Graph decompositions in projective geometries

Marco Buratti1 | Anamari Nakić2 | Alfred Wassermann3

1Dipartimento di Matematica e Informatica, Università di Perugia, Perugia, Italy
2Faculty of Electrical Engineering and Computing, University at Zagreb, Zagreb, Croatia
3Department of Mathematics, University of Bayreuth, Bayreuth, Germany

Abstract
Let $\text{PG}(\mathbb{F}_q^v)$ be the $(v - 1)$-dimensional projective space over $\mathbb{F}_q$ and let $\Gamma$ be a simple graph of order $q^k - 1$ for some $k$. A $2 - (v, \Gamma, \lambda)$ design over $\mathbb{F}_q$ is a collection $B$ of graphs (blocks) isomorphic to $\Gamma$ with the following properties: the vertex set of every block is a subspace of $\text{PG}(\mathbb{F}_q^v)$; every two distinct points of $\text{PG}(\mathbb{F}_q^v)$ are adjacent in exactly $\lambda$ blocks. This new definition covers, in particular, the well-known concept of a $2 - (v, k, \lambda)$ design over $\mathbb{F}_q$ corresponding to the case that $\Gamma$ is complete. In this study of a foundational nature we illustrate how difference methods allow us to get concrete nontrivial examples of $\Gamma$-decompositions over $\mathbb{F}_2$ or $\mathbb{F}_3$ for which $\Gamma$ is a cycle, a path, a prism, a generalized Petersen graph, or a Möbius ladder. In particular, we will discuss in detail the special and very hard case that $\Gamma$ is complete and $\lambda = 1$, that is, the Steiner 2-designs over a finite field. Also, we briefly touch the new topic of near resolvable $2 - (v, 2, 1)$ designs over $\mathbb{F}_q$. This study has led us to some (probably new) collateral problems concerning difference sets. Supported by multiple examples, we conjecture the existence of infinite families of $\Gamma$-decompositions over a finite field that can...
be obtained by suitably labeling the vertices of $\Gamma$ with the elements of a Singer difference set.

**KEYWORDS**
design over a finite field, difference family, difference set, graph decomposition, group divisible design over a finite field, projective space, spread

**MATHEMATICS SUBJECT CLASSIFICATION (2010)**
05B05; 05B10; 05B25; 05B30

# INTRODUCTION

This study has been inspired by the natural relationship between classic 2-designs and 2-designs over a finite field, and between classic 2-designs and graph decompositions. Hence, it involves three of the main characters of combinatorics that are designs, graphs, and finite geometries.

Designs over finite fields have been introduced in the 1970s [19,20,22]. Even though they are a generalization of the classic $t$-designs that date back to the 1930s, they are not $t$-designs in the classic sense when $t > 2$. Instead, a 2-design over a finite field $F_q$ is a 2-design in the classic sense with the tremendous constraint that its points are those of a projective space $P$ over $F_q$ and that its blocks are suitable subspaces of $P$. This is the reason for which in this paper we are interested only in the special case $t = 2$.

The theory of graph decompositions originates from design theory, especially from the quite evident fact that a $2 - (v, k, 1)$ design is completely equivalent to a decomposition of the complete graph of order $v$ into cliques of order $k$. Thus, for what said above, a 2-design over a finite field $F_q$ can be seen as a decomposition of the complete graph whose vertices are the points of a projective space $P$ over $F_q$ into cliques each of which has a subspace of $P$ as vertex set.

On the basis of the above observations, we propose to consider, much more generally, decompositions of a graph $K$ with vertex set the points of a projective space $P$ into copies of a graph $\Gamma$ each of which has a subspace of $P$ as vertex set. If $P$ is over $F_q$ and its dimension is $v - 1$, we will refer to this decomposition as a $2 - (v, \Gamma, 1)$ design over $F_q$.

Designs over finite fields have recently received a huge amount of attention because of the discovering in [4] of a nontrivial Steiner 2-design over a finite field which was conjectured could not exist for a long time. Unfortunately, for the time being, it seems that there is no hope to find others. To relax the definition of a Steiner 2-design over $F_q$ to that of a $2 - (v, \Gamma, 1)$ design over $F_q$ seems to promise much more results even though the related problems still appear very difficult, hence challenging. Thus we hope that this new topic of “graph decompositions over a finite field” may open the doors to a fruitful research in the future.

The article will be structured as follows. Section 2 is useful for understanding the notation and terminology used throughout the paper. In Section 3 we recall the definitions of a classic 2-design, of a group divisible design (GDD), and their versions over a finite field. All these definitions will be relaxed in Section 4 in terms of graph decompositions. In Section 5, generalizing what has already been done by the first two authors in [18], the difference methods of the classic design theory will be adapted to graph decompositions over a finite field; these methods will be crucial for all the concrete constructions that we are able to exhibit in the paper.
In Section 6 we discuss the possible existence of a Steiner 2-design over a finite field. In particular, we prove a necessary condition which seems to have gone unnoticed before and we revisit the nontrivial Steiner 2-design over a finite field mentioned above. In Sections 7 and 8 we give necessary conditions for the existence of cycle- and path-decompositions over a finite field providing some concrete examples over \( \mathbb{F}_2 \) and \( \mathbb{F}_3 \). In Section 9 we propose some problems on difference sets. In particular, given a \((2s + 1, k, \lambda)\) difference set \( D \) in a group \( G \), and given a graph \( \Gamma \) of order \( k \) and size \( s \), we ask whether it is possible to label the vertices of \( \Gamma \) with the elements of \( D \) in such a way that every nonidentity element of \( G \) may be expressed as a difference of two “adjacent labels.” We conjecture that the answer is always affirmative if \( \Gamma \) is regular and connected. The proof of this conjecture when \( D \) is a Singer difference set would give an infinite family of nontrivial decompositions over a finite field, that is, a \( v_2(\Gamma, 1) \) design over \( \mathbb{F}_q \) for every regular and connected graph \( \Gamma \) of order \( q^2 - 1 - v - 1 \).

In Section 10 such a design has been found in each of the following cases: \( v \in \{4, 5, 6, 7\} \), \( q = 2 \), and \( \Gamma \) is the \((2^v - 1)\)-cycle; \( v = 5 \), \( q = 3 \), and \( \Gamma \) is a prism or a generalized Petersen graph or a Möbius ladder on 40 vertices. Finally, in Section 11, we make a short discussion about improper graph decompositions over a finite field, that is, \( v_2(\Gamma, 1) \) designs over \( \mathbb{F}_q \) where \( \Gamma \) has at least one isolated vertex.

### 2 | NOTATION AND TERMINOLOGY

For \( q \) a prime power, \( \mathbb{F}_q \) will denote the finite field of order \( q \) and \( \text{PG}(\mathbb{F}_q^v) \) is the \((v - 1)\)-dimensional projective space over \( \mathbb{F}_q \). The number of points of \( \text{PG}(\mathbb{F}_q^v) \) will be denoted by \([v]_q\).

Hence we have

\[
[v]_q = \frac{q^v - 1}{q - 1} = \sum_{i=0}^{v-1} q^i.
\]

By \([Z_v]_q\) we will denote the Singer group of order \([v]_q\), that is, the quotient group between the multiplicative groups of the fields of order \( q^v \) and \( q \):

\[ [Z_v]_q = \mathbb{F}_q^*/\mathbb{F}_q^* . \]

This group acts sharply transitively on the point-set of \( \text{PG}(\mathbb{F}_q^v) \). Hence, the points of \( \text{PG}(\mathbb{F}_q^v) \) will be always identified with the elements of \([Z_v]_q\).

By analogy, given that \( m\mathbb{Z}_{mn} = \{mi | 0 \leq i \leq n - 1\} \) is the subgroup of \( \mathbb{Z}_{mn} \) of order \( n \), the subgroup of \([Z_{mn}]_q\) of order \([n]_q\) will be denoted by \([m\mathbb{Z}_{mn}]_q\). Thus, if \( g \) is a generator of \( \mathbb{F}_q^* \), we have

\[ [m\mathbb{Z}_{mn}]_q = \{g^{i|m|q^i} | 0 \leq i \leq [n]_q - 1\} . \]

Throughout the paper, \( \mathbb{K}_v \) is the complete graph on an abstract set of \( v \) vertices, \( \mathbb{K}_v^V \) is the complete graph on a concrete set \( V \), and \( \mathbb{K}_{m \times n} \) is the complete \( m \)-partite graph whose parts have size \( n \). The cycle and the path on \( k \)-vertices will be denoted by \( C_k \) and \( P_k \), respectively. If \( \lambda \) is a positive integer and \( \Gamma \) is a graph, then \( \lambda \Gamma \) will denote the \( \lambda \)-fold of \( \Gamma \).

If \( \Gamma \) is an abstract graph, when we refer to a \( \Gamma \)-subgraph of \( \mathbb{K}_v \), we will mean a subgraph of \( \mathbb{K}_v \) isomorphic to \( \Gamma \). If \( q \) is a prime power, an abstract graph \( \Gamma \) will be called \( q \)-spaceable if its order is the number of points of a projective space over \( \mathbb{F}_q \) of a suitable dimension, that is, if its
vertex set has size $[k]_q$ for some $k$. Finally, speaking of a $\Gamma$-subspace of $\text{PG}(\mathbb{F}_q^v)$ we will mean a graph isomorphic to $\Gamma$ whose vertex set is a subspace of $\text{PG}(\mathbb{F}_q^v)$. Of course, in this case $\Gamma$ must be $q$-spaceable.

Let $G$ be a group and let $B$ be a simple graph with vertices in $G$. By list of differences of $B$ we will mean the multiset $\Delta B$ of all possible differences $x - y$ or quotients $xy^{-1}$ (depending on whether $G$ is additive or multiplicative) with $(x, y)$ an ordered pair of adjacent vertices of $B$. Note that if $B$ is complete with vertex set $V(B)$, then $\Delta B$ coincides with the list of differences of the set $V(B)$ in the usual sense.

The list of differences of $B$ can be conveniently displayed by means of its difference table. This is the square matrix $T(B)$ whose rows and columns are labeled with the vertices $b_1, ..., b_k$ of $B$ and where the entry $t_{ij}$ is empty or equal to the difference $b_i - b_j$ (or the quotient $b_i b_j^{-1}$ if $G$ is multiplicative) according to whether $b_i$ is not adjacent or adjacent to $b_j$, respectively.

If $\mathcal{F}$ is a family of subgraphs of $\mathbb{K}_G$, then the list of differences of $\mathcal{F}$ is the multiset sum $\Delta \mathcal{F} = \bigcup_{B \in \mathcal{F}} \Delta(B)$.

The development of $B$ and $\mathcal{F}$, denoted by $\text{dev}B$ and $\text{dev} \mathcal{F}$, is the multisets of graphs defined by

$$\text{dev}(B) = \{B_g | g \in G\} \quad \text{and} \quad \text{dev} \mathcal{F} = \bigcup_{B \in \mathcal{F}} \text{dev}(B),$$

where $B_g$ is the graph obtained from $B$ by replacing each $b \in V(B)$ with $b + g$ or $bg$ according to whether $G$ is additive or multiplicative, respectively.

### 3 | DESIGNS OVER A FINITE FIELD

Let us recall the well-known notion of a $t$-design.

**Definition 3.1.** A $t - (v, k, \lambda)$ design is a pair $(\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is a set of $v$ points, and $\mathcal{B}$ is a collection of $k$-subsets (blocks) of $\mathcal{P}$ such that every $t$-subset of $\mathcal{P}$ is contained in exactly $\lambda$ blocks.

The above definition has been generalized as follows.

**Definition 3.2.** A $t - (v, k, \lambda)$ design over $\mathbb{F}_q$—or a $t - (v, k, \lambda)_q$ design to be brief—is a collection $S$ of $k$-dimensional subspaces of the vector space $\mathbb{F}_q^v$ with the property that any $t$-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly $\lambda$ members of $S$.

A $t - (v, k, \lambda)$ design over $\mathbb{F}_q$ is also said the $q$-analog of a $t - (v, k, \lambda)$ design or a $t - (v, k, \lambda)_q$ subspace design.

In this paper we are interested only in the special case that $t = 2$. Every $q$-analog of a 2-design can be seen as a 2-design in the classic sense. Indeed, if $\text{PG}(\mathbb{F}_q^v)$ is the $(v - 1)$-dimensional projective space over $\mathbb{F}_q$, the definition of a $2 - (v, k, \lambda)_q$ design can be equivalently reformulated as follows.

**Definition 3.3.** A $2 - (v, k, \lambda)$ design over $\mathbb{F}_q$ is a classic $2 - ([v]_q, [k]_q, \lambda)$ design $(\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is the set of points of $\text{PG}(\mathbb{F}_q^v)$ and where every $B \in \mathcal{B}$ is a $(k - 1)$-dimensional subspace of $\text{PG}(\mathbb{F}_q^v)$.
The set of points and the set of all possible \((k - 1)\)-dimensional subspaces of \(\text{PG}(\mathbb{F}_q^k)\) are the complete \(2 - (v, k, \lambda)_q\) design where \(\lambda = \prod_{i=1}^{k-2} \frac{q^{i+1} - 1}{q^i - 1}\). In particular, for \(k = 2\), the set of points and the set of lines of \(\text{PG}(\mathbb{F}_q^2)\) are a \(2 - (v, 2, 1)_q\) design. For an overview of known results about \(2 - (v, k, \lambda)_q\) designs see [7].

Now we recall the definitions of a classic group divisible design and of a group divisible design over a finite field.

**Definition 3.4.** An \((mn, n, k, \lambda)\) group divisible design is a triple \((\mathcal{P}, \mathcal{G}, \mathcal{B})\) where \(\mathcal{P}\) is a set of \(mn\) points, \(\mathcal{G}\) is a partition of \(\mathcal{P}\) into \(m\) sets (classes) of size \(n\), and \(\mathcal{B}\) is a collection of \(k\)-subsets of \(\mathcal{P}\) (blocks) such that each block meets each class in at most one point and any two points belonging to different classes are contained in exactly \(\lambda\) blocks.

We also recall that GDDs are often useful to construct 2-designs in many ways. In particular, it is evident that the existence of a \((mn, n, k, \lambda)\)-GDD and of a \(2 - (n, k, \lambda)\) design implies the existence of a \(2 - (mn, k, \lambda)\) design.

The \(q\)-analog of a classic GDD has been recently introduced in [14]. Its definition requires the notion of a \(d\)-spread of \(\text{PG}(\mathbb{F}_q^k)\), that is, a partition of the set of points of \(\text{PG}(\mathbb{F}_q^k)\) into \(d\)-dimensional subspaces. Such a \(d\)-spread exists if and only if \(d + 1\) is a divisor of \(v\). In particular, the Desarguesian \((n - 1)\)-spread of \(\text{PG}(\mathbb{F}_q^{mn})\) is the partition of \([m\mathbb{Z}_{mn}]_q\) into the cosets of \([m\mathbb{Z}_{mn}]_q\) (see, e.g., [30]).

**Definition 3.5.** An \((mn, n, k, \lambda)\)-GDD over \(\mathbb{F}_q\)—or an \((mn, n, k, \lambda)_q\)-GDD to be brief—is an \(([mn]_q, [n]_q, [k]_q, \lambda, \lambda)\)-GDD where the points are those of \(\text{PG}(\mathbb{F}_q^{mn})\), the classes are the members of an \((n - 1)\)-spread of \(\text{PG}(\mathbb{F}_q^{mn})\), and the blocks are \((k - 1)\)-dimensional subspaces of \(\text{PG}(\mathbb{F}_q^{mn})\).

As a special case of the remark that we have done on classic GDDs we can say that combining an \((mn, n, k, \lambda)_q\)-GDD with a \(2 - (n, k, \lambda)_q\) design one obtains a \(2 - (mn, k, \lambda)_q\) design.

## 4 GRAPH DECOMPOSITIONS OVER A FINITE FIELD

Now we want to make a link between designs over finite fields and graph decompositions.

**Definition 4.1.** Let \(\Gamma\) be a simple graph. A \(2 - (v, \Gamma, \lambda)\) design is a pair \((\mathcal{P}, \mathcal{B})\) where \(\mathcal{P}\) is a set of \(v\) points and where \(\mathcal{B}\) is a collection of \(\Gamma\)-subgraphs (blocks) of \(K_v\) such that any two distinct points are adjacent in exactly \(\lambda\) blocks.

In most of the literature (see, e.g., [9]) a design as above is said to be a \((\lambda K_v, \Gamma)\)-design or a \(\Gamma\)-decomposition of \(\lambda K_v\). Indeed, to say that \((\mathcal{P}, \mathcal{B})\) is a \(2 - (v, \Gamma, \lambda)\) design is equivalent to say that the edge sets of its blocks partition the edge multiset of \(\lambda K_v\). We changed a bit the formal definition just to keep notation and terminology of graph decompositions similar to those of classic 2-designs. It is evident that a \(2 - (v, K_k, \lambda)\) design is nothing but a classic \(2 - (v, k, \lambda)\) design. Thus, by Definition 3.3, any \(2 - (v, k, \lambda)_q\) design can be equivalently interpreted as a decomposition of the \(\lambda\)-fold of the complete graph on the points of \(\text{PG}(\mathbb{F}_q^v)\) into a collection of \(K_{[k]_q}\)-subspaces of \(\text{PG}(\mathbb{F}_q^v)\). This leads to the following new notion of a graph decomposition over a finite field.
Definition 4.2. A \( 2 - (v, \Gamma, \lambda) \) design over \( \mathbb{F}_q \) is a \( 2 - ([v]_q, \Gamma, \lambda) \) design \((\mathcal{P}, \mathcal{B})\) such that \( \mathcal{P} \) is the set of points of \( \text{PG}(\mathbb{F}_q^2) \), and each \( B \in \mathcal{B} \) is a \( \Gamma \)-subspace of \( \text{PG}(\mathbb{F}_q^2) \).

Note that a \( 2 - (v, [k]_q, \lambda) \) design over \( \mathbb{F}_q \) is essentially a \( 2 - (v, k, \lambda) \) design. Consistently, when \( \Gamma \) is a \( q \)-spaceable cycle or a \( q \)-spaceable path, we will adopt the following notation.

Notation 4.3. Speaking of a \( 2 - (v, C_k, \lambda) \) design" we will mean a \( 2 - (v, C_{[k]_q}, \lambda) \) design over \( \mathbb{F}_q \). Analogously, speaking of a \( 2 - (v, P_k, \lambda) \) design" we will mean a \( 2 - (v, P_{[k]_q}, \lambda) \) design over \( \mathbb{F}_q \).

Let us say that a \( 2 - (v, \Gamma, \lambda) \) design \((\mathcal{P}, \mathcal{B})\) is spanning if \( \Gamma \) has order \( v \), hence if all its blocks are spanning subgraphs of \( \mathbb{K}_\mathcal{P} \). It is obvious that every spanning \( 2 - ([v]_q, \Gamma, \lambda) \) design can be seen as a \( 2 - (v, \Gamma, \lambda) \) design over \( \mathbb{F}_q \); it is enough to rename the vertices of \( \mathbb{K}_{[v]_q} \) with the points of \( \text{PG}(\mathbb{F}_q^2) \). Thus, in the framework of designs over finite fields, the spanning designs will be considered trivial. In spite of this fact they could be helpful for the construction of some graph decompositions over a finite field which are not trivial at all (see Corollary 4.8).

Let us see which are the obvious necessary conditions for the existence of a graph decomposition over a finite field.

Proposition 4.4. The trivial necessary conditions for the existence of a \( 2 - (v, \Gamma, \lambda) \) design over \( \mathbb{F}_q \) are the following:

(i) \( \Gamma \) is \( q \)-spaceable;
(ii) the size of \( \Gamma \) is a divisor of \( \frac{1}{2} \lambda q [v]_q [v - 1]_q \);
(iii) the greatest common divisor of the degrees of the vertices of \( \Gamma \) divides \( \lambda q [v - 1]_q \).

Proof. Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be a \( 2 - (v, \Gamma, \lambda) \) design over \( \mathbb{F}_q \). By definition, the vertex set of every \( B \in \mathcal{B} \) is a subspace of \( \text{PG}(\mathbb{F}_q^2) \), hence \( \Gamma \) is \( q \)-spaceable. The other conditions follow from the necessary conditions for the existence of a classic graph decomposition. The size of \( \Gamma \) must be a divisor of the size of the \( \lambda \)-fold of \( \mathbb{K}_\mathcal{P} \), which is equal to \( \lambda \left( \frac{[v]_q}{2} \right) \), and a trivial computation shows that \( \left( \frac{[v]_q}{2} \right) = \frac{1}{2} q [v]_q [v - 1]_q \). Finally, for \( P \in \mathcal{P} \) and \( B \in \mathcal{B} \), let \( \deg_B(P) \) be the degree of \( P \) in the graph \( B \). Then it is obvious that the sum \( \sum_{B \in \mathcal{B}} \deg_B(P) \) is the degree of \( P \) in \( \lambda \mathbb{K}_\mathcal{P} \), that is, \( \lambda ([v]_q - 1) = \lambda q [v - 1]_q \). Considering that each block is isomorphic to \( \Gamma \), it is clear that \( \deg_B(P) \) is a degree of a vertex of \( \Gamma \) for each \( B \), hence \( \lambda q [v - 1]_q \) is divisible by the greatest common divisor of the degrees of the vertices of \( \Gamma \). \( \square \)

Note that the third admissibility condition is empty in the case that the greatest common divisor of the degrees of the vertices of \( \Gamma \) is 1. In contrast, it is particularly important when \( \Gamma \) is regular. Indeed in this case condition (iii) can be more conveniently reformulated as follows.

(iii') If \( \Gamma \) is a regular graph of degree \( d \), then \( d \) must be a divisor of \( \lambda q [v - 1]_q \).

For instance, a nontrivial \( 2 - (7, \Gamma, 1) \) design over \( \mathbb{F}_2 \) with \( \Gamma = (V, E) \) connected, may exist only when the order and the size of \( \Gamma \) are as follows.
The size is in boldface only when $\Gamma$ might be regular, hence in the cases that $|V|$ divides $2|E|$. Note that $(|V|, |E|) = (7, 21)$ corresponds to the case that $\Gamma$ is complete, that is, equivalent to the 2-analog of a Fano plane, namely, to a $2-(7, 3, 1)_2$ design. There is a great deal of doubt on the existence of such a design; indeed it has been proved that if it exists, then its full automorphism group has order at most two \([6, 29, 35]\). The case $(|V|, |E|) = (7, 7)$ corresponds to a $2-(7, C_3, 1)_2$ design that will be constructed in Section 7. The case $(|V|, |E|) = (63, 63)$ corresponds to a $2-(7, C_6, 1)_6$ design that will be constructed in Section 10.1.

Now note that an $m n n \lambda(\Gamma)$-GDD is equivalent to a $K_k$-decomposition of $\lambda K_{mn}$. Thus, in particular, an $(mn, n, k, \lambda)_q$-GDD can be seen as a decomposition of the $[m]_q^n$-partite graph whose parts are the members of an $(n - 1)$-spread of $\text{PG}(\mathbb{F}_q^m)$ into $K_k$-subspaces of $\text{PG}(\mathbb{F}_q^m)$. These observations naturally lead to the following definitions.

**Definition 4.5.** Let $\Gamma$ be a simple graph. An $(mn, n, \Gamma, \lambda)$-GDD is a triple $(\mathcal{P}, \mathcal{G}, \mathcal{B})$ where $\mathcal{P}$ is a set of $mn$ points, $\mathcal{G}$ is a partition of $\mathcal{P}$ into $m$ classes of size $n$, and $\mathcal{B}$ is a collection of $\Gamma$-subgraphs (blocks) of $K_\mathcal{P}$ such that the two vertices of any edge of any block belong to distinct classes, and two points belonging to different classes are adjacent in exactly $\lambda$ blocks.

**Definition 4.6.** Let $\Gamma$ be a $q$-spaceable graph. An $(mn, n, \Gamma, \lambda)$-GDD over $E_q$ is an $([mn]_q, [n]_q, \Gamma, \lambda)$-GDD whose points are those of $\text{PG}(\mathbb{F}_q^m)$, whose classes are the members of an $(n - 1)$-spread, and whose blocks are $\Gamma$-subspaces of $\text{PG}(\mathbb{F}_q^m)$.

Here is a very elementary but useful composition construction.

**Proposition 4.7.** If there exist both an $(mn, n, \Gamma, \lambda)$-GDD over $E_q$ and a $2-(n, \Gamma, \lambda)$ design over $E_q$, then there exists a $2-(mn, \Gamma, \lambda)$ design over $E_q$.

**Proof:** Let $(\mathcal{P}, \mathcal{S}, \mathcal{B})$ be an $(mn, n, \Gamma, \lambda)$-GDD over $E_q$. Each $S \in \mathcal{S}$ is a $\text{PG}(\mathbb{F}_q^n)$ and then, by assumption, we can construct a $2-(n, \Gamma, \lambda)$ design over $E_q$, say $(S, B_S)$. It is then clear that $(\mathcal{P}, \mathcal{B} \cup \bigcup_{S \in \mathcal{S}} B_S)$ is the required $2-(mn, \Gamma, \lambda)$ design over $E_q$. \qed

We already commented that every spanning $2-([n]_q, \Gamma, \lambda)$ design can be seen as a $2-(n, \Gamma, \lambda)$ design over $E_q$. These designs, apparently uninteresting, could be crucial for the construction of some $2-(mn, \Gamma, \lambda)$ designs over $E_q$. Indeed, as an immediate consequence of the previous proposition we can state the following.

**Corollary 4.8.** If there exist an $(mn, n, \Gamma, \lambda)$-GDD over $E_q$ and a spanning $2-([n]_q, \Gamma, \lambda)$ design, then there exists a $2-(mn, \Gamma, \lambda)$ design over $E_q$. 

| $|V|$  | $|E|$  |
|-------|-------|
| 7     | 7, 9, 21 |
| 15    | 21, 63  |
| 31    | 63, 127, 381 |
| 63    | 63, 127, 381, 889, 1143 |
An automorphism of a 2-design \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \), possibly over a finite field, is a bijection \( \alpha : \mathcal{P} \rightarrow \mathcal{P} \) preserving \( \mathcal{B} \). Note that if \( \mathcal{D} \) is over a finite field, then \( \alpha \) necessarily maps subspaces into subspaces and therefore it necessarily belongs to the projective general linear group \( \text{PGL}_v(q) \). If \( \mathcal{D} \) is over a finite field, from what we have said above we have \( \text{Aut}(\mathcal{D}) \leq \text{PGL}_v(q) \leq \text{Sym}(\mathcal{P}) \). A 2-\((v, \Gamma, \lambda)\) design \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) is cyclic if \( \text{Aut}(\mathcal{D}) \) has a cyclic subgroup acting sharply transitively on \( \mathcal{P} \).

Using techniques based on automorphism groups of objects is not a novelty in the construction of combinatorial structures. We highlight a few of them used to construct designs over finite fields: the Kramer–Mesner method [5,8], the tactical-decomposition method [8,32], and the method of differences [18]. The last method will be used here to obtain some nontrivial cyclic graph decompositions over a finite field.

### 5.1 Difference families

**Definition 5.1.** Let \( G \) be a group of order \( v \) and let \( \Gamma \) be a simple graph. A \((v, \Gamma, \lambda)\) difference family in \( G \) is a collection \( \mathcal{F} \) of \( \Gamma \)-subgraphs of \( \mathbb{K}_G \) (base blocks) such that \( \Delta \mathcal{F} \) covers exactly \( \lambda \) times the set \( G^* \) of nonidentity elements of \( G \).

If \( \Gamma \) has size \( s \), then the list of differences of a \( \Gamma \)-subgraph of \( \mathbb{K}_G \) has size \( 2s \) and then it is evident that a necessary condition for the existence of a \((v, \Gamma, \lambda)\) difference family is that \( \lambda(v - 1) \) is divisible by \( 2s \). In the case that \( \Gamma \) is the complete graph \( \mathbb{K}_k \), one simply speaks of a \((v, k, \lambda)\) difference family in \( G \). If we speak of a \((v, \Gamma, \lambda)\) difference family or a \([v]_q, \Gamma, \lambda)\) difference family without specifying the group \( G \), it will be understood that \( G = \mathbb{Z}_v \) or \( G = [\mathbb{Z}_v]_q \), respectively.

The notion of a difference family is important in view of the following result that is very well known when \( \Gamma \) is complete (see, e.g., [1,3]). For a generic \( \Gamma \) one can see [16,17].

**Theorem 5.2.** If \( \mathcal{F} \) is a \((v, \Gamma, \lambda)\) difference family in \( G \), then the pair \((G, \text{dev} \mathcal{F})\) is a cyclic \( 2 - (v, \Gamma, \lambda) \) design.

The following definition is the \( q \)-analog of Definition 5.1.

**Definition 5.3.** Let \( q \) be a prime power and let \( \Gamma \) be a \( q \)-spaceable graph. A \((v, \Gamma, \lambda)\) difference family over \( \mathbb{F}_q \) is a \([v]_q, \Gamma, \lambda)\) difference family in which every base block is a \( \Gamma \)-subspace of \( \text{PG}(\mathbb{F}_q^v) \).

Consistently with Notation 4.3, speaking of a \((v, C_k, \lambda)\) \( q \) difference family we will mean a \((v, C_k[q], \lambda)\) difference family over \( \mathbb{F}_q \). In particular, \((v, k, \lambda)\) \( q \) difference family will mean \((v, \mathbb{K}_k, \lambda)\) difference family over \( \mathbb{F}_q \).

As a special case of Theorem 5.2 we can state the following.
Theorem 5.4. The development of a \((v, \Gamma, \lambda)\) difference family over \(\mathbb{F}_q\) is a \(2 - (v, \Gamma, \lambda)\) design over \(\mathbb{F}_q\).

The above theorem has been recently used in [18] to prove the existence of a cyclic \(2 - (v, 3, 7)\) design—that is, a \(2 - (v, \mathbb{K}_3, 7)\) design—for every odd \(v\). That was an improvement of [35] where the same result was obtained with a different approach and the additional hypothesis that \(v\) was not divisible by 3. We also recall that all the \(2 - (13, 3, 1)\) designs discovered in [4] are obtainable via \(2 - (13, 3, 1)_2\) difference families. We will revisit one of these difference families in Section 6.1.

5.2 Relative difference families

Here we consider an important variation of a \((v, \Gamma, \lambda)\) difference family, that is, the notion of a relative difference family.

If \(H\) is a subgroup of a group \(G\), we denote by \(\mathbb{K}_{G:H}\) the complete multipartite graph whose parts are the right cosets of \(H\) in \(G\).

Definition 5.5. Let \(H\) be a subgroup of order \(n\) of a group \(G\) of order \(mn\), and let \(\Gamma\) be a simple graph. An \((mn, n, \Gamma, \lambda)\) difference family in \(G\) and relative to \(H\) is a collection \(\mathcal{F}\) of \(\Gamma\)-subgraphs of \(\mathbb{K}_{G:H}\) such that \(\Delta \mathcal{F}\) covers \(G\setminus H\) exactly \(\lambda\) times.

Note that the list of differences of a difference family as above is clearly disjoint with \(H\). Thus, if \(\Gamma\) has size \(s\), then the obvious necessary condition for the existence of an \((mn, n, \Gamma, \lambda)\) difference family is that \(\lambda (m - 1)n\) is divisible by \(2s\). Of course, an \((mn, 1, \Gamma, \lambda)\) difference family relative to the trivial subgroup of \(G\) is nothing but an \((mn, \Gamma, \lambda)\) difference family in \(G\) as defined in Section 5.1.

Speaking of an \((mn, n, \Gamma, \lambda)\) difference family or an \(([mn]_q, [n]_q, \Gamma, \lambda)\) difference family without specifying the group \(G\) and the subgroup \(H\), it will be understood that \((G, H) = (\mathbb{Z}_{mn}, m\mathbb{Z}_{mn})\) in the former case, and that \((G, H) = ([mn]_q, [m\mathbb{Z}_{mn}]_q)\) in the latter.

The members of a relative difference family are called base blocks as for ordinary difference families. Here we are interested in relative difference families over finite fields.

Definition 5.6. Let \(q\) be a prime power and let \(\Gamma\) be a \(q\)-spaceable graph. An \((mn, n, \Gamma, \lambda)\) difference family over \(\mathbb{F}_q\) is an \(([mn]_q, [n]_q, \Gamma, \lambda)\) difference family whose base blocks are \(\Gamma\)-subspaces of \(\text{PG}(\mathbb{F}_q^{mn})\).

Consistently with Notation 4.3, speaking of an \((mn, n, C_k, \lambda)_q\) or an \((mn, n, P_k, \lambda)_q\) difference family, we will mean an \((mn, n, \Gamma, \lambda)\) difference family over \(\mathbb{F}_q\) where \(\Gamma\) is the cycle or the path of order \([k]_q\), respectively.

We have the following result.

Theorem 5.7. If \(\mathcal{F}\) is an \((mn, n, \Gamma, \lambda)\) difference family, then \(\text{dev} \mathcal{F}\) is a cyclic \((mn, n, \Gamma, \lambda)\)-GDD.

For the important case that \(\Gamma\) is complete see [10], for a general \(\Gamma\) see [13,15,17]. As a special case of the above theorem we can state the following.
The development of an \((mn, n, \Gamma, \lambda)\) difference family over \(\mathbb{F}_q\) is an \((mn, n, \Gamma, \lambda)\)-GDD over \(\mathbb{F}_q\).

The above theorem has been used in [18] to prove the existence of a cyclic \((3n, 3, 3, 7)\)₂-GDD—that is, a \((3n, 3, \mathbb{F}_7, 7)\) design over \(\mathbb{F}_2\)—for every odd \(n\).

As an immediate consequence of Theorem 5.8 and Corollary 4.8 we can state the following.

**Proposition 5.9.** If there exists an \((mn, n, \Gamma, \lambda)\) difference family over \(\mathbb{F}_q\) and a spanning \(2 - ([n]_q, \Gamma, \lambda)\) design, then there exists a \(2 - (mn, n, \Gamma, \lambda)\) design over \(\mathbb{F}_q\) which is cyclic if the spanning design has this property.

### 5.3 Use of Multipliers

Let \(\mathcal{F}\) be a difference family in a group \(G\) and let \(\alpha\) be an automorphism of \(G\). One says that \(\alpha\) is a **multiplier** of \(\mathcal{F}\) if it leaves \(\mathcal{F}\) invariant. Then the multipliers of \(\mathcal{F}\) clearly form a subgroup of the automorphism group of the design \(\mathcal{D}\) generated by \(\mathcal{F}\). Of course, it is not said that every automorphism of \(\mathcal{D}\) is a composition of a translation with a multiplier. Indeed the normalizer of the group of translations in the symmetric group on \(G\) may contain elements that are not multipliers.

Using a difference family \(\mathcal{F}\) in a group \(G\) to construct a design \(\mathcal{D}\) significantly reduces the number of blocks one needs to find. Yet, \(|\mathcal{F}|\) can be still quite “big,” hence the problem could appear to be hard anyway. So one could try to impose that \(\mathcal{F}\) has a big group \(A\) of multipliers with a “small” number of orbits (possibly one!) on \(\mathcal{F}\). In this case it is enough to give a set of **initial base blocks** for \(\mathcal{F}\), that is, a complete system \(S\) of representatives for the \(A\)-orbits on the base blocks of \(\mathcal{F}\); only one block, chosen arbitrarily, in each \(A\)-orbit on \(\mathcal{F}\).

In Section 10 we will see how the construction of some “difference graphs” (that are difference families with only one base block) is facilitated if one imposes a group of multipliers.

Most constructions for difference families in a group \(G\) have a group \(A\) of multipliers acting **semiregularly** on \(G^*\), that is, on \(G\) minus its identity element. This means that the nonidentity elements of \(A\) do not fix any element of \(G^*\). For instance, in [11] it is proved that there exists a **disjoint** \((v, k, k - 1)\) difference family in \(G\) whenever \(\text{Aut}(G)\) has a subgroup \(A\) of order \(k\) acting semiregularly on \(G^*\). The base blocks of this difference family \(\mathcal{F}\) are simply the \(A\)-orbits on \(G^*\), hence \(A\) is a group of multipliers of \(\mathcal{F}\) fixing every base block.

More frequently, the construction of an ordinary difference family \(\mathcal{F}\) in a group \(G\) can be realized by imposing a group \(A\) of multipliers acting semiregularly both on \(G^*\) and \(\mathcal{F}\). This strategy is often successful when \(G\) is elementary abelian, that is, the additive group of a finite field.

As far as we are aware, a formal description of how this strategy works in the general case is lacking. We give this description in the proof of the following theorem.

**Theorem 5.10.** Let \(\Gamma\) be a graph of size \(s\) and let \(G\) be a group of order \(v\) with \(\lambda(v - 1) = 2st\). Assume that \(A\) is a subgroup of \(\text{Aut}(G)\) of order a divisor \(d\) of \(\gcd(v - 1, t)\) acting semiregularly on \(G^*\). Also assume that \(\mathcal{I}\) is a \(\frac{s}{d}\)-collection of \(\Gamma\)-subgraphs of \(\mathbb{F}_q^d\) with \(\Delta\mathcal{I}\) evenly distributed over the \(\frac{s - 1}{d}\) orbits of \(A\) on \(G^d\). Then \(\mathcal{I}\) is a collection of initial base blocks of a \((v, \Gamma, \lambda)\) difference family in \(G\).

**Proof.** Set \(\mathcal{F} = \{B^\alpha | B \in \mathcal{I}, \alpha \in A\}\). We have \(\Delta B^\alpha = \{x^\alpha | x \in \Delta B\}\) for every pair \((B, \alpha) \in \mathcal{I} \times A\) and then \(\Delta \mathcal{F} = \{x^\alpha | x \in \Delta \mathcal{I}, \alpha \in A\}\). We have \(|\Delta \mathcal{I}| = 2s|\mathcal{I}| = \frac{2st}{d} = \lambda \frac{v - 1}{d}\).
and then $\Delta I$ has exactly $\lambda$ elements in each $A$-orbit on $G^*$ by our assumption that $\Delta I$ is evenly distributed over the orbits of $A$. This means that $\Delta I$ is the multiset sum of $\lambda$ complete systems of representatives for the $A$-orbits on $G^*$, say $S_1, ..., S_\lambda$. Thus we can write

$$\Delta F = \bigcup_{i=1}^{\lambda} \bigcup_{x \in S_i} \{x^\alpha | \alpha \in A\}.$$  

Let $\text{Stab}(x)$ and $\text{Orb}(x)$ be the stabilizer and the orbit of $x$ under the action of $A$. Then \(\{x^\alpha | \alpha \in A\}\) is the multiset sum of $\frac{|A|}{|\text{Stab}(x)|}$ copies of $\text{Orb}(x)$. On the other hand $A$ acts semiregularly on $G^*$ by assumption, hence $\text{Stab}(x)$ is always trivial and then \(\{x^\alpha | \alpha \in A\} = \text{Orb}(x)\) for every $x \in S_i$. Thus we have $\bigcup_{x \in S_i} \{x^\alpha | \alpha \in A\} = G^*$ for $1 \leq i \leq \lambda$ and we conclude that $\Delta F$ is the multiset sum of $\lambda$ copies of $G^*$, that is, $F$ is a $(v, \Gamma, \lambda)$ difference family in $G$. The assertion follows.

Assume, for instance, that $q = k(k-1)t + 1$ is a prime power and that we want to find a $(q, k, 1)$ difference family in the elementary abelian group $EA(q)$, that is, the additive group of $\mathbb{F}_q$. Thus we want a $(q, \Gamma, 1)$ difference family in $EA(q)$ where $\Gamma = \mathbb{K}_k$ has size $s = \frac{k(k-1)}{2}$. Let $C$ be the subgroup of $t$-th roots of unity of $\mathbb{F}_q^*$ and set $A = \{\alpha_c | c \in C\}$ where $\alpha_c$ is the automorphism of $EA(q)$ defined by $\alpha_c(x) = cx$ for every $x \in \mathbb{F}_q$. It is obvious that $A$ is a group of automorphisms of $EA(q)$ isomorphic to $C$ that acts semiregularly on $\mathbb{F}_q^*$ and that the $A$-orbits on $\mathbb{F}_q^*$ are the $k(k-1)$ cosets of $C$ in $\mathbb{F}_q^*$. Thus, if we find a $k$-subset $B$ of $\mathbb{F}_q$ such that $\Delta B$ has exactly one element in each of these cosets, then a set $I$ of initial base blocks for the required family is the singleton $\{B\}$ by Theorem 5.10. This is the famous “Wilson’s lemma on evenly distributed differences” [37]. At first sight one could think that to find such a set $B$ is almost a miracle but, as proved by Wilson himself, this strategy always succeeds whenever $v$ is sufficiently large (see also [17]).

It is easy to see that Theorem 5.10 can be generalized to the following.

**Theorem 5.11.** Let $\Gamma$ be a graph of size $s$, let $G$ be a group of order $mn$ with $\lambda(m-1)n = 2st$, and let $H$ be a subgroup of $G$ of order $n$. Assume that $A$ is a subgroup of $\text{Aut}(G)$ of order $d$ dividing $\gcd(mn-n, t)$ acting semiregularly on $G \setminus H$. Also assume that $I$ is a $\frac{1}{d}$-collection of $\Gamma$-subgraphs of $\mathbb{K}_{G:H}$ with $\Delta I$ evenly distributed over the $\frac{(m-1)n}{d}$ orbits of $A$ on $G \setminus H$. Then $I$ is a collection of initial base blocks of a $(mn, n, \Gamma, \lambda)$ difference family in $G$ relative to $H$.

The above two theorems can be reformulated—mutatis mutandis—almost in the same way for difference families over a finite field but now there is a very big “handicap”; indeed in this case the subgroup $A$ of $\text{Aut}([Z_v]_q)$ cannot be arbitrary since it must map subspaces into subspaces. This may happen only if $A$ is a subgroup of the (unfortunately quite “small”) group

$$\text{Frob}([Z_v]_q) = \{\phi^i | 0 \leq i \leq v - 1\},$$

where $\phi$ is the Frobenius automorphism defined by $\phi(x) = x^q$ for every $x \in [Z_v]_q$.

A further inconvenience is that $\text{Frob}([Z_v]_q)$ may not have any subgroup acting semiregularly on the complement of the subgroup $H$ of $[Z_v]_q$ that one needs. Let us examine, for instance, what happens in the case that $H = \{1\}$. 

Proposition 5.12. Frob([Z_v]_q) has a nontrivial subgroup acting semiregularly on [Z_v]_q \{1\} if and only if v is a prime and q \neq 1(\mod v).

Proof. Let F be the group of units of Z_{[v]}_q that is the image of Frob([Z_v]_q) under the natural isomorphism between [Z_v]_q and Z_{[v]}_q, hence F = \{q^i\mid 0 \leq i \leq v - 1\}. We have to show, equivalently, that F has a subgroup A acting semiregularly on Z_{[v]}_q \{0\} if and only if v is a prime and q \neq 1(\mod v).

(\Rightarrow). Given that F is the cyclic group of order v generated by q, we have A = \langle q^d \rangle for some divisor d of v. We have q^d \cdot q^\frac{v-1}{d} = (q^v - 1) + q^\frac{v-1}{d} \equiv q^\frac{v-1}{d} \equiv 0(\mod [v]_q), hence q^\frac{v-1}{d} is fixed by A. It necessarily follows that q^\frac{v-1}{d} \equiv 0(\mod [v]_q) and this is possible only for d = 1. Thus A = \langle q \rangle, that is, A is necessarily the whole F. This fact naturally implies that F has prime order. Indeed, in the opposite case, any proper subgroup of F would also act semiregularly on Z_{[v]}_q \{0\}.

The F-orbits on Z_{[v]}_q \{0\} have all size v, hence we have [v]_q - 1 \equiv 0(\mod v). This gives \sum_{i=1}^{v-1} q^i \equiv 0(\mod v) and then q \equiv 1(\mod v) otherwise we would have v - 1 \equiv 0(\mod v) which is absurd.

(\Leftarrow). Let d = \gcd(q - 1, [v]_q) so that we have q \equiv 1(\mod d) and [v]_q \equiv 0(\mod d). Hence we can write [v]_q = \sum_{i=0}^{d-1} q^i \equiv v(\mod d). We deduce that v \equiv 0(\mod d). Thus, given that v is a prime, we have either d = v or 1. The former case cannot happen since q \equiv 1(\mod v) by assumption. We conclude that gcd(q - 1, [v]_q) = 1. Now assume that there is an element x \in Z_{[v]}_q whose F-stabilizer Stab(x) is not trivial. Then, considering that F has prime order, we necessarily have Stab(x) = F. This implies, in particular, that qx \equiv x(\mod [v]_q) so that (q - 1)x is divisible by [v]_q. Thus, recalling that [v]_q and q - 1 are coprime, [v]_q is a divisor of x, that means that x is the zero element of Z_{[v]}_q. We conclude that F acts semiregularly on all elements of Z_{[v]}_q \{0\}.

In view of the above proposition, the “q-analog” of Theorem 5.10 should be more conveniently stated as follows.

Theorem 5.13. Let v be a prime and let \Gamma be a q-spaceable graph of size s with \lambda([v]_q - 1) = 2st. Assume that v divides t and that \mathcal{I} is a \lambda\{-\}\collection of \Gamma\{-\}\subspaces of PG(F_q^s) with \Delta\mathcal{I} evenly distributed over the \frac{[v]_q - 1}{\gcd(v, q - 1)} orbits of Frob([Z_v]_q) on [Z_v]_q^{\ast q}. Then \mathcal{I} is a collection of initial base blocks of a (v, \Gamma, \lambda) difference family over F_q.

The shortage of multipliers is one of the main reasons why constructing difference families over a finite field is in general a very hard task. The search for difference families in a group G could be enormously facilitated by the use of the automorphisms of G to the point that, in some cases, it is enough to find only an initial base block for them. On the other hand, for a difference family \mathcal{F} over a finite field the number of automorphisms that one can use is very small compared with the size of \mathcal{F} and hence, in general, one needs a huge number of initial base blocks anyway.

5.4 An example of a (7, Q^*, 1) difference family over F_2

Let us show a concrete example where Theorem 5.13 can be applied. Other examples will be given in the next sections.
Let $Q^*_3$ be the cube $Q_3$ with one vertex deleted and let us construct a cyclic $2 - (7, Q^*_3, 1)$ design over $\mathbb{F}_2$. By Theorem 5.4, it is enough to exhibit a $(7, Q^*_3, 1)$ difference family over $\mathbb{F}_2$. Note that $Q^*_3$ has size $s = 9$ and that we have $[7]_2 - 1 = 126 = 2st$ with $t = 7$. Thus, by Theorem 5.13 we need only one initial $Q^*_3$-plane $B$ of $\mathbb{P}^G_7$ with the property that its list of differences has exactly one element in each orbit of $\text{Frob}([\mathbb{Z}_7]_2^*)$ on $[\mathbb{Z}_7]^*\mathbb{Z}_2^*$. 

Let us take a root $g$ of the polynomial $x^7 + x + 1$ as generator of $[\mathbb{Z}_7]_2$ and consider the natural isomorphism $f$ between $[\mathbb{Z}_7]_2$ and $\mathbb{Z}_{127}$ mapping $g$ into 1. Note that $p = 127$ is a prime and that the image under $f$ of the orbits of $\text{Frob}([\mathbb{Z}_7]_2)$ on $[\mathbb{Z}_7]_2^*$ are the cosets of the group $\{2^i | 0 \leq i \leq 6\}$ of the seventh roots of unity in $\mathbb{Z}_p^*$, that is, the cyclotomic classes of order 18. Also note that $f$ maps the list of differences of $B$ into the list of differences of $f(B)$. Thus a $Q^*_3$-plane $B$ satisfies our requirement provided that the list of differences of $B' := f(B)$ has exactly one element in each cyclotomic class of order 18. Let $r$ denote a primitive element of $\mathbb{Z}_p$. It is a standard exercise to verify that this means that the logarithmic map

$$\text{Log}: r^i \in \mathbb{Z}_p^* \mapsto i \in \mathbb{Z}_{18}$$

is bijective on $\Delta B'$. Then our strategy to find the $Q^*_3$-plane $B$ is the following:

(i) Find a plane $\pi$ of $\mathbb{P}G_7$ such that the list of differences of $f(\pi)$ intersects each cyclotomic class of order 18 in at least one element or, equivalently, in such a way that the map $\text{Log}$ is surjective on $\Delta f(\pi)$.

(ii) Construct a copy $B'$ of $Q^*_3$ with vertex set $f(\pi)$ in such a way that the map $\text{Log}$ is injective on $\Delta B'$.

Consider the plane $\pi = \langle 1, g^2, g^5 \rangle$ generated by the three points $1 = g^0$, $g^2$, and $g^5$. Taking into account of the algebraic rule $g^7 = g + 1$, one can easily check that for the remaining points of $\pi$, that are $g^2 + 1$, $g^5 + 1$, $g^5 + g^2$, and $g^5 + g^2 + 1$, we have

$$g^2 + 1 = g^{14}, \quad g^5 + 1 = g^{54}, \quad g^5 + g^2 = g^{65}, \quad g^5 + g^2 + 1 = g^{95}.$$ 

Thus $f(\pi) = \{0, 2, 5, 14, 54, 65, 95\}$. The difference table of $f(\pi)$ is the following:

|   | 0  | 2  | 5  | 14 | 54 | 65 | 95 |
|---|----|----|----|----|----|----|----|
| 0 | 125| 122| 113| 73 | 62 | 32 |
| 2 | 2  | 124| 115| 75 | 64 | 34 |
| 5 | 3  | 118| 78 | 67 | 37 |
| 14| 14 | 12 | 87 | 76 | 46 |
| 54| 54 | 52 | 49 | 40 | 116| 86 |
| 65| 65 | 63 | 60 | 51 | 11 | 97 |
| 95| 95 | 93 | 90 | 81 | 41 | 30 |

Choosing $r = 3$ as a primitive element of $\mathbb{Z}_p$, one can see that the image of the above table under the map Log is
and then that condition (i) is satisfied; indeed each element of $\mathbb{Z}_{18}$ appears at least once in the entries of the above table. Now we have to label the vertices of the abstract graph $Q_3^*$ with the points of $f(\pi)$ to get a graph $B'$ satisfying (ii). We claim that such a graph $B'$ is, for instance, the following.

![Graph Image]

This is clearly recognizable looking at the image under Log of the difference table of $B'$, that is, the following.

And then that condition (i) is satisfied; indeed each element of $\mathbb{Z}_{18}$ appears at least once in the entries of the above table. Now we have to label the vertices of the abstract graph $Q_3^*$ with the points of $f(\pi)$ to get a graph $B'$ satisfying (ii). We claim that such a graph $B'$ is, for instance, the following.

![Graph Image]

This is clearly recognizable looking at the image under Log of the difference table of $B'$, that is, the following.

|   | 0 | 2 | 5 | 14 | 54 | 65 | 95 |
|---|---|---|---|----|----|----|----|
| 0 |  9 | 6 | 16 | 12 | 10 |  0 |    |
| 2 |   0 | 10 | 10 | 13 |  0 |  2 |    |
| 5 |  15 |  1 | 11 |  5 |  7 |  8 |    |
| 14 |  7 |  1 |  2 |  6 | 12 | 13 |    |
| 54 |  3 |  4 | 14 | 15 |  5 | 17 |    |
| 65 |  1 |  9 | 16 |  3 | 14 |  7 |    |
| 95 |  9 | 11 | 17 |  4 |  8 | 16 |    |

6 | STEINER 2-DESIGNS OVER FINITE FIELDS

A $2 - (v, k, \lambda)$ design is said to be a Steiner 2-design when $\lambda = 1$. In this section we will discuss Steiner 2-designs over $\mathbb{F}_q$, namely, $2 - (v, k, 1)_q$ designs or also $2 - (v, k_k, 1)_q$ designs. It has already been observed that a $2 - (v, 3, 1)_q$ design possibly exists only if $v \equiv 1$ or 3 (mod 6) (see, e.g., [6]). As far as we are aware, nobody noticed that, much more generally, the trivial
admissibility conditions for the existence of a $2 - (v, k, 1)_q$ design can be stated in the following very convenient and simple way.

**Theorem 6.1.** A $2 - (v, k, 1)_q$ design exists only if $v \equiv 1 \text{ or } k \pmod{k(k-1)}$.

This is as immediate consequence of the following more general fact.

**Proposition 6.2.** A classic $2 - (q^r - 1, q^k - 1, 1)_q$ design exists only if $v \equiv 1 \text{ or } k \pmod{k(k-1)}$.

Proof. First recall that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ and therefore that $\gcd\left(\frac{a^m - 1}{a - 1}, \frac{a^n - 1}{a - 1}\right) = a^{\gcd(m,n) - 1}$ for every triple of positive integers $(a, m, n)$ with $a > 1$. This is a standard exercise of elementary number theory (see, e.g., [33, Example 245, p. 36]). Specializing this to the case that $a$ is a prime power, we can say that

$$\gcd([m]_q, [n]_q) = [\gcd(m, n)]_q$$  \hspace{1cm} (1)

for every prime power $q$ and every pair $(m, n)$ of positive integers. This fact implies, in particular, that

$$[m]_q \text{ divides } [n]_q \iff m \text{ divides } n.$$  \hspace{1cm} (2)

Indeed $[m]_q$ is a divisor of $[n]_q$ if and only if $\gcd([m]_q, [n]_q) = [m]_q$ which, by (1), is equivalent to say that $[\gcd(m, n)]_q = [m]_q$. Hence $[m]_q$ is a divisor of $[n]_q$ iff $\gcd(m, n) = m$, that is, iff $m$ is a divisor of $n$.

Now assume that a $2 - ([v]_q, [k]_q, 1)$ design exists. Here the divisibility conditions give

$$\frac{v-1}{k-1} \in \mathbb{N} \text{ and } \frac{[v]_q[v-1]_q}{[k]_q[k-1]_q} \in \mathbb{N}.$$  \hspace{1cm} (3)

By (2) and the first condition above, $k - 1$ must be a divisor of $v - 1$, that is, $v \equiv 1 \pmod{k-1}$.

By (1) we have $\gcd([v]_q, [v-1]_q) = [\gcd(v, v-1)]_q = [1]_q = 1$, that is, $[v]_q$ and $[v-1]_q$ are relatively prime. Thus, given that $[k]_q$ is a divisor of their product by the second condition in (3), $[k]_q$ is the product of $\gcd([k]_q, [v]_q)$ and $\gcd([k]_q, [v-1]_q)$. It follows, by (1), that $[k]_q = [g]_q \cdot [g']_q$ where $g = \gcd(k, v)$ and $g' = \gcd(k, v-1)$. Thus we can write

$$(q-1)(q^k - 1) = (q^g - 1)(q^{g'} - 1).$$  \hspace{1cm} (4)

If $g \leq g'$, reducing (4) modulo $q^g$ we get $q \equiv 0 \pmod{q^g}$ which implies $g = 1$ and hence $g' = k$, that is, $k$ divides $v - 1$. If $g \geq g'$, reducing (4) modulo $q^{g'}$ we get $q \equiv 0 \pmod{q^{g'}}$ which implies $g' = 1$ and hence $g = k$, that is, $k$ divides $v$. Thus we have $v \equiv 0$ or 1
Recalling that \( v \equiv 1 \pmod{k} \), we necessarily conclude that \( v \equiv 1 \) or \( k \pmod{k(k-1)} \) and the assertion follows.

The following result is elementary and can be considered folklore. Already in 1987, Mathon [31] introduced it (end of p. 353), without a proof, saying “An orbit analysis of a cyclic Steiner \( C(v, k, 1) \) yields the following existence condition ....”.

**Proposition 6.3.** A cyclic \( 2 - (v, k, 1) \) design may exist only for \( v \equiv 1 \) or \( k \pmod{k(k-1)} \). The block set of such a design is the development of a \( (v, k, 1) \) difference family when \( v \equiv 1 \pmod{k(k-1)} \) or the development of a \( (v, k, k, 1) \) difference family plus the cosets of \( \frac{v}{k} \mathbb{Z}_v \) in \( \mathbb{Z}_v \) when \( v \equiv k \pmod{k(k-1)} \).

By Theorem 6.1 and Proposition 6.3 the necessary conditions for the existence of a \( 2 - (v, k, 1)_q \) design exactly coincide with the necessary conditions for the existence of a cyclic classic \( 2 - (v, k, 1)_q \) design. Thus, if \( k \) is not a prime power, the “\( 2 - (v, k, 1)_q \) admissibility conditions” are much more strict than the “\( 2 - (v, k, 1) \) admissibility conditions.” Consider, for instance, the case \( k = 6 \). The admissible values of \( v \) for a classic \( 2 - (v, 6, 1) \) design are those congruent to 1, 6, 16, or 21 (mod 30). On the other hand the admissible values of \( v \) for a \( 2 - (v, 6, 1)_q \) design are only those congruent to 1 or 6 (mod 30).

Now note that \( v \equiv 1 \) or \( k \pmod{k(k-1)} \) implies that \([v]_q \equiv 1 \) or \([k]_q \) (mod \( [k]_q([k]_q - 1) \)), respectively. Thus, by Theorem 6.1 and Proposition 6.3 again, it makes sense to try establishing the existence of a \( 2 - (v, k, 1)_q \) design by searching for a cyclic example. Also, improving Theorem 7 in [4], we can state the following.

**Theorem 6.4.** There exists a cyclic \( 2 - (v, k, 1)_q \) design if and only if there exists a \( (v, r, k, 1)_q \) difference family where \( r \) is the remainder of the Euclidean division of \( v \) by \( k(k-1) \).

A trivial counting shows that the size a difference family \( \mathcal{F} \) as in the above theorem is

\[
|\mathcal{F}| = \begin{cases} 
\frac{(q - 1)(q^{v-1} - 1)}{(q^k - 1)(q^{k-1} - 1)} & \text{if } v \equiv 1 \pmod{k(k-1)}, \\
\frac{q^{k-1}(q - 1)(q^{v-k} - 1)}{(q^k - 1)(q^{k-1} - 1)} & \text{if } v \equiv k \pmod{k(k-1)}. 
\end{cases}
\]

It is clear that this size is quite “big” even for very “small” values of the parameters \( v, k, \) and \( q \). Thus, it would be convenient to use multipliers, when this is possible. Specializing Theorem 5.13 to a \( 2 - (k(k-1)t + 1, k, 1)_q \) design (hence \( \Gamma = \mathbb{K}_k \) and \( \lambda = 1 \)) we get the following.

**Theorem 6.5.** Let \( v \equiv 1 \pmod{k(k-1)} \) be a prime. Assume that \( \frac{[v]_{k-1} - 1}{[k]_q[k-1]_q} = uv \) for some integer \( u \) and that \( q \not\equiv 1 \pmod{v} \). If \( \mathcal{I} \) is a \( u \)-set of \((k-1)\)-dimensional subspaces of \( PG(\mathbb{F}_q^v) \) with \( \Delta \mathcal{I} \) evenly distributed over the \( \frac{[v]_{k-1} - 1}{v} \) orbits of \( \text{Frob}[\mathbb{Z}_v]_q \) on \( [\mathbb{Z}_v]_q^* \), then \( \mathcal{I} \) is a collection of initial base blocks of a \( (v, k, 1)_q \) difference family.
6.1 Revisiting the $2 - (13, 3, 1)_2$ design

The longstanding conjecture that there is no nontrivial $2 - (v, k, 1)_q$ design was disproved in [4] where over 400 nonisomorphic cyclic $2 - (13, 3, 1)_2$ designs have been constructed. Given that they are cyclic, each of them can be obtained by means of a suitable $(13, 3, 1)_2$ difference family. Here we revisit the solution presented in [4] giving some more details. Our purpose is to make the reader able to check its correctness almost by hand and, above all, we want to emphasize how multipliers are crucial for its achievement.

Let us take a root $g$ of the polynomial $x^{13} + x^{12} + x^{10} + x^9 + 1$ as generator of $\mathbb{Z}_{13}[2]$ and let us consider the natural isomorphism $f : g^i \in [\mathbb{Z}_{13}]_2 \longrightarrow i \in \mathbb{Z}_{2^{13} - 1}$. Note that $p = [13]_2 = 2^{13} - 1 = 8191$ is a prime so that it makes sense to speak of a primitive root (mod $p$). Such a primitive root is, for instance, $r = 17$.

Let us use Theorem 6.5 with $v = 13$, $k = 3$, and $q = 2$. We have $\frac{v - 1}{k} = \frac{2^{12} - 1}{7 \cdot 3} = 195 = 15v$. Thus the required difference family could be realized by means of a $15$-set $I$ of initial planes of $PG(\mathbb{F}_{2}^{13})$ with the property that $\Delta I$ has exactly one element in each orbit of $Frob(\mathbb{Z}_{2}^{*})$ on $[\mathbb{Z}_{13}]^*_2$. Note that the images of these orbits under the isomorphism $f$ are the cosets of $\{2^i | 0 \leq i \leq 12\}$, that is, the group of 13th roots of unity, in $\mathbb{Z}^*_p$. Equivalently, they are the cyclotomic classes of order $p - 1 = 630$. Reasoning as in Section 5.4 we conclude that $I = \{B_1, ..., B_{13}\}$ is the required set of initial planes provided that the logarithmic map

$$Log : 17^i \in \mathbb{Z}^*_p \longrightarrow i \in \mathbb{Z}_{630}$$

is bijective on $S := \bigcup_{i=1}^{15} \Delta f(B_i)$. That said, the required set of initial planes is the one consisting of the preimages under $f$ of the following subsets of $\mathbb{Z}_p$.

$$B_1' = \{0, 1, 1249, 7258, 8105, 5040, 7978\},$$
$$B_2' = \{0, 7, 1857, 6681, 7259, 7381, 7908\},$$
$$B_3' = \{0, 9, 1144, 7714, 1945, 8102, 6771\},$$
$$B_4' = \{0, 11, 209, 1941, 3565, 6579, 2926\},$$
$$B_5' = \{0, 12, 2181, 3696, 6673, 6965, 2519\},$$
$$B_6' = \{0, 13, 4821, 8110, 8052, 5178, 7823\},$$
$$B_7' = \{0, 17, 291, 5132, 1199, 8057, 6266\},$$
$$B_8' = \{0, 20, 1075, 3996, 7313, 4776, 3939\},$$
$$B_9' = \{0, 21, 2900, 6087, 4915, 4226, 8008\},$$
$$B_{10}' = \{0, 27, 1190, 3572, 6710, 4989, 5199\},$$
$$B_{11}' = \{0, 30, 141, 682, 6256, 6406, 2024\},$$
$$B_{12}' = \{0, 31, 814, 1243, 4434, 1161, 6254\},$$
$$B_{13}' = \{0, 37, 258, 5396, 6469, 2093, 4703\},$$
$$B_{14}' = \{0, 115, 949, 1272, 4539, 4873, 1580\},$$
$$B_{15}' = \{0, 119, 490, 6670, 6812, 7312, 5941\}.$$

The reader who wants to check this concretely has to make the following three steps.
First of all one needs to ensure that the preimages of the $B_i$'s are actually planes. To facilitate this task each $B_i'$ has been ordered—differently from [4] where the order is increasing—in the form $B_i' = \{0, b_{1i}, ..., b_{16i}\}$ in such a way that

$$
g_{b_{13}} = g_{b_{11}} + 1, \quad g_{b_{14}} = g_{b_{12}} + 1, \quad g_{b_{15}} = g_{b_{11}} + g_{b_{12}}, \quad g_{b_{16}} = g_{b_{11}} + g_{b_{12}} + 1.
$$

This can be easily verified by using the identity $g^{13} = g^{12} + g^{10} + g^{9} + 1$. Hence $B_i := f^{-1}(B_i')$ is the plane $\langle 1, g_{b_{11}}, g_{b_{12}} \rangle$ generated by the three points 1, $g_{b_{11}}$, and $g_{b_{12}}$.

Then one has to calculate $\text{Log}(\Delta B_i')$ for each $i$. Here is, for instance, the image under Log of the difference table of $B_1'$.

|     | 0   | 1   | 1249 | 7258 | 8105 | 5040 | 7978 |
|-----|-----|-----|------|------|------|------|------|
| 0   | 315 | 376 | 460  | 543  | 230  | 325  |
| 1   | 0   | 454 | 547  | 203  | 94   | 540  |
| 1249| 61  | 139 | 10   | 10   | 328  | 344  |
| 7258| 145 | 232 | 580  | 478  | 100  | 105  |
| 8105| 28  | 518 | 603  | 163  | 5    | 548  |
| 5040| 545 | 409 | 13   | 415  | 320  | 308  |
| 7978| 10  | 225 | 29   | 420  | 233  | 623  |

Finally, one has to check that the “miracle” happens: the union of these images covers all $\mathbb{Z}_{630}$.

The success of the above construction actually looks like a miracle. It is even more amazing that, in the same way, more than 400 pairwise nonisomorphic $2 - (13, 3, 1)_2$ designs have been obtained. This fact seems to suggest that there is a “magic” combinatorial structure on $2^{13} - 1 = 8191$ points hidden behind these designs. Thus, given that $8191 = 90^2 + 90 + 1$, we hazard the outrageous conjecture that there exists a projective plane of order 90.

### 6.2 Searching for other cyclic $2 - (v, k, 1)_q$ designs

The existence problem for Steiner 2-designs over $\mathbb{F}_q$ is very hard. For the time being, the only theoretical tool available to get them is the method of differences that requires the construction of a (relative) difference family whose size is almost always quite big. The possible existence of multipliers does not help so much since the number of initial base blocks usually remains too big. Let us show, for instance, what happens if we want to find the $q$-analog of a Fano plane that is a $2 - (7, 3, 1)_q$ design. In the following table we give the size of a putative $2 - (7, 3, 1)_q$ difference family $\mathcal{F}$ and the minimal size of a set $\mathcal{I}$ of initial base blocks for $\mathcal{F}$ for each prime power $q \leq 19$.

| $q$ | 2  | 3  | 4  | 5  | 7  | 9  | 11 | 13 | 16 | 17 | 19 |
|-----|----|----|----|----|----|----|----|----|----|----|----|
| $|\mathcal{F}|/|\mathcal{I}|$ | 3  | ?  | 13 | 21 | 43 | 73 | 111| 157| 241| 273| 343|
| $\mathcal{I}$ | N  | N  | ?  | N  | ?  | ?  | ?  | ?  | ?  | N  | ?  |
| $|\mathcal{F}|$ | 3  | ?  | 13 | 21 | 43 | 73 | 111| 157| 241| 273| 343|
If the cell \( (|\mathcal{F}|, q) \) contains two numbers \( f_i \) it means that \( f \) is the size of \( \mathcal{F} \) and that \( i \) is the number of initial base blocks for \( \mathcal{F} \) in the putative case that it admits a group of multipliers. If the cell \( (|\mathcal{F}|, q) \) contains only one number \( f \) it means that \( \mathcal{F} \) has size \( f \) and cannot have a nontrivial group of multipliers.

In the line labeled “∃” we put “N” or “?” according to whether the nonexistence has been checked by computer (see [4] for the cases \( q \in \{2, 3, 5\} \)) or it is still undecided, respectively. Note that we have checked by computer that a putative \( 2 - (7, 3, 1)_{17} \) difference family does not have nontrivial multipliers even though, a priori, it may have \( \text{Frob}[\mathbb{Z}_{17}] \) as a group of multipliers.

For \( (v, k) \neq (7, 3) \) the situation becomes even worse. We first recall that an exhaustive computer search [4] excluded the existence of cyclic \((9, 3, 1)_2\) and \((13, 4, 1)_2\) designs. In the following table we report the size of a putative \((v, r, k, 1)_q\) difference family \( \mathcal{F} \) and the size of a minimal set \( \mathcal{I} \) of initial base blocks for \( \mathcal{F} \). It is impressive how these numbers almost immediately “explode.” When the cell corresponding to \( \mathcal{I} \) is empty it will mean that \( \mathcal{F} \) cannot have nontrivial multipliers.

\[
\begin{array}{|c|c|c|c|c|}
\hline
v & k & q & |\mathcal{F}| & |\mathcal{I}| \\
\hline
13 & 3 & 2 & 195 & 15 \\
15 & 3 & 2 & 780 & 260 \\
19 & 3 & 2 & 12483 & 657 \\
21 & 3 & 2 & 49932 & 16644 \\
13 & 3 & 3 & 5110 & \\
19 & 3 & 3 & 3725197 & 196063 \\
21 & 3 & 3 & 33526773 & 111755591 \\
25 & 3 & 3 & 2715668620 & \\
\hline
\end{array}
\]

\[
\begin{array}{|c|c|c|c|c|}
\hline
v & k & q & |\mathcal{F}| & |\mathcal{I}| \\
\hline
16 & 4 & 2 & 312 & \\
25 & 4 & 2 & 159783 & \\
28 & 4 & 2 & 1278264 & 319566 \\
13 & 4 & 3 & 511 & \\
16 & 4 & 3 & 13797 & \\
25 & 4 & 3 & 271666862 & \\
28 & 4 & 3 & 7332305274 & \\
37 & 4 & 3 & > 10^{15} & > 10^{13} \\
\hline
\end{array}
\]

### 7 | CYCLE DECOMPOSITIONS OVER FINITE FIELDS

The admissibility conditions for the existence of a cycle decomposition over a finite field are the following.

**Proposition 7.1.** A \( 2 - (v, C_k, 1)_q \)-design with \( q \) even possibly exists only for \( v \equiv 0 \) or \( 1(\text{mod } k) \). A \( 2 - (v, C_k, 1)_q \)-design with \( q \) odd and \( k \) even possibly exists only for \( v \equiv 1(\text{mod } k) \). A \( 2 - (v, C_k, 1)_q \)-design with both \( q \) and \( k \) odd possibly exists only for \( v \equiv 1 \) or \( k \equiv 0(\text{mod } 2k) \).

**Proof.** Here conditions (iii) and (iv) of Proposition 4.4 are

\[
q [v]_q [v - 1]_q \equiv 0 \pmod{2[k]_q} \quad \text{and} \quad q [v - 1]_q \equiv 0 \pmod{2}.
\]  

From the first congruence \([k]_q \) must be a divisor of \([v]_q [v - 1]_q \) and then, reasoning as in the proof of Proposition 4, we get \( v \equiv 0 \) or \( 1 \pmod{k} \). If \( q \) is odd, the second congruence
gives $\sum_{i=0}^{v-2} q^i \equiv 0 \pmod{2}$ and then $v - 1 \equiv 0 \pmod{2}$, that is, $v$ is odd. The assertion easily follows. \hfill \square

As a consequence of the above proposition, one can try to construct every putative $2 - (v, C_k, 1)_q$ design as follows.

**Case** $v \equiv 1 \pmod{k}$, say $v = kt + 1$.

Find a collection $S$ of $\binom{q}{2}[t]_q$ subspaces of $\PG(F_q^v)$ of dimension $k - 1$ whose lists of differences cover, all together, every nonidentity element of $[Z_v]_q$ at least once.

Arrange the points of each $S \in S$ into a $[k]_q$-cycle $C_S$ in such a way that $F := \{C_S | S \in S\}$ is a $(v, C_k, 1)_q$ difference family. The development of $F$ is the desired $2 - (v, C_k, 1)_q$ design by Theorem 5.4.

**Case** $v \equiv 0 \pmod{k}$, say $v = kt$.

Find a collection $S$ of $\binom{q}{2}[t - 1]_q$ subspaces of $\PG(F_q^v)$ of dimension $k - 1$ such that $\Delta S$ covers every element of $[Z_v]_q \setminus [tZ_v]_q$ at least once.

Arrange the points of each $S \in S$ into a $[k]_q$-cycle $C_S$ in such a way that $F := \{C_S | S \in S\}$ is a $(v, k, C_k, 1)_q$ difference family. At this point, let us recall that for every odd integer $u \geq 3$ there exists a Hamiltonian cycle system of order $u$, that is, a $2 - (u, C_u, 1)$ design (see, e.g., [12]). Thus, in particular, there exists a spanning $([k]_q, C_{[k]_q}, 1)$ design over $F_q$ and the existence of the desired $2 - (v, C_k, 1)_q$ design follows from Proposition 5.9.

Let us see how the above strategy is successful to find a $2 - (v, C_3, 1)_2$ design for $v = 6, 7, 9$.

**A cyclic $2 - (7, C_3, 1)_2$ design.**

Let us take a root $g$ of the polynomial $x^7 + x + 1$ as generator of $[Z_7]_2$. We need a $(7, C_3, 1)_2$ difference family, namely, a set $F$ of nine $C_3$-planes of $\PG(F_2^7)$ whose list of differences covers $[Z_7]_2 \setminus \{1\}$ exactly once. We first need a set $\{\pi_1, ..., \pi_9\}$ of nine planes of $\PG(F_2^7)$ forming a difference cover of $[Z_7]_2 \setminus \{1\}$. We claim that such a difference cover is the one in which the $i$-th plane

$$\pi_i = \langle 1, g^{x_i}, g^{y_i} \rangle = \{1, g^{x_i}, g^{y_i}, g^{x_i} + 1, g^{y_i} + 1, g^{x_i} + g^{y_i}, g^{x_i} + g^{y_i} + 1\}$$

is generated by the three points 1, $g^{x_i}$, and $g^{y_i}$ where the pairs $(x_i, y_i), ..., (x_9, y_9)$ are as follows:

$$\begin{align*}
(1, 3), & \quad (1, 71), \quad (2, 18), \\
(2, 22), & \quad (2, 41), \quad (3, 13), \\
(3, 20), & \quad (8, 19), \quad (10, 40).
\end{align*}$$

Using the identity $g^7 = g + 1$, the reader can check that the images $f(\pi_1), ..., f(\pi_9)$ of the nine planes in $Z_7$ are the following:

$$\begin{align*}
\{0, 1, 3, 7, 63, 15, 31\}, & \quad \{0, 1, 71, 7, 79, 92, 74\}, \quad \{0, 2, 18, 14, 53, 114, 42\}, \\
\{0, 2, 22, 14, 47, 91, 70\}, & \quad \{0, 2, 41, 14, 75, 102, 80\}, \quad \{0, 3, 13, 63, 55, 111, 96\}, \\
\{0, 3, 20, 63, 89, 46, 37\}, & \quad \{0, 8, 19, 56, 29, 95, 65\}, \quad \{0, 10, 40, 108, 51, 72, 85\}.
\end{align*}$$

Now arrange the points of each $f(\pi_i)$ into a 7-cycle $B_i$ as follows:
The lists of differences \( \Delta B_1, \ldots, \Delta B_9 \) of the above cycles are the following:

\[
\pm\{1, 2, 4, 8, 16, 32, 63\}, \pm\{7, 6, 57, 3, 5, 13, 35\}, \pm\{18, 24, 28, 12, 15, 61, 53\}, \\
\pm\{14, 33, 23, 21, 38, 20, 22\}, \pm\{47, 49, 54, 34, 27, 39, 25\}, \pm\{55, 52, 19, 48, 50, 44, 31\}, \\
\pm\{29, 10, 11, 40, 30, 9, 56\}, \pm\{37, 17, 58, 26, 60, 43, 46\}, \pm\{51, 41, 62, 36, 59, 45, 42\}.
\]

We see that the above lists partition \( \mathbb{Z}_{127} \setminus \{0\} \), hence \( \{B_1, \ldots, B_9\} \) is a \((127, C_7, 1)\) difference family and then \( \mathcal{F} = \{f^{-1}(B_1), \ldots, f^{-1}(B_9)\} \) is a \((7, C_1, 1)\) difference family.

### A cyclic \((6, C_3, 1)\)\(_2\) design.

Let us take a root \( g \) of the polynomial \( x^6 + x^4 + x^3 + x + 1 \) as generator of \( \mathbb{Z}_6 \) and let \( f \) be the natural isomorphism between \( \mathbb{Z}_6 \) and \( \mathbb{Z}_6 \), mapping \( g \) to 1. Here we need a \((6, 3, C_3, 1)\) difference family, namely, a set \( \mathcal{F} \) of four \( C_7 \)-planes of \( \text{PG}(\mathbb{F}_2) \) whose list of differences covers \( \mathbb{Z}_6 \setminus [2\mathbb{Z}_6] \) exactly once. We first need a set \( \{\pi_1, \ldots, \pi_4\} \) of four planes of \( \text{PG}(\mathbb{F}_2) \) forming a difference cover of \( \mathbb{Z}_6 \). Such a difference cover is the one for which the \( i \)-th plane

\[
\pi_i = \langle 1, g^{x_i}, g^{y_i} \rangle = \langle 1, g^{x_i}, g^{y_i}, g^{x_i} + 1, g^{y_i} + 1, g^{x_i} + g^{y_i}, g^{x_i} + g^{y_i} + 1 \rangle
\]

is generated by the three points 1, \( g^{x_i} \), and \( g^{y_i} \) where the pairs \((x_1, y_1), \ldots, (x_4, y_4)\) are as follows:

\[
(1, 21), \quad (2, 21), \quad (2, 9), \quad (9, 12).
\]

Using the identity \( g^6 + g^4 + g^3 + g + 1 = 0 \), the reader can check that the images \( f(\pi_1), \ldots, f(\pi_4) \) of the four planes in \( \mathbb{Z}_6 \) are the following:

\[
\begin{align*}
\{0, 1, 21, 56, 42, 58, 25\}, & \quad \{0, 2, 21, 49, 42, 50, 53\}, \\
\{0, 2, 9, 49, 27, 10, 60\}, & \quad \{0, 9, 12, 27, 52, 22, 46\}.
\end{align*}
\]

Now arrange the points of each \( f(\pi_i) \) into a 7-cycle \( B_i \) as follows:

\[
\begin{align*}
(0, 1, 58, 25, 21, 56, 42), & \quad (0, 50, 42, 49, 2, 21, 53), \\
(0, 2, 27, 10, 49, 9, 60), & \quad (0, 22, 27, 12, 46, 9, 52).
\end{align*}
\]

The lists of differences \( \Delta B_1, \ldots, \Delta B_4 \) of the above cycles are the following:

\[
\begin{align*}
\pm\{1, 6, 30, 4, 28, 14, 21\}, & \quad \pm\{13, 8, 7, 16, 19, 31, 10\}, \\
\pm\{2, 25, 17, 24, 23, 12, 3\}, & \quad \pm\{22, 5, 15, 29, 26, 20, 11\}.
\end{align*}
\]

The above lists partition \( \mathbb{Z}_{63} \setminus 9\mathbb{Z}_{63} \), hence \( \{B_1, \ldots, B_4\} \) is a \((63, 7, C_7, 1)\) difference family and then \( \mathcal{F} = \{f^{-1}(B_1), \ldots, f^{-1}(B_4)\} \) is a \((6, 3, C_1, 1)\) difference family.

### A cyclic \((9, C_3, 1)\)\(_2\) design.

Let us take a root \( g \) of the polynomial \( x^9 + x^4 + 1 \) as generator of \( \mathbb{Z}_9 \) and let \( f \) be the natural isomorphism between \( \mathbb{Z}_9 \) and \( \mathbb{Z}_9 \), mapping \( g \) to 1. Here we need a \((9, 3, C_3, 1)\) design.
difference family, namely, a set $\mathcal{F}$ of thirty-six $C_7$-planes of $\text{PG}(F_9^3)$ whose list of differences covers $[Z_9]_2 \setminus [3Z_9]_2$ exactly once. Note that $\text{Frob}([Z_9]_2)$ acts semiregularly on $[Z_9]_2 \setminus [3Z_9]_2$. Thus, by a suitable specialization of Theorem 5.11, the required difference family can be realized by means of a set $\mathcal{I}$ of four $C_7$-planes whose 56 differences form a complete system of representatives for the orbits of $\text{Frob}([Z_9]_2)$ on $[Z_9]_2 \setminus [3Z_9]_2$. One can check that such a set $\mathcal{I}$ is the one formed by the preimages of the following 7-cycles of $Z_{511}$:

$$(0, 60, 1, 470, 130, 11, 504), \quad (0, 134, 130, 14, 1, 333, 139),$$

$$(0, 24, 130, 1, 294, 338, 474), \quad (0, 27, 130, 277, 1, 185, 142).$$

8 | PATH DECOMPOSITIONS OVER FINITE FIELDS

The admissibility conditions for the existence of a path decomposition over a finite field are the following.

**Proposition 8.1.** A $2 - (v, P_k, 1)_q$ design with $q$ even cannot exist. A $2 - (v, P_k, 1)_q$ design with $q$ odd and $k$ even possibly exists only for $v \equiv 0$ or 1 (mod $k - 1$). A $2 - (v, P_k, 1)_q$ design with $q$ odd and $k$ odd possibly exists only for $v \equiv 0$ or 1 (mod $2(k - 1)$).

**Proof.** A path with $n$ vertices has size $n - 1$, hence the size of $[P_k]_q$ is $[k]_q = 1 - q[k - 1]_q$. Thus, if a $2 - (v, P_k, 1)_q$ design exists, condition (iii) of Proposition 4.4 gives $[v]_q[v - 1]_q \equiv 0$ (mod $2[q(k - 1)]_q$), hence $2[k - 1]_q$ must be a divisor of $[v]_q[v - 1]_q$. It is obvious that this is not possible for $q$ even since in this case both $[v]_q$ and $[v - 1]_q$ are odd. Thus $q$ must be odd and $[k - 1]_q$ must be a divisor of $[v]_q[v - 1]_q$. Reasoning as in the proof of Proposition 4, we get $v \equiv 0$ or 1 (mod $k - 1$). Thus we have $v = (k - 1)t + r$ with $r = 0$ or 1 for a suitable $t$ and a trivial counting shows that we have

$$\frac{[v]_q[v - 1]_q}{2[k - 1]_q} = \frac{1}{2} \cdot \sum_{i=0}^{t-1} q^{(k-1)i} \cdot \sum_{i=0}^{(k-1)t-r} q^i.$$

The reduction (mod 2) of the two sums in the above formula is, respectively, equal to $t$ and $(k - 1)t + 1$. Thus, for $k$ odd, their product is even only for $t$ even. The assertion follows. 

Differently from Steiner 2-designs and cycle decompositions over finite fields, we note that there are admissible triples $(v, k, q)$ for which, a priori, a $2 - (v, P_k, 1)_q$ design cannot be obtained via difference families. The first of these triples is $(4, 3, 3$; according to Proposition 8.1 a $2 - (4, P_3, 1)_3$ design may exist but it does not make sense to speak of a $(4, P_3, 1)_3$ difference family.

The “smallest” admissible nontrivial triple $(v, k, q)$ for which a $(v, P_k, 1)_q$ difference family may exist is $(5, 3, 3$). Thus let us construct a $(5, P_3, 1)_3$ difference family, that is, a set $\mathcal{F}$ of $P_{13}$-planes of $\text{PG}(3^5)$ whose list of differences covers $[Z_5]_3^*$ exactly once. The size of $P_{13}$ is $s = 12$ and we have $[5]_3 - 1 = 120 = 2st$ with $t = 5$. Thus, by Theorem 5.10, a possible way to realize the difference family $\mathcal{F}$ is to look for only one $P_{13}$-plane of $\text{PG}(3^5)$ whose list of differences is a complete system of representatives for the orbits of $\text{Frob}([Z_5]_3)$. Let us take a root $g$ of the polynomial $x^5 + 2x + 1$ as generator of $[Z_5]_3$, and let $h$ be the natural isomorphism between $[Z_5]_3$ and $Z_{[5]_3}$ mapping $g$ to 1. Consider the plane $\pi = (1, g, g^3)$ generated by the three points $1 = g^0$, $g$, and $g^3$. The remaining points of $\pi$ are the following:
\[
g + 1 = g^{69}, \quad g + 2 = g^{5}, \quad g^3 + 1 = g^{86}, \quad g^3 + 2 = g^{15},
g^3 + g = g^{47}, \quad g^3 + g + 1 = g^{91}, \quad g^3 + g + 2 = g^{49},
g^3 + 2g = g^{75}, \quad g^3 + 2g + 1 = g^{77}, \quad g^3 + 2g + 2 = g^{28}.
\]

One can check that the list of differences of \( \pi \) has at least one element in each of the 24 orbits of \( \text{Frob}(\mathbb{Z}_3) \) on \( \mathbb{Z}_3^* \). Then it makes sense to look for a \( P_{13} \)-plane \( B \) with vertex set \( \pi \) whose list of differences has exactly one element in each of those orbits. Such a \( B \) will be the desired \( P_{13} \)-plane. The reader can easily recognize that a good \( B \) is, for instance, the preimage under \( f \) of the path depicted below.

![Diagram of a path labeled with numbers](image)

9 | VERTEX LABELINGS OF A DIFFERENCE GRAPH WITH ELEMENTS OF A DIFFERENCE SET

In this section we make a digression on a (probably new) problem which is only seemingly unrelated to the main topic of this paper. As a matter of fact, in Section 10 we will see how a specialization of this problem allows us to get several \( 2 - (v, \Gamma, \lambda) \) designs over \( \mathbb{F}_q \) with \( \Gamma \) of order \( [v - 1]_q \).

A \((v, \Gamma, \lambda)\) difference family in \( G \) with only one base block will be naturally called a \((v, \Gamma, \lambda)\) difference graph. Anyway, we warn the reader that the term “difference graph” already exists in other contexts with a completely different meaning (see, e.g., [26]). We note that when \( G \) is cyclic and \( \lambda = 1 \) this notion is completely equivalent to that of a \( \rho \)-labeling of \( \Gamma \) (see [9]). We also note that the vertex set of a \((v, \mathbb{K}_k, \lambda)\) difference graph in \( G \) is nothing but a \((v, k, \lambda)\) difference set in \( G \). There is a wide literature on difference sets, for general background on them we refer to [3,28]. Here we recall the definitions of the Paley and the Singer difference sets. If \( p \equiv 3 \pmod{4} \) is a prime, then the set of nonzero squares of \( \mathbb{Z}_p \) is a \((p, \frac{p+1}{2}, \frac{p^2-1}{4})\) difference set, which is called a Paley difference set. A Singer difference set is essentially the image of an arbitrary hyperplane of \( \text{PG}(\mathbb{F}_q^v) \) in \( \mathbb{Z}_q \). So its parameters are \([v]_q, [v - 1]_q, [v - 2]_q \). Its development gives rise to the set of all the hyperplanes of \( \text{PG}(\mathbb{F}_q^v) \), that is, to the trivial complete \( 2 - (v, v - 1, [v - 2]_q) \) design.

The obvious necessary condition for the existence of a \((v, \Gamma, \lambda)\) difference graph in a certain group \( G \) is that \( \Gamma \) has size \( \frac{\lambda(v-1)}{2} \). If this condition is satisfied and \( D \) is a \((v, k, \mu)\) difference set in \( G \) for some pair \((\mu, k)\) with \( k \) not smaller than the order of \( \Gamma \) we can ask whether it is possible to realize the required difference graph in such a way that its vertex set is contained in \( D \). In other words, we want to label the vertices of \( \Gamma \) with elements of \( D \) in such a way that the list of differences of adjacent labels covers every nonidentity element of \( G \) exactly \( \lambda \) times. A labeling as above will be called a graceful \( D \)-labeling of \( \Gamma \) since, especially when \( \lambda = 1 \), is reminiscent of the well-known notion of a graceful labeling (see [25] for a dynamic survey on this topic).

**Definition 9.1.** Let \( D \) be a \((v, k, \mu)\) difference set in a group \( G \) and let \( \Gamma = (V, E) \) be a graph with \( |V| \leq k \) and \( |E| = \frac{\lambda(v-1)}{2} \) for some \( \lambda \). A graceful \( D \)-labeling of \( \Gamma \) is an injective map \( f: V \rightarrow D \) such that the pair \((f(V), \{f(e) | e \in E\})\) is a \((v, k, \lambda)\) difference graph.

We say that a pair \((D, \Gamma)\) as in the above definition is admissible or that \( \Gamma \) is \( D \)-admissible. Also, we say that \( \Gamma \) is \( D \)-graceful if it admits a graceful \( D \)-labeling. The problem of establishing which
D-admissible graphs are D-graceful seems to us to be new. We speak of a graceful Singer or Paley-labeling of a graph \( \Gamma \) to mean a graceful D-labeling of \( \Gamma \) with D a difference set with the respective type.

Note that if \( G \) is a group, then \( G \) itself is trivially a \((v, v, v)\) difference set. Thus \( \Gamma \) is G-graceful if and only if there exists a \((v, \Gamma, \lambda)\) difference graph in \( G \). For instance, the well-known fact that there is no \((43, 7, 1)\) difference set can be also expressed by saying that \( K_7 \) is not \( \mathbb{Z}_{43} \)-graceful.

In the case that \( \Gamma \) is complete, say \( \Gamma = K_h \), we also note that \( \Gamma \) is D-graceful if and only if that there exists a \((v, h, \lambda)\) difference set in \( G \) which is contained in the \((v, k, \mu)\) difference set \( D \).

Here is a remarkable example. The difference set

\[
D = \{1, 3, 5, 6, 7, 11, 17, 18, 20, 21, 24, 25, 26, 27, 29\}
\]

is a Singer \((31, 15, 7)\) difference set in \( \mathbb{Z}_{31} \) which contains the Singer \((31, 6, 1)\) difference set \( D' = \{1, 5, 11, 24, 25, 27\} \). Thus, considering that the development of \( D \) is the set of hyperplanes of \( \text{PG}(\mathbb{F}_3^2) \) and that the development of \( D' \) is the set of lines of \( \text{PG}(\mathbb{F}_3^2) \), one might say that the projective plane of order 5 is “nested” in the point-hyperplane design associated with the four-dimensional projective space of order 2. As far as we are aware nobody observed this before. Sophisticated “games” using difference sets in the same group \( G \), such as tiling \( G \) with difference sets of the same parameters \([21]\), have been considered recently. Hence, it would be surprising if the problem of determining whether two difference sets in the same group \( G \) can be in inclusion relation was not considered before.

We could exhibit several examples of D-admissible graphs \( \Gamma \) which are G-graceful but not D-graceful. Consider, for instance, the \((15, 7, 3)\) difference set \( D = \{0, 1, 2, 4, 5, 8, 10\} \) in \( \mathbb{Z}_{15} \) and the D-admissible graph \( \Gamma = C_3 \cup C_4 \) whose connected components are a 3-cycle and a 4-cycle. There are many \((15, \Gamma, 1)\) difference graphs; one of them is depicted below.

On the other hand, by exhaustive search we have checked that none of them has vertex set \( D \). Thus \( C_3 \cup C_4 \) is \( \mathbb{Z}_{15} \)-graceful but not D-graceful.

Here is instead an example of a D-admissible graph which is also D-graceful. Let \( D = \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \) be the Paley \((19, 9, 4)\) difference set and let \( \Gamma \) be the 3-prism. A graceful Paley-labeling of \( \Gamma \) is the following:

The notion introduced in Definition 9.1 seems to be particularly interesting when \( \Gamma \) has order \( |D| \). We do not have at the moment any example of an admissible pair \((D, \Gamma)\) where \( \Gamma \) is a
regular connected graph of order $|D|$ that is not $D$-graceful. Thus we hazard the following conjecture.

**Conjecture 9.2.** Let $D$ be a $(v, k, \mu)$ difference set in $G$ and set $\lambda_i = \frac{\mu i}{\gcd(k - 1, \mu)}$ for $1 \leq i \leq \gcd(k - 1, \mu)$. Then, any connected and regular graph $\Gamma$ of order $k$ and degree $\frac{(k - 1)i}{\gcd(k - 1, \mu)}$ is $D$-graceful, hence there exists a $(v, \Gamma, \lambda_i)$ difference graph with vertex set $D$.

The conjecture is trivially true in the extremal case $i = \gcd(k - 1, \mu)$. Indeed in this case $\Gamma$ should have degree $k - 1$, hence it is necessarily the complete graph and the above statement says that there exists a $D$-graceful labeling of $\mathbb{K}_{k}$. This is equivalent to saying that $D$ is a difference set, which holds by assumption. Thus, in particular, the conjecture is trivially true when $\gcd(k - 1, \mu) = 1$.

The following proposition shows that the conjecture is true when $D$ is a Paley difference set and $\Gamma$ is circulant. For convenience of the reader we recall that if $S$ is a subset of $\{1, \ldots, \lfloor \frac{n}{2} \rfloor \}$, then the circulant graph $C(\mathbb{Z}_n; S)$ is the graph with vertex set $\mathbb{Z}_n$ whose edges are all pairs of the form $\{x, x + s\}$ with $x \in \mathbb{Z}_n$ and $s \in S$.

**Proposition 9.3.** Let $D$ be the Paley $(4n + 3, 2n + 1, n)$ difference set and let $\Gamma$ be a circulant graph of order $2n + 1$. Then $\Gamma$ is $D$-graceful.

**Proof.** By assumption, $4n + 3$ is a prime and $D$ is the set of nonzero squares of $\mathbb{Z}_{4n+3}$, that is, the subgroup $D$ of order $2n + 1$ of the multiplicative group of $\mathbb{Z}_{4n+3}$. Also by assumption we have $\Gamma = C(\mathbb{Z}_{2n+1}; S)$ for a suitable set $S$. We claim that any isomorphism $f$ between the two groups $(\mathbb{Z}_{2n+1}, +)$ and $(D, \cdot)$ is a $D$-graceful labeling of $\Gamma$. It is enough to show that the list of differences, in $\mathbb{Z}_{4n+3}$, of the graph $\Gamma' := f(\Gamma)$ is evenly distributed over the nonzero elements of $\mathbb{Z}_{4n+3}$. The edge-set of $\Gamma'$ consists of all possible pairs of the form $\{d, ds'\}$ with $d \in D$ and $s' \in S' := f(S)$. Thus we have

$$\Delta \Gamma' = \{1, -1\} \cdot \{d(1 - s')|d \in D, s' \in S'\} = \{1, -1\} \cdot D \cdot \{1 - s'|s' \in S'\}.$$

Now recall that $4n + 3$ is a prime and that $-1$ is a nonsquare in every field of order congruent to 3 (mod 4). It follows that we have $\{1, -1\} \cdot D = \mathbb{Z}_{4n+3}^{*}$. Hence we see that $\Delta \Gamma'$ covers every nonzero element of $\mathbb{Z}_{4n+3}$ exactly $|S| \times 2$ times and the assertion follows. $\square$

10 | SINGER-GRACEFUL GRAPHS AND RELATED GRAPH DECOMPOSITIONS OVER A FINITE FIELD

By Definition 9.1 and Theorem 5.4, we can state the following.

**Proposition 10.1.** If a graph $\Gamma$ of order $[v - 1]_q$ and size $\frac{\lambda q[v - 1]_k}{2}$ is Singer graceful, then there exists a cyclic $2 - (v, \Gamma, \lambda)$ design over $\mathbb{F}_q$.

Thus, if Conjecture 9.2 were true, we would have an infinite family of nontrivial graph decompositions over a finite field. Indeed, specializing the conjecture to the case that $D$ is the
Singer \((v, [v], [v - 1], [v - 2])\) difference set, we note that \(\lambda_i = i\) for each \(i\) and hence we obtain the following subconjecture.

**Conjecture 10.2.** Any regular graph \(\Gamma\) of order \([v - 1]\) and degree \(q\) with \(1 \leq i \leq [v - 2]\) is Singer graceful, hence there exists a cyclic \(2 - (v, \Gamma, i)\) design over \(\mathbb{F}_q\).

Now we give some examples supporting the above subconjecture; namely, a graceful Singer-labeling of some cycles, of a prism, of a Moebius ladder and of some generalized Petersen graphs.

### 10.1 A cyclic \(2 - (v, C_{v-1}, 1)\) design for \(v = 4, 5, 6, 7\)

By Proposition 10.1, to prove the existence of a cyclic \(2 - (v, C_{v-1}, 1)\) design it is enough to show a Singer-graceful labeling of \([C_{v-1}]_2\), the cycle of length \([v - 1]_2\). We do this for \(v = 4, 5, 6, 7\).

**\(v = 4\).**

The image of a Singer \((15, 7, 3)\) difference set in \(\mathbb{Z}_{15}\) is

\[D_{15} = \{0, 1, 2, 4, 5, 8, 10\}\]

and a graceful \(D_{15}\)-labeling of \(C_7\) is given by

![Diagram](image1)

**\(v = 5\).**

The image of a Singer \((31, 15, 7)\) difference set in \(\mathbb{Z}_{31}\) is

\[D_{31} = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}\]

and a graceful \(D_{31}\)-labeling of \(C_{15}\) is given by

![Diagram](image2)

**\(v = 6\).**

The image of a Singer \((63, 31, 15)\) difference set in \(\mathbb{Z}_{63}\) is
and a graceful $D_{63}$-labeling of $C_{31}$ is given by

$$v = 7.$$  

The image of a Singer $(127, 63, 31)$ difference set in $\mathbb{Z}_{127}$ is

$$D_{127} = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 15, 16, 17, 18, 20, 22, 23, 24, 29, 30, 32, 33, 34, 36, 39, 40, 44, 46, 48, 49, 55, 57, 58, 59, 60, 64, 65, 66, 68, 69, 71, 72, 75, 78, 80, 83, 88, 91, 92, 93, 96, 98, 99, 101, 105, 109, 110, 113, 114, 116, 118, 120\}.$$  

The above difference set $D_{127}$ admits 2 as a multiplier. In this case we have $2 \cdot D_{127} = D_{127}$, that is, $D_{127}$ is fixed by the multiplication by 2. The task of finding a graceful $D_{127}$-labeling of $C_{63}$ is facilitated if we impose that the resultant $(127, C_{63}, 1)$ difference graph is also fixed by the multiplication by 2. This happens provided that the multiplication by 2 acts as a rotation about the center of this graph by $\frac{2\pi}{7}$. Equivalently, the required difference graph has to be the union of the orbits of a path of size 9 under $\text{Frob}(\mathbb{Z}_7)$. A solution is represented in the next figure. The reader can recognize that the resulting cycle is indeed the union of the orbits of the path $[1, 3, 9, 101, 91, 5, 83, 113, 11, 2]$ under $\text{Frob}(\mathbb{Z}_7)$.  

$$D_{63} = \{0, 1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 18, 19, 24, 26, 27, 28, 32, 33, 35, 36, 38, 41, 45, 48, 49, 52, 54, 56\}$$
10.1.1 | A prism decomposition over $\mathbb{F}_3$

The prism graph on $2n$ vertices is the cubic graph corresponding to the skeleton of an $n$-prism. Following [27] we denote it by $\Pi_n$.

Let us construct a cyclic $2 - (5, \Pi_{40}, 1)$ design over $\mathbb{F}_3$. For this, it is enough to give a Singer-graceful labeling of $\Pi_{40}$. The image of a Singer $(121, 40, 13)$ difference set in $\mathbb{Z}_{121}$ is

$$D = \{1, 2, 3, 6, 7, 9, 11, 18, 20, 21, 25, 27, 33, 34, 38, 41, 44, 47, 53, 54, 55, 56, 58, 59, 60, 63, 64, 68, 70, 71, 75, 81, 83, 89, 92, 99, 100, 102, 104, 114\}$$

and a $D$-graceful labeling of $\Pi_{40}$ is the following:
Note that the above graph is fixed by the multiplication by 3. Indeed, denoting by $v_i$ the label of the $i$th “outer” vertex and by $v'_i$ the label of the corresponding “inner” vertex, one can check that $v_{i+4} \equiv 3v_i \pmod{121}$ and $v'_{i+4} \equiv 3v'_i \pmod{121}$ for every possible $i$ (it is understood that the indices have to be considered modulo 40 and that the $(i + 1)$th vertex of the outer cycle follows the $i$th one clockwise). This means that the multiplication by 3 corresponds to a clockwise rotation of the above graph about its center by 72°.

10.1.2 Generalized Petersen decompositions over $\mathbb{F}_3$

Let $n \geq 5$ be an integer, let $\mathbb{Z}'_n = \{0', 1', ..., (n - 1)\}'$ be a disjoint isomorphic copy of $\mathbb{Z}_n$, and let $k$ be an integer in the closed interval $[2, n - 2]$. The generalized Petersen graph $P(n, k)$ is the graph of order $2n$ with vertex set $\mathbb{Z}_n \cup \mathbb{Z}'_n$ which is the union of the circulant graphs $C(\mathbb{Z}_n; \{\pm 1\}), C(\mathbb{Z}'_n; \{\pm k\})$ and the perfect matching $\{(i, i')|0 \leq i \leq n - 1\}$.

We want to construct a cyclic $2 - (5, P(20, k), 1)$ design over $\mathbb{F}_3$ for each possible $k$, hence for $k = 2, 3, 4, 5, 6, 7, 8, 9$. For this, it is enough to give a $D$-graceful labeling of $P(20, k)$ where $D$ is the Singer $(121, 40, 13)$ difference set that we gave in Section 10.1.1. Here is, for instance, a Singer-labeling of $P(20, 3)$:
Also here, as for the prism seen below, the multiplication by 3 corresponds to a clockwise rotation of the graph about its center by 72°. We report below how to label the eight vertices \(0, 1, 2, 3, 0', 1', 2', 3'\) of \(P(20, k)\) to obtain, with the same method, a \(D\)-graceful labeling of \(P(20, k)\) for \(2 \leq k \leq 9\).

| \(k\) | \(\{v_0, v_1, v_2, v_3\}\) | \(\{v'_0, v'_1, v'_2, v'_3\}\) |
|-----|-----------------|-----------------|
| 2   | \{1, 7, 2, 34\} | \{70, 20, 11, 53\} |
| 3   | \{1, 11, 7, 2\} | \{20, 34, 25, 58\} |
| 4   | \{1, 7, 2, 100\} | \{11, 20, 64, 25\} |
| 5   | \{1, 20, 2, 25\} | \{64, 7, 53, 11\} |

As a matter of fact it would not have been necessary to treat both \(k = 3\) and 7 since \(P(20, 3)\) and \(P(20, 7)\) are isomorphic (see, e.g., \([34]\)).

In conclusion, we have given a \((5, P(20, k), 1)\) difference graph over \(\mathbb{F}_3\) which is fixed by \(\text{Frob}[\mathbb{Z}_3]\) for \(2 \leq k \leq 9\).

### 10.1.3 A Moebius ladder decomposition over \(\mathbb{F}_3\)

The Moebius ladder \(M_{2n}\) is the circulant graph \(C(\mathbb{Z}_{2n}; \{1, n\})\). In simpler words, it is the cubic graph of order \(2n\) obtained from the \(2n\)-cycle \((c_0, c_1, ..., c_{2n-1})\) by adding all possible diameters, that is, all edges of the form \(\{c_i, c_{i+n}\}\) with \(1 \leq i \leq n\).

Let us construct a cyclic \(2 - (5, M_{40}, 1)\) design over \(\mathbb{F}_3\). For this, it is enough to give a \(D\)-graceful labeling of \(M_{40}\) where \(D\) is the Singer \((121, 40, 13)\) difference set that we gave in Section 10.1.1. Such a labeling is the one shown below:

![Moebius ladder diagram](image-url)
The reader can recognize, once again, that the $(121, M_{40}, 1)$ difference graph constructed above is fixed by $\text{Frob}[\mathbb{Z}_q]$. The external $40$-cycle is obtainable by joining the orbits of the path $[1, 2, 25, 7, 20, 34, 100, 11, 3]$ under this group.

### 10.2 Near resolvable $(v, 2, 1)_q$ designs

We recall that a resolvable $2 - (v, k, \lambda)$ design is a triple $(\mathcal{P}, B, \mathcal{R})$ where $(\mathcal{P}, B)$ is a $2 - (v, k, \lambda)$ design and $\mathcal{R}$ is a partition of $B$ into classes (parallel classes) each of which is, in its turn, a partition of $\mathcal{P}$.

We also recall that a near resolvable $2 - (v, k - 1, \lambda)$ design is a triple $(\mathcal{P}, B, \mathcal{R})$ where $(\mathcal{P}, B)$ is a $2 - (v, k - 1, \lambda)$ design and $\mathcal{R}$ is a partition of $B$ into classes (near parallel classes) each of which gives a partition of all points except one.

A $2 - (v, 2, 1)$ design is nothing but the complete graph $\mathbb{K}_v$ and its $q$-analog, namely, a $2 - (v, 2, 1)_q$ design, is the point-line design of $\text{PG}(\mathbb{F}_q^v)$. These designs are clearly trivial.

A resolvable $2 - (v, 2, 1)$ design (more commonly known as a one-factorization of $\mathbb{K}_v$) is a partition of the edges of $\mathbb{K}_v$ into perfect matchings.\footnote{A perfect matching of a graph $\Gamma$ is a subset of $E(\Gamma)$ partitioning $V(\Gamma)$.} The $q$-analog of a perfect matching of $\mathbb{K}_v$ is clearly a parallel class of the point-line design associated with $\text{PG}(\mathbb{F}_q^v)$, that is, a line spread of $\text{PG}(\mathbb{F}_q^v)$. It is then natural to give the following definition.

**Definition 10.3.** A resolvable $2 - (v, 2, 1)_q$ design is a partition of the lines of $\text{PG}(\mathbb{F}_q^v)$ into classes each of which is a line spread of $\text{PG}(\mathbb{F}_q^v)$.

Adopting this terminology, a famous result by Baker [2] can be restated as follows.

**Theorem 10.4** (Baker [2]). There exists a resolvable $2 - (v, 2, 1)_2$ design if and only if $v$ is even.

A near resolvable $2 - (v, 2, 1)$ design is a partition of the edges of $\mathbb{K}_v$ into near perfect matchings.\footnote{A near perfect matching of a graph $\Gamma$ is a subset of $E(\Gamma)$ partitioning $V(\Gamma) \setminus \{x\}$ for a suitable missing vertex $x$.} Obviously, a near perfect matching $N$ of $\mathbb{K}_v$ can be seen as a perfect matching of $\mathbb{K}_{v-1}$. Thus, for what we have said above, the $q$-analog of $N$ should be a 1-spread of a $\text{PG}(\mathbb{F}_q^{v-1})$, that is, a 1-spread of a hyperplane of $\text{PG}(\mathbb{F}_q^v)$. It is then natural to give the following definition.

**Definition 10.5.** A near resolvable $2 - (v, 2, 1)_q$ design is a partition of the lines of $\text{PG}(\mathbb{F}_q^v)$ into classes each of which forms a spread of a hyperplane.
generator of \([\mathbb{Z}_6]_2\), take the Singer \((31, 15, 7)\) difference set \(D = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}\) considered in Section 10.1, and let \(\Gamma\) be the graph whose connected components are five 3-cliques. A \(D\)-graceful labeling of \(\Gamma\) is

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
7 & 8 & 9 & 10 & 11 & 12 \\
13 & 14 & 15 & 16 & 17 & 18 \\
19 & 20 & 21 & 22 & 23 & 24 \\
25 & 26 & 27 & 28 & 29 & 30 \\
\end{array}
\]

On the other hand none of the cliques of the above graph is a line of \(\text{PG}(\mathbb{F}_2^3)\). Indeed the sum of the three elements of the \(i\)th clique is \(g^i + 1\).

11 | IMPROPER GRAPH DECOMPOSITIONS OVER A FINITE FIELD

Given a graph \(\Gamma\), let us denote by \(I(\Gamma)\) the set of its isolated vertices and by \(\Gamma \setminus I(\Gamma)\) the graph obtained from \(\Gamma\) by deleting all its isolated vertices. The graph obtained with the opposite operation of adding a certain number \(d\) of isolated vertices to a graph \(\Gamma\) will be denoted by \(\Gamma \cup N_d\). Indeed, by \(N_d\) we mean the null graph of order \(d\), that is, the edgeless graph with \(d\) vertices.

Usually, speaking of a \(2-(v, \Gamma, \lambda)\) design, it is understood that \(I(\Gamma)\) is empty. This is because if \(B\) is the collection of blocks of a \(2-(v, \Gamma, \lambda)\) design, then it is obvious that \(\{B \setminus I(B) | B \in B\}\) is the collection of blocks of a \(2-(v, \Gamma \setminus I(\Gamma), \lambda)\) design. Conversely, it is clear that from a \(2-(v, \Gamma, \lambda)\) design one can immediately obtain a \(2-(v, \Gamma \cup N_d, \lambda)\) design provided that \(d \leq v - k\) where \(k\) is the order of \(\Gamma\).

Anyway, to allow isolated vertices in the context of graph decompositions over a finite field is meaningful. Indeed, deleting the isolated vertices of each block of a \(2-(v, \Gamma, \lambda)\) design over \(\mathbb{F}_q\) we do not obtain a \(2-(v, \Gamma \setminus I(\Gamma), \lambda)\) design over \(\mathbb{F}_q\).

We will say that a \(2-(v, \Gamma, \lambda)\) design over \(\mathbb{F}_q\) is improper of degree \(d\) if \(\Gamma\) has exactly \(d\) isolated vertices. An improper design of degree 0 will be said proper. That said, it is clear that the most interesting designs are the proper ones. Suffice it to say that every possible \(2-(v, \Gamma, \lambda)\) design can be “extended” to a suitable \(2-(v, \Gamma, \lambda)\) design over \(\mathbb{F}_q\); in the worst of the cases, said \(k\) the order of \(\Gamma\), it gives a spanning \(2-(|v|_q, \Gamma \cup N_{|v|_q-k}, \lambda)\) design over \(\mathbb{F}_q\).

As an example, we give a \(2-(7, \Pi_3 \cup N_1, 1)\) design over \(\mathbb{F}_2\), so improper of degree 1. Reasoning exactly as in Section 5.4 the reader can check that such a design can be obtained by means of only one initial base block that is the preimage under \(f\) of the graph depicted below.

\[
\begin{array}{cccc}
0 & 25 & 60 & 1 \\
& 124 & & \\
& & 185 & \\
& & & 7 \\
\end{array}
\]
12 | CONCLUSION

It would be nice to conclude with a list of open problems. The fact is that almost everything is still open. Even though the topic of designs over finite fields has been considerably relaxed, to find general answers seems to be extremely difficult. At the moment, for the case $\lambda = 1$, we are not even able to exhibit an infinite family of nontrivial $\Gamma$-decompositions over a finite field. So a natural target, hopefully not too ambitious, should be to prove that there are infinitely many values of $v$ for which there exists a $2 - (v, \Gamma, 1)$ design over $\mathbb{F}_q$ for at least one pair $(q, \Gamma)$.

ACKNOWLEDGMENTS

The authors are grateful to the anonymous referees for their comments which improved the readability of the paper. This study has been performed under the auspices of the G.N.S.A.G.A. of the C.N.R. (National Research Council) of Italy. The second author is supported in part by the Croatian Science Foundation under the project 6732.

ORCID

Marco Buratti http://orcid.org/0000-0003-1140-2251
Anamari Nakić http://orcid.org/0000-0001-5237-7203
Alfred Wassermann http://orcid.org/0000-0001-5946-668X

REFERENCES

1. R. J. R. Abel and M. Buratti, Difference families, Handbook of Combinatorial Designs (C. J. Colbourn and J. H. Dinitz, eds.), 2nd ed., Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. 392–410.
2. R. D. Baker, Partitioning the planes of $AG(2m, 2)$ into 2-designs, Discrete Math. 15 (1976), 205–211.
3. T. Beth, D. Jungnickel, and H. Lenz, Design theory, Cambridge University Press, Cambridge, 1999.
4. M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann, On the existence of $q$-analogs of Steiner systems, Forum Math. 4 (2016).
5. M. Braun, A. Kerber, and R. Laue, Systematic construction of $q$-analogs of designs, Des. Codes Cryptogr. 34 (2005), 55–70.
6. M. Braun, M. Kiermaier, and A. Nakić, On the automorphism group of a binary $q$-analog of the Fano plane, European J. Combin. 51 (2016), 443–457.
7. M. Braun, M. Kiermaier, and A. Wassermann, $q$-Analogs of designs: Subspace designs, Chapter in Network Coding and Subspace Designs, Springer, 2018.
8. M. Braun, M. Kiermaier, and A. Wassermann, Computational methods in subspace designs, Chapter in Network Coding and Subspace Designs (M. Greferath, M. O. Pavčević, N. Silberstein, M. Á. Vázquez-Castro, eds.), Springer International Publishing, 2018.
9. D. Bryant and S. El-Zanati, Graph decompositions, Handbook of Combinatorial Designs (C. J. Colbourn and J. H. Dinitz, eds.), 2nd ed., Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. 477–486.
10. M. Buratti, Recursive constructions for difference matrices and relative difference families, J. Combin. Des. 6 (1998), 165–182.
11. M. Buratti, On disjoint $(v, k, k - 1)$ difference families, Des. Codes Cryptogr. 87 (2019), 745–755.
12. M. Buratti, S. Capparelli, F. Merola, G. Rinaldi, and T. Traetta, A collection of results on Hamiltonian cycle systems with a nice automorphism group, Electron. Notes Discrete Math. 40 (2013), 245–252.
13. M. Buratti and L. Gionfriddo, Strong difference families over arbitrary groups, J. Combin. Des. 16 (2008), 443–461.
14. M. Buratti, M. Kiermaier, S. Kurz, A. Nakić, and A. Wassermann, $q$-Analogs of group divisible designs, Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications. Radon Series on Computational and Applied Mathematics (K.-U. Schmidt, and A. Winterhof, eds.), De Gruyter, Berlin.
15. M. Buratti and A. Pasotti, *Graph decompositions with the use of difference matrices*, Bull. Inst. Combin. Appl. **47** (2006), 23–32.
16. M. Buratti and A. Pasotti, *On perfect Γ-decompositions of the complete graph*, J. Combin. Des. **17** (2009), 197–209.
17. M. Buratti and A. Pasotti, *Combinatorial designs and the theorem of Weil on multiplicative character sums*, Finite Fields Appl. **15** (2009), 332–344.
18. M. Buratti and A. Nakić, *Designs over finite fields by difference methods*, Finite Fields Appl. **57** (2019), 128–138.
19. P. Cameron, *Generalisation of Fisher’s inequality to fields with more than one element*, Combinatorics: Proceedings of the British Combinatorial Conference 1973, London Mathematical Society Lecture Notes Series (T. P. McDonough, and V. C. Mavron, eds.), Cambridge University Press, Cambridge, 1974, pp. 9–13.
20. P. Cameron, *Locally symmetric designs*, Geom. Dedicata **3** (1974), 56–76.
21. A. Ćustić, V. Krčadinac, and Y. Zhou, *Tiling groups with difference sets*, Electron. J. Combin. **22** (2015), 13.
22. P. Delsarte, *Association schemes and t-designs in regular semilattices*, J. Combin. Theory Ser. A **20** (1976), 230–243.
23. R. Fuji-Hara, M. Jimbo, and S. Vanstone, *Some results on the line partitioning problem in PG(2k, q)*, Util. Math. **30** (1986), 235–241.
24. R. Fuji-Hara, A. Munemasa, and V. Tonchev, *Hyperplane partitions and difference systems of sets*, J. Combin. Theory Ser. A **113** (2006), 1689–1698.
25. J. A. Gallian, *A dynamic survey of graph labeling*, Electron. J. Combin. **14** (2007), #DS6.
26. P. L. Hammer, U. N. Peled, and X. Sun, *Difference graphs*, Discrete Appl. Math. **28** (1990), 35–44.
27. M. Hladnik, D. Marušić, and T. Pisanski, *Cyclic Haar graphs*, Discrete Math. **244** (2002), 137–152.
28. D. Jungnickel, A. Pott, and K. W. Smith, *Difference sets*, Handbook of Combinatorial Designs (C. J. Colbourn and J. H. Dinitz, eds.), 2nd ed., Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. 419–435.
29. M. Kiermaier, S. Kurz, and A. Wassermann, *The order of the automorphism group of a binary q-analog of the Fano plane is at most two*, Des. Codes Cryptogr. **86** (2018), 239–250.
30. M. Lavrauw and G. Van de Voorde, *Field reduction and linear sets in finite geometry*, Contemporary Mathematics (G. Kyureghyan, G. Mullen, and A. Pott, eds.), American Mathematical Society, Providence, RI, USA 2015, pp. 271–293.
31. R. Mathon, *Constructions for cyclic Steiner 2-designs*, Ann. Discrete Math. **34** (1987), 353–362.
32. A. Nakić and M. Pavčević, *Tactical decompositions of designs over finite fields*, Des. Codes Cryptogr. **77** (2015), 49–60.
33. D. A. Santos, *Number theory for mathematical contests*, available at https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf
34. A. Steimle and W. Staton, *The isomorphism classes of the generalized Petersen graphs*, Discrete Math. **309** (2009), no. 1, 231–237.
35. S. Thomas, *Designs over finite fields*, Geom. Dedicata **24** (1987), 237–242.
36. V. Tonchev, *Partitions of difference sets and code synchronization*, Finite Fields Appl. **11** (2005), 605–621.
37. R. M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory **4** (1972), 17–42.

**How to cite this article:** Buratti M, Nakić A, Wassermann A. Graph decompositions in projective geometries. *J Combin Des*. 2021;29:141–174. https://doi.org/10.1002/jcd.21761