Università degli Studi Roma Tre
Scuola dottorale in Scienze Matematiche e Fisiche

Dottorato di Ricerca in Matematica
XXVIII ciclo

New combinatorial designs via Strong Difference Families

Candidate
Simone Costa

Advisor
Prof. Marco Buratti

Coordinator
Prof. Luigi Chierchia

Anno Accademico 2015-2016

Contents

Introduction

Combinatorial design theory is the study of arranging elements of a finite set into patterns (subsets, words, arrays) according to specified rules. Basically a design is a pair $(V, \mathcal{B})$ where V is a set of points and $\mathcal{B}$ is a collection of subsets of V that satisfies suitable balance properties. According to these additional properties we can define several kinds of designs. Because of this flexibility, design theory is a field of combinatorics with close ties to several other branches of mathematics including group theory, the theory of finite fields, finite geometries, number theory, combinatorial matrix theory and graph theory. This theory has also a wide range of applications in areas such as information theory, statistics, computer science, biology and engineering.

Some types of designs that we will discuss in the present work include 2-designs, pairwise balanced designs, group divisible designs and graph decompositions. In all these cases the fundamental question is the existence question. Does a design of a specified type exist?

Probably the most important objects under consideration are 2-designs. Specifically a 2-(v, k, λ) design (also called (v, k, λ)-$BIBD$ or balanced incomplete block design) is a pair $(V, \mathcal{B})$ where V is a set of v elements and $\mathcal{B}$ is a collection of subsets, or blocks, of V such that:

- every block contains exactly k points;
- every pair of distinct points is contained in exactly λ blocks.

The concept of 2-(v, k, λ) design was introduced by R. Fisher (1934) studying the design of experiments. These structures turn out to be very useful also in many other fields of mathematics. Therefore now there is a vast literature on combinatorial designs and specifically on 2-designs (thousands of papers on `mathscinet`). Here, we refer the readers to [10, 38, 44] and [60] which are good introductions and surveys to the topic and to [2, 3, 9, 43, 54] which are closely related to the present work in techniques and topics.

In regard to the problem of existence of 2-designs, a big progress was done by H. Hanani (see [44], 1975) who solved the case in which the blocks have size less or equal to 5. Another remarkable result is due to R.M. Wilson (1972) who proved the asymptotical existence of a 2-(v, k, λ) design if the well known necessary conditions are satisfied (see Corollary 1.1.7). However, despite the fact that many authors worked on the case $6 \leq k \leq 9$, there are still many open cases and little is known when $9 < k$. We will review these designs in depth in Chapter 1, giving the known

necessary conditions of existence, enunciating the existence results and listing the open cases.

As we will see in Chapter 1, the problem of existence of a 2-(v, k, λ) design can be described in terms of decompositions of the multigraph $\lambda\mathbb{K}_v$, that is the multigraph with v vertices and with λ edges between each pair of vertices, into copies of the complete graph $\mathbb{K}_k$. Since many other combinatorial problems can be described in similar terms the more general definition of Λ-decomposition of Γ (or briefly (Γ, Λ)-design) was introduced: given a multigraph Γ and a graph Λ, a Λ-decomposition of Γ is a set $\mathcal{C}$ of subgraphs of Γ isomorphic to Λ whose edges partition the set $E(\Gamma)$ of the edges of Γ. Another relevant case of such designs is given by the k-cycle decompositions of $\mathbb{K}_v$, or briefly $(\mathbb{K}_v, C_k)$-designs, where C_k is a cycle of length k and $\mathbb{K}_v$ is the complete graph with v vertices. The existence problem for such designs has been completely solved by B. Alspach, H. Gavlas (see [8], 2001) and by M. Sajna (see [57], 2002, see also M. Buratti [17], 2003). However a lot of related problems, such as the existence of k-cycle decompositions of $\mathbb{K}_v$ with additional properties, are still open. A class of such designs is given by the i-perfect k-cycle decompositions. A k-cycle decomposition is called i-perfect if, for any pair of vertices of $\mathbb{K}_v$, there is exactly one cycle of $\mathcal{C}$ in which x and y have distance i. Such designs has been introduced by C.C. Lindner and C.A. Rodger (see [48], 1991), in the case $i = 2$, in order to construct quasi-groups. The interest on these decompositions is also given by the fact that being i-perfect is an invariant property with respect to design isomorphisms. In Chapter 1, we will introduce the known theory about these kind of designs, giving the known necessary conditions of existence, enunciating the existence results and listing the open cases.

An important link between 2-designs and the k-cycle decompositions is given by the construction method of difference families and more generally of relative difference families. These methods were introduced by R.C. Bose in his seminal paper of 1939 (see [14]) in order to construct 2-designs with suitable symmetries. However, as we will see in Chapter 2, these kinds of methods turn out to be very useful to construct, more in general, graph decompositions and in particular k-cycle decompositions.

We continue this thesis by exposing, in Chapter 2, the theory of strong difference families ($SDFs$). This concept was introduced by M. Buratti in [22] (and then generalized by M. Buratti and L. Gionfriddo in [25]) in order to obtain a systematic method of construction of difference families, graph decompositions and designs.

The study of strong difference families is the leitmotif of this thesis: in particular, in Chapters 3 and 4, we introduce a new class of SDFs in order to approach a problem of existence of particular combinatorial structures.

The first problem we will see concerns the existence of i-perfect k-cycle decompositions of the complete graph $\mathbb{K}_{mk}$. In fact, in Chapter 3, we will present the results of a joint work with M. Buratti and X. Wang (see [24]) on this problem. In particular, generalizing a result here denoted by "the Buratti, Rania and Zuanni construction" see [29], we present a construction for i-perfect k-cycle decompositions of the complete m-partite graph with parts of size k that implicitely uses the concept of strong difference families. This tecnique works whenever an *i-perfect map* $f : \mathbb{Z}_k \longrightarrow R$ exists for a suitable ring R of cardinality m. We show that,

in order to determe the set of all triples (i, k, m) for which such a map exists, it is crucial to calculate the chromatic numbers of some auxiliary graphs. We completely determine this set except for the case where $k > 1000$ is the product of two distinct primes, $i > 2$ is even, and $\gcd(m, 25) = 5$. Then we return to the existence problem of i-perfect k-cycle decompositions of the complete graph $\mathbb{K}_{mk}$. In particular, as a consequence the above considerations, we completely solve the case $k \leq 19$.

Theorem 3.6.5 (M. Buratti, S. C., X. Wang)**.** *Let m and k be odd integers. Then there exists an i-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ whenever $k \leq 19$ and for any possible i with the only exceptions of a 2-perfect $(\mathbb{K}_{15}, C_5)$-design, and of a 2- and a 4-perfect $(\mathbb{K}_9, C_9)$-design.*

Then, in Chapter 4, we provide a further generalization of the Buratti, Rania and Zuanni construction introducing a technique that makes use of the so called i-perfect (Z_k, C_k, μ)-SDF. In this chapter we present the results of a joint work with X. Wang (strongly inspired by the ideas of M. Buratti and by the papers [28] and [25]), in which we study this class of strong difference families obtaining the following result:

Theorem 4.3.4 (S. C., X. Wang)**.** *Let m and k be positive integers, then there exists a 3-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ if and only if mk is odd and $k \geq 7$. Moreover, if $m \notin E := \{3, 15, 33, 39, 51, 75, 87\}$ and mk is odd, there exists an i-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ in the following cases:*

- *k a prime and any possible i;*
- *$k < 56$ odd and any possible i except for:*

$$(i, k) \in \{(2, 9), (4, 9), (7, 21), (13, 39), (15, 45), (6, 51)\}.$$

Finally, in Chapter 5, we will see that it is still possible to use the SDFs in order to construct new 2-(v, k, λ) designs. In particular we build, using a computer search, five new SDFs and we use them to prove the existence of several infinite series of 2-designs. For this purpose, we apply also a theorem of M. Buratti and A. Pasotti (that makes use of Weil's theorem on the sum of multiplicative characters). Among these series, we have found a 2-design for seven triples of values (v, k, λ) whose existence was an open problem. The main result of the chapter is the following:

Theorem 5.4.1 (S. C., X. Wang)**.** *There exists a 2-(v, k, λ) design in the following cases:*

(v, k, λ)	*Possible exceptions*
$(694, 7, 2)$ $(1576, 8, 1)$ $(2025, 9, 1)$, $(765, 9, 2)$ *and* $(1845, 9, 2)$ $(459, 9, 4)$ *and* $(783, 9, 4)$	
$(13p, 13, 1) : \ p \equiv 1 \pmod{12}$, *prime* $(13q, 13, 3) : \ q \equiv 1 \pmod 4, q \geq 13$	*List of* 19 *values*
$(17p, 17, 2) : \ p \equiv 1 \pmod 8$, *prime* $(17q, 17, 4) : \ q \equiv 1 \pmod 4, q \geq 17$	$41, 73, 89, 193$

Chapter 1

Preliminaries

1.1 2-designs: definition and basic properties

Design theory concerns the study of arranging elements of a finite set into patterns (subsets, words, arrays) according to specified rules. In this work a *design* can be described as a pair $(V, \mathcal{B})$ where V is a set of *points* and $\mathcal{B}$ is a collection of non-empty subsets, called *blocks*, of V with suitable properties. In general the family $\mathcal{B}$ can have repeated blocks: this is why we refer to $\mathcal{B}$ as a collection or a multiset (we will use also the terms family and list) of blocks and not as a set. Because of that we use the notation $\mathcal{B} = [B_1, \ldots, B_b]$ instead of $\mathcal{B} = \{B_1, \ldots, B_b\}$. In fact, in this work, we will use the notation $\{\ \}$ to denote a simple set and we will use the notation $[\ ]$ to denote the more general concept of multiset. We note that if no element of a multiset is repeated then the multiset is a set. For example, we have that $[1, 6, 5] = \{1, 6, 5\}$ while $[3, 7, 9, 3] \neq \{3, 7, 9, 3\} = \{3, 7, 9\}$.

We recall the definition of 2-*designs* that are probably the most studied type of designs. Here is the formal definition:

Definition 1.1.1. *Let v, k and λ be positive integers such that $v > k \geq 2$. A 2-(v, k, λ) design (also called (v, k, λ)-BIBD or balanced incomplete block design) is a pair $(V, \mathcal{B})$ where V is a set of v elements, called points, and $\mathcal{B} = [B_1, \ldots, B_b]$ is a collection of subsets, called blocks, of V such that:*

1 every block contains exactly k points;

2 every pair of distinct points is contained in exactly λ blocks.

Such designs are called "balanced" due to property 2.

As usual for a mathematical structures, it is interesting to define and to study the maps that preserve that structure.

Definition 1.1.2. *Two designs $(V, \mathcal{B})$ and $(V', \mathcal{B}')$ are isomorphic if there exists a bijection $\alpha : V \to V'$ mapping $\mathcal{B}$ into $\mathcal{B}'$ or, in other words:*

$$[\{\alpha(x) :\ x \in B\} : B \in \mathcal{B}] = \mathcal{B}'.$$

The bijection α is called an isomorphism. If $(V, \mathcal{B}) = (V', \mathcal{B}')$ the map α is called an automorphism of $(V, \mathcal{B})$. We denote with $Aut(V, \mathcal{B})$ the set of all automorphisms of $(V, \mathcal{B})$.

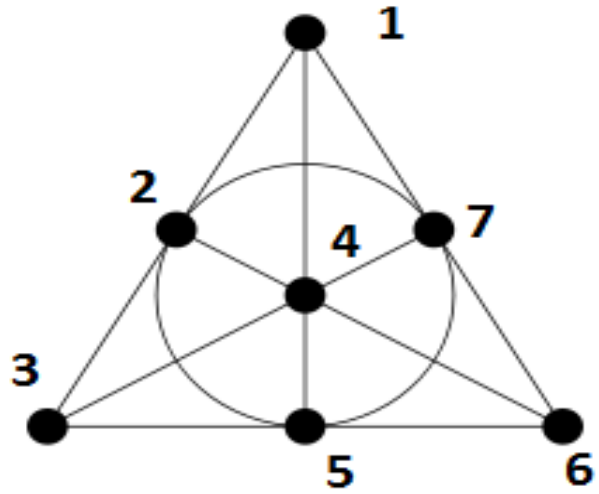
We give now some examples of 2-designs that arise from a geometrical context.

Example 1.1.3 (Fano Plane)**.** *The following pair* $(V, \mathcal{B})$ *is a* 2-$(7, 3, 1)$ *design:*

$$V := \{1, 2, 3, 4, 5, 6, 7\}, \text{ and}$$

$$\mathcal{B} := [\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}].$$

This collection of blocks can be represented geometrically with the following picture:



From this picture it is clear that every pair of distinct points is contained in exactly one block.

We remark that the Fano Plane is the *projective plane* over the field $\mathbb{F}_2$ and it is also the smallest existent projective plane. In general all the *projective planes* over a finite field are examples of 2-designs:

Example 1.1.4 (Projective plane over the field $\mathbb{F}_q$)**.** *Let* q *be a prime power and let us consider the finite field* $\mathbb{F}_q$ *of cardinality* q*.*

Let (x_0, x_1, x_2) *and* (y_0, y_1, y_2) *be two elements of* $\mathbb{F}_q^3 \setminus \{0\}$*. Then we define the equivalence relation* $\sim$ *as follows:* $(x_0, x_1, x_2) \sim (y_0, y_1, y_2)$ *if there is a non-zero element* $\lambda \in \mathbb{F}_q$ *such that* $(x_0, x_1, x_2) = \lambda(y_0, y_1, y_2)$*.*

We consider the set of points given by:

$$V := \frac{\mathbb{F}_q^3 \setminus \{0\}}{\sim}.$$

As collection of blocks, we consider the set $\mathcal{B}$ *given by the subsets* B *of* V *such that there exists a 2-dimensional subspace* L *of* $\mathbb{F}_q^3$ *and* $\frac{L\setminus\{0\}}{\sim} = B$*.*

Then the pair $(V, \mathcal{B})$ *is a* 2-$(q^2 + q + 1, q + 1, 1)$ *design.*

In fact, it is well known that, given two points of a projective planes, there exists exactly one line through them. Moreover we have that $|\mathbb{F}_q^3 \setminus \{0\}| = q^3 - 1$ and each equivalence class has size $q - 1$ therefore $|V| = \frac{q^3-1}{q-1} = q^2 + q + 1$. Similarly, given a 2-dimensional subspace L of $\mathbb{F}_q^3$, we have that $|L \setminus \{0\}| = q^2 - 1$. Thus $|\frac{L\setminus\{0\}}{\sim}| = |B| = \frac{q^2-1}{q-1} = q + 1$.

1.1.1 Necessary conditions and existence results

One of the main goals of combinatorial design theory is to determine necessary and sufficient conditions for the existence of a 2-(v, k, λ) design. In this subsection we list some theorems and basic properties of such designs that give us necessary conditions of existence. We will see that, in general, it is not known whether these conditions are sufficient.

Theorem 1.1.5. *In a* 2-(v, k, λ) *design, every point occurs in exactly*

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks.

Proof. Let $(V, \mathcal{B})$ be a 2-(v, k, λ) design. Suppose $x \in V$ and let r_x denote the number of blocks containing x. We define the set:

$$I_x := \{(y, A) : y \in V,\ y \neq x,\ A \in \mathcal{B}, \{x, y\} \subseteq A\}.$$

We want to do a double counting of the cardinality of this set.

First, there are $v-1$ ways to choose $y \in V$ such that $y \neq x$. For each choice there are λ ways to choose $A \in \mathcal{B}$ such that $\{x, y\} \subseteq A$. Hence,

$$|I_x| = \lambda(v-1).$$

On the other hand, there are r_x ways to choose a block A such that $x \in A$. For each choice of A, there are $k-1$ ways to choose $y \in A,\ y \neq x$. Hence,

$$|I_x| = r_x(k-1).$$

Combining these two equations, we see that:

$$r_x = \frac{\lambda(v-1)}{k-1}$$

is independent of x and the claim follows. □

Theorem 1.1.6. *A* 2-(v, k, λ) *design has exactly*

$$b = \frac{\lambda(v(v-1))}{k(k-1)}$$

blocks.

Proof. Let $(V, \mathcal{B})$ be a 2-(v, k, λ) design and let $b = |\mathcal{B}|$. Define the set:

$$I = \{(x, A) :\ x \in V,\ A \in \mathcal{B}, x \in A\}.$$

We want to do a double counting of the cardinality of this set.

First, there are v ways to choose $x \in V$. For each of such choices, there are r blocks A such that $x \in A$. Hence:

$$|I| = vr.$$

On the other hand, there are b ways to choose a block $A \in \mathcal{B}$. For each choice of A, there are k ways to choose $x \in A$. Hence

$$|I| = bk.$$

Combining these equations we see that $bk = vr$ as desired. □

In particular the values b and r must be integers: through these two theorems we can conclude that 2-designs with certain parameters do not exist.

Corollary 1.1.7. *If a 2-(v, k, λ) design exists, then $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.*

We give the following definition in order to get another, important, necessary condition for the existence of such designs:

Definition 1.1.8. *Let $(V, \mathcal{B})$ be a design where $V = \{x_1, \ldots, x_v\}$ and $\mathcal{B} := \{B_1, \ldots, B_b\}$. The incidence matrix of $(V, \mathcal{B})$ is the $v \times b$, 0-1 matrix $M = (m_{i,j})$ defined by the rule:*

$$m_{i,j} := \begin{cases} 1 \text{ if } x_i \in B_j; \\ 0 \text{ if } x_i \notin B_j. \end{cases}$$

The incidence matrix M of a 2-(v, k, λ) design satisfies the following properties:

1 Every column of M contains exactly k times the value 1: this property holds because the size of each block is k.

2 Every row of M contains exactly r times the value 1: this property holds because every point lies in exactly r blocks.

3 Two distinct rows of M both contains 1s in exactly λ columns: this property holds because two distinct points lie together in exactly λ blocks.

Now we are ready to state Fisher's Inequality:

Theorem 1.1.9 (Fisher's Inequality)**.** *In any 2-(v, k, λ) design with $v > k$, we have that the number of blocks b is greater or equal than the number of points v.*

Proof. Let $(V, \mathcal{B})$ be a design and let M be the incidence matrix of $(V, \mathcal{B})$. We consider the matrix $N = MM^T$, that is a $v \times v$ matrix. Set $N = (n_{i,j})$, because of properties 2 and 3 enumerated above, we have:

$$n_{i,j} = \sum_{h=1}^{b} m_{i,h} m_{j,h} = \begin{cases} r \text{ if } i = j; \\ \lambda \text{ if } i \neq j. \end{cases}$$

Since $r = \frac{\lambda(v-1)}{k-1} \neq \lambda$ we have $det(N) \neq 0$ and hence $rank(N) = v$. On the other hand

$$rank(MM^T) \leq rank(M) \leq b.$$

It follows that $v \leq b$. □

Definition 1.1.10. *In case the number of blocks b of a 2-(v, k, λ) design equals the number of points v the design is called symmetric.*

The conditions of Corollary 1.1.7 and the one of Theorem 1.1.9 are not, in general, also sufficient conditions for the existence of a 2-(v, k, λ) design: the smallest counterexample is given by the nonexistence of a 2-$(36, 6, 1)$ design. Therefore one of the main problems about such designs is now to see for which values of (v, k, λ) those conditions are sufficient. A remarkable result is due to R.M. Wilson (see [62], 1972). He proved that, if v is big enough, then there exists a 2-(v, k, λ) design for all parameters that satisfy the conditions of Corollary 1.1.7 and the one of Theorem 1.1.9: therefore those conditions are asymptotically sufficient. Another big progress was done by H. Hanani (see [44], 1975) who solved the case in which the blocks have size less or equal than 5: also in this case the conditions of Corollary 1.1.7 and the one of Theorem 1.1.9 are sufficient. However, despite the fact that many authors worked on the case $6 \leq k \leq 9$, see for instance [1, 2, 31, 42] and [43], there are still many open cases and little is known when $k > 9$. We recall some of these results in the following tables. For an exhaustive treatment of the topic we refer to [38].

Table 1.1.11. *In the following table we give a partial summary of known results.*

Values for which a 2-(v, k, λ) design could exist	*Exceptions*	*Biggest open case*
$(v, k, 1) : v \equiv 1, k \pmod{k(k-1)}$ $k \in \{3, 4, 5\}$		
$(v, 6, 1) : \ v \equiv 1, 6 \pmod{15}$	$16, 21, 36, 46$	801
$(v, 7, 1) : \ v \equiv 1, 7 \pmod{42}$	43	2605
$(v, 7, 2) : \ v \equiv 1, 7 \pmod{21}$	22	994
$(v, 8, 1) : \ v \equiv 1, 8 \pmod{56}$		3753
$(v, 9, 1) : \ v \equiv 1, 9 \pmod{72}$		16497
$(v, 9, 2) : \ v \equiv 1, 9 \pmod{36}$		1845
$(v, 9, 4) : \ v \equiv 1, 9 \pmod{18}$		783.

Table 1.1.12. *Values of v for which existence of a 2-$(v, 6, 1)$ design remains undecided:*

$51, 61, 81, 166, 226, 231, 256, 261, 286, 316, 321$
$346, 351, 376, 406, 411, 436, 441, 471, 501, 561, 591$
$616, 646, 651, 676, 771, 796, 801.$

Table 1.1.13. *Values of t for which existence of a 2-$(42t + 1, 7, 1)$ design remains undecided:*

$2, 3, 5, 6, 12, 14, 17, 19, 22, 27, 33, 37, 39, 42, 47, 59, 62.$

Table 1.1.14. *Values of t for which existence of a 2-$(42t + 7, 7, 1)$ design remains undecided:*

$3, 19, 34, 39.$

Table 1.1.15. *Values of v for which existence of a 2-$(v, 7, 2)$ design remains undecided:*

$274, 358, 574, 694, 988, 994.$

Table 1.1.16. *Values of t for which existence of a 2-$(56t+1, 8, 1)$ design remains undecided:*

$2, 3, 4, 5, 6, 7, 14, 19, 20, 21, 22, 24, 25, 26$
$27, 28, 31, 32, 34, 35, 39, 40, 46, 52, 59, 61, 62, 67.$

Table 1.1.17. *Values of t for which existence of a 2-$(56t+8, 8, 1)$ design remains undecided:*

$3, 11, 13, 20, 22, 23, 25, 26, 27, 28.$

Table 1.1.18. *Values of t for which existence of a 2-$(72t+1, 9, 1)$ design remains undecided:*

$2, 3, 4, 5, 7, 11, 12, 15, 20, 21, 22, 24, 27, 31$
$32, 34, 37, 38, 40, 42, 43, 45, 47, 50, 52, 53, 56, 60$
$61, 62, 67, 68, 75, 76, 84, 92, 94, 96, 102, 132, 174, 191$
$194, 196, 201, 204, 209.$

Table 1.1.19. *Values of t for which existence of a 2-$(72t+9, 9, 1)$ design remains undecided:*

$2, 3, 4, 5, 12, 13, 14, 18, 22, 23, 25, 26, 27, 28, 31$
$33, 34, 38, 40, 41, 43, 46, 47, 52, 59, 61, 62, 67, 68, 76$
$85, 93, 94, 102, 103, 139, 148, 174, 183, 192, 202, 203, 209, 229.$

Table 1.1.20. *Values of v for which existence of a 2-$(v, 9, 2)$ design remains undecided:*

$189, 253, 505, 765, 837, 1197, 1837, 1845.$

Table 1.1.21. *Values of v for which existence of a 2-$(v, 9, 4)$ design remains undecided:*

$315, 459, 783.$

1.1.2 Resolvable 2-designs

We define the following important class of 2-(v, k, λ) designs:

Definition 1.1.22. *Suppose $(V, \mathcal{B})$ is a 2-(v, k, λ) design. A parallel class in $(V, \mathcal{B})$ is a subset of disjoint blocks from $\mathcal{B}$ whose union is V. A partition of $\mathcal{B}$ into r parallel classes is called a resolution of $\mathcal{B}$. A 2-design, $(V, \mathcal{B})$ is said to be resolvable (or a RBIBD) if $\mathcal{B}$ has at least one resolution.*

An interesting class of examples of resolvable designs is provided by the affine planes.

Example 1.1.23 (Affine planes over the fields $\mathbb{F}_q$)**.** *Let us consider the set of points given by $V := \mathbb{F}_q^2$ and the set of blocks $\mathcal{B}$ (called also lines) given by the blocks of the form $B_{a,b} := \{(x, ax+b) : \ x \in \mathbb{F}_q\}$ where $a, b \in \mathbb{F}_q$ and by the ones of the form $B_c := \{(c, x) : \ x \in \mathbb{F}_q\}$ where $c \in \mathbb{F}_q$. Then the pair $(V, \mathcal{B})$ is a resolvable 2-$(q^2, q, 1)$ design.*

In the case of resolvable designs we can give the following necessary conditions for the existence:

Theorem 1.1.24. *If a resolvable* 2-(v, k, λ) *design exists, then* $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ *and* $v \equiv 0 \pmod{k}$.

Proof. Observe that a parallel class contains $\frac{v}{k}$ blocks and therefore a design can have a parallel class only if $v \equiv 0 \pmod{k}$. Then, because of Corollary 1.1.7, the claim follows. □

As in the general case, even here there are still many cases for which the existence problem remains open. The following table reports some of the known results about the existence of a resolvable 2-(v, k, λ) design for small values of k. For an exhaustive treatment of the topic we refer to [38].

Table 1.1.25. *In the following table we give a partial summary of known results.*

Values for which a resolvable 2-(v, k, λ) *design could exist*	*Exceptions*	*Largest open case*
$k \in \{3, 4\}$, (v, k, λ) : $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ *and* $v \equiv 0 \pmod{k}$	$(6, 3, 2)$	
$(v, 5, 1), v \equiv 5 \pmod{20}$		645
$(v, 5, 2), v \equiv 5 \pmod{10}$	$(15, 5, 2)$	395
$(v, 5, 4), v \equiv 0 \pmod{5}$	$(10, 5, 4)$, $(15, 5, 4)$	195
$(v, 6, 5), v \equiv 0 \pmod{6}$		*none*
$(v, 7, 1), v \equiv 7 \pmod{42}$		294427
$(v, 7, 6), v \equiv 0 \pmod{7}$		462
$(v, 8, 1), v \equiv 8 \pmod{56}$		24480
$(v, 8, 7), v \equiv 0 \pmod{8}$		1488.

1.1.3 Some generalizations

In this paragraph we define three generalizations of 2-designs. The first generalization explains the role of the number 2 in the definition.

Definition 1.1.26. *Let* v, k *and* λ *be positive integers such that* $v > k \geq t$. *A* t-(v, k, λ) *designs is a pair* $(V, \mathcal{B})$ *where* V *is a set of* v *elements (called points) and* $\mathcal{B} = [B_1, \ldots, B_b]$ *is a collection of subsets, called blocks, of* V *such that:*

1 every block contains exactly k *points;*

2 every set of t *distinct points of* V *is contained in exactly* λ *blocks.*

Of course, when t equals 2 we are in the case of 2-designs. The case in which $\lambda = 1$ is of particular interest: such designs are called also Steiner systems. We refer to [38] for a list of classical results related to this topic. A very important result has been recently obtained by P. Keevash (see [45], 2014) who establishes the existence of infinitely many t-$(v, k, 1)$ designs for all $t \geq 2$.

Now we define other two generalizations that we will use in the rest of this work.

Definition 1.1.27. *Let K be a subset of positive integers and let λ be a positive integer. A pairwise balanced design, $PBD(v, K, \lambda)$, with block sizes from K is a pair $(V, \mathcal{B})$ where V is a finite set of cardinality v and $\mathcal{B}$ is a family of subset (blocks) of V that satisfies:*

- *if $B \in \mathcal{B}$ then $|B| \in K$ and*
- *every pair of distinct elements (points) of V occurs in exactly λ blocks of $\mathcal{B}$.*

The integer λ is the index of the PBD. The notation $PBD(v, K)$ is used when $\lambda = 1$.

It is easy to see that, when all blocks have the same size k (i.e. $K = \{k\}$), we are in the case of 2-designs.

The following class of designs is a generalization both of 2-designs and of pairwise balanced designs:

Definition 1.1.28. *Let K and G be sets of positive integers and let λ be a positive integer. A group divisible design (GDD) of index λ and order v is a triple $(V, \mathcal{G}, \mathfrak{B})$, where V is a finite set of cardinality v, $\mathcal{G}$ is a partition of V into at least two parts (groups) whose sizes lie in G, and $\mathfrak{B}$ is a family of subsets (blocks) of V that satisfies:*

1) *if $B \in \mathfrak{B}$ then $|B| \in K$;*
2) *every pair of distinct elements of V occurs in exactly λ blocks or in one group, but not both.*

If $v = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s$, and if there are a_i groups of size $g_i, i = 1, 2, \ldots, s$, then the (K, λ)-GDD is of type $g_1^{a_1} g_2^{a_2} \ldots g_s^{a_s}$. The notation (k, λ)-GDD is used when $K = \{k\}$ and the notation k-GDD is used when $K = \{k\}$ and $\lambda = 1$.

When $G = \{1\}$ we obtain the case of paiwise balanced designs and, when $G = \{1\}$ and $K = \{k\}$, we obtain the case of 2-designs. It is worth recalling the definition of isomorphism between two group divisible designs.

Definition 1.1.29. *Two group divisible designs $(V, \mathcal{G}, \mathfrak{B})$ and $(V, \mathcal{G}', \mathfrak{B}')$ are isomorphic if there exists a bijection $\alpha : V \to V'$ mapping $\mathfrak{B}$ into $\mathfrak{B}'$ and $\mathcal{G}$ into $\mathcal{G}'$ or, in other words:*

$$[\{\alpha(x) : \ x \in B\} : B \in \mathfrak{B}] = \mathfrak{B}';$$

$$[\{\alpha(x) : \ x \in G\} : G \in \mathcal{G}] = \mathcal{G}'.$$

The bijection α is called an isomorphism. If $(V, \mathcal{G}, \mathfrak{B}) = (V, \mathcal{G}', \mathfrak{B}')$ the map α is called an automorphism of $(V, \mathcal{G}, \mathfrak{B})$. We denote with $Aut(V, \mathcal{G}, \mathfrak{B})$ the set of all automorphisms of $(V, \mathcal{G}, \mathfrak{B})$.

A relevant application of GDDs is given by the following remark:

Remark 1.1.30. *Let us suppose there exists a (k, λ)-GDD of type n^m and there exists a 2-(n, k, λ) design then we have a 2-(nm, k, λ) design.*

Similarly if there exists a (k, λ)-GDD of type n^m and there exists a 2-$(n+1, k, \lambda)$ design then we have a 2-$(nm + 1, k, \lambda)$ design.

Proof. For the first part of this remark it is sufficient to cover each group of the GDD with a copy of the 2-(n, k, λ) design. The result is a 2-(nm, k, λ) design.

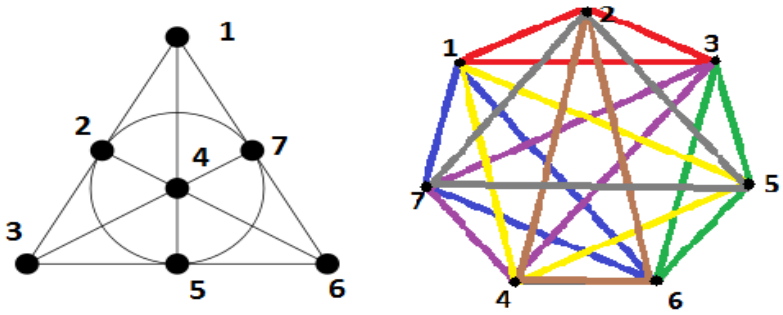
For the second part of this remark we add a point p to the set of points V of the GDD. Then, for each group $G \in \mathcal{G}$, we cover the set $G \cup \{p\}$ with a copy of the 2-$(n+1, k, \lambda)$ design. The result is a 2-$(nm+1, k, \lambda)$ design. □

Also in the cases of group divisible designs and pairwise balanced designs the most interesting problem is the existence question: we refer to [38] for a comprehensive list of the known results and open questions related to these topics.

1.2 k-cycle decompositions

Other combinatorial objects that are strictly related with 2-designs are the *decompositions* of a graph. In this contest we define a graph Γ as a pair $(V(\Gamma), E(\Gamma))$ where $V(\Gamma)$ is a set of *points* and $E(\Gamma)$ is a set of *edges* (unordered pairs of points). However sometime it is useful to consider also repeated edges: in this case we speak of *multigraphs* and $E(\Gamma)$ is a *family of edges*.

The link with 2-designs is given by the fact that a 2-$(v, k, 1)$ design can be seen as a complete graph $\mathbb{K}_v$ (that is the graph on v vertices with all the possible edges) which is decomposed into copies of complete graphs $\mathbb{K}_k$. In the following picture, for example, we can see the Fano plane, that is a 2-$(7, 3, 1)$ design, as a decomposition of $\mathbb{K}_7$ into copies of $\mathbb{K}_3$.



The formal definition of a *decomposition of a graph* Γ into subgraphs $\Lambda_1, \ldots, \Lambda_n$ is the following one:

Definition 1.2.1. *Let us consider a graph Γ and a set $\mathfrak{C} = \{\Lambda_1, \ldots, \Lambda_n\}$ of subgraphs of Γ whose edges partition $E(\Gamma)$. Then the set $\mathfrak{C}$ is called a decomposition of the graph Γ and the pair $(\Gamma, \mathfrak{C})$ is called a $(\Gamma, \mathfrak{C})$-design.*

Of course we can give the same definition also for the decompositions of a multigraph Γ into a family $\mathfrak{C} = [\Lambda_1, \ldots, \Lambda_n]$ of its sub-multigraphs. Note that, in this case, we can have repetition of elements in $\mathfrak{C}$ and hence $\mathfrak{C}$ is not, in general, a simple set. Also in these cases the fundamental question is the existence question. Does a decomposition of a specified type exist?

In the case of the $(\Gamma, \mathfrak{C})$-designs, an *isomorphism* α has to preserve the structure of the decomposition, more precisely:

Definition 1.2.2. *We say that a* $(\Gamma, \mathfrak{C})$*-design and a* $(\Gamma', \mathfrak{C}')$*-design are isomorphic if there exists a bijection* $\alpha : V(\Gamma) \to V(\Gamma')$ *such that:*

- $\alpha : V(\Gamma) \to V(\Gamma')$ *is an isomorphism between the graphs* Γ *and* Γ'*. This means that* $\alpha(V(\Gamma)) = V(\Gamma')$ *and* $\alpha(E(\Gamma)) = \{(\alpha(x), \alpha(y)) : \ (x, y) \in E(\Gamma)\} = E(\Gamma')$
- *Denoted with* $\alpha(\Lambda_i)$ *the graph with vertices* $\alpha(V(\Lambda_i))$ *and edges* $\alpha(E(\Lambda_i))$*, we have:*

$$[\alpha(\Lambda_i) : \Lambda_i \in \mathfrak{C}] = \mathfrak{C}'.$$

The bijection α *is called an isomorphism between the designs* $(\Gamma, \mathfrak{C})$ *and* $(\Gamma', \mathfrak{C}')$*. If* $(\Gamma, \mathfrak{C}) = (\Gamma', \mathfrak{C}')$ *the map* α *is called an automorphism of* $(\Gamma, \mathfrak{C})$*. We denote with* $Aut((\Gamma, \mathfrak{C}))$ *the set of all automorphisms of* $(\Gamma, \mathfrak{C})$*.*

We will call a decomposition $\mathfrak{C}$ *of* Γ *regular if it admits an automorphism group acting regularly, namely sharply transitively, on the vertex-set.*

In the case that $\mathfrak{C}$ is a set of subgraphs of Γ all isomorphic to a given graph Λ we use the notation of (Γ, Λ)-design. Similarly, in the case that $\mathfrak{C}$ consists of cycles of length k (or briefly k-cycles), we say that $\mathfrak{C}$ is a k-cycle decomposition of Γ or a (Γ, C_k)-design. Moreover, if Γ is the complete graph on v vertices $\mathbb{K}_v$, we say that $\mathfrak{C}$ is a k-cycle system.

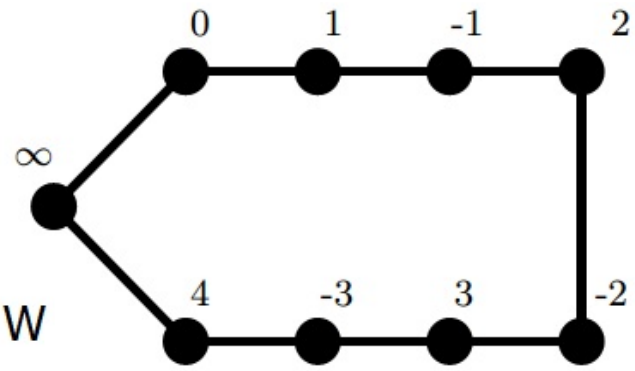
The latter case is of particular relevance and its existence problem has been completely solved. We first see the solution of this problem in the special case where the length of the cycles, denoted by k, equals the number of vertices of $\mathbb{K}_v$, i.e. $k = v$ and hence the cycles are Hamiltonian. In this case the v-cycle system is said Hamiltonian or briefly a $HCS(v)$ and the following theorem holds:

Theorem 1.2.3 (Walecki, 1890)**.** *There exists a* $HCS(v)$ *if and only if* $v \geq 3$ *is an odd integer.*

Proof. Let us suppose there exists a $HCS(v)$, $\mathfrak{C}$. Then, given $C \in \mathfrak{C}$ and $x \in V(\mathbb{K}_v)$, we have that x appears in two edges of C. Therefore the degree of x in $\mathbb{K}_v$ is even. Since the degree of x is $v - 1$ we have that v is an odd integer.

Let $v = 2n + 1$. Then we identify the vertices of $\mathbb{K}_v$ with the set $(\infty, 1 - n, \ldots, 0, \ldots, n)$. We consider the following cycle:

$$W := (\infty, 0, 1, -1, 2, -2, \ldots, i, -i, \ldots, n - 1, 1 - n, n).$$



The cycle W has the property that the differences between adjacent vertices (different from ∞) cover $\mathbb{Z}_{2n}$ twice.

We define an action of $\mathbb{Z}_{v-1} = \mathbb{Z}_{2n}$ on W in the following way: $t \to W_t$ where

$$W_t := (\infty, 0+t, 1+t, -1+t, 2+t, -2+t, \ldots, i+t, -i+t, \ldots, n-1+t, 1-n+t, n+t),$$

and the sums are in $\mathbb{Z}_{2n}$.

Let us consider the set of cycles $\mathfrak{C} := \{W, W_1, \ldots, W_{n-1}\}$. We want to prove that $\mathfrak{C}$ is a Hamiltonian decomposition of $\mathbb{K}_v$.

First of all we prove that, given two cycles $W_t, W_{t'}$ of $\mathfrak{C}$, the intersection of their edges is empty. In fact, by contradiction, let us suppose that the edge $e = \{x, y\}$ lies both in W_t and in $W_{t'}$.

The edges through ∞ of W_t are $\{\infty, t\}$ and $\{\infty, n+t\}$ while the edges through ∞ of W_t are $\{\infty, t'\}$ and $\{\infty, n+t'\}$. We have that $t \neq t'$ and, since $0 \leq t, t' \leq n-1$, we have also that $t \neq n + t'$. Therefore $\infty \notin e$. Then we have that $x = x_0 + t$, $y = y_0 + t$ and $x = x_1 + t'$, $y = y_1 + t'$ where the pairs $\{x_0, y_0\}$ and $\{x_1, y_1\}$ are adjacent in W and where $x - y = x_0 - y_0 = x_1 - y_1$. Because of the definition of W we have that $x_0 - y_0 = x_1 - y_1$ just in the following two cases:

- $x_0 = x_1$ and $y_0 = y_1$ or,
- $x_0 = n + x_1$ and $y_0 = n + y_1$.

Since $t \neq t'$ we have that $x_0 \neq x_1$ and hence $x_0 = n + x_1$ and $y_0 = n + y_1$. Thus we have $x = x_0 + t = (n + x_1) + t = x_1 + t'$. It follows that $t' = n + t$ but this is a contradiction because $t, t' \in \{0, \ldots, n-1\}$.

Therefore the edges of the cycles $W, W_1, \ldots, W_{n-1}$ are all distinct. Since these edges are $n(2n+1)$ that is the number of edges of $\mathbb{K}_v$ we have that $\mathfrak{C}$ is a Hamiltonian decomposition of $\mathbb{K}_v$. □

The action of $\mathbb{Z}_{2n}$ defined in this proof is called 1-*rotational* because it fixes one point and acts transitively on the others.

In regard to the general case, we can easily state the following necessary conditions for the existence of a k-cycle system of $\mathbb{K}_v$:

Proposition 1.2.4. *Let k be an integer $3 \leq k \leq v$, then, if the graph $\mathbb{K}_v$ has a k-cycle decomposition, it follows that v is odd and $|E(\mathbb{K}_v)| \equiv 0 \pmod{k}$.*

Proof. Let us consider a k-cycle decomposition $\mathfrak{C}$ of $\mathbb{K}_v$, a cycle $C \in \mathfrak{C}$ and a vertex $x \in \mathbb{K}_v$. We have that x is incident with either two or zero edges of C. Since each edge through x lies in exactly one cycle we have that the degree of x is even. Because the degree of $\mathbb{K}_v$ is $v - 1$ we have that v is odd.

The edges of $E(\mathbb{K}_v)$ are partitioned by the edges of the cycles of $\mathfrak{C}$. Since each cycle has k edges, it follows that $|E(\mathbb{K}_v)| \equiv 0 \pmod{k}$. □

It has been recently shown that these conditions are also sufficient. In fact the problem of existence of a k-cycle decomposition of the complete graph $\mathbb{K}_v$ has been solved by B. Alspach, H. Gavlas (see [8], 2001) and by M. Sajna (see [57], 2002, see also M. Buratti [17], 2003):

Theorem 1.2.5. *Let k be an integer $3 \leq k \leq v$, then the graph $\mathbb{K}_v$ has a k-cycle decomposition if and only if v is odd and $|E(\mathbb{K}_v)| \equiv 0 \pmod{k}$.*

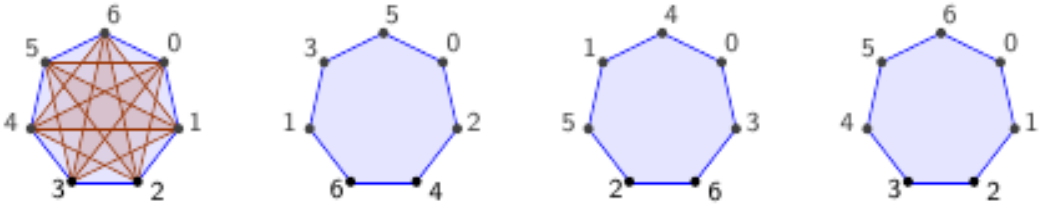
1.2.1 Perfect decompositions

In this paragraph we consider a particular type of k-cycle decompositions that are the *i-perfect k-cycle decompositions*. First of all we need to introduce some notation: given two vertices x and y of a graph Γ the *distance* between x and y is the minimum length of the paths connecting them.

Definition 1.2.6. *A k-cycle decomposition $\mathfrak{C}$ of Γ is called i-perfect if for any pair x, y of vertices there is exactly one cycle of $\mathfrak{C}$ in which x and y have distance i.*

Cycle decompositions of the complete graph $\mathbb{K}_v$, which are 2-perfect or 3-perfect are a well-studied topic, see for instance [4, 5, 30, 46, 48, 49, 50]. Larger values of i are considered in [6] where, however, the length k of the cycles does not exceed 19.

The following is an example of 2- and 3-perfect decomposition of $\mathbb{K}_7$:



The following proposition generalizes the previous example:

Proposition 1.2.7. *Let v be an odd prime and let $i \leq \frac{v-1}{2}$ be an integer. Then there exists an i-perfect $HCS(v)$.*

Proof. We identify the vertices of $\mathbb{K}_v$ with the set $\{1, \ldots, v\}$. Let us consider the set of cycles $\mathfrak{C} := \{C_j : j \in [1, \frac{v-1}{2}]\}$ where:

$$C_j := (0, j \pmod v, 2j \pmod v, \ldots, (v-1)j \pmod v).$$

Then, in the cycle C_j, the pairs of vertices at distance i have difference $\pm ji \pmod v$. Given two vertices x and y and an integer $i \in [1, \frac{v-1}{2}]$, there exists only one $j \in [1, \frac{v-1}{2}]$ such that $x - y = \pm ji \pmod v$. This means that $\mathfrak{C}$ is a Hamiltonian i-perfect decomposition of $\mathbb{K}_v$. □

In [48] C.C. Lindner, K.T. Phelps, and C.A. Rodger introduced the idea of 2-perfect cycle systems in order to give a construction of quasi-groups. A quasi-group is a pair $(Q, \star)$, where Q is a set and $\star$ is a binary operation of Q such that, for all a and b in Q there exist a unique element x and a unique element y that satisfy the following equations:

- $a \star x = b$;
- $y \star a = b$.

Their construction is the following:

Theorem 1.2.8. *Let $\mathfrak{C}$ be a 2-perfect k-cycle decomposition of $\mathbb{K}_v$. Then, given x and y in $\mathbb{K}_v$, there exists only one $C \in \mathfrak{C}$ such that x is adjacent to y i.e:*

$$C = (x, y, v_3, \ldots, v_k).$$

Then we define $x \star y = v_3$. We have that the pair $(V(\mathbb{K}_v), \star)$ is a quasi-group.

Proof. Let us consider $a, b \in Q$.

Because $\mathfrak{C}$ is 2-perfect, there is a unique cycle $C = (a, x, b, \dots)$, $C \in \mathfrak{C}$ in which a and b have distance 2. It follows that there exists a unique x such that $a \star x = b$.

Because $\mathfrak{C}$ is a decomposition of $\mathbb{K}_v$, there is a unique cycle $C = (y, a, b, \dots)$, $C \in \mathfrak{C}$ in which a and b are adjacent. It follows that there exists a unique y such that $y \star a = b$. □

However the study of i-perfect k-cycle systems is also motivated by the fact that being i-perfect is a property that is invariant under isomorphism:

Theorem 1.2.9. *Let $\mathfrak{C}$ be an i-perfect k-cycle decomposition of Γ and let $\mathfrak{C}'$ be a k-cycle decomposition of Γ'. If $(\Gamma, \mathfrak{C})$ and $(\Gamma', \mathfrak{C}')$ are isomorphic, as designs, then $\mathfrak{C}'$ is also an i-perfect k-cycle decomposition of Γ'.*

Proof. Let α be an isomorphism between $(\Gamma, \mathfrak{C})$ and $(\Gamma', \mathfrak{C}')$. Then, given $x, y \in V(\Gamma')$, we consider the pair $(\alpha^{-1}(x), \alpha^{-1}(y))$ of vertices of Γ. There exists one and only one $C \in \mathfrak{C}$ such that $\alpha^{-1}(x)$ and $\alpha^{-1}(y)$ have distance i in C. Since the distance is an invariant under isomorphism, the cycles in which $\alpha^{-1}(x)$ and $\alpha^{-1}(y)$ have distance i are mapped onto the cycles in which x and y have distance i. It follows that there exists one and only one cycle $C' \in \mathfrak{C}'$ such that x and y have distance i in C'. □

In regard to the problem of existence of i-perfect k-cycle systems, the known necessary conditions are the ones given by Proposition 1.2.4. However these conditions are not, in general, also sufficient (see the exceptions of Table 1.2.10 below). The existence problem, in the cases in which k is small, was studied essentially by C.C. Lindner, C.A. Rodger and others (see [48, 49, 50]) for $i = 2$ and by P. Adams, D.E. Bryant and others (see [4, 5, 6]) for other values of i. Their results are the following:

Table 1.2.10. *If $k \leq 19$ there exists an i-perfect k-cycle decomposition of $\mathbb{K}_v$ for all odd v such that $\frac{v(v-1)}{2} \equiv 0 \pmod{k}$ up to the following exceptions ([6, 49]):*

k	*Exceptions* (v, i)	*Possible exceptions* (v, i)
5	$(15, 2)$	
6	$(9, 2)$	
$7, 8, 11$		
9	$(9, 2); (9, 4)$	$(45, 2); (45, 4)$
10		$(221, 2); (221, 4); (20t + 5, 2); (20t + 5, 4)$
$12, 16, 17$		
13		*see the table below*
14		$(309, 2); (477, 2); (28t + 21, 2) \dots (28t + 21, 6)$
15		*see the table below*
18		$(217, 4); (217, 6); (36t + 9, 2) \dots (36t + 9, 7)$
19		$(57, 2); (57, 9)$.

Values of i and v for which existence of an i-perfect 13-cycle decomposition of $\mathbb{K}_v$ remains undecided:

i	v
5	$183, 209, 235, 261, 287, 339, 391, 703, 807, 885, 963,$ $1015, 1119, 1197, 1431, 1639,$ $26t + 13$ *for* $t \geq 1$.

Values of i and v for which existence of an i-perfect 15-cycle decomposition of $\mathbb{K}_v$ remains undecided:

i	v
$2, 4, 5, 7$	$55,$
$3, 6$	$55, 30t + 21$ *for* $t \geq 2,$ $30t + 25$ *for* $t \geq 1$.

Another important result of existence has been obtained independently in [30] by M. Buratti, G. Rinaldi and T. Traetta and in [46] by K. Kobayashi, B. McKay, M. Mutoh, G. Nakamura and N. Nara. Before stating their result, we recall a proposition that gives a criterion to establish whether a given $(2n + 1)$-cycle with vertex set $\mathbb{Z}_{2n} \cup \{\infty\}$ generates a 3-perfect $HCS(2n + 1)$.

Proposition 1.2.11. *Let us consider $\mathbb{Z}_{2n}$ and let C be a cycle with vertex set $\mathbb{Z}_{2n} \cup \{\infty\}$. We denote by $\Delta_1 C = \cup_{\{x,y\} \in E(C)}[x-y]$ and by $\Delta_3 C = \cup_{\{x,y\} \in E(C^3)}[x-y]$ where C^3 is the graph with the same vertices as C and with edges the pairs of vertices at distance three in C.*

Then, if $C + n = C$ and both the lists $\Delta_1 C$ and $\Delta_3 C$ cover every non-zero element of $\mathbb{Z}_{2n}$, the set of distinct translates of C under the 1-rotational action (see Theorem 1.2.3) is an i-perfect $HCS(2n + 1)$.

We omit the proof of the previous proposition since it is very similar to that of Theorem 1.2.3. Now we are ready to state the result of [30] and [46]. In particular we follow the proof of [30].

Theorem 1.2.12 ([30] and [46])**.** *There exists a 3-perfect $HCS(k)$ whenever k is odd and $k \geq 7$.*

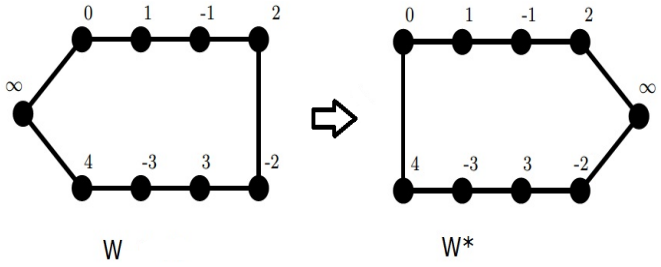
Proof. Let W^* be the cycle obtainable from the base cycle W of the $HCS(2n + 1)$ of Walecki (see Theorem 1.2.3) by joining the two neighbours 0 and n of ∞ and moving ∞ between the two endpoints $-\lfloor \frac{n}{2} \rfloor$ and $\lfloor \frac{n}{2} \rfloor$ of the edge which is opposite to ∞. Thus we have:

$$W^* = (0, 1, -1, 2, -2, \ldots, \frac{n}{2}, \infty, -\frac{n}{2}, \ldots, n-1, -(n-1), n)$$

or

$$W^* = (0, 1, -1, 2, -2, \ldots, \frac{n-1}{2}, \infty, -\frac{n-1}{2}, \ldots, n-1, -(n-1), n)$$

according to whether n is even or odd respectively. The figure below illustrates how to move from W to W^* when $n = 4$.



It is clear that W^* is fixed by adding n. It is also clear that the list $\Delta_1 W^*$ is obtainable from the list $\Delta_1 W$ by replacing the two differences $\pm(\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil)$ with the two differences $\pm(n-0)$. On the other hand the values of these differences coincide and are both n. Thus we have $\Delta_1 W^* = \Delta_1 W$. Since it is known that considering $\Delta_1 W$ we have $\Delta_1 W = \mathbb{Z}_{2n} \setminus \{0\}$ it follows that considering also $\Delta_1 W^*$ as a set we have that $\Delta_1 W^* = \mathbb{Z}_{2n} \setminus \{0\}$.

Now note that $\Delta_3 W^*$ can be seen as the list of all possible differences between the two endpoints of a subpath with four vertices of W^*. Among the 4-subpaths of W^* we have all those of the form $P_x = [x, -x, -x+1, -x-1]$ with $x \in \{1, \ldots, n-1\} \setminus X$ where $X = \{\frac{n}{2} - 1, \frac{n}{2}\}$ or $X = \frac{n-1}{2}$ according to whether n is even or odd. Hence, considering that the difference between the two endpoints x and $-x-1$ of P_x is $2x+1$ we obtain that $\Delta_3 W^*$ covers all odd elements of $\mathbb{Z}_{2n}$ with the only possible exceptions of ± 1 and $\pm(n-1)$ for n even and the only possible exceptions of ± 1 and $\pm n$ for n odd.

Among the 4-subpaths of W^* there are also those of the form $Q_y = [1-y, y, -y, y+1]$ with $y \in \{1, \ldots, n-1\} \setminus Y$ where $Y = \{\frac{n}{2}\}$ or $Y = \{\frac{n-1}{2}, \frac{n+1}{2}\}$ according to whether n is even or odd respectively. Hence, considering that the difference between the two endpoints $y+1$ and $1-y$ of Q_y is $2y$ we see that $\Delta_3 W^*$ covers all even elements of $\mathbb{Z}_{2n} \setminus \{0\}$ with the only possible exception of n in the case of n even, and the only possible exception of $\pm(n-1)$ in the case of n odd.

On the other hand, if we set

$$P_0 = [\frac{n}{2}, \infty, -\frac{n}{2}, \frac{n}{2}+1] \text{ or } P_0 = [\frac{n-1}{2}, \infty, -\frac{n-1}{2}, \frac{n+1}{2}],$$

according to whether n is even or odd we see that the endpoints have differences ± 1. We also see that

$$[n, 0, 1, -1] \text{ and } [1-n, n, 0, 1]$$

are 4-subpath of W^* whose endpoints have difference $\pm(n-1)$ and n respectively. We conclude that, in all cases, considering $\Delta_1 W^*$ as a set, we have $\Delta_3 W^* = \mathbb{Z}_{2n} \setminus \{0\}$. Thus the claim follows from Proposition 1.2.11. □

Chapter 2

Difference methods

2.1 Difference sets and difference families

The systematic use of *cyclic difference sets* and related methods for the construction of 2-designs dates back to R.C. Bose and his seminal paper of 1939. However, various examples appeared earlier than this such as those of R. Paley which date back to 1933 (see [55]). In this chapter we intend to describe such methods but first of all we need to introduce some notation.

Given a multiset X we denote by λX the disjoint union of λ copies of X. From now we will consider sets and multisets of elements of a finite group $(G, +)$, we write this group in additive form and we denote by 0 its identity element. Then, if X is a multiset of elements of $(G, +)$, for any $g \in G$, we define:

$$X + g := [x + g : \ x \in X].$$

Any multiset $X + g$ is called a *translate* of X. We note that if X is a simple set also $X + g$ is a simple set. Then we define:

$$Dev(X) := [X + g : \ g \in G].$$

$Dev(X)$ is called the *development* of X. Similarly, given a family of multisets of elements of G, say $\mathfrak{F} := [X_1, \ldots, X_l]$, we define:

$$Dev(\mathfrak{F}) := \bigcup_{i=1}^{l} Dev(X_i),$$

Also in this case, $Dev(\mathfrak{F})$ is called the *development* of the family $\mathfrak{F}$.

Given a set $D = \{d_1, \ldots, d_k\}$ of elements of G, we define the *difference table* of D as the matrix $M(D)$ whose element $m_{i,j}$ is $d_i - d_j$ if $i \neq j$ while it is the symbol $\bullet$ if $i = j$. Then we define the *list of differences* of the set D as the list ΔD of elements of the difference table of D that are not in the main diagonal. We can write this list as follows:

$$\Delta D = [d_i - d_j : \ i, j \in [1, k], i \neq j].$$

We note that, since for $i \neq j$ the elements d_i and d_j are different, 0 never belongs to ΔD.

Example 2.1.1. *Let us consider the group $\mathbb{Z}_7$ and the subset $D = \{1, 2, 4\}$ of $\mathbb{Z}_7$. Then the difference table of the set D is the matrix:*

$$M(D) := \begin{pmatrix} \bullet & 6 & 4 \\ 1 & \bullet & 5 \\ 3 & 2 & \bullet \end{pmatrix}.$$

Thus the list of differences of the set D is $\Delta D = [1, 2, 3, 4, 5, 6]$.

Similarly, given a multiset $X = [x_1, \ldots, x_k]$ of elements of G, we define the *difference table* of X as the matrix $M(X)$ whose element $m_{i,j}$ is $x_i - x_j$ if $i \neq j$ while it is the symbol $\bullet$ if $i = j$. Then we define *the list of differences* of the multiset X as the list $\Delta X := [x_i - x_j : \ i, j \in [1, k], i \neq j]$. In this case, since x_i can be equal to x_j for $i \neq j$, the element 0 is allowed to belong to ΔX.

Example 2.1.2. *Let us consider the group $\mathbb{Z}_7$ and the multiset $X = [0, 1, 2, 4, 1, 2, 4]$ of elements of $\mathbb{Z}_7$. Then the difference table of the set X is the matrix:*

$$M(X) := \begin{pmatrix} \bullet & 6 & 5 & 3 & 6 & 5 & 3 \\ 1 & \bullet & 6 & 4 & 0 & 6 & 4 \\ 2 & 1 & \bullet & 5 & 6 & 0 & 5 \\ 4 & 3 & 2 & \bullet & 3 & 2 & 0 \\ 1 & 0 & 1 & 4 & \bullet & 6 & 4 \\ 2 & 1 & 0 & 5 & 1 & \bullet & 5 \\ 6 & 3 & 2 & 0 & 3 & 2 & \bullet \end{pmatrix}.$$

Thus the list of differences of the multiset X is $\Delta X = 6[0, 1, 2, 3, 4, 5, 6]$.

Now we give the following definition:

Definition 2.1.3. *Suppose $(G, +)$ is a finite group of order v. Let k and λ be positive integers such that $2 \leq k < v$. A (v, k, λ)-difference set, or briefly DS, is a subset $D \subseteq G$ that satisfies the following properties:*

- *$|D| = k$.*
- *the list ΔD contains every element of $G \setminus \{0\}$ exactly λ.*

If the group G is the cyclic group $\mathbb{Z}_v$ the difference set D is called cyclic.

Example 2.1.4. *We consider the subset $D = \{1, 2, 4\}$ of $\mathbb{Z}_7$ of Example 2.1.1. We have seen that $\Delta D = [1, 2, 3, 4, 5, 6]$ and hence D is a cyclic $(7, 3, 1)$-difference set*

We note that, since the number of ordered pairs of D is $k(k-1)$ and each element of $G \setminus \{0\}$ appears as a difference λ times, we have:

$$\lambda(v - 1) = k(k - 1).$$

Here we illustrate the "Paley difference sets":

Theorem 2.1.5 (Paley difference sets)**.** *Let $q \equiv 3 \pmod 4$ be a prime power. In the additive group of $\mathbb{F}_q$, we consider the set D of all non-zero squares. Then D is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-difference set.*

Proof. Given a generator g of the multiplicative group of $\mathbb{F}_q$, we have that the non-zero squares are the elements of the form g^{2i} for $1 \leq i \leq \frac{q-1}{2}$. Therefore $|D| = \frac{q-1}{2}$. We need to prove that every non-zero element of $\mathbb{F}_q$ appears $\frac{q-3}{4}$ times as a difference of two elements in D.

For any $d \in \mathbb{F}_q \setminus \{0\}$, we define

$$a_d = |\{(x, y) : x, y \in D,\ x - y = d\}|.$$

Given $h \in \mathbb{F}_q \setminus \{0\}$, we have that $hx - hy = h(x - y)$, so the number of times that d appears as difference from D is the same as the number of times that hd appears as a difference from $hD = \{hx : x \in D\}$. Now if h is a square we have that $hD = D$ and hence $a_d = a_{hd}$ for all squares $h \in D$. Let now consider a non square $h \in \mathbb{F}_q \setminus \{0\}$. Since $q \equiv 3 \pmod 4$ we have that -1 is not a square in $\mathbb{F}_q$. It follows that $-h$ is a square in $\mathbb{F}_q$. Hence we have that $a_d = a_{-hd}$. Now, since $x - y = d$ if and only if $y - x = -d$, it is clear from the definition that:

$$a_d = |\{(x, y) : x, y \in D,\ x - y = d\}| = a_{-d} = |\{(y, x) : y, x \in D,\ y - x = -d\}|.$$

It follows that $a_d = a_{-hd} = a_{hd}$ also for the non square elements h. Thus a_d does not depend on d, namely a_d is a constant λ for all $d \in \mathbb{F}_q \setminus \{0\}$. We can compute λ from the equation $\lambda(v - 1) = k(k - 1)$, which gives $\lambda = \frac{q-3}{4}$ and hence the claim follows. □

We are now ready to illustrate the utility of difference sets in order to construct 2-designs.

Theorem 2.1.6. *Let D be a (v, k, λ)-difference set in the group $(G, +)$. Then $(G, Dev(D))$ is a symmetric 2-(v, k, λ) design.*

This theorem is a very classical result of R.C. Bose (see [14]) and we will give several generalizations of it. We will finally prove the more general result that is Theorem 2.1.23 and thus we omit the proofs of all the intermediate theorems. Here we give, as an example, an application of this theorem.

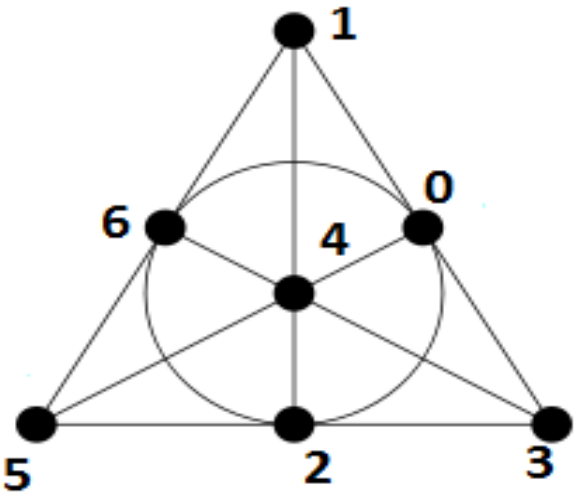
Example 2.1.7. *Let us consider the Paley difference set over $\mathbb{F}_7$ that is $D = \{1, 4, 2\}$. Then:*

$$Dev(D) := [\{1, 4, 2\} + g :\ g \in \mathbb{F}_7] = [\{1 + g, 4 + g, 2 + g\} :\ g \in \mathbb{F}_7].$$

It follows that:

$$Dev(D) = [\{1, 4, 2\}, \{2, 5, 3\}, \{3, 6, 4\}, \{4, 0, 5\}, \{5, 1, 6\}, \{6, 2, 0\}, \{0, 3, 1\}].$$

The pair $(\mathbb{F}_7, Dev(D))$ is a symmetric 2-$(7, 3, 1)$ design. Specifically it is the Fano plane (see also Example 1.1.3), and can be represented with the following picture:



Moreover, as we will see in Theorem 2.1.23, the 2-designs constructed from difference sets in the group G have the special property that their *automorphism group* contains a copy of the group G. More precisely:

Theorem 2.1.8. *Suppose $(G, Dev(D))$ is a 2-design constructed from a (v, k, λ)-difference set D in the group $(G, +)$. Then $Aut(G, Dev(D))$ contains a subgroup isomorphic to G that acts sharply transitively on the set of points.*

Now we give a generalization of Definition 2.1.3:

Definition 2.1.9. *Suppose $(G, +)$ is a finite group of order v. Let k and λ be positive integers such that $2 \leq k < v$. A (v, k, λ)-difference family in $(G, +)$ is a collection of subsets of G, say $\mathfrak{F} := [D_1, \ldots, D_l]$, such that the following properties are satisfied:*

- *$|D_i| = k$ for $1 \leq i \leq l$;*
- *The multiset union:*
$$\Delta\mathfrak{F} := \bigcup_{D \in \mathfrak{F}} \Delta D$$
contains every element in $G \setminus \{0\}$ exactly λ times.

Example 2.1.10. *We consider the family of subsets of $\mathbb{F}_{13}$ given by $\mathfrak{F} := [\{0, 1, 4\}, \{0, 2, 7\}]$. Then we have:*
$$\Delta\mathfrak{F} = \Delta\{0, 1, 4\} \cup \Delta\{0, 2, 7\},$$
where $\Delta\{0, 1, 4\} = \pm[1, 3, 4]$ and $\Delta\{0, 2, 7\} = \pm[2, 5, 7]$. Thus
$$\Delta\mathfrak{F} = \pm[1, 3, 4, 2, 5, 7] = \mathbb{F}_{13} \setminus \{0\}.$$
It follows that $\mathfrak{F}$ is a $(13, 3, 1)$-DF.

Here we give a first generalization of Theorem 2.1.6 to the case of difference families.

Theorem 2.1.11. *Suppose $\mathfrak{F} := [D_1, \ldots, D_l]$ is a (v, k, λ)-difference family in the group $(G, +)$. Then $(G, Dev(\mathfrak{F}))$ is a 2-(v, k, λ) design and $Aut(G, Dev(\mathfrak{F}))$ contains a group isomorphic to G that acts sharply transitively on the set of points.*

We will see that also this theorem is a special case of Theorem 2.1.23 and thus we omit its proof. However we try to explain this construction through an example.

Example 2.1.12. *We resume Example 2.1.10 where $\mathfrak{F} := [\{0, 1, 4\}, \{0, 2, 7\}]$. Here the development of $\mathfrak{F}$ is given by*

$$Dev(\mathfrak{F}) := [\{0, 1, 4\} + g : \ g \in \mathbb{F}_{13}] \cup [\{0, 2, 7\} + g : \ g \in \mathbb{F}_{13}].$$

Thus $Dev(\mathfrak{F})$ is given by the set of blocks:

$$\begin{array}{lll}
[\{0,1,4\}, & \{1,2,5\}, & \{2,3,6\}., \\
\{3,4,7\}, & \{4,5,8\}, & \{5,6,9\}, \\
\{6,7,10\}, & \{7,8,11\}, & \{8,9,12\}, \\
\{9,10,0\}, & \{10,11,1\}, & \{11,12,2\}, \\
\{12,0,3\}, & \{0,2,7\}, & \{1,3,8\}, \\
\{2,4,9\}, & \{3,5,10\}, & \{4,6,11\}, \\
\{5,7,12\}, & \{6,8,0\}, & \{7,9,1\}, \\
\{8,10,2\}, & \{9,11,3\}, & \{10,12,4\}, \\
\{11,0,5\}, & \{12,1,6\}]. &
\end{array}$$

Then the pair $(\mathbb{F}_{13}, Dev(\mathfrak{F}))$ is a 2-$(13, 3, 1)$ design.

2.1.1 Relative difference families

The concept of a "*relative difference family*" is a further generalization of the idea of "*difference family*". This concept, formally introduced by M. Buratti in [21] allows to achieve $GDDs$, 2-designs and other kind of combinatorial designs:

Definition 2.1.13. *Given an additive group G of order v and a subgroup H of G of order n, a (G, H, k, λ)-DF, or (v, n, k, λ)-DF over G and relative to H, is a family $\mathfrak{F} := [D_1, \ldots, D_l]$ of subsets of G of cardinality k such that the list*

$$\Delta\mathfrak{F} = \bigcup_{i=1}^{l} \Delta D_i$$

covers $G \setminus H$ exactly λ times while it does not contain any element of H.

If $l = 1$, i.e. the family $\mathfrak{F} = [D_1]$ is given by a single set, we say that the set D_1 is a (G, H, k, λ) relative difference set (see [56]).

Then it is immediate to note that, if $H = \{0\}$, we meet again the case of difference families.

Example 2.1.14. *Let us consider the set D of elements of $\mathbb{Z}_5 \times \mathbb{Z}_5$ defined by:*

$$D = \{(0, 0), (1, 1), (1, 4), (4, 2), (4, 3)\}.$$

We have that

$$\Delta D = \pm[(1,1),(1,4),(4,2),(4,3),(0,2),(2,4),(2,3),(2,2),(2,1),(0,4)].$$

Therefore $\Delta D = (\mathbb{Z}_5 \times \mathbb{Z}_5) \setminus (\mathbb{Z}_5 \times \{0\})$ *and hence* D *is a* $(\mathbb{Z}_5 \times \mathbb{Z}_5, \mathbb{Z}_5 \times \{0\}, 5, 1)$ *relative difference set.*

Example 2.1.15. *Let us consider the family of sets of elements of* $\mathbb{Z}_{21}$ *given by*

$$\mathfrak{F} := [\{0,1,3\},\{0,8,17\},\{0,10,15\}].$$

We have that

$$\Delta\mathfrak{F} = \Delta\{0,1,3\} \cup \Delta\{0,8,17\} \cup \Delta\{0,10,15\}$$

where:

$$\Delta\{0,1,3\} = \pm[1,3,2];$$

$$\Delta\{0,8,17\} = \pm[8,17,9];$$

$$\Delta\{0,10,15\} = \pm[10,15,5].$$

Therefore $\Delta\mathfrak{F} = \mathbb{Z}_{21}\setminus\{0,7,14\} = \mathbb{Z}_{21}\setminus\langle 7\rangle_{\mathbb{Z}_{21}}$ *and hence* $\mathfrak{F}$ *is a* $(\mathbb{Z}_{21}, \langle 7\rangle_{\mathbb{Z}_{21}}, 3, 1)$*-DF.*

Here we present a more elaborate example. This construction was found by M. Buratti in [23].

Example 2.1.16 (M. Buratti)**.** *Let us consider a prime* $p \equiv 1 \pmod 6$*. Then, denoted by* g *a primitive root of unity of* $\mathbb{Z}_p$*, we have that* $\epsilon = g^{\frac{p-1}{3}}$ *is a cube primitive root of unity of* $\mathbb{Z}_p$ *that is* $\epsilon^3 \equiv 1 \pmod p$ *and* $\epsilon \not\equiv 1 \pmod p$*. Since* $0 \equiv \epsilon^3 - 1 \equiv (\epsilon - 1)(\epsilon^2 + \epsilon + 1) \pmod p$*, it follows that* ϵ *satisfies the equation* $\epsilon^2 + \epsilon + 1 = 0$*.*

We consider the following subsets of $\mathbb{Z}_8 \times \mathbb{Z}_p$*:*

$$B_i = \{(0,0),(1,2\epsilon^i),(3,-\epsilon^{i+1}),(5,-\epsilon^i)\}\ i = 0,1,2$$
$$B_3 = \{(0,2),(0,2\epsilon),(0,2\epsilon^2),(1,0)\}.$$

Then the list $\bigcup_{i=0}^{3}\Delta B_i$ *can be written in the form* $\bigcup_{i=0}^{7}\{i\} \times L_i$ *where* $L_i = -L_{8-i}$ *and:*

$$L_0 = \pm 2[1-\epsilon, 1-\epsilon^2, \epsilon-\epsilon^2],$$
$$L_1 = 2[1, \epsilon, \epsilon^2, -1, -\epsilon, -\epsilon^2],$$
$$L_2 = [-2-\epsilon, -(2+\epsilon)\epsilon, -(2+\epsilon)\epsilon^2, -(1-\epsilon), -(1-\epsilon)\epsilon, -(1-\epsilon)\epsilon^2],$$
$$L_3 = [-\epsilon, -\epsilon^2, -\epsilon^3, 1, \epsilon, \epsilon^3],$$
$$L_4 = \pm[3, 3\epsilon, 3\epsilon^3].$$

Since $\epsilon^2 + \epsilon + 1 = 0$*, it follows that* $1 - \epsilon^2 = (1+\epsilon)(1-\epsilon) = (\epsilon-1)\epsilon^2$ *and* $-2 - \epsilon = \epsilon^2 - 1 = (\epsilon-1)(\epsilon+1) = (1-\epsilon)\epsilon^2$*. Thus we have:*

$$L_0 = \pm 2(\epsilon-1)[\epsilon, \epsilon^2, 1], \quad L_1 = \pm 2[\epsilon, \epsilon^2, 1],$$
$$L_2 = \pm(\epsilon-1)[\epsilon, \epsilon^2, 1], \quad L_3 = \pm[\epsilon, \epsilon^2, 1],$$
$$L_4 = \pm 3[\epsilon, \epsilon^2, 1], \quad L_5 = \pm[\epsilon, \epsilon^2, 1],$$
$$L_6 = \pm(\epsilon-1)[\epsilon, \epsilon^2, 1], \quad L_7 = \pm 2[\epsilon, \epsilon^2, 1].$$

Therefore, if S is a a complete system of representatives for the cosets of $\langle -\epsilon \rangle$ in $\mathbb{Z}_p^*$, we have that:

$$[L_i \cdot s|\ s \in S] = \mathbb{Z}_p \setminus \{0\}, \text{ for } 0 \leq i \leq 3.$$

It follows that:

$$\mathfrak{F} := [B_i \cdot (1, s)|\ 0 \leq i \leq 3; s \in S]$$

is a $(\mathbb{Z}_8 \times \mathbb{Z}_p, \mathbb{Z}_8 \times \{0\}, 4, 1)$-DF.

Now we give a further generalization of Theorem 2.1.6 to the case of relative difference families.

Theorem 2.1.17 ([21])**.** *A (G, H, k, λ)-DF yields a (k, λ)-GDD of type n^m, say $\mathcal{X}$, where $m = |G : H|$ and $n = |H|$. Moreover $Aut(\mathcal{X})$ contains a group isomorphic to $(G, +)$ that acts sharply transitively on the set of points of $\mathcal{X}$.*

Since also this theorem is a special case of Theorem 2.1.23 we omit its proof.

Remark 2.1.18. *Let G be a group of order v and let $\mathfrak{F} := [D_1, \ldots, D_l]$ be a (G, H, k, λ)-DF. In case H is $\{0\}$ we have that $\mathfrak{F}$ is a (v, k, λ)-DF. In this case $(G, \mathcal{G}, Dev(\mathfrak{F}))$ is a 2-(v, k, λ) design and Theorem 2.1.17 reduces to Theorem 2.1.11. Moreover, if we also have that $\mathfrak{F} = [D_1]$, the set D_1 is a (v, k, λ)-difference set and we obtain Theorem 2.1.6.*

Now we consider the graph $\mathbb{K}_n^{(m)}$, that is the complete m-partite graph with m parts of size n, see for instance [58] and [59]. Given an integer λ we define also the multigraph $\lambda\mathbb{K}_n^{(m)}$ whose vertices are the ones of $\mathbb{K}_n^{(m)}$ and whose edges consist of λ copies of the edges of $\mathbb{K}_n^{(m)}$.

We note that a (k, λ)-GDD of type n^m is equivalent to a $\mathbb{K}_k$-decomposition of $\lambda\mathbb{K}_n^{(m)}$. In fact, given a (k, λ)-GDD of type n^m $(V, \mathcal{G}, \mathfrak{B})$, we have that:

1) The graph with set of vertices V and whose edges are the pairs $\{x, y\}$ such that x and y are not in a same group of $\mathcal{G}$ is the complete m-partite graph $\lambda\mathbb{K}_n^{(m)}$.

2) Let us consider the set of graphs $\mathfrak{C} := \{\mathbb{K}^B :\ B \in \mathfrak{B}\}$ where $\mathbb{K}^B$ is the complete graph whose vertices are the k elements of B. Then $\mathfrak{C}$ is a decomposition of $\lambda\mathbb{K}_n^{(m)}$.

According to this link we want to extend the concept of a relative difference family to get Γ-decompositions of complete m-partite graphs. First of all we need to consider the following, more general, definition of relative difference families:

Definition 2.1.19 ([25])**.** *Let us consider an additive group G of order v, a subgroup H of G of order n and a graph Γ. A (G, H, Γ, λ)-DF, or (v, n, Γ, λ)-DF over G and relative to H, is a collection $\mathfrak{F}$ of injective maps from $V(\Gamma)$ to G such that the list*

$$\Delta_\Gamma\mathfrak{F} = \bigcup_{f \in \mathfrak{F}} [f(x) - f(y)|\{x, y\} \in E(\Gamma)]$$

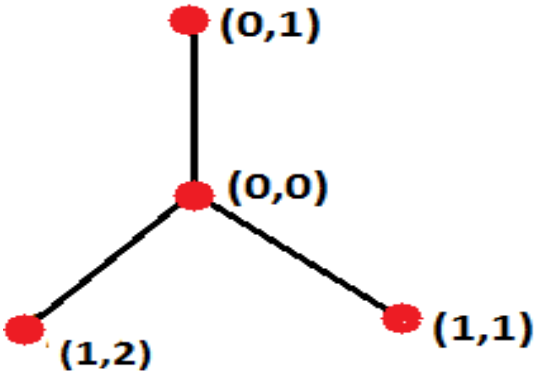
covers $G \setminus H$ exactly λ times while it does not contain any element of H.

If the family $\mathfrak{F} = [f]$ is given by a single map f, we say that f is a (G, H, Γ, λ) difference graph.

Example 2.1.20. *Let Γ be the graph with vertices $V(\Gamma) := \{v_1, v_2, v_3, v_4\}$ and edges $E(\Gamma) := \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}\}$. We consider the map $f : V(\Gamma) \to (\mathbb{Z}_3 \times \mathbb{Z}_3)$ such that:*

$$f(v_1) = (0,0);\ \ f(v_2) = (0,1);\ \ f(v_3) = (1,1);\ \ f(v_4) = (1,2).$$

We have that $\Delta_\Gamma f = [f(x) - f(y) | \{x, y\} \in E(\Gamma)] = \pm[(0,1), (1,1), (1,2)]$ and hence f is a $(\mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \{0\}, \Gamma, 1)$ difference graph. We can represent this example with the following picture:



Example 2.1.21. *Let Γ be the same graph of Example 2.1.20, whose vertices are $\{v_1, v_2, v_3, v_4\}$ and whose edges are $\{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}\}$. We consider the maps $f_1, f_2 : V(\Gamma) \to \mathbb{Z}_{15}$ such that:*

$$f_1(v_1) = 0;\ \ f_1(v_2) = 1;\ \ f_1(v_3) = 4;\ \ f_1(v_4) = 3;$$

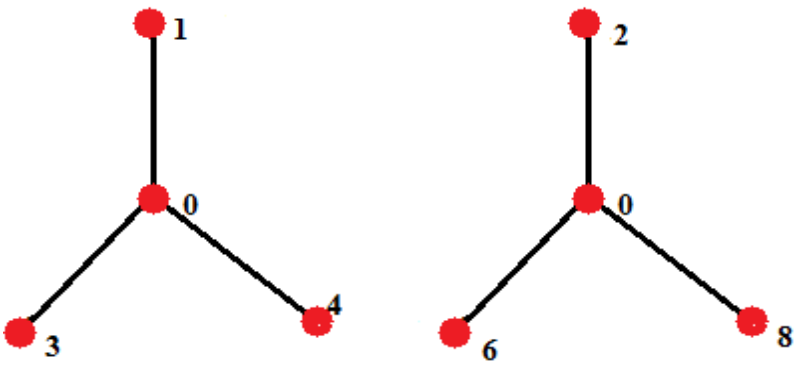
$$f_2(v_1) = 0;\ \ f_2(v_2) = 2;\ \ f_2(v_3) = 8;\ \ f_2(v_4) = 6.$$

We have that $\Delta_\Gamma \mathfrak{F} = [f_1(x) - f_1(y) | \{x, y\} \in E(\Gamma)] \cup [f_2(x) - f_2(y) | \{x, y\} \in E(\Gamma)]$ where

$$[f_1(x) - f_1(y) | \{x, y\} \in E(\Gamma)] = \pm[1, 4, 3];$$

$$[f_2(x) - f_2(y) | \{x, y\} \in E(\Gamma)] = \pm[2, 8, 6].$$

Therefore $\Delta_\Gamma \mathfrak{F} = \mathbb{Z}_{15} \setminus \{0, 5, 10\} = \mathbb{Z}_{15} \setminus \langle 5 \rangle_{\mathbb{Z}_{15}}$ and hence $\mathfrak{F}$ is a $(\mathbb{Z}_{15}, \langle 5 \rangle_{\mathbb{Z}_{15}}, \Gamma, 1)$ relative difference family. We can represent this example with the following pictures:



Remark 2.1.22. *Let us consider a $(G, H, \mathbb{K}_k, \lambda)$-DF, say $\mathfrak{F}$. Then, if we identify each map f of $\mathfrak{F}$ with its image $\{f(v)|\ v \in V(\mathbb{K}_k)\}$, we can see the family $\mathfrak{F}$ as a collection of subsets $[D_1, \ldots, D_l]$ of G such that each D_i has size k and*

$$\Delta\mathfrak{F} := \bigcup_{D\in\mathfrak{F}} [x - y : x, y \in D,\ x \neq y]$$

covers $G \setminus H$ exactly λ times while it does not contain any element of H. It follows that a $(G, H, \mathbb{K}_k, \lambda)$-DF is equivalent to a (G, H, k, λ)-DF.

Then, similarly to case of Theorem 2.1.17, the following theorem holds true:

Theorem 2.1.23 ([25])**.** *A (G, H, Γ, λ)-DF yields a regular Γ-decomposition of $\lambda\mathbb{K}_k^{(m)}$, where $m = |G : H|$ and $k = |H|$.*

Proof. Let $\mathfrak{F}$ be a (G, H, Γ, λ)-DF. We consider the graph $\mathbb{K}_{G:H}$ whose vertices are the elements of G and whose edges are the pairs of vertices $\{x, y\}$ such that x and y belong to different right cosets of H in G. Since this graph is a complete multipartite graph, we identify $\mathbb{K}_{G:H}$ with the complete m-partite graph $\mathbb{K}_n^{(m)}$ where $m = |G : H|$ and $n = |H|$. For each $f \in \mathfrak{F}$ and each $g \in G$, we define the graph $f(\Gamma) + g$ whose vertex set is $Im(f) + g \subseteq G$ and whose edge set is $\{\{f(x) + g, f(y) + g\} :\ \{x, y\} \in E(\Gamma)\}$. We denote by $\mathfrak{C}$ the family of all graphs $f(\Gamma) + g$ such that $f \in \mathfrak{F}$ and $g \in G$. Then we want to prove that $\mathfrak{C}$ is a regular Γ-decomposition of $\lambda\mathbb{K}_{G:H}$ or equivalently of $\lambda\mathbb{K}_n^{(m)}$.

Let x and y be two different elements of G. First of all we prove that, if x and y are in different right cosets of H in G, there are exactly λ graphs Λ of $\mathfrak{C}$ such that $\{x, y\} \in E(\Lambda)$. Denote $x - y = d$. Since $d \notin H$, there are exactly λ ordered triples (x', y', f) such that $x' - y' = d$ and $\{x', y'\} \in E(f(\Gamma))$ for some $f \in \mathfrak{F}$. Let these ordered triples be denoted by $(x_i, y_i, f_i),\ 1 \leq i \leq \lambda$. For $1 \leq i \leq \lambda$ we have the equality:

$$-x_i + x = -x_i + (x - y) + y = -x_i + (x_i - y_i) + y = -y_i + y.$$

Thus we define $g_i = -x_i + x = -y_i + y$. Then we have $\{x, y\} = \{x_i + g_i, y_i + g_i\} \in E(f_i(\Gamma) + g_i)$. It follows that there exist at least λ graphs Λ of $\mathfrak{C}$ such that $\{x, y\} \in E(\Lambda)$.

Conversely, suppose that $\{x, y\} \in E(f(\Gamma) + g)$ for some $f \in \mathfrak{F}$ and $g \in G$, then we have that $\{x, y\} = \{\bar{x} + g, \bar{y} + g\}$ where $\bar{x} - \bar{y} = x - y$ and $\{\bar{x}, \bar{y}\} \in E(f(\Gamma))$. It follows that $\bar{x} = x_i$ and $\bar{y} = y_i$ for some $1 \leq i \leq \lambda$. Thus there are exactly λ graphs Λ of $\mathfrak{C}$ such that $\{x, y\} \in E(\Lambda)$.

Now we consider x and y to be in the same right coset of H in G, i.e. $x - y \in H$. Let us suppose that $\{x, y\}$ belongs to $E(f(\Gamma) + g)$ for some $f \in \mathfrak{F}$ and $g \in G$. Then we have $\{x, y\} = \{\bar{x} + g, \bar{y} + g\}$ where $\bar{x} - \bar{y} = x - y$ and $\{\bar{x}, \bar{y}\} \in E(f(\Gamma))$. Thus $\bar{x} - \bar{y} \in H$ that is a contradiction since $\Delta\mathfrak{F}$ does not cover any element of H. Therefore the edge $\{x, y\}$ does not belong to any graph of $\mathfrak{C}$. Since every graph of $\mathfrak{C}$ is isomorphic to Γ, it follows that $\mathfrak{C}$ is a Γ-decomposition of $\lambda\mathbb{K}_n^{(m)}$.

Now, for every $g \in G$ we define the permutation $\tilde{g}$ of G as follows: $\tilde{g}(x) = x + g$ for all $x \in G$. We define $\tilde{G} = \{\tilde{g} : g \in G\}$. Then $(\tilde{G}, \circ)$, where the group operation $\circ$ denotes composition of permutations, is a permutation group isomorphic

to $(G,+)$ and it is known as the *permutation representation of* G. Moreover $(\tilde{G},\circ)$ is a subgroup of $Aut(\lambda\mathbb{K}_n^{(m)},\mathfrak{C})$. In order to prove this statement it is enough to observe that $\tilde{G}$ is an automorphism group of $\mathbb{K}_{G:H}$ and the action of this group maps graphs of $\mathfrak{C}$ into graphs of $\mathfrak{C}$. In fact given $\tilde{g}\in\tilde{G}$ and $f(\Gamma)+h\in\mathfrak{C}$ we have:

$$\tilde{g}(f(\Gamma)+h)=\{\tilde{g}(x):\ x\in f(\Gamma)+h\}=\{x+g:\ x\in f(\Gamma)+h\}=$$

$$=\{y+h+g:y\in f(\Gamma)\}=f(\Gamma)+h+g.$$

Similarly, given a right coset $H+h$ of H in G, we have:

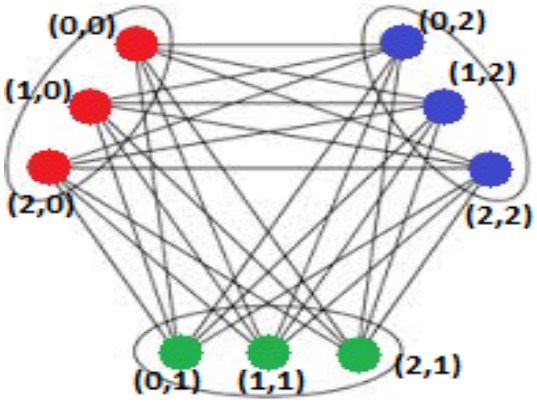
$$\tilde{g}(H+h)=\{\tilde{g}(x):\ x\in H+h\}=\{x+g:\ x\in H+h\}=$$

$$=\{y+h+g:y\in H\}=H+h+g.$$

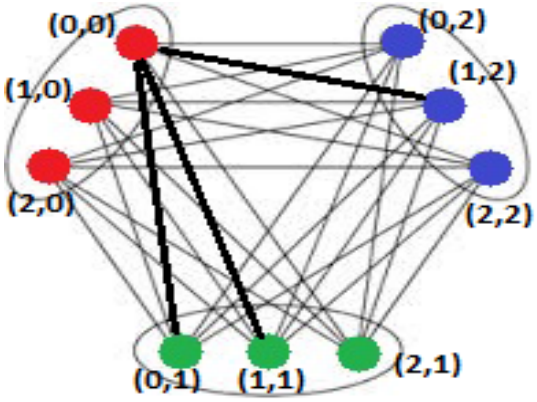
Since $f(\Gamma)+h+g\in\mathfrak{C}$ and $H+h+g$ is a right coset of H in G, each $\tilde{g}\in\tilde{G}$ is an automorphism of $\mathfrak{C}$ and hence $(\tilde{G},\circ)$ is a subgroup of $Aut(\lambda\mathbb{K}_n^{(m)},\mathfrak{C})$ that acts sharply transitively on the set of points. □

Remark 2.1.24. *According to Remark 2.1.22, in case* $\Gamma=\mathbb{K}_k$ *Theorem 2.1.23 reduces to Theorem 2.1.17. Therefore also Theorems 2.1.11, 2.1.8 and 2.1.6 are special cases of Theorem 2.1.23.*

In the proof of Theorem 2.1.23 the vertex set of $\mathbb{K}_n^{(m)}$ has been identified with G and its m parts with the right cosets of H. If we consider $G=\mathbb{Z}_3\times\mathbb{Z}_3$ and $H=\mathbb{Z}_3\times\{0\}$, as we have done in Example 2.1.20, we obtain the following representation of the complete 3-partite graph $\mathbb{K}_3^{(3)}$:



Then we can see the regular decomposition of the proof of Theorem 2.1.23 also in the following way. Let us consider a collection $\mathfrak{D}$ of subgraphs of $\mathbb{K}_n^{(m)}$ all isomorphic to a given graph Γ. In case of Example 2.1.20 the collection $\mathfrak{D}$ is given by the following graph:



We call *list of differences* of $\mathfrak{D}$ the multiset $\Delta\mathfrak{D}$ of all the differences $x-y$ with (x,y) an ordered pair of vertices which are adjacent in some graph of $\mathfrak{D}$. If we have $\Delta\mathfrak{D} = \lambda(G \setminus H)$, then the collection $\mathfrak{C}$ of all translates under the group G of all graphs of $\mathfrak{D}$ forms the desired regular decomposition of $\lambda\mathbb{K}_n^{(m)}$.

2.2 Strong difference families

In the nineties, several constructions of *relative difference families* were developed (see, for example, [9, 20, 43]). This idea allows to achieve a plethora of *GDD*s and, according to Remark 1.1.30, of 2-designs. Despite this fact, a systematic treatment of constructions of *DF*s has been performed only later. The concept of a *strong difference family* was introduced by M. Buratti in [22], in order to cover such problem, as follows:

Definition 2.2.1. *Let $\Sigma := [X_1, \dots, X_t]$ be a family of multisets of size k of an additive group G of order g.*
We say that Σ is a (G,k,μ) strong difference family (SDF), or a (g,k,μ)-SDF over to the group G, if the list

$$\Delta\Sigma = \bigcup_{X\in\Sigma} \Delta X,$$

covers all of G exactly μ times.

If $t=1$, i.e. the family $\Sigma = [X_1]$ is given by a single multiset, we say that the multiset X_1 is a (G,k,μ) strong difference multiset (SDM).

Example 2.2.2. *Let us consider the family of multisets of elements of $\mathbb{Z}_{15}$:*

$$\Sigma := [[0,0,5],[0,1,4],[0,2,8],[0,1,4],[0,2,8]].$$

Then

$$\Delta\Sigma = \Delta[0,0,5] \cup 2\Delta[0,1,4] \cup 2\Delta[0,2,8]$$

where

$$\Delta[0,0,5] = \pm[0,5,5];$$
$$\Delta[0,1,4] = \pm[1,3,4];$$
$$\Delta[0,2,8] = \pm[2,8,6].$$

Therefore $\Delta\Sigma = 2\mathbb{Z}_{15}$ and hence Σ is a $(\mathbb{Z}_{15},3,2)$ strong difference family.

This idea was generalized later by M. Buratti and L. Gionfriddo in a graph theoretic context (see [25]). We report here the more general definition that is the following:

Definition 2.2.3. *Let G be a group, Γ be a graph and let $\Sigma := [\sigma_1, \dots, \sigma_t]$ be a family of maps such that $\sigma_j : V(\Gamma) \to G$ for $j \in \{1, \dots, t\}$.*
We say that Σ is a (G, Γ, μ) strong difference family (SDF) if the list

$$\Delta_\Gamma \Sigma = \bigcup_{\sigma \in \Sigma} [\sigma(x) - \sigma(y) | \{x, y\} \in E(\Gamma)],$$

covers all of G exactly μ times.

If $t = 1$, i.e. the family $\Sigma = [\sigma_1]$ is given by a single map, we say that the map σ_1 is a (G, Γ, μ) strong difference map (SDM).

Remark 2.2.4. *Let us consider a $(G, \mathbb{K}_k, \mu)$-SDF, say Σ. We identify each map $\sigma \in \Sigma$ with its image $X = [\sigma(v) | v \in V(\mathbb{K}_k)]$. Then the list $[\sigma(x) - \sigma(y) | \{x, y\} \in E(\mathbb{K}_k)]$ is equal to the list ΔX. Thus we can see the family Σ as a collection of multisets $[X_1, \dots, X_t]$ of G such that each X_j has size k and the list*

$$\Delta \Sigma = \bigcup_{X \in \Sigma} \Delta X,$$

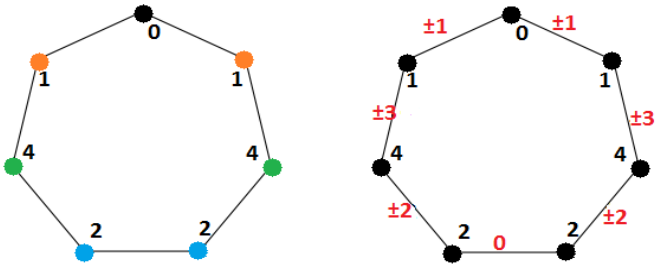
covers all of G exactly μ times. It follows that a $(G, \mathbb{K}_k, \mu)$-SDF is equivalent to a (G, k, μ)-SDF. Similarly a $(G, \mathbb{K}_k, \mu)$ strong difference map (or briefly SDM) is equivalent to a (G, k, μ) strong difference multiset (or briefly SDM).

We denote by C_k the k-cycle $(x_0, x_1, \dots, x_{k-1})$.

Example 2.2.5. *Let us consider the map $\sigma_7 : \ x_j \in C_7 \to j^2 \in \mathbb{Z}_7$. We have that:*

$$\Delta_{C_7} \sigma_7 = [\sigma_7(x) - \sigma_7(y) | \{x, y\} \in E(C_7)] = 2\mathbb{Z}_7.$$

Therefore the map σ_7 is a $(\mathbb{Z}_7, C_7, 2)$-SDM.



We can generalize this example and construct an infinite family of SDFs with the use of the Paley difference sets (see [55]):

Theorem 2.2.6 (Paley SDM)**.** *If k is odd the map $\sigma_k : \ x_j \in C_k \to j^2 \in \mathbb{Z}_k$ is a $(\mathbb{Z}_k, C_k, 2)$-SDM. Moreover, if k is an odd prime, $\sigma_k : \ x_j \in \mathbb{K}_k \to j^2 \in \mathbb{Z}_k$ is also a $(\mathbb{Z}_k, \mathbb{K}_k, k-1)$-SDM (or equivalently a $(\mathbb{Z}_k, k, k-1)$-SDM).*

Proof. It follows from the definition that the difference

$$\sigma_k(x_{i+1}) - \sigma_k(x_i) = (i+1)^2 - i^2 = 2i + 1.$$

Therefore, since k is odd, the list:

$$\Delta_{C_k}[\sigma_k] = \bigcup_{\{x,y\}\in E(C_k)} [\sigma_k(x) - \sigma_k(y)] = \bigcup_{i=0}^{k-1} \pm\{2i+1\} = 2(\mathbb{Z}_k \setminus \{0\}).$$

It follows that σ_k is a $(\mathbb{Z}_k, C_k, 2)$-SDM.

We can split the proof of the second point of the claim in two parts: when the prime $k \equiv -1 \pmod 4$ and when $k \equiv 1 \pmod 4$. In both cases, since the set D of the squares of $\mathbb{Z}_k$ has cardinality $\frac{k-1}{2}$, we have that 0 occurs $k-1$ times in the list of differences $\Delta_{\mathbb{K}_k}(\sigma_k)$. We have to show that each nonzero element of $\mathbb{Z}_k$ appears the same number of times in this list.

In case $k \equiv -1 \pmod 4$ because of Theorem 2.1.5, for all $d \in \mathbb{Z}_k \setminus \{0\}$, there are exactly $\frac{k-3}{4}$ representations of d as a difference from D. Each of them has to be counted four times in the number of representations of d as a difference from $\Delta_{\mathbb{K}_k}(\sigma_k)$. The remaining representations of d as a difference from $\Delta_{\mathbb{K}_k}(\sigma_k)$ are $d = d - 0$ that appears twice if d is a square, or $d = 0 - (-d)$ that appears twice if d is not a square. Therefore d appears $k-1$ times in $\Delta_{\mathbb{K}_k}(\sigma_k)$.

Now consider the case $k \equiv 1 \pmod 4$. Let $d \in D$. There are exactly $\frac{k-5}{4}$ representations of d as a difference from D (see [22]). Each of them has to be counted four times in the number of representations of d as a difference from $\Delta_{\mathbb{K}_k}(\sigma_k)$. The remaining representations of d as a difference from $\Delta_{\mathbb{K}_k}(\sigma_k)$ are $d = d - 0$ and $d = 0 - (-d)$ both present twice. Therefore d appears $k-1$ times as a difference in $\Delta_{\mathbb{K}_k}(\sigma_k)$. Let now $e \notin D$. Then there are exactly $\frac{k-1}{4}$ representations of e as a difference from D (see again [22]). Also here, each of them has to be counted four times in the number of representations of d as a difference from $\Delta_{\mathbb{K}_k}(\sigma_k)$. Then, since no difference from $\Delta_{\mathbb{K}_k}(\sigma_k)$ involving 0 gives e, we have that e appears $k-1$ times in $\Delta_{\mathbb{K}_k}(\sigma_k)$. □

This example has been implicitly used in [9] and [20] and will be studied in depth later in this thesis.

The following theorem motivates the study of SDFs over arbitrary graphs. First of all we need to introduce some notation. Given multisets S and L of elements of a finite ring R we denote by $S{\cdot}L$ the multiset on R defined by $S{\cdot}L = [s{\cdot}l | s \in S;\ l \in L]$. The group of units of R will be denoted, as usual, by $U(R)$.

Let us consider a multiset A whose elements belong to a cartesian product $G \times H$. Then we can write A, univocally, as union of multisets of the form $\{g\} \times L_g$ where $g \in G$ and the elements of L_g belong to H. For example if we consider the multiset $A = [(0,2),(0,1),(1,2),(0,1)]$ whose elements belong to $\mathbb{Z}_3 \times \mathbb{Z}_5$ then:

$$A = (\{0\} \times [2,1,2]) \cup (\{1\} \times [2]) \cup (\{2\} \times \emptyset).$$

Theorem 2.2.7 (The fundamental construction, M. Buratti, L. Gionfriddo, [25])**.** *Let Γ be a graph, let G be an additive group, and let R be a ring with additive group H. Given an n-tuple $(f_1, \ldots, f_n)$ of maps from $V(\Gamma)$ to $G \times H$ we set:*

$$f_i(x) = (\sigma_i(x), \tau_i(x))\ \forall x \in V(\Gamma),\ \forall i \in \{1, \ldots, n\};$$

$$\Delta_\Gamma[f_1,\dots,f_n]=\bigcup_{i=1}^{n}\bigcup_{\{x,y\}\in E(\Gamma)}[f_i(x)-f_i(y)];$$

as we have seen above there exist multisets L_g of elements of H such that:

$$\Delta_\Gamma[f_1,\dots,f_n]=\bigcup_{g\in G}\{g\}\times L_g.$$

Assume that the following conditions hold:

1) $\sigma_i(x)=\sigma_i(y)$ *with* $x\neq y \implies \tau_i(x)-\tau_i(y)\in U(R)$;

2) $\exists\ S\subset H\setminus\{0\}$ *such that* $S\cdot L_g=\lambda(H\setminus\{0\})\ \forall g\in G$.

Then there exists a $(G\times H, G\times\{0\},\Gamma,\lambda)$*-DF.*

Proof. For every pair $(i,s)\in\{1,\dots,n\}\times S$, we consider the map:

$$f_{i,s}: x\in V(\Gamma)\to(\sigma_i(x),s\cdot\tau_i(x))\in G\times H.$$

We claim that the family $\mathfrak{F}=[f_{i,s}|i=1,\dots,n;s\in S]$ is the required $(G\times H, G\times\{0\},\Gamma,\lambda)$-$DF$.

First of all each map $f_{i,s}$ is injective since if x and y are distinct vertices of $V(\Gamma)$ such that $f_{i,s}(x)=f_{i,s}(y)$ then we would have $(\sigma(x),s\cdot\tau_i(x))=(\sigma(y),s\cdot\tau_i(y))$ and hence $\sigma_i(x)=\sigma_i(y)$ and $s\cdot(\tau_i(x)-\tau_i(y))=0$ that is a contradiction in view of the condition (1).

Then note that for any fixed $s\in S$ we have

$$\Delta_\Gamma[f_{1,s},\dots,f_{n,s}]=\bigcup_{g\in G}\{g\}\times(s\cdot L_g)$$

so that we can write:

$$\Delta_\Gamma\mathfrak{F}=\bigcup_{s\in S}\bigcup_{i=1}^{n}\Delta_\Gamma f_{i,s}=\bigcup_{s\in S}\bigcup_{g\in G}\{g\}\times(s\cdot L_g)=\bigcup_{g\in G}\{g\}\times(S\cdot L_g).$$

Thus, by condition (2), we have $\Delta_\Gamma\mathfrak{F}=\lambda[(G\times H)\setminus(G\times\{0\}]$. The assertion follows. □

We remark that, if $\{f_1,\dots,f_n\}$ is an n-tuple of maps satisfying the hypothesis of the previous theorem, then each L_g has size equal to $\mu=\frac{\lambda(|H|-1)}{|S|}$. On the other hand it is clear that the size of L_g is the number of times that the element g appears in the list of differences

$$\bigcup_{i=1}^{n}\Delta_\Gamma[\sigma_i]=\bigcup_{i=1}^{n}[\sigma_i(x)-\sigma_i(y):\ \{x,y\}\in E(\Gamma)].$$

Therefore, denoted by $\Sigma=[\sigma_1,\dots,\sigma_n]$, Σ is a (G,Γ,μ)-SDF.

Usually, in the applications, we start from a SDF, Σ and we provide the family of maps $\tau_1,\dots,\tau_n$ such that the pairs $(\sigma_1,\tau_1),\dots,(\sigma_n,\tau_n)$ satisfy the hypothesis of the previous theorem.

Going on with the parallelism of Remark 2.2.4, in case Γ is the complete graph $\mathbb{K}_k$, the fundamental construction becomes:

Theorem 2.2.8 ([22]). *Let $\Sigma = [[s_1^1, \dots, s_k^1], \dots, [s_1^n, \dots, s_k^n]]$ be a (G, k, μ)-SDF, and let R be a ring with additive group H. Given n multisets of H, $[t_1^1, \dots, t_k^1], \dots, [t_1^n, \dots, t_k^n]$, we set:*

$$A_i = [(s_j^i, t_j^i),\ j \in \{1, \dots, k\}],\ \forall i \in \{1, \dots, n\};$$

$$\Delta[A_1, \dots, A_n] = \bigcup_{i=1}^{n} [x - y | x, y \in A_i,\ x \neq y];$$

as we have seen in Theorem 2.2.7, there exist multisets L_g of elements of H such that:

$$\Delta[A_1, \dots, A_n] = \bigcup_{g \in G} \{g\} \times L_g.$$

Assume that the following conditions hold:

1) For $i \in \{1, \dots, n\}$ we have: $s_j^i = s_{j'}^i$ with $j \neq j' \implies t_j^i - t_{j'}^i \in U(R)$;

2) $\exists\ S \subset H \setminus \{0\}$ such that $S \cdot L_g = \lambda(H \setminus \{0\})\ \forall g \in G$.

Then there exists a $(G \times H, G \times \{0\}, k, \lambda)$-DF. Moreover the multisets $A_1, \dots, A_n$ turn out to be simple sets.

We remark that Example 2.1.16 implicitly uses this construction and the concept of a strong difference family. Then, as an application of the fundamental construction, it is also possible to provide the following asymptotical theorems of existence of graph decompositions:

Theorem 2.2.9 (M. Buratti, L. Gionfriddo, [25]). *If there exists a (G, Γ, μ)-SDF with G of order n and $|V(\Gamma)| = k$ then there exists a regular Γ-decomposition of $\mu\mathbb{K}_n^{(m)}$ for any positive integer m such that $\gcd(m, (k-1)!) = 1$.*

Theorem 2.2.10 (M. Buratti, A. Pasotti, [26]). *If there exists a (G, Γ, μ)-SDF, then there exists also a regular Γ-decomposition of $\mathbb{K}_{|G|}^{(q)}$ for all prime powers $q \equiv \mu + 1 \pmod{2\mu}$ big enough. In particular if there exists a (g, k, μ)-SDF then there exists also a k-GDD of type g^q.*

In the last chapter of this work, we will return on the previous theorem in order to give a quantitative statement of it.

2.3 Applications of SDFs

2.3.1 A construction of designs

In this subsection we present a simple example that shows how we can use Theorem 2.2.8 in order to construct an infinite family of 2-designs. This example was first found by R.C. Bose in [14] and then rediscovered by M. Buratti in [22]. Here we follow the proof of [22].

Example 2.3.1. *Let q be a prime power such that $q \equiv 1 \pmod 4$. Then there exists a 2-$(5q, 5, 1)$ design.*

Proof. Let us consider the $(\mathbb{F}_5, 5, 4)$ strong difference multiset given by:

$$X = [0, 1, 1, -1, -1].$$

Since $q \equiv 1 \pmod 4$ there exists ξ such that $\xi^2 = -1$. Thus we define the following subset of $\mathbb{F}_5 \times \mathbb{F}_q$ whose first components are the elements of X:

$$A := \{(0,0), (1,1), (1,-1), (-1,\xi), (-1,-\xi)\}.$$

Let us consider the list $\Delta[A] = [x - y |\ x, y \in A, x \neq y]$. Now we set $\Delta[A] = \bigcup_{g \in \mathbb{F}_5} \{g\} \times L_g$ where $L_g \subseteq \mathbb{F}_q$. We have that:

- $L_0 := 2 \cdot \{1, -1, \xi, -\xi\}$
- $L_1 = L_{-1} := \{1, -1, \xi, -\xi\}$
- $L_2 = L_{-2} := (1 - \xi) \cdot \{1, -1, \xi, -\xi\}$.

We note that the set $\{1, -1, \xi, -\xi\}$ is a subgroup of $\mathbb{F}_q^*$. In fact we have:

$$\xi(-\xi) = \xi(-1)(\xi) = (\xi)^2(-1) = (-1)(-1) = 1.$$

Then, if we consider S to be a complete system of representatives for the cosets of $\{1, -1, \xi, -\xi\}$ in $\mathbb{F}_q^*$, it follows that $S \cdot L_g = (\mathbb{F}_q)^*$ for all $g \in \mathbb{F}_5$.

Therefore, as a consequence of Theorem 2.2.8, there exists a $(\mathbb{F}_5 \times \mathbb{F}_q, \mathbb{F}_5 \times \{0\}, 5, 1)$-$DF$. Because of Theorem 2.1.17 we obtain a 5-GDD of type 5^q. Since it trivally exists a 2-$(5, 5, 1)$ design, by Remark 1.1.30, we get a 2-$(5q, 5, 1)$ design. □

The previous example (and in particular its proof of M. Buratti) is source of inspiration of several constructions of Chapter 5.

2.3.2 The Buratti, Rania and Zuanni construction

As we have seen in Definition 1.2.2, a k-cycle decomposition is *regular* if it admits an automorphism group acting regularly, namely sharply transitively, on the vertex-set. In this paragraph however, a k-cycle decomposition of the complete m-partite graph $\mathbb{K}_k^{(m)}$ will be said *regular* if the automorphism group acting regularly on the vertices is the additive group of $\mathbb{Z}_k \times R$ where R is a finite ring with identity of order m; the set of units of a ring R will be denoted by $\mathbb{U}(R)$.

Such a regular decomposition can be obtained with the methods of difference families (see Theorem 2.1.19) as follows. Let us consider a family $\mathfrak{F} = [f_1, \ldots, f_n]$ of injective maps from C_k to $(\mathbb{Z}_k \times R)$. Let us call *list of i-differences* of the family $\mathfrak{F}$ the multiset $\Delta_{C_k^i}\mathfrak{F}$ (denoted also $\Delta_i\mathfrak{F}$) of all the differences $f(x) - f(y)$ with (x, y) an ordered pair of vertices which are at distance i in C_k and $f \in \mathfrak{F}$. If we have $\Delta_{C_k}\mathfrak{F} = (\mathbb{Z}_k \times R) \setminus (\mathbb{Z}_k \times \{0\})$, then $\mathfrak{F}$ is a $(\mathbb{Z}_k \times R, \mathbb{Z}_k \times \{0\}, C_k, 1)$-$DF$. Identifying the vertices of $\mathbb{K}_k^{(m)}$ with the elements of $\mathbb{Z}_k \times R$ and its m parts with the sets of the form $\mathbb{Z}_k \times \{y\}$ with y a fixed element of R, the maps of $\mathfrak{F}$ determine a set of cycles. Then, according to the proof of Theorem 2.1.19, the collection $\mathfrak{C}$ of all translates under the group $\mathbb{Z}_k \times R$ of all cycles of $\mathfrak{F}$ forms the desired k-cycle decomposition

of $\mathbb{K}_k^{(m)}$. If, in addition, we have $\Delta_{C_k^i}\mathfrak{F} = \Delta_{C_k}\mathfrak{F}$ for some value of $i > 1$, then $\mathfrak{C}$ is also i-perfect.

A general construction for regular i-perfect k-cycle decompositions of $\mathbb{K}_k^{(m)}$, here denoted by "the Buratti, Rania and Zuanni construction" or the BRZ-construction, has been obtained in [29] taking as R the ring $\mathbb{Z}_m$. In [24] we generalize that construction assuming that R is any ring of order m. The crucial ingredient in the construction is a special map, that we call *i-perfect map* defined as follows.

Definition 2.3.2. *Let k, i be integers with $\gcd(2i,k) = 1$, $2 \le i \le \frac{k-1}{2}$, and let R be a ring. A map $\tau : \mathbb{Z}_k \longrightarrow R$ is said to be i-perfect if the following conditions hold:*

C1. *τ is odd, i.e., $\tau(-x) = -\tau(x) \quad \forall x \in \mathbb{Z}_k$;*

C2. *$x, y \in \mathbb{Z}_k$ and $x^2 = y^2 \Longrightarrow x = y$ or $\tau(x) - \tau(y) \in \mathbb{U}(R)$;*

C3. *$\tau(x+1) - \tau(x) \in \mathbb{U}(R)$ $\forall x \in \mathbb{Z}_k$;*

C4. *$\tau(x+i) - \tau(x) \in \mathbb{U}(R)$ $\forall x \in \mathbb{Z}_k$.*

We are now able to state the following theorem that is a generalization of theBRZ-construction (Theorem 4.2 of [29]).

Theorem 2.3.3. *Let R be a ring of order m. If there exists an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R$, then there exists a regular i-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$.*

Proof. Assume that $\tau : \mathbb{Z}_k \longrightarrow R$ is i-perfect and consider the map $f : V(C_k) \to \mathbb{Z}_k \longrightarrow R :\ f(x) = (x^2, \tau(x))$.

Let Ω be a subset of $\mathbb{Z}_k \setminus \{0\}$ such that if $\omega \in \Omega$ then also $-\omega \in \Omega$. We recall that the *circulant graph* of order k and with connection set Ω is the simple graph with vertex-set $\mathbb{Z}_k$ and whose edges are precisely those of the form $\{x, \omega + x\}$ with $x \in \mathbb{Z}_k$ and $\omega \in \Omega$. As a special case of Proposition 4.5 in [25], the map $\sigma : x \in \mathbb{Z}_k \longrightarrow x^2 \in \mathbb{Z}_k$ is a $(\mathbb{Z}_k, \Gamma, 2)$ *strong difference map* for every *circulant graph* Γ of order k and connection set of the form $\{j, -j\}$ with $\gcd(j,k) = 1$. This means that the list $[\sigma(x+j) - \sigma(x), \sigma(x) - \sigma(x+j) \mid x \in \mathbb{Z}_k]$ covers all elements of $\mathbb{Z}_k$ exactly twice for any $j \in \mathbb{U}(\mathbb{Z}_k)$. It follows that for any such j the list of j-differences of $[f]$ has the form $\Delta_{C_k^j}[f] = \bigcup_{z \in \mathbb{Z}_k} \{z\} \times [\delta_j(z), \epsilon_j(z)]$ where $[\delta_j(z), \epsilon_j(z)]$ is a suitable pair of elements of R. Now condition C1 easily implies that $\epsilon_j(z) = -\delta_j(z)$ for every $z \in \mathbb{Z}_k$. Hence, for every $j \in \{1, \ldots, \frac{k-1}{2}\} \cap \mathbb{U}(\mathbb{Z}_k)$, the list of j-differences of $[f]$ is of the form

$$\Delta_{C_k^j}[f] = \bigcup_{z \in \mathbb{Z}_k} \{z\} \times [\delta_j(z), -\delta_j(z)]$$

Finally, conditions C3 and C4 imply that $\delta_j(z)$ is a unit of R for $j \in \{1, i\}$ and for every $z \in \mathbb{Z}_k$. Now let S be a complete system of representatives for the equivalence relation in $R \setminus \{0\}$ defined by $r \sim r'$ if and only if $r' = \pm r$. It is clear that we have $\bigcup_{s \in S} [s\delta_j(z), -s\delta_j(z)] = R \setminus \{0\}$ and hence, if f_s is the map obtained from f by multiplying the second coordinates of all its vertices by s, we see that $\mathfrak{F} := [f_s \mid s \in S]$ is a $(\mathbb{Z}_k \times R, \mathbb{Z}_k \times \{0\}, C_k, 1)$-$DF$. Since we have also that $\Delta_{C_k^i}\mathfrak{F} = \Delta_{C_k}\mathfrak{F}$, this difference family generates an i-perfect k-cycle decomposition $\mathfrak{C}$ of $\mathbb{K}_k^{(m)}$. □

Using this construction in case $R = \mathbb{Z}_m$, M. Buratti, F. Rania and F. Zuanni got i-perfect k-cycle decompositions of $\mathbb{K}_k^{(m)}$ for infinitely many values of k.

Theorem 2.3.4 (M. Buratti, F. Rania, F. Zuanni)**.** *If $gcd(k, 2i) = 1$ there exists an i-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$ for all m such that $gcd(m, (k-1)!) = 1$.*

Proof. It is sufficient to consider the map $\tau : \mathbb{Z}_k \to \mathbb{Z}_m$ such that $\tau(x) = x$ for $x \in [0, \frac{k-1}{2}]$ and $\tau(x) = x - k$ otherwise. This map satisfies the property C1 of Definition 2.3.2 by construction and, because $gcd(m, (k-1)!) = 1$, it satisfies also the other properties. Thus τ is i-perfect and the claim follows from Theorem 2.3.3. □

Note that, if k is a prime, they obtained also an i-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ as a consequence of this theorem and of Proposition 1.2.7. Moreover, again as a consequence of this theorem and of Theorem 1.2.12, M. Buratti, G. Rinaldi and T. Traetta in [30], got a 3-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ for all k coprime with 6 and suitable values of m.

Theorem 2.3.5. *If $gcd(k, 6) = 1$ then there exists a 3-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ for all m such that $gcd(m, (k-1)!) = 1$.*

In Chapters 3 and 4 of this work we will see that, with a careful application of the *BRZ*-construction and of Theorem 2.3.3, it is possible to improve Theorems 2.3.4 and 2.3.5.

Chapter 3

Perfect decompositions via graph colorings

In this chapter we will find infinite classes of i-perfect k-cycle decompositions of $\mathbb{K}_v$ where $v = mk$ is odd and i ($\leq \frac{k-1}{2}$) is arbitrary. The two ingredients for achieving this are: an i-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$ and an i-perfect Hamiltonian decomposition of $\mathbb{K}_k$, i.e., an i-perfect k-cycle decomposition of $\mathbb{K}_k$.

The core of this chapter is devoted to a careful investigation about the existence of the first object. The main tool will be the BRZ-construction, that uses a special map (*i-perfect map*, see Definition 2.3.2) from $\mathbb{Z}_k$ to a suitable ring of order m. We will also use some elementary but useful remarks on vertex-colorings of a graph. The main result is that an i-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$ with k odd and i admissible exists whenever the parameters satisfy suitable conditions which, in general, are not very strict; in the worst of the cases, $k = 3\ell^2$, the existence is assured when $\gcd(i, k) = 1$ and each prime power factor of m is greater than $\frac{7\sqrt{k}}{6}$. The best case is when k is a prime; here it is enough that $\gcd(m, 9) \neq 3$.

Unfortunately to obtain constructions of the second object, an i-perfect Hamiltonian decomposition of $\mathbb{K}_k$ (also called Hamiltonian cycle system or briefly $HCS(k)$), seems to be a much harder target in general. On the other hand the few known results on this problem led us to a plethora of new i-perfect k-cycle decompositions of the complete graph anyway. In particular we prove that if k is an odd prime, then there exists an i-perfect k-cycle decomposition of $\mathbb{K}_v$ (or briefly a $(\mathbb{K}_v, C_k)$-design) for any $v = mk$ odd and any admissible i with the only possible exception of the case that we simultaneously have $k \geq 23$ and $\gcd(m, 9) = 3$.

Incidentally, we also update the known results about i-perfect k-cycle decompositions (or briefly, $(\mathbb{K}_v, C_k)$-designs) with $k \leq 19$ (see Table 12.50 in [15] or Table 1.2.10 of this thesis) proving the existence of a 2-perfect $(\mathbb{K}_{45}, C_9)$-design, of a 2-perfect $(\mathbb{K}_{57}, C_{19})$-design, and of a 5-perfect $(\mathbb{K}_{13m}, C_k)$ design for any odd m.

Still more results could be obtained if we knew more about the existence of i-perfect Hamiltonian cycle systems, a topic that we hope will receive some attention in the near future.

3.1 More about i-perfect maps

Let R be a finite ring of order m with identity; we denote by $\mathbb{U}(R)$ the set of units of a ring R. It will be useful to recall that every ring R of order m is isomorphic to a direct product $R_1 \times \cdots \times R_n$ of rings whose orders, $q_1, \ldots q_n$, are the prime power factors of m (see, e.g., Theorem 1.1 in [53]). We will refer to this result as *the structure theorem of finite rings*.

We briefly recall that (see Definition 2.3.2) an i-perfect map τ from $\mathbb{Z}_k$ to R is an odd map (C1) such that if $x, y \in \mathbb{Z}_k$ and $x^2 = y^2$ then $x = y$ or $\tau(x) - \tau(y) \in \mathbb{U}(R)$ (C2); $\tau(x+1) - \tau(x) \in \mathbb{U}(R)\ \forall x \in \mathbb{Z}_k$ (C3); and finally, $\tau(x+i) - \tau(x) \in \mathbb{U}(R)\ \forall x \in \mathbb{Z}_k$ (C4).

Assume now that an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R$ exists. Given $x \in \mathbb{Z}_k \setminus \{0\}$, we have $\tau(x) - \tau(-x) \in \mathbb{U}(R)$ from C2 and hence, from C1, we have $2\tau(x) \in \mathbb{U}(R)$. This implies that both $2 = 1 + 1$ and $\tau(x)$ are units.

Note, in particular, that the order of R is necessarily odd; in the opposite case, if y is an involution of the additive group of R, we would have $0 = 2y$ and then, considering that 2 is a unit, we would have $y = 0$ which is absurd.

From C1, we have $\tau(0) = -\tau(0)$ and hence $2\tau(0) = 0$ which implies $\tau(0) = 0$ recalling that $2 \in \mathbb{U}(R)$.

Now assume that the order of R is divisible by 3 but not by 9. Then, up to isomorphism, considering that $\mathbb{Z}_3$ is the only ring of order 3, we have $R = \mathbb{Z}_3 \times R'$ for a suitable ring R' by the structure theorem of finite rings. The projection of the sequence $(\tau(0), \tau(1), \ldots, \tau(k-1))$ onto $\mathbb{Z}_3$ is necessarily of the form $(0, 1, 2, 1, 2, \ldots 1, 2)$ or $(0, 2, 1, 2, 1, \ldots, 2, 1)$ since $\tau(x) - \tau(x+1)$ cannot be in $\{0\} \times R'$ in view of C3, and we also have $\tau(x) \notin \{0\} \times R'$ for $x \neq 0$ since, as commented above, $\tau(x)$ is a unit for every such x. Then, for i even, we would have $\tau(i+1) - \tau(1) \in \{0\} \times R'$ and, for i odd, we would have $\tau(i-1) - \tau(-1) \in \{0\} \times R'$. In both cases C4 would be contradicted.

The above observations can be summarized as follows.

Remark 3.1.1. *If there exists an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R$ then we have:*

$|R|$ *is odd;*

$\tau(0) = 0$*;*

$\tau(x) \in \mathbb{U}(R)\ \forall x \in \mathbb{Z}_k \setminus \{0\}$*;*

$\gcd(|R|, 9) \neq 3$.

We will say that a triple (k, i, m) is *admissible* if k is odd, $\gcd(i, k) = 1$, $1 \leq i \leq \lfloor \frac{k}{2} \rfloor$, and $\gcd(m, 18) = 1$ or 9. In view of the above remark, it is clear that if an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R$ exists, then $(k, i, |R|)$ is admissible.

Given a natural number m, we will denote by $R(m)$ the ring of order m which is the direct product of all fields whose orders are the prime power factors of m. Note, in particular, that $R(m) = \mathbb{Z}_m$ if and only if m is square-free. In the next section we will see that $R(m)$, among all rings R of order m, is an optimal candidate for the existence of an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R$. So our goal will be to determine the set of all admissible triples (k, i, m) for which there exists an i-perfect map

$\tau : \mathbb{Z}_k \longrightarrow R(m)$. We will see that an effective way for attacking this problem is to calculate the chromatic numbers of some auxiliary graphs associated with the pair (k, i). In section 5 we will prove the following main result.

Theorem 3.1.2. *A necessary condition for the existence of an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R(m)$ is that (k, i, m) is admissible and that every prime power factor of m is not smaller than $w(k) := 2^t\sqrt{k/k^*}$ where k^* is the square-free part of k, and t is the number of prime factors of k^*.*

The condition is also sufficient with the possible exception of the case where the following facts simultaneously hold: $k > 1000$ is the product of two distinct primes; $i > 2$ is even; $\gcd(m, 25) = 5$.

The exception mentioned in the theorem can be removed if one was able to prove the bipartiteness of some special graphs of order the product of two distinct odd primes.

In the last section we will show how our main result allows to obtain a plethora of new i-perfect k-cycle systems of order $v = mn$ (odd). In particular, the existence of such a system with k a prime remains undecided only for $k \geq 23$ and $\gcd(m, 9) = 3$.

Now note that the main theorem in conjunction with Theorem 2.3.3 immediately implies the following result.

Corollary 3.1.3. *If (k, i, m) are admissible and all prime power factors of m are at least equal to $w(k)$, then there exists an i-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$ with the same possible exceptions of Theorem 3.1.2.*

3.2 Necessity

Given a positive odd integer k, throughout the chapter we will denote by $\mathbb{Z}_k^{\square}$ the set of squares of $\mathbb{Z}_k$, by $\mathbb{Z}_k^+$ the subset $\{1, \ldots, \frac{k-1}{2}\}$ of $\mathbb{Z}_k$, and by $\mathbb{Z}_k^-$ the subset $\{\frac{k+1}{2}, \ldots, k-1\}$ of $\mathbb{Z}_k$. Given $\sigma \in \mathbb{Z}_k^{\square}$, we set

$$A_\sigma := \{x \in \mathbb{Z}_k : \ x^2 = \sigma\}; \qquad A_\sigma^* := A_\sigma \setminus \{0\}; \qquad A_\sigma^+ = A_\sigma \ \cap \ \mathbb{Z}_k^+.$$

Let Σ_k be the multiset on $\mathbb{Z}_k^{\square}$ defined by $\Sigma_k = \{x^2 \mid x \in \mathbb{Z}_k\}$. The *weight* of Σ_k, denoted by $w(k)$, is defined to be the maximum number of occurrences of an integer in Σ_k. Equivalently, we have

$$w(k) := \max_{\sigma \in \mathbb{Z}_k^{\square}} |A_\sigma|.$$

It has been proved in [29] that if $k = p_1^{e_1} \ldots p_n^{e_n}$ is the prime-factorization of k, then we have

$$w(k) = 2^t p_1^{g_1} \ldots p_n^{g_n}$$

where $g_i = \lfloor \frac{e_i}{2} \rfloor$ and t is the number of odd e_is.

Here we note that if we set $k = k^*\ell^2$ with k^* the *square-free part* of k, then a more readable presentation of $w(k)$ is the one given in the statement of our main theorem:

$$w(k) = 2^t \ell$$

where t is the number of prime factors of k^*.

We will also need to consider the integer $w^*(k)$ defined as follows.

$$w^*(k) := \max_{\sigma \in \mathbb{Z}_k^\square} |A_\sigma^*|.$$

It is clear that $w^*(k)$ is either $w(k)-1$ or $w(k)$. Note that $w^*(k)$ is always even since, obviously, if x is an element of A_σ^*, then $-x$ is also in A_σ^*. Also note that $w(k)$ is odd if and only if k is a square. These remarks allow us to write:

$$w^*(k) = \begin{cases} w(k)-1 \text{ if } \ k \ \text{ is a square;} \\ w(k) \text{ otherwise.} \end{cases}$$

Definition 3.2.1. *Let us define the* weight *of a ring R as the integer $w(R)$ expressing the maximum size of a subset of R whose list of differences is entirely contained in $\mathbb{U}(R)$.*

It is an easy exercise to see that $w(\mathbb{Z}_m)$ is the least prime factor of m while $w(R(m))$ is the least prime power factor of m. Now recall that every ring R of order m is isomorphic to a direct product $R_1 \oplus \cdots \oplus R_n$ of rings whose orders, q_1, $\ldots q_n$, are the prime power factors of m (see, e.g., Theorem 1.1 in [53]). Assume that q_1 is the least prime power factor of m and let X be a subset of R of size greater than q_1. By the pigeon hole principle, there are two elements x and y of X having the same first coordinate so that $x-y$ is not a unit of R. Thus ΔX, the list of differences of X, is not entirely contained in $\mathbb{U}(R)$ and therefore $w(R) \leq q_1 = w(R(m))$. We conclude that no ring of order m is strictly weightier than $R(m)$.

Lemma 3.2.2. *A necessary condition for the existence of an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R$ with $(k, i, |R|)$ admissible, is that $w(R) \geq w(k)$.*

Proof. Let $\tau : \mathbb{Z}_k \longrightarrow R$ be i-perfect and take $\sigma \in \mathbb{Z}_k^\square$ such that $|A_\sigma| = w(k)$. By condition C2 of Definition 2.3.2, the image of A_σ is a $w(k)$-subset of R whose list of differences is entirely contained in $\mathbb{U}(R)$. □

Corollary 3.2.3. *A necessary condition for the existence of an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R(m)$ is that (k, i, m) is admissible and that every prime power factor of m is not smaller than $w(k)$.*

In view of Lemma 3.2.2, in order to construct perfect maps from $\mathbb{Z}_k$ to a ring R of order m, it is better to choose R as weighty as possible. Thus, for what seen above, the ring $R(m)$ is optimal in this sense.

3.3 The auxiliary graphs $G(k, i, \rho)$ and their chromatic numbers

In this section we introduce some auxiliary graphs associated with the pair (k, i) and we show how the knowledge of their chromatic numbers may be helpful in determining the values of m for which there exists an i-perfect map from $\mathbb{Z}_k$ to $R(m)$.

Definition 3.3.1. *For any given map $\rho : \mathbb{Z}_k^+ \longrightarrow \{1, -1\}$, let $G(k, i, \rho)$ be the graph with vertex-set $\mathbb{Z}_k^+$ and edge-set*

$$E(k, i, \rho) = E^{\square}(k) \ \cup \ E(k, 1, \rho) \ \cup \ E^{-}(k, i, \rho) \ \cup \ E^{+}(k, i, \rho)$$

defined as follows:

$\{x, y\} \in E^{\square}(k) \iff x^2 \equiv y^2 \ (mod\ k)$;

$\{x, y\} \in E(k, 1, \rho) \iff x - y \equiv \pm 1 \ (mod\ k)$ *and* $\rho(x) = \rho(y)$;

$\{x, y\} \in E^{-}(k, i, \rho) \iff x - y \equiv \pm i \ (mod\ k)$ *and* $\rho(x) = \rho(y)$;

$\{x, y\} \in E^{+}(k, i, \rho) \iff x + y \equiv \pm i \ (mod\ k)$ *and* $\rho(x) \neq \rho(y)$.

We will denote by $G^{\square}(k)$, $G(k, 1, \rho)$, $G^{-}(k, i, \rho)$ and $G^{+}(k, i, \rho)$ the graphs whose edge-sets are $E^{\square}(k)$, $E(k, 1, \rho)$, $E^{-}(k, i, \rho)$ and $E^{+}(k, i, \rho)$, respectively.

Lemma 3.3.2. *Let (k, i, m) be admissible. If all prime power factors of m are greater than twice the chromatic number of $G(k, i, \rho)$ for a suitable map $\rho : \mathbb{Z}_k^+ \longrightarrow \{1, -1\}$, then there exists an i-perfect map $\tau : \mathbb{Z}_k \longrightarrow R(m)$.*

Proof. Let $\rho : \mathbb{Z}_k^+ \longrightarrow \{1, -1\}$ and let t be the chromatic number of $G(k, i, \rho)$. Assume that all prime power factors of m are greater than $2t$ and let ω be an element of $R(m)$ whose j-th coordinate is a primitive element of the j-th factor of $R(m)$. Then take a vertex coloring c of $G(k, i, \rho)$ whose colors are the elements of the subset $\{\omega^j \mid 0 \leq j \leq t - 1\}$ of $R(m)$.

It is clear that for any two elements x and y of $\mathbb{Z}_k^+$, we have $c(x) + c(y) \in \mathbb{U}(R(m))$. It is also clear that $c(x) - c(y) \in \mathbb{U}(R(m))$ provided that $c(x) \neq c(y)$. This remark will be tacitly used in the following to show that the odd map $\tau : \mathbb{Z}_k \longrightarrow R(m)$ defined by

$$\tau(x) = \rho(x)c(x) \quad \forall x \in \mathbb{Z}_k^+$$

is i-perfect.

The map τ satisfies condition C1 by definition.

The map τ satisfies Condition C2.

Let x, y be distinct elements of $\mathbb{Z}_k$ such that $x^2 \equiv y^2 \pmod{k}$. Set $\overline{x} = x$ or $-x$ according to whether $x \in \mathbb{Z}_k^+$ or $x \in \mathbb{Z}_k^-$, respectively. Analogously, set $\overline{y} = y$ or $-y$ according to whether $y \in \mathbb{Z}_k^+$ or $y \in \mathbb{Z}_k^-$, respectively. It is clear that we have $\tau(x) - \tau(y) = \pm(c(\overline{x}) \pm c(\overline{y}))$ for a suitable choice of the signs. We also have $c(\overline{x}) \neq c(\overline{y})$ since $\{\overline{x}, \overline{y}\} \in E^{\square}(k)$ is an edge of $G(k, i, \rho)$. Then $\tau(x) - \tau(y) \in \mathbb{U}(R(m))$.

The map τ satisfies Condition C3.

For $x = 0$ or $k-1$ we have $\tau(x) - \tau(x+1) = \pm c(1) \in \mathbb{U}(R(m))$ while for $x = \frac{k-1}{2}$ we have $\tau(x) - \tau(x+1) = \pm 2c(\frac{k-1}{2}) \in \mathbb{U}(R(m))$.

Now assume that $x \in \mathbb{Z}_k^+ \setminus \{\frac{k-1}{2}\}$. If $\rho(x) \neq \rho(x+1)$, we have $\tau(x+1) - \tau(x) = \pm(c(x) + c(x+1)) \in \mathbb{U}(R(m))$. If $\rho(x) = \rho(x+1)$, then $\{x, x+1\} \in E(k, 1, \rho)$ is an edge of $G(k, i, \rho)$ so that we have $c(x) \neq c(x+1)$. Then we have $\tau(x+1) - \tau(x) = \pm(c(x) - c(x+1)) \in \mathbb{U}(R(m))$.

The case when $x \in \mathbb{Z}_k^- \setminus \{k-1\}$ can be done similarly.

The map τ satisfies Condition C4.

For $x = 0$ or $x = k - i$ we have $\tau(x) - \tau(x+i) = \pm c(i) \in \mathbb{U}(R(m))$.

Assume that both x and $x+i$ are in $\mathbb{Z}_k^+$. If $\rho(x) \neq \rho(x+i)$, we have $\tau(x) - \tau(x+i) = \pm(c(x+i) + c(x)) \in \mathbb{U}(R(m))$. If $\rho(x) = \rho(x+i)$, then $\{x, x+i\} \in E^-(k,i,\rho)$ is an edge of $G(k,i,\rho)$ so that we have $c(x) \neq c(x+i)$. Then we have $\tau(x) - \tau(x+i) = \pm(c(x) - c(x+i)) \in \mathbb{U}(R(m))$.

The case when both x and $x+i$ are in $\mathbb{Z}_k^-$ can be done similarly.

Now assume that $x \in \mathbb{Z}_k^+$ and $x+i \in \mathbb{Z}_k^-$ so that $y := -x - i \in \mathbb{Z}_k^+$. If $\rho(x) \neq \rho(y)$, then $\{x, y\} \in E^+(k,i,\rho)$ so that we have $c(x) \neq c(y)$. Then we have $\tau(x) - \tau(x+i) = \tau(x) + \tau(y) = \pm(c(x) - c(y)) \in \mathbb{U}(R(m))$. If $\rho(x) = \rho(y)$, then we have $\tau(x) - \tau(x+i) = \tau(x) + \tau(y) = \pm(c(x) + c(y)) \in \mathbb{U}(R(m))$.

The case when $x \in \mathbb{Z}_k^-$ and $x+i \in \mathbb{Z}_k^+$ can be done similarly. □

The above lemma is crucial for proving our main result. Indeed, given positive integers k and i with $i \leq \frac{k-1}{2}$ and $\gcd(2i,k) = 1$, our strategy will be to find a suitable map $\rho : \mathbb{Z}_k^+ \longrightarrow \{1,-1\}$ such that the graph $G(k,i,\rho)$ has chromatic index equal to $\frac{w^*(k)}{2}$.

3.4 A pair of elementary lemmas on vertex-graph-colorings

In order to determine the chromatic numbers of some graphs $G(k,i,\rho)$ we need two easy lemmas on vertex-graph-colorings. For a given graph G we will use the standard notation $\chi(G)$ and $\Delta(G)$ to denote the chromatic number and the maximum degree of G, respectively.

Lemma 3.4.1. *Let G be a graph of chromatic number at least two (hence with at least one edge) whose connected components are complete graphs and let M be a matching on $V(G)$. Then we have $\chi(G \cup M) = \chi(G)$.*

Proof. The assertion will be proven if we show that $\chi(H) \leq \chi(G)$ for any connected component H of $G \cup M$. This is clear if H is entirely contained in G. So, from now on, H will denote a connected component of $G \cup M$ having at least one edge in $E(M) \setminus E(G)$.

Assume that H is a complete graph and let $e \in E(M) \setminus E(G)$. Since each component of G is complete, e must join two components of G; these components must each be $\mathbb{K}_1$ since H is complete. So $H = \mathbb{K}_2$. Now assume H is a cycle with at least one edge $e \in E(M)$. Since each component of G is complete, H must be an even cycle in which the edges are alternately in $E(M) \setminus E(G)$ and in $E(G) \setminus E(M)$. So $\chi(H) = 2 \leq \chi(G)$.

If H is neither a complete graph nor a cycle then $\chi(H)$ does not exceed $\Delta(H)$ by Brooks' Theorem on vertex colorings (see, e.g., [61]). On the other hand we have $\Delta(H) \leq \Delta(G) + \Delta(M) = (\chi(G) - 1) + 1 = \chi(G)$ and hence $\chi(H) \leq \chi(G)$ once again. □

The next lemma is in the same spirit of Proposition 2.2 of [7].

Lemma 3.4.2. *Let G be a graph whose connected components are complete graphs and let $\chi(G) \geq 3$. Let H be a graph with the same vertex-set as G and connected components that are edges and a path P of order 3. Then $\chi(G \cup H) = \chi(G)$.*

Proof. Let G and H be graphs as in the statement and set $P = (x, y, z)$. By Lemma 3.4.1 there exists a proper vertex-coloring γ of $G \cup (H - \{x, y\})$ using the colors of a set C of size $\chi(G)$. Of course γ is also a proper vertex-coloring of $G \cup H$ in the case that we have $\gamma(x) \neq \gamma(y)$. So, let assume that $\gamma(x) = \gamma(y) = c$. Having $\chi(G) \geq 3$, there is at least one color c^* of $C \backslash \{c\}$ for which we have $\gamma(z) \neq c^*$. It is convenient to denote these special colors c and c^* by 1 and -1. Let $X = (x_0, x_1, \ldots, x_n)$ be a path of maximum length in the set $\mathcal{X}$ of all $\{1, -1\}$-colored subpath of $G \cup (H - \{x, y\})$ (in the fixed coloring γ) with an endpoint in $x_0 = x$.

Since $\gamma(x) = 1$, it is evident that $\gamma(x_i)$ is 1 or -1 according to whether i is even or odd, respectively. Considering the forms of the graphs G and H, it is also evident that $\{x_i, x_{i+1}\}$ is in $E(G)$ or in $E(H)$ according to whether i is even or odd, respectively. So, denoting by A_i the connected component of G through x_i, we have $V(A_i) \cap V(X) = \{x_i, x_{i+1}\}$ for $i < n$ even or $\{x_i, x_{i-1}\}$ for i odd. We also have $V(A_n) \cap V(X) = \{x_n\}$ when n is even.

In view of the above remarks we also notice that $y \notin V(X)$. Indeed in the opposite case we would have $y = x_i$ for an even $i > 0$ since we are supposing $\gamma(x) = \gamma(y) = 1$. Therefore $\{x_{i-1}, x_i\} \in E(H)$ and then x_{i-1} is either x or z considering that the only edges of $E(H)$ through y are $\{x, y\}$ and $\{y, z\}$. In the former case we would have $y = x_1$ and then $\gamma(y) = -1$, a contradiction. In the latter case we have $\gamma(z) = \gamma(x_{i-1}) \in \{1, -1\}$ which is also a contradiction.

If $0 \leq i < n$, the vertex x_i is incident with just one edge of $E(H)$, and hence all neighbors of x_i not in X (except y when $i = 0$) must be in a clique of G, so cannot be colored either 1 or -1. Since X is maximal, the only neighbors in $G \cup H$ of x_n colored the negative of the color of x_n must be in X. Therefore interchanging colors along X produces a proper coloring of $G \cup H$. □

3.5 Existence of i-perfect maps

Now we have all necessary ingredients for proving our main result. We split the proof into two parts according to whether i is odd or even.

Proposition 3.5.1. *The necessary condition given by Corollary 3.2.3 is also sufficient except, possibly, in the case that $k > 1000$ is the product of two distinct primes, $i > 2$ is even and $\gcd(m, 25) = 5$.*

Proof. Case 1: Suppose that i is odd.

Let $\rho : x \in \mathbb{Z}_k^+ \longrightarrow (-1)^x \in \{1, -1\}$. One can see that both $G(k, 1, \rho)$ and $G^-(k, i, \rho)$ are totally disconnected so that $G(k, i, \rho)$ is the union of $G^{\square}(k)$ and $G^+(k, i, \rho)$. It is clear that the connected components of $G^{\square}(k)$ are the complete graphs on all sets of the form $A_\sigma^* \cap \mathbb{Z}_k^+$ with $\sigma \in \mathbb{Z}_k^{\square}$. Thus it is obvious that the

chromatic number of $G^{\square}(k)$ is $\frac{w^*(k)}{2}$. Moreover we see that $G^+(k,i,\rho)$ is a matching since we have

$$E^+(k,i,\rho) = \{\{j, i-j\} \mid 1 \leq j \leq \frac{i-1}{2}\}.$$

For k prime or $k = 9$ we have $w(k) = 2$ or 3, respectively. In both cases the graph $G^{\square}(k)$ is totally disconnected so that $G(k,i,\rho)$ is a matching and then its chromatic number is 2. If q is a prime power factor of m we have by assumption $q \geq w(k)$ but also $q \geq 5$ since the triple (k,i,m) is admissible and hence $\gcd(m,18) \in \{1,9\}$. Thus we have $q \geq 5 > 2\chi(G(k,i,\rho)) = 4$ and the assertion follows from Lemma 3.3.2.

For all other values of k the graph $G^{\square}(k)$ is not totally disconnected. Therefore, by Lemma 3.4.1, the chromatic number of $G(k,i,\rho)$ is equal to the chromatic number of $G^{\square}(k)$ that is $\frac{w^*(k)}{2}$. For every prime power factor q of m we have $q \geq w(k)$ by assumption. Then we can write

$$q \geq w(k) \geq w^*(k) = 2\chi(G(k,i,\rho)).$$

Thus we certainly have $q > 2\chi(G(k,i,\rho))$ because q must be odd and the assertion follows from Lemma 3.3.2.

Case 2: Suppose that i is even.

Let $\frac{k-i-1}{2} = ni + r$ be the Euclidean division of $\frac{k-i-1}{2}$ by i so that we have $k = (2n+1)i + 2r + 1$ with $0 \leq r < i$. Now let $\rho : \mathbb{Z}_k^+ \longrightarrow \{1,-1\}$ be the map implicitly defined by the rules

$$\rho(1) = 1; \qquad \rho(x) = \rho(x+1) \Longleftrightarrow x \equiv r \pmod{i} \tag{3.1}$$

and let $G^*(k,i,\rho)$ be the subgraph of $G(k,i,\rho)$ obtained by removing all edges of $E^{\square}(k)$.

By (4.1), we have $\rho(x) = \rho(x+1)$ if and only if $x \equiv r \pmod{i}$. Thus we have

$$E(k,1,\rho) = \{\{r, r+1\}, \{i+r, i+r+1\}, \ldots, \{vi+r, vi+r+1\}\}$$

with $v = \lfloor \frac{k-3-2r}{2i} \rfloor$ and hence we see that $G(k,1,\rho)$ is a matching.

Assume that x and $x+i$ are elements of $\mathbb{Z}_k^+$. Recall that we have $0 \leq r < i$, therefore there is exactly one element $\xi \in \mathbb{Z}_k^+$ such that $x \leq \xi < x+i$ and $\xi \equiv r \pmod{i}$. It is clear by (4.1) that for $x \leq z \leq \xi$ we have $\rho(z) = \rho(x)$ if and only if x and z have the same parity. Applying this remark in the particular case $z = \xi$ we get:

$$\rho(\xi) = (-1)^{x+\xi}\rho(x). \tag{3.2}$$

Analogously, by (4.1), for $\xi + 1 \leq z \leq x + i$ we have $\rho(z) = \rho(\xi+1)$ if and only if z and $\xi+1$ have the same parity. Thus, in particular, we have $\rho(x+i) = (-1)^{\xi+1+x+i}\rho(\xi+1)$. By (4.1) again, we have $\rho(\xi+1) = \rho(\xi)$ since $\xi \equiv r \pmod{i}$. Hence, using (4.2) and recalling that i is even, we can write:

$$\rho(x+i) = (-1)^{\xi+1+x+i}\rho(\xi) = (-1)^{2\xi+2x+i+1}\rho(x) = -\rho(x). \tag{3.3}$$

The above equality guarantees that $E^-(k,i,\rho)$ is empty.

The set of pairs of elements of $\mathbb{Z}_k^+$ summing up to i or $-i$ modulo k is the union of the two matchings M and M' defined as follows:

$M = \{\{j, i-j\} \mid 1 \le j \le \frac{i}{2} - 1\}$;

$M' = \{\{\frac{k-1}{2} - i + j, \frac{k+1}{2} - j\} \mid 1 \le j \le \frac{i}{2}\}$

For $1 \le j < \frac{i}{2}$ we have $\rho(j) = -\rho(i-j)$ if and only if $j \le r \le i - j - 1$. Thus the pairs $\{j, i-j\}$ of M belonging to $E^+(k, i, \rho)$ are those having $j \le r$ if $r < \frac{i}{2}$ or those having $j \le i - r - 1$ if $r \ge \frac{i}{2}$.

By definition of r, the element $\xi := \frac{k-1}{2} - \frac{i}{2}$ is the only element of the interval $[\frac{k-1}{2} - i, \frac{k-1}{2}]$ which is congruent to r modulo i. Now note that we have $\frac{k-1}{2} - i + j \le \xi < \frac{k+1}{2} - j$ for $1 \le j \le \frac{i}{2}$. Hence, with the same reasoning leading to (4.3), we have that $\rho(x) = \rho(y)$ for every pair $\{x, y\} \in M'$. Thus no pair of M' belongs to $E^+(k, i, \rho)$.

We conclude that we have

$$E^+(k, i, \rho) = \begin{cases} \{\{j, i-j\} \mid 1 \le j \le r\} \text{ if } r < \frac{i}{2} \\ \{\{j, i-j\} \mid 1 \le j \le i - r - 1\} \quad \text{if } r \ge \frac{i}{2}. \end{cases}$$

Note, in particular, that $E^+(k, i, \rho)$ is empty when $r = 0$ or $i - 1$. Thus, in the extremal cases that $r = 0$ or $i - 1$, which means $k \equiv i \pm 1 \pmod{2i}$, the graph $G^*(k, i, \rho)$ is a matching.

For $1 \le r \le i - 2$ the graph $G^*(k, i, \rho)$ fails to be a matching just because, among its connected components there is a path on 3 vertices that is $(i - r, r, r + 1)$ or $(i - r - 1, r + 1, r)$ according to whether $r < \frac{i}{2}$ or not, respectively.

Case 2.1: $r = 0$ or $r = i - 1$.

Here, for what said above, the graph $G^*(k, i, \rho)$ with ρ defined as in (4.1) is a matching. Hence the graph $G(k, i, \rho) = G^{\square}(k) \cup G^*(k, i, \rho)$ has chromatic number $\frac{w^*(k)}{2}$ by Lemma 3.4.1. If q is any prime power factor of m, we have $q \ge w(k)$ by assumption so that $q \ge w^*(k) = 2\chi(G(k, i, \rho))$. The assertion follows again by Lemma 3.3.2.

Note that the case $i = 2$ is a special case of Case 2.1.

Case 2.2: $0 < r < i - 1$.

Consider again the graph $G(k, i, \rho) = G^{\square}(k) \cup G^*(k, i, \rho)$ with ρ defined as in (4.1). In this case we have seen that the connected components of $G^*(k, i, \rho)$ are single edges and a path on three vertices. Also recall that the connected components of $G^{\square}(k)$ are complete graphs and that the chromatic number of $G^{\square}(k)$ is $\frac{w^*(k)}{2}$.

Case 2.2.1: k is a prime or $k = 9$.
We have $w(k) = 2$ or 3 and the graph $G^{\square}(k)$ is totally disconnected so that $G(k, i, \rho) = G^*(k, i, \rho)$ has chromatic number equal to 2. Then it is enough to reason as in Case 1.

Case 2.2.2: $k = 25$.
We have $w(k) = 5$, hence every prime power factor of m is at least equal to 5. Take an element ω of $R(m)$ whose j-th coordinate is a primitive element of the j-th

factor of $R(m)$. Now consider the odd maps τ_1 and τ_2 from $\mathbb{Z}_{25}$ to $R(m)$ defined as follows:

$$\tau_1(x) = \begin{cases} 1 \text{ for } x \in \{1,4,7,10\}; \\ -1 \text{ for } x \in \{6,9,12\}; \\ \omega \text{ for } x \in \{2,5,8,11\}; \\ -\omega \text{ for } x = 3. \end{cases}$$

$$\tau_2(x) = \begin{cases} 1 \text{ for } x \in \{1,3,6,8,10\}; \\ \omega \text{ for } x \in \{5,7,12\}; \\ -\omega \text{ for } x \in \{2,4,9,11\}. \end{cases}$$

One can check that τ_1 is i-perfect for $i = 2$ and $i = 4$ while τ_2 is i-perfect for every $i \in \{6,8,12\}$.

Case 2.2.3: $9 \neq k \neq 25$ and k is not the product of two distinct primes.
The hypotheses on k easily imply that $w(k) \geq 6$ and hence the chromatic number of $G^{\square}(k)$ is at least 3. It follows, by Lemma 3.4.2, that the chromatic number of $G(k,i,\rho)$ is also equal to $\frac{w^*(k)}{2}$. Then the assertion again follows from Lemma 3.3.2.

Case 2.2.4: k is the product of two distinct primes and $gcd(m,25) \neq 5$.
Here the chromatic number of $G^{\square}(k)$ is 2, hence Lemma 3.4.2 cannot be applied. On the other hand, it is clear that every connected component of $G(k,i,\rho)$ is a path or a cycle or a cycle with a pendent path so that its chromatic number does not exceed 3. Thus, for the hypotheses that (k,i,m) is admissible and that $\gcd(m,25) \neq 5$, we have $q \geq 7 > 2\chi(G(k,i,\rho))$ for every prime power factor q of m. The assertion follows again from Lemma 3.3.2.

Case 2.2.5: $k < 10^3$ is the product of two distinct primes and $gcd(m,25) = 5$.
Here we have checked by computer that the graph $G(k,i,\rho)$ has chromatic index 2, i.e., it is bipartite. Thus we have $q \geq 5 > 2\chi(G(k,i,\rho))$ for every prime power factor q of m and the assertion follows once again from Lemma 3.3.2. □

Putting together Corollary 3.2.3 and the above proposition we finally get Theorem 3.1.2.

By Lemma 3.3.2, the exception mentioned in the main theorem could be removed if one proves that when $k > 1000$ is the product of two distinct primes and $i > 2$ is even there is a suitable graph $G(k,i,\rho)$ which is bipartite, namely with chromatic number equal to 2. So we have the following open question.

Problem 3.5.2. *Given $k = pq$ with p, q odd distinct primes, and given i even with $\gcd(k,i) = 1$ and $4 \leq i \leq \frac{pq-1}{2}$, establish whether $G(k,i,\rho)$ with ρ defined as in (4.1) is bipartite or not.*

3.6 Infinite classes of i-perfect k-cycle systems

The knowledge of an i-perfect cycle decomposition of a complete multipartite graph is sometimes crucial for establishing the existence of an i-perfect cycle decomposition of the complete graph of the same order. This is because of the following straightforward result.

Lemma 3.6.1. *If there exists an i-perfect k-cycle decomposition of $\mathbb{K}_n^{(m)}$ and an i-perfect k-cycle decomposition of $\mathbb{K}_n$, then there exists an i-perfect k-cycle decomposition of $\mathbb{K}_{mn}$.*

As recalled in Chapter 1, a Hamiltonian cycle system of order k, or $HCS(k)$ for short, is a k-cycle decomposition of $\mathbb{K}_k$. Note that, as a special case of the above lemma, the main result of this chapter allows to get an i-perfect k-cycle decompositions of $\mathbb{K}_{km}$ whenever (i,k,m) is admissible, no prime power factor of m is less than $w(k)$, and an i-perfect $HCS(k)$ is available.

If k is a prime, we have $w(k)=2$ and the 2-transitive $HCS(k)$ (see [12]) is a *Steiner k-cycle system*, i.e., it is i-perfect for any possible i. Thus, by Corollary 3.1.3 and Lemma 3.6.1, the existence of an i-perfect $(\mathbb{K}_v, C_k)$-design with k a prime and $v \equiv k \pmod{2k}$ remains undecided only when $\gcd(\frac{v}{k}, 9) = 3$. We do not have these uncertain cases for the smallest primes k up to 19 in view of the results of Adams and Bryant [6] apart from the cases of an i-perfect $(\mathbb{K}_{57}, C_{19})$-design with $i = 2$ or 9, and of a 5-perfect $(\mathbb{K}_{13m}, C_{13})$-design for any odd m (see also [15], Table 12.50). The only other open case in [6] of an i-perfect $(\mathbb{K}_v, C_k)$-design with $k \le 19$ and $v \equiv k \pmod{2k}$, is that of an i-perfect $(\mathbb{K}_{45}, C_9)$-design with $i = 2$ or 4. We solve these cases in the next two propositions.

Proposition 3.6.2. *There exists a 2-perfect and a 4-perfect $(\mathbb{K}_{45}, C_9)$-design. There exists a 2-perfect and a 9-perfect $(\mathbb{K}_{57}, C_{19})$-design.*

Proof. Consider the following four 9-cycles with vertices in $\mathbb{Z}_{45}$:

$$A = (0,5,10,15,20,25,30,35,40); \quad B = (0,1,3,15,16,18,30,31,33);$$
$$C = (0,3,7,1,8,19,4,40,23); \quad D = (0,8,22,38,13,26,7,34,24).$$

One can check that

$$\{A+j \mid 0 \le j \le 4\} \cup \{B+j \mid 0 \le j \le 14\} \cup \{C+j, D+j \mid 0 \le j \le 44\}$$

is a (cyclic) 2-perfect $(\mathbb{K}_{45}, C_9)$-design.

Now consider the following two 19-cycles with vertices in $\mathbb{Z}_{56} \cup \{\infty\}$:

$$A = (\infty, 0, 26, 36, 1, 23, 47, 4, 33, 22, 50, 5, 32, 19, 51, 29, 8, 54, 28);$$

$$B = (0,1,3,6,2,8,13,4,19,11,27,20,43,5,22,34,54,12,31).$$

Here one can check that $[A+j \mid 0 \le j \le 27] \cup [B+j \mid 0 \le j \le 55]$ is a (1-rotational) 2-perfect $(\mathbb{K}_{57}, C_{19})$-design.

The above two constructions immediately give a 4-perfect $(\mathbb{K}_{45}, C_9)$-design and a 9-perfect $(\mathbb{K}_{57}, C_{19})$-design, respectively. This is because, as observed in [6], the existence of an i-perfect $(\mathbb{K}_v, C_k)$-design implies that of a j-perfect $(\mathbb{K}_v, C_k)$-design for any j such that $1 \le j \le \frac{k-1}{2}$ and $ij \equiv \pm 1 \pmod{k}$. □

Now we solve the existence question concerning 5-perfect $(\mathbb{K}_{13m}, C_{13})$-designs with m odd. In view of our result concerning i-perfect $(\mathbb{K}_{km}, C_k)$ designs with k an arbitrary prime, it is enough to assume that $\gcd(\frac{v}{13}, 9) = 3$, i.e., that $v = 39t$ with t odd and not divisible by 3.

Proposition 3.6.3. *Let t be a positive odd integer not divisible by 3. Then there exists a 5-perfect $(\mathbb{K}_{39t}, C_{13})$-design.*

Proof. We split the proof into two cases.

Case 1: $t = 1$.

Consider the following two 13-cycles with vertices in $\mathbb{Z}_{38} \cup \{\infty\}$:

$$A = (\infty, 0, 14, 37, 16, 5, 15, 34, 24, 35, 18, 33, 19),$$

$$B = (0, 1, 3, 6, 2, 7, 13, 4, 11, 31, 9, 34, 26).$$

One can check that $[A + j \mid 0 \leq j \leq 18] \cup [B + j \mid 0 \leq j \leq 37]$ is a (1-rotational) 5-perfect $(\mathbb{K}_{39}, C_{13})$-design.

Case 2: $t > 1$.

Consider the following three cycles with vertices in $\mathbb{Z}_{39} \times \mathbb{Z}_t$ where, in order to save space, we will write x_y instead of (x, y).

$$C_1 = (0_0,\ 18_1,\ 37_{-1},\ 22_2,\ 9_{-2},\ 25_1,\ 14_{-1},\ 14_1,\ 25_{-1},\ 9_2,\ 22_{-2},\ 37_1,\ 18_{-1});$$

$$C_2 = (0_0,\ 1_1,\ 3_{-1},\ 6_1,\ 2_{-1},\ 7_1,\ 13_{-1},\ 4_1,\ 11_{-1},\ 19_2\ , 9_{-2},\ 26_2,\ 12_{-2});$$

$$C_3 = (0_0,\ 1_{-1},\ 3_1,\ 6_{-1},\ 2_1,\ 7_{-1},\ 13_1,\ 4_{-1},\ 11_1,\ 19_{-2}\ , 9_2,\ 26_{-2},\ 12_2).$$

It is straightforward to check that we have:

$$\bigcup_{j=1}^{3} \Delta_i[C_j] = \bigcup_{x \in \mathbb{Z}_{39}} \{x\} \times [u_i(x), -u_i(x)] \qquad \text{for } i = 1 \text{ and } 5$$

where

$$u_1(x) = \begin{cases} 1 \text{ for } x \in \{\pm 1, \pm 18\}; \\ 2 \text{ for } x \in \{0, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 9, \pm 11, \pm 12, \pm 19\}; \\ 3 \text{ for } x \in \{\pm 8, \pm 15, \pm 16\}; \\ 4 \text{ for } x \in \{\pm 10, \pm 13, \pm 14, \pm 17\}. \end{cases}$$

and where

$$u_5(x) = \begin{cases} 1 \text{ for } x \in \{\pm 6, \pm 7, \pm 9, \pm 10, \pm 11, \pm 14, \pm 15, \pm 18 \pm 19\}; \\ 2 \text{ for } x \in \{\pm 1, \pm 4, \pm 5, \pm 12, \pm 16\}; \\ 3 \text{ for } x \in \{\pm 2, \pm 3, \pm 8, \pm 13, \pm 17\}; \\ 4 \text{ for } x = 0. \end{cases}$$

Considering that t is odd and not divisible by 3 by assumption, we have that $u_1(x)$ and $u_5(x)$ are units of $\mathbb{Z}_t$ for any $x \in \mathbb{Z}_{39}$. Thus we can write $[su_i(x), -su_i(x) \mid 1 \leq s \leq \frac{t-1}{2}] = \mathbb{Z}_t \setminus \{0\}$ for $i = 1$ and 5. Then, setting $\mathcal{C} = [(1, s) \cdot C_j \mid 1 \leq s \leq \frac{t-1}{2}; 1 \leq j \leq 3]$, we have

$$\Delta_1(\mathcal{C}) = \Delta_5(\mathcal{C}) = (\mathbb{Z}_{39} \times \mathbb{Z}_t) \setminus (\mathbb{Z}_{39} \times \{0\})$$

which means that $\mathcal{C}$ is a set of base cycles of a 5-perfect $(\mathbb{K}_{39}^{(t)}, C_{13})$-design. The assertion then follows by Lemma 3.6.1 because we also have a 5-perfect $(\mathbb{K}_{39}, C_{13})$-design constructed in Case 1. □

To find general constructions for i-perfect $HCS(k)$ with k a non-prime does not seem to be easy. The 1-*rotational* approach seems to be the more promising; it consists in finding a k-cycle C whose vertices are the elements of $\mathbb{Z}_{k-1} \cup \{\infty\}$ with the following properties:

- $C + \frac{k-1}{2} = C$;
- every $x \in \mathbb{Z}_{k-1} \setminus \{0\}$ can be represented as a difference of two adjacent vertices of C and also as a difference of two vertices which are at distance i in C.

Indeed, if one has a cycle C as above, then $\{C + i \mid 0 \leq i \leq \frac{k-3}{2}\}$ is an i-perfect $HCS(k)$.

In [30] and, independently, in [46], it has been recently proved that there exists a 1-rotational 3-perfect $HCS(k)$ whenever k is an odd integer greater than 5. Using a computer (see results in the Appendix 1) we have been able to prove the following result making believable that an i-perfect $HCS(k)$ exists for almost all possible pairs (i, k).

Proposition 3.6.4. *There exists an i-perfect $HCS(k)$ for any possible pair (i, k) with $k < 56$ except for $(i, k) \in \{(2, 9), (4, 9)\}$ and, possibly, for $(i, k) \in \{(7, 21), (6, 51), (13, 39), (15, 45)\}$.*

In view of Corollary 3.1.3, Lemma 3.6.1, and all the above results we can state the following theorem.

Theorem 3.6.5 (M. Buratti, S. C., X. Wang)**.** *Let $k \geq 3$ and let $v = mk$ be odd. An i-perfect k-cycle decomposition of $\mathbb{K}_v$ exists in each of the following cases:*

- *$k \leq 19$ and any possible i with the only definite exceptions of a 2-perfect $(\mathbb{K}_{15}, C_5)$-design, a 2-perfect $HCS(9)$, and a 4-perfect $HCS(9)$;*
- *$k \geq 23$ prime and any possible i provided that $\gcd(m, 9) \neq 3$;*
- *$i = 3$ and any $k \geq 7$ provided that $\gcd(m, 9) \neq 3$ and no prime power factor of m is less than $w(k)$;*
- *$k \in \{21, 25, 33, 35, 39, 51, 55\}$ and any possible i provided that $\gcd(i, k) = 1$ and $\gcd(m, 9) \neq 3$;*
- *$k \in \{27, 45, 49\}$ and any possible i provided that $\gcd(i, k) = 1$ and $\gcd(m, 9 \cdot 25) \in \{1, 9, 25, 9 \cdot 25\}$.*

Chapter 4

Perfect decompositions via strong difference families

In Chapter 3 we used the BRZ-construction in order to find i-perfect decompositions of the m-partite graphs $\mathbb{K}_k^{(m)}$. We succeeded for all odd values m and k such that the prime power factors of m are big enough. The strength of our work is that this result is independent of the value of i. On the contrary the weak point of this procedure is the assumption on m. In fact if k is odd it could be possible to get the existence of i-perfect decompositions of the m-partite graphs $\mathbb{K}_k^{(m)}$ for all odd m.

In this chapter instead we will focus our attention just on some special values of i but we try to get the existence of i-perfect k-cycle decompositions of the m-partite complete graphs $\mathbb{K}_k^{(m)}$ for all odd values of mk without any additional hypothesis on m.

For this purpose we introduce and study a new class of strong difference families: the i-perfect strong difference families (SDFs). In particular also the BRZ-construction turns out to use, implicitly, an i-perfect SDF. A first family of examples of i-perfect strong difference families in fact is given by the Paley SDMs used in the BRZ-construction. Then we develop a recursive construction of i-perfect strong difference maps and, focusing our attention on the values of $i \in \{3, 5, 7, 9, 11\}$, we provide infinite families of i-perfect SDMs.

Using this tool we prove that, if $i \in \{3, 5, 7, 9, 11\}$, there exists an i-perfect k-cycle decomposition of the complete m-partite graph $\mathbb{K}_k^{(m)}$ for all odd $k > 2i$ and for all odd m up to a set of seven possible exceptions. In case $i = 3$ we are able to remove these exceptions. Then, as usual, according to Lemma 3.6.1, we apply these new i-perfect decompositions of the m-partite graphs in order to achieve new i-perfect decompositions of the complete graphs $\mathbb{K}_{mk}$. In particular, for $i = 3$, using the known result on the existence of a Hamiltonian 3-perfect decomposition of $\mathbb{K}_k$ (see [30] and [46]), we prove that there exists a 3-perfect k-cycle decomposition of the complete graph $\mathbb{K}_{mk}$ if and only if mk is odd and $k \geq 7$.

4.1 The i-perfect SDFs

The concept of relative difference families has been introduced by M. Buratti (see [21]) in order to provide constructions of GDDs and then considered also over an

arbitrary graph in order to obtain decompositions of the complete m-partite graphs (see Definition 2.1.19 and Theorem 2.1.23). Here we recall the definition of i-perfect relative difference family (briefly DF) given by M. Buratti and A. Pasotti in [28].

Definition 4.1.1. *Let Γ be a graph and let Γ^i be the graph with the same vertices as Γ and whose edges are the pairs of vertices at distance i in Γ.*
An i-perfect (G, H, Γ, λ)-DF is a collection $\mathfrak{F}$ of injective maps from $V(\Gamma)$ to G such that both the lists

$$\Delta_\Gamma \mathfrak{F} := \bigcup_{f\in\mathfrak{F}} [f(x) - f(y)|\ \{x, y\} \in E(\Gamma)]$$

$$\Delta_{\Gamma^i} \mathfrak{F} := \bigcup_{f\in\mathfrak{F}} [f(x) - f(y)|\ \{x, y\} \in E(\Gamma^i)]$$

cover $G \setminus H$ exactly λ times while they do not contain any element of H.

This kind of DFs have been introduced in order to construct i-perfect decompositions of the complete m-partite graphs. The link between i-perfect DFs and i-perfect decompositions is explained by the following proposition (see [28]):

Proposition 4.1.2 (M. Buratti, A. Pasotti)**.** *An i-perfect (G, H, C_k, λ)-DF yields an i-perfect k-cycle decomposition of $\lambda\mathbb{K}_n^{(m)}$ where $m = |G : H|$ and $n = |H|$.*

Proof. Let $\mathfrak{F}$ be an i-perfect (G, H, C_k, λ)-DF. Then, because of Theorem 2.1.23, we have that $\mathfrak{F}$ yields a k-cycle decomposition $\mathfrak{C}$ of $\lambda\mathbb{K}_n^{(m)}$.

Given a graph Γ we denote by Γ^i the graph with the same vertices as Γ and whose edges are the pairs of vertices at distance i in Γ (see Definition 4.1.1). Moreover, since $\mathfrak{F}$ is i-perfect, we have that $\mathfrak{F}$ is a (G, H, C_k^i, λ)-DF. Therefore, again because of Theorem 2.1.23, also the family of cycles $\mathfrak{C}^i := [C^i : C \in \mathfrak{C}]$ is a k-cycle decomposition of $\lambda\mathbb{K}_n^{(m)}$. But this means that $\mathfrak{C}$ is an i-perfect k-cycle decomposition of $\lambda\mathbb{K}_n^{(m)}$ □

As we have seen in Chapter 2, M. Buratti and L. Gionfriddo introduced the concept of a strong difference family over an arbitrary graph Γ in order to obtain a construction of DFs. Here we define a class of strong difference families, in order to obtain a construction of i-perfect DFs.

Definition 4.1.3. *Given a graph Γ let Γ^i be the graph with the same vertices as Γ and whose edges are the pairs of vertices at distance i in Γ (see Definition 4.1.1). Let G be a group and let $\Sigma := [\sigma_1, \ldots, \sigma_t]$ be a family of maps $\sigma_j : V(\Gamma) \to G$ for $j \in \{1, \ldots, t\}$.*
We say that Σ is an i-perfect (G, Γ, μ)-SDF if both the lists:

$$\Delta_\Gamma \Sigma = \bigcup_{\sigma\in\Sigma} [\sigma(x) - \sigma(y)|\ \{x, y\} \in E(\Gamma)]$$

$$\Delta_{\Gamma^i} \Sigma = \bigcup_{\sigma\in\Sigma} [\sigma(x) - \sigma(y)|\ \{x, y\} \in E(\Gamma^i)]$$

cover all of G exactly μ times.

In case the family is formed by just one map, i.e. $\Sigma := [\sigma]$ we say that σ is a (G, Γ, μ) strong difference map (SDM).

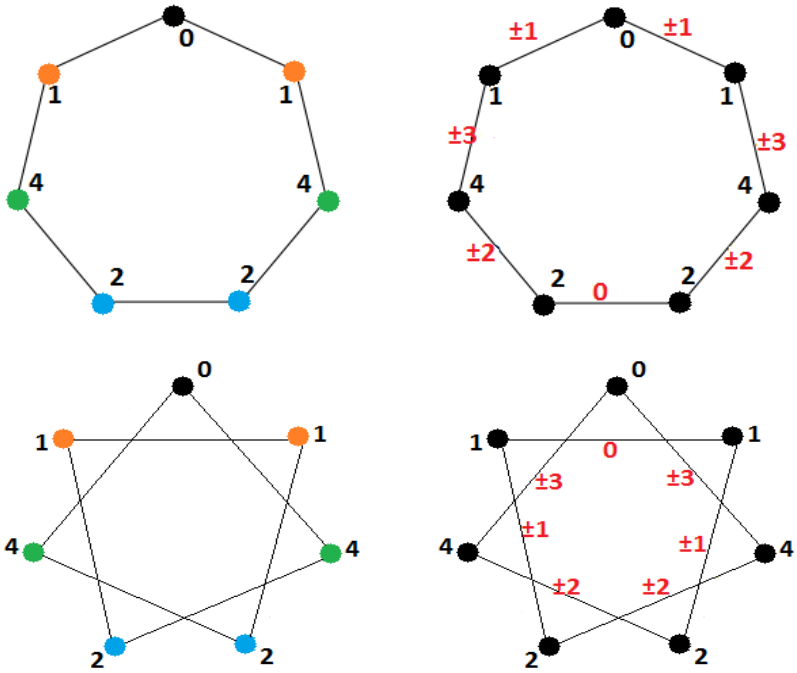
The first example of i-perfect SDF we provide is given by a Paley SDM. We have already seen these maps in Theorem 2.2.6. Moreover the fact that these maps are i-perfect has been implicitly used in Chapter 2 in the proof of Theorem 2.3.3. As usual we denote by $C_k := (v_0, \dots, v_{k-1})$ a cycle of length k.

Example 4.1.4. *Let us consider the map* $\sigma_7 : \ v_j \in C_7 \to j^2 \in \mathbb{Z}_7$. *We have already seen in Theorem 2.2.6 that* σ_7 *is a* $(\mathbb{Z}_7, C_7, 2)$*-SDM. Moreover we have that, for* i *equals to* 2 *and for* i *equals to* 3,

$$\Delta_{C_7^i}\sigma = [\sigma(x) - \sigma(y)| \ \{x, y\} \in E(C_7^i)]$$

cover all of G *exactly twice. Therefore* σ *is a* 2*- and* 3*-perfect* $(\mathbb{Z}_7, C_7, 2)$*-SDM.*

In the following pictures are shown $\Delta_{C_7}\{\sigma_7\}$ and $\Delta_{C_7^2}\{\sigma_7\}$:



We can generalize this example getting the following theorem.

Theorem 4.1.5 (Paley SDM)**.** *Let* k *be an odd integer. The map* $\sigma_k : \ v_j \in C_k \to j^2 \in \mathbb{Z}_k$ *is an* i*-perfect* $(\mathbb{Z}_k, C_k, 2)$*-SDM (strong difference map) for all* i*'s such that* $gcd(i, k) = 1$.

Proof. Let Ω be a subset of $\mathbb{Z}_k \setminus \{0\}$ such that if $\omega \in \Omega$ then also $-\omega \in \Omega$. We recall that the *circulant graph* of order k and with connection set Ω is the simple graph with vertex-set $\mathbb{Z}_k$ and whose edges are precisely those of the form $\{x, \omega + x\}$ with $x \in \mathbb{Z}_k$ and $\omega \in \Omega$. As a special case of Proposition 4.5 in [25], the map $\sigma_k : j \longrightarrow j^2$ is a $(\mathbb{Z}_k, \Gamma, 2)$ *strong difference map* for every *circulant graph* Γ of order k and connection set of the form $\{l, -l\}$ with $\gcd(l, k) = 1$. It follows that the map $\sigma_k : \ v_j \in C_k \to j^2 \in \mathbb{Z}_k$ is an i-perfect $(\mathbb{Z}_k, C_k, 2)$*-SDM* for all i's such that $gcd(i, k) = 1$. □

4.1.1 The fundamental construction II

In this paragraph we follow the underlying idea, and the notation, of the fundamental construction of [25] (see Theorem 2.2.7) adapted to the i-perfect case. In this way we will get a construction of i-perfect difference families.

The following Theorem formalizes a simple but effective idea, that has been already implicitly used in [24] (see Theorem 2.3.3) and in [29] in order to construct i-perfect decompositions of the complete graph $\mathbb{K}_v$ and of the complete m-partite graph $\mathbb{K}_n^{(m)}$.

Theorem 4.1.6. *Let Γ be a graph, let G be an additive group, and let R be a ring with additive group H. Given an n-tuple $(f_1, \dots f_n)$ of maps from $V(\Gamma)$ to $G \times H$ we set:*

$$f_j(x) = (\sigma_j(x), \tau_j(x)) \ \forall x \in V(\Gamma), \forall j \in \{1, \dots, n\}$$

$$\Delta_\Gamma[f_1, \dots, f_n] = \bigcup_{j=1}^{n} \bigcup_{\{x,y\} \in E(\Gamma)} [f_j(x) - f_j(y)];$$

as we have seen in Chapter 2, there exist multisets L_g of elements of H such that:

$$\Delta_\Gamma[f_1, \dots, f_n] = \bigcup_{g \in G} \{g\} \times L_g.$$

Similarly, given a positive integer i, we set:

$$\Delta_{\Gamma^i}[f_1, \dots, f_n] = \bigcup_{j=1}^{n} \bigcup_{\{x,y\} \in E(\Gamma^i)} [f_j(x) - f_j(y)];$$

as above, there exist multisets L_g^i of elements of H such that:

$$\Delta_{\Gamma^i}[f_1, \dots, f_n] = \bigcup_{g \in G} \{g\} \times L_g^i.$$

Assume that the following conditions hold:

1) $\sigma_j(x) = \sigma_j(y)$ with $x \neq y \implies \tau_j(x) - \tau_j(y) \in U(R), \forall j \in \{1, \dots, n\}$;

2) $\exists S \subset H \setminus \{0\}$ such that $S \cdot L_g = S \cdot L_g^i = \lambda(H \setminus \{0\})$ $\forall g \in G$.

Then there exists an i-perfect $(G \times H, G \times \{0\}, \Gamma, \lambda)$-$DF$.

Proof. Because of Theorem 2.2.7 there exists a $(G \times H, G \times \{0\}, \Gamma, \lambda)$-$DF$ that we denote by $\mathfrak{F}$. Moreover, we also have that

$$\Delta_{\Gamma^i}[f_1, \dots, f_n] = \bigcup_{g \in G} \{g\} \times L_g^i.$$

Therefore, again because of Theorem 2.2.7, $\mathfrak{F}$ is also a $(G \times H, G \times \{0\}, \Gamma^i, \lambda)$-$DF$ and hence $\mathfrak{F}$ is an i-perfect $(G \times H, G \times \{0\}, \Gamma, \lambda)$-$DF$. □

As a consequence of Theorem 4.1.6 we can provide the main construction of this chapter. We first give the following definition.

Definition 4.1.7. *Let σ be an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM. We consider the family of graphs $\Omega = \Omega(i,k,\rho)$: $V(\Omega) = \{1,\dots,\frac{k-1}{2}\}$, ρ is a function $\mathbb{Z}_k \to \{-1,1\}$ and the edges are given by $E^\sigma \cup E(k,1,\rho) \cup E^-(k,i,\rho) \cup E^+(k,i,\rho)$ where:*

$\{x,y\} \in E^\sigma \iff \sigma(v_x) = \sigma(v_y)$ *or, with abuse of notation,* $\sigma(x) = \sigma(y)$;

$\{x,y\} \in E(k,1,\rho) \iff x - y \equiv \pm 1 \ (mod\ k)$ *and* $\rho(x) = \rho(y)$;

$\{x,y\} \in E^-(k,i,\rho) \iff x - y \equiv \pm i \ (mod\ k)$ *and* $\rho(x) = \rho(y)$;

$\{x,y\} \in E^+(k,i,\rho) \iff x + y \equiv \pm i \ (mod\ k)$ *and* $\rho(x) \neq \rho(y)$.

Then we define the function $w(\sigma)$ as two times the minimum $\chi(\Omega)$ (chromatic number of Ω) where Ω lies in the family $\Omega(i,k,\rho)$.

We are now ready to provide a further generalization of the BRZ-construction that shows how we use the i-perfect SDMs in order to construct i-perfect k-cycle decompositions of $\mathbb{K}_k^{(m)}$.

Theorem 4.1.8 (Generalized BRZ-construction)**.** *Let σ be an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM such that $\sigma(v_j) = \sigma(v_{k-j})$.*
Then there exists an i-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$ whenever mk is odd and all prime power factors of m are greater than the function $w(\sigma)$.

Proof. As done in Chapter 3, given a natural number m, we denote by $R(m)$ the ring of order m which is the direct product of all fields whose orders are the prime power factors of m. Let $\rho : \mathbb{Z}_k^+ = \{1,\dots,\frac{k-1}{2}\} \longrightarrow \{1,-1\}$ and let t be the chromatic number of $\Omega(k,i,\rho)$. Assume that all prime power factors of m are greater than $2t$ and let ω be an element of $R(m)$ whose j-th coordinate is a primitive element of the j-th factor of $R(m)$. Then take a vertex coloring c of $\Omega(k,i,\rho)$ whose colors are the elements of the subset $\{\omega^j \mid 0 \leq j \leq t-1\}$ of $R(m)$.

Then, identified $V(C_k)$ with $\mathbb{Z}_k$, we consider the odd function $\tau : V(C_k) = \mathbb{Z}_k \to R(m)$ such that:

$$\begin{cases} \tau(0) = 0; \\ \tau(x) = \rho(x)c(x) \text{ for } x \in \{1,\dots,\frac{k-1}{2}\}; \\ \tau(x) = -\tau(k-x) \text{ for } x \in \{\frac{k+1}{2},\dots,k-1\}. \end{cases}$$

We want to prove that such function satisfies the hypothesis of Theorem 4.1.6. Let S be a complete system of representatives for the equivalence relation in $R \setminus \{0\}$ defined by $r \sim r'$ if and only if $r' = \pm r$. By the symmetry of σ and τ we have:

$$\Delta_{C_k}[(\sigma,\tau)] = \bigcup_{g \in \mathbb{Z}_k} \{g\} \times L_g = \bigcup_{g \in \mathbb{Z}_k} \{g\} \times [\delta(g), -\delta(g)]$$

and

$$\Delta_{C_k^i}[(\sigma,\tau)] = \bigcup_{g \in \mathbb{Z}_k} \{g\} \times L_g^i = \bigcup_{g \in \mathbb{Z}_k} \{g\} \times [\delta_i(g), -\delta_i(g)].$$

Since all prime power factors of m are greater than $2t$ we have that $\delta(g) \in \mathbb{U}(R(m))$ and $\delta_i(g) \in \mathbb{U}(R(m))$. Hence it follows that:

$$S \cdot L_g = S \cdot L_g^i = (H \setminus \{0\}) \ \forall g \in \mathbb{Z}_k.$$

Because of the hypothesis on the prime power factors of m:

$$\sigma(x) = \sigma(y) \implies \tau(x) - \tau(y) \in \mathbb{U}(R(m)).$$

Therefore, by Theorem 4.1.6, we obtain the existence of an i-perfect $(\mathbb{Z}_k \times R(m), \mathbb{Z}_k \times \{0\}, C_k, 1)$-$DF$. It follows that there exists an i-perfect decomposition of the m-partite graph $\mathbb{K}_k^{(m)}$. □

In view of the Definition 4.1.7 and Theorem 4.1.8 the main result of [24], that is Theorem 3.1.2 of the previous section, can be seen as follows:

Theorem 4.1.9 (M. Buratti, S. C., X. Wang)**.** *Let us consider the Paley SDM σ_k. We have that $w(\sigma_k) := \max(4, 2^t\sqrt{k/k^*})$ where k^* is the square-free part of k, and t is the number of prime factors of k^* with the possible exception of the case where the following facts simultaneously hold: $k > 1000$ is the product of two distinct primes; $i > 2$ is even;* $\gcd(m, 25) = 5$.

Now, similarly to what we have done in Chapter 3 (see also [24]), given an odd integer k and $l \in \mathbb{Z}_k$, we define the sets $A_l(\sigma) := \{x |\ x \in \{1, \ldots, \frac{k-1}{2}\}$ and $\sigma(x) = l\}$. We want to use the size $\max_{l \in \mathbb{Z}_k} |A_l(\sigma)|$ in order to give an upperbound to the function $w(\sigma)$. In this regard we use Lemma 3.4.1 and Lemma 3.4.2 of Chapter 3. These results are consequences of Brooks' Theorem on vertex colorings (see, e.g., [61]). Here we apply these lemmas in the same spirit of Proposition 3.5.1 providing the following bound:

Lemma 4.1.10. *Let σ be an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM and let*

$$M = \max_{l \in \mathbb{Z}_k} |A_l(\sigma)|.$$

Then we have that $w(\sigma) = \max(4, 2M)$ with the possible exception of the case in which $M = 2$ and i is even. In this case $w(\sigma) \in \{4, 6\}$.

The proof of this Lemma is essentially the same as of Proposition 3.5.1, we just have to replace $\frac{w^*(k)}{2}$ with M, G with Ω and $G^{\square}(k)$ with Ω^{σ} that is the graph with the same vertices as Ω and with edges set E^{σ}. However, for completeness, we write the proof anyway.

Proof. We divide the proof in two cases.

Case 1: Suppose that i is odd.

Let us consider the map $\bar{\rho} : \mathbb{Z}_k \to \{-1, 1\}$ such that $\bar{\rho}(x) := (-1)^x$. Since i is odd, the edges of $\Omega(i, k, \bar{\rho})$ are the following ones:

$$E(\Omega) := \begin{cases} E^{\sigma} := \{x, y\} : x \neq y \text{ and } \sigma(x) = \sigma(y) \\ \{x, y\} : x + y = i. \end{cases}$$

Since the edges of the form $\{x, y\} : x+y = i$ are a matching, if $M > 1$ because of Lemma 3.4.1 we have that the chromatic number of Ω that of Ω^σ that is the graph with the same vertex set of Ω and with edges set E^σ. Since Ω^σ is a disjoint union of complete graphs we have that, in case $M > 1$, $\chi(\Omega^\sigma) = \chi(\Omega) = M$. In case $M = 1$ we have that $E^\sigma = \emptyset$ and therefore $\chi(\Omega) = 2$. It follows that $w(\sigma) \leq 2(M + 1)$ and the equality holds if and only if $M = 1$.

Case 2: Suppose that i is even.

Let $\frac{k-i-1}{2} = ni+r$, with $0 \leq r \leq i$, be the Euclidean division of $\frac{k-i-1}{2}$ by i so that we have $k = (2n + 1)i + 2r + 1$ with $0 \leq r < i$. Now let $\rho : \mathbb{Z}_k^+ = \{1, \ldots, \frac{k-1}{2}\} \longrightarrow \{1, -1\}$ be the map implicitly defined by the rules

$$\rho(1) = 1; \qquad \rho(x) = \rho(x + 1) \Longleftrightarrow x \equiv r \pmod{i} \tag{4.1}$$

and let $\Omega^*(k, i, \rho)$ be the subgraph of $\Omega(k, i, \rho)$ obtained by removing all edges of E^σ. By (4.1), we have $\rho(x) = \rho(x + 1)$ if and only if $x \equiv r \pmod{i}$. Thus we have

$$E(k, 1, \rho) = \{\{r, r + 1\}, \{i + r, i + r + 1\}, \ldots, \{vi + r, vi + r + 1\}\}$$

with $v = \lfloor \frac{k-3-2r}{2i} \rfloor$ and hence we see that $\Omega(k, 1, \rho)$ is a matching.

Assume that x and $x + i$ are elements of $\mathbb{Z}_k^+$. Recall that we have $0 \leq r < i$, therefore there is exactly one element $\xi \in \mathbb{Z}_k^+$ such that $x \leq \xi < x + i$ and $\xi \equiv r \pmod{i}$. It is clear by (4.1) that for $x \leq z \leq \xi$ we have $\rho(z) = \rho(x)$ if and only if x and z have the same parity. Applying this remark in the particular case $z = \xi$ we get:

$$\rho(\xi) = (-1)^{x+\xi}\rho(x) \tag{4.2}$$

Analogously, by (4.1), for $\xi + 1 \leq z \leq x + i$ we have $\rho(z) = \rho(\xi + 1)$ if and only if z and $\xi + 1$ have the same parity. Thus, in particular, we have $\rho(x + i) = (-1)^{\xi+1+x+i}\rho(\xi + 1)$. By (4.1) again, we have $\rho(\xi + 1) = \rho(\xi)$ since $\xi \equiv r \pmod{i}$. Hence, using (4.2) and recalling that i is even, we can write:

$$\rho(x + i) = (-1)^{\xi+1+x+i}\rho(\xi) = (-1)^{2\xi+2x+i+1}\rho(x) = -\rho(x) \tag{4.3}$$

The above equality guarantees that $E^-(k, i, \rho)$ is empty.

The set of pairs of elements of $\mathbb{Z}_k^+$ summing up to i or $-i$ modulo k is the union of the two matchings N and N' defined as follows:

$N = \{\{j, i - j\} \mid 1 \leq j \leq \frac{i}{2} - 1\}$;

$N' = \{\{\frac{k-1}{2} - i + j, \frac{k+1}{2} - j\} \mid 1 \leq j \leq \frac{i}{2}\}$

For $1 \leq j < \frac{i}{2}$ we have $\rho(j) = -\rho(i - j)$ if and only if $j \leq r \leq i - j - 1$. Thus the pairs $\{j, i - j\}$ of N belonging to $E^+(k, i, \rho)$ are those having $j \leq r$ if $r < \frac{i}{2}$ or those having $j \leq i - r - 1$ if $r \geq \frac{i}{2}$.

By definition of r, the element $\xi := \frac{k-1}{2} - \frac{i}{2}$ is the only element of the interval $[\frac{k-1}{2} - i, \frac{k-1}{2}]$ which is congruent to r modulo i. Now note that we have $\frac{k-1}{2} - i + j \leq \xi < \frac{k+1}{2} - j$ for $1 \leq j \leq \frac{i}{2}$. Hence, with the same reasoning leading to (4.3), we have that $\rho(x) = \rho(y)$ for every pair $\{x, y\} \in N'$. Thus no pair of N' belongs to $E^+(k, i, \rho)$.

We conclude that we have

$$E^+(k,i,\rho) = \begin{cases} \{\{j, i-j\} \mid 1 \le j \le r\} \text{ if } r < \frac{i}{2} \\ \{\{j, i-j\} \mid 1 \le j \le i-r-1\} \quad \text{if } r \ge \frac{i}{2} \end{cases}$$

Note, in particular, that $E^+(k,i,\rho)$ is empty when $r = 0$ or $i-1$. Thus, in the extremal cases that $r = 0$ or $i-1$, which means $k \equiv i \pm 1 \pmod{2i}$, the graph $\Omega^*(k,i,\rho)$ is a matching.

For $1 \le r \le i-2$ the graph $\Omega^*(k,i,\rho)$ fails to be a matching just because, among its connected components there is a path on 3 vertices that is $(i-r, r, r+1)$ or $(i-r-1, r+1, r)$ according to whether $r < \frac{i}{2}$ or not, respectively. Anyway, because of Lemma 3.4.2 (see also [24]), if $M \ge 3$ we have that $\chi(\Omega) = M$. Moreover if $M = 1$ we have that E^σ is empty and therefore $\chi(\Omega) = 2$. Lastly, if $M = 2$ we consider $\Omega - \{x, y\}$, that is the graph with the same vertices as Ω and with edges $E(\Omega) - \{x, y\}$. Because of the Lemma 3.4.1 we have $\chi(\Omega - \{x, y\}) = 2$ and therefore $\chi(\Omega) \le 3 = M + 1$. It follows $w(\sigma) \le 2(M+1)$ and the equality holds if $M = 1$ and possibly if $M = 2$. □

4.2 A recursive construction

This section, that is the core of this chapter, is devote to provide a recursive construction of i-perfect SDFs that works for odd values of i and k. We first show a special case of it.

We note that, identifying $V(C_k) = (v_0, \dots, v_{k-1})$ with $\mathbb{Z}_k$, we can see a $(\mathbb{Z}_k, C_k, 2)$-SDM, say σ, as the k-tuple of elements of $\mathbb{Z}_k$ given by:

$$(\sigma(0), \sigma(1), \dots, \sigma(k-2), \sigma(k-1)).$$

Example 4.2.1. *Let now $k = 15$ and let us consider the following map:*

$$\sigma := (5, -3, 3, -2, 2, -1, 1, 0, 0, 1, -1, 2, -2, 3, -3).$$

Here we check that σ is a 3-perfect $(\mathbb{Z}_{15}, C_{15}, 2)$-$SDM$. In fact we have that

$$\Delta_{C_{15}}(\sigma) = \pm(2[5+3, -3-3, 3+2, -2-2, 2+1, -1-1, 1-0] \cup [0]) = 2\mathbb{Z}_{15}$$

and

$$\Delta_{C_{15}^3}(\sigma) = \pm(2[-3-3, 5+2, -3-2, 3+1, -2-1, 2+0, -1+0] \cup [0]) = 2\mathbb{Z}_{15}.$$

We call, with abuse of language, negative the terms that appear with a minus sign in σ and positive the others. We extend the map σ adding 1 to the positive terms, subtracting 1 to the negative ones and to the zeros and finally inserting the string $(1, 0, 0, 1)$ in the middle of σ. This procedure gives us the following map:

$$\sigma' := (6, -4, 4, -3, 3, -2, 2, -1, 1, 0, 0, 1, -1, 2, -2, 3, -3, 4, -4).$$

Then, by reiterating this process, if $k = 4l - 1$ we obtain the following map:

$$\sigma^k := (l+1, 1-l, l-1, \dots, -2, 2, -1, 1, 0, 0, 1, -1, 2, -2, \dots, l-1, 1-l).$$

We will prove in Proposition 4.2.6 that also this map is a 3-perfect strong difference map.

In order to generalize this example we need, as an ingredient, a suitable kind of i-perfect SDMs. Let $k = 2h+1$ be an odd positive integer, we denote $\mathbb{Z}_k^+ = \{1, \dots, h\}$ and $\mathbb{Z}_k^- = \{-h, \dots, -1\} = \{h, \dots, k-1\}$.

Definition 4.2.2. *Let $\sigma : V(C_k) \to \mathbb{Z}_k = \mathbb{Z}_{2h+1}$ be an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM. We say that σ is recursive if, identifying $V(C_k) = (v_0, \dots, v_{k-1})$ with $\mathbb{Z}_k := \{0, 1, \dots, k-1\}$, we have:*

1 $\sigma(j) = \sigma(k-j)$ for all $j \in \mathbb{Z}_k$.

2 $\sigma(h-j) = (-1)^{j+1}\lceil \frac{j}{2} \rceil$ for $0 \leq j \leq i$. In particular $\sigma(h) = 0$.

3 Let $0 < j \leq h$ then $\sigma(h-j) \in \mathbb{Z}_k^+$ if j is odd and $\sigma(h-j) \in \mathbb{Z}_k^-$ if j is even.

Remark 4.2.3. *We remark that, if σ is a recursive i-perfect $(\mathbb{Z}_{2h+1}, C_{2h+1}, 2)$-$SDM$, then i is necessarily odd. In fact, by contradiction, let us suppose that i is even. Then we would have that:*

$$\frac{i}{2} = \sigma(h) - \sigma(h-i) = \sigma(h-i+1) - \sigma(h+1) = \sigma(h+1) - \sigma(h+1+i) = \sigma(h+i) - \sigma(h).$$

Therefore the value $\frac{i}{2}$ would appear at least four times in the list $\Delta_{C_{2h+1}^i}(\sigma)$. But this is a contradiction since the list $\Delta_{C_{2h+1}^i}(\sigma)$ should cover every element of $\mathbb{Z}_{2h+1}$ exactly twice.

This definition is inspired by the Walecki construction (see Theorem 1.2.3): in fact, in these SDMs, the labels $\sigma(h-i), \dots, \sigma(h)$ of the vertices between v_{h-i} and v_h are the same of the ones of the cycle of Theorem 1.2.3. We can understand better this property with the following example:

Example 4.2.4. *Let us consider the map of Example 4.2.1:*

$$\sigma := (5, -3, 3, -2, 2, -1, 1, 0, 0, 1, -1, 2, -2, 3, -3).$$

We can check that σ is a recursive 3-perfect $(\mathbb{Z}_{15}, C_{15}, 2)$-$SDM$. Moreover the labels of the vertices $(v_1, v_2, v_3, v_4, v_5, v_6, v_7)$ are $(-3, 3, -2, 2, -1, 1, 0)$, that are the same of the Walecki sequence.

Then, given a recursive SDM, we obtain an infinite family of SDMs as follows:

Construction 4.2.5. *Let σ be a recursive i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM. Then there exists a recursive i-perfect $(\mathbb{Z}_{k'}, C_{k'}, 2)$-$SDM$, σ', for all $k' \equiv k \pmod 4$ greater than k. Moreover we have that:*

$$\max_{l \in \mathbb{Z}_k} |A_l(\sigma)| = \max_{l \in \mathbb{Z}_{k'}} |A_l(\sigma')|.$$

Proof. We proceed by induction. Therefore it is sufficient to prove the existence of a recursive i-perfect $(\mathbb{Z}_{k+4}, C_{k+4}, 2)$-$SDM$. Let us consider $\sigma' : \mathbb{Z}_{k+4} \to \mathbb{Z}_{k+4}$ defined as:

- $\sigma'(j) = \sigma(j) + 1$ if $0 \leq j \leq h$ (where $k = 2h+1$) and $h - j$ is odd.
- $\sigma'(j) = \sigma(j) - 1$ if $0 \leq j \leq h$ and $h - j$ is even.

- $\sigma'(h+2) = 0$ and $\sigma'(h+1) = 1$.
- σ' is symmetric i.e. $\sigma'(j) = \sigma'((k+4) - j)$, $\forall j \in \mathbb{Z}_{k+4}$.

First of all we note that, since $\sigma(h-j) = (-1)^{j+1}\lceil \frac{j}{2} \rceil$ for all $0 \leq j \leq i$, we have that $\sigma'(h+2-j) = (-1)^{j+1}\lceil \frac{j}{2} \rceil$ for all $0 \leq j \leq i+2$. Thus σ' satisfies the property 2 of Definition 4.2.2.

We set $\Delta_1(\sigma') = [\sigma'(x) - \sigma'(y) | \{x,y\} \in E(C_{k+4})]$ and $\Delta_i(\sigma') = [\sigma'(x) - \sigma'(y) | \{x,y\} \in E(C^i_{k+4})]$. Let us prove that $\Delta_1(\sigma') = 2\mathbb{Z}_{k+4}$. Since σ is a strong difference map such that $\sigma(j) = \sigma(k-j)$, we know that the list:

$$\bigcup_{j \in \{0,\ldots,\frac{k-1}{2}-1\}} \pm[\sigma(j+1) - \sigma(j)] = \mathbb{Z}_k \setminus \{0\}.$$

Since if $\sigma'(j) = \sigma(j) + 1$ then $\sigma'(j+1) = \sigma(j+1) - 1$ and viceversa, it follows that

$$\bigcup_{j \in \{0,\ldots,\frac{k-1}{2}-1\}} \pm[\sigma'(j+1) - \sigma'(j)] = \mathbb{Z}_{k+4} \setminus [0,1,-1,2,-2].$$

Since $\sigma'(h+1) - \sigma'(h) = 2$ and $\sigma'(h+2) - \sigma'(h+1) = -1$ we obtain that:

$$\bigcup_{j \in \{0,\ldots,\frac{k-1}{2}+1\}} \pm[\sigma'(j+1) - \sigma'(j)] = \mathbb{Z}_{k+4} \setminus \{0\}.$$

As consequence, because of the symmetry of σ', we have that $\Delta_1(\sigma') = 2\mathbb{Z}_{k+4}$.

Similarly we prove that $\Delta_i(\sigma') = 2\mathbb{Z}_{k+4}$. In fact we know that:

$$\mathbb{Z}_k \setminus \{0\} = \bigcup_{j \in \{-\frac{i-1}{2},\ldots,\frac{k-i}{2}-1\}} \pm[\sigma(j+i) - \sigma(j)] =$$

$$\Big(\bigcup_{j \in \{-\frac{i-1}{2},\ldots,\frac{k-i}{2}-i\}} \pm[\sigma(j+i) - \sigma(j)] \Big) \cup \Big(\bigcup_{j \in \{\frac{k-i}{2}-i+1,\ldots,\frac{k-i}{2}-1\}} \pm[\sigma(j+i) - \sigma(j)] \Big).$$

Moreover, since σ is recursive (because of the property 2 of Definition 4.2.2) we have that

$$\bigcup_{j \in \{\frac{k-i}{2}-i+1,\ldots,\frac{k-i}{2}-1\}} \pm[\sigma(j+i) - \sigma(j)] = \pm\{1,\ldots,i-1\}$$

and hence

$$\bigcup_{j \in \{-\frac{i-1}{2},\ldots,\frac{k-i}{2}-i\}} \pm[\sigma(j+i) - \sigma(j)] = \mathbb{Z}_k \setminus \pm\{0,\ldots,i-1\}.$$

Then, because of the definition of σ' we have that, for $j \in \{-\frac{i-1}{2},\ldots,\frac{k-i}{2}-i\}$ if $\sigma'(j) = \sigma(j)+1$ then $\sigma'(j+i) = \sigma(j+i) - 1$ and viceversa. Thus

$$|\sigma'(j+i) - \sigma'(j)| = |(\sigma(j+i) - \sigma(j))| + 2.$$

It follows that:

$$\bigcup_{j\in\{-\frac{i-1}{2},\ldots,\frac{k-i}{2}-i\}} \pm[\sigma'(j+i)-\sigma'(j)] = \mathbb{Z}_{k+4} \setminus \pm\{0,\ldots,i-1+2\}.$$

Since we also have that $\sigma'(h+2-j) = (-1)^{j+1}\lceil\frac{j}{2}\rceil$ for $0 \leq j \leq i+2$, we get:

$$\bigcup_{j\in\{\frac{k-i}{2}-i+1,\ldots,\frac{k-i}{2}-1+2\}} \pm[\sigma'(j+i)-\sigma'(j)] = \pm\{1,\ldots,i-1+2\}.$$

Therefore

$$\bigcup_{j\in\{-\frac{i-1}{2},\ldots,\frac{k-i}{2}+1\}} \pm[\sigma'(j+i)-\sigma'(j)] = \mathbb{Z}_{k+4} \setminus \{0\}.$$

It follows that σ' is an i-perfect SDM. Since, for construction, σ' realizes also the other properties (1 and 3) of the definition of recursive SDM we obtain the existence of a recursive, i-perfect $(\mathbb{Z}_{k+4}, C_{k+4}, 2)$-$SDM$.

For the second part of the theorem we only need to show that

$$\max_{l\in\mathbb{Z}_k} |A_l(\sigma)| = \max_{l\in\mathbb{Z}_{k+4}} |A_l(\sigma')|,$$

where σ' is the i-perfect $(\mathbb{Z}_{k+4}, C_{k+4}, 2)$-$SDM$ defined above, then the conclusion follows by induction. Suppose that $\sigma'(x) = \sigma'(y)$ and $1 \leq x < y \leq (k+3)/2$. We have the following three possibilities.

Case 1: $1 \leq x < y \leq (k-1)/2 = h$, x and y have the same parity, and $\sigma(x) = \sigma(y)$.

Case 2: $y = (k+1)/2 = h+1$, and $\sigma'(x) = \sigma'(y)$. Then $\sigma'(y) = 1$, we get $\sigma'(x) = 1$ for $1 \leq x \leq h$. Since $1 \in \mathbb{Z}^+_{k+4}$ and σ' is recursive we have that $h+2-x$ is odd. Therefore also $h-x$ is odd and hence $\sigma(x) = 0$. It follows that we have $x = h$ due to $\sigma(x) = 0$, and hence $h - x = 0$ which is a contradiction.

Case 3: $y = (k+3)/2 = h+2$, and $\sigma'(x) = \sigma'(y)$. Then $\sigma'(y) = 0$, and thus $\sigma'(x) = 0$. Since σ' is recursive and $0 \notin (\mathbb{Z}^+_{k+4} \cup \mathbb{Z}^-_{k+4})$ we have $\sigma'(x) \neq 0$ for all $0 \leq x \leq h+1$. Hence a contradiction occurs.

Therefore, only Case 1 may occur. It follows that:

$$\max_{l\in\mathbb{Z}_k} |A_l(\sigma)| \geq \max_{l\in\mathbb{Z}_{k'}} |A_l(\sigma')|.$$

Since, for $0 \leq x < y \leq h$, whenever $\sigma(x) = \sigma(y)$ we also have that $\sigma'(x) = \sigma'(y)$, the conclusion follows. □

Now we improve the results of Chapter 3 by looking for a strong difference map σ with $w(\sigma)$ as small as possible. In particular we obtain the following proposition:

Proposition 4.2.6. *There exists an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM, denoted by σ, such that $w(\sigma) = 4$ and $\sigma(j) = \sigma(k-j)$ in the following cases:*

1 k a prime and any possible i;

2 $k < 56$ odd and any possible i.

3 $i \in \{3,5,7,9,11\}$ *and any odd* $k \geq 2i+1$*;*

Proof. CASE 1. If k is an odd prime then, because of the proof of Theorem 2.3.3 the Paley SDM σ_k is an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM (see also Theorem 4.1.5).

We also know that $w(\sigma_k) := \max(4, 2^t\sqrt{k/k^*})$ where k^* is the square-free part of k, and t is the number of prime factors of k^* (see Theorem 4.1.9). In this case, since k is a prime $k^* = k$ and therefore $w(\sigma_k) = 4$.

CASE 2. We cover these cases with a complete computer search (see Appendix 2).

CASE 3. Construction 4.2.5 and a computer search (see case 2) give us the existence of an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM for $i \in \{3,5,7,9,11\}$ and any odd $k \geq 2i+1$.

In particular we use the following recursive i-perfect $SDMs$. Because of the symmetry we write just the first half of each map.

- For $i = 3$:

$$k = 11,\ (4,-2,2,-1,1,0,\dots);$$

We remark that this map generates Example 4.2.1.

$$k = 9,\ (-3,2,-1,1,0,\dots).$$

- For $i = 5$:

$$k = 19,\ (3,-4,7,-3,3,-2,2,-1,1,0,\dots);$$

$$k = 17,\ (-2,4,-6,3,-2,2,-1,1,0,\dots);$$

- For $i = 7$:

$$k = 29,\ (20,7,15,5,-4,-19,-7,4,-3,3,-2,2,-1,1,0,\dots);$$

$$k = 31,\ (-21,-7,-16,-5,5,21,8,-4,4,-3,3,-2,2,-1,1,0,\dots).$$

- For $i = 9$:

$$k = 33,\ (-7,-18,-4,7,-6,4,-5,-20,-4,4,-3,3,-2,2,-1,1,0,\dots);$$

$$k = 39,\ (-34,-19,-32,-14,-25,-9,-21,-7,12,-5,5,-4,4,-3,3,-2,2,-1,1,0,\dots).$$

- For $i = 11$:

$$k = 39,\ (9,21,4,-9,6,-8,-29,-13,6,-5,5,-4,4,-3,3,-2,2,-1,1,0,\dots);$$

$$k = 41,\ (25,12,-6,-22,-10,5,-9,-33,-14,6,-5,5,-4,4,-3,3,-2,2,-1,1,0,\dots).$$

Moreover for all these SDMs, σ, set $M = \max_{l\in\mathbb{Z}_k} |A_l(\sigma)| = \max_{l\in\mathbb{Z}_k} |\{x : x \in \{1,\dots,\frac{k-1}{2}\},\ \sigma(x) = l\}|$, we have that $M = 1$ or $M = 2$ therefore, using Construction 4.2.5, we obtain the required SDMs with $w(\sigma) = 4$. □

4.3 Infinite classes of i-perfect k-cycle systems II

Because of Theorem 4.1.8, the SDMs of Proposition 4.2.6 immediately give us many families of i-perfect decompositions of the complete m-partite graphs $\mathbb{K}_k^{(m)}$. Unfortunately our construction always fails for $m = 3$. However, if $i = 3$, we can attack this case directly:

Lemma 4.3.1. *There exists a regular 3-perfect $(\mathbb{K}_k^{(3)}, C_k)$-design for all odd integers $k \geq 11$.*

Proof. Let β be the map from $C_k = \mathbb{Z}_k$ to $\mathbb{Z}_{3k}$ defined by $\beta(i) = b_i$ where:
$b_i = (-1)^i(3i + 10)$ for $1 \leq i \leq k - 7$,
$b_{k-6} = 6$, $b_{k-5} = -5$, $b_{k-4} = 18$, $b_{k-3} = 5$, $b_{k-2} = 12$, $b_{k-1} = 11$, $b_k = -8$.
It is easy to see that the b_i's are pairwise distinct. Observing that

$$Z_{3k} - \langle 3 \rangle_{\mathbb{Z}_{3k}} = \pm[6x + 1|\ 0 \leq x \leq k - 1],$$

it suffices to check that $6x + 1 \in \Delta_1[\beta]$ and $\Delta_3[\beta]$ for each $x \in \{0, 1, \ldots, k - 1\}$.

(1) $6x + 1 \in \Delta_1[\beta]$ for each $x \in \{0, 1, \ldots, k - 1\}$, in fact:
$6 \times 0 + 1 = b_{k-2} - b_{k-1}$, $6 \times 1 + 1 = b_{k-2} - b_{k-3}$,
$6 \times 2 + 1 = b_{k-4} - b_{k-3}$, $6 \times 3 + 1 = b_{k-1} - b_k$,
$6 \times (k - 4) + 1 = b_{k-5} - b_{k-4}$, $6 \times (k - 3) + 1 = b_{k-7} - b_{k-6}$,
$6 \times (k - 2) + 1 = b_{k-5} - b_{k-6}$, $6 \times (k - 1) + 1 = b_1 - b_k$,
$6 \times x + 1 = (-1)^x(b_{k-x-4} - b_{k-x-3})$ for $4 \leq x \leq k - 5$.

(2) $6x + 1 \in \Delta_3[\beta]$ for each $x \in \{0, 1, \ldots, k - 1\}$, in fact:
$6 \times 0 + 1 = b_{k-6} - b_{k-3}$, $6 \times 1 + 1 = b_{k-4} - b_{k-1}$,
$6 \times 2 + 1 = b_{k-3} - b_k$, $6 \times 3 + 1 = b_{k-8} - b_{k-5}$,
$6 \times 4 + 1 = b_{k-2} - b_1$, $6 \times (k - 5) + 1 = b_{k-7} - b_{k-4}$,
$6 \times (k - 4) + 1 = b_{k-9} - b_{k-6}$, $6 \times (k - 3) + 1 = b_{k-5} - b_{k-2}$,
$6 \times (k - 2) + 1 = b_3 - b_k$, $6 \times (k - 1) + 1 = b_{k-1} - b_2$,
$6 \times x + 1 = (-1)^x(b_{k-x-2} - b_{k-x-5})$ for $5 \leq x \leq k - 6$.

Therefore $[\beta]$ is a 3-perfect $(\mathbb{Z}_{3k}, \langle 3 \rangle_{\mathbb{Z}_{3k}}, C_k, 1)$-$DF$ and the claim follows by Theorem 4.1.2. □

We obtain even more i-perfect decompositions by using the recursive method of [6]. The structures that underlie this method are the pairwise balanced designs (see Definition 1.1.27). Let K be a subset of positive integers and let λ be a positive integer. We recall that a pairwise balanced design ($PBD(v, K, \lambda)$) of order v with block sizes from K is a pair $(V, \mathcal{B})$ where V is a finite set (the point set) of cardinality v and $\mathcal{B}$ is a family of subsets (blocks) of V that satisfy:

- if $B \in \mathcal{B}$ then $|B| \in K$;
- every pair of distinct elements of V occurs in exactly λ blocks of $\mathcal{B}$.

The notation $PBD(v, K)$ is often used when $\lambda = 1$.

This concept turns out to be very useful for getting decompositions of the complete m-partite graph $\mathbb{K}_k^{(m)}$. In fact the following theorem holds true.

Theorem 4.3.2 (P. Adams, D.E. Bryant [6]). *Let $M = \{m_1, \ldots, m_n\}$ be a set of positive integers. Let us suppose there exists a $PBD(m, M, 1)$, which we denote by $\mathfrak{P}$, then there exists also a decomposition of the complete m-partite graph $\mathbb{K}_k^{(m)}$ in the complete m_i partite graphs $\mathbb{K}_k^{(m_i)}$ with $m_i \in M$.*

Proof. We identify $\mathbb{K}_k^{(m)}$ with the graph with vertices the ordered pairs $(x, y) : x \in \{1, \ldots m\}$ and $y \in \{1, \ldots, k\}$ and with edges the pairs of vertices $\{(x_1, y_1); (x_2, y_2)\}$ such that $x_1 \neq x_2$.

Let B be a block of $\mathfrak{P}$ of size m_i; we define the subgraph $\mathbb{K}_k^B$ of $\mathbb{K}_k^{(m)}$, that is a complete m_i-partite graph, with vertices $(x, y) : x \in B$ and $y \in \{1, \ldots, k\}$ and with edges $\{(x_1, y_1); (x_2, y_2)\}$ such that $x_1 \neq x_2$.

Given $e = \{(x_1, y_1); (x_2, y_2)\} \in E(\mathbb{K}_k^{(m)})$ there exists a unique block B of $\mathfrak{P}$ such that $\{x_1, x_2\} \subseteq B$. Therefore there exists a unique $\mathbb{K}_k^B$ such that $e \in E(\mathbb{K}_k^B)$ and the subgraphs $\mathbb{K}_k^B : B \in \mathfrak{B}$, decompose $\mathbb{K}_k^{(m)}$. Since the graph $\mathbb{K}_k^B$ is isomorphic to the graph $\mathbb{K}_k^{(m_i)}$, where $|B| = m_i$, we obtain the claim. □

We recall the following results of existence of PBDs (see page 253 of [38]):

Proposition 4.3.3. *Let us consider the set $OQ_{\geq t}$ given by:*

$$OQ_{\geq t} := \{x : x \text{ is a prime power; } x \geq t, \ x \text{ is odd}\}.$$

Then:

- *there exists a $PBD(v, OQ_{\geq 3})$ for all odd integers $v > 1$ and*
- *there exists a $PBD(v, OQ_{\geq 5})$ for all odd integers $v > 1$ with the exceptions of $3, 15, 33, 39$ and with the possible exceptions of $51, 75$ and 87.*

Now we first find decompositions of the complete m-partite graphs $\mathbb{K}_k^{(m)}$ and then we fill them using i-perfect $HCS(k)$s according to Lemma 3.6.1. For this purpose we use the known results about the existence of i-perfect $HCS(k)$s (see Proposition 3.6.4, [30] and [46]). We are ready to state the main result of this chapter:

Theorem 4.3.4 (S. C., X. Wang). *Let m and k be positive integers, then there exists a 3-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ if and only if mk is odd and $k \geq 7$. Moreover, if $m \notin E := \{3, 15, 33, 39, 51, 75, 87\}$ and mk is odd, there exists an i-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ in the following cases:*

- *k a prime and any possible i;*
- *$k < 56$ odd and any possible i except for:*

$$(i, k) \in \{(2, 9), (4, 9), (7, 21), (13, 39), (15, 45), (6, 51)\}.$$

Proof. CASE 1, $i = 3$: Because of Proposition 1.2.4 and Definition 1.2.6, if there exists a 3-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ then mk is necessarily odd and $k \geq 7$.

Let us suppose that $i = 3$ and k is odd. Then, because of Proposition 4.2.6, there exists a 3-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM σ with $w(\sigma) = 4$. According to Theorem 4.1.8, we have a 3-perfect decomposition of $\mathbb{K}_k^{(m)}$ for all odd m whose prime power factors are greater than 4. Because of Lemma 4.3.1, if $k \geq 11$, there exists also a 3-perfect decomposition of $\mathbb{K}_k^{(3)}$. Therefore, because of Theorem 4.3.2 and Proposition 4.3.3, if $k \geq 11$, there exists a 3-perfect decomposition of $\mathbb{K}_k^{(m)}$ for all odd $m > 1$. Then, since the existence of a Hamiltonian 3-perfect decomposition of $\mathbb{K}_k$ has been obtained in [30] (see also [46]) and the case $k < 11$ has been solved in [6], there exists a 3-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ for all odd m and all $k \geq 7$.

CASE 2, k is a prime: Let us suppose that k is an odd prime. Then, because of Proposition 4.2.6, there exists an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM σ with $w(\sigma) = 4$. As in the previous case, this means that there exists an i-perfect decomposition of $\mathbb{K}_k^{(m)}$ for all odd $m > 1$ with prime power factors different from 3. Therefore, because of Theorem 4.3.2 and Proposition 4.3.3, there exists also an i-perfect decomposition of $\mathbb{K}_k^{(m)}$ for all odd $m > 1$ not in the set E. Then, since it is known that there exists a Hamiltonian i-perfect decomposition of $\mathbb{K}_k$ for the prime values of k (see Proposition 1.2.7), there exists an i-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ for all $m \notin E$.

CASE 3, $k < 56$: Let us suppose that $k < 56$. Then, because of Proposition 4.2.6 there exists an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM σ with $w(\sigma) = 4$. As in the previous cases, this means that there exists an i-perfect decomposition of $\mathbb{K}_k^{(m)}$ for all odd m with prime power factors different from 3. Therefore, because of Theorem 4.3.2 and Proposition 4.3.3, there exists also an i-perfect decomposition of $\mathbb{K}_k^{(m)}$ for all odd $m > 1$ not in the set E. Then, since the existence of a Hamiltonian i-perfect decomposition of $\mathbb{K}_k$ has been obtained in Proposition 3.6.4, up to the listed exceptions, there exists an i-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ for all $m \notin E$. □

Remark 4.3.5. *With the same proof of Theorem 4.3.4 we get the existence of an i-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$, $i \in \{5, 7, 9, 11\}$ for all odd $m \notin E$ and we get the existence of a 3-perfect k-cycle decomposition of $\mathbb{K}_k^{(m)}$, for all odd m. Therefore, according to Lemma 3.6.1, we get an i-perfect k-cycle decomposition of $\mathbb{K}_{mk}$ whenever an i-perfect $HCS(k)$ exists.*

Due to Theorem 4.3.4 we can improve the known results on the existence of i-perfect k-cycle decompositions of $\mathbb{K}_v$ with $v = mk$ odd obtaining the following table:

k	Exceptions (v,i)	Possible exceptions (v,i)
5	$(15;2)$	
$7, 11, 13, 15, 17, 19$		
9	$(9,2);\ (9,4)$	
21		$(v,7); (km,i) : m \in E,\ i \neq 3$
$23, 25, 27, 29, 31, 33, 35, 37$		$(km,i) : m \in E,\ i \neq 3$
$41, 43, 47, 49, 53, 55$		$(km,i) : m \in E,\ i \neq 3$
39		$(v,13); (km,i) : m \in E,\ i \neq 3$
45		$(v,15); (km,i) : m \in E,\ i \neq 3$
51		$(v,6); (km,i) : m \in E,\ i \neq 3$

We point out that the red cases have been obtained using i-perfect SDMs either here or in [24].

Chapter 5

New 2-designs via strong difference families

In Chapter 2 we presented a powerful idea for obtaining GDDs and 2-designs: the concept of "relative difference family" (see Definition 2.1.13 and Theorem 2.1.17). In the nineties, M. Buratti, R.J.R. Abel, M. Greig and other authors developed several constructions of relative difference families (see for example [1, 2, 9, 16, 20, 31, 43, 63]) and, as a consequence, they obtained a lot of new 2-designs. However, a systematic treatment of constructions of DFs, has been performed only later: M. Buratti introduced the concept of strong difference families in [22] in order to cover such problem. Then he generalized this idea with L. Gionfriddo in [25]. Here we recall his first definition. Let $X = [x^1, \ldots, x^k]$ be a multiset of size k of an additive group G then we define the list of differences $\Delta X := [x^i - x^j | i \neq j]$.

Definition 2.2.1 (M. Buratti)**.** *Let us consider $\Sigma := [X_1, \ldots, X_t]$ a family of multisets of size k of an additive group G of order g. We say that Σ is a (G, k, μ) strong difference family (SDF), or a (g, k, μ)-SDF over to the group G, if the list*

$$\Delta\Sigma = \bigcup_{X \in \Sigma} \Delta X,$$

covers all of G exactly μ times.

If $t = 1$, i.e. the family $\Sigma = [X_1]$ is given by a single multiset, we say that the multiset X_1 is a (G, k, μ) strong difference multiset (SDM).

Through the use of SDFs, as a consequence of the "fundamental construction" (see Theorem 2.2.8), it was possible to provide a lot of new DFs and to rediscover many old ones. We recall the statement of this theorem:

Theorem 2.2.8. *Let $\Sigma = [[s_1^1, \ldots, s_k^1], \ldots, [s_1^n, \ldots, s_k^n]]$ be a (G, k, μ)-SDF, and let R be a ring with additive group H. Given n multisets of H, $[t_1^1, \ldots, t_k^1], \ldots, [t_1^n, \ldots, t_k^n]$ we set:*

$$A_i = [(s_j^i, t_j^i),\ j \in \{1, \ldots, k\}],\ \forall i \in \{1, \ldots, n\};$$

$$\Delta[A_1, \ldots, A_n] = \bigcup_{i=1}^{n} [x - y | x, y \in A_i,\ x \neq y];$$

as we have seen in Chapter 2 there exist multisets L_g of elements of H such that:

$$\Delta[A_1, \ldots, A_n] = \bigcup_{g \in G} \{g\} \times L_g.$$

Assume that the following conditions hold:

1) For all $i \in \{1, \ldots, n\}$ we have: $s^i_j = s^i_{j'}$ with $j \neq j' \implies t^i_j - t^i_{j'} \in U(R)$;

2) $\exists\ S \subset H \setminus \{0\}$ such that $S \cdot L_g = \lambda(H \setminus \{0\})\ \forall g \in G$.

Then there exists a $(G \times H, G \times \{0\}, k, \lambda)$-$DF$. Moreover the multisets $A_1, \ldots, A_n$ turn out to be simple sets.

Before this idea was formalized by M. Buratti, it was implicitly used in several papers, see for instance [9, 20, 31, 40, 41] and [43].

We recall that, despite the fact that many authors worked on the existence of 2-(v, k, λ) designs with $6 \leq k \leq 9$, there are still many open cases and little is known when $9 < k$. In this chapter we show that, with a careful application of the "fundamental construction", it is possible to establish the existence of a 2-(v, k, λ) design in some of the open cases.

In particular to obtain such designs we proceed as follows. First of all, through a careful analysis of the open cases (see Chapter 1), we try to understand which $(G \times \mathbb{F}_q^*, G \times \{0\}, k, \lambda)$-$DF$s are useful for our purpose. Then, with the use of a computer, we construct a (G, k, μ)-SDF.

Secondary for getting a $(G \times \mathbb{F}_q^*, G \times \{0\}, k, \lambda)$-$DF$, using the notation of Theorem 2.2.8, we have to provide multisets $[t^1_1, \ldots, t^1_k], \ldots, [t^n_1, \ldots, t^n_k]$ of second components on $\mathbb{F}_q^*$ that satisfy the assumptions of the "fundamental construction". This is the less trivial part of the procedure and in order to do it we need to apply an asymptotical result of M. Buratti and A. Pasotti (see [26], Theorem 5.1.2 and its consequences) or to do a computer research. Then, because of Theorem 2.2.8, we get a $(G \times \mathbb{F}_q^*, G \times \{0\}, k, \lambda)$-$DF$. Finally we apply this relative difference family, as done in Example 2.3.1, to obtain the required design.

Within this procedure we can establish the existence of a 2-(v, k, λ) design for seven values of (v, k, λ), with $7 \leq k \leq 9$, for which the existence problem was open and in one of this cases we find a new resolvable design (see Definition 1.1.22). In particular, regarding the case of 2-$(v, 9, 4)$ designs, we left the problem of existence open only for $v = 315$. We also provide infinite series of 2-designs with $k = 13$ and $k = 17$, values for which little was previously known.

In conclusion, although the procedure followed in this chapter seems to be technical and quite standard, we believe that the results we obtain are interesting. We also believe that the way in which we apply Theorem 5.1.2 can be generalized and can still give new existence results for 2-designs, GDDs and resolvable 2-designs.

5.1 Weil's theorem

The theorem of Weil on the sum of multiplicative characters has been recently used by several authors (M. Buratti, A. Pasotti [26], Y. Chang, L. Ji [32], K. Momihara

[54] and many others, see for example [3, 23, 33, 52, 64]) in order to obtain new DFs, 2-designs and other combinatorial structures. We introduce some notations in order to give the statement of Weil's theorem. As usual, we denote by $\mathbb{F}_q$ the finite field of order q and by $\mathbb{F}_q^*$ its multiplicative group. If $q \equiv 1 \pmod{e}$ then C_0^e will denote its subgroup of nonzero eth powers. Once a primitive root g has been fixed we set $C_i^e = g^i C_0^e$.

We recall that a multiplicative character of $\mathbb{F}_q$ is an homomorphism χ from $\mathbb{F}_q^*$ to the multiplicative group $\mathbb{C}^*$ of non negative complex numbers i.e a map χ such that: $\chi(1) = 1$; $\chi(xy) = \chi(x)\chi(y)$ for any $x, y \in \mathbb{F}_q$. By convention we set $\chi(0) = 0$. Here is the statement of Weil's theorem on the sum of multiplicative characters (see [47]):

Theorem 5.1.1. *Let χ be a multiplicative character of order $m > 1$ of $\mathbb{F}_q$ and let $f \in \mathbb{F}_q[\chi]$ be a polynomial that is not of the form kg^m for some $k \in \mathbb{F}_q$ and $g \in \mathbb{F}_q[\chi]$. Then, we have:*

$$\Big| \sum_{x \in \mathbb{F}_q} \chi[f(x)] \Big| \leq (d-1)\sqrt{q}$$

where d is the number of distinct roots of f in its splitting field over $\mathbb{F}_q$.

In their paper [26], M. Buratti and A. Pasotti proved the following consequence of Theorem 5.1.1 that concerns cyclotomic systems. Let

$$Q(e,m,d) = \frac{1}{4}(U + \sqrt{U^2 + 4e^{m-1}(m+ed)})^2 \text{ where } U = \sum_{h=1}^{m} \binom{m}{h}(e-1)^h(h-1).$$

If $d = 0$ we denote $Q(e,m) := Q(e,m,0)$.

Theorem 5.1.2 ([26])**.** *Let $q \equiv 1 \pmod{e}$ be a prime power, let $B = \{\beta_1, \ldots, \beta_m\}$ be an arbitrary m-subset of $\mathbb{F}_q$ and let $(b_1, \ldots, b_m)$ be an arbitrary element of $\mathbb{Z}_e^m$. Set $X = \{x \in \mathbb{F}_q : x - \beta_i \in C_{b_i}^e \text{ for } i = 1, \ldots, m\}$. Then we have that, for $q > Q(e,m,d)$, the set X is such that $|X| > d$.*

In [26] is also given the following application of Weil's theorem that makes use of strong difference families:

Theorem 5.1.3 ([26])**.** *If there is a (G,k,μ)-SDF, then there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-$DF$ for any prime power $q \equiv \mu + 1 \pmod{2\mu}$ greater than $Q(\mu, k-1)$.*

Theorem 5.1.3 is essentially a quantitative statement of Theorem 2.2.10. K. Momihara (see [54]) provide also the following generalization of Theorem 5.1.3:

Theorem 5.1.4. *If there is a (G,k,μ)-SDF with $\mu = 2d\lambda$ then there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, 2\lambda)$-$DF$ for any prime power $q \equiv 1 \pmod{d}$ with $q \geq Q(d, k-1)$.*

5.2 New 2-designs via SDFs I

The aim of this chapter is to obtain DFs via Theorem 2.2.8. Given a SDF, the crucial part in this process is to provide suitable multisets of elements of $\mathbb{F}_q$, as done in Example 2.3.1. In this section we solve this problem by a computer search and by applying the asymptotical results of Theorems 5.1.3 and 5.1.4.

5.2.1 A 2-$(694, 7, 2)$ design

Lemma 5.2.1. *There exists a* $(63p, 63, 7, 1)$*-DF for any prime* $p \equiv 3 \pmod 4$ *such that* $p \geq 11$.

Proof. We first construct a $(\mathbb{Z}_{63}, 7, 2)$-SDF, say Σ_1 as follows:

$$\Sigma_1 := [[0, 4, 15, 23, 37, 58, 58], \quad [0, 1, 3, 7, 13, 25, 39], \quad [0, 1, 3, 11, 18, 34, 47]].$$

Now we want to apply Theorem 2.2.8, as done in Example 2.3.1, in order to get a $(63p, 63, 7, 1)$-DF. For this purpose we consider the following blocks on $\mathbb{Z}_{63} \times \mathbb{F}_p$ having, as first coordinates, the elements of Σ_1:

$$\begin{aligned} A_1 &:= \{(0,0), (4, y_1), (15, y_2), (23, y_3), (37, y_4), (58, y_5), (58, -y_5)\}, \\ A_2 &:= \{(0,0), (1, y_6), (3, y_7), (7, y_8), (13, y_9), (25, y_{10}), (39, y_{11})\}, \\ A_3 &:= \{(0,0), (1, y_{12}), (3, y_{13}), (11, y_{14}), (18, y_{15}), (34, y_{16}), (47, y_{17})\}. \end{aligned}$$

Using the notation of Theorem 2.2.8 we have that $\Delta[A_1, A_2, A_3] = \bigcup_{i=0}^{62} \{i\} \times L_i$ where $L_i = -L_{63-i}$ and:

$$\begin{array}{lll}
L_0 = \pm[2y_5], & L_1 = [y_6, y_{12}], & L_2 = [y_7 - y_6, y_{13} - y_{12}], \\
L_3 = [y_7, y_{13}], & L_4 = [y_1, y_8 - y_7], & L_5 = \pm[y_5], \\
L_6 = [y_8 - y_6, y_9 - y_8], & L_7 = [y_8, y_{15} - y_{14}], & L_8 = [y_3 - y_2, y_{14} - y_{13}], \\
L_9 = [y_1 - y_5, y_1 + y_5], & L_{10} = [y_9 - y_7, y_{14} - y_{12}], & L_{11} = [y_2 - y_1, y_{14}], \\
L_{12} = [y_9 - y_6, y_{10} - y_9], & L_{13} = [y_9, y_{17} - y_{16}], & L_{14} = [y_4 - y_3, y_{11} - y_{10}], \\
L_{15} = [y_2, y_{15} - y_{13}], & L_{16} = [y_{16} - y_{15}, -y_{17}], & L_{17} = [y_{15} - y_{12}, y_{12} - y_{17}], \\
L_{18} = [y_{15}, y_{10} - y_8], & L_{19} = [y_3 - y_1, y_{13} - y_{17}], & L_{20} = [y_2 - y_5, y_2 + y_5], \\
L_{21} = [y_5 - y_4, -y_5 - y_4], & L_{22} = [y_{10} - y_7, y_4 - y_2], & L_{23} = [y_3, y_{16} - y_{14}], \\
L_{24} = [y_{10} - y_6, -y_{11}], & L_{25} = [y_{10}, y_6 - y_{11}], & L_{26} = [-y_4, y_{11} - y_9], \\
L_{27} = [y_7 - y_{11}, y_{14} - y_{17}], & L_{28} = [y_3 - y_5, y_3 + y_5], & L_{29} = [-y_{16}, y_{17} - y_{15}], \\
L_{30} = [y_1 - y_4, y_{12} - y_{16}], & L_{31} = [y_{16} - y_{13}, y_8 - y_{11}]. &
\end{array}$$

Let S be C_0^2. Let us suppose that the two elements of each set L_i, $0 \leq i \leq 31$ belong to different cosets of $\mathbb{F}_p^*$ respect to C_0^2. Then it would follows that:

$$S \cdot L_i = \bigcup_{s \in S} sL_i = \mathbb{F}_p^*.$$

Therefore the blocks A_1, A_2, A_3 and the set S would satisfy the assumptions of Theorem 2.2.8.

We can find these second components, using a computer, for all primes $p \equiv 3 \pmod 4$ such that $11 \leq p \leq Q(2, 6)$. In fact, for these values of p, a computer search shows that there exists a 17-tuple $(y_1, \ldots, y_{17})$ such that the two elements of each set L_i, $0 \leq i \leq 31$ belong to different cosets of $\mathbb{F}_p^*$ respect to C_0^2. For example, when $p = 11$, we can take the values:

$$\boxed{\begin{array}{l} y_1 = 3,\ y_2 = 5,\ y_3 = 6,\ y_4 = 8,\ y_5 = 1,\ y_6 = 2,\ y_7 = 4,\ y_8 = 6, \\ y_9 = 1,\ y_{10} = 10,\ y_{11} = 8,\ y_{12} = 4,\ y_{13} = 7,\ y_{14} = 9,\ y_{15} = 2,\ y_{16} = 3,\ y_{17} = 5. \end{array}}$$

It follows that, for these choices of second components, the blocks A_1, A_2, A_3 satisfy the hypothesis of Theorem 2.2.8. Hence there exists a $(63p, 63, 7, 1)$-DF for all primes $11 \leq p \leq Q(2, 6)$ with $p \equiv 3 \pmod 4$.

Because of Theorem 5.1.3 there exists a $(63p, 63, 7, 1)$-DF for any prime $p \equiv 3 \pmod 4$ such that $p > Q(2, 6)$. We conclude that there exists a $(63p, 63, 7, 1)$-DF for any prime $p \equiv 3 \pmod 4$ such that $p \geq 11$. □

Using the previous lemma we construct the following 2-designs.

Proposition 5.2.2. *There exists a* 2-$(63p + 1, 7, 2)$ *design for any prime* $p \equiv 3 \pmod 4$ *such that* $p \geq 11$.

Proof. By Lemma 5.2.1, there exists a $(63p, 63, 7, 1)$-DF, which gives a 7-GDD of type 63^p. According to Remark 1.1.30, we start with a $(7, 2)$-GDD of type 63^p, then we add a point and we cover the groups of this GDD with a 2-$(64, 7, 2)$ design through the new point. We get a 2-$(63p + 1, 7, 2)$ design. □

In the case $p = 11$ we obtain the following new 2-design:

Corollary 5.2.3. *There exists a* 2-$(694, 7, 2)$ *design.*

5.2.2 A 2-$(459, 9, 4)$ design and a 2-$(783, 9, 4)$ design

Lemma 5.2.4. *There exists a* $(27q, 27, 9, 4)$-DF *for all odd prime powers* $q \geq Q(2, 8)$ *and for* $q \in \{17, 29\}$.

Proof. We start by considering the following $(27, 9, 8)$-SDF, say Σ_2:

$$[[0, 3, 3, 8, 8, 17, 17, 23, 23],\ [0, 1, 2, 3, 19, 4, 5, 8, 12],\ [0, 1, 2, 3, 19, 6, 11, 13, 17]].$$

Now we want to apply Theorem 2.2.8, as done in Example 2.3.1, in order to get a $(27q, 27, 9, 1)$-DF. We first construct the following blocks on $Z_{27} \times \mathbb{F}_q$ having, as first coordinates, the elements of Σ_2:

$$\begin{aligned}
A_1 &:= \{(0, 0), (3, y_1), (3, -y_1), (8, y_2), (8, -y_2), (17, y_3), (17, -y_3), (23, y_4), (23, -y_4)\},\\
A_2 &:= \{(0, 0), (1, y_5), (2, y_6), (3, y_7), (19, y_8), (4, y_9), (5, y_{10}), (8, y_{11}), (12, y_{12})\},\\
A_3 &:= \{(0, 0), (1, -y_5), (2, -y_6), (3, -y_7), (19, -y_8), (6, y_{13}), (11, y_{14}), (13, y_{15}), (17, y_{16})\}.
\end{aligned}$$

Using the notation of Theorem 2.2.8 we have that $\Delta[A_1, A_2, A_3] = \bigcup_{i=0}^{26} \{i\} \times L_i$ where $L_i = -L_{27-i}$ and:

$$
\begin{aligned}
L_0 &= \pm[2y_1, 2y_2, 2y_3, 2y_4],\\
L_1 &= [\pm(y_5 - y_6), \pm(y_7 - y_6), \pm y_5, y_9 - y_7, y_{10} - y_9],\\
L_2 &= [\pm y_6, \pm(y_7 - y_5), y_9 - y_6, y_{10} - y_7, y_{15} - y_{14}, -y_8 - y_{16}],\\
L_3 &= [\pm y_7, y_9 - y_5, y_{10} - y_6, y_{11} - y_{10}, y_{13} + y_7, \pm y_1],\\
L_4 &= [y_9, y_{11} - y_9, \pm y_4, y_{10} - y_5, y_{12} - y_{11}, y_{13} + y_6, y_{16} - y_{15}],\\
L_5 &= [\pm(y_1 \pm y_2), y_{10}, -y_7 + y_{11}, y_{13} + y_5, y_{14} - y_{13}],\\
L_6 &= [y_{13}, \pm(y_3 \pm y_4), y_{11} - y_6, -y_{15} - y_8, y_{16} - y_{14}],\\
L_7 &= [\pm(y_4 \pm y_1), y_8 - y_{12}, y_{11} - y_5, y_{15} - y_{13}, -y_{10} + y_{12}],\\
L_8 &= [\pm y_2, y_{11}, y_{12} - y_9, -y_{14} - y_8, \pm y_8, y_{14} + y_7],\\
L_9 &= [\pm(y_8 - y_5), y_{12} - y_7, y_{14} + y_6, \pm(y_2 \pm y_3)],\\
L_{10} &= [\pm y_3, -y_{16}, \pm(y_8 - y_6), y_{12} - y_6, y_{14} + y_5, y_{15} + y_7],\\
L_{11} &= [y_{14}, -y_5 - y_{16}, y_{12} - y_5, y_8 - y_{11}, \pm(y_8 - y_7), y_{15} + y_6, y_{16} - y_{13}],\\
L_{12} &= [\pm(y_2 \pm y_4), y_{15} + y_5, -y_8 + y_9, y_{12}, -y_{16} - y_6],\\
L_{13} &= [\pm(y_1 \pm y_3), y_{15}, -y_8 - y_{13}, -y_{16} - y_7, -y_8 + y_{10}].
\end{aligned}
$$

Let S be C_0^2. Let us suppose that four elements of each L_i belong to C_0^2 and four elements of each L_i belong to C_1^2. Then it would follows that:

$$S \cdot L_i = \bigcup_{s \in S} sL_i = 4\mathbb{F}_q^*.$$

Therefore the blocks A_1, A_2, A_3 and the set S would satisfy the assumptions of Theorem 2.2.8. Using a computer we can find these second components for $q \in \{17, 29\}$. In fact we find a 16-tuple $(y_1, \ldots, y_{16})$ of elements of $\mathbb{F}_{17}$ and another 16-tuple of elements of $\mathbb{F}_{29}$ such that for each L_i four elements lie in C_0^2 and four elements lie in C_1^2. The explicit solutions are, respectively, the following:

For $q = 17$:
$A_1 := \{(0,0), (3,1), (3,-1), (8,2), (8,-2), (17,3), (17,-3), (23,5), (23,-5)\}$,
$A_2 := \{(0,0), (1,1), (2,2), (3,7), (19,11), (4,10), (5,5), (8,14), (12,16)\}$,
$A_3 := \{(0,0), (1,-1), (2,-2), (3,-7), (19,-11), (6,3), (11,2), (13,12), (17,13)\}$.

For $q = 29$:
$A_1 := \{(0,0), (3,1), (3,-1), (8,2), (8,-2), (17,3), (17,-3), (23,4), (23,-4)\}$,
$A_2 := \{(0,0), (1,1), (2,2), (3,4), (19,11), (4,15), (5,5), (8,13), (12,21)\}$,
$A_3 := \{(0,0), (1,-1), (2,-2), (3,-4), (19,-11), (6,11), (11,19), (13,10), (17,22)\}$.

If follows that, for these choices of second components, the blocks A_1, A_2, A_3 satisfy the hypothesis of Theorem 2.2.8. Hence, for $q \in \{17, 29\}$, there exists a $(27q, 27, 9, 4)$-DF. Moreover because of Theorem 5.1.4 there exists a $(27q, 27, 9, 4)$-DF also for all prime powers $q \geq Q(2, 8)$. □

As a consequence of this lemma we get the following result:

Corollary 5.2.5. *There exists a* 2-$(459, 9, 4)$ *design and a* 2-$(783, 9, 4)$ *design.*

Proof. We start with a $(27q, 27, 9, 4)$-DF, for $q \in \{17, 29\}$, which defines a $(9, 4)$-GDD of type 27^q. According to Remark 1.1.30, since there exists a 2-$(27, 9, 4)$ design, we can fill the groups of this GDD in order to obtain a 2-$(459, 9, 4)$ design and a 2-$(783, 9, 4)$ design. □

This corollary leaves the existence of a 2-$(v, 9, 4)$ design open only for $v = 315$.

5.3 New 2-designs via SDFs II

Also in this section, given a SDF, we want to obtain a DF via Theorem 2.2.8. We recall that the crucial part in this process is to provide suitable multisets of elements of $\mathbb{F}_q$, as done in Example 2.3.1. In the examples we discuss in this section we construct this multisets by applying directly Theorem 5.1.2.

5.3.1 2-designs from the Paley $(13, 13, 12)$-SDM

We start by considering the Paley $(13, 13, 12)$-SDM, say σ_{13}. Proceeding as in Lemma 5.2.1 and using Theorem 5.1.3 we could easily obtain the existence of a 2-$(13q, 13, 1)$ design for all prime powers $q \geq Q(12, 12)$ such that $q \equiv 13 \pmod{24}$. However, since this bound is huge we apply directly Theorem 5.1.2. We obtain the following result:

Proposition 5.3.1. *There exists a* 2-$(13p, 13, 1)$ *design for all primes* $p \equiv 1 \pmod{12}$ *up to the following possible exceptions:*

$$\{37, 61, 73, 97, 109, 181, 313, 337, 349, 373, 409, 421, 541, 577, 829, 853, 1129, 1741, 2473\}.$$

Proof. Let us consider the Paley $(13, 13, 12)$-SDM:

$$\sigma_{13} := [0, 1, 1, -1, -1, 3, 3, -3, -3, 4, 4, -4, -4].$$

We consider the block A of elements of $\mathbb{F}_{13} \times \mathbb{F}_p$ having, as first coordinates, the elements of σ_{13}:

$$A := \{(0,0), (1,1), (1,-1), (-1,\xi), (-1,-\xi), (3,y_1),$$

$$(3,-y_1), (-3,y_1\xi), (-3,-y_1\xi), (4,y_2), (4,-y_2), (-4,y_2\xi), (-4,-y_2\xi)\},$$

where g is a primitive rooth of $\mathbb{F}_p$, $\xi = g^{\frac{p-1}{4}}$ and $p \equiv 1 \pmod{12}$.
Using the notation of Theorem 2.2.8 we have that $\Delta[A] = \bigcup_{i=0}^{12} \{i\} \times L_i$. We set $L_i = \{1, -1, \xi, -\xi\} \cdot D_i$ where $D_i = D_{13-i}$ and:

$$\begin{array}{ll} D_0 = 2 \cdot [1, y_1, y_2], & D_1 = [1, y_1 - y_2, y_1 + y_2], \\ D_2 = [1 - \xi, y_1 - 1, y_1 + 1], & D_3 = [y_1, y_2 - 1, y_2 + 1], \\ D_4 = [y_2, y_1 - \xi, y_1 + \xi], & D_5 = [y_2 + \xi, y_2 - \xi, y_2(1 - \xi)], \\ D_6 = [y_1(1 - \xi), y_1 + y_2\xi, y_1 - y_2\xi]. & \end{array}$$

Let us consider S to be a complete set of representatives for the cosets of $\{+1, -1, -\xi, \xi\}$ in C_0^3. Let us suppose that each D_i contains an element of C_0^3, an element of C_1^3 and an element of C_2^3. Then we would have that:

$$S \cdot L_i = \bigcup_{s \in S} s\{+1, -1, +\xi, -\xi\} \cdot D_i = \mathbb{F}_p^*.$$

Therefore the block A would satisfies the assumptions of Theorem 2.2.8. Hence, in order to get a $(13p, 13, 13, 1)$-DF, we want that each D_i contains an element of C_0^3, an element of C_1^3 and an element of C_2^3. We can impose these conditions by considering y_1 and y_2 to be the solutions of one of the following cyclotomic systems, according to the class of $1 - \xi$ in $\mathbb{F}_p^*$:

- Case 1: If $1-\xi \in C_0^3$:
  We need y_1 and y_2 such that:

$$\mathfrak{C}^1 := \begin{cases} y_1 \in C_1^3; \\ y_1 - 1 \in C_1^3; \\ y_1 + 1 \in C_2^3; \\ y_1 - \xi \in C_0^3; \\ y_1 + \xi \in C_1^3; \end{cases} \quad \mathfrak{C}^2 := \begin{cases} y_2 \in C_2^3; \\ y_1 - y_2 \in C_1^3; \\ y_1 + y_2 \in C_2^3; \\ y_2 - 1 \in C_0^3; \\ y_2 + 1 \in C_2^3; \\ \xi + y_2 \in C_0^3; \\ \xi - y_2 \in C_1^3; \\ \xi y_2 + y_1 \in C_0^3; \\ \xi y_2 - y_1 \in C_2^3. \end{cases}$$

- Case 2: If $1-\xi \in C_1^3$:
  We need y_1 and y_2 such that:

$$\mathfrak{C}^1 := \begin{cases} y_1 \in C_1^3; \\ y_1 - 1 \in C_0^3; \\ y_1 + 1 \in C_2^3; \\ y_1 - \xi \in C_0^3; \\ y_1 + \xi \in C_1^3; \end{cases} \quad \mathfrak{C}^2 := \begin{cases} y_2 \in C_2^3; \\ y_1 - y_2 \in C_1^3; \\ y_1 + y_2 \in C_2^3; \\ y_2 - 1 \in C_0^3; \\ y_2 + 1 \in C_2^3; \\ \xi + y_2 \in C_2^3; \\ \xi - y_2 \in C_1^3; \\ \xi y_2 + y_1 \in C_0^3; \\ \xi y_2 - y_1 \in C_1^3. \end{cases}$$

- Case 3: If $1-\xi \in C_2^3$:
  We need y_1 and y_2 such that:

$$\mathfrak{C}^1 := \begin{cases} y_1 \in C_1^3; \\ y_1 - 1 \in C_1^3; \\ y_1 + 1 \in C_0^3; \\ y_1 - \xi \in C_0^3; \\ y_1 + \xi \in C_1^3; \end{cases} \quad \mathfrak{C}^2 := \begin{cases} y_2 \in C_2^3; \\ y_1 - y_2 \in C_1^3; \\ y_1 + y_2 \in C_2^3; \\ y_2 - 1 \in C_0^3; \\ y_2 + 1 \in C_2^3; \\ \xi + y_2 \in C_2^3; \\ \xi - y_2 \in C_0^3; \\ \xi y_2 + y_1 \in C_2^3; \\ \xi y_2 - y_1 \in C_1^3. \end{cases}$$

Because of Theorem 5.1.2 these systems have solution for $p > Q(3,9)$. Therefore, for these choices of y_1, y_2 each D_i contains an element of C_0^3, an element of C_1^3 and an element of C_2^3.

Instead, for the primes $p \equiv 1 \pmod{12}$ such that $p < Q(3,9)$, we can find directly, by a computer search, a pair y_1, y_2, such that each D_i contains an element of C_0^3, an element of C_1^3 and an element of C_2^3 up to a small set of exceptions. In fact we have that $10^{10} > Q(3,9)$ and hence, because of the prime number theorem, the cases that we need to check are $\approx \frac{10^{10}}{4 \log 10^{10}} < 10^8$. Beside the fact that this number seems to be huge, with a suitable code, it is possible to check more than 20 cases each second and, surprisingly, the speed of the checks is almost constant in this range. However we have not checked the case in which p is a prime power because this case runs too slowly. We add a GAP code for doing this check as an Appendix (see Appendix 3), but we remark that the same code written in C is even faster (but less clear to read). Running this program we found only the following possible exceptions:

$$\{37, 61, 73, 97, 109, 181, 313, 337, 349, 373, 409, 421, 541, 577, 829, 853, 1129, 1741, 2473\}.$$

Thus, for these choices of y_1, y_2, the block A satisfies the hypothesis of Theorem 2.2.8. It follows that there exists a $(13p, 13, 13, 1)$-DF for all primes $p \equiv 1 \pmod{12}$ up to the exceptions listed above. Because of Theorem 2.1.17 we obtain a 13-GDD of type $(13)^p$ and hence, according to Remark 1.1.30, we get a 2-$(13p, 13, 1)$ design. □

In a very similar way we can prove that:

Proposition 5.3.2. *There exists a* 2-$(13q, 13, 3)$ *design for all prime powers* $q \equiv 1 \pmod{4}$ *such that* $q \geq 13$.

Proof. Let us consider the Paley $(13, 13, 12)$-SDM:

$$\sigma_{13} := [0, 1, 1, -1, -1, 3, 3, -3, -3, 4, 4, -4, -4].$$

We consider the block of elements of $\mathbb{F}_{13} \times \mathbb{F}_q$ having, as first coordinates, the elements of σ_{13}:

$$A := \{(0,0), (1,1), (1,-1), (-1,\xi), (-1,-\xi), (3,y_1),$$

$$(3,-y_1), (-3,y_1\xi), (-3,-y_1\xi), (4,y_2), (4,-y_2), (-4,y_2\xi), (-4,-y_2\xi)\},$$

where g is a primitive rooth of $\mathbb{F}_q$, $\xi = g^{\frac{q-1}{4}}$ and $q \equiv 1 \pmod{4}$.
Using the notation of Theorem 2.2.8 we have that $\Delta[A] = \bigcup_{i=0}^{12} \{i\} \times L_i$. We set $L_i = \{1, -1, \xi, -\xi\} \cdot D_i$ where $D_i = D_{13-i}$:

$$\begin{array}{ll} D_0 = 2 \cdot [1, y_1, y_2], & D_1 = [1, y_1 - y_2, y_1 + y_2], \\ D_2 = [1 - \xi, y_1 - 1, y_1 + 1], & D_3 = [y_1, y_2 - 1, y_2 + 1], \\ D_4 = [y_2, y_1 - \xi, y_1 + \xi], & D_5 = [y_2 + \xi, y_2 - \xi, y_2(1 - \xi)], \\ D_6 = [y_1(1 - \xi), y_1 + y_2\xi, y_1 - y_2\xi]. & \end{array}$$

We note that if $q \geq 13$ we can choose y_1, y_2 such that all elements of each D_i are nonzero. In this case let us consider S to be a complete set of representatives for the cosets of $\{+1, -1, -\xi, \xi\}$ in $\mathbb{F}_q^*$. Then we have that:

$$S \cdot L_i = \bigcup_{s \in S} s\{+1, -1, +\xi, -\xi\} \cdot D_i = 3\mathbb{F}_q^*.$$

Therefore the block A satisfies the hypothesis of Theorem 2.2.8. It follows that there exists a $(13q, 13, 13, 3)$-DF for all prime powers $q \geq 13$ with $q \equiv 1 \pmod 4$. Because of Theorem 2.1.17 we obtain a $(13, 3)$-GDD of type $(13)^q$ and hence, according to Remark 1.1.30, we get a 2-$(13q, 13, 3)$ design. □

Summing up Propositions 5.3.1 and 5.3.2, it follows that:

Theorem 5.3.3 (S. C., X. Wang)**.** *There exists a* 2-(v, k, λ) *design in the following cases:*

(v, k, λ)	*Possible exceptions*
$(13p, 13, 1) :\ p \equiv 1 \pmod{12}$, *prime* $(13q, 13, 3) :\ q \equiv 1 \pmod 4, q \geq 13$, *prime power.*	*List of* 19 *values*

5.3.2 2-designs from the Paley $(17, 17, 16)$-SDM

Now we consider the Paley $(17, 17, 16)$-SDM, say σ_{17}. Proceeding as in Lemma 5.2.1 and using Theorem 5.1.3 we could easily obtain the existence of a 2-$(17q, 17, 1)$ design for all prime powers $q \geq Q(16, 16)$ such that $q \equiv 13 \pmod{24}$. However, since this bound is huge we apply directly Theorem 5.1.2. We get the following result:

Proposition 5.3.4. *There exists a* 2-$(17q, 17, 1)$ *design for all prime powers* $q \geq Q(4, 13)$ *such that* $q \equiv 1 \pmod{16}$.

Proof. Let us consider the Paley $(17, 17, 16)$-SDM:

$$\sigma_{17} := [0, 1, 1, -1, -1, 2, 2, -2, -2, 4, 4, -4, -4, 8, 8, -8, -8].$$

We consider the block A of elements of $\mathbb{F}_{17} \times \mathbb{F}_q$ having, as first coordinates, the elements of σ_{17}:

$$\{(0,0), (1,1), (1,-1), (-1,\xi), (-1,-\xi), (2,y_1), (2,-y_1), (-2,y_1\xi), (-2,-y_1\xi),$$

$$(4,y_2), (4,-y_2), (-4,y_2\xi), (-4,-y_2\xi), (8,y_3), (8,-y_3), (-8,y_3\xi), (-8,-y_3\xi)\},$$

where g is a primitive root of $\mathbb{F}_q$, $\xi = g^{\frac{q-1}{4}}$ and $q \equiv 1 \pmod{16}$.
Using the notation of Theorem 2.2.8 we have that $\Delta[A] = \bigcup_{i=0}^{16} \{i\} \times L_i$. We set $L_i = \{1, -1, \xi, -\xi\} \cdot D_i$ where $D_i = D_{17-i}$ and:

$$\begin{array}{ll}
D_0 = 2 \cdot [1, y_1, y_2, y_3], & D_1 = [1, 1-y_1, 1+y_1, y_3(1-\xi)], \\
D_2 = [1-\xi, y_1, y_1-y_2, y_1+y_2], & D_3 = [y_1+\xi, y_1-\xi, y_2-1, y_2+1], \\
D_4 = [y_2, y_2-y_3, y_2+y_3, y_1(1-\xi)], & D_5 = [y_2+\xi, y_2-\xi, y_3+y_2\xi, y_3-y_2\xi], \\
D_6 = [y_2+y_1\xi, y_2-y_1\xi, y_3-y_1, y_3+y_1], & D_7 = [y_3+y_1\xi, y_3-y_1\xi, y_3-1, y_3+1], \\
D_8 = [y_3, y_2(1-\xi), y_3-\xi, y_3+\xi]. &
\end{array}$$

Let us consider S to be a complete set of representatives for the cosets of $\{+1, -1, -\xi, \xi\}$ in C_0^4. Let us suppose that each D_i contains an element of C_0^4, an element of C_1^4, an element of C_2^4 and an element of C_3^4. Then we would have that:

$$S \cdot L_i = \bigcup_{s \in S} s\{+1, -1, +\xi, -\xi\} \cdot D_i = \mathbb{F}_q^*.$$

Therefore the block A would satisfies the assumptions of Theorem 2.2.8. Hence, in order to get a $(17q, 17, 17, 1)$-DF, we want that each D_i contains an element of C_0^4, an element of C_1^4, an element of C_2^4 and an element of C_3^4. We can impose this condition by considering y_1, y_2 and y_3 to be the solutions of one of the following cyclotomic systems, according to the class of $1-\xi$ in $\mathbb{F}_q^*$:

- Case 1: If $1-\xi \in C_0^4$:
  We need y_1, y_2 and y_3 such that:

$$\mathfrak{C}^1 = \begin{cases} y_1 \in C_1^4; \\ y_1 - 1 \in C_1^4; \\ y_1 + 1 \in C_2^4; \\ y_1 - \xi \in C_1^4; \\ y_1 + \xi \in C_0^4. \end{cases} \quad \mathfrak{C}^2 = \begin{cases} y_2 \in C_2^4; \\ y_2 - y_1 \in C_2^4; \\ y_2 + y_1 \in C_3^4; \\ y_2 - 1 \in C_2^4; \\ y_2 + 1 \in C_3^4; \\ y_2 + \xi \in C_0^4; \\ y_2 - \xi \in C_1^4; \\ y_2\xi + y_1 \in C_0^4; \\ y_2\xi - y_1 \in C_1^4. \end{cases} \quad \mathfrak{C}^3 = \begin{cases} y_3 \in C_3^4; \\ y_3 - y_1 \in C_2^4; \\ y_3 + y_1 \in C_3^4; \\ y_3 - 1 \in C_2^4; \\ y_3 + 1 \in C_3^4; \\ y_3 + \xi \in C_0^4; \\ y_3 - \xi \in C_1^4; \\ y_3\xi + y_1 \in C_0^4; \\ y_3\xi - y_1 \in C_1^4; \\ y_3\xi + y_2 \in C_2^4; \\ y_3\xi - y_2 \in C_3^4; \\ y_3 - y_2 \in C_0^4; \\ y_3 + y_2 \in C_3^4. \end{cases}$$

- Case 2: If $1-\xi \in C_1^4$:
  We need y_1, y_2 and y_3 such that:

$$\mathfrak{C}^1 = \begin{cases} y_1 \in C_3^4; \\ y_1 - 1 \in C_1^4; \\ y_1 + 1 \in C_3^4; \\ y_1 - \xi \in C_1^4; \\ y_1 + \xi \in C_0^4. \end{cases} \quad \mathfrak{C}^2 = \begin{cases} y_2 \in C_2^4; \\ y_2 - y_1 \in C_0^4; \\ y_2 + y_1 \in C_2^4; \\ y_2 - 1 \in C_2^4; \\ y_2 + 1 \in C_3^4; \\ y_2 + \xi \in C_0^4; \\ y_2 - \xi \in C_1^4; \\ y_2\xi + y_1 \in C_0^4; \\ y_2\xi - y_1 \in C_1^4. \end{cases} \quad \mathfrak{C}^3 = \begin{cases} y_3 \in C_1^4; \\ y_3 - y_1 \in C_2^4; \\ y_3 + y_1 \in C_3^4; \\ y_3 - 1 \in C_2^4; \\ y_3 + 1 \in C_3^4; \\ y_3 + \xi \in C_0^4; \\ y_3 - \xi \in C_2^4; \\ y_3\xi + y_1 \in C_0^4; \\ y_3\xi - y_1 \in C_1^4; \\ y_3\xi + y_2 \in C_2^4; \\ y_3\xi - y_2 \in C_3^4; \\ y_3 - y_2 \in C_1^4; \\ y_3 + y_2 \in C_3^4. \end{cases}$$

- Case 3: If $1-\xi \in C_2^4$:
  We need y_1, y_2 and y_3 such that:

$$\mathfrak{C}^1=\begin{cases} y_1\in C_1^4;\\ y_1-1\in C_3^4;\\ y_1+1\in C_2^4;\\ y_1-\xi\in C_1^4;\\ y_1+\xi\in C_0^4. \end{cases} \quad \mathfrak{C}^2=\begin{cases} y_2\in C_2^4;\\ y_2-y_1\in C_0^4;\\ y_2+y_1\in C_3^4;\\ y_2-1\in C_2^4;\\ y_2+1\in C_3^4;\\ y_2+\xi\in C_0^4;\\ y_2-\xi\in C_1^4;\\ y_2\xi+y_1\in C_0^4;\\ y_2\xi-y_1\in C_1^4. \end{cases} \quad \mathfrak{C}^3=\begin{cases} y_3\in C_3^4;\\ y_3-y_1\in C_2^4;\\ y_3+y_1\in C_3^4;\\ y_3-1\in C_2^4;\\ y_3+1\in C_3^4;\\ y_3+\xi\in C_2^4;\\ y_3-\xi\in C_1^4;\\ y_3\xi+y_1\in C_0^4;\\ y_3\xi-y_1\in C_1^4;\\ y_3\xi+y_2\in C_2^4;\\ y_3\xi-y_2\in C_3^4;\\ y_3-y_2\in C_0^4;\\ y_3+y_2\in C_1^4. \end{cases}$$

- Case 4: If $1-\xi\in C_3^4$:
  We need y_1, y_2 and y_3 such that:

$$\mathfrak{C}^1=\begin{cases} y_1\in C_1^4;\\ y_1-1\in C_1^4;\\ y_1+1\in C_3^4;\\ y_1-\xi\in C_1^4;\\ y_1+\xi\in C_0^4. \end{cases} \quad \mathfrak{C}^2=\begin{cases} y_2\in C_2^4;\\ y_2-y_1\in C_2^4;\\ y_2+y_1\in C_0^4;\\ y_2-1\in C_2^4;\\ y_2+1\in C_3^4;\\ y_2+\xi\in C_0^4;\\ y_2-\xi\in C_1^4;\\ y_2\xi+y_1\in C_0^4;\\ y_2\xi-y_1\in C_1^4. \end{cases} \quad \mathfrak{C}^3=\begin{cases} y_3\in C_3^4;\\ y_3-y_1\in C_2^4;\\ y_3+y_1\in C_3^4;\\ y_3-1\in C_2^4;\\ y_3+1\in C_3^4;\\ y_3+\xi\in C_0^4;\\ y_3-\xi\in C_2^4;\\ y_3\xi+y_1\in C_0^4;\\ y_3\xi-y_1\in C_1^4;\\ y_3\xi+y_2\in C_2^4;\\ y_3\xi-y_2\in C_3^4;\\ y_3-y_2\in C_1^4;\\ y_3+y_2\in C_3^4. \end{cases}$$

Because of Theorem 5.1.2 these systems have solutions for $q > Q(4, 13)$. Therefore, for these choices of y_1, y_2, y_3 each D_i contains an element of C_0^4, an element of C_1^4, an element of C_2^4 and an element of C_3^4. Thus the block A satisfies the hypothesis of Theorem 2.2.8. It follows that there exists a $(17q, 17, 17, 1)$-DF for all prime powers $q \geq Q(4, 13)$ with $q \equiv 1 \pmod{16}$. Because of Theorem 2.1.17 we obtain a 17-GDD of type $(17)^q$ and hence, according to Remark 1.1.30, we get a 2-$(17q, 17, 1)$ design. □

Moreover, by a computer search, we can find directly y_1, y_2 and y_3 such that each D_i contains an element of C_0^4, an element of C_1^4, an element of C_2^4 and an element of C_3^4 for several others values of q and hence we can construct many 2-$(17q, 17, 1)$ designs. In the following table we list those with q smaller than 10^4:

2-$(17q, 17, 1)$ design for $q \in$
$\{17, 881, 929, 1009, 1297, 1409, 1601, 1873, 2017, 2081, 2129, 2161, 2417, 2609,$
$2657, 2753, 2801, 2897, 3041, 3089, 3121, 3169, 3217, 3313, 3329, 3361, 3457,$
$3617, 3697, 3761, 3793, 3889, 4001, 4049, 4129, 4241, 4273, 4289, 4337, 4481,$
$4561, 4657, 4673, 4721, 4801, 4817, 4993, 5009, 5153, 5233, 5281, 5297, 5393,$
$5441, 5521, 5569, 5857, 5953, 6113, 6257, 6337, 6449, 6529, 6577, 6673, 6689,$
$6737, 6833, 6961, 6977, 7057, 7121, 7297, 7393, 7457, 7489, 7537, 7649, 7681,$
$7793, 7841, 7873, 7937, 8081, 8161, 8209, 8273, 8353, 8369, 8513, 8609, 8641,$
$8689, 8737, 8753, 8849, 8929, 9041, 9137, 9281, 9377, 9473, 9521, 9601, 9649,$
$9697, 9857\}$.

In a very similar way we can prove that:

Proposition 5.3.5. *There exists a* 2-$(17p, 17, 2)$ *design for all primes* $p \equiv 1 \pmod 8$ *up to the following set of possible exceptions:* $\{41, 73, 89, 193\}$.

Proof. Let us consider the Paley $(17, 17, 16)$-SDM:

$$\sigma_{17} := [0, 1, 1, -1, -1, 2, 2, -2, -2, 4, 4, -4, -4, 8, 8, -8, -8].$$

As in the previous proposition we consider the block A of elements of $\mathbb{F}_{17} \times \mathbb{F}_p$ having, as first coordinates, the elements of σ_{17}:

$$\{(0,0), (1,1), (1,-1), (-1,\xi), (-1,-\xi), (2,y_1), (2,-y_1), (-2,y_1\xi), (-2,-y_1\xi),$$

$$(4,y_2), (4,-y_2), (-4,y_2\xi), (-4,-y_2\xi), (8,y_3), (8,-y_3), (-8,y_3\xi), (-8,-y_3\xi)\},$$

where g is a primitive root of $\mathbb{F}_p$, $\xi = g^{\frac{p-1}{4}}$ and $p \equiv 1 \pmod 8$.
Using the notation of Theorem 2.2.8 we have that $\Delta[A] = \bigcup_{i=0}^{16} \{i\} \times L_i$. We set $L_i = \{1, -1, \xi, -\xi\} \cdot D_i$ where $D_i = D_{17-i}$ and:

$$\begin{array}{ll}
D_0 = 2 \cdot [1, y_1, y_2, y_3], & D_1 = [1, 1-y_1, 1+y_1, y_3(1-\xi)], \\
D_2 = [1-\xi, y_1, y_1-y_2, y_1+y_2], & D_3 = [y_1+\xi, y_1-\xi, y_2-1, y_2+1], \\
D_4 = [y_2, y_2-y_3, y_2+y_3, y_1(1-\xi)], & D_5 = [y_2+\xi, y_2-\xi, y_3+y_2\xi, y_3-y_2\xi], \\
D_6 = [y_2+y_1\xi, y_2-y_1\xi, y_3-y_1, y_3+y_1], & D_7 = [y_3+y_1\xi, y_3-y_1\xi, y_3-1, y_3+1], \\
D_8 = [y_3, y_2(1-\xi), y_3-\xi, y_3+\xi]. &
\end{array}$$

Let us consider S to be a complete set of representatives for the cosets of $\{+1, -1, -\xi, \xi\}$ in C_0^2. Let us suppose that each D_i contains two elements of C_0^2 and two elements of C_1^2. Then we would have that:

$$S \cdot L_i = \bigcup_{s \in S} s\{+1, -1, +\xi, -\xi\} \cdot D_i = 2\mathbb{F}_p^*.$$

Therefore the block A would satisfies the assumptions of Theorem 2.2.8. Hence, in order to get a $(17p, 17, 17, 2)$-DF, we want that each D_i contains two elements of C_0^2 and two elements of C_1^2. We can impose this condition by considering y_1, y_2 and y_3 to be the solutions of one of the following cyclotomic systems, according to the class of $1 - \xi$ in $\mathbb{F}_p^*$:

- Case 1: If $1-\xi \in C_0^2$:
  We need y_1, y_2 and y_3 such that:

$$\mathfrak{C}^1 = \begin{cases} y_1 \in C_1^2; \\ y_1 - 1 \in C_1^2; \\ y_1 + 1 \in C_0^2; \\ y_1 - \xi \in C_1^2; \\ y_1 + \xi \in C_0^2. \end{cases} \quad \mathfrak{C}^2 = \begin{cases} y_2 \in C_0^2; \\ y_2 - y_1 \in C_0^2; \\ y_2 + y_1 \in C_1^2; \\ y_2 - 1 \in C_0^2; \\ y_2 + 1 \in C_1^2; \\ y_2 + \xi \in C_0^2; \\ y_2 - \xi \in C_1^2; \\ y_2\xi + y_1 \in C_0^2; \\ y_2\xi - y_1 \in C_1^2. \end{cases} \quad \mathfrak{C}^3 = \begin{cases} y_3 \in C_1^2; \\ y_3 - y_1 \in C_0^2; \\ y_3 + y_1 \in C_1^2; \\ y_3 - 1 \in C_0^2; \\ y_3 + 1 \in C_1^2; \\ y_3 + \xi \in C_0^2; \\ y_3 - \xi \in C_1^2; \\ y_3\xi + y_1 \in C_0^2; \\ y_3\xi - y_1 \in C_1^2; \\ y_3\xi + y_2 \in C_0^2; \\ y_3\xi - y_2 \in C_1^2; \\ y_3 - y_2 \in C_0^2; \\ y_3 + y_2 \in C_1^2. \end{cases}$$

- Case 2: If $1-\xi \in C_1^2$:
  We need y_1, y_2 and y_3 such that:

$$\mathfrak{C}^1 = \begin{cases} y_1 \in C_1^2; \\ y_1 - 1 \in C_1^2; \\ y_1 + 1 \in C_1^2; \\ y_1 - \xi \in C_1^2; \\ y_1 + \xi \in C_0^2. \end{cases} \quad \mathfrak{C}^2 = \begin{cases} y_2 \in C_0^2; \\ y_2 - y_1 \in C_0^2; \\ y_2 + y_1 \in C_0^2; \\ y_2 - 1 \in C_0^2; \\ y_2 + 1 \in C_1^2; \\ y_2 + \xi \in C_0^2; \\ y_2 - \xi \in C_1^2; \\ y_2\xi + y_1 \in C_0^2; \\ y_2\xi - y_1 \in C_1^2. \end{cases} \quad \mathfrak{C}^3 = \begin{cases} y_3 \in C_1^2; \\ y_3 - y_1 \in C_0^2; \\ y_3 + y_1 \in C_1^2; \\ y_3 - 1 \in C_0^2; \\ y_3 + 1 \in C_1^2; \\ y_3 + \xi \in C_0^2; \\ y_3 - \xi \in C_0^2; \\ y_3\xi + y_1 \in C_0^2; \\ y_3\xi - y_1 \in C_1^2; \\ y_3\xi + y_2 \in C_0^2; \\ y_3\xi - y_2 \in C_1^2; \\ y_3 - y_2 \in C_1^2; \\ y_3 + y_2 \in C_1^2. \end{cases}$$

Because of Theorem 5.1.2 these systems have solutions for $p \geq Q(2, 13)$. Therefore, for these choices of y_1, y_2, y_3 each D_i contains two elements of C_0^2 and two elements of C_1^2.

Instead, for the primes $p \equiv 1 \pmod 8$, $p < Q(2, 13)$, we can find directly, by a computer search, y_1, y_2, y_3, such that each D_i contains two elements of C_0^2 and two elements of C_1^2 with the possible exceptions of $41, 73, 89, 193$. Also here we have not checked the case in which p is a prime power only because this case runs too slowly.

Thus, for these choices of y_1, y_2 and y_3, the block A satisfies the hypothesis of Theorem 2.2.8. It follows that there exists a $(17p, 17, 17, 2)$-DF for all primes $p \equiv 1$

(mod 8) with the possible exceptions of $41, 73, 89, 193$. Because of Theorem 2.1.17 we obtain a $(17, 2)$-GDD of type $(17)^p$ and hence, according to Remark 1.1.30, we get a 2-$(17p, 17, 2)$ design. □

Finally we obtain the following result that is analogous to the one of Proposition 5.3.2:

Proposition 5.3.6. *There exists a* 2-$(17q, 17, 4)$ *design for all prime powers* $q \geq 17$ *such that* $q \equiv 1 \pmod 4$.

Proof. Let us consider the Paley $(17, 17, 16)$-SDM:

$$\sigma_{17} := [0, 1, 1, -1, -1, 2, 2, -2, -2, 4, 4, -4, -4, 8, 8, -8, -8].$$

We consider the block A of elements of $\mathbb{F}_{17} \times \mathbb{F}_q$ having, as first coordinates, the elements of σ_{17}:

$$\{(0,0), (1,1), (1,-1), (-1,\xi), (-1,-\xi), (2,y_1), (2,-y_1), (-2,y_1\xi), (-2,-y_1\xi),$$

$$(4,y_2), (4,-y_2), (-4,y_2\xi), (-4,-y_2\xi), (8,y_3), (8,-y_3), (-8,y_3\xi), (-8,-y_3\xi)\},$$

where g is a primitive root of $\mathbb{F}_q$, $\xi = g^{\frac{q-1}{4}}$ and $q \equiv 1 \pmod 4$.
Using the notation of Theorem 2.2.8 we have that $\Delta[A] = \bigcup_{i=0}^{16} \{i\} \times L_i$. We set $L_i = \{1, -1, \xi, -\xi\} \cdot D_i$ where $D_i = D_{17-i}$ and:

$$\begin{array}{ll}
D_0 = 2 \cdot [1, y_1, y_2, y_3], & D_1 = [1, 1-y_1, 1+y_1, y_3(1-\xi)], \\
D_2 = [1-\xi, y_1, y_1-y_2, y_1+y_2], & D_3 = [y_1+\xi, y_1-\xi, y_2-1, y_2+1], \\
D_4 = [y_2, y_2-y_3, y_2+y_3, y_1(1-\xi)], & D_5 = [y_2+\xi, y_2-\xi, y_3+y_2\xi, y_3-y_2\xi], \\
D_6 = [y_2+y_1\xi, y_2-y_1\xi, y_3-y_1, y_3+y_1], & D_7 = [y_3+y_1\xi, y_3-y_1\xi, y_3-1, y_3+1], \\
D_8 = [y_3, y_2(1-\xi), y_3-\xi, y_3+\xi]. &
\end{array}$$

We note that if $q \geq 17$ we can choose y_1, y_2, y_3 such that all elements of each D_i are nonzero. In this case let us consider S to be a complete set of representatives for the cosets of $\{+1, -1, -\xi, \xi\}$ in $\mathbb{F}_q^*$. Then we have that:

$$S \cdot L_i = \bigcup_{s \in S} s\{+1, -1, +\xi, -\xi\} \cdot D_i = 4\mathbb{F}_q^*.$$

Therefore the block A satisfies the hypothesis of Theorem 2.2.8. It follows that there exists a $(17q, 17, 17, 4)$-DF for all prime powers $q \geq 17$ with $q \equiv 1 \pmod 4$. Because of Theorem 2.1.17 we obtain a $(17, 4)$-GDD of type $(17)^q$ and hence, according to Remark 1.1.30, we get a 2-$(17q, 17, 4)$ design. □

Summing up Propositions 5.3.5 and 5.3.6 it follows that:

Theorem 5.3.7 (S. C., X. Wang)**.** *There exists a* 2-(v, k, λ) *design in the following cases:*

(v, k, λ)	*Possible exceptions*
$(17p, 17, 2)$: $p \equiv 1 \pmod 8$, *prime* $(17q, 17, 4)$: $q \equiv 1 \pmod 4, q \geq 17$, *prime power.*	$41, 73, 89, 193$

5.3.3 2-designs from a $(63, 8, 8)$-SDF

Now we present a $(63, 8, 8)$-SDF, say Σ_3. Proceeding as in Lemma 5.2.1 and using Theorem 5.1.3 we could easily obtain the existence of a $(63q, 63, 8, 1)$-DF for all prime powers $q \geq Q(8, 7)$ with $q \equiv 9 \pmod{16}$. However, since this bound is huge we apply directly Theorem 5.1.2. We get the following result:

Lemma 5.3.8. *There exists a $(63q, 63, 8, 1)$-DF for all prime powers q such that $q \equiv 1 \pmod 8$ with the possible exceptions of $q = 17$ and $q = 81$.*

Proof. We define a $(63, 8, 8)$-SDF, say $\Sigma_3 = [X_1, \ldots, X_9]$ by giving the following multisets:

$$\begin{aligned} X_1 &:= [20, 20, -20, -20, 29, 29, -29, -29]; \\ X_2 = X_3 = X_4 = X_5 &:= [0, 1, 3, 7, 19, 34, 42, 53]; \\ X_6 = X_7 = X_8 = X_9 &:= [0, 1, 4, 6, 26, 36, 43, 51]. \end{aligned}$$

Let us consider $q \equiv 1 \pmod 8$, g a generator of $\mathbb{F}_q$ and $\xi = g^{\frac{q-1}{4}}$. We define the following blocks on $\mathbb{Z}_{63} \times \mathbb{F}_q$ having, as first coordinates the elements of Σ_3:

$$\begin{aligned} &A_1 := \{(20, 1), (20, -1), (-20, \xi), (-20, -\xi), (29, y_1), (29, -y_1), (-29, y_1\xi), (-29, -y_1\xi)\}; \\ &A_2 := \{(0, 0), (1, y_2), (3, y_3), (7, y_4), (19, y_5), (34, y_6), (42, y_7), (53, y_8)\}; \\ &A_3 := (1, -1) \cdot A_2;\ A_4 := (1, \xi) \cdot A_2;\ A_5 := (1, -\xi) \cdot A_2; \\ &A_6 := \{(0, 0), (1, y_9), (4, y_{10}), (6, y_{11}), (26, y_{12}), (36, y_{13}), (43, y_{14}), (51, y_{15})\}; \\ &A_7 := (1, -1) \cdot A_6;\ A_8 := (1, \xi) \cdot A_6;\ A_9 := (1, -\xi) \cdot A_6. \end{aligned}$$

Using the notation of Theorem 2.2.8 we have that $\Delta[A_1, \ldots, A_9] = \bigcup_{i=0}^{62} \{i\} \times L_i$ where each $L_i = \{+1, -1, \xi, -\xi\} \cdot D_i$, $D_i = D_{63-i}$ and:

$$\begin{aligned} &D_0 = 2 \cdot [1, y_1], && D_1 = [y_2, y_9], && D_2 = [y_3 - y_2, y_{11} - y_{10}], \\ &D_3 = [y_3, y_{10} - y_9], && D_4 = [y_4 - y_3, y_{10}], && D_5 = [y_1(1 - \xi), y_{11} - y_9], \\ &D_6 = [y_4 - y_2, y_{11}], && D_7 = [y_4, y_{14} - y_{13}], && D_8 = [y_{15} - y_{14}, y_7 - y_6], \\ &D_9 = [y_1 + 1, y_1 - 1], && D_{10} = [y_8, y_{13} - y_{12}], && D_{11} = [y_8 - y_2, y_8 - y_7], \\ &D_{12} = [y_5 - y_4, y_{15}], && D_{13} = [y_8 - y_3, y_{15} - y_9], && D_{14} = [y_1 + \xi, y_1 - \xi], \\ &D_{15} = [y_6 - y_5, y_{15} - y_{13}], && D_{16} = [y_5 - y_3, y_{15} - y_{10}], && D_{17} = [y_8 - y_4, y_{14} - y_{12}], \\ &D_{18} = [y_5 - y_2, y_{15} - y_{11}], && D_{19} = [y_5, y_8 - y_6], && D_{20} = [y_{14}, y_{12} - y_{11}], \\ &D_{21} = [y_7, y_{14} - y_9], && D_{22} = [y_7 - y_2, y_{12} - y_{10}], && D_{23} = [1 - \xi, y_7 - y_5], \\ &D_{24} = [y_7 - y_3, y_{14} - y_{10}], && D_{25} = [y_{12} - y_9, y_{15} - y_{12}], && D_{26} = [y_{12}, y_{14} - y_{11}], \\ &D_{27} = [y_6 - y_4, y_{13}], && D_{28} = [y_7 - y_4, y_{13} - y_9], && D_{29} = [y_6, y_8 - y_5], \\ &D_{30} = [y_6 - y_2, y_{13} - y_{11}], && D_{31} = [y_6 - y_3, y_{13} - y_{10}]. \end{aligned}$$

Let us consider S to be a complete set of representatives for the cosets of $\{+1, -1, -\xi, \xi\}$ in C_0^2. Let us suppose that each D_i contains an element of C_0^2 and an element of C_1^2. Then we would have that:

$$S \cdot L_i = \bigcup_{s \in S} s\{+1, -1, +\xi, -\xi\} \cdot D_i = \mathbb{F}_q^*.$$

Therefore the blocks $A_1, \dots, A_9$ would satisfy the assumptions of Theorem 2.2.8. Hence, in order to get a $(63q, 63, 8, 1)$-DF, we want that each D_i contains an element of C_0^2 and an element of C_1^2.

In case $q < Q(2,7)$ is a prime power $q \equiv 1 \pmod 8$, we can find directly, by a computer search, a 15-tuple $y_1, \dots, y_{15}$, such that each D_i contains an element of C_0^2 and an element of C_1^2 with the exceptions of $q = 17$ and $q = 81$.

In case $q \geq Q(2,7)$ is a prime power $q \equiv 1 \pmod 8$, similarly to Proposition 5.3.1, we can write a suitable cyclotomic systems $\mathfrak{C}^1, \dots, \mathfrak{C}^{15}$ such that given a common solution $y_1, \dots, y_{15}$ of them, each D_i contains one element of C_0^2 and one element of C_1^2. Because of Theorem 5.1.2 these systems have a common solution $y_1, \dots, y_{15}$ for all prime powers $q \geq Q(2,7)$ with $q \equiv 1 \pmod 8$. Therefore, for these choices of $y_1, \dots, y_{15}$, each D_i contains one element of C_0^2 and one element of C_1^2.

Therefore the blocks $A_1, \dots, A_9$ satisfy the hypothesis of Theorem 2.2.8. It follows that there exists a $(63q, 63, 8, 1)$-DF for all prime powers with $q \equiv 1 \pmod 8$ with the possible exceptions of 17 and 81. □

Using the previous lemma we construct the following 2-designs.

Proposition 5.3.9. *Let q be a prime power $q \equiv 1 \pmod 8$ different from 17 and 81. Then there exists a 2-$(63q + 1, 8, 1)$ design.*

Proof. Because of Lemma 5.3.8 there exists a $(63q, 63, 8, 1)$-DF and hence we get an 8-GDD of type 63^q with set of points V. According to Remark 1.1.30 we add a point to V and we cover each group of this GDD with a 2-$(64, 8, 1)$ design through the new point. We obtain a 2-$(63q + 1, 8, 1)$ design. □

This result is very interesting when $q = 25$: in fact $1576 = 63 \cdot 25 + 1$ and this value was a possible exception for the existence of such design! Therefore we can state:

Corollary 5.3.10 (S. C., X. Wang and S. C., T. Feng)**.** *There exists a 2-$(1576, 8, 1)$ design.*

To be clear, we write explicitly the solution of this case.
Called g a generator of $\mathbb{F}_{25}$ and $\xi = g^6$, we consider the following blocks[1]:

$$
\begin{array}{|l|}
\hline
A_1 : \{(20,1),(20,-1),(-20,\xi),(-20,-\xi),(29,g),(29,-g),(-29,g\xi),(-29,-g\xi)\}; \\
A_2 : \{(0,1),(1,g^6),(3,g^{18}),(7,g^{11}),(19,g^{23}),(34,g^5),(42,g^{12}),(53,g^{17})\}; \\
A_6 : \{(0,1),(1,g^6),(4,g^{17}),(6,g^{18}),(26,g^{23}),(36,g^{12}),(43,g^5),(51,g^{11})\}; \\
A_3 : (1,-1) \times A_2; \qquad A_4 : (1,\xi) \times A_2; \qquad A_5 : (1,-\xi) \times A_2; \\
A_7 : (1,-1) \times A_6; \qquad A_8 : (1,\xi) \times A_6; \qquad A_9 : (1,-\xi) \times A_6. \\
\hline
\end{array}
$$

Then we multiply each block by $(1, x)$ where x runs over S and S is a complete system of representatives of the cosets of $\{1, -1, \xi, -\xi\}$ in the multiplicative subgroup C_0^2 of $\mathbb{F}_{25}^*$ (note that ξ and $-\xi$ are squares) and we obtain a $(63 \cdot 25, 63, 8, 1)$-DF

[1]The first 2-$(1576, 8, 1)$ design we found, had different blocks and was not resolvable. This example has been found in a joint work, still in progress, with T. Feng.

and therefore a 2-$(63 \cdot 25 + 1, 8, 1)$ design. Moreover we can check using a computer that this design is actually resolvable.

5.3.4 2-designs from a $(81, 9, 8)$-SDF

Now we present a $(81, 9, 8)$-SDF, say Σ_4. Proceeding as in Lemma 5.2.1 and using Theorem 5.1.3 we could easily obtain the existence of a $(81q, 81, 9, 1)$-DF for all prime powers $q \geq Q(8, 8)$ with $q \equiv 9 \pmod{16}$. However, since this bound is huge we apply directly Theorem 5.1.2. We obtain the following result:

Lemma 5.3.11. *There exists a $(81q, 81, 9, 1)$-DF for all prime powers q such that $q \equiv 1 \pmod 8$ with the possible exceptions of $q = 9, 17, 41$ and $q = 81$.*

Proof. We define a $(81, 9, 8)$-SDF, say $\Sigma_4 = [X_1, \ldots, X_9]$ by giving the following multisets:

$$\begin{aligned} &X_1 := [0, 4, 4, -4, -4, 37, 37, -37, -37];\\ &X_2 = X_3 = X_4 = X_5 := [0, 1, 4, 6, 17, 18, 38, 63, 72];\\ &X_6 = X_7 = X_8 = X_9 := [0, 2, 7, 27, 30, 38, 53, 59, 69]. \end{aligned}$$

Let us consider $q \equiv 1 \pmod 8$, g a generator of $\mathbb{F}_q$ and $\xi = g^{\frac{q-1}{4}}$. We define the following blocks on $\mathbb{Z}_{81} \times \mathbb{F}_q$ having, as first coordinates the elements of Σ_4:

$$\begin{aligned} &A_1 := \{(0,0), (4,1), (4,-1), (-4,\xi), (-4,-\xi), (37,y_1), (37,-y_1), (-37,y_1\xi), (-37,-y_1\xi)\};\\ &A_2 := \{(0,0), (1,y_2), (4,y_3), (6,y_4), (17,y_5), (18,y_6), (38,y_7), (63,y_8), (72,y_9)\};\\ &A_3 := (1,-1) \cdot A_2;\ A_4 := (1,\xi) \cdot A_2;\ A_5 := (1,-\xi) \cdot A_2;\\ &A_6 := \{(0,9), (2,y_{10}), (7,y_{11}), (27,y_{12}), (30,y_{13}), (38,y_{14}), (53,y_{15}), (59,y_{16}), (69,y_{17})\};\\ &A_7 := (1,-1) \cdot A_6;\ A_8 := (1,\xi) \cdot A_6;\ A_9 := (1,-\xi) \cdot A_6. \end{aligned}$$

Using the notation of Theorem 2.2.8 we have that $\Delta[A_1, \ldots, A_9] = \bigcup_{i=0}^{80} \{i\} \times L_i$ where each $L_i = \{+1, -1, \xi, -\xi\} \cdot D_i$, $D_i = D_{81-i}$ and:

$$\begin{aligned} D_0 &= 2 \cdot [1, y_1], & D_1 &= [y_2, y_6 - y_5],\\ D_2 &= [y_4 - y_3, y_{10}], & D_3 &= [y_3 - y_2, y_{13} - y_{12}],\\ D_4 &= [1, y_3], & D_5 &= [y_4 - y_2, y_{11} - y_{10}],\\ D_6 &= [y_4, y_{16} - y_{15}], & D_7 &= [(1-\xi)y_1, y_{11}],\\ D_8 &= [1 - \xi, y_{14} - y_{13}], & D_9 &= [y_9, y_9 - y_8],\\ D_{10} &= [y_9 - y_2, y_{17} - y_{16}], & D_{11} &= [y_5 - y_4, y_{14} - y_{12}],\\ D_{12} &= [y_6 - y_4, y_{17}], & D_{13} &= [y_5 - y_3, y_9 - y_3],\\ D_{14} &= [y_6 - y_3, y_{17} - y_{10}], & D_{15} &= [y_9 - y_4, y_{15} - y_{14}],\\ D_{16} &= [y_5 - y_2, y_{17} - y_{15}], & D_{17} &= [y_5, y_6 - y_2],\\ D_{18} &= [y_6, y_8], & D_{19} &= [y_8 - y_2, y_{17} - y_{11}],\\ D_{20} &= [y_7 - y_6, y_{12} - y_{11}], & D_{21} &= [y_7 - y_5, y_{16} - y_{14}],\\ D_{22} &= [y_8 - y_3, y_{16}], & D_{23} &= [y_{13} - y_{11}, y_{15} - y_{13}],\\ D_{24} &= [y_8 - y_4, y_{16} - y_{10}], & D_{25} &= [y_8 - y_7, y_{12} - y_{10}],\\ D_{26} &= [y_9 - y_5, y_{15} - y_{12}], & D_{27} &= [y_9 - y_6, y_{12}],\\ D_{28} &= [y_{15}, y_{13} - y_{10}], & D_{29} &= [y_{16} - y_{11}, y_{16} - y_{13}], \end{aligned}$$

$$\begin{array}{ll} D_{30} = [y_{13}, y_{15} - y_{10}], & D_{31} = [y_{14} - y_{11}, y_{17} - y_{14}], \\ D_{32} = [y_7 - y_4, y_{16} - y_{12}], & D_{33} = [y_1 - 1, y_1 + 1], \\ D_{34} = [y_7 - y_3, y_9 - y_7], & D_{35} = [y_8 - y_5, y_{15} - y_{11}], \\ D_{36} = [y_8 - y_6, y_{14} - y_{10}], & D_{37} = [y_1, y_7 - y_2], \\ D_{38} = [y_7, y_{14}], & D_{39} = [y_{17} - y_{12}, y_{17} - y_{13}], \\ D_{40} = [y_1 + \xi, y_1 - \xi]. & \end{array}$$

Let us consider S to be a complete set of representatives for the cosets of $\{+1, -1, -\xi, \xi\}$ in C_0^2. Let us suppose that each D_i contains an element of C_0^2 and an element of C_1^2. Then we would have that:

$$S \cdot L_i = \bigcup_{s \in S} s\{+1, -1, +\xi, -\xi\} \cdot D_i = \mathbb{F}_q^*.$$

Therefore the blocks $A_1, \ldots, A_9$ would satisfies the assumptions of Theorem 2.2.8. Hence, in order to get a $(81q, 81, 9, 1)$-DF, we want that each D_i contains an element of C_0^2 and an element of C_1^2.

In case $q < Q(2, 8)$ is a prime power $q \equiv 1 \pmod 8$, we can find directly, by a computer search, a 17-tuple $y_1, \ldots, y_{17}$, such that each D_i contains an element of C_0^2 and an element of C_1^2 with the exceptions of $q = 9, 17, 41$ and $q = 81$.

In case $q \geq Q(2, 8)$ is a prime power $q \equiv 1 \pmod 8$, similarly to Proposition 5.3.1, we can write a suitable cyclotomic systems $\mathfrak{C}^1, \ldots, \mathfrak{C}^{17}$ such that given a common solution $y_1, \ldots, y_{17}$ of them, each D_i contains one element of C_0^2 and one element of C_1^2. Because of Theorem 5.1.2 these systems have a common solution $y_1, \ldots, y_{17}$ for all prime powers $q \geq Q(2, 8)$ with $q \equiv 1 \pmod 8$. Therefore, for these choices of $y_1, \ldots, y_{17}$, each D_i contains one element of C_0^2 and one element of C_1^2.

Thus the blocks $A_1, \ldots, A_9$ satisfy the hypothesis of Theorem 2.2.8. It follows that there exists an $(81q, 81, 9, 1)$-DF for all prime powers $q \equiv 1 \pmod 8$ with the possible exceptions of $9, 17, 41$ and 81. □

Using the previous lemma we construct the following 2-designs:

Proposition 5.3.12. *Let q be a prime power $q \equiv 1 \pmod 8$ different from $9, 17, 41$ and 81. Then there exists a 2-$(81q, 9, 1)$ design.*

Proof. For this kind of q, according to Theorem 2.1.17, we get a 9-GDD of type 81^q and, covering the groups of this GDD with a 2-$(81, 9, 1)$ design, we obtain a 2-$(81q, 9, 1)$ design. □

This result is very interesting when $q = 25$: in fact $2025 = 25 \cdot 81$ and this value was a possible exception for the existence of such design! Therefore we can state:

Corollary 5.3.13. *There exists a 2-$(2025, 9, 1)$ design.*

In order to be clear we write explicitly the solution of this case.
Called g a generator of $\mathbb{F}_{25}$ and $\xi = g^6$ we consider the following blocks:

$A_1 : \{(0,0),(4,1),(4,-1),(-4,\xi),(-4,-\xi),(37,g^1),(37,-g^1),(-37,g^1\xi),(-37,-g^1\xi)\}$;
$A_2 : \{(0,0),(1,1),(4,g),(6,g^2),(17,g^3),(18,g^6),(38,g^4),(63,g^5),(72,g^7)\}$;
$A_6 : \{(0,0),(2,g),(7,g^8),(27,g^{12}),(30,g^{11}),(38,g^5),(53,g^{15}),(59,g^{18}),(69,g^{21})\}$;
$A_3 : (1,-1) \times A_2$; $A_4 : (1,\xi) \times A_2$; $A_5 : (1,-\xi) \times A_2$;
$A_7 : (1,-1) \times A_6$; $A_8 : (1,\xi) \times A_6$; $A_9 : (1,-\xi) \times A_6$.

Then we multiply each block by $(1,x)$ where x runs over S and S is a complete system of representatives of the cosets of $\{1,-1,\xi,-\xi\}$ in the multiplicative subgroup C_0^2 of $\mathbb{F}_{25}^*$ (note that ξ and $-\xi$ are squares) and we obtain a $(81 \cdot 25, 81, 9, 1)$-DF and therefore a 2-$(81 \cdot 25, 9, 1)$ design.

5.3.5 2-designs from a $(45,9,8)$-SDF

Now we present a $(45,9,8)$-SDF, say Σ_5. Proceeding as in Proposition 5.2.4 and using Theorem 5.1.4 we could easily obtain the existence of a $(45q,45,9,2)$-DF for all prime powers $q \geq Q(4,8)$ with $q \equiv 1 \pmod 4$. However, also in this case we can get a better bound by applying directly Theorem 5.1.2. We obtain the following result:

Lemma 5.3.14. *There exists a $(45q,45,9,2)$-DF for all prime powers $q \geq Q(2,8)$, $q \equiv 1 \pmod 4$ and for $q \in \{17,41\}$.*

Proof. We define a $(45,9,8)$-SDF, say $\Sigma_5 = [X_1,\ldots,X_5]$ by giving the following multisets:

$$X_1 := [0,2,2,15,15,23,23,33,33];$$
$$X_2 = X_3 := [0,1,4,5,6,7,13,22,33];$$
$$X_4 = X_5 := [0,2,5,11,21,25,28,36,40];$$

Let us consider $q \equiv 1 \pmod 4$. We define the following blocks on $\mathbb{Z}_{45} \times \mathbb{F}_q$ having, as first coordinates the elements of Σ_5:

$$A_1 := \{(0,0),(2,1),(2,-1),(15,y_1),(15,-y_1),(23,y_2),(23,-y_2),(33,y_3),(33,-y_3)\};$$
$$A_2 := \{(0,0),(1,y_4),(4,y_5),(5,y_6),(6,y_7),(7,y_8),(13,y_9),(22,y_{10}),(33,y_{11})\};$$
$$A_4 := \{(0,0),(2,y_{12}),(5,y_{13}),(11,y_{14}),(21,y_{15}),(25,y_{16}),(28,y_{17}),(36,y_{18}),(40,y_{19})\}.$$
$$A_3 := (1,-1) \cdot A_2;\ A_5 := (1,-1) \cdot A_4.$$

Using the notation of Theorem 2.2.8 we have that $\Delta[A_1,\ldots,A_5] = \bigcup_{i=0}^{44}\{i\} \times L_i$ where each $L_i = \{+1,-1\} \cdot D_i$, $D_i = D_{45-i}$ and:

$$D_0 = 2 \cdot [1,y_1,y_2,y_3], \qquad D_1 = [y_4, y_6-y_5, y_7-y_6, y_8-y_7],$$
$$D_2 = [1, y_7-y_5, y_8-y_6, y_{12}], \qquad D_3 = [y_5-y_4, y_8-y_5, y_{13}-y_{12}, y_{17}-y_{16}],$$
$$D_4 = [y_5, y_6-y_4, y_{16}-y_{15}, y_{19}-y_{18}], \qquad D_5 = [y_6, y_7-y_4, y_{13}, y_{19}],$$
$$D_6 = [y_7, y_8-y_4, y_9-y_8, y_{14}-y_{13}], \qquad D_7 = [y_8, y_9-y_7, y_{19}-y_{12}, y_{17}-y_{15}],$$
$$D_8 = [y_2-y_1, y_2+y_1, y_9-y_6, y_{18}-y_{17}], \qquad D_9 = [y_9-y_5, y_{10}-y_9, y_{18}, y_{14}-y_{12}],$$
$$D_{10} = [y_3-y_2, y_3+y_2, y_{19}-y_{13}, y_{15}-y_{14}], \qquad D_{11} = [y_{11}-y_{10}, y_{14}, y_{18}-y_{12}, y_{18}-y_{16}],$$

$D_{12} = [y_3, y_9 - y_4, y_{11}, y_{19} - y_{17}]$, $D_{13} = [y_1 - 1, y_1 + 1, y_9, y_{11} - y_4]$,
$D_{14} = [y_3 - 1, y_3 + 1, y_{18} - y_{13}, y_{16} - y_{14}]$, $D_{15} = [y_1, y_{10} - y_8, y_{18} - y_{15}, y_{19} - y_{16}]$,
$D_{16} = [y_{11} - y_5, y_{10} - y_7, y_{15} - y_{13}, y_{19} - y_{14}]$, $D_{17} = [y_{10} - y_6, y_{11} - y_6, y_{17}, y_{17} - y_{14}]$,
$D_{18} = [y_3 - y_1, y_3 + y_1, y_{10} - y_5, y_{11} - y_7]$, $D_{19} = [y_{11} - y_8, y_{15} - y_{12}, y_{17} - y_{12}, y_{19} - y_{15}]$,
$D_{20} = [y_{11} - y_9, y_{16}, y_{16} - y_{13}, y_{18} - y_{14}]$, $D_{21} = [y_2 - 1, y_2 + 1, y_{10} - y_4, y_{15}]$,
$D_{22} = [y_2, y_{10}, y_{16} - y_{12}, y_{17} - y_{13}]$

Let us consider S to be a complete set of representatives for the cosets of $\{+1, -1\}$ in C_0^2. Let us suppose that two elements of each D_i belong to C_0^2 and two elements of each D_i belong to C_1^2. Then it would follows that:

$$S \cdot L_i = \bigcup_{s \in S} sL_i = 2\mathbb{F}_q^*.$$

Therefore the blocks $A_1, \ldots, A_5$ and the set S would satisfy the assumptions of Theorem 2.2.8. Using a computer we can find these second components for $q \in \{17, 41\}$. In fact we find a 19-tuple $(y_1, \ldots, y_{19})$ of elements of $\mathbb{F}_{17}$ and another 19-tuple of elements of $\mathbb{F}_{41}$ such that for each D_i two elements lie in C_0^2 and two elements lie in C_1^2. The explicit solutions are, respectively, the following:

$q = 41$:
$A_1 = \{(0,0), (2,1), (2,-1), (15,2), (15,-2), (23,3), (23,-3), (33,6), (33,-6)\}$;
$A_2 = \{(0,0), (1,1), (4,7), (5,21), (6,12), (7,15), (13,24), (22,4), (33,34)\}$;
$A_3 = (1,-1) \cdot A_2$;
$A_4 = \{(0,0), (2,3), (5,31), (11,32), (21,15), (25,9), (28,40), (36,25), (40,35)\}$;
$A_5 = (1,-1) \cdot A_4$.
$q = 17$:
$A_1 = \{(0,0), (2,1), (2,-1), (15,2), (15,-2), (23,3), (23,-3), (33,5), (33,-5)\}$;
$A_2 = \{(0,0), (1,1), (4,2), (5,3), (6,6), (7,9), (13,4), (22,11), (33,15)\}$;
$A_3 = (1,-1) \cdot A_2$;
$A_4 = \{(0,0), (2,3), (5,8), (11,6), (21,12), (25,7), (28,9), (36,2), (40,13)\}$;
$A_5 = (1,-1) \cdot A_4$.

Now, similarly to Proposition 5.3.1, we can write a suitable cyclotomic systems $\mathfrak{C}^1, \ldots, \mathfrak{C}^{19}$ such that given a common solution of them $y_1, \ldots, y_{19}$, each D_i contains two elements of C_0^2 and two elements of C_1^2. Because of Theorem 5.1.2 these systems have a common solution $y_1, \ldots, y_{19}$ for all prime powers $q \geq Q(2,8)$ with $q \equiv 1 \pmod 2$. Therefore, for these choices of $y_1, \ldots, y_{19}$, each D_i contains two elements of C_0^2 and two elements of C_1^2.

Thus the blocks $A_1, \ldots, A_5$ satisfy the hypothesis of Theorem 2.2.8. It follows that there exists a $(45q, 45, 9, 2)$-DF for all prime powers $q \geq Q(2,8)$ such that $q \equiv 1 \pmod 4$ and for $q \in \{17, 41\}$. □

Using the previous lemma we construct the following new 2-designs:

Corollary 5.3.15. *There exists a* 2-$(v, 9, 2)$ *design for* $v \in \{45 \cdot 17, 45 \cdot 41\}$.

Proof. We consider $(9,2)$-GDDs of type 45^{17} and of type 45^{41} defined respectively by a $(45\cdot 17, 45, 9, 2)$-DF and a $(45\cdot 41, 45, 9, 2)$-DF (see Theorem 2.1.17). According to Remark 1.1.30 we fill the groups of these GDDs with a 2-$(45, 9, 2)$ design and we obtain the required 2-$(v, 9, 2)$ design. □

5.4 Concluding remarks

First of all it is worth summarizing the main results of this chapter in the following theorem:

Theorem 5.4.1 (S. C., X. Wang)**.** *There exists a* 2-(v, k, λ) *design in the following cases:*

(v, k, λ)	*Possible exceptions*
$(694, 7, 2)$ $(1576, 8, 1)$ $(2025, 9, 1)$, $(765, 9, 2)$ *and* $(1845, 9, 2)$ $(459, 9, 4)$ *and* $(783, 9, 4)$	
$(13p, 13, 1)$: $p \equiv 1 \pmod{12}$, *prime* $(13q, 13, 3)$: $q \equiv 1 \pmod 4, q \geq 13$, *prime power*	*List of* 19 *values*
$(17p, 17, 2)$: $p \equiv 1 \pmod 8$, *prime* $(17q, 17, 4)$: $q \equiv 1 \pmod 4, q \geq 17$, *prime power.*	$41, 73, 89, 193$

We also remark that, as we have seen in the second part of this chapter, in some cases, given a (g, k, λ)-SDF, by applying directly Theorem 5.1.2 it is possible to get theoretically a much better bound for the existence of a $(gq, g, k, 1)$-DF, compared to that of Theorem 5.1.3. In a joint work, still in progress, with X. Wang we have seen that this idea works for all Paley $(q_1, q_1, q_1 - 1)$-SDMs with $q_1 \equiv 5 \pmod 8$. In this case we get the following theorem:

Theorem 5.4.2. *Let* q *and* q_1 *be prime powers. Then there exists a* 2-(v, k, λ) *design in the following cases:*

1) A 2-$(q_1 q, q_1, \frac{q_1-1}{4})$ *design where* $q, q_1 \equiv 1 \pmod 4$ *and* $q \geq q_1$*;*

2) A 2-$(q_1 q, q_1, \lambda)$ *design where* $q_1 \equiv 5 \pmod 8$, $q \equiv 1 \pmod{\frac{q_1-1}{\lambda}}$ *and* $q \geq Q(\frac{q_1-1}{4\lambda}, q_1 - 4)$*;*

3) A 2-$(q_1 q, q_1, \lambda)$ *design where* $q_1 \equiv 1 \pmod 2$, $q \equiv 1 \pmod{\frac{q_1-1}{\lambda}}$ *and* $q > Q(\frac{q_1-1}{2\lambda}, q_1 - 1)$.

We omit the proof since it is very similar but much longer and even more technical than that of Proposition 5.3.1 and because it goes out of the purposes of this discussion. However, in accordance to Proposition 5.3.4, we conjecture that the result of point 2 can be obtained also for all prime powers $q_1 \equiv 1 \pmod 4$ that are not powers of 3. More generally, our future project is to write explicitly the hypothesis under which a SDF leads to such good bound (in a future joint work with T. Feng and X. Wang). In fact we believe that these ideas can still give new existence results for 2-designs, GDDs and resolvable 2-designs.

Bibliography

[1] R.J.R. Abel, Forty-three balanced incomplete block designs, Journal of Combinatorial Theory, Series A, 65 (1994), 252-267.

[2] R.J.R. Abel, Some New BIBDs with $\lambda = 1$ and $6 \leq k \leq 10$, Journal of Combinatorial Designs, 4 (1) (1996), 27-50.

[3] R.J.R. Abel and M. Buratti, Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes, J. Combin. Theory Ser. A 106 (2004), 59-75.

[4] P. Adams, E. J. Billington, and C.C. Lindner, The spectrum for 3-perfect 9-cycle systems, Australas J. Combin. 5 (1992), 103-108.

[5] P. Adams and E.J. Billington, Completing some spectra for 2-perfect cycle systems, Australas. J. Combin. 7 (1993), 175-187.

[6] P. Adams and D. E. Bryant, i-perfect m-cycle systems, $m \leq 19$, Aequationes Math 53 (1997), 275-294.

[7] N. Alon, The strong chromatic number of a graph, Random Structures Algorithms 3 (2006), 1-7.

[8] B. Alspach and H. Gavlas, Cycle decompositions of $\mathbb{K}_n$ and $\mathbb{K}_n - I$, J. Combin. Theory Ser. B 81, (2001), 77-99.

[9] S. Bagchi and B. Bagchi, Designs from pairs of finite fields. A cyclic unital $U(6)$ and other regular Steiner 2-designs, J. Combin. Theory Ser. A 52 (1989), 51-61.

[10] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge (1999).

[11] S. Bitan and T. Etzion, Constructions for optimal constant weight cyclically permutable codes and difference families, IEEE Trans. Inform. Theory 41 (1995), 77-87.

[12] A. Bonisoli, M. Buratti and G. Mazzuoccolo, *Doubly transitive* 2*-factorizations*, J. Combin. Des. **15** (2007), 120-132.

[13] R.C. Bose, An affine analogue of Singer's theorem, J. Indian Math. Soc. 6 (1942), 1-15.

[14] R.C. Bose, On the construction of balanced incomplete block designs, Annals of Eugenics 9 (1939), 353-399.

[15] D. Bryant, and C. Rodger, Cycle decompositions, in: C.J. Colbourn and J.H. Dinitz (Eds), The CRC Handbook of Combinatorial Designs, 2nd edition, CRC Press, Boca Raton (2007), 373-382.

[16] A.E. Brouwer, A. Schrijver, and H. Hanani, Group divisible designs with block size four, Discrete Math. 20 (1977), 1-10.

[17] M. Buratti, Rotational k-cycle systems of order $v < 3k$; another proof of the existence of odd cycle systems, J. Combin. Des. 11 (2003), 433-441.

[18] M. Buratti, Constructions for $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, Discrete Math. 138 (1995) 169-175.

[19] M. Buratti, Constructions for point-regular linear spaces, J. Statist. Plann. Inference 94 (2001), 139-146.

[20] M. Buratti, Cyclotomic conditions leading to new Steiner 2-designs, Finite Fields Appl. 3 (1997), 300-313.

[21] M. Buratti, Recursive constructions for difference matrices and relative difference families, J. Combin. Des. 6 (1998), 165-182.

[22] M. Buratti, Old and new designs via difference multisets and strong difference families, J. Combin. Des. 7 (1999), 406-425.

[23] M. Buratti, Cyclic Designs with Block Size 4 and Related Optimal Optical Orthogonal Codes, Des. Codes Cryptogr. 26 (2002), 111-125.

[24] M. Buratti, S. Costa and X. Wang, New i-perfect cycle decompositions via vertex colorings of graphs, J. Combin. Des. To Appear.

[25] M. Buratti and L. Gionfriddo, Strong difference families over arbitrary groups, J. Combin. Des. 16 (2008), 443-461.

[26] M. Buratti and A. Pasotti, Combinatorial designs and the Theorem of Weil on multiplicative character sums, Finite Fields Appl. 15 (2009), 332-344.

[27] M. Buratti and A. Pasotti, Further progress on difference families with block size 4 or 5, Des. Codes Cryptogr. 56 (2010), 1-20.

[28] M. Buratti and A. Pasotti, On perfect Γ-decompositions of the complete graph, J Combin Des. 17, Issue 2, (2009), 197-209.

[29] M. Buratti, F. Rania and F. Zuanni, Some constructions for cyclic perfect cycle systems, Discrete Math. 299 (2005), 33-48.

[30] M. Buratti, G. Rinaldi and T. Traetta, Some results on 1-rotational Hamiltonian cycle systems, J. Combin. Des. 22 (2014), 231-251.

[31] M. Buratti and F. Zuanni, G-invariantly resolvable Steiner 2-designs which are 1-rotational over G, Bull. Belg. Math. Soc. Simon Stevin 5 (1998), 221-235.

[32] Y. Chang and L. Ji, Optimal $(4up, 5, 1)$ optical orthogonal codes, J. Combin. Des. 12 (2004), 346-361.

[33] Y. Chang and J. Yin, Further results on optimal optical orthogonal codes with weight 4, Discrete Math. 279 (2004), 135-151.

[34] K. Chen, G. Ge, and L. Zhu, Starters and their related codes, J. Statist. Plann. Inference, 86 (2000), 379-395.

[35] K. Chen, R. Wei, and L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, Des. Codes Cryptogr. 15 (1998), 167-173.

[36] K. Chen and L. Zhu, Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, J. Combin. Des. 7 (1999), 21-30.

[37] K. Chen and L. Zhu, Existence of $(q, 7, 1)$ difference families with q a prime power, J. Combin. Des. 10 (2002), 126-138.

[38] C.J. Colbourn and J.H. Dinitz, The CRC Handbook of Combinatorial Designs, CRC press, Boca Raton (2007).

[39] R. Fuji-Hara and Y. Miao, Optical orthogonal codes: their bounds and new optimal constructions, IEEE Trans. Inform. Theory 46 (2000), 2396-2406.

[40] R. Fuji-Hara, Y. Miao, and J. Yin, Optimal $(9v, 4, 1)$ optical orthogonal codes, SIAM J. Discrete Math. 14 (2001), 256-266.

[41] G. Ge and J. Yin, Constructions for optimal $(v, 4, 1)$ optical orthogonal codes, IEEE Trans. Inform. Theory 47 (2001), 2999-3004.

[42] M. Greig, Recursive constructions of balanced incomplete block designs with block size of $7, 8$ or 9, Ars Combin. 60 (2001), 3-54.

[43] M. Greig, Some group divisible design constructions, J. Combin. Math. Combin. Comput. 27 (1998), 33-52.

[44] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975), 255-369.

[45] P. Keevash, The existence of designs. arXiv:1401.3665.

[46] M. Kobayashi, B. McKay, N. Mutoh, G. Nakamura and C. Nara, 3-perfect Hamiltonian decomposition of the complete graph, Australas. J. Combin. 56 (2013), 219-224.

[47] R. Lidl, H. Neiderreiter, Finite Fields, Encyclopedia Math., vol. 20, Cambridge University Press, Cambridge, UK, 1983.

[48] C. C. Lindner, K. T. Phelps, and C. A. Rodger, The spectrum for 2-perfect 6-cycle systems, J. Combin. Theory Ser. A 57 (1991), 76-85.

[49] C.C. Lindner and C.A. Rodger, 2-perfect m-cycle systems, Discrete Math. 104 (1992), 83-90.

[50] C.C. Lindner and C.A. Rodger, *Decomposition into cycles II. Cycle systems*, in: J.H. Dinitz and D.R. Stinson (Eds), Contemporary Design Theory: A Collection of Surveys, Wiley, New York (1992), 325-369.

[51] S. Ma and Y. Chang, A new class of optimal optical orthogonal codes with weight five, IEEE Trans. Inform. Theory 50 (2004) 1848-1850.

[52] S. Ma and Y. Chang, Constructions of optimal optical orthogonal codes with weight five, J. Combin. Des. 13 (2005), 54-69.

[53] B.R. McDonald, Finite rings with identity. Marcel Dekker Incorporated, 1974.

[54] K. Momihara, Strong difference families, difference covers, and their applications for relative difference families, Des. Codes Cryptogr. 51 (2008), 253-273.

[55] R.E.A.C. Paley, On orthogonal matrices, J. Math and Phys, 12, (1933), 311-320.

[56] A. Pott, *A survey on relative difference sets*, in: K.T. Arasu, J.F. Dillon, K. Harada, S. Sehgal, R. Solomon, Groups, Difference Sets and the Monster, Walter de Gruyter and Co, Hawthorne (1996),195-232.

[57] M. Šajna, Cycle decompositions III: Complete graphs and fixed length cycles, J. Combin. Des. 10 (2002), 27-78.

[58] B.R. Smith and N. Cavenagh, Decomposing complete equipartite graphs into short odd cycles, Electron. J. Combin. 17 (2010), 21 pp.

[59] B.R. Smith and N. Cavenagh, Decomposing complete equipartite graphs into short even cycles, J. Combin. Des. 19 (2011), 131-143.

[60] D. R. Stinson, Combinatorial Designs: Constructions and Analysis, Springer, Heidelberg (2005).

[61] D. West, Introduction to Graph Theory. Prentice Hall, 2007.

[62] R.M.Wilson, An Existence Theory for Pairwise Balanced Designs I. Composition Theorems and Morphisms, Journal of Combinatorial Theory 13 (1972), 220-245.

[63] J. Yin, Some combinatorial constructions for optical orthogonal codes, Discrete Math. 185 (1998), 201-219.

[64] J. Yin, X. Yang, and Y. Li, Some 20-regular $CDP(5,1;20u)$ and their applications, Finite Fields Appl. 17 (2011), 317-328.

Appendix 1

Here we present the generating cycle C_k^i of a 1-rotational $HCS(k)$ for all pairs (i,k) that are necessary for proving Proposition 3.6.4. Thus, if a pair (i,k) with $k < 56$ is missing, it is either because it is one of the exceptional pairs mentioned in the statement or because an i-perfect $HCS(k)$ can be deduced from already known facts. So we omit to consider all pairs with k a prime or $i = 3$. We also omit all pairs with $i = 2$ and $k \in \{15, 21, 25, 27, 33, 35, 39\}$ because in this case a 2-perfect 1-rotational $HCS(k)$ has been given in [29]. Finally, for the reason explained in the end of the proof of Proposition 3.6.2, if an i-perfect $HCS(k)$ is known or we report C_k^i, then we omit to report C_k^j whenever we have $ij \equiv \pm 1 \pmod{k}$ with $j \neq i$.

Each C_k^i is presented by giving one of the two subpaths of it of order $\frac{k+1}{2}$ with an endpoint in ∞. This is because its remaining part can be determined by the rule that to add $\frac{k-1}{2} \pmod{k-1}$ reflects C_k^i around its axis through ∞.

$C_{45}^2 : [\infty, 0, 1, 3, 6, 2, 8, 13, 27, 36, 18, 7, 38, 19, 12, 33, 4, 20, 10, 37, 17, 9, 21]$
$C_{49}^2 : [\infty, 0, 2, 1, 4, 8, 13, 3, 9, 21, 36, 5, 14, 43, 17, 35, 42, 15, 31, 44, 16, 30, 22, 47, 10]$
$C_{51}^2 : [\infty, 0, 3, 2, 4, 8, 1, 12, 6, 23, 39, 44, 7, 22, 42, 30, 16, 43, 35, 9, 49, 21, 40, 11, 20, 38]$
$C_{55}^2 : [\infty, 0, 2, 1, 4, 8, 13, 3, 9, 16, 32, 41, 17, 52, 34, 20, 46, 12, 49, 6, 21, 42, 11, 23, 45, 53, 24, 37]$

$C_{15}^4 : [\infty, 0, 2, 3, 6, 1, 11, 5]$
$C_{21}^4 : [\infty, 0, 1, 3, 6, 17, 9, 14, 8, 12, 5]$
$C_{25}^4 : [\infty, 0, 1, 3, 7, 18, 8, 5, 21, 2, 11, 4, 10]$
$C_{27}^4 : [\infty, 0, 1, 3, 8, 11, 15, 23, 17, 7, 22, 5, 19, 12]$
$C_{33}^4 : [\infty, 0, 1, 3, 7, 2, 5, 25, 15, 8, 14, 28, 4, 13, 26, 11, 22]$
$C_{35}^4 : [\infty, 0, 1, 3, 6, 2, 9, 28, 12, 33, 4, 24, 13, 22, 14, 8, 32, 10]$
$C_{39}^4 : [\infty, 0, 21, 22, 25, 30, 23, 32, 26, 24, 36, 9, 33, 8, 12, 35, 15, 37, 29, 1]$
$C_{45}^4 : [\infty, 0, 21, 23, 24, 27, 31, 42, 33, 38, 28, 3, 10, 18, 34, 19, 36, 30, 4, 17, 29, 15, 35]$
$C_{49}^4 : [\infty, 0, 2, 1, 4, 8, 3, 10, 16, 35, 7, 21, 33, 41, 20, 43, 13, 39, 30, 14, 47, 36, 46, 29, 42]$
$C_{51}^4 : [\infty, 0, 24, 26, 27, 30, 34, 28, 39, 46, 37, 32, 45, 35, 16, 8, 23, 43, 31, 17, 40, 11, 44, 22, 4, 38]$
$C_{55}^4 : [\infty, 0, 2, 1, 4, 8, 3, 10, 16, 5, 13, 42, 51, 41, 53, 21, 47, 17, 33, 52, 34, 19, 50, 36, 49, 12, 45, 11]$

$C_{25}^5 : [\infty, 0, 1, 3, 7, 18, 9, 17, 10, 20, 14, 11, 16]$
$C_{27}^5 : [\infty, 0, 1, 3, 6, 20, 12, 22, 5, 24, 4, 8, 23, 2]$
$C_{33}^5 : [\infty, 0, 1, 3, 6, 2, 25, 30, 15, 4, 11, 21, 29, 23, 10, 28, 8]$
$C_{35}^5 : [\infty, 0, 1, 3, 6, 2, 8, 15, 24, 12, 26, 5, 10, 33, 14, 30, 4, 28]$
$C_{39}^5 : [\infty, 0, 1, 3, 6, 2, 7, 28, 15, 24, 32, 16, 31, 11, 23, 37, 10, 17, 27, 33]$
$C_{45}^5 : [\infty, 0, 1, 3, 6, 2, 7, 13, 4, 20, 12, 36, 19, 37, 16, 30, 5, 17, 10, 21, 11, 40, 9]$
$C_{49}^5 : [\infty, 0, 20, 21, 23, 26, 22, 27, 33, 25, 37, 28, 11, 41, 16, 32, 42, 7, 14, 36, 15, 29, 10, 43, 6]$
$C_{51}^5 : [\infty, 0, 22, 23, 26, 24, 28, 33, 42, 29, 39, 45, 37, 44, 11, 46, 7, 31, 15, 38, 9, 27, 41, 10, 30, 18]$
$C_{55}^5 : [\infty, 0, 24, 25, 28, 26, 30, 35, 29, 38, 31, 46, 33, 49, 5, 17, 39, 16, 37, 18, 36, 47, 7, 15, 41, 21, 50, 13]$

$C_{15}^6 : [\infty, 0, 2, 3, 6, 1, 11, 5]$
$C_{21}^6 : [\infty, 0, 1, 4, 8, 6, 13, 2, 7, 15, 9]$
$C_{27}^6 : [\infty, 0, 1, 3, 9, 6, 18, 25, 7, 11, 21, 4, 15, 10]$
$C_{33}^6 : [\infty, 0, 1, 3, 6, 10, 27, 2, 21, 31, 23, 9, 14, 20, 29, 8, 28]$
$C_{35}^6 : [\infty, 0, 1, 3, 6, 2, 8, 33, 11, 24, 13, 32, 22, 27, 9, 29, 21, 14]$
$C_{39}^6 : [\infty, 0, 1, 3, 6, 2, 7, 15, 5, 16, 32, 12, 29, 17, 23, 8, 33, 9, 18, 11]$
$C_{45}^6 : [\infty, 0, 15, 16, 18, 21, 17, 23, 28, 20, 34, 14, 2, 13, 4, 29, 8, 25, 32, 19, 9, 27, 11]$
$C_{49}^6 : [\infty, 0, 20, 21, 23, 26, 31, 25, 39, 30, 38, 22, 43, 33, 40, 27, 10, 32, 36, 11, 29, 41, 4, 37, 18]$
$C_{55}^6 : [\infty, 0, 1, 3, 6, 2, 7, 13, 20, 12, 21, 45, 14, 31, 16, 35, 19, 51, 11, 36, 15, 25, 5, 17, 53, 10, 23, 49]$

C_{25}^{7} : $[\infty, 0, 1, 3, 6, 20, 16, 7, 23, 17, 22, 9, 2]$
C_{33}^{7} : $[\infty, 0, 1, 3, 6, 2, 12, 31, 23, 11, 29, 20, 26, 5, 30, 25, 8]$
C_{35}^{7} : $[\infty, 0, 1, 3, 6, 2, 7, 32, 11, 22, 10, 25, 31, 4, 30, 12, 26, 16]$
C_{39}^{7} : $[\infty, 0, 1, 3, 6, 2, 7, 15, 27, 10, 16, 9, 36, 13, 23, 37, 24, 33, 11, 31]$
C_{45}^{7} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 5, 12, 41, 10, 38, 14, 40, 15, 26, 43, 11, 20, 30, 9, 39]$
C_{49}^{7} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 4, 12, 29, 41, 9, 46, 23, 44, 10, 43, 8, 15, 45, 35, 16, 42, 14]$
C_{51}^{7} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 49, 33, 21, 48, 9, 40, 22, 12, 45, 10, 39, 17, 41, 5, 18]$
C_{55}^{7} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 8, 42, 25, 44, 12, 53, 41, 23, 9, 24, 47, 18, 48, 22, 32, 16, 37]$

C_{21}^{8} : $[\infty, 0, 1, 3, 17, 2, 18, 5, 14, 6, 9]$
C_{27}^{8} : $[\infty, 0, 1, 3, 6, 25, 10, 5, 11, 15, 7, 17, 8, 22]$
C_{35}^{8} : $[\infty, 0, 1, 3, 6, 2, 8, 30, 7, 15, 5, 10, 26, 11, 31, 4, 29, 16]$
C_{45}^{8} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 5, 34, 18, 32, 39, 26, 37, 16, 42, 8, 43, 19, 31, 14, 33]$
C_{51}^{8} : $[\infty, 0, 2, 1, 4, 8, 3, 9, 17, 10, 22, 5, 41, 20, 38, 12, 40, 31, 44, 14, 49, 18, 7, 23, 46, 36]$

C_{21}^{9} : $[\infty, 0, 1, 4, 9, 18, 12, 16, 3, 5, 17]$
C_{25}^{9} : $[\infty, 0, 1, 3, 7, 10, 21, 16, 8, 18, 11, 17, 2]$
C_{27}^{9} : $[\infty, 0, 1, 3, 6, 10, 24, 4, 12, 22, 5, 20, 15, 8]$
C_{33}^{9} : $[\infty, 0, 1, 3, 6, 10, 15, 7, 25, 12, 21, 27, 20, 8, 18, 29, 14]$
C_{39}^{9} : $[\infty, 0, 1, 3, 6, 2, 8, 17, 10, 31, 11, 23, 37, 14, 9, 34, 7, 35, 13, 5]$
C_{45}^{9} : $[\infty, 0, 1, 3, 6, 2, 8, 13, 27, 14, 31, 39, 32, 7, 16, 4, 37, 11, 21, 42, 18, 34, 19]$
C_{49}^{9} : $[\infty, 0, 23, 25, 26, 29, 33, 45, 37, 30, 41, 35, 44, 27, 32, 10, 40, 7, 39, 4, 18, 38, 19, 46, 36]$
C_{51}^{9} : $[\infty, 0, 24, 26, 27, 30, 34, 39, 46, 31, 48, 38, 32, 43, 11, 33, 19, 35, 4, 16, 45, 37, 28, 15, 42, 22]$

C_{25}^{10} : $[\infty, 0, 1, 3, 6, 2, 8, 23, 7, 21, 16, 5, 22]$
C_{33}^{10} : $[\infty, 0, 1, 3, 6, 2, 28, 11, 29, 9, 14, 21, 10, 20, 7, 15, 24]$
C_{35}^{10} : $[\infty, 0, 1, 3, 6, 2, 7, 33, 11, 31, 13, 26, 32, 25, 10, 21, 12, 22]$
C_{45}^{10} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 32, 15, 39, 9, 38, 12, 21, 40, 27, 4, 14, 30, 41, 33]$
C_{55}^{10} : $[\infty, 0, 2, 1, 4, 8, 3, 9, 16, 24, 12, 32, 22, 53, 37, 23, 40, 21, 6, 42, 20, 41, 11, 52, 7, 18, 46, 17]$

C_{33}^{11} : $[\infty, 0, 1, 3, 6, 2, 7, 15, 25, 14, 29, 10, 28, 21, 27, 4, 24]$
C_{35}^{11} : $[\infty, 0, 1, 3, 6, 2, 9, 25, 11, 33, 12, 31, 7, 15, 21, 10, 5, 30]$
C_{51}^{11} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 4, 11, 22, 9, 23, 39, 19, 37, 45, 35, 8, 41, 15, 30, 42, 21, 49, 18]$
C_{55}^{11} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 32, 49, 37, 18, 51, 25, 36, 20, 44, 12, 43, 53, 14, 50, 21, 35, 15]$

C_{27}^{12} : $[\infty, 0, 1, 3, 8, 2, 25, 18, 7, 11, 23, 6, 22, 4]$
C_{33}^{12} : $[\infty, 0, 1, 3, 6, 2, 9, 20, 10, 5, 28, 13, 31, 7, 27, 8, 14]$
C_{39}^{12} : $[\infty, 0, 1, 3, 6, 2, 7, 15, 24, 13, 28, 16, 37, 23, 29, 36, 8, 33, 11, 31]$
C_{45}^{12} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 31, 42, 17, 27, 40, 8, 16, 33, 19, 4, 32, 12, 21, 14, 37]$
C_{51}^{12} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 33, 22, 44, 24, 16, 40, 4, 23, 11, 46, 12, 30, 17, 34, 43, 14]$
C_{55}^{12} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 12, 21, 31, 53, 42, 11, 24, 5, 19, 35, 18, 44, 14, 50, 25, 10, 22, 43, 9]$

C_{49}^{13} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 35, 14, 28, 40, 9, 41, 22, 47, 39, 21, 32, 12, 34, 43, 5, 18]$
C_{55}^{13} : $[\infty, 0, 2, 1, 4, 8, 3, 9, 16, 5, 13, 39, 23, 37, 47, 18, 41, 21, 42, 6, 51, 34, 46, 22, 44, 25, 38, 53]$

C_{35}^{14} : $[\infty, 0, 1, 3, 6, 2, 9, 22, 30, 8, 33, 28, 12, 31, 7, 27, 4, 32]$
C_{39}^{14} : $[\infty, 0, 1, 3, 6, 2, 7, 14, 24, 37, 10, 31, 15, 23, 32, 17, 11, 35, 9, 27]$
C_{45}^{14} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 5, 30, 39, 18, 11, 38, 4, 34, 14, 43, 15, 41, 10, 42, 31]$
C_{49}^{14} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 12, 32, 10, 21, 11, 43, 9, 42, 15, 38, 47, 28, 41, 5, 22, 40]$

C_{33}^{15} : $[\infty, 0, 1, 3, 6, 2, 9, 27, 4, 23, 15, 21, 10, 30, 8, 13, 28]$
C_{35}^{15} : $[\infty, 0, 1, 3, 6, 2, 9, 15, 25, 13, 21, 7, 12, 33, 14, 5, 28, 10]$
C_{39}^{15} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 35, 24, 14, 37, 30, 4, 34, 9, 29, 12, 36, 27]$
C_{51}^{15} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 41, 24, 12, 47, 17, 33, 19, 48, 9, 36, 4, 46, 18, 5, 14, 40]$
C_{55}^{15} : $[\infty, 0, 2, 1, 4, 8, 3, 9, 16, 5, 13, 45, 33, 12, 53, 38, 24, 49, 14, 23, 47, 19, 42, 25, 7, 17, 37, 21]$

C_{39}^{16} : $[\infty, 0, 1, 3, 6, 2, 7, 36, 29, 11, 28, 4, 16, 27, 33, 18, 31, 15, 5, 13]$
C_{51}^{16} : $[\infty, 0, 2, 1, 4, 8, 3, 9, 16, 24, 11, 39, 18, 6, 23, 32, 13, 45, 21, 35, 19, 30, 40, 17, 37, 22]$
C_{55}^{16} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 31, 14, 37, 50, 18, 26, 16, 52, 32, 17, 42, 9, 21, 12, 38, 19, 49, 35, 51]$

C_{49}^{17} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 36, 19, 11, 41, 5, 21, 42, 14, 23, 8, 22, 33, 4, 39, 16]$
C_{51}^{17} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 33, 18, 39, 30, 44, 16, 34, 22, 42, 23, 40, 29, 21, 37, 11, 24]$

C_{39}^{18} : $[\infty, 0, 1, 3, 6, 2, 7, 24, 33, 11, 17, 32, 12, 23, 10, 34, 27, 35, 9, 37]$
C_{45}^{18} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 38, 26, 34, 10, 37, 18, 5, 14, 43, 9, 30, 41, 11, 39]$
C_{49}^{18} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 12, 40, 4, 19, 32, 41, 11, 33, 47, 22, 38, 21, 42, 5, 15, 34]$
C_{51}^{18} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 11, 44, 14, 29, 47, 23, 37, 8, 46, 24, 34, 18, 10, 41, 30, 17, 40]$

C_{45}^{19} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 42, 32, 19, 36, 16, 30, 21, 40, 12, 33, 26, 37, 5, 31, 39]$
C_{55}^{19} : $[\infty, 0, 2, 1, 4, 8, 3, 9, 16, 5, 13, 53, 18, 34, 46, 17, 37, 52, 39, 22, 48, 15, 47, 24, 6, 50, 41, 11]$

C_{45}^{20} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 4, 14, 32, 40, 19, 12, 42, 15, 39, 8, 33, 21, 5, 16, 31]$
C_{49}^{20} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 21, 28, 41, 5, 35, 12, 34, 43, 14, 47, 33, 22, 39, 18, 8, 40, 20]$
C_{51}^{20} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 33, 42, 11, 19, 30, 47, 18, 40, 16, 4, 34, 49, 12, 48, 14, 46]$
C_{55}^{20} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 12, 21, 41, 53, 37, 23, 8, 32, 43, 11, 52, 15, 46, 36, 17, 45, 24, 49, 31]$

C_{45}^{21} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 4, 17, 37, 9, 34, 19, 36, 10, 40, 8, 16, 27, 20, 43, 33]$
C_{49}^{21} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 29, 10, 21, 33, 47, 14, 35, 15, 28, 12, 43, 17, 42, 32, 40, 22]$
C_{51}^{21} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 41, 18, 30, 48, 12, 4, 19, 40, 24, 33, 46, 22, 11, 39, 9, 42]$
C_{55}^{21} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 18, 52, 38, 17, 43, 26, 50, 15, 4, 19, 41, 32, 48, 12, 35, 22, 51, 9]$

C_{55}^{22} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 12, 24, 43, 15, 49, 38, 9, 46, 25, 35, 50, 14, 5, 45, 21, 44, 31, 53, 37]$

C_{51}^{24} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 34, 49, 19, 37, 29, 40, 18, 47, 11, 42, 30, 21, 8, 41, 14, 48]$

C_{55}^{25} : $[\infty, 0, 1, 3, 6, 2, 7, 13, 20, 10, 18, 32, 50, 21, 49, 25, 44, 11, 24, 8, 53, 14, 36, 19, 39, 16, 4, 15]$

Appendix 2

Given $k < 56$ and admissible i, here we list an i-perfect $(\mathbb{Z}_k, C_k, 2)$-SDM for all values of k and i that are not covered by Theorem 4.1.9 and by Case 3 of Proposition 4.2.6. All the following SDMs are of type $\sigma := (b_0, b_1, \ldots, b_{(k-1)/2}, b_{(k-1)/2}, \ldots, b_1)$ and such that $w(\sigma) = 4$. Because of the symmetry, we only list $b_0, b_1, \ldots, b_{(k-1)/2}$ as follows.

The 5-perfect $(\mathbb{Z}_{15}, C_{15}, 2)$-SDF is: $2, -3, 6, -2, 2, -1, 1, 0$
The 6-perfect $(\mathbb{Z}_{15}, C_{15}, 2)$-SDF is: $0, 1, 3, 7, 10, 5, 13, 4$
The 6-perfect $(\mathbb{Z}_{21}, C_{21}, 2)$-SDF is: $0, 1, 3, 6, 2, 9, 18, 7, 12, 4, 19$
The 7-perfect $(\mathbb{Z}_{21}, C_{21}, 2)$-SDF is: $13, 7, 3, -4, -9, -17, -8, 2, -1, 1, 0$
The 9-perfect $(\mathbb{Z}_{21}, C_{21}, 2)$-SDF is: $10, 15, 19, 14, 17, 10, 18, 9, -1, 1, 0$
The 10-perfect $(\mathbb{Z}_{25}, C_{25}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 15, 21, 14, 24, 8, 22, 9$
The 6-perfect $(\mathbb{Z}_{33}, C_{33}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 12, 24, 9, 28, 11, 18, 29, 19, 32$
The 11-perfect $(\mathbb{Z}_{33}, C_{33}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 14, 27, 5, 20, 12, 26, 9, 21, 28$
The 12-perfect $(\mathbb{Z}_{33}, C_{33}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 19, 30, 18, 11, 31, 23, 9, 25, 15$
The 15-perfect $(\mathbb{Z}_{33}, C_{33}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 26, 11, 30, 20, 12, 28, 21, 9, 29$
The 10-perfect $(\mathbb{Z}_{35}, C_{35}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 11, 31, 23, 33, 10, 27, 8, 22, 9, 20$
The 14-perfect $(\mathbb{Z}_{35}, C_{35}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 11, 23, 34, 19, 27, 10, 29, 8, 30, 20$
The 15-perfect $(\mathbb{Z}_{35}, C_{35}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 11, 32, 16, 31, 9, 17, 5, 30, 12, 23$
The 6-perfect $(\mathbb{Z}_{39}, C_{39}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 21, 32, 18, 36, 14, 33, 17, 25, 37, 22, 35$
The 12-perfect $(\mathbb{Z}_{39}, C_{39}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 32, 17, 37, 25, 36, 20, 10, 28, 14, 31$
The 13-perfect $(\mathbb{Z}_{39}, C_{39}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 26, 14, 24, 35, 15, 37, 21, 36, 10$
The 15-perfect $(\mathbb{Z}_{39}, C_{39}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 31, 18, 35, 21, 36, 8, 28, 5, 26, 16$
The 18-perfect $(\mathbb{Z}_{39}, C_{39}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 9, 30, 14, 27, 8, 20, 34, 12, 36, 25$
The 6-perfect $(\mathbb{Z}_{51}, C_{51}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 21, 9, 17, 30, 8, 22, 43, 27, 44, 25, 45, 20, 31, 46, 23, 5, 29$
The 12-perfect $(\mathbb{Z}_{51}, C_{51}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 24, 39, 10, 31, 48, 35, 16, 36, 9, 21, 49, 23$
The 15-perfect $(\mathbb{Z}_{51}, C_{51}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 27, 47, 30, 17, 45, 18, 39, 24, 12, 41, 16, 32$
The 17-perfect $(\mathbb{Z}_{51}, C_{51}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 20, 36, 23, 47, 16, 41, 9, 32, 17, 38, 21, 50$
The 18-perfect $(\mathbb{Z}_{51}, C_{51}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 32, 45, 28, 48, 9, 30, 49, 34, 50, 24, 46, 18$
The 21-perfect $(\mathbb{Z}_{51}, C_{51}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 27, 42, 25, 45, 22, 35, 14, 40, 16, 28, 12, 41$
The 24-perfect $(\mathbb{Z}_{51}, C_{51}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 25, 44, 16, 45, 10, 34, 47, 27, 39, 14, 35, 50$
The 10-perfect $(\mathbb{Z}_{55}, C_{55}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 9, 21, 8, 38, 53, 20, 43, 12, 48, 22, 49, 31, 51, 17, 33$
The 11-perfect $(\mathbb{Z}_{55}, C_{55}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 10, 23, 38, 8, 39, 22, 44, 16, 28, 46, 17, 51, 31, 50, 18$
The 15-perfect $(\mathbb{Z}_{55}, C_{55}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 20, 37, 52, 24, 46, 27, 40, 16, 32, 12, 35, 14, 44, 18$
The 20-perfect $(\mathbb{Z}_{55}, C_{55}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 9, 21, 34, 54, 29, 47, 32, 53, 22, 51, 12, 40, 17, 39, 20$
The 22-perfect $(\mathbb{Z}_{55}, C_{55}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 20, 37, 10, 39, 52, 22, 38, 18, 51, 32, 9, 24, 45, 14$

The 25-perfect $(\mathbb{Z}_{55}, C_{55}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 20, 35, 18, 43, 14, 30, 49, 16, 37, 10, 52, 28, 48, 25$
The 2-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 8, 15, 25, 7, 18, 23, 9, 17, 5$
The 4-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 5, 16, 25, 10, 24, 4, 14$
The 6-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 5, 21, 4, 22, 10, 23, 16$
The 7-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $-9, -1, 6, -5, -14, -4, -16, -3, 3, -2, 2, -1, 1, 0$
The 8-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 4, 11, 24, 5, 20, 9, 19$
The 9-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $-20, -10, -3, -19, -11, -5, 4, 16, 3, -2, 2, -1, 1, 0$
The 10-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 13, 23, 9, 16, 24, 15, 26, 11$
The 11-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 16, 24, 12, 5, 15, 4, 17, 23$
The 12-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 16, 8, 18, 4, 25, 5, 20, 9$
The 13-perfect $(\mathbb{Z}_{27}, C_{27}, 2)$-SDF is: $0, 1, 3, 6, 2, 7, 14, 23, 9, 15, 5, 13, 24, 12$
The 2-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 8, 13, 4, 19, 11, 33, 44, 20, 27, 43, 18, 28, 42, 10, 22, 39, 12, 31$
The 4-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 5, 14, 4, 17, 24, 35, 11, 37, 10, 27, 43, 28, 40, 9, 32, 12$
The 6-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 21, 9, 17, 31, 15, 28, 5, 30, 12, 29, 40, 14, 38, 8$
The 8-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 27, 38, 20, 44, 28, 41, 21, 36, 8, 34, 12$
The 10-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 32, 10, 40, 16, 34, 23, 43, 31, 44, 25, 9$
The 11-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 35, 20, 32, 9, 25, 38, 17, 44, 18, 29, 12$
The 12-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 33, 8, 30, 14, 25, 42, 9, 24, 37, 18, 39$
The 13-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 42, 27, 8, 30, 18, 38, 20, 41, 9, 37$
The 14-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 37, 18, 31, 20, 44, 26, 41, 8, 28, 12, 29$
The 15-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 32, 43, 31, 44, 17, 40, 10, 35, 16, 37, 21$
The 16-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 17, 30, 10, 26, 15, 43, 25, 35, 12, 38, 8, 29$
The 17-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 9, 21, 36, 12, 25, 41, 16, 35, 8, 30$
The 18-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 44, 29, 17, 41, 16, 42, 24, 37, 20, 31, 9$
The 19-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 31, 10, 40, 17, 29, 9, 27, 38, 21, 8, 34$
The 20-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 28, 10, 22, 38, 17, 40, 29, 14, 42, 23, 43$
The 21-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 32, 12, 24, 40, 16, 43, 28, 41, 30, 8, 34$
The 22-perfect $(\mathbb{Z}_{45}, C_{45}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 41, 30, 12, 44, 21, 37, 25, 8, 38, 17, 42$
The 2-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 8, 13, 4, 19, 11, 27, 37, 5, 25, 36, 10, 46, 24, 17, 45, 26, 12, 43, 31, 7$
The 4-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 5, 14, 4, 17, 24, 35, 11, 25, 46, 12, 43, 10, 33, 45, 18, 48, 19, 36$
The 6-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 21, 9, 17, 30, 8, 29, 40, 14, 28, 44, 20, 38, 19, 39, 5, 22$
The 8-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 14, 32, 12, 25, 41, 9, 28, 43, 20, 48, 24, 46$
The 10-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 9, 32, 8, 38, 10, 47, 29, 14, 27, 43, 16, 36$
The 11-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 10, 29, 14, 43, 30, 18, 40, 9, 33, 16, 44, 21$
The 12-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 9, 42, 23, 44, 18, 38, 20, 33, 48, 24, 36, 14$
The 13-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 36, 9, 25, 40, 28, 47, 27, 14, 46, 21, 44$
The 14-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 35, 16, 48, 33, 46, 17, 45, 29, 41, 18, 43$
The 15-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 24, 37, 9, 21, 36, 16, 39, 17, 42, 12, 29$
The 16-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 16, 26, 10, 42, 23, 35, 14, 29, 9, 22, 45, 18, 36, 12$
The 17-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 14, 35, 48, 28, 43, 17, 39, 9, 41, 16, 34, 18$

The 18-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 42, 14, 33, 48, 17, 41, 24, 47, 25, 12, 32, 44$
The 19-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 10, 46, 31, 48, 18, 44, 16, 41, 14, 43, 25, 37$
The 20-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 42, 14, 34, 21, 43, 28, 10, 35, 9, 46, 16, 33$
The 21-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 39, 27, 43, 21, 42, 8, 34, 17, 36, 12, 32, 14$
The 22-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 8, 45, 28, 12, 34, 9, 24, 47, 17, 30, 10, 38$
The 23-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:
$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 9, 40, 17, 41, 29, 8, 24, 37, 22, 42, 23, 45$
The 24-perfect $(\mathbb{Z}_{49}, C_{49}, 2)$-SDF is:

$0, 1, 3, 6, 2, 7, 13, 4, 11, 19, 5, 15, 26, 43, 16, 28, 9, 38, 10, 44, 31, 47, 22, 45, 14$

Appendix 3

Here we write the cyclotomic systems and the code we used to find a 2-$(13p, 13, 1)$ design, for all primes $p \equiv 1 \pmod{12}$ such that $p \in [2 \cdot 10^4, 10^{10}]$. For values smaller than $2 \cdot 10^4$ this code obtain some failures but, if we change the cyclotomic systems, we can cover also this range up to the possible exceptions of Proposition 5.3.1.

We denote by g a generator of $\mathbb{F}_p$ and by $\xi := g^{\frac{p-1}{4}}$. We start with the case in which $\xi - 1 \in C_0^3$. In this case we considered the following cyclotomic systems and we used the following code:

$$\mathfrak{C}^1 := \begin{cases} x_1 \in C_1^3; \\ x_1 - 1 \in C_1^3; \\ x_1 + 1 \in C_2^3; \\ x_1 - \xi \in C_0^3; \\ x_1 + \xi \in C_1^3; \end{cases}$$

$$\mathfrak{C}^2 := \begin{cases} x_2 \in C_2^3; \\ x_1 - x_2 \in C_1^3; \\ x_1 + x_2 \in C_2^3; \\ x_2 - 1 \in C_0^3; \\ x_2 + 1 \in C_2^3; \\ \xi + x_2 \in C_0^3; \\ \xi - x_2 \in C_1^3; \\ \xi x_2 + x_1 \in C_0^3; \\ \xi x_2 - x_1 \in C_2^3. \end{cases}$$

```
p:=20000;
while p<10000000000 do
if IsInt((p-1)/12) and  IsPrime(p) then
i:=0;
indice:=0;
g:=Z(p);
c0:=g^0;
c1:=g^((p-1)/3);
c2:=g^(2*(p-1)/3);
e:=((p-1)/3);
xi:=g^((p-1)/4);
if (xi-1)^e=c0 then
        while (indice=0) and (i<p) do
                x1:=g^i;
                if (x1)^e=c1
                and (x1-1)^e=c1
                and (x1+1)^e=c2
                and (x1-xi)^e=c0
                and (x1+xi)^e=c1 then
                        j:=0;
                        while (indice=0) and (j<p) do
                                x2:=g^j;
                                if (x2)^e=c2
                                and (x1-x2)^e=c1
                                and (x2+x1)^e=c2
                                and (x2-g^0)^e=c0
                                and (x2+g^0)^e=c2
                                and (xi+x2)^e=c0
                                and (xi-x2)^e=c1
                                and (xi*x2+x1)^e=c0
                                and (xi*x2-x1)^e=c2 then
                                        indice:=1;
                                else
                                j:=j+1;
                                fi;
                        od;
                if (j=p) then
                i:=i+1;
                fi;
                else
                i:=i+1;
                fi;
        od;
fi;
```

Here we write the cyclotomic systems and the code we used to find a 2-$(13p, 13, 1)$ design, for all primes $p \equiv 1 \pmod{12}$ such that, if we denote by g a generator of $\mathbb{F}_p$ and by $\xi := g^{\frac{p-1}{4}}$, we have $\xi - 1 \in C_1^3$ and $p \in [2 \cdot 10^4, 10^{10}]$.

$$\mathfrak{C}^1 := \begin{cases} x_1 \in C_1^3; \\ x_1 - 1 \in C_0^3; \\ x_1 + 1 \in C_2^3; \\ x_1 - \xi \in C_0^3; \\ x_1 + \xi \in C_1^3; \end{cases} \qquad \mathfrak{C}^2 := \begin{cases} x_2 \in C_2^3; \\ x_1 - x_2 \in C_1^3; \\ x_1 + x_2 \in C_2^3; \\ x_2 - 1 \in C_0^3; \\ x_2 + 1 \in C_2^3; \\ \xi + x_2 \in C_2^3; \\ \xi - x_2 \in C_1^3; \\ \xi x_2 + x_1 \in C_0^3; \\ \xi x_2 - x_1 \in C_1^3. \end{cases}$$

```
if (xi-1)^e=c1 then
        while (indice=0) and (i<p) do
                x1:=g^i;
                if (x1)^e=c1
                and (x1-1)^e=c0
                and (x1+1)^e=c2
                and (x1-xi)^e=c0
                and (x1+xi)^e=c1 then
                        j:=0;

                        while (indice=0) and (j<p) do
                                x2:=g^j;
                                if (x2)^e=c2
                                and (x1-x2)^e=c1
                                and (x2+x1)^e=c2
                                and (x2-g^0)^e=c0
                                and (x2+g^0)^e=c2
                                and (xi+x2)^e=c2
                                and (xi-x2)^e=c1
                                and (xi*x2+x1)^e=c0
                                and (xi*x2-x1)^e=c1 then
                                        indice:=1;
                                else
                                j:=j+1;
                                fi;
                        od;
                if (j=p) then
                i:=i+1;
                fi;

                else
                i:=i+1;
                fi;
        od;
fi;
```

Finally, here we write the cyclotomic systems and the code we used to find a 2-$(13p, 13, 1)$ design, for all primes $p \equiv 1 \pmod{12}$ such that, if we denote by g a generator of $\mathbb{F}_p$ and by $\xi := g^{\frac{p-1}{4}}$, we have $\xi - 1 \in C_2^3$ and $p \in [2 \cdot 10^4, 10^{10}]$.

$$\mathfrak{C}^1 := \begin{cases} x_1 \in C_1^3; \\ x_1 - 1 \in C_1^3; \\ x_1 + 1 \in C_0^3; \\ x_1 - \xi \in C_0^3; \\ x_1 + \xi \in C_1^3; \end{cases} \qquad \mathfrak{C}^2 := \begin{cases} x_2 \in C_2^3; \\ x_1 - x_2 \in C_1^3; \\ x_1 + x_2 \in C_2^3; \\ x_2 - 1 \in C_0^3; \\ x_2 + 1 \in C_2^3; \\ \xi + x_2 \in C_2^3; \\ \xi - x_2 \in C_0^3; \\ \xi x_2 + x_1 \in C_2^3; \\ \xi x_2 - x_1 \in C_1^3. \end{cases}$$

```
if (xi-1)^e=c2 then
        while (indice=0) and (i<p) do
                x1:=g^i;
                if (x1)^e=c1
                and (x1-1)^e=c1
                and (x1+1)^e=c0
                and (x1-xi)^e=c0
                and (x1+xi)^e=c1 then
                        j:=0;

                        while (indice=0) and (j<p) do
                                x2:=g^j;
                                if (x2)^e=c2
                                and (x1-x2)^e=c1
                                and (x2+x1)^e=c2
                                and (x2-g^0)^e=c0
                                and (x2+g^0)^e=c2
                                and (xi+x2)^e=c2
                                and (xi-x2)^e=c0
                                and (xi*x2+x1)^e=c2
                                and (xi*x2-x1)^e=c1 then
                                        indice:=1;
                                else
                                j:=j+1;
                                fi;
                        od;
                if (j=p) then
                i:=i+1;
                fi;

                else
                i:=i+1;
                fi;
        od;
fi;
if(i=p) then
Print(p," ");
fi;
fi;
p:=p+1;
od;
```