



Subset sums and block designs in a finite vector space

Marco Pavone¹

Received: 29 September 2022 / Revised: 31 January 2023 / Accepted: 5 March 2023 /

Published online: 19 April 2023

© The Author(s) 2023

Abstract

In this paper we settle the question of whether a finite-dimensional vector space $\mathcal{V}$ over $\mathbb{F}_p$, with p an odd prime, and the family of all the k -sets of elements of $\mathcal{V}$ summing up to a given element x , form a 1 -(v, k, λ_1) or a 2 -(v, k, λ_2) block design, and, in either case, we find a closed form for λ_i and characterize the automorphism group. The question is discussed also in the case where the elements of the k -sets are required to be all nonzero, as the two cases happen to be intrinsically inseparable. The “twin case” $p = 2$, which has strict connections with coding theory, was completely discussed in a recent paper by G. Falcone and the present author.

Keywords Block design · Additive design · Finite vector space · Subset sums · Permutations of subset sums · Automorphism group

Mathematics Subject Classification Primary 05B05 · 05B25 · 51E05 · 11B75 · Secondary 11P70 · 11B13 · 05A05 · 05A18

1 Introduction

We recall that a (simple) t -(v, k, λ_t) *block design* is a pair $\mathcal{D} = (\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a finite set with v elements, called *points*, and $\mathcal{B}$ is a family of (mutually distinct) subsets of $\mathcal{V}$, called *blocks*, such that each block contains exactly k points and any t -subset of $\mathcal{V}$ is contained in exactly λ_t blocks (see [2, 8] for a general reference on block designs). Also, for $t = 1$, it is customary to denote λ_1 by r and call it the *replication number* of $\mathcal{D}$, whereas, for $t = 2$, the parameter λ_2 is usually denoted simply by λ . A 1-design is also known as a *tactical configuration*. By standard double-counting arguments, one finds that the number b of blocks in a 1 -(v, k, r) design is equal to vr/k , and that a 2 -(v, k, λ) design is a 1 -(v, k, r) design as well, with $r(k - 1) = \lambda(v - 1)$. An *automorphism* of $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ is an invertible map $\varphi : \mathcal{V} \rightarrow \mathcal{V}$ that preserves blocks, that is, with the property that, for any k -subset b of

Communicated by T. Feng.

✉ Marco Pavone
marco.pavone@unipa.it

¹ Dipartimento di Ingegneria, Università degli Studi di Palermo, Palermo 90128, Italy

$\mathcal{V}$, $\varphi(b) \in \mathcal{B}$ if and only if $b \in \mathcal{B}$. The group of all the automorphisms of $\mathcal{D}$ is denoted by $\text{Aut}(\mathcal{D})$.

A classic example of a 2-design is the *point-flat design* of the affine geometry $\text{AG}(d, p)$ over the Galois field $\mathbb{F}_p$, where the point-set $\mathcal{V}$ is the additive group of the d -dimensional vector space $\mathbb{F}_p^d$, and the blocks are the affine subspaces of a fixed dimension n . For such a design, each block has $k = p^n$ elements and has the property, for $k > 2$, that the sum of its points is zero. Moreover, as soon as $k > 4$, the family $\mathcal{B}$ of blocks of the point-flat design is strictly contained in the family of all the k -subsets of $\mathcal{V}$ whose elements sum up to zero. Another classic example is the point-flat design of the projective geometry $\text{PG}(d, 2)$ over $\mathbb{F}_2$, where the point-set $\mathcal{V}$ is the set of all nonzero elements of the additive group of the vector space $\mathbb{F}_2^{d+1}$, and the blocks are the projective subspaces of a fixed dimension; again, the blocks have the property that the sum of their points is zero.

This motivates the two following, and somewhat complementary, questions. On the one hand, it is natural to ask what 2 -(v, k, λ) designs $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ are *additive*, that is, can be embedded in a commutative group $(G, +)$ in such a way that the sum of the k elements in each block is zero [6, Proposition 2.7]. This algebraic representation of $\mathcal{D}$ is even more significant in the case where, for a suitable G , the blocks in $\mathcal{B}$ are the only k -subsets of $\mathcal{V}$ whose elements sum up to zero in G (in this case, $\mathcal{D}$ is said to be *strongly additive* [16], and, for a suitable G , $\text{Aut}(\mathcal{D})$ is the stabilizer of $\mathcal{V}$ in $\text{Aut}(G)$).

On the other hand, one may ask under what conditions the family $\mathcal{B}_k$ of all the zero-sum k -sets of elements in a finite-dimensional vector space $\mathcal{V}$ over $\mathbb{F}_p$ determines a (necessarily strongly additive) 2 -(v, k, λ) design, and, in this case, whether there exists a closed form for λ and whether one can determine the automorphism group. The same can be asked also for the family $\mathcal{B}_k^*$ of all the zero-sum k -sets of elements in $\mathcal{V}^* = \mathcal{V} \setminus \{0\}$. More generally, the problem can be addressed also in the case where $\mathcal{V}$ is an arbitrary finite (abelian) group.

Note that the families $\mathcal{B}_k$ and $\mathcal{B}_k^*$ appear also in the context of additive combinatorics and additive number theory, in connection with the *subset sum problem* over finite fields [12] and over finite abelian groups [13], which arises from a number of relevant applications in combinatorics, coding theory, and graph theory.

The first question is answered in the affirmative for symmetric 2-designs [6], affine resolvable 2-designs [7] (with few trivial exceptions), geometric Steiner triple systems [6], and Boolean Steiner quadruple systems [10, 14]. In addition, all these designs are also strongly additive. Moreover, some infinite classes of new additive Steiner 2-designs are constructed in [3] by means of difference methods of various kinds, and other new additive 2-designs have been presented in [4].

The second question is completely answered in [10] (for $p = 2$) and in the present paper (for an arbitrary odd prime p). The two papers are strictly related, and constitute the latter piece of a larger ongoing project on additive designs. In the more general case where $\mathcal{V}$ is an arbitrary finite abelian group, the question is still open as to whether $(\mathcal{V}, \mathcal{B}_k)$ is a 2-design only if $\mathcal{V}$ is an elementary abelian group.

The binary case $p = 2$, with $\mathcal{V} = \mathbb{F}_2^d$, shows a specific and distinguished behaviour for its connections with coding theory, as the blocks in $\mathcal{B}_k^*$ (resp., in $\mathcal{B}_k$) can be seen as codewords of weight k in the *binary Hamming code* of length $2^d - 1$ (resp., in the extended binary Hamming code of length 2^d). In [10], where the problem is treated from the point of view of combinatorial design theory, we give alternative and purely combinatorial proofs that, for k even, $\mathcal{D}_k = (\mathcal{V}, \mathcal{B}_k)$ is a 3 -($2^d, k, \lambda_3$) design (see also [1, Theorem 3]), and that, for any integer k , with $3 \leq k \leq 2^d - 4$, $\mathcal{D}_k^* = (\mathcal{V}^*, \mathcal{B}_k^*)$ is a 2 -($2^d - 1, k, \lambda$) design (see also [9, Theorem 5.7]). Also, we compute the parameters λ_3 and λ explicitly, and show that the group

of automorphisms of $\mathcal{D}_k$ (resp., $\mathcal{D}_k^*$) is (isomorphic to) the group of invertible affine (resp., linear) mappings on $\mathcal{V}$ over $\mathbb{F}_2$.

In this paper we consider the case where p is an odd prime and, more generally, we consider the family $\mathcal{B}_k^x$ (resp., $\mathcal{B}_k^{x,*}$) of all the k -subsets of $\mathcal{V} = \mathbb{F}_p^d$ (resp., $\mathcal{V}^*$) whose elements sum up to a given element x in $\mathcal{V}$. We investigate under what conditions, for $x \in \mathcal{V}$ and $k \in \{1, \dots, p^d\}$, the incidence structure $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is either a block 2-design or a block 1-design, and under what conditions, for $x \in \mathcal{V}$ and $k \in \{1, \dots, p^d - 1\}$, the incidence structure $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is a block 1-design. In either case, we explicitly determine the fundamental parameters of the design, and characterize the automorphism group.

First of all, we show that, for any x in $\mathcal{V}$, the incidence structure $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a $1-(p^d, k, r)$ design if and only if p divides k . Moreover, if this is the case, then $r = |\mathcal{B}_{k-1}^{x,*}|$ and, as x ranges over $\mathcal{V}^*$, the $1-(p^d, k, |\mathcal{B}_{k-1}^{x,*}|)$ designs $(\mathcal{V}, \mathcal{B}_k^x)$ are all mutually isomorphic, and not isomorphic to the $1-(p^d, k, |\mathcal{B}_{k-1}^{0,*}|)$ design $(\mathcal{V}, \mathcal{B}_k^0)$ (see Theorem 3.1). Also, for $p \leq k < p^d$, $d \geq 2$, and $x \in \mathcal{V}$, the group of automorphisms of the 1-design $(\mathcal{V}, \mathcal{B}_k^x)$ is the group of all the invertible affine maps on $\mathcal{V}$ of the form $\varphi(z) = L(z) + b$, where b is in $\mathcal{V}$ and L is an invertible linear map on $\mathcal{V}$ over $\mathbb{F}_p$ fixing x (with the only exception $p^d = 9$, in the case where $x \neq 0$).

As the main result of the paper, we prove that $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a $2-(p^d, k, \lambda)$ design (where, necessarily, $\lambda = |\mathcal{B}_{k-1}^{x,*}|(k-1)/(p^d-1)$) if and only if $(p$ divides k and $x = 0$). Also, if this is the case, then the group of automorphisms of $\mathcal{D}$ is the group of invertible affine mappings of the d -dimensional affine space $\mathcal{V}$ over $\mathbb{F}_p$ (see Theorem 3.6). The latter result can be somehow interpreted as analogous to the fundamental theorem of affine geometry, which yields that a collineation over $\mathbb{F}_p$ is an invertible affine mapping, the analogy being strict in the special case where $p^d = 9$ and $k = 3$, that is, for the affine plane $\text{AG}(2, 3)$ (see also Example 3.10.1). Moreover, for $d \geq 2$, the 2-design $(\mathcal{V}, \mathcal{B}_p)$ is not a 3-design (see Proposition 3.9).

Finally, we prove that the incidence structure $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is a $1-(p^d - 1, k, r^*)$ design (where, necessarily, $r^* = |\mathcal{B}_k^{x,*}|k/(p^d - 1)$) if and only if $x = 0$ and $k \notin \{1, p^d - 2\}$. Moreover, in this case, the group of automorphisms of $\mathcal{D}^*$ is the group of invertible linear mappings on $\mathcal{V}$ over $\mathbb{F}_p$ (see Theorem 3.4). Also, for $d \geq 2$, the 1-design $(\mathcal{V}^*, \mathcal{B}_p^*)$ is not a 2-design (see Proposition 3.9).

It is worth mentioning that, if p is an odd prime and $\mathcal{C}$ is the p -ary Hamming code of length $(p^d - 1)/(p - 1)$, then there exists a one-to-one correspondence between the k -sets in $\mathcal{B}_k^*$ and the codewords of weight k in $\mathcal{C}$ if and only if $p \in \{3, 5\}$ and $k = 3$. It would be interesting to know whether some connection between the block-design approach and the coding-theory point of view can be found also in the general case.

2 Preliminaries

Throughout the paper we will denote by p an odd prime and by $\mathcal{V}$ a d -dimensional vector space, $d \geq 1$, over a field with p elements. Also, let $\mathcal{V}^* = \mathcal{V} \setminus \{0\}$.

In this section we give closed forms for all the coefficients introduced in the following Definition 2.1, which turn out to be all nonzero, except in the trivial cases described in [11, Theorem 2.2]. These coefficients are related, and in some cases equal, to the parameters of the block designs considered in Sect. 3.

Definition 2.1 For any integer $1 \leq k \leq p^d$ (resp., $1 \leq k \leq p^d - 1$), and for any $x \in \mathcal{V}$, we denote by $\mathcal{B}_k^x$ (resp., $\mathcal{B}_k^{x,*}$) the family of all the k -sets of elements of $\mathcal{V}$ (resp., of $\mathcal{V}^*$) whose sum is x , and we let $b_k^x = |\mathcal{B}_k^x|$ (resp., $b_k^{x,*} = |\mathcal{B}_k^{x,*}|$). Also, we define $b_0^{x,*} = 1 - b_1^{x,*}$ for all $x \in \mathcal{V}$.

Moreover, for any $y \in \mathcal{V}$ (resp., in $\mathcal{V}^*$) and any $x \in \mathcal{V}$, we denote by $r_k^x(y)$ (resp., $r_k^{x,*}(y)$) the number of the k -sets in $\mathcal{B}_k^x$ (resp., $\mathcal{B}_k^{x,*}$) containing y .

Finally, whenever $x = 0$, the superscript x will always be omitted, for short (e.g., $b_k^{0,*}$ will be abbreviated as b_k^*).

We first give closed forms for the numbers b_k^x and $b_k^{x,*}$ introduced in Definition 2.1. An alternative, simpler proof than the original proof in [12, Theorem 1.2] can be found in [15, Theorem 1.1].

Proposition 2.2 ([12, Theorem 1.2]) *Let p be an odd prime. If $1 \leq k \leq p^d$, and if p does not divide k , then, for any $x \in \mathcal{V}$,*

$$b_k^x = b_k = \frac{1}{p^d} \binom{p^d}{k}, \quad (1)$$

whereas, if p divides k , then

$$b_k = \frac{1}{p^d} \binom{p^d}{k} + \frac{p^d - 1}{p^d} \binom{p^d - 1}{k/p}, \quad (2)$$

and, for any $x \in \mathcal{V}^*$,

$$b_k^x = \frac{1}{p^d} \binom{p^d}{k} - \frac{1}{p^d} \binom{p^d - 1}{k/p}. \quad (3)$$

Furthermore, for any $0 \leq k \leq p^d - 1$,

$$b_k^* = \frac{1}{p^d} \binom{p^d - 1}{k} + (-1)^{k+[k/p]} \frac{p^d - 1}{p^d} \binom{p^d - 1}{[k/p]}, \quad (4)$$

and, for any $x \in \mathcal{V}^*$,

$$b_k^{x,*} = \frac{1}{p^d} \binom{p^d - 1}{k} - (-1)^{k+[k/p]} \frac{1}{p^d} \binom{p^d - 1}{[k/p]}. \quad (5)$$

We now give closed forms for the numbers $r_k^x(y)$ and $r_k^{x,*}(y)$ introduced in Definition 2.1. In spite of the simple argument used for $r_k^x(y)$, the case of $r_k^{x,*}(y)$ turns out to be intrinsically more complicated.

Proposition 2.3 ([11, Theorem 2.5]) *Let p be an odd prime, and let $1 \leq k \leq p^d$. If x and y are in $\mathcal{V}$, then*

$$r_k^x(y) = b_{k-1}^{x-ky,*}.$$

In particular, if p divides k , then $r_k^x(y) = b_{k-1}^{x,}$ is independent of y .*

Remark 2.4 If p does not divide k , then, in the case where $x = 0$ and $y \neq 0$ (respectively, $x \neq 0$ and $y = \frac{1}{k}x$), the formula in Proposition 2.3 reduces to $r_k(y) = b_{k-1}^{-ky,*}$ (respectively, to $r_k^x(y) = b_{k-1}^*$). Note that, in this case, the left-hand side of the formula involves k -subsets

of $\mathcal{V}$ whose elements sum up to zero (respectively, to a nonzero element), whereas the right-hand side involves $(k-1)$ -subsets of $\mathcal{V}^*$ whose elements sum up to some nonzero element (respectively, to zero). This confirms that the theory of zero sums in a finite vector space $\mathcal{V}$ involves necessarily, as the other side of the same coin, the investigation of the families of k -subsets of both $\mathcal{V}$ and $\mathcal{V}^*$ whose elements sum up to zero or to a nonzero element. This connection will become even more intimate and evident in the next section of the paper.

As for the numbers $r_k^{x,*}(y)$, a formula can be found in [12], although in an implicit form. Indeed, if $\mathcal{V}$ is endowed with the structure of a Galois field with p^d elements, and 1 is the identity of the multiplicative group $\mathcal{V}^*$, then, for any y in $\mathcal{V}^*$,

$$r_k^{x,*}(y) = r_k^{xy^{-1},*}(1) = N(k-1, xy^{-1} - 1, \mathcal{V} \setminus \{0, 1\}),$$

where the right-most term N is the number, computed in (almost) closed form in [12, Theorem 1.3], of all the $(k-1)$ -subsets of $\mathcal{V} \setminus \{0, 1\}$ whose elements add up to $xy^{-1} - 1$. Alternatively, we give now an explicit formula for the numbers $r_k^{x,*}(y)$. The proof, somehow lengthy and “technical”, will be given in the final Appendix of the paper.

Proposition 2.5 *Let p be an odd prime, let $1 \leq k \leq p^d - 1$ and $M = \lfloor (k-1)/p \rfloor$, and let*

$$S_k^* = \begin{cases} \frac{1}{p^d} \binom{p^d - 2}{k-1} + (-1)^k \frac{k}{p^d} & \text{if } M = 0 \\ \frac{1}{p^d} \binom{p^d - 2}{k-1} + \frac{(-1)^{k+M}}{p^d} \left((k-Mp) \binom{p^{d-1} - 1}{M} - p \binom{p^{d-1} - 2}{M-1} \right) & \text{if } M \geq 1. \end{cases} \quad (6)$$

Let x be in $\mathcal{V}$, and let y be in $\mathcal{V}^$.*

(1) *If $x - iy \neq 0$ for all $i = 1, \dots, k$, then*

$$r_k^{x,*}(y) = S_k^*.$$

(2) *If $x - iy = 0$ for some index $1 \leq i \leq k$, then one of the two following cases occurs.*

(a) *If $d = 1$, then*

$$r_k^{x,*}(y) = S_k^* + (-1)^{k-1}.$$

(b) *If $d \geq 2$, then let h be the unique index in $\{1, \dots, p\}$ such that $x - hy = 0$, and let*

$$m_h = \lfloor (k-h)/p \rfloor.$$

In this case,

$$r_k^{x,*}(y) = \begin{cases} S_k^* + (-1)^{k+m_h-1} \binom{p^{d-1} - 2}{m_h} & \text{if } 0 \leq m_h \leq p^{d-1} - 2 \\ S_k^* & \text{if } m_h = p^{d-1} - 1. \end{cases} \quad (7)$$

We conclude this section by presenting a result on permutations of $\mathcal{V}$, which is interesting in its own right and which was not included in [11], where it was proposed as an open problem in Remark 3.6. This result will be applied in Sect. 3, to characterize the automorphisms of some of the 1-designs considered in Theorem 3.1. The proof will be given in the final Appendix of the paper.

Theorem 2.6 Let p be an odd prime, and let $d \geq 2$, with the only exception $p^d = 9$. Let k be a multiple of p , with $p \leq k < p^d$, and let x be a point in $\mathcal{V}^* = \mathcal{V} \setminus \{0\}$. A permutation φ of $\mathcal{V}$ induces a permutation of $\mathcal{B}_k^x$ (that is, $\varphi(x_1) + \cdots + \varphi(x_k) = x$ whenever $\{x_1, \dots, x_k\}$ is in $\mathcal{B}_k^x$) if and only if φ is an invertible affine map on $\mathcal{V}$ over $\mathbb{F}_p$ of the form

$$\varphi(y) = L(y) + b,$$

for some b in $\mathcal{V}$ and some invertible linear map L on $\mathcal{V}$ over $\mathbb{F}_p$, with $L(x) = x$.

3 The main results

We begin by studying under what conditions either $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ or $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ happens to be a 1-design. If this is the case, then its number of blocks and its replication number will both be found among the numbers b_k^x and $b_k^{x,*}$ introduced in Definition 2.1, with the one exception of the parameter $r^* = b_k^* \frac{k}{p^d-1}$ in Theorem 3.4. Moreover, for $x = 0$, such designs are trivially additive, thus providing new examples of additive designs not considered in [6, 7, 10].

In order to avoid trivialities, in the following theorem the case $k = p^d$ is disregarded. For such a value of k , $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a 1-design if and only if $x = 0$, in which case it is the trivial $1-(p^d, p^d, 1)$ design.

Theorem 3.1 Let p be an odd prime, let $d \geq 1$, and let x be in $\mathcal{V} = \mathbb{F}_p^d$. For $1 \leq k < p^d$, $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a $1-(p^d, k, r)$ design if and only if p divides k . If this is the case, then

$$r = b_{k-1}^{x,*} = \begin{cases} \frac{1}{p^d} \binom{p^d-1}{k-1} + (-1)^{k-1+\lfloor (k-1)/p \rfloor} \frac{p^d-1}{p^d} \binom{p^{d-1}-1}{\lfloor (k-1)/p \rfloor} & \text{if } x = 0 \\ \frac{1}{p^d} \binom{p^d-1}{k-1} - (-1)^{k-1+\lfloor (k-1)/p \rfloor} \frac{1}{p^d} \binom{p^{d-1}-1}{\lfloor (k-1)/p \rfloor} & \text{if } x \neq 0. \end{cases}$$

Moreover, as x ranges over $\mathcal{V}^*$, the $1-(p^d, k, b_{k-1}^{x,*})$ designs $(\mathcal{V}, \mathcal{B}_k^x)$ are all mutually isomorphic, and not isomorphic to the $1-(p^d, k, b_{k-1}^*)$ design $(\mathcal{V}, \mathcal{B}_k)$.

Finally, let $d \geq 2$, and let p divide k , with $p \leq k < p^d$. Then the group of automorphisms of the 1-design $(\mathcal{V}, \mathcal{B}_k)$ is the group of all the invertible affine maps on the affine space $\mathcal{V}$ over $\mathbb{F}_p$. Moreover, if $p^d > 9$ and $x \in \mathcal{V}^*$, then the group of automorphisms of the 1-design $(\mathcal{V}, \mathcal{B}_k^x)$ is the group of all the invertible affine maps on $\mathcal{V}$ of the form $\varphi(z) = L(z) + b$, where b is in $\mathcal{V}$ and L is an invertible linear map on $\mathcal{V}$ over $\mathbb{F}_p$ fixing x .

Proof Let $1 \leq k < p^d$. By Proposition 2.3, for any y in $\mathcal{V}$ the number $r_k^x(y)$ of k -sets in $\mathcal{B}_k^x$ containing y is $b_{k-1}^{x-ky,*}$. If p divides k , then $ky = 0$ and $r_k^x(y)$ is independent of y , hence $(\mathcal{V}, \mathcal{B}_k^x)$ is a $1-(p^d, k, r)$ design with $r = b_{k-1}^{x,*}$, whose value is given in (4) and (5) in Proposition 2.2, and which is not zero by [11, Theorem 2.2(iv)], since k is a multiple of p and $k \neq p^d$. Alternatively, in the case where p divides k , the fact that $(\mathcal{V}, \mathcal{B}_k^x)$ is a 1-design can also be proved by noting that, for all $y_1, y_2 \in \mathcal{V}$, the map $v \mapsto v + y_2 - y_1$, $v \in \mathcal{V}$, induces a one-to-one correspondence between the k -sets in $\mathcal{B}_k^x$ containing y_1 and the k -sets in $\mathcal{B}_k^x$ containing y_2 .

If p does not divide k , then $r_k^x(\frac{1}{k}x) = b_{k-1}^*$, whereas, if $y \in \mathcal{V} \setminus \{\frac{1}{k}x\}$, then $x - ky \neq 0$ and $r_k^x(y) = b_{k-1}^{x-ky,*} \neq b_{k-1}^*$, by (4) and (5) in Proposition 2.2. Therefore $(\mathcal{V}, \mathcal{B}_k^x)$ is not a 1-design.

Moreover, if p divides k , then, given x_1 and x_2 in the multiplicative group $\mathcal{V}^*$ of $\mathcal{V}$ (where $\mathcal{V}$ is seen here as a Galois field with p^d elements), the map $g \mapsto x_2 x_1^{-1} g$ induces an isomorphism between $(\mathcal{V}, \mathcal{B}_k^{x_1})$ and $(\mathcal{V}, \mathcal{B}_k^{x_2})$. Since, by (4) and (5), $b_{k-1}^{x_1,*} \neq b_{k-1}^{x_2,*}$ for any $x \neq 0$, the 1-designs $(\mathcal{V}, \mathcal{B}_k^x)$, $x \neq 0$, are not isomorphic to the 1-design $(\mathcal{V}, \mathcal{B}_k)$.

Finally, let $d \geq 2$, and let p divide k , with $p \leq k < p^d$. Then the automorphisms of $(\mathcal{V}, \mathcal{B}_k)$ are exactly all the invertible affine maps on the affine space $\mathcal{V}$ over $\mathbb{F}_p$ by [11, Theorem 3.5]. The final characterization of the automorphisms of $(\mathcal{V}, \mathcal{B}_k^x)$, for x in $\mathcal{V}^*$ and $p^d > 9$, is just a rephrasing of Theorem 2.6.

This completes the proof of the theorem. $\square$

By the above Theorem 3.1, the condition that p be a divisor of k is a necessary condition for $(\mathcal{V}, \mathcal{B}_k^x)$ to be a 2-design. Under such a condition, the following lemma characterizes the 1-designs $(\mathcal{V}, \mathcal{B}_k^x)$ that are also 2-designs.

Lemma 3.2 *Let p be an odd prime, let $d \geq 2$, and let p divide k , $p \leq k < p^d$. For any x in $\mathcal{V}$, the following conditions are equivalent.*

- (a) $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a 2 -(p^d, k, λ) design.
- (b) $\widehat{\mathcal{D}}^* = (\mathcal{V}^*, \mathcal{B}_{k-1}^{x,*})$ is a 1 -($p^d - 1, k - 1, \tilde{r}^*$) design.
- (c) $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is a 1 -($p^d - 1, k, r^*$) design.

Moreover, if the above conditions are satisfied, then $\tilde{r}^* = \lambda$ and $r^* = r - \lambda$, where r is the replication number of the 1-design $(\mathcal{V}, \mathcal{B}_k^x)$.

Proof As p divides k , the blocks in $\mathcal{B}_k^x$ through two distinct elements y and z of $\mathcal{V}$ are in a one-to-one correspondence with the blocks in $\mathcal{B}_k^x$ through 0 and $z - y$, via the translation by $-y$. The latter blocks, in turn, are as many as the blocks in $\mathcal{B}_{k-1}^{x,*}$ through $z - y$, and this shows that (a) $\iff$ (b). Furthermore, if either condition is satisfied, then $\tilde{r}^* = \lambda$.

By Theorem 3.1, $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a 1-design, hence the number r of blocks in $\mathcal{B}_k^x$ through a given point y in $\mathcal{V}^*$ does not depend on y . Now, the family of such blocks is the disjoint union of the family of k -sets in $\mathcal{B}_k^x$ through 0 and y , and the family of k -sets in $\mathcal{B}_k^x$ through y , not containing 0 . But the former family is in a one-to-one correspondence with the family of $(k - 1)$ -sets in $\mathcal{B}_{k-1}^{x,*}$ through y , and the latter family is precisely the family of k -sets in $\mathcal{B}_k^{x,*}$ through y , hence

$$r = r_{k-1}^{x,*}(y) + r_k^{x,*}(y).$$

This shows that (b) $\iff$ (c), and that, if either condition is satisfied, then $r^* = r - \tilde{r}^*$, that is, $r^* = r - \lambda$, because condition (a) is satisfied, as well. $\square$

Remark 3.3 In Lemma 3.2, the implications (a) $\Rightarrow$ (b) and (a) $\Rightarrow$ (c), respectively, are just special cases of general results about block designs, because $\widehat{\mathcal{D}}^*$ and $\mathcal{D}^*$ are the *derived* design at 0 and the *residual* design at 0 of $\mathcal{D}$, respectively.

According to Theorem 3.1, $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a 1 -(p^d, k, r) design if and only if p divides k , with no conditions on x . On the contrary, $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is a 1 -($p^d - 1, k, r^*$) design for $x = 0$, with no conditions on k (except in the trivial cases where $\mathcal{B}_k^*$ is empty), and is never a 1-design for $x \neq 0$, as shown in the next result.

Theorem 3.4 Let p be an odd prime, let $d \geq 1$, and let $1 \leq k \leq p^d - 1$. For x in $\mathcal{V} = \mathbb{F}_p^d$, the incidence structure $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is a $1-(p^d - 1, k, r^*)$ design if and only if $x = 0$ and $k \notin \{1, p^d - 2\}$. If this is the case, then

$$r^* = \frac{1}{p^d} \binom{p^d - 2}{k - 1} + (-1)^{k + \lfloor k/p \rfloor} \frac{k}{p^d} \binom{p^{d-1} - 1}{\lfloor k/p \rfloor}.$$

Moreover, if $x = 0$, $p^d \geq 9$, and $3 \leq k \leq p^d - 4$, with $k \neq 4$ in the case where $p^d = 9$, then the automorphism group of $\mathcal{D}^*$ is isomorphic to the group of invertible linear mappings on $\mathcal{V}$ over $\mathbb{F}_p$, that is,

$$\text{Aut}(\mathcal{D}^*) \simeq \text{GL}(d, p).$$

Proof Let $x = 0$ and $2 \leq k \leq p^d - 1$, with $k \neq p^d - 2$. Thus $\mathcal{B}_k^* \neq \emptyset$ by [11, Theorem 2.2(iii)]. Also, by Proposition 2.5, the number $r_k^*(y)$ of all the k -sets in $\mathcal{B}_k^*$ containing y is independent of $y \in \mathcal{V}^*$. Alternatively, it suffices to note that the map $v \mapsto y_2 y_1^{-1} v$, $v \in \mathcal{V}^*$, induces a one-to-one correspondence between the k -sets in $\mathcal{B}_k^*$ containing y_1 and the k -sets in $\mathcal{B}_k^*$ containing y_2 (where $\mathcal{V}^*$ is seen as the multiplicative group of a Galois field with p^d elements). Therefore $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^*)$ is a $1-(p^d - 1, k, r^*)$ design with b_k^* blocks. From the basic relation

$$b_k^* k = (p^d - 1) r^*,$$

and from the equality (4), one obtains for r^* the desired equality. It is easy to check, in passing, that such a value of r^* coincides with the values $r_k^{0,*}(y)$ given in Proposition 2.5.

The final characterization of the automorphisms of $\mathcal{D}^*$ follows directly from [11, Theorem 3.2].

Now let $x \neq 0$. In this case, $\mathcal{B}_k^{x,*} = \emptyset$ if and only if $k = p^d - 1$ by [11, Theorem 2.2(iii)], hence we can assume that

$$1 \leq k \leq p^d - 2. \quad (8)$$

We will prove that $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is not a 1-design by showing that, for a suitable $y \neq x$ in $\mathcal{V}^*$, the difference $r_k^{x,*}(y) - r_k^{x,*}(x)$ is not zero. By Proposition 2.5, the numbers $r_k^{x,*}(y)$, y in $\mathcal{V}^*$, depend in some cases on the numbers $m_1, \dots, m_p$, where

$$m_h = \lfloor (k - h)/p \rfloor$$

for all $h \in \{1, \dots, p\}$. Also, let S_k^* be defined as in (6).

Assume first that $d = 1$. In this case, by (8), $1 \leq k \leq p - 2$. For $y = -x$, $x - iy = (1 + i)x \neq 0$ for all $i = 1, \dots, k$, whereas, for $y = x$, $x - iy = 0$ for $i = 1$. Hence $r_k^{x,*}(-x) = S_k^*$ and $r_k^{x,*}(x) = S_k^* + (-1)^{k-1}$ by Proposition 2.5. Therefore we can conclude that, for $y = -x$, $r_k^{x,*}(y) - r_k^{x,*}(x) = (-1)^k \neq 0$.

Assume now that $d \geq 2$. If $y = x$, then $x - hy = 0$ for $h = 1$, hence $r_k^{x,*}(x)$ depends on the value of the number m_1 . Let us first consider the case where

$$m_1 = p^{d-1} - 1. \quad (9)$$

In this case, $r_k^{x,*}(x) = S_k^*$ by (7). On the other hand, for $y = -x$, $x - (p - 1)y = 0$, hence $r_k^{x,*}(y)$ depends on the value of the number m_{p-1} . By (8) and (9), it is easy to show that $m_{p-1} = p^{d-1} - 2$. Therefore $r_k^{x,*}(-x) = S_k^* + (-1)^{k+p^{d-1}-3}$ by (7), whence again, for $y = -x$, $r_k^{x,*}(y) - r_k^{x,*}(x) = (-1)^k \neq 0$.

Let us finally consider the case where $m_1 \leq p^{d-1} - 2$. In this case,

$$r_k^{x,*}(x) = S_k^* + (-1)^{k+m_1-1} \binom{p^{d-1}-2}{m_1},$$

by (7). As $d \geq 2$, we can take an element $y \in \mathcal{V} \setminus \langle x \rangle = \mathcal{V} \setminus \{0, x, \dots, (p-1)x\}$, thus $x - iy \neq 0$ for all $i = 1, \dots, k$, because $x \neq 0$, hence $r_k^{x,*}(y) = S_k^*$ by Proposition 2.5.

Therefore $r_k^{x,*}(y) - r_k^{x,*}(x) = (-1)^{k+m_1} \binom{p^{d-1}-2}{m_1} \neq 0$.

This shows that $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is not a 1-design for $x \neq 0$, as claimed. $\square$

Remark 3.5 We noted in the proof of Theorem 3.1 (resp., Theorem 3.4) that the question of whether $(\mathcal{V}, \mathcal{B}_k^x)$ (resp., $(\mathcal{V}^*, \mathcal{B}_k^{x,*})$) is a 1-design can be approached from the point of view of transformation groups, that is, by considering the action of $\mathcal{V}$ on itself by translation or the action of $\mathcal{V}^*$ on itself by multiplication (see also Remark 3.7). Hence one might wonder whether there exists also a simpler and more direct proof that $(\mathcal{V}^*, \mathcal{B}_k^{x,*})$ is not a 1-design in the case where $x \neq 0$. This case, however, is sensibly harder, because the family $\mathcal{B}_k^{x,*}$ is not invariant by translations, nor by multiplication by a nonzero element of the Galois field $\text{GF}(p^d)$. Furthermore, what makes the proof even less trivial is the fact that, for $x \neq 0$, the suitable element $y \neq x$ in $\mathcal{V}^*$ such that the difference $r_k^{x,*}(x) - r_k^{x,*}(y)$ is not zero cannot be chosen in the same way for all possible cases, as shown in the proof of Theorem 3.4.

We can now state and prove the main result of this paper. Recall that, if k is not divisible by p , then, by Theorem 3.1, the incidence structure $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ fails to be even a 1-design. Again, in order to avoid trivialities, the case $k = p^d$ is disregarded. For such a value of k , $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a 2-design if and only if $x = 0$, in which case it is the trivial 2 -($p^d, p^d, 1$) design.

Theorem 3.6 *Let p be an odd prime, let $d \geq 2$, and let p divide k , with $p \leq k < p^d$. Given $x \in \mathcal{V} = \mathbb{F}_p^d$, the 1 -($p^d, k, b_{k-1}^{x,*}$) design $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a 2 -(p^d, k, λ) design if and only if $x = 0$. In this case,*

$$\lambda = \frac{1}{p^d} \binom{p^d-2}{k-2} + \frac{k-1}{p^d} \binom{p^{d-1}-1}{k/p-1}. \quad (10)$$

Moreover, the group of automorphisms of $\mathcal{D}$ is isomorphic to the group of affine mappings of $\mathcal{V}$ over $\mathbb{F}_p$, that is,

$$\text{Aut}(\mathcal{D}) \simeq \text{AGL}(d, p).$$

Proof Let $x \in \mathcal{V}$. In view of Lemma 3.2, Theorem 3.4 ensures that $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k^x)$ is a 2 -(p^d, k, λ) design if and only if $x = 0$. Hence, in this case, the desired equality for λ follows by combining the basic relation $\lambda(p^d - 1) = r(k - 1)$, where $r = b_{k-1}^{x,*}$, with the equality (4).

The final characterization of the automorphisms of $\mathcal{D}$ follows directly from [11, Theorem 3.5]. $\square$

Remark 3.7 For $x = 0$ (and p divisor of k), the property that $(\mathcal{V}, \mathcal{B}_k)$ is a 2-design can be proved, alternatively, by using the fact that the group of affine mappings of $\mathcal{V}$ over $\mathbb{F}_p$ acts 2-transitively on $\mathcal{V}$. Given $x_1 \neq x_2$ and $y_1 \neq y_2$ in $\mathcal{V}$, let T be an affine mapping of $\mathcal{V}$ over $\mathbb{F}_p$ such that $T(x_1) = y_1$ and $T(x_2) = y_2$. Then T induces a one-to-one correspondence between the k -sets in $\mathcal{B}_k$ containing x_1 and x_2 and the k -sets in $\mathcal{B}_k$ containing y_1 and y_2 . Hence $(\mathcal{V}, \mathcal{B}_k)$ is a 2-design. Also, the formula for λ in Theorem 3.6 can be obtained by

noting that, by Lemma 3.2, λ is equal to the replication number of the 1-design $(\mathcal{V}^*, \mathcal{B}_{k-1}^*)$, which, in turn, can be computed by means of the formula in Theorem 3.4.

Under the hypotheses of Theorem 3.6, one may ask whether $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k)$ is also a 3- (p^d, k, λ_3) design. The question appears to be legitimate, since the answer is affirmative in the case where $p = 2$ and $d \geq 3$, for any even k with $4 \leq k \leq 2^d - 4$ [10, Proposition 2.5] (see also [5, Remark 2.4]). For p odd, however, $\mathcal{D}$ is not necessarily a 3-design. In fact, we will now answer the question in the negative in the special case where $k = p$ and $d \geq 2$. We begin by giving a preliminary result, whose proof is just a trivial modification of the proof of Lemma 3.2.

Lemma 3.8 *Let p be an odd prime, let $d \geq 2$, and let p divide k , with $p \leq k < p^d$. Then the following conditions are equivalent.*

- (a) $\mathcal{D} = (\mathcal{V}, \mathcal{B}_k)$ is a 3- (p^d, k, λ_3) design.
- (b) $\tilde{\mathcal{D}}^* = (\mathcal{V}^*, \mathcal{B}_{k-1}^*)$ is a 2- $(p^d - 1, k - 1, \tilde{\lambda}^*)$ design.
- (c) $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_k^*)$ is a 2- $(p^d - 1, k, \lambda^*)$ design.

Proposition 3.9 *Let p be an odd prime, and let $d \geq 2$. Then the 2- (p^d, p, λ) design $\mathcal{D} = (\mathcal{V}, \mathcal{B}_p)$ is not a 3-design. Equivalently, the 1- $(p^d - 1, p, r^*)$ design $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_p^*)$ is not a 2-design.*

Proof Let p be odd, and let $d \geq 2$. By Lemma 3.8, it is sufficient to prove that $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_p^*)$ is not a 2-design. For any x in $\mathcal{V}$, for any pair of distinct points y, z in $\mathcal{V}^*$, and for any odd $3 \leq k \leq p$, let us set

$$r_k^{x,*}(y, z) = \# \text{ of blocks in } \mathcal{B}_k^{x,*} \text{ containing both } y \text{ and } z.$$

By definition of 2-design, one needs to prove that the parameter $r_p^{0,*}(y, z)$ is not a constant as y, z range over all the pairs of distinct points in $\mathcal{V}^*$. If y is a given point in $\mathcal{V}^*$, and z is any point in $\mathcal{V} \setminus \{y\} = \mathcal{V} \setminus \{0, y, 2y, \dots, (p-1)y\}$ (z exists because $d \geq 2$), then $y, z, -y - z$ are three distinct points in $\mathcal{V}^*$, summing up to zero, hence

$$r_3^{0,*}(y, z) = 1 \neq 0 = r_3^{0,*}(y, -y).$$

In particular, $(\mathcal{V}^*, \mathcal{B}_3^*)$ is not a 2-design, and we can assume that $p \geq 5$. In this case, for any odd k , with $5 \leq k \leq p$, for any x in $\mathcal{V}$, and for any pair of distinct points y, z in $\mathcal{V}^*$, a block in $\mathcal{B}_k^{x,*}$ contains both y and z if and only if it is of the form $\{y, z, x_1, x_2, \dots, x_{k-2}\}$, where $\{x_1, x_2, \dots, x_{k-2}\}$ is a block in $\mathcal{B}_{k-2}^{x-y-z,*}$ not containing y nor z . Therefore, by the inclusion-exclusion principle,

$$r_k^{x,*}(y, z) = b_{k-2}^{x-(y+z),*} - r_{k-2}^{x-(y+z),*}(y) - r_{k-2}^{x-(y+z),*}(z) + r_{k-2}^{x-(y+z),*}(y, z).$$

By iterating this formula, one finds that

$$\begin{aligned} r_p^{0,*}(y, z) &= b_{p-2}^{-(y+z),*} - r_{p-2}^{-(y+z),*}(y) - r_{p-2}^{-(y+z),*}(z) \\ &\quad + b_{p-4}^{-2(y+z),*} - r_{p-4}^{-2(y+z),*}(y) - r_{p-4}^{-2(y+z),*}(z) \\ &\quad + \dots \\ &\quad + b_3^{-((p-3)/2)(y+z),*} - r_3^{-((p-3)/2)(y+z),*}(y) - r_3^{-((p-3)/2)(y+z),*}(z) \\ &\quad + r_3^{-((p-3)/2)(y+z),*}(y, z). \end{aligned} \tag{11}$$

Let y be a given point in $\mathcal{V}^*$. By Proposition 2.5, $r_k^{0,*}(y) = S_k^*$ and $r_k^{0,*}(-y) = S_k^*$ for all (odd) k , with $3 \leq k \leq p-2$, where S_k^* is the number introduced in (6). Since $r_3^{0,*}(y, -y) = 0$, it follows from (11) that

$$r_p^{0,*}(y, -y) = b_{p-2}^{0,*} - 2S_{p-2}^* + b_{p-4}^{0,*} - 2S_{p-4}^* + \dots + b_3^{0,*} - 2S_3^*. \quad (12)$$

Now let z be a point in $\mathcal{V}$ such that $z \notin \langle y \rangle = \{0, y, 2y, \dots, (p-1)y\}$ (again, z exists because $d \geq 2$). If we let $x = -(y + z)$, then $x \notin \langle y \rangle$ and $x \notin \langle z \rangle$ (in particular, $x \neq 0$). It follows from Proposition 2.5 that $r_k^{jx,*}(y) = S_k^*$ and $r_k^{jx,*}(z) = S_k^*$ for all (odd) k , with $3 \leq k \leq p-2$, and for all $1 \leq j \leq (p-3)/2$. Also, $r_3^{((p-3)/2)x,*}(y, z) = 1$, since $\{y, z, \frac{p-1}{2}x\}$ is the only 3-subset of $\mathcal{V}^*$ that contains y, z , and whose elements sum up to $((p-3)/2)x$. Therefore, by (11),

$$r_p^{0,*}(y, z) = b_{p-2}^{x,*} - 2S_{p-2}^* + b_{p-4}^{2x,*} - 2S_{p-4}^* + \dots + b_3^{((p-3)/2)x,*} - 2S_3^* + 1. \quad (13)$$

Finally, it follows from (12) and (13) that

$$\begin{aligned} r_p^{0,*}(y, z) - r_p^{0,*}(y, -y) &= \left(b_{p-2}^{x,*} - b_{p-2}^{0,*}\right) + \left(b_{p-4}^{2x,*} - b_{p-4}^{0,*}\right) + \dots + \left(b_3^{((p-3)/2)x,*} - b_3^{0,*}\right) + 1. \end{aligned}$$

Therefore, by (4) and (5),

$$r_p^{0,*}(y, z) - r_p^{0,*}(y, -y) = \frac{p-3}{2} + 1,$$

whence $r_p^{0,*}(y, z) - r_p^{0,*}(y, -y) \neq 0$. This completes the proof of the proposition. $\square$

Example 3.10 (1) The smallest non-trivial example where Theorem 3.6 applies is that where $p = 3$, $d = 2$, and $k = 3$. In this case, by the equalities (2), (4), and (10), $\mathcal{D} = (\mathcal{V}, \mathcal{B}_3)$ is a 2-(9, 3, 1) design with 12 blocks and replication number $r = 4$, that is, $\mathcal{D}$ is (isomorphic to) the point-line design of the affine plane $\text{AG}(2, 3)$, or, equivalently, to the unique Steiner triple system with 9 points. By Theorem 3.6, the group of automorphisms of $\mathcal{D}$ is equal to the group of affine mappings of $\mathcal{V}$ over $\mathbb{F}_3$, in accordance with the fundamental theorem of affine geometry. By Lemma 3.2 (or, directly, by Theorem 3.4), and by equality (4), $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_3^*)$ is a 1-(8, 3, 3) design with 8 blocks.

(2) Let $p = 5$, $d = 2$, and $k = 5$. By Theorems 3.6 and 3.1, and by the equalities (2), (4), and (10), $\mathcal{D} = (\mathcal{V}, \mathcal{B}_5)$ is a 2-(25, 5, 71) design with 2130 blocks and replication number $r = 426$. By Lemma 3.2 (or, directly, by Theorem 3.4), and by equality (4), $\mathcal{D}^* = (\mathcal{V}^*, \mathcal{B}_5^*)$ is a 1-(24, 5, 355) design with 1704 blocks.

On the other hand, for the same values of the parameters p , d , and k , and for any x in $\mathcal{V}^*$, $(\mathcal{V}, \mathcal{B}_5^x)$ is a 1-(25, 5, 425) design with 2125 blocks and replication number $r = 425$ by Theorem 3.1 and equality (3), but it is not a 2-design by Theorem 3.6. In this case, however, it is not necessary to invoke Theorem 3.6 to prove that $(\mathcal{V}, \mathcal{B}_5^x)$ is not a 2-design, as $(\mathcal{V}, \mathcal{B}_5^x)$ does not even satisfy the necessary condition for being a 2-design, since there exists no positive integer λ such that $\lambda(v-1) = r(k-1)$. Equivalently, by Lemma 3.2, $(\mathcal{V}^*, \mathcal{B}_5^{x,*})$ is not a 1-design (and it does not even satisfy the necessary condition $bk = rv$ for being a 1-design).

Finally, note that $\mathcal{D} = (\mathcal{V}, \mathcal{B}_5)$ contains, as a minimal 2-subdesign, the point-line design of the affine plane $\text{AG}(2, 5)$, which is a 2-(25, 5, 1) design with 30 blocks and replication number $r = 6$. By Theorem 3.6, every automorphism of $\mathcal{D}$ is an invertible affine mapping of $\mathcal{V}$ over $\mathbb{F}_5$, hence it induces an automorphism of $\text{AG}(2, 5)$, and conversely, by the fundamental theorem of affine geometry.

(3) Let $p = 11$, $d = 2$, and $k = 33$. By Theorem 3.6, $\mathcal{D} = (\mathcal{V}, \mathcal{B}_{33})$ is a 2 -(v, k, λ) design with $v = 121$, $k = 33$, and $b = b_{33}$ blocks. By Theorem 3.1, its replication number is $r = b_{32}^*$, thus the parameters of the design satisfy the basic relation $\lambda(v - 1) = r(k - 1)$, that is,

$$\lambda \cdot 120 = b_{32}^* \cdot 32. \quad (14)$$

For any x in $\mathcal{V}^*$, $\mathcal{D}(x) = (\mathcal{V}, \mathcal{B}_{33}^x)$ is a 1 -($121, 33, r(x)$) design with replication number $r(x) = b_{32}^{x,*}$, by Theorem 3.1. By the equalities (4) and (5), $b_{32}^* - b_{32}^{x,*} = \binom{10}{2} = 45$, hence, by equality (14), $b_{32}^{x,*} \cdot 32 = (b_{32}^* - 45) \cdot 32 = \lambda \cdot 120 - 12 \cdot 120$. This shows that $\lambda(x) = \lambda - 12$ is a positive integer that satisfies the relation

$$\lambda(x) \cdot 120 = r(x) \cdot 32.$$

This says precisely that $\mathcal{D}(x) = (\mathcal{V}, \mathcal{B}_{33}^x)$ satisfies the necessary condition $\lambda(x)(v - 1) = r(x)(k - 1)$ for being a 2 -design. On the other hand, $\mathcal{D}(x)$ is not a 2 -design by Theorem 3.6, hence this example ultimately shows that, unlike in the previous example, it is not possible, in general, in the case where p divides k and $x \in \mathcal{V}$, to determine whether $(\mathcal{V}, \mathcal{B}_k^x)$ is a 2 -design by relying only on the necessary condition $\lambda(v - 1) = r(k - 1)$, without resorting to Theorem 3.6.

Funding Open access funding provided by Università degli Studi di Palermo within the CRUI-CARE Agreement. Università di Palermo (FFR2023 Pavone).

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Appendix

Proof of Proposition 2.5 Let p be an odd prime, let $k \in \{1, \dots, p^d - 1\}$, let x be in $\mathcal{V}$, and let y be in $\mathcal{V}^*$. It follows from Definition 2.1 that

$$r_1^{x,*}(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{if } y \neq x \end{cases} = b_0^{x-y,*},$$

and that, for $2 \leq h \leq k$,

$$r_h^{x,*}(y) = b_{h-1}^{x-y,*} - r_{h-1}^{x-y,*}(y),$$

since the left-hand side amounts to the number of $(h - 1)$ -sets in $\mathcal{B}_{h-1}^{x-y,*}$ not containing y . Note that, by [11, Theorem 2.2], the latter equality reduces to $0 = 0$ in the cases where $b_{h-1}^{x-y,*} = 0$, that is, when $x = y$ and either $h = 2$ or $h = k = p^d - 1$. Recursively,

$$r_k^{x,*}(y) = \sum_{i=1}^k (-1)^{i-1} b_{k-i}^{x-y,*}, \quad (15)$$

where the numbers $b_j^{x-iy,*}$, $j \geq 0$, are given in (4), if $x - iy = 0$, and in (5), if $x - iy \neq 0$.

Note that, for any i such that $x - iy \neq 0$, the number $b_{k-i}^{x-iy,*}$ is equal, by (5), to any number $b_{k-i}^{z,*}$, with $z \neq 0$, hence, in particular, $b_{k-i}^{x-iy,*} = b_{k-i}^{y,*}$. Thus let us consider, for our convenience, the integer S_k^* defined by

$$S_k^* = \sum_{i=1}^k (-1)^{i-1} b_{k-i}^{y,*}, \quad (16)$$

which, again by (5), is independent of $y \in \mathcal{V}^*$, and which trivially coincides with $r_k^{x,*}(y)$ in the case where $x - iy \neq 0$ for all $i = 1, \dots, k$. We will now show that $r_k^{x,*}(y)$ can be expressed in terms of S_k^* also in the case where $x - iy = 0$ for some $i = 1, \dots, k$.

We first want to express S_k^* in closed form. If we define

$$M = \left\lfloor \frac{k-1}{p} \right\rfloor,$$

then $0 \leq M \leq p^{d-1} - 1$, since $1 \leq k \leq p^d - 1$. Also,

$$Mp \leq k-1 < (M+1)p.$$

Note that $d \geq 2$ if $M \geq 1$, because, if $d = 1$, then $M = 0$ for all possible values of $k \in \{1, \dots, p-1\}$. In view of (16) and (5), it is necessary to establish, for each index $i = 1, \dots, k$, what is the exact interval $[np, (n+1)p)$ containing $k-i$. Note that $n = M$, that is, $Mp \leq k-i < (M+1)p$, if and only if $1 \leq i \leq k-Mp$, and that, for any $0 \leq n \leq M-1$ (provided that $M \geq 1$), $np \leq k-i < (n+1)p$ if and only if $k-(n+1)p+1 \leq i \leq k-np$. Therefore, if $M \geq 1$, then, by (16) and (5), we may conclude that

$$\begin{aligned} S_k^* &= \sum_{i=1}^k (-1)^{i-1} \frac{1}{p^d} \binom{p^d-1}{k-i} - \sum_{i=1}^{k-Mp} (-1)^{i-1} (-1)^{k+M-i} \frac{1}{p^d} \binom{p^{d-1}-1}{M} \\ &\quad - \sum_{n=0}^{M-1} \sum_{i=k-(n+1)p+1}^{k-np} (-1)^{i-1} (-1)^{k+n-i} \frac{1}{p^d} \binom{p^{d-1}-1}{n}, \end{aligned}$$

which can be rewritten as

$$S_k^* = S_{k,1}^* + S_{k,2}^* + S_{k,3}^*,$$

where

$$\begin{aligned}
 S_{k,1}^* &= \sum_{i=1}^k (-1)^{i-1} \frac{1}{p^d} \binom{p^d - 1}{k-i} \\
 &= \frac{1}{p^d} \left(\sum_{i=1}^{k-1} (-1)^{i-1} \binom{p^d - 1}{k-i} + (-1)^{k-1} \binom{p^d - 1}{0} \right) \\
 &= \frac{1}{p^d} \left(\sum_{i=1}^{k-1} (-1)^{i-1} \left(\binom{p^d - 2}{k-i} + \binom{p^d - 2}{k-i-1} \right) + (-1)^{k-1} \binom{p^d - 2}{0} \right) \\
 &= \frac{1}{p^d} \binom{p^d - 2}{k-1},
 \end{aligned}$$

$$\begin{aligned}
 S_{k,2}^* &= - \sum_{i=1}^{k-Mp} (-1)^{i-1} (-1)^{k+M-i} \frac{1}{p^d} \binom{p^{d-1} - 1}{M} \\
 &= \sum_{i=1}^{k-Mp} (-1)^{k+M} \frac{1}{p^d} \binom{p^{d-1} - 1}{M} \\
 &= (-1)^{k+M} \frac{k-Mp}{p^d} \binom{p^{d-1} - 1}{M},
 \end{aligned}$$

$$\begin{aligned}
 S_{k,3}^* &= - \sum_{n=0}^{M-1} \sum_{i=k-(n+1)p+1}^{k-np} (-1)^{i-1} (-1)^{k+n-i} \frac{1}{p^d} \binom{p^{d-1} - 1}{n} \\
 &= \sum_{n=0}^{M-1} (-1)^{k+n} \sum_{i=k-(n+1)p+1}^{k-np} \frac{1}{p^d} \binom{p^{d-1} - 1}{n} \\
 &= (-1)^k \sum_{n=0}^{M-1} (-1)^n \frac{p}{p^d} \binom{p^{d-1} - 1}{n} \\
 &= (-1)^k \frac{1}{p^{d-1}} \left(\binom{p^{d-1} - 2}{0} + \sum_{n=1}^{M-1} (-1)^n \left(\binom{p^{d-1} - 2}{n-1} + \binom{p^{d-1} - 2}{n} \right) \right) \\
 &= (-1)^k \frac{1}{p^{d-1}} (-1)^{M-1} \binom{p^{d-1} - 2}{M-1} \\
 &= -(-1)^{k+M} \frac{1}{p^{d-1}} \binom{p^{d-1} - 2}{M-1}.
 \end{aligned}$$

Hence, finally, for the current case $M \geq 1$ (and necessarily $d \geq 2$),

$$S_k^* = \frac{1}{p^d} \binom{p^d - 2}{k-1} + \frac{(-1)^{k+M}}{p^d} \left((k-Mp) \binom{p^{d-1} - 1}{M} - p \binom{p^{d-1} - 2}{M-1} \right).$$

In the remaining case $M = 0$, the exact interval containing $k - i$ is $[0, p)$, for each index $i = 1, \dots, k$. Hence S_k^* simply reduces to $S_{k,1}^* + S_{k,2}^*$, thus

$$S_k^* = \frac{1}{p^d} \binom{p^d - 2}{k - 1} + (-1)^k \frac{k}{p^d}.$$

Now we will find closed forms for the numbers $r_k^{x,*}(y)$, by expressing them in terms of S_k^* for all possible values of x in $\mathcal{V}$ and y in $\mathcal{V}^*$.

If $x - iy \neq 0$ for all $i = 1, \dots, k$, then, as we mentioned earlier,

$$r_k^{x,*}(y) = S_k^*.$$

Now let us consider the case where $x - iy = 0$ for some $i = 1, \dots, k$. In this case, there exists a (necessarily unique) $h \in \{1, \dots, p\}$, $h \leq k$, such that $x - hy = 0$. Let us set

$$m_h = \lfloor (k - h)/p \rfloor.$$

Since $h + m_h p \leq k < h + (m_h + 1)p$, it follows that, for $i \in \{1, \dots, k\}$, $x - iy = 0$ if and only if $i \in \{h, h + p, h + 2p, \dots, h + m_h p\}$. Thus $b_{k-i}^{x-iy,*} = b_{k-i}^{y,*}$ for all other values of i , by (5). In view of (15), (16), (4), and (5), it is necessary to establish the exact interval $[np, (n + 1)p)$ containing $k - i$, for the only values of i for which $x - iy = 0$, that is, for the values $i = h + lp$, with $l \in \{0, 1, \dots, m_h\}$. Since, for all $l \in \{0, 1, \dots, m_h\}$, $(m_h - l)p \leq k - lp - h < (m_h - l + 1)p$, it follows from (15), (16), (4), and (5), that

$$\begin{aligned} r_k^{x,*}(y) - S_k^* &= \sum_{i=1}^k (-1)^{i-1} (b_{k-i}^{x-iy,*} - b_{k-i}^{y,*}) \\ &= \sum_{l=0}^{m_h} (-1)^{h+lp-1} (-1)^{(k-lp-h)+m_h-l} \binom{p^{d-1}-1}{m_h-l} \\ &= (-1)^{k+m_h-1} \sum_{l=0}^{m_h} (-1)^l \binom{p^{d-1}-1}{m_h-l}. \end{aligned}$$

If $d = 1$, then $0 \leq k - h < k \leq p - 1$, hence $m_h = 0$ and

$$r_k^{x,*}(y) - S_k^* = (-1)^{k-1}.$$

If $d \geq 2$, then, by arguing as for the previous computations of $S_{k,1}^*$ and $S_{k,3}^*$, one obtains that

$$r_k^{x,*}(y) - S_k^* = \begin{cases} (-1)^{k+m_h-1} \binom{p^{d-1}-2}{m_h} & \text{if } 0 \leq m_h \leq p^{d-1} - 2 \\ 0 & \text{if } m_h = p^{d-1} - 1. \end{cases}$$

Note that, unlike in the two mentioned cases, for $m_h \geq 1$ the telescopic sum obtained from $\sum_{l=0}^{m_h} (-1)^l \binom{p^{d-1}-1}{m_h-l}$ can be equal to zero, which happens exactly in the case where it contains all the p^{d-1} binomial coefficients, that is, when $m_h = p^{d-1} - 1$.

The proof is now complete. $\square$

Lemma 4.1 *Let p be an odd prime, and let $d \geq 1$, with $p^d \geq 9$. Let x be in $\mathcal{V}^*$, and let k be an integer satisfying $3 \leq k \leq p^d - 3$. Let φ be a permutation of $\mathcal{V}$. If p does not divide k ,*

then φ induces a permutation of $\mathcal{B}_k^x$ if and only if there exists an invertible linear map L on $\mathcal{V}$ over $\mathbb{F}_p$ such that

$$\varphi(y) = L(y) + \frac{1}{k}(x - L(x))$$

for all y in $\mathcal{V}$ (where $1/k$ denotes the inverse of k in the multiplicative group of $\mathbb{F}_p$).

Moreover, φ is linear $\iff \varphi(0) = 0 \iff L(x) = x$.

Proof Let L be an invertible linear map on $\mathcal{V}$ over $\mathbb{F}_p$, and let φ be the permutation of $\mathcal{V}$ defined by $\varphi(y) = L(y) + \frac{1}{k}(x - L(x))$ for all y in $\mathcal{V}$. If $\{x_1, \dots, x_k\}$ is in $\mathcal{B}_k^x$, then $\varphi(x_1) + \dots + \varphi(x_k) = L(x_1) + \dots + L(x_k) + x - L(x) = L(x_1 + \dots + x_k) + x - L(x) = x$. Hence φ induces a permutation of $\mathcal{B}_k^x$.

Conversely, suppose that φ is a permutation of $\mathcal{V}$ that induces a permutation of $\mathcal{B}_k^x$. If $T_x : \mathcal{V} \rightarrow \mathcal{V}$ is the permutation of $\mathcal{V}$ defined by $T_x(y) = y + \frac{1}{k}x$, then T_x maps $\mathcal{B}_k^0$ onto $\mathcal{B}_k^x$, hence the map $L = T_x^{-1}\varphi T_x$ induces a permutation of $\mathcal{B}_k = \mathcal{B}_k^0$. Therefore L is an invertible linear map on $\mathcal{V}$ over $\mathbb{F}_p$ by [11, Theorem 3.5(i)], and, for all y in $\mathcal{V}$, $\varphi(y) = T_x L T_x^{-1}(y) = L(y - \frac{1}{k}x) + \frac{1}{k}x = L(y) + \frac{1}{k}(x - L(x))$. Finally, it is immediate that

$$\varphi \text{ is linear} \implies \varphi(0) = 0 \implies L(x) = x \implies \varphi \text{ is linear,}$$

as claimed. $\square$

Proof of Theorem 2.6 Let p be an odd prime, and let $d \geq 2$. Let p divide k , with $p \leq k < p^d$, and let x be a point in $\mathcal{V}^*$.

Let L be an invertible linear map on $\mathcal{V}$ over $\mathbb{F}_p$, with $L(x) = x$, and let b be a point in $\mathcal{V}$. Then $\varphi = L + b$ is a permutation of $\mathcal{V}$ and, moreover, if $\{x_1, \dots, x_k\}$ is in $\mathcal{B}_k^x$, then, since p divides k , $x = L(x) + kb = L(x_1 + \dots + x_k) + kb = (L(x_1) + b) + \dots + (L(x_k) + b) = \varphi(x_1) + \dots + \varphi(x_k)$, that is, $\{\varphi(x_1), \dots, \varphi(x_k)\} \in \mathcal{B}_k^x$. Therefore φ induces a permutation of $\mathcal{B}_k^x$.

Conversely, suppose that

$$p^d > 9. \tag{17}$$

Let $\varphi : \mathcal{V} \rightarrow \mathcal{V}$ be a permutation of $\mathcal{V}$ that induces a permutation of $\mathcal{B}_k^x$. Up to translation, we may and will assume that

$$\varphi(0) = 0. \tag{18}$$

Indeed, if we let $b = \varphi(0)$, then $L = \varphi - b$ is a permutation of $\mathcal{V}$ that permutes $\mathcal{B}_k^x$, and $L(0) = 0$. If L is linear over $\mathbb{F}_p$ and $L(x) = x$, then $\varphi = L + b$ is of the desired form. Hence, once we assume that $\varphi(0) = 0$, it suffices to prove that φ is linear over $\mathbb{F}_p$ and $\varphi(x) = x$.

Also note that, since the elements of $\mathcal{V}$ sum up to zero, a k -subset $\mathcal{S}$ of $\mathcal{V}$ is in $\mathcal{B}_k^x$ if and only if its complement $\mathcal{V} \setminus \mathcal{S}$ is in $\mathcal{B}_{p^d-k}^{-x}$. It follows that φ permutes $\mathcal{B}_k^x$ if and only if φ permutes $\mathcal{B}_{p^d-k}^{-x}$. Therefore, since p divides $p^d - k$, up to replacing x by $-x$ and k by $p^d - k$, we may assume that

$$k \leq \frac{p^d - 1}{2}. \tag{19}$$

We claim that

$$\varphi(y) + \varphi(-y) = 0 \text{ for all } y \in \mathcal{V}^*. \tag{20}$$

Case 1. $k = 3$ (hence, necessarily, $p = 3$ and $d \geq 3$ by (17)).

Since $\mathcal{V}$ is a d -dimensional vector space over $\mathbb{F}_3$, with $d \geq 3$, and since $x \in \mathcal{V} \setminus \{0\}$, we may extend x to a triple x, x_1, x_2 of linearly independent vectors in $\mathcal{V}$. Then the six 3-sets $\mathbf{b}_1 = \{x_1, -x_1, x\}$, $\mathbf{b}_2 = \{x_2, -x_2, x\}$, $\mathbf{b}_3 = \{0, -x_2, x+x_2\}$, $\mathbf{b}_4 = \{x+x_2, -x_1, x_1-x_2\}$, $\mathbf{b}_5 = \{-x_1, -x_2, x+x_1+x_2\}$, $\mathbf{b}_6 = \{x_1, x_1-x_2, x+x_1+x_2\}$ are all in $\mathcal{B}_3^x$, hence their images under φ are again in $\mathcal{B}_3^x$. Considering $\varphi(\mathbf{b}_1)$ and $\varphi(\mathbf{b}_2)$, one gets $\varphi(x_1) + \varphi(-x_1) + \varphi(x) = x$ and $\varphi(x_2) + \varphi(-x_2) + \varphi(x) = x$, whence

$$\begin{aligned}\varphi(-x_1) &= x - \varphi(x_1) - \varphi(x) \\ \varphi(-x_2) &= x - \varphi(x_2) - \varphi(x).\end{aligned}\tag{21}$$

Considering $\varphi(\mathbf{b}_3)$ and $\varphi(\mathbf{b}_4)$, one gets, by (18), $\varphi(-x_2) + \varphi(x+x_2) = x$ and $\varphi(x+x_2) + \varphi(-x_1) + \varphi(x_1-x_2) = x$, hence $\varphi(x_1-x_2) = x - \varphi(-x_1) - (x - \varphi(-x_2)) = \varphi(-x_2) - \varphi(-x_1)$. Therefore, by (21),

$$\varphi(x_1-x_2) = \varphi(x_1) - \varphi(x_2).\tag{22}$$

Finally, considering $\varphi(\mathbf{b}_5)$ and $\varphi(\mathbf{b}_6)$, one gets, by (21) and (22), $(x - \varphi(x_1) - \varphi(x)) + (x - \varphi(x_2) - \varphi(x)) + \varphi(x+x_1+x_2) = x$ and $\varphi(x_1) + (\varphi(x_1) - \varphi(x_2)) + \varphi(x+x_1+x_2) = x$, hence $2x - 2\varphi(x) - \varphi(x_1) - \varphi(x_2) = x - \varphi(x+x_1+x_2) = 2\varphi(x_1) - \varphi(x_2)$, that is, $2x - 2\varphi(x) = 0$, whence

$$\varphi(x) = x.\tag{23}$$

If $y \in \mathcal{V} \setminus \{0, x, -x\}$, then $\{x, y, -y\} \in \mathcal{B}_3^x$, hence $\varphi(x) + \varphi(y) + \varphi(-y) = x$, that is, $\varphi(y) + \varphi(-y) = 0$ by (23). Since $\mathcal{V} = \varphi(\mathcal{V}) = \{0\} \cup \{\varphi(z) \mid z \neq 0\}$, and since the sum of all the elements of $\mathcal{V}$ is zero, it follows that $\varphi(x) + \varphi(-x) = 0$. Hence (20) holds and, moreover, it follows from (23) that

$$\varphi(-x) = -x.\tag{24}$$

Case 2. $k > 3$ (hence, necessarily, $k \geq 5$).

Let y, z be two given distinct points in $\mathcal{V} \setminus \{0\}$, such that $\{y, -y\} \cap \{z, -z\} = \emptyset$. Let $\{a, b\}$ be any 2-set in $\mathcal{B}_2^x$ disjoint from $\{0, y, -y, z, -z\}$, that is, different from $\{0, x\}$, $\{y, x-y\}$, $\{-y, x+y\}$, $\{z, x-z\}$, $\{-z, x+z\}$ (such a 2-set exists, since $\mathcal{B}_2^x$ contains $(p^d-1)/2$ 2-sets and $(p^d-1)/2 > 5$ by (17)). The set

$$\mathcal{A} = \mathcal{V} \setminus \{0, y, -y, z, -z, a, -a, b, -b\}$$

has precisely $p^d - 9$ elements, and is the disjoint union of $(p^d - 9)/2$ 2-sets of the form $\{x_i, -x_i\}$. Also, $p^d - 9 \geq k - 4$, since $k \leq (p^d - 1)/2 \leq p^d - 5$ (by (19) and (17)). It follows that, if k is even (resp., odd), then one can construct two k -sets $\{y, -y, a, b, x_1, -x_1, \dots, x_{(k-4)/2}, -x_{(k-4)/2}\}$ and $\{z, -z, a, b, x_1, -x_1, \dots, x_{(k-4)/2}, -x_{(k-4)/2}\}$ (resp., $\{0, y, -y, a, b, x_1, -x_1, \dots, x_{(k-5)/2}, -x_{(k-5)/2}\}$ and $\{0, z, -z, a, b, x_1, -x_1, \dots, x_{(k-5)/2}, -x_{(k-5)/2}\}$) in $\mathcal{B}_k^x$, where the pairs $x_i, -x_i$ are taken in $\mathcal{A}$ (for $k = 5$, no such pairs are taken). Since φ permutes $\mathcal{B}_k^x$, and since $\varphi(0) = 0$, by computing the images of the two k -sets under φ it follows that

$$\varphi(y) + \varphi(-y) = \varphi(z) + \varphi(-z).$$

If ω is the common value of all the points $\varphi(y) + \varphi(-y)$, $y \in \mathcal{V}^*$, then

$$\frac{p^d - 1}{2} \omega = \sum_{\{y, -y\} \subseteq \mathcal{V}^*} \varphi(y) + \varphi(-y) = \sum_{t \in \mathcal{V}^*} \varphi(t) = \sum_{t \in \mathcal{V}^*} t = 0,$$

hence $\omega = 0$, since $\frac{p^d-1}{2} \neq 0$ in $\mathbb{F}_p$. Therefore (20) is satisfied.

We are now left to prove that φ is linear over $\mathbb{F}_p$ and $\varphi(x) = x$. Again, we need to distinguish the cases $k = 3$ and $k > 3$.

Case 1. $k = 3$ (hence, necessarily, $p = 3$ and $d \geq 3$ by (17)).

Since $\varphi(x) = x$ by (23), and $\varphi(2y) = \varphi(-y) = -\varphi(y) = 2\varphi(y)$ by (18) and (20), we only have to prove that

$$\varphi(v + w) = \varphi(v) + \varphi(w) \quad \text{for all } v, w \in \mathcal{V}. \quad (25)$$

In order to do so, it suffices to prove that

$$\varphi(y + z) + \varphi(y - z) = 2\varphi(y) \quad \text{for all } y, z \in \mathcal{V}. \quad (26)$$

Indeed, suppose that (26) holds. Then, for all $v, w \in \mathcal{V}$,

$$\begin{aligned} \varphi(v) + \varphi(w) &= \varphi(2(v + w) + 2(v - w)) + \varphi(2(v + w) - 2(v - w)) \\ &= 2\varphi(2(v + w)) \\ &= -\varphi(-(v + w)) \\ &= \varphi(v + w), \end{aligned}$$

by (20) and (18). Therefore (25) holds.

In order to prove (26), we first claim that

$$x - \varphi(v + x) = 2\varphi(v) \quad \text{for all } v \in \mathcal{V}. \quad (27)$$

For $v = 0, x, -x$, the equality $x - \varphi(v + x) = 2\varphi(v)$ reduces to $0 = 0$, $2\varphi(x) = 2\varphi(x)$, $x = x$, respectively, hence it is satisfied. For $v \notin \{0, x, -x\}$, the 3-set $\{-x, v, -v - x\}$ is in $\mathcal{B}_3^x$, hence $\varphi(-x) + \varphi(v) + \varphi(-v - x) = x$, that is, $-x + \varphi(v) - \varphi(v + x) = x$ by (20) and (24), whence $x - \varphi(v + x) = 2\varphi(v)$, thus (27) holds.

Now let y, z be in $\mathcal{V}$. If $z \notin \{0, x, -x\}$, then $\{y + z, y - z, y + x\}$ is in $\mathcal{B}_3^x$, hence $\varphi(y + z) + \varphi(y - z) = x - \varphi(y + x) = 2\varphi(y)$ by (27). Since the equality in (26) is trivially satisfied for $z = 0$, we are only left to prove that it holds for $z = x$. By applying (27) for $v = y$ and $v = -y$, and by recalling (20) and (18), one gets

$$\begin{aligned} \varphi(y + x) + \varphi(y - x) &= \varphi(y + x) - \varphi(-y + x) \\ &= (x - 2\varphi(y)) - (x - 2\varphi(-y)) \\ &= 2\varphi(y). \end{aligned}$$

This concludes the proof of the case $k = 3$.

Case 2. $k > 3$ (hence, necessarily, $k \geq 5$).

We claim that φ induces a permutation of $\mathcal{B}_{k-2}^x$. Indeed, if $\{x_1, x_2, \dots, x_{k-2}\}$ is in $\mathcal{B}_{k-2}^x$, then let $\{y, -y\}$ be any 2-set contained in

$$\mathcal{U} = \mathcal{V} \setminus \{0, x_1, -x_1, x_2, -x_2, \dots, x_{k-2}, -x_{k-2}\}$$

(such a 2-set exists, since $\mathcal{U}$ has at least $p^d - 2k + 3$ elements, and $p^d - 2k + 3 \geq 2$ by (19)). Then $\{x_1, x_2, \dots, x_{k-2}, y, -y\}$ is in $\mathcal{B}_k^x$, hence $\varphi(x_1) + \dots + \varphi(x_{k-2}) + \varphi(y) + \varphi(-y) = x$. Therefore $\varphi(x_1) + \dots + \varphi(x_{k-2}) = x$ by (20), that is, $\{\varphi(x_1), \varphi(x_2), \dots, \varphi(x_{k-2})\}$ is in $\mathcal{B}_{k-2}^x$, as claimed.

Since $3 \leq k - 2 \leq p^d - 3$ and p does not divide $k - 2$, it follows from (18) and Lemma 4.1 that φ is linear over $\mathbb{F}_p$ and $\varphi(x) = x$.

This concludes the proof of the case $k > 3$.

Finally, we are only left to prove that the case $p^d = 9$ is an exception. Hence we need to prove that if $p = 3$ and $d = 2$, then there exist $k \in \{3, 6\}$, $x \in \mathcal{V}^*$ and a permutation φ of $\mathcal{V}$ that induces a permutation of $\mathcal{B}_k^x$ but is not an affine map. Let us consider, for instance, the case where $k = 3$, and $x = (1, 0)$. One easily finds that $\mathcal{B}_3^x$ consists of the following nine 3-subsets of $\mathcal{V} = \mathbb{F}_3^2$ (in particular, $b_3^x = 9$, in accordance with formula (3) in Proposition 2.2).

$$\begin{aligned} &\{(0, 0), (0, 1), (1, 2)\} \\ &\{(0, 0), (1, 1), (0, 2)\} \\ &\{(0, 0), (2, 1), (2, 2)\} \\ &\{(1, 0), (1, 1), (2, 2)\} \\ &\{(1, 0), (2, 1), (1, 2)\} \\ &\{(1, 0), (0, 1), (0, 2)\} \\ &\{(2, 0), (2, 1), (0, 2)\} \\ &\{(2, 0), (0, 1), (2, 2)\} \\ &\{(2, 0), (1, 1), (1, 2)\} \end{aligned}$$

Let us define an invertible map $\varphi : \mathcal{V} \rightarrow \mathcal{V}$ as follows: $\varphi(0, 0) = (0, 0)$, $\varphi(1, 0) = (2, 0)$, $\varphi(2, 0) = (1, 0)$, $\varphi(0, 1) = (0, 1)$, $\varphi(1, 1) = (2, 1)$, $\varphi(2, 1) = (1, 1)$, $\varphi(0, 2) = (2, 2)$, $\varphi(1, 2) = (1, 2)$, $\varphi(2, 2) = (0, 2)$. Then it is readily seen that φ permutes the nine blocks in $\mathcal{B}_3^x$. However, φ is not of the form $L + b$, with L linear, since this would imply that $\varphi = L + \varphi(0, 0) = L$, in contradiction with the fact that φ is not linear, as $\varphi(0, 2) = (2, 2) \neq (0, 2) = 2\varphi(0, 1)$.

This completes the proof of the theorem. $\square$

References

1. Bassalygo L.A., Zinov'ev V.A.: A note on uniformly-packed codes (in Russian). *Probl. Peredachi Inform.* **13**(3), 22–25 (1977).
2. Beth T., Jungnickel D., Lenz H.: *Design Theory*, 2nd edn. Cambridge University Press, Cambridge (1999).
3. Buratti M., Nakić A.: Super-regular Steiner 2-designs. *Finite Fields Appl.* **85**, 102116 (2023).
4. Buratti M., Nakić A.: New Series of 2-Designs Via the Method of Partial Differences, preprint
5. Caggegi A.: A new family of additive designs. *Ars. Math. Contemp.* **23**(2), #P2.07 (2023).
6. Caggegi A., Falcone G., Pavone M.: On the additivity of block designs. *J. Algebr. Comb.* **45**, 271–294 (2017).
7. Caggegi A., Falcone G., Pavone M.: Additivity of affine designs. *J. Algebr. Comb.* **53**, 755–770 (2021).
8. Colbourn C.J., Dinitz J.H.: *The CRC Handbook of Combinatorial Designs*, 2nd edn. CRC Press, Boca Raton (2007).
9. Delsarte P.: Four fundamental parameters of a code and their combinatorial significance. *Inf. Control* **23**(5), 407–438 (1973).
10. Falcone G., Pavone M.: Binary Hamming codes and Boolean designs. *Des. Codes Cryptogr.* **89**, 1261–1277 (2021).
11. Falcone G., Pavone M.: Permutations of zero-sumsets in a finite vector space. *Forum Math.* **33**(2), 349–359 (2021).
12. Li J., Wan D.: On the subset sum problem over finite fields. *Finite Fields Appl.* **14**(4), 911–929 (2008).
13. Li J., Wan D.: Counting subset sums of finite abelian groups. *J. Combin. Theory Ser. A* **119**(1), 170–182 (2012).
14. Nilov F.K., Polyanskii A.A.: A Sylvester–Gallai type theorem for abelian groups. *Math. Notes* **110**, 110–117 (2021).
15. Pavone M.: On the subset sum problem for finite fields. *Finite Fields Appl.* **76**, 101912 (2021).
16. Pavone M.: A quasidouble of the affine plane of order 4 and the solution of a problem on additive designs (under review).