Applications of finite geometry in coding theory and cryptography

A. KLEIN, L. STORME

Department of Mathematics, Ghent University, Krijgslaan 281 - Building S22, 9000 Ghent, Belgium (Email: {klein,ls}@cage.ugent.be) (WWW: http://cage.ugent.be/∼ {klein,ls})

Abstract. We present in this article the basic properties of projective geometry, coding theory, and cryptography, and show how finite geometry can contribute to coding theory and cryptography. In this way, we show links between three research areas, and in particular, show that finite geometry is not only interesting from a pure mathematical point of view, but also of interest for applications. We concentrate on introducing the basic concepts of these three research areas and give standard references for all these three research areas. We also mention particular results involving ideas from finite geometry, and particular results in cryptography involving ideas from coding theory.

Keywords. Finite geometry, MDS codes, Griesmer bound, Secret sharing, AES

1. Introduction to projective geometry

The classical Euclidean geometry contains two very interesting weaker geometries.

- The *absolute geometry* which explores what can be proved without the famous parallel postulate.
- The *affine geometry* which explores what can be proved without the axiom of measure (length and angles).

The axioms of the affine plane are:

(A1) Each two points are joined by exactly one line.
(A2) For each line l and each point P not on l, there is exactly one line through P which does not intersect l.
(A3) There are three points which do not lie on a common line.

When working in the affine plane, one almost always distinguishes between parallel and intersecting lines. This distinction can be removed by going to the projective closure. For each parallel class of lines we add a "point at infinity" which lies on all lines of the parallel class. There is also a "line at infinity" which goes through all the points at infinity.

This leads to the projective plane with the axioms:

(P1) Each two points are joined by exactly one line.

(P2) Each two lines meet in exactly one point.
(P3) There are at least two lines and each line contains at least three points.

To extend the projective geometry to higher dimensions, we must replace (P2) by an axiom that states that two lines in a plane have a common point. The Veblen-Young axiom does exactly this but avoids the use of the word plane.

(P2') Let A, B, C and D be four points such that the lines AB and CD intersect. Then AC and BD have a common point.

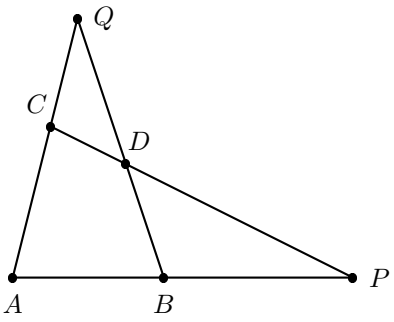

Figure 1. The Veblen-Young axiom

We now present the classical construction of a projective space.

Theorem 1
Let V be a vector space of dimension $d+1 \geq 3$ over a (skew) field $\mathbb{F}$. The geometry $PG(V)$ is defined by

- *The points of $PG(V)$ are the 1-dimensional subspaces of V.*
- *The lines of $PG(V)$ are the 2-dimensional subspaces of V.*
- *A point of $PG(V)$ is incident with a line of $PG(V)$ if the corresponding 1-dimensional subspace is contained in the corresponding 2-dimensional subspace.*

Then $PG(V)$ is a projective space.

Proof. Let $\langle v\rangle$, $\langle w\rangle$ be two points of PG(V), then $\langle v, w\rangle$ is the unique 2-dimensional subspace containing v and w, which proves axiom (P1).

Let $A = \langle u\rangle$, $B = \langle v\rangle$, $C = \langle w\rangle$, $D = \langle x\rangle$ be four points of $PG(V)$. If the lines $AB = \langle u, v\rangle$ and $CD = \langle w, x\rangle$ intersect in a common point, the dimension formula gives

$$\dim\langle u, v, w, x\rangle = \dim\langle u, v\rangle + \dim\langle w, x\rangle - \dim(\langle u, v\rangle \cap \langle w, x\rangle) = 2 + 2 - 1 = 3\,.$$

Again by the dimension formula, we get

$$\dim(\langle u, w\rangle \cap \langle v, x\rangle) = \dim\langle u, w\rangle + \dim\langle v, x\rangle - \dim\langle u, v, w, x\rangle = 2 + 2 - 3 = 1,$$

and hence $AC = \langle u, w\rangle$ and $BD = \langle v, x\rangle$ meet in a common point of PG(V). This proves axiom (P2').

Each line $\langle v, w\rangle$ of PG(V) contains at least three points $\langle v\rangle$, $\langle w\rangle$ and $\langle v + w\rangle$. Since $\dim V \geq 3$, there are at least two subspaces of dimension 2. This proves axiom (P3). $\square$

Two extremely important "Theorems" of projective geometry are:

Theorem 2 (Desargues Theorem)
Let $A_1A_2A_3$ and $B_1B_2B_3$ be two triangles for which the lines A_1B_1, A_2B_2 and A_3B_3 are different and go through a common point C.

Then the points $P_{12} = A_1A_2 \cap B_1B_2$, $P_{13} = A_1A_3 \cap B_1B_3$ and $P_{23} = A_2A_3 \cap B_2B_3$ lie on a common line.

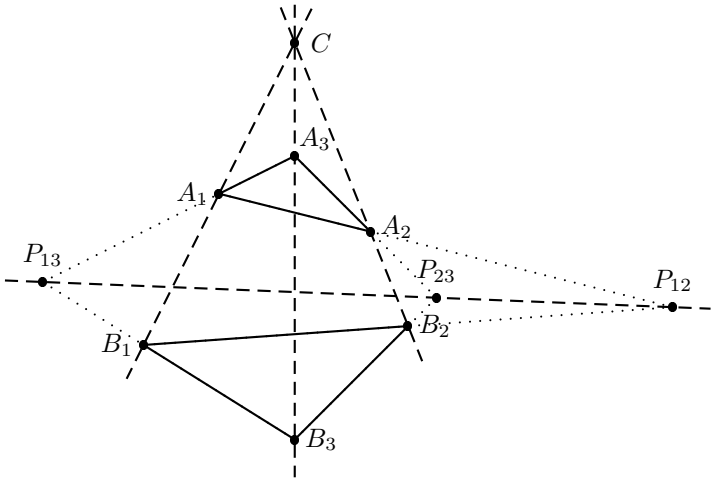

Figure 2. Desargues Theorem

Theorem 3 (Pappus Theorem)
Let l and h be two intersecting lines. Let A_1, A_2, A_3 be distinct points on l different from $l \cap h$ and let B_1, B_2, B_3 be distinct points on h different from $l \cap h$.

Then the points $G_{12} = A_1B_2 \cap A_2B_1$, $G_{13} = A_1B_3 \cap A_3B_1$ and $G_{23} = A_2B_3 \cap A_3B_2$ lie on a common line.

Without proof we note:

Theorem 4
A projective space satisfies the Theorem of Desargues if and only if it is of the form $PG(V)$ for some vector space V.

A projective space satisfies the Theorem of Pappus if and only if it is of the form $PG(V)$ for some vector space V over a commutative field $\mathbb{F}$.

In the following, all projective spaces will be of the form PG(V) where V is a finite dimensional vector space over a finite field $\mathbb{F}_q$ of order q. Let $d + 1$ be the dimension of V, then we also write PG(d, q) for PG(V).

Fix a basis $v_0, \ldots, v_d$ of V. Let $u = v_0 + \cdots + v_d$. Then any vector $v = a_0v_0 + \cdots + a_dv_d \in V$ is uniquely determined by its coordinates $(a_0, \ldots, a_d)$.

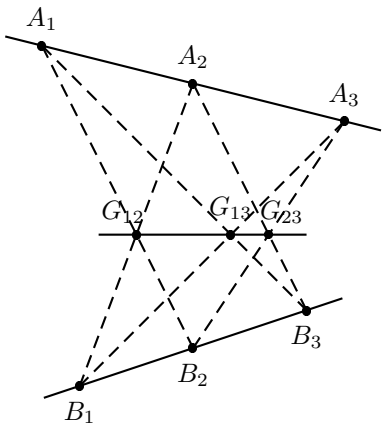

Figure 3. Pappus Theorem

We call $(a_0, \ldots, a_d)$ the *homogeneous coordinates* of the point $\langle v \rangle$ of PG(V) with respect to the projective reference system $\{\langle v_0 \rangle, \ldots, \langle v_d \rangle, \langle u \rangle\}$, where $u = v_0 + \cdots + v_d$. Since $\langle v \rangle = \langle \mu v \rangle$ for any $\mu \neq 0$ the homogeneous coordinates of a projective point are unique up to a nonzero scalar factor.

Example 1
The line through the points with homogeneous coordinates $(a_0, \ldots, a_d)$ *and* $(b_0, \ldots, b_d)$ *consists of the points with the following coordinates* $(a_0, \ldots, a_d)$ *and* $(b_0, \ldots, b_d) + x(a_0, \ldots, a_d)$*, with* $x \in \mathbb{F}$*.*

If V is a vector space over a finite field, then PG(V) has a finite number of points and lines. Theorem 5 counts them.

Theorem 5
The projective space $PG(d, q)$ *has* $\frac{q^{d+1}-1}{q-1} = q^d + q^{d-1} + \cdots + q + 1$ *points. and* $\frac{(q^d+q^{d-1}+\cdots+q+1)(q^{d-1}+q^{d-2}+\cdots+q+1)}{q+1}$ *lines.*

Each line of $PG(d, q)$ *contains exactly* $q + 1$ *points.*

Proof. The vector space $\mathbb{F}_q^{d+1}$ contains $q^{d+1} - 1$ nonzero vectors and a 1-dimensional subspace of $\mathbb{F}_q^{d+1}$ contains $q - 1$ nonzero vectors. Thus $\mathbb{F}_q^{d+1}$ has $\frac{q^{d+1}-1}{q-1}$ subspaces of dimension 1.

As special cases we have that a two dimensional vector space over $\mathbb{F}_q$ has $q + 1$ subspaces of dimension 1, i.e. a line of PG(d, q) has $q + 1$ points.

There are $(q^{d+1} - 1)(q^{d+1} - q)$ possibilities to choose linearly independent vectors $u, v \in \mathbb{F}_q^{d+1}$. Every two dimensional space $\langle u, v \rangle$ has $(q^2 - 1)(q^2 - q)$ different bases. Thus $\mathbb{F}_q^{d+1}$ contains

$$\frac{(q^{d+1} - 1)(q^{d+1} - q)}{(q^2 - 1)(q^2 - q)} = \frac{(q^d + \cdots + q + 1)(q^{d-1} + \cdots + q + 1)}{q + 1}$$

subspaces of dimension 2. □

As indicated in the abstract, projective geometry is first of all investigated because of its pure mathematical importance. But projective geometry is also important because of its links to other research areas. We now present coding theory, one of the most important research areas linked to projective geometry. For a detailed discussion of finite projective spaces we refer to [12, 13, 15].

2. Coding theory

2.1. Introduction to coding theory

When sending a message there is always a small probability for transmission errors. The goal of coding theory is to develop good codes to detect and correct transmission errors.

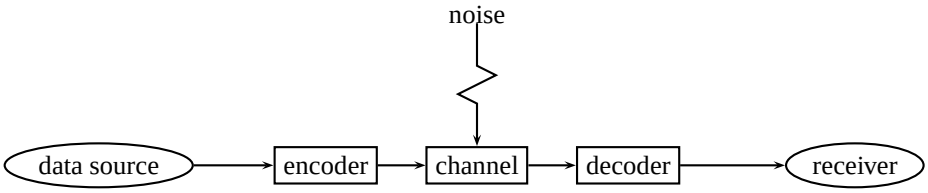

Figure 4. Transmission of data through a noisy communication channel

Suppose for example that we transmit a binary message. With a probability p of 2% a transmission error occurs and one 1 is received as 0 and vice versa.

Example 2 (Triple repetition code)
We repeat every symbol three times, i.e. we send 000 *instead of* 0 *and* 111 *instead of* 1*. If an error occurs we guess that the majority of the received symbols is correct, i.e. we will decode* 110 *as* 1*.*

The probability that more than 1 *error occurs in a triplet is* $3p^2(1-p)+p^3$*. If* $p = 0.02$ *we lowered the probability for incorrect decoding to* 0.0012*. The price is that we have to send* 3 *times more symbols.*

Example 3 (The Hamming code)
Now we use the following encoding

$$(x_0, x_1, x_2, x_3) \mapsto (x_0, \ldots, x_6)$$

with

$$\begin{aligned} x_4 &\equiv x_1 + x_2 + x_3 \mod 2\,, \\ x_5 &\equiv x_0 + x_2 + x_3 \mod 2\,, \\ x_6 &\equiv x_0 + x_1 + x_3 \mod 2\,. \end{aligned}$$

For example (1101) *is encoded as* (1101001).

Every 7*-bit word is either a codeword or differs at most one place from a codeword. The decoding will send the received word to the "most similar" codeword.*

If you compute the error probability for this example you will find that the average probability for a wrong bit is 0.0034 *when* $p = 0.02$.

Thus the Hamming code gives almost the same error probability as the simple triple repetition code, but we must send only $\frac{7}{4}$ *times more symbols. Thus the Hamming code allows a faster data transmission.*

The last example shows some important aspects:

- Linear mappings are often good codes.
- The mapping itself is not so important; the image under the map is the most important aspect of a code.
- Codewords should differ in as many positions as possible to obtain a good error correction rate.

This motivates the following definition.

Definition 1
The Hamming distance $d(x, y)$ *of* $x, y \in \mathbb{F}_q^n$*, with* $x = (x_1, \ldots, x_n)$ *and* $y = (y_1, \ldots, y_n)$*, is*

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

The Hamming distance of x *to* 0 *is called the* weight *of* x*;* $w(x) = d(x, 0)$.

A linear $[n, k]_q$ block code C *is a* k*-dimensional subspace of* $\mathbb{F}_q^n$.

The minimum distance d *of a linear* $[n, k]_q$ *block code* C *is defined as*

$$d = \min_{x \neq y \in C} d(x, y) = \min_{0 \neq x \in C} w(x) .$$

An $[n, k, d]_q$-code *is an* $[n, k]_q$*-code with minimum distance* d*.*

A generator matrix G *for an* $[n, k, d]_q$*-code* C *is a* $k \times n$ *matrix whose rows form a basis for the code* C.

A parity check matrix H *for an* $[n, k, d]_q$*-code* C *is an* $(n - k) \times n$ *matrix of rank* $n - k$ *whose rows are orthogonal to all the codewords of* C*, i.e.,*

$$c \in C \Leftrightarrow c \cdot H^t = 0.$$

A main goal of coding theory is to determine for given n, k and q the largest d for which an $[n, k, d]_q$-code exists.

A good introduction into coding theory is [20]. For further reference, see also [21, 25].

2.2. MDS codes

We start with a very simple upper bound on the minimum distance of an $[n, k]_q$-code. Consider the systematic generator matrix of an $[n, k]_q$-code:

$$G = \begin{pmatrix} 1 & & 0 & g_{1,k+1} & \dots & g_{1,n} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & g_{k,k+1} & \dots & g_{k,n} \end{pmatrix} = \left(I_k \; G_{k\times(n-k)} \right).$$

Each row of G has at most $n-k+1$ nonzero entries and hence $n-k+1 \geq d$.

Theorem 6 (Singleton bound [29])
An $[n,k,d]_q$-code satisfies $n-k+1 \geq d$.

Codes that meet the Singleton bound are called *maximum distance separable* codes (MDS codes).

Let C be an $[n,k,d]_q$ MDS code. Its parity check matrix H is an $(n-k)\times n$ matrix with the property that any $n-k$ columns of H are linearly independent.

Example 4 (Generalized Doubly-Extended Reed-Solomon (GDRS) codes [26])
Let $\mathbb{F}_q = \{0, a_1, \dots, a_{q-1}\}$.

Let

$$H = \begin{pmatrix} 0 & 1 & \cdots & 1 & 0 \\ 0 & a_1 & \cdots & a_{q-1} & 0 \\ 0 & a_1^2 & \cdots & a_{q-1}^2 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & a_1^{n-k-2} & \cdots & a_{q-1}^{n-k-2} & 0 \\ 1 & a_1^{n-k-1} & \cdots & a_{q-1}^{n-k-1} & 1 \end{pmatrix}.$$

For instance, the determinant of the $(n-k)\times(n-k)$ submatrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_{n-k} \\ \vdots & & \vdots \\ a_1^{n-k-1} & \cdots & a_{n-k}^{n-k-1} \end{pmatrix}$$

is $\prod_{1\leq i<j\leq n-k}(a_j - a_i) \neq 0$.

Any $n-k$ columns of H are linearly independent, i.e. H is a parity check matrix of an MDS code.

Interpreting the columns of H as points in a projective space, we get a structure called *arc*.

Definition 2
*An r-*arc *of $PG(n,q)$ is a set of r points that span $PG(n,q)$ and such that any hyperplane contains at most n points of this r-arc.*

The $(q+1)$-arc corresponding to a GDRS-code is called a *normal rational curve*. Here, $\{(1,t,\dots,t^{k-1}) | t \in \mathbb{F}_q\} \cup \{(0,\dots,0,1)\}$ is the standard form for a normal rational curve in PG$(k-1,q)$.

The study of linear MDS codes was performed mostly by geometrical methods. We now mention a number of the most important results.

Theorem 7 (Segre, Thas [27, 32])
For

- q *an odd prime power,*
- $2 \leq k < \sqrt{q}/4$*,*

every $[n = q + 1, k, d = q + 2 - k]$*-MDS code is a GDRS code.*

This preceding result was obtained using methods from algebraic geometry and projection arguments.

The motivation for the next result is as follows. The GDRS codes are MDS codes of length $q + 1$. Maybe they can be extended to MDS codes of length $q + 2$. The following result proves that this is practically never the case.

Theorem 8 (Storme [31])
Consider the $[q + 1, k, q - k + 2]_q$*-GDRS code.*

For q *odd and* $2 \leq k \leq q + 3 - 6\sqrt{q \log q}$*, and for* q *even and* $4 \leq k \leq q + 3 - 6\sqrt{q \log q}$*, this* $[q+1, k, q+2-k]_q$*-GDRS code cannot be not extended to a* $[q+2, k, q+3-k]_q$*-MDS code.*

2.3. Minihypers and the Griesmer bound

Let $N_q(d, k)$ denote the minimal n for which an $[n, k, d]_q$-code exists and let $\lceil x \rceil$ denote the smallest integer larger than or equal to x.

Theorem 9 (Griesmer bound [9, 30])

$$N_q(k, d) \geq d + N_q(k - 1, \lceil \frac{d}{q} \rceil) \tag{1}$$

and

$$N_q(k, d) \geq G_q(k, d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil . \tag{2}$$

Proof. Let C be an $[n, k, d]_q$-code. Without loss of generality we can assume that C contains the codeword $(0, \ldots, 0, 1, \ldots, 1)$ of weight d.

Thus we have a generator matrix of the form

$$G = \begin{pmatrix} 0 \cdots 0 & 1 \cdots 1 \\ G_1 & G_2 \end{pmatrix}.$$

This matrix G_1 has rank $k - 1$ since otherwise we could make a row of G_1 zero and C would contain a codeword of weight less than d. Thus G_1 is the generator matrix of an $[n - d, k - 1, d_1]_q$-code.

Let $(u, v) \in C$, with $w(u) = d_1$. Since also all codewords of the form $(u, v + a\mathbf{1})$ are in C, we can select v with weight at most $\lfloor \frac{q-1}{q} d \rfloor$.

Since $(u, v) \in C$, we have $w(u) + w(v) \geq d$ or $d_1 \geq d - \lceil \frac{d}{q} \rceil$. This proves Equation (1).

Iterating Equation (1) gives:

$$\begin{aligned} N_q(k,d) &\geq d + N_q(k-1, \lceil \frac{d}{q} \rceil) \\ &\geq d + \lceil \frac{d}{q} \rceil + N_q(k-2, \lceil \frac{d}{q^2} \rceil) \\ &\vdots \\ &\geq \sum_{i=0}^{k-2} \left\lceil \frac{d}{q^i} \right\rceil + N_q(1, \lceil \frac{d}{q^{k-1}} \rceil) \\ &\geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil . \end{aligned}$$

□

Now we want to construct linear codes that meet the Griesmer bound, i.e. we are interested in $[G_q(k,d), k, d]_q$-codes.

By $\theta_k = \frac{q^k-1}{q-1}$, we denote the number of 1-dimensional subspaces of $\mathbb{F}_q^k$, i.e. the number of points in PG$(k-1, q)$.

The *simplex* code S_k is a $[\theta_k, k, q^{k-1}]_q$-code whose generator matrix is formed by θ_k pairwise linearly independent vectors in $\mathbb{F}_q^k$. For each t, the copy of t simplex codes is a $[t\theta_k, tk, tq^{k-1}]_q$-code that satisfies the Griesmer bound.

An excellent way to construct more linear codes satisfying the Griesmer bound is to start with a copy of t simplex codes and delete columns of the generator matrix. The columns to be deleted form the generator matrix of what is called an *anticode*. This is a code with an upper bound on the distance between its codewords. Even the distance 0 between codewords is allowed, i.e. an anticode may contain repeated codewords.

Definition 3
If G is a $k \times m$ matrix of $\mathbb{F}_q$, then the q^k combinations of its rows form the codewords of an anticode *of length m. The* maximum distance *δ of the anticode is the maximum weight of any of its codewords. If $rank\, G = r$, each codeword occurs q^{k-r} times.*

If we start with t copies of the simplex code and delete m columns that form an anticode with maximum distance δ, we obtain a $[t\theta_k - m, k, tq^{k-1} - \delta]_q$-code.

Codes meeting the Griesmer bound and their anticodes have a nice geometrical interpretation.

Let C be an $[n,k]_q$-code with generator matrix G. Each column of the generator matrix describes a point of PG$(k-1, q)$. We represent C by the multiset M of these n points.

For instance, the simplex code S_k is represented by the point set of PG$(k-1, q)$.

An i-point is a point of multiplicity i. For each subset S of PG$(k-1, q)$, we denote the number of points of M in S by $c(S)$. Let

$$\gamma_i = \max\{c(S) \mid S \text{ is a subspace of dimension } i\} .$$

Then γ_0 is the maximal i for which an i-point in M exists. The minimum distance of C is the minimal number of points of M lying in the complement of a hyperplane, i.e. $d = n - \gamma_{k-2}$.

If an $[n, k, d]_q$-code meets the Griesmer bound we can compute the values γ_i from its parameters. At this moment we only need the following lemma.

Lemma 1 (Maruta [22])
Let $(s-1)q^{k-1} < d \leq sq^{k-1}$ and let C be an $[n, k, d]_q$-code meeting the Griesmer bound. Then $\gamma_0 = \max\{c(P) \mid P \in PG(k-1, q)\} = s$.

Proof. By the pigeonhole principle, we get $\gamma_0 \geq \frac{n}{\theta_{k-1}} > s - 1$.

Assume $\gamma_0 > s$, then there exists a point $P = (p_0, \ldots, p_{k-1})$ described by at least $s + 1$ columns of the generator matrix. Consider the subcode C' of C defined by

$$C' = \{x = (x_0, \ldots, x_{k-1}) \in \mathbb{F}_q^k \mid \sum_{i=0}^{k-1} x_i p_i = 0\}G \, .$$

The codewords of C' have entry 0 at the columns corresponding to P. Puncturing C' at these columns yields an $[n', k', d']_q$-code with $n' \leq n - s - 1$, $k' = k - 1$ and $d' \geq d$. But the Griesmer bound says that

$$n - s - 1 \geq n' \geq \sum_{i=0}^{k'} \lceil \frac{d'}{q^i} \rceil \geq \sum_{i=0}^{k-2} \lceil \frac{d}{q^i} \rceil = \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil - \lceil \frac{d}{q^{k-1}} \rceil = n - s,$$

a contradiction. □

We represent the linear code C by the multiset M' in which each point P of PG$(k-1, q)$ has weight $w(P)$ equal to s minus the number of columns in the generator matrix defining P. In fact, M' is the multiset of columns of the anticode corresponding to C in the copy of s simplex codes. We have shown above that for linear codes meeting the Griesmer bound $w(P) \geq 0$ for each point P. Let $d = sq^{k-1} - \sum_{i=0}^{k-2} t_i q^i$, $0 \leq t_i \leq q-1$ for $i = 0, \ldots, k-2$. Then the total weight of all points in M' is $\sum_{i=0}^{k-2} t_i \theta_{i+1}$ and each hyperplane has a weight of at least $n - d = \sum_{i=0}^{k-2} t_i \theta_i$.

This geometrical structure is important enough to deserve a name.

Definition 4
An $(n, w; d, q)$-minihyper *is a multiset of n points in $PG(d, q)$ with the property that every hyperplane meets it in at least w points.*

Many characterisation theorems of minihypers are known. The simplest is:

Theorem 10 (Bose and Burton [2])
Let $k \leq d$. A $(\theta_{k+1}, \theta_k; d, q)$-minihyper always is a k-dimensional subspace of $PG(d, q)$.

Proof. Let $\mathcal{H}$ be a $(\theta_{k+1}, \theta_k; d, q)$-minihyper. We claim that for $s \leq k$ every codimension s space of $PG(d, q)$ meets H in at least θ_{k-s+1} points.

For $s = 1$ this is the definition of a minihyper. Now let $s > 1$ and assume that a codimension s space π meets $\mathcal{H}$ in less than θ_{k-s+1} points. Then the average number of points of $\mathcal{H}$ in a codimension $s - 1$ space through π is less than

$$\frac{\theta_{k+1} - \theta_{k-s+1}}{\theta_s} + \theta_{k-s+1} = q^{k-s+1} + \theta_{k-s+1} = \theta_{k-s+2},$$

in contradiction to the already proved result that a codimension $s-1$ space contains at least θ_{k-s+2} points of $\mathcal{H}$.

Now assume that $\mathcal{H}$ is not a k-space of PG(d,q), i.e. there is a line l that contains at least two points of $\mathcal{H}$ but does not lie completely in $\mathcal{H}$. Let $P \in l \backslash \mathcal{H}$. There exists a subspace π' of dimension $d-k-1$ through P that has no point in common with $\mathcal{H}$. (There are simply not enough points in $\mathcal{H}$ to block all the $(d-k-1)$-spaces through P).

The average number of points of $\mathcal{H}$ in a $(d-k)$-space through π' is $\theta_{k+1}/\theta_{k+1} = 1$. But the $(d-k)$-space containing l contains at least 2 points of $\mathcal{H}$, thus there must be a $(d-k)$-space through π' that contains no point of $\mathcal{H}$. A contradiction, i.e. $\mathcal{H}$ is a subspace. □

There are many other characterization results on minihypers. We refer to the literature for the known results. As a concrete example of a deep characterization result, we mention the following result of Hamada, Helleseth, and Maekawa.

Theorem 11 (Hamada, Helleseth, and Maekawa [10, 11])
Let F be a $(\sum_{i=0}^{k-2} \epsilon_i \theta_{i+1}, \sum_{i=0}^{k-2} \epsilon_i \theta_i; k-1, q)$-minihyper, with $\sum_{i=0}^{k-2} \epsilon_i < \sqrt{q}+1$, then F is the union of ϵ_0 points, ϵ_1 lines, ..., ϵ_{k-2} $(k-2)$-dimensional subspaces, which all are pairwise disjoint.

2.4. Covering radius

For an e-error correcting code, we search for a large set of pairwise disjoint spheres of radius e in the Hamming space $\mathbb{F}_q^n$. The problem of covering codes is an opposite problem. Here, we wish to cover all the points of the Hamming space $\mathbb{F}_q^n$ with as few spheres as possible. Covering codes find applications in data compression.

Formally we define:

Definition 5
Let C be a linear $[n,k,d]_q$-code. The covering radius *of the code C is the smallest integer R such that every n-tuple in $\mathbb{F}_q^n$ lies at Hamming distance at most R from a codeword in C.*

The following theorem will be the basis for making the link with the geometrically equivalent objects of the *saturating sets in finite geometry*.

Theorem 12
Let C be a linear $[n,k,d]_q$-code with parity check matrix $H = (h_1 \cdots h_n)$.

Then the covering radius of C is equal to R if and only if every $(n-k)$-tuple over $\mathbb{F}_q$ can be written as a linear combination of at most R columns of H.

Definition 6
Let S be a subset of $PG(N,q)$. The set S is called ρ-saturating *when every point P from $PG(N,q)$ can be written as a linear combination of at most $\rho+1$ points of S.*

Taking into account Theorem 12, the preceding definition means that:

ρ-saturating sets S in $PG(n-k-1,q)$ determine the parity check matrices of linear $[n,k,d]_q$-codes with covering radius $R=\rho+1$.

Covering codes are linked to many geometrical objects.

Obviously the goal of covering codewords becomes easier when one can use more codewords. So we are interested in small covering codes or equivalently in small saturating sets.

Example 5 (Brualdi et al. [3], Davydov [5])
We construct a 1-saturating set in $PG(3,q)$ of size $2q+1$. We give the description via coordinates.

Take a conic $c=\{(1,t,t^2,0)|t\in\mathbb{F}_q\}\cup\{(0,0,1,0)\}$ in a plane $\pi: X_3=0$ of $PG(3,q)$ and let $P=(0,0,1,0)$ be a point of this conic c. For q even, let $P'=(0,1,0,0)$ be the nucleus of the conic. For q odd, let $P'=(0,1,0,0)$ be a point of the tangent line to c through P. Let l be a line through P not in π.

We claim that $\mathcal{S}=(c\cup l\cup\{P'\})\backslash\{P\}$ is a 1-saturating set in $PG(3,q)$.

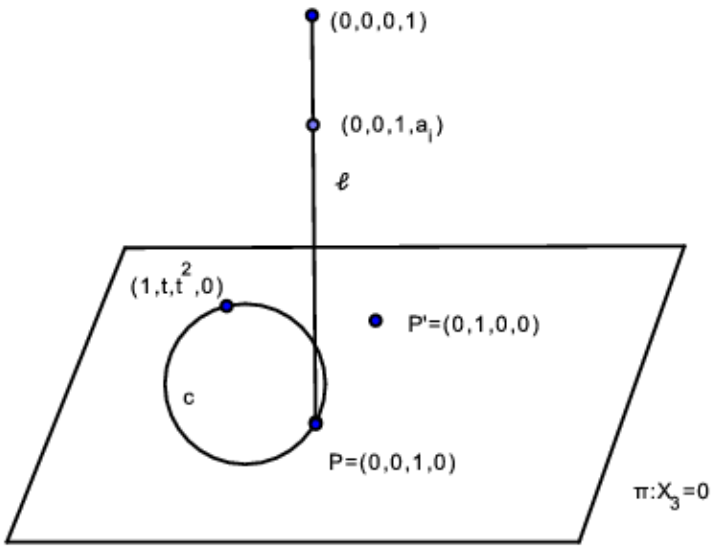

Figure 5. A 1-saturating set in PG$(3,q)$

First note that every point in the plane π lies on a secant of c. Now take a point Q not in π. Together with l, it spans a plane that either intersects the conic c in a point different from P or contains P'. Thus Q lies on a line which meets $\mathcal{S}$ in two points.

Example 6 (Östergård and Davydov [6])
Example 5 can be extended to a 2-saturating set in $PG(5,q)$ of size $3q+1$. We again give the description via coordinates.

Take two skew planes π and $\bar{\pi}$. Let c be a conic in π and let $\bar{c}$ be a conic in $\bar{\pi}$. Let P be a point of c and let $\bar{P}$ be a point of $\bar{c}$. For q even, let P' be the nucleus of c and for q odd, choose P' on the tangent line to c through P. Similarly choose $\bar{P}'$.

Then $\mathcal{S} = (c \cup \bar{c} \cup P\bar{P} \cup \{P', \bar{P}'\})\backslash\{P, \bar{P}\}$ is a 2-saturating set in PG$(5, q)$.

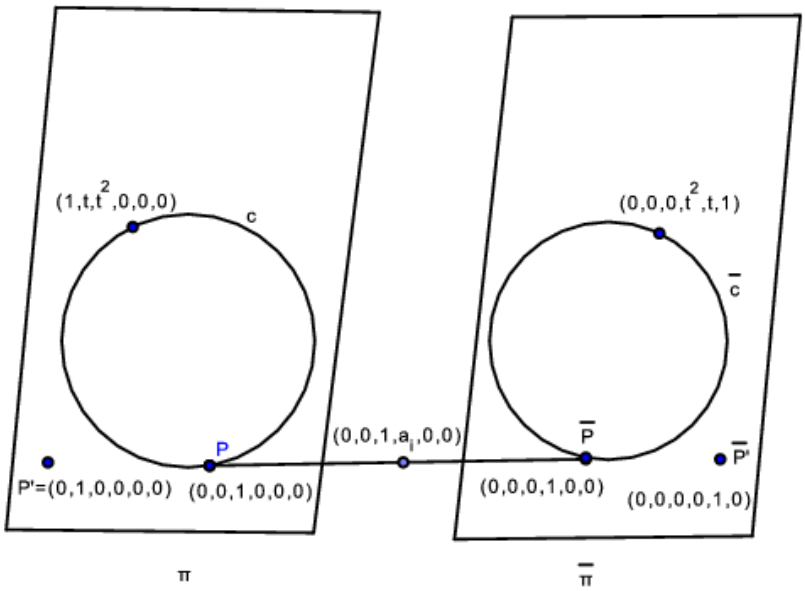

Figure 6. A 2-saturating set in PG$(5, q)$

As in Example 5, a point of π or $\bar{\pi}$ lies on a line meeting $\mathcal{S}$ in two points.

A point Q not in π or $\bar{\pi}$ lies on a unique line l' that meets both planes. As in Example 5, we get that $\langle l, l' \rangle$ meets $(c \cup \{P'\})\backslash\{P\}$ and $(\bar{c} \cup \{\bar{P}'\})\backslash\{\bar{P}\}$ in Q_1 and Q_2. The span $\langle Q, Q_1, Q_2 \rangle$ meets l in a point Q_3 and hence Q lies in the plane $\langle Q_1, Q_2, Q_3 \rangle$.

An interesting geometrical research problem, that in fact solves problems in coding theory, is therefore the problem of constructing small ρ-saturating sets in finite projective spaces.

3. Cryptography

3.1. Secret sharing

Secret sharing schemes are the cryptographic equivalents of a vault that needs several keys to be opened. In the simplest cases there are n participants and each group of k participants can reconstruct the secret, but less than k participants have no way to learn anything about the secret.

Example 7 (Shamir's k-out-of-n secret sharing scheme [28])
Let $\mathbb{F}$ be a finite field.

The dealer chooses a polynomial $f \in \mathbb{F}[x]$ of degree at most $k-1$ and gives participant number i a point $(x_i, f(x_i))$ on the graph of f ($x_i \neq 0$). The value $f(0)$ is the secret.

A set of k participants can reconstruct f by interpolation. Then they can compute the secret $f(0)$. If $k' < k$ persons try to reconstruct the secret, they see that for every value $y \in \mathbb{F}$ there are exactly $|\mathbb{F}|^{k-k'-1}$ polynomials of degree at most $k-1$ which pass through their shares and the point $(0, y)$. Thus they gain no information about $f(0)$.

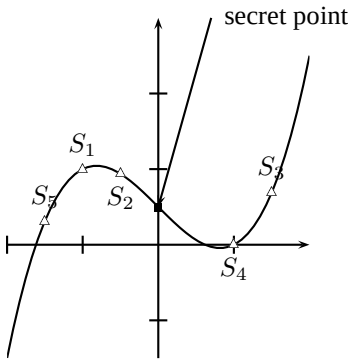

Figure 7. Example for the Shamir secret sharing scheme

Many secret sharing schemes are constructed by finite geometry. For example one can use arcs to construct a k-out-of-n secret sharing scheme.

Example 8
Let π be a hyperplane of $PG(k, q)$ and let $P_0, \ldots, P_n$ be an $(n+1)$-arc in π. Let l be a line of $PG(k, q)$ with $\pi \cap l = P_0$.

The participant number i ($1 \leq i \leq n$) gets the point P_i as his share. All participants are told that the secret point P_0 lies on l, but the hyperplane π is kept secret by the dealer.

Less than k participants see the following: their shares $P_1, \ldots, P_i$ ($i < k$) span an $(i-1)$-dimensional space skew to l. For every point $P' \in l$ there exists a hyperplane π' with an arc containing $P', P_1, \ldots, P_i$. Thus there is no way to decide which point of l is the secret P_0.

At least k participants can compute the span $\langle P_1, \ldots, P_k \rangle = \pi$ with their shares. The secret point P_0 is computed as $\pi \cap l$.

Thus we have constructed a k-out-of-n secret sharing scheme.

One can consider more complex access structures. For example, we want that three staff members together can open the vault, but also two senior staff members alone can open the vault. Definition 7 formalises the idea of an access structure.

Definition 7
Let P be a set of persons.

An access structure Γ *is a subset of $\mathcal{P}(P)$ with the property*

$$A \in \Gamma \implies B \in \Gamma$$

for every $B \supset A$.

Example 8 shows how to realise a k-out-of-n access structure with finite geometry. We want to generalise this example. The secret and the shares should be subspaces of a finite projective space PG(n, q). As in Example 8, the reconstruction of the secret should be done by computing the span of the shares. This leads to the following definition.

Definition 8
Let Γ be an access structure for the person set P. A subspace configuration *for Γ is a set of subspaces S_p, with $p \in P$, and a secret space S with the properties*

- $S \cap \langle S_p \mid p \in A \rangle = \emptyset$ *for all* $A \notin \Gamma$.
- $S \subseteq \langle S_p \mid p \in A \rangle$ *for all* $A \in \Gamma$.

Theorem 13 (Ito, Saito and Nishizeki [16])
Let Γ be an access structure, then there exists a subspace configuration realising Γ in PG(d, q), for d large enough.

Proof. Let $\mathfrak{U} = \{U_0, \ldots, U_d\}$ be the set of maximal unauthorised sets of Γ. (A set $A \notin \Gamma$ is maximal unauthorised if every proper superset $B \supset A$ is in Γ.) We will construct a subspace configuration for Γ in PG(d, q). Let e_i, the i-th vector of unity, correspond to the set U_i.

For $p \in P$, define $S_p = \langle e_i \mid p \notin U_i \rangle$ and let $S = \langle (1, \ldots, 1) \rangle$.

An unauthorised set of persons U is contained in at least one maximal unauthorised set U_i. By construction, $e_i \notin \bigcup_{p \in U} S_p$ and hence $\langle \bigcup_{p \in U} S_p \rangle$ cannot contain e_i and $S = \langle (1, \ldots, 1) \rangle$, i.e. the secret is not reconstructed.

If Q is a qualified set of persons then for every maximal unauthorised set U_i, Q contains a person p_i not in U_i. Hence, $e_i \in S_{p_i} \subseteq \bigcup_{p \in Q} S_p$ for every i. This proves that $S = \langle (1, \ldots, 1) \rangle \subseteq \langle S_p \mid p \in Q \rangle$, i.e. the persons from Q can reconstruct the secret. □

For further applications of finite geometry in secret sharing, see [17].

Secret sharing schemes can also be constructed by error-correcting codes.

Example 9 (McEliece and Sarwarte [24])
Let C be an $[n + 1, k, n - k + 2]_q$ MDS code.

For a secret $c_0 \in \mathbb{F}_q$, the dealer creates a codeword $c = (c_0, c_1, \ldots, c_n) \in C$. The share of the participant number i is symbol c_i.

Since C is an MDS code with minimum distance $n - k + 2$, the codeword c can be uniquely reconstructed if only k symbols are known.

So any set of k persons can compute the secret c_0.

On the other hand, less than k persons do not learn anything about the secret, since for any possible secret c', the same number of codewords that fit to the secret c' and their shares exist.

This is an alternative description of the k-out-of-n secret sharing scheme from Example 8.

The use of error-correcting codes for describing secret sharing schemes motivates the following definition.

Definition 9 (Massey [23])
The support *of a word $c \in \mathbb{F}_q^n$ is defined by*

$$\sup(c) = \{i \mid c_i \neq 0\}.$$

Let C be a linear code.

A nonzero codeword $c \in C$ is called minimal *if*

$$\forall c' \in C : \sup(c') \subseteq \sup(c) \implies c' \in \langle c \rangle .$$

Lemma 2 (Massey [23])
Let C be an $[n+1, k]_q$-code. A secret sharing scheme is constructed from C by choosing a codeword $c = (c_0, \ldots, c_n)$. The secret is c_0 and the shares of the participants are the coordinates c_i ($1 \leq i \leq n$).

The minimal qualified sets of the secret sharing scheme correspond to the minimal codewords of $C^\perp$ with 0 in their supports.

Proof. Suppose the set $\{1, \ldots, k\}$ is a qualified set. This means that c_0 can be determined from $c_1, \ldots, c_k$, i.e. there exist constants $a_1, \ldots, a_k$, with

$$c_0 = a_1 c_1 + \cdots + a_k c_k, \tag{3}$$

which means that $(1, -a_1, \ldots, -a_k, 0, \ldots, 0)$ is a codeword of $C^\perp$ with 0 in its support.

On the other hand a codeword of $C^\perp$ with 0 in its support gives an equation of type (3) and hence its support, minus the zero position, defines a qualified set of participants. □

3.2. Authentication codes

Consider the following cryptographic problem: Alice wants to send Bob a message m. Perhaps an attacker intercepts the message and sends an alternated message to Bob. How can Bob be sure that the message he gets is the correct one. One solution is that Alice and Bob agree on a secret key K. Alice computes an authentication tag $e_K(m)$ and sends $m \| e_K(m)$ to Bob. Then Bob can check that the authentication tag fits to the message and since the key K is private he knows that Alice has computed $e_K(m)$. This leads to:

Definition 10
A message authentication code (MAC) *is a 4-tuple $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ with*

1. *$\mathcal{S}$ a finite set of source states (messages).*
2. *$\mathcal{A}$ a finite set of authentication tags.*
3. *$\mathcal{K}$ a finite set of keys.*
4. *For each $K \in \mathcal{K}$, we have an authentication rule $e_K \in \mathcal{E}$ with $e_K : \mathcal{S} \to \mathcal{A}$.*

The security of a MAC is measured by the following probabilities.

Definition 11
Let p_i denote the probability of an attacker to construct a pair $(s, e_K(s))$ without knowledge of the key K, if he only knows i different pairs $(s_j, e_K(s_j))$. The smallest value r for which $p_{r+1} = 1$ is called the order *of the scheme.*

For $r = 1$, the probability p_0 is also known as the probability of an impersonation attack *and the probability p_1 is called the probability of a* substitution attack.

Example 10
Let π be a projective plane of order q and let l be a line of π.

The possible messages should be the points of l. As keys we take the points in the affine plane $\pi \backslash l$ and as authentication tags $e_K(s)$ we take the line through the message s and the key K.

If an attacker wants to create a message $(s, e_K(s))$ without knowing the key K, he must guess an affine line through s. There are q possibilities, i.e. the chance for an impersonation attack is $\frac{1}{q}$.

If the attacker already knows an authenticated message $(s', e_K(s'))$, he knows that the key K must lie on the line $e_K(s')$. But for every of the q affine points on that line there exists a line through s. So he cannot do better than guess the key on $e_K(s')$ which gives a probability of $\frac{1}{q}$ for a successful substitution attack.

In the following we will generalise Example 10 and show that it is optimal.

One can bound the number of keys by the attack probabilities. For $r = 1$ and $p_0 = p_1$, it is stated in [8], and for arbitrary r with $p_0 = p_1 = \cdots = p_r$, it was proven in [7].

Theorem 14
If a MAC has attack probabilities $p_i = 1/n_i$ ($0 \leq i \leq r$), then $|\mathcal{K}| \geq n_0 \cdots n_r$.

Proof. Suppose that we send the messages $(s_1, e_K(s_1)), \ldots, (s_r, e_K(s_r))$. Let $\mathcal{K}_i$ be the set of all keys which give the same authentication tag for the first i messages, i.e.

$$\mathcal{K}_i = \{\hat{K} \in \mathcal{K} \mid e_{\hat{K}}(s_j) = e_K(s_j) \text{ for } j \leq i\} .$$

By definition, we have $\mathcal{K}_0 = \mathcal{K}$. Formally, we define $\mathcal{K}_{r+1} = \{K\}$.

An attacker who knows the first i messages can create a false signature by guessing a key $\hat{K} \in \mathcal{K}_i$ and computing $e_{\hat{K}}(s_{i+1})$. The attack is successful if $\hat{K} \in \mathcal{K}_{i+1}$. Therefore

$$p_i \leq \frac{|\mathcal{K}_{i+1}|}{|\mathcal{K}_i|}.$$

Multiplying these inequalities proves the theorem. □

A MAC that satisfies this theorem with equality is called *perfect*.

A geometrical construction of perfect MACs uses generalised dual arcs [18, 19].

Definition 12
A generalised dual arc *$\mathcal{D}$ of order l with dimensions $d_1 > d_2 > \cdots > d_{l+1}$ of $PG(n, q)$ is a set of subspaces of dimension d_1 such that:*

1. *each j of these subspaces intersect in a subspace of dimension d_j, $1 \leq j \leq l+1$,*
2. *each $l + 2$ of these subspaces have no common intersection.*

We call $(n, d_1, \ldots, d_{l+1})$ the parameters *of the dual arc.*

Construction 1
Let $PG(V)$ be an n-dimensional space with basis e_i ($0 \leq i \leq n$).

Let $PG(W)$ be an $\left(\binom{n+d+1}{d+1} - 1\right)$-dimensional space with basis $e_{i_0,\ldots,i_d}$ ($0 \leq i_0 \leq i_1 \leq \cdots \leq i_d \leq n$).

To simplify notations, we will write $e_{i_0,\ldots,i_d}$ with $0 \leq i_0, \ldots, i_d \leq n$ when we mean the vector $e_{i_{\sigma(0)},\ldots,i_{\sigma(d)}}$ where σ is a permutation with $0 \leq i_{\sigma(0)} \leq i_{\sigma(1)} \leq \cdots \leq i_{\sigma(d)} \leq n$.

Let $\theta : V^{d+1} \to W$ be the multilinear mapping

$$\theta : (\sum_{i_0=0}^{n} x_{i_0}^{(0)} e_{i_0}, \ldots, \sum_{i_d=0}^{n} x_{i_d}^{(d)} e_{i_d}) \mapsto \sum_{0 \leq i_0,\ldots,i_d \leq n} x_{i_0}^{(0)} \cdot \ldots \cdot x_{i_d}^{(d)} e_{i_0,\ldots,i_d} \ . \quad (4)$$

For each point $P = [x]$ of $PG(V)$, we define a subspace $D(P)$ of $PG(W)$ by

$$D(P) = \langle \theta(x, v_1, \ldots, v_d) \mid v_1, \ldots, v_d \in V \rangle \ . \quad (5)$$

.

Theorem 15
The set $\mathcal{D} = \{D(P) \mid P \in PG(V)\}$ is a generalised dual arc with dimensions $d_i = \binom{n+d+1-i}{d+1-i} - 1, i = 0, \ldots, d+1$.

Proof. Since θ is a multilinear form, we get

$$D(P_0) \cap \cdots \cap D(P_{k-1}) = \langle \theta(x_0, \ldots, x_{k-1}, v_k, \ldots, v_d) \mid v_k, \ldots, v_d \in V \rangle$$

and hence $\dim(D(P_0) \cap \cdots \cap D(P_{k-1})) = \binom{n+d+1-k}{d+1-k} - 1$. (The -1 is because the projective dimension is one less than the vector space dimension). □

The link between dual arcs and MACs is:

Theorem 16
Let π be a hyperplane of $PG(n+1, q)$ and let $\mathcal{D}$ be a generalised dual arc of order l in π with parameters $(n, d_1, \ldots, d_{l+1})$.

The elements of $\mathcal{D}$ are the messages and the points of $PG(n+1, q)$ not in π are the keys. The authentication tag that belongs to a message and a key is the generated (d_1+1)-dimensional subspace.

This defines a perfect MAC of order $r = l + 1$ with attack probabilities

$$p_i = q^{d_{i+1} - d_i}.$$

Proof. After i message tag pairs $(m_1, t_1), \ldots, (m_i, t_i)$ are sent, the attacker knows that the key must lie in the (d_i+1)-dimensional space $\pi = t_1 \cap \cdots \cap t_i$. This space contains q^{d_i+1} different keys. A message m_{i+1} intersects $m_1 \cap \cdots \cap m_i$ in a d_{i+1}-dimensional space π'. Two keys K and $\bar{K}$ generate the same authentication tag if and only if K and $\bar{K}$ generate together with π' the same $(d_{i+1}+1)$-dimensional space. Thus the keys form groups of size $q^{d_{i+1}+1}$ and keys from the same group give the same authentication tag.

The attacker has to guess a group. The probability to guess the correct group is $p_i = q^{d_{i+1}+1}/q^{d_i+1}$. □

3.3. AES

In 1997 the American National Institute of Standards and Technology started a competition to design a successor for the old Data Encryption Standard DES. In 2000 the proposal of J. Daemen and V. Rijmen was selected as the new advanced encryption standard AES [4].

AES works on 128 bit words which are interpreted as 4×4 matrices over the field $\mathbb{F}_{256}$.

The non-linear part of the AES substitution replaces every matrix element by its inverse in $\mathbb{F}_{256}$.

An other part of the AES is the mix column step which has a link to coding theory. Purpose of this step is to spread a change in the input (Diffusion).

The input of the mix column step is a vector of four bytes $(a_1, \ldots, a_4)$ and its output are four bytes $(b_1, \ldots, b_4)$. It should have the following properties:

- Implementation of the mix column step should be simple and fast.
- It should have optimal diffusion (a difference in k input bytes ($1 \leq k \leq 4$) should result in the difference of at least $5 - k$ output bytes).

To satisfy the first condition the designers chose the mix column step to be a linear mapping, i.e. mix column is done by

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} m_{1,1}\, m_{1,2}\, m_{1,3}\, m_{1,4} \\ m_{2,1}\, m_{2,2}\, m_{2,3}\, m_{2,4} \\ m_{3,1}\, m_{3,2}\, m_{3,3}\, m_{3,4} \\ m_{4,1}\, m_{4,2}\, m_{4,3}\, m_{4,4} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}.$$

To satisfy the second property, every square submatrix of $M = (m_{i,j})$ must be non-singular. This is equivalent to

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

is the parity check matrix of a $[8, 4, 5]$ MDS code over $\mathbb{F}_{256}$.

Any MDS code would do the job. The designers of AES chose the following matrix:

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

where α is a root of $x^8 + x^4 + x^3 + x + 1$.

The simple structure of AES mix columns has some additional advantages for the implementation.

- We have $b_1 = f(a_1, a_2, a_3, a_4)$, $b_2 = f(a_2, a_3, a_4, a_1)$, $b_3 = f(a_3, a_4, a_1, a_2)$ and $b_4 = f(a_4, a_1, a_2, a_3)$. Thus we must implement only one linear function $f : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}$.

- $f(a_1, a_2, a_3, a_4) = \alpha(a_1 + a_2) + (a_2 + a_3 + a_4)$
  Addition in $\mathbb{F}_{256}$ is just a bitwise XOR. This is a cheap operation.
  The only difficult operation is the multiplication with α. Most AES implementations do this operation by a table look up.

Remark 1
This concludes this article describing applications of finite geometry in coding theory and cryptography, and also ideas from coding theory applied to cryptography. For all three research areas, we have given standard references. For a survey article containing a large number of tables with results on substructures in finite geometry, we refer to [14], and for a collected work describing current research topics in finite geometry and their applications in coding theory and cryptography, we refer to [1]. This latter collected work can guide interested readers to research in finite geometry and its applications, enabling them to contribute to finite geometry and its applications.

References

[1] J. De Beule and L. Storme, editors. *Current Research Topics in Galois Geometry*. Nova Academic Publishers, to appear.

[2] R.C. Bose and R.C. Burton. A characterization of flat spaces in a finite projective geometry and the uniqueness of the Hamming and the Macdonald codes. *J. Comb. Theory*, 1:96–104, 1966.

[3] R.A. Brualdi, V.S. Pless, and R.M. Wilson. Short codes with a given covering radius. *IEEE Trans. Inform. Theory*, 35:99–109, 1989.

[4] J. Daemen and V. Rijmen. *The Design of Rijndael, AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer Verlag, 2002.

[5] A.A. Davydov. Constructions and families of covering codes and saturated sets of points in projective geometry. *IEEE Trans. Inform. Theory*, 41(6, part 2):2071–2080, 1995.

[6] A.A. Davydov and P. Östergård. On saturating sets in small projective geometries. *European J. Combin.*, 21:563–570, 2000.

[7] V. Fåk. Repeated use of codes which detect deception. *IEEE Trans. Inform. Theory*, IT-25(2):233–234, 1979.

[8] E.N. Gilbert. Codes which detect deception. *The Bell System Technical Journal*, 53(3):405–421, 1974.

[9] J.H. Griesmer. A bound for error correcting codes. *IBM J. Res. Develop.*, 4:532–542, 1960.

[10] N. Hamada and T. Helleseth. A characterization of some q-ary codes ($q > (h-1)^2$, $h \geq 3$) meeting the Griesmer bound. *Math. Japon.*, 38:925–939, 1993.

[11] N. Hamada and T. Maekawa. A characterization of some q-ary linear codes ($q > (h-1)^2$, $h \geq 3$) meeting the Griesmer bound. II. *Math. Japon.*, 46:241–252, 1997.

[12] J.W.P. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. The Clarendon Press Oxford University Press, 1985.

[13] J.W.P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[14] J.W.P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. In *Finite Geometries, Proceedings of the* Fourth Isle of Thorns Conference *(Chelwood Gate, July 16-21, 2000) (Eds. A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel and J.A. Thas), Developments in Mathematics*, volume 3, pages 201–246. Kluwer Academic Publishers, 2001.

[15] J.W.P. Hirschfeld and J.A. Thas. *General Galois geometries*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991.

[16] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. *J. Cryptology*, 6:15–20, 1993.

[17] W.-A. Jackson, K.M. Martin, and C.M. O'Keefe. Geometrical contributions to secret sharing theory. *J. Geom.*, 79:102–133, 2004.

[18] A. Klein, J. Schillewaert, and L. Storme. Generalised dual arcs and Veronesean surfaces, with applications to cryptography. *J. Combin. Theory, Ser. A*, 116:684–698, 2009.

[19] A. Klein, J. Schillewaert, and L. Storme. Generalised Veroneseans. *Adv. Geom.*, submitted.
[20] J.H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, 3 edition, 1998.
[21] F.J. MacWilliams and N.J.A. Sloane. *The theory of error correcting codes*, volume 16 of *North-Holland Mathematical Library*. North-Holland, Amsterdam, London, New York, Tokyo, 1977.
[22] T. Maruta. On the Achievement of the Griesmer Bound. *Des. Codes Cryptogr.*, 12:83–87, 1997.
[23] J.L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, 1993.
[24] R.J. McEliece. On sharing secrets and Reed-Solomon codes. *Comm. ACM*, 24:583–584, 1981.
[25] V.S. Pless, W.C. Huffman, and R.A. Brualdi, editors. *Handbook of coding theory. Vol. I, II*. North-Holland, Amsterdam, 1998.
[26] I.S. Reed and G. Solomon. Polynomial codes over certain finite fields. *J. SIAM*, 8:300–304, 1960.
[27] B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl. (4)*, 39:357–379, 1955.
[28] A. Shamir. How to share a secret. *Comm. ACM*, 22:612–613, 1979.
[29] R.C. Singleton. Maximum distance q-ary codes. *IEEE Trans. Inform. Theory*, 10:116–118, 1964.
[30] G. Solomon and J.J. Stiffler. Algebraically punctured cyclic codes. *Inform. and Control*, 8:170–179, 1965.
[31] L. Storme. Completeness of normal rational curves. *J. Algebraic Combin.*, 1:197–202, 1992.
[32] J.A. Thas. Normal rational curves and k-arcs in Galois spaces. *Rend. Mat. (6)*, 1:331–334, 1968.