Snapshots of modern mathematics
from Oberwolfach

№ 10/2021

# Finite geometries: pure mathematics close to applications

Leo Storme

The research field of finite geometries investigates structures with a finite number of objects. Classical examples include vector spaces, projective spaces, and affine spaces over finite fields. Although many of these structures are studied for their geometrical importance, they are also of great interest in other, more applied domains of mathematics. In this snapshot, finite vector spaces are introduced. We discuss the geometrical concept of partial $t$-spreads together with its implications for the "packing problem" and a recent application in the existence of "cooling codes".

## 1 Finite fields and finite vector spaces

### 1.1 Finite fields

A *field* is a mathematical structure in which addition, subtraction, multiplication, and division between its objects are defined. The set of real numbers $\mathbb{R}$ equipped with the usual arithmetic operators is one example of a field.

We are all used to performing arithmetic with real numbers. But many people do not realise that, even from a young age, they also know how to perform arithmetic with numbers from another field known as a "prime field". Before we explain the precise meaning of this term, we first recall that a *prime* *number* is a positive integer $p > 1$, only divisible by 1 and itself. For example, the first few prime numbers are $2, 3, 5, 7$, and 11.

Once a prime number $p$ is fixed, it is possible to perform calculations within the set of non-negative integers less than $p$ using *modulo arithmetic*. The key difference in modulo arithmetic, as compared to standard arithmetic, is that the result of any calculation is always a non-negative integer less than $p$.

In order to be more precise, let us denote $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ where $p$ is our fixed prime number. To compute using modulo arithmetic in $\mathbb{F}_p$, we first calculate as usual in the set of integers. If the end result does not belong to $\mathbb{F}_p$, then we replace it by its remainder when divided by $p$. When equipped with modulo arithmetic, the set $\mathbb{F}_p$ is a *prime field* or, more precisely, a *prime field of order p*. Here "order $p$" refers to the size of the field $\mathbb{F}_p$ in the sense that it contains $p$ numbers.

We illustrate this via examples in $\mathbb{F}_7 = \{0, 1, \ldots, 6\}$. When we want to make it clear that calculations have been performed using modulo arithmetic in $\mathbb{F}_7$, we write "mod 7" at the end of a computation.

$$\begin{aligned} 2 + 3 &= 5 \pmod 7 \\ 2 \cdot 3 &= 6 \pmod 7 \\ 3 \cdot 4 &= 5 \pmod 7 \end{aligned}$$

In the first two examples, the result of standard integer arithmetic was already contained in $\mathbb{F}_p$ and hence the final result in modulo arithmetic is the same. We now explain the last example which is more involved. First of all, we note that $3 \cdot 4 = 12$, which is larger than 6. Since we perform calculations modulo 7, we then divide 12 by 7, leading to $12 = 1 \cdot 7 + 5$. Thus, as the remainder of 12 after division by 7 is equal to 5, we have $3 \cdot 4 = 5 \pmod 7$ as claimed.

Note that the above examples did not rely on the non-negative integer $p$ being prime. One of the reasons for this requirement arises when we want to perform division. For instance, in standard arithmetic with real numbers, an equation of the form

$$2 \cdot x = 1$$

always has exactly one solution, although it need not necessarily be an integer. Indeed, the non-integer solution in our example is given by $x = {}^1\!/_2$. In modulo arithmetic, however, it is necessary for $p$ to be prime in order for such equations to always have a unique solution in $\mathbb{F}_p$. For instance, the above equation in $\mathbb{F}_7$ yields

$$2 \cdot x = 1 \pmod 7 \quad \Longleftrightarrow \quad x = 4.$$

This idea of modulo arithmetic in $\mathbb{F}_7$ is actually more familiar than it may first seem. In fact, everybody does it when calculating with the days of the week. To see this, we assign an integer to each day of the week as follows:

$$\text{SUNDAY} = 0, \text{MONDAY} = 1, \text{TUESDAY} = 2, \text{WEDNESDAY} = 3,$$
$$\text{THURSDAY} = 4, \text{FRIDAY} = 5, \text{SATURDAY} = 6.$$

Suppose that today is Thursday. Which day in the week is five days later? Five days later is Tuesday next week. How did we calculate this?

Thursday is day 4 of the week. Five days later is day 9 of the week. This is not possible since a week has only seven days. So day 9 of the week is interpreted as day 2 of the following week, that is, Tuesday next week. When transferring between weeks, we add or subtract seven, since a week has seven days. This is in fact calculating arithmetic modulo 7.

Generally, for every prime number $p$, there exists a unique finite field $\mathbb{F}_p$ of order $p$, in which arithmetic is performed modulo $p$. This is precisely the non-negative integers less than $p$ as described above. There also exists a unique finite field $\mathbb{F}_q$, containing $q$ symbols whenever $q = p^h$ for some prime number $p$ and $h > 1$. However, its structure is more complicated and no longer directly identifiable with the set of non-negative integers less than $q$.

## 1.2 Finite vector spaces

A *vector space* $V$ over a field $\mathbb{F}$ is a mathematical structure consisting of a set of "vectors" which can be added to one another, and multiplied by elements of the field $\mathbb{F}$. A familiar example of a vector space over $\mathbb{R}$ is the *Cartesian plane.* In mathematical notation, this is the vector space

$$V = \mathbb{R}^2 = \{(x_1, x_2) : x_1, x_2 \in \mathbb{R}\},$$

with addition and scalar multiplication given by

- (addition)
$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$
- (scalar multiplication)
$$\alpha \cdot (x_1, x_2) = (\alpha \cdot x_1, \alpha \cdot x_2), \text{ for } \alpha \in \mathbb{R}.$$

In this section, we define a vector space over the finite field $\mathbb{F}_q$ where $q = p^h$, $p$ is a prime number, and $h \geq 1$. That is, we consider vectors whose coordinates are elements of the finite field $\mathbb{F}_q$. In mathematical notation, this is the *finite vector space* $V$ given by

$$V = \mathbb{F}_q^n = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{F}_q\}.$$

In this vector space, addition and scalar multiplication are given coordinate-wise by the corresponding operations in the underlying field $\mathbb{F}_q$:

- (addition)

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

- (scalar multiplication)

$$\alpha \cdot (x_1, \ldots, x_n) = (\alpha \cdot x_1, \ldots, \alpha \cdot x_n), \text{ for } \alpha \in \mathbb{F}_q.$$

The "size" of a vector space can be measured using the concept of *dimension* which represents the number of degrees of freedom in its vectors. For instance, the vector space $V = \mathbb{F}_q^n$ has dimension $n$ since each coordinate represents a degree of freedom. Furthermore, the vector space $V$ contains 1-dimensional vector spaces (called "vector lines"), 2-dimensional vector spaces (called "vector planes"), ..., $i$-dimensional vector spaces, ..., $(n-1)$-dimensional vector spaces. An $i$-dimensional vector space over $\mathbb{F}_q$ contains $q^i$ vectors from $\mathbb{F}_q^n$. This is because its vectors have $i$ degrees of freedom, and each degree of freedom has $q$ possible values.

## 2 A packing problem for a cube

Consider a 3-dimensional cube with sides of length $x$ metres (Figure 1).

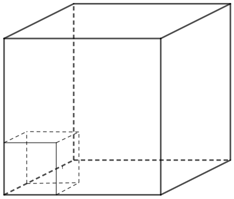

Figure 1: Packing smaller cubes into a larger cube.

Suppose a person is asked to fill the larger cube with smaller cubes having sides of length $y$ metres such that the amount of empty space is minimised.

If the length $y$ of the sides of the smaller cube is a divisor of the length $x$, then $d = {}^x\!/_y$ is a positive integer. In this case, the larger cube can be completely filled by $d^3$ smaller cubes whose sides have length $y$. An example of this is illustrated in Figure 1 which shows a smaller cube whose sides have length $y = 1$ inside a larger cube whose sides have length $x = 3$. The larger cube can be filled completely by cubes whose sides have length 1 metre.

However, if the length $y$ of the sides of the smaller cube is not a divisor of the length $x$ of the sides of the larger cube, then the larger cube cannot be completely filled by these smaller cubes. In this case, the smaller cubes can only fill part of the larger cube. One could instead try to fill the larger cube as much as possible by using smaller cubes whose sides have length $y$. This type of problem is called a *packing problem*, and whether or not the larger cube can be completed filled is determined by whether $y$ divides $x$.

In finite geometry, it is also possible to consider an analogous packing problem in the finite vector space $\mathbb{F}_q^n$. In this context, the goal is to pack as many $t$-dimensional subspaces of $\mathbb{F}_q^n$ which pairwise share only the zero vector into the finite vector space $\mathbb{F}_q^n$. This packing problem is analogous in the sense that the finite vector space $\mathbb{F}_q^n$ plays the same role as the larger cube in Figure 1, and the $t$-dimensional subspaces play the same role as the smaller cubes.

The packing problem in $\mathbb{F}_q^n$ is equivalent to the mathematical problem of constructing "$t$-spreads" and large "partial $t$-spreads" in finite vector spaces. The nice fact about studying (partial) $t$-spreads in finite vector spaces is that the same mathematical object also arises in other seemingly unrelated problems. For instance, we will discuss another application of partial $t$-spreads arising in computer science in Section 4.

We now present important results on $t$-spreads and partial $t$-spreads in finite vector spaces.

## 3 $t$-Spreads and partial $t$-spreads in finite vector spaces

Consider the vector space $V = \mathbb{F}_q^n$ of dimension $n$ over the finite field $\mathbb{F}_q$ where $q = p^h$ for a prime number $p$ and $h \geq 1$.

A geometrical question that can be posed is whether the non-zero vectors of $V$ can be partitioned into $t$-dimensional subspaces. In the field of finite geometry, this question has lead to the study of "$t$-spreads". A *$t$-spread* of $V = \mathbb{F}_q^n$ is a set of $t$-dimensional subspaces of $V$ with the property that each non-zero vector is contained in precisely one subspace.

It turns out that, in some cases, questions about the existence of $t$-spreads of $V$ can be answered by considering the relationships between the values of $n, q$ and $t$. If a $t$-spread exists, then $q^t - 1$ must divide $q^n - 1$ since a $t$-dimensional subspace contains $q^t - 1$ non-zero vectors and $V$ itself contains $q^n - 1$ non-zero vectors. Elementary number theory then leads to the condition that $t$ must divide $n$. Hence, the condition that $t$ divides $n$ is a necessary condition for a $t$-spread to exist in $V = \mathbb{F}_q^n$. Conversely, a very nice geometrical result proves that it is also sufficient. Indeed, when $t$ divides $n$, Hirschfeld showed how to construct a $t$-spread in $V = \mathbb{F}_q^n$ [7].

Now a new research problem arises: for $t$ not a divisor of $n$, what are the largest partial $t$-spreads in $V = \mathbb{F}_q^n$? A *partial $t$-spread* in $V = \mathbb{F}_q^n$ is a set of $t$-dimensional subspaces of $V$ with the property that each non-zero vector is contained in at most one subspace. This has proven to be a very difficult mathematical problem. In the 1970s, Beutelspacher discovered a construction of large partial $t$-spreads of $V = \mathbb{F}_q^n$ [3] which leads to the following theorem.

**Theorem 3.1 (Beutelspacher)** *Let $r = n \pmod{t}$. Then, for all $q$, $\mathbb{F}_q^n$ contains a partial $t$-spread of size $\frac{q^n - q^t(q^r-1)-1}{q^t-1}$.*

The question arose whether this was the largest possible size for a partial $t$-spread in $V = \mathbb{F}_q^n$, when $t$ does not divide $n$. Beutelspacher succeeded in proving this when $n = 1 \pmod{t}$ [1, 2]. It was generally believed that this indeed was the largest possible size for a partial $t$-spread in $V = \mathbb{F}_q^n$ for all $n$. But El-Zanati, Jordon, Seelinger, Sissokho and Spence found a larger example for $q = 2$ and $t = 3$ [5].

**Theorem 3.2 (El-Zanati *et al*)** *Let $r = n \pmod{3}$. Then the largest partial 3-spreads of $\mathbb{F}_2^n$ have size equal to $\frac{2^n-2^r}{7} - r$.*

The most recent breakthrough came when Năstase and Sissokho were able to prove that Beutelspacher's construction has the largest possible size under the following condition [12].

**Theorem 3.3 (Năstase and Sissokho)** *Let $r = n \pmod{t}$. For all $q$, if $t > \frac{q^r-1}{q-1}$, then the largest partial $t$-spreads of $\mathbb{F}_q^n$ have size equal to $\frac{q^n-q^t(q^r-1)-1}{q^t-1}$.*

Similarly, Kurz succeeded in finding the largest size of partial $t$-spreads in the following case [11].

**Theorem 3.4 (Kurz)** *Let $2 = n \pmod{t}$. Then, for $t \geq 4$, $n \geq 2t+2$, the largest partial $t$-spreads of $\mathbb{F}_2^n$ have a size equal to $\frac{2^n-3\cdot 2^t-1}{2^t-1}$.*

## 4 Cooling codes

Inside a computer, information encoded as zeros and ones is transferred along wires. A wire with electrical current passing through it represents a one, and a wire with no electrical current represents a zero. To transfer information between one another, two components inside a computer communicate using a system known as a "bus". A *bus* consists of an "encoder" and a "decoder" connected by multiple wires. The encoder converts a message to a vector of zeros and ones, which is transmitted as electrical current along the wires, before

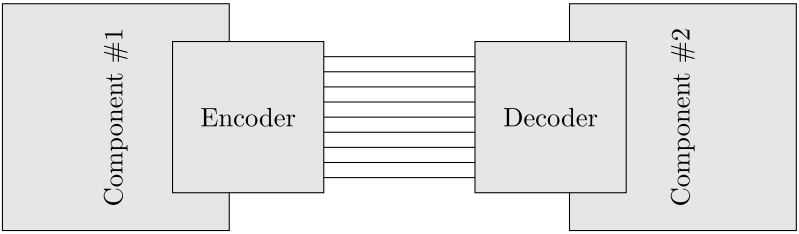

Figure 2: A schematic of a bus for two computer components consisting of an encoder and a decoder connected by wires.

being converted back to the original message by the decoder. Note that vectors with $n$ entries of zeros and ones are precisely the elements of the finite vector space $\mathbb{F}_2^n$. The rules for how the encoder and decoder convert between messages and vectors of zeros and ones are called a *coding scheme*.

When electrical current passes through a wire inside a bus, the temperature of that wire increases. If the temperature of a wire becomes too high, then its ability to transmit current deteriorates leading to communication errors in the bus. One way to overcome this issue is by using a special type of coding scheme known as a “cooling code” [4]. In a basic coding scheme, a given message is always encoded and transmitted along the same wires every time, even if those wires are hot. In a cooling code, there are multiple ways to encode and transmit each given message. When presented with a message to transmit, the bus checks which wires are the hottest and then determines an encoding of the message which avoids using said wires, thus allowing them to cool back to normal operating temperatures.

Consider a bus with $n$ wires which wants to avoid transmitting along its hottest $t$ wires where $t < n$. Mathematically, an $(n, t)$*-cooling code of size* $M$ consists of disjoint subsets $C_1, \ldots, C_M$ of $\mathbb{F}_2^n$, known as “codesets”, with the following property: for any set of wires $S \subset \{1, \ldots, n\}$ of size $|S| = t$ and any $i \in \{1, \ldots, M\}$, there exists $x \in C_i$ which does not use the wires in $S$. Each message that could be sent across the bus corresponds to exactly one codeset and the elements of this codeset represent the different possible encodings of the message.

To transmit a message represented by a binary vector in $\mathbb{F}_2^n$, the bus:

1. Determines the codeset $C_i$, corresponding to the message, and the set $S$, corresponding to the $t$ hottest wires.
2. Encodes the message by selecting a vector $x \in C_i$ which does not use the wires in $S$ (*i.e.*, $x_j = 0$ if $j \in S$).
3. Sends the encoded message $x$ across the wires to the decoder.

4. Since the codesets $C_1, \ldots, C_M$ are disjoint, the decoder determines that the codeset $C_i$ was used based on the property that $x \in C_i$.
5. The decoder recovers the original message from the codeset $C_i$.

With this idea in mind, the question of how to construct cooling codes arises. As the following theorem shows, partial spreads provide a way to do so.

**Theorem 4.1** *Let $V_1, \ldots, V_M$ be a partial $(t+1)$-spread of $\mathbb{F}_2^n$, and denote $V_i^* = V_i \setminus \{0\}$ for all $i$. Then $V_1^*, \ldots, V_M^*$ is an $(n,t)$-cooling code of size $M$.*

The preceding theorem is a very nice example of how a purely mathematical concept that has been studied since the 1970s suddenly becomes relevant for a practical problem. This often happens with substructures in finite geometry. It proves that finite geometry is pure mathematics, close to practical applications.

For readers interested in finite geometry, we refer to the standard volumes of Hirschfeld [6, 7] and to the standard volume of Hirschfeld and Thas [10] for elaborate information on finite geometries. For specific results on the packing problem in finite geometries, coding theory, and statistics, we refer to the two survey articles by Hirschfeld and Storme [8, 9].

# References

[1] A. Beutelspacher, *Partial spreads in finite projective spaces and partial designs*, Mathematische Zeitschrift **145** (1975), no. 3, 211–229.

[2] ———, *Correction to: Partial spreads in finite projective spaces and partial designs*, Mathematische Zeitschrift **147** (1976), no. 3, 303.

[3] ———, *On $t$-covers in finite projective spaces*, Journal of Geometry **12** (1979), no. 1, 10–16.

[4] Y. M. Chee, T. Etzion, H. M. Kiah, and A. Vardy, *Cooling codes: Thermal-management coding for high-performance interconnects*, IEEE Transactions on Information Theory **64** (2018), no. 4, 3062–3085.

[5] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence, *The maximum size of a partial 3-spread in a finite vector space over GF(2)*, Designs, Codes and Cryptography **54** (2010), no. 2, 101–107.

[6] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford Mathematical Monographs, Clarendon Press, 1985.

[7] ———, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, Clarendon Press, 1998.

[8] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces*, vol. 72, 1998, R. C. Bose Memorial Conference (Fort Collins, CO, 1995), pp. 355–380.

[9] ———, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, Finite geometries, vol. 3, Kluwer Academic Publishers, 2001, pp. 201–246.

[10] J. W. P. Hirschfeld and J. A. Thas, *General Galois geometries*, Springer Monographs in Mathematics, Springer, 2016.

[11] S. Kurz, *Improved upper bounds for partial spreads*, Designs, Codes and Cryptography **85** (2017), no. 1, 97–106.

[12] E. L. Năstase and P. A. Sissokho, *The maximum size of a partial spread in a finite projective space*, Journal of Combinatorial Theory, Series A **152** (2017), 353–362.

Leo Storme *is a professor of pure mathematics at Ghent University, Belgium.*

*Mathematical subjects*
Algebra and Number Theory, Discrete Mathematics and Foundations, Geometry and Topology

*Connections to other fields*
Computer Science, Engineering and Technology

*DOI*
10.14760/SNAP-2021-010-EN

*Snapshots of modern mathematics from Oberwolfach* provide exciting insights into current mathematical research. They are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the interested public worldwide. All snapshots are published in cooperation with the IMAGINARY platform and can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

ISSN 2626-1995

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9 –11
77709 Oberwolfach
Germany

*Director*
Gerhard Huisken

Mathematisches
Forschungsinstitut
Oberwolfach

Member of
Leibniz
Leibniz
Association

IMAGINARY
open mathematics