ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Geometric Constructions of Set Systems and Their Hypergraph Representations

Cristina Martínez*, Alberto Besana, and Estela Jimen´Ez

PhD Mathematics University of Castilla-La Mancha, Spain

ABSTRACT

We study t-designs of parameters (n, k, λ) over finite fields as group divisible designs and set systems admitting a transitive action of a linear group represented by an hypergraph G whose vertex set of size n is partitioned into sets of size k in such a way that every tsubset is contained in at least λ subsets of G. We relate the problem to the representation theory of the general linear group $GL(n, \mathbb{F}_q)$ and the constructions of AG codes over finite fields. As a byproduct we construct a RS code based encryption scheme.

***Corresponding author**

Cristina Martinez, PhD Mathematics University of Castilla-La Mancha, Spain.

Received: July 28, 2025; **Accepted:** August 04, 2025, **Published:** August 12, 2025

1. Introduction

Let q be a power of a prime number and $\mathbb{F}_q$ the finite field with q elements. Finite fields have the remarkable property that finite dimensional vector spaces over them are naturally endowed with a canonical and compatible field structure. In particular an element $\alpha \in \mathbb{F}_{q^n}$ is primitive if α generates the cyclic multiplicative group $\mathbb{F}_{q^n}^*$, then α has multiplicative order $q^n - 1$. Primitive elements are frequently used in cryptographic applications such as discrete logarithmic problem and pseudo random number generators. Also $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if the set $\{1, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ forms a basis of $(\mathbb{F}_q)^n$ as a $\mathbb{F}_q$-vector space.

We refer to network coding as the best way to disseminate information over a network. A network is usually represented by a directed multigraph with error free unit capacity edges. There are several source nodes and several destination nodes and data is transferred over a network using packets, where a packet is just an m-length vector over a finite field $\mathbb{F}_q$. The network nodes exchange messages being represented as a matrix. It is convenient to describe a coding process in terms of operations in the extended field $\mathbb{F}_{q^m}$.

Let V be an $n+1$ dimensional vector space over the field $\mathbb{F}_q$, we denote by $\mathbb{P}(V)$ the n-dimensional projective space over it. The set of all subspaces of dimension r is the Grassmannian $\mathcal{G}_{r,n}(\mathbb{F}_q)$ of r-dimensional subspaces in $(\mathbb{F}_q)^n$. A subspace code is a constant dimension code (CDC), that is a subset of the Grassmannian.

In general, for any integers n, r with $n \geq r \geq 0$, we call $\phi(r; n, q) := |\mathrm{PG}^r(n, q)|$, the number of r dimensional subspaces of an n dimensional subspace over $\mathbb{F}_q$. It is the number of ways of choosing $r+1$ linearly independent points in $\mathrm{PG}(n, q)$ divided by the number of ways of choosing such a set of points in a particular r-space. It is given by the q-ary binomial coefficient,

2000 *Mathematics Subject Classification.* 11T71 (primary) ; 05E10 (secondary) .
Key words and phrases. Algebraic code, t-design, bases.

$$\phi(q;n,r) = \begin{bmatrix} n \\ r \end{bmatrix}_q = \frac{(q^{n+1}-1)(q^{n+1}-q)\dots(q^{n+1}-q^r)}{(q^{r+1}-1)(q^{r+1}-q)\dots(q^{r+1}-q^r)}.$$

The general linear group $\mathrm{GL}(n,\mathbb{F}_q)$ acts transitively on $\mathcal{G}_{k,n}(\mathbb{F}_q)$:

$$\begin{aligned} (1) \qquad \mathcal{G}_{k,n}(\mathbb{F}_q) \times \mathrm{GL}(n,\mathbb{F}_q) &\to \mathcal{G}_{k,n}(\mathbb{F}_q) \\ (2) \qquad (\mathcal{U}, A) &\to \mathcal{U}A. \end{aligned}$$

The matrix $\mathcal{U}$ acts on A, by multiplication on the left. Observe that the action is defined independent of the choice of the representation matrix $\mathcal{U} \in \mathbb{F}_q^{k\times n}$.

In order to classify the orbits of $\mathcal{G}_{k,n}(\mathbb{F}_q)$ by the action of the general linear group $\mathrm{GL}(n,\mathbb{F}_q)$ we need to classify all the conjugacy classes of subgroups in $\mathrm{GL}(n,\mathbb{F}_q)$.

A group divisible design (GDD) is an incidence structure $(X,\mathcal{G},\mathcal{B})$ where X is a set of points, $\mathcal{G}$ is a partition of X into groups, and $\mathcal{B}$ is a collection of subsets of X called blocks such that no block intersect any group more than once and any two points from distinct groups appear together in exactly one block. Let n,k,t,λ integers with $n > k > t > 1$, a $t-$design is a pair $(X,\mathcal{B})$, where X is a set of points, $\mathcal{B}$ is a family of $k-$subsets of X called blocks. Any $t-$subset of distinct points are contained in exactly $\lambda-$blocks. When $t = 2$ and $\lambda = 1$ the design is called a Steiner triple system of order n and it is denoted as $STS(n)$.

Recently, q-ary designs (designs over finite fields) gained a lot of attention because of its applications for error-correcting in networks, and secret sharing scheme, a way for sharing a secret data among a group of participants so that only specific subsets (which are called qualified subsets) are able to recover the secret by combining their shares.

In this paper, we give an explicit method to construct large sets of t-designs over finite fields of given parameters n,q,s, by deriving ordered basis of $(\mathbb{F}_q)^n$.

Notation. For d a positive integer, $\alpha = (\alpha_1,\dots,\alpha_m)$ is a partition of d into m parts if the α_i are positive and decreasing. We will denote as $\mathcal{P}(d)$, the set of all partitions of d. We set $l(\alpha) = m$ for the length of α, that is the number of cycles in α, and l_i for the length of α_i. The notation $(a_1,\dots,a_k)$ stands for a permutation in S_d that sends a_i to a_{i+1}. We write $\mathrm{PGL}(2,k) = \mathrm{GL}(2,k)/k^*$, and elements of $\mathrm{PGL}(2,k)$ will be represented by equivalence classes of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with $ad - bc \neq 0$. In the sequel, an $[n,k]_q$-code C is a $k-$dimensional subspace of $(\mathbb{F}_q)^n$.

2. $t-(n,k,\lambda;q)$-DESIGNS

Consider the GDD given by the incidence structure $(\mathcal{P},\mathcal{B},I)$ on a 3-dimensional vector space V over the finite field $\mathbb{F}_p$, where $\mathcal{P}$ is a set of v smooth, reduced points in V, $\mathcal{B}$ is a set whose elements are triples of points $(p,q,r) \in \mathcal{P}\times\mathcal{P}\times\mathcal{P}$ defined by the condition $(p,q,r) \in \mathcal{B}$ if either $p+q+r$ is the full intersection cycle of the projective line with a $\mathbb{F}_p$-line

$l \subset \mathbb{P}(V)(\mathbb{F}_p)$ with the right multiplicities, or else if there exists a $\mathbb{F}_p-$line $l \subset V$, such that $p, q, r \in l$, then the triple is called a plane section. The number of points in the projective plane $PG(2,p)$ is $\frac{p^3-1}{p-1} = p^2+p+1$ and dually there are p^2+p+1 lines in $PG(2,p)$.

There are two types of GD designs on V:

(1) For any $(p,q) \in \mathcal{P}^2(V^*)$, there exists an $r \in \mathcal{P}(S^dV^*)$ such that $(p,q,r) \in l$, where S^dV is the d^{th} symmetric power of the dual of V. The triple (p,q,r) is strictly collinear if r is unique with this property, and p,q,r are pairwise distinct. The subset of strictly collinear triples is a symmetric ternary relation.

(2) Assume that $p \neq q$ and there are two distinct points $r_1, r_2 \in \mathcal{P}$ with $(p,q,r_1) \in \mathcal{B}$ and $(p,q,r_2) \in \mathcal{B}$. Denote by $l = l(p,q)$ the set of all such points, then $l^3 \in \mathcal{B}$, that is, any triple (r_1,r_2,r_3) of points in l is collinear. Such sets are called lines in $\mathcal{B}$.

If X is the finite field $\mathbb{F}_{q^n}$, we consider the GDD where the set points correspond to vectors of $(\mathbb{F}_q)^n$ as n-dimensional vector space over $\mathbb{F}_q$ and the block set $\mathcal{B}$ is a collection of $i-$subspaces $K \subseteq \mathbb{F}_q^n$ which geometrically correspond to points in the Grassmannian $\mathcal{G}_{n,i}(\mathbb{F}_q)$. They live in a natural way as subspaces of the vector space $(\mathbb{F}_q)^n$. More generally, assuming that $\dim K_j = j$ for $j = 1, \ldots, n$, the sequence of nested subspaces

$$\{0\} \subset K_1 \subset K_2 \subset \ldots \subset K_n = \mathbb{F}_q^n,$$

live in the whole lattice of subspaces of the vector space $(\mathbb{F}_q)^n$.

If each t-subspace of X is contained in exactly λ blocks of $\mathcal{B}$ then it is called a t-$(n,k,\lambda;q)$ design. A permutation matrix $\sigma \in \mathrm{GL}(n,q)$ acts on the Grassmannian by multiplication on the right of the corresponding representation matrix. In particular σ is an automorphism of the design $\mathcal{D} = (X,\mathcal{B})$ if and only if σ leaves the Grassmannian invariant, that is $\mathcal{B}^\sigma = \mathcal{B}$. In particular, we are interested in understanding the orbits by the action of any permutation matrix of $\mathrm{GL}(n,q)$ and moreover of any subgroup G contained in $\mathrm{GL}(n,q)$. Further, it is possible to count the orbits of the action in several cases and these correspond to blocks of the design satisfying certain geometrical properties.

Definition 2.1. *Let $\alpha \in \mathbb{F}_{q^n}$ be an element of the extension field of $\mathbb{F}_q$. Then an r-dimensional W subspace of the underlying vector space over $\mathbb{F}_q$ is α-splitting if $\alpha^i W = W$ is invariant under the action of any element α^i in the Galois group of the extension $\mathbb{F}_q \hookrightarrow \mathbb{F}_q(\alpha)$. More precisely, given any $\mathbb{F}_q$-linear endomorphism $T : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, an r-dimensional subspace W is T-splitting if $\mathbb{F}_{q^n} = W \oplus T(W) \oplus \cdots \oplus T^{n-1}(W)$, where T^j denotes the j-fold composite of T with itself.*

Definition 2.2. *Let T be the standard shift operator on $\mathbb{F}_q^n$, a linear code C is said to be quasi-cyclic of index l or $l-$quasi-cyclic if and only if is invariant under T^l. If $l = 1$, it is just a cyclic code. The quantity $m := n/l$ is called the co-index of C. Namely, if we view a codeword $(c_0, c_1, \ldots, c_{n-1})$ of C as a polynomial $c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$, then $T(c(x)) = x \cdot c(x) \bmod (x^n - 1)$. In particular a cyclic code $C \subset (\mathbb{F}_q)^n$ is identified with*

an ideal in the ring $\mathbb{F}_q[x]/(x^n-1)$ *generated by a polynomial* $g(x)$ *which divides* (x^n-1).

Proposition 2.3. *Let* λ *be the number of* α*-splitting subspaces of* $\mathbb{F}_q^n$*, then the design whose blocks are the* α*-splitting subspaces of* $\mathbb{F}_q^n$ *is a* $t-(n,r,\lambda;q)$ *design.*

Proof. Suppose $n = r\cdot s$, where r, s are coprime positive integer numbers, that is $(r,s)=1$. If $r=1$, n is a prime power p^s and there is an element $\alpha \in \mathbb{F}_{q^n}$ of order s, so that $\{1,\alpha,\ldots,\alpha^{s-1}\}$ with $\alpha^s=1$ is a basis of the vector space $\mathbb{F}_q^s$ over $\mathbb{F}_q$. If $r\neq 1$, the set $\{1,\alpha^s,\alpha^{2s}\ldots,\alpha^{(r-1)s}\}$ of $s-$powers of α, spans an r-dimensional α-splitting subspace of $\mathbb{F}_{q^n}$, say W. If we complete α to a basis of $\mathbb{F}_{q^n}$ by adding elements $v_1,\ldots,v_m \in \mathbb{F}_{q^n}$, we get,

$$\mathcal{B}^{\alpha}_{(v_1,\ldots,v_m)} := \{v_1,\ldots,v_m,\alpha v_1,\ldots,\alpha v_m,\ldots,\alpha^{n-1}v_1,\ldots,\alpha^{n-1}v_m\},$$

where $\mathcal{B}^{\alpha}_{(v_1,\ldots,v_m)}$ is regarded as an ordered set with $n = r\cdot m$ elements. Define an isomorphism between $\mathbb{F}_q^{rs}$ and $\mathbb{F}_{q^s}^r$, for $i=0,1,\ldots,,r-1$ associating each s-tuple $(v_{i,0},v_{i,1},\ldots,v_{i,s-1})$, with the element $v_i \in \mathbb{F}_{q^s}$, where $v_i = v_{i,0}+v_{i,1}\alpha+\ldots+v_{i,s-1}\alpha^{s-1}$. Then every element in $\mathbb{F}_q^{rs}$ is in correspondence with an element in $\mathbb{F}_{q^s}^r$. Thus $\mathcal{B}^{\alpha}_{(v_1,\ldots,v_s)}$, is necessarily a $\mathbb{F}_q-$basis of an s-dimensional subspace of $\mathbb{F}_{q^{rs}}$, and we will refer to $\mathcal{B}^{\alpha}_{(v_1,\ldots,v_s)}$ as an α-splitting ordered basis of $\mathbb{F}_q^{rs}$. Call V the vector space generated by $\langle v_1,\ldots,v_s\rangle$, then $(\mathbb{F}_q)^n = V\oplus W$. If W is the whole $(\mathbb{F}_q)^n$, we finish. Otherwise take an element $v_1 \in (\mathbb{F}_q)^n|W$, considered as difference of sets. Now if v_1 generates V, we conclude. Otherwise, we take an element $v_2 \in (\mathbb{F}_q)^n|\langle W,v_1\rangle$. So finally, we get a basis of V. The subspaces generated by the $\alpha-$splitting ordered basis constitute an $r-$design of parameters $(n,s,\lambda;q)$, where λ is the number of α-splitting subspaces of $\mathbb{F}_{q^n}$ of dimension m incident with an r-dimensional subspace, and k is the number of blocks of the design which coincides with the number of different ordered basis of $(\mathbb{F}_q)^m$, which is exactly $|\mathrm{GL}(m,\mathbb{F}_q)| = \prod_{i=0}^{m-1}(q^m-q^i)$. Here m is any divisor of n coprime with r.

The subspaces generated by the $\alpha-$splitting ordered basis constitute an $r-$design of parameters $(n,s,\lambda;q)$, where λ is the number of ordered basis, which is exactly $|\mathrm{GL}(m,\mathbb{F}_q)| = \prod_{i=0}^{m-1}(q^m-q^i)$ and $m=s$.

Let's define $S(\alpha,r,s;q)$ to be the number of α-splitting subspaces of $\mathbb{F}_{q^n}$ of dimension s. Let $N(\alpha,r,s;q)$ be the number of ordered basis of $\mathbb{F}_{q^{rs}}$, then

$$S(\alpha,r,s;q) = \frac{N(\alpha,r,s;q)}{|\mathrm{GL}(s,\mathbb{F}_q)|} = \frac{N(\alpha,r,s;q)}{\prod_{i=0}^{s-1}(q^s-q^i)}.$$

$$\lambda = \frac{S(\alpha,r,s;q)}{order(\alpha)} = \frac{|\mathrm{GL}_n(s,\mathbb{F}_q)|}{order(\alpha)} = \frac{\prod_{i=0}^{s-1}(q^s-q^i)}{s!}.$$

□

Definition 2.4. *Let* $\alpha \in \mathbb{F}_{q^n}$ *and let* $g_\alpha(x) = \sum_{i=0}^{n-1}\alpha^{q^i}x^{n-1-i} \in \mathbb{F}_{q^n}[x]$. *If* $gcd(x^n-1, g_\alpha(x))$ *over* $\mathbb{F}_{q^n}$ *has degree* k *where* $(0\leq k\leq n-1)$*, then* α *is a* $k-$*normal element of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$.

Remark 2.5. *For any divisor* r *of* n*, let* ξ *a non-trivial* $r-$*root of unity,one can consider the symbols* $\xi^{q^r},\ldots,\xi^q,\xi$ *and the polynomial which has them as*

roots, $q(x) = \prod_{i=0}^{i=r}(1 - \xi^{q^i})$ *gives an extension field of* $\mathbb{F}_q$ *of degree* r*. Now let* $s = \frac{n}{r}$*, and we consider* ψ *an* s*-root of unity, for example* $\psi = \exp(\frac{2\pi i}{s})$*, then the multiplication in the extended field is defined as* $\xi\psi = \exp(\frac{2\pi i}{n}) = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$*.*

Remark 2.6. *Each element of* $\mathrm{GL}(n, q)$ *represents a linear map that carries the standard ordered basis to another ordered basis. Moreover there is a bijection between the ordered basis of* $\mathbb{F}_{q^n}$ *and the elements of* $\mathrm{GL}(n, q)$*. For* $n = 6$*, we consider the factorization into prime factors* $r = 2, s = 3$*, and let* α *be a primitive element of* $\mathbb{F}_{q^6}$*, then there are as many 2-subspaces of* $(\mathbb{F}_q)^6$ *as* $|\,\mathrm{GL}(2, \mathbb{F}_q)| = (q^3 - 1)(q^3 - q)(q^3 - q^2)$*. There are as many 3-subspaces of* $(\mathbb{F}_q)^6$ *as* $|\,\mathrm{GL}(2, \mathbb{F}_q)| = (q^2 - 1)(q^2 - q)$*. For* $q = 2$*, we get a 2-(6,3,3) design.*

One can study the orbits of $\mathcal{G}_{k,n}(\mathbb{F}_q)$ by the action of any subgroup in the general linear group $\mathrm{GL}(n, \mathbb{F}_q)$. For example we can study the orbit of any triangle group: the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$, the dihedral group, the alternated groups A_4 and A_5 or the symmetric group S_n. We study the special case of the Grassmannian $\mathcal{G}_{2,4}(\mathbb{F}_q)$ of lines in a 3-dimensional projective space.

Now consider $\mathbb{F}_q$ the field of q elements, where $q = 4$ and K its extension field of degree n with Galois group the dihedral group D_4 which is generated by a reflection σ and a cyclic element τ of order $n = 4$.

Lemma 2.7. *The orbit of* $\mathcal{G}_{2,4}(\mathbb{F}_q)$ *by the action of a reflection* σ *of order 2 is in correspondence with the cyclic codes of order* n*.*

Proof. We study the action of a reflection element σ of order 2 on the Grassmanian $\mathcal{G}_{2,4}(\mathbb{F}_q)$ of lines in a 3-dimensional projective space $PG(3, q) = \mathbb{PF}_q^4$.

Recall that the Grassmannian $\mathcal{G}_{2,4}(\mathbb{F}_q)$ is a four dimensional space generated by the diagonals of the unit cube in $PG(3, q)$:

$$< d_1 = (1, 1, 1), d_2 = (-1, 1, 1), d_3 = (1, -1, 1), d_4 = (1, 1, -1) > .$$

We apply to any line d_i a reflection σ of order 2, represented by the matrix:

$$A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

and a rotation τ of angle $\alpha = \frac{2\pi}{n}$, represented by the matrix:

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\alpha) & -sin(\alpha) \\ 0 & sin(\alpha), & cos(\alpha) \end{pmatrix}.$$

By Proposition 2.3, the projective space $\mathbb{PF}_q^4$ can be decomposed into two splitting subspaces corresponding to the eigenspaces invariant by the reflection element σ and the rotation τ. In particular the orbit code corresponding to the eigenspace invariant by the action of σ is the quotient variety $\mathcal{G}_{2,4}(\mathbb{F}_q)/ < \sigma >$. □

If we denote by $\mathcal{P}(n)$ the set of all linear subspaces inside the vector space $\mathbb{F}_q^n$, there is a natural metric on it defined by the function:

$$d_S(U, W) := \dim(\mathrm{U} + \mathrm{W}) - \dim(\mathrm{U} \cap \mathrm{W}).$$

The metric on $\mathcal{P}(n)$ induces a metric on the Grassmannian $\mathcal{G}_{n,k}(\mathbb{F}_q)$. For any subspace code $\mathcal{C} \subset \mathcal{P}(n)$, we define its distance through:

$$\operatorname{dist}(\mathcal{C}) := \min\{\mathrm{d_S}(\mathrm{U},\mathrm{W}) |\, \mathrm{U},\mathrm{W} \in \mathcal{C},\, \mathrm{U} \neq \mathrm{W}\},$$

and its size as $M := |\mathcal{C}|$. A code is said to have minimum distance d if $d_S(U,W) \geq d$ for all distinct words $U, W \in \mathcal{C}$. If the norm $|U| = w$ for every codeword in $\mathcal{C}$, then $\mathcal{C}$ is said to be of constant weight w. The number of codewords in $\mathcal{C}$ is called the size of the code.

We will say that a code $\mathcal{C}$ is of type $[n,k,d]$ if $\mathcal{C}$ has length n, minimum distance d, and its dimension is k.

Definition 2.8. *Given a linear $[n,k,d]$-code, a parity check matrix for $\mathcal{C}$ is an $(n-k)\times n$ matrix H of rank $n-k$ such that $\mathcal{C} = \{x \in (\mathbb{F}_q)^n : Hc^T = 0\}$. Then the dual code $\mathcal{C}^\perp$ is the linear $[n, n-k, d]$ code generated by the parity check matrix of $\mathcal{C}$.*

Definition 2.9. *Given a linear $[n,k,d]$-code, a parity check matrix for $\mathcal{C}$ is an $(n-k)\times n$ matrix H of rank $n-k$ such that $\mathcal{C} = \{x \in (\mathbb{F}_q)^n : Hc^T = 0\}$. Then the dual code $\mathcal{C}^\perp$ is the linear $[n, n-k, d]$ code generated by the parity check matrix of $\mathcal{C}$.*

Any element σ of the general linear group $\mathrm{GL}(n,\mathbb{F}_q)$ induces another code

$$\mathcal{C}^\sigma = \{\big(f(\sigma(\alpha^i))_{i=0}^n\big) : f \in I\},$$

where $I = \{f \in \mathbb{F}_q[x] : degree(f) \leq k\}$. A Singer cycle of $\mathrm{GL}(n,\mathbb{F}_q)$ is an element of order $q^n - 1$. Singer cycles can be constructed, for example, by identifying vectors in $\mathbb{F}_q^n$ with elements of the finite field $\mathbb{F}_{q^n}$. Since multiplication by a primitive element $\alpha \in \mathbb{F}_{q^n}$ is a linear operation, it corresponds to a singer cycle in $\mathrm{GL}(n,\mathbb{F}_q)$. For example, consider the codeword $a = (a_1,\ldots,a_n) \in \mathcal{C}$ and the permutation $\sigma \in \mathrm{GL}(n,\mathbb{F}_q)$ which reverse the coordinates, so $\sigma(a) = (a_n, a_{n-1}, \ldots, a_2, a_1)$. If $\sigma(a) \in \mathcal{C}$, the code is called reversible.

The intersection code space $\mathcal{C} \bigcap \mathcal{C}^\sigma$ is given by the system of linear Diophantine equations:

$$f(\alpha^i) = g(\sigma(\alpha^i))\, \forall\, i = 0,\ldots,n.$$

In particular if σ is a Singer cycle $\sigma(\alpha^i) = (\sigma\alpha)^i$ permutes the elements (α^i). Moreover if the permutation is in the automorphism group of the code, we get an equivalent code. Given two permutation codes $\mathcal{C}$ and $\mathcal{C}^\sigma$ the distance between them in the subspace metric is given by the formula:

$$d(\mathcal{C},\mathcal{C}^\sigma) := \dim(\mathcal{C} + \mathcal{C}^\sigma) - \dim(\mathcal{C} \cap \mathcal{C}^\sigma).$$

Definition 2.10. *Let a be a word in $\mathcal{C}$, then the coset of a is the set:*

$$\{\pi(u) + a : u \in \mathcal{C}, \pi \in S_n\}.$$

A coset leader is a word of minimum weight of any particular coset.

Given a linear code $\mathcal{C}$, a non-trivial coset is a translation of $\mathcal{C}$ by a vector v not in $\mathcal{C}$. The main idea of coset coding is to map an information message not to a particular codeword but to a coset of this code. We observe that two cosets are either equal or disjoint.

Remark 2.11. *The incidence vectors of the blocks of a* t-$(v, k, \lambda; q)$ *design with maximum block intersection number* s *form a constant weight code of weight* $w = k$*, lenght* $n = v$*, and minimum distance* $d = 2(k - s)$*.*

Remark 2.12. *A partition of the complete set of* $k-$*subspaces of* X *into disjoint* t-$(n, k, \lambda; q)$ *designs is called a large set of* t*-designs over finite fields. Thus a partition of the Grassmannian* $\mathcal{G}_{k,n}(\mathbb{F}_q)$*. Any point* $\mathbb{F}_{q^k,q^n} \subseteq \mathbb{F}_{q^n}$ *in* $\mathcal{G}_{k,n}(\mathbb{F}_q)$ *is a code of parameters* $[n, k, d]$ *where* d *is the minimum distance defined as* $\min\{d(V, W) | V, W \in \mathcal{G}_q(k, n),\ V \neq W\}$*.*

2.1. **Relation of** $t-$**designs with AG codes.** Algebraic geometric codes (AGC), use as an alphabet a set $\mathcal{P} = \{P_1, \ldots, P_N\}$ of N-$\mathbb{F}_q$-rational points lying on a smooth projective curve $\mathcal{C}$ defined over $\mathbb{F}_q$, that is, in projective coordinates $P_i = [a_i : 1]$ with $a_i \in \mathbb{F}_q$. Namely, let $F/\mathbb{F}_q$ be the function field of the curve, D a divisor of $F/\mathbb{F}_q$ supported on the set $\mathcal{P}$, and G another divisor such that $\mathrm{Supp\,G} \cap \mathrm{Supp\,D} = \emptyset$. Then the geometric Goppa code $C(D, G)$ associated with the divisors D and G is defined by evaluation of a rational map $\varphi \in \mathcal{L}(G)$ in the linear series attached to the divisor G:

$$C(D, G) = \{(\varphi(P_1), \ldots, \varphi(P_n)) : \varphi \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

It's an $\mathbb{F}_q-$subspace of $(\mathbb{F}_q)^n$ and its dimension k as an $\mathbb{F}_q-$vector space is the dimension of the associated Grassmannian code $G(n, k)$. Geometrically, it corresponds to a point in the Grassmannian $\mathcal{G}_{n,k}(\mathbb{F}_q)$.

Observe that for the same subset of evaluation points and any $k' \leq k$, we have $G(n, k') \subseteq G(n, k) \subseteq \mathbb{F}_q^n$. In particular any $t-$design constructed from $G(n, k)$ is a $j-$design for $0 \leq j \leq t - 1$. It's well known that if $\deg(G) < n$, then $C(D, G)$ is a linear $[n, k, d]$ code over $\mathbb{F}_q$ with length n, $k = l(G)$ and minimum distance $d \geq n - \deg(G)$. We have $l(G) \geq deg(G) + 1 - g$ by the Riemann-Roch theorem, where g is the genus of F.

More precisely, to each non constant rational function φ over C which is defined as the quotient of two polynomials $f(x), g(x) \in \mathbb{F}_q[x]$, one can associate a matrix A with entries in the ring $\mathbb{F}_q[x]$. Then the generator matrix associated to the Goppa code $C(D, G)$ is defined to be the diagonal matrix with entries $q_1, q_2, \ldots, q_k, k \leq n$, corresponding to the continued fraction expansion of the rational function φ. Namely, let us call $f_0 := f(x)$ and call f_1 the divisor polynomial $g(x)$, and f_2 the remainder polynomial, then by repeated use of the Euclid's algorithm, we construct a sequence of polynomials corresponding to the quotients $q_1, \ldots, q_k$, $k \leq n$ of the continued fraction expansion $\frac{f}{g} = q_1 + 1/(q_2 + 1/q_3 + 1/(q_4 + \ldots)))$. Observe that if $\deg \frac{f(x)}{g(x)} < 1$, then q_1 belongs to the ground field.These matrices are in correspondence with endormorphisms $T : R \to R$, of $\mathbb{F}_q[x]$-modules, where $R = \mathbb{F}_q(\alpha)$, and α is a generator of $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space.

Lemma 2.13. *The set of functions* $\{q_1, \ldots, q_k\}$ *is in bijective correspondence with the set of codeword positions* f_i *coming from the decomposition of the rational function* φ *into partial fractions* $f_i \in \mathbb{F}_q[x]$, $1 \leq i \leq n$*. Moreover, they are linearly equivalently as* $\mathbb{F}_q[x]$*-vector spaces.*

Proof. We write the denominator g of the rational function φ as a product of powers of distinct irreducible polynomials.

$$\frac{f}{g} = \frac{c_1}{x-\alpha_1} + \frac{c_2}{x-\alpha_2} + \ldots + \frac{c_n}{x-\alpha_n},$$

where the linear factors $(x-\alpha_i)$ correspond to the roots of $g(x)$ counted with multiplicity. Since we are working over the finite field $\mathbb{F}_{q^n}$, the number of codeword positions $\{f_i\}_{i=1}^n$ is in correspondence with a base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$, and they have the same cardinality as sets. □

Definition 2.14. *Let C be the AG code associated with a rational function φ defined over a smooth projective curve C. A typical codeword is an element of the form $\sum_{j=1}^k a_{ji} f_i \equiv 0 \mod f$, where f_i are the functions obtained from the decompostion of f into partial simple fractions, and $a_i \in \mathbb{F}_{q^n}$.*

Let $\mathbb{F}_l$ be the finite field of prime-power order l and let F be an algebraic function field with full constant field $\mathbb{F}_l$. Note that F can also be considered as an algebraic function field over any subfield $\mathbb{F}_q$ of $\mathbb{F}_l$. One of the main problems in coding theory concerns the size of the alphabet $\mathcal{P}$, thus one of the aims is to obtain non trivial lower bounds of the number $N(F_i)$ of rational places of towers of function fields $\{F_i/\mathbb{F}_q\}_{i=1}^\infty$ such that $F_i \subset F_{i+1}$.

The first case of study will be when the rational function φ admits a decomposition into linear simple fractions. These rational functions define what are known as Reed-Solomon codes. In the case where α is a generator of $\mathbb{F}_{q^n}$, as an $\mathbb{F}_q$-vector space, the set of codeword positions is identified with the set of linear fractions $\{\frac{1}{x-1}, \frac{1}{x-\alpha}, \frac{1}{x-\alpha^2} \ldots, \frac{1}{x}\}$. Any linear combination of these elements produces a vector $a = (a_1, \ldots, a_n)$ in $(\mathbb{F}_q)^n$ and thus a codeword of our AG code $\mathcal{C}$. Let l be the maximum integer number such that the codeword position $a_l \neq 0$. The set of codewords a satisfies the relation

$$\sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} \cong 0 \bmod f,$$

where $L = \{\alpha_i\}_{i=1}^n$ is a subset of the Galois field $\mathbb{F}_{q^n}$. In several cases, it is possible to count the number of codewords of the AG code, by a simple count of the number of normalised polynomials of degree l irreducible over $\mathbb{F}_{q^n}$. In the case of binary codes, where $q = 2$, S. Bezzateev and N. Shekhunova have obtained several closed formulas[1]. The number of normalised polynomials $I_{2^m}(l)$ of degree l over $\mathbb{F}_{2^m}$ satisfy the following equation:

$$I_{2^m}(l) = \frac{1}{l} \sum_{d/l} \mu(d) 2^{m\frac{l}{d}}, \tag{3}$$

where $\mu(d)$ is the Möebius function. The number of unitary separable polynomials with coefficients from the field $\mathbb{F}_{2^m}$ whose degrees do not exceed $(l > 1)$ is equal to:

$$N_{2^m}^l = \sum_{i=2}^{l} (2^{mi} - 2^{m(i-1)}) + 2^m = 2^{ml}. \tag{4}$$

Definition 2.15. *The length of a codeword* $(a_1, \ldots, a_n)$ *in* $(\mathbb{F}_q)^n$ *is* $n = n_1 + n_2 + \ldots + n_k$*, where* n_i *is the number of positions of the vector* a *with weight* v_i *corresponding to the exponent of the corresponding fraction* $f_i = \frac{1}{x-\alpha^i}$ *in the partial fraction decomposition of the rational function* f *associated to the AG code.*

We observe that in the case of cyclic codes the weight v_i coincides with the exponent of the corresponding function f_i whose denominator is a linear function and thus with the integer n_i.

Lemma 2.16. *The set of AG codes defined over the rational normal curve is in bijective correspondence with the set of generalised Reed-Solomon codes.*

Proof. We observe that the n-Veronese embedding of the n-dimensional projective space $\mathrm{PG}(n, q)$ maps the line spanned by the vector $v \in \mathbb{F}_q^{n+1}$ to the line spanned by $v^n \in \mathbb{P}S^n\mathbb{F}_q^{n+1}$, where $\mathbb{P}S^n\mathbb{F}_q^{n+1}$ is the projectivization of the $n-$tensor power of the vector space $\mathbb{F}_q^{n+1}$, which is a projective space of dimension n. In particular, if the finite field $\mathbb{F}_q^{n+1}$ is generated as a vector space over $\mathbb{F}_q$ by a unique element $\alpha \in \mathbb{F}_q$, then the set $\{1, \alpha, \ldots, \alpha^n\}$ forms a basis of $\mathbb{F}_q^n$. Thus the rational normal curve is defined as:

$$\mathcal{C}^n := \{\mathbb{F}_q(1, \alpha, \ldots, \alpha^n) : \alpha \in \mathbb{F}_q \cup \{\infty\}\}.$$

In other words, its underlying vector space is the $\mathbb{F}_q$-vector space whose elements are the polynomials of degree less than n with coefficients in $\mathbb{F}_q$ that we will denote as $\mathbb{F}_q[x]_n$. Let $\alpha_1, \ldots, \alpha_n$ be a sequence of n distinct elements in $\mathbb{F}_q$, if $k \leq n$, then the map

$$\epsilon : \mathbb{F}_q[x] \to \mathbb{F}_q^n, \quad f \mapsto (f(\alpha_1, \ldots, \alpha_n)) \tag{5}$$

is injective, since the existence of a non-zero polynomial of degree less than k vanishing on all α_i implies $n < k$ by the fundamental theorem of algebra (a non-zero polynomial of degree r with coefficients in a field can have at most r roots). The image of ϵ is therefore an AG code of type $[n, k, d]$, where the minimum distance d is always at least $n + 2$. Just observe that since $\mathcal{C}^n$ is a rational normal curve in $\mathbb{P}(\mathbb{F}_q^n)$, any $n + 1$ of its points happen to be in general position.

Reciprocally, the AG codes of dimension n defined over $\mathcal{C}^n$ are constructed by evaluating non-zero polynomials of degree less than n over a location set $\{1, \alpha_1, \ldots, \alpha_n\}$ which coincide with the set of Reed-Solomon codes. Namely, consider a Reed-Solomon code of parameters $[n, k, d]$ over a finite field $\mathbb{F}_q$, with parity check polynomial $h(x) = \prod_{i=1}^{q}(x - \alpha^i)$, where α is a primitive root of $\mathbb{F}_q$ such that $\alpha^{k+1} = \alpha + 1$. Any codeword $(c_0, c_1, \ldots, c_{n-1})$ can be expanded into a q-ary k vector with respect to the basis $\{1, \alpha, \ldots, \alpha^{k-1}\}$, that is, codewords from an $[n, k, d]$ code over a finite field are identified with the coefficients of a degree $k - 1$ polynomial $f(x) \in \mathbb{F}_q[x]$. □

Example 1. *Consider the AG code defined by the rational function* $G(x) = \frac{5x^2+20x+6}{x^3+2x^2+x}$ *which admits the decomposition* $G(x) := \frac{6}{x} - \frac{1}{x+1} + \frac{9}{(x+1)^2}$ *into partial fractions . The presence of a double factor* $(x+1)^2$ *corresponds to the existence of an eigenspace* E *in the vector space* $\mathbb{F}_q^n$ *and thus an* $\alpha-$*splitting subspace where the operator* α *is just the linear operator* $A - \lambda I$*, with* λ *the*

eigenvalue of multiplicity 2 associated to E and A is the generator matrix of the code.

Proposition 2.17. *The variety of $[n,k,d]_q$-codes over $\mathbb{F}_q$ is parametrized by a Grassmannian $\mathcal{G}_{n,k}(\mathbb{F}_q)$ of k-dimensional subspaces in the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$, and the set of Reed-Solomon (RS) codes arises as the set of S_n-invariants.*

Proof. Let $n = r\,s$ be a factorisation of an integer positive number n into irreducible coprime factors and assume $s < r$, then there is a sequence of field extensions $\mathbb{F}_{q^r} \subset \mathbb{F}_{q^s} \subset \mathbb{F}_{q^n}$. Namely, consider the map $T_n : F^n \mapsto F^n$

$$t_j = (-1)^j \sigma_j(x_1, \ldots, x_n),$$

where σ_j is the j^{th} elementary symmetric function in the variables x_i. Thus $\{t_j, j = 1, \cdots n\}$, are the coefficients of the equation:

$$f(z, t_1, \ldots, t_n) = z^n + (-1)\, t_1 z^{n-1} + \cdots + (-1)^n\, t_n = (z - x_1)\,(z - x_2) \cdots (z - x_n).$$

Then by Hilbert's irreducibility theorem (see Theorem 1 of [Se]), it is well known that the splitting field of the polynomial $f(x) = x^n - t_1 x^{n-1} + \ldots + (-1)^n t_n$, is the field of S_n invariants of the polynomial $f(z, t_1, \ldots, t_n)$, where S_n is the symmetric group in n variables and it contains an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. Moreover, for any divisor r of n, one can consider the field of S_r invariants, and apply Hilbert theorem to the symbols $\alpha, \alpha^{q^{2s}}, \ldots, \alpha^{q^{rs}}$, where $n = rs$. Then we get an extension $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^r}$ and all its $\mathbb{F}_q$-subspaces are stable under $Gal(\mathbb{F}_{q^s}/\mathbb{F}_{q^r})$. These are just the RS codes.

□

Corollary 2.18. *The set of RS codes is a closed set in the Zariski topology.*

*Proof.*This follows easily as a consequence of Proposition 2.17, since the Grassmannian is a compact variety. It is well known that the corresponding points $\mathbb{F}_{q^k,q^n} \subset \mathbb{F}_{q^n}$ and $\mathbb{F}_{q^{n-k},q^n} \subset \mathbb{F}_{q^n}$ in the Grassmannians $\mathcal{G}_{k,n}(\mathbb{F}_q)$ of $k-$dimensional subspaces and the Grassmannian $\mathcal{G}_{n-k}(\mathbb{F}_q)$ of $n-k$ dimensional subspaces are respectively dual subspaces in the underlying vector space $(\mathbb{F}_q)^n$ for the Euclidean inner product. Note that the Hamming weight is preserved under invertible linear transformation □

Theorem 2.19. *Let $S \leqslant \mathrm{GL}(n, \mathbb{F}_q)$ be a subgroup containing a primitive element α in $\mathbb{F}_q$, where $q \geq 2$. Then the family of AG codes $\{C^\sigma\}_{\sigma \in S}$ constitute a j-(v, r, λ) design where j is the number of generators of the subgroup S, r is the number of orbits in the Grassmannian $\mathcal{G}_{k,n}(\mathbb{F}_q)$ by the action of the subgroup S, v is the size of the code and λ is the number of $\alpha-$splitting subspaces of $\mathbb{F}_{q^n}$.*

Proof. Consider the family of AG codes constructed out of the vector space of polynomials $I = \{f \in \mathbb{F}_q[x] : \partial f \leq k\}$, where ∂f is the degree of the polynomial and fix a basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. To each polynomial f we associate the AG code $C = \{\big(f(\alpha^i)_{i=0}^n\big) : f \in I\}$.

We construct a j-design where the point set are the codewords of the AG codes and each AG code of constant dimension r is a block, where r is the number of orbits in the Grassmanian $\mathcal{G}_{k,n}(\mathbb{F}_q)$ by the action of any

representative of a conjugacy class in S. Each polynomial $f(x) = a_0 + a_1x + \ldots + a_jx^j$ defines a codeword $(a_0, \ldots, a_j) \in \mathbb{F}_q^j$ of the code. Since the number of invariant polynomials in I by conjugated elements A and B in $\mathrm{GL}(n, \mathbb{F}_q)$ is the same, r is the number of conjugacy classes in S. The intersection vector space is given by the evaluation set

$$\{\big(f(\alpha^i)\big)_{i=0}^n : f \in \mathbb{F}_q[x]_j,\ 1 \leq j \leq r\},$$

of the polynomials of degree j with coefficients in $\mathbb{F}_q$, v is the size of the block codes which is constant and λ is the number of α-splitting subspaces of $\mathbb{F}_{q^n}$ as computed in [2]. □

Example 2. *An application to construct a design. One can consider more generally as an alphabet the set $\mathcal{P} = \{p_1, \ldots, p_n\}$ of $\mathbb{F}_q$-rational points lying on a smooth projective curve defined over a finite field in $\mathbb{P}^d$, and algebraic codes are constructed by evaluation of the global sections of a line bundle or a vector bundle on the curve. The configuration space of n ordered points in $\mathbb{P}^d$ that lie on a rational normal curve is naturally a subvariety of $(\mathbb{P}^d)^n$, and by taking the Zariski closure we obtain a compactification of this configuration space which we call the Veronese compactification. The Veronese compactification $V_{d,n} \subset (\mathbb{P}^d)^n$ parameterizes configurations of (possibly coincident) points supported on a flat limit of a rational normal curve. When the curve is plane, then $V_{2,n}$ is defined scheme theoretically by $\binom{n}{6}$ determinants of 6×6 matrices whose entries are quadratic monomials (see Theorem 1.1 of* [CGMS]*). A subset $\mathcal{T} \subseteq \binom{[n]}{6}$ of these determinants defines $V_{2,n}$ set-theoretically if and only if for any partition $\mathcal{P} = I_1 \cup \ldots \cup I_6$, there exists $J \in \mathcal{T}$ such that $|J \cap I_j| = 1$ for all $1 \leq j \leq 6$, that is $([n], \mathcal{P}, \mathcal{T})$ is part of a GDD, where $\mathcal{T}$ is a block and consequently, the number of these determinants that suffice set-theoretically is at least $\frac{2}{n-4}\binom{n}{6}$.*

Let F be a field of characteristic p and $\alpha \in \overline{F}$ be an n^{th} primitive root of unity, where $\overline{F}$ denotes the algebraic closure of F. The n^{th} cyclotomic polynomial $\Phi_n(x) = \prod_{1<j<n,(j,n)=1} (x - \alpha^j) \in \overline{F}[x]$ is the minimal polynomial of α over F. It is monic of degree the Euler's totient function $\varphi(n)$. It has integer coefficients and it is irreducible over $\mathbb{Q}$. In $\mathbb{Q}[x]$, we have the factorization into irreducible polynomials:

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

By Möebius inversion:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

Example 3. *Consider the action of a permutation matrix β in $\mathrm{GL}(n, q)$ given by the element $\beta \in \mathbb{F}_q^n : x \to a\,x$, which is given by multiplication by an element $a \in \mathbb{F}_q^*$ of multiplicative order $k > 1$ with $n = km$. Then by Lemma 2.16, counting the codewords of the constant dimension code defined by the action of β in the Grassmannian $\mathcal{G}_{k,n}(\mathbb{F}_q)$, is equivalent to count the number $\mathcal{N}_{a,m}$ of irreducible monic polynomials of degree n such that $f(x) = f(ax)$.*

This number is expressed in terms of the Möebius function:

$$\mathcal{N}_{a,m} = \frac{\Phi(k)}{km} \sum_{d|m, gcd(d,k)=1} = \mu(d)(q^{\frac{m}{d}} - 1).$$

Example 4. *We consider the roots of the polynomial $x^8 - 1 \in \mathbb{F}_5[x]$ in the splitting field $\mathbb{F}_{5^2}$. The decomposition into irreducible polynomials over $\mathbb{F}_5[x]$ is $(x-1)(x+1)(x-2)(x+2)(x^2+1)(x^2-2)(x^2+2)$. Now, we consider the field extensions $F_1 \coloneqq \mathbb{F}_5[x]/(x^2-2)$ and $F_2 \coloneqq \mathbb{F}_5[x]/(x^2+2)$ of $\mathbb{F}_5$ that are isomorphic to the field extension $\mathbb{F}_{25}$ of $\mathbb{F}_5$. Call α the root of x^2-2 in the field extension F_1, then $4 \cdot \alpha$ is the other root of x^2-2, and $2 \cdot \alpha$, $3 \cdot \alpha$ the roots of x^2+2 in F_1. So $g(x) = (x-\alpha)(x-2\alpha)(x-3\alpha)(x-4\alpha)$ generates a Reed-Solomon code over $\mathbb{F}_5[x]/(x^8-1)$. We say that two roots are conjugated if they are roots of the same polynomial in the decomposition of x^8-1 in $\mathbb{F}_5[x]$, in particular this defines a non-crossing partition of the total set of roots and it is a 2-design of the splitting field $\mathbb{F}_{25}$ with parameters $n=2$, $k=4$ and $\lambda = 2$.*

From a geometric point of view, the point $(\alpha, 0) \in \mathbb{P}(\mathbb{F}_q^2)$ with $\alpha^4 = 4$ is an $\mathbb{F}_{25}-$rational point of the affine curve $y^2 = (x^4+1)$. The other rational places are $(2,0), (-2,0)$ and the place $(0,\alpha)$ at ∞.

It is well known how to factorize a polynomial over finite fields (see for example [PFG]). In we give an updated proof expressing the number of polynomials decomposable into distinct linear factors in terms of Stirling numbers[2].

Given an integer n, it is possible to count the number of cyclic codes of parameters $[n,k]$ for each $0 \leq k \leq n$ and set of roots $\alpha_1, \ldots, \alpha_k$ in the splitting field of $x^n - 1$, the corresponding polynomial $g(x) = \prod_{i=1}^{k}(x-\alpha_i)$ generates a linear cyclic code in the ring $\mathbb{F}_q[x]/(x^n-1)$. Thus for each $0 \leq k \leq n$ there are exactly $(q)_k/(q^2-q)$ cyclic codes. These codes are of great importance in ADN-computing and as they are linear codes, they can be described as function fields.

Remark 2.20. *A much greater variety of linear codes is obtained if one uses places of arbitrary degree rather than just places of degree 1 as in Goppa's construction. For example, the polynomial x^3+4 factorises as $(x-1)(x^2+x+1)$ over $\mathbb{F}_5[x]$, then the roots of the polynomial in the splitting field $\mathbb{F}_5[x]/x^2+x+1 \cong \mathbb{F}_{25}$ correspond to one place of degree 2 over the function field $\mathbb{F}_5(x)$ but of degree 1 over $\mathbb{F}_{25}$.*

2.2. **$t-$designs with an action of a $p-$group.** During the last years, there has been an increasing interest in studying finite abelian groups due to its relationship with public key cryptography, quantum computing and error-correcting codes. Abelian groups as the groups $\mathbb{Z}_n^*$ of invertible elements of $\mathbb{Z}_n$, multiplicative groups of finite fields, the groups of elements of elliptic curves over finite fields, finite $p-$groups with unique cyclic subgroups of given order have been used for the designation of public key cryptosystems. In order to use cryptography to insure privacy, it is currently necessary for the communicating parties to share a key which is known to no one else. As we showed in Theorem 2.19, we can construct t-designs from any $p-$group containing a cyclic subgroup.

Proposition 2.21. *For $q \geq 2$, the group $\mathrm{GL}(n,q)$ contains a least two different cyclic subgroups of orders $q-1$ and $q+1$ respectively. Each one corresponding to elements α, γ in $\mathrm{GL}(n,q)$ fixing an $\alpha-$splitting and $\gamma-$splitting subspaces respectively and the $t-$designs whose incidence vectors are the $\alpha-$splitting subspaces and $\gamma-$splitting subspaces respectively correspond to RS codes of length $n = q-1$ (respectively $n = q+1$) and dimension r the maximum divisor of n.*

Proof. For any divisor d of $q-1$ (respectively of $q+1$), the d-$(q-1, \frac{q-1}{d}, \lambda)$ design (respectively d-$(q+1, \frac{q+1}{d}), \lambda)$) corresponds to RS codes of length $n = q-1$ (respectively $n = q+1$) and dimension d. Moreover the matrix A of row vectors the incidence vectors of the design, satisfies $\frac{q+1}{r} \leq rank(A) \leq \frac{q-1}{2}$, where r is the maximum divisor of $q-1$ (respectively $q+1$). □

Remark 2.22. *The generators of the cyclic groups of order $q-1$ ($q+1$, respectively) are the relative integers coprime with $(q-1)$ (respectively with $q+1$), that is $\varphi(q-1)$ (respectively $\varphi(q+1)$). Let $m = \varphi(q-1)$ (respectively $m = \varphi(q+1)$), by Theorem 2.19, the family of RS codes of length $q-1$ (respectively $q+1$) constitute a m-$(q-1, r, \lambda)$ design (respectively a m-$(q+1, r, \lambda)$ design). These codes are indeed AG codes arising from genus 0 curves, and by Riemann-Roch theorem, their parameters satisfy the bound $d \geq n+1-k$, where d is the minimum distance.*

The normalizer groups of the cyclic groups generated by α and γ are dihedral groups, and it is possible to construct t-designs from them as we showed in Proposition 3.5 of[2]. Next tables show t-designs constructed from abelian p-groups and their normalizers. We assume that $q \leq 31$.

Table 1. $t-$designs constructed from a p-group.

q	group type	$t-(n,k,\lambda)$
q odd prime $q+1 \equiv 0(3)$	cyclic of order $q+1$	3-$(q+1, \frac{q+1}{3}, \lambda)$
q odd prime $q-1 \equiv 0(3)$	cyclic of order $q-1$	3-$(q-1, \frac{q-1}{3}, \lambda)$
q odd	cyclic of order q	3-$(q, \frac{q}{3}, \lambda)$
$q = p^e$	abelian p group	p-(q, p^l, λ), $l < e$

Table 2. $t-$designs constructed from their corresponding normalizers.

q	group type	$t-(n,k,\lambda)$
q odd	dihedral of order $2(q-1)$	3-$(2(q-1), q-1, \lambda)$
q even	dihedral of order $2(q+1)$	2-$(2(q+1), q+1, \lambda)$
$q = p^e$	Borel	p-$(q(q-1), (q-1), \lambda)$

Recall that the dihedral group of order $2\,(q-1)$ (respectively of order $2\,(q+1)$) is generated by a rotation τ_{q-1} of order $(q-1)$, (respectively of order $2frm{-}e, (q+1)$ and a reflection. In particular the discrete logarithm problem (DLP) applied to this group reads: Given an element $h \in D_{2\,(q-1)}$ find an integer m satisfying $\tau^{\,m} = h$. The smallest integer m satisfying the identity is called the index of h with respect to τ, and is denoted as $m = log_\tau(h)$ or $m = ind_\tau(h)$. The DLP is used as underlying hard problem in many cryptographic constructions, including for example Diffie-Hellman key exchange, [3]. Solving DLP takes time that is exponential in the order of the group G. For example, the group defined by the elliptic curve over a finite field $\mathbb{F}_p$ takes time $O(\sqrt(p)$. For this reason, it is used for cryptographic purposes.

2.3. **Diffie-Hellman key exchange for dihedral groups.** In Diffie-Hellman key exchange cryptosystem, the public key is an element of a group G of public knowledge, in the case of study as in [4] is a dihedral group of order $2\,(q-1)$ generated by a reflection σ of order 2, and a rotation τ of order $(q-1)$. There are two participants involved in the encryption process, participant P_1 and participant P_2 who want to communicate with each other over a public channel.

The generating algorithm produces an element τ which is the public key. Observe that since the group generated by τ is cyclic of order $q-1$, its elements $1, \tau, \tau^2, \ldots, \tau^{q-2}$ are roots of unity, that is, $x - \tau^i$ divides the polynomial $x^n - 1$, and the code is cyclic. Moreover it is the RS code of length $n = q-1$ and dimension k. First participant P_1 randomly choose a secret $0 < d < (q-1)$ and computes $D = \tau^d$. Second participant P_2 randomly choose a secret $0 < e < (q-1)$ and computes $E = \tau^e$. Participant P_1 sends D to participant P_2, and P_2 sends E to P_1. Then P_1 computes $E^d = \tau^{e\,d}$ and P_2 computes $D^e = \tau^{d\,e}$ so that both participants P_1 and P_2 have the shared value $\tau^{d\,e}$ up to reflection $\sigma \in D_{q-1}$. Thus computing $\tau^{e\,d}$ from τ^e requires solving the discrete logarithm problem (DLP) $log_{\tau^e}(\tau^{e\,d}) = d$. At each time t, the probability of selecting the element τ^j is distributed as a Bernoulli distribution with $Pr(x = \tau^j) = \left(\frac{1}{q}\right)^j (1 - \frac{1}{q})^j$, $j \in \{0, 1, \ldots q-1\}$.

There are two people involved in the encryption process, Bob and Alice and the trapdoor function is the discrete logarithm. The cryptographic protocol consist in repeating k times the following 3 exchanges:

Key selection: Bob selects a random integer $0 < d < (q-1)$ and computes $D = \tau^d$.
Alice selects a random integer $0 < a < (q-1)$ and computes $A = \tau^a$.
Encryption: Bob sends D to Alice, and Alice sends A to Bob.
Decryption: Then Bob computes $A^d = \tau^{a\,d}$ and Alice computes $D^a = \tau^{d\,a}$ so that Bob and Alice have the shared value $\tau^{d\,a}$ up to reflection $\sigma \in D_{q-1}$.

3. Relation of t-designs with graph networks

Consider a network represented by a simple graph $G = (V(G), E(G))$, with vertex set $V(G)$ or set of nodes and edge set $E(G)$, or pairs of nodes, that is, a graph with no loops (edges whose endpoints are equal) nor multiple edges. A subset of the vertex set is called independent set, if there is no edge between vertices in X. A matching is a set of disjoint edges of a graph. A clique in an undirected graph is a subset of its vertices such that every two vertices in the subset are connected by an edge. A hypergraph is a generalization of a graph in which an edge can join any number of vertices. A $k-$hypergraph has all such hyperedges connecting exactly $k-$vertices, a normal graph is thus a 2-hypergraph. A matching is a set of disjoint edges of a graph.

Let G be a graph, for a subset $S \subset V(G)$ let us consider the induced subgraph H of G. A G-design of H is a pair where S is the vertex set of H and $\mathcal{B}$ is an edge-disjoint decomposition of H also known as block decomposition of the vertex set and $\mathcal{G}$ is a partition of the vertex set into groups, such that any two nodes from distinct groups appear together in exactly one block. We will represent the relationship that exists between two sets by zero-one. If an element is present then it is represented by 1 else it is represented by 0. Each block of a given partition identifies the positions where the matchings interconnecting edges take place. In particular if $q = 2$, we have the binary finite field $\mathbb{F}_{2^n}$ that it is known in the literature as n-cube as the GDD of parameters k and n whose points are vectors in $(\mathbb{F}_2)^n$, and the $k-$blocks are the collection of $t-$subspaces or induced subcubes for $t \leq n-1$.

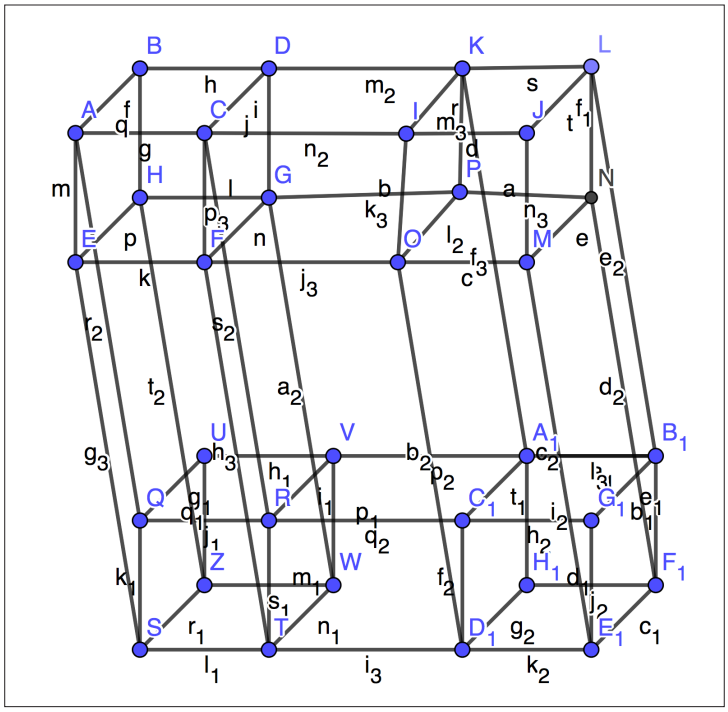

Figure 1

We say G is a split graph if the vertex set $V(G)$ can be partitioned into a clique C and an independent set I, where (C, I) is called a plot partition of G. The best known cryptographic problem is that of privacy: preventing an authorised extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else.

An automorphism is a permutation of the vertices of the network which preserves adjacency. The set of automorphisms under composition forms a group Aut(G) of size a_G which compactly describes network symmetry. The orbit of a vertex $v \in V(G)$ is the set:

$$\triangle(v) = \{\pi v \in V(G) : \pi \in \mathrm{Aut(G)}\}.$$

Automorphism group orbits naturally partition network vertices into disjoint structural equivalence classes. Since two vertices in the same orbit may be permuted without altering network adjacency, they are structurally equivalent in the strongest possible way: they play exactly the same structural role in the network.

Let G be a network with automorphism group Aut(G). Let $1 \neq S$ be a set of generators of Aut(G). Suppose that we partition S into n support-disjoint subsets $S = S_1 \cup \ldots \cup S_n$ such that each S_i cannot itself be decomposed into smaller support-disjoint subsets. Call H_i the subgroup generated by S_i. Since S is a generating set and elements from different factors H_i, H_j commute, this procedure gives a direct product decomposition:

$$\mathrm{Aut(G)} = \mathrm{H_1} \times \mathrm{H_2} \times \ldots \times \mathrm{H_n}.$$

The network automorphism group decomposition relates automorphism group structure to network topology. Moreover, automorphism groups of real-world networks such as scientific collaboration networks or technological networks such as the internet can typically be decomposed into direct and wreath products of symmetric groups, [5]. Reciprocally, given a group presentation S of $\mathrm{GL}(n, \mathbb{F}_q)$, we can attach to it a Cayley graph which is defined as the directed graph having one vertex associated with each group element and directed edges (e_1, e_2) whenever $e_1^2 e^{-1} \in S$. The Cayley graph may depend on the choice of a generating set, and it is connected if and only if S generates $\mathrm{GL}(n, \mathbb{F}_q)$.

A subset S of an additive group is called sum-free if it contains no elements x, y, z such that $x + y = z$. In particular, this means the corresponding vertices constitute an independent set in the Cayley graph, (see [KTSZ]). Moreover, there are two distinguished sets of vertices, the set of independent vertices L which satisfy the property that there is no edge between two vertices and the complement graph.

We pass from network topology to vector network coding by thinking of the vertex set $V(G) = \{a_1, \ldots, a_n\}$ as an alphabet of n letters and defining a vector space V on these n-generators over a ground field k. There is a natural representation $\rho : S_n \to \mathrm{GL}(V)$, where S_n is the group of permutations of n elements. As we showed in vector network coding and moreover codes over a finite field $\mathbb{F}_q$ are very much related with the study of the representation theory of the symmetric group over finite fields and

further with the representation theory of $\mathrm{GL}(n, \mathbb{F}_q)$ over finite fields. From this representation, one can recognise more easily patterns and extract information from them. In terms of designs over $\mathbb{F}_q$, we want to understand which subspaces are invariant by the action of elements of the general linear group $\mathrm{GL}(n, \mathbb{F}_q)$ or finite subgroups of $\mathrm{GL}(n, \mathbb{F}_q)$. In this way, one can construct designs with prescribed groups where the blocks are the orbits by the action, and thus to generalise to other Galois extensions not necessarily cyclic[6].

Recall that the adjacency matrix A of a multigraph is a $n \times n$ matrix (where $n = |V|$) with rows and columns indexed by the elements of the vertex set and the (x, y)-entry is the number of edges connecting x and y. If the graph is directed, the matrix A is symmetric and therefore all its eigenvalues are real. The degree of a vertex $deg(v)$ is the number of edges incident with v, where we count a loop with multiplicity 2. The largest eigenvalue λ of the adjacency matrix describes the spectrum character of the graph topology. A graph is regular if all the vertices have the same degree. The neighborhood design of a regular graph on v vertices, is the 1-design formed by taking the points to be the vertices of the graph and the blocks to be the sets of neighbours of a vertex for each vertex, if any two distinct vertices have exactly λ common neighbours it is a 1-(v, k, λ) design.

Given a t-design you can associate to it a regular graph, where the points are the nodes of the graph, all the nodes have the same degree and two different nodes are connected if and only if they are in the same block of the design, that is, the neighbours of the vertices are the blocks. It is also possible to design a code which matches the network graph. Specifically, the code of a graph over a finite field F is the row span of an adjacency matrix A over the field F, denoted by $C_F(G)$ or $C_F(A)$.

Example 5. *The $n-$cubes belong to the class of graphs Γ_n^k, for $n \geq 1$, $k \geq 0$ integers and $k \geq 0$, $k \leq n$, with vertices the 2^n vectors of $\mathbb{F}_2^n$ and adjacency defined by two vectors being adjacent if they intersect in an $(n-k)$-dimensional subspace.*

3.1. **Set systems.** A set system is a pair $(X, \mathcal{A})$ such that X is a finite set of points and $\mathcal{A}$ is a set of subsets of X, called blocks. The number of points, $|X|$, is the order of the set system. Let K be a set of positive integers. A set system $(X, \mathcal{A})$ is said to be K-uniform if $|A| \in K$ for all $A \in \mathcal{A}$. Let $\mathcal{G} = \{G_1, \ldots, G_s\}$ be a partition of X into subsets called groups. The triple $(X, \mathcal{G}, \mathcal{A})$ is a group divisible design (GDD) when every 2-subset of X not contained in a group appear in exactly one block and $|A \bigcup G| \leq 1$ for all $A \in \mathcal{A}$ and $G \in \mathcal{G}$. A 3-GDD in which all the groups are of size 1 is known as a Steiner triple system.

Proposition 3.1. *There is a bijective correspondence between ordered basis sets of $(\mathbb{F}_q)^n$ and set systems of order n.*

Proof. This correspondence can be established by associating to any list of t elements contained in $\mathrm{GL}(n, q)$ a partition of t groups of size the order of the corresponding element in $\mathrm{GL}(n, q)$. Namely, to any list $\{\gamma_1, \ldots, \gamma t\}$ of t elements we associate the subgroup G_λ generated by these t elements. This is a group of type λ the partition of orders $\lambda_i = ord(\gamma_i)$ ordered in

increasing order $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_t > 0$.We assume that $n \geq q-1$ and G is a group containing a Singer cycle $\alpha \in \mathrm{GL}(n,q)$. Let $\Gamma(G_\lambda)$ be the Cayley graph attached to the subgroup G_λ, that is, the graph in which vertices 1 through t corresponding to each generator are placed in a row with each vertex connected by an unlabelled edge of its immediate neighbors . There is an action of the symmetric group S_n on the combinatorial class $\mathcal{G}_n$ of regular graphs with n vertices. For any $\sigma \in S_n$ and $g \in \mathcal{G}_n$, the graph $\sigma \cdot g$ has the same vertex set and edge set as g, but each label i in g is replaced by $\sigma^{-1}(i)$ in $\sigma \cdot g$, they are isomorphic graphs. We define the following linear map over $(\mathbb{F}_q)^n$:

$$\Phi(\Gamma(G_\lambda))(x) = A_{t,k}^{G_\lambda}\, x. \tag{6}$$

Here $A_{t,k}^{G}$ is the adjacency matrix of graph $\Gamma(G)$, thus it is a $\{0,1\}$ matrix with rows and columns indexed by the t-subspaces and the k-subspaces of $\mathbb{F}_q^n$. In particular, constructing $t-$designs over $\mathbb{F}_q$ is equivalent to solving the systems of linear Diophantine equations 6. There is a 1 in row X and column Y of M iff $t-$subspaces X is contained in $k-$subspaces Y. With this definition, a $t-(n,k,\lambda)$ design over $\mathbb{F}_q$ is precisely a $\{0,1\}$ solution to $A_{t,k}^{G}x = (\lambda,\lambda,\ldots,\lambda)^T$, where λ is the number of $k-$subspaces containing at least a t-subspace, in particular $rank\,(A_{t,k}^{G}) \geq t$. □

3.2. **r-designs constructed from the projective line.** Let X be a v-set and $\mathcal{P}_k(X)$ denote the set of all k-subsets of X. A $t-(v,k,\lambda)$-design is a set system $\mathcal{D} = (X, D)$ in which D is a collection of $\mathcal{P}_k(X)$ (called blocks) such that every t-subset of X appears in exactly λ-blocks A 2-(v,k,λ) design is a collection $\mathcal{B}$ of elements of $\mathcal{P}_k(X)$ (called blocks) such that every line of the incidence structure $(\mathcal{P}(X), \mathcal{B}(X), I)$ intersect $\mathcal{B}$ in exactly λ points. A 3-(v,k,λ) design is a collection of $\mathcal{B}$ of elements of $\mathcal{P}_k(X)$ (called blocks) such that any triple (r_1, r_2, r_3) of points is collinear. Such sets are called lines in $\mathcal{B}$ and every line intersect $\mathcal{B}$ in exactly λ points. In general r-designs admitting $\mathrm{PG}(2,q)$ as a group of automorphisms are known as $(k;r)$ arcs.

Let V be a 3-dimensional vector space over $\mathbb{F}_q$ and consider the projective plane $PG(2,q)$ defined by the incidence structure $(\mathcal{P}(V), \mathcal{B}(V), I)$.

Definition 3.2. *A $(k;r)$-arc $\mathcal{K}$ in $PG(2,q)$ is a set of k-points such that some r, but not $r+1$ of them are collinear. In other words, some line of the plane meets $\mathcal{K}$ in r points and no more than r-points. A $(k;r)$-arc is complete if there is no $(k+1;r)$ arc containing it.*

Definition 3.3. *A k-arc is a $(k;n,n-1;n,p)$ set with $n \geq 3$ of k-points such that, every subset of s points with $s \leq n$ points is linearly independent.*

Following the classification of conjugacy classes in $PG(2,q)$ in next Lemma classifies designs constructed from the projective line[7].

Lemma 3.4. *There are 3 types of r-designs constructed from $\mathrm{PG}(2,q)$: unipotent type, semisimple split or semisimple non-split according to the eigenvalues of the representation matrix of the generating elements in $\mathrm{PG}(2,q)$.*

Proof. If the characteristic polynomial $P(\lambda)$ of the representation matrix A has only one root, call it α, it is a primitive element of order p a prime

number, then the derived design is called unipotent. It is an arc containing $p+1$ points and for $n < p$ every set of $n+1$ points are linearly independent. If $P(\lambda)$ has two different roots $a, a^{-1} \in \mathbb{F}_q^*$, $tr(A) = a + a^{-1}$ is an element α of order dividing $\frac{q-1}{d}$. The corresponding design is called semisimple split, and finally if there are no roots, $tr(A) = a + a^q = \alpha$, where $a \in \mathbb{F}_{q^2}^* \backslash \mathbb{F}_q^*$ is an element α dividing $\frac{q+1}{d}$, the corresponding design is called semisimple non-split. □

We associate to the 2-design generated by τ and σ the graph which has as vertex set V the points of the projective system $\mathbb{P}((\mathbb{F}_2)^m)$ and edge set $E \subseteq [V]^2$ the lines of the projective space which corresponds to the blocks of the design. There are $\begin{bmatrix} m \\ 2 \end{bmatrix}_q$ lines. For any two points there are as much blocks (lines) containing these points as eigenspaces W_j by the action of the linear operators τ and σ. This special design with parameters $t = 2$ and $k = 3$ is a Steiner triple system. The automorphism group of the projective line $\mathbb{P}(\mathbb{F}_q)$ is the projective linear group $\mathrm{PGL}(2, q)$. Any finite subgroup $A \subset \mathrm{PGL}(2, q)$ defines a $k-$uniform Cayley (sum) hypergraph $\Gamma^k(A)$ whose vertices are the generating $k-$tuples of A and the edges are $k-$element sets $\{x_1, \ldots, x_k\} \in \binom{G}{k}$ represented by random variables $x_1, \ldots, x_k$. In particular, if $f(z)$ is the ordinary generating function that enumerates A, that is, number of conjugacy classes in A, then $\frac{1}{1-f(z)}$ is the ordinary generating function enumerating sequences of k elements in A. If G is an abelian group, then $x_1 + \cdots + x_k \in A$. In general, we will consider k-arcs in $\Gamma(A)$ which represent casual connections between the variables.

The group $\mathrm{GL}(n, q)$ acts transitively on subsets of size $n + 1$ of the projective line whenever $q \equiv n+1 (mod\, n+2)$. We can construct secret sharing schemes from configurations of points of size $n + 1$ on the projective line. Moreover we can construct secret sharing schemes from configuration of points on curves admitting a transitive linear action. Let p be a prime number and $p \geq n + 2$, then the Normal Rational Curve defined as:

$$\mathcal{V}_1^n := \left\{ F(1, x, x^2, \ldots, x^n) |\ x \in \mathbb{F}_p \bigcup \{\infty\} \right\}$$

is an example of a $(p+1)$-arc. It contains $p+1$ points, and every set of $n+1$ points are linearly independent[8-19].

1. S Bezzateev, N Shekhunova (2013) Class of generalized Goppa codes perfect in weighted Hamming metric, Des. Codes Criptogr., 66:391-399.
2. A Besana, C Martínez (2020) A Geometrical Realisation of Quasi-Cyclic Codes, in Book: Combinatorics, Probability and Control https://www.researchgate.net/publication/337293717_A_Geometrical_Realisation_of_Quasi-Cyclic_Codes.
3. W Diffieand, ME Hellman (1976) New directions in cryptography, IEEE Trans actions on Information Theory https://www-ee.stanford.edu/~hellman/publications/24.pdf.
4. H Arslan, A Altoum, M Zaarour (2024) Integer representations of classical Weyl groups, Turkish Journal of Mathematics 48:377-390.
5. BD Mac Arthur, RJ Sanchez Garcıa, James N Anderson (2008) Symmetry in complex networks, Discrete Applied Mathematics 156: 525-531.
6. A Besana, C Martínez (2018) AGC, t-designs, and set partitions, Electronics notes in Discrete Mathematics, 65:3-9.
7. Shelly Garion (2005) Expansion of conjugacy classes, Journal of Group Theory https://arxiv.org/abs/1307.6662.
8. K Behrend, B Noohi (2006) Uniformization of Deligne-Mumford curves, J. Reine Angew. Math https://arxiv.org/abs/math/0504309.
9. GV Belyi, On galois (1980) extensions of a maximal cyclotomic field, Math. U.S.S. R Izvestija 14:247-256.
10. D Crmkoviıc, N Mostarac, S Rukavina (2016) Self dual codes from quotient matrices of

symmetric divisible designs with the dual property, Discrete Mathematics 339: 409-414.

11. Y Meng Chee, San Ling (2017) Constructions for qAry Constant-Weight Codes, IEEE Transactions on Information Theory https://arxiv.org/abs/0705.0081.
12. G Ge, H Wei (2014) Group divisible designs with block sizes from K1(3) and Kirkman frames of type hum1, Discrete Mathematics 329: 42-68.
13. Willem h Haemers, Hadi Kharaghani, Maaike A (2011) Menlenberg. Divisible design graphs, J. of Combinatorial Theory, Series A 118: 978-992.
14. M Hattori, R J Mc Eliece, G Solomon (1998) Subspaces subcodes of Reed Solomon Codes IEEE Transactions on Information Theory https://dl.acm.org/doi/abs/10.1109/18.705564.
15. R Kotter, F R Kschischang (2008) Coding for Errors and Erasures in Random Network Coding, IEEE Transactions on information Theory https://arxiv.org/abs/cs/0703061.
16. A Knopf Macher, RF Tichy, S Wagner, V Ziegler (2007) Graphs, partitions and Fibonacci Numbers, Discrete Applied Mathematics https://www.sciencedirect.com/science/article/pii/S0166218X06005026.
17. D Panario, P Flajolet, X Gourdon (2001) The complete analysis of a polynomial factorization algorithm over finite fields Journal of Algorithms 40: 37- 41.
18. JP Serre (1988) Topics in Galois Theory, Course at Harvard University, Fall http://cm2vivi2002.free.fr/JPS-biblio/JPS-32.pdf.
19. A Caminata, N Giansiracusa, Han-Bom Moon, L Schaffler (2018) Equations for point configurations to lie on a rational normal curve, Advances In mathematics 340: 653-683.