) = wt(x - y).$$

Proof. We have

$$d(x, y) = \# \{i|x_i \neq y_i\}$$

$$= \# \{i|x_i - y_i \neq 0\}$$

$$= wt(x - y)\square$$

Theorem 12 *Let C be a linear code. Then*

$$d = Min \{wt(x)|x \in C - \{(0, ..., 0)\}\}.$$

Proof. See the proof of Theorem 5.2 in [3].

This way of finding a minimum distance of the code is much easier since we don't need to check all possible pairs of code words.

Definition 13 *The support of codeword x is*

$$Supp(x) = \{i|x_i \neq 0\}$$

The support of a set of codewords is just the union of the supports of the codewords

$$Supp(S) = \bigcup_{x \in S} Supp(x) = \{i|\exists x \in S, x_i \neq 0\}$$

Definition 14 *Let C be a $[n, k]$ code. Then the generalized Hamming weights are*

d_i=Min{# Supp(D)—D is a subcode of dimension i of C }

Definition 15 *A $k{\times}n$ matrix whose rows from a basis of a linear $[n, k]-$code is called a generator matrix of the code.*

The generator matrix G for the $[n, k]$ −code is not unique since the basis for $[n, k]$ −code is not unique.

Definition 16 *Two linear codes over $\mathbb{F}_q$ are called equivalent if one can be obtained from the other by a combination of operations of the following types.*

(1) Permutation of the position of the code;
(2) Multiplication of the symbols appearing in a fixed position by a non-zero scalar.

Theorem 17 *Two $k{\times}n$ matrices generate equivalent linear $[n, k]-$codes over $\mathbb{F}_q$ if one matrix can be obtained from the other by a sequence of operations of the following types:*

(R1) Permutation of the rows.
(R2) Multiplication of a row by a non-zero scalar.
(R3) Addition of a scalar multiple of one row to another.
(C1) Permutation of the columns.
(C2) Multiplication of any column by a non-zero scalar.

Proof. See the proof of Theorem 5.4 in [3].

Proposition 18 *Two equivalent codes have the same parameters n, k and d.*
Proof. It is quite obvious that the length m of two equivalent codes is the same. Dimension k also will not change by using the operations above, which follows from standard linear algebra.

Remark 19 *If we only use rows transformations such that (R1), (R2) and (R3), we obtain a different generator matrix for the same code.*

Theorem 20 *Let G be a generator matrix of an $[n, k]-$code. Then by performing operations of types represented above, G can be transformed to the standard form*

$$[I_k|A],$$

where I_k is the $k \times k$ identity matrix, and A is a $k \times (n-k)$ matrix.
Proof. See the proof of Theorem 5.5 in [3].

Definition 21 *Given a linear $[n, k]-$code C, the dual code of C, denoted $C^{\perp}$, is defined to be the set of those vectors of $\mathbb{F}_q^n$ which are orthogonal to every codeword of C. i.e.*
$C^{\perp} = \{y \in \mathbb{F}_q^n | x \cdot y = 0,$ *for all* $x \in C\}$

The code $C^{\perp}$ is also a linear code since the set of all orthogonal vectors to $\mathbb{F}_q^k$ vector space gives us vector space $\mathbb{F}_q^{n-k}$. So the code $C^{\perp}$ is a linear [n, n-k]-code.

Definition 22 *A generator matrix of $C^{\perp}$ is called a parity check matrix of C.*

Remark 23 *If H is a parity check matrix for C, then*

$$C = \{x | H \cdot x^T = 0\}.$$

Theorem 24 *Let C be a linear [n,k]-code with generator matrix G under standard form*

$$G = [I_k|A].$$

Then a parity check matrix for C is given by

$$H = [-A^T|I_{n-k}].$$

Proof. See the proof of Theorem 4.6 in [5].

Definition 25 *A parity check matrix $H = [B|I_{n-k}]$ is also called a parity check matrix in standard form.*

Corollary 26 *Let C be a linear code with H as a parity check matrix. Then, by performing operations of type (R1), (R2), (R3), (C1) and (C2), we can obtain a parity check matrix in standard form.*

Proof. We can find generator matrix $G = [I|A]$ for a $C^{\perp}$ in a standard form for generator matrixes and all we need to obtain a parity check matrix in standard form is to simply swap I and A and call A as B. Need to be noticed that swaping is a combination of allowed operations.

Theorem 27 *Let C be a linear [n,k]-code with parity check matrix H. Then the minimum distance of C is d if and only if any d-1 columns of H are linearly independent, but some d columns are linearly dependent.*

Proof. Let $H = [C_1|C_2|\cdots|C_n]$ be the parity check matrix for code C, where C_i is a i-th column. According to Theorem 12, $d(C) = d \Leftrightarrow d = Min\{wt(x)|x \in C - \{(0,\cdots,0)\}\}$ i. e.

$$\exists x \in C - (0,\cdots,0)|wt(x) = d$$

and

$$\nexists x \in C - (0,\cdots,0)|wt(x) < d$$

But what does it mean that wt(x)=j, it means $x = (0,\cdots x_1,\cdots 0, x_j)$ where only $x_{\overline{1,j}}$ not equal to zero. Then

$$[C_1|C_2|\cdots|C_n] \cdot [0,\cdots x_1,\cdots 0, x_j)]^T = 0$$

$$x_1 C_{i1} + \cdots + x_j C_{ij} = 0$$

It is a linear relation between exactly j columns. As a result we have a linear relation between d columns and there is no linear relation between less then d columns □

Example 28 *The [5,3]-code C over $\mathbb{F}_5$ is given by its generator matrix:*

$$G = \begin{pmatrix} 2 & 2 & 0 & 4 & 3 \\ 1 & 2 & 1 & 4 & 2 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

First of all, we are going to obtain a generator matrix in standard form. Subtract row 3 from row 2:

$$\begin{pmatrix} 2 & 2 & 0 & 4 & 3 \\ 0 & 1 & 0 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Then we multiply the first row by 3:

$$\begin{pmatrix} 1 & 1 & 0 & 2 & 4 \\ 0 & 1 & 0 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Then we subtract the first row from the third:

$$\begin{pmatrix} 1 & 1 & 0 & 2 & 4 \\ 0 & 1 & 0 & 3 & 1 \\ 0 & 0 & 1 & 4 & 2 \end{pmatrix}$$

Finally, we obtained generator matrix in standard form by subtracting row 2 from row 1:

$$\begin{pmatrix} 1 & 0 & 0 & 4 & 3 \\ 0 & 1 & 0 & 3 & 1 \\ 0 & 0 & 1 & 4 & 2 \end{pmatrix}$$

Now we use the Theorem 25 and find parity check matrix H for our code C :

$$H = \begin{pmatrix} 1 & 2 & 1 & 1 & 0 \\ 2 & 4 & 3 & 0 & 1 \end{pmatrix}$$

It is easy to see that first two columns are linearly dependent and there is no zero columns. Following the Theorem 27, Its gives us that minimum distance is 2. Now lets find the minimum distance of the orthogonal compliment of C by finding 3×3 determinants of generator matrix in standard form:

$$det \begin{pmatrix} 0 & 4 & 3 \\ 0 & 3 & 1 \\ 1 & 4 & 2 \end{pmatrix} = -5 = 0 \ mod \ 5$$

We found 3 columns are dependent which means the minimum distance of the orthogonal compliment of C is at most 3. But all pairs of columns are linearly independent. Hence minimum distance is 3.

Theorem 29 *Let C be a linear [n,k]-code, and $C^{\perp}$ its dual code. Let $d_1 < \cdots < d_k$ and $d_1^* < \cdots < d_{n-k}^*$ be the weight hierarchies of C and $C^{\perp}$ respectively. Then*

$$\left\{d_1, \cdots, d_n, n+1-d_1^*, n+1-d_{n-k}^*\right\} = \{1, \cdots, n\}.$$

Proof. See the proof in [5].

3 Introduction to Matroids

There are many equivalent definitions of matroids, we first start with a definition through independence sets.

Definition 30 *A finite matroid is a pair (E, $\mathcal{I}$) where E is a finite set $\{1, \ldots, n\}$ (called the ground set), and $\mathcal{I}$ is a family of subsets of E (called independent sets). And $\mathcal{I}$ satisfies following axioms:*

(I_1) $\emptyset \in \mathcal{I}$,

(I_2) If $I_1 \in \mathcal{I}$ *and* $I_2 \subset I_1$, *then* $I_2 \in \mathcal{I}$,

(I_3) If I_1 *and* I_2 *are both elements of* $\mathcal{I}$ *with* $|I_1| < |I_2|$, *then there exists* $x \in I_2 - I_1$ *such that* $I_1 \cup \{x\} \in \mathcal{I}$.

Definition 31 *Let F be a field and* $A \in F^{m \times n}$ *an* $m \times n$ *matrix. Let* $E = \{1, ..., n\}$ *be the index set of the columns of A. Then* $I \subseteq E$ *is independent if the columns indexed by I are linearly independent. The matroid (E, $\mathcal{I}$) constructed in this way called a linear matroid*

Definition 32 *Let F be a field, a matroid is said to be representable over given a field F if it can be expressed as a linear matroid with matrix A and independence taken over F.*

Definition 33 *A matroid is called regular if its representable over any field.*

Definition 34 *A maximal independent set is called a basis and denoted by B.*

Proposition 35 *The bases of a matroid all have the same cardinality.*

Proof. Suppose that B_1 *and* B_2 *are two bases with different cardinality and* $|B_1| < |B_2|$. *Since* B_1 *and* B_2 *are independent sets we can use axiom* (I_3) *and find* $x \in B_2 - B_1$ *such that* $B_1 \cup \{x\}$ *is still independent. This is contradiction because* B_1 *supposed to be a maximal independent set.* □

Definition 36 *Let E be a finite set and* $\mathcal{B} \subset 2^E$. *We say that* $\mathcal{B}$ *is set of bases if it satisfies the two following axioms*

(B_1)$\mathcal{B} \neq \emptyset$,

(B_2)$\forall B_1, B_2 \in \mathcal{B}, \forall x \in B_2 - B_1, \exists y \in B_1 - B_2, B_2 \cup \{y\} - \{x\} \in \mathcal{B}$.

Now we show that a matroid defined by axioms for independent sets $\mathcal{I}$ satisfies axioms for bases $\mathcal{B}$.

Corollary 37 *Let* $M = (E, \mathcal{I})$ *be matriod, then the set of bases* $\mathcal{B}$ *from the Definition 33 satisfies the definition 36.*

Proof. *According to (I_1), $\emptyset \in \mathcal{I}$, so $\mathcal{B}$ is not empty. It proves (B_1). To prove (B_2) we assume that (B_2) is false, then its negation is true:*

$\exists B_1, B_2 \in \mathcal{B}, \exists x \in B_2 - B_1, \nexists y \in B_1 - B_2, B_2 \cup \{y\} - \{x\} \in \mathcal{B}$

We can take $I_1 = B_2 - \{x\}$ and $I_2 = B_1$. Since $|I_1| < |I_2|$ and $B_2 \cup \{y\} - \{x\} \in \mathcal{B}$ is equal to $I_1 \cup \{y\} \in \mathcal{I}$, we have contradiction to axiom (I_3). So our assumption is wrong and axiom (B_2) works□

Now we can describe matroids through the set of bases.

Theorem 38 *Let $\mathcal{B}$ be a set of bases on E. Let $\mathcal{I} = \{X \subset B, B \in \mathcal{B}\}$. Then M($\mathcal{B}$) $= (E, \mathcal{I})$ is a matroid, whose set of bases is $\mathcal{B}$.*

Proof. *The axiom (I_1) follows from (B_1) and the statement that any set has the empty set as a subset. Axiom (I_2) is also obvious because if I_2 is a subset of I_1 it is a subset of the same base B as I_1. The proof of the third axiom (I_3) can be found in [5]*□

Example 39 *We construct the matroid from the given matrix M over $\mathbb{R}$*

$$M = \begin{pmatrix} 0 & 0 & 2 & 4 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 1 & 1 & 1 & 2 & 3 \end{pmatrix}$$

The ground set is $E = \{1, 2, 3, 4, 5\}$ and $\mathcal{I}$ consist of all linearly independent sets of columns.

$\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,5\}, \{4,5\}, \{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{1,3,5\}, \{1,4,5\}, \{2,3,5\}\}$.

And it is easy to see that $\mathcal{B} = \{\{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{1,3,5\}, \{1,4,5\}, \{2,3,5\}\}$.

Definition 40 *A matroid $U_{a,b}$ is called uniform matroid if it based on the ground set of b elements and every subset of a elements is a basis of $U_{a,b}$.*

Now we introduce the circuits of a matroids.

Definition 41 *The circuit of a matroid is a minimal dependent subset (for inclusion) of E.*

We define the set of all circuits of a matroid by $\mathcal{C}$

Proposition 42 *A circuits of a matroid satisfy the following properties:*

(C_1) $\emptyset \notin \mathcal{C}$,

(C_2) *If $C_1, C_2 \in \mathcal{C}$ with $C_1 \subset C_2$, then $C_1 = C_2$,*

(C_3) If $C_1, C_2 \in \mathcal{C}$ are distinct and not disjoint, then for any $e \in C_1 \cap C_2$, there exists $C_3 \in \mathcal{C}$ such that $C_3 \subset (C_1 \cup C_2) - \{e\}$

Proof. We need to show that the matroid's axioms $(I_1), (I_2), (I_3)$ in the Definition 30 imply the above properties. If $\emptyset$ belongs to C it means that $\emptyset$ is dependent set but this is a contradiction to (I_1). The property (C_2) comes straight from minimality of circuits. The proof of (C_3) is in the Proposition 20 in [5].

Now we are going to construct an object which looks like a matroid by using circuits and theirs properties taken as axioms. And we will prove it is a matroid.

Theorem 43 *Let E be a finite set, and $\mathcal{C} \in 2^E$ satisfying $(C_1), (C_2)$ and (C_3), now interpreted as axioms. Let*

$$\mathcal{I} = \{X \subset E, \nexists C \in \mathcal{C}, C \subset X\}$$

Then $(E, \mathcal{I})$ is a matroid whose set of circuits is $\mathcal{C}$.

Proof. See the Theorem 6.7 in [5].

Example 44 *Let's find the circuits of Example 39. According to the definition the matroid M has $\mathcal{C} = \{\{3,4\}, \{1,2,4,5\}, \{1,2,3,5\}\}$.*

Definition 45 *Let G be a graph. Then set of minimal cycles of the graph is the set of circuits of a matroid. A matroid isomorphic to such a matroid is called a graphic matroid.*

Remark 46 *It can be shown that all graphic matroids are regular. But there are many representable matroids that are not graphic.*

Example 47 *To illustrate the remark above we can take a uniform matroid $U_{2,4}$. It is a matroid with $|E| = 4$ and any set consists of up to 2 elements is independent. It is easy to check that there is no graph with four edges such that each collection of three edges is a cycle and each two edges must not contain a cycle. But the matrix*

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

gives us a representation of our matroid over $\mathbb{R}$.

Now we introduce the rank function of a matroid.

Definition 48 *Let $M = (E, \mathcal{I})$ be a matroid. The rank of the matroid M is the function*

$$r : 2^E \to \mathbb{N}$$
$$X \mapsto Max\{|I|, I \subset X, I \in \mathcal{I}\}$$

The nullity function is $n : 2^E \to \mathbb{N}$ defined by $n(X) = |X| - r(X)$. By abuse of notation, we shall write r(M)=r(E).

The rank function of a matroid satisfies the following properties:

Proposition 49 *The rank function of a matroid M=(E, $\mathcal{I}$) satisfies the following properties:*

(R_1) $r(\emptyset) = 0$,

(R_2) *If* $X \subset E$ *and* $x \in E$, *then* $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$,

(R_3) *If* $X \subset E$ *and* $x, y \in E$, *are such that* $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$, *then* $r(X \cup \{x, y\}) = r(X)$.

Proof. The first property follows from the definition. As for the second, by adding an element to X we can either not change its biggest independent set or increase its cardinality by one. As for the third, we choose two elements which separately don't affect on the maximal independent set of X, so if we add them together we will not affect on the maximal independent set as well.
It was just an idea of a proof, for more careful proof check the proof of the Proposition 17 of [5].

We will give an alternative description.

Proposition 50 *Let* $r : 2^E \rightarrow \mathbb{N}$ *be a function. Then the 3 following properties:*

(R_1') $0 \leq r(X) \leq |X|$,
(R_2') *If* $X \subset Y \subset E, r(X) \leq r(Y)$,
(R_3') *If* $X \subset Y \subset E, r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$.

are equivalent to the properties $(R_1), (R_2)$ *and* (R_3).
Proof. See the proof of the Proposition 18 in [5].

Now we are going to describe a matroid through its rank function.

Theorem 51 *Let E be a finite set and* $r : 2^E \rightarrow \mathbb{N}$ *a function satisfying* $(R_1), (R_2)$ *and* (R_3). *Then if*

$$\mathcal{I} = \{I \in 2^E, r(I) = |I|\},$$

then the pair (E, $\mathcal{I}$) is a matroid.

Proof. See the proof of the Theorem 6.5 in [5].

Example 52 *Now we find ranks of some subsets of the ground set of the matroid M from Example 39.*

$$r(\{1\}) = r(\{3\}) = r(\{5\}) = r(\{3,4\}) = 1,$$
$$r(\{1,2\}) = r(\{2,5\}) = r(\{4,5\}) = r(\{1,3,4\}) = 2,$$
$$r(\{1,2,3\}) = r(\{2,3,5\}) = r(\{1,2,3,4\}) = r(\{1,2,3,4,5\}) = 3.$$

Eventually we have defined matriods through independent sets, bases, circuits and rank function. And we saw that all of these definitions are equal.

Duality of matroids.

Definition 53 *Let M be a matroid on the ground set E and set of bases $\mathcal{B}$. Then the matroid on E with set of bases $\{\bar{B}|B \in \mathcal{B}\}$ is called the dual M, and denoted by M*.*

Remark 54 *To justify this definition one has to show that the set $\{\bar{B}|B \in \mathcal{B}\}$ satisfies the axioms (B_1) and (B_2) of the Definition 36.*

Proof. See the proof of the Theorem 7.2 in [5].

Remark 55 *We have that $(M^*)^* = M$.*

Proof. It is true since $\forall B \in \mathcal{B}|\bar{\bar{B}} = B$.

Example 56 *Let's find a dual matroid of the matroid of Example 39. We have*

$$\mathcal{B} = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 5\}, \{1, 4, 5\}, \{2, 3, 5\}\}$$

and its compliment looks like:

$$\bar{\mathcal{B}} = \{\{4, 5\}, \{3, 5\}, \{3, 4\}, \{2, 4\}, \{2, 3\}, \{1, 4\}\}.$$

So $M^* = (E, \bar{\mathcal{B}})$.

Example 57 *An uniform matroid $U_{a,b}$ has the uniform matroid $U_{b-a,b}$ as its dual.*

Proposition 58 *Let M be a matroid of rank r on the ground set E. Then the rank of M^* is $|E| - r$.*

Proof. The rank of M is equal to the cardinality of any base, and cardinality of a compliment to any base is exactly $|E| - r$.

Theorem 59 *Let M be a matroid of rank function r. Then the rank function r^* of M^* is given by*

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

Proof. See the proof of Theorem 7.3 in [5].

Corollary 60 *Let M be a matroid with nullity function n. Then the nullity function n^* of M^* is given by*

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

Proof.

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

and

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

Since $r(E) = r(M)$, we have

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

and

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

Definition 61 *Two matroids $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ are isomorphic if there exists a bijection $\phi : E_1 \to E_2$ such that*

$$X \in \mathcal{I}_1 \Leftrightarrow \phi(X) \in \mathcal{I}_2.$$

Theorem 62 *Let M, N be two isomorphic matroids. Then M* and N* are isomorphic.*
Proof. See the Theorem 7.5 in [5].

Proposition 63 *The class of representable matroids is closed under duality.*

Proposition 64 *The class of regular matroids is closed under duality.*

Theorem 65 *Let C be a $[n, k]_q$ linear code defined by a generator matrix G or a parity check matrix H. Let G' be another generator matrix of C, and H' be another parity check matrix of C. Then*

$$M[G] = M[G']$$

and

$$M[H] = M[H'].$$

Proof. As we mentioned before, we can get G' from G (or H' from H) by performing row operations on a matrix. But this does not change dependence relations between columns, so $M[G] = M[G']$ and $M[H] = M[H']$.

Definition 66 *Let C be a $[n, k]_q$ linear code. Then the matroid M_C associated to the code is*

$$M_C = M[H]$$

where H is a parity check matrix of C.

Theorem 67 *Let C be a $[n,k]_q$ linear code. Then M_C is a matroid on $E = \{1,\dots,n\}$, of rank n-k. Moreover, we have*

$$M_C^* = M_{C^\perp}.$$

Proof. See the Theorem 7.12 in [5].

Remark 68 *The theorem above helps us to explain why the Proposition 63 and Proposition 64 are true. If M is a representable matroid over a field F it has the matrix as a 'representation'. Every matrix can be assumed to be a parity check matrix of a linear code for example, called C. Every code C has an orthogonal compliment $C^\perp$ which is a also linear code over the same alphabet and can be defined by another parity check matrix over that field. And the matroid build over $C^\perp$ is exactly dual to our original matroid M by construction.*

Definition 69 *Let M be a matroid over the ground set E and with rank function r. Let $1 \leqslant i \leqslant \#E - r(E)$. Then the i-th generalized Hamming weight of M is*

$$d_i = Min\{\#X | \#X - r(X) = i\}.$$

Theorem 70 *Let C be a linear code over finite field $\mathbb{F}_q$. If $M = M_C$, then*

$$d_i(C) = d_i(M), \text{ for } i = 1,\dots,k = rank(M).$$

Proof. See p.108-110 in [5].

Proposition 71 *Let M be a matroid of rank r on the ground set E. Then we have*

$$d_1 < \cdots < d_{|E|-r}.$$

Example 72 *Lets find d_i of the code in Example 28. These are equal to d_i of the matroid M_C, defined by the parity check matrix H in Example 28. There are three of them because $|E| - r(E) = 5 - 2 = 3.$, where r is the rank function of M_C.*

$$d_1 = Min\{|Supp(D)| \text{ where D is 1-dimensional subspace of } C\}$$
$$d_1 = Min\{wt(x) | x \in C\}$$

and we already know from Example 28 that it is 2;

$$d_3 = Min\{|Supp(D)| \text{ where D is 3-dimensional subspace of } C\} = |Supp(C)| = 5.$$

To find d_2 we use Theorem 70.

$$d_2 = Min\{\#X | \#X - r(X) = 2\}$$

from the Proposition above it must be 3 or 4. It can not be 3 since each subset of cardinality 3 has nullity 1, because it has three different subsets of cardinality 2, but there is the only one pair of elements which is dependent - $\{1,2\}$. So it is 4.

Theorem 73 *Let M be a matroid on the ground set E and rank r. Let*

$$d_1 < \cdots < d_{|E|-r}$$

be its weight hierarchy. Let

$$e_1 < \cdots < e_r$$

be the weight hierarchy of M^*. Then we have

$$\{d_1, \cdots, d_{|E|-r}\} \cup \{n+1-e_1, \cdots, n+1-e_r\} = \{1, \cdots, n\}$$

and the union is disjoint.

Example 74 *Now we take an example of non-representable matroid called Vamos matroid. It is a matroid $V = (E, \mathcal{I})$ with $|E| = 8$, $r(V) = 4$ and all subsets of cardinality 4 or less are independent except $\{1,2,5,6\}$, $\{1,2,7,8\}$, $\{3,4,5,6\}$, $\{3,4,7,8\}$ and $\{5,6,7,8\}$. Vamos matroid has d_1, d_2, d_3 and d_4, since $|E| - r(V) = 8 - 4 = 4$. It is clear that $d_1 = 4$ and $d_4 \leqslant 8$ and according to the Proposition 71 we have*

$$4 = d_1 < d_2 < d_3 < d_4 \leqslant 8.$$

It is also known that V is isomorphic to V^*. Hence $d_i = d_i^*$ for the Hamming weights d_i of V. In particular $d_1^* = 4$. Now by using Theorem 73 we have $n + 1 - d_1^* = 9 - 4 = 5$, so 5 doesn't belong to the inequality above. Hence this inequality has the only one solution left, namely $d_1 = 4$, $d_2 = 6$, $d_3 = 7$, $d_4 = 8$. And as we mentioned before $d_1^* = 4$, $d_2^* = 6$, $d_3^* = 7$, $d_4^* = 8$.

4 Back to Codes

We define almost affine codes and a class of codes which is even bigger than it and see how there are matroids associated to almost affine codes.

Up until now we have studied mostly a linear codes but these codes are a part of the 'code world' which is slightly bigger:

1. Linear codes
2. Affine codes
3. Multilinear codes
4. Almost affine codes
5. Quasi-uniform codes

Definition 75 *An affine code is a subset S of F^n for a finite field F, such that $S = C + \bar{w}$ for a fixed word $\bar{w}$, and a linear code C.*

Hence linear codes are special case for affine codes for $\bar{w} = \bar{0}$.

Definition 76 *Let F be a finite set of cardinality at least 2, and E be a finite set of cardinality $n \geqslant 1$. We may assume $E = \{1, 2, \cdots, n\}$, let $X = \{x_1, \cdots, x_s\} \subseteq E$. Define*

$$\rho_x : F^E \to F^X$$
$$(c_1, \cdots, c_n) \to (c_{x1}, \cdots, c_{xs}).$$

Example 77 *$F = \mathbb{Z}_7$, $n = 5$ and $X = \{2, 3, 5\}$, then $\rho_X : (5, 4, 3, 2, 1) \to (4, 3, 1)$.*

Definition 78 *Let C be a code, then $C_X = \rho_X(C)$. If $X = \emptyset$, let $|C_X| = 1$*

Definition 79 *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 $dim_{\mathbb{F}_q}(C_X)$ is divisible by m, for each $X \subset E = \{1, 2, \cdots, n\}$.*

Remark 80 *Linear codes are special case of multilinear codes, with m=1.*

Definition 81 *A code $C \subseteq F^E$ is called almost affine if it satisfies the condition*

$$r(X) = log_{|F|}(|C_X|) \in \mathbb{N} \text{ for all } X \subseteq E.$$

Proposition 82 *Multilinear codes are almost affine codes.*
Proof. Let $X \subseteq E$, then $|C_X| = q^{mg}$, for some $g \in \mathbb{N}$, since C_X is multilinear. But $|C_X| = (q^m)^g = |F|^q$. But then

$$rk(X) = log_{|F|}(|C_X|) = log_{|F|}(|F|^g) = g \in \mathbb{N}.$$

Corollary 83 *Linear codes and affine codes are almost affine codes.*

Proof. *Linear codes are multilinear codes, and multilinear codes are almost affine codes. Since $C = C' + \bar{w}$, for a linear code C' and $|C_X| = |C'_X|$, for all X, since C' is linear, it is almost affine and then C is almost affine.*

Theorem 84 *Let $C \subseteq F^E$ be an almost affine code and r be the function in sense of Definition 81. Then we can build a matroid M(C) over E by using r as a rank function of a matroid.*

Proof. *We have to check that all $X \subseteq E$ and all $i, j \in E$ satisfy the following axioms for rank function of matriod:*
(R_1) $r(\emptyset) = 0$;
(R_2) $r(X) \leqslant r(X \cup \{i\}) \leqslant r(X) + 1$;
(R_3) *if* $r(X \cup \{i\}) = r(X \cup \{j\}) = r(X)$, *then* $r(X \cup \{i, j\}) = r(X)$.
The first axiom follows from Definition 78. Also it is quite obvious that $|C_X| \leqslant |C_{X \cup \{i\}}| \leqslant |C_X| \cdot |F|$, which gives us R_2. And if each of two coordinates i, j fails to increase a cardinality of the projection, their combination fails to do so as well.

Example 85 *Let C be a linear code. Then it has a generator matrix G. Let $X \subseteq E$, let G_X be a matrix where we have deleted all the columns of $E \setminus X$. Then $r(X) = log_{|F|}|C_X| = rk(G_X)$. This means that we have:*

$$M(C) = M[G] = M_{C^\perp} = M^*_C.$$

Example 86 *Let C be 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*

In our case $|F| = 4$. And all we need to see to prove that C is an almost affine code is that $|C_X|$ is a power of 4, for all $X \subseteq \{0, 1, 2, 3\}$. If X has only one element $|C_X| = 4$. If X has two elements it is easy to see that $|C_X| = 16$ (after deleting one position of all codewords we still have 16 different codewords). So C is an almost affine code but it is not equivalent to a linear code, and not even to a multilinear code.

Quasi-Uniform codes.

For a code $C \subseteq F^n$ and for a finite alphabet F, we have that

$$P(Z = x) = \begin{cases} \frac{1}{|C|} & \text{, if } x \in C \\ 0 & \text{, if } x \in F^n \backslash C. \end{cases}$$

Another words, if we pick a codeword Z from C, then all choices of codeword have the same probability. Assume that we project the code C down to $A \subseteq E$ by using ρ_A, and pick the projection Z_A of an arbitrary codeword Z. We say that C is quasi-uniform code if

$$P(Z_A = y) = \begin{cases} \frac{1}{|\rho_A(C)|} & \text{, if } y \in \rho_A(C) \\ 0 & \text{, otherwise.} \end{cases}$$

Theorem 87 *Almost affine codes are quasi-uniform.*

Proof. By Proposition 2 of [10], the number of codewords with projection $\underline{y}$ *is* $q^{r(E)-r(A)}$*, and hence*

$$P(Z_A = \underline{y}) = \frac{q^{r(E)-r(A)}}{|C|} = \frac{q^{r(E)-r(A)}}{q^{r(E)}} = q^{-r(A)}$$

for all $y \in \rho_A(C)$*, and 0 otherwise. So it satisfies the definition above.*

The binary and ternary case.

The following text is taken from [10], p.187-188.
It can be shown that a subset $A \subseteq \mathbb{F}_2^n$ is an affine subspace if and only if $x + y + z \in A$ for all $x, y, z \in A$. In particular, the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ are quadruplets $\{x, y, z, u\}$ with $x + y + z + u = 0$.

Proposition 88 *All binary almost affine codes are affine.*

Proof. For any almost affine code $C \subseteq \mathbb{F}_2^n$*, we have to show that each triplet* $\{x, y, z\} \subset C$ *is contained in a 2-dimensional affine subcode* $\{x, y, z, u\}$ *of* C*. Lets apply the induction method with respect to* $dimC$*. If* $dimC \leqslant 1$*, there is nothing to prove. Suppose that the proposition holds for all binary almost affine codes of dimension* $< k$*, and let* $dimC = k$*. Choose a base* $B \subseteq E$ *for the matroid* $M(C)$*. For any three distinct* $x, y, z \in C$ *exists a unique codeword u s. t.* $x_B + y_B + z_B + u_B = 0$*. We claim that* $x + y + z + u = 0$*. If not, there is an* $i \in \bar{B}$ *with* $x_i + y_i + z_i + u_i = 1$*. Without loss of generality, we may assume that* $u_i = x_i = y_i$ *and* $u_i \neq z_i$*. Then the subcode*

$$T = \{c \in C | c_i = u_i\}$$

of C *has dimension k-1. By the induction hypothesis, a codeword* $v \in T$ *exists such that* $x + y + v + u = 0$*. This implies that* $x_B + y_B + v_B + u_B = 0$*. Hence* $v_B = z_B, v = z$ *and* $x + y + z + u = 0$*.*

For the ternary case (alphabet $\mathbb{F}_3$) one sees that a subset $S \subseteq \mathbb{F}_3^n$ is affine subspace if and only if $-x - y \in S$ for all $x, y \in S$, and the 1-dimensional affine subspaces are the triplets $\{x, y, z\}$ with x+y+z=0. Using this, and an argument similar to the proof of Proposition 88, are concludes

Proposition 89 *All ternary almost affine codes are affine.*

5 Demi-matroids and flags of almost affine codes

We will now give 2 different definitions of a demi-matroid, a tool that will be used to study flags of almost affine codes.

Definition 90 *A demi-matroid is a pair (E, r) where E is a finite set, called the ground set, and r is a function on the power set of E into $\mathbb{N}$ satisfying the following axioms:*

(R_1) $r(\emptyset) = 0$,

(R_2) $r(X) \leqslant r(X \cup \{x\}) \leqslant r(X) + 1$.

In other word, a demi-matroid is a matroid without the following axiom

(R_3) if $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$, then $r(X \cup \{x, y\}) = r(X)$.

Thus a matroid is automatically a demi-matroid. On the other hand we have the following definition:

Definition 91 *A demi-matroid is a triple (E,s,t) where E is a finite set, and r, s are two functions on the power set of E into $\mathbb{N}$ satisfying the following two conditions for all subsets $X \subseteq Y \subseteq E$:*

(R) $0 \leqslant s(X) \leqslant s(Y) \leqslant |Y|$ *and* $0 \leqslant t(X) \leqslant t(Y) \leqslant |Y|$*;*

(D) $|E - X| - s(E - X) = t(E) - t(X)$.

Proposition 92 *The condition (D) is equivalent to the following condition:*

$$(D') \ |E - X| - t(E - X) = s(E) - s(X).$$

Proof. Use (D) on $E - X$*:*

$$|E - (E - X)| - s(E - (E - X)) = t(E) - t(E - X)$$

so

$$|X| - s(X) = t(E) - t(E - X)$$

note that $s(\emptyset) = t(\emptyset) = 0$ *by (R) and use (D) on* $\emptyset$ *we have:*

$$|E| - s(E) = t(E)$$

putting this expression for t(E) into the previous equality gives us:

$$|X| - s(X) = |E| - s(E) - t(E - X).$$

Thus

$$|E| - |X| - t(E - X) = s(E) - s(X),$$

hence we obtain

$$(D')\ |E - X| - t(E - X) = s(E) - s(X).$$

To obtain (D) from (D') we just interchange the roles of s and t in the proof we just gave for the fact (D') follows from (R) and (D).

We gave two different definitions, since they define the same object they are supposed to be equivalent. We now prove this.

Proposition 93 *Definitions 90 and 91 are equivalent.*

Proof. Firstly we obtain Definition 90 from Definition 91, replace $r = s$ and just forget about t. (R) with $X = Y = \emptyset$ gives us:

$$0 \leqslant r(\emptyset) \leqslant r(\emptyset) \leqslant |\emptyset| = 0,$$

so $r(\emptyset) = 0$ which is (R_1). From (R) with $X = X$, and $Y = X \cup \{x\}$ we get $r(X) \leqslant r(X \cup \{x\})$. And the last inequation to compelete is:

$$r(X \cup \{x\} \leqslant r(X) + 1,$$

i. e.

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

By (D') we have

$$s(X) = s(E) - |E - X| + t(E - X),$$

by (R) we have

$$t(E - X) \geqslant t(E - \{X \cup \{x\}\}).$$

Hence:

$$s(X) \geqslant s(E) - |E - (X \cup \{x\})| - 1 + t(E - (X \cup \{x\})).$$

More over, by D' applied to $X \cup \{x\}$ we have:

$$s(E) - |E - (X \cup \{\boldsymbol{x})| - 1 + t(E - (X \cup \{x\})) = s(X \cup \{x\}) - 1.$$

Hence $s(X) \geqslant s(X \cup \{x\}) - 1$, and therefore

$$r(X \cup \{x\}) = s(X \cup \{x\}) \leqslant s(X) + 1 = r(X) + 1.$$

Now we will prove that Definition 91 can be obtained from Definition 90, i. e. start with (R_1) *and* (R_2) *we will prove* (R) *and* (D).
First we define: $s = r$. *Then we define* t *the same way as we define* $r*$ *when* r *is the rank function of a matroid. In other words:*

$$t(X) := |X| + s(E - X) - s(E), \tag{1}$$

or

$$t(X) = |X| + r(E - X) - r(E),$$

First we prove (D). Rewriting (D), it is:

$$t(X) = t(E) + s(E - X) - |E - X|.$$

Comparing the two expressions, we have to prove:

$$|X| - s(E) = t(E) - |E - X|,$$

hence it is enough to prove:

$$t(E) = |E| - s(E).$$

The equality (1) gives us:

$$t(E) = |E| + s(\emptyset) - s(E),$$

but $s(\emptyset) = 0$ *by* (R_1), *so* $t(E) = |E| - s(E)$ *holds.*

Now we prove (R). There are six inequalities with $X \subseteq Y$:

$$\begin{array}{c} 0 \leqslant s(X) \leqslant s(Y) \leqslant |Y| \\ 0 \leqslant t(X) \leqslant t(Y) \leqslant |Y|. \end{array}$$

Let us prove the first three in the order that they appear.

$$0 \leqslant s(X)$$

this holds since $s(= r)$ *defined as a function into* $\mathbb{N}$.

The second inequality. Let $Y = X \cup \{y_1, \cdots, y_m\}$, *then*

$$s(X) = r(X) \leqslant r(X \cup \{y_1\}) \leqslant r((X \cup \{y_1\}) \cup \{y_2\}) \leqslant \cdots \leqslant r((X \cup \{y_1, \cdots, y_{m-1}\}) \cup \{y_m\}) = \\ = r(Y) = s(Y).$$

And the last inequality related to s. *Let* $Y = \{y_1, \cdots, y_m\}$, *also*

$$Y = \{\emptyset \cup \{y_1\} \cup \cdots \cup \{y_m\}\},$$

apply (R_2) *to each* y_i *and notice that* r *can be increased by 0 or 1 each time we add an element, we have:*

$$s(Y) \leqslant s(\emptyset) + m = r(\emptyset) + m = 0 + m = |Y|.$$

Now we prove the last three inequalities. We start with $t(Y) \leqslant |Y|$ *or* $t(Y) - |Y| \leqslant 0$. *But:*

$$t(Y) = |Y| + s(E - Y) - s(E)$$

so

$$t(Y) - |Y| = s(E - Y) - s(E).$$

And $s(E - Y) - s(E) \leqslant 0$ *since* $E - Y \subseteq E$ *and by the already proven inequality for* s.
Let us prove that if $X \subseteq Y \Rightarrow t(X) \leqslant t(Y)$.

$$\begin{gathered} t(X) - t(Y) = |X| + s(E - X) - s(E) - |Y| - s(E - Y) + s(E) = \\ = |X| - |Y| - s(E - Y) + s(E - X) \end{gathered}$$

i.e. we need to prove:

$$s(E - X) - s(E - Y) \leqslant |Y| - |X|.$$

We assume that $Y = X \cup \{y_1, \cdots, y_m\}$, *otherwise* $(X = Y)$ *it is trivial.*

$$\begin{gathered} (E - X) = (E - Y) \cup \{y_1, \cdots, y_m\} \\ s(E - X) \leqslant s(E - Y) + m = s(E - Y) + |Y| - |X|. \end{gathered}$$

And the last inequality to prove is $0 \leqslant t(X)$, *or*

$$\begin{gathered} 0 \leqslant |X| + s(E - X) - s(E) \\ s(E) \leqslant s(E - X) + |X|. \end{gathered}$$

Assume $X = \{x_1, \cdots, x_n\}$, *then*

$$\begin{gathered} E = (E - X) \cup \{x_1, \cdots, x_n\} \\ s(E) \leqslant s(E - X) + n = s(E - X) + |X|. \end{gathered}$$

Pairs and flags

The material in this section has been inspired by [7]

Definition 94 *Let* C *be a k-dimensional almost q-ary affine code. For any* $\underline{w} \in C$ *and* $X \subseteq C$, *we define*

$$C(X, \underline{w}) = \{\underline{c} \in C \mid \underline{c}_X = \underline{w}_X\}.$$

Example 95 *Let us take the code* C *from Example 86. Let* $w = 123$ *and* $X = \{2\}$. *Then* $C(X, w) = \{022, 123, 220, 321\}$

Proposition 96 *Let* C *be a q-ary almost affine code over an alphabet E, with rank function* r_C. *Let* $X \subseteq E$. *Then* $C(X, \underline{w})$ *is an almost affine code, and*

$$|C(X, \underline{w})| = q^{r_C(E) - r_C(X)}.$$

Proof. *See the proofs of Proposition 2 and Corollary 1 in [10].*

Lemma 97 *Let C be an almost affine code, $w \in C$. Let $X \subset E$ and $x \in E - X$. Then*

$$r(X \cup \{x\}) = r(X) \Leftrightarrow C(X \cup \{x\}, w) = C(X, w).$$

Proof. *We know that $C(X \cup \{x\}, w) \subseteq C(X, w)$, so by using Proposition 96 we have:*

$$C(X \cup \{x\}, w) = C(X, w) \Leftrightarrow |C(X \cup \{x\}, w)| = |C(X, w)| \Leftrightarrow q^{r_C(E) - r_C(X \cup \{x\})} = q^{r_C(E) - r_C(X)} \Leftrightarrow r(X \cup \{x\}) = r(X).$$

Theorem 98 *Let $D \subseteq C$ be a pair of two almost affine codes over an alphabet E. Then $(E, \rho = r_C - r_D)$ is a demi-matroid.*

Proof. *Firstly we prove (R_1):*

$$\rho(\emptyset) = r_C(\emptyset) - r_D(\emptyset) = 0.$$

Now we prove (R_2). In the case where $x \in X$ (R_2) reduces to

$$\rho(X) = \rho(X) < \rho(X) + 1,$$

which obviously holds. Let us treat the case where $x \notin X$. Since r_C and r_D are both rank functions we have four cases:

$$r_C(X \cup \{x\}) = r_C(X) \text{ or } r_C(X) + 1$$
$$\text{and}$$
$$r_D(X \cup \{x\}) = r_D(X) \text{ or } r_D(X) + 1$$

Case number one. $r_C(X \cup \{x\}) = r_C(X)$ and $r_D(X \cup \{x\}) = r_D(X)$. Then we have:

$$\rho(X \cup \{x\}) = r_C(X) - r_D(X) = \rho(X),$$

so inequality for (R_2), which is $\rho(X) \leqslant \rho(X \cup \{x\}) \leqslant \rho(X) + 1$, holds.
Case number two. $r_C(X \cup \{x\}) = r_C(X) + 1$ and $r_D(X \cup \{x\}) = r_D(X)$. Then:

$$\rho(X \cup \{x\}) = r_C(X) + 1 - r_D(X) = \rho(X) + 1,$$

this is also satisfies (R_2).
Case number three. $r_C(X \cup \{x\}) = r_C(X)$ and $r_D(X \cup \{x\}) = r_D(X) + 1$. Then:

$$\rho(X \cup \{x\}) = r_C(X) - r_D(X) - 1 = \rho(X) - 1$$

This case does not satisfy (R_2).
Case number four. $r_C(X \cup \{x\}) = r_C(X) + 1$ and $r_D(X \cup \{x\}) = r_D(X) + 1$. Then:

$$\rho(X \cup \{x\}) = r_C(X) + 1 - r_D(X) - 1 = \rho(X),$$

which is O.K.
Now we will prove that the case number three never happens. We show that from $r_C(X \cup \{x\}) = r_C(X)$ follows $r_D(X \cup \{x\}) = r_D(X)$. Let $w \in D \subset C$, by using Lemma 97 we have:

$$\begin{gathered} r_C(X \cup \{x\}) = r_C(X) \Leftrightarrow C(X \cup \{x\}, w) = C(X, w) \\ \Rightarrow D(X \cup \{x\}, w) = D \cap C(X \cup \{x\}, w) = D \cap C(X, w) = D(X, w) \\ \Rightarrow r_D(X \cup \{x\}) = r_D(X). \end{gathered}$$

Hence the case number three is not a case anymore, and (E, ρ) is a demi-matroid.

Definition 99 *Let (E, r) be a demi-matroid, define*

$$\mathcal{E}' = \{(X, x),\, r(X) = r(X - \{x\})\}.$$

For two matroids $M_1 = (E, r_1)$ and $M_2 = (E, r_2)$ we say that $M_2 \leqslant M_1$ if $\mathcal{I}_2 \subseteq \mathcal{I}_1$.

Lemma 100 *$M_2 \leqslant M_1 \Leftrightarrow r_2 \leqslant r_1$.*

Proof. First we assume that the right hand side holds. We have $r_2 \leqslant r_1$, let $X \subseteq E$, assume

$$X \in \mathcal{I}_2 \Rightarrow r_2(X) = |X|,$$

and then, by the given and the matroid's axiom for a rank function we have:

$$|X| \geqslant r_1(X) \geqslant r_2(X) = |X|,$$

so $r_1(X) = |X| \Rightarrow X \in \mathcal{I}_1$ which means $\mathcal{I}_2 \subseteq \mathcal{I}_1$. Now we start with $\mathcal{I}_2 \subseteq \mathcal{I}_1$. Let $X \subseteq E$ and $r_2(X) = r$. Then

$$r = \{max|Y| \mid Y \in \mathcal{I}_2, Y \subseteq X\}.$$

But $Y \in \mathcal{I}_2 \subseteq \mathcal{I}_1$, so $Y \in \mathcal{I}_1$ also. Then

$$r_1(X) = \{max|Y| \mid Y \in \mathcal{I}_1\} \geqslant r = r_2(X),$$

so $r_2 \leqslant r_1$.

Since there is no such a $\mathcal{I}$ for a demi-matroids, we define $M_2 \leqslant M_1$ if $r_2 \leqslant r_1$.

Definition 101 *We say that $\{M_i$, for $i = 1, \cdots, m\}$ is a flag of demi-matroid if*

$$M_m \leqslant M_{m-1} \leqslant \cdots \leqslant M_2 \leqslant M_1.$$

In particular $\{M_1$ and $M_2\}$ is a pair of demi-matroids if $M_2 \leqslant M_1$.

The next two theorems will be given without proofs. The proofs can be found in [7], p 10-11.

Theorem 102 *Let $M_2 \leqslant M_1$ be a pair of demi-matroids on the ground set E with the rank functions r_1 and r_2 respectively. Then $(E, \rho = r_1 - r_2)$ is a demi-matroid if and only if $\mathcal{E}'_1 \subset \mathcal{E}'_2$.*

Theorem 103 *Let* $\{(E, r_i)$ *for* $1 \leqslant i \leqslant n\}$ *be a flag of demi-matroids. Then* (E, ρ) *with* $\rho = \sum_{i=1}^{n}(-1)^{i+1}r_i$ *is a demi-matroid if and only if* $\mathcal{E}'_i \subset \mathcal{E}'_{i+1}$ *for all* i.

Corollary 104 *Let* $C_n \subset \cdots \subset C_1$ *be a flag of almost affine codes. Then* (E, ρ) *with* $\rho = \sum_{i=1}^{n}(-1)^{i+1}r_i$ *is a demi-matroid.*

Proof. According to Theorem 98, for every $1 \leqslant j < n$, *the pair* $C_{j+1} \subset C_j$ *of almost affine code gives rise to a demi-matroid. Since every affine code is a matroid and every matroid is a demi-matroid, Theorem 102 gives us* $\mathcal{E}'_j \subset \mathcal{E}'_{j+1}$ *for all* $j \in \overline{1, n-1}$. *Which means that conditions for Theorem 103 are met and* (E, ρ) *with* $\rho = \sum_{i=1}^{n}(-1)^{i+1}r_i$ *is a demi-matroid.*

Proposition 105 *If* $M_1 = (E, s_1, t_1)$, $M_2 = (E, s_2, t_2)$ *and* $(E, s_1 - s_2)$ *are demi-matroids and* $M_2 \leqslant M_1$, *then* $(E, t_2 - t_1)$ *is a demi-matroid also.*

Proof. Let $\rho := s_1 - s_2$. *For* $X \subseteq E$, *recall that*

$$t(X) = |X| + s(E - X) - s(E).$$

So is $t_1 \leqslant t_2$*? Let us find their difference:*

$$\begin{gathered} t_2(X) - t_1(X) = [|X| + s_2(E - X) - s_2(E)] - [|X| + s_1(E - X) - s_1(E)] = \\ = [s_1(E) - s_2(E)] - [s_1(E - X) - s_2(E - X)] = (s_1 - s_2)(E) - (s_1 - s_2)(E - X) = \\ = \rho(E) - \rho(E - X). \end{gathered}$$

Since ρ *is a rank function of a demi-matroid and* $E - X \subseteq E$, *the last subtraction gives us non negative result, so* $t_1 \leqslant t_2$. *Now we prove that* $\eta := t_2 - t_1$ *is a demi-matroid. First of all, it is clear that* η *maps* $\{X \mid X \subseteq E\}$ *into* $\mathbb{N}$. *Now we prove* (R_1):

$$\eta(\emptyset) = t_2(\emptyset) - t_1(\emptyset) = 0 - 0 = 0.$$

Now we prove the first inequality of (R_2)

$$\eta(X) \leqslant \eta(X \cup \{x\})$$

it is equivalent to

$$\begin{gathered} \rho(E) - \rho(E - X) \leqslant \rho(E) - \rho(E - (X \cup \{x\})) \\ \rho(E - (X \cup \{x\})) \leqslant \rho(E - X). \end{gathered}$$

But this is correct, since ρ *is a demi-matroid, and* $E - (X \cup \{x\}) \subseteq E - X$. *And the last inequality to be proven is*

$$\begin{gathered} \eta(X \cup \{\boldsymbol{x}\}) \leqslant \eta(X) + 1 \\ or \\ \eta(X \cup \{\boldsymbol{x}\}) - \eta(X) \leqslant 1. \end{gathered}$$

Let us write the left part in terms of ρ:

$$\begin{gathered}\rho(E)-\rho(E-(X\cup\{x\}))-[\rho(E)-\rho(E-X)]=\\ =\rho(E-X)-\rho(E-(X\cup\{x\})).\end{gathered}$$

But this at most 1, since ρ is a demi-matroid and the arguments of ρ have only one element x as a difference. So, we conclude that $(E, t_2 - t_1)$ is a demi-matroid.

Remark 106 *If we have $M_1 = (E, s_1, t_1)$, $M_2 = (E, s_2, t_2)$ and $M_2 \leqslant M_1$ and $(E, s_1 - s_2)$ be a demi-matroid, its also means that $M_2^* \geqslant M_1^*$ since $t_1 \leqslant t_2$.*

Notice that we can extend the previous theorem and remark naturally to a flag of demi-matroids by applying its to every pair of demi-matroids.

Theorem 107 *If $M_m \leqslant \cdots \leqslant M_2 \leqslant M_1$ is a flag of demi-matroids, and $(E, s_i - s_{i+1})$ is a demi-matroid for each i, then $(E, t_m - t_{m-1} + \cdots + (-1)^{m+1}t_1)$ is a demi-matroid.*

Proof. *As we know, $(E, t_{i+1} - t_i)$ for each $i \in \overline{1, m-1}$ is a demi-matroid, by Remark 106 we have $M_1^* \leqslant \cdots \leqslant M_{m-1}^* \leqslant M_m^*$. Now we can apply Theorem 102, which gives us $\mathcal{E}'_{i+1} \subset \mathcal{E}'_i$ for all i. Which means that canditions for Theorem 103 are met, but we need to 'reverse' the summ for ρ to match it completely. So we have (E, ρ) is a demi-matroid with $\rho = \sum_{i=1}^{m}(-1)^{i+1}t_{m-i+1}$.*

Corollary 108 *If $C_m \subset \cdots \subset C_1$ is a flag of almost affine codes with rank functions $r_m \leqslant \cdots \leqslant r_1$. Then $(E, r_m^* - r_{m-1}^* + \cdots + (-1)^{m+1}r_1^*)$ is a demi-matroid.*

Proof. *According to Theorem 98, for every $1 \leqslant j < n$, the pair $C_{j+1} \subset C_j$ of almost affine code gives rise to a demi-matroid. And then we apply Theorem 107.*

Definition 109 *Let (E, s) be a demi-matroid. Then the supplement dual is $(E, \bar{s})$, where $\bar{s}(X) = s(E) - s(E - X)$, for all $X \subseteq E$.*

Proposition 110 *Let (E, s) be a demi-matroid. Then $\bar{\bar{s}} = s$, and $(\bar{s})^* = \overline{s^*}$.*

Proof. *For all $X \subseteq E$ we have:*

$$\bar{\bar{s}}(X)=\bar{s}(E)-\bar{s}(E-X)=s(E)-s(\emptyset)-s(E)+s(X)=s(X).$$

Recall that $s^*(X) = |X| + s(E - X) - s(E)$. Now we take

$$\begin{gathered}\overline{s^*}(X)=s^*(E)-s^*(E-X)=|E|+s(\emptyset)-s(E)-[|S|-|X|+s(X)-s(E)]=\\ =|X|-s(X)\end{gathered}$$

And at the same time we have:

$$\begin{gathered}(\bar{s})^*(X)=|X|+\bar{s}(E-X)-\bar{s}(E)=|X|+s(E)+s(X)-s(E)+s(\emptyset)=\\ =|X|-s(X).\end{gathered}$$

Theorem 111 *Let $C_m \subset \cdots \subset C_1$ be a flag of almost affine codes with rank functions $r_m \leqslant \cdots \leqslant r_1$. And $\rho = r_1 - r_2 + \cdots + (-1)^{m+1} r_m$ and $\eta := r_m^* - r_{m-1}^* + \cdots + (-1)^{m+1} r^*$. Then $\eta = \rho^*$ if m is odd and $\eta = \bar{\rho}$ if m is even.*

Proof. $\eta_1 = \rho_1^*$, *and for all n we need to prove*

$$(**) \begin{cases} \eta_{2n} = \bar{\rho_{2n}}, & \textit{and} \\ \eta_{2n+1} = (\rho_{2n+1})^* & \textit{for all } n \geqslant 1. \end{cases}$$

Let us prove it for $n = 1$. For all $X \subseteq E$ we have

$$\eta_2 = r_2^* - r_1^* = |X| + r_2(E - X) - r_2(E) - [|X| + r_1(E - X) - r_1(E)] = \\ = (r_1 - r_2)(E) - (r_1 - r_2)(E - X) = \bar{\rho}_2(X).$$

And

$$\begin{gathered} \eta_3 = r_3^* - r_2^* + r_1^* = |X| + r_3(E - X) - r_3(E) \\ -|X| - r_2(E - X) + r_2(E) + \\ +|X| + r_1(E - X) - r_1(E) = \\ = |X| + (r_1 - r_2 + r_3)(E - X) - (r_1 - r_2 + r_3)(E) = \rho_3^*(X). \end{gathered}$$

Assume $(**)$ is true for $i \leqslant n$, so $\eta_{2n} = \bar{\rho_{2n}}$, and $\eta_{2n+1} = (\rho_{2n+1})^*$. Let us prove $(**)$ for $n + 1$, i.e.

$$\begin{gathered} \eta_{2n+2} = \bar{\rho_{2n+2}} \\ \textit{and} \\ \eta_{2n+3} = (\rho_{2n+3})^*. \end{gathered}$$

By assumption, we have $\eta_{2n+1} = (\rho_{2n+1})^*$, so

$$\eta_{2n+2} = r_{2n+2}^* - (\rho_{2n+1})^* = |X| + r_{2n+2}(E - X) - r_{2n+2}(E) - [|X| + \rho_{2n+1}(E - X) - \rho_{2n+1}(E)] = \\ = (\rho_{2n+1} - r_{2n+2})(E) - (\rho_{2n+1} - r_{2n+2})(E - X) = \bar{\rho_{2n+2}}(X).$$

Now we have $\eta_{2n+2} = \bar{\rho_{2n+2}}$, let us add r_{2n+3}^* to η_{2n+2} :

$$\eta_{2n+3} = r_{2n+3}^* - \bar{\rho_{2n+2}} = |X| + r_{2n+3}(E - X) - r_{2n+3}(E) - [\rho_{2n+2}(E) - \rho_{2n+2}(E - X)] = \\ = |X| + (\rho_{2n+2} + r_{2n+3})(E - X) - (\rho_{2n+2} + r_{2n+3})(E) = (\rho_{2n+3})^*(X).$$

Hence, all conditions for induction are met and $(**)$ is proven.

Remark 112 *Since it is well known (see [2] and [1]) that $(E, \bar{s}, \bar{t})$ and (E, t, s) are demi-matroids if (E, s, t) is a demi-matroid, Theorem 111 gives another proof of Corollary 108.*

Remark 113 *The two important results Corollary 104 and Theorem 111 are given in [2] also, but only for linear codes (see Theorem 9 and Theorem 10 respectively). It is clear that the proof of Theorem 9 in [2] only applied for linear codes, and we have a completely new proof for almost affine codes. The proof of Theorem 10 in [1], hovever, could have been used also for almost affine codes in general, but the proof given above is different.*

6 Multilinear codes and generalized Hamming weights

Definition 114 *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 $X \subset E = \{1, 2, \cdots, n\}$.*

Example 115 *Let us take the following matrix over $\mathbb{F}_{11}$ and $(\mathbb{F}_{11})^2 = F$*

$$\begin{pmatrix} 1\,1 & 1\,1 & 1\,1 & 1\,1 \\ 1\,2 & 3\,4 & 5\,6 & 7\,8 \\ 1\,2^2 & 3^2 4^2 & 5^2 6^2 & 7^2 8^2 \\ 1\,2^3 & 3^3 4^3 & 5^3 6^3 & 7^3 8^3 \end{pmatrix}$$

In this case we have $n = 4$ and $m = 2$. Also such a matrix is known as a $[4\times 8]$ Vandermonde matrix. And we also know that for such a Vandermonde matrix we have $rk_{\mathbb{F}_{11}}(C_Y) = min\{|Y|, 4\}$, for each $Y \subset E = \{1, 2, \cdots, 8\}$. It is easy to see that for each $X \subset E = \{1, 2, 3, 4\}$, $rk_{\mathbb{F}_{11}}(C_X)$ will be either two or four which is divisible by $m = 2$. So, the code with the given matrix as its generator matrix is a multilinear code.

Let C be such a multilinear code for a given m and n, and let G be a generator matrix for C over $\mathbb{F}_q$. The set of column positions of G are $1_m \bigcup 2_m \bigcup \cdots \bigcup n_m$, where

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

for any natural number $a \leqslant n$.

For a given multilinear code, we denote it by C_1 over $\mathbb{F}_q$ and by C_2 over F. These codes have two rank functions r_1 and r_2 which leads us to two matroids M_1 and M_2.

By using the notation for the columns of G we have $r_1(X_m) = dim_{\mathbb{F}_q} C_X = m dim_F C_X = mr_2(X)$, for any $X \subset E$.

Let H be a parity check matrix of C_1 (over $\mathbb{F}_q$). The column rank function of H is r_1^* which is the rank of the matroid dual to M_1. For any $X \in E$ we have:

$$\begin{aligned} r_1^*(X_m) &= |X_m| - r_1(E_m) + r_1(E_m - X_m) \\ &= |X_m| - r_1(E_m) + r_1((E - X)_m) \\ &= m|X| - mr_2(E) + mr_2(E - X) \\ &= mr_2^*(X). \end{aligned}$$

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 successive symbols in each row of H as an element of $F = \mathbb{F}_q^m$. The following result is explained also in [6]

Proposition 116 *$C_1^{\perp}$ code is a multilinear code.*

Proof. For each $X \in E$ we have:

$$dim_{\mathbb{F}_q}(C^{\perp})_X = r_1^*(X_m) = mr_2^*(X)$$

which is divisible by m, since $r_2^*(X)$ is natural number. So $C_1^{\perp}$ satisfies Definition 114.

Taking the rank of X over F, we get $r_2^*(X)$. Hence $C_1^{\perp}$ is a natural dual code also over F, we may define it as C_2^*.

Notice that all the following:

$$M(C_1) = (\{1, 2, \cdots, mn\}, r_1),$$
$$M(C_1^*) = (\{1, 2, \cdots, mn\}, r_1^*),$$
$$M(C_2) = (\{1, 2, \cdots, n\}, r_2),$$
$$M(C_2^*) = (\{1, 2, \cdots, n\}, r_2^*)$$

are matroids. Since every code we used is at least an almost affine code and, according to Theorem 84, it gives us a matroid, build over ground set whose cardinality is the length of the code and the associated rank function.

In the very beginning of this paper we defined what the support of code word is for linear codes, now we extend this definition for almost affine codes.

Definition 117 *Let $c \in C$, and $w \in C$, then*

$$Supp(w, c) = \{i \mid w_i \neq c_i\}.$$

If $D \subseteq C$, then

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

Since the support of a set of codewords is independent of the choice of c (it will be proven next), we call it $Supp(D)$.

Lemma 118 *Let D be an almost affine code, and $c, d \in D$. Then we have*

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

Proof. Assume, there is an i which belongs to $\bigcup_{w \in D} Supp(w, c)$ and does not belong to $\bigcup_{w \in D} Supp(w, d)$. Now we look at c_i and d_i, they are not equal since $i \notin \bigcup_{w \in D} Supp(w, d)$. But at the same time we have found an element i which we have to add to $\bigcup_{w \in D} Supp(w, d)$. By symmetry, we get equality.

Now we will give two definitions of Generalized Hamming weights for almost affine codes.

Definition 119 *Let C be an almost affine code aver an alphabet F. C has an associated matroid M, with rank function r. Then $d_i(C)$, for $i = 1, \cdots, rank(C)$ are:*

$$d_i(C) = d_i(M_C^*) = Min\{|X| \mid |X| - r^*(X) = i\}.$$

Definition 120 *Let C be an almost affine code aver an alphabet F. C has an associated matroid M, with rank function r. Then $d_i(C)$, for $i = 1, \cdots, rank(C)$ are:*

$$d_i(C) = Min\{|Supp(D)| \mid D \text{ is an almost affine subcode of dimensional } i\}.$$

Since we have two definitions of the same,the following theorem is natural.

Theorem 121 *Definition 119 and Definition 120 are equivalent.*

Proof. See the proof of Theorem 1 in [6].

Example 122 *Let us find the Hamming weights of Example 115 of* C_1 *over* $\mathbb{F}_{11}$*. To do so we will use another property of a Vandermonde matrix it is well known that it is an MDS code. Then we have:*

$$d_1 = Min\{|X|, |X| - r^*(X) = 1\} = 5;$$

and $d_2 = 6$*,* $d_3 = 7$*,* $d_4 = 8$*. By the property of MDS-codes we know that the dual of an [n,k] MDS-code is an [n,n-k] MDS-code. So, we also have:* $d_1^* = 5$*,* $d_2^* = 6$*,* $d_3^* = 7$ *and* $d_4^* = 8$*.*

Now we will find the Hamming weights of the code based on the same matrix but consider it over $(\mathbb{F}_{11})^2 = F$*. By notation above this code is called* C_2*. Since* $length(C_2) - dim_F(C_2) = 4 - 2 = 2$*, we need to find* D_1 *and* D_2*. For* $i = 1, 2$*, we have:*

$$D_i = min\{|X|, |X| - r_2^*(X) = i\}.$$

Also we know that

$$r_2^*(X) = \tfrac{1}{2} r_1^*(X_m) = \tfrac{1}{2} Min\{|X_m|, 4\}$$

All possible values for X *are*
$\{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$.
And we can see that only $|X| = 3$ *gives us* D_1 *and* $|X| = 4$ *gives us* D_2*. So* $D_1 = 3, D_2 = 4$*.*

Theorem 123 *Wei duality holds for the codes* C_2 *and* C_2^**.*

Proof. Since Wei duality holds between the matroid $M(C_2) = (\{1, 2, \cdots, n\}, r_2)$ *and its dual matroid* $M(C_2^*) = (\{1, 2, \cdots, n\}, r_2)$ *it holds between* C_2 *and* C_2^**.*

Now we are able to find D_1^* and D_2^* by using the Wei duality theorem.

$$\{D_1, D_2\} \cup \{5 - D_1^*, 5 - D_2^*\} = \{1, 2, 3, 4\}$$

So we have $D_1^* = 3$ and $D_2^* = 4$.

Remark 124 *In the previous examples we see that the matroids* C_2 *and* C_2^* *are the uniform code* $U(2, 4)$ *because we used* $U(4, 8)$ *as the original code, but in general cases it is not so simple.*

Definition 125 *Let* C *be a non-degenerate multi-linear code over F,* $F = (\mathbb{F}_q)^m$ *for the finite field* $\mathbb{F}_q$*. For* $1 \leqslant i \leqslant n$ *we define:* c_i *is the smallest integer* l *such that there exists* l *codewords over F, whose union of supports has cardinality at least i.*

Definition 126 *For a linear [n,k]-code, we define the Singleton defect* $s_i = (n - k + i) - d_i$*, and* $s_i^{\perp} = k + i - d_i^{\perp}$*.*

Remark 127 *For a multi-linear code which is an [mn,nk]-code over* $\mathbb{F}_q$ *we get* $s_j^{\perp} = mk + j - d_j^{\perp}$*.*

Theorem 128 *For a multi-linear code C with $n > k$ we have $c_i \leqslant s^{\perp}_{m(n+1-i)} + 2$ for $1 \leqslant i \leqslant n$, with the convention $s^{\perp}_j = -1$ for $m(n-k)+1 \leqslant j \leqslant mn$.*

Proof. Since C is an almost affine code over F, there exist k columns of G over F, whose rank over $\mathbb{F}_q$ is mk. After a permutation of columns over F, we assume that these correspond to the mk leftmost columns of G over $\mathbb{F}_q$. After row reduction we may assume that G is of the form $[I \mid A]$, where I is an $(mk \times mk)$-identity matrix, and A is an $(mk \times m(n-k))$-matrix over $\mathbb{F}_q$. By taking sum of all vectors of this matrix we obtain a codeword over $\mathbb{F}_q$ with ones on the first mk places. Hence its support over F contains $\{1, \cdots, k\}$.

Now we take t row vectors of G and assume their support over F intersected by $\{k+1, \cdots, n\}$ is a set of cardinality at most i-k-1. By taking zeroes of these rows and their unique representations as linear combinations of the columns in the I-matrix, it can be shown that $t \leqslant s^{\perp}_{m(n+1-i)}$. So to get the cardinality at least i-k it is enough with $t \geqslant s^{\perp}_{m(n+1-i)} + 1$. And with adding the codeword we started with we are guaranteed a support of cardinality i. Hence $c_i \leqslant s^{\perp}_{m(n+1-i)} + 2$.

Corollary 129 *If m=1 we have $c_i \leqslant s^{\perp}_{n+1-i} + 2$ which is classic Kung's result for linear codes.*

Corollary 130 *If m=1, and i=n we have $c_1 \leqslant s^{\perp}_1 + 2 = k - d^{\perp}_1 + 3 = k - d^{\perp} + 3$*
This is a classical result shown in [8].

7 Extended weight polynomials of almost affine codes

In this chapter the main result is a generalization of weight polynomials for almost affine codes.

Let F be an alphabet with cardinality q and $C \subsetneq F^n$ be an almost affine code. Let $Q := q^s$, $F_Q = F^s$, and $C_Q := C^s$.

For $W \in C^s$ we have:

$$W = (w_1, w_2, \cdots, w_s),$$

where $w_i \in C$, for all $i = 1, \cdots, s$. So we have:

$$W = [(c_{11}, \cdots, c_{1n}), (c_{21}, \cdots, c_{2n}), \cdots, (c_{s1}, \cdots, c_{sn})] \in (F^n)^s.$$

Now we will rearrange W in the following way:

$$[(c_{11}, c_{21}, \cdots, c_{s1}), (c_{12}, c_{22}, \cdots, c_{s2}), \cdots, (c_{1n}, c_{2n}, \cdots, c_{sn})] \in (F^s)^n = (F_Q)^n.$$

So, a code C_Q can be viewed as a subcode of $(F_Q)^n$.

Let $X \subseteq E = \{1, 2, \cdots, n\}$. For $C \subseteq F$ and $C_Q \subseteq F_Q$ we have their rank functions: $log_{|F|}|C_X|$ and $log_{|F_Q|}|(C_Q)_X|$. It is easy to see it from the way we rearranged W that $|(C_Q)_X| = |C_X|^s$, so we have:

$$log_{|F_Q|}|(C_Q)_X| = log_{q^s}|C_X|^s = \frac{1}{s}log_q|C_X|^s = \frac{1}{s} \cdot s \cdot log_q|C_X| = log_q|C_X| = log_{|F|}|C_X|.$$

Hence we have the equality between two given rank functions, let us call it r.

Now we see that the matroid $M(C)$ viewed over F is equal to the matroid $M(C_Q)$ viewed over F_Q with the rank function r.

Now we are over F_Q with the code C_Q. Let $\underline{c_Q} \in C_Q$ and $U \subseteq E$ and $r(E) = k$. Then we define

$$S_U(Q) = \{\underline{w} \in C_Q \mid \underline{w}|_U = (c_Q)|_U\}.$$

By Proposition 95 we have that

$$|S_U(Q)| = Q^{k-r(U)}$$

We say that a codeword has weight w if it is different from $\underline{c_Q}$ in exactly w positions. For simplicity, in further notations we will use C instead of C_Q.

Definition 131 *Let $A_{C,j}(Q)$ be a cardinality of the set of code words of C_Q of weight j, for $0 \leqslant j \leqslant n$.*

Theorem 132 $A_{C,n}(Q) = (-1)^n \sum_{X \subseteq E} (-1)^{|X|} \cdot Q^{n^*(X)}$.

Proof. *First we define $S_i(Q) = \{$code words which are equal to $\underline{c_Q}$ in position number $i\}$. Now we have:*

$$A_{C,n}(Q) = |C_Q| - |\bigcup_{i=1}^{n} S_i(Q)|$$

We know that $|C_Q| = Q^k$*, and by using well known principle of inclusion-exclusion we have:*

$$A_{C,n}(Q) = Q^k - \sum_{i=1}^{n} |S_i| + \sum_{1\leqslant i<j\leqslant n} |S_i \cap S_j| -$$

$$\sum_{1\leqslant i<j<k\leqslant n} |S_i \cap S_j \cap S_k| + \cdots + (-1)^n |S_1 \cap S_2 \cap \cdots \cap S_n|.$$

We now have, for $U \subseteq E$ *and* $U \neq \emptyset$*:*

$$S_U(Q) = \cap_{u\in U} S_u(Q).$$

And for $U = \emptyset$ *we define* $S_\emptyset = C_Q$ *which is also very natural. So, by applying this notation to the previous expression we have:*

$$A_{C,n}(Q) = \sum_{|U|=0} |S_U(Q)| - \sum_{|U|=1} |S_U(Q)| + \sum_{|U|=2} |S_U(Q)| - \sum_{|U|=3} |S_U(Q)| + \\ + \cdots + (-1)^n \sum_{|U|=n} |S_U(Q)| =$$

$$= \sum_{U\subseteq E} (-1)^{|U|} \cdot |S_U(Q)| = \sum_{U\subseteq E} (-1)^{|U|} \cdot Q^{k-r(U)}$$

We also have:

$$k - r(U) = r(E) - r(U) = |E - U| - r^*(E - U) = n^*(E - U),$$

since $r^*(E - U) = |E - U| - r(E) + r(U)$.
We conclude:

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

Definition 133 *For* $X \subseteq E$

$$a_{C,X}(Q) = |\{\underline{w} \in C_Q \mid Supp(\underline{w}) = X\}|.$$

It is easy to see that all codewords with support X are in

$$C_Q(E - X, \underline{c}) = \{\underline{w} \in C_Q \mid \underline{w}|_{E-X} = \underline{c}|_{E-X}\},$$

and by Proposition 95 $|C_Q(E - X, \underline{c})| = Q^{k-r(E-X)}$ and it is an almost affine code. Since all points on the $E - X$ positions are fixed we may assume that it is an affine code C_1 on the ground set X.

An almost affine code C_1 has the rank function r_1 which gives us a matroid $M_1 = (X, r_1)$ with its n_1, r_1^* and n_1^* functions. So we have $a_{C,X}(Q)$ is a number of codewords in C_1 with support exactly X. And since X matches the ground set we can apply Theorem 132:

$$a_{C,X}(Q) = (-1)^{|X|} \sum_{U\subseteq X} (-1)^{|U|} \cdot Q^{k-r(E-X)-r_1(U)} = (-1)^{|X|} \sum_{U\subseteq X} (-1)^{|U|} \cdot Q^{n_1^*(U)}.$$

Lemma 134 *For* $U \subseteq X \subseteq E$*, we have* $n_1^*(U) = n^*(U)$.

Proof. We recall that n_1^* *is associated to* $M_1 = (X, r_1)$*, where* r_1 *is the rank function of* $C_Q(E - X, \underline{c}_Q)$ *interpreted as a code on* X*. And we have:*

$$n_1^*(U) = |U| - r_1^*(U) = |U| - (|U| - r_1(X) + r_1(X-U)) = r_1(X) - r_1(X-U) = \\ = k - r(E-X) - r_1(X-U).$$

And for n^* we have:

$$n^*(U) = |U| - r^*(U) = |U| - (|U| - r(E) + r(E-U)) = r(E) - r(E-U) = k - r(E-U).$$

So enough to prove that $r(E-U) = r(E-X) + r_1(X-U)$. The following definitions will help us to see the picture:

$$r \longrightarrow C_Q; \\ r_1 \longrightarrow C_Q(E-X, \underline{c}_Q) := C_1; \\ r_2 \longrightarrow C_{E-U} := C_2.$$

We can see that $r(E-U) = r_2(E-U)$ and $r(E-X) = r_2(E-X)$. Now we work inside C_2. Let $\underline{c}_{2,Q} = (\underline{c}_Q)|_{E-U}$ and $C_2(E-X, \underline{c}_{2,Q}) = \{\underline{w} \in C_2 \mid \underline{w}_{E-X} = \underline{c}_{2,Q}\}$. By using Proposition 96 we have:

$$dim C_2(E-X, \underline{c}_2) = rank(C_2) - r_2(E-X) = r_2(E-U) - r_2(E-X) = \\ = r(E-U) - r(E-X).$$

Hence, it will be enough to prove that $r_1(X-U)$ is also equal to $dim C_2(E-X, \underline{c}_2)$. We have:

$$Q^{r_1(X-U)} = |(C_1)_{X-U}| = |\{\underline{w} \in C_Q \mid \underline{w}_{E-X} = \underline{C}_{QE-X}\}_{X-U}|.$$

And on the other hand we have:

$$Q^{dim C_2(E-X, \underline{c}_2)} = |C_2(E-X, \underline{c}_2)| = |\{\underline{w} \in C_2 \mid \underline{w}_{E-X} = \underline{c}_{2,Q}\}|.$$

But these two are equal since we basically picked a set of codewords and then just cut them in the first case, and we first cut and then picked in the second case.

This Lemma leads us to the following result.

Theorem 135 *For $1 \leqslant m \leqslant n$,*

$$A_{C,m}(Q) = (-1)^m \cdot \textstyle\sum_{|X|=m} \sum_{U \subseteq X} (-1)^{|U|} \cdot Q^{n^*(U)}.$$

Remark 136 *For a code C with length n, any codeword $\overline{c}$ has weight from 0 up to n. So*

$$|C| = \textstyle\sum_{j=0}^{n} A_{C,j}(Q)$$

Definition 137 *Let M be a matroid on $E = \{1, 2, \cdots, n\}$. We define the polynomial $P_{M,j}(Z)$ by letting $P_{M,0}(Z) = 1$ and for $1 \leqslant j \leqslant n$:*

$$P_{M,j}(Z) = (-1)^j \cdot \textstyle\sum_{|X|=j} \sum_{U \subseteq X} (-1)^{|U|} \cdot Z^{n^*(U)}$$

Proposition 138 *$d_i(M) = Min\{j : degP_{M,j} = i\}$.*

Proof. *We know that $d_i(M) = Min\{|U| \mid n^*(U) = i\}$. And from the definition above we see that $degP_{M,j} = n^*(U)$ for some j, X, U with $j = |X| = |U|$, because if $U \subset X$ then replace X by U.*

Example 139 *Let us find all $A_{C,m}$ for the multilinear code C over $(\mathbb{F}_{11})^2$ from Example 115.*

$$A_{C,0} = (-1)^0 \sum_{|X|=0} \sum_{U \subseteq X} (-1)^{|U|} Q^{n^*(U)} = (-1)^0 \sum_{|X|=0} \sum_{U=\emptyset} (-1)^0 Q^{n^*(\emptyset)} = Q^0 = 1;$$

it seems pretty natural since the only codeword taken as an origin has weight 0.

$$A_{C,1} = (-1)^1 \sum_{|X|=1} \sum_{U \subseteq X} (-1)^{|U|} Q^{n^*(U)};$$

in this case all X-es which satisfy the condition $|X| = 1$ are $\{1\}$, $\{2\}$, $\{3\}$ and $\{4\}$. Any of these X-es gives 0, so $A_{C,1} = 0$.

$$A_{C,2} = (-1)^2 \sum_{|X|=2} \sum_{U \subseteq X} (-1)^{|U|} Q^{n^*(U)};$$

in this case all X-es which satisfy the condition $|X| = 2$ are $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$ and $\{3,4\}$. Let us take a closer look at $X = \{1,2\}$. It gives us the set of U-es: $\emptyset, \{1\}, \{2\}, \{1,2\}$ and

$$\sum_{U \subseteq X} (-1)^{|U|} Q^{n^*(U)} = (-1)^0 Q^0 + (-1)^1 Q^0 + (-1)^1 Q^0 + (-1)^2 Q^0 = 1 - 1 - 1 + 1 = 0.$$

The rest of the X-es gives 0 as well, so $A_{C,2} = 0$. For $A_{C,3}$ we have the following set of X-es: $\{1,2,3\}$, $\{1,2,4\}$, $\{1,3,4\}$ and $\{2,3,4\}$. Let us take a closer look at $X = \{1,2,3\}$. It gives us the set of U-es: $\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}$ and $\{1,2,3\}$. And

$$\sum_{U \subseteq X} (-1)^{|U|} Q^{n^*(U)} = (-1)^0 Q^0 + 3(-1)^1 Q^0 + 3(-1)^2 Q^0 + (-1)^3 Q^1 = 1 - Q.$$

This is leading us to $A_{C,3} = 4(Q - 1)$, since we have four such an X and $(-1)^3$ in front of the summ. And the last one $A_{C,4}$ gives us the only one possible $X = \{1,2,3,4\}$. And the set of U-es has the following structure: $\emptyset$, $4 \cdot \{a\}$, $6 \cdot \{a,b\}$, $4 \cdot \{a,b,c\}$ and $\{1,2,3,4\}$. So we have:

$$A_{C,4} = (-1)^4[(-1)^0 Q^0 + 4(-1)^1 Q^0 + 6(-1)^2 Q^0 + 4(-1)^3 Q^1 + (-1)^4 Q^2] = 3 - 4Q + Q^2$$

By using Remark 136 we can check our calculations as follows: $A_{C,0} + A_{C,1} + A_{C,2} + A_{C,3} + A_{C,4} = |C|$. We have $1 + 0 + 0 + 4Q - 4 + 3 - 4Q + Q^2 = Q^2 = |C|$.

Example 140 *In this example we will work with the code $C \subseteq [(\mathbb{F}_3)^2]^9$, described in Example 2 of [10]. Hence $q = 3^2 = 9$, and $C_Q = C^S \subseteq F^S = F_Q$, where $F = \mathbb{F}_3^2$. The matroid associated to all these codes is the "non-Pappus" matroid. This matroid based on the ground set $E = \{1,2,3,4,5,6,7,8,9\}$, and all subsets X have rank equal to $min(|X|, 3)$ except the following subsets: (1,2,3), (1,5,7), (1,6,8), (2,4,7), (2,6,9), (3,4,8), (3,5,9), (4,5,6). These have rank 2 and they are the set of circuits ($\mathcal{C}$) in sense of Definition 41. Let us find all of $A_{C,j}$.*

Firstly we recall that $n^*(X) = |X| - r^*(X)$ and $r^*(X) = |X| - r(E) + r(E - X)$. So, it is easy to see that for all X with cardinality less or equal to 5 we have $n^*(X) = 0$. For $|X| = 6$ occurs that $|E - X| = 3$ and we have two cases: $E - X \in \mathcal{C} \Rightarrow r(E - X) = 2 \Rightarrow r^*(E - X) = 5 \Rightarrow n^*(E - X) = 1$ and $E - X \notin \mathcal{C} \Rightarrow r(E - X) = 3 \Rightarrow r^*(E - X) = 6 \Rightarrow n^*(E - X) = 0$. If $|X| = 7$ then $n^*(X) = 1$, if $|X| = 8$ then $n^*(X) = 2$, if $|X| = 9$ then $n^*(X) = 3$. Now we are ready to use the formula:

$$A_{C,m}(Q) = (-1)^m \cdot \textstyle\sum_{|X|=m} \sum_{U \subseteq X} (-1)^{|U|} \cdot Q^{n^*(U)}.$$

For $m = 0$ we already know that $A_{C,0}(Q) = 1$. For $m = 1$ we have:

$$A_{C,1}(Q) = (-1)^1 \textstyle\sum_{|X|=1} [(-1)^0 Q^0 + (-1)^1 Q^0] = 0.$$

For $m = 2$ we have:

$$A_{C,2}(Q) = (-1)^2 \textstyle\sum_{|X|=2} [(-1)^0 Q^0 + 2(-1)^1 Q^0 + (-1)^2 Q^0] = 0.$$

We can see the pattern and as long as $n^*(X)$ is equal for X with the same cardinality we can rewrite the general formula as:

$$A_{C,m}(Q) = (-1)^m \textstyle\sum_{|X|=m} [(-1)^0 \cdot \binom{m}{0} \cdot Q^{n^*(X_0)} + (-1)^1 \cdot \binom{m}{1} \cdot Q^{n^*(X_1)} + \cdots + (-1)^m \cdot \binom{m}{m} \cdot Q^{n^*(X_m)}];$$

where $n^*(X_a)$ is nullity for X with cardinality a. And as long as $n^*(X) = 0$ well known property of the binomial coefficient gives us 0. So, $A_{C,3}(Q) = A_{C,4}(Q) = A_{C,5}(Q) = 0$. Moreover, $A_{C,6}(Q) = 0$ for $X \notin \overline{\mathcal{C}}$. But we have eight such X that $X \in \overline{\mathcal{C}}$ and $n^*(X) = 1$ which is leading us to:

$$A_{C,6}(Q) = (-1)^6 \cdot 8 \cdot [(-1)^0 \cdot \tbinom{6}{0} \cdot Q^0 + (-1)^1 \cdot \tbinom{6}{1} \cdot Q^0 + \cdots + (-1)^6 \cdot \tbinom{6}{6} \cdot Q^1] = 8(Q - 1).$$

For $|X| = 7$ it is getting more interesting. We have $\binom{9}{7} = \binom{9}{2} = 36$ sets of cardinality 7. Because of the way $\mathcal{C}$ is set on the "non-Pappus" matroid every pair (a, b) determine only one of element $\mathcal{C}$. And we have 24 such pairs and 12 "normal" pairs. So we have:

$$\begin{gathered} A_{C,7}(Q) = [(-1)^7 24 \cdot [(-1)^0 \cdot \tbinom{7}{0} \cdot Q^0 + (-1)^1 \cdot \tbinom{7}{1} \cdot Q^0 + \cdots + (-1)^6 \cdot (Q+6) + (-1)^7 \cdot \tbinom{7}{7} \cdot Q^1](=0)] + \\ + [(-1)^7 12 \cdot [(-1)^0 \cdot \tbinom{7}{0} \cdot Q^0 + (-1)^1 \cdot \tbinom{7}{1} \cdot Q^0 + \cdots + (-1)^6 \cdot \tbinom{7}{6} \cdot Q^0 + (-1)^7 \cdot \tbinom{7}{7} \cdot Q^1]] = \\ = 12(Q - 1) \end{gathered}$$

So, $A_{C,7}(Q) = 12(Q - 1)$. Now we find $A_{C,8}(Q)$. There are 9 sets of cardinality 8. Let us look at $\overline{\{1\}}$, it has 28 subsets X of cardinality 6. We are interested in $E - X$, and in this case they are just all of the triplets containing 1. And only three of them belong to $\mathcal{C}$. Making the same observations for the rest of possible sets of cardinality 8 gives us the following: $\overline{\{1\}}$, $\overline{\{2\}}$, $\overline{\{3\}}$, $\overline{\{4\}}$, $\overline{\{5\}}$, $\overline{\{6\}}$ have 3 circuits out of 28; $\overline{\{7\}}$, $\overline{\{8\}}$, $\overline{\{9\}}$ have 2 circuits out of 28. So

$$\begin{gathered} A_{C,8}(Q) = 6[(-1)^0 \cdot \tbinom{8}{0} \cdot Q^0 + (-1)^6 \cdot (3Q + 25) + (-1)^7 \cdot \tbinom{8}{7} \cdot Q^1 + (-1)^8 \cdot \tbinom{8}{8} \cdot Q^2] = \\ = 6(Q^2 - 5Q + 4) \\ \textit{plus} \\ 3[(-1)^0 \cdot \tbinom{8}{0} \cdot Q^0 + (-1)^6 \cdot (2Q + 26) + (-1)^7 \cdot \tbinom{8}{7} \cdot Q^1 + (-1)^8 \cdot \tbinom{8}{8} \cdot Q^2] = \\ = 3(Q^2 - 6Q + 5) \end{gathered}$$

So $A_{C,8}(Q) = 9Q^2 - 48Q + 39$. And the last one is $A_{C,9}(Q)$. Since there is only one subset of cardinality 9 and we already know that only 8 out of 84 subsets of cardinality 6 give us circuits:

$$A_{C,9}(Q) =$$
$$(-1)^9 \cdot [(-1)^0 \cdot \binom{9}{0} \cdot Q^0 + \cdots + (-1)^6 \cdot (8Q+76) + (-1)^7 \cdot \binom{9}{7} \cdot Q^1 + (-1)^8 \cdot \binom{9}{8} \cdot Q^2 + (-1)^9 \cdot \binom{9}{9} \cdot Q^3] =$$
$$= Q^3 - 9Q^2 + 28Q - 20$$

Also we can see that our calculations satisfy the equality from Remark 130:

$$1 + 8(Q-1) + 12(Q-1) + 9Q^2 - 48Q + 39 + Q^3 - 9Q^2 + 28Q - 20 = Q^3$$

Proposition 141 *For all codes C^s, viewed as a subcodes of $(\mathbb{F}_Q^n)$, where C is the code from Example 2 of [10]. and $Q = (9)^s$, we have $d_1 = 6$, $d_2 = 8$ and $d_3 = 9$.*

Proof. All codes C^S have the same matroid, which is "non-Pappus" matroid. Then we apply Proposition 138.

References

[1] T. Britz, T. Johnsen, J.A. Martin, ”Chains, Demi-matroids and Profiles”, IEEE Trans. of Info. Th. **60**(2) pp. 986–991, 2014

[2] T. Britz, T. Johnsen, D. Mayhew, K. Shiromoto, ”Wei-type duality theorems for matroids”, Designs, Codes and Cryptography, **62**(3) pp. 331–341, 2012

[3] R. Hill, ”A First Course in Coding Theory”, Clarendon Press, Oxford, 1986

[4] T. Johnsen, J.N. Roksvold, H. Verdure, ”A generalization of weight polynomials to matroids”, Discrete Mathematics, arXiv 1311.6291, **339**(2) 2016.

[5] T. Johnsen, H. Verdure, ”Code Theory and Matroid Theory”, Preprint, University of Tromsø, 2013

[6] T. Johnsen, H. Verdure, ”Generalized Hamming weights for almost affine codes”, preprint, IEEE Transactions on Information Theory, **63**(4), pp. 1941–1953, 2017.

[7] T. Johnsen, H. Verdure, ”Flags of almost affine codes”, Preprint, University of Tromsø, November 30, 2016

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

[9] J. Martin, ”Matroids, Demi-matroids, and Chains of Linear Codes”, Master’s thesis, University of Tromsø (2010).

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