Almost affine codes

Report 96-22

Juriaan Simonis
Alexey Ashikhmin

TU Delft
Faculteit der Technische Wiskunde en Informatica
Faculty of Technical Mathematics and Informatics

Technische Universiteit Delft
Delft University of Technology

ISSN 0922-5641

Copyright © 1996 by the Faculty of Technical Mathematics and Informatics, Delft, The Netherlands.
No part of this Journal may be reproduced in any form, by print, photoprint, microfilm, or any other means without permission from the Faculty of Technical Mathematics and Informatics, Delft University of Technology, The Netherlands.

Copies of these reports may be obtained from the bureau of the Faculty of Technical Mathematics and Informatics, Julianalaan 132, 2628 BL Delft, phone +31152784568.
A selection of these reports is available in PostScript form at the Faculty's anonymous ftp-site. They are located in the directory /pub/publications/tech-reports at ftp.twi.tudelft.nl

Almost Affine Codes

Juriaan Simonis*and Alexey Ashikhmin†
Delft University of Technology
Faculty of Technical Mathematics and Informatics
P.O. Box 5031
2600 GA Delft, the Netherlands

March 7, 1996

Abstract

An almost affine code is a code $\mathcal{C}$ for which the size of all codes obtained by multiple puncturing of $\mathcal{C}$ is a power of the alphabet size. Essentially, almost affine codes are the same as ideal perfect secret sharing schemes or partial affine spaces. The present paper explores these interrelations, gives short proofs of known (and new) results, and derives some properties of the distance distribution of almost affine codes.

1 Introduction

A linear code $\mathcal{C}$ of length n and alphabet size q is a linear subspace of the standard vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$. So its size is a power of q. Since the projection $\mathcal{C}_X$ of $\mathcal{C}$ into any coordinate space $\mathbb{F}^X := \prod_{i \in X} \mathbb{F}_q$, $X \subseteq \{1, 2, \ldots, n\}$, again is a linear code, the size of this projection $\mathcal{C}_X$ is a power of q as well. There are other subsets of $\mathbb{F}_q^n$ that possess the property that all projections have a size which is a power of the alphabet size, the most obvious ones being the *affine* codes, i.e. the cosets of linear codes. In fact, if q equals 2 or 3, there are no other ones, as we shall see in section 5. But the situation changes drastically with increasing alphabet size. This more general class of codes, which we propose to call *almost affine*, has a definite

*J.Simonis@twi.tudelft.nl
†aea@twi.tudelft.nl

cryptographic relevance. In fact, it virtually coincides with the family of the ideal perfect secret sharing schemes. Another point of view is geometry. We shall see in section 9 that almost affine codes represent certain combinatorial objects that share important features with affine geometries. Since, however, they generally do not possess sufficiently many flats, we call these objects *partial* affine geometries.

To give a formal definition of almost affine codes, we need a formal definition of *projection* (or *puncturing* in coding vernacular). Let F be a finite set of size $q \geq 2$. We can identify the Cartesian product F^n with F^S, the set of all mappings of the coordinate index set $S := \{1, 2, \ldots, n\}$ into F. For any subset $X \subseteq S$, let

$$\rho_X^S : F^S \to F^X$$

be the mapping induced by the inclusion mapping

$$X \hookrightarrow S.$$

A q-ary *code* of length n is a non-empty subset of F^S. The image $\rho_X^S(\mathcal{C})$ of a code $\mathcal{C} \subseteq F^S$ under ρ_X^S will be denoted by $\mathcal{C}_X$. We say that $\mathcal{C}_X$ is the *projection* of $\mathcal{C}$ into the coordinate space F^S, or the *puncturing* of $\mathcal{C}$ with respect to the complementary set $\overline{X} := S \setminus X$ of coordinate positions.

Definition 1 *A code $\mathcal{C} \subseteq F^S$ is called* almost affine *if it satisfies the condition*

$$r(X) := \log_q(|\mathcal{C}_X|) \in \mathbb{N} \text{ for all } X \subseteq S.$$

Example 1 *If $F := \mathbb{F}_q$ is a finite field of order q, then the affine subspaces (cosets of linear subspaces) of F^n are almost affine.*

Example 2 *Let F be an m-dimensional vector space over a finite field $\mathbb{F}_q$ and let $\mathcal{C}$ be a linear subspace of the nm-dimensional vector space F^n. Then $\mathcal{C}$ is an almost affine code of length n over the alphabet F if and only if for all subsets $X \subseteq \{1, 2, \ldots, n\}$ the dimension of the vector space $\mathcal{C}_X$ is divisible by m. We could call these codes* multilinear codes *in contrast to the ordinary linear codes of the preceding example. If, for instance, $F := (\mathbb{F}_3)^2$, then the row space of the matrix*

$$\begin{bmatrix}
10 & 10 & 00 & 10 & 00 & 10 & 10 & 10 & 00 \\
01 & 01 & 00 & 01 & 00 & 01 & 01 & 01 & 00 \\
00 & 00 & 00 & 10 & 10 & 21 & 01 & 10 & 10 \\
00 & 00 & 00 & 02 & 01 & 20 & 12 & 02 & 01 \\
00 & 10 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\
00 & 01 & 01 & 21 & 00 & 21 & 00 & 10 & 01
\end{bmatrix}$$

is an almost affine code of length 9 over F. (We checked this using the computer algebra systems AXIOM and MAPLE.)

Example 3 *Orthogonal arrays of size q^k, n constraints, q levels and strength k are q-ary almost affine codes of length n. (Cf. [9]). These are exactly the (unrestricted) codes that attain the Singleton bound. The Latin squares correspond to the parameters $k := 2$ and $n := 3$. Since the number $L(q)$ of nonequivalent Latin squares grows very rapidly with q (cf. [13]), we may expect that the class of the almost affine codes is considerably larger than the class of the affine codes.*

Definition 2 *The* dimension *of the almost affine code $\mathcal{C}$ is the integer*

$$\dim \mathcal{C} := r(S).$$

Definition 3 *Two almost affine codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq F^S$ are said to be* equivalent *if a permutation σ of S and permutations π_i, $i \in S$, of F exist such that the bijection*

$$F^S \to F^S, \quad (c_i)_{i \in S} \longmapsto (\pi_i(c_{\sigma(i)}))_{i \in S},$$

maps $\mathcal{C}_1$ onto $\mathcal{C}_2$.

A basic problem is to determine or at least estimate the number of nonequivalent almost affine codes of given dimension, length and alphabet size.

2 The matroid of an almost affine code

Let $\mathcal{C}$ be an almost affine code. We claim that the function

$$r : \mathcal{P}(S) \to \mathbb{N}$$

introduced in definition 1 is the *rank function* of a *matroid* $\mathcal{M}(\mathcal{C})$ over S. According to [14], Theorem 1.1.2, we have to check that for all $X \subseteq S$ and all $i, j \in S$

R1 $r(\emptyset) = 0$;

R2 $r(X) \leq r(X \cup \{i\}) \leq r(X) + 1$;

R3 if $r(X \cup \{i\}) = r(X \cup \{j\}) = r(X)$, then $r(X \cup \{i, j\}) = r(X)$.

But these properties are obvious. A new coordinate position i can increase the number of codewords at most by a factor q, and if each of two new coordinate positions i, j fails to distinguish between codewords, their combination fails to do so as well.

From now on, we feel free to use all notions and results in [14] or [6] that are applicable to the matroid $\mathcal{M}(\mathcal{C})$. For instance, the *independent sets* of $\mathcal{M}(\mathcal{C})$ are the subsets $X \subseteq S$ such that $r(X) = |X|$, i.e. such that

$$\mathcal{C}_X = F^X.$$

A *base* B of $\mathcal{M}(\mathcal{C})$ is a maximal independent set:

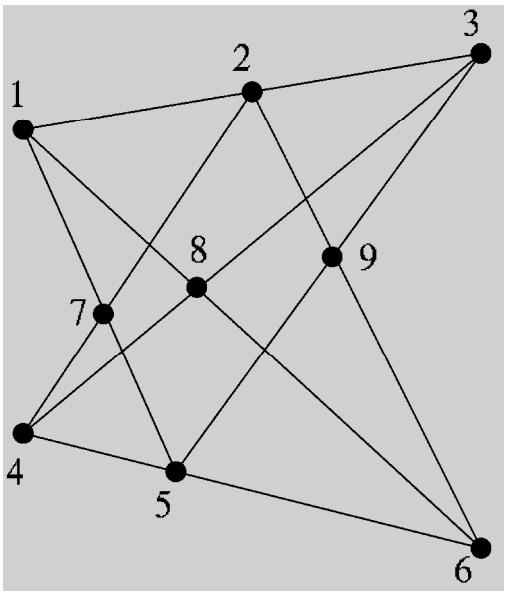
$$r(B) = |B| = r(S).$$

The *uniform* matroid $\mathcal{U}_{k,n}$ is the matroid over S for which the bases are the k-subsets of S. So the orthogonal arrays are precisely the almost affine codes $\mathcal{C}$ for which $\mathcal{M}(\mathcal{C})$ is a uniform matroid.
A *circuit* C of $\mathcal{M}(\mathcal{C})$ is a minimal dependent set:

$$r(C) = |C| - 1 = r(C \setminus \{x\}) \text{ for all } x \in C.$$

Latin squares, for instance, produce circuits of length 3.

Example 4 *The matroid of the specific almost affine code in example 2 is the "non-Pappus" matroid, with geometric representation*



(Cf. [14], p. 138 or [6], p. 43.) The lines in the picture correspond to the circuits of rank two. Pappus' theorem implies that this matroid is not linearly representable over any field.

Definition 4 *A matroid $\mathcal{M}$ is said to be* almost affinely representable *if an almost affine code $\mathcal{C}$ exists such that $\mathcal{M} = \mathcal{M}(\mathcal{C})$. If $\mathcal{C}$ is equivalent to a code of the type described in example* 2, *then $\mathcal{M}$ is said to be* multilinearly representable.

A fundamental problem of almost affine codes is to characterize the almost affinely representable matroids. Note that the "non-Pappus" matroid is an instance of a matroid that is almost affinely representable, and even multilinearly representable, but not linearly representable. It is an open problem whether matroids do exist that are almost affinely representable but not multilinearly representable.

3 Ideal perfect secret sharing schemes

3.1 The relation with almost affine codes

Let $S := \{1, 2, \ldots, n\}$ be a set of n participants.

Definition 5 *An* access structure *over S is a monotone subset Γ of the power set $\mathcal{P}(S)$. (Monotonicity means that $A \in \Gamma$ implies that $B \in \Gamma$ for all $B \supseteq A$.)*
The set of the minimal elements *of Γ with respect to the partial ordering $\subseteq$ is denoted by $\partial\Gamma$. The access structure Γ is said to be* connected *if*

$$\bigcup_{A \in \partial\Gamma} A = S.$$

Let F be finite set of secrets. A *perfect secret sharing scheme* for the access structure Γ is a method of distributing *shares* to the participants in such a way that all groups of participants in Γ can retrieve the secret, but no other group has any a posteriori information about the secret. A perfect secret sharing scheme is said to be *ideal* if the share set for each participant is equal to the set of secrets F. We can formalize this as follows:

Definition 6 *Put $A' := \{0\} \cup A$ for $A \subseteq S$. An* ideal perfect secret sharing scheme *for the access structure Γ is a subset $\mathcal{C} \subseteq F^{S'}$ such that*

1. $\mathcal{C}_{\{i\}} = F$ *for all* $i \in S'$,
2. $|\mathcal{C}_{A'}| = |\mathcal{C}_A|$ *for all* $A \in \Gamma$,
3. $|\mathcal{C}_{A'}| = q\,|\mathcal{C}_A|$ *for all* $A \in \mathcal{P}(S) \setminus \Gamma$.

Clearly, any almost affine code $\mathcal{C} \subseteq F^{S'}$ such that the matroid $\mathcal{M}(\mathcal{C})$ has no loops is an ideal secret sharing scheme for the access structure $\Gamma(\mathcal{C})$ defined by

$$\partial\Gamma(\mathcal{C}) := \{A \subseteq S \mid A' \text{ is circuit in } \mathcal{M}(\mathcal{C})\}.$$

The access structure $\Gamma(\mathcal{C})$ is connected if and only if the matroid $\mathcal{M}(\mathcal{C})$ is connected.

Brickell and Davenport showed in [3], proposition 1, that the converse also is true:

Proposition 1 *An ideal secret sharing scheme for a connected access structure is an almost affine code.*

Remark 1 *It follows from theorem 5.4.1. in [14] that, in the connected case, the access structure $\Gamma(\mathcal{C})$ completely determines the matroid $\mathcal{M}(\mathcal{C})$. The first to make this observation were the authors of [5].*

Remark 2 *In [2], Bertilsson claims that "if it is impossible to construct an ideal scheme with only one column for the secret, it is impossible to construct an ideal scheme for the given access structure". In our terminology, he claims that all multilinearly representable matroids are linearly representable. But we have seen at the end of section 2 that the "non-Pappus" matroid is a counterexample.*

3.2 A flaw in a proof by Brickell and Davenport

In [3], Brickell and Davenport stated the following theorem:

> **Theorem 2.** Let $\mathcal{T} = (V, \mathcal{I})$ be a connected matroid representable over a nearfield, R. Let $v_0 \in V$. Then there exists a connected ideal secret sharing scheme M such that $R = \mathcal{K}$, $p_0 = v_0$, $P = V$, and $D(M) =$ the dependent sets of $\mathcal{T}$.

A *right nearfield* is an algebraic structure that satisfies all field axioms except, possibly, the left distributive law. Cf. [7] or [11]. The smallest example of a nondistributive right nearfield is $N(9) := \{0, 1, 2, a, b, c, d, e, f\}$ with the addition table

+	0	1	2	a	b	c	d	e	f
0	0	1	2	a	b	c	d	e	f
1	1	2	0	b	c	a	e	f	d
2	2	0	1	c	a	b	f	d	e
a	a	b	c	d	e	f	0	1	2
b	b	c	a	e	f	d	1	2	0
c	c	a	b	f	d	e	2	0	1
d	d	e	f	0	1	2	a	b	c
e	e	f	d	1	2	0	b	c	a
f	f	d	e	2	0	1	c	a	b

and the multiplication table

×	1	2	a	b	c	d	e	f
1	1	2	a	b	c	d	e	f
2	2	1	d	f	e	a	c	b
a	a	d	2	e	b	1	f	c
b	b	f	c	2	d	e	a	1
c	c	e	f	a	2	b	1	d
d	d	a	1	c	f	2	b	e
e	e	c	b	d	1	f	2	a
f	f	b	e	1	a	c	d	2

.

Now the proof of Theorem 2 in [3] is based on the (implicit) assumption that any k×n-matrix G over a right nearfield R generates an almost affine code $\mathcal{C} := \{\mathbf{x}G \mid \mathbf{x} \in R^k\}$. But the example

$$G := \begin{bmatrix} 1 & 1 & b \\ 2 & 0 & c \\ 0 & 2 & d \end{bmatrix}$$

shows that this certainly is not true for the nearfield $N(9)$. Indeed, the size of the corresponding code $\mathcal{C}$ is equal to 243, which is not an integer power of 9. Probably, almost affine codes that are generated by means of nondistributive right nearfields are quite rare.

4 Basic constructions for almost affine codes

4.1 Puncturing

Let $\mathcal{C} \subseteq F^S$ be an almost affine code, and let X be any subset of S. Then the code $\mathcal{C}_X \subseteq F^X$ defined in the introduction is an almost affine code of dimension $r(X)$.

Definition 7 *The almost affine code $\mathcal{C}_X \subseteq F^X$ is said to be obtained by* puncturing *$\mathcal{C}$ with respect to $\bar{X}$, the complement of X in S.*

Remark 3 *The matroid $\mathcal{M}(\mathcal{C}_X)$ corresponding to $\mathcal{C}_X$ is the* reduction *$\mathcal{M}(\mathcal{C}) \mid X$ of the matroid $\mathcal{M}(\mathcal{C})$ to X.*

4.2 Shortening

Recall that

$$\rho_X^S : F^S \to F^X$$

denotes the restriction mapping, i.e. the mapping induced by the inclusion

$$X \hookrightarrow S.$$

The image $\rho_X^S(\mathbf{w})$ of an element $\mathbf{w} \in F^S$ under ρ_X^S will be denoted by $\mathbf{w}_X$. Let $\mathcal{C} \subseteq F^S$ be a k-dimensional q-ary almost affine code. We consider the fibers of the mapping

$$\rho_X^S \mid_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}_X,$$

i.e. the subsets

$$\mathcal{C}(X, \mathbf{x}) := \{\mathbf{c} \in \mathcal{C} \mid \mathbf{c}_X = \mathbf{x}_X\}, \quad \mathbf{x} \in \mathcal{C}, \tag{1}$$

of $\mathcal{C}$.

Proposition 2 *If $r := r(X)$, then*

$$|\mathcal{C}(X, \mathbf{x})| = q^{k-r}$$

for all $\mathbf{x} \in \mathcal{C}_X$. Hence the sets $\mathcal{C}(X, \mathbf{x})$, $\mathbf{x} \in \mathcal{C}$, have the same size.

Proof. Choose a maximal independent subset $Y \subseteq X$ and a base B such that $Y = X \cap B$. Then the mappings

$$\rho_B^S \mid_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}_B = F^B$$

and

$$\rho_Y^X \mid_{\mathcal{C}_X} : \mathcal{C}_X \to \mathcal{C}_Y = F^Y$$

are bijective. Hence

$$|\mathcal{C}(X, \mathbf{x})| = |\mathcal{C}_B(X \cap B, \mathbf{x}_B)| = |\mathcal{C}_B(Y, \mathbf{x}_B)| =$$

$$\left|\{\mathbf{b} \in F^B \mid \mathbf{b}_Y = \mathbf{x}_Y\}\right| = q^{k-r}.$$

■

Corollary 1 *The sets $\mathcal{C}(X, \mathbf{x})$ are almost affine subcodes of $\mathcal{C}$. (These subcodes will play an important role in section 9.)*

Proof. If $Y \subseteq S$, then

$$|\mathcal{C}(X, \mathbf{x})_Y| = |(\mathcal{C}_{X \cup Y}(X, \mathbf{x}_{X \cup Y}))_Y| = |\mathcal{C}_{X \cup Y}(X, \mathbf{x}_{X \cup Y})| = q^{r(X \cup Y) - r(X)}.$$

■

Definition 8 *The almost affine codes*

$$\mathcal{C}^{\bar{X}}(\mathbf{x}) := \mathcal{C}(X, \mathbf{x})_{\overline{X}},$$

are said to be obtained by shortening *$\mathcal{C}$ with respect to $X \subseteq S$.*

Remark 4 *Proposition 2 implies that the dimension of the shortened code $\mathcal{C}^{\bar{X}}(\mathbf{x})$ is equal to $k - r = \dim \mathcal{C} - r(X)$.*

Remark 5 *For different choices of $\mathbf{x} \in \mathcal{C}_X$, we obtain different, not necessarily equivalent, shortened codes $\mathcal{C}^{\bar{X}}(\mathbf{x})$. But since the sizes of the sets*

$$\mathcal{C}(X, \mathbf{x})_Y, \quad Y \subseteq \overline{X},$$

are independent of $\mathbf{x}$, the matroids

$$\mathcal{M}(\mathcal{C}^{\bar{X}}(\mathbf{x}))$$

are all the same. In fact they coincide with the contraction *$\mathcal{M}(\mathcal{C}) \times \bar{X}$ of the matroid $M(\mathcal{C})$ to $\bar{X}$.*

4.3 Almost affine subcodes

An almost affine subcode of an almost affine code $\mathcal{C}$ is a subset of $\mathcal{C}$ which is an almost affine code. The number of r-dimensional *affine* subcodes of a q-ary k-dimensional *affine* code is equal to

$$q^{k-r} \begin{bmatrix} k \\ r \end{bmatrix}_q,$$

where $\begin{bmatrix} k \\ r \end{bmatrix}_q$ is a *Gaussian number*. (For an extensive description, see chapter 24 of [13].) The following example shows that the number of r-dimensional *almost affine* subcodes of a q-ary k-dimensional *almost affine* code cannot be expressed in k, r and q alone.

Example 5 *Let* $F := \{0,1,2,3\}$. *The number of 1-dimensional almost affine subcodes of* F^2 *is equal to* 32, *whereas the number of 1-dimensional almost affine subcodes of the almost affine code* $\mathcal{C} \subseteq F^3$ *consisting of the words*

$$\begin{array}{cccc} 000 & 011 & 022 & 033 \\ 101 & 110 & 123 & 132 \\ 202 & 213 & 220 & 231 \\ 303 & 312 & 321 & 330 \end{array}$$

is equal to 20. *If* $\rho : \mathcal{C} \to F^2$ *is the restriction mapping with respect to the first two coordinates, we see that the inverse image of the 1-dimensional almost affine subcode* $\{01, 10, 22, 33\} \subseteq F^2$ *is not an almost affine subcode of* $\mathcal{C}$.

It is even not true that the number of r*-dimensional almost affine subcodes of a* q*-ary* k*-dimensional almost affine code* $\mathcal{C}$ *is determined by the matroid* $\mathcal{M}(\mathcal{C})$. *Consider, for example, the almost affine code* $\mathcal{C}' \subseteq F^3$ *consisting of the words*

$$\begin{array}{cccc} 000 & 011 & 022 & 033 \\ 101 & 112 & 123 & 130 \\ 202 & 213 & 220 & 231 \\ 303 & 310 & 321 & 332 \end{array} .$$

Its matroid, the uniform matroid $\mathcal{U}_{2,3}$, *is the same as that of the almost affine code* $\mathcal{C}$ *defined above, but the number of 1-dimensional almost affine subcodes of* $\mathcal{C}'$ *is equal to 12. Note that* $\mathcal{C}'$ *possesses pairs of codewords, e.g.* $\{000, 112\}$, *that are not contained in any 1-dimensional almost affine subcode of* $\mathcal{C}'$.

5 The binary and ternary case

Affine subspaces of $\mathbb{F}_2^n$ can be characterized by the following closure property: A subset $\mathcal{A} \subseteq \mathbb{F}_2^n$ is an affine subspace if and only if $\mathbf{x}+\mathbf{y}+\mathbf{z} \in \mathcal{A}$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{A}$. In particular, the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ are the quadruplets $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{u}\}$ with $\mathbf{x}+\mathbf{y}+\mathbf{z}+\mathbf{u} = \mathbf{o}$.

Proposition 3 *Let* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *be a binary almost affine code. Then each triplet of distinct codewords* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{C}$ *is contained in a 2-dimensional* affine *subcode* $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{u}\}$ *of* $\mathcal{C}$.

Proof. We apply induction with respect to $\dim \mathcal{C}$. If $\dim \mathcal{C} \leq 1$, there is nothing to prove. Suppose that the proposition holds for all binary almost affine codes of dimension $< k$, and let $\dim \mathcal{C} = k$. Choose a base $B \subseteq S$ for the matroid $\mathcal{M}(\mathcal{C})$. For any three distinct $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{C}$, a unique codeword $\mathbf{u} \in \mathcal{C}$

exists such that $\mathbf{x}_B + \mathbf{y}_B + \mathbf{z}_B + \mathbf{u}_B = \mathbf{o}$. We claim that $\mathbf{x}+\mathbf{y}+\mathbf{z}+\mathbf{u} = \mathbf{o}$. If not, a coordinate $i \in \bar{B}$ exists such that $x_i + y_i + z_i + u_i = 1$. Without loss of generality, we may assume that $u_i = x_i = y_i$ and $u_i \neq z_i$. Then the subcode

$$\mathcal{E} := \{\mathbf{c} \in \mathcal{C} \mid c_i = u_i\}$$

of $\mathcal{C}$ has dimension $k-1$. So the induction hypothesis guarantees the existence of a codeword $\mathbf{v} \in \mathcal{E}$ such that $\mathbf{x} + \mathbf{y} + \mathbf{v} + \mathbf{u} = \mathbf{o}$. This implies that $\mathbf{x}_B + \mathbf{y}_B + \mathbf{v}_B + \mathbf{u}_B = \mathbf{o}$. Hence $\mathbf{v}_B = \mathbf{z}_B$, $\mathbf{v} = \mathbf{z}$ and $\mathbf{x} + \mathbf{y} + \mathbf{z} + \mathbf{u} = \mathbf{o}$. ■

Corollary 2 *All binary almost affine codes are affine.*

Now we turn to the ternary case. Affine subspaces of $\mathbb{F}_3^n$ can be characterized by the following closure property:
A subset $\mathcal{A} \subseteq \mathbb{F}_3^n$ is an affine subspace if and only if $-\mathbf{x} - \mathbf{y} \in \mathcal{A}$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{A}$. In particular, the 1-dimensional affine subspaces of $\mathbb{F}_3^n$ are the triplets $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ with $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{o}$.

Proposition 4 *Let $\mathcal{C} \subseteq \mathbb{F}_3^n$ be a ternary almost affine code. Then each pair of distinct codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ is contained in a 1-dimensional* affine *subcode $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ of $\mathcal{C}$.*

Proof. We apply induction with respect to $\dim \mathcal{C}$. If $\dim \mathcal{C} = 0$, there is nothing to prove. Suppose that the proposition holds for all ternary almost affine codes of dimension $< k$, and let $\dim \mathcal{C} = k$. Choose a base $B \subseteq S$ for the matroid $\mathcal{M}(\mathcal{C})$. For any two distinct $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, a unique codeword $\mathbf{z} \in \mathcal{C}$ exists such that $\mathbf{x}_B + \mathbf{y}_B + \mathbf{z}_B = \mathbf{o}$. We claim that $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{o}$. If not, a coordinate $i \in \bar{B}$ exists such that $x_i + y_i + z_i \neq 0$. Without loss of generality, we may assume that $z_i = x_i$ and $z_i \neq y_i$. Then the subcode

$$\mathcal{E} := \{c \in \mathcal{C} \mid c_i = z_i\}$$

of $\mathcal{C}$ has dimension $k-1$. So the induction hypothesis guarantees the existence of a codeword $\mathbf{u} \in \mathcal{E}$ such that $\mathbf{x}+\mathbf{u}+\mathbf{z} = \mathbf{o}$. This implies that $\mathbf{x}_B+\mathbf{u}_B+\mathbf{z}_B = \mathbf{o}$. Hence $\mathbf{u}_B = \mathbf{y}_B$, $\mathbf{u} = \mathbf{y}$ and $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{o}$. ■

Corollary 3 *All ternary almost affine codes are affine.*

Remark 6 *The paper [1] of Beimel and Chor contains two lemmas (3.10 and 3.12) that are equivalent to our Corollaries 2 and 3, but their proofs are different.*

Remark 7 *The corollaries 2 and 3 cannot be generalized to fields of size greater than three. Indeed the code $\mathcal{C}'$ in example 5 is a quaternary almost affine code that is not even* equivalent *to an affine code.*

6 The dual matroid

Let $\mathcal{C} \subseteq F^S$ be a k–dimensional q-ary almost affine code, and let $\bar{\mathbf{c}}$ be a fixed element of $\mathcal{C}$.

Definition 9 *The* $\bar{\mathbf{c}}$-support *of an element* $\mathbf{c} \in \mathcal{C}$ *is the subset*

$$\mathrm{supp}(\mathbf{c}, \bar{\mathbf{c}}) := \{i \in S \mid \mathbf{c}_i \neq \bar{\mathbf{c}}_i\}$$

of S.

Definition 10 *A codeword* $\mathbf{c} \neq \bar{\mathbf{c}}$ *is said to be* $\bar{\mathbf{c}}$-minimal *if* $\bar{\mathbf{c}}$ *and* $\mathbf{c}$ *are the only codewords* $\mathbf{d}$ *such that*

$$\mathrm{supp}(\mathbf{d}, \bar{\mathbf{c}}) \subseteq \mathrm{supp}(\mathbf{c}, \bar{\mathbf{c}}).$$

Remark 8 *Let* $\mathbf{c}$ *is be any codeword distinct from* $\bar{\mathbf{c}}$*, and let* $X := \mathrm{supp}(\mathbf{c}, \bar{\mathbf{c}})$*. Since the shortened code* $\mathcal{C}^X(\bar{\mathbf{c}})$ *contains the two distinct codewords* $\mathbf{c}_X$ *and* $\bar{\mathbf{c}}_X$*, the integer* $\delta := \dim \mathcal{C}^X(\bar{\mathbf{c}})$ *is positive. Moreover,* $\dim \mathcal{C}^Y(\bar{\mathbf{c}}) = \delta - 1$ *for all subsets* $Y \subset X$ *with* $|Y| = |X| - 1$*. If* $\delta > 1$*, then the codeword* $\mathbf{c}$ *is not* $\bar{\mathbf{c}}$*-minimal. Indeed, for any* $Y \subset X$ *of size* $|X| - 1$ *we can find codewords* $\mathbf{d} \neq \bar{\mathbf{c}}$ *such that* $\mathrm{supp}(\mathbf{d}, \bar{\mathbf{c}}) \subseteq Y \subset X = \mathrm{supp}(\mathbf{c}, \bar{\mathbf{c}})$*. If, on the other hand,* $\delta = 1$*, then* $\mathbf{c}$ *is* $\bar{\mathbf{c}}$*-minimal. Note that in that case* $\mathcal{C}^X(\bar{\mathbf{c}})$ *is equivalent to the* q*-ary repetition code of length* $|X|$*.*

Proposition 5 *The* $\bar{\mathbf{c}}$*-supports of the* $\bar{\mathbf{c}}$*-minimal codewords are the circuits of the dual matroid* $\mathcal{M}(\mathcal{C})^*$*.*

Proof. By definition, the independent sets of $\mathcal{M}(\mathcal{C})^*$ are the subsets $X \subseteq S$ such that $\bar{X}$ contains a base of $\mathcal{M}(\mathcal{C})$. Keeping in mind Remark 4, we see that X is an independent set of $\mathcal{M}(\mathcal{C})^*$ if and only if $\dim \mathcal{C}^X(\bar{\mathbf{c}}) = 0$. A circuit C of $\mathcal{M}(\mathcal{C})^*$ is a minimal dependent set, i.e. a set C such that $\dim \mathcal{C}^C(\bar{\mathbf{c}}) = 1$ and $\dim \mathcal{C}^Y(\bar{\mathbf{c}}) = 0$ for all proper subsets $Y \subset C$. But these properties coincide with the characterization of the support of a minimal codeword that we gave in Remark 8. ■

It is important to note that the matroid $\mathcal{M}(\mathcal{C})^*$ does not depend on the choice of $\bar{\mathbf{c}} \in \mathcal{C}$. This suggests the following conjecture.

Conjecture 1 *Let* $\mathcal{C}$ *be an unrestricted code such that the* $\bar{\mathbf{c}}$*-supports of the* $\bar{\mathbf{c}}$*-minimal codewords are the circuits of a matroid that does not depend on the choice of* $\bar{\mathbf{c}} \in \mathcal{C}$*. Then* $\mathcal{C}$ *is an almost affine code.*

7 Distance distribution and the rank function.

Let $\mathcal{C} \subseteq F^S$ be a k–dimensional q-ary almost affine code of length $n := |S|$, and let $\bar{\mathbf{c}}$ be a fixed element of $\mathcal{C}$.

Definition 11 *The* $\bar{\mathbf{c}}$-distance distribution *of* $\mathcal{C}$ *is the sequence of nonnegative integers*

$$A_i(\bar{\mathbf{c}}) := \left|\{\mathbf{c} \in \mathcal{C} \mid |\mathrm{supp}(\mathbf{c}, \bar{\mathbf{c}})| = i\}\right|, \qquad i = 0, 1, \ldots, n.$$

The following theorem expresses a relation between the distance distribution of $\mathcal{C}$ and the rank function r.

Theorem 1 *Let*

$$R_v^u := \left|\{X \subseteq S \mid r(X) = u \text{ and } |X| = v\}\right|.$$

Then

$$\sum_{j=0}^{n} \binom{n-j}{n-i} A_j(\bar{\mathbf{c}}) = \sum_{u=0}^{n} q^{k-u} R_{n-i}^u, \qquad i = 0, 1, \ldots, n. \tag{2}$$

Proof. Count the set

$$\{(\mathbf{c}, X) \mid \mathbf{c} \in \mathcal{C}, X \subseteq S, \mathrm{supp}(\mathbf{c}, \bar{\mathbf{c}}) \subseteq X, |X| = i\}$$

in two ways. Note that $\mathrm{supp}(\mathbf{c}, \bar{\mathbf{c}}) \subseteq X$ if and only if $\mathbf{c}$ and $\bar{\mathbf{c}}$ lie in the same fiber of the mapping

$$\rho_{\overline{X}}^{S}|_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}_{\overline{X}}.$$

■

Remark 9 *Note that the polynomial*

$$R(\mathcal{M}; x, y) := \sum_{u,v} R_v^u x^{k-u} y^{v-u}$$

is the (Whitney) rank generating function *of the matroid* $\mathcal{M} := \mathcal{M}(\mathcal{C})$. *(Cf. [14], p. 297.)*

Remark 10 *Since the binomial matrix*

$$\left[\binom{n-j}{n-i}\right]_{i,j=0,\ldots,n}$$

is invertible, we can solve the linear system (2) for the $A_i(\bar{\mathbf{c}})$:

$$A_j(\bar{\mathbf{c}}) = \sum_{i=0}^{n} (-1)^{i+j} \binom{n-i}{n-j} \sum_{u=0}^{n} q^{k-u} R_{n-i}^u, \qquad j = 0, 1, \ldots, n. \tag{3}$$

Corollary 4 *The* $\bar{\mathbf{c}}$-distance distribution *of* $\mathcal{C}$ *is completely determined by the rank function, i.e. by the matroid* $\mathcal{M}(\mathcal{C})$. *Hence it does not depend on* $\bar{\mathbf{c}}$. *In other words, an almost affine code is* distance invariant. *So we feel free to write* A_j *for* $A_j(\bar{\mathbf{c}})$.

The equations (3) provide a simple but not always conclusive test whether a matroid is almost affinely representable for a given alphabet size: The right hand sides must be nonnegative!

Example 6 *If* $\mathcal{M} := \mathcal{U}_{k,n}$, *the uniform matroid, then*

$$R_v^u = \begin{cases} \binom{n}{v} & \text{if } v = u \text{ or } v > k = u \\ \\ 0 & \text{otherwise.} \end{cases}$$

After substitution in (3), we find $A_0 = 1$, $A_j = 0$ *for* $1 \leq j \leq n-k$ *and*

$$A_{n-k+t} = \binom{n}{k-t} \sum_{i=0}^{t-1} (-1)^i \binom{n-k+t}{i} (q^{t-i} - 1), \qquad t = 1, \ldots, k.$$

(Compare this with Chapter 11, section 3 of [9], where the same result is derived for linear *MDS codes. In [12], Tolhuizen gave a different proof for the* unrestricted *case.) If* $k \geq 2$, *the inequality* $A_{n-k+2} \geq 0$ *implies the condition*

$$q \geq n - k + 1.$$

In other words, a q*-ary code of size* $M > q$ *and length* $n > q + \log_q(M) - 1$ *cannot attain the Singleton bound.*

Analogous to [10], we can use partitions of the set S of coordinate positions to strengthen the preceding results. Let $\mathcal{T} := (T_1, T_2, \ldots, T_p)$ be a fixed partition of S into p subsets T_α of respective size $n_\alpha := |T_\alpha|$, and put

$$W(\mathcal{T}) := \{i \in \mathbb{N}^p \mid i_\alpha \leq n_\alpha \text{ for } \alpha = 1, \ldots, p\}$$

and

$$\mathbf{n} := (n_1, n_2 + 1, \ldots, n_p).$$

Definition 12

1. *If* r *is the rank function of a matroid* $\mathcal{M}$ *over* S, *then*

$$R_{\mathbf{i}}^u(\mathcal{M}) := |\{X \subseteq S \mid r(X) = u \text{ and } |X| = i_\alpha, \alpha = 1, .., p\}|.$$

The same counting argument as in Theorem 1 yields

Theorem 2 *With the notations introduced above (putting* $R^u_{\mathbf{i}} := R^u_{\mathbf{i}}(\mathcal{M}(\mathcal{C}))$*, we have*

$$\sum_{\mathbf{j}\in W(T)} \left[\prod_{\alpha=1}^{p} \binom{n_\alpha - j_\alpha}{n_\alpha - i_\alpha}\right] A_{\mathbf{j}}(\bar{\mathbf{c}}) = \sum_{u=1}^{n} q^{k-u} R^u_{\mathbf{n}-\mathbf{i}}, \qquad \mathbf{i} \in W(\mathcal{T}). \tag{4}$$

or, after solving for the $A_{\mathbf{j}}(\bar{\mathbf{c}})$*,*

$$A_{\mathbf{j}}(\bar{\mathbf{c}}) = \sum_{\mathbf{i}\in W(T)} \left[\prod_{\alpha=1}^{p} (-1)^{i_\alpha + j_\alpha} \binom{n_\alpha - i_\alpha}{n_\alpha - j_\alpha}\right] \sum_{u=0}^{n} q^{k-u} R^u_{\mathbf{n}-\mathbf{i}}, \qquad \mathbf{j} \in W(\mathcal{T}). \tag{5}$$

Remark 11 *Note that the* $\bar{\mathbf{c}}$*-distance distribution of* $\mathcal{C}$ *with respect to the partition* $\mathcal{T}$ *does not depend on* $\bar{\mathbf{c}}$*. So we usually write* $A_{\mathbf{j}}$ *for* $A_{\mathbf{j}}(\bar{\mathbf{c}})$*.*

An interesting case is the partition of S into its one element subsets. $A_{\mathbf{j}}(\bar{\mathbf{c}})$ is the number of codewords in $\mathcal{C}$ whose $\bar{\mathbf{c}}$-supports coincide with the subset $\{\alpha \mid j_\alpha = 1\}$ of S. Then equation (5) reduces to

Proposition 6 *The number of codewords in* $\mathcal{C}$ *with given* $\bar{\mathbf{c}}$*-support* Y *is equal to*

$$\sum_{X\subseteq Y} (-1)^{|Y\setminus X|} q^{k-r(\bar{X})}.$$

If we combine this result with Proposition 5, we obtain

Corollary 5 *The* $\bar{\mathbf{c}}$*-supports of the codewords of a* q*-ary almost affine code* $\mathcal{C}$ *are completely determined by* q *and the* $\bar{\mathbf{c}}$*-minimal codewords of* $\mathcal{C}$*, i.e. by the alphabet size* q *and the matroid* $\mathcal{M}(\mathcal{C})$*.*

8 The dual distance distribution

Let $(A_0, A_1, \ldots, A_n)$ be the distance distribution of a k-dimensional q-ary almost affine code $\mathcal{C} \subseteq F^S$ of length $n := S$. The *dual distance distribution* $(B_0, B_1, \ldots, B_n)$ of $\mathcal{C}$ is the *MacWilliams transform* of $(A_0, A_1, \ldots, A_n)$. Cf. [9], Ch. 5. The B_i and the A_i satisfy the following set of equations:

$$\sum_{j=0}^{n} \binom{n-j}{n-i} A_j = q^{k-n+i} \sum_{j=0}^{n} \binom{n-j}{i} B_j, \qquad i = 0, 1, \ldots, n. \tag{6}$$

A famous theorem of Delsarte [4] states that the B_i are nonnegative rational numbers.

Proposition 7 *Let $\tilde{r}$ be the rank function of the dual matroid $\mathcal{M}(\mathcal{C})^*$, and let*

$$\tilde{R}_v^u := |\{X \subseteq S \mid \tilde{r}(X) = u \text{ and } |X| = v\}|$$

Then the dual distance distribution of $\mathcal{C}$ is given by

$$B_j = \sum_{i=0}^{n} (-1)^{i+j} \binom{n-i}{n-j} \sum_{u=0}^{n} q^{n-k-u} \tilde{R}_{n-i}^u, \qquad j = 0, 1, \ldots, n. \tag{7}$$

Proof. From the equations (1) and (6), we get

$$\sum_{j=0}^{n} \binom{n-j}{i} B_j = \sum_{v=0}^{n} q^{n-i-v} R_{n-i}^v, \qquad i = 0, 1, \ldots, n,$$

or

$$\sum_{j=0}^{n} \binom{n-j}{n-i} B_j = \sum_{v=0}^{n} q^{i-v} R_i^v, \qquad i = 0, 1, \ldots, n, \tag{8}$$

Now from [14], p. 35, we know that the rank functions r and $\tilde{r}$ are related as follows:

$$\tilde{r}(X) = |X| + r(\bar{X}) - k.$$

Hence

$$R_i^v = \tilde{R}_{n-i}^{v+n-k-i}$$

for all u and i. Substituting this into (8) and changing the summation variable of the right hand side into $u := v + n - k - i$, we get

$$\sum_{j=0}^{n} \binom{n-j}{n-i} B_j = \sum_{u=0}^{n} q^{n-k-u} \tilde{R}_{n-i}^u, \qquad i = 0, 1, \ldots, n.$$

Now solve for the B_j. ■

Corollary 6 *The dual distance distribution of an almost affine code consists of nonnegative* integers.

Example 7 *(Continuation of Example 6). Substituting the values of R_v^u in (3), we obtain $B_0 = 1$, $B_j = 0$ for $1 \leq j \leq k$ and*

$$B_{k+t} = \binom{n}{n-k-t} \sum_{i=0}^{t-1} (-1)^i \binom{k+t}{i} (q^{t-i} - 1), \qquad t = 1, \ldots, n-k.$$

If $k \leq n-2$, the inequality $B_{k+2} \geq 0$ implies the condition

$$q \geq k + 1.$$

Combining this with the result of Example 6, we infer:
A q-ary code of length $n \geq 2q - 3$ and size M, $q < M < q^{n-1}$, cannot attain the Singleton bound.

Remark 12 *Using the notation of page 14, we can define the distance distribution* $(B_{\mathbf{j}})_{\mathbf{j}\in W(\mathcal{T})}$ *of a code* $\mathcal{C}$ *with* respect to a partition $\mathcal{T}$ *by means of the equations*

$$\sum_{\mathbf{j}\in W(\mathcal{T})}\left[\prod_{\alpha=1}^{p}\binom{n_\alpha-j_\alpha}{n_\alpha-i_\alpha}\right]A_{\mathbf{j}}=q^{k-n+\sum_\alpha i_\alpha}\sum_{\mathbf{j}\in W(\mathcal{T})}\left[\prod_{\alpha=1}^{p}\binom{n_\alpha-j_\alpha}{i_\alpha}\right]B_{\mathbf{j}},\quad \mathbf{i}\in W(\mathcal{T}).$$

The paper [10] contains a proof that the $B_{\mathbf{j}}$ *are nonnegative rational numbers. If* $\mathcal{C}$ *is* almost affine, *we can express the* $B_{\mathbf{j}}$ *in terms of the* $\tilde{R}^v_{\mathbf{i}}:=\tilde{R}^{v+k-\sum_\alpha i_\alpha}_{\mathbf{n}-\mathbf{i}}$:

$$B_{\mathbf{j}}=\sum_{\mathbf{i}\in W(\mathcal{T})}\left[\prod_{\alpha=1}^{p}(-1)^{i_\alpha+j_\alpha}\binom{n_\alpha-i_\alpha}{n_\alpha-j_\alpha}\right]\sum_{u=0}^{n}q^{n-k-u}\tilde{R}^u_{\mathbf{n}-\mathbf{i}},\quad \mathbf{j}\in W(\mathcal{T}).$$

(The proof is completely analogous to that of Proposition 7.) Hence the $B_{\mathbf{j}}$ *are nonnegative* integers.

9 Partial affine geometries

Let $\mathcal{C}\subseteq F^S$ be a k–dimensional q-ary almost affine code of length $n:=|S|$. We have seen in Corollary 1 that for any choice of $X\subseteq S$ and $\mathbf{x}\in\mathcal{C}$, the subset

$$\mathcal{C}(X,\mathbf{x}):=\{\mathbf{c}\in\mathcal{C}\mid \mathbf{c}_X=\mathbf{x}_X\}$$

of $\mathcal{C}$ is an almost affine subcode of $\mathcal{C}$ with dimension $d:=k-r(X)$. We shall call $\mathcal{C}(X,\mathbf{x})$ a d-dimensional *flat* of $\mathcal{C}$. Flats of dimension 0, 1, 2 and $k-1$ are called *points*, *lines*, *planes* and *hyperplanes* respectively. Two flats of the form

$$L_1:=C(X,\mathbf{x}),\ L_2:=C(X,\mathbf{y})$$

are said to be *parallel* (notation: $L_1\|L_2$). Note that parallel flats have the same dimension. The intersection properties of the flats in C follow directly from the obvious

Proposition 8 *If* $\mathbf{z}\in\mathcal{C}(X,\mathbf{x})\cap\mathcal{C}(Y,\mathbf{y})$ *then* $\mathcal{C}(X,\mathbf{x})\cap\mathcal{C}(Y,\mathbf{y})=\mathcal{C}(X\cup Y,\mathbf{z})$.

Remark 13 *If* $Y\supseteq X$, *then* $\mathcal{C}(Y,\mathbf{x})\subseteq\mathcal{C}(X,\mathbf{x})$. *The maximal set* $Y\supseteq X$ *such that* $\mathcal{C}(Y,\mathbf{x})=\mathcal{C}(X,\mathbf{x})$ *is the* closure $\mathrm{cl}(X)$ *of* X *in the matroid* $\mathcal{M}(\mathcal{C})$. *The closed sets of a matroid* $\mathcal{M}$, *i.e. the sets* X *with* $X=\mathrm{cl}(X)$, *are known to form a* geometric lattice *with respect to the inclusion ordering. (Cf. [14] or [6].)*

The flats of $\mathcal{C}$ share many properties with the affine subspaces of an affine space. We list a few:

- The flats parallel to a given flat partition $\mathcal{C}$. In other words, for each flat L and each point P there is exactly one flat L' with $P \in L'$ and $L' \| L$. The parallel classes are of the form

$$\mathcal{L}(X) := \{\mathcal{C}(X, \mathbf{x}) \mid \mathbf{x} \in \mathcal{C}\}.$$

  Note that the elements of parallel class $\mathcal{L}(X)$ are in one-one correspondence with the elements of $\mathcal{C}_X$ and that the parallel classes are in one-one correspondence with the closed sets of $\mathcal{M}(\mathcal{C})$.

- The intersection of two flats is either empty or a flat. So we can define the *span* $L \vee L'$ of two flats L, L' to be the smallest flat containing both L and L'. Generally, there is no "dimension formula", but if $L \cap L' \neq \emptyset$, then

$$\dim L \cap L' \geq \dim L + \dim L' - \dim L \vee L' \geq \dim L + \dim L' - k.$$

  This immediatyly follows from the fact that

$$\mathcal{C}(X, \mathbf{x}) \vee \mathcal{C}(Y, \mathbf{y}) \supseteq \mathcal{C}(X \cap Y, \mathbf{x})$$

  and the submodularity of the rank function:

$$r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y).$$

- If $L_1 \| L_2$, $L \cap L_1 \neq \emptyset$ and $L \cap L_2 \neq \emptyset$, then $(L \cap L_1) \| (L \cap L_2)$.

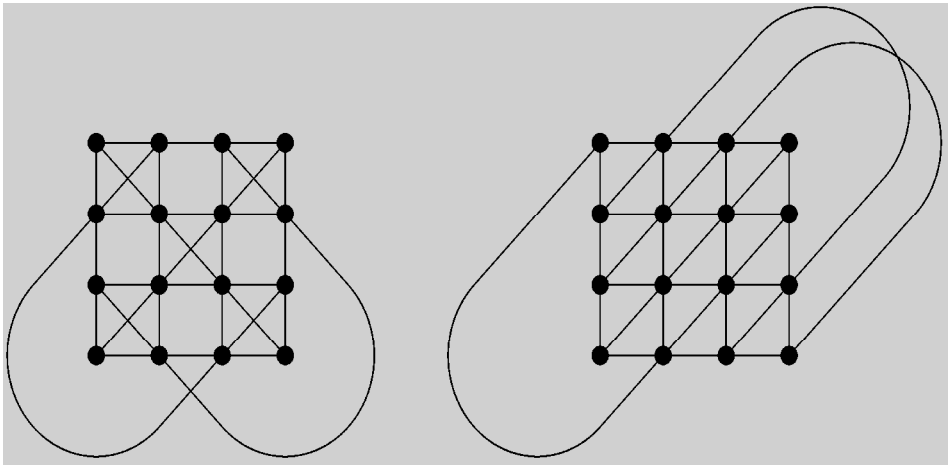
- Two hyperplanes either are parallel or intersect in a flat of dimension $k - 2$.

Generally, however, some properties of affine spaces are lacking because there are not enough flats. For example, $\mathcal{C}$ usually contains pairs of non-collinear points. This is why we call $\mathcal{C}$, together with its flats, a *partial affine geometry*. A formal definition is given at the end of this section.

Example 8 *Consider the almost affine codes $\mathcal{C}$ and $\mathcal{C}'$ of Example 5. In both cases, we have sixteen points and three sets of four parallel lines. If we arrange the points*

$$P_{i,j} := \{c_1 = i, c_2 = j\}$$

in a square grid in the obvious way, then the geometry can be depicted as follows



In the left hand geometry, we can add eight more lines to obtain the affine plane over the field $\mathbb{F}_4$. In the right hand geometry, not a single line can be added that intersects all existing lines in one point.

The partial affine geometry structure of an almost affine code can be used to show that certain matroids are not almost affinely representable. As an example, we treat the *Vámos matroid*. Let $S := \{1, 2, \ldots, 8\}$, and put $a := \{1, 2\}$, $b := \{3, 4\}$, $c := \{5, 6\}$ and $d := \{7, 8\}$. Then the Vámos matroid is the rank 4 matroid $\mathcal{V}$ over S for which all 4-sets are bases except $a \cup c$, $a \cup d$, $b \cup c$, $b \cup d$ and $c \cup d$.

Proposition 9 *The Vámos matroid is not almost affinely representable.*

Proof. Suppose that $\mathcal{C} \subseteq F^S$ is an almost affine code with $\mathcal{M}(\mathcal{C}) = \mathcal{V}$. Without loss of generality, we may assume that $F = \{0, 1, \ldots, q-1\}$, and that the zero vector $\mathbf{o}$ is contained in $\mathcal{C}$. Consider the four planes

$$L_i := \{\mathbf{c} \in \mathcal{C} \mid \mathbf{c}_i = \mathbf{o}_i\}, \quad i = a, b, c, d.$$

Then $L_a \cap L_b = \{\mathbf{o}\}$, because $a \cup b$ is a base. The other proper intersections $L_i \cap L_j$ are distinct lines passing through $\mathbf{o}$. Choose any point $\mathbf{x} \in L_b \cap L_c$, $\mathbf{x} \neq \mathbf{o}$, and put

$$L'_d := \{\mathbf{c} \in \mathcal{C} \mid \mathbf{c}_d = \mathbf{x}_d\}.$$

L'_d is the plane parallel to L_d and passing through $\mathbf{x}$. Note that $\mathbf{o} \notin L'_d$ because $L_b \cap L_c \cap L_d = \{\mathbf{o}\}$. (The set $b \cup c \cup d$ contains a base.) The plane L'_d intersects both L_b and L_c in lines containing x. Since $L'_d \cap L_c$ and $L_a \cap L_c$ are

nonparallel coplanar lines, they have a nonempty intersection. Hence $L'_d \cap L_a$ is a line. Similarly, since $L'_d \cap L_a$ and $L'_d \cap L_b$ are nonparallel coplanar lines, they have a nonempty intersection. But $L_a \cap L_b = \{\mathbf{o}\}$ and $\mathbf{o} \notin L'_d$. ■

Remark 14 *Since reduction and contraction of the matroid $\mathcal{M}(\mathcal{C})$ corresponds to puncturing and shortening of $\mathcal{C}$, the Vámos matroid is an excluded minor for almost affine representability.*

Remark 15 *In [8], Seymour proved that the Vámos matroid is not secret-sharing, a result that is equivalent to our Proposition 9. He ingeniously used graph theory, while our proof is based on geometric arguments of the kind that is generally used in matroid texts that treat the linear representability of matroids.*

In the beginning of this section, we promised a formal definition of a partial affine geometry. Here it is:

Definition 13 *A (finite)* partial affine geometry *is a pair $(A, \mathcal{H})$ where A is a finite set of* points *and where $\mathcal{H}$ is a family of subsets of equal size called* hyperplanes *such that*

1. *each point is an intersection of hyperplanes,*
2. *to each point $P \in A$ and each hyperplane $H \in \mathcal{H}$ there is exactly one hyperplane $H' \in \mathcal{H}$ such that $P \in H'$ and $H \cap H' \in \{\emptyset, H\}$. (We say that H and H' are* parallel *and write $H \| H'$),*
3. *if $\{H_1, H_2, \ldots, H_r\}, \{H'_1, H'_2, \ldots, H'_r\} \in \mathcal{H}$ are such that $\cap H_i \neq \emptyset, \cap H'_i \neq \emptyset$ and $H_i \| H'_i$ for $i = 1, 2, \ldots, r$, then $|\cap H_i| = |\cap H'_i|$.*

It is not hard to derive the basic properties of partial affine geometries:

- Parallelism defines an equivalence relation on $\mathcal{H}$. All classes have the same size, say q.
- Let us define a *flat* to be a nonempty intersection of hyperplanes. Then the size of all flats (the space A included) is a power of q. The exponent is called the *dimension* of the flat. Obviously, an intersection of flats is either empty or a flat.
- Two flats $L := \cap H_i, L' := \cap H'_i$ such that $H_i \| H'_i$ for $i = 1, 2, \ldots, r$ are said to be *parallel*. Notation $L \| L'$. Parallelism defines an equivalence relation on the family of the flats of a given dimension.

Remark 16 *A partial affine space $(A, \mathcal{H})$ can be used to construct an almost affine code: Let the sets*

$$\mathcal{H}_i := \{H_{i,1}, H_{i,2}, \ldots, H_{i,q}\}, \quad i = 1, 2, \ldots, n,$$

be the parallel classes of $\mathcal{H}$. Put $F := \{1, 2, \ldots, q\}$ and $S := \{1, 2, \ldots, n\}$. Then

$$\mathcal{C} := \{\mathbf{x} \in F^S \mid \bigcap_{i=1}^{n} H_{i,x_i} \neq \emptyset\}$$

is an almost affine code. In this way, we obtain, up to equivalence, all almost affine codes without constant or multiple columns, i.e. all almost affine codes with dual weights $B_1 = B_2 = 0$, i.e. all almost affine codes whose matroid is simple.

References

[1] Beimel, A. and B. Chor: *Universally Ideal Secret Sharing Schemes.* IEEE Transactions on Information Theory 40 (1994), pp. 786-794.

[2] Bertilsson, M.: *Linear Codes and Secret Sharing.* PhD Thesis. Linköping University (1993).

[3] Brickell, E.F. and D.M. Davenport: *On the Classification of Ideal Secret Sharing Schemes.* Journal of Cryptology 4 (1991)

[4] Delsarte, P.: *An Algebraic Approach to the Association Schemes of Coding Theory.* Philips Research Reports Supplements, No.10 (1973)

[5] Jackson, W.A. and K.M. Martin: *Geometric Secret Sharing Schemes and Their Duals.* Designs, Codes and Cryptography 4 (1994)

[6] Oxley, J.G.: *Matroid Theory.* Oxford University Press, Oxford (1992)

[7] Pilz, G.: *Near-Rings.* North-Holland, Amsterdam (1977)

[8] Seymour, P.D.: *On Secret-Sharing Matroids.* Journal of Combinatorial Theory B, 56 (1992)

[9] MacWilliams, F.J. and N.J.A. Sloane: *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam (1983)

[10] Simonis, J.: *MacWilliams Identities and Coordinate Partitions.* Linear Algebra and its Applications 216 (1995)

[11] Stevenson, F.W.: *Projective Planes.* Freeman, San Francisco (1972)

[12] Tolhuizen, L.M.G.M.: *On Maximum Distance separable codes over alphabets of arbitrary size.* Proc. 1994 IEEE International Symposium on Information Theory, Trondheim (1994), p.431.

[13] Van Lint, J.H. and R.M. Wilson: *A Course in Combinatorics.* Cambridge U.P., Cambridge (1992)

[14] Welsh, D.J.A.: *Matroid Theory.* Academic Press, London (1976)