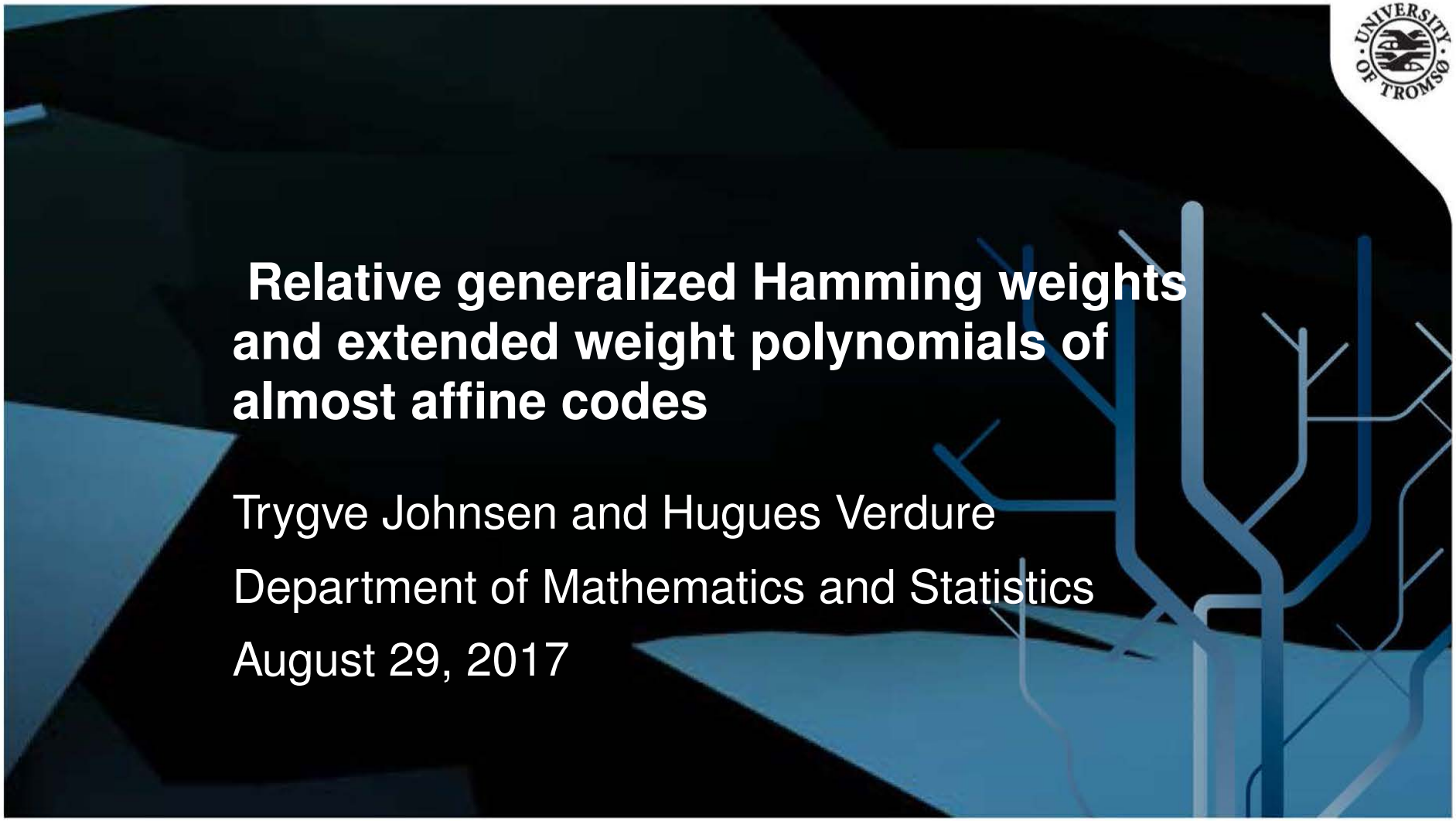
UNIVERSITY OF TROMSØ UiT



Relative generalized Hamming weights and extended weight polynomials of almost affine codes

Trygve Johnsen and Hugues Verdure

Department of Mathematics and Statistics

August 29, 2017

Content

Matroids, equivalent definitions

— Matroids initially arose from matrices M over a field F. The matroid associated to M is a pair

$$(E = \{1, 2, \cdots, n\}, \mathcal{N}),$$

where $\mathcal{N}$ is the set of subsets of E indexing those sets of columns of M that are linearly independent.

Matroids, equivalent definitions

— Matroids initially arose from matrices M over a field F. The matroid associated to M is a pair

$$(E = \{1, 2, \cdots, n\}, \mathcal{N}),$$

where $\mathcal{N}$ is the set of subsets of E indexing those sets of columns of M that are linearly independent.

— Example

$$M = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

over any field. Then $E = \{1, 2, 3, 4, 5\}$, and the maximal elements in $\mathcal{N}$ are

$$\{1, 2, 3\}, \{1, 3, 5\}, \{2, 3, 4\}, \{3, 4, 5\}.$$

The set $\mathcal{B}$ with these 4 subsets as elements, certainly determines $\mathcal{N}$, which contain of 14 additional, smaller subsets of E.

Matroids, equivalent definitions

— Matroids initially arose from matrices M over a field F. The matroid associated to M is a pair

$$(E = \{1, 2, \cdots, n\}, \mathcal{N}),$$

where $\mathcal{N}$ is the set of subsets of E indexing those sets of columns of M that are linearly independent.

— Example

$$M = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

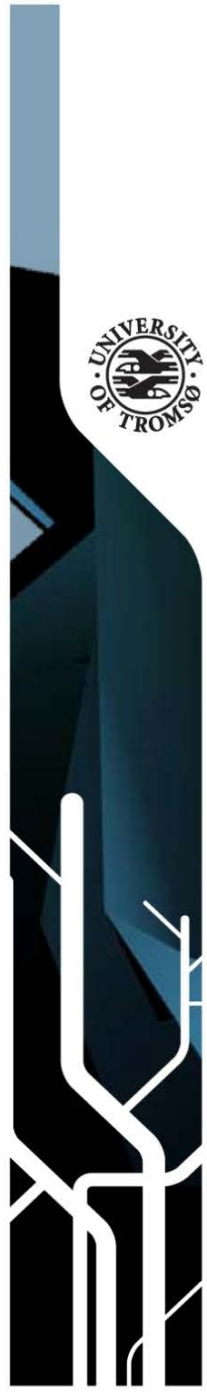
over any field. Then $E = \{1, 2, 3, 4, 5\}$, and the maximal elements in $\mathcal{N}$ are

$$\{1, 2, 3\}, \{1, 3, 5\}, \{2, 3, 4\}, \{3, 4, 5\}.$$

The set $\mathcal{B}$ with these 4 subsets as elements, certainly determines $\mathcal{N}$, which contain of 14 additional, smaller subsets of E.

The elements I of $\mathcal{N}$ satisfy:

- 1. $\emptyset \in \mathcal{N}$
- 2. If $I \in \mathcal{N}$, and $I' \subset I$, then $I' \in \mathcal{N}$.
- 3. If I_1 and I_2 are in $\mathcal{N}$, and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{N}$.



The elements I of $\mathcal{N}$ satisfy:

- 1. $\emptyset \in \mathcal{N}$
- 2. If $I \in \mathcal{N}$, and $I' \subset I$, then $I' \in \mathcal{N}$.
- 3. If I_1 and I_2 are in $\mathcal{N}$, and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{N}$.

DEFINITION OF A MATROID:
A (finite) matroid is a pair $(E = \{1, 2, \cdots, n\}, \mathcal{N})$, where $\mathcal{N} \subset 2^E$ satisfies (1), (2), (3). The basis $\mathcal{B}$ of a matroid are the maximal elements of $\mathcal{N}$. They all have the same cardinality and this cardinality is the RANK of the matroid. The elements of $\mathcal{N}$ are the called the INDEPENDENT subsets of E.

The elements I of $\mathcal{N}$ satisfy:

- 1. $\emptyset \in \mathcal{N}$
- 2. If $I \in \mathcal{N}$, and $I' \subset I$, then $I' \in \mathcal{N}$.
- 3. If I_1 and I_2 are in $\mathcal{N}$, and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{N}$.

DEFINITION OF A MATROID:
A (finite) matroid is a pair $(E = \{1, 2, \cdots, n\}, \mathcal{N})$, where $\mathcal{N} \subset 2^E$ satisfies (1), (2), (3). The basis $\mathcal{B}$ of a matroid are the maximal elements of $\mathcal{N}$. They all have the same cardinality and this cardinality is the RANK of the matroid. The elements of $\mathcal{N}$ are the called the INDEPENDENT subsets of E.
CAUTION: There are matroids that do not come from matrices (over any field). Example for $n = 8, 9$. These are said to be non-vectorial.

DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $r(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = r(E)$. The rank function $2^E \to N_0$ satisfies:

DEFINITION OF RANK FUNCTION OF A MATROID:

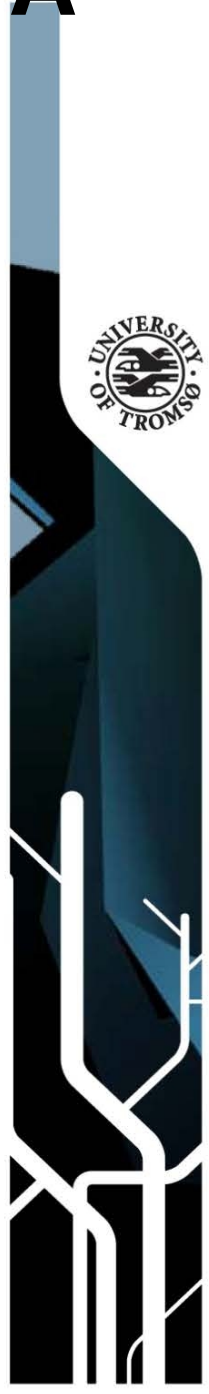
If $X \subset E$, then $r(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = r(E)$. The rank function $2^E \to N_0$ satisfies:

— (R1) $r(\emptyset) = 0$.

DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $r(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = r(E)$. The rank function $2^E \to N_0$ satisfies:

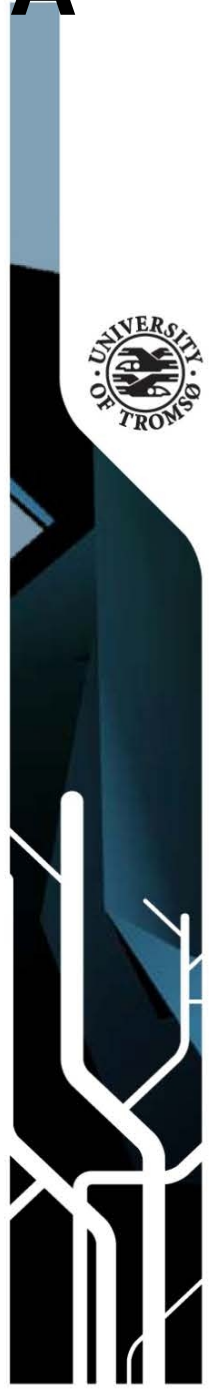
- (R1) $r(\emptyset) = 0$.
- (R2) If $X \subset E$, and $x \in E$, then $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$.



DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $r(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = r(E)$. The rank function $2^E \to N_0$ satisfies:

- (R1) $r(\emptyset) = 0$.
- (R2) If $X \subset E$, and $x \in E$, then $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$.
- (R3) If $X \subset E$, and $x, y \in E$ are such that $r(X) = r(X \cup \{x\}) = r(X \cup \{y\})$, then $r(X \cup \{x, y\}) = r(X)$.



DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $r(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = r(E)$. The rank function $2^E \to N_0$ satisfies:

- (R1) $r(\emptyset) = 0$.
- (R2) If $X \subset E$, and $x \in E$, then $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$.
- (R3) If $X \subset E$, and $x, y \in E$ are such that $r(X) = r(X \cup \{x\}) = r(X \cup \{y\})$, then $r(X \cup \{x, y\}) = r(X)$.

COMMENT: Any function $2^E \to N_0$ satisfying $(R1), (R2), (R3)$ determines a matroid: $\mathcal{N} =$ the set of those I with $r(I) = |I|$. We sometimes denote it by $M = (E, r)$.

DEFINITION OF RANK FUNCTION OF A DEMI-MATROID:

Any function $2^E \rightarrow N_0$ satisfying $(R1), (R2)$ determines a demi-matroid:

DEFINITION OF RANK FUNCTION OF A DEMI-MATROID:

Any function $2^E \to N_0$ satisfying $(R1), (R2)$ determines a demi-matroid:

— (R1) $r(\emptyset) = 0$.

DEFINITION OF RANK FUNCTION OF A DEMI-MATROID:

Any function $2^E \to N_0$ satisfying $(R1), (R2)$ determines a demi-matroid:

- (R1) $r(\emptyset) = 0$.
- (R2) If $X \subset E$, and $x \in E$, then $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$.

DUAL RANK FUNCTION

Given a matroid or demi-matroid M with rank function r. Put

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

DUAL RANK FUNCTION

Given a matroid or demi-matroid M with rank function r. Put

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

Then r^* is the rank function of the dual (demi-)matroid $M^* = (E, r^*)$.

DUAL RANK FUNCTION

Given a matroid or demi-matroid M with rank function r.
Put

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

Then r^* is the rank function of the dual (demi-)matroid $M^* = (E, r^*)$.
For a demi-matroid (E, r), set
$\overline{r}(X) = r(E) - r(E - X)$, for any $X \subset E$.
Then $\overline{M} = (E, \overline{r})$ is a demi-matroid.
We have: $\overline{\overline{M}} = (M^*)^* = M$, and $(\overline{M})^* = \overline{M^*}$

THE DUAL MATROID - ALTERNATIVE DEFINITION

— THE DUAL MATROID $M^* = (E = \{1, 2, \cdots, n\}, \mathcal{N}^*)$ is the one whose basis $\mathcal{B}^*$ consists of the complements of the elements of $\mathcal{B}$. In the example above: $\mathcal{B}^* = \{\{4, 5\}, \{2, 4\}, \{1, 5\}, \{1, 2\}.\}$ This is well defined. The rank of M^* is $n - rk(M)$.

MATROID OF A LINEAR CODE

MATROID OF A LINEAR CODE:
If C is a linear code over a finite field let $M(C)$ be the matroid associated to any parity check matrix of C (well defined). Then C is an $[n, n - rk(M)]$-code, and $M_C = M(C)^*$ is the matroid associated to any generator matrix of C, i.e. it is $M(C^*)$, where C^* is the orthogonal complement of C.

Generalized Hamming weights

Generalized Hamming weights

Definition

Let M be a matroid on the ground set E, The generalized Hamming weights of M are

$$d_i(M) = m_i(M) = Min\{\#\sigma |\ n(\sigma) = i\}.$$

Here $n(X) = |X| - r(X)$, for any $X \subset E$.

ALMOST AFFINE CODES:

Let $C \subset F^n$ for some finite alphabet F, with $|F| = q$. Assume that the projection C_X has cardinality q^s, for some integer s depending on X, for any non-empty $X \subset E = \{1, \cdots, n\}$. Then C is called an almost affine code.

ALMOST AFFINE CODES:

Let $C \subset F^n$ for some finite alphabet F, with $|F| = q$. Assume that the projection C_X has cardinality q^s, for some integer s depending on X, for any non-empty $X \subset E = \{1, \cdots, n\}$. Then C is called an almost affine code. Set $r(\emptyset) = 0$, and for any non-empty $X \in E = \{1, \cdots, n\}$, set

$$r(X) = log_q |C_X|.$$

The dimension of C is $r(E) = log_q |C|$, and C is called an $[n, k]$-almost affine code.

ALMOST AFFINE CODES:

Let $C \subset F^n$ for some finite alphabet F, with $|F| = q$. Assume that the projection C_X has cardinality q^s, for some integer s depending on X, for any non-empty $X \subset E = \{1, \cdots, n\}$. Then C is called an almost affine code. Set $r(\emptyset) = 0$, and for any non-empty $X \in E = \{1, \cdots, n\}$, set

$$r(X) = log_q|C_X|.$$

The dimension of C is $r(E) = log_q|C|$, and C is called an $[n, k]$-almost affine code.
Then r is the rank function of a matroid $M_C = M(C)^*$.
Linear codes is a particular case of almost affine codes, and for these codes the two definitions coincide. So $M(C)$ is the matroid with rank function r^*.

Matroids of the kind M_C for almost affine codes C are called secret sharing matroids, since almost affine codes in an intimate way are associated to so-called ideal perfect secret sharing schemes.

Matroids of the kind M_C for almost affine codes C are called secret sharing matroids, since almost affine codes in an intimate way are associated to so-called ideal perfect secret sharing schemes.

There are matroids that are secret sharing, but not vectorial. The non-Pappus matroid on 9 elements is M_C for an almost affine code of length 9 and dimension 3 over the alphabet F_3^2. Thus it is secret sharing. But it is not vectorial (because of its non-Pappus-ness). Furthermore: The Vamos matroid on 8 elements is NOT even secret sharing.

Matroids of the kind M_C for almost affine codes C are called secret sharing matroids, since almost affine codes in an intimate way are associated to so-called ideal perfect secret sharing schemes.

There are matroids that are secret sharing, but not vectorial. The non-Pappus matroid on 9 elements is M_C for an almost affine code of length 9 and dimension 3 over the alphabet F_3^2. Thus it is secret sharing. But it is not vectorial (because of its non-Pappus-ness). Furthermore: The Vamos matroid on 8 elements is NOT even secret sharing.

It is not known whether duals of secret sharing matroids are always secret sharing, since there is in general no natural way to produce the dual of an almost affine code (unless it belongs to some smaller subclass).

Generalized Hamming weights

Let C be an $[n, k]$- linear code over a field $\mathbb{K}$.
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C \text{ linear subcode of dimension } i\}.$$

Generalized Hamming weights

Let C be an $[n, k]$- linear code over a field $\mathbb{K}$.
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C \text{ linear subcode of dimension } i\}.$$

Let C be an $[n, k]$-almost affine code
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C \text{ is an almost affine subcode of dimension } i\}.$$

Generalized Hamming weights

Let C be an $[n, k]$- linear code over a field $\mathbb{K}$.
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C \text{ linear subcode of dimension } i\}.$$

Let C be an $[n, k]$-almost affine code
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C \text{ is an almost affine subcode of dimension } i\}.$$

Theorem

For an $[n, k]$-almost affine code C we have
$d_i = d_i(M(C))$, *for* $i = 1, \cdots, k$.

Here $M(C)$ is by convention the matroid of a parity check matrix of the code if C is linear.
Fact: For an $[n, k]$-linear code C all 3 definitions coincide.

This enables us to define dual Hamming weights $d_1^*, \cdots, d_{n-k}^*$ for almost affine code (in terms of those of the dual matroid of $M(C)$), and give meaning to Wei duality, although dual codes of almost affine codes do not in general exist.

Theorem

$$\{d_1, \cdots, d_k\} \cup \{n+1-d_{n-k}^*, \cdots, n+1-d_1^*\} = \{1, 2, \cdots, n\}.$$

STANDARD SUBCODES

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

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

STANDARD SUBCODES

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

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

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

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

where c_X is the projection of c to X.

STANDARD SUBCODES

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

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

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

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

where c_X is the projection of c to X.

SIMPLE KEY RESULT (A-S): This is an almost affine subcode of dimension $k - r(X)$.
Such codes are called **standard** subcodes.

STANDARD SUBCODES

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

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

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

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

where c_X is the projection of c to X.

SIMPLE KEY RESULT (A-S): This is an almost affine subcode of dimension $k - r(X)$.
Such codes are called **standard** subcodes. This gives that almost affine subcodes of every concecutive dimension from 0 to k actually exist, since the rank of X increases with 0 or 1 each time you add a point.

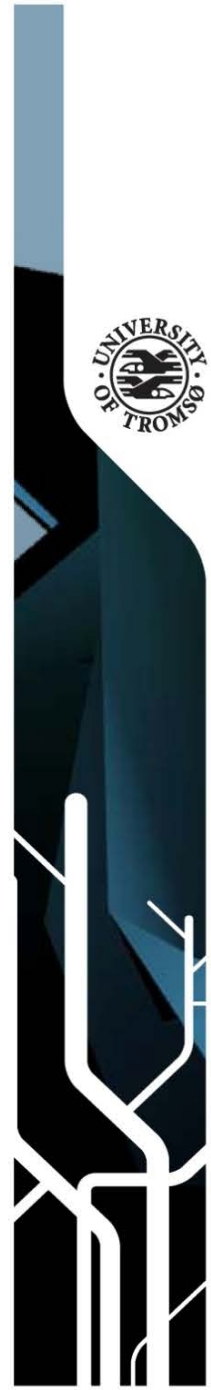
The matroid $M_{C(X,c)}$ is M_C, contracted in X, thus a matroid with ground set $E - X$, and so $M(C(X, c))$ is $M(C)$ with X deleted, thus also a matroid with ground set $E - X$.

Theorem

Let C be an $[n, k]$-almost affine code
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C$$

$$is\ a\ standard\ almost\ affine\ subcode\ of\ dimension\ i\}.$$



CHAINS OF ALMOST AFFINE CODES:

Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a flag, or chain, F, of almost affine codes for some finite alphabet.

CHAINS OF ALMOST AFFINE CODES:

Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a flag, or chain, F, of almost affine codes for some finite alphabet.

Look at $r(X) = \rho_F(X) = \Sigma_{i=1}^{m}(-1)^{i+1} r_i(X)$, for any $X \subset E$, for the rank functions r_i, associated to the codes C_i, for $i = 1, \cdots, m$.

CHAINS OF ALMOST AFFINE CODES:

Let $C_m \subset C_{m-1} \subset \cdots \subset C_1$ be a flag, or chain, F, of almost affine codes for some finite alphabet.

Look at $r(X) = \rho_F(X) = \Sigma_{i=1}^{m}(-1)^{i+1} r_i(X)$, for any $X \subset E$, for the rank functions r_i, associated to the codes C_i, for $i = 1, \cdots, m$.

Then r is the rank function of a demi-matroid.

Define the following functions:

$$\eta_F = \sum_{i=1}^{m} (-1)^{m-i} r_i^*,$$

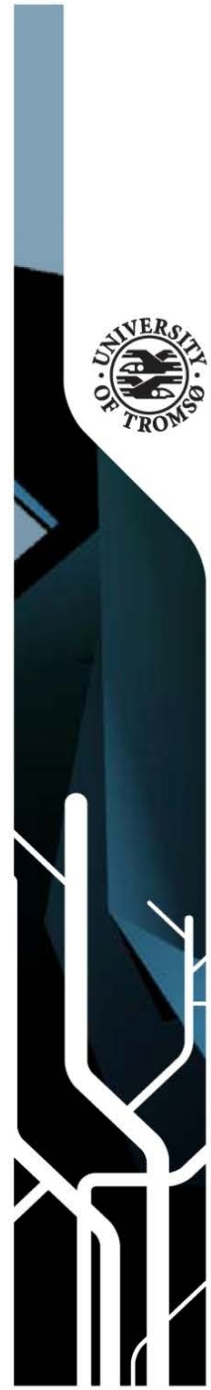
$$\theta_F = \sum_{i=1}^{m} (-1)^{i+1} \overline{r_i},$$

$$\pi_F = \sum_{i=1}^{m} (-1)^{m-i} \overline{r_i^*}.$$

Then (E, η_F), (E, θ_F) and (E, π_F) are all demi-matroids. Moreover, we have the following duality relations:

$$\eta_F = \begin{cases} \overline{\rho_F} & \text{if } m \text{ is even} \\ \rho_F^* & \text{if } m \text{ is odd} \end{cases}, \quad \theta_F = \overline{\rho_F},$$

$$\pi_F = \begin{cases} \rho_F & \text{if } m \text{ is even} \\ \overline{\rho_F}^* & \text{if } m \text{ is odd} \end{cases}.$$



Define the following functions:

$$\eta_F = \sum_{i=1}^{m} (-1)^{m-i} r_i^*,$$

$$\theta_F = \sum_{i=1}^{m} (-1)^{i+1} \overline{r_i},$$

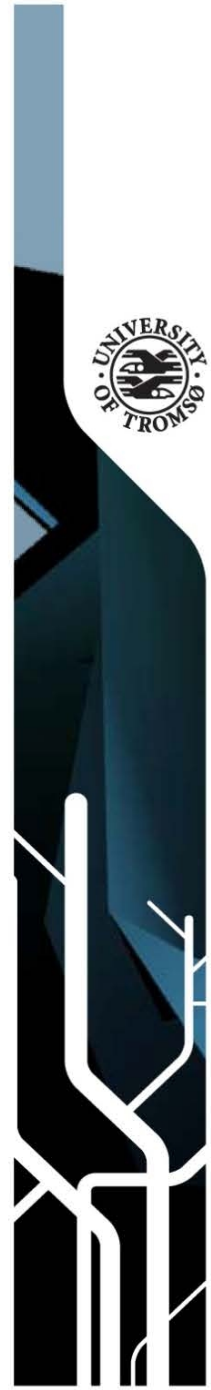
$$\pi_F = \sum_{i=1}^{m} (-1)^{m-i} \overline{r_i^*}.$$

Then (E, η_F), (E, θ_F) and (E, π_F) are all demi-matroids. Moreover, we have the following duality relations:

$$\eta_F = \begin{cases} \overline{\rho_F} & \text{if } m \text{ is even} \\ \rho_F^* & \text{if } m \text{ is odd} \end{cases}, \quad \theta_F = \overline{\rho_F},$$

$$\pi_F = \begin{cases} \rho_F & \text{if } m \text{ is even} \\ \overline{\rho_F}^* & \text{if } m \text{ is odd} \end{cases}.$$

This reduces to: $\eta_F = \overline{\rho_F}$ and $\theta_F = \overline{\rho_F}$ and $\pi_F = \rho_F$ if $m = 2$.

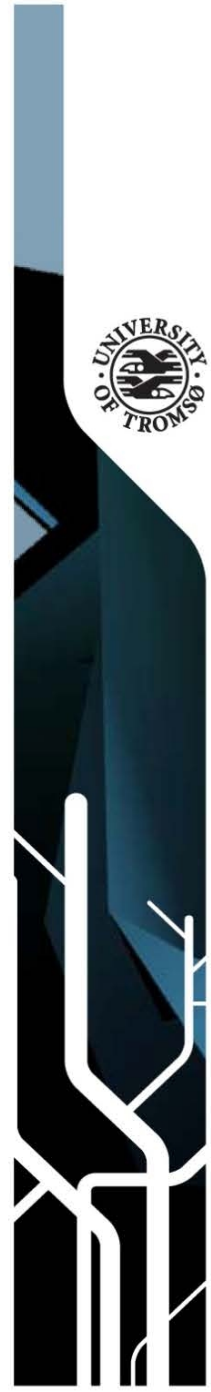


REMARK: These formulas are in general true for chains $r_m \leq r_{m-1} \leq \cdots \leq r_1$ of demi-matroid functions provided that $\epsilon_i \subset \epsilon_{i+1}$, for all i, where

$$\epsilon_i = \{(X, x) | r_i(X) = r_i(X - \{x\})\},$$

for $i = 1, \cdots, m-1$. It can be shown that this condition holds for chains of almost affine codes.

We will be interested in the case $m = 2$, and the simple chain/flag/pair $C_2 \subset C_1$, and rank function $\rho = r_1 - r_2$.



We will be interested in the case $m = 2$, and the simple chain/flag/pair $C_2 \subset C_1$, and rank function $\rho = r_1 - r_2$. While the $i'th$ generalized Hamming weight for a single almost affine code can be expressed as:

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

for $i = 1, \cdots, k$, and r^* is the rank function of M_C^*, and $\overline{r}$ is the rank function of $\overline{M_C}$, we make a similar definition for the pair $C_2 \subset C_1$ of almost affine codes:

We will be interested in the case $m = 2$, and the simple chain/flag/pair $C_2 \subset C_1$, and rank function $\rho = r_1 - r_2$. While the $i'th$ generalized Hamming weight for a single almost affine code can be expressed as:

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

for $i = 1, \cdots, k$, and r^* is the rank function of M_C^*, and $\overline{r}$ is the rank function of $\overline{M_C}$, we make a similar definition for the pair $C_2 \subset C_1$ of almost affine codes:

Definition

For $0 \leqslant i \leqslant \dim C_1 - \dim C_2$, we define the RLDP (Relative Length/Dimension Profile), or relative generalized Hamming weight, of the pair (C_1, C_2) as follows:

$$m_i = \min\{|X|,\ \overline{\rho}(X) = i\}.$$

Theorem

Let $C_2 \subset C_1$ be a pair of almost affine codes with associated demi-matroid (E, ρ). Then for $0 \leqslant i \leqslant \dim C_1 - \dim C_2$,

$$m_i = \min\{w(D),\ |D \cap C_2| = 1,$$

$$and\ \ D \subset C_1\ \ is\ \ a\ \textbf{standard subcode with}\ \dim D = i\}.$$

Here $w(D)$ means $|\cup_{d \in D} Supp(d, c)|$, for a fixed reference word $c \in C$, and is independent of c.

The proof is a straightforward, but tedious calculation, where one shows both $b_i \leq m_i$, and $m_i \leq b_i$, where

$$b_i = \min\{w(D),\ |D \cap C_2| = 1,\ D \subset C_1$$

$$\text{is a } \textbf{standard} \text{ almost affine subcode with } \dim D = i\},$$

for each $0 \leqslant i \leqslant \dim C_1 - \dim C_2$.

The proof is a straightforward, but tedious calculation, where one shows both $b_i \leq m_i$, and $m_i \leq b_i$, where

$$b_i = \min\{w(D),\ |D \cap C_2| = 1,\ D \subset C_1$$

$$\text{is a } \textbf{standard} \text{ almost affine subcode with } \dim D = i\},$$

for each $0 \leqslant i \leqslant \dim C_1 - \dim C_2$.
The result above is an analogue of a result by Liu, Chen, Luo for linear codes. It is not clear that we can drop the word "standard" in our theorem.

The proof is a straightforward, but tedious calculation, where one shows both $b_i \leq m_i$, and $m_i \leq b_i$, where

$$b_i = \min\{w(D),\ |D \cap C_2| = 1,\ D \subset C_1$$

$$\text{is a } \textbf{standard} \text{ almost affine subcode with } \dim D = i\},$$

for each $0 \leqslant i \leqslant \dim C_1 - \dim C_2$.
The result above is an analogue of a result by Liu, Chen, Luo for linear codes. It is not clear that we can drop the word "standard" in our theorem.
Let

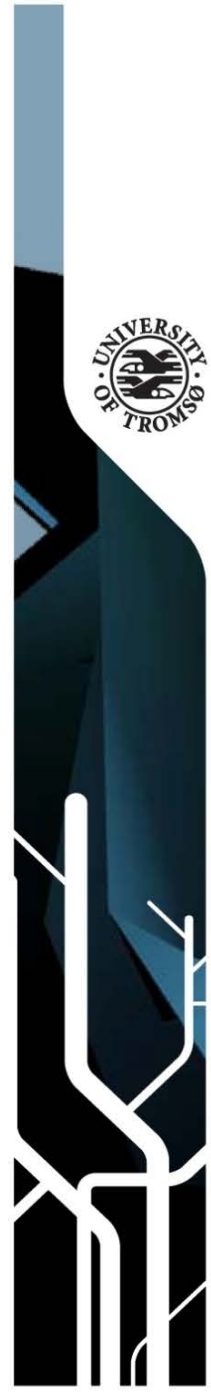
$$b_i' = \min\{w(D),\ |D \cap C_2| = 1,\ D \subset C_1$$

$$\text{is } \textbf{any} \text{ almost affine subcode with } \dim D = i\},$$

for all non-negative integers $i \leq \dim C_1$.

Obviously $m_i = b_i \geq b'_i$, for all $0 \leq i \leq \dim C_1 - \dim C_2$. The entities m_i and b_i do not make sense, other than as ∞, if $i > \dim C_1 - \dim C_2$.

Obviously $m_i = b_i \geq b'_i$, for all $0 \leq i \leq \dim C_1 - \dim C_2$.
The entities m_i and b_i do not make sense, other than as ∞, if $i > \dim C_1 - \dim C_2$.
For b_i this is clear since any standard subcode of dimension i will have non-trivial intersection with C_2, since $C_1(X, \tilde{c}) \cap C_2 = C_2(X, \tilde{c})$, with dimension $k_2 - r(X) = k_1 - r(X) - (k_1 - k_2) = i - (k_1 - k_2) > 0$.



Let $F = \{0, 1, 2, 3\}$, and $C_1 = F^3$. Let C_2 and D be the almost affine subcodes

$$\{000, 012, 023, 031, 103, 110, 121, 132, 201, 213, 222, 230,$$
$$302, 311, 320, 333\}$$

and

$$\{000, 011, 022, 033, 102, 113, 120, 131, 203, 210, 221, 232,$$
$$301, 312, 323, 330\}$$

respectively. Both subcodes have dimension 2, while C_1 has dimension 3. But we have $C_2 \cap D = \{000\}$ and look at $i = 2 = \dim D > \dim C_1 - \dim C_2 = 3 - 2 = 1$. We see that b_2' is defined as an integer (and is at most 3), while m_2 and b_2 could be said to be ∞ if one insists on defining them. Hence "$m_2 > b_2$", since "$\infty > 3$.

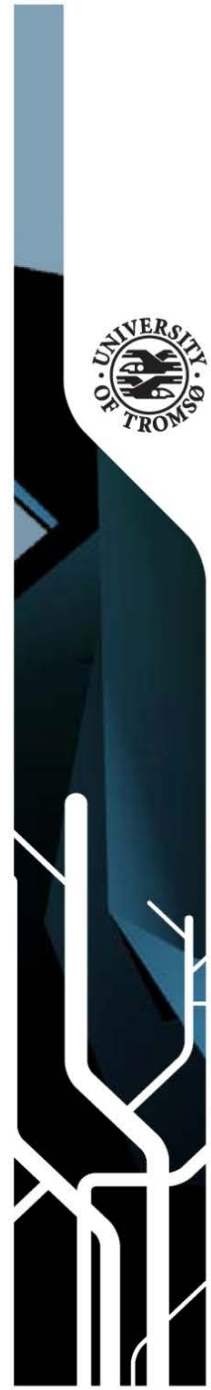
Let $F = \{0, 1, 2, 3\}$, and $C_1 = F^3$. Let C_2 and D be the almost affine subcodes

$$\{000, 012, 023, 031, 103, 110, 121, 132, 201, 213, 222, 230,$$
$$302, 311, 320, 333\}$$

and

$$\{000, 011, 022, 033, 102, 113, 120, 131, 203, 210, 221, 232,$$
$$301, 312, 323, 330\}$$

respectively. Both subcodes have dimension 2, while C_1 has dimension 3. But we have $C_2 \cap D = \{000\}$ and look at $i = 2 = \dim D > \dim C_1 - \dim C_2 = 3 - 2 = 1$. We see that b_2' is defined as an integer (and is at most 3), while m_2 and b_2 could be said to be ∞ if one insists on defining them. Hence "$m_2 > b_2$", since "$\infty > 3$.
Nevertheless it is an open question to us whether $m_i > b_i$ is possible for $0 \leq i \leq \dim C_1 - \dim C_2$.



Content

We want to study the polynomial

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leq j \leq n,$$

which we refer to as the generalized weight enumerator of M.

We want to study the polynomial

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leq j \leq n,$$

which we refer to as the generalized weight enumerator of M. Why ?

We want to study the polynomial

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leq j \leq n,$$

which we refer to as the generalized weight enumerator of M. Why ?
After an argument similar to one of Jurrius/Pellikaan, one shows that:

$$P_{M(H),i}(q^s)$$

is the number of codewords of weight i in $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^s}$ for a linear code C with parity check matrix H.

Definition

For each $j = 1, \cdots, n$, let $A_{C,j}(s)$ be the number of codewords of weight j in $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^s}$ viewed as code over the alphabet $\mathbb{F}_{q^s}$.

Using the exclusion/inclusion principle we we obtain the formula for linear codes :

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

This interpretation, and essentially the same calculation, also makes sense for almost affine codes C in general (over an alphabet F of cardinality q). Instead of working with a code specified as $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ one simply works with C^s interpreted as a code over the alphabet F^s after rearranging coordinates. These codes have identical associated matroids for all s.

After a refined study, restricting to each subset X of cardinality j, and using some basic results of almost afine codes mentioned above, one finds: For each $j = 0, 1, \cdots, n$ there are polynomials

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

counting the number over codewords of weight j in C^s over the alphabet F^s. Hence knowledge of a finite number of coefficients give the weight distribution of an infinite series of codes.

Hence all results in pure matroid theory about how one can find the coefficients of a polynomial $P_{M,i}(Z)$ are applicable to almost affine codes, just as well as in the case of linear codes. In particular we have:
$P_{M,i}(Z)$ is determined by certain Betti numbers of M, and so-called elongations of M, where these Betti numbers refer to coefficients of certain resolutions of the Stanley-Reisner rings of the simplicial independence complexes of the matroids involved.