CONSTRUCTING SET SYSTEMS FROM GRAPH ALPHABETS

CRISTINA MARTÍNEZ AND ALBERTO BESANA

ABSTRACT. We construct an algebraic equivalence between set systems with a given alphabet graph G and constant dimension codes (CDC) over finite fields. Moreover, we see that set systems generalise $t-$designs and groups divisible designs. Furthermore in the context of secret sharing schemes, we construct 2-designs from the projective line.

1. INTRODUCTION

Methods of classification of data sets which can be recorded as strings of sequences of letters over a finite alphabet, use graph theory. One of the most important classes of graphs considered in this framework is that of Cayley graphs. Consider a network represented by a directed multigraph $G = (V(G), E(G))$, with vertex set $V(G)$ and edge set, $E(G)$ with error free unit capacity edges, that is, a graph with loops (edges whose endpoints are equal) and multiple edges. Let G be a simple graph and H a subgraph of G. A $G-$design of H is a pair where X is the vertex set of H and $\mathscr{B}$ is an edge-disjoint decomposition of H also known as partition of the vertex set. The best known cryptographic problem is that of privacy: preventing the unauthorized 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.

A group divisible design (GDD) is an incidence structure $(X, \mathscr{G}, \mathscr{B})$ where X is a set of points, $\mathscr{G}$ is a partition of X into groups, and $\mathscr{B}$ is a collection of subsets of X called blocks such that any pair of distinct points from X occurs either in some group or in exactly one block, but not both, see [GW]. 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. The adjacency matrix of the graph is interpreted as the incidence matrix of the design. 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.

2000 *Mathematics Subject Classification.* 11T71 (primary) ; 05E10 (secondary) .

Key words and phrases. Algebraic code, t-design, bases.

2. CONSTANT DIMENSION CODES OVER FINITE FIELDS FROM $t-$DESIGNS

A simple $t-$design over a finite field or, more precisely, a $t-(n,k,\lambda;q)$ design is a set $\mathscr{B}$ of $k-$subspaces of an $n-$dimensional vector space V over the finite field $\mathbb{F}_q$ such that each $t-$subspace of V is contained in exactly λ blocks of $\mathscr{B}$. Recently, designs over finite fields gained a lot of attention because of its applications for error-correcting in networks. If V is the finite field $\mathbb{F}_q^n$, then the set of points are the vectors and the block set $\mathscr{B}$ of k subspaces $K \subseteq \mathbb{F}_q^n$ are the points in the Grassmannian $\mathscr{G}_{k,n}(\mathbb{F}_q)$.

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 neighbors of the vertices are the blocks. Reciprocally given a $k-$regular graph on v vertices, if any two distinct vertices have exactly λ common neighbors it is a 2-(v,k,λ) design.

2.1. **Set systems.** A set system is a pair $(X,\mathscr{A})$ such that X is a finite set of points and $\mathscr{A}$ 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 $(X,\mathscr{A})$ is said to be $K-$uniform if $|A| \in K$ for all $A \in \mathscr{A}$. Let $\mathscr{G} = \{G_1,\ldots,G_s\}$ be a partition of X into subsets called groups. The triple $(X,\mathscr{G},\mathscr{A})$ 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 $A \in \mathscr{A}$ and $G \in \mathscr{G}$.

Proposition 2.1. *There is 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 neighboors . There is an action of the symmetric group S_n on the combinatorial class $\mathscr{G}_n$ of regular graphs with n vertices. For any $\sigma \in S_n$ and $g \in \mathscr{G}_n$, 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 $(\mathbb{F}_q)^n$:

$$\Phi(\Gamma(G_\lambda))(x) = A_{t,k}^{G_\lambda}\, x. \tag{1}$$

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 1. 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 $rank\,(A_{t,k}^G) \geq t$.

□

2.2. **r-designs constructed from the projective line.** Let X be a v-set and $\mathscr{P}_k(X)$ denote the set of all $k-$subsets of X. A $t-(v,k,\lambda)-$design is a set system $\mathscr{D} = (X,D)$ in which D is a collection of $\mathscr{P}_k(X)$ (called blocks) such that every $t-$subset of X appears in exactly $\lambda-$blocks

Definition 2.2. *A $(k;r)-$arc $\mathscr{K}$ 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 $\mathscr{K}$ 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.*

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 $(\mathscr{P}(V),\mathscr{B}(V),I)$.

A 2-(v,k,λ) design is a collection $\mathscr{B}$ of elements of $\mathscr{P}_k(X)$ (called blocks) such that every line of the incidence structure $(\mathscr{P}(X),\mathscr{B}(X),I)$ intersect $\mathscr{B}$ in exactly λ points. This is also known as a perfect secret sharing scheme S for a finite graph G access structure of v vertices. Namely, a partition of subsets of vertices of G of size k such that every 2-subset is contained in at least $\lambda-$subsets of G.

A 3-(v,k,λ) design is a collection of $\mathscr{B}$ of elements of $\mathscr{P}_k(X)$ (called blocks) such that any triple (r_1,r_2,r_3) of points is collinear. Such sets are called lines in $\mathscr{B}$ and every line intersect $\mathscr{B}$ in exactly λ points. In general $r-$designs admitting $\mathrm{PG}(2,q)$ as a group of automorphisms are known as $(k;r)$ arcs.

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

Lemma 2.3. *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 in [BM] 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.

REFERENCES

[BB] K. Behrend, B. Noohi, *Uniformization of Deligne-Mumford curves*, J. Reine Angew. Math., 599 (2006), 111-153.

[Be] G. V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Math. U.S.S. R. Izvestija 14, 247-256 (1980).

[BS1] S. V. Bezzateev, N. Shekhunova, *Class of generalized Goppa codes perfect in weighted Hamming metric*, Des. Codes Criptogr. (2013), 66:391-399.

[BS2] S. V. Bezzateev, N. A. Shekhunova, *Subclass of cyclic Goppa codes*, IEEE Transactions on Information Theory, Vol. 59, No. 11, Nov. 2013.

[BM] A. Besana, C. Martínez, *AG codes, $t-$designs and partition sets)*, Electronic notes in Discrete Mathematics, Vol. 65, 3-9 (2018).

[Go] Goppa, V. D.: Codes on algebraic curves (Russian). Dokl. Akad. Nauk. SSSR 259, 1289-1290 (1981).

[GW] G. Ge, H. Wei, *Group divisible designs with block sizes from $K_{1(3)}$ and Kirkman frames of type $h^u m^1$*, Discrete Mathematics 329 (2014), 42-68.

[KK] R. Kötter, F. R. Kschischang, *Coding for errors and erasures in random Network Coding*, IEEE Transactions on Information Theory, Vol. 54, no. 8, 2008.

[MWS] F.J. Mac Williams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland.

[SG] Shelly Garion, *Expansion of conjugacy classes*, Journal of Group Theory, Vol. 18, No. 6, 2005.

[SRSK] N.M.G. Al-Saidi, N. A. Rajab, M. R. Md. Said, K. A. Kadhim, *Perfect secret sharing scheme based on vertex domination set*, International Journal of Computer Mathematics, Vol. 92, no. 9, 2015.

UNIVERSITAT AUTÒNOMA DE BARCELONA, 08193 BELLATERRA, BARCELONA
E-mail address: cristina@iiia.csic.es
E-mail address: abesana@amaris.cat