Similarity between the Algebraic Structure Associated Projective Spaces and Design Combinatorics via Hasse Diagram

Leandro Bezerra de Lima and Reginaldo Palazzo Jr.

School of Electrical and Computer Engineering (FEEC) - University of Campinas -UNICAMP, Campinas-SP, Brazil

XXI Colóquio Latinoamericano de Álgebra - UBA - Buenos Aires - ARG

Introduction

Abstract: Combinatorial design is an important combinatorial structure having a high degree of regularity and which is related to the existence and construction of systems of sets with finite cardinality, [3]. As examples we mention the existing relationship between error-correcting codes in the Hamming space and combinatorial design, where the codewords of weight 3 of the Hamming code form a triple Steiner system STS(7), a projective plane of order 2, known as the Fano plane, as well as q-analogs of a code whose codewords have constant Hamming weight in the Hamming space, a code belonging to a Grassmannian in the projective space. Projective space of order m over a finite field $\mathbb{F}_p$, denoted by $\mathcal{P}(\mathbb{F}_p^m)$, (note that $\mathbb{F}_{p^m}$ is isomorphic to $\mathbb{F}_p^m$), is the set of all the subspaces in the vector space $\mathbb{F}_p^m$. The projective space endowed with the subspace distance $d(X,Y) = dim(X) + dim(Y) - 2dim(X \cap Y)$ is a metric space. Hence, the subspace code $\mathcal{C}$ with parameters (n, M, d) in the projective space is a subset of $\mathcal{P}(\mathbb{F}_p^m)$ with cardinality M with a subspace distance at least d between any two codewords, [2]. In this paper we show the existing similarity between the Hasse diagram of an Abelian group consisting of the product of multiplicative finite Abelian groups $\mathbb{Z}_p^m$ and the Hasse diagram of the projective space $\mathcal{P}(\mathbb{F}_p^m)$, with the aim to provide the elements that may be useful in the identification and in the construction of good subspaces codes, [1].

Partially Ordered Sets - Poset:

Definition 10 *Let P be a non-empty set. We say that a binary relation is a* **partial order** *in P, denoted by "$\leq$", if it satisfies the following properties:*

- *$a \leq a$, for every $a \in P$ (reflexive);*
- *If $a, b \in P$ are such that $a \leq b$ and $b \leq a$, then $a = b$ (anti-symmetric);*
- *If $a, b, c \in P$ are such that $a \leq b$ and $b \leq c$, then $a \leq c$ (transitive).*

Observation 3 *In this context, we say that $(P, \leq)$ is a* **poset**. *We may say that if $a \leq b$ then a precede b, and that a and b are comparable. We also say that b is a successor of a if $a < b$ and if there is no $x \in P$ such that $a < x < b$.*

Combinatorial Design

Example 1 *Let G be a group. The set of subgroups of G, with the inclusion relation, is a poset, denoted by $R(G)$.*

Definition 1 *Let P and Q be two posets. We say that an application $\varphi : P \to Q$ is:*

- **isotone**, *if for $a, b \in P$ such that $a \leq b$ we have $\varphi(a) \leq \varphi(b)$.*
- **antitone**, *if for $a, b \in P$ such that $a \leq b$ we have $\varphi(b) \leq \varphi(a)$.*

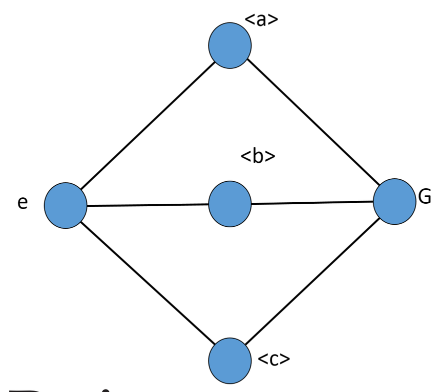
Definition 2 *An* **isomorphism** *of ordered sets is defined as the isotone bijection with an isotone inverse. If there exists an isomorphism $\varphi : P \to Q$ we say that P and Q are isomorphic sets, and denote this by $P \simeq Q$.*

Observation 1 *If $\varphi : P \to Q$ is an isomorphism of the ordered sets and $x, y \in P$ are distinct elements, then:*

$$x < y \leftrightarrow \varphi(x) < \varphi(y)$$

Therefore, all the hierarchical relations among elements are preserved by isomorphism, thus having the same Hasse diagram. The converse is also true, that is, posets having the same Hasse diagram are isomorphic.

Example 2 *G with this operation is the Klein group. The corresponding subgroups are $\{e\}, G, \langle a \rangle = \{e, a\}, \langle b \rangle = \{e, b\}, \langle c \rangle = \{e, c\}$. Hence, $R(G)$ has 5 elements, among them G and $\{e\}$ are the maximum and the minimum, respectively, whereas the remaining are two-by-two not comparable. Therefore, the Hasse diagram of $R(G)$ is:*



Combinatorial Design:

Definition 3 *Let $X \neq \emptyset$ be a set with v elements and $B \neq \emptyset$ a collection of b distinct subsets of X with cardinality $k > 0$. Define (X, B) as a* **t-design** *with parameters (v, k, λ), where $0 < t < k < v$ and $\lambda > 0$, if each subset with cardinality t is contained in exactly λ elements of B. The elements of B are called* **blocks**.

Projective Spaces and Subspace Codes

In this work our attention is in the construction of special designs with $t = 2$, each pair of elements of X is contained in λ blocks. For this case, we use the following notation (v, k, λ) - **BIBD** (BIBD - Balanced Incomplete Block Design).

Proposition 1 *If (X, B) is a (v, k, λ)-BIBD, then each element of X belongs to r blocks, where:*

$$b.k = r.v \quad and \quad r(k-1) = \lambda(v-1)$$

Definition 4 *A (v, k, λ)-BIBD (X, B) is said to be* **symmetric** *if $|X| = |B| = v = b$.*

Definition 5 *A* **pairwise balanced design - PBD** *is a design (X, B), such that each pair of distinct elements of X is contained in exactly λ blocks, where λ is a positive integer. Furthermore, (X, B) is a* **regular pairwise balanced design - PBD Regular** *if for every element $x \in X$ occurs exactly in $B_{i's} \in B$, such that r is a positive integer.*

Definition 6 *A t-design with parameters $(v, k, 1)$ is defined as a* **Steiner system** *and denote it by $S(t, v, k)$.*

Definition 7 *Define a* **triple Steiner system** *of order v, denoted by $STS(v)$, as being a Steiner system with parameters $(2, v, 3)$.*

A triple Steiner system $STS(v)$ is a $(v, 3, 1)$-BIBD.

Proposition 2 *A necessary condition for the existence of a triple Steiner system of order v, with $v \geq 3$, is that $v \equiv 1 mod\, 6$ or $v \equiv 3 mod\, 6$.*

Definition 8 *Let W be a vector space with dimension m over $\mathbb{F}_q$. The* **projective space** *of W is defined as the set of all the vector subspaces of W and it is denoted by $\mathbb{P}(W)$. Furthermore, the set of all the subspaces with a given dimension k is called* **Grassmannian** *and denoted by $\mathcal{G}(W, k)$.*

Observation 2 *Every vector space W of dimension n over $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_q^n$. Thus, we may consider $W = \mathbb{F}_q^n$, without loss of generality. Hence, the vector space are n-tuples with elements in $\mathbb{F}_q$.*

Definition 9 **Hasse diagram***: In our context, it is possible to construct a Hasse diagram, since the projective space $\mathbb{P}(F_q^n)$ with the following order relation $\preceq$, such that $V_1 \preceq V_2$ if, and only if, V_1 is a subspace of V_2, and it is partially ordered. Two subspaces are connected if, and only if, V_1 is a subspace of V_2 and $dimV_2 = dimV_1 + 1$ or vice-versa. Hence, from the Hasse diagram, we may interpret the distance between two subspaces V_1, V_2 in $\mathbb{P}(F_q^n)$ as the path with the least distance connecting V_1 and V_2 (geodesic).*

Relations between Combinatorial Design and Projective Spaces and Similarities:

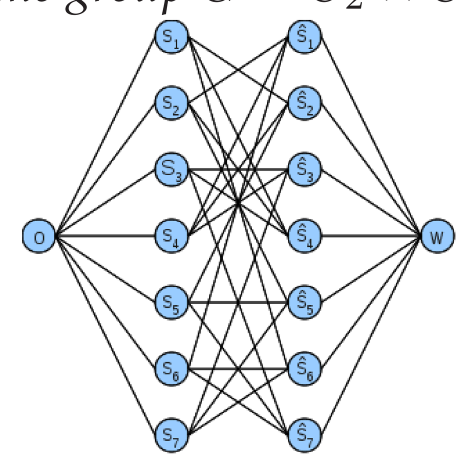
Theorem 1 *Let $q \geq 2$ be a prime power and $d \geq 2$ an integer. Then there exists a symmetric design:*

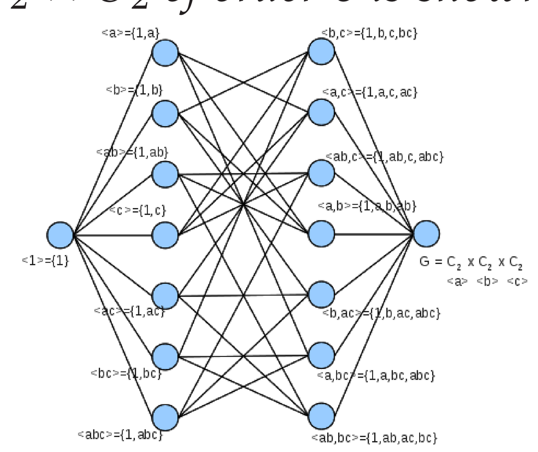
$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right) - BIBD.$$

Corollary 1 *For each prime power $q \geq 2$ and $d = 2$. Then there exists a symmetric $(q^2+q+1, q+1, 1)$-BIBD, that is, a projective plane of order q.*

Example 3 *There exists a symmetric $(31, 6, 1)$-BIBD (projective plane of order 5) and one symmetric $(57, 8, 1)$-BIBD (projective plane of order 7) describing, respectively, the projective spaces $\mathbb{P}(\mathbb{F}_5^3)$ and $\mathbb{P}(\mathbb{F}_7^3)$.*

Example 4 *A relation between the projective space $\mathbb{P}(\mathbb{F}_2^3)$ and the group $G = C_2 \times C_2 \times C_2$ of order 8 is shown next.*





Algebraic Structure of a Class of Projective Spaces

Generalizing the previous examples, we have associated to the symmetric design $(q^2+q+1, q+1, 1)$-BIBD, q-prime, an algebraic structure $G = C_p \times C_p \times C_p$ of order p^3, having subgroups of order p^2, p and 1 describing the same combinatorial structure as that of the projective space $\mathbb{P}_q^3$.

References

[1] C.H.A. Costa and M. Guerreiro. *Automorphisms of finite Abelian groups(in Portuguese)*. MS thesis, Mathematics Dept, UFV, Viçosa, 2014.

[2] Khaleghi A. Silva, D. and F.R. Kschischang. *Subspace Codes*, volume 5921. Lecture Notes in Computer Science, 2009.

[3] D.R. Stinson. *Combinatorial Designs: Contructions and Analysis*. Springer Verlag, 2004.

Future Research

- Using this similarity with the aim to provide the elements that may be useful in the identificationand in the construction of good subspaces codes.
- Expand the search for similarities to other classes of projective spaces.